Теория кодирования

МФТИ, осень 2013

Александр Дайняк

www.dainiak.com

Коды Рида—Соломона (I.S. Reed, G. Solomon)

Пусть $k \leq n \leq q$.

Пусть $t_1, \ldots, t_n \in \mathbb{F}_q$ — *фиксированные, попарно различные* элементы.

Рассмотрим такое множество слов:

$$C \coloneqq \left\{ (P(t_1), \ldots, P(t_n)) \mid P \in \mathbb{F}_q[x] \wedge \deg P < k \right\}$$

Непосредственно проверяется, что C — линейное пространство:

$$\alpha \cdot \big(P_1(t_1), \ldots, P_1(t_n)\big) + \beta \cdot \big(P_2(t_1), \ldots, P_2(t_n)\big) =$$
$$= \big((\alpha P_1 + \beta P_2)(t_1), \ldots, (\alpha P_1 + \beta P_2)(t_n)\big)$$

Коды Рида—Соломона

По условию, $k \leq n \leq q$.

$$C \coloneqq \left\{(P(t_1), \ldots, P(t_n)) \mid P \in \mathbb{F}_q[x] \wedge \deg P < k\right\}$$

- У многочлена степени $< k$ может быть не более $(k-1)$ корней, поэтому если $P \not\equiv 0$, то в векторе $(P(t_1), \ldots, P(t_n))$ не более $(k-1)$ нулевых координат.

  Отсюда

$$d(C) = \min_{\substack{\boldsymbol{a} \in C \\ \boldsymbol{a} \neq \mathbf{0}}} \|\boldsymbol{a}\| = \min_{P \not\equiv 0} \#\{i \mid P(t_i) \neq 0\} = n - (k-1)$$

Коды Рида—Соломона

По условию, $k \leq n \leq q$.

$$C \coloneqq \left\{(P(t_1), \ldots, P(t_n)) \mid P \in \mathbb{F}_q[x] \wedge \deg P < k\right\}$$

- Вектора $(P(t_1), \ldots, P(t_n))$ при разных P различны: если выполнено $(P_1(t_1), \ldots, P_1(t_n)) = (P_2(t_1), \ldots, P_2(t_n))$, то у многочлена $(P_1 - P_2)$ не менее n корней, а т.к. $\deg(P_1 -$

Коды Рида—Соломона

Итак, для любых $k \leq n \leq q$ множество

$$\{(P(t_1), \ldots, P(t_n)) \mid P \in \mathbb{F}_q[x] \wedge \deg P < k\}$$

является $[n, k, d]_q$-кодом, где $d = n - k + 1$.

Вспомним границу Синглтона: «*для любого* $[n, k, d]_q$*-кода выполнено* $k \leq n - d + 1$».

То есть построенный код *достигает границы Синглтона*!

Недостаток кода: кодовый алфавит нужно брать очень большим, т.к. $q \geq n$.

Коды Рида—Соломона: декодирование

Т.к. $d(C) = n - k + 1$, то код может исправлять $\left\lfloor \frac{n-k}{2} \right\rfloor$ ошибок.

Постановка задачи декодирования:

- Дано искажённое кодовое слово кода Р.—С. $(\hat{p}_1, \ldots, \hat{p}_n) \in \mathbb{F}_q^n$
- Найти $P \in \mathbb{F}_q[x]$, такой, что $\deg P \leq k - 1$ и

$$\#\{i \mid P(t_i) \neq \hat{p}_i\} \leq \left\lfloor \frac{n-k}{2} \right\rfloor$$

(нам гарантируется, что такой P существует)

Далее приведём *алгоритм Берлекэмпа—Велча* (E.R. Berlekamp, L.R. Welch).

Коды Рида—Соломона: декодирование

Дано $(\hat{p}_1, \dots, \hat{p}_n) \in \mathbb{F}_q^n$.
Найти $P\colon \deg P < k \wedge \#\{i \mid P(t_i) \neq \hat{p}_i\} \leq (n-k)/2$

Рассмотрим *многочлен ошибок*

$$E(x) \coloneqq \prod_{i\colon P(t_i) \neq \hat{p}_i} (x - t_i)$$

и вспомогательный многочлен $U(x) \coloneqq E(x) \cdot P(x)$.

