ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

Кафедра высшей математики

Думачев В.Н.

ТЕОРИЯ ИНФОРМАЦИИ И КОДИРОВАНИЯ

Воронеж - 2016-06

УДК 519.72
Д82

Рассмотрены и одобрены на заседании кафедры высшей математики протокол №3 от 22.11.2011 г.

Рассмотрены и одобрены на заседании методического совета протокол №3 от 26.11.2011 г.

Д82 Думачев В.Н. Теория информации и кодирования - Воронеж: Воронежский институт МВД России, 2012. – 200 с.

Учебник содержит систематическое изложение всего материала по курсу "Теория информации и кодирования" и предназначен для выполнения типового расчета, проведения практических занятий, лабораторных работ и самоподготовки для курсантов радиотехнического факультета, обучающихся по специальности 090302.65 - Информационная безопасность телекоммуникационных систем.

Д $\frac{\textbf{1203021300 - 39}}{\textbf{221 - 08}}$ 1(III) **УДК 519.72**

Оглавление

Глава 1

Энтропия и информация

1.1 Энтропия и информация дискретных источников сообщений

Теорией информации называется наука, изучающая количественные закономерности, связанные с получением, передачей, обработкой и хранением информации. Одной из задач теории информации является отыскание наиболее экономных методов кодирования, позволяющих передать заданную информацию с помощью минимального количества символов. Эта задача решается как при отсутствии, так и при наличии искажений (помех) в канале связи.

Другая типичная задача теории информации ставится следующим образом: имеется источник информации (передатчик), непрерывно вырабатывающий информацию, и канал связи, по которому эта информация передается в другую инстанцию (приемник). Какова должна быть пропускная способность канала связи для того, чтобы канал «справлялся» со своей задачей, т.е. передавал всю поступающую информацию без задержек и искажений?

Ряд задач теории информации относится к определению объема запоминающих устройств, предназначенных для хранения информации, к способам ввода информации в эти запоминающие устройства и вывода ее для непосредственного использования.

Любое сообщение, с которым мы имеем дело в теории информации, представляет собой совокупность сведений о некоторой физической системе. Очевидно, если бы состояние физической системы было известно заранее, не было бы смысла передавать сообщение. Сообщение приобретает смысл только тогда, когда состояние системы заранее неизвестно, случайно.

Поэтому в качестве объекта, о котором передается информация, будем рассматривать некоторую физическую систему X, для которой событием будет возможность оказаться в том или ином состоянии, т. е. систему, которой заведомо присуща какая-то степень неопределенности. Интуитивно понятно, что если вероятность появления события равна 1, то само появление этого события для нас информации никакой не несет (мы и так знали, что оно появится). Например, если кто то вам скажет, что занятия в

нашем институте начинаются в 9-00, то для вас это не будет новостью, вероятность этого события равна 1 и вы не получите в этом сообщении никакой дополнительной информации о системе образования в нашем вузе. Рассмотрим другой крайний случай: допустим, стало известно, что всем двоечникам в нашем ВУЗе будут давать дополнительный отпуск и надбавку к стипендии. Вот это уже новость. Эту новость все будут друг другу пересказывать, опубликуют в газетах, возможно даже приедет телевидение. Ведь появление такого события очень маловероятно, поэтому оно очень значимо с точки зрения информации и дает огромные знания относительно того, как (оказывается) организован учебный процесс в нашем институте. Из этого примера видно, что вероятность появления события должна играть ключевую роль в формальном определении информации. В математике за меру информации принимают величину

$$I = \log_2 \left(\frac{1}{p}\right) = -\log_2 p.$$

Заметим, что в теории информации используется двоичный (битовый) логарифм

$$\mathrm{lb}\, a = \log_2 a,$$

а при практических вычислениях на ЭВМ используется натуральный логарифм $\log_e a = \ln a$. Переход от натурального основания к битовому осуществляется по формуле

$$\mathrm{lb}\, a = \log_2 a = \frac{\log_e a}{\log_e 2} = \frac{\ln a}{\ln 2}.$$

Информация о системе дается знанием того, какое именно из состояний примет данная система при проведении испытания и вычисляется по формуле

$$I = -\,\mathrm{lb} p.$$

Для случайной величины x с плотностью $f(x)$

$$I(x) = -\,\mathrm{lb} f(x).$$

Единица измерения информации называется **бит** (1 bit или 1 b). Бит – информация, хранящаяся в 1 ячейке с двумя значениями (0,1):

x	0	1
p	0.5	0.5

Тогда

$$I_0 = -\,\mathrm{lb} p_0 = -\log_2 \left(\frac{1}{2}\right) = \log_2 2 = 1\ bit,$$

$$I_1 = -\,\mathrm{lb} p_1 = -\log_2 \left(\frac{1}{2}\right) = \log_2 2 = 1\ bit.$$

Пример 1.1. Какая информация содержится в сообщении о том, что монетка упала гербом?

Решение. Вероятность того, что монетка упадет гербом, равна $p = \frac{1}{2}$. Поэтому, проведение данного испытания дало нам

$$I = -\operatorname{lb} p = -\operatorname{lb}\frac{1}{2} = \operatorname{lb} 2 = 1 \ bit$$

т.е. 1 бит информации. ▲

Пример 1.2. В ящике 10 гранат, из которых 8 без взрывателя. Из ящика наудачу выбирается 3 гранаты. Какое количество информации содержится в сообщении о том, что все 3 выбранные гранаты оказались без взрывателя?

Решение. Определим вероятность выбора из ящика 3 гранат без взрывателя:

$$p = \frac{8}{10} \cdot \frac{7}{9} \cdot \frac{6}{8} = \frac{7}{15} = 0.467.$$

Количество информации в сообщении определяется по формуле

$$I = \operatorname{lb}\left(\frac{1}{p}\right) = \operatorname{lb}\left(\frac{15}{7}\right) = 1.1 \ bit. \quad ▲$$

Пример 1.3. В группе 20 курсантов, среди которых 4 отличника, 6 хорошистов, 7 троечников, остальные – двоечники. По списку наудачу отобраны 5 курсантов. Какое количество информации содержится в сообщении о том, что среди отобранных курсантов 3 отличника, 1 хорошист и 1 троечник?

Решение. Приведем обозначения задачи в соответствие с формулой обобщенной гипергеометрической вероятности. Согласно условию задачи: N=20. Определим состав группы:

	имеем	выбираем
Отличники	$n_1 = 4$	$m_1 = 3$
Хорошисты	$n_2 = 6$	$m_2 = 1$
Троечники	$n_3 = 7$	$m_3 = 1$
Двоечники	$n_4 = 3$	$m_4 = 0$
Всего	N=20	M=5

Вспоминая, что

$$C_n^m = \frac{n!}{m!(n-m)!},$$

по формуле гипергеометрической вероятности получим

$$P = \frac{C_{n_1}^{m_1} \cdot C_{n_2}^{m_2} \cdot C_{n_3}^{m_3} \cdot C_{n_4}^{m_4}}{C_N^M} = \frac{C_4^3 \cdot C_6^1 \cdot C_7^1 \cdot C_3^0}{C_{20}^5} = \frac{7}{17 \cdot 19 \cdot 2} = 0.011.$$

Тогда количество информации есть

$$I = \text{ lb}\left(\frac{1}{P}\right) = -\text{ lb}\,(P) = -\text{ lb}0.011 = 6.528\ \ bit. \quad \blacktriangle$$

Задача 1.1.

1. В коробке 7 одинаковых деталей, причем 3 из них окрашены. Наудачу извлечены 4 изделия. Какое количество информации содержится в сообщении о том, что среди двух извлеченных изделий 2 два окрашенных.

2. В партии из 10 деталей имеется 8 стандартных. Наудачу отобраны 3 детали. Какое количество информации содержится в сообщении о том, что среди них 1 бракованная.

3. В отделе работают 6 мужчин и 4 женщины. По табельным номерам наудачу отобраны 7 человек. Какое количество информации содержится в сообщении о том, что среди отобранных лиц окажутся 3 женщины.

4. На складе имеются 15 мониторов, причем 10 из них Samsung. Какое количество информации содержится в сообщении о том, что среди 5 взятых наудачу мониторов 3 окажутся Samsung.

5. В группе 12 курсантов, среди которых 8 отличников. По списку наудачу отобраны 9 курсантов. Какое количество информации содержится в сообщении о том, что среди отобранных курсантов 5 отличников.

6. В коробке 5 одинаковых купюр, причем 3 из них помечены. Наудачу извлечены 4 купюры. Какое количество информации содержится в сообщении о том, что среди извлеченных купюр 2 помеченых.

7. В конверте среди 10 фотокарточек находится 2 разыскиваемых. Из конверта наудачу извлечены 8 карточек. Какое количество информации содержится в сообщении о том, что среди них оказалась 1 нужная.

8. В урне 7 белых и 5 черных шаров. Из урны вынимают сразу 5 шаров. Какое количество информации содержится в сообщении о том, что 2 из них будут белыми.

9. Среди 10 лотерейных билетов 3 выигрышных. Наудачу взяли 5 билетов. Какое количество информации содержится в сообщении о том, что среди них 2 выигрышных.

10. Во время гололеда на трассе М4-ДОН столкнулись 6 автомобилей, причем 3 из них - Mersedes. Инспектор ДПС наудачу оштрафовал 3 водителей. Какое количество информации содержится в сообщении о том, что среди них 2 будут водителями Mersedes.

11. Во время летнего отпуска 4 человека полетели в Турцию, а 6 - на Тайвань. Внезапно прибывший начальник решил провести совещание и вызвал из отпуска 5 человек. Какое количество информации содержится в сообщении о том, что среди них 2 прибудут из Турции.

12. В урне 3 белых, 4 черных и 5 красных шаров. Из урны вынимают сразу три шара. Какое количество информации содержится в сообщении о том, что все шары будут разного цвета.

13. В урне 5 белых, 6 черных и 7 красных шаров. Из урны вынимают сразу три шара. Какое количество информации содержится в сообщении о том, что все шары будут белые.

14. Имеются изделия четырех сортов, причем число изделий каждого сорта равно $n_1 = 2$, $n_2 = 3$, $n_3 = 1$, $n_4 = 3$. Для контроля наудачу берутся 5 изделий. Какое количество информации содержится в сообщении о том, что среди них $m_1 = 2$ первосортных, $m_2 = 1$ второго, $m_3 = 0$ третьего и $m_4 = 2$ четвертого сорта.

15. ППС задержали 6 хулиганов, причем 3 из них без российского гражданства. Наудачу вызывают 3 задержанных. Какое количество информации содержится в сообщении о том, что среди них 2 будут без гражданства.

16. На складе из 10 деталей имеется 8 нелицензионных. Наудачу отобраны 3 детали. Какое количество информации содержится в сообщении о том, что среди них 1 нелицензионная.

17. В отделе работают 8 мужчин и 4 женщины. По табельным номерам наудачу отобраны 7 человек. Какое количество информации содержится в сообщении о том, что среди отобранных лиц окажутся 4 женщины.

18. Через границу проезжает 15 КАМазов, причем 10 из них с наркотиками. Какое количество информации содержится в сообщении о том, что среди 5 проверенных наудачу КАМазов 3 окажутся с наркотиками.

19. В бандгруппе 15 боевиков, среди которых 8 вакхабитов. По списку наудачу отобраны 9 боевиков. Какое количество информации содержится в сообщении о том, что среди отобранных боевиков 5 вакхабитов.

20. В ящике 6 гранатометов, причем 3 из них российского производства. Наудачу извлечены 2 гранатомета. Какое количество информации содержится в сообщении о том, что среди двух извлеченных гранатометов 2 российских.

21. В конверте среди 10 фотокарточек находится одна разыскиваемая. Из конверта наудачу извлечены 5 карточек. Какое количество информации содержится в сообщении о том, что среди них окажется нужная.

22. На позициях стояло 8 БМП и 5 БТР. Установкой ГРАД было поражено сразу 5 единиц боевой техники. Какое количество информации содержится в сообщении о том, что 2 из них будут БМП.

23. Среди 10 олигархов было 3 депутата. Наудачу взяли 5 олигархов. Какое количество информации содержится в сообщении о том, что среди них 2 депутата.

24. В камере 3 таджика, 4 грузина и 6 азербайджанцев. Из камеры наудачу вызывают трех человек. Какое количество информации содержится в сообщении о том, что все вызываемые будут разной национальности.

25. В камере 3 таджика, 4 грузина и 6 азербайджанцев. Из камеры наудачу вызывают трех человек. Какое количество информации содержится в сообщении о том, что все вызываемые будут грузины.

26. Имеются изделия четырех сортов, причем число изделий каждого сорта равно $n_1 = 4$, $n_2 = 3$, $n_3 = 5$, $n_4 = 3$. Для контроля наудачу берутся 5 изделий. Какое количество информации содержится в сообщении о том, что среди них $m_1 = 1$ первосортных, $m_2 = 1$ второго, $m_3 = 0$ третьего и $m_4 = 3$ четвертого сорта.

1.2 Энтропия непрерывных источников сообщений

Поскольку возможные состояния $\mathbf{x} = (x_1, x_2, ..., x_n)$, случайно принимаемые системой, образуют полную группу несовместных событий, то в дальнейшем все изучаемые системы мы будем описывать некоторой случайной величиной $\mathbf{x}$ с плотностью вероятностей

$$f(x) = \sum p_i \delta(x - x_i).$$

В этом случае, за меру информации, содержащейся в значении x непрерывной случайной величины $\mathbf{x}$, принимают выражение

$$I = -\operatorname{lb} f(x).$$

Напомним, что математическое ожидание (среднее значение) случайной величины $\mathbf{x}$ вычисляется по формуле

$$M(x) = \langle x \rangle = \overline{x} = \int x \cdot f(x) dx.$$

Если случайная величина $\mathbf{x}$ является дискретной, то

$$M(x) = \int x \cdot f(x) dx = \sum \int x \cdot p_i \delta(x - x_i) dx = \sum x_i p_i = (\mathbf{x} \cdot \mathbf{p}).$$

Здесь мы воспользовались фильтрующим свойством δ-функции

$$\int f(x) \delta(x - a) dx = f(a).$$

Очевидно, сведения, полученные о системе, будут, вообще говоря, тем ценнее и содержательнее, чем больше была неопределенность системы до получения этих сведений («априори»). В качестве меры априорной неопределенности системы (или случайной величины **x**) в теории информации применяется специальная характеристика, называемая энтропией.

Энтропией $H(x)$ называется среднее количество информации, содержащееся в случайной величине **x**

$$H(x) = M(I) = \langle I \rangle = \int I \cdot f(x) dx.$$

Подставляя сюда $I = -\operatorname{lb} f(x)$, для непрерывной случайной величины получим

$$H(x) = -\int f \cdot \operatorname{lb} f \, dx,$$

а для дискретной:

$$H(x) = -\sum p_i \operatorname{lb} p_i.$$

причем $f \operatorname{lb} f = 0$, если $f = 0$.

Свойства энтропии.

1. $H(x) \geq 0$;
2. $H(x) \leq \operatorname{lb}|x|$;
3. Если **x** и **y** независимы, то $H(xy) = H(x) + H(y)$
4. Обработка информации не приводит к увеличению энтропии

$$H(g(x)) \leq H(x).$$

Энтропия является мерой неопределенности случайной величины **x**. Чем больше энтропия, тем больше неопределенности в распределении случайной величины.

Условная энтропия случайной величины **x** относительно случайной величины **y** дается выражениями

$$H(x/y) = -\sum p(x/y) \operatorname{lb} p(x/y),$$

$$H(x/y) = -\int f(x/y) \operatorname{lb} f(x/y) dx.$$

Математическое ожидание условной энтропии $M\left[H(x/y)\right]$ называется средней условной энтропией:

$$H_y(x) = M_y\left[H(x/y)\right] = \sum p(y) H(x/y) = -\sum \sum p(y) p(x/y) \operatorname{lb} p(x/y),$$

$$H_y(x) = -\iint f(y) f(x/y) \operatorname{lb} f(x/y) dx dy.$$

Количество информации о случайной величине **x**, которое может быть получено в результате наблюдения значений **y**, измеряется разностью энтропии $H(x)$ и ее средней условной энтропии относительно **y**:

$$I_y(x) = H(x) - H_y(x).$$

Если после получения сообщения о дискретной случайной величине **y** значение **x** полностью определено, то

$$H_y(x) = 0 \quad \text{и} \quad I_y(x) = H(x).$$

Если **x** и **y** независимы, то

$$H(x) = H_y(x) \quad \text{и} \quad I_y(x) = 0.$$

Отметим свойство симметрии условной информации

$$I_y(x) = I_x(y).$$

Энтропия $H(x)$, как мы увидим в дальнейшем, обладает рядом свойств, оправдывающих ее выбор в качестве характеристики степени неопределенности. Во-первых, она обращается в нуль, когда одно из состояний системы достоверно, а другие – невозможны. Во-вторых, при заданном числе состоянии она обращается в максимум, когда эти состояния равновероятны, а при увеличении числа состояний – увеличивается. Наконец, и это самое главное, она обладает свойством аддитивности, т. е. когда несколько независимых систем объединяются в одну, их энтропии складываются.

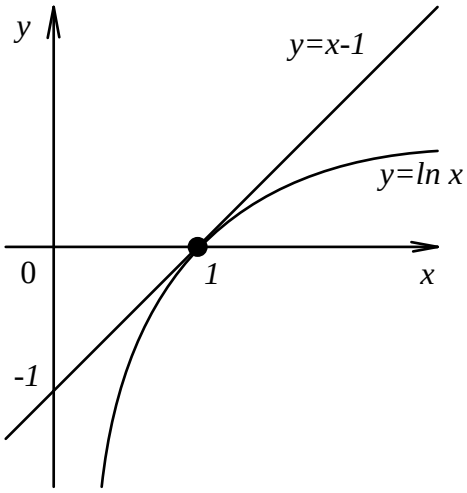
Определение 1. Среди всех законов распределения, ограниченных на интервале, наибольшую энтропию имеет равномерное.

Пример 1.4. Энтропия равномерного, на конечном интервале, распределения $\mathbf{x} = (x_1, x_2, ..., x_n)$ есть

$$H(x) = \operatorname{lb} n.$$

Действительно, поскольку вероятность всех событий данного распределения одинакова и равна $p_i = \frac{1}{n}$, то

$$H(x) = -\sum_{i=1}^{n} p_i \cdot \operatorname{lb} p_i = -\sum_{i=1}^{n} \frac{1}{n} \cdot \operatorname{lb} \frac{1}{n} = \frac{1}{n} \cdot \operatorname{lb} n \sum_{i=1}^{n} 1 = \frac{1}{n} \cdot \operatorname{lb} n \cdot n = \operatorname{lb} n. \quad \blacktriangle$$



Лемма 1. (Гиббс)
Для любых **p** и **q**, таких что

$$\sum p = 1,\ \sum q = 1$$

имеет место неравенство

$$\sum p \cdot \ \mathrm{lb} p \geq \sum p \cdot \ \mathrm{lb} q.$$

Доказательство. Из рисунка легко увидеть, что логарифмическая функция обладает простым свойством $\mathrm{lb}\, p \leq p - 1$. Тогда, для выражения

$$\sum p \cdot \ \mathrm{lb}\frac{q}{p} \leq \sum p \cdot \left(\frac{q}{p} - 1\right) = \sum p \cdot \left(\frac{q-p}{p}\right) = \sum (q-p) = \sum q - \sum p = 1 - 1 = 0,$$

получим $\sum p \cdot \ \mathrm{lb}\frac{q}{p} \leq 0$, или

$$\sum p \cdot \ \mathrm{lb}\frac{q}{p} = \sum p \cdot (\ \mathrm{lb} q - \ \mathrm{lb} p) \leq 0.$$

Отсюда следует утверждение леммы. ■

Определение 1 эквивалентно следующей теореме.

Теорема 1. Энтропия произвольной случайной величины $\mathbf{x} = (x_1, x_2, ..., x_n)$ меньше соответствующей равномерной, распределенной на том же интервале:

$$H(x) \leq \ \mathrm{lb}\, n.$$

Доказательство. Обозначим распределение **произвольной** случайной величины через $\mathbf{p} = (p_1, p_2, ..., p_n)$ а распределение **равномерной** случайной величины, через

$$\mathbf{q} = (q_1, q_2, ..., q_n) = \left(\frac{1}{n}, \frac{1}{n}, ..., \frac{1}{n}\right).$$

Тогда, по определению энтропии

$$\begin{aligned} H(x) &= -\sum p \cdot \ \mathrm{lb}\, p \leq -\sum p \cdot \ \mathrm{lb}\, q \\ &= -\sum p \cdot \ \mathrm{lb}\frac{1}{n} = \sum p \cdot \ \mathrm{lb}\, n = \ \mathrm{lb}\, n \cdot \sum p = \ \mathrm{lb}\, n \cdot 1 = \ \mathrm{lb}\, n. \end{aligned}$$ ■

Пример 1.5. Среди всех законов распределения непрерывной случайной величины **x** с одинаковой дисперсией D найти закон с максимальной энтропией.

Решение. По определению энтропии

$$H = -\int f(x)\ \mathrm{lb} f(x)dx \to \max.$$

Нам необходимо найти экстремаль функционала $H(f)$ с дополнительными ограничениями:
1) условием нормировки

$$\int f(x)dx = 1,$$

2) ограничением на дисперсию

$$\int (x-\overline{x})^2 f(x)dx = D.$$

Записывая задачу Лагранжа в виде

$$F(f,\lambda,\mu) = f\ \mathrm{lb} f + \lambda\cdot f + \mu\cdot(x-\overline{x})^2 f$$

найдем экстремум функции:

$$\frac{\partial F}{\partial f} = 0, \qquad \mathrm{lb} f + 1 + \lambda + \mu\cdot(x-\overline{x})^2 = 0,$$

откуда

$$f = e^{1-\lambda} e^{-\mu\cdot(x-\overline{x})^2}.$$

Из условия нормировки найдем

$$\int f(x)dx = e^{\lambda-1}\int e^{\mu\cdot(x-\overline{x})^2}dx = e^{\lambda-1}\sqrt{\frac{\pi}{\mu}} = 1$$

или

$$e^{1-\lambda} = \sqrt{\frac{\mu}{\pi}},$$

тогда

$$f = \sqrt{\frac{\mu}{\pi}} e^{-\mu\cdot(x-\overline{x})^2}.$$

Ограничение на дисперсию

$$\int (x-\overline{x})^2 f(x)dx = D$$

дает

$$\sqrt{\frac{\mu}{\pi}}\int (x-\overline{x})^2 e^{-\mu\cdot(x-\overline{x})^2}dx = \frac{1}{2\mu} = D$$

или

$$\mu = \frac{1}{2D},$$

тогда

$$f = \sqrt{\frac{1}{2\pi D}}\ e^{-\frac{(x-\overline{x})^2}{2D}}. \qquad \blacktriangle$$

1. Среди всех законов распределения непрерывной случайной величины $\mathbf{x}$, определенных на интервале $a \le x \le b$, найти закон распределения с максимальной энтропией. $\left(f = \frac{1}{b-a}\right)$

2. Среди всех законов распределения непрерывной случайной величины $\mathbf{x}$, определенных на полуоси $0 \le x < \infty$, при заданном математическом ожидании $M[x]$, найти закон распределения с максимальной энтропией. $\left(\frac{1}{m}e^{-\frac{x}{m}}\right)$

3. Среди всех законов распределения непрерывной случайной величины $\mathbf{x}$, при заданном втором начальном моменте μ_2, найти закон распределения с максимальной энтропией.

4. Среди всех законов распределения дискретной случайной величины $\mathbf{x}$, найти закон распределения с максимальной энтропией. $\left(p = \frac{1}{n}\right)$

Пусть теперь случайные величины $\mathbf{x} = (x_1, x_2, ..., x_n)$ и $\mathbf{y} = (y_1, y_2, ..., y_n)$ имеют совместную функцию распределения $p(x, y)$. Тогда совместная энтропия системы случайных величин x и y будет записываться как

$$H(x, y) = -\sum_x \sum_y p(x, y) \cdot \ \mathrm{lb} p(x, y).$$

Аналогичное выражение для совместной плотности вероятностей непрерывных случайных величин имеет вид

$$H(x, y) = -\iint f(x, y) \cdot \ \mathrm{lb} f(x, y) dx dy.$$

Теорема 2. Для системы случайных величин $\mathbf{x}$ и $\mathbf{y}$ имеем

$$H(x, y) \le H(x) + H(y).$$

Здесь, равенство имеет место, если $\mathbf{x}$ и $\mathbf{y}$ - независимы.

Доказательство.

Используя редуцированные законы распределения

$$p(x) = \sum_y p(x, y), \qquad p(y) = \sum_x p(x, y)$$

получим выражения

$$H(x) = -\sum_x p(x) \cdot \ \mathrm{lb}\, p(x) = -\sum_y \sum_x p(x, y) \cdot \ \mathrm{lb}\, p(x),$$

$$H(y) = -\sum_y p(y) \cdot \ \mathrm{lb}\, p(y) = -\sum_x \sum_y p(x,y) \cdot \ \mathrm{lb}\, p(y).$$

Тогда

$$\begin{aligned} H(x) + H(y) &= -\sum_y \sum_x p(x,y) \cdot (\ \mathrm{lb}\, p(x) + \ \mathrm{lb}\, p(x)) \\ &= -\sum_y \sum_x p(x,y) \cdot \ \mathrm{lb}\, (p(x)p(y)) = -\sum_y \sum_x p(x,y) \cdot \ \mathrm{lb}\, q(xy). \end{aligned}$$

Здесь мы ввели обозначение $q(xy) = p(x)p(y)$. Теперь, используя лемму Гиббса, получим

$$H(x,y) = -\sum_x \sum_y p(x,y) \cdot \ \mathrm{lb}\, p(x,y) \le -\sum_x \sum_y p(x,y) \cdot \ \mathrm{lb}\, q(x,y) = H(x) + H(y). \qquad \blacksquare$$

Очевидным способом можно доказать обобщение этой теоремы

$$H(x_1, x_1, ..., x_n) \le H(x_1) + H(x_2) + ... + H(x_n),$$

где равенство имеет место, если $(x_1, x_1, ..., x_n)$ - независимы.

1.3 Условная энтропия

Для системы двух случайных величин с совместной вероятностью $p(x,y)$ можно ввести условную вероятность $p(x|y)$. В частности: $p(x|y_i)$ - закон распределения случайной величины **x** при условии, что **y** принимает конкретное значение y_i (аналогично для $p(y|x_i)$.

Таким образом, мы можем определить условную энтропию **y** данную при $x = x_i$:

$$H(y|x = x_i) = H(y|x_i) = -\sum_k p(y_k|x_i) \cdot \ \mathrm{lb} p(y_k|x_i),$$

И среднюю условную энтропию **y** относительно **x**:

$$H(y|x) = \sum_i p(x_i) H(y|x_i) = -\sum_i p(x_i) \sum_k p(y_k|x_i) \cdot \ \mathrm{lb} p(y_k|x_i).$$

Поскольку из теории вероятностей известно, что

$$p(y,x) = p(x)p(y|x),$$

мы получим

$$H(y|x) = \sum_i p(x_i) H(y|x_i) = -\sum_i \sum_k p(x_i, y_k) \cdot \ \mathrm{lb} p(y_k|x_i).$$

Аналогично, можно определить энтропию

$$H(x,y,z) = -\sum_i \sum_k \sum_n p(x_i, y_k, z_n) \cdot \ \mathrm{lb} p(x_i, y_k, z_n)$$

и среднюю условную энтропию системы из трех случайных величин

$$H(yz|x) = -\sum_i \sum_k \sum_n p(x_i, y_k, z_n) \cdot \ \mathrm{lb} p(x_i, y_k|x_n).$$

Очень часто бывает полезной следующая

Теорема 3.

$$H(x,y) = H(x) + H(y|x) = H(y) + H(x|y)$$

Доказательство. По определению

$$\begin{aligned} H(x,y) &= -\sum_x \sum_y p(x,y) \cdot \ \mathrm{lb} p(x,y) = -\sum_x \sum_y p(x,y) \cdot \ \mathrm{lb} p(x) p(y|x) \\ &= -\sum_x \sum_y p(x,y) \cdot \ \mathrm{lb} p(x) - \sum_x \sum_y p(x,y) \cdot \ \mathrm{lb} p(y|x) \\ &= -\sum_x p(x) \cdot \ \mathrm{lb} p(x) - \sum_x p(x) \sum_y p(y|x) \cdot \ \mathrm{lb} p(y|x) = H(x) + H(y|x). \quad \blacksquare \end{aligned}$$

Теорема 4.

$$H(y|x) \le H(y)$$

Доказательство. По определению

$$H(x,y) = H(x) + H(y|x), \qquad H(y|x) = H(x,y) - H(x).$$

Но согласно **теореме 2**

$$H(x,y) \le H(x) + H(y)$$

или

$$H(x,y) - H(x) \le H(y),$$

тогда

$$H(y|x) = H(x,y) - H(x) \le H(y). \quad \blacksquare$$

Условная энтропия случайной величины **x** относительно случайной величины **y** дается выражениями

$$H(x/y) = -\sum p(x/y) \ \mathrm{lb} p(x/y),$$

$$H(x/y) = -\int f(x/y) \ \mathrm{lb} f(x/y) dx.$$

Математическое ожидание условной энтропии $M\left[H(x/y)\right]$ называется средней условной энтропией:

$$H_y(x) = M_y\left[H(x/y)\right] = \sum p(y) H(x/y) = -\sum \sum p(y) p(x/y) \ \mathrm{lb} p(x/y),$$

$$H_y(x) = -\iint f(y)f(x/y)\ \mathrm{lb} f(x/y)dxdy.$$

Количество информации о случайной величине **x**, которое может быть получено в результате наблюдения значений **y**, измеряется разностью энтропии $H(x)$ и ее средней условной энтропии относительно **y**:

$$I_y(x) = H(x) - H_y(x).$$

Если после получения сообщения о дискретной случайной величине **y** значение **x** полностью определено, то

$$H_y(x) = 0 \qquad \text{и} \qquad I_y(x) = H(x).$$

Если **x** и **y** независимы, то $H(x) = H_y(x)$ и $I_y(x) = 0$.

Отметим свойство симметрии условной информации

$$I_y(x) = I_x(y).$$

Пример 1.6. Производится стрельба по двум мишеням: по первой мишени сделано 2 выстрела, по второй три. Вероятности попадания при одном выстреле соответственно равны $1/2$ и $1/4$. Исход стрельбы по какой мишени является более определенным.

Решение. Составляем законы распределения для случайных величин **x** и **y** - числа попаданий по мишени:

x	0	1	2
p	1/4	1/2	1/4

y	0	1	2	3
p	27/64	27/64	9/64	1/64

Мерой неопределенности исхода стрельб является энтропия числа попаданий:

$$H = -\sum p_i\ \mathrm{lb} p_i$$

$$\begin{aligned}
H_1 &= -\left(\frac{1}{4}\cdot\ \mathrm{lb}\frac{1}{4} + \frac{2}{4}\cdot\ \mathrm{lb}\frac{2}{4} + \frac{1}{4}\cdot\ \mathrm{lb}\frac{1}{4}\right) \\
&= -\frac{1}{4}\left(1\cdot\ \mathrm{lb}1 + 2\cdot\ \mathrm{lb}2 + 1\cdot\ \mathrm{lb}1\right) + \ \mathrm{lb}4 = -\frac{1}{4}\left(0 + 2 + 0\right) + 2 = 1.5; \\
H_2 &= -\left(\frac{27}{64}\cdot\ \mathrm{lb}\frac{27}{64} + \frac{27}{64}\cdot\ \mathrm{lb}\frac{27}{64} + \frac{9}{64}\cdot\ \mathrm{lb}\frac{9}{64} + \frac{1}{64}\cdot\ \mathrm{lb}\frac{1}{64}\right) \\
&= \ \mathrm{lb}64 - \frac{1}{64}\left(27\cdot\ \mathrm{lb}27 + 27\cdot\ \mathrm{lb}27 + 9\cdot\ \mathrm{lb}9 + 1\cdot\ \mathrm{lb}1\right) \\
&\cong\ 6 - \frac{1}{64}\left(27\cdot 4.75 + 27\cdot 4.75 + 9\cdot 3.17 + 1\cdot 0\right) = 4.45.
\end{aligned}$$

Поскольку $H_1 < H_2$ - то исход стрельбы по первой мишени обладает большей определенностью. ▲

Задача 1.2. В двух урнах по $\mathbf{n}$ шаров, причем в первой урне $\mathbf{k}_1$ красных, $\mathbf{b}_1$ белых и $\mathbf{c}_1$ черных, а во второй соответственно – $\mathbf{k}_2$, $\mathbf{b}_2$ и $\mathbf{c}_2$. Из каждой урны вынимается по одному шару. Определить, для какой урны исход опыта является более определенным.

№	$\mathbf{k}_1$	$\mathbf{b}_1$	$\mathbf{c}_1$	$\mathbf{k}_2$	$\mathbf{b}_2$	$\mathbf{c}_2$	№	$\mathbf{k}_1$	$\mathbf{b}_1$	$\mathbf{c}_1$	$\mathbf{k}_2$	$\mathbf{b}_2$	$\mathbf{c}_2$
1	10	5	5	7	7	6	**16**	1	15	4	15	5	0
2	12	4	4	6	6	8	**17**	2	14	4	14	6	0
3	14	2	2	8	8	4	**18**	3	13	4	13	5	2
4	1	16	1	10	5	5	**19**	4	12	4	12	4	4
5	18	0	2	5	12	3	**20**	5	11	4	11	3	6
6	4	8	8	1	10	9	**21**	6	10	4	10	2	8
7	5	4	11	2	8	10	**22**	7	9	4	9	1	10
8	6	3	11	3	7	10	**23**	8	8	4	8	2	10
9	7	2	11	4	6	10	**24**	9	7	4	7	3	10
10	5	10	5	6	7	7	**25**	10	6	4	6	14	0
11	8	1	11	5	2	13	**26**	11	5	4	5	13	2
12	9	2	9	7	3	10	**27**	12	4	4	4	12	4
13	10	3	7	8	4	8	**27**	13	3	4	3	11	6
14	11	4	5	8	5	7	**29**	14	2	4	2	10	8
15	5	5	10	7	6	7	**30**	15	1	4	1	9	10

Дополнительные упражнения

1. В правильный n-угольник путем соединения середин его соседних сторон вписан другой правильный n-угольник. Точка, поставленная внутри данного многоугольника может оказаться внутри или вне вписанного многоугольника. Определить. а) энтропию опыта; б) значение n, при котором энтропия максимальна. ($P_n = \cos^2 \pi/n$)

2. Вероятность появления события при одном испытании равна p. Испытания повторяются до первого появления события. Найти энтропию числа испытаний. а) $p = 1/2$; б) в общем случае. $\left(H = -\frac{(p \operatorname{lb} p + q \operatorname{lb} q)}{p}\right)$

3. Определить энтропию случайной величины, подчиненной биноминальному закону распределения: а) $p = 1/2$, $n = 2$; б) в общем случае.

4. Определить энтропию непрерывной случайной величины подчиненной равномерному закону распределения на (a, b). ($\operatorname{lb}(b - a)$)

5. Определить энтропию непрерывной случайной величины подчиненной нормальному закону распределения.

1.4 Задачи информационного поиска

Энтропия H – удобная мера неопределённости законов распределения вероятностей, особенно в тех случаях, когда распределения являются асимметричными, многовершинными и когда использование таких числовых характеристик, как среднее значение, дисперсия и моменты высших порядков, теряет всякую наглядность.

Приведем выражения для энтропии некоторых дискретных законов распределения вероятностей:

Биномиальный $P_n(k) = C_n^k p^k q^{n-k}$

$$H(x) = -n[p\ln p + q\ln q] - \sum_{k=1}^{n-1} C_n^k p^k q^{n-k} \ln C_n^k$$

Пуассона $P_n(k) = \frac{\lambda^k}{k!} e^{-\lambda}$

$$H(x) = \lambda \ln \frac{e}{\lambda} + \sum_{k=1}^{\infty} \frac{\lambda^k}{k!} e^{-\lambda} \ln(k!)$$

Равномерный $P_n(k) = \frac{1}{n}$

$$H(x) = \text{ lb}n$$

Полиа $P_n(k) = P_0 \left(\frac{\lambda}{1+\alpha\lambda}\right)^k \times \frac{1(1+\alpha)...[1+(k-1)\alpha]}{k!}$

$$\begin{aligned} H(x) &= -\lambda\ln\lambda + \frac{1+\alpha\lambda}{\alpha}\ln(1+\alpha\lambda) \\ &- \sum_{k=1}^{\infty} P_0 \left(\frac{\lambda}{1+\alpha\lambda}\right)^k \frac{1(1+\alpha)...[1+(k-1)\alpha]}{k!} \times \ln \frac{1(1+\alpha)...[1+(k-1)\alpha]}{k!} \end{aligned}$$

Особенно эффективным является использование метода расчета энтропии при решении задач многошагового информационного поиска. Результаты каждого шага поиска образуют полную группу событий, т.е. случайную величину **x**. Необходимо выбрать такую стратегию поиска, что бы каждый шаг давал максимальное количество информации об исследуемом объекте. Поскольку среди всех законов распределения максимальной энтропией (информацией) обладает равномерный закон, то поиск необходимо производить таким образом, чтобы случайная величина **x** была распределена равномерно.

Пример 1.7. Имеется 3 монеты одного достоинства; 1 из них фальшивая. Какое наименьшее число взвешиваний на рычажных весах без гирь, позволит обнаружить фальшивую монету и выяснить, легче она или тяжелее чем остальные?

Решение. Каждая из 3 монет может оказаться фальшивой и быть при этом тяжелее или легче остальных. Таким образом имеется $N = 2 \cdot 3 = 6$ возможных исходов. Поэтому выбор отдельно взятой монеты дает информацию, равную

$$I = -\text{ lb}p = -\text{ lb}\frac{1}{N} = -\text{ lb}\frac{1}{6} = \text{ lb}6 \approx 2.585 \; bit.$$

Каждое взвешивание имеет 3 исхода: перевешивает левая чаша, правая чаша и равновесие. Поэтому произвольное единичное взвешивание дает информацию

$$I_0 = -\,\mathrm{lb}\frac{1}{3} = \mathrm{lb}3 \approx 1.6\ bit.$$

Следовательно, минимальное число взвешиваний не может быть меньше, чем

$$n = \frac{I}{I_0} = \frac{\mathrm{lb}6}{\mathrm{lb}3} = \frac{2.585}{1.6} \approx 1.631 \approx 2,$$

т.е. оно не меньше двух.

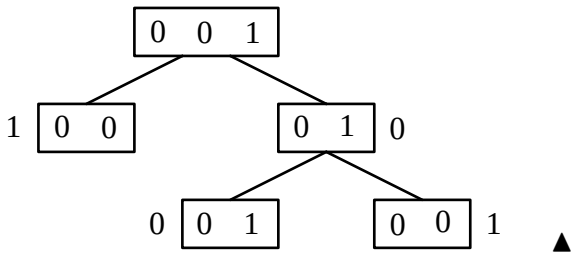
Схема решения этой задачи следующая.
Положим на обе чашки по 1 монетке.

1. Если весы остались в равновесии, то фальшивая монета осталась одна на столе и нам необходимо еще одно взвешивание чтобы определить легче она или тяжелее настоящей.

2. Если весы не в равновесии, то мы меняем монету с любой чашки на настоящую.

   (a) Если весы в равновесии – то фальшивая на столе.

   (b) Если весы не в равновесии – то фальшивая осталась на весах.



▲

Пример 1.8. Имеется 4 монеты одного достоинства; 1 из них фальшивая. Какое наименьшее число взвешиваний на рычажных весах без гирь, позволит обнаружить фальшивую монету и выяснить, легче она или тяжелее чем остальные?

Решение. Каждая из 4 монет может оказаться фальшивой и быть при этом тяжелее или легче остальных. Таким образом имеется $N = 2 \cdot 4 = 8$ возможных исходов. Поэтому выбор отдельно взятой монеты дает информацию, равную

$$I = -\,\mathrm{lb}p = -\,\mathrm{lb}\frac{1}{N} = -\,\mathrm{lb}\frac{1}{8} = \mathrm{lb}8 \simeq 3\ bit.$$

Каждое взвешивание имеет 3 исхода: перевешивает левая чаша, правая чаша и равновесие. Поэтому произвольное единичное взвешивание дает информацию

$$I_0 = -\,\mathrm{lb}\frac{1}{3} = \mathrm{lb}3 \simeq 1.6\ bit.$$

Следовательно, минимальное число взвешиваний не может быть меньше, чем

$$n = \frac{I}{I_0} = \frac{\text{lb}8}{\text{lb}3} = \frac{3}{1.6} \approx 1.893 \simeq 2,$$

т.е. оно не меньше двух (с точки зрения теории информации). К сожалению, пока не известен алгоритм решения этой задачи с помощью 2-ух взвешиваний. ▲

Пример 1.9. (Для продвинутых пользователей.) Теперь докажем, что решение предыдущей задачи с помощью 2-ух взвешиваний невозможно. Для этого вычислим реальное количество информации, получаемое нами при первом взвешивании. Оно зависит от стратегии взвешивания. Мы можем положить на обе чашки весов по 2 монеты и по 1 монете. Напомним, что $I_0 = \text{lb}3 \simeq 1.585\ bt$ это максимальная информация о системе, которую мы можем получить с помощью одного взвешивания.

Рассмотрим 1 стратегию. Пусть **x** - положение чашки весов при взвешивании $x = (-1;\ 0;\ 1)$. Поскольку при первом взвешивании на обе чашки положено по 2 монеты, то весы не смогут остаться в равновесиии и мы имеем три возможные исхода с вероятностями:

1) $x = -1$ - перевесила левая чашка, p(-1)=1/2;
2) $x = 0$ - чашки остались в равновесии, p(0)=0;
3) $x = 1$ - перевесила правая чашка, p(1)=1/2.

Построим таблицу распределения случайной величины **x**

x	-1	0	1
p	1/2	0	1/2

и найдем ее энтропию

$$H = -\left(\frac{1}{2}\,\text{lb}\frac{1}{2} + 0\cdot\ \text{lb}0 + \frac{1}{2}\,\text{lb}\frac{1}{2}\right) = \ \text{lb}2 = 1\ bt.$$

Т.е. мы получили 1 bt. информации, а энтропия системы была 3 bt. Т.е. с помощью взвешивания мы уменьшили неопределенность системы до 2 bt. и у нас осталось еще одно взвешивание, которое в идеале может дать только $\text{lb}3 \simeq 1.585\ bt$. Очевидно что оставшегося взвешивания нам недостаточно для решения задачи.

Рассмотрим другую стратегию. Положим на обе чашки по 1 монете. Тогда результат взвешивания дает три возможных исхода с вероятностями:

1) $x = -1$ - перевесила левая чашка, p(-1)=1/4;
2) $x = 0$ - чашки остались в равновесии, p(0)=1/2;
3) $x = 1$ - перевесила правая чашка, p(1)=1/4.

Построим таблицу распределения случайной величины **x**

x	-1	0	1
p	1/4	1/2	1/4

и найдем ее энтропию

$$H = -\left(\frac{1}{4}\,\mathrm{lb}\frac{1}{4} + \frac{1}{2}\,\mathrm{lb}\frac{1}{2} + \frac{1}{4}\,\mathrm{lb}\frac{1}{4}\right) = 1.5\ bt.$$

Т.е. нам осталось получить еще 1.5 bt. информации о системе с помощью одного оставшегося взвешивания. В принципе, это возможно, поскольку при удаче одно взвешивание может нам дать $\mathrm{lb}3 \simeq 1.585\ bt.$ информации.

Если в результате первого взвешивания одна из чашек перевесила, то мы точно знаем, что на столе лежат настоящие монеты. Меняя одну любую монету на весах с настоящей мы получим таблицу распределения для второго взвешивания

x	-1	0	1
p	1/4	1/2	1/4

с энтропией

$$H = 1.5\ bt.$$

Т.е. задача решена.

Однако, если в результате первого взвешивания чашки весов остались в равновесии, то фальшивая монета осталась на столе. Но для того, чтобы определить ее необходимо

$$n = \frac{I}{I_0} = \frac{\mathrm{lb}4}{\mathrm{lb}3} \approx 1.262 > 1,$$

т.е. больше одного взвешивания[1]. ▲

Пример 1.10. Имеется 5 монет одного достоинства; 1 из них фальшивая. Какое наименьшее число взвешиваний на рычажных весах без гирь, позволит обнаружить фальшивую монету и выяснить, легче она или тяжелее чем остальные?

Решение. Каждая из 5 монет может оказаться фальшивой и быть при этом тяжелее или легче остальных. Таким образом имеется $N = 2 \cdot 5 = 10$ возможных исходов. Поэтому выбор отдельно взятой монеты дает информацию, равную

$$I = -\,\mathrm{lb}p = -\,\mathrm{lb}\frac{1}{N} = -\,\mathrm{lb}\frac{1}{10} = \mathrm{lb}10 \approx 3.322\ bit.$$

Каждое взвешивание имеет 3 исхода: перевешивает левая чаша, правая чаша и равновесие. Поэтому произвольное единичное взвешивание дает информацию

$$I_0 = -\,\mathrm{lb}\frac{1}{3} = \mathrm{lb}3 \approx 1.6\ bit.$$

Следовательно, минимальное число взвешиваний не может быть меньше, чем

$$n = \frac{I}{I_0} = \frac{\mathrm{lb}10}{\mathrm{lb}3} = \frac{3.322}{1.6} \approx 2.096 < 3,$$

т.е. оно не меньше трех.

Схема решения этой задачи следующая. Положим на обе чашки по 1 монетке.

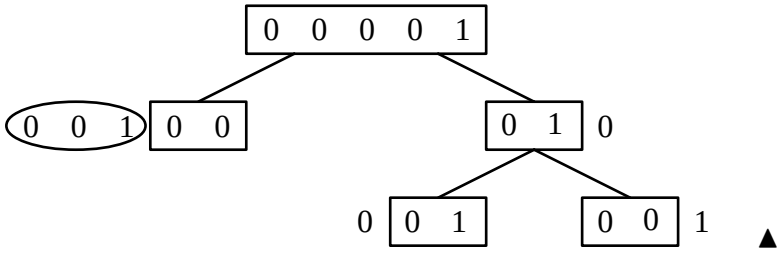
[1]Мы сможем найти фальшивую монету, но не сможем определить легче она или тяжелее настоящих.

1. Если весы остались в равновесии, то фальшивая монета осталась среди 3 подозрительных на столе и нам достаточно еще 2 взвешиваний чтобы ее идентифицировать (см. задачу о 3 монетах).

2. Если весы не в равновесии, то мы меняем монету с любой чашки на настоящую со стола.

   (a) Если весы в равновесии – то фальшивая на столе.

   (b) Если весы не в равновесии – то фальшивая осталась на весах.



Пример 1.11. Имеется 6 монет одного достоинства; 1 из них фальшивая. Какое наименьшее число взвешиваний на рычажных весах без гирь, позволит обнаружить фальшивую монету и выяснить, легче она или тяжелее чем остальные?

Решение. Минимальное число взвешиваний не может быть меньше, чем

$$n = \frac{I}{I_0} = \frac{\text{lb}12}{\text{lb}3} = \log_3 12 \approx 2.262 < 3,$$

т.е. оно не меньше трех.

Схема решения этой задачи следующая.

Определим количество монет которое необходимо положить на весы при первом взвешивании, т.е. рассчитаем стратегию взвешивания используя методы теории информации. Чтобы число взвешиваний было наименьшим, каждое взвешивание должно давать наибольшее количество информации, т.е. исход взвешивания должен обладать наибольшей энтропией. Введем случайную величину $\mathbf{x}$ положение чашки весов при взвешивании $x = (-1;\ 0;\ 1)$.

Пусть при первом взвешивании на обе чашки положено по i монет. При этом возможны три исхода:

1. $x = -1$ - перевесила левая чашка;

2. $x = 0$ - чашки остались в равновесии;

3. $x = 1$ - перевесила правая чашка;

Построим таблицу распределения случайной величины x

	x	-1	0	1
$i=1$	**p**	$1/6$	$4/6$	$1/6$
$i=2$	**p**	$2/6$	$2/6$	$2/6$
$i=3$	**p**	$3/6$	0	$3/6$

Чтобы взвешивание дало наибольшую информацию, распределение вероятностей исходов должно обладать наибольшей энтропией, чему соответствует равенство всех вероятностей исходов (равномерный закон распределения **x**). В нашем случае максимальной энтропией обладает распределение при $i = 2$.

При первом взвешивании на каждую чашку весов следует положить по 2 монеты.

Далее рассмотрим отдельно случаи:

1. Если весы остались в равновесии, то на весах мы имеем 4 настоящих, а фальшивая монета осталась среди 2 подозрительных на столе и нам достаточно еще 2 взвешиваний чтобы ее идентифицировать, (см. задачу о 3 монетах).

2. Если весы не в равновесии, то мы берем 2 монеты с одной из чашек и взвешиваем их.

   (a) Если весы в равновесии – то фальшивая на столе и мы знаем ее вес. Одним взвешиванием мы ее идентифицирум.

   (b) Если весы не в равновесии – то фальшивая осталась на весах и по предыдущему взвешиванию мы знаем ее вес (больше или меньше настоящей). Одним взвешиванием мы ее идентифицирум. ▲

Пример 1.12. Имеется 12 монет одного достоинства; 11 из них имеют одинаковый вес, а одна – фальшивая. Какое наименьшее число взвешиваний на рычажных весах без гирь, позволит обнаружить фальшивую монету и выяснить, легче она или тяжелее чем остальные?

Решение. Каждая из 12 монет может оказаться фальшивой и быть при этом тяжелее или легче остальных. Таким образом имеется $N = 2 \cdot 12 = 24$ возможных исхода. Поэтому выбор отдельно взятой монеты дает информацию, равную

$$I = -\operatorname{lb} p = -\operatorname{lb}\frac{1}{N} = -\operatorname{lb}\frac{1}{24} = \operatorname{lb}24 \approx 4.6 \; bit.$$

Каждое взвешивание имеет 3 исхода: перевешивает левая чаша, правая чаша и равновесие. Поэтому произвольное единичное взвешивание дает информацию

$$I_0 = -\operatorname{lb}\frac{1}{3} = \operatorname{lb}3 \approx 1.6 \; bit.$$

Следовательно, минимальное число взвешиваний не может быть меньше, чем

$$n = \frac{I}{I_0} = \frac{\text{lb}24}{\text{lb}3} = \frac{4.6}{1.6} \approx 2.875 \approx 3,$$

т.е. оно не меньше трех.

Напомним решение этой задачи классическим методом дискретной математики. Для этого предлагается стратегия последовательного парного разбиения с

$$\text{lb}12 \approx 3.57 \cong 4$$

взвешиваниями:

1. положить на обе чашки по 6 монет;
2. положить на обе чашки по 3 монеты;
3. положить на обе чашки по 1 монете;
4. определить вес монеты (легче или тяжелее настоящей).

Теперь рассчитаем стратегию взвешивания используя методы теории информации. Чтобы число взвешиваний было наименьшим, каждое взвешивание должно давать наибольшее количество информации, т.е. исход взвешивания должен обладать наибольшей энтропией. Введем случайную величину $\mathbf{x}$ положение чашки весов при взвешивании $\mathbf{x} = (-1;\ 0;\ 1)$.

Пусть при первом взвешивании на обе чашки положено по i монет. При этом возможны три исхода:

1. $x = -1$ - перевесила левая чашка;
2. $x = 0$ - чашки остались в равновесии;
3. $x = 1$ - перевесила правая чашка;

Построим таблицу распределения случайной величины $\mathbf{x}$

x_i	-1	0	1
p_i	$\frac{i}{12}$	$\frac{12-2i}{12}$	$\frac{i}{12}$

Чтобы взвешивание дало наибольшую информацию, распределение вероятностей исходов должно обладать наибольшей энтропией, чему соответствует равенство всех вероятностей исходов (равномерный закон распределения $\mathbf{x}$). Отсюда

$$\frac{12-2i}{12} = \frac{i}{12}, \quad \text{или} \quad i = 4.$$

Взвешивание 1: при первом взвешивании на каждую чашку весов следует положить по 4 монеты.

Далее рассмотрим отдельно случаи:
2.1. когда при первом взвешивании чашки весов остались в равновесии;
2.2. когда одна из чашек перевесила другую.

В случае 2.1. имеем 8 настоящих и 4 подозрительных монет. Для второго взвешивания мы можем положить на правую чашку i подозрительных монет, а на левую k подозрительных и $i-k$ настоящих. Все возможные значения, соответствующие вероятности исходов и энтропию случайной величины $\mathbf{x}$ сведем в таблицу

№	i	k	p_1	p_2	p_3	$H_{ik}[x]$
1	1	1	0.25	0.5	0.25	0.452
2	1	0	0.125	0.75	0.125	0.320
3	2	2	0.5	0	0.5	0.301
4	2	1	0.375	0.25	0.375	0.470
5	2	0	0.25	0.5	0.25	0.452
6	3	1	0.5	0	0.5	0.301
7	3	0	0.375	0.25	0.375	0.470
8	4	0	0.5	0	0.5	0.301

Наибольшую энтропию дают опыты 4 и 7. Выберем для примера взвешивание 7, т.е. на первую чашку ложем 3 подозрительные монеты, а на другую 3 настоящие. Здесь возможны 2 случая:
2.1.1. если весы окажутся в равновесии, то фальшивая монета останется одна и необходимо дополнительное 3 взвешивание для определения ее веса;
2.1.2. если чаша перевесила, то вес фальшивой монеты определен, из 1 чаши выбирается 2 монеты и на 3 взвешивании она обнаруживается.

В случае 2.2., когда одна из чашек перевесила другую (для определенности - левая), монеты распределяются следующим образом:

1. 4 левых (группа L);
2. 4 правых (группа R);
3. 4 настоящих (группа O).

При втором взвешивании мы можем положить:

1. на левую чашку весов - i_1 левых и i_2 правых;
2. на правую чашку весов - j_1 левых, j_2 правых и остальные настоящие.

Сравнивая все возможные 25 вариантов выберем из них случай с максимальной энтропией. Например, для второго взвешивания подойдет:

$$i_1 = 1,\ \ i_2 = 2,\ \ j_1 = 0,\ \ j_2 = 2.$$

Здесь тоже возможны 3 случая:

а) весы в равновесии;
б) перевешивает левая чашка;
в) перевешивает правая чашка.
В случае а) - равновесия мы точно знаем вес фальшивки (тяжелая фальшивка), а сама фальшивка находится в трех оставшихся монетах группы L. Третьего взвешивания в составе 1:1 из монет группы L нам достаточно, чтобы ее обнаружить.

В случае б): Третье взвешивание есть разбиение $j_2 = 2$ в составе 1:1 на обе чашки весов:

1. Если весы в равновесии, то $i_1 = 1$ - тяжелая фальшивка из группы L;
2. Если перевесила левая чашка, то из $j_2 = 2$ правая – легкая фальшивка R;
3. Если перевесила правая чашка, то из $j_2 = 2$ левая – легкая фальшивка R.

В случае в): легкая фальшивка из группы R находится в $i_2 = 2$. Третье взвешивание есть разбиение $i_2 = 2$ в составе 1:1 на обе чашки весов и определение фальшивки по верхней чашке. ▲

Дополнительные упражнения

1. Имеется N монет одного достоинства, из которых одна фальшивая, несколько легче остальных. Сколькими взвешиваниями на рычажных весах без гирь можно обнаружить фальшивую монету? При каком наибольшем N достаточно пяти взвешиваний? $(3^{k-1} < 2N < 3^{k-1})$
2. Неисправная система находится в одном из 5 различных состояний, которым соответствуют различные виды неисправностей. Для обнаружения вида неисправности может быть проведено несколько из 7 возможных проверок, приводящих при различных состояниях системы к тому, что контрольный индикатор загорается или не загорается. В приведенной таблице это обозначается соответственно единицей или нулем.

№ проверки	№ состояния				
	1	2	3	4	5
1	0	0	0	0	1
2	0	0	0	1	1
3	0	1	1	0	0
4	1	0	1	0	0
5	1	0	1	0	1
6	1	1	1	0	0
7	1	1	1	1	0

Составить последовательность из минимального числа проверок, позволяющих определить вид неисправности системы.

1.5 Взаимная информация

Количество информации, которое может быть получено в результате наблюдения полной группы несовместных событий, измеряется ее энтропией

$$I(x|y) = H(x) - H(x|y), \qquad I(y|x) = H(y) - H(y|x),$$

$$I(x|y) = H(x) + H(y) - H(x,y) = I(y|x).$$

Рассмотрим следующий эксперимент.

Пример 1.13. Во время эксперимента в течение 8 дней проводилось измерение случайной величины **x** - отклонение курса доллара от значения в 33 рубля/доллар. Данные измерения показаны в таблице.

№ измерения	1	2	3	4	5	6	7	8
значение **x**	0	0	0	1	0	0	0	1

Одновременно проводилось измерение случайной величины **y** - отклонение дневной температуры на улице от 0°C:

№ измерения	1	2	3	4	5	6	7	8
значение **y**	0	0	0	0	0	1	1	1

Определить количество информации относительно **y** которое мы получим измеряя **x**.

Решение. Другими словами нам необходимо определить взаимную информацию:

$$I(x|y) = H(x) + H(y) - H(x,y).$$

Запишем данные измерения в одну таблицу

значение **x**	0	0	0	1	0	0	0	1
значение **y**	0	0	0	0	0	1	1	1

и подсчитаем количество совпадений значений **x** и **y**:

x \ **y**	0	1
0	4	2
1	1	1

Если теперь разделить все данные в таблице на 8, то мы получим таблицу совместного распределения случайных величин **x** и **y**:

x \ **y**	0	1
0	1/2	1/4
1	1/8	1/8

Взяв суммы по строкам и столбцам найдем редуцированные законы распределений случайных величин **x** и **y**:

x \ **y**	0	1	p_x
0	1/2	1/4	3/4
1	1/8	1/8	1/4
p_y	5/8	3/8	1

Вычисляем энтропию

$$H(x) = -\sum p_x \cdot \ \mathrm{lb} p_x = -\left(\frac{3}{4}\,\mathrm{lb}\frac{3}{4} + \frac{1}{4}\,\mathrm{lb}\frac{1}{4}\right) = 0.811$$

$$H(y) = -\sum p_y \cdot \ \mathrm{lb} p_y = -\left(\frac{5}{8}\,\mathrm{lb}\frac{5}{8} + \frac{3}{8}\,\mathrm{lb}\frac{3}{8}\right) = 0.954$$

$$H(x,y) = -\sum p_{xy} \cdot \ \mathrm{lb} p_{xy} = -\left(\frac{1}{2}\,\mathrm{lb}\frac{1}{2} + \frac{1}{8}\,\mathrm{lb}\frac{1}{8} + \frac{1}{4}\,\mathrm{lb}\frac{1}{4} + \frac{1}{8}\,\mathrm{lb}\frac{1}{8}\right) = 1.75$$

и взаимную информацию.

$$I(x|y) = H(x) + H(y) - H(x,y) = 0.811 + 0.954 - 1.75 = 0.015(bit). \quad \blacktriangle$$

Заметим, что теория вероятностей также дает влияние случайной величины **x** на случайную величинц **y** с помощью коэффициента корреляции

$$r = \frac{\langle xy\rangle - \langle x\rangle\,\langle y\rangle}{\sigma_x \sigma_y}.$$

Учитывая, что

$$\langle x\rangle = \left\langle x^2\right\rangle = 1/4, \quad \langle y\rangle = \left\langle y^2\right\rangle = 3/8,$$

$$D_x = \left\langle x^2\right\rangle - \langle x\rangle^2 = 3/16, \quad D_y = \left\langle y^2\right\rangle - \langle y\rangle^2 = 15/64,$$

получим

$$r = \frac{\langle xy\rangle - \langle x\rangle\,\langle y\rangle}{\sqrt{D}_x\sqrt{D}_y} = \frac{1/8 - 1/4\cdot 3/8}{\sqrt{3/16}\,\sqrt{15/54}} = 0.149.$$

Другими словами, мы получили ненулевое значение влияния курса доллора на погоду. Очевидно, что к таким расчетам необходимо относится с осторожностью (с чувством юмора).

Для независимых случайных величин $\langle xy\rangle = \langle x\rangle\,\langle y\rangle$, поэтому коэффициент корреляции

$$r = \frac{\langle xy\rangle - \langle x\rangle\,\langle y\rangle}{\sigma_x\sigma_y} = \frac{\langle x\rangle\,\langle y\rangle - \langle x\rangle\,\langle y\rangle}{\sigma_x\sigma_y} = 0.$$

Если же случайные величины **x** и **y** линейно зависимы: $y = ax + b$, то для них

$$\begin{aligned}
\langle y\rangle &= \langle ax+b\rangle = \langle ax\rangle + \langle b\rangle = a\langle x\rangle + b,\\
\left\langle y^2\right\rangle &= \left\langle (ax+b)^2\right\rangle = a^2\left\langle x^2\right\rangle + 2ab\langle x\rangle + b^2,\\
D_y &= \left\langle y^2\right\rangle - \langle y\rangle^2 = a^2\left\langle x^2\right\rangle + 2ab\langle x\rangle + b^2 - (a\langle x\rangle + b)^2 = a^2\left\langle x^2\right\rangle - \left\langle x^2\right\rangle^2 = a^2 D_x,\\
\langle xy\rangle &= \langle x(ax+b)\rangle = \left\langle ax^2+bx\right\rangle = a\left\langle x^2\right\rangle + b\langle x\rangle
\end{aligned}$$

и коэффициент корреляции

$$r = \frac{\langle xy\rangle - \langle x\rangle\langle y\rangle}{\sqrt{D}_x\sqrt{D}_y} = \frac{a\langle x^2\rangle + b\langle x\rangle - a\langle x\rangle^2 - b\langle x\rangle}{\sqrt{D_x}\,\sqrt{a^2D_x}} = \frac{a(\langle x^2\rangle - \langle x\rangle^2)}{\sqrt{a^2D_x^2}} = \frac{aD_x}{aD_x} = 1.$$

Пример 1.14. (Ash [12]) Имеются две монеты. Одна из монет правильная, а у другой – два герба. Монета выбирается случайным образом, дважды подбрасывается, а результат записывается. Спрашивается, как много информации относительно идентичности монет мы можем получить, подсчитывая количество выпавших орлов? Очевидно, что количество орлов должно нам что-то сообщить о природе монеты.

Решение. Обозначим через **x** – случайную величину, определяющую выбранную монету ($x = 0$ - правильная, $x = 1$ - фальшивая). Вероятность выбора правильной или фальшивой монеты одинакова: $p(x = 0) = p(x = 1) = 1/2$.

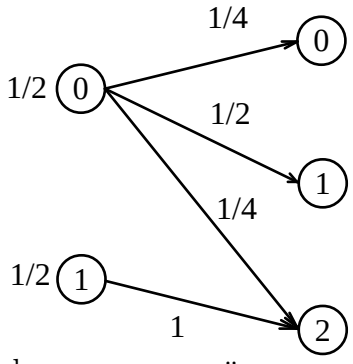
Обозначим через **y** количество выпавших гербов при двух подбрасываниях выбранной монеты. Поскольку **y** зависит от того какую монету мы взяли (правильную или фальшивую), мы получим два условных закона распределения

$x = 0$:

y	0	1	2
p	1/4	1/2	1/4

$x = 1$:

y	0	1	2
p	0	0	1



Совместный закон распределения получим по формуле полной вероятности

$$p(x,y) = p(x)p(y|x)$$

или

$$p(x,y) = \begin{pmatrix} \frac{1}{2}\cdot\frac{1}{4} & \frac{1}{2}\cdot\frac{1}{2} & \frac{1}{2}\cdot\frac{1}{4} \\ \frac{1}{2}\cdot 0 & \frac{1}{2}\cdot 0 & \frac{1}{2}\cdot 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{8} & \frac{1}{4} & \frac{1}{8} \\ 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

Складывая вероятности по строкам и столбцам, получим редуцированные (маргинальные) законы распределения p(**x**) и p(**y**):

$x \diagdown y$	0	1	2	p(x)
0	1/8	1/4	1/8	1/2
1	0	0	1/2	1/2
p(y)	1/8	1/4	5/8	$\sum = 1$

Средняя взаимная информация вычисляется по формуле

$$I(x|y) = H(x) + H(y) - H(x,y),$$

где

$$\begin{aligned}
H(x) &= -\sum_x p(x)\,\mathrm{lb}\,p(x) = -\frac{1}{2}\cdot\,\mathrm{lb}\frac{1}{2} - \frac{1}{2}\cdot\,\mathrm{lb}\frac{1}{2} = \frac{1}{2}\cdot 1 + \frac{1}{2}\cdot 1 = 1\,bit,\\
H(y) &= -\sum_y p(y)\,\mathrm{lb}\,p(y) = -\frac{1}{8}\cdot\,\mathrm{lb}\frac{1}{8} - \frac{1}{4}\cdot\,\mathrm{lb}\frac{1}{4} - \frac{5}{8}\cdot\,\mathrm{lb}\frac{5}{8} = \frac{3}{8} + \frac{2}{4} + \frac{0.678}{8} = 1.3\,bit,\\
H(x,y) &= -\sum_x\sum_y p(x,y)\,\mathrm{lb}\,p(x,y)\\
&= -\frac{1}{8}\cdot\,\mathrm{lb}\frac{1}{8} - \frac{1}{4}\cdot\,\mathrm{lb}\frac{1}{4} - \frac{1}{8}\cdot\,\mathrm{lb}\frac{1}{8} - 0\cdot\,\mathrm{lb}0 - 0\cdot\,\mathrm{lb}0 - \frac{1}{2}\cdot\,\mathrm{lb}\frac{1}{2}\\
&= \frac{3}{8} + \frac{2}{4} + \frac{3}{8} + 0 + 0 + \frac{1}{2} = \frac{14}{8} = 1.75\,bit.
\end{aligned}$$

Тогда

$$I(x|y) = H(x) + H(y) - H(x,y) = 1 + 1.3 - 1.75 = 0.55\ bit. \quad \blacktriangle$$

Задача 1.3. Найти средне количество информации, доставляемое случайной величиной **x** относительно **y**.

1. Дважды бросается игральная кость. Случайные величины **x** - появление 6, **y** - появление четной цифры.

2. Дважды бросается игральная кость. Случайные величины **x** - появление 5, **y** - появление четной цифры.

3. Дважды бросается игральная кость. Случайные величины **x** - появление 4, **y** - появление четной цифры.

4. Дважды бросается игральная кость. Случайные величины **x** - появление 5, **y** - появление четной цифры.

5. Дважды бросается игральная кость. Случайные величины **x** - появление 6, **y** - появление четной цифры.

6. Дважды бросается игральная кость. Случайные величины $\mathbf{x}$ - появление 1, $\mathbf{y}$ - появление нечетной цифры.

7. Дважды бросается игральная кость. Случайные величины $\mathbf{x}$ - появление 6, $\mathbf{y}$ - появление нечетной цифры.

8. Дважды бросается игральная кость. Случайные величины $\mathbf{x}$ - появление 5, $\mathbf{y}$ - появление нечетной цифры.

9. Дважды бросается игральная кость. Случайные величины $\mathbf{x}$ - появление 4, $\mathbf{y}$ - появление нечетной цифры.

10. Дважды бросается игральная кость. Случайные величины $\mathbf{x}$ - появление 5, $\mathbf{y}$ - появление нечетной цифры.

11. Дважды бросается игральная кость. Случайные величины $\mathbf{x}$ - появление 6, $\mathbf{y}$ - появление нечетной цифры.

12. Дважды бросается игральная кость. Случайные величины $\mathbf{x}$ - появление 1, $\mathbf{y}$ - появление нечетной цифры.

13. Один раз подбрасывается игральная кость. Случайные величины $\mathbf{x}$ - появление четной цифры, $\mathbf{y}$ - появление цифры кратной трем.

14. Иван и Петр наудачу извлекают по одному шару из урны, содержащей 6 белых и 4 черных шара. Иван извлекает шар первым. Случайные величины: $\mathbf{x}$ - количество белых шаров у Ивана, $\mathbf{y}$ - количество белых шаров у Петра

15. Решить предыдущую задачу при условии, что шары извлекаются с возвращением.

16. Из коробки, в которой 4 красных, 2 синих и 3 зеленых карандаша, наудачу извлекли 3 карандаша. Пусть $\mathbf{x}$ – число красных, а $\mathbf{y}$ – число синих карандашей среди извлеченных.

17. 10 студентов написали контрольную работу по математике, причем 4 из них получили оценку «отлично», 3 – «хорошо», а остальные «удовлетворительно». Для разбора в группе случайным образом отобрано 4 работы. Пусть $\mathbf{x}$ – число отличных, а $\mathbf{y}$ – число хороших работ среди отобранных.

18. 2 стрелка независимо друг от друга сделали по 2 выстрела по одной и той же мишени. Вероятность попадания для первого стрелка 0,8, а для второго – 0,6. Пусть $\mathbf{x}$ – число попаданий первого стрелка, а $\mathbf{y}$ –число попаданий второго.

19. В условиях предыдущей задачи пусть $\mathbf{y}$ – общее число попаданий в мишень.

20. Случайная величина $\mathbf{x}$ принимает значения $(0;\ 1;\ 2)$ с вероятностями $(0.3;\ 0.7;\ 0.1)$, а независящая от нее случайная величина $\mathbf{y}$ - значения $(-1;\ 0;\ 1)$ с вероятностями $(0.3;\ 0.5;\ 0.2)$.

21. По цели производится два независимых выстрела. Вероятность попадания в цель при первом выстреле равна p_1, при втором p_2. Случайные величины: **x** - число попаданий при первом выстреле, **y** - число попаданий при втором выстреле.

22. Из урны, содержащей 6 белых и 4 черных шара наудачу извлекают 2 шара без возвращения. Случайные величины: **x** - число извлеченных белых шаров, **y** - число черных шаров в выборке.

23. Число **x** выбирается случайным образом из множества целых чисел (1, 2, 3). Затем из того же множества выбирается наудачу число **y**, большее первого или равное ему.

24. Бросается два раз игральная кость. Случайные величины **x** - появление шестерки, **y** - появление единицы.

25. Два раза бросается монета. Случайные величины **x** - появление орла, **y** - появление решки.

26. Три раза бросается монета. Случайные величины **x** - появление орла, **y** - появление решки.

27. Бросается один раз игральная кость. Если на грани выпадает цифра 1, 2, 3 или 4, то монета бросается 1 раз. В противоположном случае – монета бросается 2 раза. Случайные величины: **x** - появление цифры 1,2,3 или 4, **y** – количество выпавших орлов на монете.

Пример 1.15. Источник сообщений вырабатывает ансамбль независимых символов **x** с частотами **n**. Вычислить энтропию источника.

x	1	2	3	4
n	25	40	0	35

Решение. Поскольку источник сообщений выработал всего

$$N = \sum n = 25 + 40 + 0 + 35 = 100$$

символов, то вероятность появления определенного символа равна

$$p_i = \frac{n_i}{\sum n} = \frac{n_i}{N},$$

и мы получаем таблицу распределения случайной величины **x** вырабатываемой источником

x	1	2	3	4
p	1/4	2/5	0	7/20

По определению, энтропия – это среднее количество информации содержащееся в случайной величине

$$H = M(I) = \sum \text{lb}\frac{1}{p} \cdot p = -\sum p \cdot \text{lb}p.$$

Для нашей задачи, получим

$$H = -\sum p \cdot \text{lb}p = -\left(\frac{1}{4} \cdot \text{lb}\frac{1}{4} + \frac{2}{5} \cdot \text{lb}\frac{2}{5} + 0 \cdot \text{lb}(0) + \frac{7}{20} \cdot \text{lb}\frac{7}{20}\right) = 1.5589\, bit. \quad \blacktriangle$$

Задача 1.4. Вычислить энтропию источника сообщений, который вырабатывает ансамбль независимых символов **x** с частотами **n**.

№	**n**								**№**	**n**							
1	23	2	1	15	3	2	1	1	**16**	4	1	2	0	2	0	0	4
2	2	20	1	20	3	0	1	5	**17**	2	1	1	13	2	2	5	22
3	1	1	2	3	11	1	23	2	**18**	23	2	1	15	1	1	9	3
4	6	1	0	3	20	1	2	20	**19**	2	23	1	12	3	9	1	1
5	2	1	1	3	15	1	21	2	**20**	1	1	1	2	3	11	11	23
6	2	21	1	14	3	1	1	2	**21**	1	1	6	3	13	2	23	2
7	2	0	1	13	3	2	3	21	**22**	2	2	1	14	2	2	5	22
8	2	1	2	3	14	1	23	2	**23**	3	20	1	20	3	4	3	1
9	1	0	6	3	20	2	21	2	**24**	3	20	12	20	3	4	3	1
10	2	20	2	20	3	6	0	1	**25**	3	20	12	20	3	4	3	3
11	2	0	1	13	3	2	5	22	**26**	23	2	1	15	3	2	1	1
12	6	3	20	2	23	2	2	0	**27**	2	20	1	20	3	0	1	5
13	20	2	22	2	3	6	0	2	**28**	6	1	0	3	20	1	2	20
14	2	2	1	15	3	1	5	25	**29**	2	0	1	13	3	2	3	21
15	23	2	1	16	1	7	3	1	**30**	2	1	2	3	14	1	23	2

1.6 Кодирование информации методом Шеннона

При передаче информации во многих случаях выгодно первоначальное сообщение источника представить при помощи другого алфавита путем кодирования.

Характеристиками кода являются значность и его основание. Значность кода n – число символов в кодовом слове (кодовой комбинации), а основание L – число различных символов кода. Наиболее распространенны двоичные (бинарные) коды с основанием $L = 2$. Равномерным является такой код, у которого значность кода для всех кодовых слов одинакова (например, код Бодо).

При кодировании сообщений, передаваемых по каналам связи без помех, необходимо выполнить два условия:

1. кодовые слова должны быть различимы и однозначно связаны с соответствующими сообщениями;

2. применяемый способ кодирования должен обеспечить максимальную экономичность (краткость) кода, при которой на передачу данного сообщения затрачивается минимальное время.

Код, удовлетворяющий второму из этих условий, называется оптимальным.

Если $\mathbf{x} = \{x_i\}$, $i = 1, 2, ..., N$ - ансамбль взаимно независимых сообщений с априорными вероятностями $p(x_i)$, а $\mathbf{y} = \{y_k\}$, $k = 1, 2, ..., L$ - ансамбль символов кода и $L < N$, то число кодовых слов по n символов в каждом слове $M = L^n$. При $L^n \geq N$, где n – наименьшее целое число, для которого выполняется это неравенство, ансамбль сообщений $\mathbf{x} = \{x_i\}$ можно однозначно закодировать при помощи N различных кодов слов по n символов в слове.

Пример 1.16. Закодировать по методу Шеннона-Фено сообщение из $N = 24$ символов:

математика_-_царица_наук

Решение. Выпишем в таблицу частоты n_i и вероятности $p_i = \frac{n_i}{N}$ появления каждой буквы сообщения:

x	М	А	Т	Е	И	К	Ц	Р	Н	У	_	-
n	2	6	2	1	2	2	2	1	1	1	3	1
p	0.08	0.25	0.08	0.04	0.08	0.08	0.08	0.04	0.04	0.04	0.15	0.04

Найдем энтропию сообщения

$$\begin{aligned} H(x) &= \sum p_i \, \mathrm{lb} p_i = 0.08 \cdot \mathrm{lb}0.08 + 0.25 \cdot \mathrm{lb}0.25 + 0.08 \cdot \mathrm{lb}0.08 + 0.04 \cdot \mathrm{lb}0.04 + \\ &+ 0.08 \cdot \mathrm{lb}0.08 + 0.08 \cdot \mathrm{lb}0.08 + 0.08 \cdot \mathrm{lb}0.08 + 0.04 \cdot \mathrm{lb}0.04 + 0.04 \cdot \mathrm{lb}0.04 + \\ &+ 0.04 \cdot \mathrm{lb}0.04 + 0.15 \cdot \mathrm{lb}0.15 + 0.04 \cdot \mathrm{lb}0.04 \cong 3.3. \end{aligned}$$

Расположим символы в порядке убывания вероятностей:

x	А	_	Ц	К	И	М	Т	Е	Р	Н	У	-
n	0.25	0.15	0.08	0.08	0.08	0.08	0.08	0.04	0.04	0.04	0.04	0.04

Разобьем таблицу на две группы таким образом, чтобы **сумма вероятностей** появления символов в каждой группе была **приблизительно** одинаковой. Пометим все буквы попавшие в первую группу символом 0, а все буквы попавшие во вторую группу символом 1.

0.64					0.36						
А	_	Ц	К	И	М	Т	Е	Р	Н	У	-
0.25	0.15	0.08	0.08	0.08	0.08	0.08	0.04	0.04	0.04	0.04	0.04
0					1						

Аналогично, разбиваем первую группу на две равные по вероятностям части и присваиваем первой группе символ 0, а второй группе – символ 1 и.т.д.

А	_	Ц	К	И	М	Т	Е	Р	Н	У	-
0.25	0.15	0.08	0.08	0.08	0.08	0.08	0.04	0.04	0.04	0.04	0.04
0					1						
0		1			0			1			
0	1	0		1	0	1		0		1	
		0	1			0	1	0	1	0	1

Объединяя символы для каждой буквы получим кодовую таблицу

А	000	И	011	Р	1100
_	001	М	100	Н	1101
Ц	0100	Т	1010	У	1110
К	0111	Е	1011	-	1111

Экономность кода – количество информации, приходящееся на один кодовый символ, вычисляется как отношение энтропии алфавита к математическому ожиданию длины кодового обозначения букв сообщения. В нашем случае буквам сообщения соответствуют коды длиной 3 символа для букв (А, _, И, М) и 4 символа - для остальных 8-ми букв. Распределение вероятностей появления кода данной длины дано в таблице

x	3	4
n	4	8
p	1/3	2/3

Таким образом, математическое ожидание длины закодированной буквы есть

$$M[n] = \sum x_i p_i = 3 \cdot \frac{1}{3} + 4 \cdot \frac{2}{3} = \frac{11}{3} \cong 3.67.$$

Для экономности кода получим

$$S = \frac{H(x)}{M(n)} = \frac{3.3}{3.67} = 0.899. \quad \blacktriangle$$

Оптимальным называется код, в котором средняя длина кодового слова равна энтропии, т.е. $S = 1$.

Задача 1.5. Закодировать по методу Шеннона-Фено сообщение

фамилия_имя_отчество

и найти экономность кода.

1.7 Избыточность сообщения

Для характеристики величины, на которую удлиняются сообщения на данном языке по сравнению с минимальной длинной, необходимой для передачи той же информации, вводят специальный параметр R – избыточность:

$$R_k = 1 - \frac{H_k}{H_0} = 1 - \frac{H_k}{\mathrm{lb}N}$$

где N – число различных букв используемого алфавита; H_k - энтропия, приходящаяся на одну букву смыслового текста при учете всех k-буквенных сочетаний; $H_0 = \mathrm{lb}N$ – максимальная энтропия, приходящаяся на букву, когда буквы независимы и равновероятны.

