5. ПОМЕХОЗАЩИТНОЕ КОДИРОВАНИЕ

5.1.Формирование базовых параметров систематического помехозащищенного кода

Погружение в проблему, вынесенную в заголовок раздела и параграфа начнем с определений.

Определение 5.1. Код называется *помехонезащищенным* (ПНЗК) кодом, если минимальное кодовое расстояние $d_{\min}\left\{K_i, K_j; i, j=\overline{1,k}\right\}$ между кодовыми комбинациями этого кода *равняется* единице. □

Определение 5.2. Код называется *помехозащищенным* (ПЗК) кодом, если минимальное кодовое расстояние $d_{\min}\left\{K_i, K_j; i, j=\overline{1,n}; n>k\right\}$ между кодовыми комбинациями этого кода *больше* единицы. □

Классическим примером ПНЗК является исходный *информационный код*, несущий информацию о передаваемых сообщениях (командах), имеющий k разрядов, двоичные кодовые комбинации которого строятся на все сочетания, а потому соседние кодовые комбинации этого кода имеют $d_{\min}\left\{K_i, K_j; i, j=\overline{1,k}\right\}$ =1.Обычно такой код задается как (k) – код.

ПЗК обеспечивает условие $d_{\min}\left\{K_i, K_j; i, j=\overline{1,n}; n>k\right\}>1$ за счет введения в структуру кода m избыточных разрядов, именуемых *проверочными*, при этом такой код задается как (n,k) – код, в котором параметр $(n=k+m)$ – полное число разрядов ПЗК, параметр k – число информационных разрядов ПЗК.

Определение 5.3. ПЗК называется *несистематическим,* если число m – проверочных разрядов формируется на основе *эвристических* способов увеличения минимального кодового расстояния между кодовыми комбинациями ПЗК за счет введения проверочных разрядов, которые не обязательно можно разделить с информационными. □

Определение 5.4. ПЗК называется *систематическим,* если m – проверочных разрядов функционально связаны с k – информационными разрядами. □

Определение 5.5. ПЗК называется *линейным* систематическим кодом, если функциональная связь m – проверочных разрядов с k – информационными разрядами является *линейной*. □

Определение 5.6. ПЗК называется *нелинейным* систематическим кодом, если функциональная связь m – проверочных разрядов с k – информационными разрядами является *нелинейной*. □

Ниже рассматривается класс *линейных систематических кодов*.

Определение 5.7. ПЗК называется систематическим кодом с *блоковой систематикой*, если в структуре кода четко зафиксированы позиции информационных и проверочных разрядов. □

Определение 5.8. ПЗК называется систематическим кодом с *полной блоковой систематикой*, если в структуре кода старшие k – являются *информационными* разрядами кода, а младшие m – разрядов являются *проверочными* разрядами кода. □

Определение 5.9. Систематический ПЗК называется кодом с *неполной блоковой систематикой*, если разряды исходного ПНЗК и проверочные разряды ПЗК *перемежаются, не образуя монолитные блоки*. □

Основными параметрами помехозащищенного кода являются:

- число k *информационных* разрядов ПЗК;
- число m *проверочных* разрядов ПЗК;
- полное число разрядов $n = k + m$ ПЗК;
- *минимальное кодовое расстояние* d_{min} на множестве кодовых комбинаций ПЗК;
- число s *исправляемых* ошибок в коде;
- число r *обнаруживаемых* ошибок в коде,

а также параметры, которые будут рассмотрены в параграфе 5.4 раздела.

Значения $k, m, n = k + m$ кода будем рассматривать в качестве *базовых параметров* ПЗК.

Исходными данными для формирования *базовых параметров* помехозащищенного кода являются:

– V_u – объем информационного массива передаваемых сообщений (команд);

– модель искажений в двоичном канале связи в виде информации искажения бита передаваемого кода $p = \max\{p_{01}, p_{10}\}$, где p_{01}, p_{10} – соответственно вероятность трансформации нулевого элементарного сигнала кода в единичный и наоборот;

– характер помехозащиты: *исправление* или *обнаружение* ошибок;

– категория проектируемой системы передачи управляющей (известительной) информации в соответствии с ГОСТ 26.205 – 88Е «Комплексы и устройства телемеханики», характеризующаяся допустимыми вероятностями $P_{доп}$ приема ложной команды (сообщения), сведенными в таблицу 5.1.

Таблица 5.1

	Категория системы передачи информации		
	I	II	III
Допустимая вероятность ложного приема $P_{доп}$	10^{-14}	10^{-10}	10^{-7}

Формирование параметров помехозащищенного (n,k) – кода может осуществлено с помощью алгоритма.

АЛГОРИТМ 5.1

формирования базовых параметров помехозащищенного (n,k) - кода

1. Задать категорию разрабатываемой системы передачи (Пд) – приема (Пр) технической информации (СПдПрТИ), охарактеризовав ее величиной $P_{доп}$ в соответствии с ГОСТ 26.205 – 88Е (таблица 5.1);

2. Получить характеристики предоставленного двоичного канала связи в виде значения $p = \max\{p_{01}, p_{10}\}$ искажения одного бита передаваемых двоичных кодов;

3. Задать информационный массив V_u передаваемых сообщений в виде их числа;

4. Выбрать характер помехозащиты в виде «исправления» ошибок в формируемом ПЗК, полагая возможным в зависимости от назначения СПдПрТИ заменой его «обнаружением» ошибок;

5. Сформировать (вычислить) число k *информационных* разрядов двоичного ПЗК из условия

$$k = \min_k arg\{2^k \geq V_u\}; \qquad (5.1)$$

6. Сформировать (вычислить) число m *проверочных* разрядов ПЗК на основе реализации условия

$$m = \min_{m} arg\left\{ N_c = 2^m - 1 \geq N_\xi = \sum_{i=1}^{s} C_n^i \;\&\; P_{ош} = \sum_{i=s+1}^{n} C_n^i p^i (1-p)^{n-i} \leq P_{доп} \right\}, \quad (5.2)$$

где N_c – число *ненулевых* синдромов (опознавателей, адресов мест) ошибок в коде, N_ξ число ошибок кратности от единицы до s, осуществляемой в виде рекуррентной процедуры:

6.1. Ввести в рассмотрение *первую априорную рабочую гипотезу* (ПАРГ) о том, что «достаточно, чтобы формируемый ПЗК исправлял ошибки только первой кратности» $(s=1)$. В этом случае для вычисления числа *m проверочных* разрядов следует воспользоваться первой частью условия (5.2), которое записывается в виде

$$m = \min_{m} arg\left\{ N_c = 2^m - 1 \geq N_\xi = \sum_{i=1}^{s} C_n^i \Big|_{s=1} = \frac{n!}{1!(n-1)!} = n = k + m \right\}; \quad (5.3)$$

6.2. Провести проверку справедливости ПАРГ для чего следует воспользоваться второй частью условия (5.2), которое записывается в виде

$$P_{ош} = \sum_{i=s+1}^{n} C_n^i p^i (1-p)^{n-i} \Big|_{s=1} = \sum_{i=2}^{n} C_n^i p^i (1-p)^{n-i} \leq P_{доп}; \quad (5.4)$$

Если условие (5.4) выполнятся, то перейти к п.7 алгоритма, в противном случае перейти к п.6.3;

6.3. Ввести в рассмотрение *вторую рабочую гипотезу* (ВРГ) о том, что «достаточно, чтобы формируемый ПЗК исправлял ошибки первой и второй кратностей» $(s=2)$. В этом случае для вычисления числа *m проверочных* разрядов следует воспользоваться первой частью условия (5.2), которое записывается в виде

$$m = \min_{m} arg\left\{ N_c = 2^m - 1 \geq N_\xi = \sum_{i=1}^{s} C_n^i \Big|_{s=2} = C_n^1 + C_n^2 = \frac{(k+m+1)(k+m)}{2} \right\};$$

(5.5)

6.4. Провести проверку справедливости ВРГ для чего следует воспользоваться второй частью условия (5.2), которое записывается в виде

$$P_{ош} = \sum_{i=s+1}^{n} C_n^i p^i (1-p)^{n-i} \Big|_{s=2} = \sum_{i=3}^{n} C_n^i p^i (1-p)^{n-i} \leq P_{доп}; \quad (5.6)$$

Если условие (5.6) выполнятся, то перейти к п.7 алгоритма, в противном случае перейти к п.6.3, в котором наращивать на единицу кратность исправляемой ошибки до выполнения условия (5.2) в полном объеме с целью получения возможности перехода к п.7 алгоритма;

7. Зафиксировать результаты п.п.5 и 6 вычисления параметров систематического ПЗК в форме (n,k) – его представления с целью дальнейшего конструирования его формата средствами *матричного* или *рекуррентного* помехозащитного преобразования кодов. ■

Завершая рассмотрение проблемы формирования базовых параметров систематического помехозащищенного кода, сформулируем следующее определение.

Определение 5.10. Систематический помехозащищенный код, параметры которого удовлетворяют условию (5.3), записанному в форме равенства $n = k + m = 2^m - 1$, называется *оптимальным* ПЗК. □

В таблице 5.2 приведены параметры примеров оптимальных систематических кодов.

Таблица 5.2

Число информационных разрядов ПЗК	k	1	4	11	26	57	120	247	502	1013
Число проверочных разрядов ПЗК	m	2	3	4	5	6	7	8	9	10
Полное число разрядов ПЗК	n	3	7	15	31	63	127	255	511	1023

Оптимальные систематические ПЗК, исправляющие ошибки первой кратности, являются хорошей основой для построения *укороченных* ПЗК, также исправляющих ошибки первой кратности.

Проиллюстрируем алгоритм 5.1 примером.

Пример 5.1. Осуществим формирование *базовых параметров* систематического помехозащищенного кода по следующим исходным данным:

- объем информационного массива передаваемых сообщений (команд) составляет величину $V_u = 60$;

- модель искажений в двоичном канале связи в виде информации искажения бита передаваемого кода $p = \max\left\{p_{01} = 5 \cdot 10^{-5}, p_{10} = 10^{-4}\right\} = 10^{-4}$, где p_{01}, p_{10} – соответственно вероятность трансформации нулевого элементарного сигнала кода в единичный и наоборот;

- характер помехозащиты: исправление;

- категория проектируемой системы передачи III – я с $P_{доп}=10^{-7}$.

Решение

1.Вычислим число $k-$ информационных разрядов кода из условия (5.1) $k=\min\limits_{k} arg\left\{2^k \ge V_u=60\right\}=6;$

2.Вычислим число $m-$ проверочных разрядов ПЗК из условия (5.2), дополнив его ПАРГ о достаточности исправления ошибок первой кратности $(s=1)$,

$$m=\min\limits_{m} arg\left\{N_c=2^m-1\ge N_\xi=\sum_{i=1}^{s}C_n^i\big|_{s=1}=n=k+m=6+m\right\}=4;$$

а также полное число разрядов ПЗК $n=k+m=6+4=10;$

2.1.Проверим справедливость ПАРГ о достаточности $(s=1)$ с помощью (5.4)

$$P_{ош}=\sum_{i=s+1}^{n}C_n^i p^i(1-p)^{n-i}\big|_{s=1}=\sum_{i=2}^{n}C_n^i p^i(1-p)^{n-i}=\sum_{i=2}^{10}C_{10}^i\left(10^{-4}\right)^i\left(1-10^{-4}\right)^{10-i}=$$

$$=\frac{10!}{2!\cdot 8!}\cdot 10^{-8}\cdot(0.9996)^8+\frac{10!}{3!\cdot 7!}\cdot 10^{-12}\cdot(0.9996)^7\cong 4.5\cdot 10^{-7}\ge 10^{-7}=P_{доп};$$

2.2. Условие (5.4) не выполнятся, поэтому вводим в рассмотрение *вторую рабочую гипотезу* (ВРГ) о том, что «достаточно, чтобы формируемый ПЗК исправлял ошибки кратности $s=2$, для вычисления числа m *проверочных* разрядов следует воспользоваться первой частью условия (5.2), которое записывается в

$$m=\min\limits_{m} arg\left\{\begin{array}{l}N_c=2^m-1\ge N_\xi=\sum\limits_{i=1}^{s}C_n^i\big|_{s=2}=C_n^1+C_n^2=n+\dfrac{n!}{2!\cdot(n-2)!}=n+\dfrac{(n-1)n}{2}=\\ =\dfrac{n(n+1)}{2}\dfrac{(k+m+1)(k+m)}{2}=\dfrac{(m+7)(m+6)}{2}\end{array}\right\}=7;$$

при этом полное число разрядов ПЗК $n=k+m=6+7=13;$

2.3. Проверим справедливость ВРГ о достаточности $s=2$ для ПЗК $(13,6)$ с помощью (5.4)

$$P_{ош}=\sum_{i=s+1}^{n}C_n^i p^i(1-p)^{n-i}\big|_{s=2}=\sum_{i=3}^{n}C_n^i p^i(1-p)^{n-i}=\sum_{i=3}^{13}C_{13}^i\left(10^{-4}\right)^i\left(1-10^{-4}\right)^{13-i}=$$

$$=\frac{13!}{3!\cdot 10!}\cdot\left(10^{-12}\right)(0.9996)^{10}+\frac{13!}{4!\cdot 9!}\cdot\left(10^{-16}\right)(0.9996)^9\cong 2.86\cdot 10^{-10}<<P_{доп}=10^{-7}.$$

3. Условие (5.6) выполнятся, в результате сформированы базовые параметры ПЗК $(n,k)=(13,6)$ с полным числом разрядов

$n=13$, с числом информационных разрядов $k=6$ и числом проверочных разрядов $m=7$. ■

5.2. Матричное представление помехозащитного преобразования кодов. Конструирование матриц систематических помехозащищенных кодов

Преобразуемые двоичные коды могут быть представлены *тремя основными способами:* в виде вектора (чаще вектора – строки), *не параметризованного дискретным временем*; в виде модулярных многочленов (ММ) над двоичным простым полем Галуа $GF(p)|_{p=2}=\{0,1\}$ и в виде кодовой последовательности, *параметризованной дискретным временем*. Процессы линейного помехозащитного кодопреобразования в фазах помехозащитного кодирования помехонезащищенного кода (ПНЗК), искажения ПЗК при передаче по двоичному каналу связи, помехозащитного декодирования с целью формирования синдрома (опознавателя) ошибки, свидетельствующего о факте, а возможно и месте ошибки в коде, и коррекции кода, принятого из канала связи, являются частными случаями линейного преобразования кодов, использующие указанные способы представления двоичных кодов.

