Лекция 8

Соотношения между параметрами линейных и нелинейных кодов

16 апреля 2011 г.

Обозначение: $(n, k, d)_q$–код и $[n, M, d]_q$–код

Обозначение

- (n, k)–код $\equiv$ линейный код длины n и размерности k
- $(n, k, d)_q$–код $\equiv$ линейный код длины n, размерности k, с кодовым расстоянием d над полем $\mathbb{F}_q$
- $[n, M, d]_q$–код $\equiv$ не обязательно линейный код длины n, мощности M, с кодовым расстоянием d над полем $\mathbb{F}_q$

- если $q = 2$, то индекс пропускается:
  (n, k, d)–код — это $(n, k, d)_2$–код,
  $[n, M, d]$–код — это $[n, M, d]_2$–код;
- $(n, k, d)_q$–код является $[n, M = q^k, d]_q$–кодом;
- обратное, вообще говоря, неверно:
  не всякий $[n, q^k, d]_q$–код линеен

Определение величины $m_q(n, d)$

Определение

Обозначим через $m_q(n, d)$ наибольшую мощность кода над $\mathbb{F}_q$ длины n с расстоянием d (не обязательно линейного)

$$m_q(n, d) = \max_{\substack{\mathcal{C} \subseteq \mathbb{F}_q^n \\ d(\mathcal{C}) = d}} |\mathcal{C}|.$$

Код длины n с расстоянием d мощности $m_q(n, d)$ над полем $\mathbb{F}_q$ называется кодом максимальной мощности.

Замечание

В случае $q = 2$ будем использовать запись $m(n, d) = m_2(n, d)$.

Пример: $m_q(n, n) = q$.

Границы сферической упаковки

Пусть $\tilde{\alpha} \in \mathbb{F}_q^n$.
Обозначение: $V_t = V_q(t) = |B_t(\tilde{\alpha})| = \sum_{k=0}^{t} \binom{n}{k}(q-1)^k$.

Теорема (Хемминг, Гилберт)

$$\frac{q^n}{V_{2t}} \leqslant m_q(n, 2t+1) \leqslant \frac{q^n}{V_t}$$

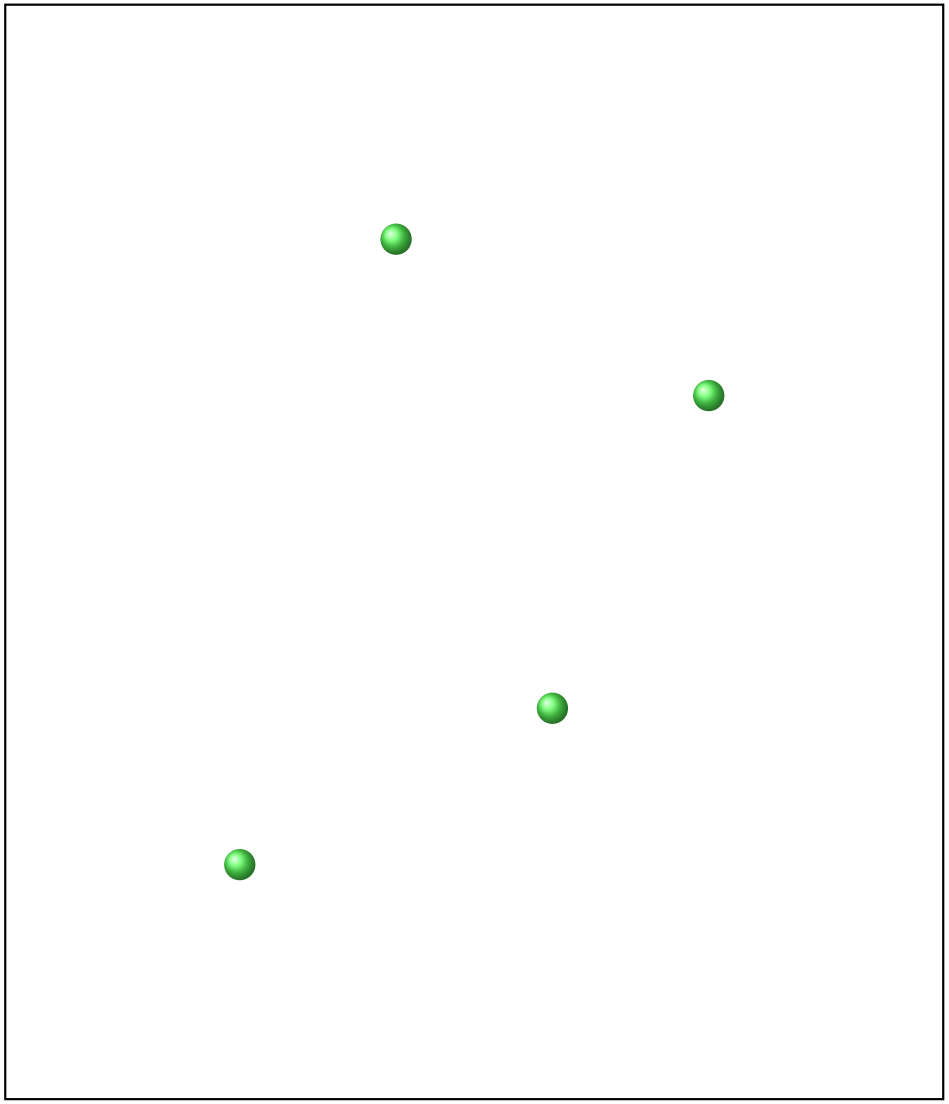
Определение

Если для кода $\mathcal{C} \subset \mathbb{F}_q^n$, исправляющего t ошибок, выполнено равенство $|\mathcal{C}| = \frac{q^n}{V_t}$, то код $\mathcal{C}$ называется совершенным кодом.

Пример

Код $\mathcal{C} = \{000, 111\} \subset \{0,1\}^3$ — совершенный.

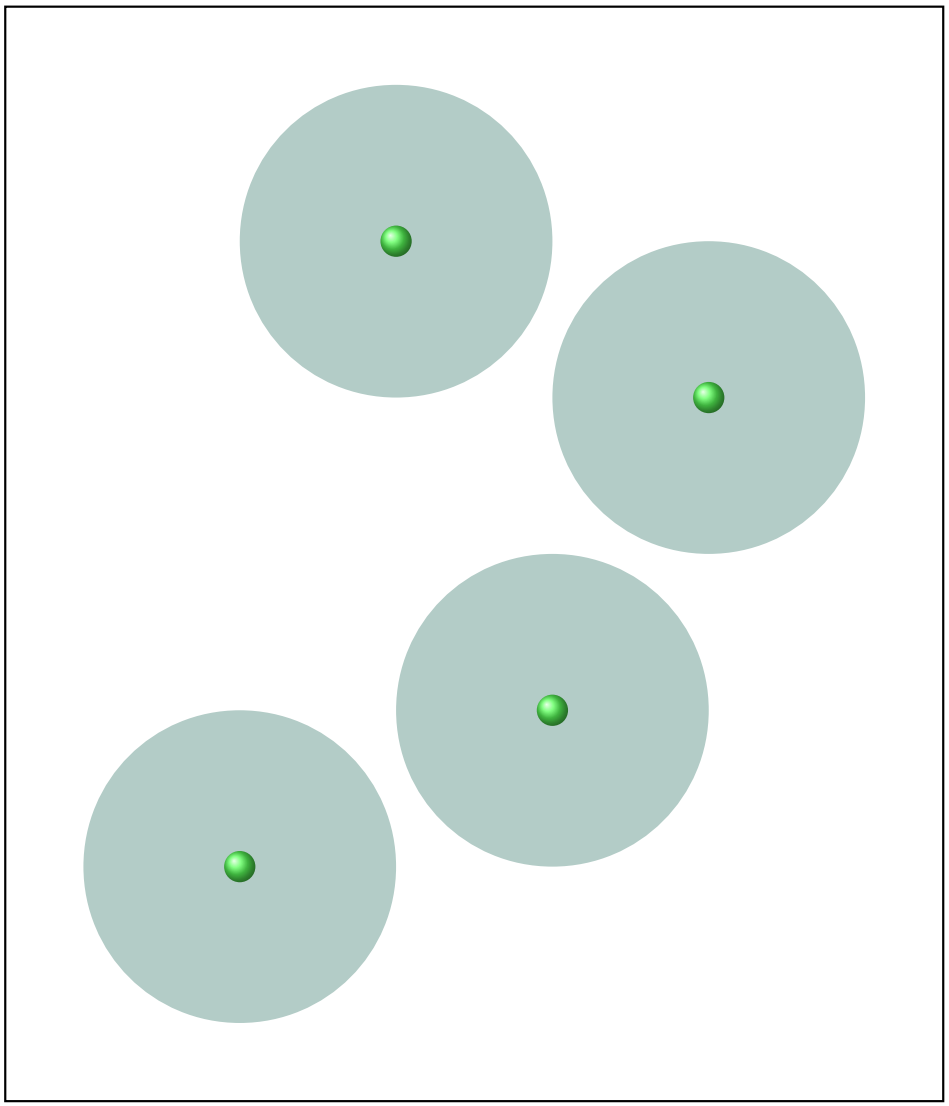
Доказательство неравенства Хемминга



$$\mathcal{C} = \{x_1, \ldots, x_m\} \subseteq \mathbb{F}_q^n$$

q-ичный код длины n, содержащий m кодовых слов и исправляющий t ошибок.