Пример 1.17. По каналу связи передается сообщение «**многоногое**». Найти:
а) избыточность R_1 источника сообщений при статистической независимости букв;
б) избыточность R_2 с учетом зависимости между буквами.

Решение. Для передаваемого сообщения, таблица распределения вероятностей появления символов имеет вид

x	м	н	о	г	е	
n(**x**)	1	2	4	2	1	$\sum = 10$
p(**x**)=n/Σ	0.1	0.2	0.4	0.2	0.1	

а) Поскольку мы имеем всего $N = 5$ различных символов, то

$$\begin{aligned} H_0 &= \mathrm{lb}N = \mathrm{lb}5 = 2.322\,bit, \\ H_1 &= -\sum_{i=1}^{4} p_i\,\mathrm{lb}p_i \\ &= -(0,1\cdot\mathrm{lb}0,1 + 0,2\cdot\mathrm{lb}0,2 + 0,4\cdot\mathrm{lb}0,4 + 0,2\cdot\mathrm{lb}0,2 + 0,1\cdot\mathrm{lb}0,1) = 2.122\,bit. \end{aligned}$$

и по определению избыточности, имеем

$$R_1 = 1 - \frac{H_1}{H_0} = 1 - \frac{H_1}{\mathrm{lb}N} = 1 - \frac{2.122}{2.322} = 0.086.$$

б) При учете статистической зависимости между буквами мы заполняем таблицу частот появления двухбуквенных сочетаний

$x \setminus y$	м	н	о	г	е	n(**x**)
м	0	1	0	0	0	1
н	0	0	2	0	0	2
о	0	1	0	2	1	4
г	0	0	2	0	0	2
е	1	0	0	0	0	1
n(**y**)	1	2	4	2	1	$\sum = 10$

Теперь, таблица распределения вероятностей имеет вид $p(\mathbf{x}) = n/\Sigma$:

$x \setminus y$	м	н	о	г	е	p(**x**)
м	0	1/10	0	0	0	1/10
н	0	0	2/10	0	0	2/10
о	0	1/10	0	2/10	1/10	4/10
г	0	0	2/10	0	0	2/10
е	1/10	0	0	0	0	1/10
p(**y**)	1/10	2/10	4/10	2/10	1/10	$\sum = 1$

Избыточность R_2 с учетом зависимости между буквами вычисляется по формуле

$$R_2 = 1 - \frac{H_2}{H_0} = 1 - \frac{H_2}{\mathrm{lb}N},$$

где H_2 – энтропия на букву при учете двухбуквенных сочетаний.

Энтропия двухбуквенного текста

$$H(x,y) = -\sum_{i=1}^{5}\sum_{j=1}^{5} p(x_j, y_i)\ \mathrm{lb}p(x_j, y_i) = -4 \cdot 0.1 \cdot\ \mathrm{lb}0.1 - 3 \cdot 0.2 \cdot\ \mathrm{lb}0.2 = 2.39\, bit$$

Следовательно $H_2 = \dfrac{H(x,y)}{2} = 1.195\ bit,$

$$R_2 = 1 - \frac{H_2}{\mathrm{lb}N} = 1 - \frac{1.195}{2.322} \approx 0.485\ \ bit. \quad \blacktriangle$$

Пример 1.18. Алфавит состоит из 8 букв $(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$, вероятности появления которых равны: $\left(\frac{8}{16}, \frac{4}{16}, \frac{2}{16}, \frac{1}{16}, \frac{1}{16}, \frac{1}{16}, \frac{1}{16}, 0\right)$. Найти избыточность R_1 источника сообщений при статистической независимости букв.

Решение. По определению избыточности имеем

$$R_1 = 1 - \frac{H_1}{H_0} = 1 - \frac{H_1}{\mathrm{lb}N}$$

Поскольку мы имеем всего N=8 различных символов, то

$$H_0 = \ \mathrm{lb}N = \ \mathrm{lb}8 = 3\, bit,$$

$$\begin{aligned} H_1 &= -\sum_{i=1}^{4} p_i \,\mathrm{lb} p_i = \\ &= -\left(\frac{8}{16}\cdot \mathrm{lb}\frac{8}{16} + \frac{4}{16}\cdot \mathrm{lb}\frac{4}{16} + \frac{2}{16}\cdot \mathrm{lb}\frac{2}{16} + 4\cdot\frac{1}{16}\cdot \mathrm{lb}\frac{1}{16} + 0\cdot \mathrm{lb}0\right) \\ &= \left(\frac{8}{16}\cdot 1 + \frac{4}{16}\cdot 2 + \frac{2}{16}\cdot 3 + 4\cdot\frac{1}{16}\cdot 4 + 0\right) = \frac{8+8+6+16}{16} = 2.375\,bit \end{aligned}$$

и

$$R_1 = 1 - \frac{2.375}{3} = 0.208. \quad \blacktriangle$$

Задача 1.6. Найти:
а) избыточность R_1 источника сообщений при статистической независимости букв;
б) избыточность R_2 с учетом зависимости между буквами.
для сообщения

№	сообщение	№	сообщение	№	сообщение
1	атомизатор	**11**	даунтаун	**21**	клочочек
2	менеджмент	**12**	плодовод	**22**	волнолом
3	кавказка	**13**	шаровары	**23**	воздуховоз
4	барбарис	**14**	эстафета	**24**	подлодка
5	берберин	**15**	прототип	**25**	размазня
6	варварка	**16**	прививка	**26**	гонгконг
7	колокол	**17**	прабабка	**27**	колокольня
8	женьшень	**18**	пленение	**28**	математик
9	чихуахуа	**19**	метатанк	**29**	постылость
10	наносность	**20**	ленинизм	**30**	водопровод

Глава 2

Каналы связи

2.1 Пропускная способность каналов связи

Пусть имеется дискретный стационарный канал связи без памяти (без последействия) с заданными характеристиками, причем все символы x_i закодированного сообщения и соответствующие им элементарные сигналы y_i имеют одинаковую длительность τ, где $F = 1/\tau$ - частота посылки символов.

Канал без памяти полностью описывается априорными вероятностями $P(x)$, характеризующими структуру закодированных сообщений, и условными вероятностями $P(x/y)$, определяющимися характеристиками канала.
Основные понятия:

1. информация, доставляемая символом x_i по каналу связи определяется формулой
$$I(x_i) = -\ \mathrm{lb} p(x_i);$$
2. условная собственная информация $I(x_i/y_k)$ переданного символа x_i при известном принятом y_k
$$I(x_i/y_k) = -\ \mathrm{lb} p(x_i/y_k);$$
3. взаимная информация $I(x_i; y_k)$ двух символов относительно друг друга (количество информации в доставленном y_k относительно отправленного x_i)
$$I(x_i; y_k) = \ \mathrm{lb}\frac{p(x_i/y_k)}{p(x_i)} = \ \mathrm{lb}\frac{p(x_i, y_k)}{p(x_i)p(y_k)};$$
4. собственная информация $I(x_i\ y_k)$ совместного события $x_i y_k$
$$I(x_i y_k) = -\ \mathrm{lb} p(x_i y_k);$$
5. среднее количество информации $I(x; y_k)$ доставляемое принятым символом y_k относительно множества всех передаваемых символов $x = \{x_i\}$
$$I(x; y_k) = \sum_i I(x_i; y_k) p(x_i/y_k) = \sum_i p(x_i/y_k)\ \mathrm{lb}\frac{p(x_i/y_k)}{p(x_i)};$$

6. среднее количество взаимной информации $I(x_i\ y)$ по множеству символов $y = \{y_i\}$ при фиксированном x_i

$$I(x_i; y) = \sum_k I(x_i; y_k) p(y_k/x_i) = \sum_k p(y_k/x_i)\ \mathrm{lb}\frac{p(y_k/x_i)}{p(y_k)};$$

7. полное среднее количество взаимной информации $I(x; y)$ в множестве символов y относительно множества символов x

$$I(x; y) = \sum_k I(x; y_k) p(y_k) = \sum_{i,k} p(x_i, y_k)\ \mathrm{lb}\frac{p(x_i/y_k)}{p(x_i)}$$

При решении большинства задач, связанных с построением систем связи наибольший интерес представляет величина $I(x; y)$.

Если символ x_i статистически связан не только с символом y_j, но и с третьим символом z_k, то при известных вероятностях $p(x_i, y_j, z_k)$ условная взаимная информация равна

$$I(x_i; y_j/z_k) = \mathrm{lb}\frac{p(x_i/y_j z_k)}{p(x_i/z_k)} = \mathrm{lb}\frac{p(x_i; y_j/z_k)}{p(x_i/z_k)p(y_j/z_k)},$$

где $I(x_i; y_j/z_k)$ - количество информации, доставляемое y_j относительно x_i, когда предварительно известен символ z_k.

По аналогии со средней взаимной информацией, средняя собственная информация определяется формулой

$$I(x) = \sum_i p(x_i) I(x_i) = -\sum_i p(x_i)\ \mathrm{lb}p(x_i) = H(x).$$

Здесь $H(x)$ - энтропия случайного сигнала x, определяет количественную меру неопределенности о сообщении до его приема.

Для энтропии справедливы следующие выражения:

$$H(y/x) = -\sum_{ik} p(x_i, y_k)\ \mathrm{lb}p(y_k/x_i) = -\sum_i p(x_i) \sum_k p(y_k/x_i)\ \mathrm{lb}p(y_k/x_i) = I(y/x),$$

$$H(x/y) = -\sum_{ik} p(x_i, y_k)\ \mathrm{lb}p(x_i/y_k) = -\sum_k p(y_k) \sum_i p(x_i/y_k)\ \mathrm{lb}p(x_i/y_k) = I(x/y),$$

$$H(xy) = -\sum_{ik} p(x_i, y_k)\ \mathrm{lb}p(x_i, y_k),$$

$$H(xy) = H(x) + H(y/x) = H(y) + H(x/y),$$

где $H(y/x)$ - условная энтропия множества событий y при данном множестве событий x; $H(xy)$ - энтропия множества совместных событий xy.

Когда множества x и y независимы, то

$$H(y/x) = H(y), H(x/y) = H(x).$$

При этом

$$H(xy) = H(x) + H(y).$$

Средняя взаимная информация связана с энтропией соотношениями

$$I(x;y) = H(x) - H(x/y) = H(y) - H(y/x) = H(x) + H(y) - H(xy),$$

$$I(x;y) \le H(x),$$

$$I(x;y) \le H(y).$$

Скорость передачи V_k – среднее количество информации, получаемое за единицу времени:

$$V_k = FI(x;y) = F\left[H(x) - H(x/y)\right] = F\left[H(y) - H(y/x)\right]$$

При отсутствии помех множества событий x и y статистически полностью взаимно зависимы, т. е. $H(x/y) = H(y/x) = 0$, следовательно,

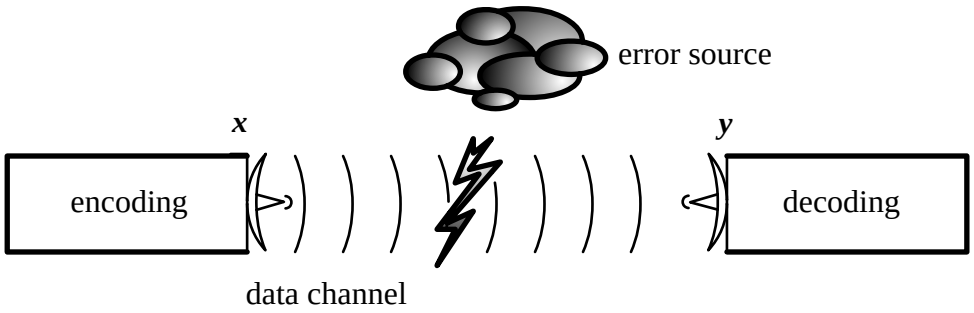
$$V_{k\,\max} = FH(x) = FH(y).$$

Пропускная способность канала связи – максимальная скорость передачи информации, которая может быть достигнута выбором оптимального распределения вероятностей передачи $P(x)$ символов сообщения:

$$C = \max_{p(x)} FI(x;y) = \max_{p(x)} F\left[H(x) - H(x/y)\right] = \max_{p(x)} F\left[H(y) - H(y/x)\right]$$

При отсутствии помех $H(x/y) = H(y/x) = 0$:

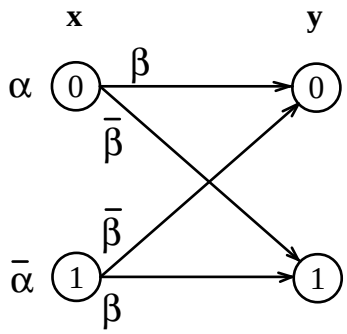
$$C = C_m = \max_{p(x)} FI(x;y) = \max_{p(x)} FH(x) = \max_{p(x)} FH(y).$$



Теорема 5. Пропускная способность двоичного симметричного канала связи равна

$$C = F[1 + (1-\beta)\cdot \text{ lb}(1-\beta) + \beta \cdot \text{ lb}\beta],$$

где β – вероятность ошибочного приема, $F = 1/\tau$ - частота посылки импульсов, τ - длительность одного сигнала.



Доказательство. Рассмотрим схему двоичного симметричного канала связи. Обозначим через **x** – случайную величину значений на входе, а **y** – случайную величину значений на выходе канала информации.

Допустим, что вероятность появления на входе канала значения **0** или **1** равны соответственно:

$$p(x=0) = p; \qquad p(x=1) = 1-p = \overline{p}.$$

Вследствие помех передаваемый сигнал проходит канал без искажения с вероятностью β и принимает противоположное значение с вероятностью $\overline{\beta}$. Такое действие описывается **канальной матрицей**:

$$p(\mathbf{y}|\mathbf{x}) = \begin{pmatrix} \beta & \overline{\beta} \\ \overline{\beta} & \beta \end{pmatrix}.$$

Вероятности, расположенные по диагонали, описывают вероятность правильного приёма, а сумма всех элементов столбца даёт вероятность появления соответствующего символа на стороне приёмника $p(\mathbf{y})$.

Матрица совместного распределения вероятностей принимает вид

$$p(x,y) = \begin{pmatrix} p\cdot\beta & p\cdot\overline{\beta} \\ \overline{p}\cdot\overline{\beta} & \overline{p}\cdot\beta \end{pmatrix}.$$

Складывая вероятности по строкам и столбцам, получим редуцированные (маргинальные) законы распределения p(**x**) и p(**y**):

$x \diagdown y$	0	1	p(x)
0	$p\cdot\beta$	$p\cdot\overline{\beta}$	p
1	$\overline{p}\cdot\overline{\beta}$	$\overline{p}\cdot\beta$	$\overline{p}$
p(y)	$p\cdot\beta + \overline{p}\cdot\overline{\beta}$	$\overline{p}\cdot\beta + p\cdot\overline{\beta}$	$\sum = 1$

Средняя взаимная информация	Средняя взаимная информация определяет скорость передачи информации и вычисляется по формуле $$I(x,y) = H(x) + H(y) - H(x,y),$$

Здесь

$$\begin{aligned}
H(x) &= -\sum_x p(x)\cdot \operatorname{lb} p(x) = -p\cdot \operatorname{lb} p - \overline{p}\cdot \operatorname{lb}\overline{p},\\
H(y) &= -\sum_y p(y)\cdot \operatorname{lb} p(y) = -(p\cdot\beta + \overline{p}\cdot\overline{\beta})\cdot \operatorname{lb}(p\cdot\beta+\overline{p}\cdot\overline{\beta})\\
&\quad -(\overline{p}\cdot\beta + p\cdot\overline{\beta})\cdot \operatorname{lb}(\overline{p}\cdot\beta + p\cdot\overline{\beta}),\\
H(x,y) &= -\sum_x\sum_y p(x,y)\cdot \operatorname{lb} p(x,y)\\
&= -p\beta\cdot \operatorname{lb} p\beta - p\overline{\beta}\cdot \operatorname{lb} p\overline{\beta} - \overline{p}\overline{\beta}\cdot \operatorname{lb}\overline{p}\overline{\beta} - \overline{p}\beta\cdot \operatorname{lb}\overline{p}\beta\,.
\end{aligned}$$

Тогда

$$\begin{aligned}
I(x;y) &= H(x)+H(y)-H(x,y)\\
&= -p\cdot \operatorname{lb}\alpha - \overline{p}\cdot \operatorname{lb}\overline{p} - (p\cdot\beta+\overline{p}\cdot\overline{\beta})\cdot \operatorname{lb}(p\cdot\beta+\overline{p}\cdot\overline{\beta})\\
&- (\overline{p}\cdot\beta + p\cdot\overline{\beta})\cdot \operatorname{lb}(\overline{p}\cdot\beta + p\cdot\overline{\beta})\\
&+ p\beta\cdot \operatorname{lb} p\beta + p\overline{\beta}\cdot \operatorname{lb} p\overline{\beta} + \overline{p}\overline{\beta}\cdot \operatorname{lb}\overline{p}\overline{\beta} + \overline{p}\beta\cdot \operatorname{lb}\overline{p}\beta.
\end{aligned}$$

Пропускная способность	Пропускная способность канала связи C – максимальная скорость передачи информации, которая может быть достигнута выбором оптимального распределения вероятности $p(x)$ символов сообщения: $$C = \underset{p(x)}{Max}\, F\cdot I(x;y).$$

Исследуем функцию $I(x|y)$ на экстремум

$$\begin{aligned}
\frac{d}{dp}I(x;y) &= -1\cdot \operatorname{lb} p - 1 + 1\cdot \operatorname{lb}\overline{p} + 1 - (\beta-\overline{\beta})\cdot \operatorname{lb}(p\cdot\beta+\overline{p}\cdot\overline{\beta}) - (\beta-\overline{\beta})\\
&- (\overline{\beta}-\beta)\cdot \operatorname{lb}(\overline{p}\cdot\beta + p\cdot\overline{\beta}) - (\overline{\beta}-\beta)\\
&+ \beta\cdot \operatorname{lb} p\beta + \beta + \overline{\beta}\cdot \operatorname{lb} p\overline{\beta} + \overline{\beta} - \overline{\beta}\cdot \operatorname{lb}\overline{p}\overline{\beta} - \overline{\beta} - \beta\cdot \operatorname{lb}\overline{p}\beta - \beta\\
&= \operatorname{lb}\frac{\overline{p}}{p} + (\beta-\overline{\beta})\cdot \operatorname{lb}\frac{(\overline{p}\cdot\beta+p\cdot\overline{\beta})}{(p\cdot\beta+\overline{p}\cdot\overline{\beta})} + \operatorname{lb}\frac{\overline{p}}{p}\\
&= (\beta-\overline{\beta})\cdot \operatorname{lb}\frac{(\overline{p}\cdot\beta+p\cdot\overline{\beta})}{(p\cdot\beta+\overline{p}\cdot\overline{\beta})} = 0.
\end{aligned}$$

Отсюда следует, что

$$\frac{(\overline{p}\cdot\beta+p\cdot\overline{\beta})}{(p\cdot\beta+\overline{p}\cdot\overline{\beta})} = 1, \quad \text{или} \quad \frac{\beta-p\beta+p-p\beta}{p\beta+1-p-\beta+p\beta} = 1$$

откуда

$$2\beta - 4p\beta + 2p = 1 \quad \text{т.е.} \quad p^* = \frac{1}{2}.$$

Подставляя полученное значение p^* в выражение для $I(x|y)$ получим

$$\begin{aligned} I(x;y) &= H(x)+H(y)-H(x,y) \\ &= -\frac{1}{2}\cdot \mathrm{lb}\frac{1}{2}-\frac{1}{2}\cdot \mathrm{lb}\frac{1}{2}-\left(\frac{\beta}{2}+\frac{\overline{\beta}}{2}\right)\cdot \mathrm{lb}\left(\frac{\beta}{2}+\frac{\overline{\beta}}{2}\right)-\left(\frac{\beta}{2}+\frac{\overline{\beta}}{2}\right)\cdot \mathrm{lb}\left(\frac{\beta}{2}+\frac{\overline{\beta}}{2}\right) \\ &+ \frac{\beta}{2}\cdot \mathrm{lb}\frac{\beta}{2}+\frac{\overline{\beta}}{2}\cdot \mathrm{lb}\frac{\overline{\beta}}{2}+\frac{\overline{\beta}}{2}\cdot \mathrm{lb}\frac{\overline{\beta}}{2}+\frac{\beta}{2}\cdot \mathrm{lb}\frac{\beta}{2} \\ &= 1+1+\beta\cdot \mathrm{lb}\frac{\beta}{2}+\overline{\beta}\cdot \mathrm{lb}\frac{\overline{\beta}}{2}=2+\beta\cdot \mathrm{lb}\beta+\overline{\beta}\cdot \mathrm{lb}\overline{\beta}-1 \\ &= 1+\beta\cdot \mathrm{lb}\beta+\overline{\beta}\cdot \mathrm{lb}\overline{\beta}. \quad \blacksquare \end{aligned}$$

При отсутствии помех ($\beta = 0$)

$$C = C_m = F.$$

Потери информации	Потери информации со стороны источника $$H(y/x) = H(x,y) - H(x),$$ Потери информации со стороны приемника $$H(x/y) = H(x,y) - H(y),$$

Пример 2.1. По двоичному симметричному каналу связи с помехами передаются сигналы (x_1, x_2) с априорными вероятностями $p(x_1) = 3/4;\ p(x_2) = 1/4$. Из-за наличия помех вероятность правильного приема каждого из сигналов (x_1, x_2) уменьшается до $\alpha = 7/8$.

Найти:

1. скорость передачи информации $I(x;y)$;
2. пропускную способность канала $C = \underset{p(x)}{Max}\, I(x;y)$.

Решение. По условию

$$p(x_1) = 3/4,$$

$$p(x_2) = 1/4,$$

$$\alpha = 7/8,$$

$$\overline{\alpha} = 1/8.$$

Предварительно, вычислим вероятности $p(y_j)$, $p(x_j, y_j)$, и $p(x_j/y_j)$. По формуле полной вероятности получим:

$$p(x_1, y_1) = p(x_1)\alpha = \frac{3}{4}\cdot\frac{7}{8} = \frac{21}{32};$$

$$p(x_1, y_2) = p(x_1)\overline{\alpha} = \frac{3}{4}\cdot\frac{1}{8} = \frac{3}{32};$$

$$p(x_2, y_1) = p(x_2)\overline{\alpha} = \frac{1}{4} \cdot \frac{1}{8} = \frac{1}{32};$$
$$p(x_2, y_2) = p(x_2)\alpha = \frac{1}{4} \cdot \frac{7}{8} = \frac{7}{32}.$$

Составим таблицу совместного распределения для передаваемых и получаемых сигналов

$x \setminus y$	0	1	$p(x)$
0	$\frac{21}{32}$	$\frac{3}{32}$	$\frac{24}{32} = \frac{3}{4}$
1	$\frac{1}{32}$	$\frac{7}{32}$	$\frac{8}{32} = \frac{1}{4}$
$p(y)$	$\frac{22}{32}$	$\frac{10}{32}$	$\sum p = 1$

1. По формулам для среднего количества информации

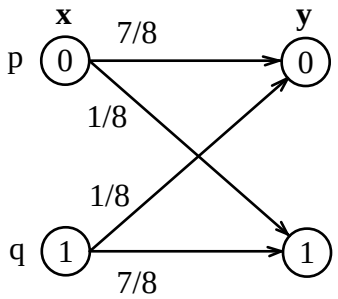
$$H(x) = -\sum_i p(x_i)\ \mathrm{lb} p(x_i) = -\frac{3}{4}\ \mathrm{lb}\frac{3}{4} - \frac{1}{4}\ \mathrm{lb}\frac{1}{4} = 0.811\ bit$$

$$H(y) = -\sum_i p(y_i)\ \mathrm{lb} p(y_i) = -\frac{22}{32}\ \mathrm{lb}\frac{22}{32} - \frac{10}{32}\ \mathrm{lb}\frac{10}{32} = 0.896\ bit$$

$$H(x,y) = -\sum\sum p(x,y)\ \mathrm{lb} p(x,y) - \frac{21}{32}\ \mathrm{lb}\frac{21}{32} - \frac{3}{32}\ \mathrm{lb}\frac{3}{32} - \frac{1}{32}\ \mathrm{lb}\frac{1}{32} - \frac{7}{32}\ \mathrm{lb}\frac{7}{32} = 1.355\ bit$$

$$\begin{aligned} I(x,y) &= H(x) + H(y) - H(x,y) \\ &= -\sum p(x)\ \mathrm{lb} p(x) - \sum p(y)\ \mathrm{lb} p(y) + \sum\sum p(x,y)\ \mathrm{lb} p(x,y) \\ &= -\frac{3}{4}\ \mathrm{lb}\left(\frac{3}{4}\right) - \frac{1}{4}\ \mathrm{lb}\left(\frac{1}{4}\right) - \frac{22}{32}\ \mathrm{lb}\left(\frac{22}{32}\right) - \frac{10}{32}\ \mathrm{lb}\left(\frac{10}{32}\right) \\ &+ \frac{21}{32}\ \mathrm{lb}\left(\frac{21}{32}\right) + \frac{3}{32}\ \mathrm{lb}\left(\frac{3}{32}\right) + \frac{1}{32}\ \mathrm{lb}\left(\frac{1}{32}\right) + \frac{7}{32}\ \mathrm{lb}\left(\frac{7}{32}\right) = 0.352\ bit \end{aligned}$$

Для нахождения пропускной способности двоичного симметричного канала, нам необходимо найти такие значения p и q при которых скорость передачи по каналу (при заданных помехах) будет максимальна. Имеем



Составим таблицу совместного распределения для передаваемых и получаемых сигналов

$x \setminus y$	0	1	$p(x)$
0	$p\frac{7}{8}$	$p\frac{1}{8}$	p
1	$q\frac{1}{8}$	$q\frac{7}{8}$	q
$p(y)$	$p\frac{7}{8} + q\frac{1}{8}$	$p\frac{1}{8} + q\frac{7}{8}$	$\sum p = 1$

По формулам для среднего количества информации

$$H(x) = -\sum_i p(x_i)\ \mathrm{lb}p(x_i) \qquad H(y) = -\sum_i p(y_i)\ \mathrm{lb}p(y_i)$$

$$H(x,y) = -\sum\sum p(x,y)\ \mathrm{lb}p(x,y)$$

$$\begin{aligned} I(x,y) &= H(x) + H(y) - H(x,y) \\ &= -\sum p(x)\ \mathrm{lb}p(x) - \sum p(y)\ \mathrm{lb}p(y) + \sum\sum p(x,y)\ \mathrm{lb}p(x,y) \\ &= -p\ \mathrm{lb}\,(p) - q\ \mathrm{lb}\,(q) - \left(p\frac{7}{8} + q\frac{1}{8}\right)\ \mathrm{lb}\left(p\frac{7}{8} + q\frac{1}{8}\right) - \left(p\frac{1}{8} + q\frac{7}{8}\right)\ \mathrm{lb}\left(p\frac{1}{8} + q\frac{7}{8}\right) \\ &+ p\frac{7}{8}\ \mathrm{lb}\left(p\frac{7}{8}\right) + p\frac{1}{8}\ \mathrm{lb}\left(p\frac{1}{8}\right) + q\frac{1}{8}\ \mathrm{lb}\left(q\frac{1}{8}\right) + q\frac{7}{8}\ \mathrm{lb}\left(q\frac{7}{8}\right) \end{aligned}$$

Теперь, учитывая что $q = 1 - p$, получим

$$\begin{aligned} I(p) &= -p\ \mathrm{lb}\,(p) - q\ \mathrm{lb}\,(q) \\ &- \left(p\frac{7}{8} + (1-p)\frac{1}{8}\right)\ \mathrm{lb}\left(p\frac{7}{8} + (1-p)\frac{1}{8}\right) - \left(p\frac{1}{8} + (1-p)\frac{7}{8}\right)\ \mathrm{lb}\left(p\frac{1}{8} + (1-p)\frac{7}{8}\right) \\ &+ p\frac{7}{8}\ \mathrm{lb}\left(p\frac{7}{8}\right) + p\frac{1}{8}\ \mathrm{lb}\left(p\frac{1}{8}\right) + (1-p)\frac{1}{8}\ \mathrm{lb}\left((1-p)\frac{1}{8}\right) + (1-p)\frac{7}{8}\ \mathrm{lb}\left((1-p)\frac{7}{8}\right) \end{aligned}$$

Исследуем функцию $I(p)$ на экстремум

$$\frac{d}{dp}I(p) = \frac{3}{4}\ \mathrm{lb}\left(\frac{1+6p}{7-6p}\right), \quad \frac{3}{4}\ \mathrm{lb}\left(\frac{1+6p}{7-6p}\right) = 0, \quad \frac{1+6p}{7-6p} = 1, \quad 1{+}6p = 7{-}6p, \quad p^* = 1/2.$$

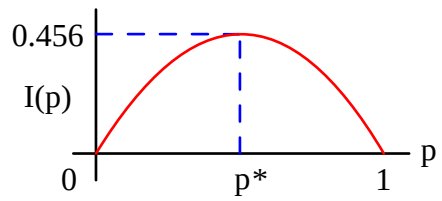
Подставляя полученное значение p^* в формулу для $I(p)$ получим выражение для пропускной способности двоичного симметричного канала при вероятности помехи $\overline{\alpha}$:

$$C = \max_{p(x)} I(p) = 1 + \alpha\ \mathrm{lb}\alpha + \overline{\alpha}\ \mathrm{lb}\overline{\alpha}.$$

Подставляя сюда $\alpha = 7/8$ получим

$$C = 1 + \frac{7}{8}\ \mathrm{lb}\frac{7}{8} + \frac{1}{8}\ \mathrm{lb}\frac{1}{8} = 0.456\ bit.$$

Это же значение легче получить графически. Для этого построим график функции $I(p)$ в Mathcad (см. рисунок). Из графика видно что максимальное значение скорости передачи данных $I_{max}(p^*) = 0.456$ в нашем канале достигается при $p^* = 1/2$. ▲



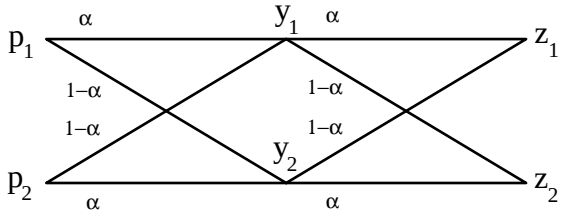
Задача 2.1. По двоичному симметричному каналу связи с помехами передаются сигналы (x_1, x_2) с априорными вероятностями $p(x_1)$; $p(x_2) = 1 - p(x_1)$. Из-за наличия помех вероятность правильного приема каждого из сигналов (x_1, x_2) уменьшается до α. Найти:

1. скорость передачи информации $I(x; y)$;
2. пропускную способность канала.

N	p	α	**N**	p	α	**N**	p	α
1	0.1	0.91	**11**	0.15	0.80	**21**	0.23	0.70
2	0.2	0.92	**12**	0.25	0.81	**22**	0.33	0.71
3	0.3	0.93	**13**	0.35	0.82	**23**	0.43	0.72
4	0.4	0.94	**14**	0.45	0.83	**24**	0.53	0.73
5	0.5	0.95	**15**	0.55	0.84	**25**	0.63	0.74
6	0.6	0.96	**16**	0.65	0.85	**26**	0.73	0.75
7	0.7	0.97	**17**	0.75	0.86	**27**	0.83	0.76
8	0.8	0.98	**18**	0.85	0.87	**28**	0.93	0.77
9	0.9	0.99	**19**	0.95	0.88	**29**	0.03	0.78
10	0.95	0.90	**20**	0.05	0.89	**30**	0.93	0.79

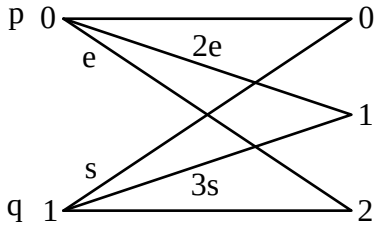
Задача 2.2. По двоичному симметричному каналу связи с помехами передаются сигналы (x_1, x_2) с априорными вероятностями $p(x_1)$; $p(x_2) = 1 - p(x_1)$. Из-за наличия помех вероятность правильного приема каждого из сигналов (x_1, x_2) уменьшается до α. Найти:

1. среднее количество информации $I(x; y)$;
2. пропускную способность канала.



N	p	α	**N**	p	α	**N**	p	α
1	0.1	0.91	**11**	0.15	0.80	**21**	0.23	0.70
2	0.2	0.92	**12**	0.25	0.81	**22**	0.33	0.71
3	0.3	0.93	**13**	0.35	0.82	**23**	0.43	0.72
4	0.4	0.94	**14**	0.45	0.83	**24**	0.53	0.73
5	0.5	0.95	**15**	0.55	0.84	**25**	0.63	0.74
6	0.6	0.96	**16**	0.65	0.85	**26**	0.73	0.75
7	0.7	0.97	**17**	0.75	0.86	**27**	0.83	0.76
8	0.8	0.98	**18**	0.85	0.87	**28**	0.93	0.77
9	0.9	0.99	**19**	0.95	0.88	**29**	0.03	0.78
10	0.95	0.90	**20**	0.05	0.89	**30**	0.93	0.79

Пример 2.2. По каналу связи с помехами передаются сигналы (**0,1**). Из-за наличия помех сигнал **0** искажается на **1** с вероятностью e=0.1 и на **2** с вероятностью 2e=0.2. Сигнал **1** искажается на **0** с вероятностью s=0.2 и на **2** с вероятностью 3s=0.6. Найти пропускную способность канала.



Решение. По условию канал связи имеет вид показанный на рисунке.

x \ y	0	1	2	p(**x**)
0	p(1-3e)	pe	2pe	p
1	qs	q(1-4s)	3qs	q
p(**y**)	p(1-3e)+qe	pe+ q(1-4s)	2pe+3qs	$\sum = 1$

Подставляя конкретные значения (e;s)=(0.1;0.2) получим

x \ y	0	1	2	p(**x**)
0	0.7p	0.1p	0.2p	p
1	0.2q	0.2q	0.6q	q
p(**y**)	0.7p+0.2q	0.1p+0.2q	0.2p+0.6q	$\sum = 1$

Тогда

$$H_x(p) = -\left(p\ \mathrm{lb}p + q\ \mathrm{lb}q = p\ \mathrm{lb}p + (1-p)\ \mathrm{lb}(1-p)\right);$$

$$\begin{aligned} H_y(p) = -(0.7p + 0.2q)\ \mathrm{lb}(0.7p + 0.2q) &+ (0.1p + 0.2q)\ \mathrm{lb}(0.1p + 0.2q) \\ &+ (0.2p + 0.6q)\ \mathrm{lb}(0.2p + 0.6q) \end{aligned}$$

$$\begin{aligned} = -(0.5p + 0.2)\ \mathrm{lb}(0.5p + 0.2) &+ (-0.1p + 0.2)\ \mathrm{lb}(-0.1p + 0.2) \\ &+ (-0.4p + 0.6)\ \mathrm{lb}(-0.4p + 0.6) \end{aligned}$$

$$\begin{aligned} H_{xy}(p) = -(0.7p)\ \mathrm{lb}(0.7p) + (0.1p)\ \mathrm{lb}(0.1p) &+ (0.2p)\ \mathrm{lb}(0.2p) + (0.2q)\ \mathrm{lb}(0.2q) \\ &+ (0.2q)\ \mathrm{lb}(0.2q) + (0.6q)\ \mathrm{lb}(0.6q) \end{aligned}$$

$$\begin{aligned} H_{xy}(p) = -(0.7p)\ \mathrm{lb}(0.7p) &+ (0.1p)\ \mathrm{lb}(0.1p) + (0.2p)\ \mathrm{lb}(0.2p) + 0.2(1-p)\ \mathrm{lb}(0.2(1-p)) \\ &+ 0.2(1-p)\ \mathrm{lb}(0.2(1-p)) + 0.6(1-p)\ \mathrm{lb}(0.6(1-p)) \end{aligned}$$

Взаимная информация есть

$$I(p) = H_x(p) + H_y(p) - H_{xy}(p)$$

Пропускная способность канала определяется таким значением $\boldsymbol{p}$, для которого скорость передачи информации $I(x, y)$ принимает максимальное значение

$$C = \max I(p) = I(p^*).$$

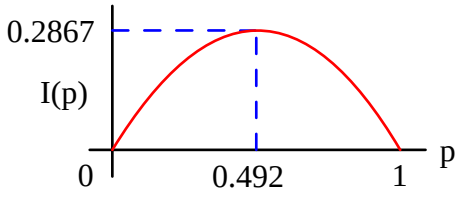
Решаем задачу на экстремум. В mathcad определим функцию

$$G(p) := \frac{d}{dp} I(p) \;\; simplify \rightarrow$$

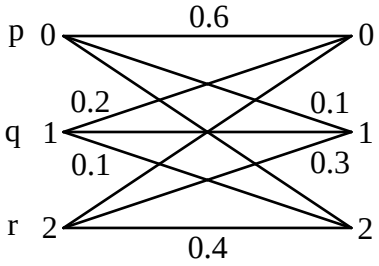
и найдем ее корень на промежутке [0;1]

$$root(G(p), p, 0, 1) = 0.492.$$

Можно решить задачу приближенно построив график функции $I(p)$. Из графика видим, что $p^* \approx 0.492$, тогда для пропускной способности канала связи получим C=I(0.492)=0.2867 bit. ▲



Пример 2.3. По каналу связи с помехами передаются сигналы (**0,1,2**). Из-за наличия помех сигнал **0** искажается на **1** с вероятностью 0.1 и на **2** с вероятностью 0.3. Сигнал **1** искажается на **0** с вероятностью s=0.2 и на **2** с вероятностью s=0.1. Сигнал **2** не искажается с вероятностью s=0.4 и принимает другие значения с равной вероятностью. Найти пропускную способность канала.



Решение. По условию канал связи имеет вид показанный на рисунке или

x \ y	0	1	2	p(**x**)
0	$\frac{6}{10}p$	$\frac{1}{10}p$	$\frac{3}{10}p$	p
1	$\frac{2}{10}q$	$\frac{7}{10}q$	$\frac{1}{10}q$	q
2	$\frac{3}{10}r$	$\frac{3}{10}r$	$\frac{4}{10}r$	r
p(**y**)	$\frac{6}{10}p+\frac{2}{10}q+\frac{3}{10}r$	$\frac{1}{10}p+\frac{7}{10}q+\frac{10}{10}r$	$\frac{3}{10}p+\frac{1}{10}q+\frac{4}{10}r$	$\sum=1$

Тогда

$$H_x(p,q,r) = -(p\ \mathrm{lb}p + q\ \mathrm{lb}q + r\ \mathrm{lb}r)$$

$$\begin{aligned} H_y(p,q,r) = &- \left(\frac{6p+2q+3r}{10}\right)\ \mathrm{lb}\left(\frac{6p+2q+3r}{10}\right) \\ &- \left(\frac{p+7q+10r}{10}\right)\ \mathrm{lb}\left(\frac{p+7q+10r}{10}\right) \\ &- \left(\frac{3p+q+4r}{10}\right)\ \mathrm{lb}\left(\frac{3p+q+4r}{10}\right) \end{aligned}$$

$$\begin{aligned} H_{xy}(p,q,r) = &- \left(\frac{6p}{10}\right)\ \mathrm{lb}\left(\frac{6p}{10}\right) - \left(\frac{p}{10}\right)\ \mathrm{lb}\left(\frac{p}{10}\right) - \left(\frac{3p}{10}\right)\ \mathrm{lb}\left(\frac{3p}{10}\right) \\ &- \left(\frac{2q}{10}\right)\ \mathrm{lb}\left(\frac{2q}{10}\right) - \left(\frac{7q}{10}\right)\ \mathrm{lb}\left(\frac{7q}{10}\right) - \left(\frac{q}{10}\right)\ \mathrm{lb}\left(\frac{q}{10}\right) \\ &- \left(\frac{3r}{10}\right)\ \mathrm{lb}\left(\frac{3r}{10}\right) - \left(\frac{3r}{10}\right)\ \mathrm{lb}\left(\frac{3r}{10}\right) - \left(\frac{4r}{10}\right)\ \mathrm{lb}\left(\frac{4r}{10}\right) \end{aligned}$$

С учетом $p+q+r=1$ запишем выражение для взаимной информации (скорости передачи)

$$I(p,q) = H_x(p,q,1-p-q) + H_y(p,q,1-p-q) - H_{xy}(p,q,1-p-q)$$

Пропускная способность канала определяется такими значениями p,q, для которых $I(p,q)$ принимает максимальное значение.

Решаем задачу на экстремум. В mathcad определим функции

$$G1(p,q) := \frac{d}{dp}I(p,q)\ \ simplify \rightarrow$$

$$G2(p,q) := \frac{d}{dq}I(p,q)\ \ simplify \rightarrow$$

и найдем ее корень на промежутке [0;1]: $x = \frac{1}{100}$ $y = \frac{1}{100}$

$$Given$$

$$G1(x,y) = 0 \qquad G2(x,y) = 0$$

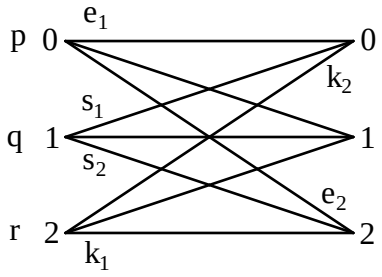
$$\begin{pmatrix} xval \\ yval \end{pmatrix} := Find(x,y)$$

$$xval = 0.47 \qquad yval = 0.42$$

Подставляя экстремальные значения $p^* = 0.47$, $q^* = 0.42$ получим пропускную способность канала связи

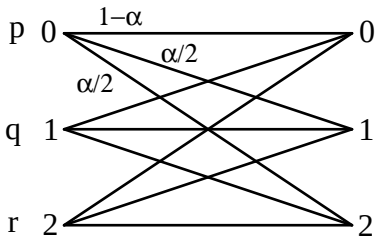
$$C = I(0.47, 0.42) = 0.227bit. \quad \blacktriangle$$

Задача 2.3. По каналу связи с помехами передаются сигналы (**0,1,2**) с вероятностями $p = q = r = 1/3$. Из-за наличия помех сигнал **0** принимается как **0** с вероятностью e_1 и как **2** с вероятностью e_2. Сигнал **1** искажается на **0** с вероятностью s_1 и на **2** с вероятностью s_2. Сигнал **2** не искажается с вероятностью k_1 и принимает значение **0** вероятностью k_2. Найти скорость передачи информации по каналу.



N	e_1	e_2	s_1	s_2	k_1	k_2	N	e_1	e_2	s_1	s_2	k_1	k_2
1	0.0	0.2	0.0	0.1	0.2	0.2	**16**	0.0	0.3	0.5	0.4	0.3	0.0
2	0.1	0.9	0.1	0.1	0.2	0.2	**17**	0.1	0.3	0.5	0.4	0.3	0.0
3	0.2	0.8	0.2	0.1	0.2	0.3	**18**	0.2	0.3	0.5	0.4	0.3	0.0
4	0.3	0.7	0.3	0.1	0.2	0.3	**19**	0.3	0.3	0.5	0.3	0.3	0.0
5	0.4	0.6	0.4	0.1	0.2	0.3	**20**	0.4	0.3	0.5	0.3	0.4	0.0
6	0.5	0.5	0.5	0.1	0.2	0.3	**21**	0.5	0.3	0.5	0.3	0.4	0.0
7	0.6	0.4	0.6	0.1	0.2	0.5	**22**	0.6	0.3	0.5	0.3	0.4	0.0
8	0.7	0.3	0.7	0.1	0.2	0.4	**23**	0.7	0.0	0.5	0.2	0.4	0.0
9	0.8	0.2	0.8	0.1	0.2	0.4	**24**	0.8	0.0	0.5	0.2	0.5	0.0
10	0.9	0.1	0.9	0.1	0.2	0.4	**25**	0.9	0.0	0.5	0.2	0.5	0.0
11	0.8	0.1	0.8	0.1	0.2	0.4	**26**	0.8	0.0	0.5	0.2	0.6	0.0
12	0.8	0.1	0.7	0.1	0.2	0.5	**27**	0.7	0.0	0.5	0.1	0.6	0.0
13	0.7	0.1	0.6	0.1	0.2	0.5	**28**	0.6	0.4	0.5	0.1	0.7	0.0
14	0.7	0.2	0.6	0.1	0.2	0.5	**29**	0.5	0.5	0.5	0.1	0.7	0.0
15	0.7	0.2	0.6	0.1	0.2	0.5	**30**	0.4	0.5	0.5	0.1	0.7	0.0

Пример 2.4. По 3-ичному симметричному каналу связи с помехами передаются сигналы (**0,1,2**). Из-за наличия помех сигнал **0** с вероятностью $\alpha/2$ может восприниматься как **1** или **2** и безошибочно принимается с вероятностью $1-\alpha$. Поскольку канал симметричный, аналогичным образом ведут себя и другие сигналы. Найти пропускную способность канала связи.



Решение. Запишем канальную матрицу

$$p(y|x) = \begin{pmatrix} 1-\alpha & \alpha/2 & \alpha/2 \\ \alpha/2 & 1-\alpha & \alpha/2 \\ \alpha/2 & \alpha/2 & 1-\alpha \end{pmatrix}$$

Тогда, матрица совместных вероятностей входного **x** и выходного **y** сигнала равна

$$p(x,y) = \begin{pmatrix} p(1-\alpha) & p\alpha/2 & p\alpha/2 \\ q\alpha/2 & q(1-\alpha) & q\alpha/2 \\ r\alpha/2 & r\alpha/2 & r(1-\alpha) \end{pmatrix}$$

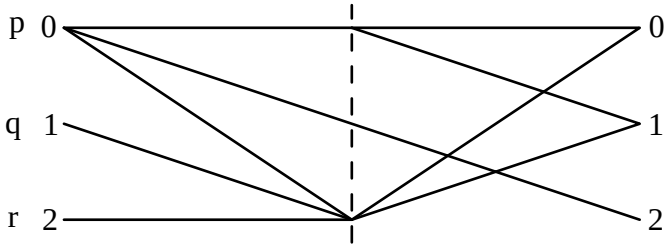
откуда пропускная способность

$$C = \text{lb}3 + (1-\alpha)\,\text{lb}(1-\alpha) + \alpha\,\text{lb}\frac{\alpha}{2}. \quad \blacktriangle$$

Аналогично, для k-ичного канала, с вероятностью ошибки $\alpha/(k-1)$, получим

$$C = \text{lb}k + (1-\alpha)\,\text{lb}(1-\alpha) + \alpha\,\text{lb}\frac{\alpha}{k-1}.$$

Пример 2.5. По каналу связи с ретранслятором



передаются сигналы (**0,1,2**). Из-за наличия помех каждое значение сигнала не искажается с вероятностью $\alpha = 0.8$ и принимает другие значения с равной вероятностью. Найти пропускную способность канала.

Решение. По условию таблица распределения для канала связи имеет вид

y x	0	1	2	p(**x**)
0	$p\cdot\alpha\cdot\alpha+p\cdot\frac{1-\alpha}{2}\cdot\frac{1}{2}$	$p\cdot\alpha\cdot(1-\alpha)+p\cdot\frac{1-\alpha}{2}\cdot\frac{1}{2}$	$p\cdot\frac{1-\alpha}{2}\cdot 1$	p
1	$q\cdot 1\cdot\frac{1}{2}$	$q\cdot 1\cdot\frac{1}{2}$	0	q
2	$r\cdot 1\cdot\frac{1}{2}$	$r\cdot 1\cdot\frac{1}{2}$	0	r
p(**y**)	$p\alpha^2+p\cdot\frac{1-\alpha}{4}+\frac{q+r}{2}$	$p\alpha(1-\alpha)+p\frac{1-\alpha}{4}+\frac{q+r1}{2}$	$p\cdot\frac{1-\alpha}{2}$	$\sum=1$

Тогда

$$
\begin{aligned}
H_x(p,q,r) &= -(p\ \mathrm{lb}p+q\ \mathrm{lb}q+r\ \mathrm{lb}r)\\
H_y(p,q,r) &= -\left(p\alpha^2+p\cdot\frac{1-\alpha}{4}+\frac{q+r}{2}\right)\ \mathrm{lb}\left(p\alpha^2+p\cdot\frac{1-\alpha}{4}+\frac{q+r}{2}\right)\\
&- \left(p\alpha(1-\alpha)+p\frac{1-\alpha}{4}+\frac{q+r}{2}\right)\ \mathrm{lb}\left(p\alpha(1-\alpha)+p\frac{1-\alpha}{4}+\frac{q+r}{2}\right)\\
&- \left(p\cdot\frac{1-\alpha}{2}\right)\ \mathrm{lb}\left(p\cdot\frac{1-\alpha}{2}\right)\\
H_{xy}(p,q,r) &= -\left(p\alpha^2+p\cdot\frac{1-\alpha}{4}\right)\ \mathrm{lb}\left(p\alpha^2+p\cdot\frac{1-\alpha}{4}\right)-\left(\frac{q}{2}\right)\ \mathrm{lb}\left(\frac{q}{2}\right)-\left(\frac{r}{2}\right)\ \mathrm{lb}\left(\frac{r}{2}\right)\\
&- \left(p\alpha(1-\alpha)+p\frac{1-\alpha}{4}\right)\ \mathrm{lb}\left(p\alpha(1-\alpha)+p\frac{1-\alpha}{4}\right)-\left(\frac{q}{2}\right)\ \mathrm{lb}\left(\frac{q}{2}\right)\\
&- \left(\frac{r}{2}\right)\ \mathrm{lb}\left(\frac{r}{2}\right)-\left(p\cdot\frac{1-\alpha}{2}\right)\ \mathrm{lb}\left(p\cdot\frac{1-\alpha}{2}\right)
\end{aligned}
$$

С учетом $p+q+r=1$ запишем выражение для взаимной информации

$$I(p,q)=H_x(p,q,1-p-q)+H_y(p,q,1-p-q)-H_{xy}(p,q,1-p-q)$$

Пропускная способность канала определяется такими значениями **p,q**, для которых $I(p,q)$ принимает максимальное значение.

Решаем задачу на экстремум. В mathcad определим функции

$$G1(p,q):=\frac{d}{dp}I(p,q)\ \ simplify\rightarrow$$

$$G2(p,q):=\frac{d}{dq}I(p,q)\ \ simplify\rightarrow$$

и найдем ее корень на промежутке [0;1]: $x=\frac{1}{100}\qquad y=\frac{1}{100}$

$$Given$$

$$G1(x,y)=0\qquad G2(x,y)=0$$

$$\begin{pmatrix} xval\\ yval\end{pmatrix}:=Find(x,y)$$

$$xval = 0.47, \qquad yval = 0.42$$

Подставляя экстремальные значения $p^* = 0.45$, $q^* = 0.001$ получим пропускную способность канала связи

$$C = I(0.45, 0.001) = 0.0072bit. \quad \blacktriangle$$

Пример 2.6. По известной канальной матрице

$$p(\mathbf{y}|\mathbf{x}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0.8 & 0.2 \\ 0 & 0.3 & 0.7 \end{pmatrix}$$

определить скорость передачи и потери информации в канале с помехами, если входные символы сообщения появляются с вероятностями

$$p(\mathbf{x}) = (1/2, 1/3, 1/6).$$

Решение. Матрицу совместных вероятностей получим по формуле

$$\begin{aligned} p(\mathbf{x},\mathbf{y}) &= p(\mathbf{y}|\mathbf{x}) \times p(\mathbf{x}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0.8 & 0.2 \\ 0 & 0.3 & 0.7 \end{pmatrix} \times \begin{pmatrix} 1/2 \\ 1/3 \\ 1/6 \end{pmatrix} \\ &= \begin{pmatrix} 1 \cdot 1/2 & 0 \cdot 1/2 & 0 \cdot 1/2 \\ 0 \cdot 1/3 & 0.8 \cdot 1/3 & 0.2 \cdot 1/3 \\ 0 \cdot 1/6 & 0.3 \cdot 1/6 & 0.7 \cdot 1/6 \end{pmatrix} = \begin{pmatrix} 1/2 & 0 & 0 \\ 0 & 8/30 & 2/30 \\ 0 & 3/60 & 7/60 \end{pmatrix} \end{aligned}$$

Складывая элементы полученной матрицы, получим редуцированные законы распределения:
по строкам - для входного сигнала

$$p(\mathbf{x}) = (1/2, 1/3, 1/6).$$

по столбцам - для выходного сигнала

$$p(\mathbf{y}) = (1/2, 19/60, 11/60).$$

Вычисляем энтропию

$$\begin{aligned} H(x) &= \sum p(x)\ \mathrm{lb}p(x) = -\left(\frac{1}{2}\ \mathrm{lb}\frac{1}{2} + \frac{1}{3}\ \mathrm{lb}\frac{1}{3} + \frac{1}{6}\ \mathrm{lb}\frac{1}{6}\right) = 1.459 \\ H(y) &= \sum p(y)\ \mathrm{lb}p(y) = -\left(\frac{1}{2}\ \mathrm{lb}\frac{1}{2} + \frac{19}{60}\ \mathrm{lb}\frac{19}{60} + \frac{11}{60}\ \mathrm{lb}\frac{11}{60}\right) = 1.474 \\ H(xy) &= \sum p(xy)\ \mathrm{lb}p(xy) \\ &= -\left(\frac{1}{2}\ \mathrm{lb}\frac{1}{2} + \frac{8}{30}\ \mathrm{lb}\frac{8}{30} + \frac{2}{30}\ \mathrm{lb}\frac{2}{30} + \frac{3}{60}\ \mathrm{lb}\frac{3}{60} + \frac{7}{60}\ \mathrm{lb}\frac{7}{60}\right) = 1.847 \end{aligned}$$

Потери информации со стороны источника

$$H(y/x) = H(x,y) - H(x) = 1.847 - 1.459 = 0.388.$$

Потери информации со стороны приемника

$$H(x/y) = H(x,y) - H(y) = 1.847 - 1.474 = 0.373.$$

Скорость передачи информации

$$I(x,y) = H(x) + H(y) - H(x,y) = 1.459 + 1.474 - 1.847 = 1.086. \quad \blacktriangle$$

Задача 2.4. По каналу связи с ретранслятором передаются сигналы (**0,1,2**). Из-за наличия помех каждое значение сигнала не искажается с вероятностью $\alpha = \frac{1}{N}$ и принимает другие значения с равной вероятностью. Найти пропускную способность канала.

Пример 2.7. Имеется источник информации с энтропией в единицу времени H=100 (бит) и два канала связи; каждый из них может передавать в единицу времени F=70 бит (0 или 1): в результате помехи каждое значение бита заменяется противоположным с вероятностью . Требуется выяснить: достаточна ли пропускная способность этих каналов для передачи информации, поставляемой источником?

Решение. При отсутствии помех два канала с частотой генерации сигналов F=70 бит/сек. смогут обеспечить пропускную способность 2F=140 бит/сек., т.е. больше скорости источника H=100 бит/сек

При наличии помех пропускная способность двоичного симметричного канала уменьшается и определяется по формуле

$$C = F \cdot [1 + p \operatorname{lb} p + (1-p) \operatorname{lb}(1-p)] .$$

Тогда

$$p \operatorname{lb} p = 0.1 \cdot \operatorname{lb}(0.1) = -0.332, \quad (1-p) \operatorname{lb}(1-p) = 0.9 \operatorname{lb}(0.9) = -0.137$$

$$C = F \cdot (1 - 0.332 - 0.137] = 37.17 \; bit/s.$$

Максимальное количество информации, передаваемое по одному каналу в единицу времени C=37.17 бит/сек. Это означает, что два канала смогут обеспечить скорость 2C=74.34 бит/сек., т.е. меньше чем H=100 бит/сек., Поэтому при данном уровне помех двух каналов недостаточно для обеспечения передачи всей информации от источника.

Задача 2.5. Имеется источник информации с энтропией в единицу времени H бит и K каналов связи; каждый из которых может передавать в единицу времени F бит. В результате помехи каждое значение бита заменяется противоположным с вероятностью P. Требуется выяснить: достаточна ли пропускная способность этих каналов для передачи информации, поставляемой источником?

N	H	K	F	P	N	H	K	F	P
1	290	4	80	0.021	**16**	160	4	50	0.036
2	280	5	60	0.022	**17**	170	3	60	0.037
3	289	3	100	0.023	**18**	180	4	70	0.038
4	270	4	80	0.024	**19**	190	3	80	0.039
5	270	4	70	0.025	**20**	130	7	20	0.040
6	270	4	100	0.026	**21**	110	6	20	0.041
7	280	3	110	0.027	**22**	120	4	35	0.042
8	288	6	55	0.028	**23**	130	3	45	0.043
9	289	6	50	0.029	**24**	140	4	35	0.044
10	278	4	70	0.030	**25**	150	3	60	0.045
11	210	3	75	0.031	**26**	160	4	40	0.046
12	220	4	80	0.032	**27**	170	3	60	0.047
13	230	3	80	0.033	**28**	180	4	50	0.048
14	240	4	65	0.034	**29**	190	3	70	0.049
15	250	3	65	0.035	**30**	140	4	30	0.050

2.2 Теоремы Котельникова и Шеннона

Непрерывный сигнал характерен тем, что он задается для любых моментов времени на некотором отрезке длительности T. В противном случае сигнал не будет непрерывным. Однако применение всех видов импульсной модуляции принципиально связано с необходимостью дискретизации (квантования) сигнала по времени. При этом естественно поставить вопрос – какие условия необходимо соблюдать, чтобы обеспечить передачу непрерывного сигнала с надлежащей точностью при наличии его квантования по времени. Ответ на поставленный вопрос не является единственным – возможны различные решения.

Рассмотрим квантование непрерывного сигнала по времени в смысле Котельникова. Основным условием при этом является ограниченность спектра сигнала. Итак, пусть сигнал, представляющий собой непрерывную функцию времени $x(t)$, имеет ограниченный спектр.

Теорему Котельникова можно формулировать следующим образом.

Всякий непрерывный сигнал, со спектром, ограниченным ω_c, полностью определяется своими дискретными значениями в моменты отсчета, отстоящие друг от друга во времени на интервалы $\Delta t = 1/2\omega_c$

$$\mathrm{x}(t) = \sum_{k=-\infty}^{+\infty} x(k\Delta t)\frac{\sin\omega_c(t-k\Delta t)}{\omega_c(t-k\Delta t)}.$$

Базисную функцию $sinc(y) = sin(y)/y$, называют **функцией отсчетов**, а $x(k\Delta t)$ - отсчетами. Таким образом, если известны значения функции $x(t)$ в точках отсчета, то она может быть полностью восстановлена для всех t посредством суммирования типовых функций отсчетов с соответствующими коэффициентами.

Однако при практическом применении теоремы Котельникова возникают два принципиальных затруднения, не позволяющие использовать ее строго для интересующих нас сигналов.

Во-первых, всякий реальный сигнал имеет конечную длительность, т. е. бесконечно широкоий спектр, что противоречит основному условию теоремы Котельникова.

Во-вторых, для восстановления сигнала $x(t)$ на приемном конце связи по его значениям в моменты отсчета необходимо в приемнике генерировать функции отсчетов, а так как последние имеют бесконечную протяженность во времени для отрицательных значений t, соответствующие фильтры физически неосуществимы. Таким образом, сигнал при приеме может быть восстановлен только приближенно.

Однако отмеченные особенности теоремы Котельникова существенно затрудняют ее использование лишь в том случае, когда не делается никаких ограничений в точности воспроизведения передаваемого сигнала. На практике же никогда не требуется идеально точного воспроизведения, более того, такая постановка задачи противоречила бы реальным условиям работы систем связи и управления. Поэтому приближенный характер представления сигнала вполне возможен, если степень приближения не превосходит некоторых допустимых значений.

На практике используют 2 следствия теоремы Котельникова:

★ Любой аналоговый сигнал может быть восстановлен с какой угодно точностью по своим дискретным отсчётам, взятым с частотой $\omega > 2\omega_c$, где ω_c — максимальная частота, которой ограничен спектр реального сигнала.

★ Если максимальная частота в сигнале превышает половину **частоты дискретизации**, то способа восстановить сигнал из дискретного в аналоговый без искажений не существует.

Частота дискретизации (или частота семплирования, англ. sample rate) — частота взятия отсчетов непрерывного во времени сигнала при его дискретизации (в частности, аналого-цифровым преобразователем). Измеряется в Герцах.

Частота Найквиста — в цифровой обработке сигналов частота, равная половине частоты дискретизации. Названа в честь Гарри Найквиста. Из теоремы Котельникова следует, что при дискретизации аналогового сигнала потерь информации не будет только в том случае, если спектр (спектральная плотность) сигнала равен нулю выше частоты Найквиста.

Поэтому частоту дискретизации выбирают с запасом, к примеру, в аудио компакт-дисках используется частота дискретизации 44100 Герц, в то время как высшей частотой в спектре звуковых сигналов считается частота 20000 Гц.

Используемые частоты дискретизации звука:

8 000 Гц — телефон, достаточно для речи;
11 025 Гц; 16 000 Гц;
22 050 Гц — радио;
32 000 Гц;
44 100 Гц — используется в Audio CD;
48 000 Гц — DVD, DAT.
96 000 Гц — DVD-Audio (MLP 5.1)
192 000 Гц — DVD-Audio (MLP 2.0)
2 822 400 Гц — SACD Super audio
CD 5.1 — максимальная на 2008 г.

Клод Шеннон определил зависимость пропускной способности канала , обладающего определенной полосой пропускания F, от отношения сигнала S к шуму N

$$C = F \cdot \text{ lb}\left(1 + \frac{S}{N}\right).$$

Пример 2.8. Для стандартного телефонного канала $F = 3\ kHz$ и $S/N = 31\ db$ получим

$$C = F \cdot \text{ lb}\left(1 + \frac{S}{N}\right) = 3000 \cdot \text{ lb}\,(1 + 31) \simeq 15\ kb/s. \qquad \blacktriangle$$

Однако к данной формуле надо относится осторожно, поскольку из нее следует, что при нулевом уровне шума можно получить бесконечно большую скорость передачи информации.

Согласно **теореме Найквиста** максимальная скорость передачи данных C по каналу без шума определяется формулой:

$$C = 2F \cdot \text{ lb}(n),$$

где n - число дискретных уровней сигнала. Данная формула согласуется с теоремой Котельникова. При полосе сигнала F частота стробирования должна быть больше $2F$, чтобы принимающая сторона могла корректно восстановить форму исходного сигнала.

Пример 2.9. Для стандартного телефоного канала без шума с $F = 3kHz$ при $n = 2$ получим

$$C = 2F \cdot \text{ lb}(n) = 2 \cdot 3000 \cdot \text{ lb}(2) \simeq 6\ kb/s,$$

а при $n = 256$:

$$C = 2 \cdot 3000 \cdot \text{ lb}(256) = 6000 \cdot 8 \simeq 48\ kb/s. \qquad \blacktriangle$$

Задача 2.6. Пользуясь формулой Найквиста определить количество допустимых уровней сигнала n в телефонном канале связи с пропускной способностью $C\ kb/s$.

N	**C**	**N**	**C**	**N**	**C**	**N**	**C**	**N**	**C**	**N**	**C**	**N**	**C**	**N**	**C**	**N**	**C**	**N**	**C**
1	8	**4**	12	**7**	15	**10**	18	**13**	21	**16**	24	**19**	27	**22**	30	**25**	33	**28**	36
2	6	**5**	13	**8**	16	**11**	19	**14**	22	**17**	25	**20**	28	**23**	31	**26**	34	**29**	37
3	8	**6**	14	**9**	17	**12**	20	**15**	23	**18**	26	**21**	29	**24**	32	**27**	35	**30**	38

2.3 Теория массового обслуживания

2.3.1 Цепи Маркова

Неограниченная последовательность опытов с единственно возможными и попарно несовместными исходами $(s_1, s_2, ..., s_n)$ называется цепью Маркова, если вероятность любого из этих исходов в очередном опыте однозначно определяется результатом непосредственно предшествующего опыта. Совокупность несовместных исходов $s = (s_1, s_2, ..., s_n)$ называется вектором состояния системы, компоненты которого образует полную группу событий:

$$s_1 + s_2 + ... + s_n = 1.$$

Обозначения: $p_j^{(0)}$ - вероятность j-го исхода в первом опыте $(j = 1, 2, ..., m)$;

$$(p_1^{(0)} + p_2^{(0)} + ... + p_m^{(0)} = 1);$$

p_{ji}^n - вероятность j-го исхода в n-м опыте при условии, что в $(n-1)$ -м опыте наступил i-й исход, $(n = 2, 3, ...; i, j = 1, 2, ..., m; p_{1i}^{(n)} + p_{2i}^{(n)} + ... + p_{mi}^{(n)} = 1)$. Введенными вероятностями полностью описывается цепь Маркова.

Цепь Маркова называется однородной, если вероятность $p_{ij}^{(n)}$ от n не зависят, в этом случае они обозначаются без верхнего индекса: p_{ij}. Числа p_{ij} называются вероятностями переходов, а

$$P = (p_{ij}) = \begin{pmatrix} p_{11} & p_{12} & ... & p_{1m} \\ p_{21} & p_{22} & ... & p_{2m} \\ ... & ... & ... & ... \\ p_{m1} & p_{m2} & ... & p_{mm} \end{pmatrix}$$

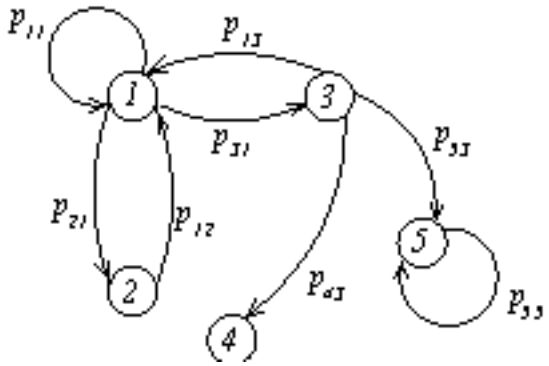
- матрицей перехода.

По матрице перехода можно построить граф состояний, если в качестве узлов взять состояния $s = (s_1, s_2, ..., s_n)$ системы, а стрелками – возможные переходы из одного состояния в другое состояние.

Например, для матрицы перехода

$$P = \begin{pmatrix} p_{11} & p_{12} & p_{13} & 0 & 0 \\ p_{21} & 0 & 0 & 0 & 0 \\ p_{31} & 0 & 0 & 0 & 0 \\ 0 & 0 & p_{43} & 0 & 0 \\ 0 & 0 & p_{53} & 0 & p_{55} \end{pmatrix}$$

граф состояния имеет вид



Обозначим: $p_{ij}(n)$ – вероятность того, что через n шагов произойдет переход от s_j к s_i $(i, j = 1, 2, ..., m)$, $P(n)$ – матрицу переходов за n шагов, т.е. матрицу, состоящую из $p_{ij}(n)$. Если в начальный момент система находилась в состоянии $s^0 = (s_1, s_2, ..., s_n)$, то на следующем шаге она перейдет в состояние

$$s^1 = Ps^0.$$

На втором шаге состояние системы есть:

$$s^2 = Ps^1 = PPs^0 = P^2s^0.$$

Очевидно, что через n шагов состояние системы s^n будет выражаться через исходное состояние системы s^0 формулой

$$s^n = P^n s^0.$$

Т.о. справедлива формула

$$P(n) = P^n.$$

Теорема Маркова (о предельных вероятностях): если существует такое натуральное число n_0, что все элементы матрицы $P(n_0) = P^{n_0}$ строго положительны, то для каждого $(j = 1, 2, ..., m)$ существует предельная вероятность $\lim\limits_{n\to\infty} P(n) = P^*$.

Предельные вероятности (если они существуют) можно найти из уравнений:

$$Ps = s, \quad \text{или} \quad p_{ij}s_j = \delta_{ij}s_j, \quad (p_{ij} - \delta_{ij})\, s_j = 0.$$

Перепишем задачу в матричном виде $(P - I)s = 0$:

$$\begin{pmatrix} p_{11}-1 & p_{12} & ... & p_{1n} \\ p_{21} & p_{22}-1 & ... & p_{2n} \\ ... & ... & ... & ... \\ p_{n1} & p_{n2} & ... & p_{nn}-1 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ ... \\ s_n \end{pmatrix} = 0.$$

Таким образом, вместе с условием нормировки на компоненты вектора состояния, задача на отыскание предельного состояния сводится к решению системы уравнений:

$$\begin{cases} (p_{11}-1)s_1 + p_{12}s_2 + ... + p_{1n}s_n = 0 \\ p_{21}s_1 + (p_{22}-1)s_2 + ... + p_{21}s_n = 0 \\ ... \\ p_{n1}s_1 + p_{n2}s_2 + ... + (p_{nn}-1)s_n = 0 \\ s_1 + s_2 + ... + s_n = 1 \end{cases}.$$

Поскольку данная система переопределена (в ней содержится лишнее уравнение), то из него можно вычеркнуть одно уравнение. Нежелательно вычеркивать последнее уравнение нормировки вектора состояния.

Пример 2.10. Пусть (A_1, A_2, A_3) – точки числовой оси с целочисленными координатами $(x = 1, x = 2, x = 3)$. Представим себе частицу, которая движется по этим точкам следующим образом: если в какой-то момент времени $t = n$ $(n = 0, 1, 2, 3, ...)$ частица находится во внутренней точке A_2, то в следующий момент $t = n + 1$ она переходит в A_1 с вероятностью q или в A_3 – с вероятностью $p = 1 - q$; если частица оказалась в левой граничной точке A_1, то в следующий момент времени с вероятностью q она там остается или с вероятностью p возвращается в A_2; если же частица оказалась в правой граничной точке A_3, то в следующий момент времени она там остается с вероятностью или возвращается в A_2 с вероятностью q.

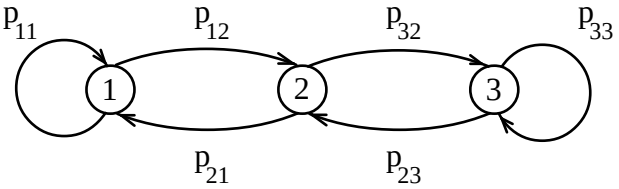
а) Найдите матрицу переходов и постройте ее граф состояний.

б) Найдите матрицу переходов за 2 шага.

в) Проверьте существование предельных состояний.

г) Если существуют предельные состояния, то найдите их.

Решение. а) Изобразим граф состояний.



Напомним, что начальному состоянию перехода соответствует второй индекс k, а конечному первый индекс i матрицы p_{ik}. Находим вероятности переходов p_{ik} за один шаг:

$$p_{11} = q, p_{21} = p, p_{12} = q, p_{32} = p, p_{23} = q, p_{33} = p.$$

В результате матрица переходов имеет вид:

$$P = \begin{pmatrix} q & q & 0 \\ p & 0 & q \\ 0 & p & p \end{pmatrix}.$$

В качестве проверки, заметим, что сумма элементов по столбцам матрицы равна 1, согласно условию нормировки для вектора состояния.

б) Для нахождения $P(2)$ вычисляем P^2:

$$P(2) = P^2 = \begin{pmatrix} q & q & 0 \\ p & 0 & q \\ 0 & p & p \end{pmatrix} \cdot \begin{pmatrix} q & q & 0 \\ p & 0 & q \\ 0 & p & p \end{pmatrix} = \begin{pmatrix} q & q^2 & q^2 \\ pq & 2pq & pq \\ p^2 & p^2 & p \end{pmatrix}.$$

в) Так как все элементы P^2 строго положительны, то условие теоремы Маркова о предельных вероятностях выполняется. Следовательно, предельные вероятности (s_1^*, s_2^*, s_3^*) существуют.
г) Для нахождения предельных состояний решим систему:

$$\begin{pmatrix} q-1 & q & 0 \\ p & 0-1 & q \\ 0 & p & p-1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = 0$$

с дополнительным условием $s_1 + s_2 + s_3 = 1$:

$$\begin{cases} (q-1)s_1 + qs_2 + 0 \cdot s_3 = 0 \\ ps_1 + (0-1)s_2 + qs_3 = 0 \\ 0 \cdot s_1 + ps_2 + (p-1)s_3 = 0 \\ s_1 + s_2 + s_3 = 1 \end{cases}$$

Поскольку система переопределена, вычеркнем любое уравнение (кроме последнего):

$$\begin{cases} (q-1)s_1 + qs_2 + 0 \cdot s_3 = 0 \\ ps_1 + (0-1)s_2 + qs_3 = 0 \\ s_1 + s_2 + s_3 = 1 \end{cases} .$$

Решая систему, получим:

$$s_1 = \frac{q^2}{q^2+pq+p^2}, \quad s_2 = \frac{pq}{q^2+pq+p^2}, \quad s_3 = \frac{p^2}{q^2+pq+p^2}. \quad \blacktriangle$$

2.3.2 Работа телефонного коммутатора

Пример 2.11. Исследуемая система (коммутатор) может принимать два состояния: она может быть свободной в момент времени t с вероятностью $P_0(t)$ и занятой с вероятностью $P_1(t)$. Если линия свободна, то за промежуток времени Δt на коммутатор приходит сигнал с вероятностью $\alpha\Delta t$, и переводит систему в состояние занято. Если коммутатор занят, то с вероятностью $\beta\Delta t$ он обрабатывает сигнал и переходит в состояние свободно. Найти предельное состояние системы при $\alpha = 0.5;\ \beta = 0.3$.

Решение. Допустим, что в момент времени $(t + \Delta t)$ система была свободна. Это означает, что в предыдущий момент времени t:

1. система находилась в состоянии свободно $P_0(t)$ и на нее не пришел сигнал (вероятность непоступления сигнала равна $1 - \alpha\Delta t$);

2. система находилась в состоянии занято $P_1(t)$, но за промежуток времени Δt запрос был обработан с вероятностью $\beta\Delta t$.

Тогда по формуле полной вероятности получим:

$$P_0(t+\Delta t) = P_0(t)(1-\alpha\Delta t) + P_1(t)\beta\Delta t$$

или

$$P_0(t+\Delta t) - P_0(t) = -P_0(t)\alpha\Delta t + P_1(t)\beta\Delta t.$$

Разделим обе части уравнения на Δt и возьмем предел $\Delta t \to 0$

$$\lim_{\Delta t\to 0} \frac{P_0(t+\Delta t) - P_0(t)}{\Delta t} = -P_0(t)\alpha + P_1(t)\beta$$

Поскольку, по определению производной

$$\lim_{\Delta t\to 0} \frac{P_0(t+\Delta t) - P_0(t)}{\Delta t} = \frac{dP_0(t)}{dt} = P_0',$$

то мы получили дифференциальное уравнение первого порядка

$$P_0' = -P_0\alpha + P_1\beta.$$

Теперь допустим, что в момент времени $(t+\Delta t)$ система была занята. Это означает, что в предыдущий момент времени t:

1. система находилась в состоянии свободно (с вероятностью $P_0(t)$) и на нее пришел сигнал (вероятость поступления сигнала равна $\alpha\Delta t$);

2. система находилась в состоянии занято (с вероятностью $P_1(t)$) и за промежуток времени Δt запрос так и не был обработан (вероятность необработки сигнала равна $1-\beta\Delta t$).

Тогда, по формуле полной вероятности получим:

$$P_1(t+\Delta t) = P_0(t)\alpha\Delta t + P_1(t)(1-\beta\Delta t),$$

или

$$P_1(t+\Delta t) - P_1(t) = P_0(t)\alpha\Delta t - P_1(t)\beta\Delta t.$$

Разделим обе части уравнения на Δt и возьмем предел $\Delta t \to 0$:

$$P_1' = \alpha P_0 - \beta P_1.$$

Предполагая, что в начальный момент времени $t = 0$ система была свободной (с вероятностью $P_0(0) = 1$ (тогда $P_1(0) = 0$)) мы получим систему дифференциальных уравнений

$$\begin{cases} P_0' = -\alpha P_0 + P_1\beta, & P_0(0) = 1, \\ P_1' = P_0\alpha - P_1\beta, & P_1(0) = 0. \end{cases}$$

Для получения данного решения в математическом пакете **Maple** необходимо ввести следующие операторы задающие систему дифференциальных уравнений:

$> s1 := diff(p0(t), t) + a * p0(t) - b * p1(t);$ (нажать Shift+Enter)

$s2 := diff(p1(t), t) - a * p0(t) + b * p1(t);$ (нажать Enter)

$$s1 := \left(\frac{d}{dt}(p0(t)\right) + ap0(t) - bp1(t)$$

$$s2 := \left(\frac{d}{dt}(p1(t)\right) - ap0(t) + bp1(t)$$

Решение ищем с учетом краевых условий ($p_0(0) = 1, p_1(0) = 0$):

$> dsolve([s1, s2, p0(0) = 1, p1(0) = 0], p0(t), p1(t));$ ↲

$$p0(t) = \frac{\beta}{\beta + \alpha} + \frac{\alpha}{\beta + \alpha} e^{-(\beta+\alpha)t}$$

$$p1(t) = \frac{\alpha}{\beta + \alpha} - \frac{\alpha}{\beta + \alpha} e^{-(\beta+\alpha)t}$$

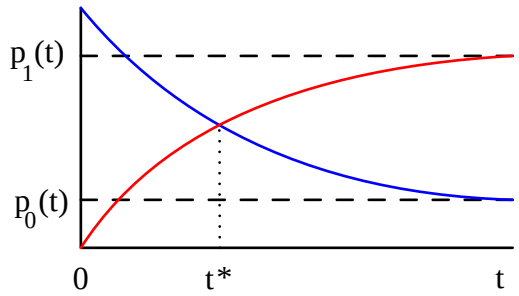
Для конкретных значений $\alpha = 0.5$; $\beta = 0.3$ несложно получить и графики зависимости состояния системы $p0(t)$ и $p1(t)$ от времени

$> a := 0.5; b := 0.3;$ ↲

$p0(t) := b/(a + b) + a * exp((-a - b) * t)/(a + b);$ ↲

$p1(t) := (-a * exp((-a - b) * t) * b/(a + b) + a * b/(a + b))/b;$ ↲

$> plot([p0(t), p1(t)], t = 0..5);$ ↲



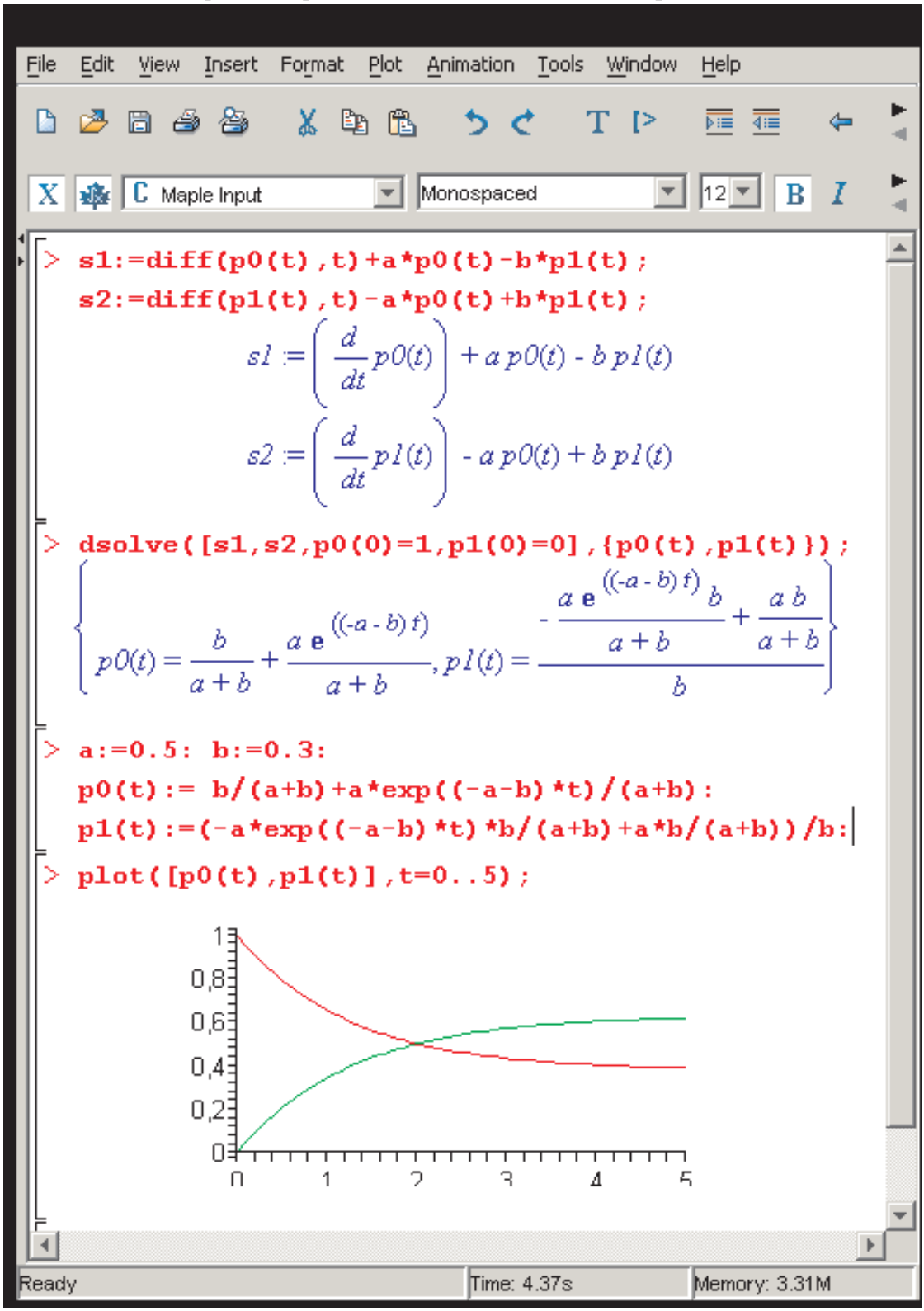
При $t \to \infty$ предельные состояния системы имеют вид

$$P_0(t) = \frac{\beta}{\alpha + \beta}, \qquad P_1(t) = \frac{\alpha}{\alpha + \beta}.$$

Из графика видно, что кривая вероятности свободного состояния пересекается с кривой загруженного состояния.