Заметим, что

- $\deg E = s$ и $\operatorname{coef}_{x^s} E = 1$, где $s \coloneqq \#\{i \mid P(t_i) \neq \hat{p}_i\}$
- $\deg U \leq \deg E + \deg P \leq s + k - 1$
- Для любого $i \in \{1, \dots, n\}$ выполнено равенство

$$U(t_i) = E(t_i) \cdot \hat{p}_i$$

Коды Рида—Соломона: декодирование

Дано $(\hat{p}_1, \ldots, \hat{p}_n) \in \mathbb{F}_q^n$.
Найти $P\colon \deg P < k \wedge \#\{i \mid P(t_i) \neq \hat{p}_i\} \leq (n-k)/2$

Идея: мы не знаем P, так что попытаемся найти *какие-то* многочлены $\tilde{E}$ и $\widetilde{U}$, для которых

- $\deg \tilde{E} = s$ и $\operatorname{coef}_{x^s} \tilde{E} = 1$, где $s \leq (n-k)/2$
- $\deg \widetilde{U} \leq s + k - 1$
- Для любого $i \in \{1, \ldots, n\}$ выполнено равенство

$$\widetilde{U}(t_i) = \tilde{E}(t_i) \cdot \hat{p}_i$$

Мы знаем, что $\tilde{E}$ и $\widetilde{U}$ точно найдутся. Вопросы:
1) как это сделать эффективно, и
2) что если найденные $\tilde{E}$ и $\widetilde{U}$ не совпадут с нужными нам E и U?

Коды Рида—Соломона: декодирование

- $\deg \tilde{E} = s$ и $\operatorname{coef}_{x^s} \tilde{E} = 1$, где $s \leq (n-k)/2$
- $\deg \widetilde{U} \leq s + k - 1$
- $\forall i \in \{1, \dots, n\}$ выполнено $\widetilde{U}(t_i) = \hat{p}_i \cdot \tilde{E}(t_i)$

Зафиксируем s и положим $\tilde{E} = x^s + \sum_{j \leq s-1} e_j x^j$ и $\widetilde{U} = \sum_{j \leq s+k-1} u_j x^j$, где $e_0, \dots, e_{s-1}, u_0, \dots, u_{s+k-1}$ — неопределённые коэффициенты. Получим систему:

$$\begin{cases} \hat{p}_1 t_1^s + \sum\limits_{0 \leq j \leq s-1} \hat{p}_1 e_j t_1^j = \sum\limits_{0 \leq j \leq k+s-1} u_j t_1^j \\ \vdots \\ \hat{p}_n t_n^s + \sum\limits_{0 \leq j \leq s-1} \hat{p}_n e_j t_n^j = \sum\limits_{0 \leq j \leq k+s-1} u_j t_n^j \end{cases}$$

Коды Рида—Соломона: декодирование

При любом фиксированном $s \leq (n-k)/2$ система

$$\begin{cases} \hat{p}_1 t_1^s = -\sum\limits_{0 \leq j \leq s-1} \hat{p}_1 t_1^j \cdot e_j + \sum\limits_{0 \leq j \leq k+s-1} t_1^j \cdot u_j \\ \vdots \\ \hat{p}_n t_n^s = -\sum\limits_{0 \leq j \leq s-1} \hat{p}_n t_n^j \cdot e_j + \sum\limits_{0 \leq j \leq k+s-1} t_n^j \cdot u_j \end{cases}$$

линейная относительно $e_0, \ldots, e_{s-1}, u_0, \ldots, u_{s+k-1}$.

Коды Рида—Соломона: декодирование

При любом фиксированном s система

$$\begin{cases} \hat{p}_1 t_1^s = -\sum\limits_{0 \le j \le s-1} \hat{p}_1 t_1^j \cdot e_j + \sum\limits_{0 \le j \le k+s-1} t_1^j \cdot u_j \\ \vdots \\ \hat{p}_n t_n^s = -\sum\limits_{0 \le j \le s-1} \hat{p}_n t_n^j \cdot e_j + \sum\limits_{0 \le j \le k+s-1} t_n^j \cdot u_j \end{cases}$$

линейная относительно $e_0, \dots, e_{s-1}, u_0, \dots, u_{s+k-1}$ $\Rightarrow$ если у неё есть решение, находится оно быстро.

