

Квазигруппы и коды

В. Н. Потапов

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

XVI Международная конференция
<ПРОБЛЕМЫ ТЕОРЕТИЧЕСКОЙ КИБЕРНЕТИКИ>,
г. Нижний Новгород, 20-25 июня 2011 г.

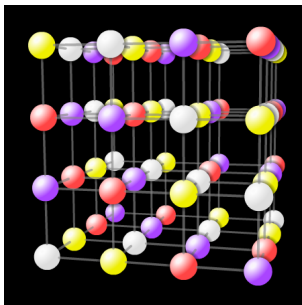
Определение

Пусть Σ — некоторое непустое множество. Функция $f : \Sigma^n \rightarrow \Sigma$ называется **n -арной квазигруппой** если f обратима по каждой своей переменной. **Порядком** квазигруппы называется $|\Sigma|$.

Пусть $\Sigma = \{0, 1, \dots, k-1\}$ — конечное множество. Условие обратимости можно записать в виде $f(\bar{x}) \neq f(\bar{y})$ для любых $\bar{x}, \bar{y} \in \Sigma^n$ таких, что $d(\bar{x}, \bar{y}) = 1$, где $d(\bar{x}, \bar{y})$ — расстояние Хэмминга.

Определение

Таблица значений n -арной квазигруппы называется **латинским гиперкубом** (n -мерное обобщение латинского квадрата).

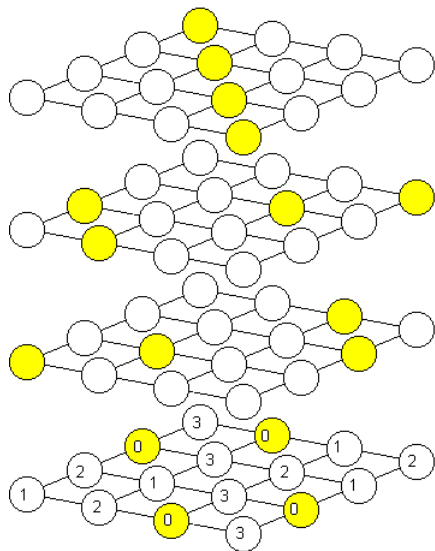


0	1	2	3
1	0	3	2
2	3	1	0
3	2	0	1

Определение

Множество $M \subset \Sigma^{n+1}$ называется **МДР-кодом (с расстоянием 2)** если $|M| = |\Sigma|^n$ и $d(\bar{x}, \bar{y}) \geq 2$ для любых различных $\bar{x}, \bar{y} \in M$.

График $M[f] = \{(\bar{x}, f(\bar{x})) \mid \bar{x} \in \Sigma^n\}$ n -арной квазигруппы f является МДР-кодом. Более того, имеется взаимно однозначное соответствие между n -арными квазигруппами, латинскими гиперкубами и МДР-кодами.



"... n -квазигруппы оказываются столь же естественным объектом изучения, как и квазигруппы (т. е. 2-квазигруппы), и их изучение уже началось."

Курош А. Г. *Общая алгебра. Лекции 1969-1970 учебного года*. М.:Наука, 1974.

Белоусов В. Д. *n -Арные квазигруппы*. Кишинёв: "Штиинца", 1972.

Кротов Д. С. Совершенные коды и n -арные квазигруппы: конструкции и классификация, *Дисс... доктора физ.-мат.наук*, Новосибирск, 2011.

Определение

Изотопией в Σ^n называется упорядоченный набор из n перестановок $\theta_i : \Sigma \rightarrow \Sigma$, $i \in [n]$. Пусть $\bar{\theta} = (\theta_1, \dots, \theta_n)$ является изотопией и $M \subseteq \Sigma^n$.

$$\bar{\theta}M \triangleq \{(\theta_1 x_1, \dots, \theta_n x_n) \mid (x_1, \dots, x_n) \in M\}.$$

Определение

Парастрофией в Σ^n называется перестановка координат $\tau \in S_n$.

$$M_\tau \triangleq \{(x_{\tau(1)}, \dots, x_{\tau(n)}) \mid (x_1, \dots, x_n) \in M\}.$$