Это означает, что после достижения некоторого времени t^* система перестанет справляется с потоком заявок. Поэтому необходимо либо увеличивать производительность системы (уменьшить время обслуживания заявки), либо уменьшить сам поток заявок. ▲

Ниже показан скриншот решения данной задачи в **Maple**.



Пример 2.12. Исследуется микропроцессор, рассчитанный на одновременное обслуживание 3 контроллеров. Найти предельное состояние системы, если вероятность поступления прерывания на микропроцессор за промежуток времени Δt равна $\alpha\Delta t$. Вероятность обработки прерывания за промежуток времени Δt равна $\beta\Delta t$. ($\alpha = 0.3\,,\ \beta = 0.5$)

Решение.

Обозначим через $P_0(t)$ вероятность того, что микропроцессор свободен (на него не поступило ни одного прерывания). Тогда $P_1(t)$ - вероятность обработки микропроцессором одного прерывания, $P_2(t)$ - двух прерываний, $P_3(t)$-трех прерываний. Введем обозначения для следующих состояний микропроцессора:

x_0- свободен;

x_1- занят ровно один вход

x_2-занято два входа

x_3-заняты все три входа.

0. Допустим, что в момент времени $(t+\Delta t)$ система была свободна. Это означает, что в предыдущий момент времени t:

1. система находилась в состоянии свободно x_0 (с вероятностью $P_0(t)$) и на нее не пришел сигнал (вероятность непоступления сигнала равна $1-\alpha\Delta t$);

2. система находилась в состоянии занято x_1 , (с вероятностью $P_1(t)$), но за промежуток времени Δt запрос был обработан с вероятностью $\beta\Delta t$.

Тогда по формуле полной вероятности получим:

$$P_0(t+\Delta t) = P_0(t)(1-\alpha\Delta t) + P_1(t)\beta\Delta t$$

или

$$P_0(t+\Delta t) - P_0(t) = -P_0(t)\alpha\Delta t + P_1(t)\beta\Delta t.$$

Разделим обе части уравнения на Δt и возьмем предел $\Delta t \to 0$

$$\lim_{\Delta t\to 0}\frac{P_0(t+\Delta t) - P_0(t)}{\Delta t} = -P_0(t)\alpha + P_1(t)\beta$$

Поскольку, по определению производной

$$\lim_{\Delta t\to 0}\frac{P_0(t+\Delta t) - P_0(t)}{\Delta t} = \frac{dP_0(t)}{dt} = P_0',$$

то мы получили дифференциальное уравнение первого порядка

$$P_0^{'} = -P_0\alpha + P_1\beta.$$

1. Теперь допустим, что в момент времени $(t+\Delta t)$ микропроцессор был занят обработкой одного прерывания. Это означает, что в предыдущий момент времени t:

1. система находилась в состоянии x_0 свободно (с вероятностью $P_0(t)$) и на нее пришел сигнал (вероятность поступления сигнала равна $\alpha\Delta t$);
2. система находилась в состоянии x_1 и за промежуток времени Δt система не обработала прерывание и на нее не пришел ни один сигнал (вероятность $1 - \alpha\Delta t - \beta\Delta t$).
3. система находилась в состоянии x_2 и за промежуток времени Δt обработал один запрос из двух (вероятность $2\beta\Delta t$).

Тогда по формуле полной вероятности получим:

$$P_1(t + \Delta t) = P_0(t)\alpha\Delta t + P_1(t)(1 - \alpha\Delta t - \beta\Delta t) + 2\beta\Delta t P_2(t),$$

или

$$P_1(t + \Delta t) - P_1(t) = P_0(t)\alpha\Delta t - (\alpha + \beta)P_1(t)\Delta t + 2P_2(t)\beta\Delta t.$$

Разделим обе части уравнения на Δt и возьмем предел $\Delta t \to 0$:

$$P_1' = \alpha P_0 - (\alpha + \beta)P_1 + 2\beta P_2.$$

2. Теперь допустим, что в момент времени $(t + \Delta t)$ микропроцессор находился в состоянии x_2 (был занят обработкой двух прерываний). Это означает, что в предыдущий момент времени t:

1. система находилась в состоянии x_1 (с вероятностью $P_1(t)$) и на нее пришел сигнал (с вероятностью $\alpha\Delta t$);
2. система находилась в состоянии x_2 (с вероятностью $P_2(t)$) и за промежуток времени Δt запрос так и не был обработан и не пришел ни один запрос (вероятность $1 - \alpha\Delta t - 2\beta\Delta t$).
3. микропроцессор был полностью загружен обработкой трех прерываний (с вероятностью $P_3(t)$) и за промежуток времени Δt обработал одно из 3 прерываний. Т.е. перешел из состояния x_3 в состояние x_2 с вероятностью $3\beta\Delta t$.

Тогда по формуле полной вероятности получим:

$$P_2(t + \Delta t) = P_1(t)\alpha\Delta t + P_2(t)(1 - \alpha\Delta t - 2\beta\Delta t) + 3\beta\Delta t P_3(t),$$

или

$$P_2(t + \Delta t) - P_2(t) = P_1(t)\alpha\Delta t - P_2(t)(\alpha + 2\beta)\Delta t + P_3(t)3\beta\Delta t.$$

Разделим обе части уравнения на Δt и возьмем предел $\Delta t \to 0$:

$$P_2' = \alpha P_1 - (\alpha + 2\beta)P_2 + 3\beta P_3.$$

3. Теперь допустим, что в момент времени $(t + \Delta t)$ микропроцессор находился в состоянии x_3 (был полностью загружен). Это означает, что в предыдущий момент времени t:

1. система находилась в состоянии x_2 (с вероятностью $P_2(t)$) и на нее пришел сигнал (с вероятностью $\alpha\Delta t$);

2. система находилась в состоянии x_3 (с вероятностью $P_3(t)$) и за промежуток времени Δt запрос так и не был обработан ни один из 3 запросов (вероятность необработки сигналов равна $1 - 3\beta\Delta t$).

Тогда по формуле полной вероятности получим:

$$P_3(t + \Delta t) = P_2(t)\alpha\Delta t + P_3(t)(1 - 3\beta\Delta t),$$

или

$$P_3(t + \Delta t) - P_3(t) = P_2(t)\alpha\Delta t - 3P_3(t)\beta\Delta t.$$

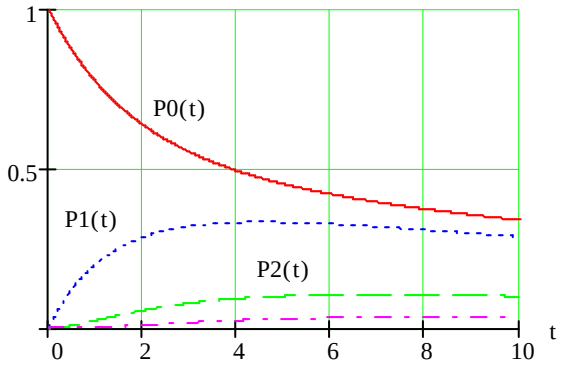
Разделим обе части уравнения на Δt и возьмем предел $\Delta t \to 0$:

$$P_3^{'} = \alpha P_2 - 3\beta P_3.$$

Предполагая, что в начальный момент времени $t = 0$ система была свободной (с вероятностью $P_0(0) = 1$ (тогда $P_1(0) = 0, \;\; P_2(0) = 0, \;\; P_3(0) = 0$) мы получим систему дифференциальных уравнений

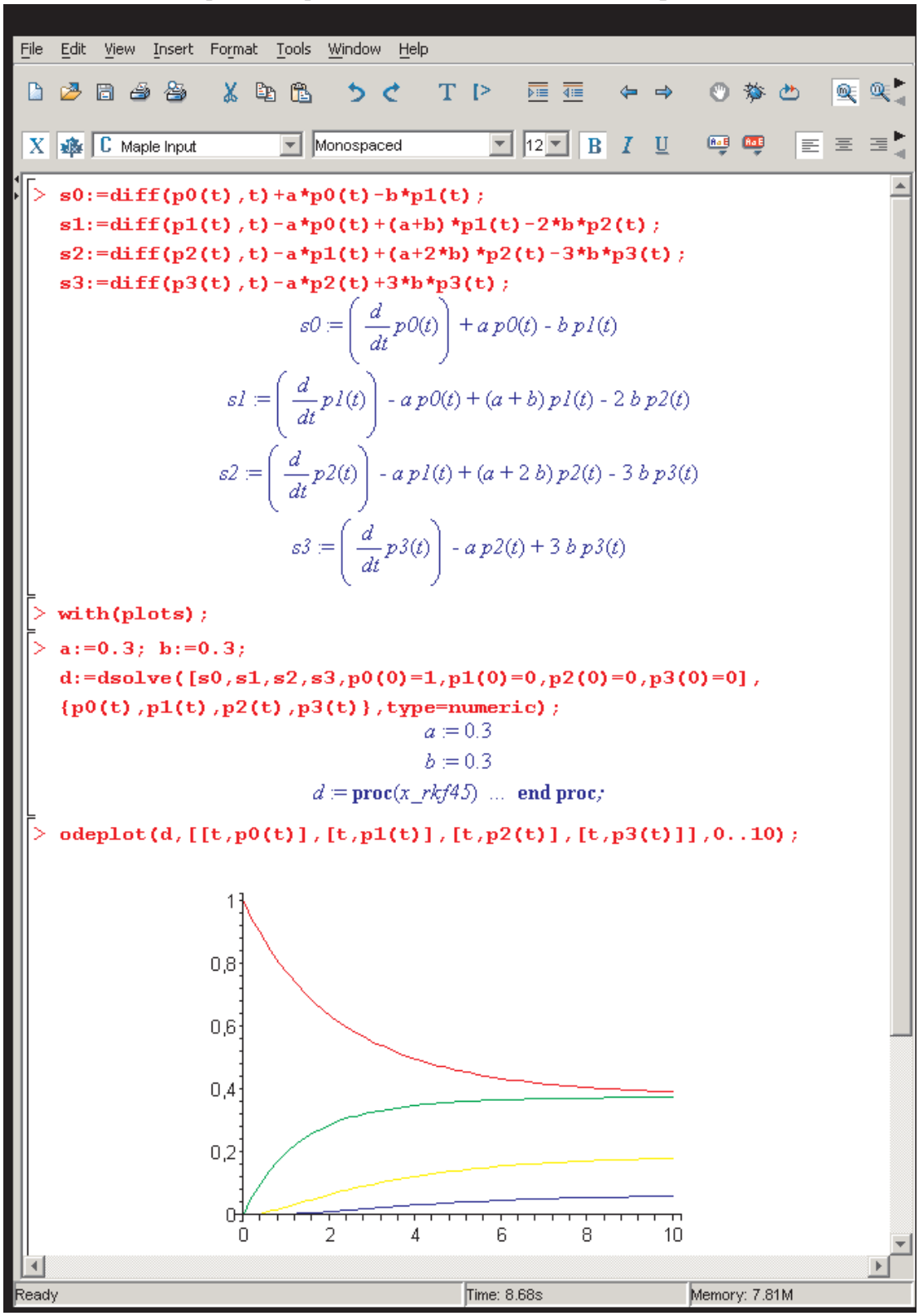
$$\begin{cases} P_0^{'} = -\alpha P_0 + P_1\beta, & P_0(0) = 1, \\ P_1^{'} = P_0\alpha - (\alpha + \beta)P_1 + 2P_2\beta, & P_1(0) = 0, \\ P_2^{'} = P_1\alpha - (\alpha + 2\beta)P_2 + 3P_3\beta, & P_2(0) = 0, \\ P_3^{'} = P_2\alpha - 3P_3\beta, & P_3(0) = 0. \end{cases}$$

Для конкретных значений $\alpha = 0.3; \;\; \beta = 0.5$ график решений принимает вид



Из графика видно, что кривые вероятности свободного состояния $P_0(t)$ не пересекается с кривыми загруженного состояния. Это означает, что система справляется с потоком заявок и ее производительности хватает на обслуживание всех прерываний. ▲

Ниже показан скриншот решения данной задачи в **Maple**.



Задача 2.7. Рассматривается работа офисной мини-АТС, рассчитанной на одновременное обслуживание n абонентов (n-канальная система). Найти предельное состояние системы.

N	n	α	β	**N**	n	α	β	**N**	n	α	β
1	5	0.21	0.36	**11**	5	0.11	0.31	**21**	5	0.21	0.19
2	6	0.22	0.37	**12**	6	0.12	0.32	**22**	6	0.22	0.20
3	7	0.23	0.38	**13**	7	0.13	0.33	**23**	7	0.23	0.21
4	8	0.24	0.39	**14**	8	0.14	0.34	**24**	8	0.24	0.22
5	9	0.25	0.40	**15**	9	0.15	0.35	**25**	9	0.25	0.23
6	5	0.26	0.41	**16**	5	0.16	0.49	**26**	5	0.26	0.24
7	6	0.27	0.42	**17**	6	0.17	0.50	**27**	6	0.27	0.25
8	7	0.28	0.43	**18**	7	0.18	0.21	**28**	7	0.28	0.46
9	8	0.29	0.44	**19**	8	0.19	0.33	**29**	8	0.29	0.47
10	9	0.30	0.45	**20**	9	0.20	0.34	**30**	9	0.30	0.48

2.3.3 Система массового обслуживания с ожиданием

Рассмотрим ситуацию, в которой заявка, заставшая все n каналов занятыми, становится в очередь и ждет, пока не освободится какой либо канал. Очевидно, что для постановки заявки в очередь должны быть выделены соответствующие ресурсы (объем кэш-памяти процессора, количество мест в приемной у начальника). Если ресурсы (места) для ожидания заполнены, то заявка в очередь не становится. Обозначим
$\alpha\Delta t$- вероятность поступления заявки в систему;
$\beta\Delta t$- вероятность обслуживания заявки;
$\gamma\Delta t$- вероятность ухода заявки из очереди.

В общем случае n-канальная система с k-разрядной памятью (память удерживающая k-заявок) может принимать следующие состояния

x_0-все каналы свободны;
x_1-один канал занят;
x_2-два канала заняты;
...
x_n-все n-каналов заняты;
x_{n+1}-все каналы заняты и одна заявка в очереди;
x_{n+2}-занято два места в очереди;
...
x_{n+k}-заняты все n-каналов и k-мест в очереди.

Система дифференциальных уравнений для данного случая принимает вид

$$\begin{cases} P_0' = -\alpha P_0 + \beta P_1 \\ P_1' = P_0\alpha - (\alpha+\beta)P_1 + 2\beta P_2 \\ P_2' = P_1\alpha - (\alpha+2\beta)P_2 + 3\beta P_3 \\ \dots \\ P_{n-1}' = P_{n-2}\alpha - (\alpha+(n-1)\beta)P_{n-1} + n\beta P_n \\ P_n' = P_{n-1}\alpha - (\alpha+n\beta)P_n + (n\beta+\gamma)P_{n+1} \\ P_{n+1}' = P_n\alpha - (\alpha+n\beta+\gamma)P_{n+1} + (n\beta+2\gamma)P_{n+2} \\ P_{n+2}' = P_{n+1}\alpha - (\alpha+n\beta+2\gamma)P_{n+2} + (n\beta+3\gamma)P_{n+3} \\ \dots \\ P_{n+k}' = P_{n+k-1}\alpha - (n\beta+k\gamma)P_{n+k} \end{cases}$$

Начальные условия $P_0(0) = 1,\ \ P_1(0) = P_2(0) = P_3(0) = P_4(0) = \dots = P_{n+k}(0) = 0.$

Пример 2.13. На 3 канальный коммутатор с 2 разрядной памятью приходит поток заявок. Вероятность поступления заявки на коммутатор за промежуток времени Δt равна $\alpha\Delta t$; вероятность обслуживания $\beta\Delta t$; вероятность ухода заявки из очереди $\gamma\Delta t$.

Найти предельное состояние системы при $\alpha = 0.5;\ \ \beta = 0.3.$

Решение.

Система может принимать одно из следующих возможных состояний:

x_0-ни один канал не занят

x_1-занят ровно один канал

x_2-занято два канала

x_3-заняты три канала

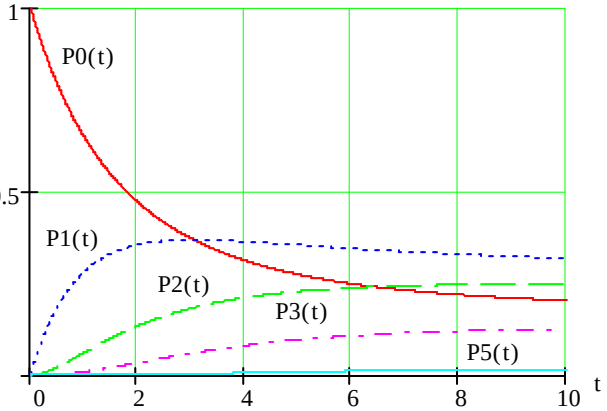
x_4-заняты все каналы, и одна заявка стоит в очереди

x_5- заняты все каналы, и две заявки стоит в очереди

Тогда, система дифференциальных уравнений для соответствующих вероятностей имеет вид:

$$\begin{cases} P_0' = -P_0\alpha + P_1\beta \\ P_1' = P_0\alpha - (\alpha+\beta)P_1 + 2\beta P_2 \\ P_2' = P_1\alpha - (\alpha+2\beta)P_2 + 3\beta P_3 \\ P_3' = P_2\alpha - (\alpha+3\beta)P_3 + (3\beta+\gamma)P_4 \\ P_4' = P_3\alpha - (\alpha+3\beta+\gamma)P_4 + (3\beta+2\gamma)P_5 \\ P_5' = P_4\alpha - (3\beta+2\gamma)P_5 \end{cases}$$

Начальные условия $P_0(0) = 1,$
$P_1(0) = P_2(0) = P_3(0) = P_4(0) = P_5(0) = 0.$



Для конкретных значений $\alpha = 0.5;\ \ \beta = 0.3;\ \ \gamma = 0.1$ график решений принимает вид, показанный на рисунке.

Задача 2.8. Рассматривается работа офисной мини-АТС, рассчитанной на одновременное обслуживание n абонентов (n-канальная система), которая может держать в памяти (на очереди k вызовов). Найти предельное состояние системы.

№	n	k	α	β	γ	№	n	k	α	β	γ
1	2	4	0.11	0.36	0.21	**16**	3	3	0.11	0.21	0.36
2	3	5	0.12	0.37	0.22	**17**	4	4	0.12	0.22	0.37
3	4	6	0.13	0.38	0.23	**18**	5	5	0.13	0.23	0.38
4	5	7	0.14	0.39	0.24	**19**	6	6	0.14	0.24	0.39
5	6	8	0.15	0.40	0.25	**20**	7	5	0.15	0.25	0.40
6	7	7	0.16	0.41	0.26	**21**	8	4	0.16	0.26	0.41
7	8	6	0.17	0.42	0.27	**22**	9	3	0.17	0.27	0.42
8	9	5	0.18	0.43	0.28	**23**	8	3	0.18	0.28	0.43
9	8	4	0.19	0.44	0.29	**24**	7	3	0.19	0.29	0.44
10	7	3	0.20	0.45	0.30	**25**	6	4	0.20	0.30	0.45
11	6	4	0.21	0.46	0.31	**26**	5	4	0.21	0.31	0.46
12	5	5	0.22	0.47	0.32	**27**	4	4	0.22	0.32	0.47
13	4	6	0.23	0.48	0.33	**28**	3	5	0.23	0.33	0.48
14	3	7	0.24	0.49	0.34	**29**	4	3	0.24	0.34	0.49
15	4	8	0.25	0.50	0.35	**30**	5	4	0.25	0.35	0.50

2.4 Стандарт сотовой связи GSM

GSM сначала означало Groupe Special Mobile, по названию группы анализа, которая создавала стандарт. Теперь он известен как Global System for Mobile Communications (Глобальная Система для Мобильной Связи), хотя слово «Связь» не включается в сокращение.

Система синхронизации рассчитана на компенсацию абсолютного времени задержки сигналов до 233 мкс, что соответствует максимальной дальности связи или максимальному радиусу ячейки (соты) 35 км.

Общая скорость преобразования речевого сигнала - 13 кбит/с.

Скорость передачи сообщений в радиоканале, кбит/с 270, 833

Скорость преобразования речевого кодека, кбит/с 13

Ширина полосы канала связи, кГц 200

Максимальное количество каналов связи 124

Максимальное количество каналов, организуемых в базовой станции 16-20

GSM 900

BS	$935MHz$			$\Leftarrow$ $25MHz$ $\Rightarrow$			$960MHz$
	$\Uparrow$			125×200			$\Uparrow$
	$45MHz$						$45MHz$
	$\Downarrow$						$\Downarrow$
MS	$890MHz$	$200KHz$	$200KHz$	...	$200KHz$	$200KHz$	$915MHz$
№ канала			1	...	123	124	

Стандарт GSM разработан для создания сотовых систем подвижной связи в следующих полосах частот: 890-915 МГц - для передачи мобильными станциями (телефоном) (линия "вверх"); 935-960 МГц- для передачи базовыми станциями (сотовой антенной) (линия "вниз").

Каждая из полос, выделенных для сетей GSM, разделяется на частотные каналы. Разнос каналов составляет 200 кГц, что позволяет организовать в сетях GSM 124 частотных канала. Частоты, выделенные для передачи сообщений подвижной станцией на базовую и в обратном направлении, группируются парами, организуя дуплексный канал с разносом 45 МГц. Эти пары частот сохраняются и при перескоках частоты. Каждая сота характеризуется фиксированным присвоением определенного количества пар частот.

Если обозначить FI (n) - номер несущей частоты в полосе 890-915 МГц, Fu (n) - номер несущей частоты в полосе 935-960 МГц, то частоты каналов определяются по следующим формулам: FI (n) = 890,2 + 0,2 (n-1), МГц; Fu (n) = FI (n) + 45, МГц; 1<n<124.

Этим каналам присваиваются номера (n) от 0 до 123. Тогда частоты восходящего (FR) и нисходящего (FF) направлений каждого из каналов можно вычислить по формулам: FR(n) = 890+0.2n (МГц), FF(n) = FR(n) + 45 (МГц).

Аналогичное разделение организуется и для GSM-1800. Для передатчиков сотового телефона выделяются частоты 1710-1785 MHz, а для передатчиков базовых станций: 1805-1880 MHz. Тогда при ширине в 200 KHz в каждом направлении выделяется 374 канала с разносом частоты в 95 MHz.

GSM 1800

BS	$1805MHz$		$\Leftarrow$	$75MHz$	$\Rightarrow$		$1880MHz$
	$\Uparrow$			375×200			$\Uparrow$
	$95MHz$						$95MHz$
	$\Downarrow$						$\Downarrow$
MS	$1710MHz$	$200KHz$	$200KHz$	...	$200KHz$	$200KHz$	$1785MHz$
№ канала			1	...	373	374	

Одна базовая станция стандарта GSM обычно способна поддерживать до 12 передатчиков, а каждый передатчик способен одновременно поддерживать связь с 8-ю общающимися абонентами (8 каналов). Один из каналов выделяется как управляющий канал или **канал вызова**. Все БС системы соединены с АТС по выделенным проводным (оптическими) или радиорелейным каналам связи.

Работа MS

Каждый мобильный телефон имеет кнопку **положение трубки**, которая может быть в состоянии трубка **поднята** и трубка **положена**. Когда «трубка положена», телефон постоянно сканирует либо все каналы системы, либо только управляющие. Во время набора номера радиотелефон занимает тот свободный канал, уровень сигнала в котором особенно велик. По мере удаления абонента от данной базовой станции и

перемещения его в зону действия другой БС, уровень сигнала падает и качество разговора ухудшается. Специальная процедура, называемая передачей управления вызовом или «эстафетной передачей» (в иностранной технической литературе - handover или handoff), позволяет переключить разговор на свободный канал другой БС, в зоне действия которой оказался абонент. Для осуществления «эстафетной передачи» БС снабжена специальным приемником, периодически измеряющим уровень сигнала сотового телефона и сравнивающего его с допустимым пределом. Если сигнал слишком мал, информация об этом автоматически передается на коммутатор. ЦКП выдает команду об измерении уровня сигнала на ближайшие к нему базовые станции. После чего разговор переключается на ту из них, где величина измеренного сигнала оказалась наибольшей. Все занимает доли секунды. В зависимости от загруженности каналов телефон так же может выбирать между сетью 900 и 1800 МГц, причем переключение возможно даже во время разговора абсолютно незаметно для говорящего.

Вызов подвижного абонента. Для поиска мобильного абонента всеми базовыми станциями системы по управляющим каналам передается «широковещательный» сигнал вызова. Сотовый телефон, который постоянно сканирует каналы (обычно управляющие), отвечает на одном из них. Базовые станции, принявшие ответный сигнал, передают информацию на коммутатор, который, в свою очередь, переключает разговор на ту БС. Где после измерения уровень сигнала оказался наибольшим.

Базовая станция

Рассмотрим подробнее принципы работы базовых станций.

Антенна

Базовая станция осуществляет связь с абонентами при помощи приемо-передатчиков (TRX - transmitter/receiver). 1 базовая станция может обслуживать до 24 приемо-передатчиков (антенн).

Антенны бывают: 360°, 120°, 60°, поэтому можно создавать соты с 1 антенной, и теоретически построить сеть из 24 сот на 1 БС. Ширины диаграммы направленности антенн в вертикальной плоскости, составляющей обычно менее 10°. Часто антенны, размещенные на мачте, имеют незначительный угол наклона, то есть они слегка опущены вниз таким образом, чтобы специально ограничить радиус действия станций. Это позволяет, в связи с выше сказанным, неоднократно использовать одни и те же каналы на других базовых станциях, расположенных на относительно небольшом расстоянии.

В распоряжение каждой базовой станции может быть предоставлено от одной до 16 частот

По статистическим оценкам количество звонящих составляет 16 чел. на 1000 абонентов. Поэтому на 500 чел. хватит 1 антенны (8 каналов).

Приемо-передатчик

Мощность излучения приемо-передатчика непостоянна во времени и зависит от количества абонентов, обслуживаемых БС в данный момент. Максимальная, мощность

на выходе передатчика может составлять около 30 Вт при работе на частоте 1800 МГц и 300 Вт – на частоте 900 МГц, но реально на практике не превышает 5-10 Вт на несущую.

Классификация мощности GSM900 на 1998 г.

Класс мощности	Максимальный уровень мощности передатчика	Базовая станция
1	20 Вт	320W
2	8 Вт	160W
3	5 Вт	80W
4	2 Вт	40W
5	0.8 Вт	20W
6		10W
7		5W
8		2.5W

В качестве сравнения заметим, что СВЧ печь имеет частоту 2450MHz и при 500W без труда разогревает 50 граммовую сосиску. 2450MHz - это одна из резонансных частот колебаний молекул воды. Мощность 650nm ИК лазера DVD - 0.1W. Спутниковые передающие антенны, находящиеся на геостационарных орбитах в космосе на расстоянии 35 тыс. км от Земли, питаются от солнечных батарей, поэтому мощность передающего сигнала очень невелика - как правило, 150 ватт - и рассеивается она по огромной площади. Современные наземные ТВ-передатчики в городах имеют мощность от 100 ватт (в районах) до 25 кВт (в областных центрах).

Мощность излучения сотового телефона меняется от 0.5W до 2W в зависимости от расстояния до базовой станции. Согласно стандарта максимальная излучаемая мощность MS GSM900 - 2Вт., а GSM1800 - 1 Вт. Однако, далее мы увидим, что средняя мощность телефона в 8 раз меньше установленной, поскольку 7/8 передача не ведется и антена не излучает.

Кодирование речи

С микрофона речевой сигнал поступает в речевой кодек[1]. Там он на первом этапе сегментируется (разбивается на сегменты длительностью 20 мс), а затем преобразуется в цифровой поток со скоростью 13 кбит/с (один сегмент составляет кодовую последовательность из 260 бит). Поскольку частотный спектр передаваемого сигнала ограничен узкой полосой пропускания радиотракта, речь кодируют по специальному алгоритму LCP-LTP-RPE-кодирования. Следует отметить, что GSM-кодирование оптимизировано исключительно для передачи речи с максимальным качеством.

[1]Частотный диапазон человеческого голоса: Бас 75-330Hz; Тенор 120-500Hz; Меццо-сопрано 170-700Hz; Сопрано 230-1100.

Ранее мы рассматривали теорему Найквиста, согласно которой частота "оцифровки"звука должна как минимум в 2 раза превышать максимальную частоту, входящую в состав спектра сигнала.

Речевой кодек передает каждые 260 бит информационной последовательности со скоростью 13 кбит/с на схему канального кодирования. Первые 182 бита этого кадра, называемые в стандарте GSM битами 1 класса, защищаются с помощью слабого блочного кода для обнаружения ошибок в приемнике.

Кодирование осуществляется следующим образом: биты класса 1 разделяются дополнительно на проверки на четность. Блочный код представляет собой укороченный систематический 50 бит класса 1а и 132 бита класса 1б. Биты класса 1а дополняются тремя битами циклический код (53, 50).

В соответствии с принятым правилом формирования систематического кода, ключ Sw закрыт на время первых пяти-десяти тактовых импульсов, а информационные биты, поступающие на вход кодирующего устройства, одновременно поступают на блок переупорядочения и формирования бит проверки на четность. После пятидесяти тактовых импульсов переключатель Sw срабатывает и биты проверки на четность поступают из кодирующего устройства. На этой стадии проводится первый шаг перемежения. Биты с четными индексами собираются в первой части информационного слова, за которыми следуют три бита проверки на четность. Затем биты с нечетными индексами запоминаются в буферной памяти и переставляются. Далее следуют четыре нулевых бита, которые необходимы для работы кодера, формирующего код, исправляющий случайные ошибки в канале. После чего 189 бит класса 1 кодируются сверточным кодом (2,1,5) со скоростью r=1/2.

После сверточного кодирования общая длина кадра составляет 2x189+78=456 бит. После этого кадр из 456 бит делится на восемь 57 битовых подблоков, которые подвергаются диагональному и внутрикадровому перемежению. Более точно подблоки B0 и B4 формируются в пакеты по 114 бит, которые являются результатом блочно-диагонального перемежения (DI/B). Биты B0 и B4 подблоков попарно перемежаются, образуя процесс внутрикадрового битового перемежения (IBI/B). В результирующий пакет включены два опережающих флага h1, h0, которые используются для классификации различных пакетов передачи

Структура связи MS-BS

При каждом соединении сигнал преобразуется в цифровой поток информации, то есть оцифровывается, и далее 456bt. блоки разбивается на небольшие пакеты по 148bt. На передачу каждого пакета отводится интервал длительностью 0,577 мс, каждые 4,616 мс (то есть точно 8 x 0,577). Следовательно, мобильный телефон в режиме соединения выдает пачку очень коротких импульсов каждые 4,616 мс, что соответствует скорости 32.116kbs и частоте 217Hz. Именно непосредственным детектированием этих импульсных сигналов и объясняется характерное низкочастотное гудение в трубке телефона, которое слышно, когда мобильный телефон используется слишком близко от различной аудиоаппаратуры, имеющей недостаточно хорошее экранирование. Заметим, что скорость передачи данных с одного телефона в этом

случае составляет $148bt \times 217Hz = 32.116kbs$. В тоже время при полной загрузке 8 каналов скорость приема-передачи трансивера составит $32.116kbs \times 8 = 257kbs$.

Когда абонент получает канал, ему выделяется не только частотный канал, но и один из конкретных канальных интервалов, и он должен вести передачу в строго отведенном временном интервале, не выходя за его пределы - иначе будут создаваться помехи в других каналах.

Система с разделением частот (FDMA) позволяет получить 8 каналов по 25кГц ($200 = 8{\times}25$), которые, в свою очередь, разделяются по принципу системы с разделением времени (TDMA) еще на 8 каналов. В GSM используется GMSK-модуляция, а несущая частота изменяется 217 раз в секунду для того, чтобы компенсировать возможное ухудшение качества.

В каждом частотном канале данные передаются в 8 канальных интервалах (КИ), т.е. используется временное разделение каналов. Длительность КИ - 576.56 mks. В начале и в конце КИ отводится по 28 mks на затухание переходных процессов, в ходе которых мощность излучения передатчика меняется на 70dB (вверх или вниз) и 30.44mks защитного времени (Shield Time), в течение которого передатчик "молчит". Полезная продолжительность КИ - 546.12mks служит для передачи 148bt.

	Полезная длительность КИ 546.12 mks, 148bt		Защитное время 30.44mks
Переходные процессы 28mks	3bt(флаг)+57bt+1bt+ +26bt(синхронизация)+ 1bt+57bt++3bt	Переходные процессы 28mks	

Базовая станция (BS) всегда передает на три канальных интервала раньше подвижного аппарата (HS).

Передача сигнала на АТС

Транскодер обычно располагается вместе с MSC, тогда передача цифровых сообщений в направлении к контроллеру базовых станций - BSC ведется с добавлением к потоку со скоростью передачи 13 кбит/с, дополнительных битов (стафинг) до скорости передачи данных 16 кбит/с. Затем осуществляется уплотнение с кратностью 4 в стандартный канал 64 кбит/с. Так формируется определенная Рекомендациями GSM 30-канальная ИКМ линия, обеспечивающая передачу 120 речевых каналов. Шестнадцатый канал (64 кбит/с), "канальный интервал", выделяется отдельно для передачи информации сигнализации и часто содержит трафик SS N7 или LAPD. В другом канале (64 кбит/с) могут передаваться также пакеты данных, согласующиеся с протоколом X.25 МСЭ-Т.

Таким образом, результирующая скорость передачи по указанному интерфейсу составляет 30х64 кбит/с + 64 кбит/с + 64 кбит/с = 2048 кбит/с.

Сеть связывается с мобильным телефоном только в течение интервалов времени длительностью 0,577 мс. При скорости 300 000 км/с радиоволнам потребуется 0,233 мс, чтобы преодолеть путь в 70 км (туда и обратно) между базовой станцией и

мобильным телефоном. За пределами радиуса действия 35 км пакеты битов, передаваемые сотовым телефоном, достигают базовой станции в тот момент, когда она уже прекратила их ожидание и перешла на прием сигнала от другого сотового телефона.

Когда мобильный аппарат находит базовую станцию и происходит синхронизация, контроллер базовой станции формирует полнодуплексный канал на мобильный коммутирующий центр через фиксированную сеть. Центр передает информацию о мобильном терминале в четыре регистра: посетительский регистр подвижных абонентов или "гостей"(VLR - Visitor Layer Register), "домашний"регистр местных подвижных абонентов (HRL - Home Register Layer), регистр подписчика или аутентификации (AUC - AUthentiCator) и регистр идентификации оборудования (EIR - Equipment Identification Register). Эта информация уникальна и находится в пластиковой абонентской микроэлектронной телекарточке или модуле (SIM - Subscriber Identity Module), по которому производятся проверка правомочности абонента и тарификация.

2.5 Стандарты зписи CD и DVD

Audio CD (Музыкальный компакт-диск)

Формат, являющийся родоначальником всех появившихся в последующем форматов компакт-дисков. Год его рождения — 1980 год. Родителями стали компании Philips и Sony. Стандарт CD-DA описывает те диски, которые предназначены для записи цифрового звука. В стандарте были определены физические параметры и оптические характеристики дисков, системы модуляции сигнала, коррекции ошибок, а также порядок размещения на диске информации и управляющих данных. Этим стандартом был введен самый распространенный сейчас формат оцифровки звука: 16-разрядное квантование с частотой дискретизации 44.1 кГц. Очевидно,что чем больше частота дискретизации, тем точнее цифровой сигнал воспроизводит аналоговый. Откуда же взялась цифра 44.1 кГц? На самом деле тут все просто. По теореме Найквиста непрерывный сигнал можно точно восстановить по его отсчетам, если частота дискретизации вдвое больше максимальной звуковой частоты в сигнале. Так как человек может слышать звук частотой до 20 кГц, частота дискретизации должна быть как минимум в два раза больше, то есть не менее 40 кГц. На сегодня распространены частоты 44.1 кГц и 48 кГц. Оцифровка звука выполняется с помощью аналого-цифрового преобразователя (АЦП) и называется импульсно-кодовой модуляцией (ИКМ). Но этим процессом дело не заканчивается. Звук подвергается дальнейшему преобразованию. Сначала оформляются микрокадры, содержащие по шесть отсчетов с двух каналов (стерео), размером 6x2x16=192 бита или 24 байта. 98 микрокадров составляют блок (сектор) размером 2352 байта. Размер одинаков для всех стандартов, основанных на CD-DA. В формате Audio CD все байты задействованы под звук, а в некоторых других форматах (CD-ROM) часть сектора отводится под служебные данные. На следующем этапе блок кодируется для защиты от ошибок чтения (CIRC). При этом каждому микрокадру добавляется 8 контрольных байтов. В начало микрокадра вставляются 24 бита синхронизации и один символ (8 бит) субкода, а также биты слияния —

по три между байтами. Затем микрокадр подвергается канальному кодированию — модуляции 8/14 (EFM). В результате каждый байт превращается в слово из 14 бит, называемых канальными битами. В итоге микрокадр, содержащий 24 байта данных, занимает 24 (синхронизация) + 3 (биты слияния) + 14 (байт субкода) + 3 (биты слияния) + (14 + 3) x 32 (байты данных с битами слияния) = 588 битов. Это и есть физический кадр стандарта CD-DA. Скорость воспроизведения музыкального диска с 16-разрядным стереозвуком и частотой 44.1 кГц равна 2x16x44100/8=176400 байт/с. Отсюда можно получить скорость чтения 176400/2352=75 секторов в секунду. Сектора объединяются в дорожки. Регламентировано минимальное количество блоков в одной дорожке. Их не должно быть меньше 300. Есть ограничения и на количество дорожек. Их не должно быть больше 99. Хотя число созданных дорожек обычно больше чем одна, на самом деле на компакт-диске находится одна большая дорожка (примерно 5000 м) в виде спирали, начинающаяся изнури диска и заканчивающаяся на внешнем крае. Адрес сектора задается во временном формате минута:секунда:сектор (1/75 секунды), что досталось в наследство от грампластинок. Чтобы при разной скорости чтения не получилось расхождение, расчет времени производится исходя из одноразовой скорости. Каждая композиция обычно содержит собственную дорожку. При необходимости пауз между дорожками вставляются зазоры (150 блоков=2 секунды). Теперь разберемся, куда на диске записываются данные стандарта CD-DA (рис. 1.4). Эта часть диска называется информационной. Она состоит из трех зон. Подробно рассмотрим каждую из них: • Зона lead-in. Находится на внутреннем краю информационной области. Представляет собой одну дорожку, состоящую из нулей и заканчивающуюся двухсекундным интервалом пустых блоков. Эта зона отвечает за синхронизацию читающей головки перед чтением данных. В субканале Q находится таблица оглавления диска (TOC), адреса фрагментов, формат дорожек, обозначение временных меток, сведения о производителе, время выпуска альбома (данные соответствуют стандарту ISRC, международному стандартному коду записи), а также с помощью него можно разделить дорожку до 99 фрагментов. • Зона lead-out. Находится на внешнем краю диска и отделена от зоны данных двух-трехсекундным интервалом единиц. Содержит в себе нули и единицы, чередующиеся между собой с частотой 2 Гц и служит для обозначения конца записанной области. Не содержащие зоны lead-out диски могут быть не прочитаны на некоторых проигрывателях.• Зона данных (Program Area). Содержит сами данные, состоящие из одной или нескольких дорожек. Номера треков состоят из десятичных цифр и хранятся в формате XX. Поэтому максимально возможное число получается 99. Дорожка с номером AA служит в качестве выводной зоны.

Спиральный трек совершает 22188 оборотов по кругу CD, проходя примерно шестьсот оборотов на миллиметр при движении в направлении края диска

Второе – именно на поликарбонате, в прямом смысле этого слова, печатается информация с матрицы — будь то фильм, музыка или программы.

Естественно, что поликарбонат и лак прозрачны для лазерного излучения, поэтому «напечатанную» информацию для лазера необходимо сделать «видимой», для чего поверхность покрывают тонким слоем алюминия (слой B).

глубина вложенности каталогов - до 8, расширения в именах каталогов запрещены

и т.д.).

Кодиры Рида-Соломона являются ключевым компонентом компакт-диска. Это было первым использованием мложного помехоустойчивого кодирования в массовом производстве бытовой электроники. В компакт-диске двух уровневая схема кодирования дает схему, называемую кросс-чередованием Рида-Соломона кодирования (Cross-Interleaved Reed Solomon Coding-CIRC). Первый элемент декодера CIRC является RS [32,28], как сокращенный от [255,223] с 8-битными символами. Второй уровень 28-байтное блочное чередование.

Т.о. используется кодо Рида-Соломона RS(255,223) с 8-битными символами. Каждое кодовое слово содержит 255 байт, из которых 223 являются информационными и 32 байтами четности. Для этого кода:

n = 255, k = 223, s = 8 2t = 32, t = 16

Декодер может исправить любые 16 символов с ошибками в кодовом слове: то есть, ошибки могут быть исправлены, если число искаженных байт не превышает 16.

При размере символа s, максимальная длина кодового слова (n) для кода Рида-Соломона равна n = 2s – 1.

Например, максимальная длина кода с 8-битными символами (s=8) равна 255 байтам.

Коды Рида-Соломона могут быть в принципе укорочены путем обнуления некоторого числа информационных символов на входе кодировщика (передавать их в этом случае не нужно). При передаче данных декодеру эти нули снова вводятся в массив.

Например, код (255,223), описанный выше, может быть укорочен до (200,168). Кодировщик будет работать с блоком данных 168 байт, добавит 55 нулевых байт, сформирует кодовое слово (255,223) и передаст только 168 информационных байт и 32 байта четности.

Объем вычислительной мощности, необходимой для кодирования и декодирования кодов Рида-Соломона зависит от числа символов четности. Большое значение t означает, что большее число ошибок может быть исправлено, но это потребует большей вычислительной мощности по сравнению с вариантом при меньшем t.

Ошибки в символах Одна ошибка в символе происходит, когда 1 бит символа оказывается неверным или когда все биты не верны.

Пример: Код RS(255,223) может исправить до 16 ошибок в символах. В худшем случае, могут иметь место 16 битовых ошибок в разных символах (байтах). В лучшем случае, корректируются 16 полностью неверных байт, при этом исправляется 16 x 8=128 битовых ошибок.

Коды Рида-Соломона особенно хорошо подходят для корректировки кластеров ошибок (когда неверными оказываются большие группы бит кодового слова, следующие подряд).

Глава 3

Теория помехоустойчивого кодирования

При передаче сообщений по цифровым каналам она кодируется. Для простоты мы будем в дальнейшем пользоваться таблицей ASCII[1] ставящей в соответствие каждой букве алфавита определенный шестнадцатеричный номер. Мы далее будем пользоваться таблицей кодов ASCII (32-255) без управляющих символов:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	_	!	”	#	$	%	&	‘	(	)	*	+	′	−	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	∧	_
6	′	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{	|	}	∼	del
8	Ђ	Ѓ	‚	ѓ	„	…	†	‡	✠	‰	Љ	<	Њ	Ќ	Ћ	Џ
9	ђ	‘	’	“	”	•	–	—	*	™	љ	>	њ	ќ	ћ	џ
A		Ў	ў	J	¤	Ґ	|	§	Ё	©	Є	«	¬	-	®	Ї
B	°	±	І	і	ґ	µ	¶	·	ё	№	є	»	j	S	s	ї
C	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
D	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
E	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
F	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я

Из данной таблицы следует, что для передачи одной буквы ее необходимо заменить соответствующей 7-разрядной кодовой комбинацией. Любая 7-разрядная двоичная комбинация представляет собой какой-то знак алфавита и если в процессе передачи произойдет одна ошибка, то принятая комбинация будет принадлежать другому знаку. Например, если при передаче буквы **"m"** ($6D_h = 1101101_2$) произошла ошибка

[1]ASCII (англ. American Standard Code for Information Interchange) — американский стандартный код для обмена информацией. ASCII - это кодировка для представления десятичных цифр, латинского и национального алфавитов, знаков препинания и управляющих символов.

во 2-м разряде (разряды считаем справа), то мы получим букву **"o"** ($1101111_2 = 6F_h$). Если возникающая ошибка просто переводит одну букву алфавита в другую, то такую ошибку обнаружить не возможно.

Идея помехоустойчивого кодирования заключается в добавлении к сообщению лишних символов, помогающих заметить ошибку. Теперь множество кодовых комбинаций увеличивается и состоит из двух подмножеств:

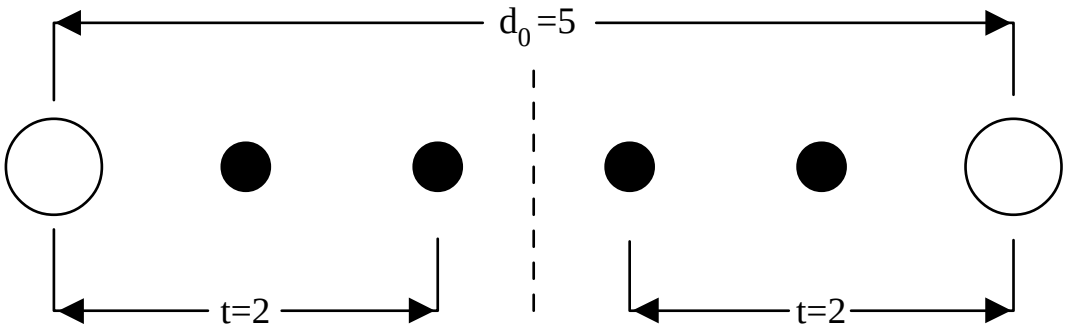
- разрешенных комбинаций и

- запрещенных комбинаций.

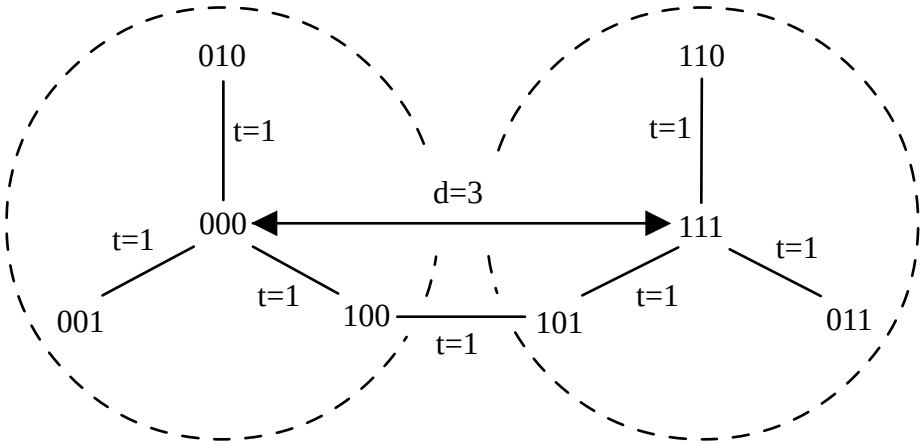
Если в результате ошибки исходная комбинация перешла в множество запрещенных, то ошибку можно обнаружить. Однако, возможно, что совокупность ошибок переведет передаваемую кодовую комбинацию в другую разрешенную. Тогда вместо одной буквы мы получим другую букву и ошибка не будет обнаружена.

Для того чтобы обнаруживать и исправлять ошибки, разрешенная комбинация должна как можно больше отличаться от запрещенной. Расстоянием между двумя комбинациями называется количество разрядов, которыми они отличаются. Например расстояние между буквами **"m"** (1101101) и **"o"** (1101111) будет 1. Расстояние между **"a"** (1100001) и **"z"** (1111010) будет 4. Весом комбинации называется количество в ней единиц. Очевидно что вес - это расстояние от нулевой комбинации (00000). Поскольку сумма комбинаций есть другая комбинация, то по аналогии с векторной алгеброй можно вычислять расстояние между комбинациями как вес их суммы (по модулю 2: $\oplus$).

$$\begin{array}{r} 0101101 \\ \oplus\ 1001010 \\ \hline 1100111 \end{array}$$ расстояние равно 5.



Здесь d_0 - расстояние между разрешенными комбинациями, t область исправляемых ошибок.



Например, если расстояние между кодовыми комбинациями (000) и (111) равно $d = 3$, то любые единичные ошибки в этих комбинациях остаются в области $t \leq 1$. Т.е. области не пересекаются и ошибки могут быть исправлены.

Обозначая число (кратность) исправляемых ошибок через t_i, а расстояние между разрешенными (передаваемыми) комбинациями через d_0, заметим, что код исправит ошибки, если

$$d_0 \geq 2t_i + 1.$$

Для построения помехоустойчивого кода требуется к k - информационным разрядам добавить r - проверочных. Количество проверочных разрядов, необходимых для построения кода, исправляющего одну ошибку вычисляется по формуле:

$$2^r \geq k + r + 1.$$

Общее количество разрядов будет $n = k+r$, поэтому построенный с такими параматрами код называют $[n, k]$ кодом. Например, для передачи 4-разрядной комбинации требуется дополнительно 3 проверочных символа и код $[7, 4]$. Для передачи 6-разрядной комбинации необходим $[10, 6]$ код с 4 проверочными разрядами.

Экономичность и эффективность кодов с обнаружением ошибок определяют коэффициент избыточности R_u и коэффициент обнаружения K_0:

$$R_u = 1 - \frac{\mathrm{lb}M_1}{\mathrm{lb}M}, \qquad K_0 = \frac{Q}{Q + Q_1},$$

где $M = 2^n$ – общее число кодовых слов, которое можно получить в n-элементном коде; M_1– количество используемых комбинаций; Q – общее количество искаженных комбинаций, ошибка в которых может быть обнаружена; Q_1 – общее число искаженных комбинаций, ошибка в которых не поддается обнаружению.

3.1 Коды Хэмминга

Рассмотрим правила построения $[7,4]$ кода Хэмминга, исправляющего одну ошибку в передаваемой информационной комбинации (a_1, a_2, a_3, a_4). Выпишем таблицу истинности для трех проверочных разрядов. Обозначим информационные разряды символом a_i, а проверочные символом b_i. Тогда, проверочные разряды восстанавливаются по информационным по следующим правилам:

x_2	x_1	x_0		
0	0	0		
0	0	①	b_0	$b_0 = a_1 \oplus a_2 \oplus a_4$
0	①	0	b_1	$b_1 = a_1 \oplus a_3 \oplus a_4$
0	1	1	a_1	
①	0	0	b_2	$b_2 = a_2 \oplus a_3 \oplus a_4$
1	0	1	a_2	
1	1	0	a_3	
1	1	1	a_4	

Т.е. значение b_0 формируется из всех a_k для которых $x_0 = 1$. Значение b_1 формируется из всех a_k для которых $x_1 = 1$, и т.д. На передатчик канала связи подается самокорректирующийся код Хэмминга $[7,4]$, который имеет вид

$$(b_0, b_1, a_1, b_2, a_2, a_3, a_4).$$

На приемном конце канала связи для проверочных символов строится аналогичная комбинация:

$$\begin{aligned} B_0 &= a_1 \oplus a_2 \oplus a_4 \\ B_1 &= a_1 \oplus a_3 \oplus a_4 \\ B_2 &= a_2 \oplus a_3 \oplus a_4 \end{aligned}$$

Разница между передаваемыми b_i и принимаемыми B_i проверочными разрядами позволяет обнаружить и локализовать ошибку. Место ошибки определяется формулой

$$M = 2^0 \cdot (b_0 \oplus B_0) + 2^1 \cdot (b_1 \oplus B_1) + 2^2 \cdot (b_2 \oplus B_2).$$

Пример 3.1. Построить по методу Хэмминга кодовое слово для сообщения (1010).

Решение. Зная количество информационных символов $k = 4$ сообщения, найдем количество проверочных символов из формулы

$$2^r \geq k + r + 1, \quad \text{или} \quad 2^3 = 8 \geq 4 + 3 + 1 = 8,$$

т.е. $n = k + r = 4 + 3 = 7$. Поскольку $r = 3$, то для передаваемой последовательности кода $[n, k] = [7, 4]$ будем иметь $(b_0, b_1, a_1, b_2, a_2, a_3, a_4)$. Учитывая, что

$$(a_1, a_2, a_3, a_4) = (1010),$$

для проверочных символов получим

$$\begin{aligned} b_0 &= a_1 \oplus a_2 \oplus a_4 = 1 \oplus 0 \oplus 0 = 1 \\ b_1 &= a_1 \oplus a_3 \oplus a_4 = 1 \oplus 1 \oplus 0 = 0 \\ b_2 &= a_2 \oplus a_3 \oplus a_4 = 0 \oplus 1 \oplus 0 = 1 \end{aligned}$$

Передаваемое кодовое слово имеет вид

$$(b_0, b_1, a_1, b_2, a_2, a_3, a_4) = (1011010). \qquad \blacktriangle$$

Пример 3.2. На приемнике было получено кодовое слово (1101101) построенное по методу Хэмминга. Восстановить исходное сообщение.

Решение. Полученное кодовое слово имеет вид

$$(b_0, b_1, a_1, b_2, a_2, a_3, a_4) = (1101101).$$

Учитывая, что здесь $a_1 = 0, \quad a_2 = 1, \quad a_3 = 0, \quad a_4 = 1$, для проверочных символов получим

$$\begin{aligned} B_0 &= a_1 \oplus a_2 \oplus a_4 = 0 \oplus 1 \oplus 1 = 0 \\ B_1 &= a_1 \oplus a_3 \oplus a_4 = 0 \oplus 0 \oplus 1 = 1 \\ B_2 &= a_2 \oplus a_3 \oplus a_4 = 1 \oplus 0 \oplus 1 = 0 \end{aligned}$$

Разница между передаваемыми b_i и принимаемыми B_i проверочными разрядами дает место ошибки определяемой формулой

$$\begin{aligned} M &= 2^0 \cdot (b_0 \oplus B_0) + 2^1 \cdot (b_1 \oplus B_1) + 2^2 \cdot (b_2 \oplus B_2) \\ &= 2^0 \cdot (1 \oplus 0) + 2^1 \cdot (1 \oplus 1) + 2^2 \cdot (1 \oplus 0) \\ &= 2^0 \cdot 1 + 2^1 \cdot 0 + 2^2 \cdot 1 = 5. \end{aligned}$$

Отсчитывая слева направо 5-й разряд в комбинации (1101101) и меняя его на противоположный, получим

$$(1101\underline{\mathbf{1}}01) \to (1101\underline{\mathbf{0}}01).$$

Теперь выделяя информационные символы, восстановим сообщение

$$a_1 = 0, \quad a_2 = 0, \quad a_3 = 0, \quad a_4 = 1, \quad \text{или } (0001). \qquad \blacktriangle$$

Пример 3.3. Построить по методу Хэмминга кодовое слово для сообщения (111001111).

Решение. Для кодирования $k = 9$ информационных разрядов методом Хэмминга требуется из неравенства

$$2^r \geq k + r + 1.$$

определить количество проверочных символов r. Простым подбором находим $r = 4$:

$$2^4 \geq 9 + 4 + 1.$$

Т.е. нам необходим код $[13, 9]$. Рассмотрим правила построения $[13, 9]$ кода Хэмминга, исправляющего одну ошибку в передаваемой информационной комбинации

$$(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9).$$

Выпишем таблицу истинности для четырех проверочных разрядов. Обозначим информационные разряды символом a_i, а проверочные символом b_i. Тогда, проверочные разряды восстанавливаются по информационным по следующим правилам:

x_3	x_2	x_1	x_0		
0	0	0	0		
0	0	0	①	b_0	$b_0 = a_1 \oplus a_2 \oplus a_4 \oplus a_5 \oplus a_7 \oplus a_9$
0	0	①	0	b_1	$b_1 = a_1 \oplus a_3 \oplus a_4 \oplus a_6 \oplus a_7$
0	0	1	1	a_1	
0	①	0	0	b_2	$b_2 = a_2 \oplus a_3 \oplus a_4 \oplus a_8 \oplus a_9$
0	1	0	1	a_2	
0	1	1	0	a_3	
0	1	1	1	a_4	
①	0	0	0	b_3	$b_3 = a_5 \oplus a_6 \oplus a_7 \oplus a_8 \oplus a_9$
1	0	0	1	a_5	
1	0	1	0	a_6	
1	0	1	1	a_7	
1	1	0	0	a_8	
1	1	0	1	a_9	

Т.е. значение b_0 формируется из всех a_k для которых $x_0 = 1$. Значение b_1 формируется из всех a_k для которых $x_1 = 1$, и т.д. Учитывая, что для комбинации

$$(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9) = (111001111),$$

для проверочных символов получим

$$\begin{aligned}
b_0 &= a_1 \oplus a_2 \oplus a_4 \oplus a_5 \oplus a_7 \oplus a_9 = 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 1 = 0 \\
b_1 &= a_1 \oplus a_3 \oplus a_4 \oplus a_6 \oplus a_7 = 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 = 0 \\
b_2 &= a_2 \oplus a_3 \oplus a_4 \oplus a_8 \oplus a_9 = 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 = 0 \\
b_3 &= a_5 \oplus a_6 \oplus a_7 \oplus a_8 \oplus a_9 = 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 = 0
\end{aligned}$$

Кодовое слово имеет вид

$$(b_0, b_1, a_1, b_2, a_2, a_3, a_4, b_3, a_5, a_6, a_7, a_8, a_9) = (0010110001111). \qquad \blacktriangle$$

Пример 3.4. На приемнике было получено кодовое слово

$$(11011100101)$$

построенное по методу Хэмминга. Восстановить исходное сообщение.

Решение. Учитывая, что длина последовательности $n = k+r = 11$, иИз выражения

$$2^r \geq k + r + 1 = n + 1 = 11 + 1 = 12$$

найдем количество проверочных символов $r = 4$. Тогда полученное кодовое слово имеет вид

$$(b_0, b_1, a_1, b_2, a_2, a_3, a_4, b_3, a_5, a_6, a_7) = (11011100101).$$

Выпишем таблицу истинности для четырех проверочных разрядов. Обозначим информационные разряды символом a_i, а проверочные символом b_i. Тогда, проверочные разряды восстанавливаются по информационным по следующим правилам:

x_3	x_2	x_1	x_0		
0	0	0	0		
0	0	0	①	b_0	$b_0 = a_1 \oplus a_2 \oplus a_4 \oplus a_5 \oplus a_7$
0	0	①	0	b_1	$b_1 = a_1 \oplus a_3 \oplus a_4 \oplus a_6 \oplus a_7$
0	0	1	1	a_1	
0	①	0	0	b_2	$b_2 = a_2 \oplus a_3 \oplus a_4$
0	1	0	1	a_2	
0	1	1	0	a_3	
0	1	1	1	a_4	
①	0	0	0	b_3	$b_3 = a_5 \oplus a_6 \oplus a_7$
1	0	0	1	a_5	
1	0	1	0	a_6	
1	0	1	1	a_7	

Как и ранее значение b_0 формируется из всех a_k для которых $x_0 = 1$. Значение b_1 формируется из всех a_k для которых $x_1 = 1$, и т.д. Учитывая, что здесь

$$(b_0, b_1, b_2, b_3) = (1110), \quad (a_1, a_2, a_3, a_4, a_5, a_6, a_7) = (0110101),$$

для проверочных символов получим

$$\begin{aligned}
B_0 &= a_1 \oplus a_2 \oplus a_4 \oplus a_5 \oplus a_7 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 = 1 \\
B_1 &= a_1 \oplus a_3 \oplus a_4 \oplus a_6 \oplus a_7 = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 = 0 \\
B_2 &= a_2 \oplus a_3 \oplus a_4 = 1 \oplus 1 \oplus 0 = 0 \\
B_3 &= a_5 \oplus a_6 \oplus a_7 = 1 \oplus 0 \oplus 1 = 0
\end{aligned}$$

Разница между передаваемыми $b_i = (1110)$ и принимаемыми $B_i = (1000)$ проверочными разрядами дает место ошибки определяемой формулой

$$\begin{aligned} M &= 2^0 \cdot (b_0 \oplus B_0) + 2^1 \cdot (b_1 \oplus B_1) + 2^2 \cdot (b_2 \oplus B_2) + 2^3 \cdot (b_3 \oplus B_3) \\ &= 2^0 \cdot (1 \oplus 1) + 2^1 \cdot (1 \oplus 0) + 2^2 \cdot (1 \oplus 0) + 2^3 \cdot (0 \oplus 0) \\ &= 2^0 \cdot 0 + 2^1 \cdot 1 + 2^2 \cdot 1 + 2^3 \cdot 0 = 6. \end{aligned}$$

Отсчитывая слева направо 6-й разряд в комбинации (11011100101) и меняя его на противоположный, получим

$$(11011\underline{1}00101) \to (11011\underline{0}00101).$$

Теперь выделяя информационные символы, восстановим сообщение

$$(a_1, a_2, a_3, a_4, a_5, a_6, a_7) = (0101110). \quad \blacktriangle$$

Пример 3.5. На приемнике было получено кодовое слово

$$(001011110111111)$$

построенное по методу Хэмминга. Восстановить исходное сообщение.

Решение. Полученное кодовое слово $[15, 11]$ имеет вид

$$(b_0, b_1, a_1, b_2, a_2, a_3, a_4, b_3, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}) = (001011110111111).$$

Учитывая, что здесь

$$(b_0, b_1, b_2, b_3) = (0001), \quad (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}) = (11110111111),$$

для проверочных символов получим

$$\begin{aligned} B_0 &= a_1 \oplus a_2 \oplus a_4 \oplus a_5 \oplus a_7 \oplus a_9 \oplus a_{11} = 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 = 0 \\ B_1 &= a_1 \oplus a_3 \oplus a_4 \oplus a_6 \oplus a_7 \oplus a_{10} \oplus a_{11} = 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 = 1 \\ B_2 &= a_2 \oplus a_3 \oplus a_4 \oplus a_8 \oplus a_9 \oplus a_{10} \oplus a_{11} = 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 = 1 \\ B_3 &= a_5 \oplus a_6 \oplus a_7 \oplus a_8 \oplus a_9 \oplus a_{10} \oplus a_{11} = 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 = 0 \end{aligned}$$

Разница между передаваемыми $b_i = (0001)$ и принимаемыми $B_i = (0110)$ проверочными разрядами дает место ошибки определяемой формулой

$$\begin{aligned} M &= 2^0 \cdot (b_0 \oplus B_0) + 2^1 \cdot (b_1 \oplus B_1) + 2^2 \cdot (b_2 \oplus B_2) + 2^3 \cdot (b_3 \oplus B_3) \\ &= 2^0 \cdot (0 \oplus 0) + 2^1 \cdot (0 \oplus 1) + 2^2 \cdot (0 \oplus 1) + 2^3 \cdot (1 \oplus 0) \\ &= 2^0 \cdot 0 + 2^1 \cdot 1 + 2^2 \cdot 1 + 2^3 \cdot 1 = 14. \end{aligned}$$

Отсчитывая слева направо 14-й разряд в комбинации (001011110111111) и меняя его на противоположный, получим

$$((001011110111\underline{1}1) \to (001011110111\underline{0}1).$$

Теперь выделяя информационные символы, восстановим сообщение

$$(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}) = (11110111101). \quad \blacktriangle$$

Задача 3.1.
Методом Хемминга закодировать информационную последовательность.

N	x	N	x	N	x
1	111001	11	11111101	21	1011010011
2	101101	12	11111011	22	1101001111
3	101111	13	11110111	23	1000111111
4	110111	14	11101111	24	1111011001
5	111011	15	11011111	25	1111101101
6	111101	16	10111111	26	1110010111
7	111110	17	10011111	27	1001111011
8	100111	18	11001111	28	1111100101
9	110011	19	11100111	29	1110011110
10	111001	20	11110011	30	1001111111

Задача 3.2.
На приемнике было получено кодовое слово $\mathbf{x}$ сформированное кодом Хемминга. Восстановить исходное сообщение.

N	x	N	x	N	x
1	1110001	11	0101001	21	1001001
2	0111010	12	1101010	22	0001010
3	1010011	13	0100011	23	1100011
4	1011100	14	0001100	24	1101100
5	0100001	15	1101110	25	0011111
6	0100111	16	1110110	26	0100111
7	0100100	17	1000110	27	0001011
8	1100111	18	0100110	28	0001101
9	1100100	19	1001111	29	0001110
10	1100010	20	0101111	30	1110010

Задача 3.3. На приемнике было получено кодовое слово **x** сформированное кодом Хемминга. Восстановить исходное сообщение.

N	x	N	x	N	x
1	1110011100	11	001001001111	21	00100101101001
2	1011010100	12	111001001111	22	11100101101001
3	1011111010	13	100001001111	23	10000101101001
4	1101110101	14	101101001111	24	10110101101001
5	1110010011	15	101011001111	25	10101101101001
6	1110100011	16	111000011011	26	10000001011001
7	1110111011	17	111001111011	27	10000111011001
8	1110110111	18	111001001011	28	10000100011001
9	1110110001	19	111001010011	29	10000101111001
10	1110110010	20	111001011111	30	10000101001001

Задача 3.4. На приемнике было получено кодовое слово **x** сформированное кодом Хемминга. Восстановить исходное сообщение.

N	x	N	x
1	00101010111110111011	16	10001000111110101111011
2	11101010111110111011	17	10001000111110110111011
3	10001010111110111011	18	10001000111110111011011
4	10111010111110111011	19	10001000111110111111111
5	10100010111110111011	20	10001000111110110111011
6	10101100111110111111	21	00001111111110101111101101
7	10101010111110111111	22	11001111111110101111101101
8	10101001111110111111	23	10101111111110101111101101
9	10101000011101111111	24	10011111111110101111101101
10	10101000101110111111	25	10000111111110101111101101
11	10001000110110111111101	26	10001011111110101111101101
12	10001000111010111111101	27	10001101111110101111101101
13	10001000111100111111101	28	10001110111110101111101101
14	10001000111111111111101	29	10001111011110101111101101
15	10001000111110011111101	30	10001111101110101111101101

3.2 Циклические коды

Одним из обобщений кода Хэмминга являются циклические коды (CRC - cyclic redundancy check)[2]. В даном коде произвольная кодовая последовательность $a = (a_1, a_2, a_3, ..., a_n)$ записывается в виде полинома

$$u(x) = a_1 x^{n-1} + a_2 x^{n-2} + ... + a_{n-2} x^2 + a_{n-1} x + a_n = \sum_{i=1}^{k} a_i x^{k-1}.$$

Например кодовой последовательности

$$\begin{aligned} (10101) \quad \text{соответствует} \quad u(x) &= 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 1 \cdot x^0 \\ &= x^4 + x^2 + 1, \\ (1011) \quad \text{соответствует} \quad u(x) &= 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1 \cdot x^0 \\ &= x^3 + x^1 + 1. \end{aligned}$$

В поле Галуа $GF(2)$ (Galous Field) коэффициенты при степенях $\mathbf{x}$ могут принимать значения только $\mathbf{0}$ или $\mathbf{1}$, тогда

$$\begin{aligned} 1 - x - x^2 &= 1 + x + x^2, \\ 5 + 2x + 3x^2 &= 1 + 0x + x^2 = 1 + x^2. \end{aligned}$$

Неприводимым называется многочлен, который не может быть представлен как произведение многочленов меньшей степени.

Приводимым называется многочлен, который может быть факторизован, т.е. представлен как произведение многочленов меньшей степени.

Например

$$\begin{aligned} x^3 + x &= x(1 + x)(1 + x), \\ x^4 + x &= x(1 + x)(1 + x + x^2). \end{aligned}$$

Произвольный двучлен $x^n + 1$ делится без остатка на неприводимый многочлен:

$$\begin{aligned} x^2 + 1 &= (1 + x)^2, \\ x^3 + 1 &= (1 + x)(1 + x + x^2), \\ x^4 + 1 &= (1 + x)^4, \\ x^5 + 1 &= (1 + x)(1 + x + x^2 + x^3 + x^4), \\ x^6 + 1 &= (1 + x)^2(1 + x + x^2)^2. \end{aligned}$$

[2]БЧХ (Bose-Chadhuri-Hocquenghem) коды являются классом циклических кодов

Обозначим остаток $R(x)$ от деления полинома $P(x)$ на полином $Q(x)$ через $\left[\frac{P(x)}{Q(x)}\right]$, тогда

$$\frac{P(x)}{Q(x)} = C(x) + \frac{R(x)}{Q(x)} \quad \text{т.е.} \quad \left[\frac{P(x)}{Q(x)}\right] = R(x).$$

Двоичную последовательность, соответствующую полиному остатков запишем в десятичном виде. Например

$$\left[\frac{x^2}{x^3+x^2+1}\right] = x^2 = 100 = 4, \quad \left[\frac{x^3}{x^3+x+1}\right] = x+1 = 011 = 3.$$

Рассмотрим остатки от деления степени x^n на неприводимый полином $p(x) = x^4 + x^3 + x^2 + x + 1$:

x^n	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7
$\left[\frac{x^n}{p(x)}\right]$	1	2	4	8	15	1	2	4

Видно, что период последовательности составленной из остатков равен 5. Теперь рассмотрим остатки от деления степени x^n на неприводимый полином $p(x) = x^4 + x + 1$:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\left[\frac{x^n}{p(x)}\right]$	1	2	4	8	3	6	12	11	5	10	7	14	15	13	9	1	2

Период последовательности составленной из остатков равен 15.

Неприводимый полином $p(x)$ степени n, генерирующий последовательность остатков максимального периода $T = 2^n - 1$ называется **примитивным** или образующим. Полученный период будем называть порядком полинома

$$\operatorname{ord} p(x) = T.$$

Как видно из примеров не все неприводимые полиномы могут быть примитивными. Например, для неприводимых полиномов небольших степеней n можно получить:

$n = 1.$	x	$\operatorname{ord} = 1$
	$x + 1$ — не примитивный	$\operatorname{ord} = 0$
$n = 2.$	$x^2 + x + 1$	$\operatorname{ord} = 3$
$n = 3.$	$x^3 + x + 1$	$\operatorname{ord} = 7$
	$x^3 + x^2 + 1$	$\operatorname{ord} = 7$
$n = 4.$	$x^4 + x + 1$	$\operatorname{ord} = 15$
	$x^4 + x^3 + 1$	$\operatorname{ord} = 15$
	$x^4 + x^3 + x^2 + x + 1$ — не примитивный	$\operatorname{ord} = 5$

В общем случае задача о нахождении всех неприводимых полиномов степени n решается с помощью формулы Мебиуса.

Функция Мебиуса	Функция Мебиуса μ_k определяется следующим образом: $\mu_k = \begin{cases} 1, & \text{если k=1} \\ (-)^s, & \text{если k - произведение s различных простых чисел} \\ 0 & \text{если k делится на квадрат} \end{cases}$

★ $\mu_1 = 1$
★ $\mu_2 = (-)^1 = -1$
★ $\mu_3 = (-)^1 = -1$
★ $\mu_4 = \mu_{2^2} = 0$
★ $\mu_5 = (-)^1 = -1$
★ $\mu_6 = \mu_{2\cdot 3} = (-)^2 = 1$
★ $\mu_7 = (-)^1 = -1$
★ $\mu_8 = \mu_{2^2\cdot 2} = 0$

Формула Мебиуса	**Количество неприводимых полиномов** степени n определяется с помощью выражения $$I_n = \frac{1}{n} \sum_{k=1,(k\mid n)}^{n} \mu_k 2^{n/k}$$

Здесь $k|n$ означает что k должно делиться на n.

★ $n = 1:\ I_1 = \frac{1}{1} \sum_{k=1,(k\mid 1)}^{1} \mu_k 2^{1/k} = \mu_1 2^1 = 2$

★ $n = 2:\ I_2 = \frac{1}{2} \sum_{k=1,(k\mid 2)}^{2} \mu_k 2^{2/k} = \frac{1}{2}(\mu_1 2^2 + \mu_2 2^1) = \frac{1}{2}(4-2) = 2$

★ $n = 3:\ I_3 = \frac{1}{3} \sum_{k=1,(k\mid 3)}^{3} \mu_k 2^{3/k} = \frac{1}{3}(\mu_1 2^{3/1} + \mu_3 2^{3/3}) = \frac{1}{3}(8-2) = 2$

★ $n = 4:\ I_4 = \frac{1}{4} \sum_{k=1,(k\mid 4)}^{4} \mu_k 2^{4/k} = \frac{1}{4}(\mu_1 2^{4/1} + \mu_2 2^{4/2}) = \frac{1}{4}(16-4) = 3$

★ $n = 5:\ I_5 = \frac{1}{5} \sum_{k=1,(k\mid 5)}^{5} \mu_k 2^{5/k} = \frac{1}{5}(\mu_1 2^{5/1} + \mu_5 2^{5/5}) = \frac{1}{5}(32-2) = 6$

★ $n = 6:\ I_6 = \frac{1}{6} \sum_{k=1,(k\mid 6)}^{6} \mu_k 2^{6/k} = \frac{1}{6}(\mu_1 2^{6/1} + \mu_2 2^{6/2} + \mu_3 2^{6/3} + \mu_6 2^{6/6})$

$= \frac{1}{6}(64 - 8 - 4 + 2) = 9$

3.2.1 Исправление 1 ошибки

Для того чтобы код смог исправить одну ошибку расстояние между словами должно быть не менее 3. (т.е. $d = 3$). Тогда количество проверочных символов r вычисляется по формуле

$$2^r \geq k + r + 1 = 4 + r + 1 = 5 + r \Rightarrow r = 3$$

Для поля Галуа GF_2 таблица образующих полиномов имеет вид

r	$P(x)$	
2	$x^2 + x + 1$	111
3	$x^3 + x + 1$	1011
	$x^3 + x^2 + 1$	1101
4	$x^4 + x + 1$	10011
	$x^4 + x^3 + 1$	11001
5	$x^5 + x^2 + 1$	100101
	$x^5 + x^4 + x^3 + x^2 + 1$	111101
	$x^5 + x^4 + x^2 + x + 1$	110111
6	$x^6 + x + 1$	1000011
	$x^6 + x^5 + x^2 + x + 1$	1100111
7	$x^7 + x^3 + 1$	10001001
	$x^7 + x^3 + x^2 + x + 1$	10001111
	$x^7 + x^4 + x^3 + x + 1$	10011101
8	$x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$	111100111
	$x^8 + x^4 + x^3 + x^2 + 1$	100011101
	$x^8 + x^6 + x^5 + x + 1$	101100011
9	$x^9 + x^5 + x^3 + x^2 + 1$	1000101101
	$x^9 + x^8 + x^7 + x^6 + x^5 + x^3 + 1$	1111101001
10	$x^{10} + x^4 + x^3 + x + 1$	10000011011
	$x^{10} + x^9 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	11001111111
11	$x^{11} + x^{10} + x^9 + x^8 + x^3 + x + 1$	111100001011
	$x^{11} + x^8 + x^6 + x^2 + 1$	100101000101
12	$x^{12} + x^{11} + x^9 + x^8 + x^7 + x^5 + x^2 + x + 1$	1101110100111
	$x^{12} + x^9 + x^3 + x^2 + 1$	1001000001101

Если информационную последовательность представить в виде полинома $m(x)$, то передаваемая комбинация F имеет вид

$$F = PC,$$

где полином C необходимо найти из выражения

$$\frac{x^r m}{P} = C + \frac{R}{P}.$$

Если в передаваемой комбинации возникает ошибка, то ее обнаруживают сравнением остатков от деления $\frac{F}{P}$ и $\frac{x^k}{P}$.