Перебирая $s = 0,1, \dots$, найдём то s, при котором решение есть (такое s точно существует, так как есть исходные многочлены E и U).

Тем самым найдём $\tilde{E}$ и $\tilde{U}$.

Коды Рида—Соломона: декодирование

Нашли *какие-то* $\tilde{E}$ и $\tilde{U}$.

Если бы это были *те самые* E и U, то мы сразу нашли бы $P(x) = \frac{U(x)}{E(x)}$.

Оказывается, и в ином случае P будет выражаться так же:

Утверждение.
Если пары (E_1, U_1) и (E_2, U_2) удовлетворяют системе

- $\deg \tilde{E} = s$ и $\operatorname{coef}_{x^s} \tilde{E} = 1$, где $s \leq (n-k)/2$
- $\deg \tilde{U} \leq s + k - 1$
- $\forall i \in \{1, \dots, n\}$ выполнено $\tilde{U}(t_i) = \hat{p}_i \cdot \tilde{E}(t_i)$

то $\frac{U_1}{E_1} \equiv \frac{U_2}{E_2}$.

Коды Рида—Соломона: декодирование

Доказательство утверждения:

Пусть (E_1, U_1) и (E_2, U_2) удовлетворяют системе

- $\deg \tilde{E} = s$ и $\operatorname{coef}_{x^s} \tilde{E} = 1$, где $s \le (n-k)/2$
- $\deg \widetilde{U} \le s + k - 1$
- $\forall i \in \{1, \dots, n\}$ выполнено $\widetilde{U}(t_i) = \hat{p}_i \cdot \tilde{E}(t_i)$

Имеем $\deg U_1 E_2 \le \deg U_1 + \deg E_2 \le \left(\frac{n-k}{2} + k - 1\right) + \frac{n-k}{2} \le n - 1.$

Аналогично $\deg E_1 U_2 \le n - 1.$

Далее, для любого i имеем

$$U_1(t_i)E_2(t_i) = \big(\hat{p}_i E_1(t_i)\big)E_2(t_i) = E_1(t_i)\big(\hat{p}_i E_2(t_i)\big) = E_1(t_i)U_2(t_i)$$

Коды Рида—Соломона: декодирование

Завершение доказательства леммы:

Мы установили, что

- $\deg(U_1E_2 - E_1U_2) \leq n - 1$
- $U_1(t_i)E_2(t_i) - E_1(t_i)U_2(t_i) = 0$ для $i = 1, \ldots, n$

Отсюда следует, что

$$U_1(x)E_2(x) - E_1(x)U_2(x) \equiv 0$$

а это эквивалентно тождеству

$$\frac{U_1}{E_1} \equiv \frac{U_2}{E_2}$$

Коды Рида—Соломона

Простор для обобщений:

- Рассматривать многочлены не от одной, а от многих переменных (*коды Рида—Маллера* и другие)
- Рассматривать не все возможные многочлены, а специально выбранное их подмножество (*алгеброгеометрические коды*)

Коды Рида—Маллера (I.S. Reed, D.E. Muller)

Зафиксируем параметры (r, m), где $r \leq m$.

Полагаем $q := 2$ и берём многочлены от m переменных степени $\leq r$.

Базис в пространстве $\{P \in \mathbb{F}_2[x_1, \ldots, x_m], \deg P \leq r\}$:

$$
\begin{aligned}
&\{1\} \cup \\
&\cup \{x_1, x_2, \ldots, x_m\} \cup \\
&\cup \{x_1x_2, x_1x_3, \ldots, x_{m-1}x_m\} \cup \\
&\vdots \\
&\cup \left\{x_{i_1}x_{i_2}\cdots x_{i_r} \mid 1 \leq i_1, \ldots, i_r \leq m\right\}
\end{aligned}
$$

Размерность этого пространства равна $k = \sum_{t \leq r} \binom{m}{t}$.

Коды Рида—Маллера

Рассматриваем значения многочленов во всех точках $\mathbb{F}_2^m$:

$$C \coloneqq \{\big(P(0\ldots00), P(0\ldots01), \ldots, P(1\ldots11)\big)$$
$$\text{где } P \in \mathbb{F}_2[x_1, \ldots, x_m] \text{ и } \deg P \leq r\}$$

Получаем $[n, k, d]$-код, где $n = 2^m$ и $k = \sum_{t \leq r} \binom{m}{t}$.

