рование в данном случае состоит в том, чтобы определить, является ли $z_1^{(1)}$ единицей или нулём. Отметим, что величины S_1, S_3 и S_5 непосредственно содержат $z_1^{(1)}$. Например, если $z_1^{(1)} = 1$, и больше никаких ошибок не произошло, то все величины S_1, S_3 и S_5 равны 1, в то время как, если ни одной ошибки не произошло, то все они равны 0.

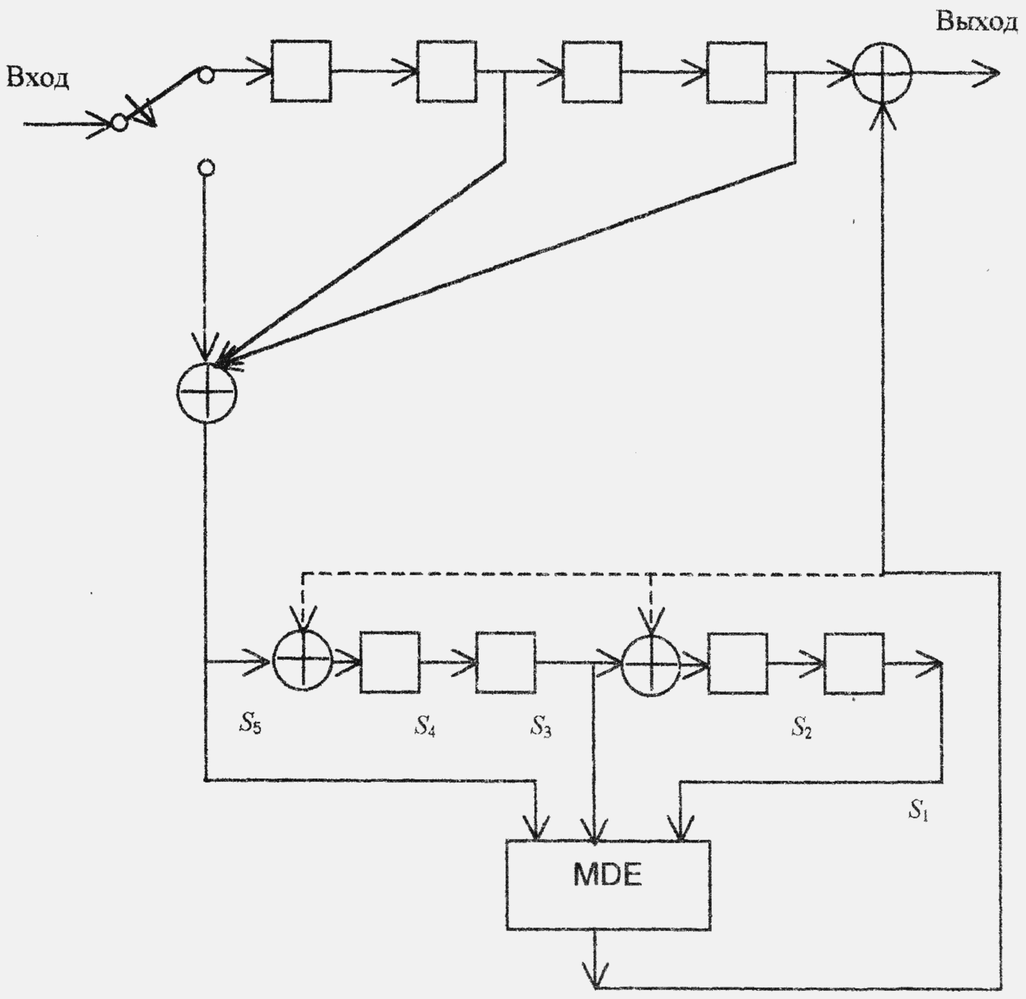

Рис. 1.6. Пример декодера для свёрточного кода

Описанное обстоятельство позволяет применять для декодирования следующую стратегию: если большинство из элементов S_1, S_3 и S_5 равны 1, то полагаем $z_1^{(1)} = 1$; в противном случае полагаем $z_1^{(1)} = 0$. Именно поэтому в составе декодера, схема которого приведена на рис. 1.6, используется мажоритарный элемент.

Для кода с рис.1.4 на рис. 1.6 приведен пример так называемого декодера с обратной связью, который получается из прямого декодера путём добавления в регистр синдрома обратных связей (пунктирные линии на рис. 1.6); здесь мажоритарный элемент MDE (majority decoding element) – пороговый элемент, порог которого равен половине числа его входов. Пунктирные линии на рис. 1.6 относятся к декодированию последующих информационных символов [1.1, с. 278 – 280; 1.2, с. 398 – 399].

1.10. НЕКОТОРЫЕ УТОЧНЕНИЯ ОПРЕДЕЛЕНИЙ ОСНОВНЫХ ПОНЯТИЙ ТЕОРИИ КОДИРОВАНИЯ

Мы приведём сейчас некоторые уточнения определений основных понятий теории кодирования применительно к двоичным блоковым кодам [1.1 – 1.5], о которых пойдёт далее речь в этой книге.