Рассмотрим n -мерный k -значный куб (Σ^n, d) как метрическое пространство с метрикой Хэмминга. Его группа **изометрий** является полупрямым произведением группы **изотопий** Θ_{nk} на группу **парастрофий** S_n .

$$\text{Aut}(\Sigma^n) = \Theta_{nk} \rtimes S_n$$

Определение

Квазигруппы $f_1, f_2 : \Sigma^n \rightarrow \Sigma$ называются **эквивалентными**, если МДР-коды $M[f_1], M[f_2] \subseteq \Sigma^{n+1}$ эквивалентны, т. е. переводятся друг в друга изометрией куба Σ^{n+1} .

Определение

Ретрактом размерности $n - 1$ МДР-кода $M \subset \Sigma^n$ называется множество

$$M|_{x_i=a} = \{\bar{x} \in M \mid x_i = a\}, \text{ где } a \in \Sigma.$$

Если зафиксировать значения m переменных в МДР-коде $M \subset \Sigma^n$, то полученное множество называется **ретрактом размерности $n - m$** , $1 \leq m \leq n - 2$.

Из определения непосредственно следует, что ретракт МДР-кода является МДР-кодом меньшей размерности.

Определение

Если у n -квазигруппы f или у функции, обратной ей по некоторому аргументу, зафиксировать один или более аргументов, то мы получим квазигруппу некоторой меньшей размерности k , называемую **ретрактом** n -квазигруппы f .

Пусть имеется $(n - m + 1)$ -квазигруппа h и m -квазигруппа g , тогда их суперпозиция

$$f(x_1, \dots, x_n) \equiv h(g(x_1, \dots, x_m), x_{m+1}, \dots, x_n)$$

является n -квазигруппой.

Таким образом, класс квазигрупп замкнут относительно операций суперпозиции и взятия подфункции.

Определение

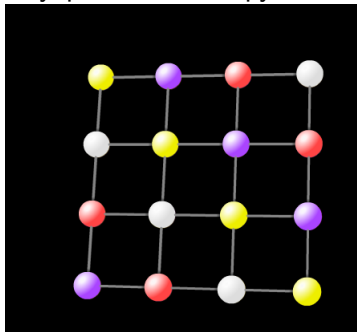
n -Квазигруппа f называется **разделимой (приводимой)**, если имеются целое число m , $2 \leq m < n$, $(n - m + 1)$ -квазигруппа h , m -квазигруппа g и перестановка $\sigma \in S_n$ такие, что

$$f(x_1, \dots, x_n) \equiv h(g(x_{\sigma(1)}, \dots, x_{\sigma(m)}), x_{\sigma(m+1)}, \dots, x_{\sigma(n)}).$$

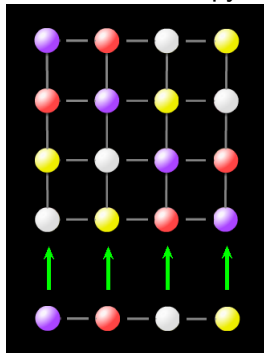
Геометрический критерий разделимости

Если n -квазигруппа порядка k при произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n - 1$, имеет только k различающихся ретракта, то она является разделимой.

Внутренняя квазигруппа:



Внешняя квазигруппа:

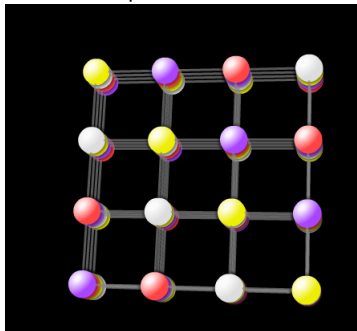


Геометрический критерий делимости

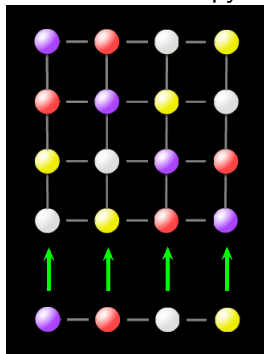
Если n -квазигруппа порядка k при произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n - 1$, имеет только k различающихся ретракта, то она является делимой.

