А. Ю. Серебряков

ДЕКОДИРОВАНИЕ КОДОВ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ ПРИ ЧИСЛЕ ОШИБОК, БОЛЬШЕМ ПОЛОВИНЫ КОНСТРУКТИВНОГО КОДОВОГО РАССТОЯНИЯ[1]

Рассматривается задача декодирования алгебро-геометрических кодов на эллиптических кривых, причем считается, что число ошибок может превышать половину конструктивного кодового расстояния (в частности, оно может превышать и половину минимального расстояния). Задача сводится к поиску нулей многочленов многих переменных. Построен синдромный вероятностный алгоритм декодирования глубины t.

§1. Введение

В работе Сидельникова [1] построен алгоритм декодирования кодов Рида—Соломона для случая, когда число ошибок превышает половину кодового расстояния. В настоящей работе предлагаются подобные алгоритмы для декодирования алгебро-геометрических кодов на кривых рода 1, т. е. на эллиптических кривых (коды Рида—Соломона — это коды на кривой рода 0). При числе ошибок $t > [(d^* - 1)/2]$, где d^* — конструктивное кодовое расстояние, задача декодирования связывается с задачей поиска нулей идеала, порожденного двумя многочленами r переменных $O_{t+1}^{(0)}(Z_1, \dots, Z_r)$, $O_{t+1}^{(1)}(Z_1, \dots, Z_r)$, $Z_i \in X$ (X — заданная эллиптическая кривая), $r = 2t - d^* + 2$. Известно [2, 3], что задача декодирования эквивалентна поиску нулей многочленов многих переменных. В известных алгоритмах с применением базисов Гребнера число переменных равно длине кода или числу ошибок t, причем такие алгоритмы строятся для случая, когда t не превышает половины минимального кодового расстояния. В настоящей работе при $t > [(d^* - 1)/2]$ мы пользуемся отображением проектирования из $X^t = X \times \ldots \times X$ (t раз) в $X^r = X \times \ldots \times X$ (r раз), где $r = 2t - d^* + 2$, что позволяет уменьшить число переменных до r, а число уравнений до двух.

§2. Основные определения

Пусть $\mathbb{F}_q$ — поле из q элементов, а X — кривая рода 1 (эллиптическая кривая) в проективном пространстве $\mathbb{P}^2(\mathbb{F}_q)$, O — ее "бесконечно удаленная" точка [4]. Функциями на кривой X у нас будут рациональные функции (как правило, многочлены). Для заданного дивизора D кривой X через $L(D)$ мы будем обозначать (конечномерное) пространство функций, имеющих дивизор нулей и полюсов, не меньший $-D$, через $l(D)$ — размерность пространства $L(D)$.

Пусть $s \geqslant 1$, $D = sO$ — дивизор. Тогда $L(D) = L(sO)$ — пространство функций на X, у которых порядок полюса в точке O не превосходит s, а других полюсов нет. По теореме Римана—Роха $l(D) = \dim L(D) = s$ [4]. Пусть $f_1, \dots, f_s$ — базис $L(D)$, $\Omega = \{P_1, \dots, P_N\}$ — множество из N точек кривой X, $O \notin \Omega$, и $N > s$. Тогда алгебро-геометрический код C, связанный с тройкой (X, Ω, D), задается проверочной матрицей размера $s \times N$:

$$H = (f_i(P_j)), \qquad i = 1, \dots, s, \qquad j = 1, \dots, N.$$

Иначе говоря, вектор $\mathbf{c} = (c_1, \dots, c_N)$ принадлежит коду C тогда и только тогда, когда $H\mathbf{c}^T = 0$. (Определение основных понятий теории кодирования содержится в [5], а определение алгебро-геометрических кодов в [6, 7].)

Известно [6], что минимальное кодовое расстояние кода C удовлетворяет неравенству

$$d_{\min}(C) \geqslant d^*(C) = s,$$

где $d^*(C)$ — конструктивное кодовое расстояние. Размерность кода C равна

$$\dim C = N - s + l(D - \sum_{i=1}^{N} P_i) = N - s,$$

[1] Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 96-01-00931).

поскольку каждая линейная зависимость между строками матрицы H дает элемент из $L(D-\sum\limits_{i=1}^{N} P_i) = \{0\}$.

Задача декодирования состоит в том, чтобы по принятому вектору $\mathbf{r} = \mathbf{c}+\mathbf{e}$, где $\mathbf{c} \in C$ — кодовый вектор, а $\mathbf{e} = (e_1, \dots, e_N)$ — вектор ошибок веса t, восстановить исходный вектор $\mathbf{c}$ (или найти $\mathbf{e}$).

Если компоненты $e_{i_1} \neq 0, \dots, e_{i_t} \neq 0$, то точки $E_1 = P_{i_1}, \dots, E_t = P_{i_t}$ называются локаторами ошибок (или позициями ошибок). Конструктивное кодовое расстояние кода C равно $d^* = s$, поэтому при числе ошибок $t \leqslant [(s-1)/2]$ задача декодирования решается однозначно. При замене базиса $L(D)$ получается эквивалентный код, и в дальнейшем мы будем считать, что у нас задана последовательность функций $f_1, f_2, \dots, f_r, \dots$, где $f_1 = 1$ — базис $L(0O) = L(1O)$, $\{f_1, \dots, f_r\}$ — базис $L(rO)$, $r \geqslant 2$. Такую последовательность можно выбрать, поскольку

$$1 \in L(0O) = L(1O) \subset L(2O) \subset \ldots \subset L(rO) \subset L((r+1)O) \subset \ldots,$$

и $\dim L(rO) = r$ при $r \geqslant 1$, а $1 \in L(0O)$. В частности, если кривая X задана в $\mathbb{F}_q^2$ уравнением $y^2 = x^3 + ax + b$, то можно выбрать $f_{2i} = x^i$, $f_{2i+1} = x^{i-1}y$, $i \geqslant 1$ (если характеристика поля $\mathbb{F}_q$ отлична от 2 и от 3, то эллиптическая кривая изоморфна кривой, заданной таким уравнением).

