ЗАДАЧИ К ЭКЗАМЕНАЦИОННЫМ БИЛЕТАМ
по курсу ***Введение в теорию кодирования***
(для группы А9-08)

1. Определить:

1) $|B_k^n|$ – число всех элементов k-го слоя куба B^n;

2) $|B^n|$ – число всех вершин куба B^n.

2. Определить:

1) $|B_k^n(\boldsymbol{b}_i)|$ – число всех элементов сферы радиуса k с центром в $\boldsymbol{b}_i = \mathbf{0}$;

2) $|S_k^n(\boldsymbol{b}_i)|$ – число всех элементов шара радиуса k с центром в $\boldsymbol{b}_i = \mathbf{0}$.

3. Показать, что для произвольных векторов $\boldsymbol{x}$, $\boldsymbol{y}$ и $\boldsymbol{z}$ из B^n справедливо соотношение:

$$d(\boldsymbol{x}, \boldsymbol{z}) = d(\boldsymbol{x} \oplus \boldsymbol{y}, \boldsymbol{y} \oplus \boldsymbol{z}).$$

4. Ниже приведены подклассы кодов из класса блоковых групповых кодов с проверкой на чётность с одинаковыми параметрами:

1) n и k,
2) n и $d_{\min}$,
3) k и $d_{\min}$.

Какой в каждом из перечисленных подклассов 1), 2) и 3) код более предпочтителен?

5. Ниже приведены различные двоичные пятизначные блоковые коды. Требуется:

определить вид кода;

охарактеризовать потенциальные обнаруживающую и исправляющую способности кода;

определить параметры d_{min} и R кода;

произвести сравнение приведенных кодов как корректирующих.

1) (5, 1)-код:

$$\boldsymbol{H}_{(5,\,1)} = \begin{bmatrix} 11000 \\ 10100 \\ 10010 \\ 11001 \end{bmatrix}.$$

2) 00011 00101 00110 01001 01010

01100 10001 10010 10100 11000.

3) (5, 2)-код:

$$\boldsymbol{H}_{(5,\,2)} = \begin{bmatrix} 11100 \\ 10010 \\ 01001 \end{bmatrix}.$$

4) (5, 3)-код:

$$\boldsymbol{H}_{(5,\,3)} = \begin{bmatrix} 11010 \\ \quad\quad\; \\ 01101 \end{bmatrix}.$$

5) 00001 00010 00100 01000 10000.

6) (5,4)-код:

$$\boldsymbol{H}_{(5,\,4)} = [11111].$$

6. Пусть вероятность искажения одиночного символа в ДСК $p = 0.01$. Определить вероятность появления q-кратной ошибки на выходе ДСК $P(q)$, q=0, 1, …, 5 при условии, что используемый с ДСК код является двоичным пятизначным, а передаваемые по каналу сообщения являются равновероятными. Определить математическое ожидание и среднеквадратическое отклонение (с.к.о) кратности ошибки q.

7. Какие предпосылки:

1) о свойствах передаваемых сообщений или о свойствах двоичных кодовых слов, поступающих на вход канала,

2) о свойствах канала,

3) о методе декодирования на приёмном конце канала

необходимы для обоснования оптимальности метода декодирования по максимуму правдоподобия (декодирование принятой комбинации $\boldsymbol{y}$ в ближайшую кодовую комбинацию в смысле расстояния Хэмминга) и почему?

8. Показать, что если на вход ДСК поступают статистически независимые *неравновероятные кодовые слова* $\boldsymbol{x}_i$, i=1, 2, …, N, то вывод (в решении задачи **1.14**), вообще говоря, не является обоснованным.

9. Показать, что если код с минимальным расстоянием Хэмминга e+1 между кодовыми блоками используется для канала со стиранием, то можно декодировать таким образом, что будут исправлены все комбинации из e (или меньше) стираний, но не все комбинации из e+1 стираний.

10. Показать, что для исправления всех комбинаций из t ошибок и e стираний необходимо и достаточно, чтобы минимальное расстояние Хэмминга между двоичными кодовыми блоками равнялось, по крайней мере, $2t$+e+1.

11. Показать, что число двоичных векторов из B^n, представимых линейными комбинациями вида

$$\lambda_1 \boldsymbol{x}_1 + \lambda_2 \boldsymbol{x}_2 + \ldots + \lambda_s \boldsymbol{x}_s, \qquad (2\text{-}77)$$

в которых $\sum_{i=1}^{s} \lambda_i \le t$, а $\{\boldsymbol{x}_i\}$ – совокупность линейно независимых комбинаций, не превосходит $\sum_{i=0}^{t} C_s^i$.

Рекомендуется решить эту же задачу, отказавшись от условия линейной независимости комбинаций $\{\boldsymbol{x}_i\}$, i = 1, 2, …, s.

12. Показать, что кодовые слова чётного веса двоичного группового (n, k)-кода C образуют подгруппу.

