2.6. Может ли порождающая матрица группового (n, k)-кода иметь:

a) нулевую вектор-строку,

b) нулевой вектор-столбец?

2.6. a) По определению порождающей матрицы её строки являются базисными кодовыми комбинациями k-мерного подпространства (n-мерного пространства) – линейного (n, k)-кода и, следовательно, являются ненулевыми комбинациями.

b) Если бы некоторый i-й столбец порождающей матрицы линейного (n, k)-кода был нулевым, то тот же самый i-й столбец кодовой матрицы C также был бы нулевым. Но в этом случае, вычеркнув нулевой столбец матрицы C, мы получили бы код с тем же кодовым расстоянием, но меньшей длины.

2.7. Может ли проверочная матрица группового (n, k)-кода иметь:

a) нулевую вектор-строку,

b) нулевой вектор-столбец?

2.7. См. решение задачи 2.6.

2.8. Определить $N^{cuc}_{(n,k)}$ – число всех различных систематических (n, k)-кодов.

2.8. Число всех различных систематических (n, k)-кодов

$$N^{cuc}_{(n,k)} = 2^{k\cdot(n-k)}.$$

2.9. Определить $N^{acuc}_{(n,k)}$ – число всех различных групповых асистематических (n, k)-кодов.

2.9. Число всех различных групповых асистематических (n, k)-кодов

$$N^{acuc}_{(n,k)} = N_{(n,k)} - 2^{k\cdot(n-k)} = \frac{(2^n - 1)(2^n - 2)(2^n - 2^2) \ldots (2^n - 2^{k-1})}{(2^k - 1)(2^k - 2)(2^k - 2^2) \ldots (2^k - 2^{k-1})} - 2^{k\cdot(n-k)}.$$

2.10. Доказать, что двоичный линейный код исправляет любые однократные ошибки тогда и только тогда, когда все столбцы его проверочной матрицы H – ненулевые и различные. Привести для рассматриваемого случая оценку $d_{\text{мин}}$ сверху и снизу.

2.10. Так как все столбцы H различны (т.е. нет ни одной пары одинаковых столбцов), то ни одна пара столбцов не образует пару линейно зависимых столбцов и, следовательно, число линейно зависимых столбцов $\theta > 2$; а так как θ – целое число, то $\theta \geq 3$. С учётом теоремы 2.8 имеем:

$$3 \leq \theta = d_{\text{мин}} \quad \text{и} \quad d_{\text{мин}} \leq n - k + 1.$$

Отсюда имеем:

$$3 \leq d_{\text{мин}} \leq n - k + 1; \quad t \geq](d_{\text{мин}} - 1)/2[\quad \text{и} \quad t \geq 1.$$

Вот ещё несколько примеров на эту тему (теорема 2.8). Ниже приведены примеры порождающих и соответствующих им проверочных матриц некоторых групповых (n, k)-кодов с указанием $d_{\text{мин}}$.

В $H_{(5,\ 3)}$ имеются одинаковые столбцы: первый и четвёртый, третий и пятый, и поэтому полученная выше оценка к этому случаю неприменима. В $H_{(3,\ 1)}$ все три столбца различны и линейно зависимы. В $H_{(5,\ 1)}$ все пять столбцов различны и линейно зависимы.

$$G_{(5,3)} := \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \qquad G_{(3,1)} := (1 \quad 1 \quad 1)$$

$$H_{(5,3)} := \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix} \qquad H_{(3,1)} := \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

$d_{мин} := 2$ $\qquad$ $d_{мин} := 3$

$$G_{(5,1)} := (1 \quad 1 \quad 1 \quad 1 \quad 1)$$

$$H_{(5,1)} := \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$d_{мин} := 5$

2.11. Показать, что если систематический (n, k)-код с проверкой на чётность имеет нечётный минимальный кодовый вес $d_{мин}$, то добавление ко всем его словам одного проверочного символа и модификация порождающей G и проверочной H матриц с сохранением их канонических форм создаёт новый систематический (n + 1, k)-код с проверкой на чётность с кодовым весом $d^*_{мин} = d_{мин} + 1$.

2.11. Структура нового кода вытекает из описания его порождающей матрицы.

Порождающая матрица нового кода G^* размерности $k\times(n+1)$ отличается от старой матрицы G размерности $k\times n$ од-

ним (например) последним *дополнительным столбцом*, содержащим дополнительные проверочные элементы векторов-строк новой порождающей матрицы.

Если проверочная матрица исходного кода H имеет размерность $(n\text{-}k)\times n$, то проверочная матрица нового кода H^* размерности $(n\text{-}k+1)\times(n+1)$ в этом случае имеет структуру, представленную на рис. 4.1.