Для вектора ошибок $\mathbf{e}$ определим синдромы

$$m_i = m_i(\mathbf{e}) = \sum_{j=1}^{N} e_j f_i(P_j) = \sum_{k=1}^{t} e_{i_k} f_i(E_k).$$

Из определения кода C следует, что для принятого вектора $\mathbf{r} = \mathbf{c} + \mathbf{e}$ при $i \leqslant s$

$$m_i = \sum_{j=1}^{N} r_j f_i(P_j) = m_i(\mathbf{r}) = m_i(\mathbf{e}).$$

Мы будем искать вектор ошибок $\mathbf{e}$ по соответствующим *известным* синдромам $m_1, \dots, m_s$, поэтому проблема декодирования сводится к решению системы уравнений

$$\sum_{j=1}^{t} x_j f_i(z_j) = m_i, \qquad i = 1, \dots, s, \tag{1}$$

где неизвестные $x_j \in \mathbb{F}_q$, $z_j \in \Omega \subset X$. Определим также синдромы

$$S_{i,j} = S_{i,j}(\mathbf{e}) = \sum_{l=1}^{N} e_l f_i(P_l) f_j(P_l) = \sum_{k=1}^{t} e_{i_k} f_i(E_k) f_j(E_k).$$

Если $i + j \leqslant s$, то $f_i f_j \in L(sO)$, т. е. $f_i f_j = \sum\limits_{l=1}^{s} c_{ij}^l f_l$, и поэтому

$$S_{i,j} = \sum_{k=1}^{s} e_k \sum_{l=1}^{N} c_{ij}^k f_l(P_l) = \sum_{k=1}^{s} c_{ij}^k m_k,$$

и синдромы $S_{i,j}$ выражаются через известные синдромы m_k, $k = 1, \dots, s$. Отметим, что $S_{i,1} = S_{1,i} = m_i$, так как $f_1 = 1$.

§ 3. Нетрадиционный алгоритм декодирования при числе ошибок $t \leqslant [(d^* - 1)/2]$

Л е м м а 1. *Пусть* $Q_k \in X$, $S_{i,j} = \sum\limits_{k=1}^{t} h_k f_i(Q_k) f_j(Q_k)$, $h_k \neq 0$, $k = 1, \dots, t$, *и*

$$S(u) = \begin{pmatrix} S_{1,1} & \dots & S_{1,u} \\ \vdots & & \vdots \\ S_{u,1} & \dots & S_{u,u} \end{pmatrix}.$$

Тогда при $u \geqslant t+1$ имеем $\operatorname{rank} S(u) = t$.

Д о к а з а т е л ь с т в о. Пусть $\mathbf{e} = (e_1, \dots, e_N)$, $e_{i_k} = h_k \neq 0$ при $k = 1, \dots, t$, и вес Хэмминга вектора $\mathbf{e}$ есть $\operatorname{wt} \mathbf{e} = t$. Тогда

$$S(u) = H(u) E H^T(u),$$

где $H(u) = (f_i(P_j))$, $i = 1, \dots, u$, $j = 1, \dots, N$, $H^T(u)$ — транспонированная матрица $H(u)$, $E = diag(e_1, \dots, e_N)$ — диагональная матрица. Поэтому $\operatorname{rank} S(u) \leqslant \operatorname{rank} E = \operatorname{wt} \mathbf{e} = t$. Имеем, что $S(t+1) = H(t+1) E H^T(t+1)$. Любые t столбцов матрицы $H(t+1)$ линейно-независимы (кодовое расстояние кода $C(t+1)$, задаваемого проверочной матрицей $H(t+1)$ не меньше $t+1$). Отсюда следует, что $\operatorname{rank} S(t+1) = t$. При $u \geqslant t+1$ имеем $\operatorname{rank} S(u) \geqslant \operatorname{rank} S(t+1) = t$, т. е. $\operatorname{rank} S(u) = t$. $\triangleright$

Имеет место также следующая очевидная

Л е м м а 2. *Пусть $\beta_1, \dots, \beta_\nu$ — различные точки кривой X,*

$$S_{i,j} = \sum_{k=1}^{\nu} h_k f_i(\beta_k) f_j(\beta_k),$$

$m_i = \sum\limits_{k=1}^{\nu} h_k f_i(\beta_k)$. *Если полином $\mathcal{L} = \sum\limits_{i=1}^{v} c_i f_i$ имеет среди своих корней $\beta_1, \dots, \beta_\nu$, то $\sum\limits_{i=1}^{v} c_i S_{i,j} = 0$, $\sum\limits_{j=1}^{v} c_j S_{i,j} = 0$, и $\sum\limits_{i=1}^{v} c_i m_i = 0$.*

Рассмотрим многочлены

$$O^{(0)}_{t+1}(Z) = \begin{vmatrix} f_1(Z) & S_{1,1} & \dots & S_{1,t-1} & S_{1,t+1} \\ \vdots & \vdots & & \vdots & \vdots \\ f_{t+1}(Z) & S_{t+1,1} & \dots & S_{t+1,t-1} & S_{t+1,t+1} \end{vmatrix}$$

и

$$O^{(1)}_{t+1}(Z) = \begin{vmatrix} f_1(Z) & S_{1,1} & \dots & S_{1,t} \\ \vdots & \vdots & & \vdots \\ f_{t+1}(Z) & S_{t+1,1} & \dots & S_{t+1,t} \end{vmatrix},$$

где $Z = (x;y) \in X$, а $O^{(0)}_{t+1}(Z)$, $O^{(1)}_{t+1}(Z)$ — функции на X (при фиксированных значениях $m_1, \dots, m_{2t+2}$).