Доказательство неравенства Хемминга

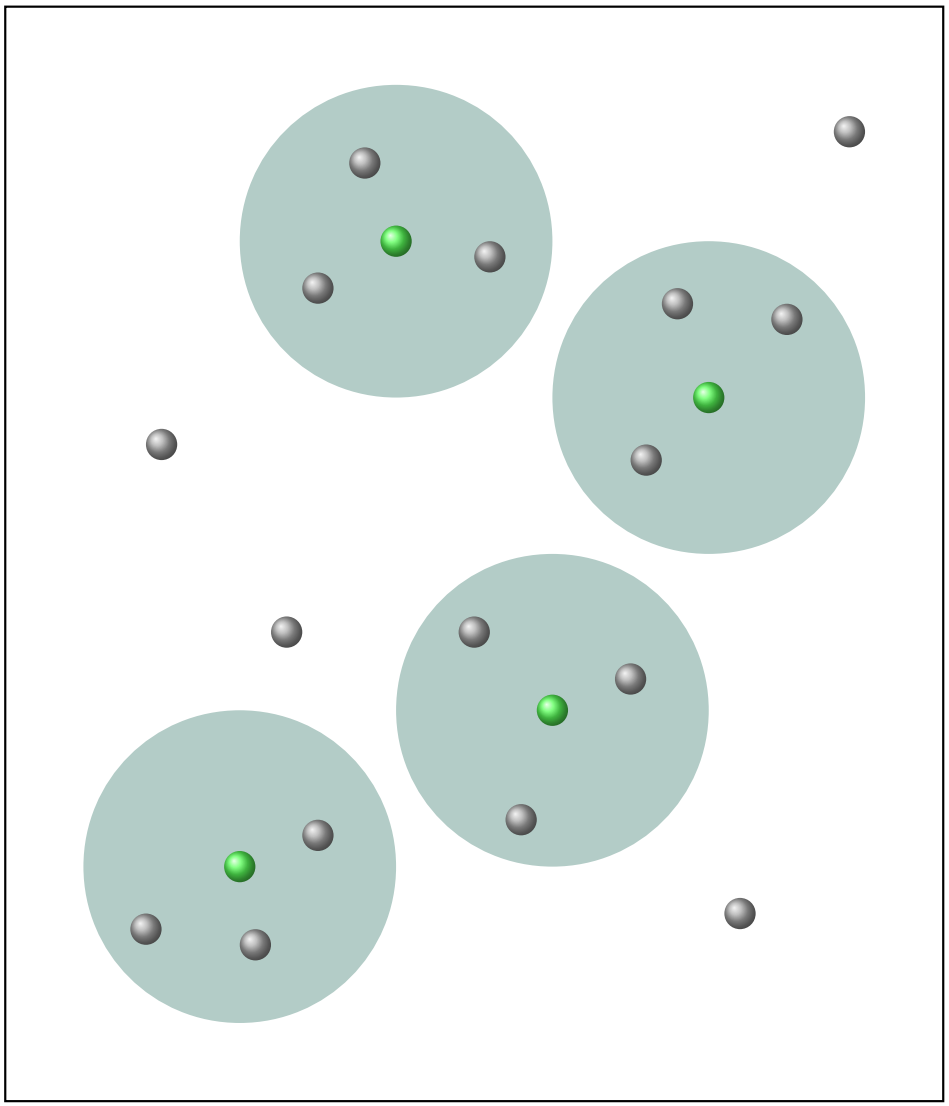


Шары радиуса t с центрами в кодовых словах не пересекаются. Каждый из этих шаров имеет объём

$$V_q(t) = |B_t(\cdot)| =$$

$$= \sum_{r=0}^{t} \binom{n}{r} (q-1)^r.$$

Доказательство неравенства Хемминга



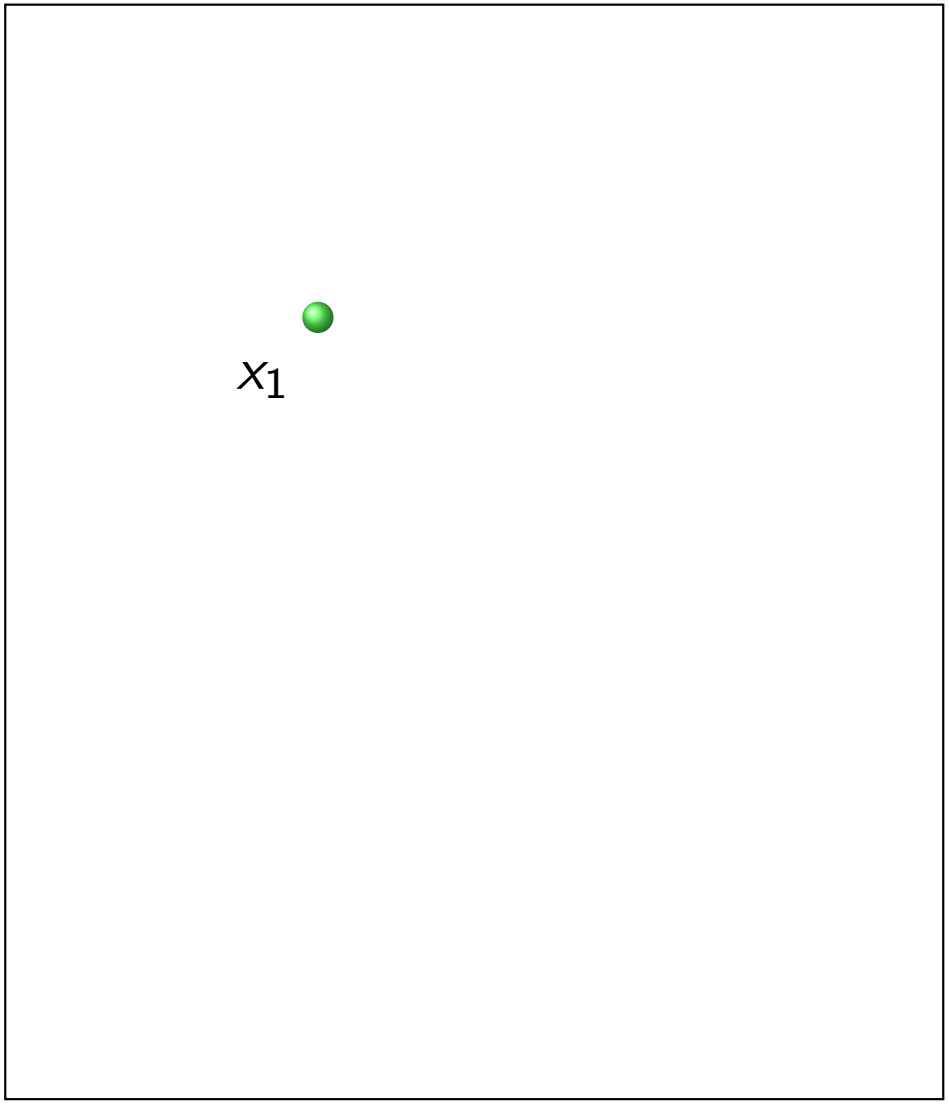
$$\left.\begin{array}{l} |\mathbb{F}_q^n| = q^n \\ \bigcup_{i=1}^{m} B_t(x_i) \subseteq \mathbb{F}_q^n \end{array}\right\} \Rightarrow$$