В данном параграфе используется векторно-матричное представление линейного помехозащитного кодопреобразования, *не параметризованное дискретным временем*, при этом особое внимание обращается *на методы формирования образующей и проверочной матриц* помехозащищенного кода.

Полная схема, описывающая процесс кодирования, состоящий в преобразовании исходного помехонезащищенного кода в помехозащищенный, его передачу по двоичному каналу связи, сопровождающуюся искажением помехозащищенного кода, и процесс декодирования принятого из КС кода с целью формирования кода синдрома (опознавателя) внесенной при передаче ошибки (искажения), приведена на рисунке 5.1.

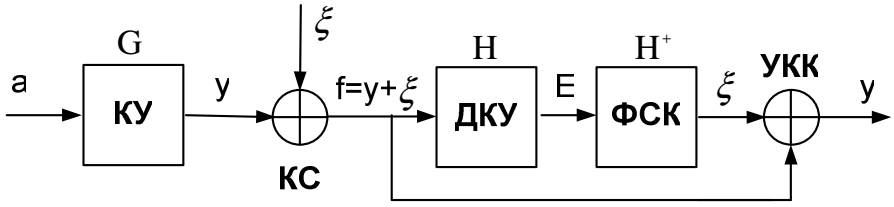

Рисунок 5.1

На рисунке 5.1: КУ – кодирующее устройство; КС – канал связи, искажение в котором моделируется сумматором по модулю два помехозащищенного кода и кода ошибки; ДКУ – декодирующее устройство, формирующее синдром ошибки; a – вектор-строка исходного помехонезащищенного кода, $dim\, a = k$; y – вектор-строка помехозащищенного (n, k)– кода, наблюдаемого на выходе КУ, $dim\, y = n,\ n > k$, $m = n - k$ – число вводимых избыточных разрядов кода y; ξ – вектор-строка помехи, воздействующей на код y при его передаче по КС, $\dim \xi = n$; $f = y + \xi$ – вектор-строка искаженного кода, принимаемого из КС; E – вектор-строка синдрома ошибки (искажения) в принятой из КС кодовой комбинации, $dim\, E = m$.

Процесс формирования *вектор-строки* помехозащищенного кода y из *вектор-строки* помехонезащищенного кода a, осуществляемый в КУ, может быть описан линейным векторно-матричным соотношением

$$y = a\boldsymbol{G}, \qquad (5.7)$$

где $\boldsymbol{G}$ – $(k \times n)$-матрица, именуемая *образующей матрицей* помехозащищенного линейного кода y.

Кодовые (n,k) комбинации ПЗК, сформированные в силу (5.7) именуются *разрешенными кодовыми комбинациями* кода, мощность множества которых составляет величину $[\{(n,k)\}] = [\{y\}] = [\{a\}] = 2^k$, остальные (n) – мерные кодовые комбинации именуются *неразрешенными*, мощность множества которых составляет величину $[\{(n)\}] = 2^n - 2^k$.

Процесс *искажения* передаваемой кодовой комбинации y в канале связи под действием помехи ξ такой, что на выходе КС формируется вектор-строка искаженного кода f, может быть представлен операцией суммирования

$$f = y + \xi, \qquad (5.8)$$

соответствующих вектор-строк.

Процесс декодирования, состоящий в формировании вектор-строки синдрома (опознавателя) E из вектор-строки принятого из КС искаженного кода f может быть описан векторно-матричным соотношением

$$E = f\,\boldsymbol{H}, \qquad (5.9)$$

где $\boldsymbol{H}$ – $(k \times n)$-матрица, именуемая *проверочной* матрицей помехозащищенного кода y.

Заметим, что все операции умножения и суммирования в соотношениях (5.7) – (5.9) и ниже осуществляются по правилам *модулярной арифметики* с модулем два ($\mathrm{mod}\,2$).

Выясним: какими свойствами должна обладать пара матриц $(\boldsymbol{G},\boldsymbol{H})$ с тем, чтобы она порождала помехозащищенный код?

С этой целью сформулируем утверждение.

Утверждение 5.1. Матрица $\boldsymbol{G}$, принятая за *образующую матрицу* ПЗК, и матрица $\boldsymbol{H}$, принятая за *проверочную матрицу*, порождают помехозащищенный код, если они удовлетворяют матричному соотношению

$$\boldsymbol{G}\,\boldsymbol{H} = \boldsymbol{O}. \qquad \square \quad (5.10)$$

Доказательство утверждения строится на использовании соотношений (5.9), (5.8) и (7). Если в (5.9) подставить (5.8), в котором учесть (5.7), то получим цепочку равенств

$$E = f\,\mathbf{H} = (\,y + \xi)\mathbf{H} = (\,a\mathbf{G} + \xi)\mathbf{H} = a\mathbf{G}\mathbf{H} + \xi\mathbf{H}. \qquad (5.11)$$

Напомним, что *помехозащитные декодирующие* устройства кодов, построенные в прямой логике, функционируют так, что *при отсутствии ошибки* в принятой кодовой комбинации декодирующее устройство *формирует нулевой синдром*, а в случае наличия ошибок, для обнаружения или исправления которых осуществлено помехозащитное кодирование, ДКУ формирует ненулевой синдром. Таким образом, ДКУ реализует соотношения

$$E = E(\xi)\big|_{\xi=0} = \mathbf{O}, \quad E = E(\xi)\big|_{\xi\neq 0} \neq \mathbf{O}. \qquad (5.12)$$

Если теперь в (5.11) положить $\xi = 0$, то в силу первого из соотношений (5.12) получим векторно-матричное равенство

$$E = a\boldsymbol{G}\boldsymbol{H} = \boldsymbol{O}, \qquad (5.13)$$

выполняемое при любых вектор-строках исходного кода a, что выполняется только при *справедливости положения* (5.10) утверждения. ■

Очевидно, условие (5.12) выполняется, если вектор – строка ξ *не принадлежит множеству разрешенных* кодовых комбинаций, или если вектор – строка f искаженного в КС кода *принадлежит множеству неразрешенных* кодовых комбинаций.

Примечание 5.1. Следует заметить, что *характеристическое свойство* (5.10) матриц ПЗК не нарушается при *произвольной перестановке строк* местами образующей матрицы $\boldsymbol{G}$ и *столбцов* проверочной матрицы $\boldsymbol{H}$, а также при *перестановке* на любой шаг столбцов матрицы $\boldsymbol{G}$ и *согласованной* с ней перестановке строк матрицы $\boldsymbol{H}$, а также при преобразовании этих матриц путем *произвольного суммирования строк* образующей матрицы $\boldsymbol{G}$ и *столбцов* проверочной матрицы $\boldsymbol{H}$. □

Нетрудно видеть, что соотношения (5.9) – (5.12) содержат доказательство следующего утверждения.

Утверждение 5.2. Процедура *формирования синдрома* E *имеет два эквивалентных представления* (5.11) $E = f\,\mathbf{H}$ и

$$E = \xi\,\mathbf{H}. \qquad \square\blacksquare(5.14)$$

Следует заметить, что векторно-матричные представления (5.11) и (5.14) имеют различную нагрузку и среду использования. Представление (5.11) используется в *аппаратной* среде при формировании синдрома в *сигнальной форме*, а второе (5.14) – в *аналитической при формировании проверочной матрицы* $\boldsymbol{H}$ помехозащищенного кода.

Поставим теперь задачу конструирования алгоритмов формирования образующей $\boldsymbol{G}$ и проверочной $\boldsymbol{H}$ матриц помехозащищенного кода. Нетрудно видеть, что ПЗК, сформированные в силу правила (5.7), являются систематическими и линейными, при этом *вся систематика* помехозащищенного линейного кода y заложена в образующей матрице $\boldsymbol{G}$. Следует заметить также, что в современной телекоммуникационной технике, в которой преобладает передача кодов «*старшим разрядом вперед*», в ПЗК с *полной блоковой систематикой* исходный ПНЗК образует старшие разряды кода, а блок проверочных разрядов – младшие его разряды так, что в помехозащитном КУ $k-$мерный вектор – строка $[a]$ ПНЗК преобразуется в $n-$мерный вектор – строку $[a \mid z]$ПЗК, где $m-$мерный вектор – строка $[z]$ есть вектор – строка проверочных разрядов ПЗК.

С целью *конструирования алгоритмов формирования* матриц $\boldsymbol{G}$ и $\boldsymbol{H}$ ПЗК сформулируем дополнительно следующее утверждение.

Утверждение 5.3 . Если помехозащищенный код *исправляет ошибки кратности* $\gamma = \overline{1,s}$, то *синдром* $E_{j\gamma}$ *ошибки* $\xi_{j\gamma}$ *в* γ *разрядах для* j*-ой их комбинации* $j = \overline{1,C_n^{\gamma}}$ равен сумме по модулю два γ строк $H^i, i = \overline{1,n}$ *проверочной матрицы* $\boldsymbol{H}$ *однократных ошибок, сумма которых образует данную ошибку* $\xi_{j\gamma}$. $\square$

Доказательство утверждения строится на использовании соотношения (5.14), в котором вектор-строку синдрома E, вектор-строку ошибки ξ следует писать в поэлементной форме

$$E = row\left\{E_{\lambda}, \lambda = \overline{1,m}\right\}, \quad \xi = row\left\{\xi_i, i = \overline{1,n}\right\}, \qquad (5.15)$$

а проверочную матрицу $\boldsymbol{H}$ записать в форме *столбца строк*

$$\boldsymbol{H} = col\left\{H^i, i = \overline{1,n}\right\}, \qquad (5.16)$$

где H^i – i-я строка матрицы $\boldsymbol{H}$. Подстановка компонентов соотношения (5.14), представленных в форме (5.15), (5.16), в соотношение (5.14) доказывает справедливость утверждения. ■

Примечание 5.2. Нетрудно видеть, что если при кодировке векторов ошибок ξ векторами-синдромами E при построении ПЗК, исправляющего ошибки кратности $s > 1$ или обнаруживающего ошибки кратности $r > 2$, *учтены условия* утверждения **5.3**, то достаточно иметь *таблицу кодировок ошибок* ξ *только первой кратности*. Ниже при построении алгоритмов формирования матриц $\boldsymbol{G}$ и $\boldsymbol{H}$ кода *предполагается*, что условия утверждения **5.3** выполняются. □

Алгоритмы формирования матриц $\boldsymbol{G}$ и $\boldsymbol{H}$ ПЗК различаются последовательностью этой процедуры. *Первая группа алгоритмов* характеризуется процедурой формирования матриц помехозащищенного кода, в которых сначала конструируется проверочная матрица $\boldsymbol{H}$, а затем на основе сформулированных утверждений вычисляется образующая матрица $\boldsymbol{G}$ ПЗК. *Вторую группу алгоритмов* составляют процедуры, в которые на первом этапе формируется матрица $\boldsymbol{G}$ кода, а затем формируется проверочная матрица $\boldsymbol{H}$ ПЗК.

К сказанному следует добавить, что решение поставленной задачи существенно зависит от уровня блоковой систематики формируемого помехозащищенного кода.

На настоящий момент первую группу алгоритмов в *инвариантной относительно уровня блоковой систематики* ПЗК постановке составляют следующие способы формирования матриц $\boldsymbol{G}$ и $\boldsymbol{H}$:

1. способ, использующий проверочные аналитические равенства процедур декодирования и кодирования;
2. *алгебраический* способ, опирающийся на структуры нуль – пространств (ядер) матриц $\boldsymbol{G}$ и $\mathbf{H}^T$;
3. способ, опирающийся на *системные матрицы* типа *матрицы управляемости* линейных *двоичных динамических систем* рекуррентного помехозащитного декодирования;
4. способ, использующий решение матричного уравнения Сильвестра при формализации *процесса декодирования как процесса наблюдения начального состояния* регистра хранения искажающей двоичной последовательности в двоичном КС, передаваемой по нему двоичной последовательности сформированного в КУ ПЗК.

