Новые метрики в теории кодирования

Евгений Чекунов
echekunov@gmail.com

Введение

- Метрика Хэмминга хороша не для всех каналов связи
- Новые метрики могут обеспечить новые возможности для исправления ошибок специального вида
- Применение новых метрик в криптографии и других областях

Определение метрики

Пусть $\Omega = \mathbf{F}_q^n$ – ***n***-мерное векторное пространство над конечным полем $\mathbf{F}_q = GF(q),\ q = p^r,\ r > 0.$

Линейной оболочкой $\langle X \rangle$ подмножества $X \subset \Omega$ будем называть наименьшее линейное подпространство $F_X \subseteq \Omega$, содержащее X

Пусть $\mathcal{F} := \{F_1, F_2, ..., F_N\}$ – любое семейство подмножеств $F_i \subset \Omega$ таких, что $\langle \bigcup_{i=1}^{N} F_i \rangle = \Omega.$

Определение метрики

Опр. 1 *$\mathcal{F}$-нормой ($\mathcal{F}$-весом)* $\mathcal{N}_{\mathcal{F}}$ вектора $x \in \Omega$ называется мощность наименьшего подмножества I множества $\{1,2,\ldots,N\}$ такого, что x принадлежит $\langle \bigcup_{i \in I} F_i \rangle$.

Опр. 2 *$\mathcal{F}$-расстоянием* между точками x и y называется норма их разности: $d_{\mathcal{F}}(x, y) = \mathcal{N}_{\mathcal{F}}(x - y)$.

1) Очевидно выполнены свойства норм

2) Справедливо равенство: $\left\langle \bigcup_{i \in I} F_i \right\rangle = \left\langle \bigcup_{i \in I} \langle F_i \rangle \right\rangle$

3) Если $F_i \subset F_j, i \neq j$, то удаление F_i из семейства не меняет норму

Примеры метрик

Пр. 1 Пусть $N = n,\ \Omega = \mathbf{F}_q^n,\ \mathcal{F} := \{E_1, E_2, ..., E_n\},$ где E_i - стандартный базис в $\mathbf{F}_q^n$. Тогда $\mathcal{F}$-норма – обычный вес Хэмминга:

$$\mathcal{N}_{\mathcal{F}}(x) = d_H(x),\ \forall x \in \mathbf{F}_q^n.$$

Если $\mathcal{F} := \{f_1, f_2, ..., f_n\}$, где векторы f_i образуют базис в $\mathbf{F}_q^n$, то данная метрика эквивалентна метрике Хэмминга.

Пр. 2 Пусть $\Omega = F_q^{m \times l}$ - пространство матриц размера $m\ x\ l$ над полем $\mathbf{F}_q$. Обозначим через $\mathcal{R}$ множество матриц еденичного ранга:

$$\mathcal{R} = \left\{ M : \operatorname{rank} M = 1,\ M \in F_q^{m \times l} \right\}$$

Тогда $\mathcal{N}_{\mathcal{R}}(A) = \operatorname{rank} A,\ \forall A \in \mathbf{F}_q^{m \times l}$, т.е. ранговая метрика.

Другие метрики

- Метрика Ли

Весом Ли вектора $(c_0, c_1, ..., c_{n-1})$, $c_i \in \mathbf{F}_p$, $p -$ простое, называется сумма весов Ли $V_L(c_i)$ его координат, где

$$V_L(c_i) = | c_i |, \; c_i \equiv | c_i | \bmod p, \; 0 \le c_i \le p/2.$$

Коды в $\mathcal{F}$-метрике

Опр. 3 Любое подмножество $C \subseteq \Omega$ называется кодом.

Опр. 4 $\mathcal{F}$-расстоянием кода $C \subset \Omega$ называется целое число

$$d_{\mathcal{F}}(C) := \min\{d_{\mathcal{F}}(x, y) \mid x, y \in C, x \neq y\}.$$

Опр. 5 Если элементы семейства $\mathcal{F} := \{F_1, F_2, ..., F_N\}$ - векторы, то метрика, порожденная данным семейством, называется *проективной $\mathcal{F}$-метрикой*. В этом случае мы будем обозначать элементы семейства через f_i: $\mathcal{F} := \{f_1, f_2, ..., f_N\}$.

