МАТЕМАТИКА

УДК 681.3.07

Н. Н. ТАШАТОВ

ДЕКОДИРОВАНИЕ КОДА РИДА – СОЛОМОНА

(Представлена академиком НАН РК М. О. Отелбаевым)

Рассмотрены вопросы возможности кодирования в систематической форме тестовое сообщение, вычисление синдрома, локализация ошибки и проверка надежности, значения ошибок и исправление принятого многочлена с помощью найденного многочлена ошибок.

С помощью кода Рида–Соломона (7, 3) тестовое сообщение можно кодировать в систематической форме. В результате получаем многочлен кодового слова, который описывается уравнением [1, 2].

$$\boldsymbol{U}(X) = \sum_{n=0}^{6} u_n X^n,$$

$$\boldsymbol{U}(X) = \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^6 X^3 + \alpha^1 X^4 + \alpha^3 X^5 + \alpha^5 X^6 \quad (100) + (001)X + (011)X^2 + (101)X^3 + (010)X^4 + (110)X^5 + (111)X^6. \quad (1)$$

Пусть в ходе передачи это кодовое слово подверглось искажению: 2 символа были приняты с ошибкой. Такое количество ошибок соответствует максимальной способности кода к коррекции ошибок. При использовании 7-символьного кодового слова модель ошибки можно представить в виде многочлена следующим образом:

$$\boldsymbol{e}(X) = \sum_{n=0}^{6} e_n X^n. \quad (2)$$

Пусть двухсимвольная ошибка будет такой, что

$$\boldsymbol{e}(X) = 0 + 0 \cdot X + 0 \cdot X^2 + \alpha^2 X^3 + \alpha^5 X^4 + 0 \cdot X^5 + 0 \cdot X^6 \quad (000) + (000)X + (000)X^2 + (001)X^3 + (111)X^4 + (000)X^5 + (000)X^6, \quad (3)$$

т.е. контрольный символ искажен 1-битовой ошибкой (представленной как α^2), а символ сообщения 3-битовой ошибкой (представленной как α^5). В этом случае принятый многочлен поврежденного кодового слова $\boldsymbol{r}(X)$ представляется в виде суммы многочлена переданного кодового слова и многочлена модели ошибки

$$\boldsymbol{r}(X) = \boldsymbol{U}(X) + \boldsymbol{e}(X). \quad (4)$$

Сложим (1) и (3), получаем следующее:

$$\boldsymbol{r}(X) = (100) + (001)X + (011)X^2 + (100)X^3 + (101)X^4 + (110)X^5 + (111)X^6 \quad \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^0 X^3 + \alpha^6 X^4 + \alpha^3 X^5 + \alpha^5 X^6. \quad (5)$$

В этом примере имеется четыре неизвестных: два относятся к расположению ошибки, а два касаются ошибочных значений. Отметим важное различие между недвоичным декодированием $\boldsymbol{r}(X)$, которое показано в уравнении и двоичным. При двоичном декодировании декодеру нужно знать лишь расположение ошибки. Если известно, где находится ошибка, то бит нужно поменять с 1 на 0 или наоборот. А недвоичные символы требуют, чтобы мы не только узнали расположение ошибки, но и определили правильное значение символа, расположенного на этой позиции. Поскольку в данном примере имеется четыре неизвестных, нам нужно четыре уравнения, чтобы найти их.

Вычисление синдрома. Синдром – это результат проверки четности, выполняемой над $\boldsymbol{r}$, чтобы определить, принадлежит ли $\boldsymbol{r}$ набору кодовых слов. Если $\boldsymbol{r}$ является членом набора, то синдром $\boldsymbol{S}$ имеет значение, равное 0. Любое ненулевое значение $\boldsymbol{S}$ означает наличие ошибок. Как и в двоичном случае, синдром $\boldsymbol{S}$ состоит из $n - k$ символов S_i (i = 1, ..., $n - k$). Таким образом, в нашем коде (7, 3) имеется по четыре символа в каждом векторе синдрома. Их значения можно вычислить из принятого многочлена $\boldsymbol{r}(X)$. Вычисления облегчаются благодаря самой структуре кода, определяемой уравнением.

$$\boldsymbol{U}(X) = \boldsymbol{m}(X)\boldsymbol{g}(X). \quad (6)$$

Из этой структуры видно, что каждый правильный многочлен кодового слова $\boldsymbol{U}(X)$ является