В данном разделе рассматриваются только первые два способа, второй из которых порожден матричным формализмом векторно-матричного описания процессов помехозащитных кодирования и декодирования. Наиболее *богатую пользовательскую практику* имеет первый способ, который можно назвать *традиционным*, он будет представлен алгоритмом реализации и иллюстрирован примером.

Два последних способа вынесены за пределы настоящего раздела, они рассматриваются и иллюстрируются примерами соответственно в п.п. 6.3 и 6.4.3.

АЛГОРИТМ 5.2

формирования матриц ПЗК с помощью аналитических проверочных равенств при кодировании и декодировании

1. Составить таблицу кодировок векторов-строк однократных ошибок ξ_j векторами-строками синдромов E_j, начиная с ошибки в старшем разряде $\xi_n = [1 \mid \mathbf{O}_{n-1}]$ и заканчивая ошибкой в младшем разряде $\xi_1 = [\mathbf{O}_{n-1} \mid 1]$, где $\boldsymbol{O}_{n-1}$ – $(n-1)$-мерная нулевая вектор-строка, так, что E_j удовлетворяют условиям утверждения 5.3 и принятым техническим соображениям относительно процедуры коррекции искаженного кода.

2. Сформировать проверочную матрицу $\boldsymbol{H}$ на основании составленной таблицы кодировок, которая построчно должна удовлетворять условию

$$\mathbf{H}^j = E_{n+1-j}\ ; \quad j = \overline{1,n}\,. \tag{5.17}$$

3. На основании составленной проверочной матрицы $\boldsymbol{H}$ кода и соотношения (5.9), описывающего процесс формирования синдрома в аппаратной среде ДКУ, составить аналитические выражения для каждого разряда $E_\lambda, \lambda = \overline{m,1}$ синдрома как функции принятой из КС искаженной кодовой комбинации $f = row\{f_{n+1-j}\,;\, j = \overline{1,n}\}$ в силу соотношения

$$E_\lambda = f\,\boldsymbol{H}_{m+1-\lambda}, \lambda = \overline{1,m}, \tag{5.18}$$

где $\boldsymbol{H}_{m+1-\lambda}$ – $(m+1-\lambda)$-ый столбец матрицы $\boldsymbol{H}$.

4. Сформировать аналитические выражения для помехозащитного кодирования помехонезащищенного кода $a = row\{a_i, i = \overline{k,1}\}$, для чего записать соотношения (5.18) в предположении, что в КС отсутствует помеха ($\xi = 0$), положив, тем самым, справедливость выполнения условий

$$E_\lambda = 0, f_{n+1-j} = y_{n+1-j},\ j = \overline{1,n}, \tag{5.19}$$

порождающих систему равенств

$$0 = y\boldsymbol{H}_{m+1-\lambda} = y_{n+1-j},\ \lambda = \overline{1,m}, \tag{5.20}$$

допускающих явное разрешение относительно разрядов y_j ПЗК как функций разрядов a_i помехонезащищенного кода в форме

$$y_j = y_j\left(a_i,\ i = \overline{1,k}\right),\ j = \overline{1,n}. \tag{5.21}$$

5. Сформировать образующую матрицу $\boldsymbol{G} = row\left\{\boldsymbol{G}_j,\ j = \overline{1,n}\right\}$ кода на основании соотношения (5.7) в силу условия

$$\mathbf{G}_j = arg\left\{y_j = a\mathbf{G}_j;\left(a_i,\ i = \overline{1,k}\right);\ j = \overline{1,n}\right\}, \tag{5.22}$$

в котором известны вектор-строка помехонезащищенного кода a, а также линейная связь y_j и a_i в форме (5.21). ■

Проиллюстрируем алгоритм 5.2 примером.

Пример 5.2. Осуществим формирование матриц $\{G, H\}$ на примере помехозащищенного кода Р.Хэмминга (7,4), характеризующегося следующими свойствами:

- полное число разрядов $n = 7$;
- число информационных разрядов $k = 4$;
- число проверочных разрядов $m = 3$ так, что синдромы ошибок в коде имеют трехразрядное представление вида $E_l = \lfloor E_{l3} E_{l2} E_{l1} \rfloor$;
- код является оптимальным так, как выполняется равенство $n = 2^m - 1$;
- минимальное кодовое расстояние между кодовыми комбинациями ПЗК Р.Хэмминга $d_{\min} = 3$;
- код способен исправлять ошибки кратности $s = 1$ в режиме *исправления*;
- код способен обнаруживать ошибки кратности $r = 2$ в режиме *обнаружения*;
- синдромы ошибок в коде строятся по правилу «синдром ошибки является *двоичным кодом номера искаженного разряда*», что позволяет *для исправления* однократных ошибок использовать *стандартный дешифратор* « $CD\ \ (3 \times 8)$ ».

Решение

1. Составим таблицу 5.3 синдромов в результате кодировки векторов-строк однократных ошибок ξ_j векторами-строками

синдромов $E_j\left(j=\overline{7,1}\right)$, начиная с ошибки в старшем (седьмом) разряде и заканчивая ошибкой в младшем (первом) разряде

Таблица 5.3

№ искаженного разряда	ξ_l – вектор-строка искажения в КС	$E_l=[E_{l3}E_{l2}E_{l1}]$ вектор- строка синдрома искажения		
		E_{l3}	E_{l2}	E_{l1}
7	$\xi_7=[1\ 0\ 0\ 0\ 0\ 0\ 0]$	1	1	1
6	$\xi_6=[0\ 1\ 0\ 0\ 0\ 0\ 0]$	1	1	0
5	$\xi_5=[0\ 0\ 1\ 0\ 0\ 0\ 0]$	1	0	1
4	$\xi_4=[0\ 0\ 0\ 1\ 0\ 0\ 0]$	1	0	0
3	$\xi_3=[0\ 0\ 0\ 0\ 1\ 0\ 0]$	0	1	1
2	$\xi_2=[0\ 0\ 0\ 0\ 0\ 1\ 0]$	0	1	0
1	$\xi_1=[0\ 0\ 0\ 0\ 0\ 0\ 1]$	0	0	1

2. Составим проверочную матрицу $\boldsymbol{H}$, используя соотношение (5.17), в результате чего получим в транспонированном виде $H^T=\left\{col\left\{H^j=E_{n+1-j};j=\overline{1,n=7}\right\}\right\}^T=\begin{bmatrix}1&1&1&1&0&0&0\\1&1&0&0&1&1&0\\1&0&1&0&1&0&1\end{bmatrix}$; (5.23)

3. Составим аналитические выражения для каждого разряда $E_\lambda,\lambda=\overline{m,1}$ синдрома в силу соотношения (5.9), которые примут вид

$$[E_3\,E_2\,E_1]=[f_7\ f_6\ f_5\ f_4\ f_3\ f_2\ f_1]\begin{bmatrix}H^1\\H^2\\H^3\\H^4\\H^5\\H^6\\H^7\end{bmatrix}=[f_7\ f_6\ f_5\ f_4\ f_3\ f_2\ f_1]\begin{bmatrix}1&1&1\\1&1&0\\1&0&1\\1&0&0\\0&1&1\\0&1&0\\0&0&1\end{bmatrix}$$

$$\begin{aligned}E_3&=f_7+f_6+f_5+f_4;\\E_2&=f_7+f_6+f_3+f_2;\\E_1&=f_7+f_5+f_3+f_1.\end{aligned}\qquad(5.24)$$

где процедура суммирования осуществляется по правилам двоичной модулярной арифметики. Соотношения (5.24) именуются

проверочными соотношениями при декодировании и кладутся в основу схемотехнической реализации помехозащитного ДКУ.

4. Сформируем *аналитические выражения для помехозащитного кодирования*, используя соотношения (5.24) для *случая отсутствия искажений* в канале связи, характеризующемся выполнением условий $\xi = 0, f = y, E = 0$, в результате чего получим соотношения

$$\begin{aligned} 0 &= y_7 + y_6 + y_5 + y_4; \\ 0 &= y_7 + y_6 + y_3 + y_2; \\ 0 &= y_7 + y_5 + y_3 + y_1. \end{aligned} \qquad (5.25)$$

допускающие однозначные разрешения каждого из уравнений в форме

$$\begin{aligned} y_4 &= y_7 + y_6 + y_5; \\ y_2 &= y_7 + y_6 + y_3; \\ y_1 &= y_7 + y_5 + y_3. \end{aligned} \qquad (5.26)$$

Если в (5.26) положить $y_7 = a_4, y_6 = a_3, y_5 = a_2, y_3 = a_1$, то получим их представления в форме

$$\begin{aligned} y_4 &= a_4 + a_3 + a_2; \\ y_2 &= a_4 + a_3 + a_1; \\ y_1 &= a_4 + a_2 + a_1. \end{aligned} \qquad (5.27)$$

Соотношения (5.27) представляют собой *аналитические выражения для помехозащитного кодирования*, которые кладутся в основу схемотехнической реализации помехозащитного кодирующего устройства, при этом следует заметить, что при разрешении равенств (5.25) в форме (5.27) *проверочными разрядами канонического кода Р.Хэмминга являются разряды, номера которых являются степенью числа два:* $y_1, y_2, y_4, y_8, y_{16}$ K .

5. Сформируем образующую матрицу $\boldsymbol{G} = row\{\boldsymbol{G}_j,\ j = \overline{1,n}\}$ на основе соотношения (5.22), для чего векторно-матричное соотношение $y = aG$ запишем в развернутой в силу (5.27) форме

$$[y_7{=}a_4\ \ y_6{=}a_3\ \ y_5{=}a_2\ \ y_4{=}a_4{+}a_3{+}a_2\ \ y_3{=}a_1\ \ y_2{=}a_4{+}a_3{+}a_1\ \ y_1{=}a_4{+}a_2{+}a_1] = [a_4\, a_3\, a_2\, a_1]\mathrm{G},$$

что позволяет для образующей матрицы G записать

$$G = \begin{bmatrix} G_1 & G_2 & G_3 & G_4 & G_5 & G_6 & G_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}. \quad \blacksquare \ (5.28)$$

Примечание 5.3. Соотношения (5.25) имеют *не единственное разрешение в форме (5.26)*, их можно разрешить относительно

разрядов $\{y_7, y_6, y_5, y_3\}$ ПЗК с проверочной матрицей (5.23) в форме равенств

$$\begin{array}{lll} y_7 = y_4 + y_2 + y_1; & y_7 = y_4 + y_2 + y_1; & y_7 = y_4 + y_2 + y_1; \\ y_6 = y_4 + y_3 + y_1; & y_6 = y_5 + y_2 + y_1; & y_5 = y_6 + y_2 + y_1; \\ y_5 = y_4 + y_3 + y_2. & y_3 = y_5 + y_4 + y_2. & y_3 = y_6 + y_4 + y_1. \end{array} \quad (5.29)$$

Матричные соотношения (5.29) порождают еще *три реализации* образующей матрицы кода Хэмминга (7,4), удовлетворяющей совместно с проверочной матрицей (5.23) характеристическому свойству ПЗК (5.10)

$$G=\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}; G=\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}; G=\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}. \quad \square (5.30)$$

Проверку характеристического свойства (5.10) сформированных пар матриц (5.23) – (5.28) и (5.23) – (5.30) *предлагается выполнить читателю*.

Рассмотрим теперь возможности *алгебраического* способа, опирающегося на структуры *нуль – пространств (ядер) матриц* $\boldsymbol{G}$ и H^T в задаче их формирования. Для этих целей сформулируем следующее утверждение

Утверждение 5.4. Столбцы $\boldsymbol{H}_\lambda, \lambda = \overline{1,m}$ матрицы $\boldsymbol{H}$ принадлежат ядру матрицы $\boldsymbol{G}$ так, что выполняются соотношения

$$\boldsymbol{H}_\lambda \in ker\boldsymbol{G} \vee \boldsymbol{G}\boldsymbol{H}_\lambda = \boldsymbol{O}; \quad (5.31)$$

в свою очередь столбцы $\boldsymbol{G}_j^T, j = \overline{1,k}$ транспонированной $\boldsymbol{G}^T$ образующей матрицы принадлежат ядру транспонированной $\boldsymbol{H}^T$ проверочной матрицы кода так, что выполняются соотношения

$$\boldsymbol{G}_j^T \in ker\boldsymbol{H}^T \vee \boldsymbol{H}^T\boldsymbol{G}_j^T = \boldsymbol{O}. \quad \square (5.32)$$

Доказательство утверждения строится на представлении матричного соотношения (5.10) в векторно-матричной форме с использованием правых вектор-столбцов

$$\boldsymbol{G}\left[\boldsymbol{H}_1 \,\vdots\, \boldsymbol{H}_2 \,\vdots\, \mathrm{K} \,\vdots\, \boldsymbol{H}_\lambda \,\vdots\, \mathrm{K} \,\vdots\, \boldsymbol{H}_m\right] = \boldsymbol{O}, \quad (5.33)$$

что позволяет записать

$$\boldsymbol{G}\boldsymbol{H}_\lambda = \boldsymbol{O}, \lambda = \overline{1,m} \vee \boldsymbol{H}_\lambda \in ker\boldsymbol{G}.$$

В свою очередь матричное соотношение (5.10) в транспонированной форме по аналогии с (5.33) может быть записано в виде

$$\boldsymbol{H}^T\boldsymbol{G}^T = \boldsymbol{H}^T\left[\boldsymbol{G}_1^T \mid \boldsymbol{G}_2^T \mid \mathrm{K} \mid \boldsymbol{G}_j^T \mid \mathrm{K} \mid \boldsymbol{G}_k^T\right] = \boldsymbol{O},$$

что позволяет записать

$$H^{\mathrm{T}}\mathbf{G}_j^{\mathrm{T}} = \mathbf{O},\ j = \overline{1,k} \vee \mathbf{G}_j^{\mathrm{T}} \in kerH^{\mathrm{T}}. \qquad \blacksquare$$

В связи с тем, что конструирование матриц ПЗК обычно начинается *с формирования проверочной матрицы* кода с последующим вычислением образующей матрицы этого кода, то построение алгоритма формирования матриц кода рассматриваемым способом опирается на соотношение (5.32).

