Теория кодирования

МФТИ, осень 2013

Александр Дайняк

www.dainiak.com

Циклический код

Циклический код — это линейный код, такой, что для любого кодового слова

$$(a_0, a_1 \dots, a_{n-1})$$

слово $(a_{n-1}, a_0 \dots, a_{n-2})$ также является кодовым.

Циклический код — это подмножество C кольца $\mathbb{F}[x]/(x^n - 1)$, такое, что

- $f_1, f_2 \in C \quad \Rightarrow \quad \forall \alpha, \beta \in \mathbb{F} \;\; \alpha f_1 + \beta f_2 \in C$
- $f \in C \quad \Rightarrow \quad x \cdot f \in C$

Примитивный элемент

Рассмотрим поле $\mathbb{F}_q$, где $q = p^m$, p простое.

Известно, что множество $\mathbb{F}_q \setminus \{0\}$ образует циклическую группу по умножению.

Каждый образующий элемент этой группы (порядок которого равен $(q-1)$) называется *примитивным элементом поля*.

Иными словами, примитивный элемент — это такой $\lambda \in \mathbb{F}_q$, что $\{1, \lambda, \lambda^2, \dots, \lambda^{q-2}\} = \mathbb{F}_q \setminus \{0\}$.

Граница Боуза—Чоудхури—Хоквингема

Теорема. (A.Hocquenghem’1959,
R.C. Bose and D.K. Ray-Chaudhuri’1960)

Пусть λ — примитивный элемент $\mathbb{F}_q$.

Пусть порождающий многочлен g кода $C \subseteq \mathbb{F}_q^n$ таков, что в $\mathbb{F}_q$ среди его корней есть (различные) числа вида

$$\lambda^b, \lambda^{b+1}, \dots, \lambda^{b+\delta-2}$$

Тогда $d(C) \geq \delta$.

Граница Боуза—Чоудхури—Хоквингема

Проблема:

- Если применять теорему «в лоб», то невозможно доказать, что кодовое расстояние больше мощности кодового алфавита, даже если это и так.

Решение:

- Код рассмотрим как подмножество в $\mathbb{F}_p^n$, но при применении границы БЧХ погрузим поле $\mathbb{F}_p$ в $\mathbb{F}_{p^m}$.

Факты о полях

- При любом простом p и любом m поле $\mathbb{F}_p$ можно вложить как подполе в $\mathbb{F}_{p^m}$.

Обычно поле $\mathbb{F}_p$ — это поле вычетов $\mathbb{F}_p$,
а $\mathbb{F}_{p^m}$ строится как множество многочленов с коэффициентами из $\mathbb{Z}_p$, которые складываются и умножаются по модулю некоторого многочлена степени m, неприводимого над $\mathbb{Z}_p$.

Тогда вложение $\mathbb{F}_p$ в $\mathbb{F}_{p^m}$ очевидно: элементам $\mathbb{F}_p$ соответствуют многочлены степени ≤ 0.

Факты о полях

- Элементам $\mathbb{F}_{p^m}$ можно сопоставить вектора из $\mathbb{F}_p^m$, так, что сумме элементов $\mathbb{F}_{p^m}$ соответствует сумма векторов в $\mathbb{F}_p^m$.

Раз $\mathbb{F}_{p^m}$ — многочлены с коэффициентами из $\mathbb{F}_p$ степени $\leq m$, то каждому элементу $\mathbb{F}_{p^m}$ сопоставим вектор коэффициентов многочлена.

Коды БЧХ

Пусть p простое.
Рассмотрим циклический код $C \subseteq \mathbb{F}_p[x]/(x^n - 1)$
с порождающим многочленом g.

Коэффициенты g берутся из $\mathbb{F}_p$, но их можно считать одновременно элементами $\mathbb{F}_{p^m}$.

Рассмотрим код $\tilde{C} \subseteq \mathbb{F}_{p^m}[x]/(x^n - 1)$, порождённый многочленом g (если считать, что $g \in \mathbb{F}_{p^m}[x]/(x^n - 1)$).

Можно в том же духе считать, что $C \subseteq \tilde{C}$.