кратным генератору многочлена $\boldsymbol{g}(X)$. Отсюда следует, что корни $\boldsymbol{g}(X)$ также должны быть корнями $\boldsymbol{U}(X)$. Так как $\boldsymbol{r}(X) = \boldsymbol{U}(X) + \boldsymbol{e}(X)$, то $\boldsymbol{r}(X)$, вычисляемый с каждым корнем $\boldsymbol{g}(X)$, должен давать нуль, если только $\boldsymbol{r}(X)$ будет правильным кодовым словом. Любые ошибки приведут в итоге к ненулевому результату в одном или более случае. Символы синдрома вычисляются следующим образом:

$$S_i = \boldsymbol{r}(X)\big|_{X=\alpha^i} = \boldsymbol{r}(\alpha^i),\ i = 1,2,\ldots,n-k. \quad (7)$$

Здесь, $\boldsymbol{r}(X)$ содержит 2-символьные ошибки, как было показано в уравнении (3). Если $\boldsymbol{r}(X)$ окажется правильным кодовым словом, то это приведет к тому, что все символы синдрома S_i будут равны нулю. Найдем четыре символа синдрома

$$S_1 = \boldsymbol{r}(\alpha) \quad \alpha^0 + \alpha^3 + \alpha^6 + \alpha^3 + \alpha^{10} + \alpha^8 + \alpha^{11} =$$
$$= \alpha^0 + \alpha^3 + \alpha^6 + \alpha^3 + \alpha^2 + \alpha^1 + \alpha^4 = \alpha^3, \quad (8)$$

$$S_2 = \boldsymbol{r}(\alpha^2) \quad \alpha^0 + \alpha^4 + \alpha^8 + \alpha^6 + \alpha^{14} + \alpha^{13} + \alpha^{17} =$$
$$= \alpha^0 + \alpha^4 + \alpha^1 + \alpha^6 + \alpha^0 + \alpha^6 + \alpha^3 = \alpha^5, \quad (9)$$

$$S_3 = \boldsymbol{r}(\alpha^3) \quad \alpha^0 + \alpha^5 + \alpha^{10} + \alpha^9 + \alpha^{18} + \alpha^{18} + \alpha^{23} =$$
$$= \alpha^0 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha^4 + \alpha^4 + \alpha^2 = \alpha^6, \quad (10)$$

$$S_4 = \boldsymbol{r}(\alpha^4) \quad \alpha^0 + \alpha^6 + \alpha^{12} + \alpha^{12} + \alpha^{22} + \alpha^{23} + \alpha^{29} =$$
$$= \alpha^0 + \alpha^6 + \alpha^5 + \alpha^5 + \alpha^1 + \alpha^2 + \alpha^1 = 0. \quad (11)$$

Результат вычисления показывает, что принятое кодовое слово содержит введенную нами ошибку, так как $\boldsymbol{S} \neq 0$.

Локализация ошибки и проверка надежности. Допустим, в кодовом слове имеется ν ошибок, расположенных на позициях $X^{j_1}, X^{j_2}, \ldots, X^{j_\nu}$. Тогда, определяемый уравнениями (2) и (3), многочлен ошибок можно записать следующим образом:

$$\boldsymbol{e}(X) = e_{j_1} X^{j_1} + e_{j_2} X^{j_2} + \ldots + e_{j_\nu} X^{j_\nu}. \quad (12)$$

Индексы $1,2,\ldots,\nu$ обозначают 1-ю, 2-ю, ..., ν-ю ошибки, а индекс j – расположение ошибки. Для коррекции искаженного кодового слова нужно определить каждое значение ошибки e_{j_l} и ее расположение X^{j_l}, где $l = 1,2,\ldots,\nu$. Обозначим номер локатора ошибки через $\beta_l = \alpha^{j_l}$. Вычислим $n - k = 2t$ символа синдрома, подставляя α_i, в принятый многочлен при $i = 1, 2, \ldots, 2t$.

$$\begin{aligned} S_1 &= \boldsymbol{r}(\alpha) \quad = e_{j_1}\beta_1 + e_{j_2}\beta_2 + \ldots + e_{j_\nu}\beta_\nu \\ S_2 &= \boldsymbol{r}(\alpha^2) = e_{j_1}\beta_1^2 + e_{j_2}\beta_2^2 + \ldots + e_{j_\nu}\beta_\nu^2 \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (13) \\ S_{2t} &= \boldsymbol{r}(\alpha^{2t}) = e_{j_1}\beta_1^{2t} + e_{j_2}\beta_2^{2t} + \ldots + e_{j_\nu}\beta_\nu^{2t} \end{aligned}$$

Имеем систему из $2t$ уравнений с $2t$ неизвестными (t значений ошибок и t расположений). Эту систему уравнений нельзя решить обычным путем, так как уравнения в ней нелинейные (некоторые неизвестные входят в уравнение в степени). Методика, позволяющая решить систему уравнений (13), называется алгоритмом декодирования Рида-Соломона.