АЛГОРИТМ 5.3

формирования матриц ПЗК на основе *алгебраического* способа, опирающегося на структуру *нуль – пространств (ядер) матрицы* H^T

1. Составить таблицу кодировок векторов-строк однократных ошибок ξ_j векторами-строками синдромов E_j, начиная с ошибки в старшем разряде $\xi_n = \left[1 \mid \mathbf{O}_{n-1}\right]$ и заканчивая ошибкой в младшем разряде $\xi_1 = \left[\mathbf{O}_{n-1} \mid 1\right]$, где $\boldsymbol{O}_{n-1}$ – $(n-1)$-мерная нулевая вектор-строка, так, что E_j удовлетворяют условиям утверждения 5.3 и принятым техническим соображениям относительно процедуры коррекции искаженного кода.

2. Сформировать проверочную матрицу $\boldsymbol{H}$ на основании составленной таблицы кодировок, которая построчно должна удовлетворять условию

$$\boldsymbol{H}^j = E_{n+1-j}\ ; \quad j = \overline{1,n}. \qquad (5.34)$$

3. Вычислить транспонированную матрицу H^{T};

4. Вычислить столбцы $\mathbf{G}_j^{\mathrm{T}} = \mathbf{O}$, $j = \overline{1,k}$, принадлежащие ядру матрицы H^{T}: $H^{\mathrm{T}}\mathbf{G}_j^{\mathrm{T}} = \mathbf{O},\ j = \overline{1,k} \vee \mathbf{G}_j^{\mathrm{T}} \in kerH^{\mathrm{T}}$;

5. Сформировать транспонированную образующую матрицу на вычисленных в п.4 алгоритма столбцах в форме

$$G^T = \left[G_1^T \mid G_2^T \mid \mathrm{K} \mid G_j^T \mid \mathrm{K} \mid G_k^T\right];$$

6. Построить образующую матрицу ПЗК, транспонировав матрицу полученную в п.5 алгоритма $\left(\mathbf{G}^T\right)^T = G$, приняв ее за *базовую*;

7. Путем перестановки и суммирования строк матрицы **G**, сформировать такую версию образующей матрицы, которая обладала необходимыми пользовательскими требованиями, главным из которых – *требование размещения проверочных разрядов на позициях младших разрядов* ПЗК.

Пример 5.3. Осуществим формирование матриц $\{G,H\}$ на примере помехозащищенного кода Р.Хэмминга (7,4), рассмотренного в примере 5.2, который при кодировании векторов искажений по схеме Р.Хэмминга получает проверочную матрицу, транспонированная версия которой имеет вид

$$H^T=\begin{bmatrix}1&1&1&1&0&0&0\\1&1&0&0&1&1&0\\1&0&1&0&1&0&1\end{bmatrix}$$

Решение

В связи с тем, что п.п.1 – 3 алгоритма выполнены при решении примера 5.2, то решение начинаем с п.4.

4., 5. Сформируем транспонированную образующую матрицу в форме

$$G^T=col\left\{G_j^T\in kerH^T;j=\overline{1,k}\right\}=\begin{bmatrix}1&0&1&1\\1&1&0&1\\1&1&1&0\\1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix};$$

6. Построим образующую матрицу ПЗК, транспонировав матрицу, полученную в п.5 алгоритма

$$\left(\mathbf{G}^T\right)^T=G=\begin{bmatrix}1&1&1&1&0&0&0\\0&1&1&0&1&0&0\\1&0&1&0&0&1&0\\1&1&0&0&0&0&1\end{bmatrix};\qquad(5.35)$$

7. Примем полученную в п.6 матрицу G за *базовую* с тем, чтобы суммированием и перестановкой строк получить *структуру образующей матрицы* ПЗК с желаемыми пользовательскими свойствами. Здесь это делаться не будет, так как полученная матрица совпадает с первой матрицей банка (5.30). ■

Примечание 5.4. При вычислении ядра $\ker\left(H^T\right)=\mathrm{null}\left(H^{\mathrm{T}}\right)$ матрицы H^{T} были использованы возможности программной оболочки Matlab 6, которая не ориентирована на решение алгебраических задач над двоичным простым полем Галуа $GF(2)$. Но, если матрица H^{T} является целочисленной, то оператор $null\left(H^{\mathrm{T}},'r'\right)$ дает целочисленный результат, который необходимо «спроектировать» на $GF(2)$ с помощью следующих процедур:

- сделать все элементы положительными;
- все четные элементы приравнять нулю;
- все нечетные элементы приравнять единице.

Так при вычислении «[illegible]» для матрицы H^{T} (5.23) получился следующий результат

$$\left(null\left(H^T,'r'\right)\right)^T=\begin{bmatrix}1 & -1 & -1 & 1 & 0 & 0 & 0\\ -2 & 1 & 1 & 0 & 1 & 0 & 0\\ -1 & 0 & 1 & 0 & 0 & 1 & 0\\ -1 & 1 & 0 & 0 & 0 & 0 & 1\end{bmatrix},$$

который с помощью перечисленных процедур приведен к виду (5.35).□

Теперь обратимся к проблеме конструирования матриц ПЗК, характеризующегося полной *блоковой систематикой*. Для этих целей сформулируем утверждение.

Утверждение 5.5. *Матрицы* $\boldsymbol{G}$ *и* $\boldsymbol{H}$ *, сформированные в виде*

$$\boldsymbol{G}=\left[\boldsymbol{I}_k \mid \tilde{\boldsymbol{G}}\right],\ \boldsymbol{H}=\begin{bmatrix}\tilde{\boldsymbol{G}}\\ \boldsymbol{I}_m\end{bmatrix}. \qquad (5.36)$$

где $\boldsymbol{I}_k$ *–* $k\times k$ *-единичная матрица,* $\boldsymbol{I}_m$ *–* $m\times m$ *-единичная матрица,* $\tilde{\boldsymbol{G}}$ *–* $k\times m$ *-матрица синдромов однократных ошибок вида*

$$\xi=\left[\tilde{\xi} \mid \mathbf{O}_m\right]', \qquad (5.37)$$

где $\tilde{\xi}$ *–* k *-мерный вектор-строка, содержащий одну единицу,* $\boldsymbol{O}_m$ *–* m *-мерная нулевая вектор-строка, порождают помехозащищенный код, обладающий полной блоковой систематикой.* □

Доказательство утверждения в первой части состоит в непосредственной подстановке матриц $\boldsymbol{G}$ и $\boldsymbol{H}$ вида (5.36) в (5.10) для проверки сохранения характеристического свойства, которая приводит в силу правил модулярной арифметики к следующей цепочке равенств

$$\boldsymbol{GH}=\left[\boldsymbol{I}_k \mid \tilde{\boldsymbol{G}}\right]\begin{bmatrix}\tilde{\boldsymbol{G}}\\ \boldsymbol{I}_m\end{bmatrix}=\tilde{\boldsymbol{G}}+\tilde{\boldsymbol{G}}=\boldsymbol{O}.$$

Доказательство второй части утверждения строится на подстановке матрицы $\boldsymbol{G}$ вида (5.36) в (5.7)

$$y = a\boldsymbol{G} = a\left[\boldsymbol{I} \mid \tilde{\boldsymbol{G}}\right] = \left[a \mid a\tilde{\boldsymbol{G}}\right], \qquad (5.38)$$

что обнаруживает полную блоковую систематику ПЗК y. ■

АЛГОРИТМ 5.4

формирования матриц ПЗК с *полной блоковой систематикой*

1. Сформировать $k-$ разрядный ПНЗК на основе мощности $[Q] = V_u$ заданного массива Q передаваемой или хранимой информации так, что

$$k = minarg\left\{2^k \geq V_u = [Q]\right\}.$$

2. Сформировать число m проверочных разрядов, удовлетворяющих требованием к достоверности передачи или хранения информации и к способу реализации корректирующей способности синтезируемого ПЗК.

3. Составить таблицу кодировок векторов-строк однократных ошибок ξ_j векторами-строками синдромов E_j, начиная с ошибки в старшем разряде $\xi_n = \left[1 \mid \mathbf{O}_{n-1}\right]$ и заканчивая ошибкой в младшем разряде $\xi_1 = \left[\mathbf{O}_{n-1} \mid 1\right]$, где $\boldsymbol{O}_{n-1} - (n-1)$-мерная нулевая вектор-строка, так, что E_j удовлетворяют условиям утверждения 5.3 и принятым техническим соображениям относительно процедуры коррекции искаженного кода, но при этом так, чтобы кодировка вектор-строк однократных ошибок ξ_j в m младших разрядах помехозащищенного (n,k)-кода векторами-строками синдромов E_j в последних m синдромах в таблице кодировок позволила образовывать $m \times m-$ единичную матрицу $\boldsymbol{I}_m$.

4. Сформировать проверочную матрицу $\boldsymbol{H}$ на основании составленной таблицы кодировок, которая построчно должна удовлетворять условию

$$\mathbf{H}^j = E_{n+1-j}\ ; \quad j = \overline{1,n},$$

и которая с учетом кодировки вектор-строк однократных ошибок ξ_j в m младших разрядах, осуществленных в п.3, оказывается наделенной *полной блоковой систематикой* так, что принимает вид

$$\mathbf{H} = \begin{bmatrix} \tilde{\mathbf{G}} \\ \hline \mathbf{I}_m \end{bmatrix}. \qquad (5.39)$$

5. На основании (5.36) и (5.39) сформировать образующую матрицу ПЗК с полной блоковой систематикой

$$\mathbf{G} = \left[\mathbf{I}_k \,\vdots\, \tilde{\mathbf{G}}\right]. \qquad \blacksquare(5.40)$$

Проиллюстрируем алгоритм 5.4 примером, при этом за основу возьмем ПЗК (7,4) из примера 5.2 лишив его *хэмминговских* свойств, но наделив матрицы кода и сам ПЗК полной блоковой систематикой.

Пример 5.4. ПЗК (7,4) характеризуется следующими свойствами:

- полное число разрядов $n = 7$;

- число информационных разрядов $k = 4$;

- число проверочных разрядов $m = 3$ так, что синдромы ошибок в коде имеют трехразрядное представление вида $E_l = \lfloor E_{l3} E_{l2} E_{l1} \rfloor$;

- код является оптимальным так, как выполняется равенство $n = 2^m - 1$;

- минимальное кодовое расстояние между кодовыми комбинациями ПЗК $d_{\min} = 3$;

- код способен исправлять ошибки кратности $s = 1$ в режиме *исправления*;

- код способен обнаруживать ошибки кратности $r = 2$ в режиме *обнаружения*;

- синдромы ошибок в коде строятся по правилу «синдромы ошибок в m младших $(m = 3)$ разрядах образуют единичную матрицу», что доставляет ПЗК *полную блоковую систематику*.

Решение

1. Составим таблицу 5.4 синдромов в результате кодировки векторов-строк однократных ошибок ξ_j векторами-строками синдромов $E_j \left(j = \overline{7,1}\right)$, начиная с ошибки в старшем (седьмом) разряде и заканчивая ошибкой в младшем (первом) разряде, так чтобы последние три синдрома образовывали единичную матрицу.

