Коды и их связь с решётками — лекция 3

Предварительная версия от 28 июля 2010 г.

В. А. Клепцын

Определение 1. (*Двоичным*) *кодом* называется произвольное подмножество $C \subset \mathbb{F}_2^n$.

Определение 2. (Двоичный) код $C \subset \mathbb{F}_2^n$ называется *линейным*, если C — линейное подпространство.

Определение 3. *Весом* $w(v)$ вектора $v \in \mathbb{F}_2^n$ называется число его ненулевых координат.

Определение 4. *Расстоянием Хэмминга* $d(u, v)$ между двумя векторами u, $v \in \mathbb{F}_2^n$ называется число координат, в которых u и v отличаются.

Задача 1. $d(u, v) = w(u + v)$.

Определение 5. *Наименьшим расстоянием* для кода C называется величина $d(C) = \min\limits_{\substack{u \neq 0, \\ u,\, v \in C}} d(u, v)$.

Задача 2. Если код C линейный, то $d(C) = \min\limits_{u \in C \setminus \{0\}} w(u)$.

Определение 6. Говорят, что линейный код C *типа* (n, k, r), если $C \subset \mathbb{F}_2^n$, $\dim C = k$, $\min\limits_{u \in C \setminus \{0\}} w(u) = r$.

Определение 7. *Порождающая матрица* для кода $C \subset \mathbb{F}_2^n$, $\dim C = k$ — матрица $k \times n$, по строкам которой написаны элементы какого-нибудь базиса C.

Задача 3. Какие из следующих кодов линейны? Какие в них наименьшие расстояния? Для линейных кодов найдите их размерность.

a) $\{0, 1\}$;

b) $\{00, 11\}$;

c) $\{001, 110\}$;

d) $\{000, 110, 011\}$;

e) $\{000, 110, 101, 011\}$.

С этого момента мы будем работать только с линейными кодами, особо этого не оговаривая.

А как проверить, что пришедшее сообщение пришло без ошибок?

Определение 8. *Скалярное произведение* — отображение $\langle \cdot, \cdot \rangle \colon \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$, определяемое как $\langle u, v \rangle = \sum_{j=1}^{n} u_j v_j$.

Определение 9. *Проверочной матрицей* кода C называется матрица, строки которой — базис ортогонального дополнения $C^\perp = \{u \in \mathbb{F}_2^n \mid \forall v \in C \ \langle u, v \rangle = 0\}$.

Задача 4. Наименьший вес $d(C)$ равен наименьшему числу линейно зависимых столбцов проверочной матрицы.

Перейдем теперь к геометрическим свойствам кодов:

Определение 10. *Двойственным кодом* к коду C называется код $C^\perp = \{u \in \mathbb{F}_2^n \mid \forall v \in C \langle u, v \rangle = 0\}$.

Определение 11. Код C называется

a) *изотропным*, если $C \subset C^\perp$;

b) *самодвойственным*, если $C = C^\perp$;

c) *четным*, если вес любого его элемента четен;

d) *дважды четным*, если вес любого его элемента делится на 4.

Задача 5. Дважды четный код изотропен.

А как, собственно, связаны коды и решетки?

Определение 12. Пусть $C \subset \mathbb{F}_2^n$ — линейный код. Определим соответствующую ему решетку как

$$\Lambda_C = \frac{1}{\sqrt{2}} p^{-1}(C),$$

где $p \colon \mathbb{Z}^n \to \mathbb{F}_2^n = (\mathbb{Z}/2\mathbb{Z})^n$ — отображение приведения по модулю 2.

Задача 6. Λ_C — решетка.

Задача 7. Как будут выглядеть решетки Λ_C для линейных кодов C из задачи 3?

Посмотрим на связь свойства кода и соответствующей ему решетки:

Задача 8. Код C:
a) изотропен $\Leftrightarrow$ решетка Λ_C целая;
b) дважды четен $\Leftrightarrow$ решетка Λ_C четная;
c) имеет размерность $n/2$ $\Leftrightarrow$ решетка Λ_C унимодулярна.

Построим еще один очень интересный код:

Определение 13. *Код Хэмминга* — код с порождающей матрицей

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Задача 9. Покажите, что матрица

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

— проверочная для кода Хэмминга.

Задача 10. Проверьте, что наименьший вес в коде Хэмминга равен 3. и код, тем самым, имеет тип $(7, 4, 3)$.

Код Хэмминга — не изотропный и не четный. Однако, к нему можно добавить последний бит — «бит контроля четности».

Определение 14. Пополненный код Хэмминга $C_{\overline{\text{H}}}$ — код с порождающей матрицей

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Задача 11. a) Пополненный код Хэмминга — дважды четный код половинной размерности.
b) Решетка $\Lambda_{\overline{\text{H}}}$ — четная самодвойственная решетка в размерности 8.
c) Опишите корни этой решетки; сколько их?
d) Попробуйте определить тип этой системы корней (ответ: E_8).

Таким — более симметричным — образом мы, на самом деле, построили уже один раз виденную решетку Γ_8.

Определение 15. *Перечисляющий многочлен* кода $C \subset \mathbb{F}_2^n$ — однородный многочлен степени n от двух переменных X и Y:

$$P_C(X,Y) = \sum_{u \in C} X^{w(u)} Y^{n-w(u)} = \sum_{j=0}^{n} \#\{u \in C \mid w(u) = j\} \cdot X^j Y^{n-j}.$$

Задача 12. Найдите перечисляющие многочлены кодов:

a) из задачи 3b;

b) из задачи 3e;

c) кода контроля четности $\{u \mid w(u) \vdots 2\}$;

d) кода Хэмминга.

Следующая серия задач посвящена исследованию дважды четных самодвойственных кодов. Для начала мы найдем, как для произвольного кода C связаны P_C и $P_{C^\perp}$.

Задача 13. a) Пусть $C \subset \mathbb{F}_2^n$ — код, $u \in \mathbb{F}_2^n$. Тогда в наборе $\{\langle v, u\rangle \mid v \in C\}$ либо все нули (если $u \in C^\perp$), либо половина нули, а половина — единицы (если $u \notin C^\perp$),

b) Выведите из этого, что

$$\frac{1}{|C|} \sum_{v \in C} (-1)^{\langle u, v\rangle} = \begin{cases} 1, & u \in C^\perp, \\ 0, & u \notin C^\perp. \end{cases}$$

Задача 14. Докажите, что

$$P_{C^\perp}(X,Y) = \frac{1}{|C|} P_C(Y - X, Y + X).$$

Но мы знаем, что самодвойственный код имеет половинную размерность, $\dim C = n/2$. Отсюда несложно вывести следующие утверждения:

Задача 15. Пусть $C \subset \mathbb{F}_2^n$ — самодвойственный код. Тогда

a) $P_C(X,Y) = P_C\left(\dfrac{Y-X}{\sqrt{2}}, \dfrac{Y+X}{\sqrt{2}}\right)$;

b) $P_C(X,Y) = P_C(-X,Y) = P_C(Y,-X)$;

c) P_C инвариантен относительно группы G, порожденной

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} -X \\ Y \end{pmatrix}, \quad \begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} X \\ -Y \end{pmatrix}, \quad \begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} \dfrac{Y-X}{\sqrt{2}} \\ \dfrac{X+Y}{\sqrt{2}} \end{pmatrix}.$$

Что это за группа?

Ответ. Это группа симметрий правильного восьмиугольника.