Чтобы оценить d, понадобится доказать лемму:

Лемма.

Если $P \in \mathbb{F}_2[x_1, \ldots, x_m]$, $P \not\equiv 0$ и $\deg P \leq r$, то

$$\#\{(s_1, \ldots, s_m) \in \mathbb{F}_2^m \mid P(s_1, \ldots, s_m) = 1\} \geq 2^{m-r}$$

Коды Рида—Маллера: кодовое расстояние

Лемма.

Если $P \in \mathbb{F}_2[x_1, \dots, x_m]$, $P \not\equiv 0$ и $\deg P \le r$, то

$$\#\{(s_1, \dots, s_m) \in \mathbb{F}_2^m \mid P(s_1, \dots, s_m) = 1\} \ge 2^{m-r}$$

Доказательство: индукция по m.

База: $m = 1$. Тогда $P \in \{1, x_1, x_1 + 1\}$ — очевидно.

Переход: $m - 1 \to m$. Б.о.о. будем считать, что P существенно зависит от x_m. Распишем

$$P(x_1, \dots, x_m) = P_1(x_1, \dots x_{m-1}) + x_m P_2(x_1, \dots x_{m-1})$$

Так как $P_2 \not\equiv 0$ и $\deg P_2 \le r - 1$, то

$$\#\{(s_1, \dots, s_{m-1}) \mid P_2(s_1, \dots, s_{m-1}) = 1\} \ge 2^{(m-1)-(r-1)}$$

Коды Рида—Маллера: кодовое расстояние

$$P(x_1, \dots, x_m) = P_1(x_1, \dots x_{m-1}) + x_m P_2(x_1, \dots x_{m-1})$$
$$\#\{(s_1, \dots, s_{m-1}) \mid P_2(s_1, \dots, s_{m-1}) = 1\} \geq 2^{m-r}$$

Каждый набор $(s_1, \dots, s_{m-1})$ на котором $P_2 = 1$, можно дополнить до набора, на котором $P = 1$:

- если $P_1(s_1, \dots, s_{m-1}) = 0$, то возьмём набор $(s_1, \dots, s_{m-1}, 1)$,
- если $P_1(s_1, \dots, s_{m-1}) = 1$, то возьмём набор $(s_1, \dots, s_{m-1}, 0)$.

Значит, $P = 1$ не менее чем на 2^{m-r} наборах.

Коды Рида—Маллера: мажоритарное декодирование

Код Рида—Маллера с параметрами (r, m) является $\left[2^m, \sum_{t \le r} \binom{m}{t}, 2^{m-r}\right]$-кодом.

Значит, он может исправлять вплоть до $(2^{m-r-1} - 1)$ ошибок, и это можно делать очень быстро *многоэтапным голосованием* (этот способ декодирования также называют *мажоритарным*).

Постановка задачи:

- В векторе из кода Р.—М. (т.е. векторе значений многочлена степени $\le r$) изменяются менее 2^{m-r-1} координат (т.е. значение многочлена искажается менее чем в стольких точках)
- Нужно восстановить по искажённому вектору значений исходный вектор значений (т.е. исходный многочлен)

Коды Рида—Маллера: мажоритарное декодирование

Кодовое слово — это значения многочлена, выразимого линейной комбинацией в базисе

$$\{1\} \cup \{x_1, x_2, \dots, x_m\} \cup \dots \cup \left\{x_{i_1} x_{i_2} \cdots x_{i_r} \mid 1 \le i_1, \dots, i_r \le m\right\}$$

Восстановить кодовое слово — это то же, что найти коэффициенты этой линейной комбинации.