Т е о р е м а 1. *Если $S_{i,j} = \sum\limits_{k=1}^{t} h_k f_i(Q_k) f_j(Q_k)$, $h_k \neq 0$ при $k = 1, \dots, t$; $Q_1, \dots, Q_t$ — различные точки на $X \setminus \{O\}$, тогда:*

1. *По крайней мере один из многочленов $O^{(0)}_{t+1}(Z)$, $O^{(1)}_{t+1}(Z)$ является ненулевым. Если $Q_1 \oplus \dots \oplus Q_t = O$, то $O^{(0)}_{t+1}(Z) \neq 0$, $O^{(1)}_{t+1}(Z) = 0$ (знак $\oplus$ обозначает операцию сложения точек на эллиптической кривой X). Если $Q_1 \oplus \dots \oplus Q_t \neq O$, то $O^{(1)}_{t+1}(Z) \neq 0$, $O^{(0)}_{t+1}(Z) = CO^{(1)}_{t+1}(Z)$;*
2. *Если $O^{(1)}_{t+1}(Z)$ — ненулевой, то $O^{(1)}_{t+1}(Z) \in L((t+1)O) \setminus L(tO)$. Если $O^{(1)}_{t+1}(Z)$ — нулевой, то $O^{(0)}_{t+1}(Z) \in L(tO) \setminus L((t-1)O)$;*
3. *При $j = 1, \dots, t$ имеем $O^{(0)}_{t+1}(Q_j) = O^{(1)}_{t+1}(Q_j) = 0$.*

Д о к а з а т е л ь с т в о. Рассмотрим дивизор $F = (t+1)O - Q_1 - \dots - Q_t$. Его степень $\deg F = 1$, и по теореме Римана—Роха $l(F) = \dim L(F) = 1$, т. е. существует единственный с точностью до пропорциональности ненулевой многочлен

$$\mathcal{F} = \sum_{i=1}^{t+1} c_i f_i \in L(F).$$

Ясно, что $c_t \neq 0$ или $c_{t+1} \neq 0$, поскольку в противном случае $\mathcal{F} \in L((t-1)O - Q_1 - \dots - Q_t) = \{0\}$. При этом $c_{t+1} = 0$ тогда и только тогда, когда $L(tO - Q_1 - \dots - Q_t) \neq \{0\}$, т. е. когда

$Q_1 \oplus \ldots \oplus Q_t = O$ [7]. Имеем $\mathcal{F}(Q_j) = 0$, $j = 1, \ldots t$, следовательно, $\sum\limits_{j=1}^{t+1} c_j S_{i,j} = 0$ (лемма 2), и поэтому t-й или $(t+1)$-й столбец матрицы $S(t+1)$ является линейной комбинацией остальных. Обозначим через S' матрицу, получающуюся из матрицы S вычеркиванием t-го столбца при $c_t \neq 0$ или $(t+1)$-го столбца при $c_{t+1} \neq 0$. Тогда S' — матрица размера $(t+1) \times t$, и $\operatorname{rank} S' = \operatorname{rank} S = t$; значит, между строками матрицы S' есть единственная линейная зависимость. Но строки матрицы $S(t+1)$ (а поэтому и строки матрицы S') по лемме 2 связаны линейной зависимостью с коэффициентами c_i. Следовательно, один из многочленов $O_{t+1}^{(0)}$, $O_{t+1}^{(1)}$ равен $C\mathcal{F}$, где $C \in \mathbb{F}_q \setminus \{0\}$. ▷

Доказанная теорема позволяет построить алгоритм декодирования в том случае, когда число ошибок есть

$$t \leqslant \left[\frac{s-1}{2}\right] = \left[\frac{d^*-1}{2}\right].$$

Определить число ошибок, если априорно известно, что их число не превосходит $(s-2)/2$, можно с помощью леммы 1:

$$t = \operatorname{rank} S(m+1), \text{ где } m = \left[\frac{s-2}{2}\right].$$

Отметим также, что если $O_{t+1}^{(1)}(Z)$ — нулевой многочлен, а $O_{t+1}^{(0)}(Z)$ — ненулевой, то $O_{t+1}^{(0)}(Z)$ или пропорциональный ему ненулевой многочлен можно вычислить, зная только $m_1, \ldots, m_{2t+1}$ и не зная m_{2t+2} (и, соответственно, не зная $S_{t+1,t+1}$). Действительно, если многочлен

$$O_t^{(1)}(Z) = \begin{vmatrix} f_1(Z) & S_{1,1}\ldots & S_{1,t-1} \\ \vdots & \vdots & \vdots \\ f_t(Z) & S_{t,1}\ldots & S_{t,t-1} \end{vmatrix}$$

— ненулевой, то очевидно, что $O_{t+1}^{(0)}(Z) = CO_t^{(1)}(Z)$, а если $O_t^{(1)}(Z) = 0$, то многочлен $O_{t+1}^{(0)}(Z)$ не зависит от $S_{t+1,t+1}$.