Пример 3.6. Рассмотрим построение повторного кода $[n,k]=[3,1]$. Представим информационную последовательность в виде $m(x)=e$, где $e\in GF_2; (e=0,1)$. Образующий полином имеет вид

$$P(x)=x^2+x+1.$$

Поскольку $r=2$, то умножим

$$x^2m(x)=ex^2$$

и найдем

$$x^2Q(x)=C(x)\cdot P(x)+R(x)=e\cdot(x^2+x+1)+ex+e.$$

Передаваемая последовательность имеет вид

$$F=C(x)\cdot P(x)=ex^2+ex+e=(eee).$$

Для кода малой размерности определение места ошибки проводится с помощью таблицы синдромов[3]. Обозначая через $\left[\frac{A(x)}{B(x)}\right]$ остаток от деления полиномов, получим

$$\left[\frac{1}{P(x)}\right]=1=(01);\quad \left[\frac{x}{P(x)}\right]=x=(10);\quad \left[\frac{x^2}{P(x)}\right]=x+1=(11).$$

Допустим мы приняли сообщение с ошибкой: $I(x)=ex^2+\overline{e}x+e=(e\overline{e}e)$, тогда

$$\left[\frac{I(x)}{P(x)}\right]=x=(10)$$

и по таблице синдромов мы определяем, что ошибка произошла во втором символе.

Пример 3.7. Построить полиномиальный код $[n,k]=[7,4]$ для передачи информационной последовательности 0111

Решение. Для построения полиномиального кода $[n,k]=[7,4]$ нам необходимо иметь дополнительно $r=3$ проверочных символа. Информационная последовательность

$$a=(0111)$$

представляется в виде

$$m(x)=x^3\cdot 0+x^2\cdot 1+x\cdot 1+1\cdot 1=x^2+x+1.$$

Поскольку $r=3$, то умножаем

$$Q(x)=x^rm=x^3Q=x^3(x^2+x+1)=x^5+x^4+x^3=0111000.$$

[3]**Синдром** - совокупность признаков характеризующих заболевание. Медицинский термин используемый в теории информации при построении корректирующих кодов. В данном случае **синдром** - это совокупность признаков характеризующих ошибку в передаваемой кодовой комбинации.

По таблице образующих полиномов для $r = 3$ находим

$$P(x) = x^3 + x + 1$$

Делим $m = x^r Q$ на образующий полином P

$$\frac{x^3 m}{P} = C + \frac{R}{P}$$

или

$$\frac{x^5 + x^4 + x^3}{x^3 + x + 1} = (x^2 + x) - \frac{2x^2 + x}{x^3 + x + 1}$$

окуда получим $R = 2x^2 + x$. Аналогичный результат можно получить в Mathcad: остаток от деления полиномов определяется оператором **parfrac** в панели **Symbolic**:

$$\frac{x^5 + x^4 + x^3}{x^3 + x + 1} \text{ convert, parfrac, x} \rightarrow x + x^2 - x \cdot \frac{2x + 1}{x^3 + x + 1}.$$

В любом случае остаток

$$R(x) = -(2x^2 + x)$$

необходимо привести по модулю 2. Поскольку в этом случае $2 = 1 \oplus 1 = 0$ и $-1 = +1$, получим

$$R(x) = -(2x^2 + x) = (2x^2 + x) = 0 \cdot x^2 + x = x = 010.$$

Поскольку

$$Q(x) = x^5 + x^4 + x^3 = 0111000$$

то передаваемая комбинация F есть прямая конкатенация $m \oplus R$, или:

$$\begin{array}{r} Q = 0111000 \\ R = \quad\quad 010 \\ \hline F = 0111010 \end{array}$$

Таким образом, передаваемая кодовая комбинация имеет вид $F = (0111010)$. ▲

Допустим во время передачи по каналу информации в F возникла ошибка (3 символ слева или 4 степень)

$$F = (01\underline{\mathbf{1}}1010) \quad \rightarrow \quad \overline{F} = (01\underline{\mathbf{0}}1010)$$

Опишем алгоритм определения и исправления ошибки полиномиальным кодом.

Пример 3.8. Обнаружить и исправить ошибку в последовательности

$$\overline{F} = (0101010),$$

сформированной полиномиальным кодом.

Решение. Поскольку $n = 7$, то по формуле

$$2^r \geq n + 1$$

получим $r = 3$. Т.е. мы должны пользоваться полиномом 3 степени из таблицы полиномов. Заметим, что полином для **раскодирования** однозначно определяется полиномом **кодирования**. В кодах CRC эти полиномы совпадают. Если мы попутаем полиномы - то получим неправильный ответ. Если для данной степени неприводимых полиномов несколько, то мы будем брать первый по списку. В нашем случае для $r = 3$ имеем $P = x^3 + x + 1$.

Найдем остаток от деления $\frac{\overline{F}}{P}$

$$R(x) = \left[\frac{\overline{F}}{P}\right] = x - x^2 = x + x^2 = 0110$$

Составим таблицу синдромов, определяющих место ошибки в передаваемом сообщении. Найдем остаток от деления $\frac{x^k}{P}$:

$$\left[\frac{1}{P}\right] = 1 = 0001; \qquad \left[\frac{x}{P}\right] = x = 0010$$

$$\left[\frac{x^2}{P}\right] = x^2 = 0100; \qquad \left[\frac{x^3}{P}\right] = x + 1 = 0011$$

$$\left[\frac{x^4}{P}\right] = x^2 + x = 0110; \qquad \left[\frac{x^5}{P}\right] = x^2 + x + 1 = 0111$$

$$\left[\frac{x^6}{P}\right] = x^2 + 1 = 0101; \qquad \left[\frac{x^7}{P}\right] = 1 = 0001$$

Заметим, что далее остатки повторяются. Место ошибки определяется степенью знаменателя синдрома, совпадающего с остатком $[\frac{F}{P}]$. В данном случае остаток 0110 соответствует синдрому с x^4, поэтому необходимо исправить ошибку в 4 степени передаваемой последовательности

$$01\underline{0}1010 \Rightarrow 01\underline{1}1010.$$

Убирая последние три проверочных символа, получаем исходную информационную последовательность $a = 0111$. Заметим, что на практике удобнее не строить всю таблицу синдромов, а увеличивать степень числителя x^k до тех пор, пока остаток $\left[\frac{x^k}{P}\right]$ не сравняется с $R(x)$. ▲

В следующих задачах образующие полиномы брались первыми в списке.

Задача 3.5.
Построить полиномиальный код для следующей информационной последовательности.

N	x	N	x	N	x
1	110010011	11	10011010111	21	00110001110
2	111001	12	010100111111	22	11111001001
3	1011101	13	1101111010	23	0001011110
4	1100001011	14	01011010111	24	1110110100010
5	10100111	15	11000011	25	110001101011
6	10111010	16	100011	26	11011001010101
7	10001101	17	11010	27	11111010101011
8	100111111	18	111011010	28	1110101010111
9	1001000101	19	100011110	29	101010101011
10	1100100111	20	01000110	30	00011010110101001

Задача 3.6. На приемнике было получено кодовое слово **x** сформированное полиномиальным кодом. Восстановить исходное сообщение.

N	x	N	x	N	x	N	x	N	x
1	1100110	7	0011111	13	1010011	19	0110011	25	1101011
2	1101000	8	0110001	14	1111111	20	1001010	26	0011011
3	1000100	9	0000110	15	0111101	21	1111010	27	1001111
4	0110011	10	1001110	16	0110110	22	0100101	28	1010011
5	0010101	11	1101110	17	1011100	23	0100010	29	0110110
6	0100100	12	1110101	18	1011110	24	1001000	30	0110011

Задача 3.7. На приемнике было получено кодовое слово **x** сформированное полиномиальным кодом. Восстановить исходное сообщение.

N	x	N	x	N	x	N	x	N	x
1	001001001	7	001101111	13	101110111	19	101011111	25	001011011
2	011011111	8	111001001	14	111101111	20	101011111	26	011110111
3	110110111	9	001111111	15	100001001	21	100101111	27	001001111
4	101001111	10	111010111	16	001011101	22	101011001	28	001011110
5	111111100	11	101111111	17	111111111	23	000011111	29	101000001
6	101011111	12	101001011	18	101100111	24	111110011	30	001011101

Задача 3.8. На приемнике было получено кодовое слово **x** сформированное полиномиальным кодом. Восстановить исходное сообщение.

N	x	N	x
1	10111111111111100111	16	11001111111111101001
2	11111111111111100001	17	11000011111111101011
3	11011111111111100111	18	11111101111111100111
4	00111111111111100001	19	00000011111111101011
5	00001111111111101001	20	11101111111111100111
6	01100011111111101011	21	01011111111111100001
7	11110111111111100111	22	01101111111111101001
8	01101111111111100001	23	01010011111111101011
9	01000111111111101001	24	11111011111111100111
10	01001011111111101011	25	01110111111111100001
11	11111101111111100111	26	01001011111111101001
12	01111110111111100001	27	01000111111111101011
13	01001101111111101001	28	11111110111111100111
14	01000001111111101011	29	01111111111110100001
15	11111111101111100111	30	01001110111111101001

3.2.2 Исправление 2 ошибок

Алгоритм исправления 2 ошибок ничем не отличается от предыдущего. Единственная особенность заключается в выборе неприводимых полиномов и количестве проверочных символов. Нам необходимо выбрать 2 полинома: один для исправления одиночных ошибок $p_1(x)$, а другой для исправления двойных ошибок $p_2(x)$. Данные полиномы имеют степени r_1 и r_2 соответственно, и длина кода будет

$$n = k + r_1 + r_2$$

символа. Тогда, согласно формуле Хэмминга $r_1 + r_2$ проверочных символа должны обнаружить и исправить

$$2^{r_1+r_2} \geq C_n^0 + C_n^1 + C_n^2 = 1 + \frac{n(n+1)}{2}$$

ошибок. Однако, порядок произведения полиномов $p_r(x)$ степени r, вычисляется по формуле

$$\operatorname{ord}(p_r \cdot p_m) = \text{НОК}(\operatorname{ord} p_r, \operatorname{ord} p_m)$$

если полиномы разного порядка (степени), и

$$\operatorname{ord}(p_r \cdot p_r) = 2\operatorname{ord}(p_r)$$

если порядок (степень) полиномов одинаковый. В таком случае формулу Хэмминга необходимо переписать в виде

$$\operatorname{ord}(p_{r_1} \cdot p_{r_2}) \geq \frac{n(n+1)}{2}.$$

Пример 3.9. Рассмотрим правила построения кода, исправляющего 2 ошибки для 1 информационного символа.

Заметим, что согласно формуле Хэмминга для этого достаточно $r = 4$ проверочных символа

$$2^4 = C_5^0 + C_5^1 + C_5^2 = 1 + 5 + 10 = 16.$$

По существу мы имеем простейший повторный код с 4 повторениями:

$$(a) \to (aaaaa).$$

★ Для построения полиномиального кода мы возьмем два примитивных полинома 2 степени $p_2 = x^2 + x + 1$. Тогда

$$\operatorname{ord}(p_r \cdot p_r) = 2\operatorname{ord}(p_r) \qquad \text{или} \qquad \operatorname{ord}(p_2 \cdot p_2) = 2\operatorname{ord}(p_2) = 2 \cdot 3 = 6.$$

Но 6 значений не достаточно чтобы обработать 15 возможных комбинаций ошибок.

★ Теперь возьмем 2 полинома различной степени. Например $p_2 = x^2 + x + 1$ и $p_3 = x^3 + x + 1$, тогда

$$\operatorname{ord}(p_r \cdot p_m) = \text{НОК}(\operatorname{ord} p_r, \operatorname{ord} p_m) \qquad \text{или} \qquad \operatorname{ord}(p_2 \cdot p_3) = \text{НОК}(3, 7) = 3 \cdot 7 = 21.$$

Поскольку мы имеем 5 проверочных разрядов, то кодовая комбинация из 6 разрядов допускает

$$C_6^1 + C_6^2 = 6 + 15 = 21$$

различных единичных или двойных ошибок. Т.е. нам необходим код $[6, 1]$. Как видно в данном случае полиномиальный код уступает по эффективности простейшему повторному коду $[5, 1]$. ▲

Пример 3.10. Рассмотрим правила построения кода, исправляющего 2 ошибки для $k = 2$ информационных символов.

★ Продолжая аналогично предыдущему примеру возьмем 2 полинома 3 степени $p_3 = x^3 + x + 1$ и $p_3 = x^3 + x^2 + 1$. Тогда

$$\operatorname{ord}(p_r \cdot p_r) = 2\operatorname{ord}(p_r) \qquad \text{или} \qquad \operatorname{ord}(p_3 \cdot p_3) = 2\operatorname{ord}(p_3) = 2 \cdot 7 = 14.$$

Это недостаточно для обработки $C_8^1 + C_8^2 = 8 + 28 = 36$ ошибок.

★ Увеличиваем степени полиномов, например $p_2 = x^2 + x + 1$ и $p_4 = x^4 + x + 1$, тогда

$$\operatorname{ord}(p_2 \cdot p_4) = \text{НОК}(3, 15) = 3 \cdot \text{НОК}(1, 5) = 3 \cdot 5 = 15.$$

Поскольку мы имеем $r = 6$ проверочных разрядов, то кодовая комбинация из $k+r = 8$ разрядов допускает $C_8^1 + C_8^2 = 36$ различных единичных или двойных ошибок. Опять неудача.

★ Увеличим степени полиномов: $p_3 = x^3 + x + 1$ и $p_4 = x^4 + x + 1$, тогда

$$\operatorname{ord}(p_3 \cdot p_4) = \text{НОК}(7, 15) = 7 \cdot 15 = 105.$$

Этого достаточно для обработки $C_9^1 + C_9^2 = 9 + 36 = 45$ ошибок. Т.е. нам необходим код $[9, 2]$. ▲

Пример 3.11. Рассмотрим правила построения кода, исправляющего 2 ошибки для $k = 3$ информационных символов.

★ Продолжая аналогично предыдущему примеру возьмем 2 полинома 3 степени $p_3 = x^3 + x + 1$. Тогда

$$\operatorname{ord}(p_r \cdot p_r) = 2\operatorname{ord}(p_r) \qquad \text{или} \qquad \operatorname{ord}(p_3 \cdot p_3) = 2\operatorname{ord}(p_3) = 2 \cdot 7 = 14.$$

Это недостаточно для обработки

$$C_9^1 + C_9^2 = 9 + 36 = 45$$

ошибок.

★ Увеличим степени полиномов: $p_3 = x^3 + x + 1$ и $p_4 = x^4 + x + 1$, тогда

$\operatorname{ord}(p_r \cdot p_m) = \text{НОК}(\operatorname{ord} p_r, \operatorname{ord} p_m)$ или $\operatorname{ord}(p_3 \cdot p_4) = \text{НОК}(7, 15) = 7 \cdot 15 = 105.$

Этого достаточно для обработки

$$C_{10}^1 + C_{10}^2 = 10 + 55 = 65$$

ошибок. Таким образом код, исправляющий 2 ошибки при передаче 3 информационных символов должен иметь 7 проверочных разрядов и вид $[n, k] = [10, 3]$. ▲

Пример 3.12. Построим код исправляющий 2 ошибки при передече информационого сообщения $a = (11)$. Полином информациоонного сообщения имеет вид $m(x) = 1 + x$. Для построения кодовой последовательности возьмем неприводимые полиномы $p_1 = 1 + x + x^3$ и $p_2 = 1 + x + x^4$. Тогда

$$\left[\frac{x^7 m(x)}{(1 + x + x^3)(1 + x + x^4)}\right] = \left[\frac{x^7(1 + x)}{1 + x^2 + x^3 + x^5 + x^7}\right] = 1 + x + x^2 + x^4 + x^5 + x^6,$$

или

$$R(x) = 1 + x + x^2 + x^4 + x^5 + x^6 = (001110111)$$

Тогда для кодовой последовательности получим $F = x^7 m(x) \oplus R(x)$:

$$\begin{array}{r} 110000000 \\ \oplus\ 001110111 \\ \hline 111110111 \end{array}$$

или

$$F = 1 + x + x^2 + x^4 + x^5 + x^6 + x^7 + x^8.$$

Допустим в кодовой последовательности возникло 2 ошибки, после чего она приняла вид

$$\overline{F} = (101110011) = 1 + x + x^4 + x^5 + x^6 + x^8.$$

Найдем остаток от деления $\frac{\overline{F}}{P}$

$$R(x) = \left[\frac{\overline{F}}{P}\right] = 1 + x^3 + x^5 = 0101001$$

Составим таблицу синдромов, определяющих место ошибки в передаваемом сообщении. Найдем остаток от деления $\frac{x^k + x^m}{P}$:

k	x^k	$1 + x^k$	$x + x^k$	$x^2 + x^k$	$x^3 + x^k$	$x^4 + x^k$	$x^5 + x^k$	$x^6 + x^k$	$x^7 + x^k$
0	0000001								
1	0000010	0000011							
2	0000100	0000101	0000110						
3	0001000	0001001	0001010	0001100					
4	0010000	0010001	0010010	0010100	0011000				
5	0100000	0100001	0100010	0100100	0101000	0110000			
6	1000000	1000001	1000010	1000100	1001000	1010000	1100000		
7	0101101	0101100	0101111	0101001	0100101	0111101	0001101	1001101	
8	1101010	1011011	1011000	1011110	1010010	1001010	1111010	0111010	1110111

Пользуясь таблицей находим, что остаток $R = 0101001$ соответствует остатку x^2+x^7, т.е. ошибкам во 2 и 7 разряде полинома кодовой комбинации. Исправляя, получим

$$1\underline{\mathbf{0}}1110\underline{\mathbf{0}}11 \Rightarrow 1\underline{\mathbf{1}}1110\underline{\mathbf{1}}11.$$

Убирая последние семь проверочных символа, получаем исходную информационную последовательность $a = (11)$. ▲

Задача 3.9. На приемнике было получено кодовое слово **x** сформированное полиномиальным кодом $[n, k] = [9, 2]$ с $p_1 = 1+x^2+x^3$ и $p_2 = 1+x+x^4$ исправляющего 2 ошибки. Восстановить исходное сообщение предварительно построив таблицу синдромов.

N	x	N	x	N	x
1	110001101	11	101101101	21	001000110
2	110001011	12	101011101	22	010000110
3	110000111	13	101000101	23	011100110
4	110011111	14	001001011	24	011010110
5	110101111	15	111001011	25	011001110
6	111001111	16	100001011	26	011000010
7	100001111	17	101101011	27	011000100
8	010001111	18	101011011	28	011010101
9	110001000	19	101000011	29	011001101
10	110000100	20	101001111	30	011000001

Задача 3.10. На приемнике было получено кодовое слово **x** сформированное полиномиальным кодом с $p_1 = 1 + x + x^2$ и $p_2 = 1 + x^3 + x^5$ исправляющего 2 ошибки. Восстановить исходное сообщение.

N	x	N	x	N	x
1	001010110111	11	000111001000	21	0100111111011
2	001010110100	12	000111001110	22	0100111110111
3	001010110010	13	000111000010	23	0100111101111
4	001010111110	14	000111011010	24	0100111011111
5	001010100110	15	000111101010	25	0100110111111
6	101110111110	16	001110011011	26	0011001001111
7	101000111110	17	001101011011	27	0011111001111
8	101011111110	18	001011011011	28	0010011001111
9	101010011110	19	000111011011	29	0001011001111
10	101010101110	20	011111011011	30	0111011001111

3.3 Коды Рида-Миллера

Коды Рида-Маллера предложены в 1954 г. и обозначаются как $RM(r,m)$, где r-порядок кода, 2^m-длина кода. Порождающая матрица кода $RM(0,m)$ имеет вид строки из 2^m единиц:

$$G_{0,m} = G_0(m) = (1,1,...,1).$$

Порождающая матрица кода $RM(1,3)$ имеет вид

$$G_{1,3} = G_1(3) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Для кодирования информационного сообщения $\mathbf{x}$ длиной $k = m+1$ необходимо подействовать на него оператором $\mathbf{G}$ справа:

$$\mathbf{y} = \mathbf{xG}.$$

Результатом кодирования будет кодовое слово $\mathbf{y}$ длиной $n = 2^m$.

Декодирование кода использует матрицу Адамара. Мы возмем рекурсивную формулу для построения матриц Адамара

$$H_{k+1} = \begin{pmatrix} H_k & H_k \\ H_k & -H_k \end{pmatrix} \qquad \text{где} \qquad H_0 = 1.$$

Например

$$H_0 = 1; \quad H_1 = \begin{pmatrix} H_0 & H_0 \\ H_0 & -H_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix};$$

$$H_2 = \begin{pmatrix} H_1 & H_1 \\ H_1 & -H_1 \end{pmatrix} = \left(\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array}\right);$$

$$H_3 = \begin{pmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{pmatrix} = \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{array}\right) \text{ ...и т.д.}$$

Декодирование по принципу максимального правдоподобия означает выбор из всех возможных кодовых слов того слова $\mathbf{y}$, которое находится на минимальном расстоянии Хэмминга от принятого слова.

Процесс декодирования выводится из формул

$$y_0 = x_0, \qquad y_{2^i} = x_0 \oplus x_{m-i}$$

или

$$x_0 = y_0, \qquad x_{m-i} = y_0 \oplus y_{2^i}, \qquad \text{где} \quad i = 0, 1, ..., m-1.$$

Пример 3.13. Построим $RM(1,3)$-код для информационого сообщения $a = (1011)$.

$$\mathbf{y} = \mathbf{xG} = (1011) \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} = (10011001).$$

Перед процессом декодирования перепишем кодовое слово используя формулу

$$\mathbf{Y} = 2\mathbf{y} - 1 \qquad \text{т.е.} \qquad \mathbf{Y} = (1, -1, -1, 1, 1, -1, -1, 1)$$

и подействунм на него матрицей Адамара $\mathbf{H}_3$ справа

$$\mathbf{z} = \mathbf{YH}_3 = (1, -1, -1, 1, 1, -1, -1, 1) \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{array}\right) = (00080000).$$

Наибольшая по модулю компонента **8** - четвертая слева. Следовательно ближайшем кодовым словом будет 4 столбец матрицы Адамара $\mathbf{H}_3$, т.е. вектор

$$\mathbf{y} = (1, -1, -1, 1, 1, -1, -1, 1) \cong (10011001).$$

Декодирование производится по формулам

$$\begin{array}{llll} x_0 & = y_0 & & = 1 \\ x_3 & = y_0 \oplus y_1 & = 1 \oplus 0 & = 1 \\ x_2 & = y_0 \oplus y_2 & = 1 \oplus 0 & = 1 \\ x_1 & = y_0 \oplus y_4 & = 1 \oplus 1 & = 0 \end{array}$$

т.е. $\mathbf{x} = (1011)$. Напомним, что в последней формуле нумерация символов производится с нуля.

Допустим, в передаваемом сообщении возникла ошибка (например в 5 символе слева)

$$\mathbf{y} = (1001\underline{\mathbf{0}}001).$$

Перед процессом декодирования перепишем кодовое слово используя формулу

$$\mathbf{Y} = 2\mathbf{y} - 1 \qquad \text{т.е.} \qquad \mathbf{Y} = (1, -1, -1, 1, -1, -1, -1, 1)$$

и подействунм на него матрицей Адамара $\mathbf{H}_3$ справа

$$\mathbf{z} = \mathbf{Y}\mathbf{H}_3 = (1, -1, -1, 1, -1, -1, -1, 1).\mathbf{H}_3 = (-2, -2, -2, 6, 2, 2, 2, 2).$$

Наибольшая по модулю компонента **6** - четвертая слева. Следовательно ближайшем кодовым словом будет 4 столбец матрицы Адамара $\mathbf{H}_3$. Декодируя аналогично предыдущему случаю получим ответ $\mathbf{x} = (1011)$.

Задача 3.11. На приемнике было получено кодовое слово $\mathbf{y}$ сформированное кодом Рида-Маллера $RM(1, 3)$. Восстановить исходное сообщение.

N	y	N	y	N	y	N	y	N	y
1	10101010	7	11000010	13	10010111	19	11011100	25	00101100
2	10101000	8	11000001	14	10010100	20	11000100	26	00110100
3	10101110	9	11000111	15	10010010	21	11001000	27	00111000
4	10100010	10	11001011	16	10011110	22	11001110	28	00111110
5	10111010	11	11010011	17	10000110	23	11111000	29	11110010
6	11100000	12	11001101	18	00111101	24	11110100	30	11110001

Задача 3.12. На приемнике было получено кодовое слово $\mathbf{y}$ сформированное кодом Рида-Маллера $RM(1, 4)$. Восстановить исходное сообщение.

N	y	N	y	N	y
1	1001011010010111	11	1001100110011000	21	1111000000001110
2	0011001111001110	12	0011110011000001	22	0011001111001110
3	1001011010010010	13	1001100110011101	23	1111000000001011
4	1001011010011110	14	1001100110010001	24	1111000000000111
5	0011001111011100	15	0011110011010011	25	0011110011010011
6	1001011010110110	16	1001100110111001	26	1111000000101111
7	1001011011010110	17	1001100111011001	27	1111000001001111
8	0011001101001100	18	0011110001000011	28	0011001101001100
9	1001011110010110	19	1001100010011001	29	1111000100001111
10	0011000111001100	20	0011111011000011	30	0011111011000011

3.4 Сверточные коды

Наиболее распространенным видом помехоустойчивого кодирования в настоящее время являются сверточные коды:

- протоколы беспроводной связи IMT-2000, GSM, IS-95
- цифровые наземные и спутниковые системы связи
- системы связи с дальним космосом.

Основные принципы работы этих кодов построены на теории автоматов.

3.4.1 Блочное чередование

При передаче информации ошибки как правило появляются пакетами. К примеру такой источник ошибок как грозовая молния длится от 10 до 100ms. Если мы используем **CDMA** на частоте 1.23MHz и скорости 153kbs, то одна вспышка молнии запросто уничтожает от 1.5 до 15kb передаваемых данных. Если вы передаете SMS по сотовому телефону **GSM** на скорости 9.6 kbs, то можете потерять до 960bt. Поскольку в кодировке UTF16 каждая русская буква занимает 2Bt=16bt, то 960bt - это сообщение из 60 символов.

Для защиты от пакетных ошибок в GSM используется алгоритм перемежения, который позволяеь преобразовать пакет в независимые ошибки. Для этого кодовая комбинация $(a_1a_2a_3...a_n)$ длиной n записывается построчно в матрицу размером $k \times k$

$$\begin{pmatrix} a_1 & a_2 & ... & a_k \\ a_{k+1} & a_{k+2} & ... & a_{2k} \\ ... & ... & ... & ... \\ & & ... & a_{k^2} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1k} \\ a_{21} & a_{22} & ... & a_{2k} \\ ... & ... & ... & ... \\ a_{k1} & a_{k2} & ... & a_{k^2} \end{pmatrix}$$

а считывается по столбцам $(a_{11}a_{21}a_{31}...a_{k^2})$. В результате исходные символы, которые следовали друг за другом, передаются в канал с интервалом в k символом, который называется **глубиной перемежения**.

Если матрица квадратная, то процесс декодирования аналогичен предыдущему алгоритму. Если же матрица прямоугольная то декодирование производится в обратном порядке: последовательность записывается по столбцам, а считывается построчно.

Например возьмем сообщение **выстрел** и закодируем его повторным кодом $[n, k] = [3, 1]$. Получим кодовую комбинацию **ввввыыыссстттрррееелллл**. Допустим во время передачи этого сообщения оно было искажено пакетной ошибкой, т.е. заменим последовательно 5 символов начиная с 8-го на букву **а ввввыыысаааааррреееллл**. Если попытаться раскодировать это сообщение как есть, то мы получим **ввв ыыы саа ааа ррр еее ллл** $\Rightarrow$ **выаарел**.

Теперь перед отправлением сообщения используем метод перемежения. Для этого

запишем исходную комбинацию в матрицу построчно

$$\begin{vmatrix} в & в & в & ы & ы \\ ы & с & с & с & т \\ т & т & р & р & р \\ е & е & е & л & л \\ л & \_ & \_ & \_ & \end{vmatrix}$$

и считаем по столбцам **вытелвсте_всре_ы срл_ытрл**. Допустим во время передачи этого сообщения оно было искажено такой же пакетной ошибкой: **вытелвсаааааре_ысрл_ытрл**. Запишем принятую комбинацию в матрицу по столбцам

$$\begin{vmatrix} в & в & а & ы & ы \\ ы & с & а & с & т \\ т & а & р & р & р \\ е & а & е & л & л \\ л & а & \_ & \_ & \end{vmatrix}$$

и прочитаем построчно **ва ыыы сас тта ррр еае ллл а__** $\Rightarrow$ **выстрел**. Как видно сообщение без труда восстанавливается в правильном виде.

3.4.2 Теория автоматов

Автоматом называется система, меняющая свое состояние под действием обрабатываемого входного сигнала. В этом случае значения выходного сигнала зависят не только от входного значения, но и от текущего состояния самой системы.

Для описания работы автомата необходимо задать

- вектор значений входящего сигнала $a = (a_1 a_2 ... a_n)$,
- вектор внутренних состояний автомата $s = (s_1 s_2 ... s_n)$.

Во время работы на вход автомата подается очередное значение сигнала a_i. В зависимости от текущего состояния s_k автомат изменяет значение сигнала на z_i, но и сам под воздействием входного сигнала меняет свое состояние на s_m. Следующее значение сигнала a_{i+1} автомат принимает находясь в состоянии s_m и в соответствии со своим состоянием формирует выходное значение z_{i+1}, а сам при этом меняет свое состояние на s_n и т.д.

Как видно, для описания работы автомата нам необходимо задать еще

- вектор возможных значений выходного сигнала $z = (z_1 z_2 ... z_n)$,
- функцию перехода g: $(a_k s_k) \to (z_k)$, которая создает значения выходного сигнала z_k из входного s_k с учетом текущего состояния автомата s_k.
- функцию перехода f: $(a_k s_k) \to (s_{k+1})$, которая меняет состояние автомата s_k на s_m в зависимости от значения принятого сигнала a_k и текущего состояния автомата s_k.

Поскольку все значения являются дискретными, то функции f и g как правило задают таблицами.

Пример 3.14. На вход автомата подается сигнал $a = (0011101010)$. Получить выходной сигнал, если функции перехода f и g автомата заданы таблицей.

	f		g	
	0	1	0	1
s_0	s_1	s_0	0	1
s_1	s_1	s_2	1	1
s_2	s_0	s_1	1	0

Решение.

1 метод. Исследование работы автомата удобнее проводить в два этапа. На первом этапе мы рассмотрим изменение состояния автомата под действием входного сигнала (т.е. функцию f).

Запишем в строку значения входного сигнала

$$a = (0011101010).$$

Начальное состояние автомата s_0 запишем над первым значением. Первое значение входного сигнала $a_1 = 0$. По таблице для f на пересечении s_0 и 0 находим новое состояние автомата s_1 и запишем его над вторым значением сигнала:

$$\begin{array}{ccc} s_0 & \longrightarrow & s_1 \\ 0 & \nearrow & \end{array}$$

Второе значение входного сигнала $a_2 = 0$. По таблице для f на пересечении s_1 и 0 находим новое состояние автомата s_1 и запишем его над третьим значением сигнала:

$$\begin{array}{ccccc} s_0 & \longrightarrow & s_1 & \longrightarrow & s_1 \\ 0 & \nearrow & 0 & \nearrow & \end{array}$$

Третье значение входного сигнала $a_3 = 1$. По таблице для f на пересечении s_1 и 1 находим новое состояние автомата s_2 и запишем его над четвертым значением сигнала:

$$\begin{array}{ccccccc} s_0 & \longrightarrow & s_1 & \longrightarrow & s_1 & \longrightarrow & s_2 \\ 0 & \nearrow & 0 & \nearrow & 1 & \nearrow & \end{array}$$

и т.д.

Полная последовательность состояний, принимаемых автоматом под воздействием входного сигнала имеет вид

$$\begin{array}{c|cccccccccccccccccc} s_k & s_0 & \to & s_1 & \to & s_1 & \to & s_2 & \to & s_1 & \to & s_2 & \to & s_0 & \to & s_0 & \to & s_1 & \to & s_2 \\ a & 0 & \nearrow & 0 & \nearrow & 1 & \nearrow & 1 & \nearrow & 1 & \nearrow & 0 & \nearrow & 1 & \nearrow & 0 & \nearrow & 1 & \nearrow & 0 \end{array}$$

Теперь, зная все состояния автомата найдем выходной сигнал используя функцию g таблицы. Для первого значения входного сигнала $a_1 = 0$ и состояния s_0 найдем выходное значение 0:

$$\begin{array}{c} s_0 \\ 0 \\ 0 \end{array}$$

Для второго значения входного сигнала $a_2 = 0$ и состояния s_1 найдем выходное значение 1:

s_0	s_1
0	0
0	1

Для третьего значения входного сигнала $a_3 = 1$ и состояния s_1 найдем выходное значение 1:

s_0	s_1	s_1
0	0	1
0	1	1

и т.д.

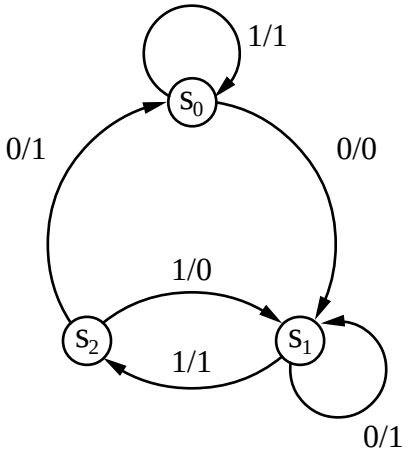
Дальнейшую динамику работы автомата можно проследить по таблице

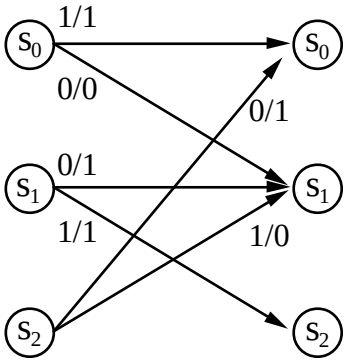
s_k	s_0	$\to$	s_1	$\to$	s_1	$\to$	s_2	$\to$	s_1	$\to$	s_2	$\to$	s_0	$\to$	s_0	$\to$	s_1	$\to$	s_2
a	0	$\nearrow$	0	$\nearrow$	1	$\nearrow$	1	$\nearrow$	1	$\nearrow$	0	$\nearrow$	1	$\nearrow$	0	$\nearrow$	1	$\nearrow$	0
F	0		1		1		0		1		1		1		0		1		1

Таким образом, выходная последовательность работы автомата имеет вид

$$z = (0110111011).$$

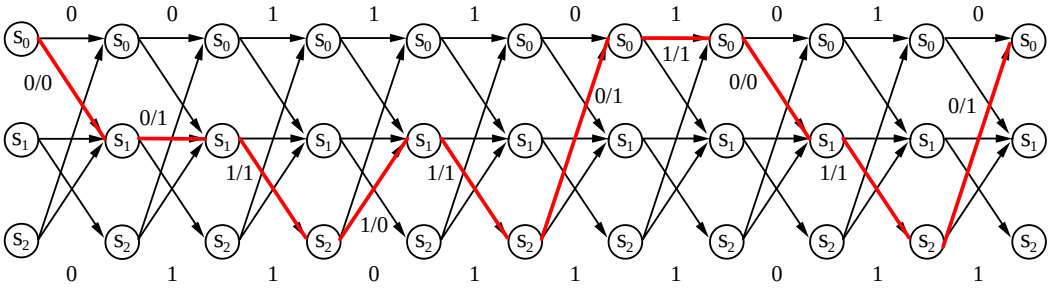
2 метод. Каждому автомату можно поставить в соответствие ориентированный граф, если в качестве узлов графа взять состояния автомата s_k, а в качестве веса ребра - значение a_k/z_k. Тогда граф, соответствующий предыдущей задаче имеет вид





По заданному графу мы построим базисный треллис - схему изменения состояний системы на одном шаге. Размножая данный базисный треллис до размера, равного длине входной последовательности мы построим треллис автомата. Теперь, начиная из состояния S_0 будем выделять ребра, числители которых на каждом шаге совпадают с данными входной последовательности.

Тогда знаменатели выделенных ребер соответствуют выходной последовательности работы автомата.

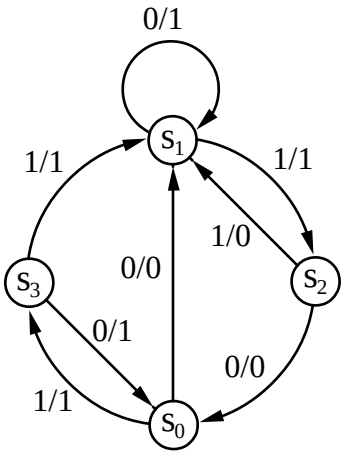


Как и в 1 случае, выходная последовательность работы автомата имеет вид

$$z = (0110111011). \qquad \blacktriangle$$

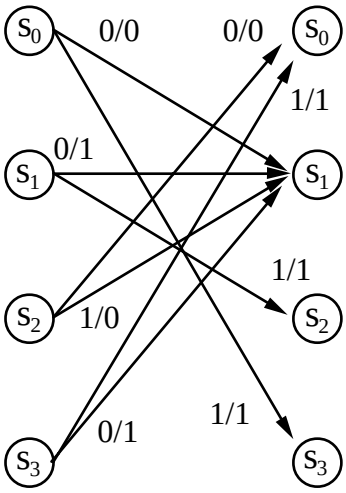
Пример 3.15. На вход автомата подается сигнал **M**. Построить граф автомата и найти выходной сигнал, если функции перехода f и g автомата заданы таблицей.

	f		g	
	0	1	0	1
s_0	s_1	s_3	0	1
s_1	s_1	s_2	1	1
s_2	s_0	s_1	0	0
s_3	s_0	s_1	1	1



Решение. Граф автомата и его базисный треллис показан на рисунке. Символу **M** соответствует ASCII код **4d** т.е. в двоичной системе исчисления на вход автомата подается сигнал

$$z = (1001101).$$



Выходная последовательность работы автомата имеет вид

$$z = (1101011) \quad \text{или} \quad \mathbf{6b}$$

что соответствует ASCII символу **k**. $\blacktriangle$

Задача 3.13. На вход автомата подается ASCII код первой буквы фамилии курсанта. Получить выходной сигнал, если функции перехода f и g автомата заданы таблицей. Начертить граф автомата.

01

	f		g	
	0	1	0	1
s_0	s_0	s_2	0	1
s_1	s_1	s_3	1	1
s_2	s_0	s_2	1	1
s_3	s_1	s_3	1	1

02

	f		g	
	0	1	0	1
s_0	s_1	s_2	0	1
s_1	s_1	s_3	0	1
s_2	s_3	s_1	1	1
s_3	s_2	s_1	1	1

03

	f		g	
	0	1	0	1
s_0	s_1	s_3	0	1
s_1	s_1	s_2	1	1
s_2	s_2	s_1	0	1
s_3	s_3	s_1	1	1

04

	f		g	
	0	1	0	1
s_0	s_1	s_2	0	1
s_1	s_1	s_2	1	1
s_2	s_1	s_2	1	1
s_3	s_1	s_2	0	1

05

	f		g	
	0	1	0	1
s_0	s_0	s_2	0	1
s_1	s_0	s_2	1	1
s_2	s_0	s_2	1	1
s_3	s_0	s_2	1	1

06

	f		g	
	0	1	0	1
s_0	s_0	s_2	0	1
s_1	s_1	s_3	1	1
s_2	s_2	s_0	1	0
s_3	s_3	s_1	1	1

07

	f		g	
	0	1	0	1
s_0	s_1	s_3	0	1
s_1	s_2	s_0	1	1
s_2	s_3	s_1	1	1
s_3	s_0	s_2	1	0

08

	f		g	
	0	1	0	1
s_0	s_1	s_2	0	1
s_1	s_2	s_3	1	0
s_2	s_3	s_0	1	1
s_3	s_0	s_1	1	1

09

	f		g	
	0	1	0	1
s_0	s_3	s_1	0	0
s_1	s_0	s_2	1	1
s_2	s_0	s_2	1	1
s_3	s_3	s_1	1	1

10

	f		g	
	0	1	0	1
s_0	s_1	s_2	0	1
s_1	s_1	s_2	0	1
s_2	s_0	s_1	1	0
s_3	s_1	s_1	1	0

11

	f		g	
	0	1	0	1
s_0	s_1	s_2	1	1
s_1	s_1	s_0	0	1
s_2	s_2	s_1	0	0
s_3	s_0	s_1	1	0

12

	f		g	
	0	1	0	1
s_0	s_1	s_0	0	1
s_1	s_1	s_2	1	1
s_2	s_0	s_2	1	0
s_3	s_0	s_2	0	0

13

	f		g	
	0	1	0	1
s_0	s_1	s_0	1	1
s_1	s_1	s_0	0	1
s_2	s_0	s_1	1	0
s_3	s_0	s_1	0	0

14

	f		g	
	0	1	0	1
s_0	s_1	s_2	1	1
s_1	s_1	s_2	1	1
s_2	s_0	s_1	0	0
s_3	s_0	s_1	0	0

15

	f		g	
	0	1	0	1
s_0	s_1	s_2	0	1
s_1	s_1	s_2	0	0
s_2	s_3	s_1	1	1
s_3	s_3	s_1	1	0

16

	f		g	
	0	1	0	1
s_0	s_1	s_3	0	1
s_1	s_2	s_3	1	0
s_2	s_3	s_1	0	1
s_3	s_0	s_1	1	0

17

	f		g	
	0	1	0	1
s_0	s_1	s_2	1	1
s_1	s_2	s_2	0	0
s_2	s_3	s_1	0	1
s_3	s_0	s_1	1	0

18

	f		g	
	0	1	0	1
s_0	s_1	s_0	0	1
s_1	s_2	s_3	1	0
s_2	s_3	s_2	1	1
s_3	s_0	s_1	0	0

19

	f		g	
	0	1	0	1
s_0	s_0	s_0	1	1
s_1	s_1	s_1	0	0
s_2	s_2	s_2	1	1
s_3	s_3	s_3	0	0

20

	f		g	
	0	1	0	1
s_0	s_0	s_3	1	1
s_1	s_3	s_1	1	0
s_2	s_2	s_2	0	1
s_3	s_1	s_0	0	0

21

	f		g	
	0	1	0	1
s_0	s_1	s_0	0	1
s_1	s_2	s_0	0	0
s_2	s_3	s_1	1	0
s_3	s_3	s_1	1	1

22

	f		g	
	0	1	0	1
s_0	s_1	s_0	0	1
s_1	s_2	s_0	1	0
s_2	s_3	s_2	0	0
s_3	s_3	s_2	1	1

23

	f		g	
	0	1	0	1
s_0	s_1	s_0	1	1
s_1	s_2	s_0	0	0
s_2	s_3	s_3	0	0
s_3	s_3	s_3	1	1

24

	f		g	
	0	1	0	1
s_0	s_0	s_0	0	1
s_1	s_1	s_3	1	0
s_2	s_2	s_0	1	0
s_3	s_3	s_3	0	1

25	f		g	
	0	1	0	1
s_0	s_0	s_2	1	1
s_1	s_1	s_3	0	0
s_2	s_2	s_0	1	0
s_3	s_3	s_1	0	1

26	f		g	
	0	1	0	1
s_0	s_0	s_1	1	1
s_1	s_1	s_2	1	0
s_2	s_2	s_3	0	0
s_3	s_3	s_0	0	1

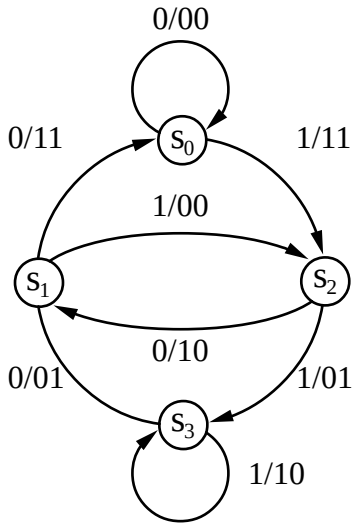
27	f		g	
	0	1	0	1
s_0	s_0	s_1	0	0
s_1	s_1	s_2	0	1
s_2	s_2	s_1	1	0
s_3	s_3	s_2	1	1

28	f		g	
	0	1	0	1
s_0	s_0	s_0	0	0
s_1	s_1	s_0	1	1
s_2	s_2	s_0	0	0
s_3	s_3	s_0	1	1

3.4.3 Сверточные коды

Сверточным кодом называется автомат, обрабатывающий двоичную последовательность и имеющий 4 состояния $s = (s_0, s_1, s_2, s_3)$:

	f		g	
	0	1	0	1
s_0	s_0	s_2	00	11
s_1	s_0	s_2	11	00
s_2	s_1	s_3	10	01
s_3	s_1	s_3	01	10

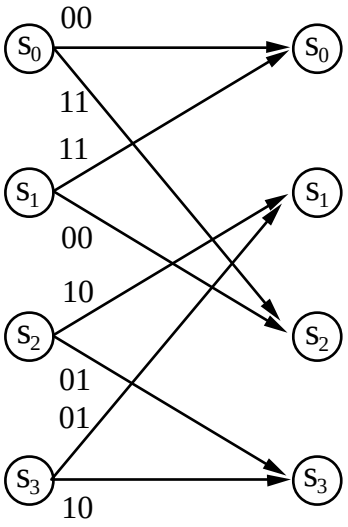


Пример 3.16. Согласно таблице перехода для входной последовательности

$$a = (1, 1, 0, 1, 1, 1, 0, 0)$$

автомат выдаст сигнал

$$F = (11, 01, 01, 00, 01, 10, 01, 11). \quad \blacktriangle$$



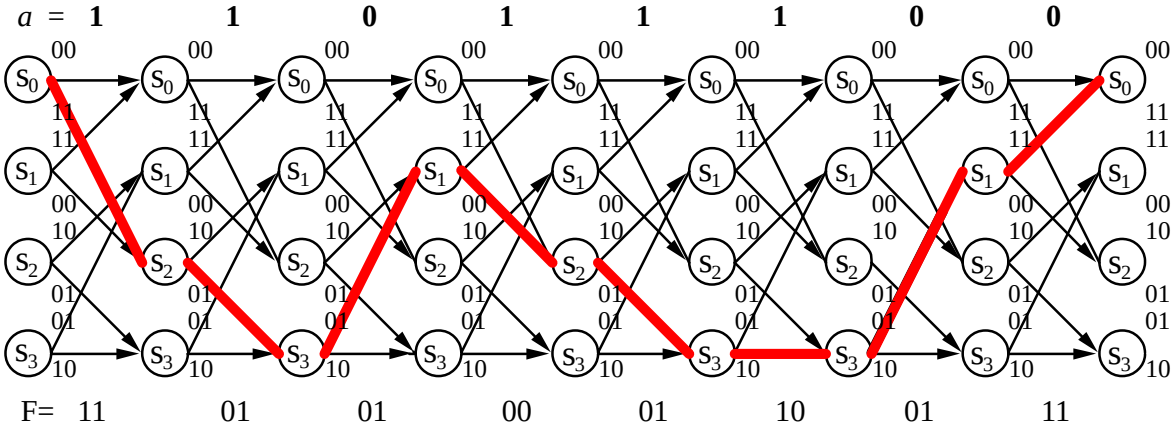
Работу автомата удобно описывать с помощью развернутой решеточной диаграммы - **треллиса**[a]. Поскольку изначально предполгается что автомат находился в состоянии s_0, то любой путь начинается из левого верхнего угла треллиса. На каждом шаге путь вдоль диаграммы может принимать два направления. Если очередной символ информационной последовательности принимает значение

0 - автомат выбирает **верхнее** ребро;

1 - автомат выбирает **нижнее** ребро.

Выходная кодовая последовательность автомата равна весу всех ребер выбранного пути.

[a] trellis diagram - (англ.) решеточная диаграмма



Треллис для кодовой последовательности

$$F = (11, 01, 01, 00, 01, 10, 01, 11)$$

показан на рисунке.

Декодирование полученной кодовой последовательности производится в обратном порядке.

Пример 3.17. Раскодировать последовательность

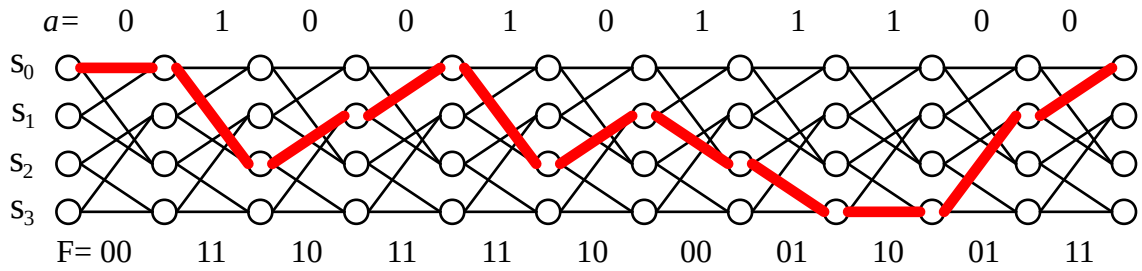
$$F = (00, 11, 10, 11, 11, 10, 00, 01, 10, 01, 11).$$

Решение. Начиная из узла s_0 треллиса мы на кждом шаге будем выбирать ребро с весом, соответствующим полученной кодовой комбинации. Так для первой пары символов мы имеем значения 00. Для треллиса это соответствует верхнему ребру выходящему из узла s_0 при t=0. Мы перешли в ребро s_0 при t=1.

Для второй пары принятой кодовой комбинации мы имеем 11. Т.к. мы находимся в узле s_0 при t=1, то с весом 11 у нас имеется только нижнее ребро и мы переходим в узел s_2 (на t=2).

Для третьей пары принятой кодовой комбинации мы имеем 10. Поскольку мы теперь находимся в узле s_2 (при t=2) то с весом 10 из него выходит только верхнее ребро. Мы выбираем ребро 10 и переходим на узел s_1 (t=3).

Четвертая пара имеет значение 11. Поскольку мы теперь находимся в узле s_1 (при t=3) то с весом 11 у нас имеется только верхнее ребро. Мы переходим по ребру 11 в узел s_0 и т.д.



Прочертив жирным следом весь путь треллиса можно приступить к раскодированию сообщения.

Каждый узел треллиса имеет два выходящих ребра: верхнее и нижнее. Если для данного узла выделенный путь пошел через верхнее ребро, то информационный символ принимает значение 0. Если для данного узла выделенный путь пошел через нижнее ребро, то информационный символ принимает значение 1. В нашем случае выходная информационная последовательность принимает вид $a = (01001011000)$. ▲

Задача 3.14. Построить сверточный код для двоичной последовательности ASCII кода первой буквы своей фамилии.

3.4.4 Коррекция ошибок сверточным кодом

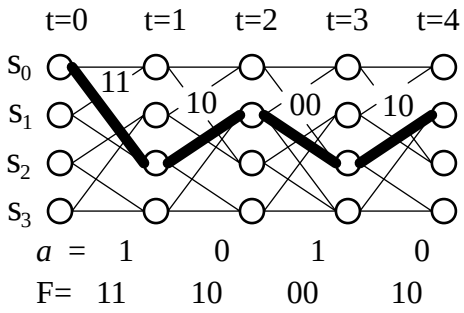
Как было показано выше каждой кодовой комбинации соответствует свой путь в треллисе. Однако обратное не верно. Не для всякой полученной последовательности можно начертить путь в треллисе. Например не существует пути для такой комбинайии как $F = (11, 11, 11)$ или $F = (01, 01, 01)$. Так же нет кодовых комбинаций, начинающихся с 01 или 10. Такие пары в F свидетельствуют о наличии ошибок. Искажение двоичной кодовой последовательности при передаче по каналу информации с помехами заключается в изменении значения некоторого бита на противоположное. Если ниформация кодируется блоками, то количество ошибок в блоке равно количеству несовпадений между принятым словом и исходным. Напомним, что расстояние между сообщениями определяется как количество несовпадающих разрядов. Поэтому каждая ошибка в передаваемой кодовой комбинации увеличивает ее расстояние от исходного значения. Соответственно новая, искаженная кодовая комбинация будет иметь искаженный путь треллиса. А в некоторых ситуациях пути может и не быть. Задача коррекции ошибки заключается в построении для F множества возможных путей и выбора среди них такого, который имеет минимальное расстояние с полученной кодовой комбинацией F.

Пример 3.18. Передаваемое информационное сообщение имеет вид

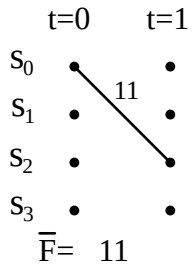
$$a = (1010).$$

Этому сообщению соответствует следующая кодовая комбинация

$$F = (11, 10, 00, 01).$$

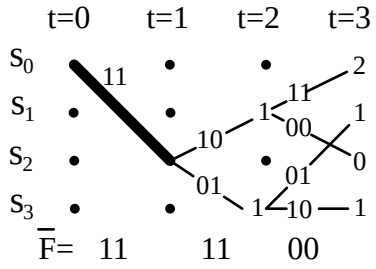


Допустим в передаваемой комбинации возникла ошибка $\overline{F(x)} = (11, 1\underline{\mathbf{1}}, 00, 10)$. Необходимо восстановить информационную последовательность.

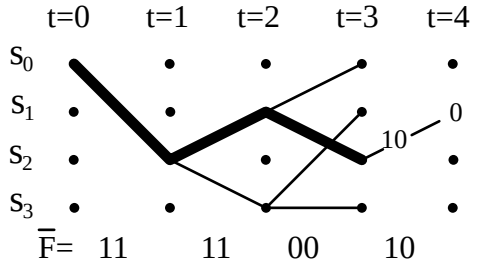


Решение. Начиная из узла s_0(t=0) треллиса мы выбирем ребро с весом, соответствующим полученной кодовой комбинации $\overline{F(x)}$. Так для первой пары символов мы имеем значения 11. Для треллиса это соответствует нижнему ребру выходящему из узла s_0. Мы перешли в узел s_2 при t=1.

На втором шаге из узла s_2(t=1) треллиса мы должны выбрать ребро с весом 11, соответствующим второй паре полученной кодовой комбинации $\overline{F(x)}$. Так как ребер с таким весом у нас нет, то мы рассмотрим оба имеющихся варианта. Для верхнего ребра имеем вес 10. Запишем расстояние между 10 и 11 в узел s_1 (t=2). Для нижнего ребра имеем вес 01. Расстояние между 01 и 11 равно 1 - запишем в узел s_3(t=2).

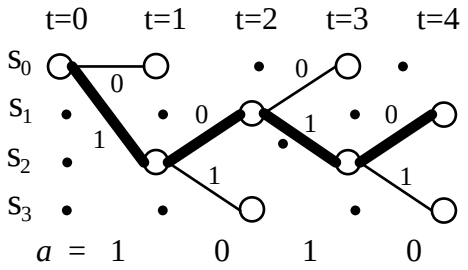


Третья пара принятой комбинации имеет значение 00. На третьем шаге мы имеем два маршрута. Из узла s_1(t=2) треллиса выходят 2 ребра с весом 11 и 00. Расстояния между ними и принятым значением запишем в соответствующих узлах: 2-для s_0 и 0-для s_2. Из узла s_3 также выходят два ребра с весом 01 и 10. Расстояние между ними и принятым знчением 00 равно 1 записывается в узлы s_1 и s_3 (t=3).



На 4 шаге нам необходимо отбросить узлы с максимальным весом, поскольку они соответствуют последовательностям наиболее сильно отличающимся от передаваемой. Для дальнейшего пути мы оставляем только узел s_2. Четвертая пара принятой комбинации имеет значение 10. Из узла s_2(t=3) треллиса выходит верхнее ребро с весом 10 и мы переходим по этому ребру в узел s_1.

В заключение мы должны определить путь проходящий через узлы с минимальным суммарным растоянием. На каждом шаге, верхнему ребру мы ставим в соответствие значение 0, а нижнему ребру значение 1. Раскодированная информационная последовательность имеет вид



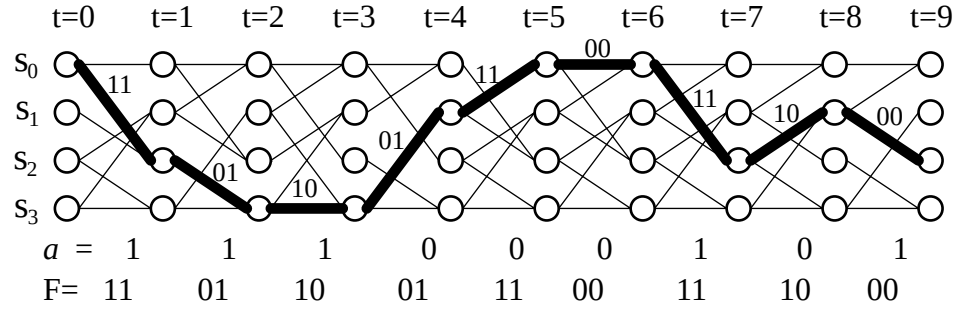
$$a = (1010). \qquad \blacktriangle$$

Пример 3.19. Передаваемое информационное сообщение имеет вид

$$a = (111000101).$$

Этому сообщению соответствует следующая кодовая комбинация, построенная по стреллису:

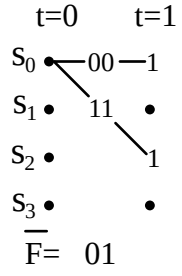
$$F = (11, 01, 10, 01, 11, 00, 11, 10, 00).$$



Допустим в передаваемой комбинации возникло несколько ошибок

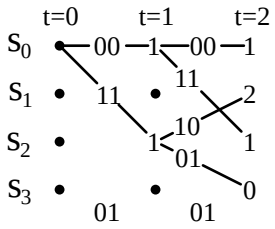
$$F = (\underline{\mathbf{0}}1, 01, 1\underline{\mathbf{1}}, 01, 1\underline{\mathbf{0}}, 00, 1\underline{\mathbf{0}}, 10, 00).$$

Необходимо восстановить информационную последовательность.

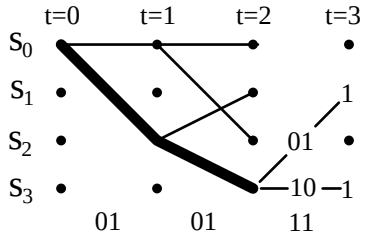


Решение. Начиная из узла s_0(t=0) треллиса мы должны выбрать ребро с весом, соответствующим полученной кодовой комбинации $\overline{F(x)}$. Так для первой пары символов мы имеем значения 01. Однако из узла s_0 не выходит ребер с таким весом. Но есть ребра с весами 00 и 11. Нам необходимо рассмотреть оба имеющихся варианта. Вес верхнего ребра 00. Запишем в узел s_0(t=1) расстояние между весом ребра 00 и значением первой пары 01 кодовой комбинации. В узел s_2(t=1) так же записывается значение 1 - расстояние между весом нижнего ребра 11 и кодом 01.

Вторая пара пара принятой комбинации имеет значение 01. Нам необходимо продолжить уже два маршрута. Из узла s_0(t=1) треллиса выходят 2 ребра с весом 11 и 00. Расстояния между ними и принятым значением 01 запишем в соответствующих узлах: 2-для s_0 и 0-для s_2. Из узла s_2 также выходят два ребра с весом 01 и 10. Расстояние между ними и принятым знчением 00 равное 1 записывается в узлы s_1 и s_3 (t=2).

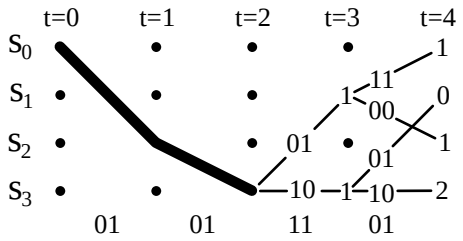


Теперь нам нам необходимо отбросить узлы с максимальным расстоянием, поскольку они соответствуют последовательностям наиболее сильно отличающимся от передаваемой. Поскольку s_3 - узел с минимальным расстоянием =0, то дальнейший маршрут мы будем прокладывать от него.

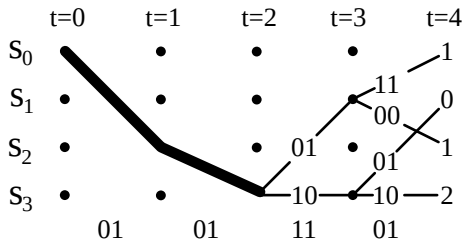


На третьем шаге из узла s_3(t=2) мы должны выбрать ребро с весом 11. Так как ребер с таким весом у нас нет, то мы рассмотрим маршруты по ребрам с весом 01 и 10. Запишем расстояние между 01 и 11 в узел s_1 (t=3). Для нижнего ребра имеем вес 10. Расстояние между 10 и 11 равно 1 - запишем в узел s_3(t=3).

Следующая пара принятой комбинации имеет значение 01. Нам необходимо продолжить уже два маршрута. Из узла s_1(t=3) выходят 2 ребра с весом 11 и 00. Расстояния между ними и принятым значением 01 запишем в соответствующих узлах: 1-для s_0 и s_2. Из узла s_3 также выходят два ребра с весами 01 и 10. Расстояние между ними и принятым значением 01 записывается в узелы s_1 (0) и s_3 (2).

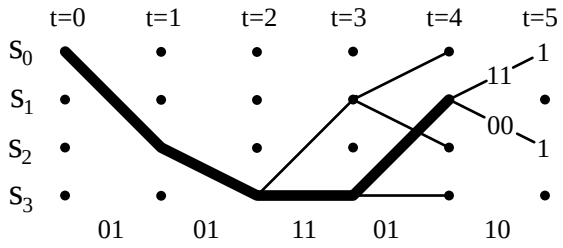


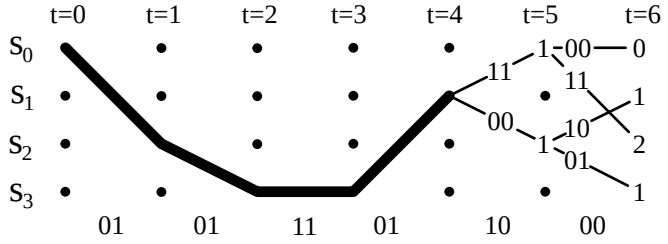
Далее, отбрасываем узлы с максимальным расстоянием поскольку они соответствуют последовательностям наиболее сильно отличающимся от передаваемой. Поскольку s_1 - узел с минимальным расстоянием =0, то дальнейший маршрут мы будем прокладывать от него.

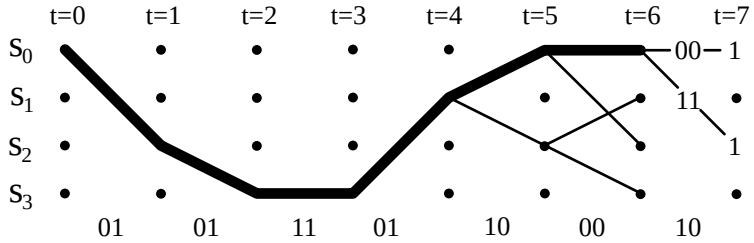


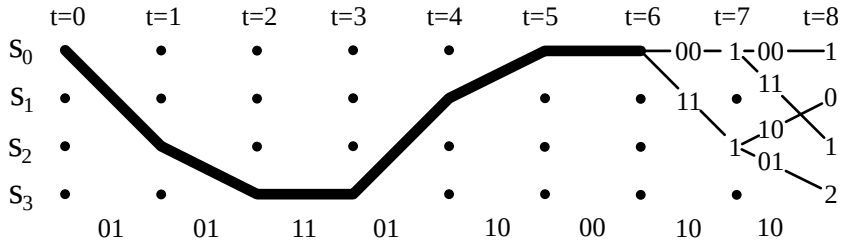
На пятом шаге из узла s_1(t=4) мы должны выбрать ребро с весом 10. Так как ребер с таким весом у нас нет, то мы рассмотрим маршруты по ребрам с весом 11 и 00. Запишем расстояние между 11 и 10 в узел s_0 (t=5). Для нижнего ребра имеем вес 00. Расстояние между 00 и 10 равно 1 - запишем в узел s_3(t=5).

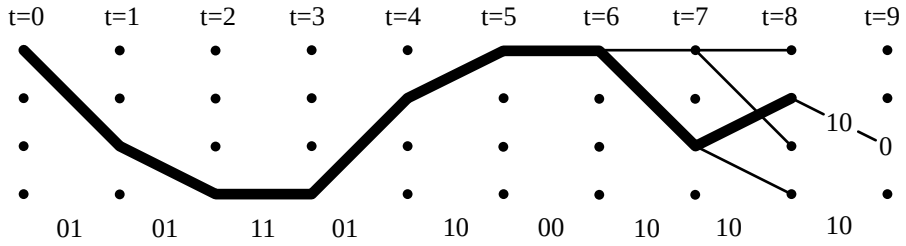
Дальнейший ход расчетов покажем на рисунках.



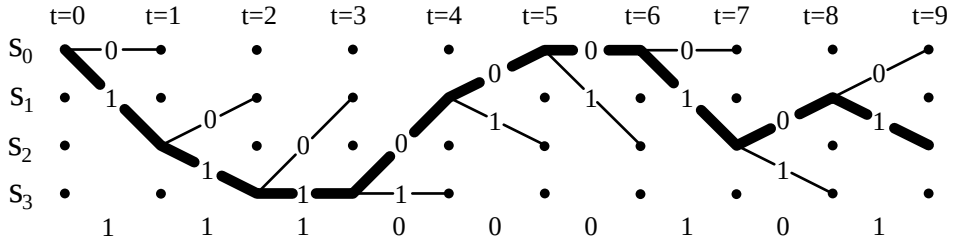








В заключение мы должны определить путь проходящий через узлы с минимальным суммарным растоянием. На каждом шаге, верхнему ребру мы ставим в соответствие значение 0, а нижнему ребру значение 1.



Раскодированная информационная последовательность имеет вид

$$a = (111000101). \qquad \blacktriangle$$

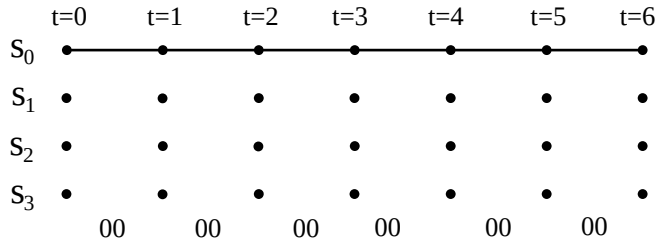
Как видно из последнего примера количество ошибок в последовательности может быть любым, главное, чтобы они отстояли друг от друга не менее чем на 5 символов. Т.е. между двумя искаженными значениями должно стоять не менее 4 неискаженных. Но это означает, что для обнаружения ошибки мы должны рассчитать расстояния по всем узлам за последние 2 шага. Очевидно, что чем плотнее расположены ошибки тем труднее их будет обнаружить и тем большее количество шагов необходимо учитывать для рассчета расстояния. Количество шагов, используемых для рассчета расстояний называется шириной окна декодирования. Рассмотрим пример двух последовательных ошибок.

Пример 3.20. Передаваемое информационное сообщение имеет вид

$$a = (000000).$$

Этому сообщению соответствует следующая кодовая комбинация, построенная по треллису:

$$F = (00, 00, 00, 00, 00, 00).$$

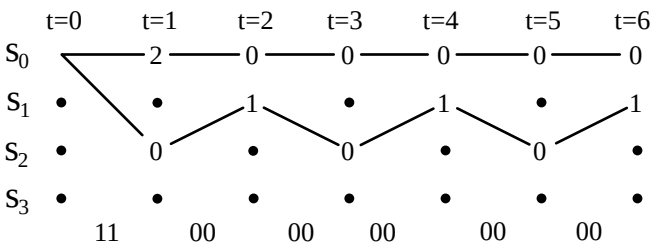


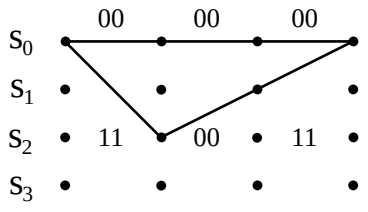
Допустим в передаваемой комбинации возникли последовательно две ошибки

$$F = (\underline{\mathbf{11}}, 00, 00, 00, 00, 00).$$

Необходимо восстановить информационную последовательность.

Решение. Для обнаружения такой ошибки нам необходимо начертить треллис глубиной до шестого уровня включительно. И только на 6 уровне сумма расстояний по верхнему пути (2) превысит расстояние альтернативного маршрута (3). Здесь ширина окна декодирования равна L=6.





Другими словами искажение парной ошибки возможно если после нее идут как минимум 10 неискаженных разрядов. Наряду с этим возможны случаи, когда ошибку вообще невозможно распознать. Например для кода $F = (00, 00, 00)$ совокупность ошибок типа $F = (11, 10, 11)$ приведут к тому, что декодер вместо последовательности $a = (000)$ выдаст сообщение $a = (100)$.

К сожалению, в этом случае даже увеличение ширины окна декодирования не позволяет обнаружить ошибку. Такого рода пакеты ошибок мы будем называть жесткими. Несложно показать что минимальный жесткий пакет ошибок имеет вид **3-1-2**. Т.е. в произвольной кодовой последовательности начиная с некоторого бита появляется подрят 3 ошибочных, затем 1 неискаженный и наконец еще 2 ошибочных (инвертированных). Например жесткими будут следующие пакеты ошибок

★ $11\underline{\mathbf{0101111}}1101 \to 11\underline{\mathbf{1011001}}1101$ $00\underline{\mathbf{1101010}}0 \to 00\underline{\mathbf{0111100}}0$

К счастью все жесткие пакеты ошибок должны начинаться с первого элемента пары, а это в свою очередь также уменьшает вероятность их появления.

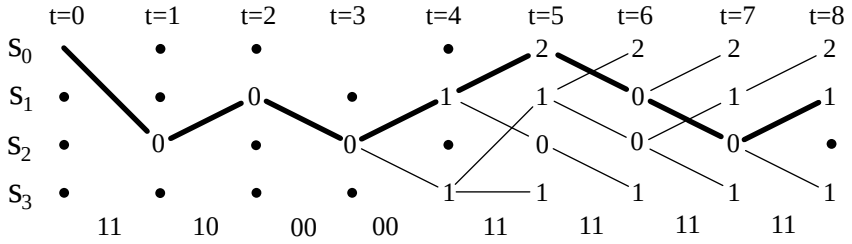
Пример 3.21. Раскодировать сообщение **(ая)** используя ширину окна декодирования $L \leq 2$.

Решение. Сообщению (**ая**) соответствуют значения **(e0,ff)** ASCII таблицы. Переведем его в двоичный вид

$$\textbf{(e0,ff)} = (11100000, 11111111).$$

Таким образом исходное кодовое слово имеет вид $F = (11, 10, 00, 00, 11, 11, 11, 11)$.

Для раскодирования сообщения воспользуемся треллисом



На рисунке показаны несколько альтернативных маршрутов с окном декодирования L=2. Очевидно, что последние 4 пары (11,11,11,11) последовательности обрауют какую-то ошибочную комбинацию. Но для ее исправления у декодера нет дополнительных символов. Поэтому декодер должен либо сообщить о невозможности декодирования, либо предложить некоторую наиболее вероятную комбинацию. В нашем случае, используя жирную линию треллиса получим

$$a = (10100110)_2 = \mathbf{a6}_h = |\ . \qquad \blacktriangle$$

Задача 3.15. Раскодировать сообщение **F** используя ширину окна декодирования $L \leq 2$.

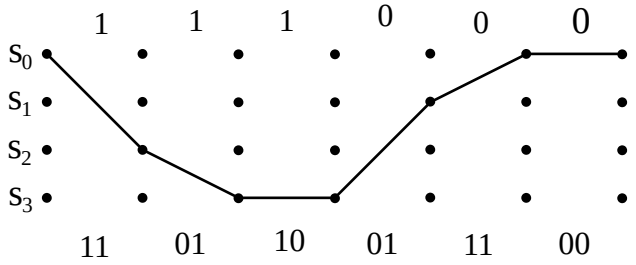
N	F	N	F	N	F
1.	0001010101001110	11.	0010010111001110	20.	0011110111101110
2.	0001101100101110	12.	0010101100011110	22.	0011001100000110
3.	1111011100101110	13.	1100011100011110	23.	1101111100000110
4.	1111100100110100	14.	1100100100000100	24.	1101000100011100
5.	1111100100000010	15.	1100100100110010	25.	1101000100101010
6.	1111011111000010	16.	1100011111110010	26.	1101111111101010
7.	1100001000000010	17.	1111001000110010	27.	1110101000101010
8.	1111010001110001	18.	1100010001000001	28.	1101110001011001
9.	0001101111001100	19.	0010101111111100	29.	0011001111100100
10.	0010111000111010	20.	0001111000001010	30.	0000011000010010

3.4.5 Алгоритм Витерби

Рассмотрим схему передачи и приема сообщения в канале с помехами сверточным кодом. Допустим информационная последовательность имеет вид

$$a = (111000).$$

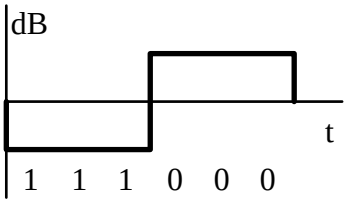
Схема кодирования показана на рисунке.



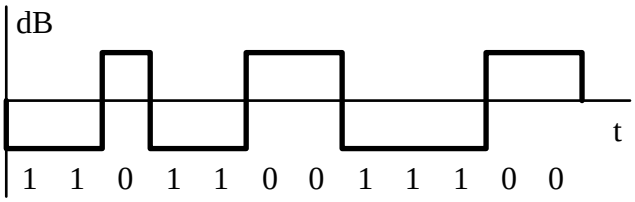
Передаваемая кодовая комбинация имеет вид

$$F = (110110011100).$$

На аппаратном уровне мы можем представить сигнал с положительным напряжением (+) как 0, а сигнал с отрицательным напряжением (-) как 1. Тогда процесс кодирования выглядит следующим образом:

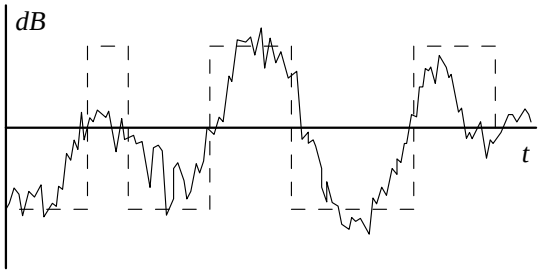


Информационная последовательность.

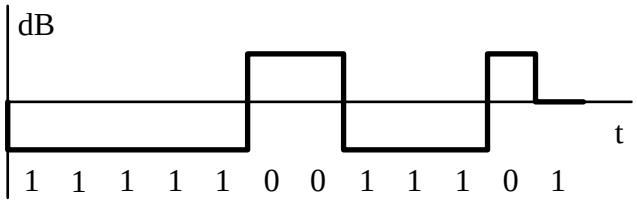


Кодовая последовательность.

В процессе передачи информации последовательность искажается как в следствие различных помех, так и в следствие естественного затухания электромагнитных волн. Принимаемый сигнал может иметь следующий вид:



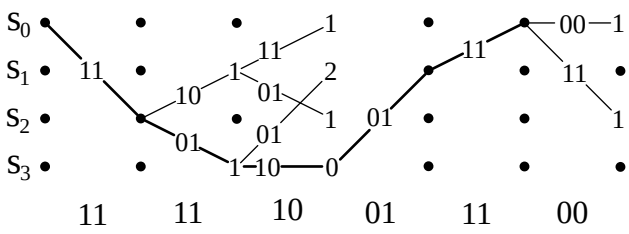
Если приемник фиксирует только знак напряженности электромагнитного поля, то цифровая аппроксимация сигнала будет такой



Другими словами, мы получили кодовую комбинацию в виде

$$F = (11\underline{\mathbf{1}}110011110\underline{\mathbf{1}})$$

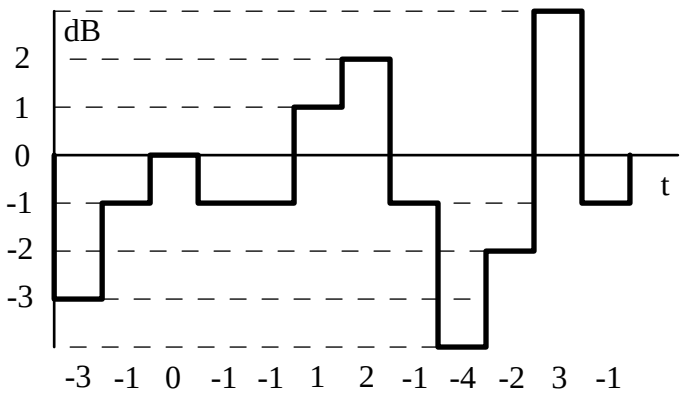
т.е. с двумя ошибками.



Допустим, мы будем придерживаться жесткой схемы декодирования, показанной на треллисе. Тогда декодер сможет исправить одну ошибку в середине последовательности, но не исправит последнюю ошибку, поскольку у него не хватит шагов для увеличения окна декодирования.

С вероятностью $1/2$ декодер может выдать правильный ответ (111000) или (111001), а возможно выдаст сообщение о невозможности декодирования.

Теперь рассмотрим алоритм Витерби мягкого декодирования. Для этого необходимо, чтобы приемник сигнала различал не только знак напряженности, но и амлитуду принимаемого сигнала. Как правило 8 уровневого квантования сигнала бывает достаточно для эффективного применения мягкой схемы декодирования.



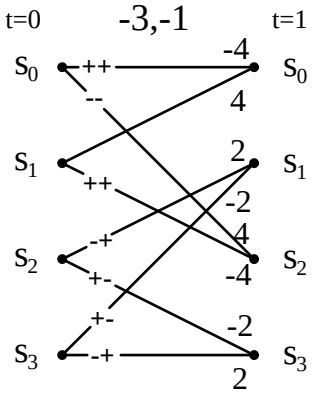
Из рисунка видно, что принятая кодовая комбинация имеет вид

$$F = (-3, -1, 0, -1, -1, 1, 2, -1, -4, -2, 3, -1)$$

Пример 3.22. Декодировать принятую кодовую комбинацию

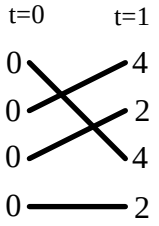
$$F = (-3, -1, 0, -1, -1, 1, 2, -1, -4, -2, 3, -1).$$

Решение. Расмотрим первый шаг декодирования. Для этого на треллисе обозначим вес ребра (00) символом (+1,+1), вес ребра (11) символом (-1,-1), вес (10) - символом (-1,+1), вес (01) - символом (+1,-1). Это означает, что для вычисления метрики очередного узла нам необходимо найти скалярное произведение веса ребра с принятой информационной парой. На первом шаге $t = 1$ принятая информационная пара есть (-3,-1). Тогда, для перехода $s_0 \to s_0$ мы должны найти скалярное произведение $(+1,+1)\cdot(-3,-1) = (+1)\cdot(-3)+(+1)\cdot(-1) = -3-1 = -4$.



