Р. Д. ПЕТРОСЯН

О НЕКОТОРЫХ ВОПРОСАХ ДЕКОДИРОВАНИЯ ЛИНЕЙНЫХ КОДОВ

Одной из наиболее актуальных проблем теории кодирования в настоящее время является задача декодирования, в частности, двоичных линейных (n, k)-кодов. Можно отметить два существенных недостатка имеющихся схем декодирования:

а) обнаружение и исправление ошибок, имевших место при передаче по каналу связи, производится не непосредственно по принятому на приемном конце слову, а обычно для этого требуется целый ряд вычислений (нередко практически трудно реализуемых), что часто приводит к необходимости дополнительного повышения скорости обработки информации;

б) весьма ограничена область применения этих схем.

Отмеченные трудности не преодолены даже в сравнительно простом и в наиболее важном случае двоичных циклических кодов.

Наиболее удачным с точки зрения технической реализации можно считать пороговое декодирование, при котором выделение помехи достигается k-кратным применением алгоритма, позволяющего установить принадлежность выделяемой помехи к одному из двух подмножеств:

1) E_1, включающему всевозможные помехи, содержащие в первом разряде единицу (т. е. когда первый информационный символ кодового слова принимается ошибочно),

2) E_2, включающему всевозможные помехи, содержащие в первом разряде нуль.

Однако эффективное применение порогового декодирования пока ограничивается в основном двоичными кодами максимальной длины. По-видимому, свойство ортоганализуемости кодов, с которым связано пороговое декодирование, как и все остальные известные свойства кодов, используемые в других методах декодирования, недостаточно глубоко вскрывают внутреннюю взаимосвязь кодовых последовательностей. Поэтому в целях дальнейшего исследования структурных свойств кодов представляется весьма интересным рассмотрение задачи декодирования (n, k)-кодов с несколько иной точки зрения: не задаваться заранее разбиением множества помех, а найти такое разбиение множества всевозможных помех на непересекающиеся подмно-

жества $E_1, E_2, \cdots E_q^{\tau}$ (не ограничивая τ), при котором существовал бы простой способ отнесения заданной помехи к соответствующему подмножеству.

Ниже на частном примере кодов максимальной длины рассматривается один из возможных методов решения этой задачи. В работе [1] показана применимость его к более широкому классу линейных кодов, а в [2] приведен другой подход к решению этой задачи.

Известные методы декодирования линейных и, в частности, циклических кодов основаны, как правило, на использовании изоморфного соответствия между множеством помех с произвольным, но известным вероятностным распределением, и множеством синдромов, определяемых следующим образом: если передавалось слово $l = (a_1, a_2, \cdots a_k, a_{k+1}, \cdots, a_n)$, $(k+j)$-ый символ которого связан с информационными символами некоторым проверочным соотношением

$$a_{k+j} = \sum_{i=1}^{k} C_{j,i} a_i, \tag{1}$$

где $j = 1, 2, \cdots, h = n - k$,
а получено слово $b = (\beta_1, \beta_2, \cdots, \beta_k, \beta_{k+1}, \cdots, \beta_n)$, отличающееся от l „шумовой последовательностью" $e = l - b = (e_1, e_2, \cdots, e_n)$, то j-ая компонента синдрома $z = (z_1, z_2, \cdots, z_h)$

$$z_j = \sum_{i=1}^{k} C_{j,i} \beta_i - \beta_{k+j},$$

или же

$$z_j = \sum_{i=1}^{k} C_{j,i} e_i - e_{k+j}.$$

Допустим, что $e_{k+1} = \cdots = e_n = 0$, т. е. при передаче по каналу связи проверочная часть кодовых слов не искажена. Тогда

$$z_j = \sum_{i=1}^{k} C_{j,i} \cdot e_i \tag{2}$$

и, следовательно, синдром $z = (z_1, z_2, \cdots, z_h)$ совпадет с проверочной частью такого кодового слова, информационные символы $a_1, a_2, \cdots, a_k$ которого равны: $a_1 = e_1$, $a_2 = e_2, \cdots, a_k = e_k$.