Пусть: A – *исходный* и B – *кодовый* (или *объектный*) конечные алфавиты (мы будем считать, что $A = B = \{0, 1\}$); $S = \{\boldsymbol{s}_i | \ i = 1, 2, \ldots, 2^k\}$ – множество всевозможных B^k двоичных последовательностей символов конечной длины k; φ – некоторое взаимно однозначное (*кодирующее*) отображение множества S ***в множество*** C – некоторое множество 2^k двоичных последовательностей конечной длины $n \geq k$, состоящих из символов алфавита B [1.17, с. 19].

Элементы множества S называются *безызбыточными* или *информационными комбинациями* или *сообщениями*. Элементы множества C называются *кодовыми комбинациями*.

Так как $A = B = \{0, 1\}$, то $S = B^k$ и $C \subseteq B^n$.

ОПРЕДЕЛЕНИЕ 1.11. *Множество C, являющееся образом множества B^k, называется* ***кодом*** *множества B^k. Процесс преобразования элементов множества B^k в элементы множества $C \subseteq B^n$ в соответствии с отображением φ при передаче информации называется* ***кодированием*** *сообщений – элементов множества B^k. Если безызбыточная комбинация $\boldsymbol{s}_i \in B^k$ при кодировании отображается в комбинацию $\boldsymbol{x}_i \in C$, то комбинацию $\boldsymbol{x}_i$ называют кодом сообщения $\boldsymbol{s}_i$, $i = 1, 2, \ldots, 2^k$.*

END

Пусть ψ – произвольное *однозначное* (*декодирующее*) отображение множества B^n ***на множество*** C [1.17, с. 19].

ОПРЕДЕЛЕНИЕ 1.12. *Процесс преобразования принятых (полученных) комбинаций $\{\boldsymbol{y}\}$ – элементов множества B^n в кодовые комбинации $\{\boldsymbol{x}\}$ – элементы множества $C \subseteq B^n$ в соответствии с отображением ψ при помехоустойчивой передаче информации по каналу называется* ***декодированием*** *принятых комбинаций.*

END

Таким образом, понятие *корректирующего блокового двоичного кода*, предполагает наличие следующих понятий и часто их физическую реализацию:

множество двоичных комбинаций B^n;

множество двоичных (безызбыточных) комбинаций B^k, которые иногда называют сообщениями;

кодирующее взаимнооднозначное отображение φ;

некоторый критерий отбора наилучшего в некотором смысле декодирующего однозначного отображения ψ (например, можно наилучшим отображением ψ считать то, которое минимизирует P_e);

декодирующее однозначное отображения ψ;

множество кодовых комбинаций

$$C \subseteq B^n, \tag{1-79}$$

получаемых в результате выполнения операции кодирования элементов B^k.

Матрица $\boldsymbol{C}$ (или C), строками которой являются кодовые слова кода $C \subseteq B^n$, называется матрицей кода C или короче – *кодовой матрицей C*. Иногда мы будем использовать обозначение $\boldsymbol{C}_{(n,\,k)}$ (или $C_{(n,\,k)}$) для обозначения кодовой матрицы (n, k)-кода.

Код $C \subseteq B^n$ с кодовым расстоянием $d_{\min}$ называется *$<n, d_{\min}>$-кодом*.

Максимально возможную мощность $<n, d_{\min}>$-кода будем обозначать как $m(n, d_{\min})$.

$<n, d_{\min}>$-код, мощность которого равна $m(n, d_{\min})$, называется *максимальным кодом*.

$<n, 2t+1>$-код, удовлетворяющий условию: для всякой вершины $\boldsymbol{v} \in B^n$ существует кодовое слово $\boldsymbol{x}$, для которого $d(\boldsymbol{v}, \boldsymbol{x}) \le t$, или, что есть то же самое, $<n, 2t+1>$-код, для которого $m(n, d_{\min}) = \dfrac{2^n}{\sum_{i=0}^{t} C_n^i}$, называется *плотно упакованным или совершенным*.

1.11. ПРИЛОЖЕНИЕ. МЕТРИЧЕСКИЕ ПРОСТРАНСТВА. ЭНЕРГИЯ СИГНАЛА

ПОНЯТИЯ И СООТНОШЕНИЯ ДЛЯ *n*-МЕРНОГО ЕВКЛИДОВОГО ПРОСТРАНСТВА

В [1.8] мы уже упоминали понятие *n*-мерного евклидового пространства. Сейчас мы продолжим изложение некоторых сведений о евклидовом пространстве и других понятиях высшей алгебры, широко используемых в теории кодирования. Безусловно, эти сведения, как и излагаемые в других разделах настоящей книги, носят лишь *справочный характер*, а их изложение ни коим образом не предназначено для первоначального изучения соответствующих разделов высшей математики [1.10 – 1.13].

n-мерный вектор или *n-мерная точка*, являющаяся концом вектора, определяются как упорядоченная совокупность *n вещественных чисел* – координат:

$$\boldsymbol{s} = (s_1, s_2, \ldots, s_n). \qquad (1\text{-}80)$$

Множество всех мыслимых *n*-мерных точек составляет *n*-мерное (арифметическое) пространство.