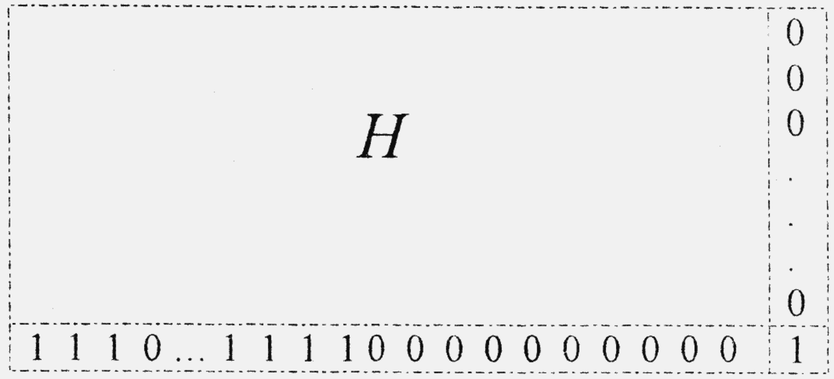

Рис. 4.1. Проверочная матрица нового кода H^*

В *нижней строке* матрицы H^*, считая слева направо, идут сначала k символов, совпадающих с символами, считая сверху вниз, последнего столбца порождающей матрицы G^*, затем идут $n\text{-}k$ нулей и затем (в последнем столбце матрицы) идёт одна единица. Ниже приведен пример для исходного (5, 2)-кода с $d_{мин} = 3$ и для модифицированного (6, 2)-кода с $d_{мин} = 4$. Пример создан в системе MATLAB 6.0 R12.

```
% Преобразование матриц

Gold=[1 0 1 0 1; 0 1 0 1 1];

Hold=[1 0 1 0 0; 0 1 0 1 0; 1 1 0 0 1];

Sold=MOD(Gold*Hold',2);
```

```
Gnew=[1 0 1 0 1 1; 0 1 0 1 1 1];

Hnew=[1 0 1 0 0 0; 0 1 0 1 0 0; 1 1 0 0 1 0; 1 1 0 0 0 1];

Snew= MOD(Gnew*Hnew',2);
```

S_{old} =

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

S_{new} =

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

2.12. Доказать, что код с повторением и код с общей проверкой на чётность – дуальные друг к другу коды.

2.12. Код с повторением – это $(n, 1)$-код, а код с общей (одной) проверкой на чётность – это $(n, n\text{-}1)$-код. Отсюда следует, что между порождающими и проверочными матрицами этих кодов имеют место соотношения:

$$G_{(n,\,1)}=H_{(n,\,n\text{-}1)}, \qquad G_{(n,\,n\text{-}1)}=H_{(n,\,1)},$$

что и доказывает требуемое.

2.13. Найти число векторов из B^n ортогональных к данному вектору v из B_k^n.

2.13. Пусть $\boldsymbol{a}=(a_1, a_2, \ldots, a_j, \ldots, a_n)$ – произвольный вектор из B^n.

Обозначим через X множество $n\text{-}k$ позиций произвольного вектора из B^n, включая вектор $\boldsymbol{v}$, с теми номерами j, которым в $\boldsymbol{v}$ соответствуют позиции, содержащие нули, а множество k остальных позиций обозначим через Y.

Произвольный вектор из B^n будет ортогонален вектору $\boldsymbol{v}$, при условии, что в его множестве позиций Y содержится чётное число единиц, независимо от содержимого в позициях из X. Очевидно, что число таких векторов равно $2^{k-1}\cdot 2^{n-k}=2^{n-1}$.

2.14. Показать, что множество всех векторов из B^n, ортогональных к каждой из строк порождающей матрицы $G_{(n,\,k)}$, образует линейное пространство. Всегда ли это пространство имеет размерность $(n - k)$?

2.14. Ответы на поставленные вопросы в двоичном случае, по сути дела, в несколько упрощенной трактовке даются теоремой 2.7. А именно, в ней доказывается, что порождающей матрице $G_{(n,\,k)}$, имеющей каноническую форму, двоичного группового (или линейного) (n, k)-кода взаимно-однозначным образом соответствует проверочная матрица $H_{(n,\,k)}$, имеющая каноническую форму; $(n\text{-}k)$ линейно независимых строк матрицы $H_{(n,\,k)}$ образуют базис, порождающий линейное пространство размерности $(n\text{-}k)$, все вектора которого принадлежат B^n и ортогональны к каждой из строк матрицы $G_{(n,\,k)}$.

Этот результат может быть обобщён, если отказаться от условия задания порождающей и проверочной матриц в канонической форме.

2.15. Может ли ненулевой вектор принадлежать одновременно групповому (n, k)-коду и дуальному к нему групповому $(n, n - k)$-коду?

2.15. Да, может. См. пример 2.19.

2.16. Пусть C – кодовая матрица двоичного (n, k)-кода, не содержащая нулевых столбцов. Показать, что:

1) каждый столбец матрицы C имеет 2^{k-1} единиц и столько же нулей;

2) сумма весов строк матрицы C равна $n2^{k-1}$.

2.16. Решение аналогично решению задачи 2.3.

2.17. Показать, что кодовое расстояние (n, k)-кода не превосходит $[n2^{k-1}/(2^k - 1)]$.

2.17. Решение основывается на решении задач 2.3 и 2.16.

2.18. Показать, что при $n = 2d_{\min} - 1$ мощность линейного $<n, d_{\min}>$-кода не превосходит $2d_{\min}$.

2.18. Из приведенного условия задачи $n = 2d_{\min} - 1$ следует: $n < 2d_{\min}$.или $2d_{\min} - n > 0$ или $n \geq 1$.

Число единиц в кодовой матрице C равно $n|C|/2$ и это число не меньше $d_{\min}(|C| - 1)$ (см. задачу 2.3). Отсюда, с учётом условия задачи $2d_{\min} - n = 1$, имеем: $|C| \leq 2d_{\min}/(2d_{\min} - n) = 2d_{\min}$.

2.19. Чему равно минимальное число элементов следующих алгебраических структур: 1) группы, 2) кольца, 3) поля, 4) идеала?

2.19. Минимальное число элементов алгебраических структур:

1) группа: 1 элемент,
примеры: $(\{0\}, +)$ или $(\{1\}, \cdot)$;

2) кольцо: 1 элемент,
пример: $(\{0\}, +, \cdot)$;

3) поле: 2 элемента,
пример: $(\{0, 1\}, +, \cdot)$;

4) идеал: 1 элемент,
пример: $(\{0\}, +, \cdot)$.

2.20. Пусть задан систематический (n, k)-код с кодовым расстоянием $d_{\min}$. Верно ли, что в этом случае существует систематический (n, k)-код с кодовым расстоянием $(d_{\min} - 1)$?

