К. т. н. И. В. ИВАНОВА

Россия, г. С.-Петербург, Северо-Западный гос. заочный технический университет
E-mail: rilala_spb@mail.ru

Дата поступления в редакцию
20.05—23.06 2005 г.
Оппонент *к. т. н. И. А. КИРЕЕВ*
(ОНАС, г. Одесса)

АНАЛИЗ МЕТОДОВ СИНДРОМНОГО ДЕКОДИРОВАНИЯ КОДОВ РИДА–СОЛОМОНА

Сделан вывод о необходимости разработки безрекуррентных процедур декодирования, что возможно с использованием ганкелевых (теплицевых) матриц при вычислении синдромов ошибок.

Как было отмечено в [1], обеспечение достаточной помехоустойчивости в технике передачи информации затруднено сложностью практической реализации устройств декодирования.

Настоящая работа посвящена поиску оптимального способа декодирования кодов Рида–Соломона, представляющих наибольший практический интерес.

Код Рида–Соломона (РС) является циклическим кодом и, следовательно, может быть задан с помощью порождающей или проверочной матриц.

По определению, полином $g(z)$ и матрица $\boldsymbol{H}$ для РС-кода над полем $GF(q=p^r)$ имеют соответственно вид:

$$g(z)=\prod_{i=\nu}^{i=m+\nu-1}\left(z-\alpha^i\right),\quad m=n-k,\quad n=q-1; \tag{1}$$

$$\boldsymbol{H}=\begin{vmatrix} \alpha^{\nu(n-1)} & \alpha^{\nu(n-2)} & \dots & 1\\ \alpha^{(\nu+1)(n-1)} & \alpha^{(\nu+1)(n-2)} & \dots & 1\\ & & \dots & \\ \alpha^{(m+\nu-1)(n-1)} & \alpha^{(m+\nu-1)(n-2)} & \dots & 1 \end{vmatrix}=\left[\alpha^{ij}\right], \tag{2}$$

где α — примитивный элемент поля $GF(q)$;
$d=(m+1)$ — минимальное кодовое расстояние;
n — длина кода;
k — число информационных символов;
m — число проверочных символов (m — четно);
$\nu=0$ или $\nu=1$.

Если поле $GF(q)$ имеет характеристику 2, т. е. $q=2^r$, то знак минус в скобках выражения (1) заменяется на плюс:

$$g(z)=(z+\alpha^\nu)(z+\alpha^{\nu+1})\dots(z+\alpha^{m+\nu-1}),\ GF(2^r).$$

Минимальное кодовое расстояние РС-кода определяется точным равенством $d=n-k+1$, т. е. он является максимально разделимым (МДР) кодом и способен исправлять до $V_{\max}=0{,}5m$ ошибок.

Полином $U(z)$ и, следовательно, кодовое слово $U=(u_{n-1}, u_{n-2},\dots,u_1, u_0)$ РС-кода в несистематической форме находится из соотношения $U(z)=Q(z)\,g(z)$, где $Q(z)$ — информационный полином. Для того чтобы получить кодовое слово $U(z)$ в систематической форме, достаточно найти остаток $R(z)$ от деления полинома $Q(z)$ на $g(z)$ и принять

$$U(z)=Q(z)z^m-R(z). \tag{3}$$

Любое неискаженное кодовое слово U удовлетворяет соотношению $UH^t=0$. Произведение $U_\varepsilon H^t=S$ определяет синдром, причем вектор U_ε, возможно, содержит ошибки. При использовании матрицы $\boldsymbol{H}$ в форме (2), т. е. для РС-кода, синдром S является вектором-изображением усеченного преобразования Фурье–Мэттсона–Соломона для вектора-оригинала U. Компоненты синдрома задаются выражением

$$S_j=\sum_{i=0}^{i=n-1}u_i\alpha^{ij},\quad n=q-1. \tag{4}$$

Часто практически удобнее компоненты S_j вычислять по следующей рекурсивной формуле, называемой схемой Горнера:

$$S_j=u_0+\alpha^j\left(u_1+\alpha^j\left(u_2+\dots+\alpha^j\left(u_{n-2}+\alpha^j u_{n-1}\right)\dots\right)\right), \tag{5}$$

где $j=1, 2, \dots, m$.