$$\Rightarrow \quad m \cdot V_q(t) \leqslant q^n$$

$$\Rightarrow \quad m \leqslant \frac{q^n}{V_q(t)}$$

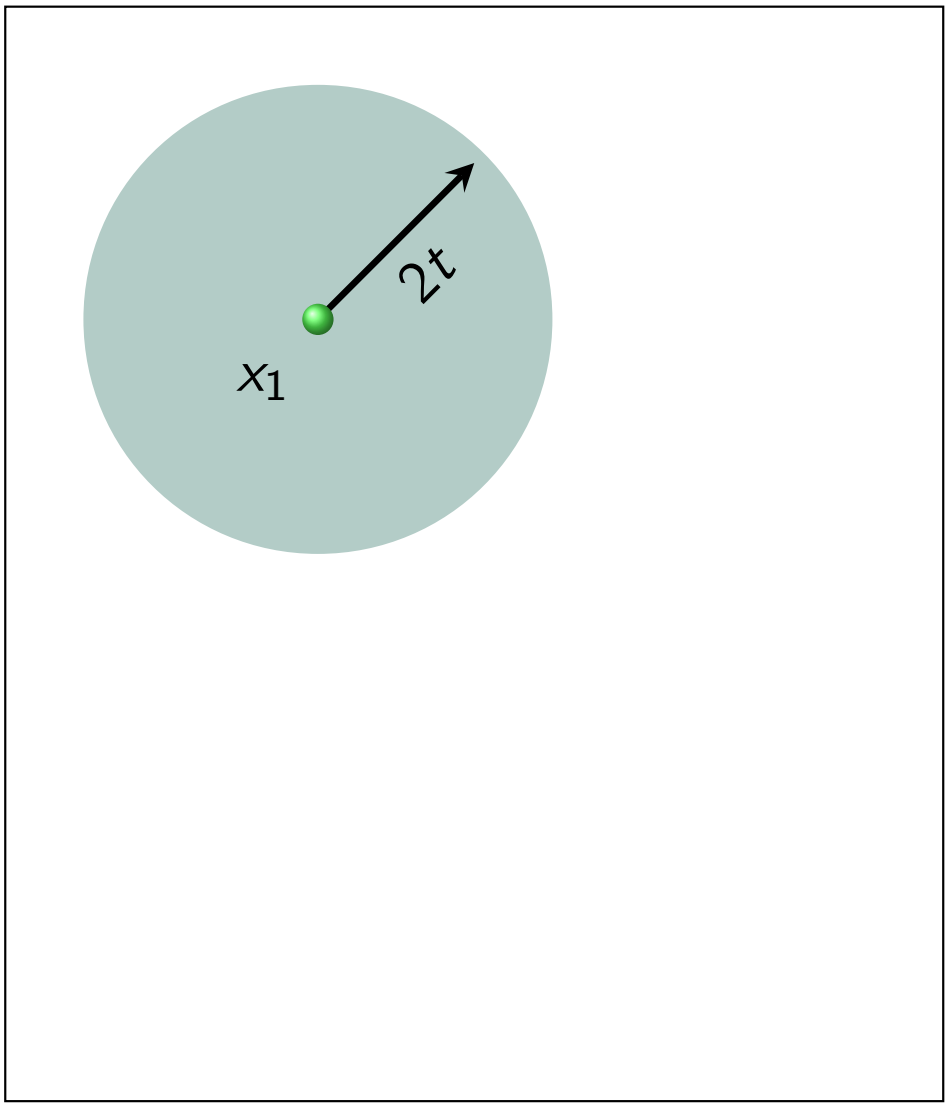
ч.т.д.

Доказательство неравенства Гильберта



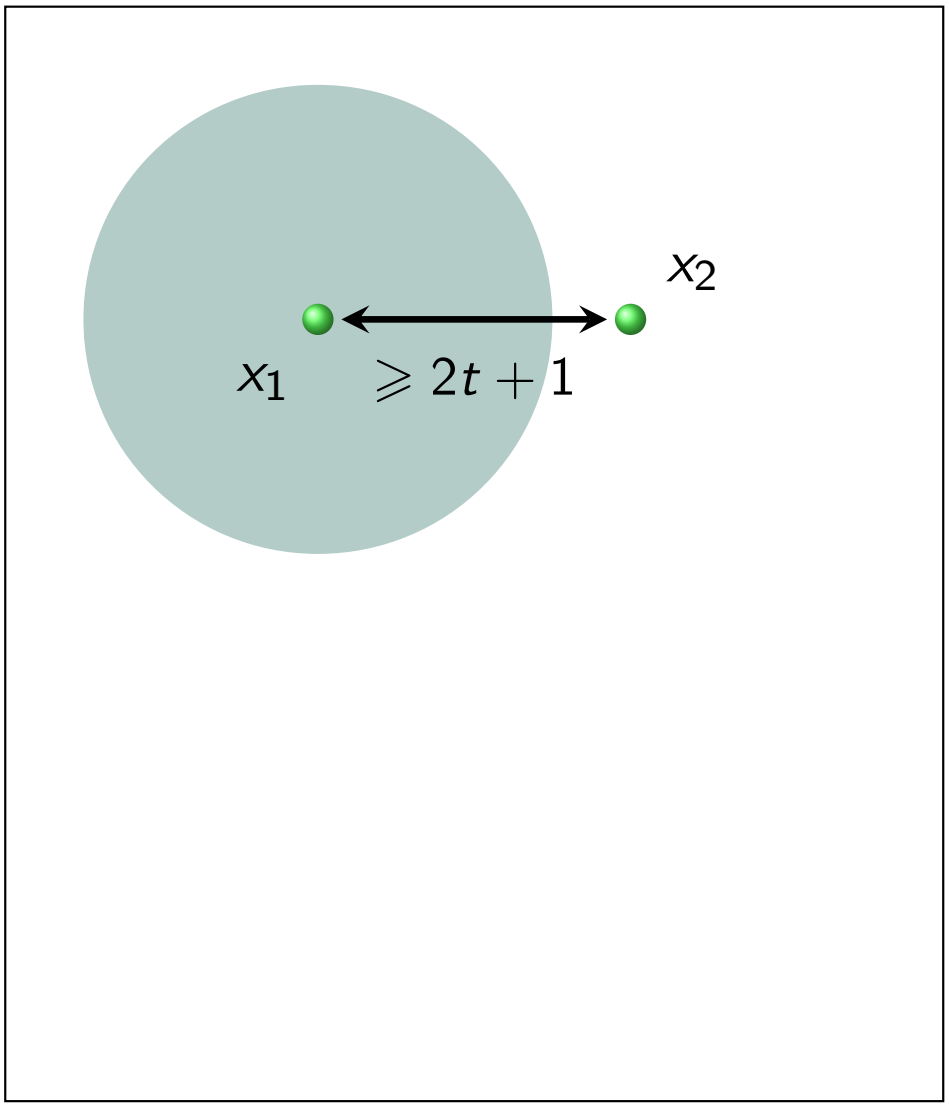
Возьмём произвольную точку $x_1 \in \mathbb{F}_q^n$