13. Показать, что в каждом двоичном линейном коде либо каждый кодовый вектор имеет чётный вес, либо половина кодовых векторов имеет чётные веса и половина – нечётные.

14. Убедиться, что множество всех кодовых слов чётного веса $C_ч$ группового (n, k)-кода C есть подпространство и найти смежные классы кода C по этому подпространству.

15. Проверить утверждение: множество всех кодовых слов группового (n, k)-кода, содержащих 0 в некоторой фиксированной позиции, есть подпространство. Найти разложение (n, k)-кода на смежные классы по этому подпространству. Проверку провести на примере (5, 3)-кода.

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

a) нулевую вектор-строку,

b) нулевой вектор-столбец?

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

a) нулевую вектор-строку,

b) нулевой вектор-столбец?

18. 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 $d^*_{мин} = d_{мин} + 1$.

19. Доказать, что число всевозможных различных базисов в B^n

$$N_{(n)} = \frac{(2^n - 1)(2^n - 2)(2^n - 2^2)\cdot\ldots\cdot(2^n - 2^{n-1})}{n!}.$$

20. Доказать методом математической индукции, что число всевозможных различных групповых (n, k)-кодов (систематических и асистематических) в B^n

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

21. Определить число различных (3, 2)-кодов в B^3 и привести их.

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

23. Найти число векторов из B^n ортогональных к данному вектору $\boldsymbol{v}$ из B^n_k.

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

25. 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 $n2^{k-1}$.

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

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

28. Пусть порождающая и проверочная матрицы некоторого группового (n, k)-кода заданы в канонической форме

$$\boldsymbol{G}_{(n,k)} = [\boldsymbol{I}_k\ \boldsymbol{R}_{k\times(n-k)}], \qquad (2\text{-}35)$$

$$\boldsymbol{H}_{(n,k)} = [\boldsymbol{R}^{\mathrm{T}}{}_{k\times(n-k)}\ \boldsymbol{I}_{(n-k)}]. \qquad (2\text{-}36)$$

Доказать, что в этом случае выполняется соотношение:

$$\boldsymbol{G}_{(n,k)}\boldsymbol{H}^{\mathrm{T}}{}_{(n,k)} = \boldsymbol{S}, \qquad (2\text{-}37)$$

где $\boldsymbol{S}$ – нулевая матрица размерности $k\times(n-k)$.

29. Рассмотреть синдромное декодирования на примере (5, 2)-кода, имеющего порождающую матрицу

30. Согласно примеру 2.17 [1] 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***, т.к. 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 $[\mathfrak{I}_{k\times k}\mathfrak{R}_{k\times(n-k)}]$.

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 $[\mathfrak{I}_{k\times k}\mathfrak{R}_{k\times(n-k)}]$.

31. 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 $[\Xi_{k\times k}\boldsymbol{R}_{k\times(n-k)}]$.

Дополнительные задачи

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

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

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?

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

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

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 $GF(2)$.

3.7. 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 $g(X)$.

3.8. 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.

3.9. 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).

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

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 $m/2$.

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

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.

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

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

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 $F_0[X]$.

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

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

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

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 $d(X)=X^5+X^4+X^3+X+1$.

3.21. 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.

3.22. 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 $GF(2^4)$?

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

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

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

ВОПРОСЫ К ЭКЗАМЕНАЦИОННЫМ БИЛЕТАМ
по курсу «***Введение в теорию кодирования***»
(группа А9-08)

1. Введение. Основные понятия и термины теории кодирования.

2. Начальные сведения о блоковых корректирующих кодах.

3. Корректирующие коды и их основные виды.

4. Блоковые корректирующие коды с многократной передачей символов.

5. Блоковые корректирующие коды с одной проверкой на чётность.

6. Блоковые корректирующие коды с разбиением множества запрещённых комбинаций на попарно не пересекающиеся подмножества.

7. Таблица декодирования.

8. Сложность кодера при использовании корректирующего кода; сложность кодера в случае группового (n, k)-кода.

9. Сложность декодера, реализующего универсальный алгоритм декодирования.

10. Корректирующая способность кода и кодовое расстояние.

11. Декодирование по методу максимального правдоподобия.

12. Блоковые корректирующие коды со стиранием символов.

13. Блоковые корректирующие коды с проверкой на чётность. Систематический код с проверкой на чётность. Общий код с проверкой на чётность.

14. Порождающая и проверочная матрицы (n, k)-кодов с проверкой на чётность. Кодирование с помощью порождающей матрицы в случае систематического и в случае общего кодов с проверкой на чётность.

15. Декодирование с помощью проверочной матрицы. Синдром.

16. Группа, поле, кольцо.

17. Группа и её подгруппа. Разложение группы по подгруппе и его применение.

18. Описание групповых (n, k)-кодов с помощью порождающих матриц.

19. Описание групповых (n, k)-кодов с помощью проверочных матриц.

20. Стандартное расположение и его применение.

21. Синдромное декодирование.

08.01.2005