Коды БЧХ

Коэффициенты g берутся из $\mathbb{F}_p$, но их можно считать одновременно элементами $\mathbb{F}_{p^m}$.

$\tilde{C} \subseteq \mathbb{F}_{p^m}[x]/(x^n - 1)$ порождён g.

Пусть λ — примитивный элемент $\mathbb{F}_{p^m}$, и

$$g\left(\lambda^b\right) = \cdots = g\left(\lambda^{b+\delta-2}\right) = 0$$

Тогда граница БЧХ гласит: $d\left(\tilde{C}\right) \geq \delta$.

Так как $C \subseteq \tilde{C}$, то и $d(C) \geq \delta$.

Коды БЧХ

- Подбираем $g \in \mathbb{F}_{p^m}[x]/(x^n - 1)$ с коэффициентами из $\mathbb{F}_p$, так, чтобы в $\mathbb{F}_{p^m}$ было выполнено $g(\lambda^b) = \cdots = g(\lambda^{b+\delta-2}) = 0$ и $g|(x^n - 1)$.
- На основе g строим циклический код в $\mathbb{F}_p[x]/(x^n - 1)$, для которого, по построению, выполнено $d(C) \geq \delta$.

Вопросы:

- Существует ли вообще такой g?
- Как оценить $\dim C$?

Минимальный многочлен

Хорошие новости (без доказательства):

Для любого $\alpha \in \mathbb{F}_{p^m} \setminus \{0\}$ существует многочлен $f \in \mathbb{F}_{p^m}[x] \setminus \{0\}$ с коэффициентами из $\mathbb{F}_p$, для которого $f(\alpha) = 0$.

Если взять такой f минимальной степени, то

- f неприводим над $\mathbb{F}_p$,
- $\deg f \leq m$,
- $f \mid \left(x^{p^m-1} - 1\right)$.

Такой f называется *минимальным многочленом* элемента α.

Коды БЧХ

Следствия из хороших новостей:

- Если $n = p^m - 1$, то существует g, такой, что $g(\lambda^b) = \cdots = g(\lambda^{b+\delta-2}) = 0$ и $g | (x^n - 1)$, причём $\deg g \leq (\delta - 1)m$.
- Такой g можно взять как

$$\mathrm{LCM}\left(f_{\lambda^b}, \dots, f_{\lambda^{b+\delta-2}}\right)$$

где $f_{\lambda^b}, \dots, f_{\lambda^{b+\delta-2}}$ — минимальные многочлены соответствующих элементов.

Коды БЧХ

Окончательный способ построения кода:

- Берём $n \coloneqq p^m - 1$ и
$$g \coloneqq \mathrm{LCM}\left(f_{\lambda^b}, \dots, f_{\lambda^{b+\delta-2}}\right)$$
где $f_{\lambda^b}, \dots, f_{\lambda^{b+\delta-2}}$ — минимальные многочлены соответствующих элементов в $\mathbb{F}_{p^m}$.
- Строим циклический код в $\mathbb{F}_p$, используя g в качестве порождающего многочлена наименьшей возможной степени

Получаем код с параметрами $[p^m - 1, k, d]_p$, где

- $k = n - \deg g \geq n - (\delta - 1)m$
- $d \geq \delta$

Задача восстановления синхронизации

Пусть по каналу передаются слова … $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ …

$$a_1 a_2 \dots a_n b_1 b_2 \dots b_n c_1 c_2 \dots c_n \dots$$

Если в канале выпадают символы, может произойти *ошибка синхронизации*:

$$a_{i+1} a_{i+2} \dots a_n b_1 b_2 \dots b_n c_1 c_2 \dots c_n \dots$$

и есть шанс неправильно разбить принятую последовательность на слова:

$$a_{i+1} \dots a_n b_1 \dots b_i \mid b_{i+1} \dots b_n c_1 \dots c_i \mid c_{i+1} \dots$$

Если при этом такие слова окажутся кодовыми, то мы далеко не сразу обнаружим ошибку!