2.20. Чтобы *ухудшить* корректирующие свойства систематического (n, k)-кода с кодовым расстоянием $d_{\min}$, попробуйте выделить в кодовой матрице C строки с минимальным весом и в проверочных разрядах этих строк, попытайтесь заменить по одной единице на нуль. Рекомендуется рассмотреть случаи: $d_{\min} = 1$ и $d_{\min} > 1$.

2.21. Показать, что не существует кода длины $n = 20$, содержащего 1000 кодовых слов и исправляющего все трёхкратные и менее кратные ошибки.

2.21. Решение задачи сводится к проверке выполнимости неравенства (2-60).

Действительно, такой код не существует, так как неравенство (2-60) не выполняется. Вот полное решение задачи в системе Mathcad 2000:

$n := 20 \qquad t := 3$

$5 \le 10 = 1$

$5 \ge 10 = 0$

$$V(t) := \sum_{i=0}^{t} \frac{n!}{i! \cdot (n-i)!}$$

$2^n = 1.049 \times 10^6$

$V(t) = 1.351 \times 10^3$

$$\frac{2^n}{V(t)} = 776.148$$

$m := m(20,7) \qquad m := 1000$

$$m \le \frac{2^n}{V(t)} = 0$$

2.22. Двоичный (8, 4)-код задан порождающей матрицей

$$G_{(8,4)} := \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}. \qquad (2\text{-}78)$$

Найти его проверочную матрицу и кодовое расстояние. К какому виду (асистематический или условно систематический первого или второго типа) относится (8, 4)-код, порождаемый приведенной в (2-78) матрицей, и к какому виду (из приведенных в табл. 2.11) относится эта матрица?

2.22. Ниже приведено решение задачи в системе MATLAB 6.0 R12.

```
G=[1 1 1 0 1 0 0 0;0 1 0 1 1 1 0 0;0 0 1 1 0 1 0 1;1 0 0 1 1 0 1 0];

r1=G(1,:); r2=G(2,:); r3=G(3,:); r4=G(4,:);

G=[r1;r2;r3;r4];
```



```
r2=r2+r3; r1=r1+r2; r4=r4+r1;

r2=r2+r3; r3=r3+r4; r2=r2+r4;

G=[r1;r2;r3;r4];  G=MOD(G,2);  R=G(1:4,5:8);

H=zeros(4,8);  H(1:4,1:4)=R';  H(1:4,5:8)=eye(4,4);

S=MOD(G*H',2);
```

$G =$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix},$$

$H =$

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix},$$

$S = GH^{\mathrm{T}} =$

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Так как минимальное число линейно зависимых столбцов проверочной матрицы H равно 2 (первый и шестой

столбцы), то кодовое расстояние $d_{мин} = 2$. Рассматриваемый в задаче (8, 4)-код является условно систематическим кодом второго типа, а форма заданной матрицы имеет тип $[\mathcal{I}_{k\times k}\mathcal{R}_{k\times(n-k)}]$; именно поэтому удалось привести форму заданной матрицы к канонической с помощью элементарных операций, применяемых только к строкам матриц.

2.23. Показать, что существует группа из двух элементов.

2.23. Из решения задачи 2.20 мы уже знаем, что существует группа, состоящая из одного элемента. Предположим, что существует группа, состоящая из двух элементов: единичного элемента e и отличного от него элемента $a \neq e$. Чтобы эта совокупность элементов $\{e, a\}$ являлась бы группой, необходимо, чтобы операция, определённая над этими элементами, удовлетворяла бы всем необходимым групповым законам, и, в частности, для a должен существовать обратный элемент, который мы обозначим как $-a$; очевидно, что групповая операция должна быть сложением (и, следовательно, $e = 0$), а ненулевой элемент a и обратный к нему элемент $-a$ должны удовлетворять условиям: $a + 0 = a \neq 0$, $-a \neq 0$ и, следовательно, $-a = a$, т.е. $a+a=0$. Так как речь идёт о группе, *состоящей из двух элементов*: $(\{0, a\}, +)$, то правила сложения должны быть такими: $0+0=0$, $0+a=a+0=a$, $a+a=0$.

2.24. Как изменится кодовое расстояние двоичного линейного кода при добавлении ко всем его словам одного *проверочного символа*, задающего общую проверку?

2.24. Добавление одного *проверочного символа* ко всем словам двоичного линейного кода при нечётном $d_{мин}$ увеличивает кодовое расстояние на единицу (см. задачу 2.11).

Добавление одного *проверочного символа* ко всем словам двоичного линейного кода при чётном $d_{мин}$ не изменяет кодового расстояния.

2.25. Согласно примеру 2.17 каждому конкретному групповому (n, k)-коду, являющемуся k-мерным подпространством, соответствует $N_{(k)}$ ***различных*** базисов, которые можно выписать с помощью некоторой ***конкретной*** совокупности $N_{(k)}$ порождающих матриц, *множества векторов-строк которых являются попарно* ***различными***, так как только в этом случае они будут представлять $N_{(k)}$ различных базисов.

Доказать, что для *любого конкретного* k-мерного подпространства, определяемого некоторым конкретным *систематическим* групповым (n, k)-кодом, найдётся, по крайней мере, одна совокупность из $N_{(k)}$ различных порождающих матриц, среди которых имеется одна матрица типа $[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$, а остальные $N_{(k)}$ - 1 матрицы являются матрицами типа $[\mathcal{I}_{k\times k}\mathcal{R}_{k\times(n-k)}]$.