Продолжая аналогичным образом, далее получим

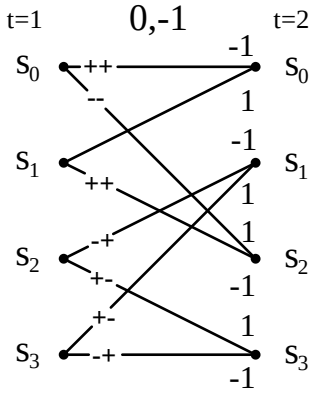
$$\begin{aligned}
s_0 \to s_0 &: \quad (+1,+1)\cdot(-3,-1) = (+1)\cdot(-3)+(+1)\cdot(-1) = -3-1 = -4,\\
s_0 \to s_2 &: \quad (-1,-1)\cdot(-3,-1) = (-1)\cdot(-3)+(-1)\cdot(-1) = +3+1 = +4,\\
s_1 \to s_0 &: \quad (-1,-1)\cdot(-3,-1) = (-1)\cdot(-3)+(-1)\cdot(-1) = +3+1 = +4,\\
s_1 \to s_2 &: \quad (+1,+1)\cdot(-3,-1) = (+1)\cdot(-3)+(+1)\cdot(-1) = -3-1 = -4,\\
s_2 \to s_1 &: \quad (-1,+1)\cdot(-3,-1) = (-1)\cdot(-3)+(+1)\cdot(-1) = +3-1 = +2,\\
s_2 \to s_3 &: \quad (+1,-1)\cdot(-3,-1) = (+1)\cdot(-3)+(-1)\cdot(-1) = -3+1 = -2,\\
s_3 \to s_1 &: \quad (+1,-1)\cdot(-3,-1) = (+1)\cdot(-3)+(-1)\cdot(-1) = -3+1 = -2,\\
s_3 \to s_3 &: \quad (-1,+1)\cdot(-3,-1) = (-1)\cdot(-3)+(+1)\cdot(-1) = +3-2 = +2.
\end{aligned}$$

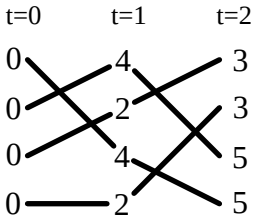


Теперь нам необходимо выбрать те ребра, которые дают максимальные значения метрик узлов. На данном шаге это все положительные значения метрик. Выделим их жирным цветом:

На втором шаге $t = 2$ принятая информационная пара есть (0,-1). Тогда, для переходов $s_i \to s_k$ соответствующие скалярные произведения дают

$$
\begin{aligned}
s_0 \to s_0 \ &: \quad (+1,+1)\cdot(0,-1) = 0+1 = -1,\\
s_0 \to s_2 \ &: \quad (-1,-1)\cdot(0,-1) = 0+1 = +1,\\
s_1 \to s_0 \ &: \quad (-1,-1)\cdot(0,-1) = 0+1 = +1,\\
s_1 \to s_2 \ &: \quad (+1,+1)\cdot(0,-1) = 0-1 = -1,\\
s_2 \to s_1 \ &: \quad (-1,+1)\cdot(0,-1) = 0-1 = -1,\\
s_2 \to s_3 \ &: \quad (+1,-1)\cdot(0,-1) = 0+1 = +1,\\
s_3 \to s_1 \ &: \quad (+1,-1)\cdot(0,-1) = 0+1 = +1,\\
s_3 \to s_3 \ &: \quad (-1,+1)\cdot(0,-1) = 0-1 = -1.
\end{aligned}
$$

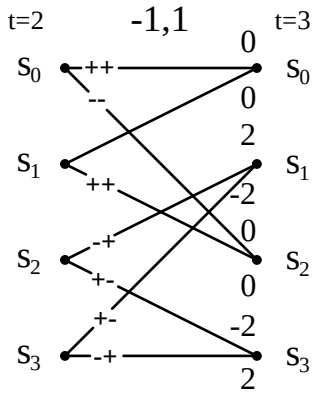


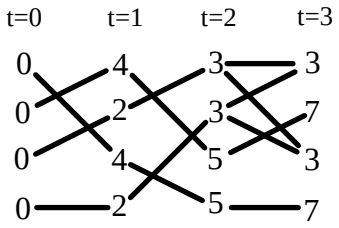


Теперь нам необходимо выбрать те ребра, которые дают максимальные значения суммарных метрик узлов. Выделим их жирным цветом.

На третьем шаге $t = 3$ принятая информационная пара есть (-1,1). Тогда, для переходов $s_i \to s_k$ соответствующие скалярные произведения дают

$$
\begin{aligned}
s_0 \to s_0 \ &: \quad (+1,+1)\cdot(-1,1) = -1+1 = \ \ 0,\\
s_0 \to s_2 \ &: \quad (-1,-1)\cdot(-1,1) = +1-1 = \ \ 0,\\
s_1 \to s_0 \ &: \quad (-1,-1)\cdot(-1,1) = +1-1 = \ \ 0,\\
s_1 \to s_2 \ &: \quad (+1,+1)\cdot(-1,1) = -1+1 = \ \ 0,\\
s_2 \to s_1 \ &: \quad (-1,+1)\cdot(-1,1) = +1+1 = \ \ 2,\\
s_2 \to s_3 \ &: \quad (+1,-1)\cdot(-1,1) = -1-1 = -2,\\
s_3 \to s_1 \ &: \quad (+1,-1)\cdot(-1,1) = -1-1 = -2,\\
s_3 \to s_3 \ &: \quad (-1,+1)\cdot(-1,1) = +1+1 = \ \ 2.
\end{aligned}
$$

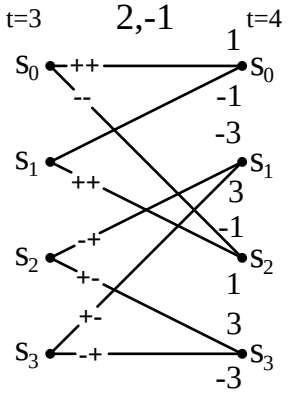




Складывая веса полученных узлов с предыдущими значениями нам необходимо выбрать те ребра, которые дают максимальные значения суммарных метрик узлов. Выделим их жирным цветом. Продолжая аналогичным образом, получим следующую последовательность действий.

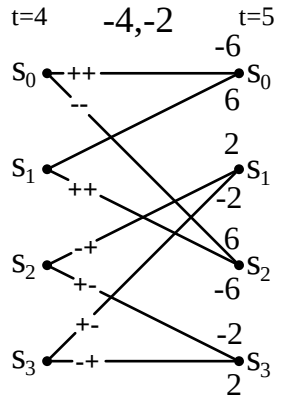
На четвертом шаге $t = 4$ принятая информационная пара есть (2,-1).

$$
\begin{aligned}
s_0 \to s_0 \ &: \quad (+1,+1)\cdot(2,-1) = +2-1 = +1,\\
s_0 \to s_2 \ &: \quad (-1,-1)\cdot(2,-1) = -2+1 = -1,\\
s_1 \to s_0 \ &: \quad (-1,-1)\cdot(2,-1) = -2+1 = -1,\\
s_1 \to s_2 \ &: \quad (+1,+1)\cdot(2,-1) = +2-1 = +1,\\
s_2 \to s_1 \ &: \quad (-1,+1)\cdot(2,-1) = -2-1 = -3,\\
s_2 \to s_3 \ &: \quad (+1,-1)\cdot(2,-1) = +2+1 = +3,\\
s_3 \to s_1 \ &: \quad (+1,-1)\cdot(2,-1) = +2+1 = +3,\\
s_3 \to s_3 \ &: \quad (-1,+1)\cdot(2,-1) = -2-1 = -3.
\end{aligned}
$$



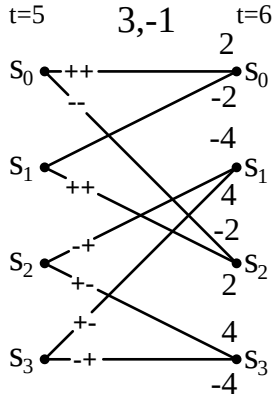
На пятом шаге $t = 5$ принятая информационная пара есть (-4,-2).

$$
\begin{aligned}
s_0 \to s_0 \ &: \quad (+1,+1)\cdot(-4,-2) = -4-2 = -6,\\
s_0 \to s_2 \ &: \quad (-1,-1)\cdot(-4,-2) = +4+2 = +6,\\
s_1 \to s_0 \ &: \quad (-1,-1)\cdot(-4,-2) = +4+2 = +6,\\
s_1 \to s_2 \ &: \quad (+1,+1)\cdot(-4,-2) = -4-2 = -6,\\
s_2 \to s_1 \ &: \quad (-1,+1)\cdot(-4,-2) = +4-2 = +2,\\
s_2 \to s_3 \ &: \quad (+1,-1)\cdot(-4,-2) = -4+2 = -2,\\
s_3 \to s_1 \ &: \quad (+1,-1)\cdot(-4,-2) = -4+2 = -2,\\
s_3 \to s_3 \ &: \quad (-1,+1)\cdot(-4,-2) = +4-2 = +2.
\end{aligned}
$$

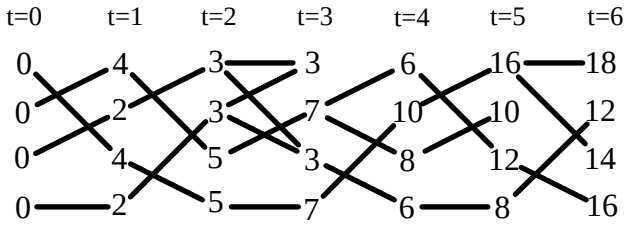


На шестом шаге $t = 6$ принятая информационная пара есть (3,-1).

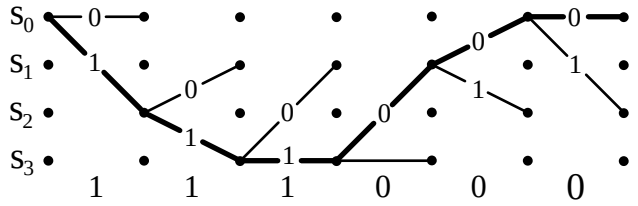
$$
\begin{aligned}
s_0 \to s_0 \ &: \quad (+1,+1)\cdot(3,-1) = +3-1 = +2,\\
s_0 \to s_2 \ &: \quad (-1,-1)\cdot(3,-1) = -3+1 = -2,\\
s_1 \to s_0 \ &: \quad (-1,-1)\cdot(3,-1) = -3+1 = -2,\\
s_1 \to s_2 \ &: \quad (+1,+1)\cdot(3,-1) = +3-1 = +2,\\
s_2 \to s_1 \ &: \quad (-1,+1)\cdot(3,-1) = -3-1 = -4,\\
s_2 \to s_3 \ &: \quad (+1,-1)\cdot(3,-1) = +3+1 = +4,\\
s_3 \to s_1 \ &: \quad (+1,-1)\cdot(3,-1) = +3+1 = +4,\\
s_3 \to s_3 \ &: \quad (-1,+1)\cdot(3,-1) = -3-1 = -4.
\end{aligned}
$$



В результате треллис будет выглядеть следующим образом.

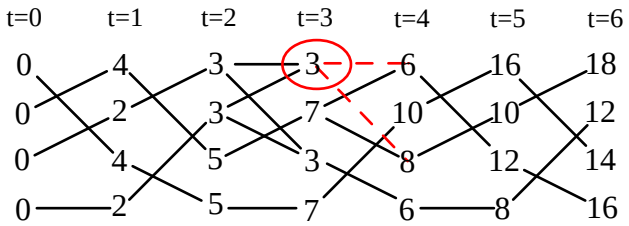


На последнем шаге $t = 6$ мы выбираем узел с максимальным весом 18 и выделяем единственный путь, по которому к нему можно прийти из $t = 0$. Как и в жесткой схеме, обозначая верхнее ребро через 0, а нижнее через 1 декодируем принятую комбинацию:



Мы получили информационную последовательность $a = (111000)$. ▲

Вопрос. Прежде чем решать следующую задачу, разберитесь почему на 4 шаге верхний путь (**веса 3**) имеет обрыв?



Задача 3.16. Декодировать сообщение F с помощью мягкого алгоритма Витерби.

N	F
1	$-4,-5,-1,1,3,0,3,2,4,0,-8,-9,-1,3,-1,0$
2	$-5,4,0,3,-2,-4,1,2,3,1,8,9,3,-2,2,0$
3	$6,-7,2,-1,4,-2,-2,4,3,1,8,-7,1,-3,-3,-9$
4	$8,7,-2,3,4,-4,3,4,2,-1,6,7,2,0,-4,-9$
5	$9,-8,2,3,4,-4,-4,-4,-4,2,-6,5,-1,2,5,-8$
6	$7,-8,3,2,-2,2,-2,2,-3,-3,6,-5,2,1,6,-8$
7	$7,6,3,0,3,-1,1,0,-4,-3,-6,-7,3,0,-7,7$
8	$-6,-7,-1,-3,2,-2,4,3,0,-2,-8,-7,1,-2,-8,7$
9	$8,-7,-3,-1,-3,1,-3,-3,-3,1,-8,9,-1,3,-9,6$
10	$-8,9,2,-3,-3,1,-4,1,-3,4,8,-9,2,0,-8,6$
11	$8,9,-3,-2,2,-3,-2,-4,-4,-4,8,-7,-3,1,7,-5$
12	$8,7,-2,-3,4,-4,4,3,2,4,6,7,0,-3,6,-5$
13	$-6,-7,3,0,2,-2,-1,-2,4,-2,6,-5,3,-2,5,-4$
14	$6,-7,1,3,3,4,3,-3,4,-2,6,-5,2,1,4,-3$
15	$-8,7,1,3,1,0,4,-3,3,1,-6,-7,2,1,-3,2$
16	$8,-9,2,-3,2,4,-3,3,-1,4,-6,7,3,2,-2,2$
17	$8,-9,2,-3,1,-4,-3,4,-3,4,6,7,0,3,-1,1$
18	$-8,-7,3,-2,4,-2,-1,1,2,3,8,-7,-3,-2,1,1$
19	$-6,-7,3,2,4,1,-1,0,4,2,-8,-9,-3,-2,-2,-2$
20	$6,5,0,1,-1,4,-1,-2,3,-3,8,9,3,2,3,-2$
21	$4,5,-1,-2,0,3,-2,-2,3,4,8,-7,-1,-2,-4,-3$
22	$-5,-6,1,2,2,3,-3,-1,-2,0,-6,-7,-3,-3,5,-3$
23	$7,6,0,3,3,-2,-3,4,0,4,6,5,-3,2,-6,4$
24	$-7,8,2,1,-3,-3,0,1,0,-4,-6,5,-2,3,7,4$
25	$-9,8,-3,3,0,-4,-1,-2,2,-1,-6,-7,-1,3,-8,5$
26	$-9,8,-1,-3,0,4,-4,-1,2,-1,8,-7,3,1,9,5$
27	$7,-8,2,1,-4,-3,3,2,-4,1,-8,-9,3,-1,-0,-6$
28	$7,-6,2,-3,-2,3,1,-3,-2,0,8,-9,2,3,-9,-6$
29	$8,7,3,0,-3,4,3,0,-1,-3,-8,-7,-2,-1,8,-7$
30	$-8,-9,-2,3,-4,-1,0,1,-1,-1,-6,7,-3,0,7,-7$

3.5 Турбокоды

Турбокоды были введены в практику в 1993 г. и по существу являются комбинацией двух сверточных кодов. Они обеспечивают значения достоверности очень близкое к пределу Шеннона.

Турбокоды в настоящее время приняты в качестве стандарта для систем связи телекоммуникаций третьего поколения 3GPP, стандарта сотовой связи CDMA-2000, цифрового телевидения DVB, используются в системах спутниковой связи VSAT и во многих др. стандартах.

Как и в случае мягкого декодирования Витерби, логические элементы 0 и 1 мы будем представлять электрическим напряжением (-1) и (+1). Проверочные символы для информационной последовательности $a = (x_1, x_2, x_3, x_4)$ строятся следующим образом. Представим последовательность x_k в виде матрицы

$$L = \begin{pmatrix} L_1 & L_2 \\ L_3 & L_4 \end{pmatrix} = \begin{matrix} \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \begin{pmatrix} x_{12} \\ x_{34} \end{pmatrix}, \\ \begin{pmatrix} x_{13} & x_{24} \end{pmatrix} \end{matrix}$$

где горизонтальные и вертикальные проверочные символы строятся следующим образом

$$\begin{pmatrix} x_{12} \\ x_{34} \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \\ x_3 \oplus x_4 \end{pmatrix}, \qquad \begin{pmatrix} x_{13} \\ x_{24} \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \oplus x_4 \end{pmatrix}.$$

Передаваемая кодовая комбинация имеет вид

$$F = (x_1, x_2, x_3, x_4, x_{12}, x_{34}, x_{13}, x_{24}).$$

Итерационный метод декодирования заключается в следующем.

1. На первом шаге мы вычисляем горизонтальную невязку проверочных символов

$$H = \begin{pmatrix} H_1 & H_2 \\ H_3 & H_4 \end{pmatrix} = \begin{pmatrix} x_2 \boxplus x_{12} & x_1 \boxplus x_{12} \\ x_4 \boxplus x_{34} & x_3 \boxplus x_{34} \end{pmatrix}.$$

Здесь новая операция $\boxplus$ определяется следующим образом

$$A \boxplus B = (-) \cdot \mathrm{sign}(A) \cdot \mathrm{sign}(B) \cdot \min(|A|, |B|).$$

2. На втором шаге вычисляются вертикальные невязки проверочных символов

$$V = \begin{pmatrix} V_1 & V_2 \\ V_3 & V_4 \end{pmatrix} = \begin{pmatrix} (L_3 + H_3) \boxplus x_{13} & (L_4 + H_4) \boxplus x_{24} \\ (L_1 + H_1) \boxplus x_{13} & (L_2 + H_2) \boxplus x_{24} \end{pmatrix}.$$

Результатом первой итерации является матрица

$$X^1 = L + H + V.$$

3. На третьем шаге мы опять вычисляем горизонтальную невязку проверочных символов

$$H = \begin{pmatrix} (L_2 + V_2) \boxplus x_{12} & (L_1 + V_1) \boxplus x_{12} \\ (L_4 + V_4) \boxplus x_{34} & (L_3 + V_3) \boxplus x_{34} \end{pmatrix}.$$

Заметим, что элементы матрицы V мы берем с предыдущего **2** шага.

4. На четвертом шаге вычисляются вертикальные невязки проверочных символов

$$V = \begin{pmatrix} V_1 & V_2 \\ V_3 & V_4 \end{pmatrix} = \begin{pmatrix} (L_3 + H_3) \boxplus x_{13} & (L_4 + H_4) \boxplus x_{24} \\ (L_1 + H_1) \boxplus x_{13} & (L_2 + H_2) \boxplus x_{24} \end{pmatrix}.$$

Заметим, что элементы матрицы H мы берем с предыдущего **3** шага. Результатом второй итерации является матрица

$$X^2 = L + H + V.$$

Как и во всех итеррационных алгоритмах нам периодически требуется проверить насколько сильно изменяются результаты вычислений при последующих итерациях. Если $X^k \approx X^{k-1}$ то процесс вычисления можно прекращать, обозначив $X = X^k$. Если же значения X^k сильно отличаются от X^{k-1}, то необходимо повторять шаги **3-4**. На заключительном этапе нам необходимо перейти от мягкого решения к жесткому ответу. Для этого всем отрицательным компонентам матрицы

$$X = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}$$

ставятся в соответсвие значения принимаемого сигнала 0, а всем положительным - значение 1:

$$a = 1/2 + 1/2\mathrm{sign}(x) \quad \text{или} \quad a = \frac{1}{2} \begin{pmatrix} 1 + \mathrm{sign}(X_1) & 1 + \mathrm{sign}(X_2) \\ 1 + \mathrm{sign}(X_3) & 1 + \mathrm{sign}(X_4) \end{pmatrix}.$$

Пример 3.23. Закодируем сообщение $a = (1011)$.

Решение. Учитывая, что $a = (x_1, x_2, x_3, x_4) = (1011)$ представим последовательность x_k в виде матрицы

$$L = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

тогда горизонтальные и вертикальные проверочные символы строятся следующим образом

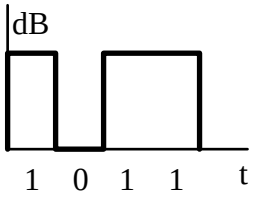
$$\begin{pmatrix} x_{12} \\ x_{34} \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \\ x_3 \oplus x_4 \end{pmatrix} = \begin{pmatrix} 1 \oplus 0 \\ 1 \oplus 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} x_{13} \\ x_{24} \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \oplus x_4 \end{pmatrix} = \begin{pmatrix} 1 \oplus 1 \\ 0 \oplus 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

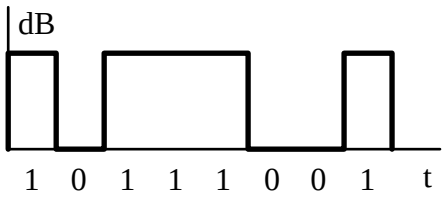
Передаваемая кодовая комбинация имеет вид

$$F = (x_1, x_2, x_3, x_4, x_{12}, x_{34}, x_{13}, x_{24}) = (10111001). \quad \blacktriangle$$

Процесс кодирования изобразим следующим образом:

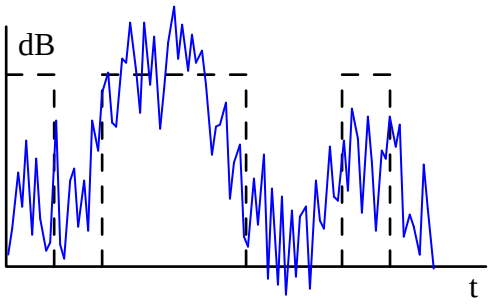


Информационная последовательность.

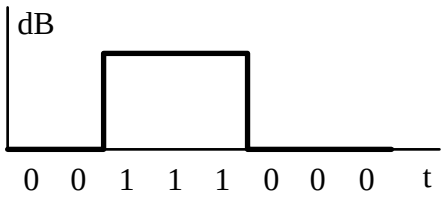


Кодовая последовательность.

В процессе передачи информации последовательность искажается как в следствие различных помех, так и в следствие естественного затухания электромагнитных волн. Принимаемый сигнал может иметь следующий вид:



Если приемник фиксирует только знак напряженности электромагнитного поля, то цифровая аппроксимация сигнала будет такой.

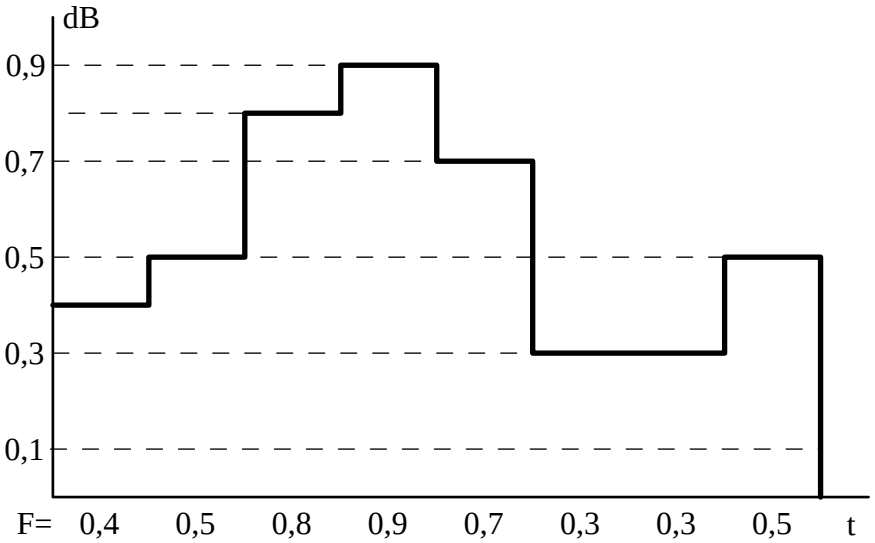


Другими словами, мы получили кодовую комбинацию в виде

$$F = (\underline{\mathbf{0}}011100\underline{\mathbf{0}})$$

т.е. с двумя ошибками.

Теперь рассмотрим алоритм мягкого декодирования. Для этого введем 10 уровневое квантование сигнала и запишем его в виде



Из рисунка видно, что принятая кодовая комбинация теперь имеет вид

$$F = (0.4, 0.5, 0.8, 0.9, 0.7, 0.3, 0.3, 0.5).$$

Пример 3.24. Декодировать принятую кодовую комбинацию

$$F = (0.4, 0.5, 0.8, 0.9, 0.7, 0.3, 0.3, 0.5).$$

Решение. Выделим из принятой информационной последовательности

$$F = (x_1, x_2, x_3, x_4, x_{12}, x_{34}, x_{13}, x_{24}) = (0.4, 0.5, 0.8, 0.9, 0.7, 0.3, 0.3, 0.5)$$

информационную матрицу

$$L = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} = \begin{pmatrix} 0.4 & 0.5 \\ 0.8 & 0.9 \end{pmatrix},$$

горизотнальные (x_{12}, x_{34}) и вертикальные (x_{13}, x_{24}) проверочные символы

$$\begin{pmatrix} x_{12} \\ x_{34} \end{pmatrix} = \begin{pmatrix} 0.7 \\ 0.3 \end{pmatrix}, \qquad \begin{pmatrix} x_{13} \\ x_{24} \end{pmatrix} = \begin{pmatrix} 0.3 \\ 0.5 \end{pmatrix}.$$

1. На первом шаге мы вычисляем горизонтальную невязку проверочных символов

$$H = \begin{pmatrix} x_2 \boxplus x_{12} & x_1 \boxplus x_{12} \\ x_4 \boxplus x_{34} & x_3 \boxplus x_{34} \end{pmatrix} = \begin{pmatrix} 0.5 \boxplus 0.7 & 0.4 \boxplus 0.7 \\ 0.9 \boxplus 0.3 & 0.8 \boxplus 0.3 \end{pmatrix}.$$

Учитывая, что

$$A \boxplus B = (-1) \cdot \operatorname{sign}(A) \cdot \operatorname{sign}(B) \cdot \min(|A|, |B|)$$

получим

$$x_2 \boxplus x_{12} = 0.5 \boxplus 0.7 = (-1) \cdot \operatorname{sign}(0.5) \cdot \operatorname{sign}(0.7) \cdot \min(|0.5|, |0.7|) = -0.5,$$
$$x_1 \boxplus x_{12} = 0.4 \boxplus 0.7 = (-1) \cdot \operatorname{sign}(0.4) \cdot \operatorname{sign}(0.7) \cdot \min(|0.4|, |0.7|) = -0.4,$$
$$x_4 \boxplus x_{34} = 0.9 \boxplus 0.3 = (-1) \cdot \operatorname{sign}(0.9) \cdot \operatorname{sign}(0.3) \cdot \min(|0.9|, |0.3|) = -0.3,$$
$$x_3 \boxplus x_{34} = 0.8 \boxplus 0.3 = (-1) \cdot \operatorname{sign}(0.8) \cdot \operatorname{sign}(0.3) \cdot \min(|0.8|, |0.3|) = -0.3,$$

и

$$H = \begin{pmatrix} H_1 & H_2 \\ H_3 & H_4 \end{pmatrix} = \begin{pmatrix} -0.5 & -0.4 \\ -0.3 & -0.3 \end{pmatrix}.$$

2. На втором шаге вычисляем вертикальную невязку проверочных символов

$$V = \begin{pmatrix} (L_3 + H_3) \boxplus x_{13} & (L_4 + H_4) \boxplus x_{24} \\ (L_1 + H_1) \boxplus x_{13} & (L_2 + H_2) \boxplus x_{24} \end{pmatrix} = \begin{pmatrix} (0.8 - 0.3) \boxplus 0.3 & (0.9 - 0.3) \boxplus 0.5 \\ (0.4 - 0.5) \boxplus 0.3 & (0.5 - 0.4) \boxplus 0.5 \end{pmatrix}.$$

или

$$V = \begin{pmatrix} V_1 & V_2 \\ V_3 & V_4 \end{pmatrix} = \begin{pmatrix} -0.3 & -0.5 \\ 0.1 & -0.1 \end{pmatrix}.$$

Результатом первой итерации является матрица

$$X_1 = L + H + V = \begin{pmatrix} 0.4 & 0.5 \\ 0.8 & 0.9 \end{pmatrix} + \begin{pmatrix} -0.5 & -0.4 \\ -0.3 & -0.3 \end{pmatrix} + \begin{pmatrix} -0.3 & -0.5 \\ 0.1 & -0.1 \end{pmatrix} = \begin{pmatrix} -0.4 & -0.4 \\ 0.6 & 0.5 \end{pmatrix}.$$

3. На третьем шаге мы опять вычисляем горизонтальную невязку проверочных символов

$$H = \begin{pmatrix} (L_2 + V_2) \boxplus x_{12} & (L_1 + V_1) \boxplus x_{12} \\ (L_4 + V_4) \boxplus x_{34} & (L_3 + V_3) \boxplus x_{34} \end{pmatrix} = \begin{pmatrix} (0.5 - 0.5) \boxplus 0.7 & (0.4 - 0.3) \boxplus 0.7 \\ (0.9 - 0.1) \boxplus 0.3 & (0.8 + 0.1) \boxplus 0.3 \end{pmatrix}.$$

Заметим, что элементы матрицы V мы берем с предыдущего **2** шага. В результате получаем

$$H = \begin{pmatrix} 0 \boxplus 0.7 & 0.1 \boxplus 0.7 \\ 0.8 \boxplus 0.3 & 0.9 \boxplus 0.3 \end{pmatrix} = \begin{pmatrix} 0 & -0.1 \\ -0.3 & -0.3 \end{pmatrix}.$$

4. На четвертом шаге вычисляем вертикальную невязку проверочных символов

$$V = \begin{pmatrix} V_1 & V_2 \\ V_3 & V_4 \end{pmatrix} = \begin{pmatrix} (L_3 + H_3) \boxplus x_{13} & (L_4 + H_4) \boxplus x_{24} \\ (L_1 + H_1) \boxplus x_{13} & (L_2 + H_2) \boxplus x_{24} \end{pmatrix}.$$

Подставляя сюда элементы матрицы H с предыдущего **3** шага, получим

$$V = \begin{pmatrix} (0.8 - 0.3) \boxplus 0.3 & (0.9 - 0.3) \boxplus 0.5 \\ (0.4 + 0) \boxplus 0.3 & (0.5 - 0.1) \boxplus 0.5 \end{pmatrix} = \begin{pmatrix} 0.5 \boxplus 0.3 & 0.6 \boxplus 0.5 \\ 0.4 \boxplus 0.3 & 0.4 \boxplus 0.5 \end{pmatrix},$$

или

$$V = \begin{pmatrix} -0.3 & -0.5 \\ -0.3 & -0.4 \end{pmatrix}$$

Результатом второй итерации является матрица

$$X_2 = L+H+V = \begin{pmatrix} 0.4 & 0.5 \\ 0.8 & 0.9 \end{pmatrix} + \begin{pmatrix} 0 & -0.1 \\ -0.3 & -0.3 \end{pmatrix} + \begin{pmatrix} -0.3 & -0.5 \\ -0.3 & -0.4 \end{pmatrix} = \begin{pmatrix} 0.1 & -0.1 \\ 0.2 & 0.2 \end{pmatrix}.$$

Читатель может смостоятельно проверить, что 5 и 6 шаг вычислений дает

$$H = \begin{pmatrix} 0 & -0.1 \\ -0.3 & -0.3 \end{pmatrix}, \quad V = \begin{pmatrix} -0.3 & -0.5 \\ -0.3 & -0.4 \end{pmatrix}, \quad X_3 = \begin{pmatrix} 0.1 & -0.1 \\ 0.2 & 0.2 \end{pmatrix}.$$

Поскольку $X = X^2 = X^3$, то дальнейшие итерации мы прекращаем.

На заключительном этапе нам необходимо перейти от мягкого решения к жесткому ответу. Для этого всем отрицательным компонентам матрицы X ставятся в соответсвие значения принимаемого сигнала 0, а всем положительным - значение 1:

$$a = \frac{1}{2}\begin{pmatrix} 1+\mathrm{sign}(X_1) & 1+\mathrm{sign}(X_2) \\ 1+\mathrm{sign}(X_3) & 1+\mathrm{sign}(X_4) \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+\mathrm{sign}(0.1) & 1+\mathrm{sign}(-0.1) \\ 1+\mathrm{sign}(0.2) & 1+\mathrm{sign}(0.2) \end{pmatrix}$$

или

$$a = \frac{1}{2}\begin{pmatrix} 1+1 & 1-1 \\ 1+1 & 1+1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Таким образом, декодированная информационная последовательность имеет вид

$$a = (1011). \quad \blacktriangle$$

Задача 3.17. Декодировать принятые сигналы F, сформированные турбокодом.

N	F	N	F
1	0.9, 0.1, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8	16	0.8, 0.1, 0.6, 0.8, 0.3, 0.8, 0.6, 0.7
2	0.9, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8	17	0.8, 0.2, 0.6, 0.8, 0.3, 0.8, 0.6, 0.7
3	0.9, 0.3, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8	18	0.8, 0.3, 0.6, 0.8, 0.3, 0.8, 0.6, 0.7
4	0.9, 0.4, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8	19	0.8, 0.4, 0.6, 0.8, 0.3, 0.8, 0.6, 0.7
5	0.9, 0.5, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8	20	0.8, 0.5, 0.6, 0.8, 0.3, 0.8, 0.6, 0.7
6	0.9, 0.6, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8	21	0.8, 0.6, 0.6, 0.8, 0.3, 0.8, 0.6, 0.7
7	0.9, 0.7, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8	22	0.8, 0.7, 0.6, 0.8, 0.3, 0.8, 0.6, 0.7
8	0.9, 0.1, 0.1, 0.4, 0.5, 0.6, 0.7, 0.8	23	0.8, 0.8, 0.6, 0.8, 0.3, 0.8, 0.6, 0.7
9	0.8, 0.1, 0.7, 0.8, 0.2, 0.7, 0.7, 0.6	24	0.8, 0.9, 0.6, 0.8, 0.3, 0.8, 0.6, 0.7
10	0.8, 0.2, 0.7, 0.8, 0.2, 0.7, 0.7, 0.6	25	0.8, 0.9, 0.5, 0.8, 0.4, 0.9, 0.5, 0.6
11	0.8, 0.3, 0.7, 0.8, 0.2, 0.7, 0.7, 0.6	26	0.8, 0.9, 0.4, 0.8, 0.4, 0.9, 0.5, 0.6
12	0.8, 0.4, 0.7, 0.8, 0.2, 0.7, 0.7, 0.6	27	0.8, 0.9, 0.3, 0.8, 0.4, 0.9, 0.5, 0.6
13	0.8, 0.5, 0.7, 0.8, 0.2, 0.7, 0.7, 0.6	28	0.8, 0.9, 0.2, 0.8, 0.4, 0.9, 0.5, 0.6
14	0.8, 0.6, 0.7, 0.8, 0.2, 0.7, 0.7, 0.6	29	0.8, 0.9, 0.1, 0.8, 0.4, 0.9, 0.5, 0.6
15	0.8, 0.7, 0.7, 0.8, 0.2, 0.7, 0.7, 0.6	30	0.7, 0.8, 0.4, 0.8, 0.4, 0.7, 0.5, 0.7

3.6 Вычисления в полях Галуа

Группой G называется множество элементов $(a_1, a_2, ..., a_n) \in G$ (с заданной ассоциативной бинарной операцией " $\circ$ "[4], для которых выполняются следующие условия:

1. $a \circ e = a$ - существование некоторого единичного элемента $e \in G$;

2. $a \circ \overline{a} = e$ - существование обратного элемента $\overline{a} \in G$ для любого элемента группы $a \in G$.

Количество элементов в группе называется порядком группы.

Множество целых чисел $(..., -3, -2, -1, 0, 1, 2, 3, ...) \in \mathbb{Z}$ относительно бинарной операции "$+$" (арифметическое сложение) образует группу, поскольку в нем элемент $e = 0$ играет роль единичного (т.е. $a + e = a + 0 = a$) и для любого числа $a \in \mathbb{Z}$ можно найти такое $b \in \mathbb{Z}$, что их сумма даст $e = 0$. Например для $a = 4$, обратным будет $b = -4$, тогда $a + b = 4 + (-4) = 0 = e$. Описанное множество далее будет называться аддитивной группой.

Множество тех же целых чисел $(..., -3, -2, -1, 0, 1, 2, 3, ...) \in \mathbb{Z}$ относительно бинарной операции "$\cdot$" (умножение) не образует группу, поскольку в нем нельзя найти обратного элемента для произволного $a \in \mathbb{Z}$. Очевидно, что роль единичного элемента здесь будет играть собственно единица $e = 1$ (т.е. $a \cdot e = a \cdot 1 = a$), но для нахождения обратного элемента необходимо для произвольного a найти такое b, чтобы выполнялось равенство $a \cdot b = e$. Например, для $a = 5$ мы должны написать $b = \frac{1}{5} = 0.2$ и тогда $5 \cdot 0.2 = 1$. Но $b = \frac{1}{5} = 0.2 \notin \mathbb{Z}$ т.е. обратное число не является целым и не принадлежит множеству $\mathbb{Z}$. Такое множество элементов называется полугруппой (мультипликативной полугруппой).

Для читателя, впервые сталкивающегося с теорией конечных групп естественно возникает вопрос: а что делать если сумма двух элементов группы будет больше максимального элемента группы?

Пример 3.25. Классические стрелочные часы имеют на циферблате значения

$$(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12).$$

Если занятия начались в 11 часов и будут длится 2 часа, то во сколько они закончатся? Обычно ответ вычисляется следующим образом

$$11 + 2 = 13,$$

но числа 13 часах не нарисовано. Тогда мы вычитаем

$$13 - 12 = 1$$

и говорим, что занятия закончились в 1 час.

[4]Ассоциативность означает, что нам безразлично в каком порядке проводить вычисления: $(a_1 \circ a_2) \circ a_3 = a_1 \circ (a_2 \circ a_3) = a_1 \circ a_2 \circ a_3$.

Пример 3.26. Если мы легли спать в 10 часов и проспали 9 часов, то во сколько мы проснулись? Вычисляя

$$10 + 9 = 19 \equiv 19 - 12 = 7$$

мы говорим, что проснулись в 7 часов.

Для того, чтобы обозначить, что для нас $19 \equiv 7$ мы использовали другой знак равенства " $\equiv$ ".

Пример 3.27. Поезд № 001М Владивосток-Москва отправляется каждый день в 04:00 (по Московскому времени). Время в пути 6 дней 2 часа. Во сколько поезд прибудет в Москву на Ярославский вокзал? Вычисляя, получим

$$04 + 6 \cdot 24 + 2 = 150.$$

Теперь, разделим 150 на 12 и найдем остаток

$$\frac{150}{12} = 12 + \frac{6}{12}$$

или

$$150 = 12 \cdot 12 + 6.$$

Т.е. поезд прибудет в Москву в 6 часов. (Мы пока не обсуждаем вопрос: утром или вечером?) Т.е. для определения данного времени нам понадобилось вычислить остаток от деления 150 на 12. Этот остаток и является ответом. Математически, данный факт записывается так

$$150 \equiv 6 \pmod{12}.$$

Теперь, решения предыдущего примера записываются в виде:

$$11 + 2 = 13 \equiv 1 \pmod{12}, \qquad 10 + 9 = 19 \equiv 7 \pmod{12}.$$

Кольцом называется множество элементов, с двумя бинарными операциями ("+"и " $\times$ "), которое является аддитивной группой, но мультипликативной полугруппой. Рассмотрим множество из трех целых чисел (0,1,2) и составим для него таблицу сложения и таблицу умножения по модулю 3:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Данное множество образует кольцо и обозначается как $\mathbb{Z}_3$.

Для кольца $\mathbb{Z}_4$ таблицы сложения и умножения по (mod 4) выглядят следующим образом

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Заметим, что для элемента 2 не существует мультипликативного обратного. Т.е. в таблице умножения нет такого числа x которое дало бы $2 \cdot x = 1$.

Для кольца $\mathbb{Z}_5$ таблицы сложения и умножения по (mod 5) выглядят следующим образом

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Из таблицы умножения для $\mathbb{Z}_5$ можно видеть что для каждого ненулевого элемента существует обратный:

$$1 \cdot 1 = 1, \quad 2 \cdot 3 = 1, \quad 3 \cdot 2 = 1, \quad 4 \cdot 4 = 1.$$

Т.е. для 2 обратным элементом будет 3, для 3 - это 2, для 1 - это 1, а для 4 - это 4. Получается что в кольце $\mathbb{Z}_5$ элементы (0,1,2,3,4) образуют группу как по сложению так и по умножению.

Полем называется множество элементов, с двумя бинарными операциями ("+"и "$\times$"), которое является группой как по сложению, так и по умножению (т.е. аддитивной и мультипликативной группой одновременно).

Несложно проверить что все кольца $\mathbb{Z}_p$, для которых p является простым числом являются конечными полями.

Для составления таблиц умножения в конечных полях и проведения в них арифметических операций часто пользуются таблицами индексов. Таблица индексов для $\mathbb{Z}_7$ строиться следующим образом. Возьмем произвольное число (например 2) и будем искать остатки при делении его степени 2^n на 7:

$$2^0 \equiv 1 \pmod 7, \quad 2^1 \equiv 2 \pmod 7, \quad 2^2 \equiv 4 \pmod 7, \quad 2^3 = 8 \equiv 1 \pmod 7 ....$$

Сведем ответы в таблицу

n	0	1	2	3	4	5	6
2^n	1	2	4	1	2	4	1

Из таблиц видно, что значения остатков

$$2^n (\text{mod } 7) = (1, 2, 4)$$

не принимают всех чисел кольца (1,2,3,4,5,6), т.е. **2** не является генератором $\mathbb{Z}_7$. Теперь возьмем в качестве основания число 3:

n	0	1	2	3	4	5	6
3^n	1	3	2	6	4	5	1

Из таблицы (экспонент) видно, что $3^n \pmod 7$ может принимать любое значение из набора (1,2,3,4,5,6), т.е. **3** является генератором $\mathbb{Z}_7$. Обратной к полученной таблице будет являтся таблица логарифмов (индексов):

n	0	1	2	3	4	5	6
ind n	6	0	2	1	4	5	3

Пользуясь таблицей индексов и экспонент несложно производить некоторые арифметические операции

$$2 \times 6 = 3^{\text{ind } 2} \times 3^{\text{ind } 6} = 3^{\text{ind } 2+\text{ind } 6} = 3^{2+3} = 3^5 = 5,$$

$$3 \times 5 = 3^{\text{ind } 3} \times 3^{\text{ind } 5} = 3^{\text{ind } 3+\text{ind } 5} = 3^{1+5} = 3^6 = 3^0 = 1,$$

$$5 \times 6 = 3^{\text{ind } 5} \times 3^{\text{ind } 6} = 3^{\text{ind } 5+\text{ind } 6} = 3^{5+3} = 3^8 = 3^2 = 2.$$

В последних двух выражения мы учли, что $6 \equiv 0 \pmod 6$ и $8 \equiv 2 \pmod 6$. Другими словами, умножение в кольце $\mathbb{Z}_p$ чисел x и y производится по следующему правилу

$$x \times y = \alpha^{\text{ind } x} \times \alpha^{\text{ind } y} = \alpha^{(\text{ind } x+\text{ind } y) \bmod (p-1)}.$$

Выпишем таблицы сложения и умножения для $\mathbb{Z}_7$:

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Кольцо $\mathbb{Z}_8$ тоже можно превратить в поле, но для этого необходимо определить другие таблицы сложения и умножения, предварительно построив таблицу индексов. Такие поля (с собственными таблицами сложения и умножения) называются полями Галуа $GF(p^k)$.

★ Для составления таблицы индексов поля $GF(2^3)$ воспользуемся следующим замечательным трюком. Возьмем неприводимый полином 3 степени с коэффициентами из $\mathbb{Z}_2$:

$$p(x) = x^3 + x + 1$$

и рассмотрим остатки от деления степеней x^n на $p(x)$:

$$\left[\frac{x^0}{p(x)}\right] = 1 = 0001; \qquad \left[\frac{x^1}{p(x)}\right] = x = 0010$$

$$\left[\frac{x^2}{p(x)}\right] = x^2 = 0100; \qquad \left[\frac{x^3}{p(x)}\right] = x + 1 = 0011$$

$$\left[\frac{x^4}{p(x)}\right] = x^2 + x = 0110; \qquad \left[\frac{x^5}{p(x)}\right] = x^2 + x + 1 = 0111$$

$$\left[\frac{x^6}{p(x)}\right] = x^2 + 1 = 0101; \qquad \left[\frac{x^7}{p(x)}\right] = 1 = 0001$$

Учитывая, что в десятичной записи

$$001 = 1,\ 010 = 2,\ 011 = 3,\ 100 = 4,\ 101 = 5,\ 110 = 6,\ 111 = 7$$

из этих остатков составим таблицу индексов для $GF(2^3)$

n	0	1	2	3	4	5	6	7
2^n	1	2	4	3	6	7	5	1
ind n	7	0	1	3	2	6	4	5

Теперь, пользуясь таблицей индексов несложно построить таблицу умножения для $GF(2^3)$:

$\oplus$	1	2	3	4	5	6	7
1	0	3	2	5	4	7	6
2	3	0	1	6	7	4	5
3	2	1	0	7	6	5	4
4	5	6	7	0	1	2	3
5	4	7	6	1	0	3	2
6	7	4	5	2	3	0	1
7	6	5	4	3	2	1	0

$\times$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	3	1	7	5
3	3	6	5	7	4	1	2
4	4	3	7	6	2	5	1
5	5	1	4	2	7	3	6
6	6	7	1	5	3	2	4
7	7	5	2	1	6	4	3

Заметим, что таблица сложения в данном случае тоже строиться по другому. В качестве операции сложения мы здесь используем оператор побитового сложения **XOR** - " $\oplus$ ". Например

$$2 + 3 = 010 \oplus 011 = 001 = 1, \qquad 5 + 6 = 101 \oplus 110 = 011 = 3.$$

Поскольку и по сложению и по умножению наши элементы образуют группы то данное множество элементов можно назвать полем $GF(2^3)$.

★ Аналогичным образом построим поле Галуа $GF(2^4)$. Для этого возьмем неприводимый полином 4 степени с коэффициентами из $\mathbb{Z}_2$:

$$p(x) = x^4 + x + 1$$

и рассмотрим остатки от деления степеней x^n на $p(x)$:

$$\left[\frac{x^0}{p}\right] = 1 = 0001 \qquad \left[\frac{x^1}{p}\right] = x = 0010 \qquad \left[\frac{x^2}{p}\right] = x^2 = 0100 \ ...$$

$$\left[\frac{x^4}{p}\right] = 1 + x = 0011 \qquad \left[\frac{x^5}{p}\right] = x + x^2 = 0110 \qquad \left[\frac{x^6}{p}\right] = x^2 + x^3 = 1100 \ ...$$

$$\left[\frac{x^8}{p}\right] = 1 + x^2 = 0101 \qquad \left[\frac{x^9}{p}\right] = x + x^3 = 1010 \qquad \left[\frac{x^{10}}{p}\right] = 1 + x + x^2 = 0111 \ ...$$

Учитывая, что в десятичной записи

$$0001 = 1,\ 0010 = 2,\ 0011 = 3,\ ...,\ 1101 = 13,\ 1110 = 14,\ 1111 = 15,$$

из этих остатков составим таблицу индексов для $GF(2^4)$

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2^n	1	2	4	8	3	6	12	11	5	10	7	14	15	13	9	1
ind n	15	0	1	4	2	8	5	10	3	14	9	7	6	13	11	12

Теперь, пользуясь таблицей индексов несложно построить таблицу умножения для $GF(2^4)$:

×	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	2	4	6	8	10	12	14	3	1	7	5	11	9	15	13
3	3	6	5	12	15	10	9	11	8	13	14	7	4	1	2
4	4	8	12	3	7	11	15	6	2	14	10	5	1	13	9
5	5	10	15	7	2	13	8	14	11	4	1	9	12	3	6
6	6	12	10	11	13	7	1	5	3	9	15	14	8	2	4
7	7	14	9	15	8	1	6	13	10	3	4	2	5	12	11
8	8	3	11	6	14	5	13	12	4	15	7	10	2	9	1
9	9	1	8	2	11	3	10	4	13	5	12	6	15	7	14
10	10	7	13	14	4	9	3	15	5	8	2	1	11	6	12
11	11	5	14	10	1	15	4	7	12	2	9	13	6	8	3
12	12	11	7	5	9	14	2	10	6	1	13	15	3	4	8
13	13	9	4	1	12	8	5	2	15	11	6	3	14	10	7
14	14	15	1	13	3	2	12	9	7	6	8	4	10	11	5
15	15	13	2	9	6	4	11	1	14	12	3	8	7	5	10

Сложение определяется как побитовая сумма по модулю 2 оператором **XOR**. В общем случае показанная схема позволяет для любого p^k построить поле $GF(p^k)$.

3.7 Коды БЧХ

Рассмотренные нами ранее полиномиальные коды для исправления ошибок требовали знания таблицы синдромов. Получается, что на приемнике информации должна быть выделена память для ее хранения. В противном случае для каждого блока принятой кодовой последоватеьльности необходимо рассчитывать синдромные остатки, а это опять задержки в передаче. Дальнейшей целью теории помехоустойчивого кодирования является построение алгоритмов, позволяющих определять ошибку пользуясь только принятой коддовой комбинацие. Очевидно что такие коды не обязаны быть совершенными, а главным параметром становиться простота их аппаратной реализации.

Коды БЧХ[5] являются разновидностью полиномиальных и формируются по тому же принципу. Информационная последовательность $a = (a_{k-1}a_{k-2}...a_1a_0)$ представляется в виде полинома

$$m = a_i x^i = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + ... + a_1x^1 + a_0x^0.$$

По формуле

$$2^r \geq \sum_{i=0}^{q} C_{k+r}^i$$

определяется количество r проверочных символов, необходимых для исправления q ошибок. После чего смещенный полином $x^r m$ делится на проверочный p:

$$\frac{x^r m}{p} = C + \frac{R}{p}$$

и формируется кодовая последовательность

$$F = Cp = \left[\frac{x^r m}{p}\right] \oplus R.$$

Поскольку коды БЧХ формируются длля работы в полях $GF(2^m)$, то полиномы $p = \psi_i,\ i \neq 0$ выбираются из множества

$$x^{2^m-1} - 1 = \psi_0\psi_1\psi_2...$$

Например

★ $GF(2^2)$:

$$x^3 - 1 = (1 + x)(1 + x + x^2)$$

★ $GF(2^3)$:

$$x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3)$$

★ $GF(2^4)$:

$$x^{15} - 1 = (1 + x)(1 + x + x^2)(1 + x + x^4)(1 + x^3 + x^4)(1 + x + x^2 + x^3 + x^4)$$

[5]Коды Боуза — Чоудхури — Хоквингема.

★ $GF(2^5)$:

$$\begin{aligned} x^{31}-1 &= (1+x)(1+x^2+x^5)(1+x^3+x^5)(1+x+x^2+x^3+x^5) \\ &\times (1+x+x^2+x^4+x^5)(1+x+x^3+x^4+x^5)(1+x^2+x^3+x^4+x^5) \end{aligned}$$

Для создания проверочных полиномов можно брать произвольную комбинацию функций ψ, например $p=\psi_1\psi_3...$ (кроме $\psi_0=1+x$).

Заметим, что длина кода и количество исправляемых ошибок напрямую связаны с размерностью поля $GF(2^m)$. Обозначим через $[n,k,q]$ код, длиной n с k информационными разрядами, исправляющий q ошибок. Тогда поле $GF(2^m)$ допускает построение следующих кодов БЧХ

★ $GF(2^2)$: $[3,1,1]$

★ $GF(2^3)$: $[7,4,1]$, $[7,1,2]$

★ $GF(2^4)$: $[15,11,1]$, $[15,7,2]$, $[15,5,3]$, $[15,1,4]$

Существует множество различных алгоритмов декодирования кода БЧХ. Мы рассмотрим некоторые из них.

3.7.1 Прямой алгебраический метод PGZ

Рассматриваемый декодер был впервые предложен В.В.Петерсоном в 1960 г.

Допустим принятая кодовая комбинация $\mathbf{A}=(A_{n-1}A_{n-2}...A_1A_0)$ имеет вид

$$F(x)=\sum A_i x^i = A_{n-1}x^{n-1}+A_{n-2}x^{n-2}+...+A_1x^1+A_0x^0.$$

★ Для исправления 1 ошибки нам достаточно подставить число 2 в принятую комбинацию

$$F(2)=\sum A_i 2^i = A_{n-1}2^{n-1}+A_{n-2}2^{n-2}+...+A_12^1+A_02^0=2^\alpha.$$

Тогда α - степень искаженного разряда в полиноме кодовой комбинации.

★ Для исправления 2 ошибок нам необходимо рассчитать 4 значения

$$\begin{aligned} S_1 &= F(2^1)=\sum A_i 2^i = A_{n-1}2^{n-1}+A_{n-2}2^{n-2}+...+A_12^1+A_02^0 \\ S_2 &= F(2^2)=\sum A_i (2^2)^i = A_{n-1}(2^2)^{n-1}+A_{n-2}(2^2)^{n-2}+...+A_1(2^2)^1+A_0(2^2)^0 \\ S_3 &= F(2^3)=\sum A_i (2^3)^i = A_{n-1}(2^3)^{n-1}+A_{n-2}(2^3)^{n-2}+...+A_1(2^3)^1+A_0(2^3)^0 \\ S_4 &= F(2^4)=\sum A_i (2^4)^i = A_{n-1}(2^4)^{n-1}+A_{n-2}(2^4)^{n-2}+...+A_1(2^4)^1+A_0(2^4)^0 \end{aligned}$$

После чего вычислить (σ_1,σ_2) из выражения

$$\begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix}\begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix}=\begin{pmatrix} S_3 \\ S_4 \end{pmatrix}$$

и найти корни уравнения

$$\Sigma(x)=1+\sigma_1x+\sigma_2x^2=(1+2^\alpha x)(1+2^\beta x).$$

Тогда α и β являются степенями искаженных разрядов в полиноме кодовой комбинации.

★ Для исправления 3 ошибок нам необходимо рассчитать 6 значений

$$S_1 = F(2^1) = \sum A_i 2^i \qquad S_2 = F(2^2) = \sum A_i (2^2)^i \qquad S_3 = F(2^3) = \sum A_i (2^3)^i$$
$$S_4 = F(2^4) = \sum A_i (2^4)^i \qquad S_5 = F(2^5) = \sum A_i (2^5)^i \qquad S_6 = F(2^6) = \sum A_i (2^6)^i$$

После чего вычислить $(\sigma_1, \sigma_2, \sigma_3)$ из выражения

$$\begin{pmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{pmatrix} \begin{pmatrix} \sigma_3 \\ \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} S_4 \\ S_5 \\ S_6 \end{pmatrix}$$

и найти корни уравнения

$$\Sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2 + \sigma_3 x^3 = (1 + 2^\alpha x)(1 + 2^\beta x)(1 + 2^\gamma x).$$

Тогда (α, β, γ) являются степенями искаженных разрядов в полиноме кодовой комбинации.

★ В самом общем случае для исправления q ошибок нам необходимо рассчитать 2q значений

$$S_k = F(2^k) = \sum A_i (2^k)^i$$

После чего вычислить $(\sigma_1, \sigma_2, ..., \sigma_q)$ из выражения

$$\begin{pmatrix} S_1 & S_2 & S_3 & ... & S_q \\ S_2 & S_3 & S_4 & ... & S_{q+1} \\ ... & ... & ... & ... & ... \\ S_q & S_{q+1} & S_{q+2} & ... & S_{2q-1} \end{pmatrix} \begin{pmatrix} \sigma_q \\ \sigma_{q-1} \\ ... \\ \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} S_{q+1} \\ S_{q+2} \\ ... \\ S_{2q-1} \\ S_{2q} \end{pmatrix}$$

и найти корни уравнения

$$1 + \sigma_1 x + \sigma_2 x^2 + \sigma_3 x^3 + ... + \sigma_q x^q = (1 + 2^{\alpha_1} x)(1 + 2^{\alpha_2} x)...(1 + 2^{\alpha_q} x)$$

или

$$\Sigma(x) = \sum_{j=0}^{q} \sigma_j x^j = \prod_{j=0}^{q} (1 + 2^{\alpha_j} x)$$

Тогда $(\alpha_1, \alpha_2, ..., \alpha_q)$ являются степенями искаженных разрядов в полиноме кодовой комбинации.

3.7.2 Коды БЧХ над $GF(2^3)$

Пример 3.28. Рассмотрим построение кода БЧХ в $GF(2^3)$ исправляющего 1 ошибку при передаче информационной последовательности $\boldsymbol{a} = (1001)$.

Решение. Пользуясь алгоритмами построения полиномиального кода из выражения

$$2^r \geq k + r + 1$$

находим $r = 3$. Информационная последовательность $\boldsymbol{a} = (1001)$ представляется в виде

$$m(x) = x^3 \cdot 1 + x^2 \cdot 0 + x \cdot 0 + 1 \cdot 1 = x^3 + 1.$$

Поскольку $r = 3$, то умножаем

$$Q(x) = x^r m = x^3 m = x^3(x^3 + x^2 + x + 1) = x^6 + x^5 + x^4 + x^3 = 1001000.$$

Поскольку таблица индексов для $GF(2^3)$ строилась относительно полинома $p = x^3 + x + 1$, то в разложении

$$x^7 - 1 = \psi_0\psi_1\psi_2 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3)$$

возьмем $p = \psi_1$. Делим $m = x^r Q$ на образующий полином p

$$\frac{x^3 m}{p} = C + \frac{R}{p} \qquad \text{или} \qquad \frac{x^6 + x^3}{x^3 + x + 1} = (x^3 + x) + \frac{x^2 + x}{x^3 + x + 1}$$

окуда получим $R = x^2 + x = (110)$. Поскольку

$$Q(x) = x^6 + x^5 + x^4 + x^3 = 1001000$$

то передаваемая комбинация $\mathbf{F}$ есть прямая конкатенация $m \oplus R$:

$$\begin{array}{r} \mathbf{Q} = 1001000 \\ \mathbf{R} = \quad\;\; 110 \\ \hline \mathbf{F} = 1001110 \end{array}$$

Таким образом, передаваемая кодовая комбинация имеет вид $\mathbf{F} = (1001110)$. ▲

Допустим во время передачи по каналу информации в F возникла ошибка в 3 символе слева.

$$\mathbf{F} = (10\underline{\mathbf{0}}1110) \quad \rightarrow \quad \mathbf{F} = (10\underline{\mathbf{1}}1110)$$

Опишем алгоритм определения и исправления ошибки кода БЧХ [7, 4].

Пример 3.29. Обнаружить и исправить ошибку в кодовой БЧХ последовательности $\mathbf{F} = (1011110)$ над $GF(2^3)$.

Решение. Перепишем принятую кодовую комбинацию $\mathbf{F} = (1011110)$ в полиномиальном виде

$$F(x) = \sum F_i x^i = x^6 + x^4 + x^3 + x^2 + x.$$

Для исправления 1 ошибки нам достаточно подставить число 2 в принятую комбинацию

$$F(2) = \sum F_i 2^i = 2^6 + 2^4 + 2^3 + 2^2 + 2 = 5 + 6 + 3 + 4 + 2 = 6 = 2^4.$$

Здесь степень 2^k вычислялась по таблице индексов поля $GF(2^3)$, а в качестве сложения использовалась операция XOR (или см. таблицу сложения для $GF(2^3)$). Поскольку $2^\alpha = 2^4$, то $\alpha = 4$ степень искаженного разряда в полиноме кодовой комбинации:

$$\mathbf{F} = (10\underline{\mathbf{1}}1110) \quad \rightarrow \quad \mathbf{F} = (10\underline{\mathbf{0}}1110).$$

Т.к. код БЧХ является систематическим, то для выделения информационной последовательности нам достаточно вычеркнуть $r = 3$ последних разряда кодовой комбинации $\boldsymbol{a} = (1001)$. ▲

Задача 3.18.

На приемнике была получена кодовая последовательность БЧХ [7,4] над $GF(2^3)$. Восстановить исходное сообщение.

N	F	N	F	N	F
1	1110001	11	0101001	21	1001001
2	0111010	12	1101010	22	0001010
3	1010011	13	0100011	23	1100011
4	1011100	14	0001100	24	1101100
5	0100001	15	1101110	25	0011111
6	0100111	16	1110110	26	0100111
7	0100100	17	1000110	27	0001011
8	1100111	18	0100110	28	0001101
9	1100100	19	1001111	29	0001110
10	1100010	20	0101111	30	1110010

Следующий пример преследует исключительно методическую цель, поскольку применение данного алгоритма на практике не рационально. Мы построим код БЧХ в $GF(8)$ исправляющий 2 ошибки.

Пример 3.30. Рассмотрим построение кода БЧХ в $GF(2^3)$ исправляющего 2 ошибки.

Решение. Для исправления 1 ошибки мы пользовались полиномом $p = \psi_1$. Для исправления 2 ошибок нам необходимо взять 2 функции ψ. Тогда проверочный полином будет выглядеть так

$$p = \psi_1\psi_2 = (1 + x + x^3)(1 + x^2 + x^3) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6.$$

Т.е. нам необходимо взять $r = 6$ проверочных символов для построения кода БЧХ $[7, 1]$ исправляющего 2 ошибки[6].

Допустим информационная последовательность имеет вид $\mathbf{a} = (1)$ представляется в виде

$$m(x) = 1.$$

Поскольку $r = 6$, то умножаем

$$Q(x) = x^r m = x^6 \cdot 1 = x^6 = 1000000.$$

Делим $Q = x^r m$ на проверочный полином p

$$\frac{x^6 m}{p} = C + \frac{R}{p}$$

или

$$\frac{x^6}{1 + x + x^2 + x^3 + x^4 + x^5 + x^6} = 1 + \frac{1 + x + x^2 + x^3 + x^4 + x^5}{1 + x + x^2 + x^3 + x^4 + x^5 + x^6}$$

окуда получим $R = 1 + x + x^2 + x^3 + x^4 + x^5$. Поскольку

$$Q(x) = x^6 = 1000000$$

то передаваемая комбинация $\mathbf{F}$ есть прямая конкатенация $m \oplus R$:

$$\begin{array}{r} \mathbf{Q} = 1000000 \\ \mathbf{R} = \ \ 111111 \\ \hline \mathbf{F} = 1111111 \end{array}$$

Таким образом, передаваемая кодовая комбинация имеет вид $\mathbf{F} = (1111111)$. ▲

Допустим во время передачи по каналу информации в $\mathbf{F}$ возникло две ошибки во 2 и 5 символе слева.

$$\mathbf{F} = (1\underline{\mathbf{1}}11\underline{\mathbf{1}}11) \quad \rightarrow \quad \overline{\mathbf{F}} = (1\underline{\mathbf{0}}11\underline{\mathbf{0}}11)$$

Опишем алгоритм определения и исправления ошибки кода БЧХ $[7, 1]$.

[6]Заметим, что повторный код $[5, 1]: \ 1 \rightarrow 11111$, исправляющий 2 ошибки имеет длину $n = 5$, а повторный код длины $n = 7$, $[n, k] = [7, 1]$ исправляет 3 ошибки. Т.е. в данном примере код БЧХ уступает по скорости $1/7 < 1/5$ даже простейшему повторному.

Пример 3.31. Обнаружить и исправить ошибки в БЧХ кодовой последовательности $\mathbf{A} = (1011011)$ над $GF(2^3)$.

Решение. Перепишем принятую кодовую комбинацию $\mathbf{A} = (1011011)$ в полиномиальном виде

$$F(x) = \sum A_i x^i = x^6 + x^4 + x^3 + x + 1.$$

Для исправления двух ошибок нам необходимо рассчитать 4 значения

$$\begin{aligned}
S_1 &= F(2^1) = \sum A_i 2^i = 2^6 + 2^4 + 2^3 + 2 + 1 = 5 + 6 + 3 + 2 + 1 = 3 \\
S_2 &= F(2^2) = \sum A_i (2^2)^i = 2^{12} + 2^8 + 2^6 + 2^2 + 1 = 7 + 2 + 5 + 4 + 1 = 5 \\
S_3 &= F(2^3) = \sum A_i (2^3)^i = x^{18} + 2^{12} + x^9 + 2^3 + 1 = 6 + 7 + 4 + 3 + 1 = 7 \\
S_4 &= F(2^4) = \sum A_i (2^4)^i = x^{24} + x^{16} + x^{12} + 2^4 + 1 = 3 + 4 + 7 + 6 + 1 = 7
\end{aligned}$$

Те читатели, которые захотят рассчитать предыдущие суммы устно (без компьютера) должны помнить, что в $GF(2^3)$ возведение в степень имеет свойства

$$2^k = 2^{k+7}, \quad \text{т.е.} \quad 2^{18} = 2^4 = 6,\ 2^{24} = 2^3 = 3,\ 2^{16} = 2^2 = 4, \quad \text{и т.д.}$$

Теперь вычислим (σ_1, σ_2) из выражения

$$\begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} S_3 \\ S_4 \end{pmatrix}, \quad \text{т.е.} \quad \begin{pmatrix} 3 & 5 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} 7 \\ 7 \end{pmatrix}$$

По методу Крамера найдем

$$\Delta = \begin{vmatrix} 3 & 5 \\ 5 & 7 \end{vmatrix} = 3 \cdot 7 - 5 \cdot 5 = 2 + 7 = 5$$

$$\Delta_2 = \begin{vmatrix} 7 & 5 \\ 7 & 7 \end{vmatrix} = 7 \cdot 7 - 7 \cdot 5 = 3 + 6 = 5; \qquad \Delta_1 = \begin{vmatrix} 3 & 7 \\ 5 & 7 \end{vmatrix} = 3 \cdot 7 - 5 \cdot 7 = 2 + 6 = 4$$

По таблице умножения в $GF(2^3)$ получим

$$\Delta^{-1} = 5^{-1} = 2.$$

Тогда

$$\sigma_1 = \frac{\Delta_1}{\Delta} = \Delta_1 \cdot \Delta^{-1} = 4 \cdot 2 = 3; \qquad \sigma_2 = \frac{\Delta_2}{\Delta} = \Delta_2 \cdot \Delta^{-1} = 5 \cdot 2 = 1$$

Теперь подставим полученные значения (σ_1, σ_2) в уравнение

$$\Sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2 = 1 + 3x + x^2.$$

Для решения данного уравнения воспользуемся формулами Виета

$$\begin{cases} x_1 + x_2 = \sigma_1 \\ x_1 \cdot x_2 = \sigma_2 \end{cases} \quad \text{или} \quad \begin{cases} x_1 + x_2 = 3 \\ x_1 \cdot x_2 = 1 \end{cases}$$

По таблицам сложения и умножения для $GF(2^3)$ находим $x_1 = 4,\ x_2 = 7$, тогда

$$\Sigma(x) = 1 + 3x + x^2 = (1 + 4x)(1 + 7x) = (1 + 2^2x)(1 + 2^5x).$$

Т.е. ошибки в коэффициентах при степенях x^2 и x^5 полинома $\overline{F(x)}$. Меняя значения разрядов на противоположные получим

$$\mathbf{F} = (1\underline{\mathbf{0}}11\underline{\mathbf{0}}11) \quad \rightarrow \quad \mathbf{F} = (1\underline{\mathbf{1}}11\underline{\mathbf{1}}11)$$

- исправленную кодовую комбинацию. ▲

Задача 3.19.

На приемнике была получена кодовая последовательность БЧХ [7,1] над $GF(2^3)$. Восстановить исходное сообщение.

N	F	N	F	N	F	N	F	N	F	N	F
1	0101111	6	1100111	11	0101111	16	1111100	21	1011110	26	1011110
2	0110111	7	1101011	12	0110111	17	1111010	22	1011101	27	1011011
3	0111011	8	1101101	13	0111011	18	1111001	23	1011011	28	1001111
4	0111101	9	1101110	14	0111101	19	1110110	24	1010111	29	1110101
5	0111110	10	1110011	15	0111110	20	1010111	25	1011101	30	1001111

3.7.3 Коды БЧХ над $GF(2^4)$

Пример 3.32. Рассмотрим построение кода БЧХ в $GF(2^4)$ исправляющего 1 ошибку при передаче информационной последовательности $\boldsymbol{a} = (11100011100)$.

Решение. Пользуясь алгоритмами построения полиномиального кода из выражения

$$2^r \geq k + r + 1 = 11 + r + 1 = 12 + r$$

находим $r = 4$. Информационная последовательность $\boldsymbol{a} = (11100011100)$ представляется в виде

$$m(x) = x^{10} + x^9 + x^8 + x^4 + x^3 + x^2.$$

Поскольку $r = 4$, то умножаем m на x^4:

$$\begin{aligned} Q(x) &= x^r m = x^4 m = x^4(x^{10} + x^9 + x^8 + x^4 + x^3 + x^2) \\ &= x^{14} + x^{13} + x^{12} + x^8 + x^7 + x^6 = 111000111000000. \end{aligned}$$

Поскольку таблица индексов для $GF(2^4)$ строилась относительно полинома $p = x^4 + x + 1$, то в разложении

$$x^{15} - 1 = \psi_0\psi_1\psi_2\psi_3\psi_4 = (1+x)(1+x+x^2)(1+x+x^4)(1+x^3+x^4)(1+x+x^2+x^3+x^4)$$

возьмем $p = \psi_2$. Делим $Q = x^r m$ на проверочный полином p

$$\frac{x^4 m}{p} = C + \frac{R}{p}$$

или

$$\frac{x^{14}+x^{13}+x^{12}+x^8+x^7+x^6}{x^4+x+1} = 1+x+x^2+x^4+x^7+x^8+x^9+\frac{1+x^3}{x^4+x+1}$$

окуда получим $R = x^3 + 1 = (1001)$. Поскольку

$$Q(x) = x^{14}+x^{13}+x^{12}+x^8+x^7+x^6 = 111000111000000$$

то передаваемая комбинация $\mathbf{F}$ есть прямая конкатенация $\mathbf{Q} \oplus \mathbf{R}$:

$$\begin{array}{r} \mathbf{Q} = 111000111000000 \\ \mathbf{R} = \qquad\qquad 1001 \\ \hline \mathbf{F} = 111000111001001 \end{array}$$

Таким образом, передаваемая кодовая комбинация имеет вид $\mathbf{F} = (111000111001001)$.▲

Допустим во время передачи по каналу информации в F возникла ошибка в 5 символе слева.

$$\mathbf{F} = (1110\underline{\mathbf{0}}0111001001) \quad \rightarrow \quad \mathbf{F} = (1110\underline{\mathbf{1}}0111001001)$$

Опишем алгоритм определения и исправления ошибки кода БЧХ [15, 11].

Пример 3.33. Обнаружить и исправить ошибку в кодовой БЧХ последовательности $\mathbf{F} = (111010111001001)$ над $GF(2^4)$.

Решение. Перепишем принятую кодовую комбинацию $\mathbf{F} = (111010111001001)$ в полиномиальном виде

$$F(x) = \sum F_i x^i = x^{14}+x^{13}+x^{12}+x^{10}+x^8+x^7+x^6+x^3+1.$$

Для исправления 1 ошибки нам достаточно подставить число 2 в принятую комбинацию

$$\begin{aligned} F(2) = \sum F_i 2^i &= 2^{14}+2^{13}+2^{12}+2^{10}+2^8+2^7+2^6+2^3+1 \\ &= 9+13+15+7+5+11+12+8+1 = 7 = 2^{10} \end{aligned}$$

Здесь степень 2^k вычислялась по таблице индексов поля $GF(2^4)$, а в качестве сложения использовалась операция XOR (или см. таблицу сложения для $GF(2^4)$). Поскольку $2^\alpha = 2^{10}$, то $\alpha = 10$ степень искаженного разряда в полиноме кодовой комбинации:

$$\mathbf{F} = (1110\underline{\mathbf{1}}0111001001) \quad \rightarrow \quad \mathbf{F} = (1110\underline{\mathbf{0}}0111001001)$$

Т.к. код БЧХ является систематическим, то для выделения информационной последовательности нам достаточно вычеркнуть $r = 4$ последних разряда кодовой комбинации $\boldsymbol{a} = (11100011100)$. ▲

Задача 3.20.

На приемнике была получена кодовая последовательность БЧХ $[15, 11]$ над $GF(2^4)$. Восстановить исходное сообщение.

N	F	N	F	N	F
1	111100001111110	11	110011001100011	21	101010101011001
2	111100001111000	12	110011001100001	22	101010101011111
3	111100001110100	13	110011001100111	23	101010101010011
4	111100001101100	14	110011001101011	24	101010101001011
5	111100001011100	15	110011001110011	25	101010101111011
6	111100000111100	16	110011001000011	26	101010100011011
7	111100011111100	17	110011000100011	27	101010111011011
8	111100101111100	18	110011011100011	28	101010001011011
9	111101001111100	19	110011101100011	29	101011101011011
10	111110001111100	20	110010001100011	30	101000101011011

Пример 3.34. Рассмотрим построение кода БЧХ в $GF(2^4)$ исправляющего 2 ошибки.

Решение. Пользуясь алгоритмами построения полиномиального кода из выражения

$$2^r \geq C_{15}^1 + C_{15}^2 = 15 + 105 = 120$$

находим $r = 7$. Т.е. нам необходимо не менее 7 проверочных разрядов. Тогда из разложения

$$x^{15} - 1 = \psi_0\psi_1\psi_2\psi_3\psi_4 = (1+x)(1+x+x^2)(1+x+x^4)(1+x^3+x^4)(1+x+x^2+x^3+x^4)$$

возьмем ψ_2 - как образующий поля $GF(2^4)$ и ψ_4:

$$p = \psi_2\psi_4 = (1+x+x^4)(1+x+x^2+x^3+x^4) = 1+x^4+x^6+x^7+x^8$$

мы получим $r = 8$. Таким образом БЧХ код в $GF(2^4)$, исправляющий 2 ошибки будет иметь вид $[n, k] = [15, 7]$.

Допустим информационная последовательность имеет вид $\boldsymbol{a} = (1110001)$ и представляется в виде

$$m(x) = 1 + x^4 + x^5 + x^6.$$

Поскольку $r = 8$, то умножаем

$$Q(x) = x^r m = x^8 \cdot (1 + x^4 + x^5 + x^6) = x^{14} + x^{13} + x^{12} + x^8.$$

Делим $m = x^r Q$ на проверочный полином p

$$\frac{x^8 m}{p} = C + \frac{R}{p}$$

или

$$\frac{x^{14} + x^{13} + x^{12} + x^8}{1 + x^4 + x^6 + x^7 + x^8} = 1 + x + x^2 + x^6 + \frac{1 + x + x^2 + x^4 + x^5 + x^6}{1 + x^4 + x^6 + x^7 + x^8}$$

окуда получим $R = 1 + x + x^2 + x^4 + x^5 + x^6 = 01110111$. Поскольку

$$Q(x) = x^{14} + x^{13} + x^{12} + x^8 = 111000100000000$$

то передаваемая комбинация $\mathbf{F}$ есть прямая конкатенация $\mathbf{Q} \oplus \mathbf{R}$:

$$\begin{array}{r} \mathbf{Q} = 111000100000000 \\ \mathbf{R} = \qquad\quad 01110111 \\ \hline \mathbf{F} = 111000101110111 \end{array}$$

Таким образом, передаваемая кодовая комбинация имеет вид $\mathbf{F} = (111000101110111)$.▲

Допустим во время передачи по каналу информации в $\mathbf{F}$ возникло две ошибки в 3 и 8 символе слева.

$$\mathbf{F} = (11\underline{\mathbf{1}}0001\underline{\mathbf{0}}1110111) \quad \rightarrow \quad \overline{\mathbf{F}} = (11\underline{\mathbf{0}}0001\underline{\mathbf{1}}1110111)$$

Опишем алгоритм определения и исправления ошибки кода БЧХ [15, 7].

Пример 3.35. Обнаружить и исправить ошибки в БЧХ кодовой последовательности $\mathbf{F} = (110000111110111)$ над $GF(2^4)$.

Решение. Перепишем принятую кодовую комбинацию $\mathbf{F} = (110000111110111)$ в полиномиальном виде

$$F(x) = \sum F_i x^i = x^{14} + x^{13} + x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + x + 1.$$

Для исправления двух ошибок нам необходимо рассчитать 4 значения

$$\begin{aligned} S_1 &= F(2^1) = \sum F_i 2^i = 2^{14} + 2^{13} + 2^8 + 2^7 + 2^6 + 2^5 + 2^4 + 2^2 + 2 + 1 = 4 \\ S_2 &= F(2^2) = \sum F_i 4^i = 4^{14} + 4^{13} + 4^8 + 4^7 + 4^6 + 4^5 + 4^4 + 4^2 + 4 + 1 = 3 \\ S_3 &= F(2^3) = \sum F_i 8^i = 8^{14} + 8^{13} + 8^8 + 8^7 + 8^6 + 8^5 + 8^4 + 8^2 + 8 + 1 = 0 \\ S_4 &= F(2^4) = \sum F_i 3^i = 3^{14} + 3^{13} + 3^8 + 3^7 + 3^6 + 3^5 + 3^4 + 3^2 + 3 + 1 = 5 \end{aligned}$$

Те читатели, которые захотят рассчитать предыдущие суммы устно (без компьютера) должны помнить, что в $GF(2^4)$ возведение в степень имеет свойства

$$2^k = 2^{k+15}, \quad \text{т.е.} \quad 2^{18} = 2^3 = 8,\ 2^{24} = 2^9 = 10,\ 2^{16} = 2^1 = 1, \quad \text{и т.д.}$$

Теперь вычислим (σ_1, σ_2) из выражения

$$\begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} S_3 \\ S_4 \end{pmatrix}, \quad \text{т.е.} \quad \begin{pmatrix} 4 & 3 \\ 3 & 0 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 5 \end{pmatrix}$$

По методу Крамера найдем

$$\Delta = \begin{vmatrix} 4 & 3 \\ 3 & 0 \end{vmatrix} = 4 \cdot 0 - 3 \cdot 3 = 0 + 5 = 5$$

$$\Delta_2 = \begin{vmatrix} 0 & 3 \\ 5 & 0 \end{vmatrix} = 0 \cdot 0 - 5 \cdot 3 = 0 + 15 = 15; \qquad \Delta_1 = \begin{vmatrix} 4 & 0 \\ 3 & 5 \end{vmatrix} = 4 \cdot 5 - 3 \cdot 0 = 7 + 0 = 7.$$

По таблице умножения в $GF(2^4)$ получим

$$\Delta^{-1} = 5^{-1} = 11.$$

Тогда

$$\sigma_1 = \frac{\Delta_1}{\Delta} = \Delta_1 \cdot \Delta^{-1} = 7 \cdot 11 = 4; \qquad \sigma_2 = \frac{\Delta_2}{\Delta} = \Delta_2 \cdot \Delta^{-1} = 15 \cdot 11 = 3.$$

Теперь подставим полученные значения (σ_1, σ_2) в уравнение

$$\Sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2 = 1 + 4x + 3x^2 = (1 + 11x)(1 + 15x) = (1 + 2^7 x)(1 + 2^{12} x).$$

Тогда $\alpha = 7$ и $\beta = 12$ являются степенями искаженных разрядов в полиноме кодовой комбинации. Меняя значения разрядов на противоположные получим

$$\mathbf{F} = (11\underline{\mathbf{0}}0001\underline{\mathbf{1}}1110111) \quad \rightarrow \quad \overline{\mathbf{F}} = (11\underline{\mathbf{1}}0001\underline{\mathbf{0}}1110111)$$

- исправленную кодовую комбинацию. ▲

Задача 3.21.