Задача восстановления синхронизации

При потере синхронизации имеем разбиение:

$$a_{i+1} \dots a_n b_1 \dots b_i \mid b_{i+1} \dots b_n c_1 \dots c_i \mid c_{i+1} \dots$$

Циклические коды очень плохие с точки зрения восстановления синхронизации: если $\boldsymbol{a} \in C$ и в канал передавалось

$$\boldsymbol{aaa} \dots$$

то при потере синхронизации мы обнаружим ошибку только в самом конце приёма.

Свобода от запятой

Пусть по каналу передаются слова … $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ …

$$a_1 a_2 \dots a_n b_1 b_2 \dots b_n c_1 c_2 \dots c_n \dots$$

Если при приёме слова $\boldsymbol{b}$ «запоздать» на i тактов, то мы примем слово

$$b_{i+1} \dots b_n c_1 \dots c_i$$

а если «забежать вперёд» на i тактов, примем

$$a_{n-i+1} \dots a_n b_1 \dots b_{n-i}$$

Код обладает *свободой от запятой степени* r, если для любых кодовых слов $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ и любого $i \le r$ коду не принадлежат слова $b_{i+1} \dots b_n c_1 \dots c_i$ и $a_{n-i+1} \dots a_n b_1 \dots b_{n-i}$.

Свобода от запятой

Код обладает *свободой от запятой степени* r, если для любых кодовых слов $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ и любого $i \leq r$ коду не принадлежат слова $b_{i+1} \dots b_n c_1 \dots c_i$ и $a_{n-i+1} \dots a_n b_1 \dots b_{n-i}$.

Если $r \geq \frac{n}{2}$, то считаем, что $r = \infty$, а код называется *кодом без запятой*.

Если $r < \infty$, то при приёме можно (перебором) исправить синхросдвиг на $\leq \frac{r}{2}$ символов.

Если $r = \infty$, то может быть исправлен любой синхросдвиг.

Свобода от запятой

Код обладает *свободой от запятой степени* r, если для любых кодовых слов $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ и любого $i \leq r$ коду не принадлежат слова $b_{i+1} \dots b_n c_1 \dots c_i$ и $a_{n-i+1} \dots a_n b_1 \dots b_{n-i}$.

- Циклические коды — не годятся
- Зато *смежные классы* циклических кодов — вполне!

Смежные классы линейных кодов

Пусть $C \subseteq \mathbb{F}^n$ — линейный код.

Его *смежный класс* — это множество вида

$$C + \boldsymbol{a} \coloneqq \{\boldsymbol{c} + \boldsymbol{a} \mid \boldsymbol{c} \in C\}$$

Заметьте: при $\boldsymbol{a} \notin C$ такой код не линейный!

Для циклического кода с порождающим многочленом g смежный класс имеет вид

$$\{f \cdot g + s \mid f \in \mathbb{F}[x]/(x^n - 1)\}$$

для некоторого $s \in \mathbb{F}[x]/(x^n - 1)$.

Смежные классы циклических кодов

Для циклического кода с порождающим многочленом g смежный класс имеет вид

$$\{f \cdot g + s \mid f \in \mathbb{F}[x]/(x^n - 1)\}$$

для некоторого $s \in \mathbb{F}[x]/(x^n - 1)$.

Теорема.
При $s \equiv 1$ степень свободы от запятой смежного класса циклического кода равна

$$\deg g - 1$$

при $n \geq 2 \deg g$, и равна ∞ при $n < 2 \deg g$.
(Подробно обоснуем только нижнюю оценку.)

Смежные классы циклических кодов

Пусть передавались слова $\boldsymbol{a}, \boldsymbol{b} \in C$.

Если при приёме слова $\boldsymbol{a}$ произошло запаздывание на i тактов, то будет принято слово, которому отвечает многочлен

$$x^{-i} \cdot (f_{\boldsymbol{a}} - t_1) + x^{n-i} \cdot t_2,$$

где t_1 и t_2 — многочлены, образованные i первыми координатами слов $\boldsymbol{a}$ и $\boldsymbol{b}$ соответственно, а $f_{\boldsymbol{a}}$ — многочлен, отвечающий слову $\boldsymbol{a}$.