Если вычислен ненулевой вектор синдрома, у которой один или более его символов не равны нулю, это означает, что была принята ошибка. Нужно узнать расположение ошибки или ошибок. Многочлен локатора ошибок определим следующим образом:

$$\boldsymbol{\sigma}(X) = (1 + \sigma_1 X)(1 + \sigma_2 X)\ldots(1 + \sigma_\nu X) =$$
$$= 1 + \sigma_1 X + \sigma_2 X^2 + \ldots + \sigma_\nu X^\nu. \quad (14)$$

$\frac{1}{\beta_1}, \frac{1}{\beta_2}, \ldots, \frac{1}{\beta_\nu}$ являются корнями $\boldsymbol{\sigma}(X)$. Величины, обратные корням $\boldsymbol{\sigma}(X)$, будут представлять номера расположений моделей ошибки $\boldsymbol{e}(X)$. Воспользуемся авторегрессионной техникой моделирования [4]. Составим из синдромов матрицу, в которой первые t синдромов будут использоваться для предсказания следующего синдрома:

$$\begin{bmatrix} S_1 & S_2 & S_3 & \ldots & S_{t-1} & S_t \\ S_2 & S_3 & S_4 & \ldots & S_t & S_{t+1} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\ \ldots \\ S_{t-1} & S_t & S_{t+1} & \ldots & S_{2t-3} & S_{2t-2} \\ S_t & S_{t+1} & S_{t+2} & & S_{2t-2} & S_{2t-1} \end{bmatrix} \times$$

$$\times \begin{bmatrix} \sigma_t \\ \sigma_{t-1} \\ \ldots \\ \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} -S_{t+1} \\ -S_{t+2} \\ \ldots \\ -S_{2t-1} \\ -S_{2t} \end{bmatrix}. \quad (15)$$

Мы воспользовались авторегрессионной моделью уравнения (15), взяв матрицу наибольшей размерности с ненулевым определителем. Для кода (7, 3) с коррекцией двухсимвольных ошибок матрица будет иметь размерность 2×2, тогда модель запишется следующим образом:

$$\begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} \cdot \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} S_3 \\ S_4 \end{bmatrix}, \qquad (16)$$

$$\begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^5 & \alpha^6 \end{bmatrix} \cdot \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \alpha^6 \\ 0 \end{bmatrix}. \qquad (17)$$

Для нахождения коэффициентов σ_1 и σ_2 многочлена локатора ошибок $\boldsymbol{\sigma}(X)$, решим уравнение (17) в матричном виде $AX = B$, где

$$A = \begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^5 & \alpha^6 \end{bmatrix}, \; X = \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix}, \; B = \begin{bmatrix} \alpha^6 \\ 0 \end{bmatrix}.$$

Найдем $X = A^{-1}B$, где

$$\det A = \det \begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^5 & \alpha^6 \end{bmatrix} =$$

$$= \alpha^3\alpha^6 - \alpha^5\alpha^5 = \alpha^9 + \alpha^{10} = \alpha^2 + \alpha^3 = \alpha^5.$$

$$A^{-1} = \frac{1}{\det\ [A]} \begin{bmatrix} A_{11} & A_{21} \\ A_{12} & A_{22} \end{bmatrix} \quad \alpha^{-5} \cdot \begin{bmatrix} \alpha^6 & \alpha^5 \\ \alpha^5 & \alpha^3 \end{bmatrix} =$$

$$\alpha^2 \cdot \begin{bmatrix} \alpha^6 & \alpha^5 \\ \alpha^5 & \alpha^3 \end{bmatrix} = \begin{bmatrix} \alpha^8 & \alpha^7 \\ \alpha^7 & \alpha^5 \end{bmatrix} = \begin{bmatrix} \alpha^1 & \alpha^0 \\ \alpha^0 & \alpha^5 \end{bmatrix}.$$

Поиск положений ошибок начнем с вычисления коэффициентов многочлена локатора ошибок $\boldsymbol{\sigma}(X)$

$$\begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \alpha^1 & \alpha^0 \\ \alpha^0 & \alpha^5 \end{bmatrix} \cdot \begin{bmatrix} \alpha^6 \\ 0 \end{bmatrix} = \begin{bmatrix} \alpha^7 \\ \alpha^6 \end{bmatrix} = \begin{bmatrix} \alpha^0 \\ \alpha^6 \end{bmatrix}. \qquad (18)$$