Лемма 1 (обобщенная граница Синглтона) Для любого линейного кода $C \subseteq \mathbf{F}_q^n$ размерности k выполняется условие $d_{\mathcal{F}}(C) \leq n - k + 1$.

Родительский код

Пусть отображение $\varphi : \mathbf{F}_q^N \to \mathbf{F}_q^n$ задано с помощью $\varphi(e_i) := f_i,\ i = 1,\ldots, N$, где $\{e_1, e_2, \ldots, e_N\}$ - стандарнтный базис $\mathbf{F}_q^N$, а $\{f_1, f_2, \ldots, f_N\}$ - векторы, задающие $\mathcal{F}$-метрику.

Опр. 6 *Родительским кодом* называется ядро $P := \ker(\varphi) \subset F_q^N$.

Т.к. $x \in \ker(\varphi) \Leftrightarrow Fx = 0,$ где F – матрица, столбцы которой координаты векторов $\varphi(e_i) := f_i,\ i = 1,\ldots, N,$ в пространстве $\mathbf{F}_q^N$, то родительский код P является $[N, N - n]$-кодом с проверочной матрицей F.

Пусть $w(D)$ - вес смежного класса $D \in F_q^N / P.$

Лемма 2 $\mathcal{F}$-норма любого $y \in F_q^n$ равна весу Хэмминга смежного класса, имеющего в качестве синдрома y: $d_{\mathcal{F}}(y) = d_H(\varphi^{-1}(y)).$

Максимальная $\mathcal{F}$-норма равна радиусу покрытия родительского кода P:

$$\rho(P) := \max\{w(D),\ D \in \mathbf{F}_q^N / P\}.$$

Коды в $\mathcal{F}$-метрике Вандермонда

$$F = \begin{pmatrix} u_1 & u_2 & \dots & u_N \\ u_1 x_1 & u_2 x_2 & \dots & u_N x_N \\ u_1 x_1^2 & u_2 x_2^2 & \dots & u_N x_N^2 \\ \dots & \dots & \dots & \dots \\ u_1 x_1^{n-1} & u_2 x_2^{n-1} & \dots & u_N x_N^{n-1} \end{pmatrix},$$

$$n \le N, x_i \in \mathbf{F}_q, x_i \ne x_j,$$

$$u_i \in \mathbf{F}_q \setminus \{0\}, \; i = 1, \dots, N.$$

Родительским кодом для данной $\mathcal{F}$-метрики является обобщенный код Рида-Соломона (ОРС-код).

Код с максимальным $\mathcal{F}$-расстоянием

Код, достигающий границы Синглтона назовем *кодом с максимальным $\mathcal{F}$-расстоянием,* $d_{\mathcal{F}} = n - k + 1$.

Пусть линейный $[n, k]$-код C задается с помощью транспонированной порождающей матрицы

$$G^{\tau} = \begin{pmatrix} g_{11} & g_{21} & \dots & g_{k1} \\ g_{12} & g_{22} & \dots & g_{k2} \\ \dots & \dots & \dots & \dots \\ g_{1n} & g_{2n} & \dots & g_{kn} \end{pmatrix} \Rightarrow \quad g = G^{\tau} a, \ a = (a_1, a_2, \dots, a_k)^{\tau}.$$

Пусть $G^{\tau} = \begin{pmatrix} v_1 & v_2 & \dots & v_k \\ v_1 y_1 & v_2 y_2 & \dots & v_k y_k \\ v_1 y_1^2 & v_2 y_2^2 & \dots & v_k y_k^2 \\ \dots & \dots & \dots & \dots \\ v_1 y_1^{n-1} & v_2 y_2^{n-1} & \dots & v_k y_k^{n-1} \end{pmatrix}, \quad v_i \in \mathbf{F}_q \setminus \{0\}, \ y_i \neq y_j, y_i \neq x_j.$

Код с максимальным F-расстоянием

$(F \mid G)-$ обобщенная матрица Вандермонда.