Таблица 5.4

№ искаженного разряда	ξ_l – вектор-строка искажения в КС	$E_l = [E_{l3} E_{l2} E_{l1}]$ вектор-строка синдрома искажения		
		E_{l3}	E_{l2}	E_{l1}
7	$\xi_7 = [1\ 0\ 0\ 0\ 0\ 0\ 0]$	1	1	1
6	$\xi_6 = [0\ 1\ 0\ 0\ 0\ 0\ 0]$	1	1	0
5	$\xi_5 = [0\ 0\ 1\ 0\ 0\ 0\ 0]$	1	0	1

4	$\xi_4=[0\ 0\ 0\ 1\ 0\ 0\ 0]$	0	1	1
3	$\xi_3=[0\ 0\ 0\ 0\ 1\ 0\ 0]$	1	0	0
2	$\xi_2=[0\ 0\ 0\ 0\ 0\ 1\ 0]$	0	1	0
1	$\xi_1=[0\ 0\ 0\ 0\ 0\ 0\ 1]$	0	0	1

2. Составим проверочную матрицу $\boldsymbol{H}$ в виде

$$\mathbf{H}=col\{E_{n+1-j}\ ;\quad j=\overline{1,n}\}=\begin{bmatrix}1&1&1\\1&1&0\\1&0&1\\0&1&1\\1&0&0\\0&1&0\\0&0&1\end{bmatrix}=\begin{bmatrix}\tilde{\mathbf{G}}\\ \hline \mathbf{I}_m\end{bmatrix};\ \text{где}\ \tilde{\mathbf{G}}=\begin{bmatrix}1&1&1\\1&1&0\\1&0&1\\0&1&1\end{bmatrix}.$$

3. Сформируем образующую матрицу $\mathbf{G}$ в виде

$$\mathbf{G}=\left[\mathbf{I}_k\ \vdots\ \tilde{\mathbf{G}}\right]=\begin{bmatrix}1&0&0&0&1&1&1\\0&1&0&0&1&1&0\\0&0&1&0&1&0&1\\0&0&0&1&0&1&1\end{bmatrix}.$$ ■

Следует заметить, что рассмотренные в настоящем параграфе ПЗК относятся к классу *групповых* кодов. *Множество кодовых комбинаций размерности n* образует группу с бинарной операцией сложения по модулю два, множество разрешенных $(n,k)-$кодовых комбинаций образует *подгруппу*, классы смежности, образованные искаженными кодовыми комбинациями, формируются векторами ξ ошибок в канале связи, осуществляя разложение группы по подгруппе.

В этой связи будет полезной информация, сведенная в таблицу 5.5., в виде синдромов однократных ошибок, удовлетворяющих условиям утверждения 5.3, для групповых кодов, способных исправлять ошибки первой и второй кратностей.

Таблица 5.5

Номер искаженного разряда	**Синдром** $E=[E_8\,E_7\,E_6\,E_5\,E_4\,E_3\,E_2\,E_1]$	**Номер искаженного разряда**	**Синдром** $E=[E_8\,E_7\,E_6\,E_5\,E_4\,E_3\,E_2\,E_1]$
15	1 1 0 1 1 0 1 1	7	0 0 1 0 0 0 0 0
14	1 0 1 1 0 1 0 1	6	0 0 0 1 0 0 0 0
13	1 0 0 1 0 1 1 0	5	0 0 0 0 1 1 1 1

12	1 0 0 0 0 0 0 0	4	0 0 0 0 1 0 0 0
11	0 1 1 0 1 0 1 0	3	0 0 0 0 0 1 0 0
10	0 1 0 1 0 1 0 1	2	0 0 0 0 0 0 1 0
9	0 1 0 0 0 0 0 0	1	0 0 0 0 0 0 0 1
8	0 0 1 1 0 0 1 1		

Завершая рассмотрения проблем данного параграфа, следует вернуться к рисунку 5.1. Рисунок содержит *два блока*, которые не были включены в первоначальное описание *функционального состава аппаратных средств* процесса формирования ПЗК средствами помехозащитного кодирования, его искажения в КС, помехозащитного декодирования с целью формирования синдрома ошибки, который в случае использования режима *обнаружения* свидетельствует только о *факте ошибки* в принятой из КС кодовой комбинации и в случае использования режима *исправления искажений* является *адресом* искаженных разрядов.

В режиме исправления в *функциональном составе аппаратных средств* процесса передачи сообщения, оформленного в виде *информационного* ПНЗК, появляется *формирователь сигнала* $\eta = \xi$ *коррекции* (ФСК), который должен быть сформирован на базе синдрома $E = fH = \xi H$, что позволяет представить его функционирование цепочкой математических равенств

$$\eta = \xi\left(E = \xi H\right) = E \cdot H^{+} = \xi, \qquad (5.41)$$

где H^{+} – псевдообратная к H матрица. *Устройство коррекции* кода (УКК) представляет собой *сумматор по модулю два*, средствами которого осуществляется *восстановление* сформированного на передающей стороне ПЗК y, в силу математических соотношений с использованием правил двоичной модальной арифметики

$$f + \eta = \left(y + \xi\right) + \xi = y + \xi + \xi = y. \qquad (5.42)$$

Проблемой в выражениях (5.41),(5.42) является *вычисление псевдообратной матрицы* H^{+} над двоичным простым полем Галуа $GF(2)$, решение которой в настоящее время достигается алгоритмическими и схемотехническими средствами.

5.3. Представление помехозащитного преобразования кодов на основе действий с модулярными многочленами. Выбор образующего модулярного многочлена кода

Начнем параграф с напоминания содержания понятия модулярный многочлен (ММ), вводившегося еще в курсе «математические основы теории систем». Под ММ понимаются многочлены, *коэффициенты* которых принадлежат простому полю

Галуа $GF(p)=\{0,1,2,...,p-1\}$, при этом сами ММ являются элементами *расширенного поля* Галуа $GF(p^n)$, результаты действия с которыми (сложение и умножение) приводятся *по двойному модулю* $\{modp, modM(x)\}$, то есть по *модулю* характеристики p поля $GF(p)$ и модулю ММ $M(x)$ степени $degM(x)=n.$ Таким образом элементами $GF(p^n)$ являются $n-$компонентные ММ $M_l(x)$ степени $degM_l(x)\le n-1.$

В задачах *преобразования двоичных* кодов используются модулярные многочлены (ММ), результаты действия с которыми приводятся по двойному модулю $\{mod2, mod(x^n+1)\}$, где n - полное число разрядов оптимального $(n,k)-$кода.

Таким образом, в настоящем параграфе используется *представление кодов в виде модулярных многочленов*, в связи с чем рисунок 5.1 преобразуется с теми же функциональными компонентами в рисунок 5.2.

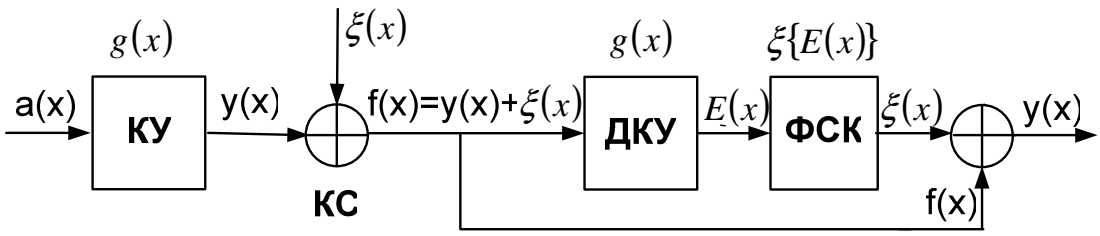

Рисунок 5.2

На рисунке 5.2: КУ – кодирующее устройство; КС – канал связи, искажение в котором моделируется сумматором по модулю два ММ помехозащищенного кода и кода ошибки (помехи); ДКУ – декодирующее устройство, формирующее синдром ошибки; $a(x)$ – модулярный многочлен (ММ) исходного помехонезащищенного кода a с $k-$элементами, степени $dega(x)\le k-1$; $y(x)$ – ММ помехозащищенного (n,k)-кода y, наблюдаемого на выходе КУ, степени $degy(x)\le n-1,\ n>k$, $m=n-k$ – число вводимых избыточных разрядов кода y; $\xi(x)$ –ММ помехи ξ, воздействующей на код y при его передаче по КС, степени $deg\xi(x)\le n-1$; $f(x)=y(x)+\xi(x)$ –ММ искаженного кода f, принимаемого из КС; $E(x)$ – ММ синдрома E ошибки (искажения) в принятой из КС кодовой комбинации, степени $degE(x)\le m-1$.

Введем определения процессов *помехозащитного* кодирования и декодирования для случая представления кодов *модулярными многочленами.*

Определение 5.11. *Помехозащитным кодированием* при использовании представления кодов ММ называется *процесс формирования* ММ $y(x)$ *помехозащищенного* кода y из ММ $a(x)$ *помехонезащищенного* кода a, осуществляемый в КУ, при котором на основе ММ $a(x)$ степени $dega(x) \le k-1$ с помощью ММ многочлена $g(x)$ степени $degg(x) = m$ ММ $y(x)$ приобретает свойство *делимости на* ММ $g(x)$ *без остатка* так, что выполняется условие

$$rest\frac{y(x)}{g(x)} = 0, \qquad (5.43)$$

где $rest(*)/(\bullet)$ – операция вычисления остатка от деления элемента $(*)$ на элемент $(\bullet)$. □

Примечание 5.5. Помехозащищенный код, на множестве кодовых комбинаций которого выполняется *характеристическое свойство* (5.43) принято называть *циклическим* ПЗК так, как характеристическое свойство (5.43) сохраняется на любой кодовой комбинации, получаемой из начальной путем ее *циклического* сдвига влево на любые $l-$разрядов, осуществляемого умножением ММ начальной кодовой комбинации на x^l с последующим приведением по двойному модулю $\{mod2, mod(x^n+1)\}$. □

Примечание 5.6. Модулярный многочлен $g(x)$ степени $degg(x) = m$ именуется *образующим многочленом циклического кода*. □

Примечание 5.7. Кодовые комбинации циклического ПЗК, то есть комбинации, обладающие *характеристическим свойством* (5.43) называются *разрешенными кодовыми* комбинации, в отличие от остальных которые именуются *не разрешенными*. □

Определение 5.12. *Помехозащитным декодированием* при использовании представления кодов ММ называется *процесс формирования ММ* $E(x)$ остатка от деления ММ $f(x)$ принятого из КС кода f на ММ $g(x)$, с целью проверки сохранности при передаче характеристического свойства ПЗК (5.43), в форме

$$E(x) = rest\frac{f(x)}{g(x)}. \qquad \square(5.44)$$

Примечание 5.7. Помехозащитное декодирующее устройство формирует:

- нулевой ММ синдрома $E(x) = 0$

в случае *отсутствия искажений* в принятом коде;

- ненулевой ММ синдрома $E(x) \ne 0$

в случае *наличия искажений* в принятом коде.

Причем в случае использования *режима обнаружения* ненулевой ММ $E(x) \ne 0$ синдрома свидетельствует только о *факте ошибки* в

принятой из КС кодовой комбинации, а в случае использования *режима исправления искажений* код $K\{E(x)\neq 0\}$ является *адресом* искаженных разрядов.

Прямого преобразования на уровне представлений с использований ММ в двоичной модальной математике ММ $E(x)\neq 0$ синдрома в ММ $\eta(x)=\xi(x)=\xi\{E(x)\}$ сигнала коррекции пока не разработано, формирование *сигнала* $\eta=\xi$ *коррекции* осуществляется путем перехода от ММ к кодам с последующим использованием последовательных и параллельных методов их преобразования в алгоритмической и схемотехнической среде. □

Покажем теперь, что ММ синдрома $E(x)$ может быть вычислен на основе использования положений следующего утверждения.

Утверждение 5.6. ММ $E(x)$ синдрома E, *аппаратно* формируемый в технической среде помехозащитного декодирующего устройства циклического кода в силу соотношения (5.44), *аналитически* вычисляем с помощью выражения

$$E(x)=rest\frac{\xi(x)}{g(x)}. \qquad \square(5.45)$$

Доказательство утверждения строится на непосредственном вычислении выражения (5.44) с учетом равенства $f(x)=y(x)+\xi(x)$ и характеристического свойства (5.43) циклического кода с ММ $y(x)$, приводящем к цепочке равенств

$$E(x)=rest\frac{f(x)}{g(x)}=rest\frac{y(x)+\xi(x)}{g(x)}=rest\frac{y(x)}{g(x)}+rest\frac{\xi(x)}{g(x)}=0+rest\frac{\xi(x)}{g(x)}=rest\frac{\xi(x)}{g(x)}.$$

■

Рассмотрим теперь *способы формирования циклических ПЗК* в форме ММ $y(x)$, обладающего характеристическим свойством (5.43). Этих методов три:

1.способ, основанный на *перемножении* ММ;

2.способ, основанный на *делении* ММ с целью вычисления остатка;

3.способ, основанный на формировании *проверочной* и *образующей* матриц циклического кода.

Первый способ формирования циклических ПЗК в форме ММ $y(x)$ опирается на положения следующего утверждения.