Из уравнений (14) и (18) следует

$$\boldsymbol{\sigma}(X) = \alpha^0 + \sigma_1 X + \sigma_2 X^2 = \alpha^0 + \alpha^6 X + \alpha^0 X^2. \qquad (19)$$

Корни $\boldsymbol{\sigma}(X)$ являются обратными числами к положениям ошибок. После того как эти корни найдены, мы узнаем расположение ошибок. Вообще, корни $\boldsymbol{\sigma}(X)$ могут быть одним или несколькими элементами поля. Определим эти корни путем полной проверки многочлена $\boldsymbol{\sigma}(X)$ со всеми элементами поля. Любой элемент X, который дает $\boldsymbol{\sigma}(X) = \mathbf{0}$, является корнем, что позволяет определить расположение ошибки.

$$\boldsymbol{\sigma}(\alpha^0) = \alpha^0 + \alpha^6 + \alpha^0 = \alpha^6 \neq \mathbf{0}$$

$$\boldsymbol{\sigma}(\alpha^1) = \alpha^2 + \alpha^7 + \alpha^0 = \alpha^2 \neq \mathbf{0}$$

$$\boldsymbol{\sigma}(\alpha^2) = \alpha^4 + \alpha^8 + \alpha^0 = \alpha^6 \neq \mathbf{0}$$

$$\boldsymbol{\sigma}(\alpha^3) = \alpha^6 + \alpha^9 + \alpha^0 = \mathbf{0} \Rightarrow \text{ОШИБКА}$$

$$\boldsymbol{\sigma}(\alpha^4) = \alpha^8 + \alpha^{10} + \alpha^0 = \mathbf{0} \Rightarrow \text{ОШИБКА}$$

$$\boldsymbol{\sigma}(\alpha^5) = \alpha^{10} + \alpha^{11} + \alpha^0 = \alpha^2 \neq \mathbf{0}$$

$$\boldsymbol{\sigma}(\alpha^6) = \alpha^{12} + \alpha^{12} + \alpha^0 = \alpha^0 \neq \mathbf{0}$$

Из уравнения (14) видно, что расположение ошибок является обратной величиной к корням многочлена. Значит, $\boldsymbol{\sigma}(\alpha^3) = \mathbf{0}$ означает, что один корень получается при $\frac{1}{\beta_{l'}} = \alpha^3$. Отсюда следует $\beta_{l'} = \frac{1}{\alpha^3} = \alpha^4$. Аналогично $\boldsymbol{\sigma}(\alpha^4) = \mathbf{0}$ означает, что другой корень появляется при $\frac{1}{\beta_{l''}} = \frac{1}{\alpha^4} = \alpha^3$, где l' и l'' обозначают 1-ю и 2-ю ошибки. Так как мы имеем дело с 2-символьными ошибками, многочлен ошибок можно записать следующим образом:

$$\boldsymbol{e}(X) = e_{j_1} X^{j_1} + e_{j_2} X^{j_2}. \qquad (20)$$

Мы нашли две ошибки на позициях α^3 и α^4. Отметим, что индексация номеров расположения ошибок является произвольной. В этом примере мы обозначили величины, $\beta_l = \alpha^{j_l}$ как $\beta_1 = \alpha^{j_1} = \alpha^3$ и $\beta_2 = \alpha^{j_2} = \alpha^4$.

Значения ошибок. Мы обозначили ошибки через e_{j_l}, где индекс j обозначает расположение ошибки, а индекс l – l-ю ошибку. Так как каждое значение ошибки связано с конкретным месторасположением, упростим систему обозначений, обозначив e_{j_l} просто как e_l. Для нахождения значений ошибок e_1 и e_2, связанных с позициями $\beta_1 = \alpha^3$ и $\beta_2 = \alpha^4$, используем любое из четырех синдромных уравнений. Запишем S_1, и S_2 из уравнения (13).

$$\begin{aligned} S_1 &= \boldsymbol{r}(\alpha) \quad = e_1\beta_1 + e_2\beta_2 \\ S_2 &= \boldsymbol{r}(\alpha^2) = e_1\beta_1^2 + e_2\beta_2^2 \end{aligned}. \qquad (21)$$