Доказать также, что с помощью применения элементарной операции транспозиции только к строкам порождающих матриц из некоторой конкретной одной упомянутой выше совокупности (содержащей матрицу $[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$) $N_{(k)}$ порождающих матриц, рассматриваемое конкретное k-мерное подпространство может быть в общем случае представлено:

с помощью $k!$ различных порождающих матриц, среди которых имеется одна матрица типа $[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$ и $(k! - 1)$ различных матриц типа $[\boldsymbol{I}_{[k]}\boldsymbol{R}_{[k\times(n-k)]}]$;
или

с помощью $k!(N_{(k)} - 1)$ различных матриц типа $[\mathcal{I}_{k\times k}\mathcal{R}_{k\times(n-k)}]$.

2.25. По определению $N_{(k)}$ – число всевозможных различных базисов в B^k, соответствующих некоторому одному и тому же конкретному групповому (n, k)-коду.

Для упрощения рассуждений допустим, что информационные символы кодовых комбинаций рассматриваемых далее кодов занимают первые k разрядов, считая слева направо.

Рассмотрим кодовую матрицу C некоторого конкретного группового (n, k)-кода. Очевидно, что, согласно определению $N_{(k)}$, из кодовой матрицы C можно извлечь $N_{(k)}$ ***различных*** k-наборов векторов-строк, являющихся ***различными*** базисами k-мерного подпространства, коим является рассматриваемый код C. Очевидно, что все эти $N_{(k)}$ различных базисов можно записать с помощью некоторой ***конкретной*** совокупности $N_{(k)}$ порождающих матриц, *множества векторов-строк которых являются* ***различными***, так как только в этом случае эти матрицы будут представлять ***различные*** базисы.

Если код C является систематическим (n, k)-кодом, то, очевидно, что среди $N_{(k)}$ базисов найдётся *только один* такой, который мы сможем записать с помощью матрицы в канонической форме $[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$, а ***остальные*** ($N_{(k)}$ -1) мы сможем записать только в форме $[\mathfrak{I}_{k\times k}\mathfrak{R}_{k\times(n-k)}]$; при этом среди этих ***остальных*** ($N_{(k)}$ -1) базисов не найдётся ни одного, который можно было бы записать в форме $[\boldsymbol{I}_{[k]}\boldsymbol{R}_{[k\times(n-k)]}]$ или в форме $[\Xi_{k\times k}\boldsymbol{R}_{k\times(n-k)}]$.

Применяя транспозицию строк выписанных $N_{(k)}$ порождающих матриц завершим решение задачи.

2.26. Доказать, что в любом конкретном семействе из $N_{(k)}$ *различных* порождающих матриц любого конкретного асистематического группового (n, k)-кода (см. задачу 25), множества векторов-строк которых *попарно различны*, ***все*** порождающие матрицы являются матрицами типа $[\Xi_{k\times k}\boldsymbol{R}_{k\times(n-k)}]$.

Доказать также, что с помощью применения элементарной операции транспозиции только к строкам порождающих матриц из упомянутого выше семейства, рассматриваемый конкретный асистематический групповой (n, k)-код может быть в общем случае представлен помощью $k!N_{(k)}$ различных порождающих матриц типа $[\Xi_{k\times k}\boldsymbol{R}_{k\times(n-k)}]$.

2.26. См. решение задачи 2.25.

4.3. ОТВЕТЫ И РЕШЕНИЯ ЗАДАЧ К РАЗДЕЛУ III

ЗАДАЧИ

3.1. Чему равно число различных многочленов степени k и меньше над полем порядка p?

3.1. Многочлен $f(X)$ степени k определяется последовательностью своих $k+1$ коэффициентов: $f_k, f_{k-1}, \ldots, f_0$. Следовательно, число различных многочленов степени k и меньше над полем порядка p равно p^{k+1}.

3.2. Пусть $g(X) \in F_0[X]$ – некоторый неприводимый многочлен степени m. Чему равно число классов вычетов в $F_0[g]$?

3.2. Так как существует взаимно-однозначное соответствие между классами вычетов из $F_0[g]$ и многочленами из $F_0{}^{m-1}[X]$, то, согласно решению задачи 3.1, число классов вычетов в $F_0[g]$ равно: $|F_0|^m$.

3.3. Пусть I_n – число двоичных неприводимых многочленов степени n. Существует ли такое n, при котором $I_n = 0$? Какими сведениями Вы располагаете по этому вопросу?

3.3. $I_1 = 2, I_2 = 1, I_3 = 2, I_4 = 3, I_5 = 6, I_6 = 9, \ldots,$
$I_{60} = 19\,215\,358\,392\,200\,893.$

Над *каждым конечным полем* существуют неприводимые многочлены произвольной степени: $I_n > 0$ для всех $n > 0$ [3.4].

В [3.2] приведена таблица неприводимых многочленов до 34 степени над полем порядка 2.

3.4. Доказать, что ожидаемое число неприводимых делителей случайно выбранного многочлена достаточно большой степени n над конечным полем порядка q приблизительно равно $\ln n$.

3.4. Смотрите указание к решению этой задачи на с. 95 в [3.4].

3.5. Показать, что элементы поля $F_0[g]$ α^{m-1}, α^{m-2}, …, 1 образуют базис в A_m, где m – степень неприводимого многочлена $g(X)$, с помощью которого создано поле $F_0[g]$.

3.5. Решение этой задачи даёт теорема 3.8. Если учесть вводимые новые обозначения для классов вычетов многочленов – элементов алгебры многочленов A_m, являющейся полем: $\alpha^i = \{X^i\}$, i=0, 1, …, m-1, где классы вычетов многочленов $\{X^i\}$ – *элементы базиса алгебры многочленов* по модулю $g(X)$ A_m, то получим требуемый результат.