Внутренняя квазигруппа $\rightarrow$

Композиция:



Внешняя квазигруппа:

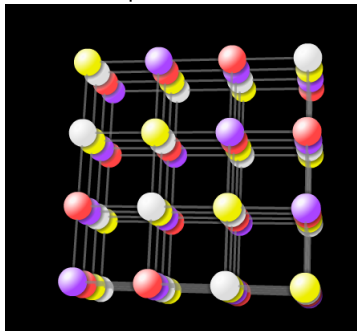


Геометрический критерий разделимости

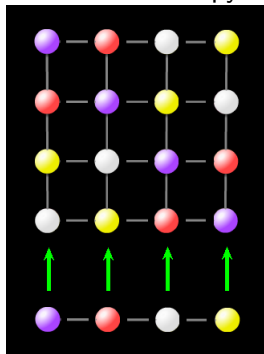
Если n -квазигруппа порядка k при произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n - 1$, имеет только k различающихся ретракта, то она является разделимой.

Внутренняя квазигруппа $\rightarrow$

Композиция:



Внешняя квазигруппа:

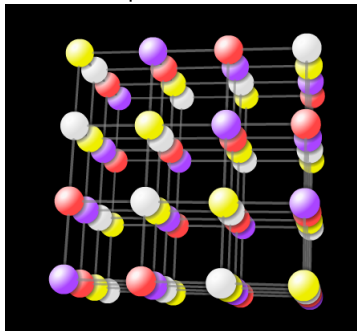


Геометрический критерий разделимости

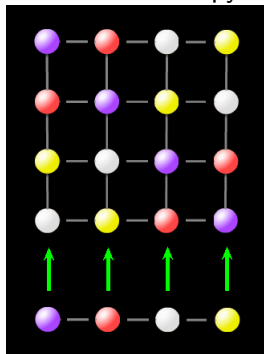
Если n -квазигруппа порядка k при произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n - 1$, имеет только k различающихся ретракта, то она является разделимой.

Внутренняя квазигруппа $\rightarrow$

Композиция:



Внешняя квазигруппа:

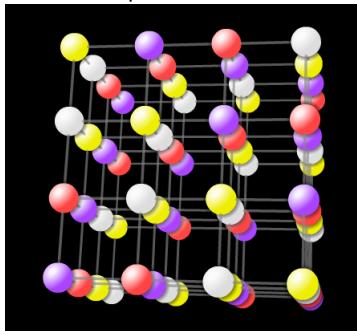


Геометрический критерий разделимости

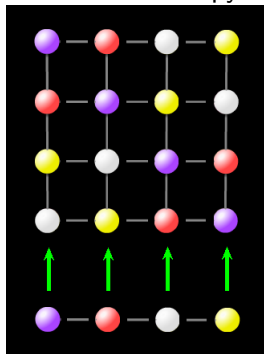
Если n -квазигруппа порядка k при произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n - 1$, имеет только k различающихся ретракта, то она является разделимой.

Внутренняя квазигруппа $\rightarrow$

Композиция:



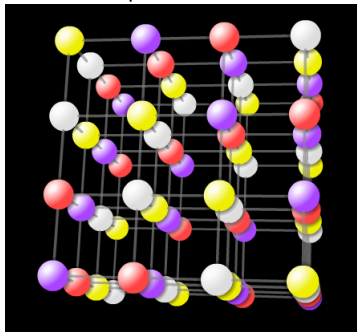
Внешняя квазигруппа:



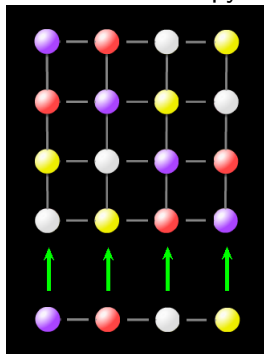
Геометрический критерий разделимости

Если n -квазигруппа порядка k при произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n - 1$, имеет только k различающихся ретракта, то она является разделимой.