Утверждение 5.7. Циклический помехозащищенный (n,k) – код, задаваемый модулярным многочленом $y(x)$, обладающим характеристическим свойством (5.43), может быть сформирован помехозащитным кодирующим устройством, осуществляющим

перемножение ММ $a(x)$ степени $dega(x) \le k-1$ исходного помехонезащищенного кода a с $k-$элементами, и ММ $g(x)$ степени $degg(x)=m$ именуемого *образующим многочленом циклического кода* так, что модулярный многочлен $y(x)$ принимает представление

$$y(x)=a(x)\cdot g(x). \qquad \square(5.46)$$

Доказательство утверждения строится на вычислении остатка по схеме (5.43) с учетом представления (5.46), которое позволяет записать

$$rest\frac{y(x)}{g(x)}=rest\frac{y(x)=a(x)\cdot g(x)}{g(x)}=rest\frac{a(x)\cdot g(x)}{g(x)}=0,$$

характеристическое свойство (5.43) на коде с ММ вида (5.46) сохраняется, следовательно код, задаваемый ММ вида (5.46) является циклическим ПЗК. ■

Примечание 5.8. Формирование циклического ПЗК на основе *перемножения* ММ в форме (5.46) не нашло практического использования по следующим соображения:

1. В ПЗК (5.46) *отсутствует* полностью какая-либо *систематика*, его разряды невозможно разделить на информационные и проверочные за счет перемешивания разрядов при перемножении. Приведем иллюстративный пример.

Пусть: 1.1. $a=[1010]$, с ММ $a(x)=1\cdot x^3+0\cdot x^2+1\cdot x^1+0\cdot x^0=x^3+x$;

1.2. Образующим ММ кода выбран ММ $g(x)=x^3+x^2+1$;

1.3. ММ ПЗК сформируем в соответствии (5.46)

$$y(x)=a(x)\cdot g(x)=\left(x^3+x\right)\left(x^3+x^2+1\right)=$$
$$=\left\{x^6+x^5+x^4+x^3+x^3+x\right\}mod2=\left(x^6+x^5+x^4+x\right);$$
$$y=K\{y(x)\}=[1110010].$$

Исходный информационный ПНЗК $a=[1010]$ *не обнаруживается* в структуре ПЗК $y=[1110010]$.

2. Код приводит к использованию *разнотипной* аппаратуры при кодировании и декодировании, так как кодирование осуществляется с помощью *средств перемножения* ММ, а декодирование – *средств деления* для вычисления ММ синдрома по схеме (5.44).

3. Более того *требуется* после исправления искаженного кода f с ММ $f(x)$ так, что восстанавливается равенство $f(x)=y(x)=a(x)g(x)$ исправленный ММ $f(x)=y(x)=a(x)g(x)$ направить в *дополнительное устройство деления* на ММ $g(x)$ для восстановления переданного информационного кода $a=K\{a(x)\}$. □

Второй способ формирования циклического ПЗК опирается на положения утверждения.

Утверждение 5.8.

Полиномиальная модальная структура

$$z(x)=a(x)x^m+r(x), \tag{5.47}$$

где $r(x)=rest\dfrac{a(x)x^m}{g(x)}$, (5.48)

представляет собой ММ *циклического ПЗК* так, что выполняется равенство $z(x)=y(x)$, где ММ $y(x)$ обладает характеристическим свойством (5.43). ■

Доказательство. Представим (5.48) в мультипликативной форме, тогда получим

$$a(x)x^m=q(x)\cdot g(x)+r(x), \tag{5.49}$$

где $q(x)$ – ММ степени $\deg q(x)\le k-1$ представляет собой «целую часть» результата деления. Подставим (5.49) в выражение (5.47) и приведем подобные по модулю два, тогда получим

$$z(x)=a(x)x^m+r(x)=\{q(x)\cdot g(x)+r(x)+r(x)\}mod2=q(x)\cdot g(x)=y(x).$$ ■

Примечание 5.9. Рассмотрим структуру циклического ПЗК, сконструированную в силу утверждения 5.8

$$y(x)=a(x)x^m+r(x),$$

она обнаруживает следующие внутренние свойства и механизм реализации.

1. Умножение ММ $a(x)$ степени $dega(x)=k-1$ информационного $k-$разрядного кода a на x^m означает формирование ММ $a(x)x^m$ степени $deg\{a(x)x^m\}\le k-1+m=n-1$ $n-$разрядного года, полученного сдвигом кода a на m разрядов влево (вперед) с одновременным освобождением (обнулением) $m-$младших разрядов;

Вычисление остатка $r(x)$ от деления ММ $a(x)x^m$ на образующий ММ $g(x)$ степени $degg(x)=m$ дает ММ степени $degr(x)\le m-1$, которому соответствует $m-$разрядный код r, которому *уготована* $m-$разрядная пустая (нулевая) вакансия в коде $K\{a(x)x^m\}$. Операция суммирования ММ $a(x)x^m$ и $r(x)$, дающая суммарный ММ $a(x)x^m+r(x)$, с согласованными по степеням в форме $mindeg\{a(x)x^m\}=m$ и $max\{degr(x)\}=m-1$ полиномиальными компонентами, сопрягает два кодовых фрагмента в единый ПЗК $(n,k)-$код, старшие $k-$разрядов которого содержат информационный код a, а младшие $m-$разрядов проверочный код r.

2. Схема (5.47) формирования циклического ПЗК в силу сказанного в п.1 примечания доставляет помехозащищенному коду с образующим ММ $g(x)$ *полную блоковую систематику.*

3. *Аппаратно* циклический $(n,k)-$ПЗК в соответствии со схемой (5.47) формируется следующим образом:

– исходный информационный код a в течение $k-$тактов из *устройства формирования кода* сообщения (УФКС) подается через линейное устройство (ЛУ) в двоичный канал связи и на вход последовательного регистра, составленного из $m-D-$триггеров с обратными связями, представляющего собой устройство деления на образующий ММ $g(x)$ ПЗК с целью вычисления остатка (5.48) $r(x)$;

– в течение первых $k-$тактов в регистре деления ММ формируется остаток от деления $r(x)$;

– на $(k+1)-$м такте разрываются обратные связи в устройстве деления ММ (УДММ) с тем, чтобы приостановить процесс деления путем перевода УДММ в последовательный *регистр сдвига*; вход ЛУ КС переключается с выхода УФКС на выход УДММ;

– в течение последних $m-$тактов остаток от деления выводится из УДММ через ЛУ в двоичный КС, чем завершается аппаратное формирование циклического $(n,k)-$ПЗК. □

Третий способ основан на конструировании *проверочной* матрицы H циклического ПЗК на основании (5.45) и *образующей* матрицы G, вычисление которой опирается на факт полной блоковой систематики циклических ПЗК. В отличие от второго способа формирования циклического ПЗК рассматриваемый способ возвращает к *параллельному преобразованию кодов* в решении задач их помехозащиты. Построенные образующая матрица G и проверочная матрица H используются для *аналитического описания* процессов помехозащитного кодирования $y = aG$ и помехозащитного декодирования $E = fH$ циклических кодов.

АЛГОРИТМ 5.5

формирования циклического ПЗК, основанный на формировании *проверочной* и *образующей* матриц кода

1.Сформировать число k информационных разрядов помехозащищенного (n,k) – кода в соответствии с алгоритмом 5.1;

2.По заданным: категории системы, характеризующейся величиной $P_{доп}-$ допустимой вероятности приема ложной команды,

и параметру модели двоичного канала связи в форме p – вероятности искажения разряда (бита) кода, определяемому выражением $p=\max\{p_{01},p_{10}\}$, определить кратность исправляемой ошибки s в силу соотношения

$$s=\min\arg\left\{ N_c=2^m-1\ge N_{ош}=\sum_{i=1}^{s} C_n^i \;\&\; \sum_{i=s+1}^{n} C_n^i p^i(1-p)^{n-i}\le P_{доп} \right\},$$

где N_c – число синдромов, $N_{ош}$ – число исправляемых ошибок, в зависимости от величины s – кратности исправляемой ошибки выбрать (при $s=1$) из таблицы П1.1 неприводимых многочленов или (при $s\ge 2$) из таблицы П1.2 неприводимых многочленов, сформированных с помощью БЧХ-технологии, образующий многочлен $g(x)$ кода степени $degg(x)=m$ и сформировать (n,k)–формат ПЗК, где $n=k+m$;

3. Представить искажение $j-$го разряда кода ММ $\xi_j(x)=x^{j-1}; j=\overline{1,n}$;

4. Вычислить остатки $r_j(x)$ от деления ММ $\xi_j(x)=x^{j-1}; j=\overline{1,n}$, на образующий ММ $g(x)$ в силу соотношения

$$r_j(x)=rest\frac{x^{j-1}}{g(x)}; j=\overline{1,n};$$

5. На основании (5.45) сформировать ММ $E_j(x)$ синдромов однократных ошибок в форме

$$E_j(x)=r_j(x)=rest\frac{x^{j-1}}{g(x)}; j=\overline{1,n}; \qquad (5.50)$$

6. Сформировать кодовые аналоги ММ $E_j(x)$ синдромов в форме m – разрядных вектор-строк $K\{E_j(x)\}$;

7. Сформировать *проверочную* матрицу H циклического (n,k) – ПЗК с учетом его полной блоковой систематики

$$H=col\left\{H^j=K\left\{E_{n+1-j}(x)=rest\frac{x^{n-j}}{g(x)}\right\}; j=\overline{1,n}\right\}=\begin{bmatrix}\tilde{G}=col\{G^j=H^j; j=\overline{1,k}\}\\ I=col\{H^j; j=\overline{k+1,n}\}\end{bmatrix}; \qquad (5.51)$$

8. Сформировать *образующую* матрицу G циклического (n,k) – ПЗК с учетом его полной блоковой систематики

$$G = \left\lfloor I_{k\times k} \quad \tilde{G} = col\left\{\tilde{G}^j = H^j;\ j = \overline{1,k}\right\}\right\rfloor. \tag{5.52}$$

9. Сформировать аналитическое описание процессов помехозащитного кодирования и декодирования на основании полученных матриц в форме $y = aG = a\left[I\ \tilde{G}\right] = \left[a\ a\tilde{G}\right], E = fH.$ ■

Примечание 5.10. Рассмотрим *последнюю* ($k-$ю) строчку $\tilde{G}^k$ матрицы $\tilde{G}$, для которой оказывается справедливой цепочка равенств

$$\tilde{G}^k = H^k = K\left\{E_{n+1-k}(x) = rest\frac{x^{n-k}}{g(x)}\right\} = K\left\{E_{m+1}(x) = rest\frac{x^m}{g(x)}\right\} = K\left\{x^m + g(x)\right\}. \tag{5.53}$$

Соотношение (5.53) обладает хорошими *идентификационными* свойствами, позволяющее по последней строке $\tilde{G}^k$ матрицы $\tilde{G}$ определять:

1. корректность составления образующей матрицы G ПЗК по заданному образующему ММ $g(x)$ кода;

2. определять образующий ММ $g(x)$ ПЗК по заданной образующей матрице G кода. □

Проиллюстрируем алгоритм 5.5 примером.

Пример 5.5. Сформировать проверочную (5.51) и образующую (5.52) матрицы на примере кода (7.4).

Решение

1. Опираясь на алгоритм 5.1 и п.1 алгоритма 5.5 осуществим формирование базовых характеристик ПЗК, приводящих к формату (7,4) кода, характеризующегося следующими свойствами:

- полное число разрядов $n = 7$;

- число информационных разрядов $k = 4$;

- число проверочных разрядов $m = 3$ так, что синдромы ошибок в коде имеют трехразрядное представление вида $E_l = \left\lfloor E_{l3}\, E_{l2} E_{l1}\right\rfloor$;

- код является оптимальным так, как выполняется равенство $n = 2^m - 1$;

- минимальное кодовое расстояние между кодовыми комбинациями ПЗК $d_{\min} = 3$;

- код способен исправлять ошибки кратности $s=1$ в режиме *исправления*;

- код способен обнаруживать ошибки кратности $r=2$ в режиме *обнаружения*;

- синдромы ошибок в коде строятся по правилу «синдромы ошибок в m младших $(m=3)$ разрядах образуют единичную матрицу», что доставляет ПЗК *полную блоковую систематику*.

2. Выберем из таблицы П1.1 неприводимых ММ многочлен степени $(m=3)$ $g(x)=x^3+x^2+1$ в качестве образующего ММ циклического кода.