Смежные классы циклических кодов

В кольце $\mathbb{F}[x]/(x^n - 1)$ имеем

$$x^{-i} \cdot (f_{\boldsymbol{a}} - t_1) + x^{n-i} \cdot t_2 = x^{n-i} \cdot (f_{\boldsymbol{a}} - t_1 + t_2)$$

Аналогично, если при приёме слова $\boldsymbol{b}$ произошло «забегание вперёд», то будет принято слово $x^i \cdot f_{\boldsymbol{b}} + (t_3 - t_4)$, где t_3 и t_4 — многочлены, образованные i старшими разрядами слова $\boldsymbol{a}$ и i младшими разрядами $\boldsymbol{b}$ соответственно. При этом

$$\deg t_1, \deg t_2, \deg t_3, \deg t_4 < i$$

Смежные классы циклических кодов

Итак, в случае рассинхронизации принятое слово будет иметь вид

$$x^{n-i} \cdot \left(\tilde{f} + \Delta\right) \quad \text{или} \quad x^{i} \cdot \tilde{f} + \Delta,$$

где $\tilde{f} \in C$ и $\deg \Delta < i$.

Нужно, чтобы $x^{n-i} \cdot \left(\tilde{f} + \Delta\right) \notin C$ и $x^{i} \cdot \tilde{f} + \Delta \notin C$ при $0 < i \leq r$.

Смежные классы циклических кодов

Пусть C — смежный класс ц.к. вида

$$\{f \cdot g + 1 \mid f \in \mathbb{F}[x]/(x^n - 1)\}$$

Нужно, чтобы для любых f_1, f_2, Δ, i, таких, что $\deg \Delta < i$ и $0 < i \leq r$ в кольце $\mathbb{F}[x]/(x^n - 1)$ было выполнено

$$f_1 \cdot g + 1 \neq x^{n-i} \cdot (f_2 \cdot g + 1 + \Delta)$$

$$f_1 \cdot g + 1 \neq x^i \cdot (f_2 \cdot g + 1) + \Delta$$

Это равносильно тому, что для любых f, Δ, i

$$f \cdot g \neq x^i + \Delta - 1$$

Смежные классы циклических кодов

Пусть C — смежный класс ц.к. вида

$$\{f \cdot g + 1 \mid f \in \mathbb{F}[x]/(x^n - 1)\}$$

Нужно, чтобы для любых f, Δ, i, таких, что $\deg \Delta < i$ и $0 < i \le r$ в кольце $\mathbb{F}[x]/(x^n - 1)$ было выполнено

$$f \cdot g \neq x^i + \Delta - 1$$

Имеем $x^i + \Delta - 1 \not\equiv 0$ при любом $i > 0$.

Т.к. $\deg\left(x^i + \Delta - 1\right) = i \le r$, то достаточно, чтобы $\deg g > r$.

Это и требовалось доказать.

Циклическое представление кодов Хемминга

Пусть λ — примитивный элемент поля $\mathbb{F}_{2^m}$.

Пусть g — минимальный многочлен для λ, и $C \subset \mathbb{F}_2^{2^m-1}$ — код, порождённый g.

Любой кодовый многочлен $f \in C$ имеет корень, равный λ. Поэтому кодовые вектора $(c_0, \ldots, c_{2^m-2})$ удовлетворяют соотношению

$$c_0 + c_1\lambda + c_2\lambda^2 + \cdots + c_{2^m-2}\lambda^{2^m-2} = 0$$

Циклическое представление кодов Хемминга

Кодовые вектора $(c_0, \dots, c_{2^m-2})$ удовлетворяют соотношению

$$c_0 + c_1\lambda + c_2\lambda^2 + \dots + c_{2^m-2}\lambda^{2^m-2} = 0$$

Так как $\{\lambda^0, \lambda^1, \dots, \lambda^{2^m-2}\} = \mathbb{F}_{2^m} \setminus \{0\}$, и так как каждому элементу $\mathbb{F}_{2^m}$ отвечает вектор из $\mathbb{F}_2^m$, то проверочная матрица кода равна

$$\left(v_{\lambda^0}, v_{\lambda^1}, \dots, v_{\lambda^{2^m-2}}\right) \in \mathbb{F}_2^{m\times(2^m-1)}$$

где v_{λ^i} — вектор, отвечающий λ^i.