Лемма о старшем коэффициенте многочленов над $\mathbb{F}_2$

Лемма.
Для любого $P \in \mathbb{F}_2[x_1, \dots, x_r]$ справедлива формула

$$\operatorname{coef}_{x_1 \cdot \dots \cdot x_r} P = \sum_{\alpha_1, \dots, \alpha_r \in \mathbb{F}_2} P(\alpha_1, \dots, \alpha_r)$$

Доказательство:
Многочлен P можно представить в виде

$$P = c \cdot x_1 \dots x_r + P_1 + \dots + P_r$$

где в P_i *не* входит x_i. Получаем

$$\sum_{\alpha_1, \dots, \alpha_r \in \mathbb{F}_2} P(\alpha_1, \dots, \alpha_r) = \underbrace{\sum_{\alpha_1, \dots, \alpha_r \in \mathbb{F}_2} c \cdot \alpha_1 \dots \alpha_r}_{=c} + \sum_{1 \le i \le r} \underbrace{\sum_{\alpha_1, \dots, \alpha_r \in \mathbb{F}_2} P_i(\alpha_1, \dots, \alpha_r)}_{=0}$$

Лемма о старшем коэффициенте многочленов над $\mathbb{F}_2$

$$\sum_{\alpha_1,\dots,\alpha_r \in \mathbb{F}_2} P_i(\alpha_1, \dots, \alpha_r) = \sum_{\alpha_1,\dots\alpha_{i-1},\alpha_{i+1},\dots,\alpha_r \in \mathbb{F}_2} \begin{pmatrix} P_i(\alpha_1, \dots \alpha_{i-1}, 0, \alpha_{i+1}, \dots, \alpha_r) \\ +P_i(\alpha_1, \dots \alpha_{i-1}, 1, \alpha_{i+1}, \dots, \alpha_r) \end{pmatrix}$$

Но т.к. в слагаемые P_i переменная x_i не входит, то

$$P_i(\alpha_1, \dots \alpha_{i-1}, 0, \alpha_{i+1}, \dots, \alpha_r) = P_i(\alpha_1, \dots \alpha_{i-1}, 1, \alpha_{i+1}, \dots, \alpha_r)$$

а значит по модулю 2 каждое слагаемое в последней сумме равно нулю.

Лемма доказана.

Коды Рида—Маллера: мажоритарное декодирование

Пусть P — произвольный многочлен из кода Рида—Маллера.

Зафиксируем произвольные $\beta_1, \dots, \beta_{m-r} \in \mathbb{F}_2$, и обозначим

$$P_{\beta_1,\dots,\beta_{m-r}} := P(x_1, \dots, x_r, \beta_1, \dots, \beta_{m-r})$$

Имеем $P_{\beta_1,\dots,\beta_{m-r}} \in \mathbb{F}_2[x_1, \dots, x_r]$, поэтому по лемме, доказанной только что, получаем

$$\sum_{\alpha_1,\dots,\alpha_r \in \mathbb{F}_2} P_{\beta_1,\dots,\beta_{m-r}}(\alpha_1, \dots, \alpha_r) = \operatorname{coef}_{x_1 \cdot \dots \cdot x_r} P_{\beta_1,\dots,\beta_{m-r}} = \operatorname{coef}_{x_1 \cdot \dots \cdot x_r} P$$

Коды Рида—Маллера: мажоритарное декодирование

Для любых $\beta_1, \dots, \beta_{m-r} \in \mathbb{F}_2$ мы получили

$$\operatorname{coef}_{x_1 \cdot \dots \cdot x_r} P = \sum_{\alpha_1, \dots, \alpha_r \in \mathbb{F}_2} P(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_{m-r})$$

Если нам дано кодовое слово с не более чем $(2^{m-r-1} - 1)$ ошибками, это означает, что нам для дан некий набор величин $\hat{P}(t_1, \dots, t_m)$, где $\hat{P}(t_1, \dots, t_m) = P(t_1, \dots, t_m)$ для всех $(t_1, \dots, t_m) \in \mathbb{F}_2^m \setminus T_{\text{bad}}$, где $|T_{\text{bad}}| \leq 2^{m-r-1} - 1$.

Подставим $\hat{P}(t_1, \dots, t_m)$ вместо $P(t_1, \dots, t_m)$ в нашу формулу…

Коды Рида—Маллера: мажоритарное декодирование

Для каждого набора $(\beta_1, \dots, \beta_{m-r}) \in \mathbb{F}_2^{m-r}$ рассмотрим сумму

$$\hat{S}_{\beta_1,\dots,\beta_{m-r}} := \sum_{\alpha_1,\dots,\alpha_r \in \mathbb{F}_2} \hat{P}(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_{m-r})$$

У сумм $\hat{S}_{\beta_1,\dots,\beta_{m-r}}$ при разных нет общих слагаемых. Поэтому

$$\hat{S}_{\beta_1,\dots,\beta_{m-r}} = \operatorname{coef}_{x_1 \cdot \dots \cdot x_r} P$$

для всех $(\beta_1, \dots, \beta_{m-r}) \in \mathbb{F}_2^{m-r}$, кроме, быть может, $|T_{\text{bad}}|$ штук.