3.6. Решить уравнение второго порядка над $GF(2)$: $g(X) = X^2+X+1= 0$. В том случае, если оно не имеет решений в поле $GF(2)$, найти корни этого уравнения, расширив соответствующим образом поле $GF(2)$.

3.6. Так как многочлен X^2+X+1 является неприводимым в поле $GF(2)$, то уравнение $X^2+X+1= 0$ не имеет решений в этом поле.

Рассмотрим расширение $GF(2)$ до поля $GF(2^m)= GF(2^2)$. Зафиксируем примитивный элемент α поля $GF(2^2)$ с помощью многочлена $g(X) = X^2+X+1$ (табл. 4.4).

Таблица 4.4

Степенное представление	Многочленное представление	Векторное представление	$g(\alpha^i)$
$\alpha^0 = 1$	1	(0 0 1)	1
α	α	(0 1 0)	0
α^2	$\alpha + 1$	(0 1 1)	0
α^3	1	(0 0 1)	1

Следовательно, уравнение $X^2+X+1= 0$ имеет в расширении степени два корня: α и α^2 и, следовательно, $g(X)=(X-\alpha)(X-\alpha^2)= X^2 +(\alpha^2 +\alpha)X +\alpha^3 = X^2+X+1$.

3.7. Убедиться, что многочлен $g(X) = X^3+X^2+1$ является неприводимым в поле $GF(2)$. Построить поле $GF(3^2)$, используя для этого неприводимый многочлен $g(X)$.

3.7. См. пример 3.6, табл. 3.14 и пункт *Многочлены* ***третьей степени.***

См. пример 3.10 и табл. 3.18.

3.8. Поле $GF(2^3)$ можно получить как с помощью неприводимого многочлена X^3+X+1, так и с помощью неприводимого многочлена X^3+X^2+1. Получить таблицу соответствия представлений элементов.

3.8. См. пример 3.10 и табл. 3.17 и 3.18.

3.9. Найти примитивные элементы поля Z_p простого порядка в случае, если p = 3, 5, 7 (при p=7 имеются два примитивных элемента 3 и 5).

3.9. См. табл. 4.5.

Таблица 4.5

p	Ненулевые элементы поля Z_p	Примитивные элементы поля Z_p	Проверка
3	1, 2	2	2: $2^0=1$, $2^1=2$, $2^2=1$
5	1, 2, 3, 4	2, 3	2: $2^0=1$, $2^1=2$, $2^2=4$, $2^3=3$, $2^4=1$
			3: $3^0=1$, $3^1=3$, $3^2=4$, $3^3=2$, $3^4=1$
7	1, 2, 3, 4, 5, 6	3, 5	3: $3^0=1$, $3^1=3$, $3^2=2$, $3^3=6$, $3^4=4$, $3^5=5$, $3^6=1$
			5: $5^0=1$, $5^1=5$, $5^2=4$, $5^3=6$, $5^4=2$, $5^5=3$, $5^6=1$

3.10. Построить таблицу сложения и умножения элементов поля $GF(7)$. Найти порядок каждого элемента. Какие элементы являются примитивными?

3.10. См. табл. 4.6 и 4.7. Примитивными элементами поля $GF(7)$ являются 3 и 5.

Таблица 4.6

+, ·	0	1	2	3	4	5	6
0	0, 0	1, 0	2, 0	3, 0	4,0	5,0	6, 0
1	1, 0	2, 1	3, 2	4, 3	5, 4	6, 5	0, 6
2	2, 0	3, 2	4, 4	5, 6	6, 1	0, 3	1, 5
3	3,0	4, 3	5, 6	6, 2	0, 5	1, 1	2, 4
4	4, 0	5, 4	6, 1	0, 5	1, 2	2, 6	3, 3
5	5, 0	6, 5	0, 3	1, 1	2, 6	3, 4	4, 2
6	6, 0	0, 6	1, 5	2, 4	3, 3	4, 2	5, 1

Таблица 4.7

Элемент	0	1	2	3	4	5	6
Порядок	—	1	3	6	3	6	2

3.11. Найти все неприводимые двоичные многочлены степени 5 или меньше над полем $GF(2)$. Заметим, что если многочлен степени m не является неприводимым, то он обладает делителем, степень которого не превосходит $m/2$.

3.11. Из рассмотрения задачи 3.3 следует, что число всех неприводимых двоичных многочленов пятой степени $I_5 = 6$.

Определим n как максимальное целое положительное число, удовлетворяющее условию: $n \mid (2^m - 1)$ при m=5; таким числом является n=31. Поэтому воспользуемся разложением бинома $X^{31}+1$.

В табл. 4.8, являющейся фрагментом таблицы из приложения 5.2, приведены все шесть различные неприводимые многочлены пятой степени.

Таблица 4.8

$X^{31}+1$	$(X^5+X^3+X^2+X+1)(X^5+X^4+X^2+X+1)(X^5+X^2+1)(X^5+X^3+1)(X^5+X^4+X^3+X+1)(X^5+X^4+X^3+X^2+1)(X+1)$

3.12. Сколько существует идеалов в алгебре многочленов по модулю X^6-1 над полем $GF(2)$? Перечислите порождающие их многочлены.

3.12. Ответ: семь нетривиальных идеалов. В табл. 4.9, являющейся фрагментом таблицы из приложения 5.2, приведено разложение бинома X^6-1.

Таблица 4.9

X^6+1	$(X^2+X+1)^2(X+1)^2$

Воспользуемся соотношением (3-47)

$$N_{ид} = (\mu_1+1)(\mu_2+1) - 2 = 7,$$

где $\mu_1 = 2$, $\mu_2 = 2$. Вот порождающие многочлены этих семи идеалов:

$(X^2 + X + 1)$,
$(X^2 + X + 1)^2$,
$(X + 1)$,
$(X + 1)^2$,
$(X^2 + X + 1)(X + 1)$
$(X^2 + X + 1)(X + 1)^2$,
$(X^2 + X + 1)^2(X + 1)$.