Сложение векторов $\boldsymbol{s}$ и $\boldsymbol{z} = (z_1, z_2, \ldots, z_n)$ определяется правилом

$$\boldsymbol{s}+\boldsymbol{z} = (s_1+z_1, s_2+z_2, \ldots, s_n+z_n); \qquad (1\text{-}81)$$

произведение вектора $\boldsymbol{s}$ и вещественного числа λ определяется правилом

$$\lambda\boldsymbol{s} = (\lambda s_1, \lambda s_2, \ldots, \lambda s_n); \qquad (1\text{-}82)$$

обозначим символом $\mathbf{0}$ *нуль-вектор* – вектор *n*-мерного арифметического векторного пространства, все координаты которого равны нулю:

$$(0\ 0\ \ldots\ 0) = \mathbf{0}. \qquad (1\text{-}83)$$

Совокупность всевозможных *n*-мерных векторов с операциями сложения векторов и умножения вектора на вещественное число, являющаяся аддитивной абелевой группой относительно операции сложения (см. раздел II настоящей книги), называется *n-мерным векторным пространством.*

Заметим, что в данное определение *n*-мерного векторного пространства не входит операция умножения вектора на вектор.

Вектор z называется *линейной комбинацией векторов* $z_1, z_2, \ldots, z_k$, если существуют такие вещественные числа $\lambda_1, \lambda_2, \ldots, \lambda_k$, что

$$z = \lambda_1 z_1 + \lambda_2 z_2 + \ldots + \lambda_k z_k. \qquad (1\text{-}84)$$

ОПРЕДЕЛЕНИЕ 1.13. *Система векторов* $z_1, z_2, \ldots, z_k$, $k \geq 1$, *называется* ***линейно зависимой****, если существует такая совокупность* ***вещественных чисел*** $\lambda_1, \lambda_2, \ldots, \lambda_k$, *хотя бы одно из которых отлично от нуля, что имеет место равенство*

$$\lambda_1 z_1 + \lambda_2 z_2 + \ldots + \lambda_k z_k = \mathbf{0}. \qquad (1\text{-}85)$$

END

Из приведенного определения следует, например, что если система векторов $z_1, z_2, \ldots, z_k$ содержит два пропорциональных вектора или нулевой вектор, то она линейно зависима [1.11, с. 64].

Очевидно, что если некоторая подсистема системы векторов $z_1, z_2, \ldots, z_k$ является линейно зависимой, то и вся система векторов $z_1, z_2, \ldots, z_k$ является линейно зависимой.

Из определения 1.13 вытекает следующее.

Система векторов $z_1, z_2, \ldots, z_k$ является *линейно независимой*, если для *любой* совокупности вещественных чисел $\lambda_1, \lambda_2, \ldots, \lambda_k$, хотя бы одно из которых отлично от нуля,

$$\lambda_1 z_1 + \lambda_2 z_2 + \ldots + \lambda_k z_k \neq \mathbf{0}. \qquad (1\text{-}86)$$

Очевидно, что если система векторов $z_1, z_2, \ldots, z_k$ линейно независима, то

всякая её подсистема также линейно независима;

ни один из векторов этой системы не является нулевым вектором.

Система линейно независимых векторов $z_1, z_2, \ldots, z_k$ называется *максимальной* линейно независимой системой, если добавление к этой системе *любого* n-мерного вектора z_{k+1} образует линейно зависимую систему.

ОПРЕДЕЛЕНИЕ 1.14. *n-мерным евклидовым пространством R_n ($n \geq 1$) называется n-мерное векторное пространство, для каждой пары элементов которого* $\boldsymbol{s}$ и z *определено* ***скалярное произведение***:

$$\boldsymbol{s} \cdot z = \sum_{i=1}^{n} s_i \cdot z_i \,, \qquad (1\text{-}87)$$

обладающее свойствами:

$\boldsymbol{s} \cdot z = z \cdot \boldsymbol{s}$ (***коммутативность***);

$(\boldsymbol{s}+y)z = \boldsymbol{s} \cdot z + y \cdot z$ (***дистрибутивность***);

$(\lambda\ \boldsymbol{s}) \cdot z = \lambda(\boldsymbol{s} \cdot z)$, λ – *действительное число* (***ассоциативность*** относительно числового множителя);

$\boldsymbol{s} \cdot \boldsymbol{s} \geq 0$, причём $\boldsymbol{s} \cdot \boldsymbol{s} = 0 \Leftrightarrow \boldsymbol{s} = \mathbf{0}$ (***положительная определённость***).

См. «2.9. Приложение. Линейные векторные пространства и линейные алгебры».

END

Обобщением понятия *длина вектора* является *норма вектора*

$$\|\boldsymbol{s}\| = \boldsymbol{s} \cdot \boldsymbol{s} = \sqrt{\sum_{i=1}^{n} s_i^2} \,. \qquad (1\text{-}88)$$

Угол между векторами α вводится с помощью соотношения

$$\cos\alpha = \frac{\boldsymbol{s} \cdot z}{\|\boldsymbol{s}\| \cdot \|z\|}. \qquad (1\text{-}89)$$

Если $\boldsymbol{s} \cdot z = 0$, $\boldsymbol{s}, z \neq \mathbf{0}$, то говорят, что эти вектора ортогональны.