3. На основании выполнения п.п. 3 – 6 алгоритма 5.5 составим таблицу 5.6 ММ ошибок и синдромов, а также их кодовых аналогов

Таблица 5.6

№ искаженного разряда	ξ_j – вектор-строка искажения в КС	ММ ошибки (искажения) $\xi_j(x)=x^{j-1}$; $j=\overline{1,n=7}$	ММ синдрома $E_j(x)$	Код ММ синдрома $K\{E_j(x)\}$		
				E_{J3}	E_{j2}	E_{j1}
7	$\xi_7=[1\ 0\ 0\ 0\ 0\ 0\ 0]$	x^6	x^2+x	1	1	0
6	$\xi_6=[0\ 1\ 0\ 0\ 0\ 0\ 0]$	x^5	$x+1$	0	1	1
5	$\xi_5=[0\ 0\ 1\ 0\ 0\ 0\ 0]$	x^4	x^2+x+1	1	1	1
4	$\xi_4=[0\ 0\ 0\ 1\ 0\ 0\ 0]$	x^3	x^2+1	1	0	1
3	$\xi_3=[0\ 0\ 0\ 0\ 1\ 0\ 0]$	x^2	x^2	1	0	0
2	$\xi_2=[0\ 0\ 0\ 0\ 0\ 1\ 0]$	$x^1=x$	x	0	1	0
1	$\xi_1=[0\ 0\ 0\ 0\ 0\ 0\ 1]$	$x^0=1$	1	0	0	1

4. На основании выполнения п.7 алгоритма формируем *проверочную* матрицу H циклического (n,k) – ПЗК с учетом его полной блоковой систематики

$$H = col\left\{H^j = K\left\{E_{n+1-j}(x)\right\}; j = \overline{1,n}\right\} = \begin{bmatrix} \tilde{G} \\ I_{m\times m} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix};$$

5. На основании выполнения п.8 алгоритма сформируем *образующую* матрицу G циклического (n,k) – ПЗК с учетом его полной блоковой систематики

$$G = \left[I_{k\times k} \quad \tilde{G} = col\left\{\tilde{G}^j = H^j; j = \overline{1,k}\right\}\right] = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

6. На основании выполнения п.9 алгоритма $y = aG = a\left[I\ \tilde{G}\right] = \left[a\ a\tilde{G}\right], E = fH$ формируем аналитическое описание процесса *помехозащитного кодирования*:

$$y_7 = a_4; y_6 = a_3; y_5 = a_2; y_4 = a_1; y_3 = a_4 + a_2 + a_1; y_2 = a_4 + a_3 + a_2; y_1 = a_3 + a_2 + a_1;$$

а также процесса *помехозащитного декодирования*:
$E_3 = f_7 + f_5 + f_4 + f_3; E_2 = f_7 + f_6 + f_5 + f_2; E_1 = f_6 + f_5 + f_4 + f_1.$ ■

Завершая рассмотрение процессов помехозащитного преобразования кодов с использованием их представлений с помощью модулярных многочленов, обратимся к *проблеме выбора образующего ММ* $g(x)$ степени $degg(x) = m$, которая *до настоящего момента по умолчанию считалась решенной.* Это не так, ситуация может быть исправлена перечислением требований, которым должен удовлетворять образующий ММ $g(x)$.

ТРЕБОВАНИЯ,

предъявляемые к образующему модулярному многочлену (ОММ) $g(x)$ кода

1. ОММ $g(x)$ должен быть *неприводимым*, то есть обладать свойством делимости «нацело» только при делении на единицу и сам на себя;

Примечание 5.11. *Свойство неприводимости* ММ эквивалентно *свойству простоты целых чисел*, в силу наличия которого деление на простое число порождает множество остатков максимальной мощности. Свойство неприводимости также порождает множество остатков максимальной мощности, а это доставляет ПЗК широкие корректирующие возможности, так как остатки от деления есть синдромы, в режиме исправления выполняющие функции адресов искаженных разрядов.

Неприводимый ММ «как правило» не имеет корней в поле $GF(2)$, его корнями являются ММ. Последнее означает, что неприводимый ММ не обнуляется ни значением $x=0,$ ни значением $x = 1$, как следствие неприводимый ММ имеет единичный свободный член и нечетное число членов. □

2. Степень ОММ $g(x)$ $degg(x)=m$, определяющая число проверочных разрядов ПЗК, выбирается из условия обеспечения корректирующей способности кода

$$m=\min_{m} arg\left\{N_c=2^m-1\geq N_\xi=\sum_{i=1}^{s}C^i{}_n=\sum_{i=1}^{s}C^i{}_{k+m}\right\},$$

где N_c- число ненулевых синдромов ПЗК; $N_\xi-$число исправляемых ошибок.

Примечание 5.12. Если требования к корректирующей способности ПЗК формулируется в форме обеспечения необходимого минимального кодового расстояния между его кодовыми комбинациями в форме $d_{\min}\geq d$, то требование к степени $degg(x)=m$ ОММ $g(x)$ формулируется следующим образом:

– в случае *нечетного* d: $m=\{\!\{log_2(n+1)\}\!\}\dfrac{d-1}{2}$;

– в случае *четного* d: $m=\{\!\{log_2(n+1)\}\!\}\dfrac{d-2}{2}$;

где $\}\!\{*\}\!\{$ результат *операции округления до целого* большего числа $\{*\}$. □

3. Образующий ММ $g(x)$ $degg(x)=m$ $(n,k)-$ПЗК должен принадлежать показателю n, то есть он *должен входить в разложение двучлена* x^n+1 и при это не должно существовать такого $\overline{n}<n$, при котором образующий ММ $g(x)$ $degg(x)=m$ входит в разложение двучлена $x^{\overline{n}}+1$.

Примечание 5.13.

Наличие свойства п.3 у образующего ММ $g(x)$ иллюстрируется следующим образом. Очевидно, в силу циклических свойств циклических ПЗК оказывается справедливой запись

$$y(x)=rest\frac{g(x)b(x)}{(x^n+1)}:rest\frac{y(x)}{g(x)}=0,$$

где $y(x)-$циклический ПЗК при $\forall b(x)$.

Запишем выражение для $y(x)$ в мультипликативной форме $y(x)=(x^n+1)Q(x)+g(x)b(x)$. Из полученного представления следует, что условие $rest\{y(x)/g(x)\}=0$ выполняется только при выполнении условия $rest\{(x^n+1)/g(x)\}=0$.При этом, если будет существовать $\bar{n}<n: rest\{(x^{\bar{n}}+1)/g(x)\}=0$, то число синдромов однократных ошибок $N_c=\bar{n}<n$.

Отметим еще одно *полезное* обстоятельство в связи с рассматриваемым свойством п.3 образующего ММ $g(x)$. Оно состоит в том, что если $n=2^m-1$, то в разложение двучлена (x^n+1) входят все без исключения неприводимые ММ, степени которых входят в разложение числа m.

Проиллюстрируем высказанное примером $n=7, m=3:(7=2^3-1)$. В разложение числа $m=3=1\cdot 3$ входят числа *1* и *3*.Это значит, что в разложение двучлена (x^7+1) будет входить ММ $(x+1)$ все неприводимые ММ степени $degg_i(x)=3$. В соответствии с таблицей П1.1 неприводимых ММ таких ММ два: $g_1(x)=x^3+x^2+1; g_2(x)=x^3+x+1$. Тогда должно выполняться равенство $(x^7+1)=(x+1)(x^3+x^2+1)(x^3+x+1)$, справедливость которого проверим простым перемножением с приведением подобных по $mod2$. В результате получим

$$(x+1)(x^3+x^2+1)(x^3+x+1)=(x+1)(x^6+x^5+x^3+x^4+x^3+x+x^3+x^2+1)mod2=$$

$$=(x+1)(x^6+x^5+x^4+x^3+x^2+x+1)=\begin{pmatrix}x^7+x^6+x^5+x^4+x^3+x^2+x+\\ +x^6+x^5+x^4+x^3+x^2+x+1\end{pmatrix}mod2=$$

$$=(x^7+1).$$

□

4. *Минимальное кодовое расстояние* $d_{\min}$ на множестве разрешенных кодовых комбинаций циклического ПЗК с образующим ММ $g(x)$ *не превышает числа ненулевых элементов ММ* $g(x)$.

Примечание 5.14. Наличие свойства п.4 у образующего ММ $g(x)$ иллюстрируется на примере циклического кодирования двух информационных кодов: $a=[0_k]$ и $a=[0_{k-1}\,1]$, которым соответствуют ММ $a(x)=a_0(x)=0$ и $a(x)=a_1(x)=1$. Если осуществить помехозащитное циклическое кодирование с образующим ММ $g(x)$, то

будут сформированы ММ $y(x)$ ПЗК вида $y(x,a_0(x))=0$ и $y(x,a_1(x))=g(x)$.Сформируем на полученных ММ ПЗК $y_0=K\{y(x,a_0(x))=0\}$ и $y_1=K\{y(x,a_1(x))=g(x)\}$, и вычислим кодовое расстояние между ними

$$d\{y_0,y_1\}=d\{K\{y(x,a_0(x))=0\},K\{y(x,a_1(x))=g(x)\}\}=n_{gн},$$

где $n_{gн}$ – число ненулевых членов образующего ММ ПЗК $g(x)$. □■

5.4. Связь корректирующей способности кода с кодовым расстоянием, экспресс – оценки корректирующей способности помехозащищенного кода

Как указывалось выше помехозащищенный (n,k) – код, имеющий $k-$информационных разрядов, $n-k=m-$проверочных разрядов и $n-$полное число разрядов, может быть сформирован на основе:

- *эвристического подхода* к фактору кодовой избыточности, вводимой в структуру кода с целью *повышения минимального кодового расстояния*, контролируемого на множестве используемых (разрешенных) кодовых комбинаций кода;

- *систематического подхода*, опирающегося на аналитические связи значений проверочных разрядов кода со значениями его информационных разрядов.

В параграфе ставится задача: на основе знания *только базовых параметров* k,m *и* n ПЗК *осуществить экспресс – оценку*:

- относительного числа N_{oo} обнаруживаемых ошибок;

- кратности s *исправляемых ошибок*;

- кратности r *обнаруживаемых ошибок*;

-минимального *кодового расстояния* между разрешенными кодовыми комбинациями кода;

- *максимального числа* $N_к=N_к(s)$ передаваемых команд при наперед заданной кратности исправляемых ошибок.

Прежде чем решать перечисленные задачи, докажем два утверждения, устанавливающих связь между минимальным кодовым расстоянием и кратностями исправляемых s и обнаруживаемых r ошибок.

Утверждение 5.9. Для того чтобы $(n,k)-$ПЗК код исправлял ошибки кратности s необходимо и достаточно, чтобы *минимальное кодовое расстояние* между разрешенными кодовыми комбинациями $(y_j$ и $y_l)$ было бы не меньше величины $(2s+1)$, то есть чтобы выполнялось неравенство

$$d(y_j, y_l) \geq 2s+1. \qquad \square(5.54)$$

Доказательство. Пусть разрешенные кодовые комбинации $(y_j$ и $y_l)$ таковы, что кодовое расстояние между ними минимально, то есть выполняется условие $d(y_j, y_l) = \min_{j,l}$. Пусть под действием кодов помех ξ нормы $\|\xi\| = s$ на базе кодовых комбинаций $(y_j$ и $y_l)$ формируются конусы $C\{y_j + \xi : \|\xi\| = s\}, C\{y_1 + \xi : \|\xi\| = s\}$ искаженных кодовых комбинаций. Тогда *условием исправления ошибок* кратности s является отсутствие пересечения приведенных конусов

$$C\{y_j + \xi : \|\xi\| = s\} \cap C\{y_l + \xi : \|\xi\| = s\} = \varnothing,$$

что имеет эквивалентное представление

$$d\{C\{y_j + \xi : \|\xi\| = s\}, C\{y_l + \xi : \|\xi\| = s\}\} \geq 1.$$

Если последнее условие записать в терминах кодовых расстояний между кодовыми комбинациями $(y_j$ и $y_l)$, то получим условие (5.54). ■

Утверждение 5.10. Для того чтобы $(n,k)-$ПЗК код обнаруживал ошибки кратности r необходимо и достаточно, чтобы *минимальное кодовое расстояние* между разрешенными кодовыми комбинациями $(y_j$ и $y_l)$ было бы не меньше величины $(r+1)$, то есть чтобы выполнялось неравенство

$$d(y_j, y_l) \geq r+1. \qquad \square(5.55)$$

Доказательство. Пусть разрешенные кодовые комбинации $(y_j$ и $y_l)$ таковы, что кодовое расстояние между ними минимально, то есть выполняется условие $d(y_j, y_l) = \min_{j,l}$. Пусть под действием кодов помех ξ нормы $\|\xi\| = r$ на базе кодовых комбинаций $(y_j$ и $y_l)$ формируются конусы $C\{y_j + \xi : \|\xi\| = r\}, C\{y_l + \xi : \|\xi\| = r\}$ искаженных кодовых комбинаций. Тогда *условием обнаружения ошибок* кратности r является *отсутствие пересечения приведенных конусов с соседними* разрешенными кодовыми комбинациями

$$C\{y_j + \xi : \|\xi\| = r\} \cap \; y_l = \varnothing; y_j \cap \; C\{y_l + \xi : \|\xi\| = r\} = \varnothing,$$

что имеет эквивалентное представление

$$d\{C\{y_j + \xi : \|\xi\| = r\}, y_l\} \geq 1; d\{y_j, C\{y_l + \xi : \|\xi\| = r\}\} \geq 1.$$

Если последние условия записать в терминах кодовых расстояний между кодовыми комбинациями $(y_j$ и $y_l)$, то получим $d\{y_j, y_l\} \geq r+1$, что совпадает с условием (5.55). ■

Из соотношений (5.54) и (5.55) видно, что, если ПЗК *в состоянии исправлять ошибки кратности* s, *то он способен обнаруживать ошибки кратности* $r = 2s$.