3.13. Рассмотрим мультипликативную циклическую группу числового поля Z_7. Очевидно, что её порядок равен 6, а элементами являются положительные целые числа 1, 2, 3, 4, 5, 6 – представители классов вычетов по mod 7. Найдите порядок каждого элемента группы и попытайтесь выписать все подгруппы этой группы.

3.13. В данной задаче речь идёт о поле $F_0 = GF(p)$ простого порядка $p = 7$ (с учётом нулевого элемента) и о его ненулевых элементах, образующих по отношению к операции умножения циклическую группу.

В решении задачи 3.10, в табл. 4.7, приведены порядки элементов рассматриваемой циклической числовой группы.

Подгруппы рассматриваемой мультипликативной группы образованы следующими совокупностями элементов:

1) 1;
2) 1, 2, 4;
3) 1, 6;
4) 1, 2, 3, 4, 5, 6.

Проверьте, все ли подгруппы здесь представлены.

3.14. Показать, что в векторном пространстве наборов длины n с элементами из $GF(2)$ любая подгруппа по сложению является подпространством.

3.14. Справедливость утверждения вытекает из определений векторного пространства, подпространства и аддитивной абелевой группы.

3.15. Пусть $g(X) = g_m X^m + g_{m-1} X^{m-1} + \ldots + g_0$ – порождающий многочлен циклического кода. Показать, что $g_0 \neq 0$.

3.15. Предположим, что $g_0 = 0$. Тогда

$$g(X) = X(g_m X^{m-1} + g_{m-1} X^{m-2} + \ldots + g_1).$$

Так как $g(X)$ – порождающий многочлен циклического (n, k)-кода, то он должен быть делителем бинома X^n+1. Однако бином X^n+1 не делится на X и, следовательно, на $g(X)$ при $g_0 = 0$. Следовательно, $g_0 \neq 0$.

3.16. Пусть $F_0 = GF(2)$, а $F_0[X]$ – множество всех многочленов над полем F_0. В $F_0[X]$ введены операции сложения и умножения многочленов и умножения многочленов на элементы из F_0.

Пусть $f(X)$ – многочлен степени n из $F_0[X]$ и рассматривается алгебра многочленов A_n по модулю $f(X)$.
Требуется:

1) перечислить все названия алгебраических структур, которыми является A_n, если многочлен $f(X)$ не является неприводимым многочленом в $F_0[X]$;

2) перечислить все названия алгебраических структур, которыми является A_n, если многочлен $f(X)$ является неприводимым многочленом в $F_0[X]$.

3.16. 1) A_n; является:

кольцом классов вычетов по модулю $f(X)$;

аддитивной абелевой группой;

линейным векторным пространством;

2) A_n; является:

кольцом классов вычетов по модулю $f(X)$;

полем, элементами которого являются классы вычетов по модулю $f(X)$;

аддитивной абелевой группой;

линейным векторным пространством;

совокупность всех ненулевых элементов A_n образует мультипликативную циклическую группу.

3.17. Показать, что в случае линейного (n, k)-кода кодовое расстояние $d_{\text{мин}} \le n\text{-}k+1=r+1$.

3.17. Кодовое расстояние рассматриваемого кода равно минимальному весу $w_{\min}$ его ненулевых кодовых комбинаций (теорема 2.7).

Вес произвольной ненулевой кодовой комбинации $w=n_k+n_r$, где n_k – число единиц, находящихся в k – информационных разрядах, а n_r – число единиц, находящихся в r – проверочных разрядах. Очевидно, что $n_k \ge 1$, а $n_r \le r$. Следовательно, для всего класса линейных (n, k)-кодов справедлива универсальная оценка сверху:

$$d_{\text{мин}} = w_{\min} \le 1 + r = n\text{-}k+1.$$

3.18. Кодом Рида-Соломона называется БЧХ-код с $m_0=1$. Показать, что для всех кодов Рида-Соломона выполняется соотношение: $d_{\text{мин}} = n\text{-}k+1=r+1$.

3.18. Корни порождающего многочлена степени r в данном случае образуют последовательность корней:

$$\beta, \beta^2, \ldots, \beta^r,$$

имеющих последовательные показатели степеней (так как всего имеется r корней, число циклов равно числу сомножителей порождающего многочлена, а суммарное число чисел во всех циклах равно r). Так как по условию $m_0 = 1$, то, согласно утверждению 3.2, $m_0 + d - 2 = r$, откуда имеем: $d = r+2 - m_0 = r+1$.

3.19. Построить умножитель произвольного входного многочлена на фиксированный многочлен $g(X) = X^3+X^2+1$.

3.19. Схема умножителя на полином $g(X) = X^3+X^2+1$ представлена на рис. 4.2.

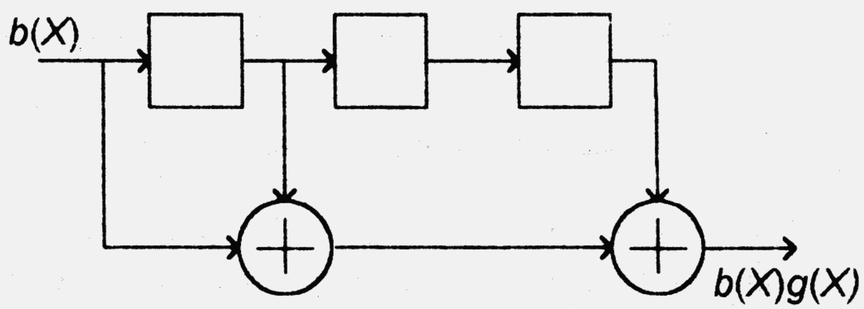

Рис. 4.2. Схема умножителя полиномов

3.20. Построить делители входного многочлена на многочлен:

1) $g_1(X) = X^3+X+1$,

2) $g_2(X) = X^3+X^2+1$.