Расстояние Евклида между двумя векторами $\boldsymbol{s}$ и z вводится как норма разности векторов

$$d(\boldsymbol{s}, z) = \|\boldsymbol{s} - z\| = \sqrt{\sum_{i=1}^{n} (s_i - z_i)^2} \,. \qquad (1\text{-}90)$$

Оказывается, что в n-мерном векторном пространстве любая линейно независимая система из n векторов является максимальной, а любая максимальная система линейно независимых векторов состоит n векторов.

Рассмотрим в n-мерном векторном пространстве максимальную совокупность линейно независимых векторов

$$\begin{array}{lll} \boldsymbol{e}_1 = & (1\ 0\ 0\ \ldots\ 0) \\ \boldsymbol{e}_2 = & (0\ 1\ 0\ \ldots\ 0) \\ \ldots & \ldots\ldots\ldots\ldots \\ \boldsymbol{e}_n = & (0\ 0\ 0\ \ldots\ 1), \end{array} \qquad (1\text{-}91)$$

состоящую из n векторов, называемых *единичными*, и являющуюся *базисом* этого пространства.

Любой вектор z пространства может быть представлен как линейная комбинация базисных векторов:

$$z = k_1 \boldsymbol{e}_1 + k_2 \boldsymbol{e}_2 + \ldots + k_n \boldsymbol{e}_n, \qquad (1\text{-}92)$$

где $k_1, k_2, \ldots, k_n$ – вещественные числа, называемые *компонентами или координатами вектора* $\boldsymbol{z}$.

Описанное n-мерное векторное пространство часто называют также n-мерным *линейным пространством*.

В рассмотренном только что n-мерном векторном пространстве существует *бесконечно много* различных базисов [1.11, с. 65, 189].

Если же

координатами n-мерного вектора в (1-80) являются не любые вещественные числа – элементы числового поля бесконечного порядка, а только, например, *целые неотрицательные числа* – элементы числового поля F_0 конечного порядка $L \geq 2$ (см. приложение 2.9),

и

сомножителем λ в (1-82) являются не любые вещественные числа – элементы числового поля бесконечного порядка, а только, например, *целые неотрицательные числа* – элементы числового поля F_0 конечного порядка $L \geq 2$ (см. приложение 2.9),

то

в таком n-мерном векторном пространстве существует *конечное* число различных базисов (см. раздел II настоящей книги).

Если координатами n-мерных векторов и их числовыми сомножителями являются целые неотрицательные числа – элементы числового поля F_0 конечного порядка $L \geq 2$, то совокупность таких векторов с операциями сложения векторов и умножения вектора на число, являющаяся аддитивной абелевой группой по отношению к операции сложения векторов, называется *n-мерным векторным пространством* L_n. В частности, при $L = 2$ число *различных* базисов двоичного n-мерного векторного пространства равно *конечному числу* $N_{(n)}$ (см. подраздел 2.2 настоящей книги).

Подмножество V линейного пространства называется *подпространством* этого пространства, если:

1) для любых векторов $\boldsymbol{x}$ и $\boldsymbol{y}$, принадлежащих V, их сумма $\boldsymbol{x} + \boldsymbol{y}$ также принадлежит V;

2) для любого вектора $\boldsymbol{x} \in V$ и для любого целого числа $\lambda \in F_0$ вектор $\lambda\boldsymbol{x} \in V$.

ПРИМЕР 1.15. Если координатами n-мерных векторов и их числовыми сомножителями являются целые неотрицательные числа – элементы числового двоичного поля F_0 (т.е. если речь идёт о *n-мерном векторном пространстве* L_n), то множество всех возможных линейных комбинаций n-мерных векторов $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_k$, $k \leq n$, из совокупности n линейно независимых векторов (1-91) является k-мерным подпространством V пространства L_n, а вектора $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_k$ являются одним из *базисов* подпространства V.

END

ОБОБЩЕНИЯ

Помимо введённых выше расстояний Хэмминга и Евклида между кодовыми комбинациями в теории кодирования в некоторых случаях используется расстояние Ли.

Весом Ли кодовой комбинации $\boldsymbol{s}=(s_1, s_2, \ldots, s_n)$, где элементы s_i выбираются из совокупности целых неотрицательных чисел $\{0, 1, 2, \ldots, L - 1\}$, $L \geq 2$, называется число

$$w_L(\boldsymbol{s}) = \sum_{i=1}^{n} |\, s_i \,|_L, \qquad (1\text{-}93)$$

где

$$|s_i|_L = \begin{cases} s_i, & \text{если } 0 \leq s_i \leq (L - 1)/2, \\ L - s_i, & \text{если } (L - 1)/2 < s_i \leq L - 1. \end{cases} \qquad (1\text{-}93\text{а})$$

Расстоянием Ли между двумя комбинациями длины n $\boldsymbol{x}$ и $\boldsymbol{z}$ называется вес Ли w_L разности этих двух комбинаций (векторов):

$$d_L(\boldsymbol{x}, \boldsymbol{y}) = w_L(\boldsymbol{x} - \boldsymbol{y}) = \sum_{i=1}^{n} | x_i - y_i |_L , \qquad (1\text{-}94)$$

при этом компоненты вектора $(\boldsymbol{x} - \boldsymbol{y})$ равны разностям соответствующих компонент $\boldsymbol{x}$ и $\boldsymbol{y}$ по модулю L.