Размерность кода k должна удовлетворять соотношению $k + N \le q$

Лемма 3 Код C, задаваемый матрицей G^{τ}, является кодом с максимальным $\mathcal{F}$-расстоянием: $d_{\mathcal{F}}(C) = n - k + 1$. Соответственно, код может исправить вплоть до $t_k = \left\lfloor \frac{n-k}{2} \right\rfloor$ $\mathcal{F}$-ошибок.

Быстрое декодирование

Пусть $c=g+e$, где g – кодовый вектор, e – вектор ошибки.

Пусть $\mathcal{N}_{\mathcal{F}}(e)=t$. Тогда e можно представить в виде линейной комбинации векторов $\{f_i\}$:

$$e=m_1 f_1+m_2 f_2+\ldots+m_N f_N,\ d_H(m)=t, m=(m_1,m_2,\ldots,m_N)^{\tau}.$$

Покажем, что существует алгоритм быстрого декодирования, если $t \le t_k$.

$$\left(F \mid G^{\tau}\right)=\left(\begin{array}{cccc|cccc} u_1 & u_2 & \ldots & u_N & v_1 & v_2 & \ldots & v_k \\ u_1x_1 & u_2x_2 & \ldots & u_Nx_N & v_1y_1 & v_2y_2 & \ldots & v_ky_k \\ u_1x_1^2 & u_2x_2^2 & \ldots & u_Nx_N^2 & v_1y_1^2 & v_2y_2^2 & \ldots & v_ky_k^2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ u_1x_1^{n-1} & u_2x_2^{n-1} & \ldots & u_Nx_N^{n-1} & v_1y_1^{n-1} & v_2y_2^{n-1} & \ldots & v_ky_k^{n-1} \end{array}\right) \qquad (*)$$

Быстрое декодирование

Пусть R – матрица, образованная последними n столбцами матрицы (*).

Тогда $$R^{-1}\left(F \mid G^{\tau}\right)=\left(\tilde{F} \mid \tilde{G}^{\tau}\right)=\left(\begin{array}{cc|c} B_1 & E_{n-k} & 0 \\ B_2 & 0 & E_k \end{array}\right),$$

E_l - еденичная матрица порядка l,

$\begin{pmatrix} B_1 \\ B_2 \end{pmatrix}$ - обобщенная матрица Коши размера $n \times (N-n+k)$ с элементами вида $b_{ij}=\dfrac{\alpha_i \beta_j}{\mu_i-\nu_j}$.

$$R^{-1}c = R^{-1}(g+e) = R^{-1}(g+Fm) = \tilde{g}+\tilde{F}m = \tilde{g}+\tilde{e}.$$

$$\tilde{g} = R^{-1}g = (0,0,\ldots,0,\tilde{g}_{n-k+1},\tilde{g}_{n-k+2},\ldots,\tilde{g}_n)^{\tau}$$

Это позволяет определить n - k координат вектора $\tilde{e} = R^{-1}Fm = \tilde{F}m.$

Быстрое декодирование

Покажем, что зная n - k координат$\tilde{e}$ можно восстановить вектор m, то есть необходимо решить систему уравнений $\tilde{F}m = \tilde{e}$:

$$\begin{pmatrix} B_1 & E_{n-k} \\ B_1 & 0 \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_N \end{pmatrix} = \begin{pmatrix} \tilde{e}_1 \\ \tilde{e}_2 \\ \vdots \\ \tilde{e}_{n-k} \\ * \\ \vdots \\ * \end{pmatrix}.$$

Рассмотрим n - k первых строк системы:

Быстрое декодирование

$$\begin{pmatrix} b_{1,1} & b_{1,2} & \dots & b_{1,N+k-n} & 1 & \dots & 0 \\ b_{2,1} & b_{2,2} & \dots & b_{2,N+k-n} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ b_{n-k,1} & b_{n-k,2} & \dots & b_{n-k,N+k-n} & 0 & \dots & 1 \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_N \end{pmatrix} = \begin{pmatrix} \tilde{e}_1 \\ \tilde{e}_2 \\ \vdots \\ \tilde{e}_{n-k} \end{pmatrix}.$$

Матрица $H = (B_1 \mid E_{n-k})$ может быть преобразована к виду обобщенной матрицы Вандермонда, путем умножения на подходящую невырожденную матрицу Ψ порядка n-k:

$$H' = (\Psi B_1 \mid \Psi).$$

Т.е. необходимо решить систему $H'm = \Psi \begin{pmatrix} \tilde{e}_1 \\ \tilde{e}_2 \\ \vdots \\ \tilde{e}_{n-k} \end{pmatrix}$

Решение этой системы представляет собой задачу декодирования ОРС-кода с проверочной матрицей H' стандартного вида.