Доказательство неравенства Гильберта



Шар $B_{2t}(x_1)$

Доказательство неравенства Гильберта

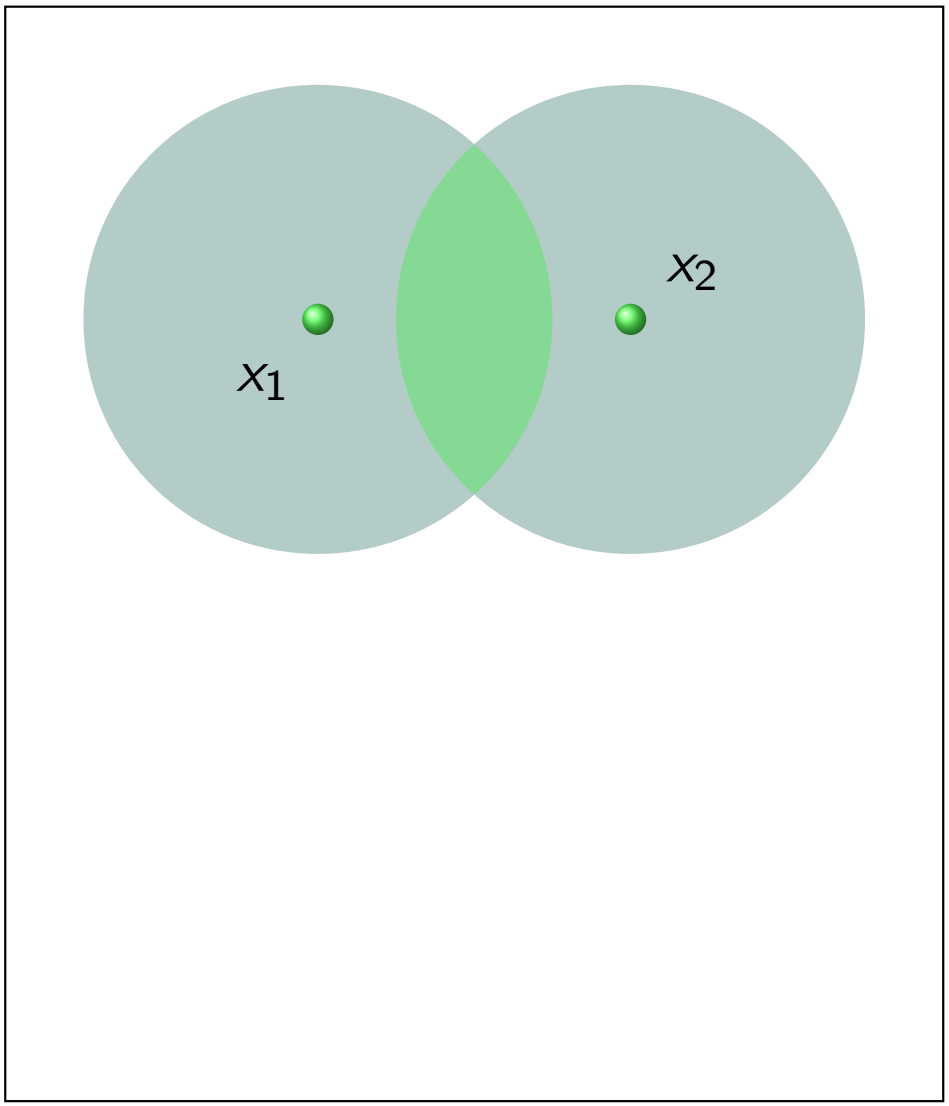


$x_2 \notin B_{2t}(x_1)$

$\Rightarrow \; d(x_1, x_2) \geqslant 2t+1$

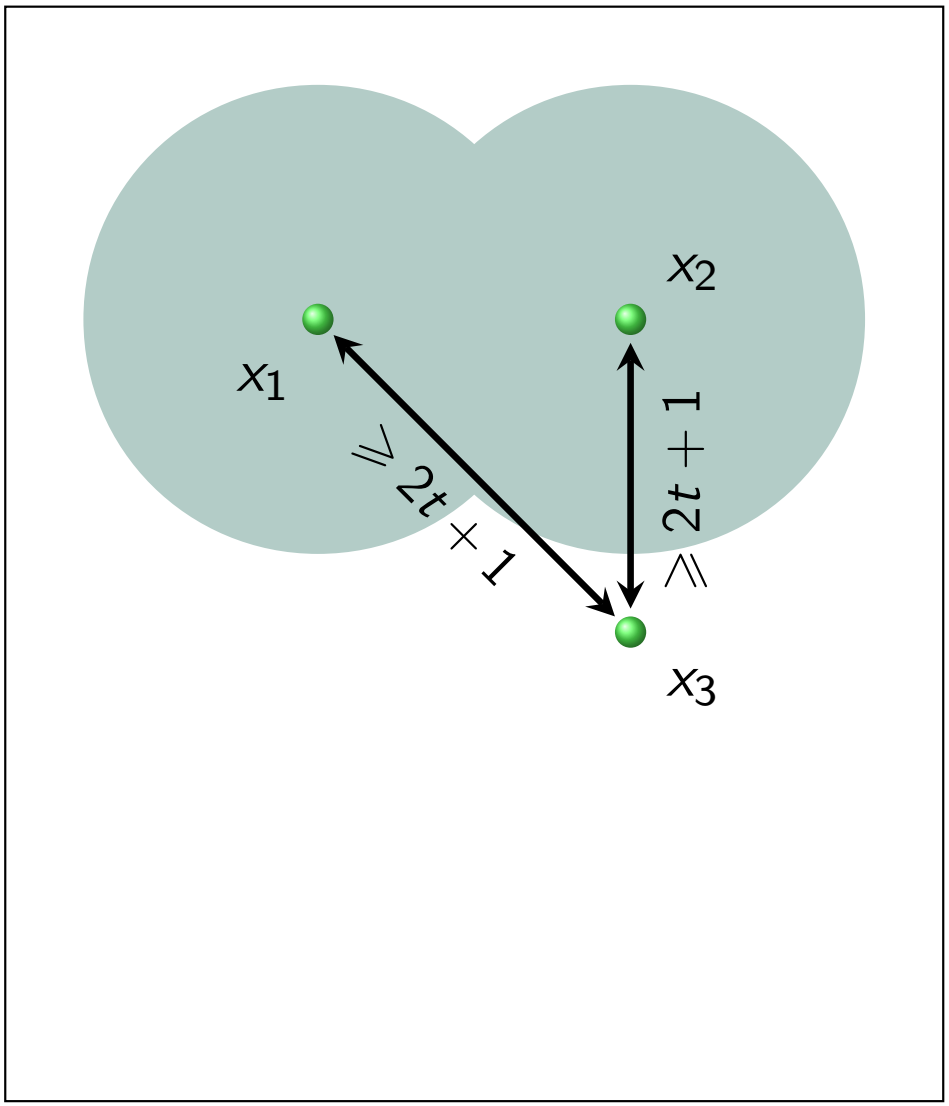
$\Rightarrow \; \mathcal{C}_2 = \{x_1, x_2\}$
исправляет t ошибок.