Композиция:



Внешняя квазигруппа:



Теорема

Разделимую n -квазигруппу f можно представить в виде

$$f(\bar{x}) \equiv q_0(q_1(\tilde{x}_1), \dots, q_m(\tilde{x}_m)),$$

где q_j суть n_j -квазигруппы при любом j , $1 \leq j \leq m$, q_0 есть неразделимая m -квазигруппа, $\tilde{x}_j$ — некоторые наборы переменных x_i , $i \in I_j$, где $\{I_j\}_{j=1, \dots, m}$ — разбиение множества $[n]$ на наборы мощности $n_1, \dots, n_m$, причём при $m \geq 3$ в данном представлении разбиение $\{I_j\}_{j=1, \dots, m}$ единственно.

Черёмушкин А. В. Каноническое разложение n -арных квазигрупп // Матем. исследования. Кишинёв: "Штиинца", 1988.

Следствие

Если разделимая n -квазигруппа f имеет неразделимый ретракт арности $m \geq 2$, который не содержится в неразделимых ретрактах большей размерности, то МДР-код $M[f]$ можно представить в виде

$$M[f] = \{\bar{x} \in \Sigma^{n+1} \mid q_{m+1}(x_{n+1}, \tilde{x}_{m+1}) = q_0(q_1(\tilde{x}_1), \dots, q_m(\tilde{x}_m))\},$$

где q_j суть n_j -квазигруппы при $j, 1 \leq j \leq m+1$, q_0 есть неразделимая m -квазигруппа, $\tilde{x}_j$ — некоторые наборы переменных $x_i, i \in I_j$, где $\{I_j\}_{j=1, \dots, m+1}$ — разбиение множества $[n]$ на наборы мощности $n_1, \dots, n_{m+1}$.

Теорема

1. Пусть $3 < m + 1 < n$ и разделимы все ретракты размерностей m и $m + 1$ n -квазигруппы f порядка k , тогда f разделима.
2. Пусть $3 \leq m < n$, k — простое и разделимы все ретракты размерности m n -квазигруппы f порядка k , тогда f разделима.

Krotov D. S., Potapov V. N. On connection between reducibility on an n -ary quasigroup and that of its retracts // Discrete Math. 2011.

Krotov D. S. On reducibility of n -ary quasigroups // Discrete Math. 2008.

Krotov D. S. On irreducible n -ary quasigroups with reducible retracts // European J. Combin. 2008.

Zaslavsky T. Associativity in multary quasigroups: the way of biased expansions: eprint math.CO/0411268: arXiv.org, 2004.

Проблема Белоусова

Для каких n и k имеются неразделимые n -квазигруппы порядка k ?

Ответ

При любых $n > 2$ и $k > 3$.

Krotov D. S., Potapov V. N., Sokolova P. V. On reconstructing reducible n -ary quasigroups and switching subquasigroups // Quasigroups and Related Systems 2008.

Борисенко В. В. Неприводимые n -квазигруппы на конечных множествах составного порядка // Мат. Исслед. Квазигруппы и лупы. Кишинев: Штиинца, 1979.

Глухов М. М. К вопросу о приводимости главных парастрофов n -квазигрупп // Мат. Исслед. Квазигруппы и их системы. Кишинев: Штиинца, 1990.

Akivis M. A., Goldberg V. V. Solution of Belousov's problem // Discuss. Math., Gen. Algebra Appl. 2001.

Классификация n -квазигрупп порядка 4

Определение

Пусть $\Sigma = \{0, 1, 2, 3\}$. Объединение двух непересекающихся МДР-кодов называется **2-кратным МДР-кодом**. 2-Кратный МДР-код называется **линейным**, если он эквивалентен 2-кратному МДР-коду $L \subset \Sigma^n$ с линейной характеристической функцией

$$\chi_L(x_1, \dots, x_n) \equiv \chi_{\{0,1\}}(x_1) \oplus \dots \oplus \chi_{\{0,1\}}(x_n).$$