Представим множество всех кодовых слов (n, k)-кода в виде матрицы $H = (H_{\text{инф.}} \; H_{\text{пров.}})$:

$$\begin{bmatrix} a_{1,1}, & a_{1,2}, \cdots, a_{1,k}, & a_{1,k+1}, \cdots, a_{1,k+h} \\ a_{2,1}, & a_{2,2}, \cdots, a_{2,k}, & a_{2,k+1}, \cdots, a_{2,k+h} \\ \cdots & \cdots & \cdots \\ a_{2^k,1}, & a_{2^k,2}, \cdots, a_{2^k,k}, & a_{2^k,k+1}, \cdots, a_{2^k,k+h} \end{bmatrix},$$

где $H_{\text{инф.}}$ — первые k столбцов — информационная часть кодовых слов,

а $H_{\text{пров.}}$ — последующие h столбцов — проверочная часть кодовых слов.

Тогда в силу (2), при $e_{k+1} = \cdots = e_n = 0$, множество всех синдромов Z совпадает с $H_{\text{пров.}}$.

Рассмотрим класс двоичных кодов максимальной длины. Разобьем множество $Z = H_{\text{пров.}}$, соответствующее данному (n, k)-коду при $e_{k+1} = \cdots = e_n = 0$, на непересекающиеся подмножества A_1, $A_2, \cdots, A_\tau$, исходя из весов синдромов z. Пусть A_1 содержит все векторы z из Z наибольшего веса. Обозначим этот вес через β,

$$A_2 — \text{все векторы веса } \beta - 1,$$
$$\cdots\cdots\cdots\cdots$$
$$A_\tau \quad „ \quad „ \quad „ \ \beta - \tau - 1.$$

Поскольку рассматривается код максимальной длины, ясно, что $\tau = k$ и A_1 будет соответствовать множеству помех

$$E_1, \text{ содержащих каждая лишь одну единицу,}$$
$$A_2 — E_2, \quad „ \quad „ \quad „ \quad \text{две единицы,}$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$A_k — E_k \quad „ \quad „ \quad „ \quad k \text{ единиц}$$

(Понятно, что эти ошибки приходятся на первые k разрядов кодового слова).

Подберем некоторую матрицу

$$P = \begin{bmatrix} p_{1,1}(\alpha), & p_{2,1}(\alpha), & \cdots, & p_{k,1}(\alpha) \\ p_{1,2}(\alpha), & p_{2,2}(\alpha), & \cdots, & p_{k,2}(\alpha) \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots\cdots \\ p_{1,h}(\alpha), & p_{2,h}(\alpha), & \cdots, & p_{k,h}(\alpha) \end{bmatrix},$$

где $P_{i,j}(\alpha)$ $(i = 1, 2 \cdots, k,\ j = 1, 2, \cdots, h,\ \alpha = 0, 1)$ — некоторые числовые функции, определенные в поле $GF(2)$. Подберем эти функции так, чтобы при умножении (условно назовем эту операцию умножением) произвольного вектора $z \in Z$ на P

$$z \times P = (z_1, z_2, \cdots, z_h) \times P = \Delta_1(z),\ \Delta_2(z), \cdots, \Delta_k(z),$$

$$\text{где } \Delta_i(z) = \sum_{j=1}^{h} P_{i,j}(z_j),$$

выполнялось условие

$$\Delta_i(z) > \max_{\substack{t=1,2,\cdots,k \\ t \neq i}} \Delta_t(z) \qquad \text{при } z \in A_i, \tag{3}$$

т. е. при $e \in E_i$.

Ясно, что если бы условие (3) выполнялось и при $e_{k+1}, \cdots, e_n \neq 0$, то тем самым была бы частично решена задача декодирования, а именно: можно было бы отнести заданную помеху к соответствующему подмножеству E.

Определим $P_{i,j}(\alpha)$ следующим образом:

$$p_{i,j}(z) = (-1)^z \frac{2}{n(A_i)} \sum_{x \in A_i} \left(\frac{1}{2} - x_j\right), \qquad (4)$$

где $n(A_i)$ — число элементов подмножества A_i, z_j — значение j-ой компоненты синдрома

$$z = (z_1, z_2, \cdots, z_k), \qquad z = \{0, 1\}.$$

Иными словами, $p_{i,j}(z)$ — дробь, числитель которой является разностью между числом единичных и числом нулевых символов в j-ом столбце A_i, а знаменатель — их сумма, т. е. число элементов A_i. Вообще говоря, $p_{i,j}(z)$ может быть определен и другим способом, в частности, ниже рассмотрен другой пример. Более подробно этот вопрос обсуждается в статье [1].