На приемнике была получена кодовая последовательность БЧХ $[15, 7]$ над $GF(2^4)$. Восстановить исходное сообщение.

N	F	N	F	N	F
1	111110111100101	11	110110111111000	21	101001100111110
2	111000111100101	12	111010111111000	22	100101100111110
3	111010011100101	13	111100111111000	23	100011100111110
4	111010101100101	14	111111111111000	24	100000100111110
5	111010110100101	15	111110011111000	25	100001000111110
6	111010111000101	16	111110101111000	26	100001110111110
7	101111111100101	17	111110110111000	27	100001101111110
8	101110011100101	18	111110111011000	28	100001100011110
9	101110101100101	19	111110111101000	29	100001100101110
10	101110110100101	20	111110111110000	30	100001100110110

Пример 3.36. Рассмотрим построение кода БЧХ $[15, 5]$ в $GF(2^4)$ исправляющего 3 ошибки.

Решение. Пользуясь алгоритмами построения полиномиального кода из выражения

$$2^r \geq C_{15}^1 + C_{15}^2 + C_{15}^3 = 15 + 105 + 455 = 575$$

находим $r = 10$. Т.е. нам необходимо не менее 10 проверочных разрядов. Тогда из разложения

$$x^{15} - 1 = \psi_0\psi_1\psi_2\psi_3\psi_4 = (1+x)(1+x+x^2)(1+x+x^4)(1+x^3+x^4)(1+x+x^2+x^3+x^4)$$

возьмем ψ_2 - как образующий поля $GF(2^4)$, ψ_4 и ψ_1:

$$p = \psi_1\psi_2\psi_4 = (1+x+x^2)(1+x+x^4)(1+x+x^2+x^3+x^4) = 1+x+x^2+x^4+x^5+x^8+x^{10}.$$

Таким образом БЧХ код в $GF(2^4)$, исправляющий 3 ошибки будет иметь вид $[n, k] = [15, 5]$.

Допустим информационная последовательность имеет вид $\boldsymbol{a} = (11110)$ и представляется в виде

$$m(x) = x + x^2 + x^3 + x^4.$$

Поскольку $r = 10$, то умножаем

$$Q(x) = x^r m = x^{10} \cdot (x + x^2 + x^3 + x^4) = x^{14} + x^{13} + x^{12} + x^{11}.$$

Делим $Q = x^r m$ на проверочный полином p

$$\frac{x^{10}m}{p} = C + \frac{R}{p}$$

или

$$\frac{x^{14} + x^{13} + x^{12} + x^{11}}{1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}} = x^3 + x^4 + \frac{x^3 + x^6 + x^7 + x^9}{1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}}$$

окуда получим $R = x^3 + x^6 + x^7 + x^9 = 1011001000$. Поскольку

$$Q(x) = x^{14} + x^{13} + x^{12} + x^8 = 111100000000000$$

то передаваемая комбинация F есть прямая конкатенация $Q \oplus R$:

$$\begin{array}{r} \mathbf{Q} = 111100000000000 \\ \mathbf{R} = \qquad 1011001000 \\ \hline \mathbf{F} = 111101011001000 \end{array}$$

Таким образом, передаваемая кодовая комбинация имеет вид $\mathbf{F} = (111101011001000)$.▲

Допустим во время передачи по каналу информации в $\mathbf{F}$ возникло три ошибки в 2, 5 и 11 символе слева.

$$\mathbf{F} = (1\underline{\mathbf{1}}11\underline{\mathbf{0}}10110\underline{\mathbf{0}}1000) \quad \rightarrow \quad \mathbf{F} = (1\underline{\mathbf{0}}11\underline{\mathbf{1}}10110\underline{\mathbf{1}}1000)$$

Опишем алгоритм определения и исправления ошибки кода БЧХ $[15, 5]$.

Пример 3.37. Обнаружить и исправить ошибки в БЧХ $[15, 5]$ кодовой последовательности $\mathbf{F} = (101111011011000)$ над $GF(2^4)$.

Решение. Перепишем принятую кодовую комбинацию $\mathbf{F} = (101111011011000)$ в полиномиальном виде

$$F(x) = \sum F_i x^i = x^{14} + x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^3.$$

Для исправления двух ошибок нам необходимо рассчитать 6 значений

$$\begin{aligned} S_1 &= F(2^1) = \sum F_i 2^i = 9 \qquad & S_2 = F(2^2) = \sum F_i 4^i = 13 \\ S_3 &= F(2^3) = \sum F_i 8^i = 4 \qquad & S_4 = F(2^4) = \sum F_i 3^i = 14 \\ S_5 &= F(2^5) = \sum F_i 6^i = 6 \qquad & S_6 = F(2^6) = \sum F_i 12^i = 3 \end{aligned}$$

Теперь вычислим $(\sigma_1, \sigma_2, \sigma_3)$ из выражения

$$\begin{pmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{pmatrix} \begin{pmatrix} \sigma_3 \\ \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} S_4 \\ S_5 \\ S_6 \end{pmatrix}, \quad \text{т.е.} \quad \begin{pmatrix} 9 & 13 & 4 \\ 13 & 4 & 14 \\ 4 & 14 & 6 \end{pmatrix} \begin{pmatrix} \sigma_3 \\ \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} 14 \\ 6 \\ 3 \end{pmatrix}$$

По методу Крамера найдем

$$\Delta = \begin{vmatrix} 9 & 13 & 4 \\ 13 & 4 & 14 \\ 4 & 14 & 6 \end{vmatrix} = 14 \qquad \Delta_3 = \begin{vmatrix} 14 & 13 & 4 \\ 6 & 4 & 14 \\ 3 & 14 & 6 \end{vmatrix} = 5$$

$$\Delta_2 = \begin{vmatrix} 9 & 14 & 4 \\ 13 & 6 & 14 \\ 4 & 3 & 6 \end{vmatrix} = 9 \qquad \Delta_1 = \begin{vmatrix} 9 & 13 & 14 \\ 13 & 4 & 6 \\ 4 & 14 & 3 \end{vmatrix} = 7$$

По таблице умножения в $GF(2^4)$ получим

$$\Delta^{-1} = 14^{-1} = 3.$$

Тогда

$$\sigma_1 = \frac{\Delta_1}{\Delta} = \Delta_1 \cdot \Delta^{-1} = 7 \cdot 3 = 9$$

$$\sigma_2 = \frac{\Delta_1}{\Delta} = \Delta_2 \cdot \Delta^{-1} = 9 \cdot 3 = 8$$

$$\sigma_1 = \frac{\Delta_1}{\Delta} = \Delta_1 \cdot \Delta^{-1} = 5 \cdot 3 = 15$$

Теперь подставим полученные значения $(\sigma_1, \sigma_2, \sigma_3)$ в уравнение

$$\begin{aligned} \Sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2 + \sigma_3 x^3 &= 1 + 9x + 8x^2 + 15x^3 \\ &= (1 + 3x)(1 + 7x)(1 + 13x) \\ &= (1 + 2^4 x)(1 + 2^{10} x)(1 + 2^{13} x). \end{aligned}$$

Тогда $\alpha_1 = 4,\ \alpha_2 = 10,\ \alpha_3 = 13$ являются степенями искаженных разрядов в полиноме кодовой комбинации. Меняя значения разрядов на противоположные получим

$$\mathbf{F} = (1\underline{\mathbf{0}}11\underline{\mathbf{1}}10110\underline{\mathbf{1}}1000) \quad \rightarrow \quad \mathbf{F} = (1\underline{\mathbf{1}}11\underline{\mathbf{0}}10110\underline{\mathbf{0}}1000)$$

- исправленную кодовую комбинацию. ▲

Задача 3.22.

На приемнике была получена кодовая последовательность БЧХ $[15, 5]$ над $GF(2^4)$. Восстановить исходное сообщение.

N	F	N	F	N	F
1	110011110101111	11	111011001000001	21	100111000010111
2	110011110101001	12	111011001001101	22	100111000010001
3	110011110100101	13	111011001010101	23	100111000011101
4	110011110111101	14	111011001100101	24	100111000000101
5	110011110001101	15	111011000000101	25	100111000110101
6	110011111101101	16	111011011000101	26	100111001010101
7	110011100101101	17	111011101000101	27	100111010010101
8	110011010101101	18	111010001000101	28	100111100010101
9	110010110101101	19	111001001000101	29	100110000010101
10	110001110101101	20	111111001000101	30	100101000010101

Для кодов исправляющих 1-2 ошибки можно предложить еще один эффективный метод декодирования. Допустим вектор F содержит две ошибки $e(x) = x^\alpha + x^\beta$, тогда

$$S_1 = 2^\alpha + 2^\beta \qquad S_3 = 2^{3\alpha} + 2^{3\beta}.$$

Если $\eta_1 = 2^\alpha,\ \eta_2 = 2^\beta$ - локаторы ошибок, то

$$S_1 = \eta_1 + \eta_2 \qquad S_3 = \eta_1^3 + \eta_2^3$$

поэтому

$$S_3 = S_1^3 + S_1^2\eta_1 + S_1\eta_1^2 \qquad \Rightarrow \qquad 1 + S_1\eta_1^{-1} + \left(S_1^2 + S_3S_1^{-1}\right)\eta_1^{-2} = 0.$$

★ Если имеется 2 ошибки, то полином локаторов имеет вид

$$1 + S_1x + \left(S_1^2 + S_3S_1^{-1}\right)x^2 = 0$$

★ Если имеется 1 ошибка, то $S_1^3 + S_3 = 0$ и полином локаторов имеет вид

$$1 + S_1x = 0$$

★ Если ошибок нет, то $S_1 = S_3 = 0$.

В заключение параграфа выпишем коэффициенты полинома локатора

$$\Sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2 + ... + \sigma_k x^k = 0$$

для кода, исправляющего k<6 ошибок:

★ Коррекция 1 ошибки $\sigma_1 = S_1$

★ Коррекция 2 ошибок $\sigma_1 = S_1$

$$\sigma_2 = \frac{S_3 + S_1^3}{S_1}$$

★ Коррекция 3 ошибок $\sigma_1 = S_1$

$$\sigma_2 = \frac{S_1^2 S_3 + S_5}{S_3 + S_1^3}, \quad \sigma_3 = S_1^3 + S_3 + S_1\sigma_2$$

★ Коррекция 4 ошибок $\sigma_1 = S_1$

$$\sigma_2 = \frac{S_1(S_7 + S_1^7) + S_3(S_1^5 + S_5)}{S_3(S_1^3 + S_3) + S_1(S_1^5 + S_5)},$$

$$\sigma_3 = S_1^3 + S_3 + S_1\sigma_2, \quad \sigma_4 = \frac{S_5 + S_1^2 S_3 + (S_1^3 + S_3)\sigma_2}{S_1}$$

★ Коррекция 5 ошибок $\sigma_1 = S_1$

$$\sigma_2 = \frac{(S_1^3+S_3)[S_1^9+S_9+S_1^4(S_5+S_1^3S_3)+S_3^2(S_1^3+S_3)]+(S_1^5+S_5)(S_1^7+S_7)+S_1(S_3^2+S_1S_5)}{(S_1^3+S_3)[S_7+S_1^7+S_1S_3(S_1^3+S_3)]+(S_5+S_1^2S_3)(S_1^5+S_5)}$$

$$\sigma_3 = S_1^3 + S_3 + S_1\sigma_2$$

$$\sigma_4 = \frac{S_1^9 + S_9 + S_3^2(S_1^3 + S_3) + S_1^4(S_5 + S_1^2 S_3) + \sigma_2[S_7 + S_1^7 + S_1 S_3(S_1^3 + S_3)]}{S_1^5 + S_5}$$

$$\sigma_5 = S_5 + S_1^2 S_3 + S_1 S_4 + \sigma_2(S_1^3 + S_3)$$

Пример 3.38. Обнаружить и исправить ошибки в БЧХ $[7, 1]$ кодовой последовательности $F = (0111111)$ над $GF(2^3)$.

Решение. Вычислим вектор синдромов: $\mathbf{S} = (S_1, S_2, S_3, S_4) = (5, 7, 6, 3)$. Поскольку код БЧХ $[7, 1]$ может исправить до двух ошибок, то

$$\sigma_1 = S_1, \qquad \sigma_2 = \frac{S_3 + S_1^3}{S_1}$$

и полином локаторов имеет вид

$$\Sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2 = 1 + S_1 x + \frac{S_3 + S_1^3}{S_1}\, x^2 = 1 + 5x + \frac{6 + 5^3}{5}\, x^2 = 1 + 5x = 1 + 2^6 x.$$

Т.е. ошибка в 6 степени. ▲

3.7.4 Расширенный алгоритм Евклида

Расширенный алгоритм евклида для определения коэффициентов Безу также является итеррационным и требует вычисления остатков полиномов. Нам необходимо найти такие полиномы (Y, Σ), которые удовлетворяют равенству Безу

$$x^r Y + S\Sigma = 1.$$

Для этого мы записываем полином x^r через $S = \sum S_k x^k$ в виде

$$x^r = S \cdot q_0 + r_1$$

После чего расширенный алгоритм Евклида (относительно S) дает

$x^r = S \cdot q_0 + r_1$		$0 - 1 \cdot q_0$	$=$	$-q_0$	$\sigma_1 = q_0$
$S = r_1 \cdot q_1 + r_2$		$1 + q_0 \cdot q_1$	$=$	$1 + q_0 q_1$	$\sigma_2 = \sigma_1 q_1 + 1$
$r_1 = r_2 \cdot q_2 + r_3$		$-q_0 - (1 + q_0 q_1) \cdot q_2$	$=$	$-(q_0 + (1 + q_0 q_1) q_2)$	$\sigma_3 = \sigma_2 q_2 + \sigma_1$
$r_2 = r_3 \cdot q_3 + r_5$	$(1 + q_0 q_1) + (q_0 + (1 + q_0 q_1) q_2) \cdot q_2$		$=$	σ_4	$\sigma_4 = \sigma_3 q_3 + \sigma_2$
...		...	...	...	...

Этот коэффициент Безу и является полиномом локаторов:

$$\sigma_{n+1} = \sigma_n q_n + \sigma_{n-1},\ \sigma_0 = 1,\ \sigma_{-1} = 0.$$

★ 1 ошибка

$$\sigma_1 = \sigma_0 q_0 = q_0$$

Т.к.

$$x^r = x^3 \qquad \text{и} \qquad S(x) = 1 + S_1 x + S_2 x^2 = 1 + S_1 x + S_1^2 x^2$$

найдем q_0

$$\begin{aligned} x^r &= S \cdot q_0 + r_1 \\ x^3 &= (1 + S_1 x + S_1^2 x^2) \left(\frac{1 + S_1 x}{S_1^3} \right) + \frac{1}{S_1^3} \end{aligned}$$

т.е. $q_0 = \frac{1 + S_1 x}{S_1^3}$ тогда $\Sigma = 1 + S_1 x$

★ 2 ошибки

$$\sigma_2 = \sigma_1 q_1 + \sigma_0 = q_0 q_1 + 1$$

нам необходимо найти q_0 и q_1 из последовательности выражений

$$\begin{aligned} x^r &= S \cdot q_0 + r_1 \\ S &= r_1 \cdot q_1 + r_2 \end{aligned}$$

Т.к.

$$x^r = x^5 \qquad \text{и} \qquad S(x) = 1 + S_1 x + S_1^2 x^2 + S_3 x^3 + S_1^4 x^2$$

получим

$$\begin{aligned} x^5 &= (1 + S_1x + S_1^2x^2 + S_3x^3 + S_1^4x^2)\left(\frac{S_3 + S_1^4x}{S_1}\right) \\ &+ \frac{S_3 + (S_1S_3 + S_1^4)x + (S_1^5 + S_1^2S_3)x + (S_1^5 + S_1^2S_3)x^2}{S_1} \end{aligned}$$

т.е. $q_0 = \frac{S_3+S_1^4x}{S_1}$.

Далее

$$\begin{aligned} & 1 + xS_1 + x^2S_1^2 + x^3S_3 + x^4S_1^4 = \\ &= \frac{S_3 + x\left(S_1^4 + S_1S_3\right) + x^2\left(S_1^5 + S_1^2S_3\right) + x^3\left(S_1^6 + S_3^2\right)}{S_1^8} \times \\ &\times \left(\frac{S_1^{14} + xS_1^{15} + S_1^{11}S_3 + xS_1^{12}S_3 + S_1^8s_3^2}{S_1^9 + S_1^6S_3 + S_1^3S_3^2 + S_3^3}\right) + \\ &+ \frac{S_1^9 + x^2S_1^{11} + x^2S_1^8S_3}{S_1^9 + S_1^6S_3 + S_1^3S_3^2 + S_3^3} \end{aligned}$$

т.е.

$$q_1 = \left(\frac{S_1^{14} + xS_1^{15} + S_1^{11}S_3 + xS_1^{12}S_3 + S_1^8S_3^2}{S_1^9 + S_1^6S_3 + S_1^3S_3^2 + S_3^3}\right)$$

тогда

$$\begin{aligned} 1 + q_0q_1 &= 1 + \frac{S_3 + S_1^4x}{S_1}\left(\frac{S_1^{14} + xS_1^{15} + S_1^{11}S_3 + xS_1^{12}S_3 + S_1^8S_3^2}{S_1^9 + S_1^6S_3 + S_1^3S_3^2 + S_3^3}\right) \\ &= \frac{S_1^2(1 + S_1x + x^2(S_1^2 + S_1^{-1}S_3))}{S_1^9 + S_1^6S_3 + S_1^3S_3^2 + S_3^3} \end{aligned}$$

и

$$\Sigma_2 = 1 + S_1x + (S_1^2 + S_1^{-1}S_3)x^2$$

★ 3 ошибки

$$\Sigma_3 = \sigma_2q_2 + \sigma_1 = q_0q_1q_2 + q_0 + q_2$$

★ 4 ошибки

$$\Sigma_4 = \sigma_3q_3 + \sigma_2 = q_0q_1q_2q_3 + q_0q_3 + q_2q_3 + q_1q_0 + 1$$

3.8 Совершенные недвоичные коды

3.8.1 Введение

Пусть $q \neq 2$ - степень простого числа. Известно [1], что при $k \neq 0, n$ не существует совершенного кода $[n, k, d]_q$, отличного от

$$\left[n = \frac{q^m - 1}{q - 1}, n - m, 3\right]_q \qquad \text{и} \qquad [11, 6, 5]_3.$$

Все совершенные двоичные коды могут быть построены методом Хэмминга [2]. Для совершенных недвоичных кодов над $\mathbb{Z}_p$ математических проблем не возникает. Построение же кодов над $GF(p^m)$ требует разработки новых методов. Это связано с тем, что кольцо $\mathbb{Z}_{p^m}$ не является полем. Так в [3] для кодирования в $GF(2^m)$ предлагается использовать дискретное преобразование Фурье. Для построения кода Рида-Соломона в [4] вводятся специфические законы сложения и умножения. Однако полученные коды имеют, соответственно, параметры $[n, k] = [2^m, 2^{m-1}]$ и $[n, k] = [2^m - 1, 2^m - 3]$ и не являются совершеннными. Несмотря на сомнительную практическую значимость, работы по созданию новых кодов над полями малых размерностей ведутся достаточно интенсивно [5], поскольку дают взможность отработать новые алгоритмы и методы. Аналогично, одной из основных причин пристального внимания к совершеннным кодам является то, что они нередко становятся базисными для построения других кодов. Удачно построенный алгоритм позволяет оставаться вблизи границы Синглтона даже при значительном расширении и изменении совершенного кода. В настоящей работе предлагается простой алгоритм построения совершенного кода над $GF(2^m)$.

3.8.2 Совершенный код в $GF(2^2)$

Построим таблицу умножения для элементов из поля Галуа $GF(2^2)$. Для этого предварительно найдем остатки от деления степеней x^n на примитивный полином
$p(x) = x^2 + x + 1$:

$$\left[\frac{x^0}{p(x)}\right] = 1 = 001; \qquad \left[\frac{x^1}{p(x)}\right] = x = 010$$

$$\left[\frac{x^2}{p(x)}\right] = x^2 = 011; \qquad \left[\frac{x^3}{p(x)}\right] = x + 1 = 001$$

Учитывая, что в десятичной записи

$$001 = 1,\ 010 = 2,\ 011 = 3$$

из этих остатков составим таблицу индексов для $GF(2^2)$

n	0	1	2	3
2^n	1	2	3	1
ind n	3	0	1	2

Теперь, пользуясь таблицей индексов несложно построить таблицу умножения для $GF(2^2)$:

$+$	**1**	**2**	**3**
1	0	3	2
2	3	0	1
3	2	1	0

$\times$	**1**	**2**	**3**
1	1	2	3
2	2	3	1
3	3	1	2

Таблица сложения строится как побитовое сложение элементов по модулю 2.

Совершенный код в $GF(2^2)$ имеет параметры $[n,k]=[5,3]$. Рассмотрим правила построения проверочных символов $(e_1\,e_2)$ по известным информационным $(a_1a_2a_3)$:

$$e_1=\sum_{k=1}^{3}a_k,\qquad e_2=\sum_{k=1}^{3}ka_k$$

Передаваемая кодовая комбинация теперь имеет вид

$$\mathbf{F}=(a_1a_2a_3e_1e_2).$$

Допустим в кодовой комбинации возникла одна ошибка:

$$\overline{\mathbf{F}}=(\overline{a}_1\overline{a}_2\overline{a}_3\overline{e}_1\overline{e}_2).$$

Тогда значение ошибки E вычисляется по формуле

$$E=\overline{e}_1+e_1,$$

где $e_1=\sum\limits_{k=1}^{3}\overline{a}_k$, а позиция ошибки j

$$j=\frac{\overline{e}_2+e_2}{E},$$

где $e_2=\sum\limits_{k=1}^{3}k\overline{e}_k$. Если $j=0$ или $E=0$, то ошибка в проверочных символах.

Пример 39. Закодировать сообщение $\boldsymbol{a}=(321)$.

Решение. Пользуясь таблицами сложения и умножения поля $GF(2^2)$ найдем проверочные символы

$$e_1=\sum a_k=3+2+1=0,\qquad e_2=\sum ka_k=1\cdot3+2\cdot2+3\cdot1=3+3+3=3.$$

Т.о. кодовая комбинация принимает вид $\mathbf{F}=(32103)$. ▲

Допустим во время передачи информации в сообщении появилась ошибка во 2-м символе

$$\overline{\mathbf{F}}=(3\mathbf{1}103).$$

Пример 40. Обнаружить и исправить ошибку в сообщении $\overline{\mathbf{F}}=(31103)$.

Решение. Из принятой кодовой комбинации имеем ($\overline{e}_1 = 0, \overline{e}_2 = 3$). Пользуясь таблицами сложения и умножения поля $GF(2^2)$ найдем новые проверочные символы

$$e_1 = \sum \overline{a}_k = 3 + 1 + 1 = 3, \qquad e_2 = \sum k\overline{a}_k = 1 \cdot 3 + 2 \cdot 1 + 3 \cdot 1 = 3 + 2 + 3 = 2.$$

Тогда значение ошибки E вычисляется по формуле

$$E = \overline{e}_1 + e_1 = 0 + 3 = 3,$$

а позиция ошибки j

$$j = \frac{\overline{e}_2 + e_2}{E} = \frac{3+2}{E} = \frac{1}{3} = 2.$$

Прибавляя $E = 3$ ко второму символу $a_2 + E = 1 + 3 = 2$ получим информационную комбинацию $\boldsymbol{a} = (321)$. ▲

Задача 3.23. Обнаружить и исправить единичную ошибку совершенного кода [n,k]=[5,3] в $GF(2^2)$.

N	F	N	F	N	F	N	F
1	$(2,2,1,1,3)$	9	$(3,2,2,2,0)$	17	$(2,0,2,2,0)$	25	$(3,1,2,1,3)$
2	$(1,2,2,2,0)$	10	$(2,1,0,1,1)$	18	$(3,3,3,1,3)$	26	$(1,0,3,0,2)$
3	$(0,2,2,2,0)$	11	$(3,2,3,1,3)$	19	$(2,3,1,2,2)$	27	$(0,3,0,2,2)$
4	$(2,1,1,1,1)$	12	$(3,3,1,1,3)$	20	$(1,3,1,0,2)$	28	$(1,0,2,0,2)$
5	$(3,0,3,1,3)$	13	$(3,2,0,1,3)$	21	$(1,2,1,1,3)$	29	$(3,1,0,1,3)$
6	$(1,2,1,0,2)$	14	$(3,3,1,2,2)$	22	$(3,0,1,1,3)$	30	$(2,1,2,2,0)$
7	$(1,3,1,2,2)$	15	$(2,3,2,1,0)$	23	$(3,2,3,1,3)$	31	$(0,2,1,1,3)$
8	$(2,2,3,2,0)$	16	$(2,1,3,1,1)$	24	$(3,1,1,1,3)$	32	$(3,1,1,1,3)$

3.8.3 Совершенный код в $GF(2^3)$

Совершенный код в $GF(2^3)$ имеет параметры $[n,k] = [9,7]$. Рассмотрим правила построения проверочных символов ($e_1\, e_2$) по известным информационным ($a_1 a_2 ... a_7$):

$$e_1 = \sum_{k=1}^{7} a_k, \qquad e_2 = \sum_{k=1}^{7} k a_k$$

Передаваемая кодовая комбинация теперь имеет вид

$$\mathbf{F} = (a_1 a_2 a_3 a_4 a_5 a_6 a_7 e_1 e_2).$$

Допустим в кодовой комбинации возникла одна ошибка:

$$\overline{\mathbf{F}} = (\overline{a}_1 \overline{a}_2 \overline{a}_3 \overline{a}_4 \overline{a}_5 \overline{a}_6 \overline{a}_7 \overline{e}_1 \overline{e}_2).$$

Тогда значение ошибки E вычисляется по формуле

$$E = \overline{e}_1 + e_1,$$

где $e_1 = \sum\limits_{k=1}^{7} \overline{a}_k$, а позиция ошибки j

$$j = \frac{\overline{e}_2 + e_2}{E},$$

где $e_2 = \sum\limits_{k=1}^{7} k\overline{e}_k$. Если $j = 0$ или $E = 0$, то ошибка в проверочных символах.

Пример 41. Закодировать сообщение $\boldsymbol{a} = (6543456)$.

Решение. Пользуясь таблицами сложения и умножения поля $GF(2^3)$ найдем проверочные символы

$$e_1 = \sum a_k = 6 + 5 + 4 + 3 + 4 + 5 + 6 = 3,$$

$$e_2 = \sum k a_k = 1 \cdot 6 + 2 \cdot 5 + 3 \cdot 4 + 4 \cdot 3 + 5 \cdot 4 + 6 \cdot 5 + 7 \cdot 6 = 6 + 1 + 7 + 7 + 2 + 3 + 4 = 2$$

Т.о. кодовая комбинация принимает вид $\mathbf{F} = (654345632)$. ▲

Допустим во время передачи информации в сообщении появилась ошибка во 3-м символе

$$\overline{\mathbf{F}} = (65\mathbf{1}345632).$$

Пример 42. Обнаружить и исправить ошибку в сообщении $\overline{\mathbf{F}} = (651345632)$.

Решение. Из принятой кодовой комбинации имеем $(\overline{e}_1 = 3, \overline{e}_2 = 2)$. Пользуясь таблицами сложения и умножения поля $GF(2^3)$ найдем новые проверочные символы

$$e_1 = \sum \overline{a}_k = 6 + 5 + 1 + 3 + 4 + 5 + 6 = 6,$$

$$e_2 = \sum k\overline{a}_k = 1 \cdot 6 + 2 \cdot 5 + 3 \cdot 1 + 4 \cdot 3 + 5 \cdot 4 + 6 \cdot 5 + 7 \cdot 6 = 6 + 1 + 3 + 7 + 2 + 3 + 4 = 6$$

Тогда значение ошибки E вычисляется по формуле

$$E = \overline{e}_1 + e_1 = 3 + 6 = 5,$$

а позиция ошибки j

$$j = \frac{\overline{e}_2 + e_2}{E} = \frac{2 + 6}{E} = \frac{4}{5} = 4 \cdot 2 = 3.$$

Прибавляя $E = 5$ к третьему символу $a_3 + E = 1 + 5 = 4$ выделим информационную комбинацию $\boldsymbol{a} = (6543456)$. ▲

Задача 3.24. Обнаружить и исправить единичную ошибку совершенного кода [n,k]=[9,7] над $GF(2^3)$.

N	F	N	F	N	F
1	$(4,4,4,3,5,2,6,1,6)$	11	$(2,3,2,1,6,4,0,7,6)$	21	$(1,2,3,2,7,5,1,7,2)$
2	$(2,3,5,1,2,3,6,3,3)$	12	$(4,6,4,3,5,2,6,1,6)$	22	$(6,3,2,2,7,0,7,2,7)$
3	$(1,2,0,2,1,5,1,7,2)$	13	$(2,3,4,0,2,3,6,3,3)$	23	$(4,2,4,3,5,2,6,1,6)$
4	$(2,3,2,0,2,3,6,0,0)$	14	$(4,3,5,0,6,7,3,2,0)$	24	$(2,0,4,1,2,3,6,3,3)$
5	$(2,3,2,5,1,4,0,7,6)$	15	$(1,2,3,2,6,5,1,7,2)$	25	$(2,3,2,1,1,4,4,7,6)$
6	$(2,3,4,1,2,3,3,3,3)$	16	$(4,3,2,1,1,1,3,0,5)$	26	$(4,3,2,0,1,6,3,0,5)$
7	$(2,3,2,5,1,3,6,1,6)$	17	$(2,3,2,4,2,3,0,0,0)$	27	$(0,3,5,2,6,7,3,2,0)$
8	$(6,3,2,1,1,6,3,0,5)$	18	$(2,3,4,1,2,6,6,3,3)$	28	$(2,0,2,3,1,3,6,1,6)$
9	$(4,3,5,2,0,7,3,2,0)$	19	$(2,0,5,5,1,3,6,1,6)$	29	$(2,0,2,4,2,3,6,0,0)$
10	$(1,7,2,2,7,0,7,2,7)$	20	$(1,4,2,2,7,0,7,2,7)$	30	$(2,3,4,5,2,3,6,3,3)$

3.9 Коды Рида-Соломона

Коды Рида-Соломона были предложены в 1960 Ирвином Ридом (Irving S. Reed) и Густавом Соломоном (Gustave Solomon), являвшимися сотрудниками Линкольнской лаборатории МТИ. Они использованы на алгоритме декодирования Berlekamp-Massey. Коды Рида-Соломона это блочные коды, которые применяются для исправления ошибок во многих системах:

- устройствах памяти CD, DVD, штриховых кодах,
- беспроводных или мобильных каналах (сотовые телефоны, микроволновые каналы и т.д.)
- спутниковых коммуникацях
- цифровом телевидении DVB (digital video broadcast).
- скоростных модемах ADSL, xDSL.

3.9.1 Исправление 1 ошибки несовершенного кода $[n,k]_q = [7,5]_8$

Как правило пораждающий полином в конечном поле Галуа $GF(2^3)$ имеет вид

$$g(x) = \prod_{i=b}^{b+2t-1} (x \oplus 2^i),$$

где t - количество ошибок, исправляемых кодом, b - произвольная целая константа (обычно 0 или 1).

Пример 3.43. Порождающие полиномы для исправления t=1 ошибки:

b=0:

$$g(x) = \prod_{i=0}^{2t-1}(x \oplus 2^i) = (x \oplus 2^0)(x \oplus 2^1) = x^2 + (1+2)x + (1 \cdot 2) = x^2 + 3x + 2,$$

b=1:

$$g(x) = \prod_{i=1}^{2t}(x \oplus 2^i) = (x \oplus 2^1)(x \oplus 2^2) = x^2 + (2+4)x + (2 \cdot 4) = x^2 + 6x + 3,$$

b=2:

$$g(x) = \prod_{i=2}^{2t+1}(x \oplus 2^i) = (x \oplus 2^2)(x \oplus 2^3) = x^2 + (4+3)x + (4 \cdot 3) = x^2 + 7x + 7. \quad \blacktriangle$$

Здесь мы непосредственно используем таблицы сложения и умножения для поля Галуа $GF(2^3)$. Однако, данные полиномы приводимы по определению и поэтому не формируют совершенных кодов, хотя и удобны в использовании. Сведем для

удобства в таблицу коэффициенты (c_i, d_i), необходимые для формирования проверочных символов по информационным для исправления 1 ошибки:

$$e_1 = \sum_{i=0}^{4} c_i a_i, \qquad e_2 = \sum_{i=0}^{4} d_i a_i,$$

b	$g(x)$	c_i	d_i
0	x^2+3x+2	$(5,2,4,7,3)$	$(4,3,5,6,2)$
1	x^2+6x+3	$(6,7,7,1,6)$	$(2,2,3,1,3)$
2	x^2+7x+7	$(4,4,2,4,7)$	$(1,5,1,3,7)$
3	x^2+5x+1	$(1,5,6,6,5)$	$(5,6,6,5,1)$
4	x^2+1x+4	$(7,3,1,5,1)$	$(7,4,2,4,4)$
5	x^2+2x+6	$(3,1,3,2,2)$	$(6,1,7,7,6)$
6	x^2+4x+5	$(2,6,5,3,4)$	$(3,7,4,2,5)$

Построение кода сводится к следующей последовательности действий.

Представим информационную последовательность $(a_0, a_1, a_2, ..., a_n)$ в виде полинома

$$u(x) = \sum_{i=0}^{n} a_i x^{n-i} = a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + ... + a_{n-1}x + a_n$$

Сдвинем информационную последовательность на $r = 2t$ разрядов влево, для этого умножим информационный полином $u(x)$ на x^r:

$$m(x) = x^r u(x).$$

Разделим полученный полином на порождающий:

$$\frac{m(x)}{g(x)} = C(x) + \frac{R(x)}{g(x)},$$

или

$$m(x) = C(x) \cdot g(x) + R(x).$$

Запишем полином остатков в виде

$$R(x) = \sum_{i=0}^{r} e_i x^{r-i}$$

Передаваемая кодовая комбинация теперь имеет вид

$$F = \boxed{a_0}\boxed{a_1}\boxed{a_2}\boxed{a_3}\boxed{a_4}\boxed{e_1}\boxed{e_2}$$

или

$$F(x) = a_0 x^6 + a_1 x^5 + a_2 x^4 + a_3 x^3 + a_4 x^2 + e_1 x + e_2.$$

Обозначим принятую кодовую комбинацию через

$$\overline{F(x)} = A_6x^6 + A_5x^5 + A_4x^4 + A_3x^3 + A_2x^2 + A_1x + A_0.$$

или $\overline{\mathbf{F}} = (A_6A_5A_4A_3A_2A_1A_0)$.

Допустим, принятая кодовая комбинация $\overline{\mathbf{F}}$ имеет 1 ошибку. Прямой алгебраический метод исправления 1 ошибки заключается в следующем. Находим синдромы ошибки по формулам

$$\begin{aligned} S_0 &= \overline{F(2^b)} = A_6(2^b)^6 + A_5(2^b)^5 + A_4(2^b)^4 + A_3(2^b)^3 + A_2(2^b)^1 + A_1(2^b) + A_0, \\ S_1 &= \overline{F(2^{b+1})} = A_6(2^{b+1})^6 + A_5(2^{b+1})^5 + A_4(2^{b+1})^4 \\ &+ A_3(2^{b+1})^3 + A_2(2^{b+1})^2 + A_1(2^{b+1}) + A_0. \end{aligned}$$

Решая уравнение

$$S_1 = S_0\sigma$$

по таблице индексов для $GF(2^3)$ находим локатор ошибки

$$\lambda = \text{ind } \sigma$$

и значение ошибки

$$S_0 = \sigma^b E.$$

Ошибка величиной E находится на λ месте кодовой последовательности.

Очевидно, что размерность синдрома позволяет локализовать только 7 разрядов, поэтому прямой алгебраический метод применяется для кода [7,5], с пятью информационными символами.

Пример 3.44. Пусть передается информационная последовательность (20105). Для построения кода Рида-Соломона с $\mathbf{b}=\mathbf{0}$, исправляющего одну ошибку сформируем по информационным символам $(a_0, a_1, a_2, a_3, a_4) = (20105)$ проверочные (e_1, e_2):

$$\begin{aligned} e_1 &= 5a_0 + 2a_1 + 4a_2 + 7a_3 + 3a_4, \\ e_2 &= 4a_0 + 3a_1 + 5a_2 + 6a_3 + 2a_4, \end{aligned}$$

или

$$\begin{aligned} e_1 &= 5 \cdot 2 + 2 \cdot 0 + 4 \cdot 1 + 7 \cdot 0 + 3 \cdot 5 = 1 + 4 + 4 = 1, \\ e_2 &= 4 \cdot 2 + 3 \cdot 0 + 5 \cdot 1 + 6 \cdot 0 + 2 \cdot 5 = 3 + 5 + 1 = 7. \end{aligned}$$

Код Рида-Соломона имеет вид $\mathbf{F} = (A_6A_5A_4A_3A_2A_1A_0) = (2010517)$.

Допустим в передаваемой кодовой последовательности возникла ошибка в 3 разряде $\overline{\mathbf{F}} = (201\underline{\mathbf{5}}517)$. Учитывая, что

$$\overline{F(x)} = 2 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 5 \cdot x^3 + 5 \cdot x^2 + 1 \cdot x^1 + 7 \cdot 1,$$

определяем синдром ошибки с помощью выражений

$$S_0 = \overline{F(2^b)}, \qquad \text{и} \qquad S_1 = \overline{F(2^{b+1})}.$$

Поскольку у нас $\mathbf{b}=\mathbf{0}$, то

$$\begin{aligned} S_0 = \overline{F(2^0)} = \overline{F(1)} &= 2\cdot 1^6 + 0\cdot 1^5 + 1\cdot 1^4 + 5\cdot 1^3 + 5\cdot 1^2 + 1\cdot 1 + 7 \\ &= 2+1+5+5+1+7 = 5, \\ S_1 = \overline{F(2^1)} = \overline{F(2)} &= 2\cdot 2^6 + 0\cdot 2^5 + 1\cdot 2^4 + 5\cdot 2^3 + 5\cdot 2^2 + 1\cdot 2 + 7, \\ &= 2\cdot 5 + 0\cdot 7 + 1\cdot 6 + 5\cdot 3 + 5\cdot 4 + 1\cdot 2 + 7, \\ &= 1+6+4+2+2+7 = 4. \end{aligned}$$

Для определения локатора ошибки решаем уравнение

$$S_1 = S_0\sigma, \qquad 4 = 5\sigma \qquad \Rightarrow \qquad \sigma = 4\cdot 5^{-1}.$$

Из таблицы умножения для $GF(2^3)$ видим, что $5\cdot 2 = 1$, т.е. обратным элементом для 5 является 2 (т.е. $5^{-1}=2$):

$$\sigma = 4\cdot 5^{-1} = 4\cdot 2 = 3.$$

По таблице индексов находим локатор ошибки

$$\lambda = \operatorname{ind}\sigma, \qquad \lambda = \operatorname{ind} 3 = 3.$$

Величину ошибки E найдем по формуле

$$S_0 = \sigma^b E, \qquad 5 = 1\cdot E.$$

Т.е. к символу A_3 необходимо прибавить $E=5$:

$$\overline{\mathbf{F}} = (201\underline{\mathbf{5}}517) \to \mathbf{F} = (201\underline{\mathbf{0}}517)$$

и передаваемую информационную последовательность записать в виде $\mathbf{a} = (20105)$[7]. ▲

Пример 3.45. Пусть передается информационная последовательность (54321). Для построения кода Рида-Соломона с $\mathbf{b}=\mathbf{2}$, исправляющего одну ошибку сформируем по информационным символам $(a_0, a_1, a_2, a_3, a_4) = (54321)$ проверочные (e_1, e_2). Учитывая что для $\mathbf{b}=\mathbf{2}$ по таблице $\mathbf{c} = (44247)$, $\mathbf{d} = (15137)$ получим

$$\begin{aligned} e_1 &= (\boldsymbol{a}\cdot\mathbf{c}) = (54321)(44247), \\ e_2 &= (\boldsymbol{a}\cdot\mathbf{d}) = (54321)(15137) \end{aligned}$$

[7]Данный результат $\mathbf{F} = (2010517)$ можно проверить следующими способами.
a) Если для $\boldsymbol{a} = (20105)$ мы получим $e_1 = 1,\ e_2 = 7$, то задача решена правильно.
b) Если для $\mathbf{F} = (2010517)$ мы получим $S_0 = 0,\ S_1 = 0$, то задача решена правильно.

или

$$\begin{aligned} e_1 &= 5\cdot 4+4\cdot 4+3\cdot 2+2\cdot 4+1\cdot 7=2+6+6+3+7=6,\\ e_2 &= 5\cdot 1+4\cdot 5+3\cdot 1+2\cdot 3+1\cdot 7=5+2+3+6+7=5. \end{aligned}$$

Код Рида-Соломона имеет вид $\mathbf{F}=(A_6A_5A_4A_3A_2A_1A_0)=(5432165)$.

Допустим в передаваемой кодовой последовательности возникла ошибка в 5 разряде $\overline{\mathbf{F}}=(5\underline{\mathbf{7}}32165)$. Учитывая, что

$$\overline{F(x)}=5\cdot x^6+7\cdot x^5+3\cdot x^4+2\cdot x^3+1\cdot x^2+6\cdot x^1+5\cdot 1,$$

определяем синдром ошибки с помощью выражений

$$S_0=\overline{F(2^b)},\qquad \text{и}\qquad S_1=\overline{F(2^{b+1})}.$$

Поскольку у нас $\mathbf{b}=\mathbf{2}$, то

$$\begin{aligned} S_0=\overline{F(2^2)}=\overline{F(4)} &= 5\cdot 4^6+7\cdot 4^5+3\cdot 4^4+2\cdot 4^3+1\cdot 4^2+6\cdot 4+5\\ &= 5\cdot 7+7\cdot 3+3\cdot 2+2\cdot 5+1\cdot 6+6\cdot 4+5\\ &= 6+2+6+1+6+5+5=5,\\ S_1=\overline{F(2^3)}=\overline{F(3)} &= 5\cdot 3^6+7\cdot 3^5+3\cdot 3^4+2\cdot 3^3+1\cdot 3^2+6\cdot 3+5\\ &= 5\cdot 3^6+7\cdot 3^5+3\cdot 3^4+2\cdot 3^3+1\cdot 3^2+6\cdot 3+5\\ &= 5\cdot 6+7\cdot 2+3\cdot 7+2\cdot 4+1\cdot 5+6\cdot 3+5\\ &= 3+5+2+3+5+1+5=6. \end{aligned}$$

Для определения локатора ошибки решаем уравнение

$$S_1=S_0\sigma,\qquad 6=5\sigma\qquad\Rightarrow\qquad \sigma=7.$$

По таблице индексов находим локатор ошибки

$$\lambda=\operatorname{ind}\sigma,\qquad \lambda=\operatorname{ind}7=5.$$

Т.е. ошибка в символе A_5. Величину ошибки E найдем по формуле

$$S_0=\sigma^bE,\qquad 5=7^2\cdot E=3\cdot E\qquad\Rightarrow\qquad E=3.$$

Т.е. к символу A_5 необходимо прибавить $E=3$:

$$\overline{\mathbf{F}}=(5\underline{\mathbf{7}}32165)\to\mathbf{F}=(5\underline{\mathbf{4}}32165)$$

и передаваемую информационную последовательность записать в виде $\boldsymbol{a}=(54321)$. ▲

Задача 3.25. Обнаружить и исправить ошибку в информационной кодовой комбинации RSC[7,5] сформированной производящим полиномом $g(x)$ поля $GF(2^3)$.

N	$g(x)$	F	N	$g(x)$	F_i
1	x^2+3x+2	$(2,0,1,7,5,7,4)$	16	x^2+6x+3	$(7,0,1,7,5,6,3)$
2	x^2+6x+3	$(5,6,1,5,5,7,2)$	17	x^2+7x+7	$(5,6,3,5,7,0,5)$
3	x^2+7x+7	$(6,3,3,4,2,7,4)$	18	x^2+5x+1	$(6,6,1,7,5,5,2)$
4	x^2+5x+1	$(4,5,1,3,1,5,3)$	19	x^2+1x+4	$(7,0,4,5,2,6,1)$
5	x^2+1x+4	$(5,5,4,4,2,2,2)$	20	x^2+2x+6	$(4,5,1,7,3,5,7)$
6	x^2+2x+6	$(6,4,1,0,7,4,7)$	21	x^2+4x+5	$(1,0,0,5,2,2,1)$
7	x^2+4x+5	$(7,0,0,4,2,6,2)$	22	x^2+3x+2	$(4,0,3,7,5,7,0)$
8	x^2+3x+2	$(2,5,1,7,4,5,2)$	23	x^2+6x+3	$(6,5,1,4,5,5,3)$
9	x^2+6x+3	$(0,3,1,5,4,4,1)$	24	x^2+7x+7	$(6,6,2,5,6,2,0)$
10	x^2+7x+7	$(4,5,6,3,4,5,6)$	25	x^2+5x+1	$(7,5,3,4,5,6,5)$
11	x^2+5x+1	$(5,3,1,5,5,6,4)$	26	x^2+1x+4	$(0,3,1,5,6,1,2)$
12	x^2+1x+4	$(6,3,5,3,5,1,7)$	27	x^2+2x+6	$(1,0,3,4,3,4,6)$
13	x^2+2x+6	$(7,4,1,5,2,7,4)$	28	x^2+4x+5	$(2,4,4,5,5,2,5)$
14	x^2+4x+5	$(1,5,1,3,5,4,2)$	29	x^2+3x+2	$(2,3,1,1,3,4,4)$
15	x^2+3x+2	$(3,4,2,1,5,2,1)$	30	x^2+6x+3	$(5,4,3,2,1,5,0)$

3.9.2 Исправление 2 ошибок несовершенного кода $[n,k]_q = [7,3]_8$

Для исправления $t=2$ ошибок мы создаем $r=2t=4$ проверочных символа которые могут принимать $8^4 = 4096$ значений, достаточных для обнаружения 1 и 2 ошибок максимум в $n=13$ разрядах, поскольку:

$$1 + C_{13}^1 7 + C_{13}^2 7^2 = 3914 < 8^4.$$

Расмотрим алгебраический метод декодирования для исправления 2 ошибок.

Пример 3.46. Порождающие полиномы для исправления t=2 ошибок:
b=0:

$$\begin{aligned} g(x) &= \prod_{i=0}^{2t-1}(x \oplus 2^i) = \prod_{i=0}^{3}(x \oplus 2^i) = (x \oplus 2^0)(x \oplus 2^1)(x \oplus 2^2)(x \oplus 2^3) \\ &= (x \oplus 1)(x \oplus 2)(x \oplus 4)(x \oplus 3) = x^4 + (1+2+4+3)x^3 \\ &\quad +(1\cdot 2 + 1\cdot 4 + 1\cdot 3 + 2\cdot 4 + 2\cdot 3 + 4\cdot 3)x^2 \\ &\quad +(1\cdot 2\cdot 4 + 1\cdot 2\cdot 3 + 1\cdot 4\cdot 3 + 2\cdot 4\cdot 3)x + 1\cdot 2\cdot 4\cdot 3 \\ &= x^4 + 4x^3 + (2+4+3+3+6+7)x^2 + (3+6+7+5)x + 5 \\ &= x^4 + 4x^3 + 7x^2 + 7x + 5 \end{aligned}$$

b=1:

$$\begin{aligned} g(x) &= \prod_{i=1}^{2t}(x \oplus 2^i) = \prod_{i=1}^{4}(x \oplus 2^i) = (x \oplus 2^1)(x \oplus 2^2)(x \oplus 2^3)(x \oplus 2^4) \\ &= (x \oplus 2)(x \oplus 4)(x \oplus 3)(x \oplus 6) = x^4 + 3x^3 + 4x^2 + 2x + 3 \end{aligned}$$

b=2:

$$\begin{aligned} g(x) &= \prod_{i=2}^{2t+1}(x \oplus 2^i) = \prod_{i=2}^{5}(x \oplus 2^i) = (x \oplus 2^2)(x \oplus 2^3)(x \oplus 2^4)(x \oplus 2^5) \\ &= (x \oplus 4)(x \oplus 3)(x \oplus 6)(x \oplus 7) = x^4 + 6x^3 + 4x^2 + 6x + 1 \quad \blacktriangle \end{aligned}$$

Сведем для удобства в таблицу коэффициенты (c_i, d_i, h_i, f_i), необходимые для формирования проверочных символов по информационным для исправления 2 ошибок:

$$e_1 = \sum a_k c_k, \quad e_2 = \sum a_k d_k, \quad e_3 = \sum a_k h_k, \quad e_4 = \sum a_k f_k$$

b	$g(x)$	c_i	d_i	h_i	f_i
0	$x^4+4x^3+7x^2+7x+5$	$(2,1,4)$	$(3,6,7)$	$(5,4,7)$	$(5,2,5)$
1	$x^4+3x^3+x^2+2x+3$	$(6,4,3)$	$(1,1,1)$	$(6,5,2)$	$(7,5,3)$
2	$x^4+6x^3+4x^2+6x+1$	$(1,6,6)$	$(6,3,4)$	$(4,3,6)$	$(6,6,1)$
3	$x^4+7x^3+6x^2+x+6$	$(3,5,7)$	$(2,5,6)$	$(1,1,1)$	$(3,4,6)$
4	$x^4+5x^3+5x^2+3x+2$	$(5,2,5)$	$(7,4,5)$	$(7,6,3)$	$(4,1,2)$
5	$x^4+x^3+2x^2+5x+7$	$(4,3,1)$	$(4,7,2)$	$(3,2,5)$	$(2,7,7)$
6	$x^4+2x^3+3x^2+4x+4$	$(7,7,2)$	$(5,2,3)$	$(2,7,4)$	$(1,3,4)$

Для исправления 2 ошибок возьмем 4 проверочных разряда. Передаваемая кодовая комбинация теперь имеет вид

$$\mathbf{F} = \left|\, a_0 \,\middle|\, a_1 \,\middle|\, a_2 \,\middle\|\, e_1 \,\middle|\, e_2 \,\middle|\, e_3 \,\middle|\, e_4 \,\right|$$

или

$$F(x) = a_0x^6 + a_1x^5 + a_2x^4 + e_1x^3 + e_2x^2 + e_3x + e_4.$$

Допустим, принятая кодовая комбинация

$$\overline{F(x)} = A_6x^6 + A_5x^5 + A_4x^4 + A_3x^3 + A_2x^2 + A_1x + A_0.$$

имеет 2 ошибки. Прямой алгебраический метод исправления 2 ошибок заключается в следующем. Находим синдромы ошибки по формулам

$$S_k = \overline{F(2^{b+k})}.$$

Например, для $\mathbf{b}=\mathbf{0}$, получим

$$\begin{aligned}
S_0 = \overline{F(2^0)} &= \overline{F(1)} = A_6 1^6 + A_5 1^5 + A_4 1^4 + A_3 1^3 + A_2 1^2 + A_1 1^1 + A_0,\\
S_1 = \overline{F(2^1)} &= \overline{F(2)} = A_6 2^6 + A_5 2^5 + A_4 2^4 + A_3 2^3 + A_2 2^2 + A_1 2^1 + A_0,\\
S_2 = \overline{F(2^2)} &= \overline{F(4)} = A_6 4^6 + A_5 4^5 + A_4 4^4 + A_3 4^3 + A_2 4^2 + A_1 4^1 + A_0,\\
S_3 = \overline{F(2^3)} &= \overline{F(3)} = A_6 3^6 + A_5 3^5 + A_4 3^4 + A_3 3^3 + A_2 3^2 + A_1 3^1 + A_0.
\end{aligned}$$

Решая уравнение

$$\begin{pmatrix} S_2 \\ S_3 \end{pmatrix} = \begin{pmatrix} S_0 & S_1 \\ S_1 & S_2 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix}$$

находим многочлен локаторов ошибок

$$\sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2 = \prod_{k=1}^{\nu} (1 + \alpha_k x)$$

корни которого равны обратным величинам локаторов ошибок.

Для нахождения значения ошибок наобходимо решить систему

$$\begin{pmatrix} S_0 \\ S_1 \end{pmatrix} = \begin{pmatrix} \alpha_1^b & \alpha_2^b \\ \alpha_1^{b+1} & \alpha_2^{b+1} \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}$$

Ошибка величиной $E_k = \mathrm{ind}(e_k)$ находится на $\lambda_k = \mathrm{ind}(\sigma_k)$ месте кодовой последовательности.

Очевидно, что размерность синдрома позволяет локализовать только 7 разрядов, поэтому прямой алгебраический метод применяется для кода [7,3], с тремя информационными символами.

Пример 3.47. Пусть передается информационная последовательность (753). Для построения кода Рида-Соломона с $\mathbf{b}=\mathbf{0}$, исправляющего две ошибки сформируем по информационным символам $(a_0, a_1, a_2) = (753)$ проверочные (e_1, e_2, e_3, e_4):

$$e_1 = \sum a_k c_k, \quad e_2 = \sum a_k d_k, \quad e_3 = \sum a_k h_k, \quad e_4 = \sum a_k f_k$$

или

$$\begin{aligned} e_1 &= 2a_1 + 1a_2 + 4a_3 = 2 \cdot 7 + 1 \cdot 5 + 4 \cdot 3 = 5 + 5 + 7 = 7, \\ e_2 &= 3a_1 + 6a_2 + 7a_3 = 3 \cdot 7 + 6 \cdot 5 + 7 \cdot 3 = 2 + 3 + 2 = 3, \\ e_3 &= 5a_1 + 4a_2 + 7a_3 = 5 \cdot 7 + 4 \cdot 5 + 7 \cdot 3 = 6 + 2 + 2 = 6, \\ e_4 &= 5a_1 + 2a_2 + 5a_3 = 5 \cdot 7 + 2 \cdot 5 + 5 \cdot 3 = 6 + 1 + 4 = 3. \end{aligned}$$

Код Рида-Соломона для данной информационной последовательности имеет вид $\mathbf{F} = (7537363)$.

Допустим в передаваемой кодовой последовательности возникли ошибки в 4 и 5 разряде $\mathbf{F} = (7\underline{\mathbf{53}}7363) \Rightarrow \overline{\mathbf{F}} = (7\underline{\mathbf{66}}7363)$. Учитывая, что

$$\overline{F(x)} = 7 \cdot x^6 + 6 \cdot x^5 + 6 \cdot x^4 + 7 \cdot x^3 + 3 \cdot x^2 + 6 \cdot x^1 + 3 \cdot 1,$$

определяем синдром ошибки с помощью выражений

$$\begin{aligned} S_0 = \overline{F(2^b)} &= 7 \cdot 1^6 + 6 \cdot 1^5 + 6 \cdot 1^4 + 7 \cdot 1^3 + 3 \cdot 1^2 + 6 \cdot 1 + 3 = 6 \\ S_1 = \overline{F(2^{b+1})} &= 7 \cdot 2^6 + 6 \cdot 2^5 + 6 \cdot 2^4 + 7 \cdot 2^3 + 3 \cdot 2^2 + 6 \cdot 2 + 3 = 1, \\ S_2 = \overline{F(2^{b+2})} &= 7 \cdot 4^6 + 6 \cdot 4^5 + 6 \cdot 4^4 + 7 \cdot 4^3 + 3 \cdot 4^2 + 6 \cdot 4 + 3 = 4, \\ S_3 = \overline{F(2^{b+3})} &= 7 \cdot 3^6 + 6 \cdot 3^5 + 6 \cdot 3^4 + 7 \cdot 3^3 + 3 \cdot 3^2 + 6 \cdot 3 + 3 = 0. \end{aligned}$$

Для определения локатора ошибки нам необходимо решить систему

$$\begin{pmatrix} S_2 \\ S_3 \end{pmatrix} = \begin{pmatrix} S_0 & S_1 \\ S_1 & S_2 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix}$$

или

$$\begin{pmatrix} 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 6 & 1 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix}.$$

Методом Крамера, получим

$$\Delta = \begin{vmatrix} 6 & 1 \\ 1 & 4 \end{vmatrix} = 6 \cdot 4 - 1 \cdot 1 = 5 + 1 = 4$$

$$\Delta_2 = \begin{vmatrix} 4 & 1 \\ 0 & 4 \end{vmatrix} = 4 \cdot 4 - 0 \cdot 1 = 6 + 0 = 6$$

$$\Delta_1 = \begin{vmatrix} 6 & 4 \\ 1 & 0 \end{vmatrix} = 6 \cdot 0 - 1 \cdot 4 = 0 + 4 = 4$$

Из таблицы умножения для $GF(2^3)$ видим, что $4 \cdot 7 = 1$, т.е. обратным элементом для 4 является 7. Тогда

$$\sigma_2 = \frac{\Delta_2}{\Delta} = \frac{6}{4} = 6 \cdot 7 = 4, \quad \sigma_1 = \frac{\Delta_1}{\Delta} = \frac{4}{4} = 4 \cdot 7 = 1.$$

Построим многочлен локаторов ошибки

$$\sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2 = 1 + x + 4x^2.$$

Для решения данного уравнения воспользуемся формулами Виета

$$\left\{ \begin{array}{c} x_1 + x_2 = \sigma_1 \\ x_1 \cdot x_2 = \sigma_2 \end{array} \right. \quad \text{или} \quad \left\{ \begin{array}{c} x_1 + x_2 = 1 \\ x_1 \cdot x_2 = 4 \end{array} \right.$$

По таблицам сложения и умножения для $GF(2^3)$ находим $x_1 = 6,\ x_2 = 7$, тогда

$$\sigma(x) = 1 + x + 4x^2 = (1 + 6x)(1 + 7x) = (1 + 2^4 x)(1 + 2^5 x).$$

и ошибки локализованы в разрядах

$$\lambda_1 = \text{ind}\, x_1 = \text{ind}\, 6 = 4 \quad \text{и} \quad \lambda_2 = \text{ind}\, x_2 = \text{ind}\, 7 = 5.$$

Т.е. ошибки в символах A_4 и A_5 (коэффициенты при степенях x^4 и x^5) полинома $\overline{F(x)}$.

Для нахождения значения ошибок решим систему

$$\left(\begin{array}{c} S_0 \\ S_1 \end{array} \right) = \left(\begin{array}{cc} x_1^b & x_2^b \\ x_1^{b+1} & x_2^{b+1} \end{array} \right) \left(\begin{array}{c} e_1 \\ e_2 \end{array} \right)$$

или

$$\left(\begin{array}{c} 6 \\ 1 \end{array} \right) = \left(\begin{array}{cc} 1 & 1 \\ 6 & 7 \end{array} \right) \left(\begin{array}{c} e_1 \\ e_2 \end{array} \right)$$

Методом Крамера, получим

$$\Delta = \left| \begin{array}{cc} 1 & 1 \\ 6 & 7 \end{array} \right| = 1 \cdot 7 - 6 \cdot 1 = 7 + 6 = 1$$

$$\Delta_1 = \left| \begin{array}{cc} 6 & 1 \\ 1 & 7 \end{array} \right| = 6 \cdot 7 - 1 \cdot 1 = 4 + 1 = 5$$

$$\Delta_2 = \left| \begin{array}{cc} 1 & 6 \\ 6 & 1 \end{array} \right| = 1 \cdot 1 - 6 \cdot 6 = 1 + 2 = 3$$

Тогда

$$e_1 = \frac{\Delta_1}{\Delta} = \frac{5}{1} = 5, \quad e_2 = \frac{\Delta_2}{\Delta} = \frac{3}{1} = 3.$$

Т.о. мы имеем ошибку в разряде x^4 со значением $E_4 = 5$ и в разряде x^5 со значением $E_5 = 3$. Исправляя ошибки, получим

$$\begin{array}{rcl} \overline{F(x)} & = & 7 \cdot x^6 + \underline{6 \cdot x^5} + \underline{6 \cdot x^4} + 7 \cdot x^3 + 3 \cdot x^2 + 6 \cdot x^1 + 3 \cdot 1, \\ F(x) & = & 7 \cdot x^6 + \underline{(6+3) \cdot x^5} + \underline{(6+5) \cdot x^4} + 7 \cdot x^3 + 3 \cdot x^2 + 6 \cdot x^1 + 3 \cdot 1 \\ & = & 7 \cdot x^6 + \underline{5 \cdot x^5} + \underline{3 \cdot x^4} + 7 \cdot x^3 + 3 \cdot x^2 + 6 \cdot x^1 + 3 \cdot 1 \end{array}$$

или

$$\overline{F(x)} = (7\underline{\mathbf{66}}7363) \quad \Rightarrow \quad F(x) = (7\underline{\mathbf{53}}7363)$$

и исправленная информационная последовательность имеет вид $\boldsymbol{a} = (753)$[8]. ▲

Пример 3.48. Построить код Рида-Соломона, исправляющего 2 ошибки для информационной последовательности $\boldsymbol{a} = (264)$.

Для построения кода Рида-Соломона с $\mathbf{b}=\mathbf{3}$, исправляющего две ошибки сформируем по информационным символам $(a_0, a_1, a_2) = (264)$ проверочные (e_1, e_2, e_3, e_4):

$$e_1 = \sum a_k c_k, \quad e_2 = \sum a_k d_k, \quad e_3 = \sum a_k h_k, \quad e_4 = \sum a_k f_k.$$

Из таблицы коэффициентов для кода $[7, 3]_8$ для $\mathbf{b}=\mathbf{3}$, $g(x) = x^4 + 7x^3 + 6x^2 + x + 6$ имеем:

$$c = (357), \quad d = (256), \quad h = (111), \quad f = (346)$$

или

$$\begin{aligned} e_1 &= (a \cdot c) = 2 \cdot 3 + 6 \cdot 5 + 4 \cdot 7 = 6 + 3 + 1 = 4, \\ e_2 &= (a \cdot d) = 2 \cdot 2 + 6 \cdot 5 + 4 \cdot 6 = 4 + 3 + 5 = 2, \\ e_3 &= (a \cdot h) = 2 \cdot 1 + 6 \cdot 1 + 4 \cdot 1 = 2 + 6 + 4 = 0, \\ e_4 &= (a \cdot f) = 2 \cdot 3 + 6 \cdot 4 + 4 \cdot 6 = 6 + 5 + 5 = 6. \end{aligned}$$

Код Рида-Соломона для данной информационной последовательности имеет вид $\mathbf{F} = (2644206)$.

Допустим в передаваемой кодовой последовательности возникли ошибки в 2 и 6 разряде $\mathbf{F} = (\underline{\mathbf{2}}644\underline{\mathbf{2}}06) \Rightarrow \overline{\mathbf{F}} = (\underline{\mathbf{7}}644\underline{\mathbf{6}}06)$. Учитывая, что

$$\overline{F(x)} = 7 \cdot x^6 + 6 \cdot x^5 + 4 \cdot x^4 + 4 \cdot x^3 + 6 \cdot x^2 + 0 \cdot x^1 + 6 \cdot 1,$$

определяем синдром ошибки при $\mathbf{b}=\mathbf{3}$ с помощью выражений

$$\begin{aligned} S_0 &= \overline{F(2^b)} = \overline{F(2^3)} = \overline{F(3)} \\ &= 7 \cdot 3^6 + 6 \cdot 3^5 + 4 \cdot 3^4 + 4 \cdot 3^3 + 6 \cdot 3^2 + 0 \cdot 3 + 6 \\ &= 7 \cdot 6 + 6 \cdot 2 + 4 \cdot 7 + 4 \cdot 4 + 6 \cdot 5 + 0 \cdot 3 + 6 \\ &= 4 + 7 + 1 + 6 + 3 + 0 + 6 = 1 \end{aligned}$$

$$\begin{aligned} S_1 &= \overline{F(2^{b+1})} = \overline{F(2^4)} = \overline{F(6)} \\ &= 7 \cdot 6^6 + 6 \cdot 6^5 + 4 \cdot 6^4 + 4 \cdot 6^3 + 6 \cdot 6^2 + 0 \cdot 6 + 6 = 1 \\ &= 7 \cdot 3 + 6 \cdot 5 + 4 \cdot 4 + 4 \cdot 7 + 6 \cdot 2 + 0 \cdot 6 + 6 \\ &= 2 + 3 + 6 + 1 + 7 + 0 + 6 = 7, \end{aligned}$$

[8] Данный результат $\mathbf{F} = (7537363)$ можно проверить следующими способами.
a) Если для $\boldsymbol{a} = (753)$ мы получим $e = (7363)$, то задача решена правильно.
b) Если для $\mathbf{F} = (7537363)$ мы получим $S_0 = S_1 = S_2 = S_3 = 0$, то задача решена правильно.

$$\begin{aligned} S_2 &= \overline{F(2^{b+2})} = \overline{F(2^5)} = \overline{F(7)} \\ &= 7\cdot 7^6 + 6\cdot 7^5 + 4\cdot 7^4 + 4\cdot 7^3 + 6\cdot 7^2 + 0\cdot 7 + 6 \\ &= 7\cdot 4 + 6\cdot 6 + 4\cdot 5 + 4\cdot 2 + 6\cdot 3 + 0\cdot 7 + 6 \\ &= 1 + 2 + 2 + 3 + 1 + 0 + 6 = 5, \end{aligned}$$

$$\begin{aligned} S_3 &= \overline{F(2^{b+3})} = \overline{F(2^6)} = \overline{F(5)} \\ &= 7\cdot 5^6 + 6\cdot 5^5 + 4\cdot 5^4 + 4\cdot 5^3 + 6\cdot 5^2 + 0\cdot 5 + 6 \\ &= 7\cdot 2 + 6\cdot 4 + 4\cdot 3 + 4\cdot 6 + 6\cdot 7 + 0\cdot 5 + 6 \\ &= 5 + 5 + 7 + 5 + 4 + 0 + 6 = 0. \end{aligned}$$

Для определения локатора ошибки нам необходимо решить систему

$$\begin{pmatrix} S_2 \\ S_3 \end{pmatrix} = \begin{pmatrix} S_0 & S_1 \\ S_1 & S_2 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix}$$

или

$$\begin{pmatrix} 5 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 7 \\ 7 & 5 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix}.$$

Методом Крамера, получим

$$\Delta = \begin{vmatrix} 1 & 7 \\ 7 & 5 \end{vmatrix} = 1\cdot 5 - 7\cdot 7 = 5 + 3 = 6$$

$$\Delta_2 = \begin{vmatrix} 5 & 7 \\ 0 & 5 \end{vmatrix} = 5\cdot 5 - 0\cdot 7 = 7 + 0 = 7$$

$$\Delta_1 = \begin{vmatrix} 1 & 5 \\ 7 & 0 \end{vmatrix} = 1\cdot 0 - 7\cdot 5 = 0 + 6 = 6$$

Из таблицы умножения для $GF(2^3)$ видим, что $6\cdot 3 = 1$, т.е. обратным элементом для 6 является 3. Тогда

$$\sigma_2 = \frac{\Delta_2}{\Delta} = \frac{7}{6} = 7\cdot 3 = 2, \quad \sigma_1 = \frac{\Delta_1}{\Delta} = \frac{6}{6} = 6\cdot 3 = 1.$$

Построим многочлен локаторов ошибки

$$\sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2 = 1 + x + 2x^2.$$

Для решения данного уравнения воспользуемся формулами Виета

$$\begin{cases} x_1 + x_2 = \sigma_1 \\ x_1 \cdot x_2 = \sigma_2 \end{cases} \quad \text{или} \quad \begin{cases} x_1 + x_2 = 1 \\ x_1 \cdot x_2 = 2 \end{cases}$$

По таблицам сложения и умножения для $GF(2^3)$ находим $x_1 = 4,\ x_2 = 5$, тогда

$$\sigma(x) = 1 + x + 2x^2 = (1 + 4x)(1 + 5x) = (1 + 2^2 x)(1 + 2^6 x).$$

и ошибки локализованы в разрядах

$$\lambda_1 = \operatorname{ind} x_1 = \operatorname{ind} 4 = 2 \quad \text{и} \quad \lambda_2 = \operatorname{ind} x_2 = \operatorname{ind} 5 = 6.$$

Т.е. ошибки в символах A_2 и A_6 (коэффициенты при степенях x^2 и x^6) полинома $\overline{F(x)}$.

Для нахождения значения ошибок решим систему

$$\begin{pmatrix} S_0 \\ S_1 \end{pmatrix} = \begin{pmatrix} x_1^b & x_2^b \\ x_1^{b+1} & x_2^{b+1} \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}$$

или

$$\begin{pmatrix} 1 \\ 7 \end{pmatrix} = \begin{pmatrix} 4^3 & 5^3 \\ 4^4 & 5^4 \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = \begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}$$

Методом Крамера, получим

$$\Delta = \begin{vmatrix} 5 & 6 \\ 2 & 3 \end{vmatrix} = 5 \cdot 3 - 2 \cdot 6 = 4 + 7 = 3$$

$$\Delta_1 = \begin{vmatrix} 1 & 6 \\ 7 & 3 \end{vmatrix} = 1 \cdot 3 - 7 \cdot 6 = 3 + 4 = 7$$

$$\Delta_2 = \begin{vmatrix} 5 & 1 \\ 2 & 7 \end{vmatrix} = 5 \cdot 7 - 2 \cdot 1 = 6 + 2 = 4$$

Тогда

$$e_1 = \frac{\Delta_1}{\Delta} = \frac{7}{3} = 7 \cdot 6 = 4, \quad e_2 = \frac{\Delta_2}{\Delta} = \frac{4}{3} = 4 \cdot 6 = 5.$$

Т.о. мы имеем ошибку в разряде x^2 со значением $E_2 = 4$ и в разряде x^6 со значением $E_6 = 5$. Исправляя ошибки, получим

$$\mathbf{F} = (\underline{\mathbf{7}}644\underline{\mathbf{6}}06) \Rightarrow \overline{F} = (\underline{\mathbf{2}}644\underline{\mathbf{2}}06)$$

и исправленная информационная последовательность имеет вид $\boldsymbol{a} = (264)$[9]. ▲

Пример 3.49. Обнаружить и исправить ошибки в принятой последовательности $\mathbf{F} = (6254420)$ кода $[n, k] = [7, 3]$ построеной при помощи полинома $\mathbf{b}{=}\mathbf{4}$ в $GF(2^3)$.

Учитывая, что

$$\overline{F(x)} = 6 \cdot x^6 + 2 \cdot x^5 + 5 \cdot x^4 + 4 \cdot x^3 + 4 \cdot x^2 + 2 \cdot x^1 + 0 \cdot 1,$$

определяем синдром ошибки при $\mathbf{b}{=}\mathbf{4}$ с помощью выражений

$$\begin{aligned} S_0 &= \overline{F(2^b)} = \overline{F(2^4)} = \overline{F(6)} \\ &= 6 \cdot 6^6 + 2 \cdot 6^5 + 5 \cdot 6^4 + 4 \cdot 6^3 + 4 \cdot 6^2 + 2 \cdot 6 + 0 \\ &= 6 \cdot 3 + 2 \cdot 5 + 5 \cdot 4 + 4 \cdot 7 + 4 \cdot 2 + 2 \cdot 6 + 0 \\ &= 1 + 1 + 2 + 1 + 3 + 7 + 0 = 7 \end{aligned}$$

[9] Данный результат $\mathbf{F} = (2644206)$ можно проверить следующими способами.

a) Если для $\boldsymbol{a} = (264)$ мы получим $\mathbf{e} = (4206)$, то задача решена правильно.

b) Если для $\mathbf{F} = (2644206)$ мы получим $S_0 = S_1 = S_2 = S_3 = 0$, то задача решена правильно.

$$\begin{aligned} S_1 &= \overline{F(2^{b+1})} = \overline{F(2^5)} = \overline{F(7)} \\ &= 6\cdot 7^6 + 2\cdot 7^5 + 5\cdot 7^4 + 4\cdot 7^3 + 4\cdot 7^2 + 2\cdot 7 + 0 \\ &= 6\cdot 4 + 2\cdot 6 + 5\cdot 5 + 4\cdot 2 + 4\cdot 3 + 2\cdot 7 + 0 \\ &= 5 + 7 + 7 + 3 + 7 + 5 + 0 = 4, \end{aligned}$$

$$\begin{aligned} S_2 &= \overline{F(2^{b+2})} = \overline{F(2^6)} = \overline{F(5)} \\ &= 6\cdot 5^6 + 2\cdot 5^5 + 5\cdot 5^4 + 4\cdot 5^3 + 4\cdot 5^2 + 2\cdot 5 + 0 \\ &= 6\cdot 2 + 2\cdot 4 + 5\cdot 3 + 4\cdot 6 + 4\cdot 7 + 2\cdot 5 + 0 \\ &= 7 + 3 + 4 + 5 + 1 + 1 + 0 = 5, \end{aligned}$$

$$\begin{aligned} S_3 &= \overline{F(2^{b+3})} = \overline{F(2^7)} = \overline{F(1)} \\ &= 6\cdot 1^6 + 2\cdot 1^5 + 5\cdot 1^4 + 4\cdot 1^3 + 4\cdot 1^2 + 2\cdot 1 + 0 \\ &= 6\cdot 1 + 2\cdot 1 + 5\cdot 1 + 4\cdot 1 + 4\cdot 1 + 2\cdot 1 + 0 \\ &= 6 + 2 + 5 + 4 + 4 + 2 + 0 = 3. \end{aligned}$$

Для определения локатора ошибки нам необходимо решить систему

$$\begin{pmatrix} S_2 \\ S_3 \end{pmatrix} = \begin{pmatrix} S_0 & S_1 \\ S_1 & S_2 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix}, \quad \text{или} \quad \begin{pmatrix} 5 \\ 3 \end{pmatrix} = \begin{pmatrix} 7 & 4 \\ 4 & 5 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix}.$$

Методом Крамера, получим

$$\Delta = \begin{vmatrix} 7 & 4 \\ 4 & 5 \end{vmatrix} = 7\cdot 5 - 4\cdot 4 = 6 + 6 = 0$$

$$\Delta_2 = \begin{vmatrix} 5 & 4 \\ 3 & 5 \end{vmatrix} = 5\cdot 5 - 3\cdot 4 = 7 + 7 = 0$$

$$\Delta_1 = \begin{vmatrix} 7 & 5 \\ 4 & 3 \end{vmatrix} = 7\cdot 3 - 4\cdot 5 = 2 + 2 = 0$$

Поскольку главный определитель равен нулю, мы заключаем, что в принятой последовательности произошла только одна ошибка. Для ее локализации решаем уравнение

$$S_1 = \sigma S_0 \quad \text{или} \quad 4 = \sigma 7 \quad \Rightarrow \quad \sigma = 6 = 2^4.$$

Т.е. ошибка локализована в символе A_4 (коэффициент при степени x^4 полинома $\overline{F(x)}$). Значение ошибки находим по формуле

$$S_0 = \sigma^b E \quad \text{или} \quad 7 = 6^4 E = 4E \quad \Rightarrow \quad E = 4^{-1}7 = 7\cdot 7 = 3.$$

Т.о. мы имеем ошибку в разряде x^4 со значением $E_4 = 3$. Исправляя ошибку, получим

$$\mathbf{F} = (62\underline{\mathbf{5}}4420) \Rightarrow \overline{F} = (62\underline{\mathbf{6}}4420)$$

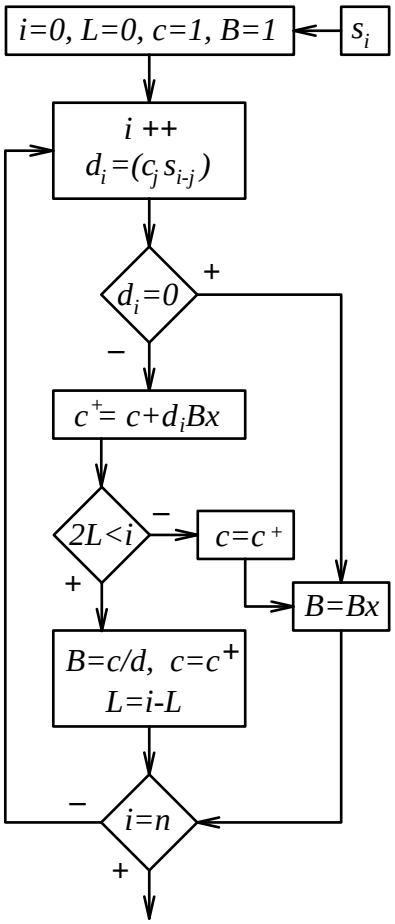
и исправленная информационная последовательность имеет вид $\boldsymbol{a} = (626)$[10]. ▲

Задача 3.26. Обнаружить и исправить 2 ошибки в информационной кодовой комбинации RSC[7,3] сформированной производящим полиномом $g(x)$ поля $GF(2^3)$.

N	$g(x)$	$\overline{F_i}$	**N**	$g(x)$	$\overline{F_i}$
1	$x^4+4x^3+7x^2+7x+5$	(4562373)	16	$x^4+3x^3+1x^2+2x+3$	(1615153)
2	$x^4+3x^3+1x^2+2x+3$	(2732576)	17	$x^4+6x^3+4x^2+6x+1$	(7563113)
3	$x^4+6x^3+4x^2+6x+1$	(1247370)	18	$x^4+7x^3+6x^2+1x+6$	(4431737)
4	$x^4+7x^3+6x^2+1x+6$	(5116230)	19	$x^4+5x^3+5x^2+3x+2$	(4661674)
5	$x^4+5x^3+5x^2+3x+2$	(2325111)	20	$x^4+1x^3+2x^2+5x+7$	(5564312)
6	$x^4+1x^3+2x^2+5x+7$	(3333005)	21	$x^4+2x^3+3x^2+4x+4$	(5471253)
7	$x^4+2x^3+3x^2+4x+4$	(4117765)	22	$x^4+4x^3+7x^2+7x+5$	(2715001)
8	$x^4+4x^3+7x^2+7x+5$	(2453626)	23	$x^4+3x^3+1x^2+2x+3$	(6262477)
9	$x^4+3x^3+1x^2+2x+3$	(0650027)	24	$x^4+6x^3+4x^2+6x+1$	(5525355)
10	$x^4+6x^3+4x^2+6x+1$	(0114252)	25	$x^4+7x^3+6x^2+1x+6$	(3270440)
11	$x^4+7x^3+6x^2+1x+6$	(2421121)	26	$x^4+5x^3+5x^2+3x+2$	(2264425)
12	$x^4+5x^3+5x^2+3x+2$	(3634162)	27	$x^4+1x^3+2x^2+5x+7$	(5253561)
13	$x^4+1x^3+2x^2+5x+7$	(3615206)	28	$x^4+2x^3+3x^2+4x+4$	(2727517)
14	$x^4+2x^3+3x^2+4x+4$	(2264027)	29	$x^4+4x^3+7x^2+7x+5$	(1426013)
15	$x^4+4x^3+7x^2+7x+5$	(3262616)	30	$x^4+3x^3+1x^2+2x+3$	(2535555)

[10] Данный результат $\mathbf{F} = (6264420)$ можно проверить следующими способами.
a) Если для $\boldsymbol{a} = (626)$ мы получим $\mathbf{e} = (4420)$, то задача решена правильно.
b) Если для $\mathbf{F} = (6264420)$ мы получим $S_0 = S_1 = S_2 = S_3 = 0$, то задача решена правильно.