Всего сумм 2^{m-r}, и $|T_{\text{bad}}| < 2^{m-r-1}$, а значит *большинство* этих сумм *равны* $\operatorname{coef}_{x_1 \cdot \dots \cdot x_r} P$.

Коды Рида—Маллера: мажоритарное декодирование

Итоговый метод определения $\mathrm{coef}_{x_1 \cdot \ldots \cdot x_r} P$:

- Для каждого $(\beta_1, \ldots, \beta_{m-r}) \in \mathbb{F}_2^{m-r}$ вычисляем соответствующую сумму $\hat{S}_{\beta_1,\ldots,\beta_{m-r}}$
- Находим $\mathrm{coef}_{x_1 \cdot \ldots \cdot x_r} P$ *голосованием*:
  т.е. как то значение, которое встречается чаще всего среди $\{\hat{S}_{\beta_1,\ldots,\beta_{m-r}}\}$.

Ясно, что так можно определить *любой* из коэффициентов $\mathrm{coef}_{x_{i_1} \cdot \ldots \cdot x_{i_r}} P$.

Коды Рида—Маллера: мажоритарное декодирование

Пусть уже найдены все $\mathrm{coef}_{x_{i_1}\cdot\ldots\cdot x_{i_r}} P$.

Рассмотрим многочлен

$$P_{[r-1]} \coloneqq P - \sum_{i_1,\ldots,i_r} \left(\mathrm{coef}_{x_{i_1}\cdot\ldots\cdot x_{i_r}} P\right) \cdot x_{i_1} \ldots x_{i_r}$$

В $P_{[r-1]}$ уже все слагаемые степени $\leq r-1$.

Рассмотрим величины $\hat{P}_{[r-1]}(t_1, \ldots, t_m)$, равные

$$\hat{P}(t_1, \ldots, t_m) - \sum_{i_1,\ldots,i_r} \left(\mathrm{coef}_{x_{i_1}\cdot\ldots\cdot x_{i_r}} P\right) \cdot t_{i_1} \ldots t_{i_r}$$

Ясно, что $\hat{P}_{[r-1]}(t_1, \ldots, t_m) = P_{[r-1]}(t_1, \ldots, t_m)$ на множестве точек $\mathbb{F}_2^m \setminus T_{\mathrm{bad}}$.

Коды Рида—Маллера: мажоритарное декодирование

Пусть уже найдены все $\mathrm{coef}_{x_{i_1}\cdot\ldots\cdot x_{i_r}} P$.

Вычисляем величины $\hat{P}_{[r-1]}(t_1, \ldots, t_m)$, равные

$$\hat{P}(t_1, \ldots, t_m) - \sum_{i_1,\ldots,i_r} \left(\mathrm{coef}_{x_{i_1}\cdot\ldots\cdot x_{i_r}} P\right) \cdot t_{i_1} \ldots t_{i_r}$$

Т.к. $\hat{P}_{[r-1]}(t_1, \ldots, t_m) = P_{[r-1]}(t_1, \ldots, t_m)$ на множестве $\mathbb{F}_2^m \setminus T_{\mathrm{bad}}$, то как и ранее, голосованием определяем $\mathrm{coef}_{x_{i_1}\cdot\ldots\cdot x_{i_{r-1}}} P_{[r-1]}$.

Но $\mathrm{coef}_{x_{i_1}\cdot\ldots\cdot x_{i_{r-1}}} P_{[r-1]} = \mathrm{coef}_{x_{i_1}\cdot\ldots\cdot x_{i_{r-1}}} P$, то есть теперь мы знаем коэффициенты при слагаемых P степени $\leq r-1$.