Проверить работу схем делителей на примере входного полинома $d(X)=X^5+X^4+X^3+X+1$.

3.20. Схемы делителей входного многочлена на многочлен:

1) $g_1(X) = X^3+X+1$ (рис. 4.3);

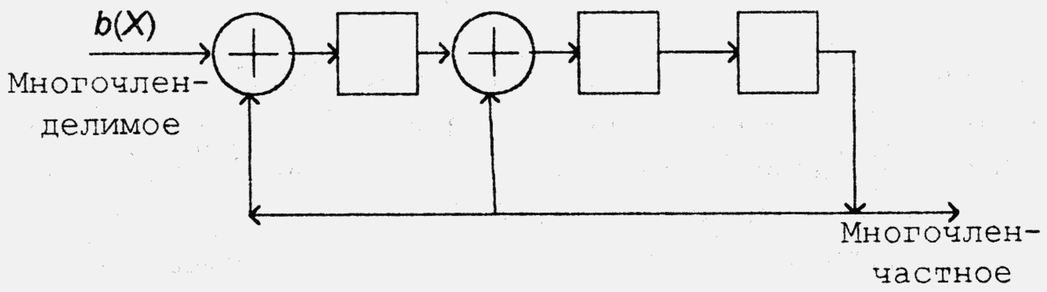

Рис. 4.3 Схема делителя многочленов

2) $g_2(X) = X^3+X^2+1$ (рис. 4.4).

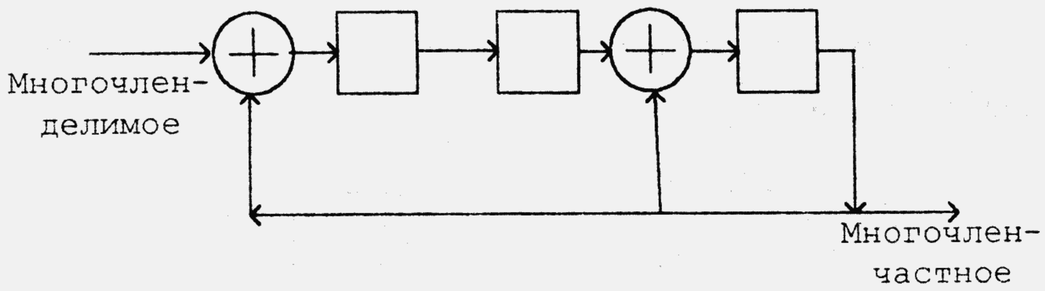

Рис. 4.4 Схема делителя м*ногочленов*

Читателю предоставляется возможность проверить работу схем делителей на примере входного многочлена $d(X)=X^5+X^4+X^3+X+1$ самостоятельно (см. подразделы 3.15 и 3.16).

3.21. Представить ненулевые элементы $GF(2^4)$ как степени примитивного элемента α, зафиксированного с помощью многочлена X^4+X+1; затем степени примитивного элемента α представить как многочлены от α по модулю $\alpha^4+\alpha+1$ и определить минимальные многочлены для ненулевых элементов поля.

3.21. Определим степень бинома X^n-1, порождающего алгебру многочленов A_n, элементы которой – многочлены степени $n-1$ и ниже образуют векторное пространство размерности n, подпространством которого и идеалом является циклический (n, k)-код с порождающим многочленом степени $m=4$ $g(X) = X^4+X+1$:

$$n=2^m-1=2^4-1=15$$

(см. табл. 4.10).

Таблица 4.10

Степенное представление	Многочленное представление	Векторное представление	Минимальные многочлены
α^0	1	(0001)	$X+1$
α	α	(0010)	X^4+X+1
α^2	α^2	(0100)	X^4+X+1
α^3	α^3	(1000)	$X^4+X^3+X^2+X+1$
α^4	$\alpha+1$	(0010)	X^4+X+1
α^5	$\alpha^2+\alpha$	(0110)	X^2+X+1
α^6	$\alpha^3+\alpha^2$	(1100)	$X^4+X^3+X^2+X+1$
α^7	$\alpha^3+\alpha+1$	(1011)	X^4+X^3+1
α^8	α^2+1	(0101)	X^4+X+1
α^9	$\alpha^3+\alpha$	(1010)	$X^4+X^3+X^2+X+1$
α^{10}	$\alpha^2+\alpha+1$	(0111)	X^2+X+1
α^{11}	$\alpha^3+\alpha^2+\alpha$	(1110)	X^4+X^3+1
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	(1111)	$X^4+X^3+X^2+X+1$
α^{13}	$\alpha^3+\alpha^2+1$	(1101)	X^4+X^3+1
α^{14}	α^3+1	(1001)	X^4+X^3+1
α^{15}	1	(0001)	$X+1$

Таблица 4.11

$X^{15}+1$	$(X^2+X+1)(X+1)(X^4+X^3+X^2+X+1)(X^4+X^3+1)(X^4+X+1)$

Заметим, что табл 4.11, являющаяся фрагментом таблицы из приложения 5.2, содержит разложение бинома $X^{15}+1$, а каждый сомножитель бинома являются минимальным многочленом некоторого элемента поля $GF(2^4)$, с другой стороны, каждый минимальный элемент любого элемента $GF(2^4)$ является сомножителем бинома $X^{15}+1$.

3.22. Продолжение задачи 3.21.