Можно убедиться, что для не искаженного помехами вектора U все компоненты синдрома S равны нулю.

Классический синдромный метод декодирования во временной области для (n, k)-РС-кода с кодовым расстоянием d состоит из следующих укрупненных этапов:

1. Вычисление синдрома S.
2. Вычисление вектора ошибок; в классическом варианте декодирования этап разбивается на два:
2а. Определение местоположений ошибок l;
2б. Нахождение величин ошибок ε_l.
3. Коррекция кодового вектора.

Охарактеризуем вкратце каждый из этапов.

1. Компоненты синдрома $S=(S_\nu, S_{\nu+1},\dots, S_{m+\nu-1})$, где $\nu\in\{0,1\}$, находятся по формулам (4) или (5). Если все $S_j=0$, $j=\nu, \nu+1, \dots, m+\nu-1$, то считаем, что ошибок нет. В противном случае, если $S_j\neq0$ хоть для одного j, то устанавливаем факт искажения кодового вектора; для его коррекции необходимо найти вектор ошибок, т. е. их местоположение и величину.

2а. Задача определения местоположений ошибок является наиболее трудной, и, как будет видно из дальнейшего, она может быть сведена к решению системы ганкелевых (теплицевых) уравнений, а затем к одному — так называемому уравнению локаторов. Если степень этого уравнения не превышает $0{,}5m$, а

его решение над полем Галуа существует, причем все корни различны, то позиции ошибок равны обратным значениям корней. При небольшом числе ошибок и, следовательно, невысоком порядке уравнения над полем Галуа его решение может быть найдено, например, табличным методом. В общем случае прибегают к упорядоченному перебору всех возможных значений для его корней; подобный перебор именуется процедурой Ченя [2, 3]. (Автором создан метод декодирования, основанный на вычислении особых продолжений ганкелевых (теплицевых) матриц и вообще не требующий решения указанного уравнения локаторов.)

2б. После того как расположение ошибок установлено, т. е. они перешли в разряд стираний, возникает задача вычисления их величины ε_i. Данная задача сводится по существу к решению системы линейных уравнений над полем Галуа относительно ε_i. Такая система может быть решена любым стандартным методом, например методами Крамера, Гаусса, обращения матриц. Однако в процедуре декодирования кодов над полями Галуа для вычисления величин ошибок удобнее использовать особые продолжения ганкелевых матриц либо применить формулу Форни [4]

$$\varepsilon_i = -\frac{\bar{\omega}\left(\alpha^{-i}\right)}{\sigma'_z\left(\alpha^{-i}\right)}, \qquad (6)$$

где i — позиция ошибки;
$\sigma'_z(z)$ — формальная производная полинома $\sigma(z)$ по z;
$\sigma'_z(\alpha^{-i})$ и $\omega(\alpha^{-i})$ — значения полиномов $\sigma(z)$ и $\omega(z)$ в точке $z=\alpha^{-i}$, обратной корню α^i полинома $\sigma(z)$.

Формальная производная для полинома

$$f(z) = \sum_{i=0}^{i=n} a_i z^i = a_0 + a_1 z + a_2 z^2 + \ldots + a_n z^n \qquad (7)$$

(где коэффициенты a_i — какие-либо числовые параметры выбранного поля) над полем Галуа определяется соотношением

$$f'_z(z) = \sum_{i=1}^{i=n} \left((i)\right) \times \left(a_i z^{i-1}\right) = \left((1)\right) \times a_i + \left((2)\right) \times \left(a_2 z\right) + \ldots$$

$$+ \left((n)\right) \times \left(a_n z^{n-1}\right), \qquad (8)$$

где $((i))=1+1+\ldots+1$ (i штук, складываемых по правилам данного поля); значком "×" обозначена операция "просуммировать" столько-то раз (эта операция не совпадает с операцией умножения над конечным полем).