Столбцы матрицы — все ненулевые вектора $\mathbb{F}_2^m$.

Циклическое представление кодов Хемминга

Утверждение.
Двоичный код Хемминга с параметрами $[2^m - 1, 2^m - 1 - m, 3]$ эквивалентен циклическому коду, порождённому минимальным многочленом примитивного элемента $\mathbb{F}_{2^m}$.

Коды Голея

М. Голей (M. J. E. Golay) предложил два кода, позже было замечено, что они циклические:

- $[23,12,7]$-код с порождающим многочленом
$$1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$$
- $[11,6,5]_3$-код с порождающим многочленом
$$2 + x^2 + 2x^3 + x^4 + x^5$$

Расширенные коды Голея:

- $[23,12,7]$-код $\quad \rightarrow \quad [24,12,8]$-код
- $[11,6,5]_3$-код $\quad \rightarrow \quad [12,6,6]_3$-код

Совершенные коды

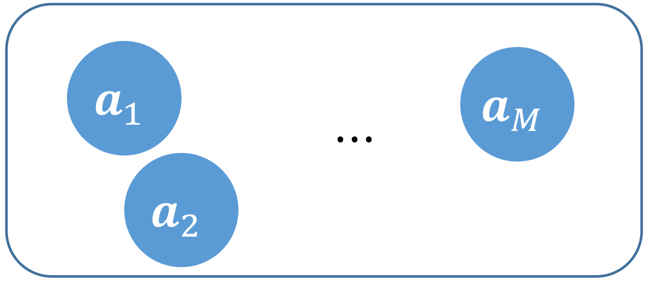
Граница Хемминга (сферической упаковки).
Для любого $(n, M, d)_q$-кода имеем

$$M \leq \frac{q^n}{\left|S_{\lfloor (d-1)/2 \rfloor}(\mathbf{0})\right|}$$

Для любого линейного $[n, k, d]_q$-кода

$$\left|S_{\lfloor (d-1)/2 \rfloor}(\mathbf{0})\right| \leq q^{n-k}$$

Коды, достигающие эту границу, — *совершенные*.



Совершенные коды

$$\left|S_{\lfloor (d-1)/2 \rfloor}(\mathbf{0})\right| = q^{n-k}$$

Утверждение.
Коды Голея и Хемминга — совершенные.

Доказательство:

- Для $[23,12,7]$-кода Голея: $\sum_{i=0}^{3} \binom{23}{i} = 2^{23-12}$
- Для $[11,6,5]_3$-кода Голея: $\sum_{i=0}^{2} \binom{n}{i} \cdot 2^i = 3^{11-6}$
- Для двоичных кодов Хемминга проверяли ранее. Теперь проверим в общем случае.

Совершенные коды

Проверочная матрица q-ичного кода Хемминга содержит все линейно независимые столбцы высоты m.

Получается $\left[n = \frac{q^m - 1}{q-1}, k = n - m, 3\right]_q$-код.

Проверяем соотношение $\left|S_{\lfloor (d-1)/2 \rfloor}(\mathbf{0})\right| = q^{n-k}$:

$$|S_1(\mathbf{0})| = 1 + n(q-1) = q^m = q^{n-k}$$

Тривиальные совершенные коды

- $(n, 1, n)_q$-код (состоит из одного слова)

- $(n, 2, n)_2$-код (пара слов-антиподов) при нечётных n

Совершенные коды

Теорема. (В. А. Зиновьев, В. К. Леонтьев ’1972, A. Tietäväinen ’1973, J. H. van Lint ’1971, M. R. Best ’1983, Y. Hong ’1983, V. Pless ’1968) — *Б/д.*

- Нетривиальных совершенных кодов с расстоянием > 7 не существует.
- Единственным с точностью до эквивалентности совершенным кодом с расстоянием 7 является $[23,12,7]$-код Голея.
- Любой нетривиальный код над алфавитом мощности $q = p^m$ с расстоянием ≤ 5 либо эквивалентен $[11,6,5]_3$-коду Голея, либо имеет те же длину, число слов и кодовое расстояние, что и $\left[\frac{q^t-1}{q-1}, \frac{q^t-1}{q-1} - t, 3\right]_q$-код Хемминга.