Для оценки относительного числа N_{oo} **обнаруживаемых ошибок** рассмотрим *возможные трансформации* массива мощностью $N_{ркк} = 2^k$ $n-$разрядных разрешенных кодовых комбинаций (РКК) при передаче по каналу связи с помехами (ξ). Граф трансформаций представлен на рисунке 5.3.

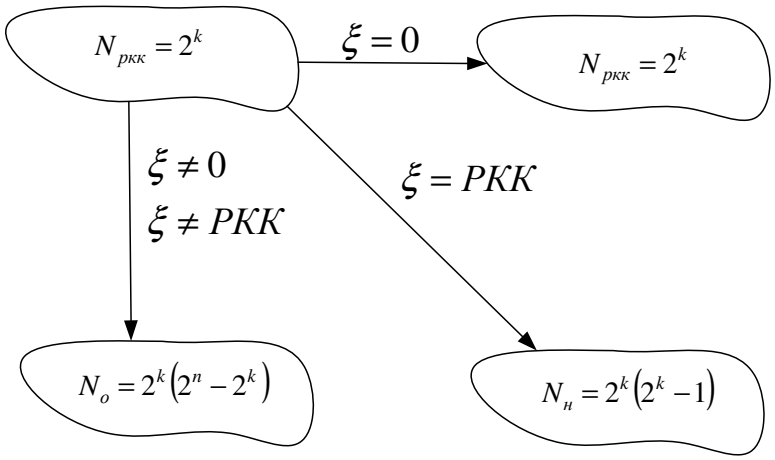

Рисунок 5.3

Нетрудно видеть из приведенного графа, что полное число N_{TP} трансформаций при передаче по КС составляет величину $N_{TP} = 2^k 2^n$, из них число обнаруживаемых составляет $N_o = 2^k\left(2^n - 2^k\right)$. Тогда относительное число обнаруживаемых ошибок составит величину

$$N_{oo} = \frac{2^k\left(2^n - 2^k\right)}{2^k 2^n} = \left(1 - \frac{1}{2^m}\right)100\%. \qquad (5.55)$$

Из формулы (5.55) видно, что относительное число обнаруживаемых ошибок не зависит от числа k информационных разрядов, полного числа n разрядов ПЗК, а зависит лишь от *числа* m *проверочных разрядов*. Для большей наглядности, вычисленные в силу (5.55) значения N_{oo} сведены в таблицу 5.7.

Таблица 5.7

m	1	2	3	4	5	6	7	8	9	10
$N_{oo}(\%)$	50	75	87.5	93.75	96.875	98.42	99.21	99.6	99.8	99.9

Из таблицы видно, что при $m = 1$, то есть *при одном проверочном разряде можно организовать только проверку на четность*

(нечетность) и тем самым обнаруживать 50% всех возможных ошибок. С ростом числа m эта зависимость усложняется и определяется характером заложенной в ПЗК систематики.

Оценка кратности s ***исправляемых ошибок*** $(n,k)-$ПЗК на основании его базовых параметров может быть произведена на основе разрешения условия (5.2) относительно s в форме

$$s = arg\left\{ N_c = 2^m - 1 \geq N_\xi = \sum_{i=1}^{s} C_n^i \right\}.$$

Оценка кратности r ***обнаруживаемых ошибок*** $(n,k)-$ПЗК на основании его базовых параметров может быть произведена на основе соотношения $r = 2s$.

Оценка кратности $d_{\min}$ ***минимального кодового расстояния*** между разрешенными кодовыми комбинациями $(n,k)-$ПЗК на основании его базовых параметров может быть произведена на основе соотношения $d_{\min} \geq 2s+1$.

Оценка ***максимального числа*** $N_к = N_к(s)$ **передаваемых команд при наперед заданной кратности** s **исправляемых ошибок** $(n,k)-$ПЗК на основании его базовых параметров может быть произведена на основе соотношения

$$N_к = N_к(s) = \frac{2^n}{1 + \sum_{i=1}^{s} C_n^i}. \qquad (5.56)$$

Оценка (5.56) именуется границей Р.Хэмминга числа $N_к = N_к(s)$.

Пример 5.6. Сформировать экспресс – оценки корректирующей способности ПЗК $(11,4)$.

Решение задачи сведено в таблицу 5.8.

Таблица 5.8

n	k	m	N_{oo}	s	r	$d_{\min}$	$N_к(s=2)$	$N_к(s=3)$
11	4	7	99.21%	2	4	5	30	8

Примеры и задачи

5.1. Осуществить формирование *базовых параметров* систематического помехозащищенного кода по следующим исходным данным:

- объем информационного массива передаваемых сообщений (команд) составляет величину $V_u = 60$;

- модель искажений в двоичном канале связи в виде информации искажения бита передаваемого кода $p = \max\{p_{01} = 5 \cdot 10^{-5}, p_{10} = 10^{-4}\} = 10^{-4}$, где p_{01}, p_{10} – соответственно вероятность трансформации нулевого элементарного сигнала кода в единичный и наоборот;

- характер помехозащиты: исправление;

- категория проектируемой системы передачи III – я с $P_{доп} = 10^{-7}$.

5.2. Осуществить формирование матриц $\{G, H\}$ на примере помехозащищенного кода Р.Хэмминга (7,4), характеризующегося следующими свойствами:

- полное число разрядов $n = 7$;

- число информационных разрядов $k = 4$;

- число проверочных разрядов $m = 3$ так, что синдромы ошибок в коде имеют трехразрядное представление вида $E_l = \lfloor E_{l3} E_{l2} E_{l1} \rfloor$;

- синдромы ошибок в коде строятся по правилу «синдром ошибки является *двоичным кодом номера искаженного разряда*».

5.3. С помощью алгоритма 5.3 осуществить формирование матриц $\{G, H\}$ на примере помехозащищенного кода Р.Хэмминга (7,4), рассмотренного в примере 5.2, который при кодировании векторов искажений по схеме Р.Хэмминга получает проверочную матрицу, транспонированная версия которой имеет вид

$$H^T = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

5.4. С использованием алгоритма 5.4 на основе ПЗК (7,4) из примера 5.2, лишив его *хэммингoвских* свойств, сконструировать помехозащищенный код с полной блоковой систематикой, характеризующийся следующими свойствами:

- полное число разрядов $n = 7$;

- число информационных разрядов $k = 4$;

- число проверочных разрядов $m = 3$ так, что синдромы ошибок в коде имеют трехразрядное представление вида $E_l = \lfloor E_{l3} E_{l2} E_{l1} \rfloor$;

- синдромы ошибок в коде строятся по правилу «синдромы ошибок в m младших $(m = 3)$ разрядах образуют единичную матрицу.

5.5. Опираясь на алгоритм 5.1 и п.1 алгоритма 5.5 сформировать проверочную (5.51) и образующую (5.52) матрицы кода (7.4), характеризующегося следующими свойствами:

- полное число разрядов $n=7$;

- число информационных разрядов $k=4$;

- число проверочных разрядов $m=3$ так, что синдромы ошибок в коде имеют трехразрядное представление вида $E_l=\lfloor E_{l3}E_{l2}E_{l1}\rfloor$;

- синдромы ошибок в коде строятся по правилу «синдромы ошибок в m младших $(m=3)$ разрядах образуют единичную матрицу», что доставляет ПЗК *полную блоковую систематику*.

5.6. На основании положений параграфа 5.4 сформировать экспресс – оценки корректирующей способности ПЗК $(11,4)$.

5.7. С помощью алгоритма 5.2 с использованием таблицы 5.5 синдромов осуществить формирование матриц $\boldsymbol{G}$ и $\boldsymbol{H}$ ПЗК $(15,7)$, исправляющего ошибки кратности $s=2$.

5.8. На основании положений параграфа 5.4 сформировать экспресс – оценки корректирующей способности ПЗК $(15,7)$.

5.9.На основании образующей матрицы циклического ПЗК $(7,4)$

$$G=\begin{bmatrix}1&0&0&0&1&1&0\\0&1&0&0&0&1&1\\0&0&1&0&1&1&1\\0&0&0&1&1&0&1\end{bmatrix}.$$

определить образующий ММ $g(x)$ кода.

5.10. На основании проверочной матрицы циклического ПЗК $(7,4)$, записанной в транспонированном виде

$$H^T=\begin{bmatrix}1&1&1&0&1&0&0\\0&1&1&1&0&1&0\\1&1&0&1&0&0&1\end{bmatrix},$$

определить образующий ММ $g(x)$ кода.

5.11.Информационный массив сообщений составляет величину $V_u=30$, на основе таблицы П1.1 неприводимых ММ сконструировать ПЗК, гарантирующий исправления ошибок кратности $s=2$. Сформировать образующую и проверочную матрицы кода.

5.12. Информационный массив сообщений составляет величину $V_u = 50$, на основе таблицы П1.1 неприводимых ММ сконструировать ПЗК, гарантирующий его кодовым комбинациям минимальное кодовое расстояние, удовлетворяющее условию $d_{\min} \geq 4$. Сформировать образующую и проверочную матрицы кода.

5.13. Осуществить выбор образующего ММ из таблицы П1.1, сконструировать образующую и проверочную матрицы ПЗК по следующим исходным данным:

- объем информационного массива передаваемых сообщений (команд) составляет величину $V_u = 40$;

- модель искажений в двоичном канале связи в виде информации искажения бита передаваемого кода $p = \max\{p_{01} = 8 \cdot 10^{-5}, p_{10} = 10^{-4}\}$, где p_{01}, p_{10} – соответственно вероятность трансформации нулевого элементарного сигнала кода в единичный и наоборот;

- характер помехозащиты: исправление;

- категория проектируемой системы передачи III – я с $P_{доп} = 10^{-7}$.

Решение вариантов задач

Задача 5.1. Осуществить формирование *базовых параметров* систематического помехозащищенного кода по следующим исходным данным:

- объем информационного массива передаваемых сообщений (команд) составляет величину $V_u = 60$;

- модель искажений в двоичном канале связи в виде информации искажения бита передаваемого кода $p = \max\{p_{01} = 5 \cdot 10^{-5}, p_{10} = 10^{-4}\} = 10^{-4}$, где p_{01}, p_{10} – соответственно вероятность трансформации нулевого элементарного сигнала кода в единичный и наоборот;

- характер помехозащиты: исправление;

- категория проектируемой системы передачи III – я с $P_{доп} = 10^{-7}$.

Решение (см. в тексте параграфа 5.1.).

Задача 5.2. Осуществить формирование матриц $\{G, H\}$ на примере помехозащищенного кода Р.Хэмминга (7,4), характеризующегося следующими свойствами:

- полное число разрядов $n = 7$;

- число информационных разрядов $k = 4$;

- число проверочных разрядов $m=3$ так, что синдромы ошибок в коде имеют трехразрядное представление вида $E_l=\lfloor E_{l3}E_{l2}E_{l1}\rfloor$;

- синдромы ошибок в коде строятся по правилу «синдром ошибки является *двоичным кодом номера искаженного разряда*».

Решение (см. в тексте параграфа 5.2.).

Задача 5.3. С помощью алгоритма 5.3 осуществить формирование матриц $\{G,H\}$ на примере помехозащищенного кода Р.Хэмминга (7,4) , рассмотренного в примере 5.2, который при кодировании векторов искажений по схеме Р.Хэмминга получает проверочную матрицу, транспонированная версия которой имеет вид

$$H^T=\begin{bmatrix}1&1&1&1&0&0&0\\1&1&0&0&1&1&0\\1&0&1&0&1&0&1\end{bmatrix}.$$

Решение (см. в тексте параграфа 5.2.).

Задача 5.4. С использованием алгоритма 5.4 на основе ПЗК (7,4) из примера 5.2, лишив его *хэммингoвских* свойств, сконструировать помехозащищенный код с полной блоковой систематикой, характеризующийся следующими свойствами:

- полное число разрядов $n=7$;

- число информационных разрядов $k=4$;

- число проверочных разрядов $m=3$ так, что синдромы ошибок в коде имеют трехразрядное представление вида $E_l=\lfloor E_{l3}E_{l2}E_{l1}\rfloor$;

- синдромы ошибок в коде строятся по правилу «синдромы ошибок в m младших $(m=3)$ разрядах образуют единичную матрицу.

Решение (см. в тексте параграфа 5.2.).

Задача 5.5. Опираясь на алгоритм 5.1 и п.1 алгоритма 5.5 сформировать проверочную (5.51) и образующую (5.52) матрицы кода (7.4), характеризующегося следующими свойствами:

- полное число разрядов $n=7$;

- число информационных разрядов $k=4$;

- число проверочных разрядов $m=3$ так, что синдромы ошибок в коде имеют трехразрядное представление вида $E_l=\lfloor E_{l3}E_{l2}E_{l1}\rfloor$;

- синдромы ошибок в коде строятся по правилу «синдромы ошибок в m младших $(m=3)$ разрядах образуют единичную матрицу», что доставляет ПЗК *полную блоковую систематику*.

Решение (см. в тексте параграфа 5.3.).

5.6. На основании положений параграфа 5.4 сформировать экспресс – оценки корректирующей способности ПЗК $(11,4)$.

Решение (см. в тексте параграфа 5.4.). ■