3.10 Алгоритм Берлекемпа-Месси



Алгоритм поиска кратчайшего регистра сдвига с линейной обратной связью для поданной на вход последовательности был предложен Берлекемпом в 1968 г. [1] В следующем 1969 г. Дж.Месси применил его к декодированию линейных кодов [14].

Данный алгоритм применяется для вычисления коэффициентов полинома локаторов и по числу операций в конечном поле $GF(2^m)$ считается одним из самых эффективных. Необходимо дать несколько коментариев относительно работы рассматриваемой блок-схемы.

1. На вход подается последовательность $s_i = (s_1, s_2, ..., s_n)$, поэтому вычисления ведутся до тех пор пока счетчик i не будет равен n.

2. Полином локаторов записывается как вектор коэффициентов при соответствующих степенях x:

$$c = c_1 + c_2x + ... + c_nx^{n-1} = (c_1, c_2, c_3, ..., c_n)$$

Пример 3.50. Построить полином лакаторов для кодовой последовательности $RS[7,3] \in GF(2^3)$: F=(7644606) при $b = 3$.

Решение. Учитывая, что $(s_1, s_2, s_3, s_4) = (1, 7, 5, 0)$ будем проводить вычисления согласно приведеному алгоритму.

★ $i = 0,\ L = 0,\ c = 1,\ B = 1$

★ $i = 1, \quad d_1 = c_1 \cdot s_1 = 1 \cdot 1 = 1$

$$\begin{aligned} c^+ &= c + dBx = 1 + 1 \cdot 1 \cdot x = 1 + x \\ & 2L < i:\ 0 < 1 \text{ да} \Rightarrow L = i - L,\ L = 1 - 0 = 1 \\ & B = \frac{c}{d} = \frac{1}{1} = 1,\ \ c = c^+ = 1 + x \end{aligned}$$

★ $i = 2, \quad d_2 = (c_1, c_2) \cdot (s_2, s_1) = (1, 1)(7, 1) = 7 + 1 = 6$

$$\begin{aligned} c^+ &= c + dBx = 1 + x + 6 \cdot 1 \cdot x = 1 + 7x \\ & 2L < i:\ 2 < 2 \text{ нет} \\ & B = xB = x,\ \ c = c^+ = 1 + 7x \end{aligned}$$

★ $i=3,\quad d_3=(c_1,c_2,c_3)\cdot(s_3,s_2,s_1)=(1,7,0)(5,7,1)=1\cdot5+7\cdot7+0\cdot1=5+3+0=6$

$$\begin{aligned} c^+ &= c+dBx=1+7x+6\cdot x\cdot x=1+7x+6x^2\\ &\quad 2L<i:\ 2\cdot1<3 \text{ да} \Rightarrow L=i-L,\ L=3-1=2\\ &\quad B=\frac{c}{d}=\frac{1+7x}{6}=3(1+7x)=3+2x,\ \ c=c^+=1+7x+6x^2 \end{aligned}$$

★ $i=4,\quad d_4=(c_1,c_2,c_3,c_4)\cdot(s_4,s_3,s_2,s_1)=(1,7,6,0)(0,5,7,1)=1\cdot0+7\cdot5+6\cdot7+0\cdot1=0+6+4+0=2$

$$\begin{aligned} c^+ &= c+dBx=1+7x+6x^2+2\cdot(3+2x)\cdot x\\ &= 1+7x+6x^2+6x+4x^2=1+x+2x^2 \end{aligned}$$

Поскольку $i=4=n$ мы прекращаем вычисления и выводим ответ полинома локаторов

$$\Sigma(x)=c=1+x+2x^2.\quad ▲$$

Пример 3.51. Построить полином лакаторов для кодовой последовательности $RS[7,3]\in GF(2^3)$: F=(62254420) при $b=4$.

Решение. Учитывая, что $(s_1,s_2,s_3,s_4)=(7,4,5,3)$ будем проводить вычисления согласно приведеному алгоритму.

★ $i=0,\ L=0,\ c=1,\ B=1$

★ $i=1,\quad d_1=s_0\cdot c_1=7\cdot1=7$

$$\begin{aligned} c^+ &= c+dBx=1+7\cdot1\cdot x=1+7x\\ &\quad 2L<i:\ 0<1 \text{ да} \Rightarrow L=i-L,\ L=1-0=1\\ &\quad B=\frac{c}{d}=\frac{1}{7}=4,\ \ c=c^+=1+7x \end{aligned}$$

★ $i=2,\quad d_2=(c_1,c_2)\cdot(s_2,s_1)=(1,7)(4,7)=4+3=7$

$$\begin{aligned} c^+ &= c+dBx=1+7x+7\cdot4\cdot x=1+7x+x=1+6x\\ &\quad 2L<i:\ 2<2 \text{ нет}\\ &\quad B=Bx=4x,\ \ c=c^+=1+6x \end{aligned}$$

★ $i=3,\quad d_3=(c_1,c_2,c_3)\cdot(s_3,s_2,s_1)=(1,6,0)(5,4,7)=1\cdot5+6\cdot4+0\cdot7=5+5=0$

$$B=Bx=4x^2,\quad c=1+6x$$

★ $i=4,\quad d_4=(c_1,c_2,c_3,c_4)\cdot(s_4,s_3,s_2,s_1)=(1,6,0,0)(3,5,4,7)=1\cdot3+6\cdot5+0\cdot4+0\cdot7=3+3=0$

$$B=Bx=4x^2,\quad c=1+6x$$

Поскольку $i=4=n$ мы прекращаем вычисления и выводим ответ полинома локаторов

$$\Sigma(x)=c=1+6x=1+2^4x.\quad ▲$$

Задача 3.27. Обнаружить и исправить ошибки в информационной кодовой комбинации $F(x) \in RS[7,3]$ сформированной производящим полиномом $g(x)$ поля $GF(2^3)$.

N	b	F	**N**	b	F	**N**	b	F	**N**	b	F
1	3	(2421121)	9	4	(2264425)	17	3	(5116230)	25	4	(4661674)
2	4	(3634162)	10	5	(5253561)	18	4	(2325111)	26	5	(5564312)
3	5	(3615206)	11	6	(2727517)	19	5	(3333005)	27	6	(5471253)
4	6	(2264027)	12	0	(1426013)	20	6	(4117765)	28	0	(2715001)
5	0	(3262616)	13	1	(2535555)	21	0	(2453626)	29	1	(6262477)
6	0	(4562373)	14	1	(1615153)	22	1	(0650027)	30	2	(5525355)
7	1	(2732576)	15	2	(7563113)	23	2	(0114252)	31	3	(3270440)
8	2	(1247370)	16	3	(4431737)	24	3	(2421121)	32	4	(2264425)

3.11 Расширенный алгоритм Евклида для кода RS

Кратко напомним расширенный алгоритм Евклида, который мы применяли для построения полинома локаторов кода БЧХ. Для этого полином x^r записываем через $S = \sum S_k x^k$ в виде

$$x^r = S \cdot q_0 + r_1$$

тогда

$$\begin{aligned} S &= r_1 \cdot q_1 + r_2 \\ r_1 &= r_2 \cdot q_2 + r_3 \\ r_2 &= r_3 \cdot q_3 + r_5 \\ &... \end{aligned}$$

и полиномы локаторов выражаются через множители $(q_0, q_1, ...)$ следующим образом

★ 1 ошибка

$$\sigma_1 = \sigma_0 q_0 = q_0$$

★ 2 ошибки

$$\sigma_2 = \sigma_1 q_1 + \sigma_0 = q_0 q_1 + 1$$

★ 3 ошибки

$$\sigma_3 = \sigma_2 q_2 + \sigma_1 = q_0 q_1 q_2 + q_0 + q_2$$

★ 4 ошибки

$$\sigma_4 = \sigma_3 q_3 + \sigma_2 = q_0 q_1 q_2 q_3 + q_0 q_3 + q_2 q_3 + q_1 q_0 + 1$$

Пример 52. Построить полином локаторов для кодовой последовательности $RS[7,3] \in GF(2^3)$: F=(7644606) при $b = 3$.

Решение. Учитывая, что $(s_1, s_2, s_3, s_4) = (1, 7, 5, 0)$ будем проводить вычисления согласно приведеному алгоритму. Поскольку

$$\begin{array}{l|l} x^5 + 0x^4 + 0x^3 + 0x^2 + 0x + 0 & 5x^3 + 7x^2 + x + 1 \\ \cline{2-2} x^5 + 5x^4 + 2x^3 + 2x^2 & 2x^2 + x + 1 \\ \cline{1-1} \quad 5x^4 + 2x^3 + 2x^2 & \\ \quad 5x^4 + 7x^3 + x^2 + x & \\ \cline{1-1} \quad\quad 5x^3 + 3x^2 + x & \\ \quad\quad 5x^3 + 7x^2 + x + 1 & \\ \cline{1-1} \quad\quad\quad\quad 4x^2 + 1 & \end{array}$$

т.е.

$$x^5 = (1 + x + 7x^2 + 5x^3)(1 + x + 2x^2) + (1 + 4x^2),$$

то полином локаторов имеет вид

$$\Sigma(x) = 1 + x + 2x^2 = (1 + 4x)(1 + 5x) = (1 + 2^2x)(1 + 2^6x). \quad \blacktriangle$$

Пример 53. Построить полином локаторов для кодовой последовательности $RS[7,3] \in GF(2^3)$: F=(62254420) при $b = 4$.

Решение. Учитывая, что $(s_1, s_2, s_3, s_4) = (7, 4, 5, 3)$ будем проводить вычисления согласно приведеному алгоритму. Поскольку

$$\begin{array}{l|l} x^5 + 0x^4 + 0x^3 + 0x^2 + 0x + 0 & 3x^4 + 5x^3 + 4x^2 + 7x + 1 \\ \cline{2-2} x^5 + 3x^4 + 5x^3 + 4x^2 + 6x & 6x + 1 \\ \cline{1-1} \quad 3x^4 + 5x^3 + 4x^2 + 6x & \\ \quad 3x^4 + 5x^3 + 4x^2 + 7x + 1 & \\ \cline{1-1} \quad\quad\quad\quad\quad\quad x + 1 & \end{array}$$

т.е.

$$x^5 = (1 + 7x + 4x^2 + 5x^3 + 3x^4)(1 + 6x) + (1 + x),$$

то полином локаторов имеет вид

$$\Sigma(x) = 1 + 6x = 1 + 2^4x. \quad \blacktriangle$$

Пример 54. Построить полином локаторов для кодовой последовательности $RS[7,3] \in GF(2^3)$: F=(0070200) при $b = 0$ (см. например [9], стр.114).

Решение. Учитывая, что $(s_1, s_2, s_3, s_4) = (5, 7, 2, 2)$ будем проводить вычисления согласно приведеному алгоритму Евклида. Поскольку

$$x^5 = (1 + 5x + 7x^2 + 2x^3 + 2x^4)(5 + 5x) + (5 + 2x + x^2 + 7x^2),$$

$$1 + 5x + 7x^2 + 2x^3 + 2x^4 = (5 + 2x + x^2 + 7x^2)(4 + 3x) + (3 + 2x + 5x^2),$$

то полином локаторов имеет вид

$$\Sigma(x) = 1 + (5 + 5x)(4 + 3x) = 3 + 6x + 4x^2 = 3(1 + 2x + 5x^2). \quad \blacktriangle$$

Для решения данного уравнения воспользуемся формулами Виета

$$\Sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2.$$

т.е.

$$\begin{cases} x_1 + x_2 = \sigma_1 \\ x_1 \cdot x_2 = \sigma_2 \end{cases} \quad \text{или} \quad \begin{cases} x_1 + x_2 = 2 \\ x_1 \cdot x_2 = 5 \end{cases}$$

По таблицам сложения и умножения для $GF(2^3)$ находим $x_1 = 4,\ x_2 = 6$, тогда

$$\Sigma(x) = 3(1 + 2x + 5x^2) = 3(1 + 4x)(1 + 6x) = 3(1 + 2^2 x)(1 + 2^4 x).$$

Т.е. ошибки в символах A_2 и A_4 (коэффициенты при степенях x^2 и x^4) полинома $\overline{F(x)}$.

Для нахождения значения ошибок решим систему

$$\begin{pmatrix} S_1 \\ S_2 \end{pmatrix} = \begin{pmatrix} x_1^b & x_2^b \\ x_1^{b+1} & x_2^{b+1} \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} \text{ или } \begin{pmatrix} 5 \\ 7 \end{pmatrix} = \begin{pmatrix} 4^0 & 6^0 \\ 4^1 & 6^1 \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 4 & 6 \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}$$

Методом Крамера, получим

$$\Delta = \begin{vmatrix} 1 & 1 \\ 4 & 6 \end{vmatrix} = 1 \cdot 6 - 4 \cdot 1 = 6 + 4 = 2$$

$$\Delta_1 = \begin{vmatrix} 5 & 1 \\ 7 & 6 \end{vmatrix} = 5 \cdot 6 - 7 \cdot 1 = 3 + 7 = 4; \quad \Delta_2 = \begin{vmatrix} 1 & 5 \\ 4 & 7 \end{vmatrix} = 1 \cdot 7 - 4 \cdot 5 = 7 + 2 = 5$$

Тогда

$$e_1 = \frac{\Delta_1}{\Delta} = \frac{4}{2} = 4 \cdot 5 = 2, \quad e_2 = \frac{\Delta_2}{\Delta} = \frac{5}{2} = 5 \cdot 5 = 7.$$

Т.о. мы имеем ошибку в разряде x^2 со значением $E_2 = 2$ и в разряде x^4 со значением $E_4 = 7$. Исправляя ошибки, получим

$$F = (00\underline{\mathbf{7}}0\underline{\mathbf{2}}00) \Rightarrow (00\underline{\mathbf{0}}00\underline{\mathbf{0}}00) \quad \blacktriangle$$

Задача 3.28. Обнаружить и исправить ошибки в информационной кодовой комбинации $F(x) \in RS[7, 3]$ сформированной производящим полиномом $g(x)$ поля $GF(2^3)$.

N	b	F	**N**	b	F	**N**	b	F	**N**	b	F
1	4	2264425	9	3	5116230	17	4	4661674	25	3	2421121
2	5	5253561	10	4	2325111	18	5	5564312	26	4	3634162
3	6	2727517	11	5	3333005	19	6	5471253	27	5	3615206
4	0	1426013	12	6	4117765	20	0	2715001	28	6	2264027
5	1	2535555	13	0	2453626	21	1	6262477	29	0	3262616
6	1	1615153	14	1	0650027	22	2	5525355	30	0	4562373
7	2	7563113	15	2	0114252	23	3	3270440	31	1	2732576
8	3	4431737	16	3	2421121	24	4	2264425	32	2	1247370

Глава 4

Квантовая информация

4.1 Основы квантовых вычислений

В этой главе, мы рассмотрим принципы теории квантовых вычислений. В настоящих цифровых компьютерах, информация хранится и обрабатывается в форме битов - объектов, которые могут принимать только два значения: логический ноль -"0", или логическую единицу -"1". Они - обычно представляют собой напряжение в узле, или направление намагниченности магнитного домена. Поскольку любая подобная физическая система должна иметь как минимум два отличных состояния, то двухуровневые квантовые системы, (например частицы со спином $1/2$, или поляризованные фотоны) тоже могут рассматриваться как носители информации. Квантовое состояние $|0\rangle$ соответствует значению бита -"0", а состояние $|1\rangle$ соответствует "1". Для spin-$1/2$ частиц, два вычислительных базисных состояния представляются спином вверх $|\uparrow\rangle$ или спином вниз $|\downarrow\rangle$, а для фотонов - горизонтальной $|\leftrightarrow\rangle$ или вертикальной $|\updownarrow\rangle$ поляризацией, соответственно. В отличие от классических битов, которые могут существовать только как "0"или "1", двухуровневые квантовые системы, называемые квантовые биты или qubits (quantum bits), могут также существовать в состоянии суперпозиции $|0\rangle$ и $|1\rangle$:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,,$$

где α и β удовлетворяют условию нормировки: $\alpha^2 + \beta^2 = 1$.

По существу мы описываем квантовое состояние системы с помощью комплексного вектора Гильбертова пространства $\mathbf{H}$ с базисными векторами $|0\rangle$ и $|1\rangle$ и скалярным произведением: $\langle\varphi|\psi\rangle$. Гильбертовым назовем нормированное векторное пространство комплексных чисел со скалярным произведением. Два вектора являются ортогональными, если их скалярное произведение равно нулю:

$$\langle\varphi|\psi\rangle = \langle\psi|\varphi\rangle = 0.$$

Отсюда следуют соотношения для скалярного произведения базисных векторов:

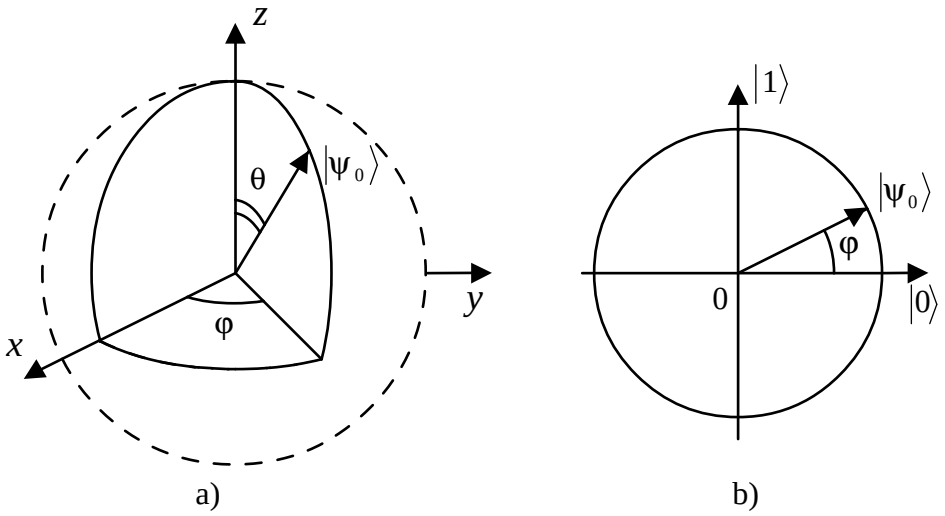
$$\langle 0|0\rangle = \langle 1|1\rangle = 1, \quad \langle 0|1\rangle = \langle 1|0\rangle = 0.$$

С учетом полной фазы квантовое состояние кубита записывается в виде

$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle\,,$$

и изображается точкой на сфере Блоха радиуса $R = 1$ и поверхностными координатами (θ, ϕ). В дальнейшем мы будем, как правило, работать с экваториальными кубитами, (для которых $\phi = 0$), и удваивать значение угла $\frac{\theta}{2} \to \theta$ для упрощения записи:

$$|\psi\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle\,.$$



Пример 4.1. Кубит имеет квантовое состояние

$$|\psi_0\rangle = \frac{\sqrt{2}}{2}\,|0\rangle + \beta\,|1\rangle\,.$$

Определить неизвестный коэффициент β.

Решение. Из условия нормировки, для произвольного квантового состояния

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad \text{имеем} \quad \alpha^2 + \beta^2 = 1.$$

Тогда для искомого состояния

$$|\psi_0\rangle = \frac{\sqrt{2}}{2}\,|0\rangle + \beta\,|1\rangle\,, \quad \text{получим} \quad \left(\frac{\sqrt{2}}{2}\right)^2 + \beta^2 = 1 \quad \text{откуда} \quad \beta = \frac{1}{\sqrt{2}}\,.$$

Таким образом

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,. \quad \blacktriangle$$

Задача 4.1. Пользуясь условием нормировки определить неизвестные коэффициенты кубитов.

1. $|\psi_0\rangle = \alpha\,|0\rangle + \frac{1}{2}\,|1\rangle$ **2.** $|\psi_0\rangle = \alpha\,|0\rangle + |1\rangle$

3. $|\psi_0\rangle = \alpha\,|0\rangle + \frac{\sqrt{3}}{2}\,|1\rangle$ **4.** $|\psi_0\rangle = |0\rangle + \beta\,|1\rangle$

Основные понятия которыми оперирует квантовая механика: состояние, наблюдаемые, динамика и измерение.

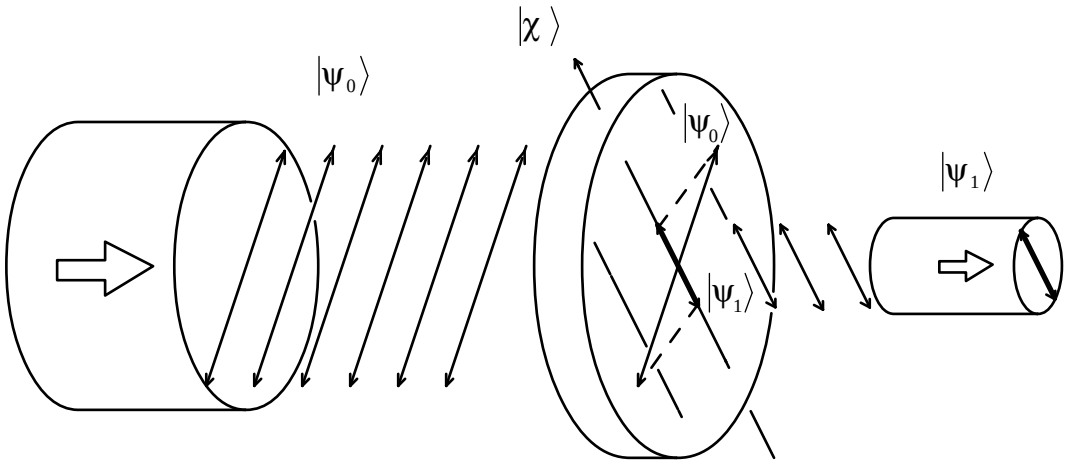
Всякая физическая система описывается с помощью своего состояния, которое содержит всю информацию о системе. Состояние квантовой системы изменяется только двумя путями: взаимодействием с другой системой и измерением. Узнать что-либо о квантовом состоянии можно только ее измерением.

Поляризованный свет легко реализуется на практике и является одним из основных претендентов на роль носителя квантовой информации - кубита. Измерение поляризации производят с помощью поляризационных пластин. Поляризационная пластина пропускает через себя фотоны только заданной поляризации. После поляризатора размещается счетчик фотонов, который определяет вероятность прохождения пучка через поляризатор. Математически поляризационной пластине ставится в соответствии проекционный оператор:

$$\Pi = |\chi\rangle\,\langle\chi|\,,$$

где $|\chi\rangle$ - вектор ориентации поляризационной пластины или квантовое состояние прибора-измерителя. При прохождении поляризационной пластины квантовое состояние кубита $|\psi\rangle$ проецируется на квантовое состояние прибора-измерителя $|\chi\rangle$. На выходе из поляризатора мы получим уже измененный кубит, т.е. его проекцию на $|\chi\rangle$:

$$|\psi'\rangle = \Pi\,|\psi\rangle = |\chi\rangle\,\langle\chi|\psi\rangle\,.$$



Поскольку скалярное произведение $\langle\chi|\psi\rangle$ - число, то выходной кубит имеет состояние параллельное квантовому состоянию прибора-измерителя $|\chi\rangle$. Это принципиальный факт квантовой механики - измерение меняет квантовое состояние.

В квантовой механике постулируется, что само состояние $|\psi\rangle$ физического смысла не имеет (т.е. не может быть непосредственно измерено). Физическим смыслом обладает его квадрат модуля:

$$P = \langle\psi|\psi\rangle = |\psi|^2$$

- это вероятность обнаружить кубит в данном квантовом состоянии.

Пример 4.2. Найти вероятность того, что кубит

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle .$$

пройдет через поляризатор, ориентированный под углом 60°.

Решение. Ориентации поляризатора с углом $\phi = 60^\circ = \pi/3$ соответствует квантовое состояние прибора измерителя

$$|\chi\rangle = \cos\phi\,|0\rangle + \sin\phi\,|1\rangle = \cos\frac{\pi}{3}|0\rangle + \sin\frac{\pi}{3}|1\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle .$$

Тогда для соответствующего проекционного оператора получим

$$\begin{aligned}
\Pi &= |\chi\rangle\langle\chi| = \left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)\left(\langle 0|\frac{1}{2} + \langle 1|\frac{\sqrt{3}}{2}\right) \\
&= \frac{1}{2}|0\rangle\langle 0|\frac{1}{2} + \frac{1}{2}|0\rangle\langle 1|\frac{\sqrt{3}}{2} + \frac{\sqrt{3}}{2}|1\rangle\langle 0|\frac{1}{2} + \frac{\sqrt{3}}{2}|1\rangle\langle 1|\frac{\sqrt{3}}{2} \\
&= \frac{1}{4}|0\rangle\langle 0| + \frac{\sqrt{3}}{4}|0\rangle\langle 1| + \frac{\sqrt{3}}{4}|1\rangle\langle 0| + \frac{3}{4}|1\rangle\langle 1|
\end{aligned}$$

После прохождения поляризатора исходный кубит $|\psi\rangle$ будет иметь состояние

$$|\psi'\rangle = \Pi|\psi\rangle = |\chi\rangle\langle\chi|\psi\rangle$$

или

$$\begin{aligned}
|\psi'\rangle &= \left(\frac{1}{4}|0\rangle\langle 0| + \frac{\sqrt{3}}{4}|0\rangle\langle 1| + \frac{\sqrt{3}}{4}|1\rangle\langle 0| + \frac{3}{4}|1\rangle\langle 1|\right)\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \\
&= \left(\frac{1}{4}\frac{1}{\sqrt{2}}|0\rangle\langle 0|0\rangle + \frac{\sqrt{3}}{4}\frac{1}{\sqrt{2}}|0\rangle\langle 1|0\rangle + \frac{\sqrt{3}}{4}\frac{1}{\sqrt{2}}|1\rangle\langle 0|0\rangle + \frac{3}{4}\frac{1}{\sqrt{2}}|1\rangle\langle 1|0\rangle\right) \\
&+ \left(\frac{1}{4}\frac{1}{\sqrt{2}}|0\rangle\langle 0|1\rangle + \frac{\sqrt{3}}{4}\frac{1}{\sqrt{2}}|0\rangle\langle 1|1\rangle + \frac{\sqrt{3}}{4}\frac{1}{\sqrt{2}}|1\rangle\langle 0|1\rangle + \frac{3}{4}\frac{1}{\sqrt{2}}|1\rangle\langle 1|1\rangle\right)
\end{aligned}$$

Учитывая, что

$$\langle 0|0\rangle = \langle 1|1\rangle = 1, \qquad \langle 1|0\rangle = \langle 0|1\rangle = 0,$$

получим

$$\begin{aligned} |\psi'\rangle &= \left(\frac{1}{4}\frac{1}{\sqrt{2}}|0\rangle + \frac{\sqrt{3}}{4}\frac{1}{\sqrt{2}}|1\rangle + \frac{\sqrt{3}}{4}\frac{1}{\sqrt{2}}|0\rangle + \frac{3}{4}\frac{1}{\sqrt{2}}|1\rangle\right) \\ &= \frac{1}{4}\left(\frac{1+\sqrt{3}}{\sqrt{2}}|0\rangle + \frac{3+\sqrt{3}}{\sqrt{2}}|1\rangle\right) \end{aligned}$$

Вероятность регистрации кубита в состоянии $|\psi'\rangle$ есть

$$\begin{aligned} P &= \langle\psi'|\psi'\rangle = \frac{1}{4}\left(\frac{1+\sqrt{3}}{\sqrt{2}}\langle 0| + \frac{3+\sqrt{3}}{\sqrt{2}}\langle 1|\right)\left(\frac{1+\sqrt{3}}{\sqrt{2}}|0\rangle + \frac{3+\sqrt{3}}{\sqrt{2}}|1\rangle\right)\frac{1}{4} \\ &= \frac{1}{4}\left(\frac{1+\sqrt{3}}{\sqrt{2}}\cdot\frac{1+\sqrt{3}}{\sqrt{2}}\langle 0|0\rangle + \frac{1+\sqrt{3}}{\sqrt{2}}\cdot\frac{3+\sqrt{3}}{\sqrt{2}}\langle 0|1\rangle\right)\frac{1}{4} \\ &+ \frac{1}{4}\left(\frac{3+\sqrt{3}}{\sqrt{2}}\cdot\frac{1+\sqrt{3}}{\sqrt{2}}\langle 1|0\rangle + \frac{3+\sqrt{3}}{\sqrt{2}}\cdot\frac{3+\sqrt{3}}{\sqrt{2}}\langle 1|1\rangle\right)\frac{1}{4} \\ &= \frac{1}{16}\left(\frac{1+\sqrt{3}}{\sqrt{2}}\cdot\frac{1+\sqrt{3}}{\sqrt{2}}\right) + \frac{1}{16}\left(\frac{3+\sqrt{3}}{\sqrt{2}}\cdot\frac{3+\sqrt{3}}{\sqrt{2}}\right) = \frac{16+8\sqrt{3}}{32} \approx 0.933. \quad \blacktriangle \end{aligned}$$

По существу, данная задача формулируется следующим образом: найти вероятность того, что кубит $|\psi_0\rangle$ будет зарегистрирован в состоянии $|\chi\rangle$. Тогда

$$P = |\langle\psi_0|\chi\rangle|^2$$

и предыдущая задача решается следующим образом. Мы должны посчитать

$$\langle\psi_0|\chi\rangle = \left(\frac{1}{\sqrt{2}}\langle 0| + \frac{1}{\sqrt{2}}\langle 1|\right)\left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) = \frac{1+\sqrt{3}}{2\sqrt{2}}$$

тогда

$$P = |\langle\psi_0|\chi\rangle|^2 = \left|\frac{1+\sqrt{3}}{2\sqrt{2}}\right|^2 \approx 0.933. \quad \blacktriangle$$

Задача 4.2. Найти вероятность того, что квант $|\psi_0\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$ пройдет через поляризатор, ориентированный под углом φ.

1. $\varphi = 0°$; **2.** $\varphi = 30°$; **3.** $\varphi = 45°$; **4.** $\varphi = 60°$.

Однако столь быстрый метод работает только тогда, когда на кубит действует только один оператор. Если же мы имеем последовательность операторов, то нам необходимо вычислить состояние кубита после каждого преобразования.

Пример 4.3. На пути пучка квантов $|\psi_0\rangle = |0\rangle$ ставится поляризационная пластина №1, ориентированная под углом 0°. После нее ставится еще один поляризатор №2 под углом 90°. Какова вероятность того, что исходный пучок пройдет через эти два поляризатора.

Решение. Поставим в соответствие поляризатору №1 проекционный оператор

$$\Pi_1 = |0\rangle\langle 0|,$$

а поляризатору №2 проекционный оператор

$$\Pi_2 = |1\rangle\langle 1|.$$

Тогда после прохождения первого поляризатора кубит принимает состояние

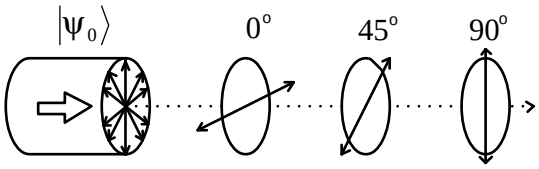
$$|\psi_1\rangle = \Pi_1|\psi_0\rangle = |0\rangle\langle 0|0\rangle = |0\rangle\cdot 1 = |0\rangle,$$

а после второго

$$|\psi_2\rangle = \Pi_2|\psi_1\rangle = |1\rangle\langle 1|0\rangle = |0\rangle\cdot 0.$$

Поэтому, вероятность прохождения кубитом двух поляризаторов равна

$$P = \langle\psi_2|\psi_2\rangle = 0. \quad \blacktriangle$$



Пример 4.4. В условиях предыдущей задачи, между поляризаторами №1 и №2 ставится дополнительная поляризационная пластина №3, ориентированная под углом 45°. Найти вероятность регистрации кванта фотодетектором на выходе полученной системы поляризаторов.

Решение. Поставим в соответствие поляризатору №3 проекционный оператор

$$\Pi_3 = |\chi\rangle\langle\chi|,$$

где

$$|\chi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

Тогда после прохождения первого поляризатора $\Pi_1 = |0\rangle\langle 0|$ кубит принимает состояние

$$|\psi_1\rangle = \Pi_1|\psi_0\rangle = |0\rangle\langle 0|0\rangle = |0\rangle\cdot 1 = |0\rangle,$$

после этого он проходит через поляризатор Π_3:

$$\begin{aligned} |\psi_3\rangle &= \Pi_3 |\psi_1\rangle = |\chi\rangle \langle\chi|0\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}\langle 0|0\rangle + \frac{1}{\sqrt{2}}\langle 1|0\rangle\right) \\ &= \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}\cdot 1 + \frac{1}{\sqrt{2}}\cdot 0\right) = \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle, \end{aligned}$$

а затем, через поляризатор $\Pi_2 = |1\rangle\langle 1|$

$$|\psi_2\rangle = \Pi_2 |\psi_3\rangle = |1\rangle\langle 1|\psi_3\rangle = |1\rangle\langle 1|\left(\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle\right) = \frac{1}{2}|1\rangle.$$

Поэтому, вероятность прохождения кубитом трех поляризаторов равна

$$P = \langle\psi_2|\psi_2\rangle = \frac{1}{4}\langle 1|1\rangle = \frac{1}{4}. \quad \blacktriangle$$

Последние два примера высвечивают один из основных фундаментальных принципов квантовой механики: операторы не просто проецируют кванты на собственное состояние, а изменяют состояние кубита. Т.е. после взаимодействия с оператором частица становится другой и приобретает свойства уже этого оператора частично теряя при этом некоторые свои свойства. Как видно из примеров квант горизонтальной поляризации $|0\rangle$ не может пройти через ортогональный вертикально-ориентированный поляризатор $\Pi = |1\rangle\langle 1|$. Однако, дополнительный оператор Π_3 искажает исходное состояние кубита, после чего он приобретает новые свойства, позволяющие пройти с ненулевой вероятностью через ортогональный поляризатор.

Пример 4.5. На пути пучка квантов $|\psi_0\rangle = |0\rangle$ ставится поляризационная пластина №1, ориентированная под углом $0°$. После нее ставится еще один поляризатор №2 под углом $30°$, далее поляризатор №3 под углом $45°$, №4 - под углом $60°$ и №5 - под углом $90°$. Какова вероятность того, что исходный пучок пройдет через эти 5 поляризаторов?

Решение. Поставим в соответствие поляризатору №1 проекционный оператор

$$\Pi_1 = |0\rangle\langle 0|,$$

поляризатору №2 - проекционный оператор

$$\Pi_2 = \left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)\left(\frac{1}{2}\langle 0| + \frac{\sqrt{3}}{2}\langle 1|\right),$$

поляризатору №3 - проекционный оператор

$$\Pi_3 = \left(\frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle\right)\left(\frac{\sqrt{2}}{2}\langle 0| + \frac{\sqrt{2}}{2}\langle 1|\right),$$

поляризатору №4 - проекционный оператор

$$\Pi_4 = \left(\frac{\sqrt{3}}{2}\,|0\rangle + \frac{1}{2}\,|1\rangle\right)\left(\frac{\sqrt{3}}{2}\,\langle 0| + \frac{1}{2}\,\langle 1|\right),$$

поляризатору №5 - проекционный оператор

$$\Pi_5 = |1\rangle\langle 1|.$$

Тогда последовательное действие этих операторов на кубит $|\psi_0\rangle = |0\rangle$ дает

$$|\psi_1\rangle = \Pi_5\Pi_4\Pi_3\Pi_2\Pi_1\,|\psi_0\rangle = \Pi_5\Pi_4\Pi_3\Pi_2\Pi_1\,|0\rangle = \frac{\sqrt{2}}{2}\,|1\rangle.$$

Поэтому, вероятность прохождения кубитом 5 поляризаторов равна

$$P = \langle\psi_1|\psi_1\rangle = \frac{1}{2}\,\langle 1|1\rangle = \frac{1}{2}. \quad \blacktriangle$$

Как видно из этих примеров: чем больше поляризаторов мы ставим - тем больше вероятность прохождения через них кубита. Другими словами, чем больше препятствий для кванта - тем легче квант через них проходит. Единственным условием является лишь то, что полряризаторы должны распологаться правильным образом - строго "по кругу". Отсюда следует, что бесконечное количество поляризаторов поворачивают кубит на любой угол без искажения.

Пример 4.6. На пути произвольного пучка квантов $|\psi_0\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ ставится поляризационная пластина №1, ориентированная под углом $0°$. После нее ставится еще один поляризатор №2 под углом $90°$. Какова вероятность того, что исходный пучок пройдет через эти два поляризатора.

Решение. Поставим в соответствие поляризатору №1 проекционный оператор

$$\Pi_1 = |0\rangle\langle 0|,$$

поляризатору №2 - проекционный оператор

$$\Pi_2 = |1\rangle\langle 1|.$$

Тогда

$$\begin{aligned} |\psi_1\rangle &= \Pi_1\,|\psi_0\rangle = |0\rangle\langle 0|\,(\alpha\,|0\rangle + \beta\,|1\rangle) = \alpha\,|0\rangle \\ |\psi_2\rangle &= \Pi_2\,|\psi_1\rangle = \alpha\,|1\rangle\langle 1|0\rangle = \alpha\,|1\rangle\cdot 0 = 0 \\ P &= \langle\psi_2|\psi_2\rangle = 0. \quad \blacktriangle \end{aligned}$$

Пример 4.7. В условиях предыдущей задачи, между поляризаторами №1 и №2 ставится дополнительная поляризационная пластина №3, ориентированная под

углом 45°. Найти вероятность регистрации кванта фотодетектором на выходе полученной системы поляризаторов.

Решение. По условию задачи

$$\Pi_1 = |0\rangle\langle 0|, \quad \Pi_2 = \frac{1}{2}\left(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|\right), \quad \Pi_3 = |1\rangle\langle 1|.$$

Тогда

$$\begin{aligned}
|\psi_1\rangle &= \Pi_1|\psi_0\rangle = |0\rangle\langle 0|\left(\alpha|0\rangle + \beta|1\rangle\right) = \alpha|0\rangle \\
|\psi_2\rangle &= \frac{\alpha}{2}\left(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|\right)|0\rangle = \frac{\alpha}{2}(|0\rangle + |1\rangle) \\
|\psi_3\rangle &= \Pi_3|\psi_2\rangle = \frac{\alpha}{2}|1\rangle\langle 1|\left(|0\rangle + |1\rangle\right) = \frac{\alpha}{2}|1\rangle \\
P &= \langle\psi_3|\psi_3\rangle = \frac{\alpha^2}{4}\langle 1|1\rangle = \frac{\alpha^2}{4}. \quad \blacktriangle
\end{aligned}$$

В общем случае поляризатор повернутый на θ° проецирует кубит $|0\rangle$ на состояние

$$|\chi\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$$

и описывается проекционным оператором

$$\Pi = |\chi\rangle\langle\chi| = \left(\cos\theta|0\rangle + \sin\theta|1\rangle\right)\left(\langle 0|\cos\theta + \langle 1|\sin\theta\right).$$

Для изменения угла поляризации пучка частиц используют фазовращательные пластины. Математически фазовращательным пластинам ставится в соответствие оператор поворота кубита на угол φ:

$$\begin{aligned}
\mathbf{R}|0\rangle &= \quad \cos\varphi|0\rangle + \sin\varphi|1\rangle, \\
\mathbf{R}|1\rangle &= -\sin\varphi|0\rangle + \cos\varphi|1\rangle.
\end{aligned}$$

Если базисное состояние представить в виде вектора-столбца

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

то оператор поворота $\mathbf{R}$ задается матрицей поворота

$$\mathbf{R} = \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix}.$$

С помощью оператора поворота можно создать из нулевого кубита $|0\rangle$ - кубит с произвольной поляризацией:

$$\mathbf{R}|0\rangle = \cos\varphi|0\rangle + \sin\varphi|1\rangle.$$

Пример 4.8. На какой угол необходимо повернуть кубит

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

чтобы получить кубит в состоянии $|1\rangle$?

Решение. Сравнивая два выражения

$$\begin{aligned} |\psi\rangle &= \cos\varphi\,|0\rangle + \sin\varphi\,|1\rangle \\ |\psi\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \end{aligned}$$

получим:

$$\cos\varphi = \frac{1}{\sqrt{2}} \qquad \text{или} \qquad \varphi = \frac{\pi}{4}.$$

Кубит в состоянии $|1\rangle$ имеет угол поляризации $\varphi' = \frac{\pi}{2}$. Поэтому нам необходимо подействовать на исходный кубит оператором поворота с углом

$$\Delta\varphi = \varphi' - \varphi = \frac{\pi}{2} - \frac{\pi}{4} = \frac{\pi}{4},$$

т.е.

$$\mathbf{R} = \begin{pmatrix} \cos\frac{\pi}{4} & \sin\frac{\pi}{4} \\ -\sin\frac{\pi}{4} & \cos\frac{\pi}{4} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}. \quad \blacktriangle$$

Задача 4.3. На какой угол необходимо повернуть кубит $|\psi\rangle$ чтобы получить кубит $|\psi'\rangle$?

1. $|\psi\rangle = \frac{\sqrt{2+\sqrt{2}}}{2}|0\rangle + \frac{\sqrt{2-\sqrt{2}}}{2}|1\rangle$ $\quad |\psi'\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$

2. $|\psi\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$ $\quad |\psi'\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$

3. $|\psi\rangle = \frac{\sqrt{2}\sqrt{5-\sqrt{5}}}{4}|0\rangle + \frac{\sqrt{5}+1}{4}|1\rangle$ $\quad |\psi'\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$

4. $|\psi\rangle = \frac{\sqrt{2+\sqrt{2}}}{2}|0\rangle + \frac{\sqrt{2-\sqrt{2}}}{2}|1\rangle$ $\quad |\psi'\rangle = \frac{\sqrt{2}\sqrt{5-\sqrt{5}}}{4}|0\rangle$

Кроме операции поворота для преобразования квантового состояния кубита часто используются матрицы Паули:

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

оператор Адамара

$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Мы будем пользоваться другими представлениями этих операторов

$$\sigma_0 = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad \sigma_1 = |0\rangle\langle 1| + |1\rangle\langle 0|,$$

$$i\sigma_2 = |0\rangle\langle 1| - |1\rangle\langle 0|, \quad \sigma_3 = |0\rangle\langle 0| - |1\rangle\langle 1|,$$

$$\mathbf{H} = \frac{1}{\sqrt{2}}(\sigma_1 + \sigma_3).$$

Не вдаваясь в физические детали, отметим, что каждый из этих операторов имеет явную техническую реализацию в качестве прибора изменяющего состояние квантового пучка когерентного лазерного излучения.

Пример 4.9. Кубит имеет произвольное состояние

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

Какова вероятность обнаружить его в состоянии $|\chi\rangle = \sigma_1|\psi\rangle$?

Решение.

1. Физически мы пропускаем пучок кубитов через поляризатор, ориентированный параллельно состоянию $|\chi\rangle$, т.е. действуем проектором

$$\Pi = |\chi\rangle\langle\chi|,$$

на $|\psi\rangle$:

$$|\psi'\rangle = \Pi|\psi\rangle = |\chi\rangle\langle\chi|\psi\rangle.$$

Выпишем явный вид квантового состояния прибора-измерителя:

$$|\chi\rangle = \sigma_1|\psi\rangle = (|0\rangle\langle 1| + |1\rangle\langle 0|)(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$$

тогда

$$\Pi = |\chi\rangle\langle\chi| = \beta^2|0\rangle\langle 0| + \alpha\beta|0\rangle\langle 1| + \alpha\beta|1\rangle\langle 0| + \alpha^2|1\rangle\langle 1|$$

и

$$\begin{aligned} |\psi'\rangle &= \Pi|\psi\rangle = |\chi\rangle\langle\chi \mid \psi\rangle \\ &= \left(\beta^2|0\rangle\langle 0| + \alpha\beta|0\rangle\langle 1| + \alpha\beta|1\rangle\langle 0| + \alpha^2|1\rangle\langle 1|\right)(\alpha|0\rangle + \beta|1\rangle) \\ &= \beta^2\alpha|0\rangle + \alpha\beta^2|0\rangle + \alpha^2\beta|1\rangle + \alpha^2\beta|1\rangle = 2\alpha\beta^2|0\rangle + 2\alpha^2\beta|1\rangle = 2\alpha\beta|\psi\rangle \end{aligned}$$

Вероятность регистрации кубита после прохождения поляризационной пластины есть

$$P = \langle\psi'|\psi'\rangle = 2^2\alpha^2\beta^2\langle\psi|\psi\rangle = 4\alpha^2\beta^2.$$

2. Поскольку оба состояния нам известны:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad |\chi\rangle = \sigma_1|\psi\rangle = \alpha|1\rangle + \beta|0\rangle,$$

то из выражения

$$\langle\psi|\chi\rangle = (\alpha\langle 0| + \beta\langle 1|)(\beta|0\rangle + \alpha|1\rangle) = 2\alpha\beta$$

получим

$$P = |\langle\psi|\chi\rangle|^2 = 4\alpha^2\beta^2. \quad \blacktriangle$$

Задача 4.4. Кубит имеет произвольное состояние $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Найти вероятность обнаружения его в состоянии

1. $|\chi\rangle = i\sigma_2|\psi\rangle$, **2.** $|\chi\rangle = \sigma_3|\psi\rangle$, **3.** $|\chi\rangle = \sigma_0|\psi\rangle$, **4.** $|\chi\rangle = \mathbf{H}|\psi\rangle$.

4.2 Матрица плотности

Рассмотрим кубит в произвольном состоянии

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

Если это состояние совпадает с квантовым состоянием прибора-измерителя

$$|\chi\rangle = \alpha|0\rangle + \beta|1\rangle = |\psi\rangle,$$

то прохождение фотона $|\psi\rangle$ через такой поляризатор

$$|\psi'\rangle = \Pi|\psi\rangle = |\chi\rangle\langle\chi|\psi\rangle = |\psi\rangle\langle\psi|\psi\rangle = |\psi\rangle$$

не изменяет его квантового состояния. Другими словами

$$\langle\psi|\chi\rangle = \langle\psi|\psi\rangle = 1 \quad \text{или} \quad P = |\langle\psi|\chi\rangle|^2 = 1$$

т.е. вероятность прохождения кванта $|\psi\rangle$ через поляризатор $\Pi = |\chi\rangle\langle\chi|$ равна 1. Такой поляризатор мы назовем собственным для данного пучка. Любой произвольно приготовленный пучок проходит через собственный поляризатор полностью, и обратно, для любого поляризатора можно приготовить такой пучок который пройдет через него без искажения (без потерь). Это дает основание рассматривать квантовые пучки в терминах своих же собственных поляризаторов.

Матрицей плотности квантового пучка $|\psi\rangle$ называется его собственный проектор

$$\rho = |\psi\rangle\langle\psi|.$$

Для кубита $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$ часто используется расширенная запись его матрицы плотности:

$$\rho_0 = |\psi_0\rangle\langle\psi_0| = \alpha^2|0\rangle\langle 0| + \alpha\beta|0\rangle\langle 1| + \beta\alpha|1\rangle\langle 0| + \beta^2|1\rangle\langle 1|.$$

или

$$\rho_0 = \begin{pmatrix} \alpha^2 & \alpha\beta \\ \beta\alpha & \beta^2 \end{pmatrix}.$$

Пример 4.10. Найдите матрицу плотности квантового состояния $|\psi_1\rangle = \sigma_1 |\psi_0\rangle$.
Решение. Действуя оператором Паули σ_1 на кубит $|\psi_0\rangle$ получим

$$|\psi_1\rangle = \sigma_1 |\psi_0\rangle = (|0\rangle\langle 1| + |1\rangle\langle 0|)(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$$

тогда

$$\rho_1 = |\psi_1\rangle\langle\psi_1| = \alpha^2|1\rangle\langle 1| + \alpha\beta|0\rangle\langle 1| + \alpha\beta|1\rangle\langle 0| + \beta^2|0\rangle\langle 0|. \quad \blacktriangle$$

Пример 4.11. Найдите матрицу плотности квантового состояния $|\psi\rangle = \mathbf{R}\left(\frac{\pi}{3}\right)|0\rangle$.
Решение. Учитывая, что

$$|\psi\rangle = R\left(\frac{\pi}{3}\right)|0\rangle = \cos\left(\frac{\pi}{3}\right)|0\rangle + \sin\left(\frac{\pi}{3}\right)|1\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$$

получим

$$\begin{aligned}
\rho &= |\psi\rangle\langle\psi| = \left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)\left(\frac{1}{2}\langle 0| + \frac{\sqrt{3}}{2}\langle 1|\right), \\
&= \frac{1}{2}\cdot\frac{1}{2}|0\rangle\langle 0| + \frac{\sqrt{3}}{2}\cdot\frac{1}{2}|1\rangle\langle 0| + \frac{1}{2}\cdot\frac{\sqrt{3}}{2}|0\rangle\langle 1| + \frac{\sqrt{3}}{2}\cdot\frac{\sqrt{3}}{2}|1\rangle\langle 1|, \\
&= \frac{1}{4}|0\rangle\langle 0| + \frac{\sqrt{3}}{4}|1\rangle\langle 0| + \frac{\sqrt{3}}{4}|0\rangle\langle 1| + \frac{3}{4}|1\rangle\langle 1|
\end{aligned}$$

или

$$\rho = \begin{pmatrix} \frac{1}{4} & \frac{\sqrt{3}}{4} \\ \frac{\sqrt{3}}{4} & \frac{3}{4} \end{pmatrix} = \frac{1}{4}\begin{pmatrix} 1 & \sqrt{3} \\ \sqrt{3} & 3 \end{pmatrix}. \quad \blacktriangle$$

Задача 4.5. Найдите матрицу плотности квантового состояния $|\psi\rangle = \mathbf{R}(\varphi)|0\rangle$.

1. $\varphi = \left(\frac{\pi}{8}\right)$, **2.** $\varphi = \left(\frac{\pi}{5}\right)$, **3.** $\varphi = \left(\frac{\pi}{6}\right)$, **4.** $\varphi = \left(\frac{\pi}{4}\right)$.

Если для одного фотона всегда можно найти собственный проектор (поляризатор, через который он проходит без искажения), то два фотона могут находится в состояниях и с различной поляризацией. Тогда мы не сможем подобрать такую ориентацию поляризатора, чтобы два фотона проходили через него без затухания. Если для одного фотона данный поляризатор будет собственным, то для другого - нет, и вероятность прохождения через него для второго фотона будет обязательно меньше единицы.

Пучок фотонов, для которого существует собственный проектор называется **чистым.**

Пучок фотонов, для которого собственного проектора не существует называется **смешанным.**

Описание смешанных квантовых состояний особенно эффективно с помощью матриц плотности. Если мы возьмем два различных фотона в состоянии $|\psi_1\rangle$ и $|\psi_2\rangle$, то их смесь описывается матрицей плотности

$$\rho = \frac{1}{2}\,\rho_1 + \frac{1}{2}\,\rho_2 = \frac{1}{2}\left(|\psi_1\rangle\,\langle\psi_1| + |\psi_2\rangle\,\langle\psi_2|\right).$$

Множители $1/2$ учитывают доли каждых фотонов в общем пучке. Если взять не два отдельных фотона, а два пучка фотонов: один из первого лазера с поляризацией $|\psi_1\rangle$, а другой из второго лазера с поляризацией $|\psi_2\rangle$, то смешать их можно с произвольными долями p_1 и p_2 (интенсивностями). Тогда матрица плотности смешанного пучка будет иметь вид

$$\rho = p_1\rho_1 + p_2\rho_2 = p_1\,|\psi_1\rangle\,\langle\psi_1| + p_2\,|\psi_2\rangle\,\langle\psi_2|,$$

где $p_1 + p_2 = 1$.

По матрице плотности чистого пучка $\rho = |\psi\rangle\,\langle\psi|$ можно однозначно восстановить единственное квантовое состояние $|\psi\rangle$.

Утверждение. Квантовый пучок

$$\rho = A\,|0\rangle\,\langle 0| + B\,|0\rangle\,\langle 1| + C\,|1\rangle\,\langle 0| + D\,|1\rangle\,\langle 1|$$

является чистым, если его коэффициенты удовлетворяют соотношениям

$$A^2 + B^2 + C^2 + D^2 = 1.$$

Доказательство. Сформируем чистый пучок $\rho = |\psi\rangle\,\langle\psi|$ кубитом в произвольном состоянии

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

тогда

$$\rho = |\psi\rangle\,\langle\psi| = \alpha^2\,|0\rangle\,\langle 0| + \alpha\beta\,|0\rangle\,\langle 1| + \alpha\beta\,|1\rangle\,\langle 0| + \beta^2\,|1\rangle\,\langle 1|,$$

или

$$A = \alpha^2, \qquad B = \alpha\beta, \qquad C = \alpha\beta, \qquad D = \beta^2$$

и

$$A^2 + B^2 + C^2 + D^2 = \alpha^4 + \alpha^2\beta^2 + \alpha^2\beta^2 + \beta^4 = (\alpha^2 + \beta^2)^2 = 1^2 = 1.$$

Теперь допустим, что пучок

$$\rho = p_1\rho_1 + p_2\rho_2 = p_1\,|\psi_1\rangle\,\langle\psi_1| + p_2\,|\psi_2\rangle\,\langle\psi_2|,$$

сформирован состояниями

$$\begin{aligned} |\psi_1\rangle &= \alpha_1\,|0\rangle + \beta_1\,|1\rangle \\ |\psi_2\rangle &= \alpha_2\,|0\rangle + \beta_2\,|1\rangle, \end{aligned}$$

тогда

$$\rho = (p_1\alpha_1^2 + p_2\alpha_2^2)\,|0\rangle\langle 0| + (p_1\alpha_1\beta_1 + p_2\alpha_2\beta_2)(|0\rangle\langle 1| + |1\rangle\langle 0|) + (p_1\beta_1^2 + p_2\beta_2^2)\,|1\rangle\langle 1|\,,$$

или

$$\begin{aligned} A &= p_1\alpha_1^2 + p_2\alpha_2^2 \\ B &= p_1\alpha_1\beta_1 + p_2\alpha_2\beta_2 \\ C &= p_1\alpha_1\beta_1 + p_2\alpha_2\beta_2 \\ D &= p_1\beta_1^2 + p_2\beta_2^2 \end{aligned}$$

и

$$A^2 + B^2 + C^2 + D^2 = p_1^2 + 2p_1p_2(\alpha_1\alpha_2 + \beta_1\beta_2) + p_2^2 = 1.$$

Последнее равенство удовлетворяется только при

$$\alpha_1\alpha_2 + \beta_1\beta_2 = 1, \qquad \Rightarrow \qquad \alpha_1 = \alpha_2,$$

или

$$(p_1 = 0,\ p_2 = 1), \qquad \text{или} \qquad (p_1 = 1,\ p_2 = 0).$$

Все эти три решения соответствуют чистому пучку, а мы имеем критерий распознования чистого пучка. Аналогичным образом можно доказать утверждение для 3, 4 или n-кубитной смеси. ■

Матрица плотности смешанного пучка может быть описана несколькими способами. Самым распространенным способом описания является разложение матрицы плотности по матрицам Паули

$$\rho = \frac{1}{2}\sum p_i\sigma_i = \frac{1}{2}\left(p_0\sigma_0 + p_1\sigma_1 + p_2\sigma_2 + p_3\sigma_3\right).$$

Сравнивая разложения

$$\begin{aligned} \rho &= \frac{1}{2}\left(p_0\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) + p_1\left(|0\rangle\langle 1| + |1\rangle\langle 0|\right)\right. \\ &+ \left. ip_2\left(|1\rangle\langle 0| - |0\rangle\langle 1|\right) + p_3\left(|0\rangle\langle 0| - |1\rangle\langle 1|\right)\right) \\ &= \frac{1}{2}\left(\left(p_0 + p_3\right)|0\rangle\langle 0| + \left(p_1 - ip_2\right)|0\rangle\langle 1|\right. \\ &+ \left.\left(p_1 + ip_2\right)|1\rangle\langle 0| + \left(p_0 - p_3\right)|1\rangle\langle 1|\right) \end{aligned}$$

и

$$\rho = A\,|0\rangle\langle 0| + B\,|0\rangle\langle 1| + C\,|1\rangle\langle 0| + D\,|1\rangle\langle 1|$$

получим систему

$$\begin{cases} p_0 = A + D \\ p_1 = C + B \\ ip_2 = C - B \\ p_3 = A - D \end{cases}$$

для нахождения неизвестных коэффициентов.

Пример 4.12. В качестве примера рассмотрим смесь двух фотонов, одного в состоянии $|0\rangle\langle 0|$, а другого - в состоянии $|1\rangle\langle 1|$:

$$\rho = A\,|0\rangle\langle 0| + D\,|1\rangle\langle 1|\,,$$

где $A + D = 1$. Через матрицы Паули эта смесь переписывается в виде

$$\rho = \frac{1}{2}\left(\sigma_0 + (A - D)\,\sigma_3\right),$$

или

$$\rho = \frac{1 + A - D}{2}\,|0\rangle\langle 0| + \frac{1 - A + D}{2}\,|1\rangle\langle 1|\,. \quad \blacktriangle$$

По матрицам Паули можно разложить даже чистый пучок, поэтому такое разложение используется в крайнем случае, если факторизовать матрицу плотности на составляющие не удается.

Пример 4.13. Восстановить квантовое состояние кубита по известной матрице плотности

$$\rho = \frac{1}{4}\left(|0\rangle\langle 0| + \sqrt{3}\,|0\rangle\langle 1| + \sqrt{3}\,|1\rangle\langle 0| + 3\,|1\rangle\langle 1|\right)$$

Решение. Сравнивая ρ с выражением

$$\rho = A\,|0\rangle\langle 0| + B\,|0\rangle\langle 1| + C\,|1\rangle\langle 0| + D\,|1\rangle\langle 1|$$

получим

$$A = \frac{1}{4}, \qquad B = \frac{\sqrt{3}}{4}, \qquad C = \frac{\sqrt{3}}{4}, \qquad D = \frac{9}{4}$$

откуда

$$A^2 + B^2 + C^2 + D^2 = \frac{1}{16} + \frac{3}{16} + \frac{3}{16} + \frac{9}{16} = 1.$$

Поэтому наша матрица плотности образована чистым пучком. Тогда из определения

$$|\psi_0\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,,$$

мы получим матрицу плотности

$$\rho_0 = \alpha^2\,|0\rangle\langle 0| + \alpha\beta\,|0\rangle\langle 1| + \beta\alpha\,|1\rangle\langle 0| + \beta^2\,|1\rangle\langle 1|\,.$$

Будем сравнивать исходные данные с матрицей плотности чистого пучка. Имеем

$$\alpha^2 = \frac{1}{4}, \quad \alpha\beta = \frac{\sqrt{3}}{4}, \quad \beta\alpha = \frac{\sqrt{3}}{4}, \quad \beta^2 = \frac{3}{4}.$$

Поскольку $\alpha\beta = \beta\alpha$, то из

$$\alpha^2 = \frac{1}{4} \quad \text{и} \quad \beta^2 = \frac{3}{4} \quad \text{следует} \quad \alpha = \frac{1}{2} \quad \text{и} \quad \beta = \frac{\sqrt{3}}{2}.$$

Таким образом исходный пучок сформирован кубитами в состоянии

$$|\psi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle \quad \text{и} \quad \rho = |\psi\rangle\langle\psi|. \quad \blacktriangle$$

Теперь рассмотрим вопрос, можно ли измерением восстановить способ, каким был приготовлен пучок? Рассмотрим пучок

$$\rho_0 = |\psi_0\rangle\langle\psi_0|, \quad \text{где} \quad |\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle.$$

Очевидно, что через фильтр

$$\Pi_0 = |0\rangle\langle 0|$$

он пройдет с вероятностью α^2, а через фильтр

$$\Pi_1 = |1\rangle\langle 1|$$

он пройдет с вероятностью β^2.

Теперь возьмем два пучка

$$\rho' = |0\rangle\langle 0|, \quad \rho'' = |1\rangle\langle 1|,$$

и создадим из них смесь

$$\rho_1 = \alpha^2\rho' + \beta^2\rho'',$$

Если пропустить теперь пучок ρ_1 через фильтры

$$\Pi_1 = |0\rangle\langle 0| \quad \text{и} \quad \Pi_2 = |1\rangle\langle 1|$$

то результаты измерения будут те же самые, что и для предыдущего состояния ρ_0.

Рассмотрим еще одну смесь, состоящую теперь уже из четырех пучков:

$$\rho_2 = (\alpha^2 - x^2)|0\rangle\langle 0| + (\beta^2 - x^2)|1\rangle\langle 1| + x^2|\psi_1\rangle\langle\psi_1| + x^2|\psi_2\rangle\langle\psi_2|,$$

где

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \quad x \leq 1.$$

Пропуская пучок ρ_2 через фильтры

$$\Pi_1 = |0\rangle\langle 0| \quad \text{и} \quad \Pi_2 = |1\rangle\langle 1|$$

мы опять получим абсолютно те же результаты, что и для ρ_0 и ρ_1.

Таким образом, смешанные пучки с точки зрения свойств поляризации могут вести себя тождественно и по матрице плотности восстановить способ, каким был приготовлен данный пучок практически невозможно. Единственным удачным вариантом является измерение чистого состояния. В этом случае можно найти такое положение поляризатора, которое полностью поглощает пучок. Это означает, что ортогональное состояние является для него собственным. Смешанное состояние никакой ориентацией фильтра погасить не возможно.

Если базисное состояние представить в виде вектора-столбца

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

то кубит

$$|\psi_0\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

можно записать так

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

тогда в матричном представлении матрица плотности кубита

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \cdot (\alpha\ \beta)$$

имеет вид

$$\rho = \begin{pmatrix} \alpha^2 & \alpha\beta \\ \beta\alpha & \beta^2 \end{pmatrix}.$$

Отсюда и происходит ее название. Несмотря на то, что это представление является неудобным для практических расчетов, оно очень эффективно для выяснения всех свойств матрицы плотности.

Основные свойства матрицы плотности:

1) для чистого состояния

$$\rho^2 = \rho;$$

2) след матрицы $a = a_{ik}$ (spur-нем. или trace-англ) - есть сумма его диагональных компонент:

$$Sp\ a = Sp \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11} + a_{22};$$

Для матрицы плотности чистого состояния

$$Sp\ \rho = 1.$$

В самом общем случае матрица плотности может быть записана в виде

$$\rho = A\left|0\right\rangle\left\langle 0\right| + B\left|0\right\rangle\left\langle 1\right| + C\left|1\right\rangle\left\langle 0\right| + D\left|1\right\rangle\left\langle 1\right|,$$

или

$$\rho = \begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

Очевидно, что элементы (A, B, C, D) матрицы плотности ρ можно получить следующим образом:

$$A = \left\langle 0\right|\rho\left|0\right\rangle, \quad B = \left\langle 0\right|\rho\left|1\right\rangle, \quad C = \left\langle 1\right|\rho\left|0\right\rangle, \quad D = \left\langle 1\right|\rho\left|1\right\rangle.$$

Эти коэффициенты имеют следующий смысл:

A - вероятность того, что квантовый пучок ρ, прошедший через поляризатор $|0\rangle$, пройдет через $|0\rangle$;

B - вероятность того, что квантовый пучок ρ, прошедший через поляризатор $|0\rangle$, пройдет через $|1\rangle$;

C - вероятность того, что квантовый пучок ρ, прошедший через поляризатор $|1\rangle$, пройдет через $|0\rangle$;

D - вероятность того, что квантовый пучок ρ, прошедший через поляризатор $|1\rangle$, пройдет через $|1\rangle$.

Наибольший интерес представляют диагональные элементы матрицы плотности:

$$Sp\ \rho = \left\langle 0\right|\rho\left|0\right\rangle + \left\langle 1\right|\rho\left|1\right\rangle = A + D$$

поскольку они имеют непосредственный физический смысл - полной вероятности того, что кубит, приготовленный в состоянии $|\psi\rangle$ будет обнаружен в соответствующем базисном состоянии $|0\rangle$ или $|1\rangle$. Другими словами след матрицы плотности пучка - это сумма результатов его измерения по базисным состояниям:

$$Sp\ \rho = \left\langle 0\right|\rho\left|0\right\rangle + \left\langle 1\right|\rho\left|1\right\rangle = a_{11}^2 + a_{22}^2$$

Поскольку квантовые пучки можно рассматривать в терминах собственных поляризаторов, то естественна и постановка дуальной задачи: рассмотрение измерительного прибора в терминах собственных пучков.

Пусть $|\chi\rangle\langle\chi|$ - проекционный оператор прибора-измерителя, который регистрирует пучок, приготовоенный в состоянии $|\psi\rangle$. Меняя значение состояния

$$\left|\chi\right\rangle = \cos x\left|0\right\rangle + \sin x\left|1\right\rangle$$

с помощью угла x мы получим полную группу событий: прохождение кубита $|\psi\rangle$ через поляризатор $|\chi\rangle\langle\chi|$. Обозначим такой проекционный оператор через $x = |\chi\rangle\langle\chi|$. Тогда каждому значению угла x ставится в соответствие вероятность ее появления (вероятность прохождения $|\psi\rangle$ через фильтр $|\chi\rangle\langle\chi|$). Другими словами x - это случайная величина. Измерение пучка $|\psi\rangle$ по всем состояниям $|\chi\rangle$ даст среднее значение $\overline{x} = \langle x\rangle$:

$$M\left[x\right] = \left\langle x\right\rangle = \left\langle\psi\right| x\left|\psi\right\rangle.$$

4.3 Редуцированные матрицы плотности

Мы описываем квантовое состояние системы с помощью комплексного вектора Гильбертова пространства $\mathbf{H}$ с базисными векторами $|0\rangle$ и $|1\rangle$ и скалярным произведением: $\langle\varphi|\psi\rangle$ [**?**]. Суперпозиция независимых кубитов

$$\begin{aligned} |\psi_1\rangle &= \alpha_1 |0\rangle + \beta_1 |1\rangle \\ |\psi_2\rangle &= \alpha_2 |0\rangle + \beta_2 |1\rangle . \end{aligned}$$

записывается в виде

$$\begin{aligned} |\Psi\rangle &= |\psi_1\rangle \otimes |\psi_1\rangle \\ &= \alpha_1\alpha_2 |0\rangle \otimes |0\rangle + \alpha_1\beta_2 |0\rangle \otimes |1\rangle + \beta_1\alpha_2 |1\rangle \otimes |0\rangle + \beta_1\beta_2 |1\rangle \otimes |1\rangle \\ &= \alpha_1\alpha_2 |00\rangle + \alpha_1\beta_2 |01\rangle + \beta_1\alpha_2 |10\rangle + \beta_1\beta_2 |11\rangle . \end{aligned}$$

Тогда из $\psi_1, \psi_2 \in \mathbf{H}$ следует $\Psi \in \mathbf{H} \otimes \mathbf{H}$. В общем случае, пучок из двух фотонов можно представить в виде вектора в гильбертовом пространстве $\mathbf{H}^2$ с базисом:

$$(|00\rangle , |01\rangle , |10\rangle , |11\rangle) ,$$

например:

$$|\Psi\rangle = a |00\rangle + b |01\rangle + c |10\rangle + d |11\rangle ,$$

где $a^2+b^2+c^2+d^2 = 1$ - условие нормировки, (т.к. $\langle\Psi|\Psi\rangle = 1$). Для такого двумерного квантового состояния можно поставить в соответствие двумерную матрицу плотности:

$$\begin{aligned} \rho = |\Psi\rangle \langle\Psi| &= a^2 |00\rangle \langle 00| + ab |00\rangle \langle 01| + ac |00\rangle \langle 10| + ad |00\rangle \langle 11| \\ &+ ba |01\rangle \langle 00| + b^2 |01\rangle \langle 01| + bc |01\rangle \langle 10| + bd |01\rangle \langle 11| \\ &+ ca |10\rangle \langle 00| + cb |10\rangle \langle 01| + c^2 |10\rangle \langle 10| + cd |10\rangle \langle 11| \\ &+ da |11\rangle \langle 00| + db |11\rangle \langle 01| + dc |11\rangle \langle 10| + d^2 |11\rangle \langle 11| \end{aligned}$$

или

$$\rho = \begin{array}{c} \left(\begin{array}{cccc} a^2 & ab & ac & ad \\ ba & b^2 & bc & bd \\ ca & cb & c^2 & cd \\ da & db & dc & d^2 \end{array} \right) \\ \langle 00| \quad \langle 01| \quad \langle 10| \quad \langle 11| \end{array} \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array}$$

В дальнейшем мы будем записывать только компоненты матрицы плотности

$$\rho = |\Psi\rangle \langle\Psi| = \left(\begin{array}{cccc} a^2 & ab & ac & ad \\ ba & b^2 & bc & bd \\ ca & cb & c^2 & cd \\ da & db & dc & d^2 \end{array} \right) .$$

Пример 4.14. Найти матрицу плотности кубита

$$|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle\,,$$

если

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \qquad |\psi_2\rangle = |0\rangle\,.$$

Решение. Для двумерного квантового состояния имеем

$$|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes |0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right).$$

Тогда по определению матрицы плотности, получим:

$$\begin{aligned}\rho = |\Psi\rangle\langle\Psi| &= \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right)\left(\langle 00| + \langle 10|\right)\frac{1}{\sqrt{2}} \\ &= \frac{1}{2}\left(|00\rangle\langle 00| + |00\rangle\langle 10| + |10\rangle\langle 00| + |10\rangle\langle 10|\right)\end{aligned}$$

или

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \quad \blacktriangle$$

Пример 4.15. Найти матрицу плотности $\rho = |\Psi\rangle\langle\Psi|$ кубита $|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, если

$$|\psi_1\rangle = |1\rangle\,, \qquad |\psi_2\rangle = \frac{1}{2}\left(|0\rangle + \sqrt{3}\,|1\rangle\right).$$

Решение.

$$\begin{aligned}|\Psi\rangle &= \frac{1}{2}\left(|10\rangle + \sqrt{3}\,|11\rangle\right), \\ \rho &= \frac{1}{4}\left(|10\rangle\langle 10| + \sqrt{3}\,|10\rangle\langle 11| + \sqrt{3}\,|11\rangle\langle 10| + 3\,|11\rangle\langle 11|\right)\end{aligned}$$

или

$$\rho = \frac{1}{4}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & \sqrt{3} \\ 0 & 0 & \sqrt{3} & 3 \end{pmatrix}. \quad \blacktriangle$$

Задача 4. 6. Найти матрицу плотности $\rho = |\Psi\rangle\langle\Psi|$ кубита $|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, если

1.

$$|\psi\rangle = \frac{\sqrt{2}\sqrt{5-\sqrt{5}}}{4}\,|0\rangle + \frac{\sqrt{5}+1}{4}\,|1\rangle\,, \quad |\psi'\rangle = \frac{\sqrt{3}}{2}\,|0\rangle + \frac{1}{2}\,|1\rangle\,;$$

2.

$$|\psi\rangle = \frac{\sqrt{2+\sqrt{2}}}{2}|0\rangle + \frac{\sqrt{2-\sqrt{2}}}{2}|1\rangle, \quad |\psi'\rangle = \frac{\sqrt{2}\sqrt{5-\sqrt{5}}}{4}|0\rangle;$$

3.

$$|\psi\rangle = \frac{\sqrt{2+\sqrt{2}}}{2}|0\rangle + \frac{\sqrt{2-\sqrt{2}}}{2}|1\rangle, \quad |\psi'\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle;$$

4.

$$|\psi\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle, \quad |\psi'\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle.$$

Аналогично классической теории вероятностей, по двумерной плотности вероятности можно получить редуцированные плотности ее составляющих :

$$\rho_1 = \sum \langle\rho\rangle_2 =_2 \langle 0|\rho|0\rangle_2 +_2 \langle 1|\rho|1\rangle_2,$$
$$\rho_2 = \sum \langle\rho\rangle_1 =_1 \langle 0|\rho|0\rangle_1 +_1 \langle 1|\rho|1\rangle_1.$$

Суммирование по базисному вектору второго кубита дает редуцированную матрицу плотности первого кубита и наоборот. Используя обозначение следа, последние выражения записываются в виде

$$\rho_1 = Sp_2\ \rho, \quad \rho_2 = Sp_1\rho.$$

Пример 4.16. Найти редуцированные матрицы плотности пучка

$$\rho = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|00\rangle\langle 10| + \frac{1}{2}|10\rangle\langle 00| + \frac{1}{2}|10\rangle\langle 10|.$$

Решение. Найдем редуцированную матрицу плотности 1 кубита:

$$\begin{aligned}
\rho_1 = Sp_2\rho &= \langle 0_2|\rho|0_2\rangle + \langle 1_2|\rho|1_2\rangle \\
&= \frac{1}{2}\left(\langle\underline{0}|0\underline{0}\rangle\langle 0\underline{0}|\underline{0}\rangle + \langle\underline{0}|0\underline{0}\rangle\langle 1\underline{0}|\underline{0}\rangle + \langle\underline{0}|1\underline{0}\rangle\langle 0\underline{0}|\underline{0}\rangle + \langle\underline{0}|1\underline{0}\rangle\langle 1\underline{0}|\underline{0}\rangle\right) \\
&+ \frac{1}{2}\left(\langle\underline{1}|0\underline{0}\rangle\langle 0\underline{0}|\underline{1}\rangle + \langle\underline{1}|0\underline{0}\rangle\langle 1\underline{0}|\underline{1}\rangle + \langle\underline{1}|1\underline{0}\rangle\langle 0\underline{0}|\,|\underline{1}\rangle + \langle\underline{1}|1\underline{0}\rangle\langle 1\underline{0}|\underline{1}\rangle\right) \\
&= \frac{1}{2}\left(1\cdot|0\rangle\langle 0|\cdot 1 + 1\cdot|0\rangle\langle 1|\cdot 1 + 1\cdot|1\rangle\langle 0|\cdot 1 + 1\cdot|1\rangle\langle 1|\cdot 1\right) \\
&+ \frac{1}{2}\left(0\cdot|0\rangle\langle 0|\cdot 0 + 0\cdot|0\rangle\langle 1|\cdot 0 + 0\cdot|1\rangle\langle 0|\cdot 0 + 0\cdot|0\rangle\langle 0|\cdot 0\right) \\
&= \frac{1}{2}\left(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|\right).
\end{aligned}$$

Найдем редуцированную матрицу плотности 2 кубита:

$$\begin{aligned}
\rho_2 = Sp_1\rho &= \langle 0_1|\,\rho\,|0_1\rangle + \langle 1_1|\,\rho\,|1_1\rangle \\
&= \frac{1}{2}\left(\langle\underline{0}|\underline{00}\rangle\,\langle\underline{00}|\underline{0}\rangle + \langle\underline{0}|\underline{00}\rangle\,\langle\underline{1}|\underline{0}\rangle + \langle\underline{0}|\underline{1}0\rangle\,\langle\underline{00}|\underline{0}\rangle + \langle\underline{0}|\underline{1}0\rangle\,\langle\underline{1}|\underline{0}\rangle\right) \\
&+ \frac{1}{2}\left(\langle\underline{1}|\underline{00}\rangle\,\langle\underline{00}|\underline{1}\rangle + \langle\underline{1}|\underline{00}\rangle\,\langle\underline{1}|\underline{1}\rangle + \langle\underline{1}|\underline{1}0\rangle\,\langle\underline{00}|\underline{1}\rangle + \langle\underline{1}|\underline{1}0\rangle\,\langle\underline{1}|\underline{1}\rangle\right) \\
&= \frac{1}{2}\left(1\cdot|0\rangle\,\langle 0|\cdot 1 + 1\cdot|0\rangle\,\langle 0|\cdot 0 + 0\cdot|1\rangle\,\langle 0|\cdot 1 + 0\cdot|1\rangle\,\langle 1|\cdot 0\right) \\
&+ \frac{1}{2}\left(0\cdot|0\rangle\,\langle 0|\cdot 0 + 0\cdot|0\rangle\,\langle 0|\cdot 1 + 1\cdot|0\rangle\,\langle 0|\cdot 0 + 1\cdot|0\rangle\,\langle 0|\cdot 1\right) \\
&= \frac{1}{2}\left(|0\rangle\,\langle 0| + |0\rangle\,\langle 0|\right) = |0\rangle\,\langle 0|
\end{aligned}$$

Таким образом, редуцированные матрицы плотности есть:

$$\rho_1 = \mathrm{Sp}_2\rho = \frac{1}{2}\left(|0\rangle\,\langle 0| + |0\rangle\,\langle 1| + |1\rangle\,\langle 0| + |1\rangle\,\langle 1|\right), \qquad \rho_2 = Sp_1\rho = |0\rangle\,\langle 0|\,,$$

или

$$\rho_1 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \qquad \rho_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \quad \blacktriangle$$

Задача 4.7. Найти редуцированные матрицы плотности пучка

$$\begin{aligned}
\textbf{1.}\ \rho &= \alpha^2\,|00\rangle\,\langle 00| + \alpha\beta\,|00\rangle\,\langle 01| + \alpha\beta\,|01\rangle\,\langle 00| + \beta^2\,|01\rangle\,\langle 01| \\
\textbf{2.}\ \rho &= \alpha^2\,|01\rangle\,\langle 01| + \alpha\beta\,|01\rangle\,\langle 11| + \alpha\beta\,|11\rangle\,\langle 01| + \beta^2\,|11\rangle\,\langle 11| \\
\textbf{3.}\ \rho &= \alpha^2\,|01\rangle\,\langle 01| + \alpha\beta\,|01\rangle\,\langle 10| + \alpha\beta\,|10\rangle\,\langle 01| + \beta^2\,|10\rangle\,\langle 10| \\
\textbf{4.}\ \rho &= \alpha^2\,|00\rangle\,\langle 00| + \alpha\beta\,|00\rangle\,\langle 11| + \alpha\beta\,|11\rangle\,\langle 00| + \beta^2\,|11\rangle\,\langle 11|
\end{aligned}$$

В общем случае для 2 мерной матрицы плотности

$$\begin{aligned}
\rho &= A_{00}\,|00\rangle\,\langle 00| + A_{01}\,|00\rangle\,\langle 01| + A_{02}\,|00\rangle\,\langle 10| + A_{03}\,|00\rangle\,\langle 11| \\
&+ A_{10}\,|01\rangle\,\langle 00| + A_{11}\,|01\rangle\,\langle 01| + A_{12}\,|01\rangle\,\langle 10| + A_{13}\,|01\rangle\,\langle 11| \\
&+ A_{20}\,|10\rangle\,\langle 00| + A_{21}\,|10\rangle\,\langle 01| + A_{22}\,|10\rangle\,\langle 10| + A_{23}\,|10\rangle\,\langle 11| \\
&+ A_{30}\,|11\rangle\,\langle 00| + A_{31}\,|11\rangle\,\langle 01| + A_{32}\,|11\rangle\,\langle 10| + A_{33}\,|11\rangle\,\langle 11|\,;
\end{aligned}$$

$$\rho = \begin{pmatrix} A_{00} & A_{01} & A_{02} & A_{03} \\ A_{10} & A_{11} & A_{12} & A_{13} \\ A_{20} & A_{21} & A_{22} & A_{23} \\ A_{30} & A_{31} & A_{32} & A_{33} \end{pmatrix}$$

редуцированные матрицы плотности можно вычислить по формулам

$$\begin{aligned}
\rho_1 &= Sp_2\rho \\
&+ (A_{00} + A_{11})\,|0\rangle\,\langle 0| + (A_{02} + A_{13})\,|0\rangle\,\langle 1| \\
&+ (A_{20} + A_{31})\,|1\rangle\,\langle 0| + (A_{22} + A_{33})\,|1\rangle\,\langle 1|\,;
\end{aligned}$$

$$\rho_1 = \begin{pmatrix} A_{00}+A_{11} & A_{02}+A_{13} \\ A_{20}+A_{31} & A_{22}+A_{33} \end{pmatrix}$$

и

$$\begin{aligned} \rho_2 &= Sp_1\rho \\ &= (A_{00}+A_{22})\,|0\rangle\langle 0| + (A_{01}+A_{23})\,|0\rangle\langle 1| \\ &+ (A_{10}+A_{32})\,|1\rangle\langle 0| + (A_{11}+A_{33})\,|1\rangle\langle 1|\,; \end{aligned}$$

$$\rho_2 = \begin{pmatrix} A_{00}+A_{22} & A_{01}+A_{23} \\ A_{10}+A_{32} & A_{11}+A_{33} \end{pmatrix}.$$

Пример 4.17. Найти редуцированные матрицы плотности пучка

$$\rho = \frac{1}{26}(2\,|00\rangle\langle 00| + 2\,|00\rangle\langle 10| - 3\,|10\rangle\langle 00| - 5\,|11\rangle\langle 10|).$$

Решение. Перепишем ρ в виде

$$\rho = \begin{pmatrix} A_{00} & A_{01} & A_{02} & A_{03} \\ A_{10} & A_{11} & A_{12} & A_{13} \\ A_{20} & A_{21} & A_{22} & A_{23} \\ A_{30} & A_{31} & A_{32} & A_{33} \end{pmatrix} = \frac{1}{26}\begin{pmatrix} 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 \\ -3 & 0 & 0 & 0 \\ 0 & 0 & -5 & 0 \end{pmatrix}$$

тогда

$$\rho_1 = \begin{pmatrix} A_{00}+A_{11} & A_{02}+A_{13} \\ A_{20}+A_{31} & A_{22}+A_{33} \end{pmatrix} = \frac{1}{26}\begin{pmatrix} 2+0 & 2+0 \\ -3+0 & 0+0 \end{pmatrix} = \frac{1}{26}\begin{pmatrix} 2 & 2 \\ -3 & 0 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} A_{00}+A_{22} & A_{01}+A_{23} \\ A_{10}+A_{32} & A_{11}+A_{33} \end{pmatrix} = \frac{1}{26}\begin{pmatrix} 2+0 & 0+0 \\ 0-5 & 0+0 \end{pmatrix} = \frac{1}{26}\begin{pmatrix} 2 & 0 \\ -5 & 0 \end{pmatrix}$$

или

$$\begin{aligned} \rho_1 &= \frac{1}{26}(2\,|0\rangle\langle 0| + 2\,|0\rangle\langle 1| - 3\,|1\rangle\langle 0|) \\ \rho_2 &= \frac{1}{26}(2\,|0\rangle\langle 0| - 5\,|1\rangle\langle 0|). \quad \blacktriangle \end{aligned}$$

Задача 4.8. Найти редуцированные матрицы плотности пучка

1. $\rho = \frac{1}{18}(|00\rangle\langle 00| + 2\,|00\rangle\langle 01| - 2\,|01\rangle\langle 00| + 3\,|01\rangle\langle 01|)$

2. $\rho = \frac{1}{35}(|01\rangle\langle 01| + 3\alpha\beta\,|01\rangle\langle 11| + 3\alpha\beta\,|11\rangle\langle 01| + 4\beta^2\,|11\rangle\langle 11|)$

3. $\rho = \frac{1}{30}(|01\rangle\langle 01| + 4\alpha\beta\,|01\rangle\langle 10| + 2\alpha\beta\,|10\rangle\langle 01| + 3\beta^2\,|10\rangle\langle 10|)$

4. $\rho = \frac{1}{34}(|00\rangle\langle 00| + 4\alpha\beta\,|00\rangle\langle 11| + 4\alpha\beta\,|11\rangle\langle 01| + \beta^2\,|11\rangle\langle 11|)$

Если пучок сформирован в чистом состоянии, т.е. $\rho = |\Psi\rangle\langle\Psi|$, то редуцированные матрицы плотности ρ_1 и ρ_2 восстанавливаются непосредственно по коэффициентам кубита

$$|\Psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$

следующим образом:

$$\begin{aligned}\rho_1 &= (a^2+b^2)\,|0\rangle\langle 0| + (ac+bd)\,(|0\rangle\langle 1| + |1\rangle\langle 0|) + (c^2+d^2)\,|1\rangle\langle 1|\,,\\ \rho_2 &= (a^2+c^2)\,|0\rangle\langle 0| + (ab+cd)\,(|0\rangle\langle 1| + |1\rangle\langle 0|) + (b^2+d^2)\,|1\rangle\langle 1|\,.\end{aligned}$$

Пример 4.18. Найти редуцированные матрицы плотности кубита

$$|\Psi\rangle = \alpha\,|00\rangle + \beta\,|10\rangle$$

Решение. Поскольку $a = \alpha, \quad b = 0, \quad c = \beta, \quad d = 0$, то

$$\begin{aligned}\rho_1 &= \alpha^2\,|0\rangle\langle 0| + \alpha\beta\,(|0\rangle\langle 1| + |1\rangle\langle 0|) + \beta^2\,|1\rangle\langle 1|\,,\\ \rho_2 &= (\alpha^2+\beta^2)\,|0\rangle\langle 0| = |0\rangle\langle 0|\,. \quad \blacktriangle\end{aligned}$$

Задача 4. 9. Найти редуцированные матрицы плотности кубита

$$\begin{aligned}\textbf{1.}\ |\Psi\rangle &= \frac{1}{\sqrt{26}}(|00\rangle + 3\,|01\rangle + 4\,|10\rangle);\\ \textbf{2.}\ |\Psi\rangle &= \frac{62}{\sqrt{1}}(|00\rangle + 5\,|01\rangle + 6\,|11\rangle);\\ \textbf{3.}\ |\Psi\rangle &= \frac{1}{\sqrt{41}}(|00\rangle + 6\,|10\rangle + 2\,|11\rangle);\\ \textbf{4.}\ |\Psi\rangle &= \frac{1}{\sqrt{21}}(|01\rangle + 2\,|10\rangle + 4\,|11\rangle).\end{aligned}$$

Для кубита $\Psi \in \mathbf{H}^3$:

$$|\Psi\rangle = a_0\,|000\rangle + a_1\,|001\rangle + a_2\,|010\rangle + a_3\,|011\rangle + a_4\,|100\rangle + a_5\,|101\rangle + a_6\,|110\rangle + a_7\,|111\rangle$$

редуцированные матрицы плотности можно получить по формулам:

$$\begin{aligned}\rho_1 &= \left(a_0^2+a_1^2+a_2^2+a_3^2\right)|0\rangle\langle 0| + (a_0a_4+a_1a_5+a_2a_6+a_3a_7)\,(|0\rangle\langle 1| + |1\rangle\langle 0|)\\ &+ \left(a_4^2+a_5^2+a_6^2+a_7^2\right)|1\rangle\langle 1|\,,\\ \rho_2 &= \left(a_0^2+a_1^2+a_4^2+a_5^2\right)|0\rangle\langle 0| + (a_0a_2+a_1a_3+a_4a_6+a_5a_7)\,(|0\rangle\langle 1| + |1\rangle\langle 0|)\\ &+ \left(a_2^2+a_3^2+a_6^2+a_7^2\right)|1\rangle\langle 1|\,,\\ \rho_3 &= \left(a_0^2+a_2^2+a_4^2+a_6^2\right)|0\rangle\langle 0| + (a_0a_1+a_2a_3+a_4a_5+a_6a_7)\,(|0\rangle\langle 1| + |1\rangle\langle 0|)\\ &+ \left(a_1^2+a_3^2+a_5^2+a_7^2\right)|1\rangle\langle 1|\,.\end{aligned}$$

Аналогичным образом несложно вывести общие формулы для $\Psi \in \mathbf{H}^n$. Так, для кубита

$$|\psi\rangle = \sum_{i=0}^{n-1} C_i |i\rangle, \quad \forall \quad i \in FG(n) = FG(2^k),$$

получим

$$\rho_k = \sum_{i=0}^{n-1} R^i_{2^{k-1}} C_i^2 |0\rangle\langle 0| + \sum_{i=0}^{n-1} R^i_{2^{k-1}} \left(C_i C_{i+n/2^k}\right) (|0\rangle\langle 1| + |1\rangle\langle 0|) + \sum_{i=0}^{n-1} \overline{R}^i_{2^{k-1}} C_i^2 |0\rangle\langle 0|.$$

Здесь

$$R^i_m = \frac{1}{2}\left(1 + H^i_m\right), \quad \overline{R}^i_m = \frac{1}{2}\left(1 - H^i_m\right),$$

H^i_m - значение m-й базисной функции Хаара в точке i отрезка $[0, 2^k]$.