Алгоритм

Шаг 1. Через известные синдромы находим коэффициенты многочлена $O_{t+1}^{(1)}(Z)$. Если он ненулевой, то полагаем $\mathcal{F}(Z) = O_{t+1}^{(1)}(Z)$. Если же $O_{t+1}^{(1)}(Z) = 0$, то находим по известным синдромам многочлен $O_{t+1}^{(0)}(Z)$ (или пропорциональный ему ненулевой многочлен) и полагаем $\mathcal{F}(Z) = O_{t+1}^{(0)}(Z)$.

Шаг 2. Находим корни $\mathcal{F}(Z)$ в Ω. Пусть это $Q_1, \ldots, Q_{t'}$, $t' \in \{t; t+1\}$.

Шаг 3. Решаем систему линейных уравнений

$$\sum_{j=1}^{t'} x_j f_i(Q_j) = m_i, \qquad i = 1, \ldots, t'+1.$$

Она имеет единственное решение $\mathbf{x} = (x_1^*, \ldots, x_{t'}^*)$, и ровно t элементов среди x_j^* отличны от нуля — это ненулевые координаты вектора ошибок, а соответствующие Q_j — позиции ошибок.

Система имеет решение, так как по теореме 1 множество $\{Q_1, \ldots, Q_{t'}\}$ содержит позиции ошибок, и решение единственно, поскольку ранг матрицы системы равен t'.

Оценим сложность алгоритма: $O(t^4)$ операций в поле $\mathbb{F}_q$ тратится на представление многочленов $O_{t+1}^{(0)}$, $O_{t+1}^{(1)}$ в виде суммы, $O(tN)$ операций — на вычисление корней ненулевого многочлена в Ω. Общая сложность равна $O(t^4+tN)$ операций в поле $\mathbb{F}_q$, что сопоставимо со сложностью традиционных алгоритмов декодирования.

При данном методе декодирования многочлен локаторов ошибок выражается в виде определителя через известные синдромы, и это соотношение можно обобщить на случай $t > (s-1)/2$.

§ 4. Декодирование при $t > [(d^*-1)/2]$

Мы построим *синдромный алгоритм декодирования заданной глубины* t [1], т. е. алгоритм, который по синдромам, определенным вектором ошибок $\mathbf{e}$ веса не более t, вычисляет некоторый соответствующий этим синдромам вектор ошибок $\mathbf{e}'$ веса также не более t. Синдромный алгоритм декодирования является алгоритмом нахождения какого-либо решения системы уравнений (1).

Л е м м а 3. *Пусть* $S_{i,j} = \sum\limits_{k=1}^{u} h_k f_i(\omega_k) f_j(\omega_k)$, $h_k \neq 0$, $k = r+1, \dots u$,

$$M_{n+1,r} = \begin{pmatrix} f_1(\omega_1) & \dots & f_1(\omega_r) & S_{1,1} & \dots & S_{1,u-r+1} \\ \vdots & & \vdots & \vdots & & \vdots \\ f_{n+1}(\omega_1) & \dots & f_{n+1}(\omega_r) & S_{n+1,1} & \dots & S_{n+1,u-r+1} \end{pmatrix}.$$

Тогда при $n \geqslant u$ *имеем* $\operatorname{rank} M_{n+1,r} = u$.

Д о к а з а т е л ь с т в о. Для $j = r+1, \dots, u+1$, $k = 1, \dots, r$ вычтем из j-го столбца матрицы $M_{n+1,r}$ ее k-й столбец, умноженный на $h_k f_j(\omega_k)$. В результате получим матрицу

$$M'_{n+1,r} = \begin{pmatrix} f_1(\omega_1) & \dots & f_1(\omega_r) & S'_{1,1} & \dots & S'_{1,u-r+1} \\ \vdots & & \vdots & \vdots & & \vdots \\ f_{n+1}(\omega_1) & \dots & f_{n+1}(\omega_r) & S'_{n+1,1} & \dots & S'_{n+1,u-r+1} \end{pmatrix},$$

где $S'_{i,j} = \sum\limits_{k=r+1}^{u} h_k f_i(\omega_k) f_j(\omega_k)$, и $\operatorname{rank} M'_{n+1,r} = \operatorname{rank} M_{n+1,r}$. Обозначим

$$S'(a,b) = (S'_{i,j}), \qquad i = 1, \dots, a, \qquad j = 1, \dots, b.$$

По лемме 1 имеем

$$\operatorname{rank} S'(n+1, u-r+1) \geqslant \operatorname{rank} S'(u-r+1, u-r+1) = u-r,$$

и

$$\operatorname{rank} S'(n+1, u-r+1) \leqslant \operatorname{rank} S'(n+1, n+1) = u-r.$$

Поэтому $\operatorname{rank} S'(n+1, u-r+1) = u-r$.

Если $\mathcal{F}_1 = \sum\limits_{i=1}^{n+1} c_i f_i \in L((n+1)O - \omega_{r+1} - \ldots - \omega_u)$, то по лемме 2 имеется линейная зависимость между строками матрицы $S'(n+1, u-r+1)$:

$$\sum_{i=1}^{n+1} c_i S'_{i,j} = 0, \qquad j = 1, \dots, u-r+1.$$

По теореме Римана—Роха $l((n+1)O - \omega_{r+1} - \ldots - \omega_u) = n-u+r+1$. Следовательно, линейное пространство линейных зависимостей между строками матрицы $S'(n+1, u-r+1)$, размерность которого равна $n+1-\operatorname{rank} S'(n+1, u-r+1) = n-u+r+1$, изоморфно $L((n+1)O - \omega_{r+1} - \ldots - \omega_u)$.