Коды Рида—Маллера: мажоритарное декодирование

Общая схема:

- Определяем все $\mathrm{coef}_{x_{i_1}\cdot\ldots\cdot x_{i_r}} P$
- Рассматриваем
$$P_{[r-1]} \coloneqq P - \sum_{i_1,\ldots,i_r} \left(\mathrm{coef}_{x_{i_1}\cdot\ldots\cdot x_{i_r}} P\right) \cdot x_{i_1} \ldots x_{i_r}$$
- Определяем все $\mathrm{coef}_{x_{i_1}\cdot\ldots\cdot x_{i_{r-1}}} P$
- Рассматриваем
$$P_{[r-2]} \coloneqq P_{[r-1]} - \sum_{i_1,\ldots,i_{r-1}} \left(\mathrm{coef}_{x_{i_1}\cdot\ldots\cdot x_{i_{r-1}}} P\right) \cdot x_{i_1} \ldots x_{i_{r-1}}$$
- Определяем все $\mathrm{coef}_{x_{i_1}\cdot\ldots\cdot x_{i_{r-2}}} P$
- И так далее…

Лемма Шварца—Зиппеля

Чтобы оценивать $d(C)$ кодов на основе многочленов многих переменных, подходит

Теорема. (R.J. Lipton, R.A. DeMillo, J. Schwartz, R. Zippel)
Пусть $P \in \mathbb{F}[x_1, \ldots, x_m]$ и $P \not\equiv 0$.
Пусть $S \subseteq \mathbb{F}$ — произвольное множество мощности N.

Тогда

$$\#\{(s_1, \ldots, s_m) \in S^m \mid P(s_1, \ldots, s_m) = 0\} \leq N^{m-1} \cdot \deg P$$

Лемма Шварца—Зиппеля

Доказательство: индукция по m.

База: $m = 1$. Это стандартная теорема из алгебры: «число корней многочлена $P \in \mathbb{F}[x_1]$ не превосходит $\deg P$».

Индукт. переход: Распишем P по степеням x_m:

$$P(x_1, \dots, x_m) = \sum_{k=0}^{t} x_m^k \cdot P_k(x_1, \dots, x_{m-1})$$

где $P_1, \dots, P_t \in \mathbb{F}[x_1, \dots, x_{m-1}]$.

Лемма Шварца—Зиппеля

$$P(x_1, \dots, x_m) = \sum_{k=0}^{t} x_m^k \cdot P_k(x_1, \dots, x_{m-1})$$

Обозначим

$$\hat{S} \coloneqq \{(s_1, \dots, s_{m-1}) \in S^{m-1} \mid P_t(s_1, \dots, s_{m-1}) = 0\}$$

Из неравенства $\deg P_t \leq \deg P - t$ и из предположения индукции следует:

$$\left|\hat{S}\right| \leq N^{m-2} \cdot \deg P_t \leq N^{m-2} \cdot (\deg P - t)$$

Лемма Шварца—Зиппеля

$$P(x_1, \dots, x_m) = \sum_{k=0}^{t} x_m^k \cdot P_k(x_1, \dots, x_{m-1})$$

$$\hat{S} \coloneqq \{(s_1, \dots, s_{m-1}) \in S^{m-1} \mid P_t(s_1, \dots, s_{m-1}) = 0\}$$

Теперь оценим:

$$\begin{aligned}
&|\{(s_1, \dots, s_m) \in S^m \mid P(s_1, \dots, s_m) = 0\}| = \\
&= \left|\left\{(s_1, \dots, s_m) \mid P(s_1, \dots, s_m) = 0 \wedge (s_1, \dots, s_{m-1}) \in \hat{S}\right\}\right| \\
&+ \left|\left\{(s_1, \dots, s_m) \mid P(s_1, \dots, s_m) = 0 \wedge (s_1, \dots, s_{m-1}) \notin \hat{S}\right\}\right| \\
&\leq \left|\hat{S}\right| \cdot N + \left(N^{m-1} - \left|\hat{S}\right|\right) \cdot t \leq \left|\hat{S}\right| \cdot N + N^{m-1} \cdot t \leq \\
&\leq N^{m-1} \cdot (\deg P - t) + N^{m-1} \cdot t = N^{m-1} \cdot \deg P
\end{aligned}$$

Лемма Шварца—Зиппеля

Формулировка леммы Шварца—Зиппеля в вероятностных терминах:

Пусть $P \in \mathbb{F}[x_1, \ldots, x_m]$ и $P \not\equiv 0$.