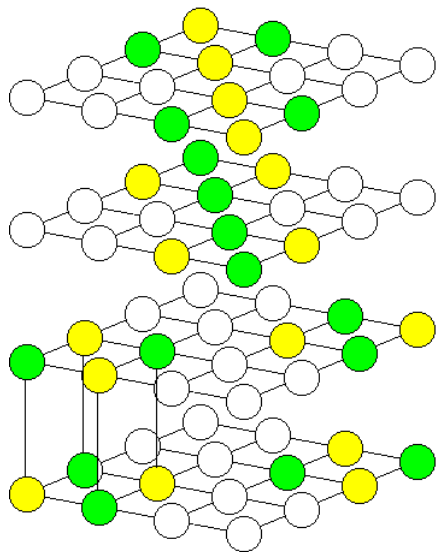
Пусть f — n -квазигруппа и $a, b \in \Sigma, a \neq b$. Множество

$$S_{a,b}(f) = \{(x_1, \dots, x_n) \in \Sigma^n \mid f(x_1, \dots, x_n) \in \{a, b\}\}$$

является 2-кратным МДР-кодом.

Определение

n -Квазигруппа f порядка 4 называется **полулинейной**, если для некоторых $a, b \in \Sigma$ множество $S_{a,b}(f)$ линейно.



Теорема

Каждая n -квазигруппа порядка 4 делима или полулинейна.

Krotov D. S., Potapov V. N. n -Ary quasigroups of order 4. SIAM J. Discrete Math., 2009.

Следствие

$Q(n, 4) = 3^{n+1}2^{2^n+1}(1 + o(1))$ при $n \rightarrow \infty$. $Q(n, k)$ — число n -квазигрупп порядка k .

Krotov D. S. On decomposability of 4-ary distance 2-MDS codes, double-codes, and n -quasigroups of order 4 // Discrete Math. 2008.

Потапов В. Н., Кротов Д. С. Асимптотика числа n -квазигрупп порядка 4 // Сиб. матем. журн. 2006.

Кротов Д. С. Нижние оценки числа m -квазигрупп порядка 4 и числа совершенных двоичных кодов // Дискрет. анализ и исслед. операций Сер. 1. 2000.

$Q'(n, k) = Q(n, k)/k((k-1)!)^n$ — число приведённых n -квазигрупп порядка k .

$n \backslash k$	3	4	5	6
2	1	4	56	9408
3	1	64	40256	95909896152
4	1	7132	31503556	— — —
5	1	201538000	50490811256	— — —

McKay B. D., Wanless I. M. A census of small Latin hypercubes // *SIAM J. Discrete Math.* 2008.

$$Q'(6, 4) = 432345572694417712,$$

$$Q'(7, 4) = 3987683987354747642922773353963277968$$

$$Q'(8, 4) = 678469272874899582559986240285280710364867063489779510427038722229750276832$$

$$Q'(9, 4) =$$

$$3928068729475370244015827636193118982659970455251677747379949641715360555691$$

$$7156893157982070341248647436315473464994454060134943960466816278059876072704$$

Теорема

$$2^{((k-3)/2)\lceil n/2 \rceil ((k-1)/2)\lfloor n/2 \rfloor} \leq Q(n, k) \leq 2^{c_k(k-2)^n},$$

где c_k не зависит от n .

Krotov D. S., Potapov V. N. On the number of n -ary quasigroups of finite order // arXiv.org eprint math., math.CO/0912.5453v1 принята в журнал Дискретная математика.

Теорема

$$Q(n, k) \leq \left(\frac{k}{e^n} (1 + o(1)) \right)^{k^n}$$

при $k \rightarrow \infty$.

Linial N., Luria Z. An upper bound on the number of high-dimensional permutation.
arXiv:1106.0649v1

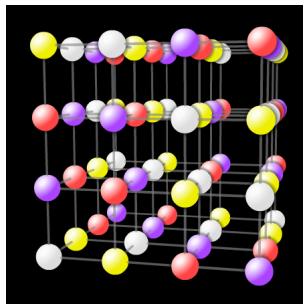
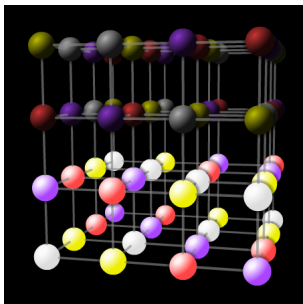
Брэгман Л. М. Некоторые свойства неотрицательных матриц и их перманентов
// Докл. АН СССР. 1973.