Пусть $\mathcal{F}_2 = \sum\limits_{i=1}^{n+1} c_i f_i$, и строки матрицы $M'_{n+1,r}$ — линейно-зависимы с коэффициентами c_i. Тогда $\mathcal{F}_2(\omega_i) = 0$, $i = 1, \dots r$, а, с другой стороны, строки матрицы $S'(n+1, u-r+2)$ — также линейно-зависимы с коэффициентами c_i, т. е. по вышедоказанному

$$\mathcal{F}_2 \in L((n+1)O - \omega_{r+1} - \ldots - \omega_u).$$

Поэтому $\mathcal{F}_2 \in L((n+1)O - \omega_1 - \ldots - \omega_u)$. Отсюда, учитывая утверждение леммы 2, получаем, что пространство линейных зависимостей между строками матрицы $M'_{n+1,r}$ изоморфно $L((n+1)O - \omega_1 - \ldots - \omega_u)$. Следовательно,

$$\operatorname{rank} M'_{n+1,r} = n+1 - l((n+1)O - \omega_1 - \ldots - \omega_u) = n+1-(n-u+1) = u. \triangleright$$

Рассмотрим многочлены

$$O^{(0)}_{u+1}(Z_1, \dots, Z_r) = \begin{vmatrix} f_1(Z_1) & \dots & f_1(Z_r) & S_{1,1} & \dots & S_{1,u-r} & S_{1,u-r+2} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots \\ f_{u+1}(Z_1) & \dots & f_{u+1}(Z_r) & S_{u+1,1} & \dots & S_{u+1,u-r} & S_{u+1,u-r+2} \end{vmatrix},$$

и

$$O^{(1)}_{u+1}(Z_1,\dots,Z_r)=\begin{vmatrix} f_1(Z_1) & \dots & f_1(Z_r) & S_{1,1} & \dots & S_{1,u-r+1}\\ \vdots & & \vdots & \vdots & & \vdots\\ f_{u+1}(Z_1) & \dots & f_{u+1}(Z_r) & S_{u+1,1} & \dots & S_{u+1,u-r+1}\end{vmatrix}.$$

Т е о р е м а 2. *Пусть $\beta_k\in X\setminus\{O\}$, $k=1,\dots,u$, $\beta_{k_1}\neq\beta_{k_2}$ при $k_1\neq k_2$; для $i,j\geqslant 1$ пусть $S_{i,j}=\sum\limits_{k=1}^{u}h_kf_i(\beta_k)f_j(\beta_k)$, $r\leqslant u$, $h_k\in\mathbb{F}_q\setminus\{0\}$, $k=r,\dots,u$; $\Omega'=\{\omega_1,\dots,\omega_{r-1}\}$ — $(r-1)$-элементное подмножество $X\setminus\{O\}$. Тогда*

1. *Каждый из многочленов $O^{(0)}_{u+1}(Z,\beta_1,\dots,\beta_{r-1})$, $O^{(1)}_{u+1}(Z,\beta_1,\dots,\beta_{r-1})$ обращается в нуль при $Z=\beta_1,\dots,\beta_u$, и по крайней мере один из них — ненулевой многочлен, корни которого образуют множество $\{\beta_1,\dots,\beta_{u'}\}$, $u'\in\{u;u+1\}$, а система уравнений*

$$\sum_{j=1}^{u'}x_jf_i(\beta_j)=m_i,\qquad i=1,\dots,2u-r+2, \tag{2}$$

имеет единственное решение $(h_1,\dots h_{u'})$; причем, если $u'=u+1$, то $h_{u'}=0$;

2. *Если $\mathcal{F}=O^{(l)}_{u+1}(Z,\omega_1,\dots,\omega_{r-1})$ — ненулевой многочлен ($l\in\{0;1\}$), $\mathcal{F}\in L((u+l)O)$, и множество корней $\mathcal{F}$ в $X\setminus\{O\}$ содержит подмножество из $u+l-r+1$ элементов $\Omega''=\{\omega_r,\dots,\omega_{u+l}\}$, $\Omega'\cap\Omega''=\varnothing$, а в случае $l=0$ $O^{(1)}_{u+1}$ — нулевой многочлен, то $\mathcal{F}$ имеет дивизор нулей и полюсов*

$$\operatorname{div}\mathcal{F}=\omega_1+\ldots+\omega_{u+l}-(u+l)O,$$

и найдутся такие элементы $h_j\in\mathbb{F}_q$, что $m_i=\sum\limits_{j=1}^{u+l}h_jf_i(\omega_j)$, $i=1,\dots 2u-r+2$, и не менее чем $u+l-1$ элементов среди $h_1,\dots,h_{u+l}$ отличны от нуля;

3. *Если $m_i=\sum\limits_{j=1}^{\nu}h_jf_i(\omega_j)$ и $\nu<u$, то $O^{(0)}_{u+1}(Z,\omega_1,\dots,\omega_{r-1})$, $O^{(1)}_{u+1}(Z,\omega_1,\dots,\omega_{r-1})$ — нулевые многочлены, и $\operatorname{rank}M_{u+1,r-1}=\nu$.*