Тогда, если $s_1, \ldots, s_m$ выбираются равновероятно и независимо из некоторого множества мощности N, то

$$\Pr\{P(s_1, \ldots, s_m) = 0\} \leq \frac{\deg P}{N}$$

Пример кода на основе многочленов от двух переменных

Пусть $\mathbb{F}_q = \{t_1, \dots, t_q\}$.

Рассмотрим код

$$C \coloneqq \left\{ \left(P(t_1, t_1), P(t_1, t_2) \dots, P\left(t_q, t_q\right) \right) \mid P(x, y) = \sum_{0 \le i,j < l} \alpha_{ij} x^i y^j \right\}$$

Он является $[q^2, l^2, q(q-2l)]_q$-кодом (оценка $d(C)$ по лемме Шварца—Зиппеля).

Можно также доказать более сильную оценку

$$d(C) \geq (q-l)^2$$

Алгеброгеометрические коды (коды В.Д. Гоппы)

Код Рида—Соломона выглядит так:

$$\left\{\left(P(t_1), \ldots, P(t_n)\right) \mid P \in \mathbb{F}_q[x] \wedge \deg P < k\right\}$$

Идея: многочлен маленькой степени имеет мало нулей.

Как можно улучшить конструкцию:

- Тщательно выбрать множество точек $\{t_1, \ldots, t_n\}$, в которых вычисляется значение P
- Брать не всевозможные многочлены ограниченной степени, а специально выбранное их подмножество.

Пример алгеброгеометрического кода

Идея: в качестве точек $t_1, \dots, t_n$ берём нули некоторого многочлена P_{base} небольшой степени.

В качестве многочленов, по которым строится C, берём многочлены, имеющие мало общих нулей с P_{base}.

Пример.
Будем работать в $\mathbb{F}_{13}$, взяв

$$P_{base} := y^2 - 2x^3 + 2x$$

Множество нулей этого многочлена:

$$S_{base} = \{(0,0), (\pm 1;\ 0), (2; \pm 5), (3; \pm 3), (4; \pm 4),$$
$$(6; \pm 2), (7; \pm 3), (9; \pm 6), (10; \pm 2), (11; \pm 1)\}$$

Пример алгеброгеометрического кода

$$q \coloneqq 13$$
$$P_{base} \coloneqq y^2 - 2x^3 + 2x$$
$$n \coloneqq |S_{base}| = 19$$

Рассмотрим множество многочленов

$$\tilde{P} \coloneqq \{\alpha_1 + \alpha_2 x + \alpha_3 x^2 + \alpha_4 x^3 + \alpha_5 y + \alpha_6 xy\}$$

Лемма.

Если $P \in \tilde{P}$ и $P \not\equiv 0$, то у многочленов P и P_{base} не больше шести общих нулей.

Следствие.

Множество $C \coloneqq \left\{\left(P(x_0, y_0)\right)_{(x_0,y_0)\in S_{\text{base}}} \mid P \in \tilde{P}\right\}$ является $[19,6,13]_{13}$-кодом.

Пример алгеброгеометрического кода

$$q \coloneqq 13$$

$$P_{base} \coloneqq y^2 - 2x^3 + 2x$$

$$n \coloneqq |S_{base}| = 19$$

$$\tilde{P} \coloneqq \{\alpha_1 + \alpha_2 x + \alpha_3 x^2 + \alpha_4 x^3 + \alpha_5 y + \alpha_6 xy\}$$

Множество $C \coloneqq \left\{\left(P(x_0, y_0)\right)_{(x_0,y_0)\in S_{\text{base}}} \mid P \in \tilde{P}\right\}$, образует $[19,6,13]_{13}$-код.

Сравнение с конструкцией Рида—Соломона:

Чтобы с помощью конструкции Р.—С. получить $k \geq 6$ и $d \geq 13$, пришлось бы взять $q \geq n \geq k + d - 1 \geq 18$, и это дало бы $[18,6,13]_{19}$-код или $[19,6,14]_{19}$-код.

Т.е. выгадали бы единицу в длине слов или расстоянии, но проиграли бы в мощности алфавита в полтора раза.