В данном случае имеем для $GF(2^r)$:

$$\left.\begin{array}{ll} \text{если} & \sigma(z) = \sum_{i=0}^{i=n} a_i z^i = a_0 + a_1 z + a_2 z^2 + \ldots + a_n z^n, \\ \text{то} & \sigma'_z(z) = \sum_{i=0}^{i=\Psi} a_{2i+1} z^{2i} = a_1 + a_3 z^2 + \ldots + a_{2\Psi} z^{2\Psi} \end{array}\right\}, \qquad (9)$$

где $\psi=\text{int } 0{,}5(n-1)$.

3. Таким образом, на втором этапе находится вектор ошибок $E=(\varepsilon_{n-1}, \varepsilon_{n-2}, \ldots, \varepsilon_0)$. Коррекция искаженного кодового вектора U_ε по вектору ошибок E тривиальна — кодовое слово U восстанавливается путем покомпонентного суммирования: $U=U_\varepsilon+E$.

Вернемся еще раз к первому этапу. На этом этапе декодирования вычисляются компоненты синдрома S. Однако при этом не известны не только позиции l и величины e_l ошибок, но даже и их число V. Для нахождения перечисленных величин необходимо решить систему из m нелинейных уравнений

$$\sum_{i\in r} \varepsilon_{l_i} \alpha^{jl_i} = S_j, \; j = \nu, \nu+1, \ldots, m+\nu-1, \; r=\{1, 2, \ldots, x\},$$

$\nu \in \{0, 1\}$,

которая может быть приведена к ганкелевой (теплицевой) системе линейных уравнений.

При декодировании кодов над конечными полями наибольшее распространение получили следующие методы решения ганкелевой (теплицевой) системы уравнений:

1) Прямой, или определительный, метод, называемый также методом Питерсона–Горенштейна–Цирлера [2, 3, 5];

2) Итеративный метод Тренча–Берлекэмпа–Месси (ТБМ-метод), получивший наибольшее применение на практике [6, 7];

3) Метод Сугиямы, основанный на алгоритме Евклида и пригодный для декодирования не только кодов Боуза–Чоудхури–Хоквингема и РС-кодов, но и ряда других альтернативных кодов [8].

Суть первого метода состоит в вычислении ряда угловых квадратных определителей для матрицы и нахождении ее ранга. Затем система уравнений решается каким-либо трафаретным способом — Крамера, Гаусса, обращением матриц и др. К сожалению, прямой метод практически целесообразен лишь при невысоком порядке матрицы, т. е. при декодировании кодов, способных исправлять небольшое число (до 6—8) ошибок.

Два других метода, по существу, позволяют по известному полиному синдромов $S(z)$ решить относительно полиномов $\sigma(z)$ и $\omega(z)$ уравнение Падэ над полем Галуа:

$$S(z)\sigma(z)=\omega(z), \bmod z^m. \qquad (10)$$

После вычисления корней полинома $\sigma(z)$, а следовательно, и определения локаторов $X_i=\alpha^{li}$ ошибок, их величина ε_i может быть рассчитана по формуле Форни (6).

В принципе в полном решении уравнения (10) нет необходимости, т. к. достаточно найти полином локаторов $\sigma(z)$, а по нему — продолжение вектора синдромов.

Как уже отмечалось, в принятом кодовом слове могут содержаться искажения двух типов — стирания, местоположение которых известно, и ошибки, местоположение которых незвестно. В этом случае удобно различать многочлен $\sigma(z)$ локаторов ошибок, определяемый как и раньше, и многочлен $\Gamma(z)$ локаторов стираний, задаваемый следующим равенством:

$$\Gamma(z) = \prod_{i=1}^{i=\tau} \left(1 - z\alpha^{l_i}\right) = \prod_{i=1}^{i=\tau} \left(1 - zZ_i\right),$$

где τ — число стираний;
l_i — позиция i-го стирания;
$Z_i=\alpha^{li}$ — локатор стирания.

Тогда ключевое уравнение Падэ примет вид

$$S(z)\Phi(z)=\omega(z), \bmod z^m, \qquad (11)$$

где $\Phi(z)=\Gamma(z)\sigma(z)$.