Обозначим число ненулевых коэффициентов в правой части уравнения (1) через v_j. Очевидно, что всего имеется

$$\begin{aligned} &c_k^2 \text{ проверочных соотношений с } v_j = 2, \\ &c_k^3 \quad . \quad . \quad . \quad . \quad v_j = 3 \\ &\cdots\cdots\cdots\cdots\cdots \\ &c_k^k = 1 \quad . \quad . \quad . \quad . \quad v_j = k, — \end{aligned}$$

в соответствии с $(c_k^2 + c_k^3 + \cdots + c_k^k)$ проверочными символами данного кода.

Рассмотрим матрицу, состоящую из C_k^i строк и k столбцов, образованную из всевозможных слов длины k и веса i. Выделим произвольные t столбцов ($t \leqslant k$). Очевидно, что число строк, содержащих в местах пересечения с выбранными t столбцами h единиц ($h \leqslant i$), будет:

$$C_t^h \cdot C_{k-t}^{i-h}.$$

Поскольку j-ый проверочный символ $a_{i,k+j} = 0$ ($a_{i,k+j} = 1$), если среди соответствующих v информационных символов содержится четное число единичных символов (соответственно нечетное число), то, исходя из вышесказанного, можно заключить, что среди векторов подмножества A_i число векторов, у которых j-ая компонента равна нулю (единице), будет:

$$\sum_{h=0}^{i} C_{v_j}^h \cdot C_{k-v_j}^{i-h},$$

где h — четное число (соответственно нечетное), а (4) примет вид:

$$P_{i,j}(z) = (-1)^z \cdot \frac{1}{C_k^i} \sum_{h=0}^{i} (-1)^h \cdot C_{v_j}^h \cdot C_{k-v_j}^{i-h}. \qquad (5)$$

Рассмотрим такую задачу: имеется k символов, среди которых l единиц и $(k-l)$ нулей. Нужно выбрать v символов ($v \leqslant k$) так, чтобы среди этих выбранных символов было l единиц и $(v-l)$ нулей

$(l \leqslant i)$. Очевидно, что для этого есть $C_i^l \cdot C_{k-i}^{v-l}$ способов. Исходя из этого можно заключить, что среди тех символов произвольного вектора из A_i, которым соответствуют $v_j = v$, будет нулевых (единичных) — $\sum_{l=0}^{i} C_i^l \cdot C_{k-i}^{v-l}$ символов, где l—четное (соответственно нечетное).

Отсюда, используя (5), получим для $\Delta_i(z)$:

$$\Delta_{i,j}(z) = \sum_{v=2}^{k} \sum_{l=0}^{j} (-1)^l C_j^l \cdot C_{k-j}^{v-l} \frac{1}{C_k^l} \sum_{h=0}^{i} (-1)^h C_v^h C_{k-v}^{l-h}, \qquad (6)$$

где $\Delta_{i,j}(z)$ — это $\Delta_i(z)$ при $z \in A_j$. Можно показать, что имеет место неравенство: $\Delta_{i,i}(z) > \Delta_{j,i}(z)$, т. е. условие (3) выполняется. Этот вопрос, в частности, рассматривается в работе [1]. А теперь приведем другое определение функции $p_{i,j}(\alpha)$, несколько отличное от (4), при котором очень просто и наглядно можно показать, что

$$\Delta_{i,i}(z) \geqslant \Delta_{j,i}(z).$$

Пусть

$$P_{i,j}(\alpha) = \begin{cases} -1, \text{ если значение } P_{i,j}(\alpha), \text{ полученное} \\ \quad \text{по формуле (4), отрицательно} \\ +1, \text{ если } \text{„} \quad \text{„} \quad \text{„ положительно} \\ 0, \text{ если } \text{„} \quad \text{„} \quad \text{„ равно нулю} \end{cases}$$