При $L = 2$ и $L = 3$ расстояние Ли и расстояние Хэмминга *совпадают*; при $L > 3$ расстояние Ли между двумя комбинациями длины n больше или равно расстояния/ю Хэмминга между ними.

ПРИМЕР 1.16. Предположим, что:

$$L = 5,\ n = 6;\ \boldsymbol{x} = (0\ 0\ 2\ 3\ 0\ 4),\ \boldsymbol{y} = (0\ 3\ 4\ 0\ 0\ 2).$$

Определить $d_L(\boldsymbol{x}, \boldsymbol{y})$.

Компоненты вектора $(\boldsymbol{x} - \boldsymbol{y})$ равны разностям соответствующих компонент $\boldsymbol{x}$ и $\boldsymbol{y}$ по модулю L

$$(\boldsymbol{x} - \boldsymbol{y}) = (0\ 2\ 3\ 3\ 0\ 2), \qquad w_L(\boldsymbol{x} - \boldsymbol{y}) = 0+2+2+2+0+2 = 8;$$

аналогично:

$$(\boldsymbol{y} - \boldsymbol{x}) = (0\ 3\ 2\ 2\ 0\ 3), \qquad w_L(\boldsymbol{y} - \boldsymbol{x}) = 0+2+2+2+0+2 = 8.$$

Таким образом,

$$w_L(\boldsymbol{x} - \boldsymbol{y}) = w_L(\boldsymbol{y} - \boldsymbol{x}) \geq 0.$$

END

ОПРЕДЕЛЕНИЕ 1.15. *Произвольное множество M некоторых элементов (векторов или точек)* $\boldsymbol{x}$, $\boldsymbol{y}$, … называется ***метрическим пространством***, *если*:

указано правило, которое позволяет для любых двух точек $\boldsymbol{x}$, $\boldsymbol{y}$ *из* M *определить число* $d(\boldsymbol{x}, \boldsymbol{y})$ *– расстояние от* $\boldsymbol{x}$ *до* $\boldsymbol{y}$,

и это правило удовлетворяет следующим аксиомам:

1) $d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{y}, \boldsymbol{x})$ для любых $\boldsymbol{x}$, $\boldsymbol{y}$ из M (***симметрия*** *расстояния*);

2) $d(\boldsymbol{x}, \boldsymbol{y}) > 0$ при $\boldsymbol{y} \neq \boldsymbol{x}$; $d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{x}, \boldsymbol{x})=0$ при $\boldsymbol{y} = \boldsymbol{x}$ для любого $\boldsymbol{x}$ (***неотрицательность*** *расстояния*);

3) $d(\boldsymbol{x}, \boldsymbol{z}) \leq d(\boldsymbol{x}, \boldsymbol{y}) + d(\boldsymbol{y}, \boldsymbol{z})$ для любых $\boldsymbol{x}$, $\boldsymbol{y}$, $\boldsymbol{z}$ (***неравенство*** *треугольника*).

При этом функция $d(\boldsymbol{x}, \boldsymbol{y})$ *есть функция координат векторов* $\boldsymbol{x}$ *и* $\boldsymbol{y}$ *и называется* ***метрикой***.

END

ПРИМЕР 1.17

1. Можно показать, что n-мерное векторное евклидово пространство R_n, $n \geq 1$, является *метрическим* пространством с мерой d, определяемой соотношением (1-90).

2. Можно показать, что любое множество M непрерывных функций, определённых на интервале $[a, b]$, с расстоянием, введённым по формуле

$$d(\boldsymbol{x}, \boldsymbol{y}) = \max_{a \leq t \leq b} |x(t) - y(t)|, \qquad (1\text{-}95)$$

является *метрическим* пространством.

END

ПРИМЕНЕНИЯ К ОПИСАНИЮ СИГНАЛОВ

Предположим, что в качестве сигнала в канале используются реализации белого шума, а шум канала является аддитивным белым шумом статистически независимым от сигнала.

Для наглядной геометрической интерпретации шума, сигнала и процесса искажения сигнала при его прохождении через канал с аддитивным белым шумом рассмотрим $2WT$-мерное евклидово пространство в декартовой прямоугольной системой координат [1.16].

Пусть $s_T(t)$ и $n_T(t)$ – реализации длительности $T > 0$ сигнала и аддитивного белого шума соответственно в канале, E_s и E_n – соответствующие им энергии, E_{sn} – их взаимная энергия, Q_s и Q_n – соответствующие им средние за время T мощности, Q_{sn} – их взаимная энергия. Очевидно, что для $s_T(t)$ справедливо соотношение [1.8, с. 58-60]

$$s_T(t) = \sum_{i=1}^{2WT} s_i \frac{sin(\pi(2WT - i))}{\pi(2WT - i)}, \qquad (1\text{-}96)$$

где s_i – отсчёты $s_T(t)$ на временном интервале $[0, T]$; поэтому можно говорить о $2WT$-мерном векторе

$$\boldsymbol{s}_T = (s_1, s_2, \ldots, s_{2WT}); \qquad (1\text{-}97)$$

кроме того, имеют место соотношения

$$E_s = \int_0^T s_T^2(t)dt = \frac{d^2}{2W}, \qquad (1\text{-}98)$$

где

$$d^2 = \sum_{i=1}^{2WT} s_i^2; \qquad (1\text{-}99)$$

$$E_s = Q_s T. \qquad (1\text{-}100)$$

Аналогичные соотношения имеют место для $n_T(t)$; кроме того, с учётом статистической независимости $s_T(t)$ и $n_T(t)$

$$E_{sn} = 2\int_0^T s_T(t)n_T(t)dt = 0, \quad (1\text{-}101) \qquad E_{sn} = Q_{sn}T = 0, \quad (101а)$$

и, следовательно, $Q_{sn} = 0$.