Доказательство неравенства Гильберта



$$B_{2t}(x_1) \cup B_{2t}(x_2)$$

Доказательство неравенства Гильберта

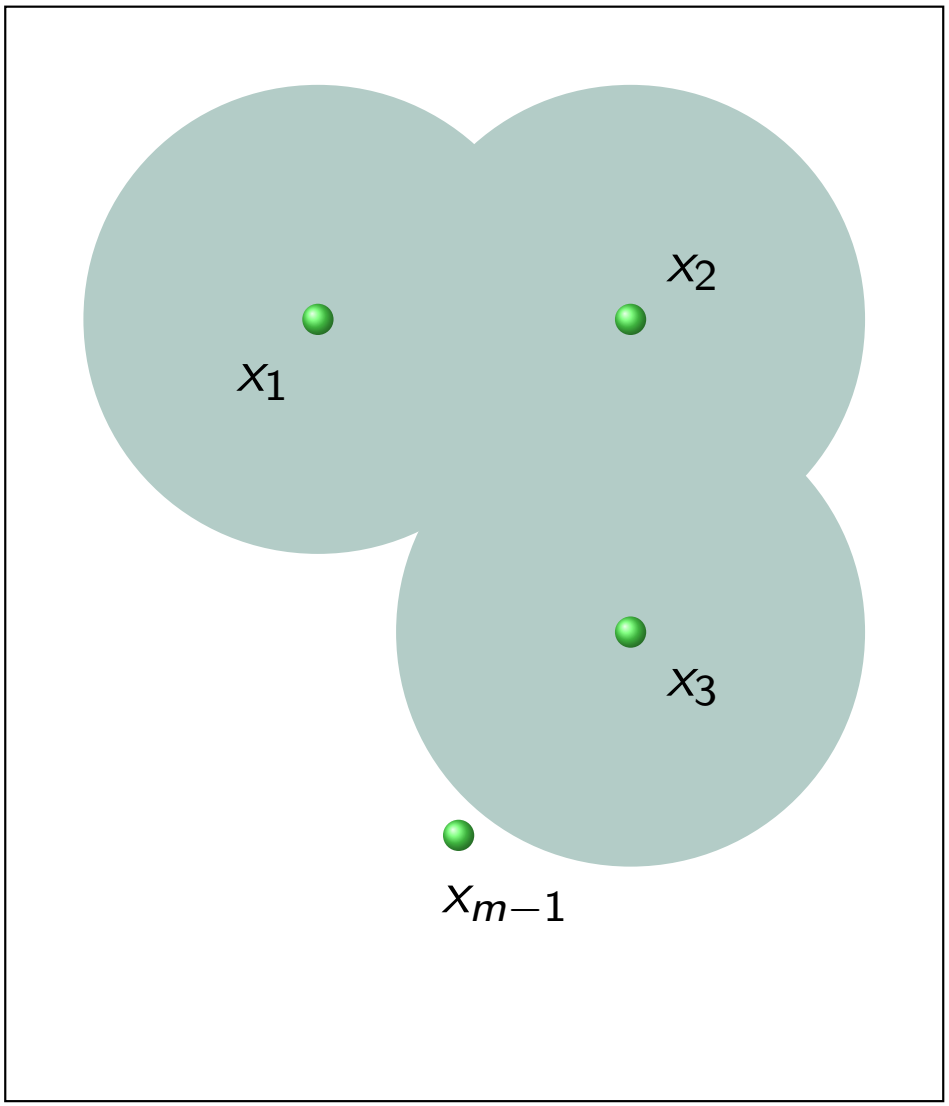


$$x_3 \notin B_{2t}(x_1) \cup B_{2t}(x_2)$$

$$\Rightarrow \begin{cases} d(x_3, x_1) \geqslant 2t+1 \\ d(x_3, x_2) \geqslant 2t+1 \end{cases}$$

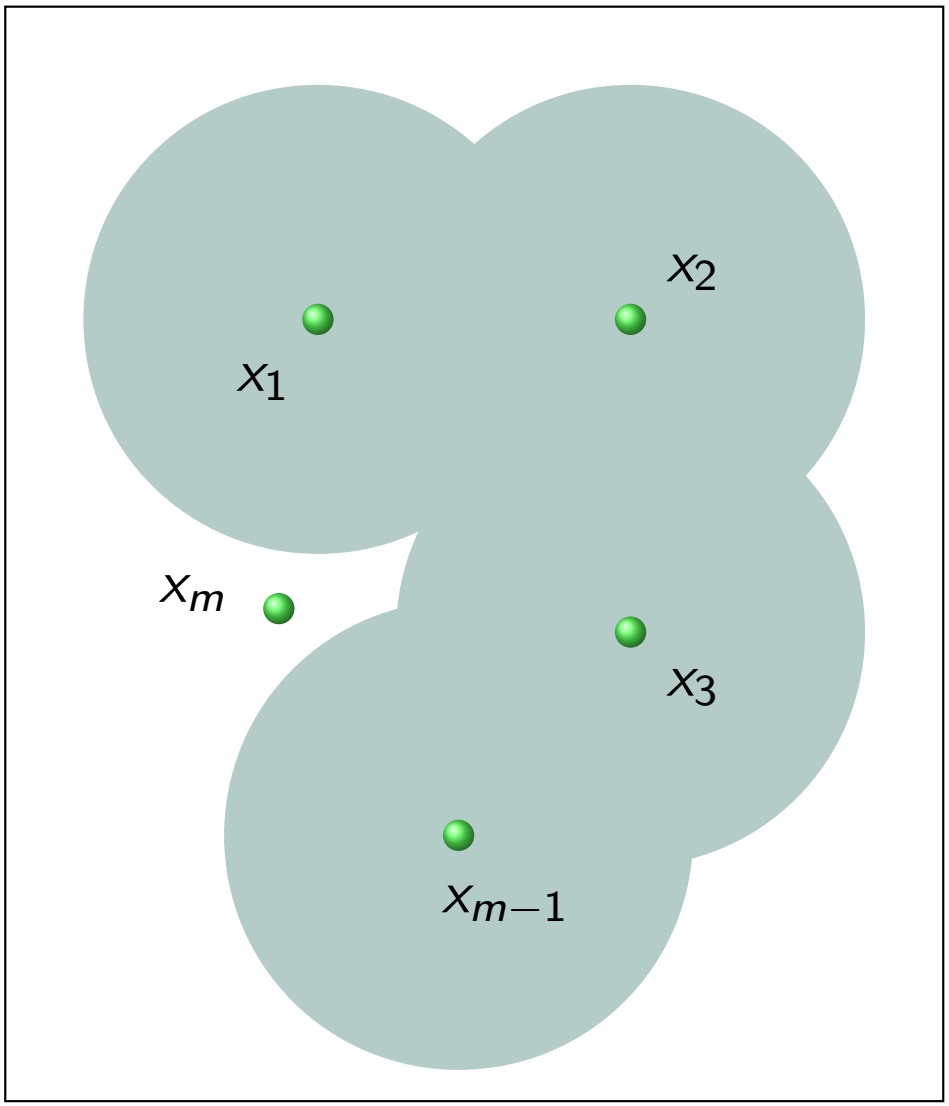
$\Rightarrow$ $C_3 = \{x_1, x_2, x_3\}$
исправляет t ошибок.

Доказательство неравенства Гильберта



. . . и так далее.

Доказательство неравенства Гильберта

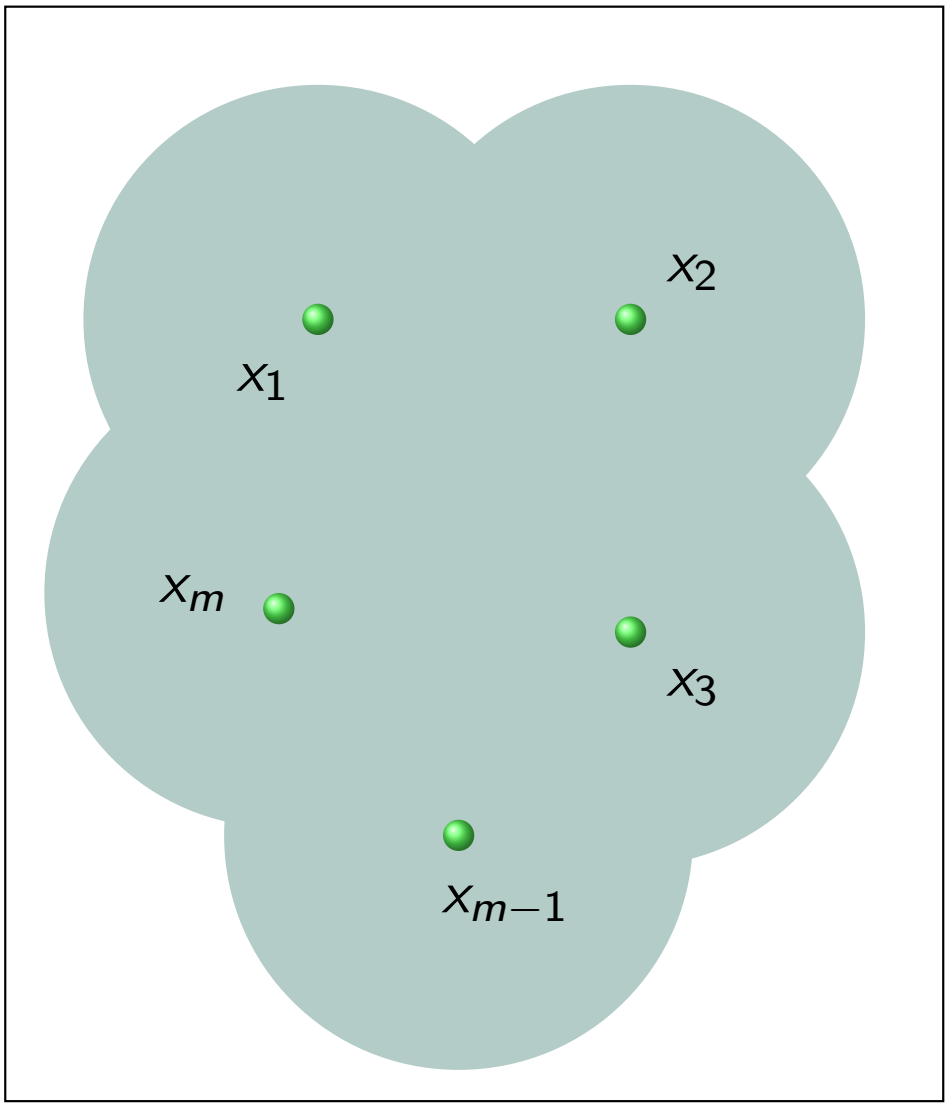


Выбраны $x_1, \ldots, x_{m-1}$,
т.ч. $d(x_i, x_j) \geqslant 2t + 1$;