Совершенные коды

Следствие теоремы:
Для любого совершенного кода над $\mathbb{F}_q$ существует *линейный* код с той же длиной слов, числом слов и кодовым расстоянием.

Нерешённая проблема:
Существуют ли совершенные коды над алфавитами мощности $\neq p^m$?

Совершенные коды

Теорема. (Ю. Л. Васильев ’1962,
обобщения: J. Schonheim ’1968, B. Lindstrom ‘1969)
Для любого $q = p^m$ существуют совершенные коды
с расстоянием 3, не эквивалентные линейным кодам.

Докажем только для случая $q = 2$:

При любом m существует нелинейный $\left(2^m - 1, 2^{2^m - m - 1}, 3\right)$-код.

Совершенные коды

Лемма. (Конструкция Васильева)
Пусть $C', C'' \subseteq \mathbb{F}_2^n$ — коды с расстояниями d' и d'', причём d' нечётно. Положим $\pi(\boldsymbol{a}) \coloneqq \sum_i a_i$.

Для произвольного $\gamma\colon C'' \to \mathbb{F}_2$ рассмотрим код

$$C \coloneqq \left\{\left(\boldsymbol{c}' \mid \boldsymbol{c}' + \boldsymbol{c}'' \mid \pi(\boldsymbol{c}') + \gamma(\boldsymbol{c}'')\right), \text{где } \boldsymbol{c}' \in C', \boldsymbol{c}'' \in C''\right\}$$

Тогда C является $(2n+1, |C'| \cdot |C''|, d)$-кодом, где

$$d \geq \min\{2d' + 1, d''\}$$

Доказательство:
Нетривиальна только оценка $d(C)$.
(Похоже на конструкцию Плоткина.)

Доказательство леммы Васильева

Возьмём пару различных слов кода C:

$$\boldsymbol{a} = \big(\boldsymbol{c}' \mid \boldsymbol{c}' + \boldsymbol{c}'' \mid \pi(\boldsymbol{c}') + \gamma(\boldsymbol{c}'')\big)$$

$$\widehat{\boldsymbol{a}} = \big(\widehat{\boldsymbol{c}}' \mid \widehat{\boldsymbol{c}}' + \widehat{\boldsymbol{c}}'' \mid \pi(\widehat{\boldsymbol{c}}') + \gamma(\widehat{\boldsymbol{c}}'')\big)$$

Рассматриваем случаи:

- $\boldsymbol{c}' \neq \widehat{\boldsymbol{c}}'$ и $\boldsymbol{c}'' = \widehat{\boldsymbol{c}}''$.
  Если $d(\boldsymbol{c}', \widehat{\boldsymbol{c}}') = d'$, то $\pi(\boldsymbol{c}') \neq \pi(\widehat{\boldsymbol{c}}')$ и следовательно
  $$d(\boldsymbol{a}, \widehat{\boldsymbol{a}}) = 2d' + 1.$$
  Если $d(\boldsymbol{c}', \widehat{\boldsymbol{c}}') > d'$, то
  $$d(\boldsymbol{a}, \widehat{\boldsymbol{a}}) > 2d'.$$

Доказательство леммы Васильева

Возьмём пару различных слов кода C:

$$\boldsymbol{a} = \left(\boldsymbol{c}' \mid \boldsymbol{c}' + \boldsymbol{c}'' \mid \pi(\boldsymbol{c}') + \gamma(\boldsymbol{c}'')\right)$$
$$\widehat{\boldsymbol{a}} = \left(\widehat{\boldsymbol{c}}' \mid \widehat{\boldsymbol{c}}' + \widehat{\boldsymbol{c}}'' \mid \pi(\widehat{\boldsymbol{c}}') + \gamma(\widehat{\boldsymbol{c}}'')\right)$$

Рассматриваем случаи:

- $\boldsymbol{c}' = \widehat{\boldsymbol{c}}'$ и $\boldsymbol{c}'' \neq \widehat{\boldsymbol{c}}''$.
  Тогда, очевидно, $d(\boldsymbol{a}, \widehat{\boldsymbol{a}}) \geq d(\boldsymbol{c}'', \widehat{\boldsymbol{c}}'') \geq d''$.