Рассмотрим матрицу A_i. Переставим ее столбцы так, чтобы в первых C_k^2 разрядах были записаны те компоненты z_j, которым соответствуют $v_j = 2$, — обозначим этот участок через 1, в следующих C_k^3 разрядах — компоненты z_j, которым соответствуют $v_j = 3$, — участок 2 и т. д. Тогда каждая строка матрицы A_i на μ-ом участке ($\mu = 1, 2, \cdots, (k-1)$) будет содержать одно и то же число единиц — пусть t_1, нулей — пусть t_0, и каждый столбец матрицы, расположенный на μ-ом участке, также будет содержать одно и то же число единиц, — пусть l_1 — и нулей — пусть l_0 — все это непосредственно следует из вывода формулы (6). Исходя из этого, можно записать:

$$l_1 = \frac{t_1 \cdot C_k^l}{C_k^{v_\mu}}, \qquad l_0 = \frac{t_0 \cdot C_k^l}{C_k^{v_\mu}}.$$

Отсюда имеем:

$$l_1 - l_0 = \frac{C_k^l \cdot (t_1 - t_0)}{C_k^{v_\mu}}$$

и, значит, если на μ-ом участке в строках A_i преобладают единицы (нули), то и в столбцах преобладают единицы (нули); равенство числа единиц и числа нулей также одновременно должно иметь место в строках и столбцах. Очевидно, что на μ-ом участке компоненты вектора $(p_{i,1}(\alpha), p_{i,2}(\alpha), \cdots, p_{i,h}(\alpha))$ (после аналогичных перестановок) будут равны между собой.

Теперь сопоставим значения $\Delta_{i,1}(z)$ и $\Delta_{j,1}(z)$, вычисленные (после соответствующих перестановок столбцов A_j) для p-го участка: $\Delta^p_{i,1}(z)$ и $\Delta^p_{j,1}(z)$. Из сказанного следует, что если компоненты векторов

$$(p_{i,1}(z),\ p_{i,2}(z),\ \cdots,\ p_{i,k}(z)) \quad \text{и} \quad (p_{j,1}(z),\ p_{j,2}(z),\ \cdots,\ p_{j,k}(z))$$

на p-ом участке совпадают, то $\Delta^p_{i,1}(z) = \Delta^p_{j,1}(z)$, если же они не совпадают, то $\Delta^p_{i,1}(z) > \Delta^p_{j,1}(z)$.
Следовательно,

$$\Delta_{i,1}(z) \geqslant \Delta_{j,1}(z).$$

Автор признателен Р. Р. Варшамову за существенную помощь при выполнении данной работы.

Ռ. Գ. ՊԵՏՐՈՍՅԱՆ

ԳԾԱՅԻՆ ԿՈԴԵՐԻ ԱՖԱԿՈԴԱՎՈՐՄԱՆ ՈՐՈՇ ՀԱՐՑԵՐԻ ՄԱՍԻՆ

Ա մ փ ո փ ո ւ մ

Դիտարկվում է առավելագույն երկարության երկուական (n, k)-կոդ: Ապացուցվում, երբ հաղորդման ժամանակ կոդային բառի ստուգողական մասը չի աղավաղված, տրված է շատ պարզ ալգորիթմ, որը ոչ բարդ հաշվումների միջոցով որոշում է կամայական $z \in Z$ ստուգող վեկտորի պատկանելությունը բոլոր ստուգող վեկտորների Z բազմությանն՝ միմյանց հետ չհատվող $Z_1, \cdots, \cdots Z_k$ ենթաբազմություններից որևէ մեկին:

Ենդրի լուծումը բերված է այն j-ի, $j = 1, 2, \cdots, k$ որոշմանը, որի դեպքում $z \in Z_j$ վեկտորի և Z_j ենթաբազմության «մոտիկությունը» բնորոշող $\Delta_{i,j}(z)$ ֆունկցիան հասնում է մաքսիմումի: Ստացված է $\Delta_{i,j}(z)$ ֆունկցիայի բանաձևը:

ЛИТЕРАТУРА

1. *Р. Д. Петросян.* О некоторых свойствах двоичных линейных кодов. Труды I Конференции молодых специалистов ВЦ АН АрмССР и ЕрГУ, т. 2, Ереван, 1969.
2. *Р. Д. Петросян.* Об одном разбиении двоичных линейных алфавитов. Труды I Конференции молодых специалистов ВЦ АН АрмССР и ЕрГУ, т. 2, Ереван, 1969.