Д о к а з а т е л ь с т в о. 1. Как следует из леммы 3 и ее доказательства, $\operatorname{rank}M_{u+1,r-1}=u$, и между строками $M^{(i)}_{u+1,r-1}$ матрицы $M_{u+1,r-1}$ есть единственная с точностью до пропорциональности линейная зависимость $\sum\limits_{i=1}^{u+1}c_iM^{(i)}_{u+1,r-1}=0$, которой соответствует ненулевой многочлен $R=\sum\limits_{i=1}^{u+1}c_if_i\in L((u+1)O-\omega_1-\ldots-\omega_u)$. Имеем $c_u\neq0$ или $c_{u+1}\neq0$. Если $c_{u+1}\neq0$, то, как и в теореме 1, получаем

$$O^{(1)}_{u+1}(Z,\omega_1,\dots,\omega_{r-1})=C_1R,\qquad C_1\neq0.$$

Если $c_{u+1}=0$, то $c_u\neq0$, и, аналогично,

$$O^{(0)}_{u+1}(Z,\omega_1,\dots,\omega_{r-1})=C_0R,\qquad C_0\neq0.$$

Система (2) по условию теоремы имеет решение, а его единственность следует из того, что ранг матрицы системы равен u'.

2. Имеем $\mathcal{F}=\sum\limits_{i=1}^{u+l}c_if_i$, и $c_{u+l}\neq0$. Строки матрицы

$$S(\nu,\mu)=(S_{i,j})\qquad i=1,\dots,\nu,\qquad j=1,\dots,\mu$$

(где при $l=0$ имеем $\nu=u$, $\mu=u-r+2$, а при $l=1$ имеем $\nu=u+1$, $\mu=u-r+1$) — линейно-зависимы с коэффициентами c_i:

$$\sum_{i=1}^{\nu}c_iS_{i,j}=0,\qquad j=1,\dots,\mu,\qquad c_\nu\neq0$$

(мы учли, что если $l=0$, то многочлен $O^{(1)}_{u+1}$ — нулевой). Следовательно,

$$S_{\nu,j}=\sum_{i<\nu}c'_iS_{i,j},\qquad j=1,\dots,\mu.$$

Так как $m_i = S_{i,1}$, то $\sum\limits_{i=1}^{\nu} c_i m_i = 0$. Поэтому система уравнений

$$\sum_{j=1}^{\nu} x_j f_i(\omega_j) = m_i, \qquad i = 1, \dots, \nu+1,$$

имеет единственное решение $(h_1, \dots, h_\nu)$.

Докажем, что $m_i = \sum\limits_{j=1}^{\nu} h_j f_i(\omega_j)$ при $\nu + 1 < i \leqslant \nu + \mu$.

При $i, j > 1$ по определению многочленов f_i имеем

$$f_i f_j = \lambda^{i,j} f_{i+j} + \sum_{k<i+j} \lambda_k^{i,j} f_k, \qquad \lambda^{i,j} \neq 0,$$

следовательно,

$$S_{i,j} = \lambda^{i,j} m_{i+j} + \sum_{k<i+j} \lambda_k^{i,j} m_k.$$

При $\alpha > 1$ получаем

$$\begin{aligned}
\lambda^{\nu,\alpha} m_{\nu+\alpha} &= S_{\nu,\alpha} - \sum_{k<\nu+\alpha} \lambda_k^{\nu,\alpha} m_k = \sum_{i<\nu} c_i' S_{i,\alpha} - \sum_{k<\nu+\alpha} \lambda_k^{\nu,\alpha} m_k = \\
&= \sum_{i<\nu} c_i' \lambda^{i,\alpha} m_{i+\alpha} + \sum_{i<nu} c_i' \sum_{k<i+\alpha} \lambda_k^{i,\alpha} m_k - \sum_{k<\nu+\alpha} \lambda_k^{\nu,\alpha} m_k = \\
= \sum_{i<\nu} c_i' \lambda^{i,\alpha} \sum_{j=1}^{\nu} h_j f_{i+\alpha}(\omega_j) &+ \sum_{i<nu} c_i' \sum_{k<i+\alpha} \lambda_k^{i,\alpha} \sum_{j=1}^{\nu} h_j f_k(\omega_j) - \sum_{k<\nu+\alpha} \lambda_k^{\nu,\alpha} \sum_{j=1}^{\nu} h_j f_k(\omega_j) = \\
&= \sum_{i<\nu} c_i' \lambda^{i,\alpha} \sum_{j=1}^{\nu} h_j f_i(\omega_j) f_\alpha(\omega_j) - \sum_{k<\nu+\alpha} \lambda_k^{\nu,\alpha} \sum_{j=1}^{\nu} h_j f_k(\omega_j) = \\
&= \lambda^{\nu,\alpha} \sum_{j=1}^{\nu} h_j f_\nu(\omega_j) f_\alpha(\omega_j) - \sum_{k<\nu+\alpha} \lambda_k^{\nu,\alpha} \sum_{j=1}^{\nu} h_j f_k(\omega_j) = \\
&= \lambda^{\nu,\alpha} \sum_{j=1}^{\nu} h_j f_{\nu+\alpha}(\omega_j).
\end{aligned}$$

То, что не менее чем $u + l - 1$ элементов среди $h_1, \dots, h_{u+l}$ отличны от 0, следует из леммы 3.

