

Транзитивные совершенные коды с квадратичной функцией сдвига

Д. С. Кротов, В. Н. Потапов

Институт математики им. С.Л.Соболева,
Новосибирский государственный университет, Новосибирск

Международная конференция "Мальцевские чтения"

г. Новосибирск, 12-16 ноября 2012 г.

Пусть F — конечное поле порядка q и F^n — векторное пространство наборов длины n над F .

Определение

Расстоянием Хэмминга $d(x, y)$ между векторами $x, y \in F^n$ называется число координат, в которых векторы x и y различаются.

Определение

Совершенным кодом в F^n называется такое множество $C \subset F^n$, что для любого $x \in F^n$ найдётся ровно один $y \in C$ такой, что $d(x, y) \leq 1$.

Определение

Группой автоморфизмов $\mathcal{AUT}(C)$ кода $C \subset F^n$ называется группа изометрий пространства F^n , оставляющих код на месте.

Определение

Код C называется **транзитивным** если для любых векторов $a, b \in C$ существует $\varphi \in \mathcal{AUT}(C)$ такой, что $\varphi(a) = b$.

Определение

Транзитивный код C называется **квазилинейным** (propelinear), если $\mathcal{AUT}(C)$ содержит регулярную подгруппу.

Конструкция Васильева — Шёнхейма

Пусть $H \subset F^n$ — совершенный код и $\lambda : H \rightarrow F$ произвольная функция. Определим $C(H, \lambda) =$

$$\{(v_0, \dots, v_{q-1}, p) : v_i \in F^n, \sum_{i \in F} v_i = c \in H, p = \sum_{i \in F} i |v_i| + \lambda(c)\}$$

где $|v_i|$ — сумма n координат вектора v_i . Тогда $C(H, \lambda)$ является совершенным кодом длины $qn + 1$.

J. Schönheim. On linear and nonlinear single-error-correcting q -ary perfect codes // *Inform. Contr.*, 12(1):23–26, 1968.

Ю.Л.Васильев. О негрупповых плотно упакованных кодах // *Проблемы кибернетики*. М.: Физматгиз, 1962. Вып. 8. С. 337–339.

Пусть $H \subseteq F^n$ — подпространство. Функция $\lambda : H \rightarrow F$ является **квадратичной**, если для любого $c \in H$ найдутся $\beta_0^c, \beta_1^c, \dots, \beta_n^c$ такие, что $\lambda(x + c) = \lambda(x) + \beta_0^c + \beta_1^c x_1 + \dots + \beta_n^c x_n$ для всех $x = (x_1, \dots, x_n) \in H$.

Теорема

Если $H \subset F^n$ — линейный совершенный код и функция $\lambda : H \rightarrow F$ является квадратичной, то $C(H, \lambda)$ транзитивный и квазилинейный совершенный код.

Следствие

Неэквивалентных транзитивных и квазилинейных совершенных кодов длины $qn + 1$ не менее $q^{\frac{n^2}{2}(1+o(1))}$.

С. А. Малюгин, "Транзитивные совершенные коды длины 15", Труды конференции "Дискретный анализ и исследование операций", Изд-во Ин-та математики СО РАН, Новосибирск, 2004, 96.

Ф. И. Соловьёва, "О построении транзитивных кодов", Проблемы передачи информации, 41:3 (2005), 23-31.

В. Н. Потапов, "О нижней оценке числа транзитивных совершенных кодов", Дискретн. анализ и исслед. опер., сер. 1, 13:4 (2006), 49-59.

Ф. И. Соловьёва, "О транзитивных разбиениях n -куба на коды", Пробл. передачи информ., 45:1 (2009), 27-35.

J. Borges, J. Rifà, I. Yu. Mogilnykh, and F. I. Solov'eva. A lower bound on the number of nonequivalent propelinear extended perfect codes. *Proc. Thirteenth Int. Workshop on Algebraic and Combinatorial Coding Theory ACCT 2012*, pages 93–98, Pomorie, Bulgaria, June 2012.

J. Borges, J. Rifà, I. Yu. Mogilnykh, and F. I. Solov'eva. Structural properties of binary propelinear codes// *Advances in Mathematics of Communications*. 2012. V. 6, N 3, P. 329 - 346, 2012.