В матричной форме уравнение (21) выглядит следующим образом:

$$\begin{bmatrix} \beta_1 & \beta_2 \\ \beta_1^2 & \beta_2^2 \end{bmatrix} \cdot \begin{bmatrix} e_1 \\ e_2 \end{bmatrix} = \begin{bmatrix} S_1 \\ S_2 \end{bmatrix}, \quad (22)$$

$$\begin{bmatrix} \alpha^3 & \alpha^4 \\ \alpha^6 & \alpha^8 \end{bmatrix} \cdot \begin{bmatrix} e_1 \\ e_2 \end{bmatrix} = \begin{bmatrix} \alpha^3 \\ \alpha^5 \end{bmatrix}. \quad (23)$$

Решая уравнение (23) в матричном виде, находим значения ошибок e_1 и e_2

$$\begin{bmatrix} e_1 \\ e_2 \end{bmatrix} = \begin{bmatrix} \alpha^2 & \alpha^5 \\ \alpha^0 & \alpha^4 \end{bmatrix} \cdot \begin{bmatrix} \alpha^3 \\ \alpha^5 \end{bmatrix} = \begin{bmatrix} \alpha^5 + \alpha^{10} \\ \alpha^3 + \alpha^9 \end{bmatrix} =$$

$$= \begin{bmatrix} \alpha^5 + \alpha^3 \\ \alpha^3 + \alpha^2 \end{bmatrix} = \begin{bmatrix} \alpha^2 \\ \alpha^5 \end{bmatrix}. \quad (24)$$

Исправление принятого многочлена с помощью найденного многочлена ошибок. Из уравнений (20) и (24) мы находим многочлен ошибок.

$$\hat{\boldsymbol{e}}(X) = e_{j_1} X^{j_1} + e_{j_2} X^{j_2} = \alpha^2 X^3 + \alpha^5 X^4. \quad (25)$$

Данный алгоритм восстанавливает принятый многочлен, выдавая в итоге предполагаемое переданное кодовое слово и, в конечном счете, декодированное сообщение.

$$\hat{\boldsymbol{U}}(X) = \boldsymbol{r}(X) + \hat{\boldsymbol{e}}(X) = \boldsymbol{U}(X) + \boldsymbol{e}(X) + \hat{\boldsymbol{e}}(X); \quad (26)$$

$$\boldsymbol{r}(X) = (100) + (001)X + (011)X^2 +$$

$$+(100)X^3 + (101)X^4 + (110)X^5 + (111)X^6;$$

$$\hat{\boldsymbol{e}}(X) = (000) + (000)X + (000)X^2 + (001)X^3 +$$

$$+(111)X^4 + (000)X^5 + (000)X^6;$$

$$\hat{\boldsymbol{U}}(X) = (100) + (001)X + (011)X^2 + (101)X^3 +$$

$$+(010)X^4 + (110)X^5 + (111)X^6. \quad (27)$$

Так как символы сообщения содержатся в крайних правых $k = 3$ символах, декодированным будет следующее сообщение [5]:

$$\underbrace{010}_{\alpha^1} \quad \underbrace{110}_{\alpha^3} \quad \underbrace{111}_{\alpha^5}.$$

ЛИТЕРАТУРА

1. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: Пер. с англ. Издательский дом «Вильямс», 2004. 1104 с. ил.

2. *Ташатов Н.Н.* Систематическое кодирование кодов Рида–Соломона с помощью (n – k)-разрядного регистра сдвига // Materialy III miedzynarodowej naukowi-praktycznej konferencji «Wiadomosci naukowej mysli – 2007», 1-15 listopada 2007 roku, tym 11, Przemysl, Nauka i studia. S. 53-57.

3. *Ташатов Н.Н.* Систематические линейные блочные коды с контролем четности // Вестник ПГУ им. С. М. Торайгырова. 2007. № 1. С. 123-135

4. *Blahut R.E.* Theory and Practice of Error Control Codes. Addison – Wesley Publishing Co., Reading, Massachusetts, 1983.

5. Reed–Solomon Codes and Their Applications, ed. Wicker S. B. and Bhargava V. K. IEEE Press, Piscataway, New Jersey, 1983.

Резюме

Тестік хабарларды, синдромды есептеуді, қате локализациясы мен сенімділіке тексеруді, қате мәнін анықтауды жүйелі түрде қалай кодтауға болатындығы және табылған қателер көпмүшелігінің көмегімен қабылданған көпмүшені түзету мәселесі қарастырылған.

Summary

The article include possibilities of coding the test message in systematic form, calculation of a syndrome, localization of a mistake and check of reliability, values of mistakes and correction of the accepted polynom with founding polynom of mistakes.

Евразийский национальный университет им. Л. Н. Гумилева, г. Астана

Поступила 20.01.08г.