Дополняемость частичных n -квазигрупп

Определение

Частичная n -квазигруппа f **дополняема** если $f = q|_{\Sigma^{n-1} \times \Sigma'}$, т. е. f есть сужение некоторой n -квазигруппы q ($\Sigma' \subset \Sigma$).

Рассмотрим задачу о возможности дополнения частичных n -квазигрупп или о дополнении латинского параллелепипеда до латинского куба.



Известно, что дополняемость латинского прямоугольника до латинского квадрата является прямым следствием теоремы Кёнига. Кроме того, нетрудно показать, что любая n -квазигруппа $f : \Sigma^{n-1} \times \Sigma' \rightarrow \Sigma$ дополняема при $|\Sigma'| = 1$ или $|\Sigma'| = |\Sigma| - 1$.

Теорема

Для любых t и m при $m/2 < t < m - 2$ существует $m \times m \times t$ латинский параллелепипед, который не дополняется до латинского куба.

Kochol M. Relatively narrow latin parallelepipeds that cannot be extended to a latin cube // Ars Comb., 1995.

Kochol M. Latin $(n \times n \times (n - 2))$ -parallelepipeds not completing to a latin cube // Math. Slovaca, 1989.

Теорема

1. Для любых $m \geq 4$ существует $2m \times 2m \times m$ латинский параллелепипед, который не дополняется до $2m \times 2m \times 2m$ латинского куба.
2. Для любых чётных $m \notin \{2, 6\}$ существует $(2m - 1) \times (2m - 1) \times (m - 1)$ латинский параллелепипед, который не дополняется до $(2m - 1) \times (2m - 1) \times m$ латинского куба.

McKay B. D., Wanless I. M. A census of small Latin hypercubes // SIAM J. Discrete Math., 2008.

Bryant D., Cavenagh N. J., Maenhaut B., Pula K., Wanless I. M. Non-extendible Latin cuboids.

Теорема

Любая частичная n -квазигруппа порядка 4 дополняема.

Потапов В. Н. О дополняемости частичных n -квазигрупп порядка 4. Принята к публикации в Математические труды.

Совершенные коды

Определение

Множество $C \subset \Sigma^n$ называется **совершенным кодом с расстоянием 3**, если $|C \cap B(\bar{x})| = 1$ для любого единичного шара $B(\bar{x}) = \{\bar{y} \in \Sigma^n \mid d(\bar{x}, \bar{y}) \leq 1\}$.

Определение

Множество $C \subset \{0, 1\}^{n+1}$ называется **совершенным кодом с расстоянием 4** (расширенным совершенным кодом), если $|C| = 2^n/(n+1)$ и $d(\bar{x}, \bar{y}) \geq 4$ для любых различных $\bar{x}, \bar{y} \in C$.

Конструкция совершенных кодов

Пусть $E = \{0, 1\}$, $|\Sigma| = 4$. Зафиксируем $R \subset E^n$ — расширенный код Хэмминга. Пусть $M_{\bar{r}} \subset \Sigma^n$ — МДР-код. Определим разбиение E^4 на коды равенством

$C_a^r = C_0 + (1+r)\bar{e}_4 + \bar{e}_a$, где $r \in \{0, 1\}$, $a \in \Sigma$, $C_0 = \{\bar{0}, \bar{1}\} \subset E^4$, $\bar{e}_i \in E^4$ — единичные вектора с 1 на i -м месте.

Теорема

Множество

$$C = \bigcup_{\bar{r} \in R} \bigcup_{\bar{a} \in M_{\bar{r}}} C_{a_1}^{r_1} \times C_{a_2}^{r_2} \times \dots \times C_{a_n}^{r_n}. \quad (1)$$

является расширенным совершенным кодом.

Зиновьев В. А. Обобщённые каскадные коды // Проблемы передачи информации. 1976.

Phelps K. T. A general product construction for error correcting codes // SIAM J. Algebraic Discrete Methods. 1984.

Определение

Рангом кода называется размерность его аффинной оболочки.

Совершенные коды в E^n имеют ранги от $n - \log(n + 1)$ (код Хемминга) до n .