Задача имеет единственное решение если $d_H(m) \le \left\lfloor \frac{n-k}{2} \right\rfloor$.

Криптосистема Нидеррайтера

Секретный ключ: $\{S, H, P\}$

H – проверочная матрица ОРС-кода размера $(n - k) \times n$

S – некоторая случайная невырожденная матрица размера $(n - k) \times (n - k)$

P – случайная перестановочная матрица размера $n \times n$

Открытый ключ: $H_{pub} = SHP$

Шифрование: $c = H_{pub} e = SHPe, d_H(e) \le \left\lfloor \frac{n-k}{2} \right\rfloor$

Расшифрование: 1) $S^{-1}c = HPe = H\tilde{e}$

2) Запускаем алгоритм быстрого декодирования и находим $\tilde{e}$

3) $P^{-1}\tilde{e} = e$

Возможные улучшения криптосистемы Нидеррайтера

1) Введение скрывающей матрицы X еденичного ранга в секретный ключ, тогда $H_{pub} = S(H + X)P$

2) Применение $\mathcal{F}$-метрики для улучшения криптосистемы Нидеррайтера, используя скрывающую матрицу большего ранга

Модификация криптосистемы Нидеррайтера

1) Легальный пользователь выбирает матрицу F, столбцы которой задают $\mathcal{F}$-метрику. Родительский код с проверочной матрицей F должен обладать быстрым алгоритмом декодирования в метрике Хэмминга

2) Выбирается транспонированная порождающая матрица G^{τ} некоторого линейного кода, обладающего быстрым алгоритмом декодирования в заданной $\mathcal{F}$-метрике

Секретный ключ: $\{F, G^{\tau}, S, P\}$

S – случайная невырожденная матрица порядка n

P – случайная перестановочная матрица порядка N

Открытый ключ: $H_{pub} = S(F + G^{\tau}U)P$

U – случайная матрица размера $k \; x \; N$

Сообщение $m = (m_1, m_2, ..., m_N)^{\tau}, m_i \in \mathbf{F}_q, d_H(m) = t_{\min} = \min\{t_k, t_p\}$

t_k - корректирующая способность кода, задаваемого G^{τ} в пространстве с $\mathcal{F}$-метрикой

t_p - корректирующая способность родительского кода

Модификация криптосистемы Нидеррайтера

Шифрование: $c = H_{pub} m = S(F + G^{\tau} U) P m = S(F + G^{\tau} U)\tilde{m} =$

$= S(\tilde{m}_1 (f_1 + G_1) + \tilde{m}_2 (f_2 + G_2) + \ldots + \tilde{m}_N (f_N + G_N)) = S(g + e),$

$\tilde{m} = Pm,\ f_i, G_i$ - столбцы матриц F и $G^{\tau} U$ соответственно.

Расшифрование: 1) $S^{-1} c = g + e$

2) С помощью быстрого алгоритма декодирования в $\mathcal{F}$-метрике находим g и e

3) С помощью быстрого алгоритма декодирования в метрике родительского кода находим $\tilde{m}$

4) Вычисляем $P^{-1}\tilde{m} = m$

Если $U = VF \Rightarrow H = S(E_n + G^{\tau} V) F P$

Литература

- Габидулин Е.М., Обернихин В.А. Коды в $\mathcal{F}$-метрике Вандермонда и их применение // Пробл. передачи информ. 2003. Т. 39. № 2. С. 3-14.
- Габидулин Э.М., Симонис Ю. Совершенные коды для метрик, порождаемых примитивными двоичными БЧХ-кодами, исправляющими двойные ошибки / / Пробл. передачи информ. 1999. Т. 35. № 3. С. 40-47.
- Берлекэмп Э. Алгебраическая теория кодирования.
- Сидельников В.М. Теория кодирования