Утверждение 3 теоремы очевидно следует из леммы 3. ▹

Воспользуемся теоремой 2 для построения алгоритма декодирования. Пусть числа u и r удовлетворяют соотношению $2u - r + 2 = s$, и

$$\Delta = \{\delta_1, \dots, \delta_t\} \subset \Omega$$

— какое-либо решение системы (1). Рассмотрим многочлены

$$O_{u+1}^{(l)}(Z_1, \dots, Z_r) = O_{u+1}^{(l)}(Z_1, \dots, Z_r; m_1, \dots, m_{2u-r+3}), \qquad l = 0, 1.$$

Пусть $\Omega' = \{\omega_1, \dots, \omega_{r-1}\}$ — $(r-1)$-элементное подмножество множества Ω, и $|\Omega \cap \Delta| = L$. Тогда по лемме 3

$$h = \operatorname{rank} M_{u+1,r-1} = t - L + r - 1.$$

Если $h = u$ (т. е. $L = t - u + r - 1$), то по теореме 2 (утверждение 1) хотя бы один из многочленов $O_{u+1}^{(0)}(Z, \omega_1, \dots, \omega_{r-1})$, $O_{u+1}^{(1)}(Z, \omega_1, \dots, \omega_{r-1})$ — ненулевой, его корни — $\omega_1, \dots, \omega_{u'}$, $u' \in \{u; u+1\}$, а система уравнений

$$\sum_{j=1}^{u'+1} x_j f_i(\omega_j) = m_i, \qquad i = 1, \dots, u'+1,$$

имеет единственное решение $(h_1, \dots, h_{u'})$, в нем ровно t ненулевых компонент, и

$$\sum_{j=1}^{u'+1} x_j f_i(\omega_j) = m_i, \qquad i = 1, \dots, s.$$

Если $h = u' < u$ (т. е. $L > t - u + r - 1$), то

$$m_i = \sum_{j=1}^{u'} h_j f_i(\omega_j), \qquad i = 1, \dots, 2u - r + 2,$$

и по теореме 2 (утверждение 3) $\operatorname{rank} M_{u+1,r-1} = u'$. Тогда один из многочленов

$$O^{(0)}_{u'+1}(Z, \omega_1, \dots, \omega_{r-1}), \quad O^{(1)}_{u'+1}(Z, \omega_1, \dots, \omega_{r-1})$$

— ненулевой и среди его корней содержатся искомые позиции ошибок $\omega_1, \dots, \omega_{u'}$.

Таким образом, задача определения Δ свелась к поиску $(r-1)$-элементного подмножества $\Omega' \subset \Omega$, для которого $|\Delta \cap \Omega'| \geqslant t - u + r - 1 = u + t - s + 2$. Как указано в работе [1], чтобы найти такое множество Ω' с помощью случайного выбора в Ω его элементов, нужно затратить в среднем

$$R(t, r, s) = C_N^{r-1} \Bigg/ \sum_{i=j}^{r-1} C_t^i C_{N-t}^{r-1-i} = O(N)$$

операций, $j = t + u - s + 2 = t - (s - r - 1)/2$, $N \to \infty$.

Отметим, что так же, как и в алгоритме декодирования при числе ошибок, меньшем половины кодового расстояния, если $O^{(1)}_{u+1}(Z, \omega_1, \dots, \omega_{r-1})$ — нулевой многочлен, а $O^{(0)}_{u+1}(Z, \omega_1, \dots, \omega_{r-1})$ — ненулевой, то пропорциональный ему ненулевой многочлен можно вычислить, зная только $m_1, \dots, m_{2u-r+2}$ и не зная m_{2u-r+3} (и, соответственно, не зная $S_{u+1,u-r+2}$). Действительно, если многочлен

$$O^{(1)}_u(Z, \omega_1, \dots, \omega_{r-1}) = \begin{vmatrix} f_1(Z) & f_1(\omega_1) & \dots & f_1(\omega_{r-1}) & S_{1,1} & \dots & S_{1,u-r} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ f_u(Z) & f_u(\omega_1) & \dots & f_u(\omega_{r-1}) & S_{u,1} & \dots & S_{u,u-r} \end{vmatrix}$$

— ненулевой, то очевидно, что $O^{(0)}_{u+1}(Z, \omega_1, \dots, \omega_{r-1}) = C O^{(1)}_u(Z, \omega_1, \dots, \omega_{r-1})$, где $C \neq 0$, если $O^{(0)}_{u+1}(Z, \omega_1, \dots, \omega_{r-1}) \neq 0$. Если же $O^{(1)}_u(Z, \omega_1, \dots, \omega_{r-1}) = 0$, то многочлен $O^{(0)}_{u+1}(Z, \omega_1, \dots, \omega_{r-1})$ не зависит от $S_{u+1,u-r+2}$.

Синдромный вероятностный алгоритм декодирования глубины t

Шаг 1. Вычисляем число r одинаковой четности с s, которое минимизирует функцию $R(t, r, s)$, и полагаем $u = (s + r - 2)/2$.

Шаг 2. Выбираем $(r-1)$-элементное подмножество $\Omega' = \{\omega_1, \dots, \omega_{r-1}\}$ множества Ω. Вычисляем многочлен $O^{(1)}_{u+1}(Z) = O^{(1)}_{u+1}(Z, \omega_1, \dots, \omega_{r-1})$. Если многочлен $O^{(1)}_{u+1}(Z)$ нулевой, то через известные синдромы находим многочлен $O^{(1)}_u(Z) = O^{(1)}_u(Z, \omega_1, \dots, \omega_{r-1})$. Если многочлен $O^{(1)}_u(Z)$ нулевой, то вычисляем

$$O^{(0)}_{u+1}(Z) = O^{(0)}_{u+1}(Z, \omega_1, \dots, \omega_{r-1}),$$

а иначе полагаем $O^{(0)}_{u+1}(Z) = O^{(1)}_u(Z)$.