Существует ли связь между минимальными многочленами элементов поля $GF(2^4)$, созданного с помощью многочлена X^4+X+1, и числовыми циклами, представляющими последовательности степеней примитивного элемента α и описывающим некоторые подмножества элементов $GF(2^4)$?

3.22. Да, существует непосредственная связь. Цикл указывает, по сути дела, последовательность степеней зафиксированного с помощью неприводимого многочлена X^4+X+1 примитивного элемента α поля $GF(2^4)$, определяя тем самым совокупность элементов $GF(2^4)$, *являющихся корнями* ***одного и того же минимального многочлена*** (табл. 4.12).

Таблица 4.12

Цикл	Корни бинома $X^{15}+1$	Минимальный многочлен
0	1	$X+1$
1, 2, 4, 8	$\alpha, \alpha^2, \alpha^4, \alpha^8$	X^4+X+1
3, 6, 9, 12	$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$X^4+X^3+X^2+X+1$
5, 10	α^5, α^{10}	X^2+X+1
7, 14	α^7, α^{14}	X^4+X^3+1

3.23. Рассмотреть поле $GF(2^4)$ многочленов по модулю X^4+X+1. Найти многочлены этого поля, принадлежащие подполю $GF(2^2)$.

3.23. Обозначим элементы подполя $GF(2^2)$ как 0, ν^0, ν, ν^2. Из рассмотрения табл. 4.10 следует, что $\nu = \alpha^5$, а $\nu^2 = \alpha^{10}$. Очевидно, что порядок элементов ν и ν^2 равен 3.

Таким образом, искомыми элементами являются: 0, 1, α^5 и α^{10}; или, что, то же самое (см. табл. 4.10), 0, 1, $\alpha^2+\alpha$, $\alpha^2+\alpha+1$; именно эта совокупность элементов поля $GF(2^4)$ образует искомое подполе $GF(2^2)$.

3.24. Найти порождающий многочлен для двоичного БЧХ-кода длины 15, исправляющего двукратные ошибки.

3.24. Допустим, что α – примитивный элемент, приведенный в табл. 4.10.

Выберем в качестве порождающего многочлена БЧХ-кода, исправляющего двукратные ошибки

$$g(X) = (X^4+X+1)(X^4+X^3+X^2+X+1),$$

при этом распределение корней многочлена $g(X)$ характеризуется числовыми циклами:

1, 2, 4, 8;
3, 6, 9, 12.

Полагая $\beta=\alpha$ и учитывая выписанные числовые циклы, получим последовательность корней полинома $g(X)$:

$$\beta, \beta^2, \beta^3, \beta^4, \beta^6, \beta^8, \beta^9, \beta^{12}.$$

Подпоследовательность корней максимальной длины этой последовательности, имеющих последовательные показатели степеней: $\beta, \beta^2, \beta^3, \beta^4$. Отсюда, согласно утверждению 3.2, имеем: $m_0=1$ и $m_0+ d_0 -2=4$, а $d_{мин} \geq d_0=5$ и, следовательно, все однократные и двукратные ошибки гарантированно исправляются: $t=](d_0 -1)/2[=2$.

3.25. Найти порождающий многочлен для двоичного БЧХ-кода длины 15, исправляющего трёхкратные ошибки.

3.25. Допустим, что α – примитивный элемент, приведенный в табл. 4.10.

Выберем в качестве порождающего многочлена БЧХ-кода, исправляющего двукратные ошибки

$$g(X) = (X^4+X+1)(X^4+X^3+X^2+X+1)(X^2+X+1),$$

при этом распределение корней многочлена $g(X)$ характеризуется числовыми циклами:

1, 2, 4, 8;
3, 6, 9, 12;
5, 10.

Полагая $\beta=\alpha$ и учитывая выписанные числовые циклы, получим последовательность корней полинома $g(X)$:

$$\beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6, \beta^8, \beta^9, \beta^{10} \beta^{12}.$$

Подпоследовательность корней максимальной длины, этой последовательности, имеющих последовательные показатели степеней: $\beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6$. Отсюда, согласно утверждению 3.2, имеем: $m_0=1$ и $m_0+ d_0 -2=6$, а $d_{мин} \geq d_0=7$ и, следовательно, все одно-, дву- и трёхкратные ошибки гарантированно исправляются: $t=](d_0 -1)/2[=3$.

4.4. ЛИТЕРАТУРА

4.1. Галлагер Р. Теория информации и надёжная связь. М.: Советское радио, 1974.
4.2. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М.: Мир, 1976.
4.3. Касами Т., Токура Н., Ивадари Ё и др. Теория кодирования. М.: Мир, 1978.
4.4. Берлекэмп Э. Алгебраическая теория кодирования. М.: Мир, 1971.
4.5. Говорухин В.Н., Цибулин В.Г. Введение в Maple. Математический пакет для всех. М.: Мир, 1997.
4.6. Дьяконов В.П. Математическая система MAPLE V R3/R4/R5. М.: «СОЛОН», 1998.
4.7. Херхагер М., Партолль Х. Mathcad 2000. Полное руководство : Пер. с немец. под ред. К.Ю. Королькова. Киев: «Ирина», BHV, 2000.
4.8. Кондрашов В.Е., Королёв С.Б. MATLAB как система программирования научно-технических расчётов. М.: Мир, 2002.
4.9. Дьяконов В.П., Абраменкова И.В. МАТЛАБ 5.0/5.3. Система символьной математики. М.: «Нолидж», 1999.
4.10. Фихтенгольц Г.М. Курс дифференциального и интегрального исчисления. Т.1. М.: ФИЗМАТЛИТ, 2001.
4.11. Панин В.В. Основы теории информации. Ч.1. М.: МИФИ, 2001.