Рассмотрим более подробно принципы построения данных выражений. Возмем рекурсивную формулу для построения матриц Адамара

$$H_{k+1} = \begin{pmatrix} H_k & H_k \\ H_k & -H_k \end{pmatrix} \qquad \text{где} \qquad H_0 = 1.$$

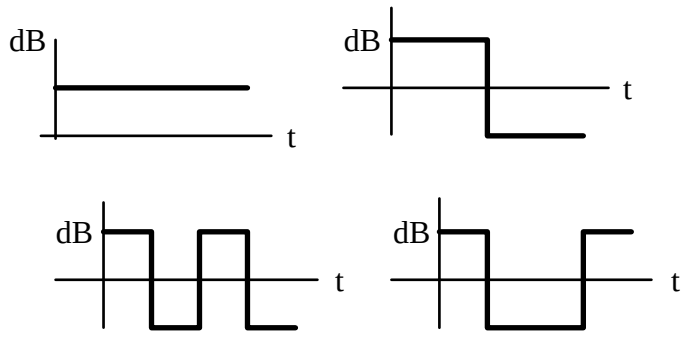
Например

$$H_0 = 1; \quad H_1 = \begin{pmatrix} H_0 & H_0 \\ H_0 & -H_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix};$$

$$H_2 = \begin{pmatrix} H_1 & H_1 \\ H_1 & -H_1 \end{pmatrix} = \left(\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array}\right);$$

$$H_3 = \begin{pmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{pmatrix} = \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{array}\right) \ldots$$

Несложно изобразить функции Адамара графически. Например для H_2 получим



Преобразование Грея

Преобразование Грея - это перестановка элементов таблицы истинности булевой функции таким образом, чтобы ее нижняя половина была симметрична верхней, за исключением старшего бита, который просто инвертируется. Если разделить каждую половину еще пополам, то свойство должно сохранятся для каждой половины и т.д.

★ 2-битное преобразование

$$\begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 00 \\ 01 \\ 10 \\ 11 \end{pmatrix} \Rightarrow \begin{pmatrix} 00 \\ 01 \\ 11 \\ 10 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 3 \\ 2 \end{pmatrix}$$

★ 3-битное преобразование

$$\begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{pmatrix} = \begin{pmatrix} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{pmatrix} \Rightarrow \begin{pmatrix} 000 \\ 001 \\ 011 \\ 010 \\ 110 \\ 111 \\ 101 \\ 100 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 3 \\ 2 \\ 6 \\ 7 \\ 5 \\ 4 \end{pmatrix}$$

Преобразование Грея числа B это его побитовое **XOR** со своим сдвинутым вправо значением:

$$G_i = Gray(B_i) = B_i \oplus B_{i+1}$$

★

$$Gray(4) = Gray(100_2) = \begin{pmatrix} 100 \\ \underline{010} \\ 110 \end{pmatrix} = 110_2 = 6$$

★

$$Gray(13) = Gray(1101_2) = \begin{pmatrix} 1101 \\ \underline{0110} \\ 1011 \end{pmatrix} = 1011_2 = 11$$

Обратный алгоритм – преобразование кода Грея в двоичный код – можно выразить рекуррентной формулой

$$B_i = B_{i+1} \oplus G_{i+1}$$

★

$$G^{-1}(6) = G^{-1}(110_2) = \begin{pmatrix} 110 \\ 011 \\ \underline{001} \\ 100 \end{pmatrix} = 100_2 = 4$$

★

$$G^{-1}(11) = G^{-1}(1011_2) = \left(\begin{array}{c} 1011 \\ 0101 \\ 0010 \\ 0001 \\ \hline 1101 \end{array} \right) = 1101_2 = 13$$

Преобразование Уолша

Функциями Уолша назвывается семейство функций, образующих ортогональную систему, принимающих значения только **1** и **-1** на всей области определения.

4.4 Разложение Шмидта

Утверждение. Произвольное двухкубитное квантовое состояние

$$|\Psi\rangle = a_{00}\,|00\rangle + a_{01}\,|01\rangle + a_{10}\,|10\rangle + a_{11}\,|11\rangle$$

можно представить в виде

$$|\Psi\rangle = \lambda_0\,|x_0 y_0\rangle + \lambda_1\,|x_1 y_1\rangle$$

где (λ_0, λ_1) являются собственными значениями, а состояния (**x,y**) - собственными векторами оператора

$$A = \left(\begin{array}{cc} a_{00} & a_{01} \\ a_{10} & a_{11} \end{array} \right)$$

построенного по коэффициентам кубита $|\Psi\rangle$.

Доказательство данного утверждения удобнее рассматривать с помощью классического матричного исчисления. Действительно, приведем матрицу коэффициентов $|\Psi\rangle$:

$$A = \left(\begin{array}{cc} a_{00} & a_{01} \\ a_{10} & a_{11} \end{array} \right)$$

к диагональному виду

$$L = \left(\begin{array}{cc} \lambda_0 & 0 \\ 0 & \lambda_1 \end{array} \right)$$

с помощью преобразования $L = U^{-1}AU$. После этого, разобъем диагональную матрицу на два слагаемых

$$L = \left(\begin{array}{cc} \lambda_0 & 0 \\ 0 & 0 \end{array} \right) + \left(\begin{array}{cc} 0 & 0 \\ 0 & \lambda_1 \end{array} \right) = L_0 + L_1$$

и произведем обратное преобразование

$$A = ULU^{-1} = UL_0U^{-1} + UL_1U^{-1} = B_0 + B_1.$$

По матрицам B_0 и B_1 элементарно восстанавливаются квантовые состояния $|\mathbf{x}\rangle$ и $|\mathbf{y}\rangle$. Для этого выпишем матрицу унитарного преобразования U в явном виде

$$U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix} \qquad \text{тогда} \qquad U^{-1} = V = \begin{pmatrix} v_{00} & v_{01} \\ v_{10} & v_{11} \end{pmatrix}$$

и

$$L = \begin{pmatrix} \lambda_0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & \lambda_1 \end{pmatrix} = L_0 + L_1$$

Из обратного соотношения получим

$$\begin{aligned} A &= ULU^{-1} = UL_0U^{-1} + UL_1U^{-1} \\ &= \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix} \begin{pmatrix} \lambda_0 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} v_{00} & v_{01} \\ v_{10} & v_{11} \end{pmatrix} + \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & \lambda_1 \end{pmatrix} \begin{pmatrix} v_{00} & v_{01} \\ v_{10} & v_{11} \end{pmatrix} \\ &= \lambda_0 \begin{pmatrix} u_{00}v_{00} & u_{00}v_{01} \\ u_{10}v_{00} & u_{10}v_{01} \end{pmatrix} + \lambda_1 \begin{pmatrix} u_{01}v_{10} & u_{01}v_{11} \\ u_{11}v_{10} & u_{11}v_{11} \end{pmatrix} = \lambda_0(\mathbf{x}_0 \otimes \mathbf{y}_0) + \lambda_1(\mathbf{x}_1 \otimes \mathbf{y}_1), \end{aligned}$$

где (**x**,**y**) - собственные векторы оператора A с компонентами

$$\mathbf{x}_0 = \begin{pmatrix} u_{00} \\ u_{10} \end{pmatrix}, \quad \mathbf{y}_0 = \begin{pmatrix} v_{00} \\ v_{01} \end{pmatrix}, \quad \mathbf{x}_1 = \begin{pmatrix} u_{01} \\ u_{11} \end{pmatrix}, \quad \mathbf{y}_1 = \begin{pmatrix} v_{10} \\ v_{11} \end{pmatrix}. \quad \blacksquare$$

В общем случае, для матрицы (2×2):

$$\lambda_{0,1} = \frac{trA \pm \sqrt{tr^2A - 4\Delta}}{2},$$

где $trA = a_{00} + a_{11}$ след матрицы, а $\Delta = a_{00}a_{11} - a_{01}a_{10}$ ее определитель, квантовое состояние $|\Psi\rangle$ можно записать в виде

$$|\Psi\rangle = \lambda_0 |x_0y_0\rangle + \lambda_1 |x_1y_1\rangle,$$

где

1 серия

$$|x_0\rangle = \frac{1}{\sqrt{a_{01}^2 + (\lambda_0 - a_{00})^2}} \left(a_{01}|0\rangle + (\lambda_0 - a_{00})|1\rangle\right)$$

$$|y_0\rangle = \frac{1}{\sqrt{a_{01}^2 + (\lambda_1 - a_{00})^2}} \left((\lambda_1 - a_{00})|0\rangle - a_{01}|1\rangle\right)$$

$$|x_1\rangle = \frac{1}{\sqrt{a_{01}^2 + (\lambda_1 - a_{00})^2}} \left(a_{01}|0\rangle + (\lambda_1 - a_{00})|1\rangle\right)$$

$$|y_1\rangle = \frac{1}{\sqrt{a_{01}^2 + (\lambda_0 - a_{00})^2}} \left(-(\lambda_0 - a_{00})\,|0\rangle + a_{01}\,|1\rangle\right)$$

Однако на практике данными формулами пользоваться бывает не удобно, поскольку они приводят к возникновению неопределенностей типа $0/0$ в коэффициентах из за выбора способа нормировки собственных векторов. Поэтому приходится искать другие комбинации решений, приводящих к ненулевым собственнным векторам. Для (2×2) матриц возможны 4 различных комбинации построения собственных векторов. Одну из них мы рассмотрели, а остальные приведены ниже.

2 серия

$$|x_0\rangle = \frac{1}{\sqrt{a_{10}^2 + (\lambda_0 - a_{11})^2}} \left((\lambda_0 - a_{11})\,|0\rangle + a_{10}\,|1\rangle\right)$$

$$|y_0\rangle = \frac{1}{\sqrt{a_{10}^2 + (\lambda_1 - a_{11})^2}} \left(-a_{10}\,|0\rangle + (\lambda_1 - a_{11})\,|1\rangle\right)$$

$$|x_1\rangle = \frac{1}{\sqrt{a_{10}^2 + (\lambda_1 - a_{11})^2}} \left((\lambda_1 - a_{11})\,|0\rangle + a_{10}\,|1\rangle\right)$$

$$|y_1\rangle = \frac{1}{\sqrt{a_{10}^2 + (\lambda_0 - a_{11})^2}} \left(a_{10}\,|0\rangle - (\lambda_0 - a_{11})\,|1\rangle\right)$$

3 серия

$$|x_0\rangle = \frac{1}{\sqrt{a_{01}^2 + (\lambda_0 - a_{00})^2}} \left(a_{01}\,|0\rangle + (\lambda_0 - a_{00})\,|1\rangle\right)$$

$$|y_0\rangle = \frac{1}{\sqrt{a_{10}^2 + (\lambda_1 - a_{11})^2}} \left(a_{10}\,|0\rangle - (\lambda_1 - a_{11})\,|1\rangle\right)$$

$$|x_1\rangle = \frac{1}{\sqrt{a_{10}^2 + (\lambda_1 - a_{11})^2}} \left((\lambda_1 - a_{11})\,|0\rangle + a_{10}\,|1\rangle\right)$$

$$|y_1\rangle = \frac{1}{\sqrt{a_{01}^2 + (\lambda_0 - a_{00})^2}} \left((a_{00} - \lambda_0)\,|0\rangle + a_{10}\,|1\rangle\right)$$

4 серия

$$|x_0\rangle = \frac{1}{\sqrt{a_{10}^2 + (\lambda_0 - a_{11})^2}} \left((a_{11} - \lambda_0)\,|0\rangle - a_{10}\,|1\rangle\right)$$

$$|y_0\rangle = \frac{1}{\sqrt{a_{01}^2 + (\lambda_1 - a_{00})^2}} \left((\lambda_1 - a_{00})\,|0\rangle - a_{01}\,|1\rangle\right)$$

$$|x_1\rangle = \frac{1}{\sqrt{a_{01}^2 + (\lambda_1 - a_{00})^2}} \left(a_{01}\,|0\rangle + (\lambda_1 - a_{00})\,|1\rangle\right)$$

$$|y_1\rangle = \frac{1}{\sqrt{a_{10}^2 + (\lambda_0 - a_{11})^2}} \left(a_{10}\,|0\rangle - (\lambda_0 - a_{11})\,|1\rangle\right)$$

Пример 4.19. Найти разложение Шмидта для кубита

$$|\Psi\rangle = \frac{1}{\sqrt{2+2x^2}} \left(|00\rangle + x\,|01\rangle + x\,|10\rangle + |11\rangle\right),$$

где $|x| \leq 1$.

Решение. Для матрицы коэффициентов $|\Psi\rangle$, без нормировки

$$A = \begin{pmatrix} 1 & x \\ x & 1 \end{pmatrix}$$

найдем собственные значения. Для этого вычислим определитель

$$\begin{vmatrix} 1-\lambda & x \\ x & 1-\lambda \end{vmatrix} = 0 \qquad \text{или} \qquad (1-\lambda)^2 - x^2 = 0.$$

Решая квадратное уравнение относительно λ получим два собственных числа $\lambda_0 = 1 - x,\ \lambda_1 = 1 + x$, и согласно **1 серии** формул получим

$$\begin{aligned} |x_0\rangle &= \frac{1}{\sqrt{a_{01}^2 + (\lambda_0 - a_{00})^2}} \left(a_{01}\,|0\rangle + (\lambda_0 - a_{00})\,|1\rangle\right) \\ &= \frac{1}{\sqrt{x^2 + (1-x-1)^2}} \left(x\,|0\rangle + (1-x-1)\,|1\rangle\right) \\ &= \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle\right), \end{aligned}$$

$$\begin{aligned} |y_0\rangle &= \frac{1}{\sqrt{a_{01}^2 + (\lambda_1 - a_{00})^2}} \left((\lambda_1 - a_{00})\,|0\rangle - a_{01}\,|1\rangle\right) \\ &= \frac{1}{\sqrt{x^2 + (1+x-1)^2}} \left((1+x-1)\,|0\rangle - x\,|1\rangle\right) \\ &= \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle\right), \end{aligned}$$

$$\begin{aligned} |x_1\rangle &= \frac{1}{\sqrt{a_{01}^2 + (\lambda_1 - a_{00})^2}} \left(a_{01}\,|0\rangle + (\lambda_1 - a_{00})\,|1\rangle\right) \\ &= \frac{1}{\sqrt{x^2 + (1+x-1)^2}} \left(x\,|0\rangle + (1+x-1)\,|1\rangle\right) \\ &= \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right), \end{aligned}$$

$$\begin{aligned} |y_1\rangle &= \frac{1}{\sqrt{a_{01}^2 + (\lambda_0 - a_{00})^2}} \left(-(\lambda_0 - a_{00})\,|0\rangle + a_{01}\,|1\rangle\right) \\ &= \frac{1}{\sqrt{x^2 + (1-x-1)^2}} \left(-(1-x-1)\,|0\rangle + x\,|1\rangle\right) \\ &= \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right). \end{aligned}$$

Тогда разложение Шмидта

$$|\Psi\rangle = \lambda_0\,|x_0 y_0\rangle + \lambda_1\,|x_1 y_1\rangle$$

с учетом нормировки $\frac{1}{\sqrt{2+2x^2}}$ записывается в виде

$$|\Psi\rangle = \frac{1-x}{\sqrt{2+2x^2}}\ |x_0 y_0\rangle + \frac{1+x}{\sqrt{2+2x^2}}\ |x_1 y_1\rangle,$$

где

$$|x_0\rangle = |y_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right), \qquad |x_1\rangle = |y_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \quad \blacktriangle$$

Пример 4.20. Найти разложение Шмидта квантового состояния

$$|\Psi\rangle = \frac{1}{\sqrt{14}}(|00\rangle + 2\,|10\rangle - 3\,|11\rangle).$$

Решение. Найдем собственные значения матрицы

$$A = \begin{pmatrix} 1 & 0 \\ 2 & -3 \end{pmatrix}.$$

Для этого вычислим определитель

$$\begin{vmatrix} 1-\lambda & 0 \\ 2 & -3-\lambda \end{vmatrix} = 0 \qquad \text{или} \qquad (1-\lambda)(-3-\lambda) - 2\cdot 0 = 0.$$

Решая квадратное уравнение относительно λ получим два собственных числа

$$\lambda_0 = -3, \qquad \lambda_1 = 1.$$

1. Пользуясь **1 серией** формул для $|y_0\rangle$ мы получим получим неопределенность типа $\frac{0}{0}$.

2. Рассмотрим **2 серию** формул:

$$
\begin{aligned}
|x_0\rangle &= \frac{1}{\sqrt{a_{10}^2+(\lambda_0-a_{11})^2}}\left((\lambda_0-a_{11})\,|0\rangle + a_{10}\,|1\rangle\right)\\
&= \frac{1}{\sqrt{2^2+(-3+3)^2}}\left((-3+3)\,|0\rangle + 2\,|1\rangle\right) = |1\rangle\\
|y_0\rangle &= \frac{1}{\sqrt{a_{10}^2+(\lambda_1-a_{11})^2}}\left(-a_{10}\,|0\rangle + (\lambda_1-a_{11})\,|1\rangle\right)\\
&= \frac{1}{\sqrt{2^2+(1+3)^2}}\left(-2\,|0\rangle + (1+3)\,|1\rangle\right) = \frac{1}{\sqrt{5}}\left(-\,|0\rangle + 2\,|1\rangle\right)\\
|x_1\rangle &= \frac{1}{\sqrt{a_{10}^2+(\lambda_1-a_{11})^2}}\left((\lambda_1-a_{11})\,|0\rangle + a_{10}\,|1\rangle\right)\\
&= \frac{1}{\sqrt{2^2+(1+3)^2}}\left((1+3)\,|0\rangle + 2\,|1\rangle\right) = \frac{1}{\sqrt{5}}\left(2\,|0\rangle + |1\rangle\right)\\
|y_1\rangle &= \frac{1}{\sqrt{a_{10}^2+(\lambda_0-a_{11})^2}}\left(a_{10}\,|0\rangle - (\lambda_0-a_{11})\,|1\rangle\right)\\
&= \frac{1}{\sqrt{2^2+(-3+3)^2}}\left(2\,|0\rangle - (-3+3)\,|1\rangle\right) = |0\rangle
\end{aligned}
$$

Теперь разложение Шмидта

$$|\Psi\rangle = \lambda_0\,|x_0y_0\rangle + \lambda_1\,|x_1y_1\rangle$$

с учетом нормировки записывается так

$$|\Psi\rangle = \sqrt{\frac{5}{56}}\ \left(-3\,|x_0y_0\rangle + |x_1y_1\rangle\right),$$

где

$$|x_0\rangle = |1\rangle\,,\ |y_0\rangle = \frac{1}{\sqrt{5}}\ \left(-\,|0\rangle + 2\,|1\rangle\right),\ |x_1\rangle = \frac{1}{\sqrt{5}}\ \left(2\,|0\rangle + |1\rangle\right),\ |y_1\rangle = \left(|0\rangle\right). \quad \blacktriangle$$

Пример 4.21. Найти разложение Шмидта квантового состояния

$$|\Psi\rangle = \frac{1}{\sqrt{10}}(|00\rangle + 3\,|10\rangle\,.$$

Решение. Если не привязываться к собственным векторам, то такого рода задачи решаются устно, без использования сложных расчетов:

$$|\Psi\rangle = \frac{1}{\sqrt{10}}(|00\rangle + 3\,|10\rangle = \frac{1}{\sqrt{10}}(|0\rangle + 3\,|1\rangle) \otimes |0\rangle = |xy\rangle\,,$$

где

$$|x\rangle = \frac{1}{\sqrt{10}}(|0\rangle + 3\,|1\rangle\,, \qquad |y\rangle = |0\rangle\,. \quad \blacktriangle$$

Пример 4.22. Найти разложение Шмидта квантового состояния

$$|\Psi\rangle = \frac{1}{\sqrt{54}}(2\,|00\rangle + 3\,|01\rangle + 4\,|10\rangle + 5\,|11\rangle).$$

Решение. Разбивая на 2 части:

$$\begin{aligned} |\Psi\rangle &= \frac{1}{\sqrt{54}}(|0\rangle \otimes (2\,|0\rangle + 3\,|1\rangle) + |1\rangle \otimes [4\,|0\rangle + 5\,|1\rangle]) \\ &= \frac{\sqrt{13}}{\sqrt{54}}\left(|0\rangle \otimes \frac{1}{\sqrt{13}}(2\,|0\rangle + 3\,|1\rangle)\right) + \frac{\sqrt{41}}{\sqrt{54}}\left(|1\rangle \otimes \frac{1}{\sqrt{41}}(4\,|0\rangle + 5\,|1\rangle)\right) \\ &= \sqrt{\frac{13}{54}}\,|x_1y_1\rangle + \sqrt{\frac{41}{54}}\,|x_2y_2\rangle \end{aligned}$$

получим

$$|x_1\rangle = |0\rangle\,, \qquad |x_2\rangle = |1\rangle$$

$$|y_1\rangle = \frac{1}{\sqrt{13}}(2\,|0\rangle + 3\,|1\rangle), \qquad |y_2\rangle = \frac{1}{\sqrt{41}}(4\,|0\rangle + 5\,|1\rangle). \quad \blacktriangle$$

Задача 4. 10. Найти разложение Шмидта квантовых состояний.

1. $|\Psi\rangle = \frac{1}{\sqrt{70}}\,(5\,|00\rangle + 2\,|01\rangle + 4\,|10\rangle + 3\,|11\rangle)$,

2. $|\Psi\rangle = \frac{1}{\sqrt{93}}\,(4\,|00\rangle + 2\,|01\rangle + 3\,|10\rangle + 8\,|11\rangle)$,

3. $|\Psi\rangle = \frac{1}{\sqrt{78}}\,(3\,|00\rangle + 4\,|01\rangle + 7\,|10\rangle + 2\,|11\rangle)$,

4. $|\Psi\rangle = \frac{1}{\sqrt{186}}\,(5\,|00\rangle + 4\,|01\rangle + 8\,|10\rangle + 9\,|11\rangle)$.

4.5 Зацепленные квантовые состояния

Двумерное квантовое состояние может быть получено суперпозицией одномерных квантовых состояний. В этом случае кубит

$$|\Psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$

может быть факторизован:

$$|\Psi\rangle = |\psi\rangle \otimes |\varphi\rangle\,.$$

Пространство таких квантовых состояний называется сепарабельным $\mathbf{H}\otimes\mathbf{H}$. Однако гильбертово пространство $\mathbf{H}^2$ допускает и несепарабельные подпространства, т.е квантовые двумерные состояния, которые не могут быть разделены. Такие состояния называются зацепленными (entangled - запутанными) квантовыми битами или забитами (ebits) [?]. Если двумерное квантовое состояние является сепарабельным и

$$\begin{array}{l} |\psi\rangle = \alpha_1\,|0\rangle + \beta_1\,|1\rangle \\ |\varphi\rangle = \alpha_2\,|0\rangle + \beta_2\,|1\rangle \end{array},$$

$$|\Psi\rangle = |\psi\rangle \otimes |\varphi\rangle = \alpha_1\alpha_2\,|00\rangle + \alpha_1\beta_2\,|01\rangle + \beta_1\alpha_2\,|10\rangle + \beta_1\beta_2\,|11\rangle\,,$$

то для определения коэффициентов общего состояния

$$|\Psi\rangle = |\psi\rangle \otimes |\varphi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$

нам необходимо решить систему уравнений

$$\left\{\begin{array}{l} \alpha_1\alpha_2 = a, \\ \alpha_1\beta_2 = b, \\ \beta_1\alpha_2 = c, \\ \beta_1\beta_2 = d. \end{array}\right.$$

Если система находится в чистом, незапутанном состоянии, то данная система имеет единственное решение. Если же состояние двух кубитов является зацепленным, то данная система несовместна и решения не имеет. Такое состояние невозможно создать простой суперпозицией кубитов и можно достичь только процессом их перепутывания. Например запутанное квантовое состояние

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

называется состоянием типа Шредингеровского кота, а состояние

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

- это Эйнштейна-Подольского-Розена пара.

Одним из методов проверки, является ли данное состояние сепарабельным является разложение Шмидта:

$$|\Psi\rangle = \lambda_0 |\psi_0\varphi_0\rangle + \lambda_1 |\psi_1\varphi_1\rangle .$$

Очевидно, для того чтобы состояние $|\Psi\rangle$ было сепарабельным необходимо и достаточно, чтобы одно из собственных значений $\lambda_{0,1}$ было равно нулю (например $\lambda_1 = 0$), тогда $|\Psi\rangle = \lambda_0 |\psi_0\varphi_0\rangle$.

Математически квантовый оператор, позволяющий запутать два кубита $|x\rangle$ и $|y\rangle$ называется оператором **CNOT** (Controlled NOT) и дается выражением:

$$\mathbf{P}_{12} |\mathbf{x,y}\rangle = |\mathbf{x,x} \oplus \mathbf{y}\rangle ,$$

где $x \oplus y$ логическая операция сложение по модулю два. Таблица истинности для оператора **CNOT** есть

Вход		Выход	
$\|x\rangle$	$\|y\rangle$	$\|x\rangle$	$\|x \oplus y\rangle$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Графически, действие оператора представляет собой систему преобразующую входные кубиты в некоторые выходные состояния. При этом выход кубита $|y\rangle$ контролируется состоянием кубита $|x\rangle$, поэтому кубит $|x\rangle$ называется контролирующим, а кубит $|y\rangle$ - контролируемым. Очевидно, что оператор может действовать и в обратном порядке:

$$\mathbf{P}_{21} |\mathbf{x,y}\rangle = |\mathbf{x} \oplus \mathbf{y,y}\rangle .$$

В этом случае кубит $|y\rangle$ называется контролирующим, а кубит $|x\rangle$ - контролируемым.

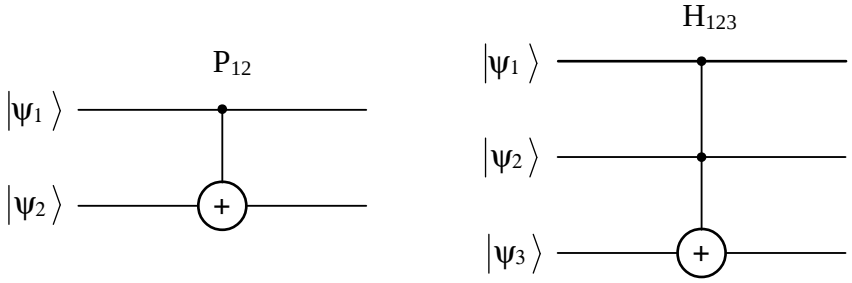


Рис. 4.1: Квантовые операторы CNOT $\mathbf{P}_{21}$ и Тоффоли $\mathbf{H}_{123}$.

Трехкубитный оператор - вентиль Тоффоли определяется следующим выражением:

$$\mathbf{H}_{123} |\mathbf{x,y,z}\rangle = |\mathbf{x,y,x}\&\mathbf{y} \oplus \mathbf{z}\rangle ,$$

с таблицей истинности

Вход			Выход		
$\|x\rangle$	$\|y\rangle$	$\|z\rangle$	$\|x\rangle$	$\|y\rangle$	$\|x\&y \oplus z\rangle$
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Пример 4.23. Найти Квантовое состояние

$$|\psi\rangle = \mathbf{P}_{12}\,|\psi_1\rangle \otimes |\psi_2\rangle \qquad \text{и} \qquad |\Phi\rangle = \mathbf{P}_{21}\,|\psi_1\rangle \otimes |\psi_2\rangle$$

если

$$|\psi_1\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad \text{и} \qquad |\psi_2\rangle = \beta\,|0\rangle - \alpha\,|1\rangle\,.$$

Решение. Найдем результат действия операторов $\mathbf{P}_{12}$ и $\mathbf{P}_{21}$ на суперпозицию $|\psi_1\rangle \otimes |\psi_2\rangle$:

$$\begin{aligned}
|\psi_1\rangle \otimes |\psi_2\rangle &= (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\beta\,|0\rangle - \alpha\,|1\rangle) \\
&= \alpha\beta\,|00\rangle - \alpha^2\,|01\rangle + \beta^2\,|10\rangle - \alpha\beta\,|11\rangle\,; \\
\mathbf{P}_{12}\,|\psi_1\rangle \otimes |\psi_2\rangle &= P_{12}\left(\alpha\beta\,|00\rangle - \alpha^2\,|01\rangle + \beta^2\,|10\rangle - \alpha\beta\,|11\rangle\right) \\
&= \alpha\beta\,|00\rangle - \alpha^2\,|01\rangle + \beta^2\,|11\rangle - \alpha\beta\,|10\rangle\,; \\
\mathbf{P}_{21}\,|\psi_1\rangle \otimes |\psi_2\rangle &= P_{21}\left(\alpha\beta\,|00\rangle - \alpha^2\,|01\rangle + \beta^2\,|10\rangle - \alpha\beta\,|11\rangle\right) \\
&= \alpha\beta\,|00\rangle - \alpha^2\,|11\rangle + \beta^2\,|10\rangle - \alpha\beta\,|01\rangle\,. \quad \blacktriangle
\end{aligned}$$

Задача 4.11. Найти Квантовое состояние

$$|\psi\rangle = \mathbf{P}_{12}\,|\psi_1\rangle \otimes |\psi_2\rangle \qquad \text{и} \qquad |\Phi\rangle = \mathbf{P}_{21}\,|\psi_1\rangle \otimes |\psi_2\rangle$$

если

1. $|\psi_1\rangle = \mathbf{R}\left(\dfrac{\pi}{2}\right)|0\rangle$ и $|\psi_2\rangle = \mathbf{R}\left(\dfrac{\pi}{3}\right)|0\rangle\,,$

2. $|\psi_1\rangle = \mathbf{R}\left(\dfrac{\pi}{3}\right)|0\rangle$ и $|\psi_2\rangle = \mathbf{R}\left(\dfrac{\pi}{4}\right)|0\rangle\,,$

3. $|\psi_1\rangle = \mathbf{R}\left(\dfrac{\pi}{4}\right)|0\rangle$ и $|\psi_2\rangle = \mathbf{R}\left(\dfrac{\pi}{6}\right)|0\rangle\,,$

4. $|\psi_1\rangle = \mathbf{R}\left(\dfrac{\pi}{6}\right)|0\rangle$ и $|\psi_2\rangle = \mathbf{R}\left(\dfrac{\pi}{3}\right)|0\rangle\,.$

4.6 Квантовые алгоритмы

Рассмотрим некоторые квантовые алгоритмы, показывающие особенности, присущие исключительно квантовым вычислениям. Все алгоритмы основаны на использовании запутанных квантовых состояний. Это означает, что действие некоторого оператора на один из кубитов забита автоматически изменяет состояние других членов ансамбля. Возникает квантовый параллелизм - фундаментальное свойство квантовых вычислений, позволяющее за одно обращение к функции $f(x)$ вычислять ее значения при различных аргументах x одновременно.

4.6.1 Алгоритм Дойча

Пусть имееются четыре функции $f_i(x)$ от двоичной переменной $x = 0, 1$. Результаты действия функций на переменные показаны в таблице.

Вход	Выход			
x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
0	0	1	0	1
1	0	1	1	0

Функции $f_1(x)$ и $f_2(x)$ называются "постоянными", поскольку они принимают одинаковое значение независимо от изменения аргумента. Функции $f_3(x)$ и $f_4(x)$ называются "сбалансированными". Задача Дойча ставится следующим образом: определить, к какой группе относится данная функция f (постоянной или сбалансированной)?

При классическом решении данной задачи мы должны определить отдельно $f(0)$ и $f(1)$, т.е. выполнить два обращения к функции f. Использование квантового параллелизма позволяет решить эту задачу за один проход. Для решения задачи рассмотрим квантовый компьютер, состоящий из двух кубитов $|x\rangle$ и $|y\rangle$. Функциям $f_i(x)$ поставим в соответствие операторы $\mathbf{U}_i$:

$$\mathbf{U}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \mathbf{U}_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

$$\mathbf{U}_3 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad \mathbf{U}_4 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Работа компьютера происходит следующим образом. На первом этапе нам необходимо приготовить запутаное состояние квантовых регистров $|x\rangle$ и $|y\rangle$. Например, создадим

Шредингеровскую пару последовательностью действия операторами Адамара $\mathbf{H}$ и CNOT $\mathbf{P}_{12}$ на нулевые кубиты $\psi^{prep} = |xy\rangle = |00\rangle$:

$$|00\rangle \to \mathbf{P}_{12}\mathbf{H}_1 |00\rangle = \mathbf{P}_{12}(|00\rangle + |10\rangle)\frac{1}{\sqrt{2}} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Аналогично, можно получить Шредингеровскую пару с обратной фазой из состояния $\psi^{prep} = |xy\rangle = |10\rangle$:

$$|10\rangle \to \mathbf{P}_{12}\mathbf{H}_1 |10\rangle = \mathbf{P}_{12}(|00\rangle - |10\rangle)\frac{1}{\sqrt{2}} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle).$$

Запишем эти состояния выражением

$$\left|\psi^{in}\right\rangle = \mathbf{P}_{12}\mathbf{H}_1 |\psi^{prep}\rangle = \mathbf{P}_{12}\mathbf{H}_1 |x0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + (-)^x |11\rangle).$$

Вычисления квантового компьютера Дойча осуществляется действием оператором $\mathbf{U}_i$ на входное состояние $|\psi^{in}\rangle$. В результате, на выходе мы получим:

для $\psi^{prep} = |00\rangle$

$\mathbf{U}_i$	$\|\psi^{in}\rangle$	$\|\psi^{out}\rangle$	$\mathbf{P}_{12}\|\psi^{out}\rangle$	$\mathbf{H}_1\mathbf{P}_{12}\|\psi^{out}\rangle$
$\mathbf{U}_1$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|10\rangle)$	$\|00\rangle$
$\mathbf{U}_2$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|11\rangle + \|00\rangle)$	$\frac{1}{\sqrt{2}}(\|10\rangle + \|00\rangle)$	$\|00\rangle$
$\mathbf{U}_3$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|11\rangle + \|01\rangle)$	$\|01\rangle$
$\mathbf{U}_4$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|01\rangle + \|11\rangle)$	$\|01\rangle$

для $\psi^{prep} = |10\rangle$

$\mathbf{U}_i$	$\|\psi^{in}\rangle$	$\|\psi^{out}\rangle$	$\mathbf{P}_{12}\|\psi^{out}\rangle$	$\mathbf{H}_1\mathbf{P}_{12}\|\psi^{out}\rangle$
$\mathbf{U}_1$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|10\rangle)$	$\|10\rangle$
$\mathbf{U}_2$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|11\rangle + \|00\rangle)$	$\frac{1}{\sqrt{2}}(\|10\rangle - \|00\rangle)$	$-\|10\rangle$
$\mathbf{U}_3$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|11\rangle - \|01\rangle)$	$-\|11\rangle$
$\mathbf{U}_4$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|01\rangle - \|11\rangle)$	$\|11\rangle$

После распутывания выходных кубитов, их можно измерить. Измерение второго кубита $|z\rangle$ дает решение задачи. Если $|z\rangle = |0\rangle$, то функция f_i принадлежит к первому классу (постоянная), если же $|z\rangle = |1\rangle$, то функция будет сбалансированной. С учетом фазы результат $\left|\psi^{sol}\right\rangle$ будет иметь вид:

$$\left|\psi^{sol}\right\rangle = (-)^{(x\oplus y)f(x)}\,|x\rangle\,|z\rangle\,.$$

Если в качестве запутанного состояния использовать состояние Эйнштейна-Подольского-Розена, которое создается последовательностью действия операторами Адамара $\mathbf{H}$ и CNOT $\mathbf{P}_{12}$ на кубиты $|\psi^{prep}\rangle = |xy\rangle = |x1\rangle$:

$$\left|\psi^{in}\right\rangle = \mathbf{P}_{12}\mathbf{H}_1\,|\psi^{prep}\rangle = \mathbf{P}_{12}\mathbf{H}_1\,|x1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + (-)^x\,|10\rangle),$$

то на выходе мы получим $|\psi^{out}\rangle = \mathbf{U}_i\,|\psi^{in}\rangle$, а распутанные состояния

$$\left|\psi^{sol}\right\rangle = \sigma_3\mathbf{P}_{12}\mathbf{H}_1\left|\psi^{out}\right\rangle = (-)^{(x\oplus y)f(x)}\,|x\rangle\,|z\rangle\,,$$

позволяют определить класс функции измерением второго кубита $|z\rangle$.

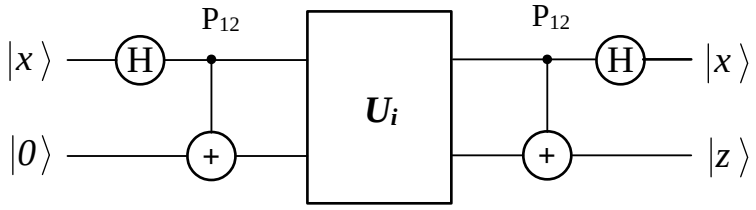


Рис. 4.2: Квантовый компьютер Дойча.

4.6.2 Квантовое плотное кодирование

Перед процессом кодирования получателю и отправителю информации передается по одной части запутанного кубита (состояние типа Шредингеровского кота):

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right).$$

Каждому значению передаваемой последовательности ставится в соответствие однокубитовый оператор

$$I = \sigma_0, X = \sigma_x, Y = i\sigma_y, Z = \sigma_z,$$

которым отправитель действует на первый кубит забита.

Значение	Преобразование	Новое состояние
0	$\psi_0 = (I \otimes I)\,\psi_0$	$\frac{1}{\sqrt{2}}\left(\|00\rangle + \|11\rangle\right)$
1	$\psi_1 = (X \otimes I)\,\psi_0$	$\frac{1}{\sqrt{2}}\left(\|10\rangle + \|01\rangle\right)$
2	$\psi_2 = (Y \otimes I)\,\psi_0$	$\frac{1}{\sqrt{2}}\left(-\|10\rangle + \|01\rangle\right)$
3	$\psi_3 = (Z \otimes I)\,\psi_0$	$\frac{1}{\sqrt{2}}\left(\|00\rangle - \|11\rangle\right)$

Затем получателю по квантовому каналу отправляется первая, преобразованная часть забита.Получатель применяет **CNOT** операцию к полученному забиту.

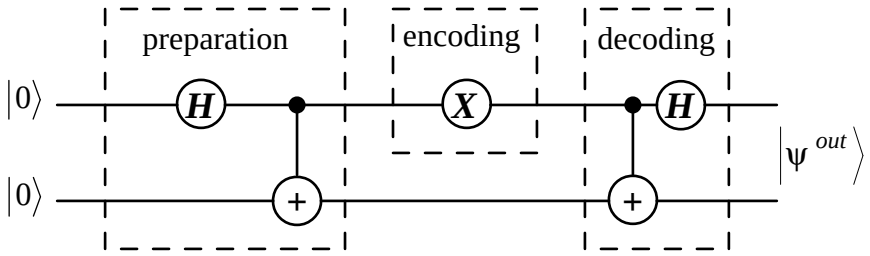
Значение	Первоначальное состояние	C-NOT	Первый кубит	Второй кубит
0	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|0\rangle$
1	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|11\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|1\rangle + \|0\rangle)$	$\|1\rangle$
2	$\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(-\|11\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(-\|1\rangle + \|0\rangle)$	$\|1\rangle$
3	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|0\rangle$

Далее получатель применяет оператор Адамара к первому кубиту

$$H = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z)$$

№	Первый кубит	C-NOT	Первый кубит	Второй кубит
0	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle) + \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)\right)$	$\|0\rangle$	$\|0\rangle$
1	$\frac{1}{\sqrt{2}}(\|1\rangle + \|0\rangle)$	$\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle) + \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)\right)$	$\|0\rangle$	$\|1\rangle$
2	$\frac{1}{\sqrt{2}}(-\|1\rangle + \|0\rangle)$	$\frac{1}{\sqrt{2}}\left(-\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle) + \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)\right)$	$\|1\rangle$	$\|1\rangle$
3	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle) - \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)\right)$	$\|1\rangle$	$\|0\rangle$

Для раскодирования информации получателю необходимо теперь измерить отдельно первый и второй кубиты.



Например, для передачи значения «3» отправитель кодирует свою часть Ш-забита Z-преобразованием и передает получателю. Получатель действует на Ш-забит сначала **CNOT** оператором, затем оператором Адамара. Полученное состояние получатель подвергает измерению. Пусть измерительное устройство настроено на проецирование входящего кубита на состояние

$$|\psi_{\Pi}\rangle = |0\rangle\,,$$

т.е. описывается проекционным оператором

$$\Pi = |\psi_{\Pi}\rangle\,\langle\psi_{\Pi}| = |0\rangle\,\langle 0|\,.$$

Тогда после измерения первого кубита имеем

$$|\psi'\rangle = \Pi\,|1\rangle_1 = |0\rangle\,\langle 0|\,|1\rangle_1 = 0.$$

Такой результат говорит, что состояние кубита и измеряющего устройства были ортогональны. Мы потеряли 1 кубит (он был поглощен измерительным устройством), однако мы получили 1 bit классической информации: оказывается кубит был в состоянии $|1\rangle$. Измеряя второй кубит тем же измерительным устройством получим

$$|\psi'\rangle = \Pi\,|0\rangle_2 = |0\rangle\,\langle 0|\,|0\rangle_2 = |0\rangle\,.$$

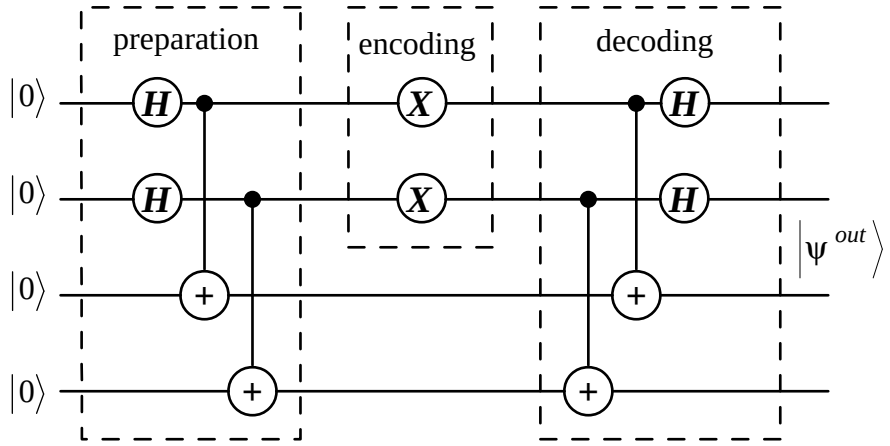
Это означает, что кубит не взаимодействует с измерительным устройством, поглощается детектором и дает нам 2-ой bit классической информации, что кубит был в состоянии $|0\rangle$. Из последней таблицы определяем, что значение передаваемой информации было равно «3». Очевидно, что для передачи всей последовательности из 4 классических бит информации нам необходимо предварительно приготовить 4 Ш-забита и с каждым проделать все описанные выше операции.

Аналогичная схема может быть построена и для передачи 2 кубитов. Для этого создается запутанное состояние

$$|\psi\rangle = \frac{1}{\sqrt{2}}\,(|0000\rangle + |1111\rangle)$$

половина из которого должна быть у получателя. Каждому значению передаваемой последовательности ставится в соответствие суперпозиция однокубитовых операторов

$$I = \sigma_0, X = \sigma_x, Y = i\sigma_y, Z = \sigma_z,$$



которым отправитель действует на первые два кубита забита. Результат работы протокола показан в таблице.

Значение	Кодирование	Декодирование
0	$\psi_0 = (I \otimes I \otimes I \otimes I)\psi_0$	$\|0000\rangle$
1	$\psi_1 = (I \otimes X \otimes I \otimes I)\psi_0$	$\|0001\rangle$
2	$\psi_2 = (I \otimes Y \otimes I \otimes I)\psi_0$	$\|0101\rangle$
3	$\psi_3 = (I \otimes Z \otimes I \otimes I)\psi_0$	$\|0100\rangle$
4	$\psi_4 = (X \otimes I \otimes I \otimes I)\psi_0$	$\|0010\rangle$
5	$\psi_5 = (X \otimes X \otimes I \otimes I)\psi_0$	$\|0011\rangle$
6	$\psi_6 = (X \otimes Y \otimes I \otimes I)\psi_0$	$\|0111\rangle$
7	$\psi_7 = (X \otimes Z \otimes I \otimes I)\psi_0$	$\|0110\rangle$
8	$\psi_8 = (Y \otimes I \otimes I \otimes I)\psi_0$	$\|1010\rangle$
9	$\psi_9 = (Y \otimes X \otimes I \otimes I)\psi_0$	$\|1011\rangle$
10	$\psi_{10} = (Y \otimes Y \otimes I \otimes I)\psi_0$	$\|1111\rangle$
11	$\psi_{11} = (Y \otimes Z \otimes I \otimes I)\psi_0$	$\|1110\rangle$
12	$\psi_{12} = (Z \otimes I \otimes I \otimes I)\psi_0$	$\|1000\rangle$
13	$\psi_{13} = (Z \otimes X \otimes I \otimes I)\psi_0$	$\|1001\rangle$
14	$\psi_{14} = (Z \otimes Y \otimes I \otimes I)\psi_0$	$\|1101\rangle$
15	$\psi_{15} = (Z \otimes Z \otimes I \otimes I)\psi_0$	$\|1100\rangle$

Очевидное обобщение данной схемы позволяет, передавая по квантовому каналу k кубитов, получить на выходе k^2 классических бит информации.

4.6.3 Квантовая телепортация

Другим эффективным алгоритмом, который может реализовываться исключительно квантовыми методами яляется алгоритм квантовой телепортации [?]. Перед процессом телепортации получателю и отправителю информации передается по одной части Шредингеровского забита

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right).$$

Отправитель создает суперпозицию передаваемого кубита

$$|\phi\rangle = a\,|0\rangle + b\,|1\rangle$$

и Ш-забита:

$$|\Psi\rangle = |\phi\rangle \otimes |\psi\rangle = \frac{1}{\sqrt{2}}\left(a\,|000\rangle + a\,|011\rangle + b\,|100\rangle + b\,|111\rangle\right).$$

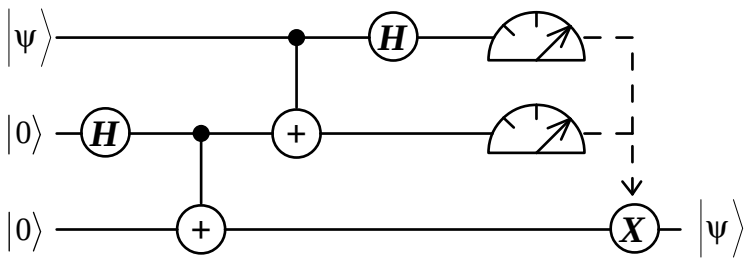
Действуя на первые два свои кубита **CNOT** операцией, а затем оператором Адамара на первый кубит отправитель получает состояние

$$\begin{aligned}\left|\Psi^{out}\right\rangle &= H_1 P_{12}\left|\Psi^{in}\right\rangle_{123} = \frac{1}{\sqrt{2}} H_1\left(a\,|000\rangle + a\,|011\rangle + b\,|110\rangle + b\,|101\rangle\right)\\ &= \frac{1}{2}\left(\begin{array}{l}|00\rangle\left(a\,|0\rangle + b\,|1\rangle\right) + |10\rangle\left(a\,|0\rangle - b\,|1\rangle\right) +\\ |01\rangle\left(a\,|1\rangle + b\,|0\rangle\right) + |11\rangle\left(a\,|1\rangle - b\,|0\rangle\right)\end{array}\right)\end{aligned}$$

Измерение двух первых кубитов отправителем влечет за собой изменение состояния Ш-забита получателя:

Результат измерения	Состояние ЭПР-забита получателя	Преобразование
$\|00\rangle$	$a\,\|0\rangle + b\,\|1\rangle$	$\mathbf{I}\phi$
$\|01\rangle$	$a\,\|1\rangle + b\,\|0\rangle$	$\mathbf{X}\phi$
$\|10\rangle$	$a\,\|0\rangle - b\,\|1\rangle$	$\mathbf{Z}\phi$
$\|11\rangle$	$a\,\|1\rangle - b\,\|0\rangle$	$\mathbf{Y}\phi$

Результат измерения отправитель сообщает получателю по классическому каналу. Эта информация определяет преобразование, которым необходимо подействовать на Ш-забит получателя.



Например, отправитель после проведения операций **CNOT**, **H** и измерения получил результат $|10\rangle$, и передал его по классическому каналу. Тогда, получатель действует согласно таблице, на свой Ш-забит преобразованием

$$Z|\phi\rangle = Z(a|0\rangle - b|1\rangle) = a|1\rangle + b|0\rangle$$

и восстанавливает телепортируемый кубит.

4.7 Коррекция ошибок в квантовых каналах информации

При передачи информации по каналам связи она может искажаться. Алгоритм квантовой коррекции ошибок аналогичен классическому и требует введения дополнительных кубитов для обнаружения и коррекции ошибки.

Рассмотрим тривиальный корректирующий код C, отоброжающий

$$\begin{array}{l} |0\rangle \to |000\rangle \\ |1\rangle \to |111\rangle \end{array}.$$

С помощью этого кода мы можем корректировать единичную ошибку отдельного кубита:

$$E = \{I\otimes I\otimes I, X\otimes I\otimes I, I\otimes X\otimes I, I\otimes I\otimes X\}.$$

Пример 4.24. По квантовому каналу информации передается кубит

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Какое квантовое состояние будет зарегистрировано на приемнике, если оператор ошибки данного канала информации имеет вид

$$E = \frac{1}{2}X\otimes I\otimes I + \frac{\sqrt{3}}{2}I\otimes I\otimes X.$$

Решение. Перед отправлением на исходный кубит

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

действует корректирующий код, поэтому на входе квантового канала информации мы имеем

$$\left|\psi^{in}\right\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

Действие оператора ошибки на передаваемый кубит есть

$$\begin{array}{l} E|\psi^{in}\rangle = \left(\frac{1}{2}X\otimes I\otimes I + \frac{\sqrt{3}}{2}I\otimes I\otimes X\right)\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = \\ = \frac{1}{2\sqrt{2}}(|100\rangle + |011\rangle) + \frac{\sqrt{3}}{2\sqrt{2}}(|001\rangle + |110\rangle) \end{array}$$

Поэтому на выходе из квантового канала информации будет зарегистрировано состояние

$$\left|\psi^{out}\right\rangle = \frac{1}{2\sqrt{2}}\left(|100\rangle + |011\rangle + \sqrt{3}|001\rangle + \sqrt{3}|110\rangle\right). \quad \blacktriangle$$

Задача 4.12.

1. По квантовому каналу информации передается кубит $|\psi\rangle = |0\rangle$. Какое квантовое состояние будет зарегистрировано на приемнике, если оператор ошибки данного канала информации имеет вид

$$E = \frac{1}{\sqrt{2}} I \otimes I \otimes I + \frac{1}{\sqrt{2}} I \otimes X \otimes I.$$

2. По квантовому каналу информации передается кубит $|\psi\rangle = \frac{1}{2}\left(|0\rangle + \sqrt{3}|1\rangle\right)$. Какое квантовое состояние будет зарегистрировано на приемнике, если оператор ошибки данного канала информации имеет вид

$$E = X \otimes I \otimes I.$$

3. По квантовому каналу информации передается кубит $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Какое квантовое состояние будет зарегистрировано на приемнике, если оператор ошибки данного канала информации имеет вид

$$E = \frac{\sqrt{3}}{2} X \otimes I \otimes I + \frac{1}{2} I \otimes I \otimes X.$$

4. По квантовому каналу информации передается кубит $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Какое квантовое состояние будет зарегистрировано на приемнике, если оператор ошибки данного канала информации имеет вид

$$E = \frac{1}{2} I \otimes X \otimes I + \frac{\sqrt{3}}{2} I \otimes I \otimes X.$$

Если мы приняли сигнал

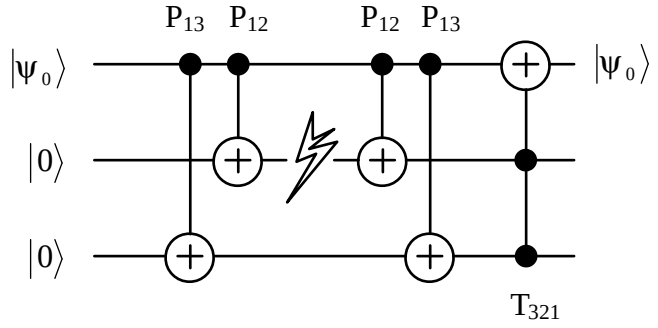
$$\left|\psi^{F}\right\rangle = |e_1, e_2, e_3\rangle,$$

то оператор выделения ошибки есть

$$\mathbf{S}|e_1, e_2, e_3\rangle \to |e_1, e_1 \oplus e_2, e_1 \oplus e_3\rangle$$

и его действие представлено в таблице.

Инвертированный бит	Признак ошибки	Коррекция ошибки
-	$\|000\rangle$	$I \otimes I \otimes I$
0	$\|110\rangle$	$X \otimes I \otimes I$
1	$\|101\rangle$	$I \otimes X \otimes I$
2	$\|011\rangle$	$I \otimes I \otimes X$



Для обнаружения и исправления единичной ошибки удобнее пользоваться следующим оператором

$$|\psi_0\rangle \otimes |z_2 z_3\rangle = \mathbf{T}_{231} S \left|\psi^F\right\rangle |e_1, e_2, e_3\rangle = \mathbf{T}_{231}\mathbf{P}_{12}\mathbf{P}_{13} \left|\psi^F\right\rangle |e_1, e_2, e_3\rangle .$$

Пример 4.25. Определить, какой кубит был передан по зашумленному квантовому каналу информации, если на выходе он имеет состояние

$$\left|\psi^{out}\right\rangle = \frac{1}{2\sqrt{2}} \Big(|100\rangle + |011\rangle + \sqrt{3}|001\rangle + \sqrt{3}|110\rangle\Big) .$$

Решение. Действуя на выходное состояние оператором выделения ошибки, получим

$$\begin{aligned}
|\psi_0\rangle \otimes |z_1 z_2\rangle &= T_{231}P_{12}P_{13}\frac{1}{2\sqrt{2}} \Big(|100\rangle + |011\rangle + \sqrt{3}\,|001\rangle + \sqrt{3}\,|110\rangle\Big) \\
&= T_{231}P_{12}\frac{1}{2\sqrt{2}} \Big(|101\rangle + |011\rangle + \sqrt{3}\,|001\rangle + \sqrt{3}\,|111\rangle\Big) \\
&= T_{231}\frac{1}{2\sqrt{2}} \Big(|111\rangle + |011\rangle + \sqrt{3}\,|001\rangle + \sqrt{3}\,|101\rangle\Big) \\
&= \frac{1}{2\sqrt{2}} \Big(|011\rangle + |111\rangle + \sqrt{3}\,|001\rangle + \sqrt{3}\,|101\rangle\Big) \\
&= \frac{1}{2\sqrt{2}} \left(|011\rangle + |111\rangle\right) + \frac{1}{2\sqrt{2}} \Big(\sqrt{3}\,|001\rangle + \sqrt{3}\,|101\rangle\Big) \\
&= \frac{1}{2\sqrt{2}} \left(|0\rangle + |1\rangle\right) \otimes |11\rangle + \frac{\sqrt{3}}{2\sqrt{2}} \left(|0\rangle + |1\rangle\right) \otimes |01\rangle \\
&= \frac{1}{2} \left(\frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right)\right) \otimes |11\rangle + \frac{\sqrt{3}}{2} \left(\frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right)\right) \otimes |01\rangle \\
&= \left(\frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right)\right) \otimes \left(\frac{1}{2}\,|11\rangle + \frac{\sqrt{3}}{2}\,|01\rangle\right) = |\psi_0\rangle \otimes |z_1 z_2\rangle
\end{aligned}$$

Измеряя два последние бита этого состояния, мы получим $|11\rangle$ (с вероятностью $1/4$) или $|01\rangle$ (с вероятностью $3/4$). В любом случае мы востанавливаем первый кубит

в исходное состояние

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right). \quad \blacktriangle$$

Задача 4. 13. Определить, какой кубит был передан по зашумленному квантовому каналу информации, если на выходе он имеет состояние

1. $|\psi^{out}\rangle = \frac{1}{\sqrt{2}}\left(|111\rangle + |101\rangle\right)$.

2. $|\psi^{out}\rangle = \frac{1}{2}\left(|100\rangle + \sqrt{3}|011\rangle\right)$.

3. $|\psi^{out}\rangle = \frac{1}{2}\left(\sqrt{3}(\alpha|100\rangle + \beta|011\rangle) + \alpha|0010\rangle + \beta|110\rangle\right)$.

4. $|\psi^{out}\rangle = \frac{1}{2}\left(\alpha|010\rangle + \sqrt{3}\alpha|001\rangle + \sqrt{3}\beta|110\rangle + \beta|101\rangle\right)$.

4.8 Клонирование квантовой информации

В 1982 г. Вуттерсом и Зуреком [15] была сформулирована следующая

Теорема. Точное копирование произвольного кубита запрещено.

Доказательство. Действительно, для этого необходимо найти такое унитарное преобразование, которое создает из одного кубита $|\psi\rangle$ два таких же $|\psi\rangle|\psi\rangle$. Т.е. мы должны найти оператор U, действующий на два кубита (один из которых нулевой) так, что

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle.$$

Возьмем ортогональный для $|\psi\rangle$ кубит $|\varphi\rangle$

$$U|\varphi\rangle|0\rangle = |\varphi\rangle|\varphi\rangle.$$

Из этих кубитов составим третий

$$|\phi\rangle = \frac{1}{\sqrt{2}}\left(|\psi\rangle + |\varphi\rangle\right),$$

для которого

$$U|\phi\rangle|0\rangle = U\frac{1}{\sqrt{2}}\left(|\psi\rangle|0\rangle + |\varphi\rangle|0\rangle\right) = \frac{1}{\sqrt{2}}\left(|\psi\rangle|\psi\rangle + |\varphi\rangle|\varphi\rangle\right).$$

С другой стороны

$$U|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle = \frac{1}{2}\left(|\psi\rangle + |\varphi\rangle\right)\left(|\psi\rangle + |\varphi\rangle\right) = \frac{1}{2}\left(|\psi\rangle|\psi\rangle + |\psi\rangle|\varphi\rangle + |\psi\rangle|\varphi\rangle + |\varphi\rangle|\varphi\rangle\right).$$

Поскольку два последних выражения не равны, мы делаем вывод что такого преобразования не существует. ■

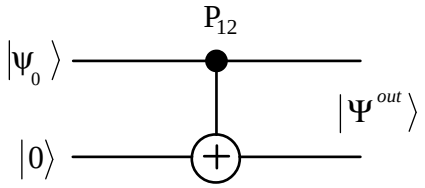
Несмотря на запрет точного клонирования кубитов, использование квантового запутывающего оператора **CNOT** позволяет построить квантовую клонирующую машину, которая создает из одного кубита два одинаковых.

Простейшая квантовая клонирующая машина может быть построена из единственного оператора **CNOT**. Подавая на один вход машины произвольное квантовое состояние $|\psi_0\rangle$

$$|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle,$$

а на другой – кубит в состоянии $|0\rangle$ получим

$$\big|\Psi^{in}\big\rangle = |\psi_0\rangle|0\rangle = \alpha|00\rangle + \beta|10\rangle.$$



Работа квантовой клонрующей машины

сводится к действию оператором **CNOT** на входные кубиты

$$\big|\Psi^{out}\big\rangle = P_{12}\big|\Psi^{in}\big\rangle = \alpha|00\rangle + \beta|11\rangle,$$

и на выходе мы получаем запутанное состояние (забит). Матрица плотности выходного забита дается выражением

$$\rho^{out} = \big|\Psi^{out}\big\rangle\big\langle\Psi^{out}\big|.$$

Редуцированные матрицы плотности выходных кубитов имеют вид

$$\rho^{out}_{1,2} = \alpha^2|0\rangle\langle 0| + \beta^2|1\rangle\langle 1|.$$

На выходе квантовой клонирующей машины получено два одинаковых состояния. Необходимо определить, насколько отличаются выходные состояния от состояния входного кубита $|\psi_0\rangle$. Сравнивая матрицы плотности исходного

$$\rho_0 = |\psi_0\rangle\langle\psi_0| = \alpha^2|0\rangle\langle 0| + \alpha\beta|0\rangle\langle 1| + \alpha\beta|1\rangle\langle 0| + \beta|1\rangle\langle 1|$$

и выходного

$$\rho^{out} = \alpha^2|0\rangle\langle 0| + \beta^2|1\rangle\langle 1|$$

кубитов, нетрудно видеть, что оператор плотности выходного состояния выражается через оператор плотности входа следующим образом:

$$\rho^{out}_{1,2} = \frac{1}{2}\rho^{in}_0 + \frac{1}{2}\rho^{in}_3.$$

Здесь

$$\rho_3 = |\psi_3\rangle\langle\psi_3| = \alpha^2|0\rangle\langle 0| - \alpha\beta|0\rangle\langle 1| - \alpha\beta|1\rangle\langle 0| + \beta|1\rangle\langle 1|,$$
$$|\psi_3\rangle = \sigma_3|\psi_0\rangle = \alpha|0\rangle - \beta|1\rangle.$$

Глядя на это выражение можно сделать предположение, что выходное состояние на 50% совпадает с входным и имеет 50% примеси. Однако более детальное рассмотрение приводит к другому выводу. Действительно, скалярное произведение

$$\langle\psi_0 \mid \psi_3\rangle = \alpha^2 - \beta^2 \neq 0,$$

т.е. состояния не ортогональны, а это означает, что волновые функции $|\psi_0\rangle$ и $|\psi_3\rangle$ перекрываются и часть информации относительно $|\psi_0\rangle$ содержится в матрице плотности ρ_3^{in}. Поэтому для вычисления степени перекрытия волновых состояний вводится понятие точности копирования

$$F = \langle\psi_0|\rho_{1,2}^{out}|\psi_0\rangle = \alpha^4 + \beta^4.$$

Из последнего выражения видно, что точность клонирования зависит от исходного состояния оригинала, а значит полученная квантовая клонирующая машина не является универсальной. Она не сможет клонировать любые, наперед неизвестные, состояния с одинаковой точностью. Усредняя точность F по всем состояниям, получим:

$$\bar{F} = \frac{1}{2\pi}\int_0^{2\pi} F d\theta = \frac{1}{2\pi}\int_0^{2\pi} (\cos^4\theta + \sin^4\theta) d\theta = \frac{3}{4}.$$

Пример 4.26. На вход квантовой клонирующей машины подается два кубита

$$|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\psi_1\rangle = R\left(\frac{\pi}{6}\right)|0\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle).$$

Найти редуцированные матрицы плотности выходных кубитов и определить среднюю точность клонирования.

Решение. На вход квантовой клонирующей машины подается состояние

$$\left|\Psi^{in}\right\rangle = |\psi_0\rangle|\psi_1\rangle = \alpha\frac{1}{2}|00\rangle + \alpha\frac{\sqrt{3}}{2}|01\rangle + \beta\frac{1}{2}|10\rangle + \beta\frac{\sqrt{3}}{2}|11\rangle.$$

Действуя на входное состояние $|\Psi^{in}\rangle$ оператором **CNOT**, получим

$$\left|\Psi^{out}\right\rangle = P_{12}\left|\Psi^{in}\right\rangle = \alpha\frac{1}{2}|00\rangle + \alpha\frac{\sqrt{3}}{2}|01\rangle + \beta\frac{1}{2}|11\rangle + \beta\frac{\sqrt{3}}{2}|10\rangle$$

Редуцированные матрицы плотности выходных кубитов имеют вид

$$\begin{array}{l}\rho_1^{out} = \alpha^2|0\rangle\langle 0| + \frac{\sqrt{3}}{2}\alpha\beta\left(|0\rangle\langle 1| + |1\rangle\langle 0|\right) + \beta^2|1\rangle\langle 1| \\ \rho_2^{out} = \frac{1}{4}(\alpha^2 + 3\beta^2)|0\rangle\langle 0| + (\alpha^2+\beta^2)\frac{\sqrt{3}}{4}\left(|0\rangle\langle 1| + |1\rangle\langle 0|\right) + \frac{1}{4}(3\alpha^2+\beta^2)|1\rangle\langle 1|\end{array}.$$

Найдем точность клонирования

$$\begin{array}{l}F_1 = \langle\psi_0|\rho_1^{out}|\psi_0\rangle = \alpha^4 + \beta^4 + \sqrt{3}\alpha\beta \\ F_2 = \langle\psi_0|\rho_2^{out}|\psi_0\rangle = \frac{1}{4}\alpha^4 + \frac{1}{4}\beta^4 + \frac{3}{2}\alpha^2\beta^2 + \frac{\sqrt{3}}{2}\alpha\beta\end{array}$$

Усредняя точность F по всем состояниям, получим:

$$\begin{array}{l}\bar{F_1} = \frac{1}{2\pi}\int_0^{2\pi} F_1 d\theta = \frac{1}{2\pi}\int_0^{2\pi}\left(\frac{1}{4}\cos^4\theta + \frac{1}{4}\sin^4\theta + \frac{\sqrt{3}}{2}\cos\theta\cdot\sin\theta\right)d\theta = \frac{3}{4} \\ \bar{F_2} = \frac{1}{2\pi}\int_0^{2\pi} F_2 d\theta = \frac{1}{2\pi}\int_0^{2\pi}\left(\frac{1}{4}\cos^4\theta + \frac{1}{4}\sin^4\theta + \frac{3}{2}\cos^2\theta\cdot\sin^2\theta + \frac{\sqrt{3}}{2}\cos\theta\cdot\sin\theta\right)d\theta = \frac{3}{8}\end{array}$$

Задача 4.14. На вход квантовой клонирующей машины подается два кубита $|\psi_0\rangle$ и $|\psi_1\rangle$ Найти редуцированные матрицы плотности выходных кубитов и определить среднюю точность клонирования.

1.

$$|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad |\psi_1\rangle = R\left(\frac{\pi}{4}\right)|0\rangle;$$

2.

$$|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad |\psi_1\rangle = R\left(\frac{\pi}{3}\right)|0\rangle;$$

3.

$$|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad |\psi_1\rangle = R\left(\frac{\pi}{2}\right)|0\rangle;$$

4.

$$|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad |\psi_1\rangle = \cos\phi|0\rangle + \sin\phi|1\rangle.$$

[1, 14]

Литература

[1] *Берлекэмп Э.* Алгебраическая теория кодирования. М.:Мир, 1971 -480 с.

[2] *Блум К.* Теория матрицы плотности и ее приложения. М.:Мир. -248 с.

[3] *Вентцель Е.С., Овчаров Л.А.* Теория вероятностей. М.:Наука, 1969. - 368 с.

[4] *Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А.* Алгеброгеометрические коды. Основные понятия. М.:МЦНМО, 2003. - 504 с.

[5] *Галлагер Р.* Теория информации и надежная связь. М.:Советское радио, 1974. -720 с.

[6] *Гоппа В.Д.* Введение в алгебраическую теорию информации. М.:Физматлит, 1995. -112 с.

[7] *Думачев В.Н.* Модели и алгоритмы квантовой информации. Воронеж: ВИ МВД России, 2009. - 232 с.

[8] *Кострикин А.И.* Основные структуры алгебры. М.:Наука, 2000. - 272 с.

[9] *Морелос-Сарагоса Р.* Искусство помехоустойчивого кодирования. Методы, алгоритмы применение. М.:Техносфера, 2005. - 320 с.

[10] *Самсонов Б.Б, Плохов Е.М., Филоненков А.И.* Компьютерная информатика. РнД:Феникс, 2002. - 512 с.

[11] *Свешников А.А.* Сборник задач по теории вероятностей, математической статистике и теории случайных функций. М.:Наука, 1970. - 448 с.

[12] *Ash Robert B.* Information theory. NY: Interscience, 1965. - 348 p.

[13] *Blahut Richard E.* Algebraic Codes for Data Transmission. NY:Cambridge Univ.Press, 2003. - 498 p.

[14] *Massey James L.* Shift-Register Synthesis and SCH Decoding.
IEEE Trans. Information theory. 1969, V.15, N1, P.122-127. Interscience, 1965. - 348 p.

[15] *Wootters W.K. and Zurek W.H.* A Single Quantum Cannot be Cloned, Nature, 1982, V.299, pp. 802-803.

.

Владислав Николаевич Думачев

ТЕОРИЯ ИНФОРМАЦИИ И КОДИРОВАНИЯ

Подписано в печать 26.12.2011 г. Формат 60×84 1/16.
Бумага офсетная. Гарнитура Таймс новая. Печать офсетная.
Усл.-печ.л. 11,62.
Тираж 100 экз. Заказ № 330

Издательство Воронежского института МВД России
394065, Воронеж, просп. Патриотов, 53

Типография Воронежского института МВД России
394065, Воронеж, просп. Патриотов, 53.