Возможны четыре случая:

(A) $O^{(1)}_{u+1}(Z) = P(Z)$ — ненулевой, $P(Z) \in L((u+1)O)$, $\Omega'' = \{\omega_1, \dots, \omega_{u+1}\}$ — корни $P(Z)$ в Ω, $|\Omega''| = u + 1$.

(B) $O^{(1)}_{u+1}(Z)$ — нулевой, $O^{(0)}_{u+1}(Z) = P(Z)$ — ненулевой, $P(Z) \in L(uO)$, $\Omega'' = \{\omega_1, \dots, \omega_u\}$ — корни $P(Z)$ в Ω, $|\Omega''| = u$.

(C) Оба многочлена $O^{(0)}_{u+1}(Z)$, $O^{(1)}_{u+1}(Z)$ — нулевые.

(D) Среди многочленов $O^{(0)}_{u+1}(Z)$, $O^{(1)}_{u+1}(Z)$ есть ненулевой, но случаи (A) и (B) не выполнены.

Ш а г 3. Если выполнен случай (C), то находим

$$u_1 = \operatorname{rank}\begin{pmatrix} f_1(\omega_1) & \dots & f_1(\omega_{r-1}) & S_{1,1} & \dots & S_{1,u-r+1} \\ \vdots & & \vdots & \vdots & & \vdots \\ f_u(\omega_1) & \dots & f_u(\omega_{r-1}) & S_{u,1} & \dots & S_{u,u-r+1} \end{pmatrix},$$

вычисляем $O^{(1)}_{u_1+1}(Z) = O^{(1)}_{u_1+1}(Z, \omega_1, \dots, \omega_{r-1}) = P(Z)$ и полагаем $l_1 = 1$. Если же $O^{(1)}_{u_1+1}(Z)$ нулевой, то находим ненулевой многочлен $O^{(0)}_{u_1+1}(Z)$ и полагаем $P(Z) = O^{(0)}_{u_1+1}(Z)$. Находим $\Omega'' = \{\omega_1, \dots, \omega_{u''}\}$ — множество корней $P(Z)$ в Ω. Если $|\Omega''| < u_1 + l_1$, то переходим к шагу 2, в противном случае полагаем $\nu = u''$.

Если выполнен случай (A), то полагаем $\nu = u + 1$.

Если выполнен случай (B), то полагаем $\nu = u$.

Если выполнен случай (D), то переходим к шагу 2.

Ш а г 4. Находим неизвестные h_j из системы уравнений

$$\sum_{j=1}^{\nu} h_j f_i(\omega_j) = m_i, \qquad i = 1, \dots, s.$$

Если число отличных от нуля элементов h_j более t или система несовместна, то переходим к шагу 2. Если число отличных от нуля элементов h_j не превосходит t, то соответствующие h_j — это ненулевые координаты вектора ошибок, а соответствующие ω_j — позиции ошибок.

Множество Ω' в данном алгоритме выбирается с помощью случайных бросаний. Как только

$$|\Omega' \cap \Delta| \geqslant u + t - s - 1 \tag{3}$$

(где Δ — искомое множество позиций ошибок мощности t), то на шаге 3 будет выполнен случай (C) (если в (3) строгое неравенство) или один из случаев (A) и (B) (если в (3) равенство), и на шаге 4 алгоритм закончится. Чтобы найти нужное множество Ω', в среднем нужно $R(t, r, s)$ случайных бросаний до первого успеха. Средняя сложность алгоритма оценивается сверху величиной

$$O((t^4 + tN)R(t, r, s)) = O((t^4 + tN)N)$$

операций.

Автор благодарит В.М.Сидельникова за постановку задачи, а также за постоянное внимание к работе и ценные замечания.

СПИСОК ЛИТЕРАТУРЫ

1. Сидельников В.М. Декодирование кода Рида—Соломона при числе ошибок, большем $(d-1)/2$, и нули многочленов нескольких переменных // Пробл. перед. информ. 1994. Т. 30. № 1. С. 51–69.

2. Chen X., Reed I.S., Helleseth T., Truong T.K. Use of Gröbner Bases to Decode Bynary Cyclic Codes up to the True Minimum Distance // IEEE Trans. Inform. Theory. 1994. V. 40. № 5. P. 1654–1661.

3. Chen X., Reed I.S., Helleseth T., Truong T.K. General Principles for the Algebraic Decoding of a Class of Algebraic-Geometric Codes // IEEE Trans. Inform. Theory. 1994. V. 40. № 5. P. 1661–1663.

4. Хартсхорн Р. Алгебраическая геометрия. М.: Мир, 1981.

5. Мак-Вильямс Ф.Дж., Слоэн Н.Дж. Теория кодов, исправляющих ошибки. М.: Связь, 1979.

6. Skorobogatov A.N, Vlăduţ S.G. On the Decoding of a Class of Algebraic-Geometric Codes // IEEE Trans. Inform. Theory. 1990. V. 36. № 5. P. 1051–1060.

7. Feng G.-L., Wei V.K., Rao T.R., Tzeng K.K. Simplified Understanding and Sufficient Decoding of a Class of Algebraic-Geometric Codes // IEEE Trans. Inform. Theory. 1994. V. 40. № 4. P. 981–1002.