Так как белый шум в канале аддитивный, то

$$E_{(s+n)} = E_s + E_n + E_{sn} = E_s + E_n, \qquad (1\text{-}102)$$

Если в качестве сигнала используются выборки белого шума, то имеет место соотношение

$$Q_s = \sigma_s^2 \qquad (1\text{-}103)$$

[1.8, с. 309], где σ_s – характеристика нормально распределённой случайной величины – сечения случайного процесса – белого шума в момент времени $t_i = i/2W$, $i = 1, 2, \ldots, 2WT$, нормального (одномерного) распределения

$$p(s_i) = \frac{1}{(\sqrt{2\pi} \cdot \sigma_s)} \exp(-\frac{s_i^2}{2\sigma_s^2}). \qquad (1\text{-}104)$$

Плотность $2WT$-мерного нормального распределения

$$p(s_1, s_2, \ldots, s_{2WT}) = \frac{1}{(2\pi Q_s)^{WT}} \exp(-\frac{d^2}{2Q_s}). \qquad (1\text{-}105)$$

Из (1-98), (1-99) и (1-100) следует

$$d = \sqrt{2WTQ_s}. \qquad (1\text{-}106)$$

Соотношения (1-96) – (1-106) позволяют дать наглядную *геометрическую интерпретацию* реализациям сигнала и

шума и процессу искажения сигнала при его передаче по каналу с шумом [1.16].

1.12. ПРИЛОЖЕНИЕ. ОБОЗНАЧЕНИЯ ЧИСЛОВЫХ МНОЖЕСТВ И ЭЛЕМЕНТЫ КОМБИНАТОРИКИ

ОБОЗНАЧЕНИЯ ЧИСЛОВЫХ МНОЖЕСТВ

Числовые множества в данной книге обозначаются большими латинскими буквами (шрифт, как правило, – обычный курсив). Однако некоторые числовые множества обозначаются иначе:

N – множество всех натуральных чисел;
N^+ – множество всех положительных целых чисел: $N^+ = N$;
N^- – множество всех отрицательных целых чисел;
Z – множество всех целых чисел (положительные, отрицательные и нуль): $Z = N^+ \cup \varnothing \cup N^- = N \cup \varnothing \cup N^-$;
Q^+ – множество всех положительных рациональных чисел;
Q^- – множество всех отрицательных рациональных чисел,
Q – множество всех рациональных чисел: $Q = Q^+ \cup 0 \cup Q^-$;
P^+ – множество всех положительных иррациональных чисел;
P^- – множество всех отрицательных иррациональных чисел;
P – множество всех иррациональных чисел: $P = P^+ \cup P^-$;
R – множество всех вещественных чисел (рациональные и иррациональные): $R = Q + P$; $P = R \backslash Q$;
C – множество всех комплексных чисел;
R_n – евклидово n-мерное векторное пространство, $n = 1, 2, \ldots$;
L_n – n-мерное векторное пространство (координаты векторов и сомножители векторов – целые числа – элементы числовых полей конечного порядка L).

ЭЛЕМЕНТЫ КОМБИНАТОРИКИ

Пусть A – некоторое заданное *конечное неупорядоченное множество*, состоящее из *n различных элементов*, которое может быть представлено в виде *любого конкретного списка входящих в него элементов*:

$$A = \{a_1, a_2, a_3, \ldots, a_n\}, \qquad (1\text{-}107)$$

причём перестановка элементов списка не меняет множества его членов A. Если мы будем применять операцию транспозиции (перестановки или обмена местами) к любым двум элементам списка, то каждый раз мы будем получать новый (относительно предыдущего) список и то же самое множество A.

СОЕДИНЕНИЯ

Общим названием *соединения* принято называть следующие три типа комбинаций некоторого числа элементов множества A – конечного неупорядоченного множества, состоящего из n различных между собою элементов. Будем называть множество A *исходным* множеством.

Рассмотрим образованные *по некоторым правилам* элементами заданного множества A ***соединения***: *перестановки*, *размещения* и *сочетания*.

ПЕРЕСТАНОВКИ ИЗ n ЭЛЕМЕНТОВ

Будем составлять с помощью операции транспозиции (перестановки) элементов всевозможные конечные *упорядоченные* множества, содержащие все n различных элементов исходного множества A.

ОПРЕДЕЛЕНИЕ 1.16. *Всевозможные конечные* ***упорядоченные*** *множества*, состоящие из *n* различных элементов, которые можно получить из исходного множества *A*, называются ***перестановками из n элементов***.

END

Число всех возможных перестановок из *n* различных элементов обозначается как P_n и определяется соотношением:

$$P_n = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n = n!;$$

по определению 0! = 1.