Лемма

Пусть $f'(x) = f(x) + \beta x_j$ при $j \in [1..n]$, $\beta \in F$. Тогда $C(H, f') = \Pi_j^\beta C(H, f)$, где Π_j^β перестановка координат, переводящая $(\alpha + \beta, j)$ -ю координату в (α, j) -ю и фиксирующая остальные координаты.

Доказательство. Пусть $x = ((v_\alpha)_{\alpha \in F}, p) \in C(H, f)$. Тогда $p = \sum_{\alpha \in F} \alpha |v_\alpha| + f(c)$. После перестановки Π_j^β , получаем $y = \Pi_j^\beta x = ((u_\alpha)_{\alpha \in F}, p)$, где координата $u_{\alpha,j}$ равна $v_{\alpha+\beta,j}$, а остальные совпадают.

$$\begin{aligned} p &= \sum_{\alpha \in F} \alpha |v_\alpha| + f(c) = \sum_{\alpha \in F} \sum_{k \neq j} \alpha v_{\alpha,k} + \sum_{\alpha \in F} \alpha v_{\alpha,j} + f(c) = \\ &= \sum_{\alpha \in F} \sum_{k \neq j} \alpha u_{\alpha,k} + \sum_{\alpha \in F} \alpha u_{\alpha-\beta,j} + f(c) = \\ &= \sum_{\alpha \in F} \sum_{k \neq j} \alpha u_{\alpha,k} + \sum_{\alpha \in F} (\alpha + \beta) u_{\alpha,j} + f(c) = \\ &= \sum_{\alpha \in F} \sum_{k=1}^n \alpha u_{\alpha,k} + \beta \sum_{\alpha \in F} u_{\alpha,j} + f(c) = \\ &= \sum_{\alpha \in F} \alpha |u_\alpha| + f(c) + \beta c_j, \\ c &= (c_1, \dots, c_n) = \sum v_\alpha = \sum u_\alpha \text{ и } \Pi_j^\beta(x) \in C(H, f'). \end{aligned}$$

Утверждение

Для любого $w = ((w_\alpha)_{\alpha \in F}, p) \in C(H, f)$ преобразование $\Phi_w(v) = \Pi^c(v) + w$, где $\Pi^c = \Pi_1^{\beta_1^c} \Pi_2^{\beta_2^c} \dots \Pi_n^{\beta_n^c}$, $c = \sum_{\alpha \in F} w_\alpha$, является автоморфизмом кода $C(H, f)$, переводящим нуль в w .

Доказательство. Пусть $v = ((v_\alpha)_{\alpha \in F}, s) \in C(H, f)$. Тогда $s = \sum_{\alpha \in F} \alpha |v_\alpha| + f(d)$, где $d = \sum_{\alpha} v_\alpha$. Применяя лемму при $j = 1..n$, получаем, что $\Pi^c(v) = ((u_\alpha)_{\alpha \in F}, s)$, где $s = \sum_{\alpha \in F} \alpha |u_\alpha| + f(d) + \beta_1^c d_1 + \dots + \beta_n^c d_n$ и $d = (d_1, \dots, d_n) = \sum_{\alpha} u_\alpha$. Прибавляя вектор $w = ((w_\alpha)_{\alpha \in F}, p)$, получаем равенство $\Pi^c(v) + w = ((u_\alpha + w_\alpha)_{\alpha \in F}, r)$,

$$\begin{aligned} r &= \sum_{\alpha \in F} \alpha |u_\alpha| + f(d) + \beta_1^c d_1 + \dots + \beta_n^c d_n + \sum_{\alpha \in F} \alpha |w_\alpha| + f(c) \\ &= \sum_{\alpha \in F} \alpha |u_\alpha + w_\alpha| + f(d + c) - \beta_0^c + f(c). \end{aligned}$$

Поскольку $f(c) = f(0) + \beta_0^c$, имеем $\Pi^c(v) + w \in C(H, f)$.

Проблема

Для векторного пространства V и группы $\mathcal{A}$ линейных изометрий на V , найти неквадратичную функцию f такую, что для любого $c \in V$ имеется $\mu \in \mathcal{A}$, удовлетворяющее равенству $f(\mu(x) + c) = f(x) + l(x)$ для некоторого аффинного l .
Например, $V = H$ и $\mathcal{A} \subset \mathcal{AUT}(H)$.