Уравнение (11) можно решить теми же методами, что и уравнение (10), если ввести обобщенный полином синдрома Форни $T(z)=S(z)\Gamma(z)$ по модулю z^m [3, 4]. Полином локаторов ошибок можно найти разделив $\Phi(z)$ на $\Gamma(z)$. В вычислении этого полинома также нет необходимости. Используя «частотный подход», достаточно найти продолжение вектора синдромов S по рекуррентной формуле типа (12) с естественной заменой $\sigma(z)$ на $\Phi(z)$:

$$\sum_{k=0}^{k=n} a_{j-k}\sigma_k = a_j\sigma_0 + a_{j-1}\sigma_1 + \ldots + a_{j-n}\sigma_n\,, \qquad (12)$$

где $j>2n$ — "продолжение вниз", $j<n+1$ — "продолжение вверх".

Соотношение (12) справедливо и при $n+1\le j\le 2n$, но в этом случае оно связывает только известные коэффициенты $a_1, a_2, \ldots, a_{2n}$.

***

Анализ методов синдромного декодирования кодов Рида–Соломона позволил сделать вывод о необходимости разработки безрекуррентных процедур декодирования, что и стало возможным с использованием ганкелевых (теплицевых) матриц при вычислении синдромов ошибок.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Иванова И. В. Классификация и синтез полиномиальных кодеков в системах автоматизированной обработки данных // Технология и конструирование в электронной аппаратуре.— 2005.— № 4.— С. 19—23.

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

3. Галлагер Р. Теория информации и надежная связь.— М.: Сов. радио, 1974.

4. Форни Д. Каскадные коды.— М.: Мир, 1970.

5. Coppersmith D. Fast evaluation of logarithms in fields of characteristic two // IEEE Transaction on Information Theory.— 1984.— Vol. IT-30, N 4.— P. 583—587.

6. Берлекэмп Э. Алгебраическая теория кодирования.— М.: Мир, 1971.

7. Trench W. F. An algorithm for the inversion of finite Toeplitz matrices // Journal of the Society for Industrial and Applied Mathematics.— 1964.— N 12.— P. 515—522.

8. Suqiyama Y., Kasahara M., Hirasawa S. A method for solving key equation for decoding Goppa codes // Information and Control.— 1975.— N 27.— P. 87—99.

НОВЫЕ КНИГИ

НОВЫЕ КНИГИ

Загидуллин Р. Ш., Карутин С. Н., Стешенко В. Б. SystemView. Системотехническое моделирование устройств обработки сигналов.— М.: Горячая линия–Телеком, 2005.— 294 с., ил.

Изложены основы инженерных методов синтеза и расчета основных классов радиотехнических устройств с использованием пакета программ SystemView компании Elanix, который обеспечивает возможность всестороннего анализа свойств систем, включая алгоритмы аналоговой или цифровой обработки сигналов, синтеза фильтров, анализа и синтеза систем управления и систем связи, моделирования динамических систем на уровне функциональных блоков. Книга содержит необходимый теоретический материал и значительное количество практических примеров. Особенностью книги является то, что изложение ведется не от описания возможностей пакета, а от постановки конкретной радиотехнической задачи.

Для специалистов; может быть полезна студентам радиотехнических специальностей.

НОВЫЕ КНИГИ

Слепов Н. Англо-русский толковый словарь сокращений в области связи, компьютерных и информационных технологий.— М.: Радио и связь, 2005.— 800 с.

Это уникальное издание несомненно вызовет живейший интерес всех, кто работает с современной оригинальной английской технической литературой в области связи и новых информационных технологий, т. к. является самым полным (35 тысяч сокращений) и наиболее современным из словарей подобного рода. Словник словаря формируется уже 15 лет, а данное издание является третьим (первое вышло в 1996 г. — 19000 терминов, второе — в 1999 г. — 26000), и оно кардинально отличается тем, что является англо-русским, а не англо-английским, как два предыдущих.

Словарь можно использовать не только для перевода сокращений, но и как терминологический справочник или как англо-русский словарь для перевода составных терминов. Кроме того, он содержит большой словарь русскоязычных сокращений (около 5100) по той же тематике.

Заказать словарь можно по почте: **125319, Москва, а/я 594**, по тел./факсу: **(095) 956-3346, 234-0110**.

E-mail: **knigi@technosphera.ru; sales@technosphera.ru**