Очевидно, что некоторая конкретная перестановка из *n* различных элементов может быть представлена конкретным списком элементов с индивидуальным порядком следования элементов в нём. При этом две *различные* перестановки из *n* различных элементов, образованные из всех *n* различных элементов исходного множества *A*, *отличаются друг от друга лишь порядком следования элементов* в представляющих их конкретных списках.

Заданное множество *A* может быть представлено любым одним из *n*! соответствующих ему списков.

РАЗМЕЩЕНИЯ ИЗ *n* ЭЛЕМЕНТОВ ПО *m* ЭЛЕМЕНТОВ

Выберем некоторым образом из *n* различных элементов исходного множества *A*, *m* различных элементов и будем составлять из этих *m* элементов различные упорядоченные множества.

ОПРЕДЕЛЕНИЕ 1.17. *Всевозможные конечные* ***упорядоченные*** *множества*, содержащие *m* элементов, выбранных из *n* элементов исходного множества *A*, называются ***размещениями из n элементов по m элементов***.

END

Число всех возможных размещений из *n* элементов по *m* обозначается как A_n^m и определяется соотношением:

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

Заметим, что

$$A_n^0 = 1, \qquad A_n^n = P_n = n!.$$

СОЧЕТАНИЯ ИЗ *n* РАЗЛИЧНЫХ ЭЛЕМЕНТОВ ПО *m*

ОПРЕДЕЛЕНИЕ 1.18. *Всевозможные конечные* ***неупорядоченные*** *множества, содержащие m различных элементов*, выбранных из *n* элементов заданного множества *A*, называются ***сочетаниями из n различных элементов по m***.

END

Число всех различных сочетаний из *n* различных элементов по *m* обозначается как C_n^m или $\binom{n}{m}$ и определяется соотношением:

$$C_n^m = \frac{A_n^m}{P_m} = \frac{n!}{m!(n-m)!}.$$

Для числа сочетаний справедливы следующие равенства:

$$C_n^m = C_n^{n-m}; \qquad C_{n+1}^{m+1} = C_n^m + C_n^{m+1};$$

$$C_n^0 + C_n^1 + \ldots + C_n^n = \sum_{i=0}^{n} C_n^i = 2^n.$$

Последнее соотношение иногда называется «теоремой о конечных множествах»: *Число всех подмножеств множества, состоящего из n элементов, равно* 2^n.

Из приведенных выше соотношений следует:

$$C_n^0 = C_n^n = 1.$$

БИНОМ НЬЮТОНА

Приведенное ниже выражение известно под названием бинома Ньютона. При целом положительном n справедливо выражение:

$$(a+b)^n = a^n + C_n^1 a^{n-1}b + C_n^2 a^{n-2}b^2 + \ldots + C_n^{n-1} ab^{n-1} + b^n =$$

$$= \sum_{i=0}^{n} C_n^i a^{n-i} b^i$$

В частном случае при $a = b = 1$

$$(1+1)^n = C_n^0 + C_n^1 + C_n^2 + \ldots + C_n^{n-1} + C_n^n = \sum_{i=0}^{n} C_n^i = 2^n .$$

1.13. ЗАДАЧИ

В приведенных ниже формулировках задач при рассмотрении векторных пространств, если не оговорено противное, подразумевается, что координаты векторов являются целыми неотрицательными числами из множества $\{0, 1, \ldots, L - 1\}$, где $L \geq 2$.

1.1. Определить:

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

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

1.2. 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 $\boldsymbol{b}_i = \mathbf{0}$.

1.3. Показать, что расстояние Евклида является метрикой.

1.4. Показать, что расстояние Хэмминга является метрикой.

1.5. Показать, что расстояние Ли является метрикой.

1.6. Показать, что при $L = 2$ и $L = 3$ расстояние Ли и расстояние Хэмминга между двумя комбинациями длины n *совпадают*, а при $L > 3$ расстояние Ли больше/равно расстояния/ю Хэмминга.

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

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

1.8. Чему равно число векторов $\boldsymbol{z} \in B_k^n$, удовлетворяющих условию:

$$2^{n-1} \leq \gamma(\boldsymbol{z}) < 2^n \, ? \qquad (1\text{-}108)$$

1.9. Пусть $\boldsymbol{x}$ и $\boldsymbol{z}$ – некоторые вектора из B^n, $d(\boldsymbol{x}, \boldsymbol{z}) = m$. Найти число векторов $\boldsymbol{y}$ из B^n, удовлетворяющих условию:

1) $d(\boldsymbol{x}, \boldsymbol{y}) + d(\boldsymbol{y}, \boldsymbol{z}) = d(\boldsymbol{x}, \boldsymbol{z})$;

2) $d(\boldsymbol{x}, \boldsymbol{y}) = k, \quad d(\boldsymbol{y}, \boldsymbol{z}) = r$;

3) $d(\boldsymbol{x}, \boldsymbol{y}) \leq k; \quad d(\boldsymbol{y}, \boldsymbol{z}) = r$.