Теорема

Любой совершенный код, ранг которого не более чем на 2 превышает ранг линейного кода эквивалентен коду, удовлетворяющему равенству (1).

Avgustinovich S. V., Heden O., Solov'eva F. I. The classification of some perfect codes. Des. Codes Cryptogr. 2004.

Определение

i -Компонентой совершенного кода $C \subset E^n$ называется такое подмножество $K \subset C$, что множество $D = (C \cup (K + e_i)) \setminus K$ является совершенным кодом. При этом говорят, что код D получен из C **свитчингом** i -компоненты K .

Теорема

Совершенный код, ранг которого не более чем на 2 превышает ранг линейного кода может быть получен из линейного кода многократным свитчингом i -компонент.

Кротов Д. С., Потапов В. Н. О свитчинговой эквивалентности n -арных квазигрупп порядка 4 и совершенных двоичных кодов // Пробл. передачи информ. 2010.

Определение

Пусть $C \subset \Sigma^n$. Группой автоморфизмов $\text{Aut}(C)$ называется множество изометрий $\varphi \in \text{Aut}(\Sigma^n)$, $\varphi(C) = C$. Код C называется **транзитивным**, если $\text{Aut}(C)$ действует на нём транзитивно.

Теорема

При $n \rightarrow \infty$ имеется не менее $\frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}} (1 + o(1))$ попарно неэквивалентных транзитивных расширенных совершенных кодов длины $4n$.

Потапов В. Н. О нижней оценке числа транзитивных совершенных кодов // Дискрет. анализ и исслед. операций. Сер. 1. 2006.

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

Соловьёва Ф. И. О построении транзитивных кодов // Проблемы передачи информации. 2005.

Число совершенных кодов

Пусть $B(n)$ — число совершенных двоичных кодов длины n .

Тогда при $n = 2^t - 1$ имеем

$$2^{2^{\frac{n+1}{2} - \log(n+1)}} \cdot 3^{2^{\frac{n-3}{4}}} \dots \leq B(n) \leq 2^{2^{n - \frac{3}{2} \log n + \log \log(en)}}$$

Васильев Ю. Л. О негрупповых плотно упакованных кодах // Проблемы кибернетики. М.: Физматгиз, 1962.

Кротов Д. С. Нижние оценки числа m -квазигрупп порядка 4 и числа совершенных двоичных кодов // Дискретн. анализ и исслед. опер., 2004.

Krotov D. S., Avgustinovich S. V. On the number of 1-perfect binary codes: a lower bound // IEEE Transactions on Information Theory, 2008.

Августинович С. В. Об одном свойстве совершенных двоичных кодов // Дискретн. анализ и исслед. опер., 1995.

Имеется 5983 неэквивалентных совершенных кода длины 15 и 2165 неэквивалентных расширенных совершенных кода длины 16.

Ostergard P. R. J., Potttonen O. The perfect binary one-error-correcting codes of length 15. I. Classification. *IEEE Trans. Inform. Theory*, 2009.

Ostergard P. R. J., Potttonen O., Phelps K. T. The perfect binary one-error-correcting codes of length 15: Part II-properties. *IEEE Trans. Inform. Theory*, 2010.

Пусть $P(n, q)$ — число совершенных q -ичных кодов длины n .
Тогда при $n = \frac{q^t - 1}{q - 1}$, q — степень простого числа имеем

Теорема

$$P(n, q) \geq \left(Q\left(\frac{n-1}{q}, q\right) \right)^{R\left(\frac{n-1}{q}\right)},$$

где $R(m) = \frac{q^m}{mq - q + 1}$ — мощность q -значного совершенного кода длины m .

Heden O., Krotov D. S. On the structure of non-full-rank perfect q -ary Codes // Advances in Mathematics of Communications, 2011.

Работа выполнена при поддержке

Российского фонда фундаментальных исследований

проект 10-01-00424 "Совершенные структуры",

проект 10-01-00616 " n -Арные квазигруппы конечного порядка"

и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009-2013 гг.

гос. контракт №02.740.11.0429 "Фундаментальные проблемы современной математики"