очередная точка

$$x_m \notin \bigcup_{i=1}^{m-1} B_{2t}(x_i).$$

Доказательство неравенства Гильберта

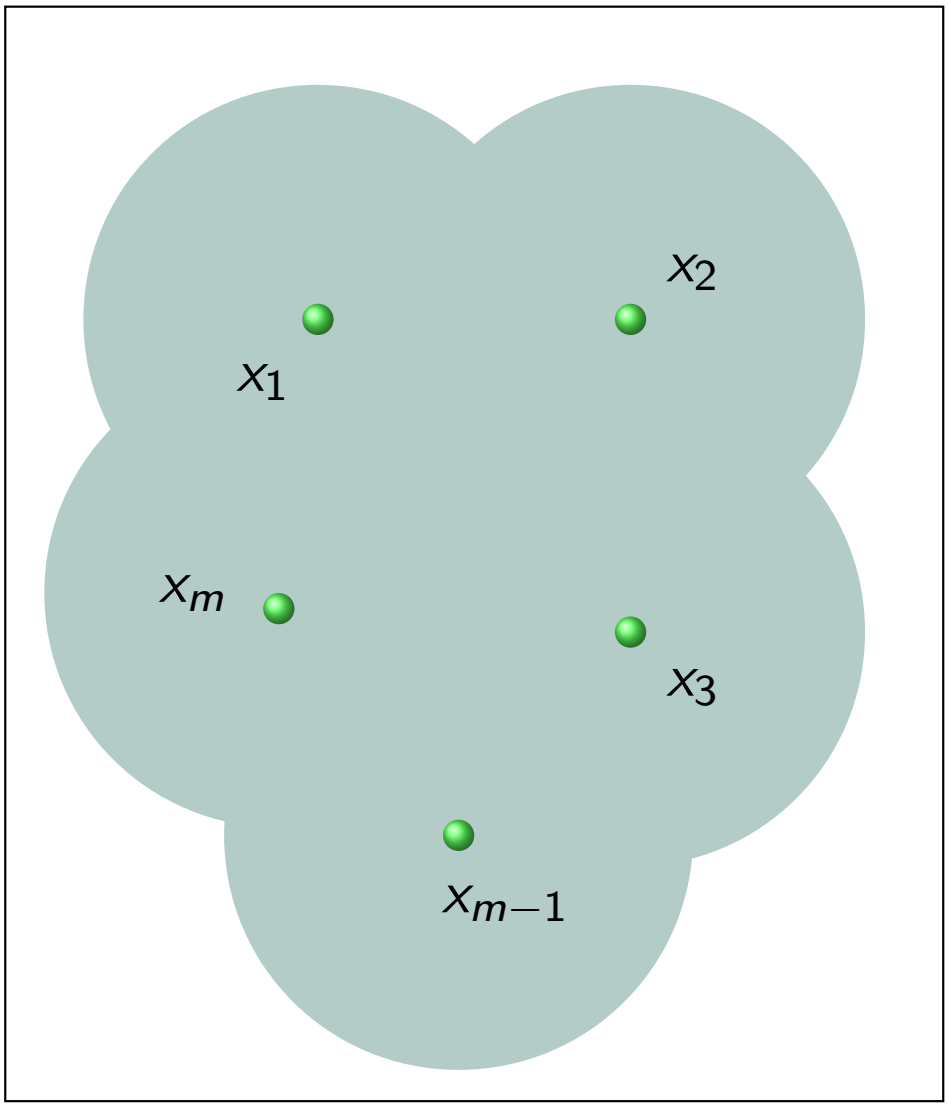


Процесс закончится на таком m, когда

$$\mathbb{F}_q^n = \bigcup_{i=1}^{m} B_{2t}(x_i),$$

и будет получен код $\mathcal{C}_m = \{x_1 \dots x_m\}$, исправляющий t ошибок.

Доказательство неравенства Гильберта



$$|\mathbb{F}_q^n| = \left|\bigcup_{i=1}^{m} B_{2t}(x_i)\right| \leqslant$$

$$\leqslant \sum_{i=1}^{m} |B_{2t}(x_i)| =$$

$$= m \cdot V_{2t}$$

$$\Rightarrow \quad m \geqslant \frac{q^n}{V_{2t}}.$$

ч.т.д.

Граница Хемминга (для линейных кодов)

- Верхняя граница сферической упаковки:
  если $\mathcal{C} \subset \mathbb{F}_q^n$ — произвольный (не обязательно линейный) код длины n, исправляющий t ошибок, то

$$|\mathcal{C}| \leqslant \frac{q^n}{V_t}$$

- $V_t = \sum_{j=0}^{t} \binom{n}{j} (q-1)^j$ — объём шара
- если код $\mathcal{C}$ линеен, то $|\mathcal{C}| = q^k$
- отсюда, логарифмируя, получаем теорему:

Теорема

Если $\mathcal{C}$ — линейный (n, k)-код над полем $\mathbb{F}_q$, исправляющий t ошибок, то

$$k \leqslant n - \log_q \sum_{j=0}^{t} \binom{n}{j} (q-1)^j.$$

Пример применения неравенства Хемминга

Задача (на засыпку)

Существует ли двоичный код длины 10 из 60 кодовых слов с кодовым расстоянием 4?

Решение:

Перебором: $\binom{1024}{60} > 8 \cdot 10^{73}$; $\quad \dfrac{2^{10}}{V_{\lfloor \frac{4-1}{2} \rfloor}} = \dfrac{2^{10}}{V_1} = \dfrac{1024}{11} > 60$?

Пусть существует искомый код $\mathcal{C}$ с параметрами $n = 10$ и $d = 4$. Рассмотрим его укороченный код

$$\mathcal{C}' = \{(\alpha_1, \ldots, \alpha_9) : (\alpha_1, \ldots, \alpha_{10}) \in \mathcal{C}\}.$$

Тогда $d(\mathcal{C}') \geqslant d(\mathcal{C}) - 1 = 3$, и значит

$$|\mathcal{C}'| \leqslant \frac{2^9}{V_1} = \frac{2^9}{1+9} = \frac{512}{10} = 51{,}2 < 60 \text{ — противоречие.} \qquad \square$$

Укороченный код

Пусть $\mathcal{C} \subset \mathbb{F}_q^n$ — некоторый код длины n с кодовым расстоянием d. Рассмотрим его кодовую таблицу:

$\mathcal{C} =$

1	2	3	4	5	6

$\rightsquigarrow$ $\mathcal{C}' =$

1	2	4	5

Определение

Код $\mathcal{C}'$ с кодовой таблицей, полученной из таблицы кода $\mathcal{C}$ выбрасыванием некоторых столбцов $i_1, \ldots, i_k$, называется укорочением кода $\mathcal{C}$ с выбрасыванием разрядов $i_1, \ldots, i_k$.

Замечание

Если код $\mathcal{C}'$ получен из кода $\mathcal{C}$ выбрасыванием m разрядов, то

$$d(\mathcal{C}') \geqslant d(\mathcal{C}) - m.$$

Код с проверкой на чётность

Определение

Пусть $\mathcal{C} \in \{0,1\}^n$ — некоторый код. Тогда говорят, что код

$$\mathcal{C}' = \{(\alpha_1, \ldots, \alpha_{n+1}) : (\alpha_1, \ldots, \alpha_n) \in \mathcal{C}, \alpha_{n+1} = \alpha_1 \oplus \ldots \oplus \alpha_n\}$$

получен из кода $\mathcal{C}$ добавлением проверки на чётность.

Пример

$\mathcal{C} = \{100, 011\} \quad \Rightarrow \quad \mathcal{C}' = \{1001, 0110\}$

Замечание

- $|\mathcal{C}'| = |\mathcal{C}|$
- $d(\mathcal{C}') \geqslant d(\mathcal{C})$
- $\forall\, \tilde{\alpha} \in \mathcal{C}' \ : \ \|\tilde{\alpha}\|$ — чётно
  (т.к. $\alpha_1 \oplus \ldots \oplus \alpha_n \oplus \alpha_{n+1} = (\alpha_1 \oplus \ldots \oplus \alpha_n) \oplus (\alpha_1 \oplus \ldots \oplus \alpha_n) = 0$)

Основное свойство добавления проверки на чётность

Утверждение

Пусть $\mathcal{C}' \in \{0,1\}^{n+1}$ получен из $\mathcal{C} \in \{0,1\}^n$ добавлением проверки на чётность и пусть $d = d(\mathcal{C})$. Тогда $d(\mathcal{C}') = d + 1$ при нечётном d.