1.10. Пусть $\boldsymbol{x}$ и $\boldsymbol{z}$ – некоторые вектора из B^n, $d(\boldsymbol{x}, \boldsymbol{z}) = m$. Найти N_y – число векторов $\boldsymbol{y}$ из B^n, удовлетворяющих условию:

$$d(\boldsymbol{x}, \boldsymbol{y}) + d(\boldsymbol{y}, \boldsymbol{z}) > d(\boldsymbol{x}, \boldsymbol{z}).$$

1.11. 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?

1.12. 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:

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

5) 00001 00010 00100 01000 10000.

6) (5,4)-код:

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

1.13. 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.

Сравнить применение в рассматриваемом канале кодов № 1 ($d_{\min}$=5) и № 3 ($d_{\min}$=3) из предыдущей задачи.

1.14. 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?

1.15. 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.

1.16. Найти максимально возможную мощность кода $C \subseteq B^n$, расстояние Хемминга $d(\boldsymbol{x}, \boldsymbol{y})$ между двумя произвольными кодовыми векторами $\boldsymbol{x}$ и $\boldsymbol{y}$ которого – чётное число.

1.17. Сколько существует максимальных $<n, 2>$-кодов ?

1.18. Показать, что мощность плотно упакованного $<n, 2t+1>$-кода равна $2^n / \sum_{i=0}^{t} C_n^i$.

1.19. Существует ли плотно упакованный $<n, 3>$-код при n=147?

1.20. Показать, что при $n > 7$ не существует плотно упакованных $<n, 7>$-кодов.

1.21. Показать, что не существует эквидистантных $<n, 2t+1>$-кодов мощности больше 2.

1.22. Показать, что при чётном $d_{\min}$ существует эквидистантный код мощности $]2n/d_{\min}[$.

1.23. 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.

1.24. 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, $2t+e+1$.

1.25. Дерево, приведенное на рис. 1.3, является периодически повторяющимся. Определить вес пути наименьшего веса, проходящего через всё дерево. Показать, что независимо от значения n не все двойные комбинации ошибок могут быть исправлены.

1.14. ВЫВОДЫ

В данном разделе книги было приведено изложение некоторых основополагающих вопросов теории кодирования. В частности, здесь были рассмотрены вопросы:

понятие корректирующего кода, потенциальные обнаруживающая и исправляющая способности корректирующего кода;

основные способы обнаружения и исправления ошибок, лежащие в основе построения корректирующих кодов;

комбинация и её вес, хэммингово расстояние между двумя комбинациями, кодовое расстояние;

вектор ошибки и назначение ошибок к исправлению;

корректирующая способность кода и кодовое расстояние;

общие соображения о сложности кодера и декодера, реализующих рассматриваемый алгоритм декодирования принятых комбинаций;

определён ряд основных корректирующих кодов; блоковые коды: коды с многократной передачей символов, коды со стиранием символов, коды с проверкой на чётность; введено понятие свёрточного (непрерывного) корректирующего кода;

введены следующие сравнительные характеристики корректирующих кодов: вероятность ошибки на сообщение

P_e, скорость передачи данных R, простота реализации кодера и декодера; для блоковых кодов введены также характеристики: длина кода n, кодовое расстояние d_{min}, число кодовых комбинаций N и другие характеристики;

связь между расстоянием точки, изображающей сигнал, от начала координат в метрическом $2WT$-мерном пространстве и энергией сигнала;

приведены некоторые необходимые справочные данные.

1.15. ЛИТЕРАТУРА

Основная

1.1. Галлагер Р. Теория информации и надёжная связь. М.: Советское радио, 1974.

1.2. Берлекэмп Э. Алгебраическая теория кодирования. М.: Мир, 1971.

1.3. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М.: Мир, 1976.

1.4. Касами Т., Токура Н., Ивадари Ё и др. Теория кодирования. М.: Мир, 1978.

1.5. Гаврилов Г.П., Сапоженко А.А. Сборник задач по дискретной математике. М.: Наука, 1977.

1.6. Аршинов М.Н., Садовский Л.Е. Коды и математика. Серия: библиотечка «Квант». М.: Наука, 1983.

1.7. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986.

Дополнительная

1.8. Панин В.В. Основы теории информации. Ч.1. М.: МИФИ, 2001.

1.9. Харкевич А.А. Борьба с помехами. М.: Наука, 1965.

1.10. Фихтенгольц Г.М. Курс дифференциального и интегрального исчисления. Т.1. М.: ФИЗМАТЛИТ, 2001

1.11. Курош А.Г. Курс высшей алгебры. М.: Физматгиз, 1963.

1.12. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров: Пер. с англ. М.: Наука, 1968.

1.13. Бронштейн И.Н., Семендяев К.А. Справочник по математике для инженеров и учащихся вузов. М.: Наука, 1980.

1.14. Яглом А.М., Яглом И.М. Вероятность и информация. М.: Наука, 1973.

1.15. Постников М.М. Теория Галуа. М.: Факториал Пресс, 2003.

1.16. Шеннон К. Связь при наличии шума, 1949./ Работы по теории информации и кибернетике. М.: ИИЛ, 1963.

1.17. Биркгоф Г., Барти Т. Современная прикладная алгебра. М.: Мир, 1976.

1.18. Вероятность и математическая статистика: Энциклопедия / Под ред. Ю.В. Прохорова. М.: Большая Российская энциклопедия, 2003.