Доказательство леммы Васильева

$$\boldsymbol{a} = \left(\boldsymbol{c}' \mid \boldsymbol{c}' + \boldsymbol{c}'' \mid \pi(\boldsymbol{c}') + \gamma(\boldsymbol{c}'')\right)$$
$$\widehat{\boldsymbol{a}} = \left(\hat{\boldsymbol{c}}' \mid \hat{\boldsymbol{c}}' + \hat{\boldsymbol{c}}'' \mid \pi(\hat{\boldsymbol{c}}') + \gamma(\hat{\boldsymbol{c}}'')\right)$$

Остался случай $\boldsymbol{c}' \neq \hat{\boldsymbol{c}}'$ и $\boldsymbol{c}'' \neq \hat{\boldsymbol{c}}''$:
Пусть $\boldsymbol{c}'$ и $\hat{\boldsymbol{c}}'$ отличаются на множестве позиций D_1,
а $\boldsymbol{c}''$ и $\hat{\boldsymbol{c}}''$ отличаются на множестве позиций D_2.

Тогда $\boldsymbol{c}' + \boldsymbol{c}''$ и $\hat{\boldsymbol{c}}' + \hat{\boldsymbol{c}}''$ отличаются по крайней мере на множестве $D_2 \setminus D_1$.

Следовательно

$$d(\boldsymbol{a}, \widehat{\boldsymbol{a}}) \geq |D_1| + |D_2 \setminus D_1| \geq |D_2| \geq d''$$

Теорема Васильева

Следствие из леммы Васильева.
Пусть $C'' \subseteq \mathbb{F}_2^n$ — код с расстоянием 3.

Для произвольного отображения $\gamma\colon C'' \to \mathbb{F}_2$ код
$$\left\{\left(\boldsymbol{c}' \mid \boldsymbol{c}' + \boldsymbol{c}'' \mid \pi(\boldsymbol{c}') + \gamma(\boldsymbol{c}'')\right), \text{где } \boldsymbol{c}' \in \mathbb{F}_2^n, \boldsymbol{c}'' \in C''\right\}$$
является $(2n + 1, 2^n \cdot |C''|, 3)$-кодом.

Доказательство: применяем Лемму с $C' \coloneqq \mathbb{F}_2^n$.

Замечание: если отображения γ и $(\gamma + 1)$ нелинейны,
то получаемый код не эквивалентен никакому линейному.

Теорема Васильева

Следствие из леммы Васильева.
Если существует $(n, M, 3)$-код, то существует $(2n + 1, 2^n \cdot M, 3)$-код, не эквивалентный никакому линейному.

Теорема.
Для любого $m \geq 2$ существует совершенный $\left(2^m - 1, 2^{2^m - m - 1}, 3\right)$-код, не эквивалентный никакому линейному.

Доказательство:
Заметим, что при каждом $m \geq 2$ есть $\left(2^{m-1} - 1, 2^{2^{m-1} - m}, 3\right)$-код Хемминга, и применим Следствие с $n \coloneqq 2^{m-1} - 1$ и $M \coloneqq 2^{2^{m-1} - m}$.

Линейные коды не всегда лучшие

Теорема. (F. P. Preparata ’1968, J.-M. Goethals and S. L. Snover ’1972)

- Для $\forall m \geq 2$ существует $\left(4^m, 2^{4^m-4m}, 6\right)$-код.
- Любой линейный код длины 4^m с расстоянием 6 имеет меньшую мощность.

Коды с параметрами $\left(4^m, 2^{4^m-4m}, 6\right)$ называют *кодами Препáраты*.