Доказательство:

Рассмотрим произвольные $\tilde{\alpha}', \tilde{\beta}' \in \mathcal{C}'$:

$$\tilde{\alpha}' = (\alpha_1, \ldots, \alpha_n, \alpha_{n+1}) = (\tilde{\alpha}, \alpha_{n+1}), \quad \tilde{\alpha} \in \mathcal{C},$$

$$\tilde{\beta}' = (\beta_1, \ldots, \beta_n, \beta_{n+1}) = (\tilde{\beta}, \beta_{n+1}), \quad \tilde{\beta} \in \mathcal{C}.$$

- Если $d(\tilde{\alpha}, \tilde{\beta}) > d$, то $d(\tilde{\alpha}', \tilde{\beta}') \geqslant d(\tilde{\alpha}, \tilde{\beta}) \geqslant d + 1$.
- Если $d(\tilde{\alpha}, \tilde{\beta}) = d$, то $\alpha_{n+1} = \overline{\beta}_{n+1}$ и

$$d(\tilde{\alpha}', \tilde{\beta}') = d(\tilde{\alpha}, \tilde{\beta}) + (\alpha_{n+1} \oplus \beta_{n+1}) = d + 1. \qquad \square$$

Простое свойство кодовой таблицы

Лемма

$$m(n-1,d) \geqslant \frac{1}{2} m(n,d)$$

Доказательство:

Рассмотрим кодовую таблицу кода $\mathcal{C}$, $d(\mathcal{C}) = d$, $|\mathcal{C}| = m(n,d)$:

$$\mathcal{C} = \begin{array}{|c|c|} \hline 0 & \mathcal{C}' \\ \hline 1 & \mathcal{C}'' \\ \hline \end{array}.$$

1. $\mathcal{C} = 0\mathcal{C}' \cup 1\mathcal{C}''$
2. $d(\mathcal{C}'), d(\mathcal{C}'') \geqslant d$
3. Один из кодов $\mathcal{C}', \mathcal{C}''$ содержит по крайней мере половину строк кодовой таблицы; без ограничения общности это код $\mathcal{C}'$.

Тогда $m(n-1,d) \geqslant |\mathcal{C}'| \geqslant \frac{1}{2}|\mathcal{C}| = \frac{1}{2} m(n,d)$. □

Неравенство Синглтона

Теорема

$$\forall \mathcal{C} \subset \{0,1\}^n : \quad d(\mathcal{C}) \leqslant n - \log_2 |\mathcal{C}| + 1$$

Доказательство:
Применим предыдущую лемму $(n-d)$ раз:

$$\begin{aligned} m(n,d) &\leqslant 2 \cdot m(n-1,d) \leqslant \\ &\leqslant 2^2 \cdot m(n-2,d) \leqslant \ldots \leqslant \\ &\leqslant 2^{n-d} \cdot m(d,d) = \\ &= 2^{n-d} \cdot 2 = 2^{n-d+1}. \end{aligned}$$

Прологарифмируем: $\log_2 m(n,d) \leqslant n - d + 1$,
если $d(\mathcal{C}) = d$, то $|\mathcal{C}| \leqslant m(n,d) \quad \Rightarrow \quad \log_2 |\mathcal{C}| \leqslant n - d + 1.$ □

Замечание: $\forall \mathcal{C} \subset \mathbb{F}_q^n : \quad d(\mathcal{C}) \leqslant n - \log_q |\mathcal{C}| + 1$ (аналогично).

Граница Синглтона для линейных кодов

Теорема (R. C. Singleton, 1964)

Пусть $\mathcal{C}$ — $(n, k, d)_q$-*код, тогда* $d \leqslant n - k + 1$.

Доказательство.

Способ 1: воспользоваться неравенством Синглтона для нелинейных кодов: $d \leqslant n - \log_q |\mathcal{C}| + 1$.
Способ 2: при переходе к эквивалентному систематическому коду не меняются n, k, d:

$$G \sim G' = \boxed{E_{k\times k} \mid A_{k\times(n-k)}}, \text{ все строки веса } \leqslant 1 + n - k.$$

Способ 3: $n - k \geqslant d - 1$, так как $n - k = \operatorname{rk} H$, а $\operatorname{rk} H$ равен наибольшему числу линейно независимых столбцов. □

Определение

Код, у которого $d = n - k + 1$, называется кодом с максимальным расстоянием (максимальным, МДР-кодом).

Граница Грайсмера

Теорема (J. H. Griesmer, 1960)

Если $\mathcal{C}$ — линейный $(n, k, d)_q$-код, то

$$n \geqslant \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil .$$

Замечание:

- Если $q > d$, то как следствие получаем неравенство Синглтона.
- Докажем для $q = 2$, остальное — упражнение.

Пример: существует ли $(n = 14, k = 5, d = 7)_2$-код?

- $\dfrac{2^n}{V_t} = \dfrac{2^{14}}{\binom{14}{0} + \binom{14}{1} + \binom{14}{2} + \binom{14}{3}} = \dfrac{16384}{470} = 34.859... > 32$
- $7 + \left\lceil \frac{7}{2} \right\rceil + \left\lceil \frac{7}{2^2} \right\rceil + \left\lceil \frac{7}{2^3} \right\rceil + \left\lceil \frac{7}{2^4} \right\rceil = 7 + 4 + 2 + 1 + 1 = 15 > 14$

Вспомогательный факт

Обозначим через $N(k, d)$ минимальную длину линейного кода размерности k с кодовым расстоянием d.

Лемма

$$N(k, d) \geqslant d + N\left(k - 1, \left\lceil \frac{d}{2} \right\rceil\right).$$

Доказательство: рассмотрим порождающую матрицу кода $\mathcal{C}$ длины $n = N(k, d)$:

- $G = \left(\begin{array}{c|c} \overbrace{0 \ldots 0}^{n-d} & \overbrace{1 \ldots 1}^{d} \\ \hline G' & G'' \end{array}\right)$
- $\operatorname{rk} G' = k - 1$
- G' — порождающая для кода $\mathcal{C}'$ длины $n - d$ с расстоянием d'.
- возьмём $\mathbf{a} \in \mathcal{C}'$, $\|\mathbf{a}\| = d'$
- $\exists\, \mathbf{b}$: $(\mathbf{a}|\mathbf{b}) \in \mathcal{C}$
- $(\mathbf{a}|\overline{\mathbf{b}}) = (\mathbf{a}|\mathbf{b}) + (0|1) \in \mathcal{C}$
- $\begin{cases} d' + \|\mathbf{b}\| \geqslant d \\ d' + d - \|\mathbf{b}\| \geqslant d \end{cases}$
- $2d' \geqslant d \Rightarrow d' \geqslant \left\lceil \frac{d}{2} \right\rceil$ $\square$

Доказательство неравенства Грайсмера

- Заметим, что $\left\lceil \frac{\lceil \frac{d}{2^i} \rceil}{2} \right\rceil = \left\lceil \frac{d}{2^{i+1}} \right\rceil$.
- Применим по индукции лемму:

$$
\begin{aligned}
n \geqslant N(k,d) &\geqslant d + N\left(k-1, \left\lceil \frac{d}{2} \right\rceil\right) \geqslant \\
&\geqslant d + \left\lceil \frac{d}{2} \right\rceil + N\left(k-2, \left\lceil \frac{d}{2^2} \right\rceil\right) \geqslant \\
&\geqslant d + \left\lceil \frac{d}{2} \right\rceil + \left\lceil \frac{d}{2^2} \right\rceil + N\left(k-3, \left\lceil \frac{d}{2^3} \right\rceil\right) \geqslant \dots \\
&\geqslant d + \left\lceil \frac{d}{2} \right\rceil + \dots + \left\lceil \frac{d}{2^{k-2}} \right\rceil + N\left(1, \left\lceil \frac{d}{2^{k-1}} \right\rceil\right).
\end{aligned}
$$

- Осталось заметить, что $N\left(1, \left\lceil \frac{d}{2^{k-1}} \right\rceil\right) = \left\lceil \frac{d}{2^{k-1}} \right\rceil$. □

Граница Плоткина

Теорема (M. Plotkin, 1951)

Пусть $\mathcal{C}$ *—* $(n, k, d)_q$*-код, тогда* $d \leqslant n\dfrac{q^{k-1}(q-1)}{q^k - 1}$.

Доказательство.

$$\mathcal{C} = \underbrace{\begin{array}{|c|c|c|}\hline & 0 & \\ \hline & * & \\ \hline\end{array}}_{n} \left.\begin{matrix} \\ \\ \end{matrix}\right\} \begin{matrix} D \subset \mathcal{C} : \dim D = k-1 \;\Rightarrow\; |D| = q^{k-1} \\ q^k - q^{k-1} \end{matrix}$$

$$\sum_{\mathbf{x} \in \mathcal{C}} \|\mathbf{x}\| \leqslant (q^k - q^{k-1}) \cdot n$$

$$\text{min вес} \leqslant \frac{\Sigma \text{ весов всех слов}}{\#\text{ ненулевых слов}} \;\Rightarrow\; d \leqslant \frac{(q^k - q^{k-1}) \cdot n}{q^k - 1}$$

□

Граница Плоткина для нелинейных кодов ($q = 2$)

Теорема (M. Plotkin, 1951)

Для всякого $[n, M, d]_2$-кода при $n < 2d$ выполнено неравенство

$$M \leqslant 2 \left\lfloor \frac{d}{2d - n} \right\rfloor,$$

причём если число $\frac{d}{2d-n}$ — целое, то равенство может иметь место только в случае эквидистантного кода.

Определение

Код $\mathcal{C}$ называется эквидистантным, если

$$\forall\, \mathbf{a}, \mathbf{b} \in \mathcal{C}, \quad \mathbf{a} \neq \mathbf{b}: \quad d(\mathbf{a}, \mathbf{b}) = d(\mathcal{C}).$$

Граница Плоткина для нелинейных кодов ($q = 2$)

Доказательство.

- $\Sigma = \sum\limits_{\mathbf{x},\mathbf{y}\in\mathcal{C}} d(\mathbf{x},\mathbf{y}) \geqslant \dfrac{M(M-1)}{2} \cdot d,$
  и равенство возможно только для эквидистантного кода.

- Вклад в эту сумму j-го столбца кодовой матрицы равен $x_j(M - x_j)$, где x_j — число единиц в столбце.

- $\dfrac{M(M-1)}{2} \cdot d \leqslant \sum\limits_{j=1}^{n} x_j(M - x_j)$

- пусть $M = 2m$ — чётное $\Rightarrow x_j = \frac{M}{2}$:
  $\frac{M(M-1)}{2} d \leqslant \Sigma \leqslant \frac{M^2}{4} n \Rightarrow 2Md - 2d \leqslant Mn \Rightarrow M \leqslant \frac{2d}{2d-n}$ при $2d > n$

- в силу чётности $M \leqslant 2\left\lfloor \frac{d}{2d-n} \right\rfloor$

Граница Плоткина для нелинейных кодов ($q = 2$)

Продолжение доказательства.

- пусть $M = 2m + 1$ — нечётное $\Rightarrow$

$$\frac{M(M-1)}{2} \cdot d \leqslant \Sigma \leqslant \frac{M-1}{2}\frac{M+1}{2} n$$

- $2(M + 1 - 1) \cdot d \leqslant (M + 1)n$
- $(M + 1) \cdot 2d - 2d \leqslant (M + 1)n$
- $M + 1 \leqslant \dfrac{2d}{2d - n} \Rightarrow M + 1 \leqslant 2 \left\lfloor \frac{d}{2d-n} \right\rfloor$. □

Следствие

Если $n = 2d$, то $M \leqslant 2n$.

Доказательство.

$$m(2d, d) \leqslant 2 \cdot m(2d - 1, d) \leqslant 2 \cdot 2 \cdot \left\lfloor \frac{d}{2d - (2d - 1)} \right\rfloor = 4d = 2n.$$ □

Граница Варшамова — Гильберта

Теорема (P. P. Варшамов, 1957; E. N. Gilbert, 1952)

$$\sum_{j=0}^{d-2} \binom{n-1}{j} (q-1)^j < q^{n-k} \;\Rightarrow\; \exists \text{ линейный } (n, k, \geqslant d)_q\text{-код}$$

Доказательство.

- Пусть в матрице $H = H_{(n-k)\times N}$ с N столбцами любые $d-1$ столбцов линейно независимы.
- Тогда существует не более $\Sigma = \sum_{j=1}^{d-2} \binom{N}{j}(q-1)^j$ различных линейных комбинаций столбцов из $\leqslant d-2$ слагаемых.
- $\Sigma < q^{n-k} - 1 \Rightarrow$ найдётся ненулевой столбец $\mathbf{h}$ высоты $n-k$, не совпадающий ни с одной из этих линейных комбинаций.
- В матрице $H' = (H\,\mathbf{h})$ любые $d-1$ столбцов линейно независимы.
- Далее по индукции $N = 1, 2, \ldots, n-1$. □

Заключительные замечания

1. Все четыре верхние границы (Хемминга, Плоткина, Синглтона и Грайсмера) достигаются: рассмотреть код Хемминга, код с повторением и код, двойственный к коду Хемминга.

2. Следствие неравенства Синглтона:

   $d = 2t + 1 \Rightarrow 2t \leqslant n - k$, то есть для испраления t ошибок необходимо добавить $\geqslant 2t$ проверочных символов.

3. Неравенство Варшамова–Гильберта является достаточным, но не является необходимым условием существования кода: если оно не выполняется, код может как существовать, так и не существовать.

   Пример: $q = 2$, $n = 6$, $k = 2$;
   теорема гарантирует существование $(6, 2, d)$–кода лишь при $d \leqslant 3$, однако наибольшее такое d равно 4.

Домашнее задание

1. Найти все двоичные коды длины $n \geqslant 3$, максимальные в смысле границы Синглтона, то есть такие, что $d = n - k + 1$.

2. Существуют ли $[16, 11, 9]_2$– и $[16, 10, 9]_2$–коды?

3. Построить $[16, 32, 8]_2$–код.
(*Указание*: как следует из доказательства теоремы Плоткина, каждый столбец кодовой таблицы должен содержать поровну нулей и единиц.)

4. Доказать, что $m_q(n, 2) = q^{n-1}$.

5. Найти число различных двоичных кодов длины n максимальной мощности, обнаруживающих одну ошибку.

Домашнее задание

6. Доказать, что $m(n, d) \neq 3$ для всех n, d. Другими словами, не существует двоичных максимальных кодов мощности 3.

7. Доказать неравенство Грайсмера над полем $\mathbb{F}_q$ при $q > 2$.

8. Доказать, что $(16, 8, 6)_2$–код не существует.
(*Указание*: аналогично доказательству неравенства Грайсмера рассмотреть код G', воспользоваться задачей 1 и получить противоречие с границей сферической упаковки.)

9. Пусть $\mathcal{C}$ — двоичный $(n, k, d)_2$–код, лежащий на границе Грайсмера, т.е. $n = \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil$. Показать, что у кода $\mathcal{C}$ есть базис, целиком состоящий из векторов минимального веса (теорема ван Тилборга, 1980).

Домашнее задание

10. Для каких из перечисленных параметров существует двоичный линейный (n, k)–код с кодовым расстоянием d:

    а) $n = 10,\ k = 3,\ d = 4$ г) $n = 15,\ k = 4,\ d = 6$

    б) $n = 10,\ k = 3,\ d = 5$ д) $n = 15,\ k = 4,\ d = 8$

    в) $n = 10,\ k = 3,\ d = 6$ е) $n = 15,\ k = 4,\ d = 9.$

11. Пусть $m(n, d) = \max_{\mathcal{C}} |\mathcal{C}|$ и $l(n, d) = \max_{\mathcal{C}'} |\mathcal{C}'|$ — мощности максимального кода и максимального линейного кода, где максимумы берутся соответственно по всем двоичным кодам $\mathcal{C}$ и по всем линейным двоичным кодам $\mathcal{C}'$ из $\{0, 1\}^n$ длины n с кодовым расстоянием d. Показать, что $l(9, 5) < m(9, 5)$. Какие оценки величин $m(n, d)$ и $l(n, d)$ следуют из границ Хемминга, Плоткина, Синглтона, Варшамова–Гильберта?