ЛИТЕРАТУРА

1. *Власова А. В.* Исследование эволюционных параметров в динамических системах двоичных векторов // Свид. о гос. регистрации программы для ЭВМ № 2009614409, выданное Роспатентом. Зарегистрировано в Реестре программ для ЭВМ 20 августа 2009 г.
2. *Жаркова А. В.* О ветвлении и непосредственных предшественниках состояний в конечной динамической системе всех возможных ориентаций графа // Прикладная дискретная математика. Приложение. 2013. № 6. С. 76–78.
3. *Жаркова А. В.* Недостижимые состояния в динамических системах, ассоциированных с цепями и циклами // Изв. Сарат. ун-та. Нов. сер. 2011. Т. 11. Сер. Математика. Механика. Информатика. Вып. 4. С. 116–123.
4. *Салий В. Н.* Об одном классе конечных динамических систем // Вестник Томского государственного университета. Приложение. 2005. № 14. С. 23–26.
5. *Barbosa V. C.* An Atlas of Edge-reversal Dynamics. Boca Raton: Chapman & Hall/CRC, 2001. 385 p.
6. *Власова А. В.* Динамические системы, определяемые пальмами // Компьютерные науки и информационные технологии: Материалы Междунар. науч. конф. Саратов: Изд-во Сарат. ун-та, 2009. С. 57–60.

УДК 519.7 DOI 10.17223/2226308X/8/45

СОВЕРШЕННЫЕ ДВОИЧНЫЕ КОДЫ БЕСКОНЕЧНОЙ ДЛИНЫ[1]

С. А. Малюгин

Подмножество C в бесконечномерном двоичном кубе $\{0,1\}^{\mathbb{N}}$ называется совершенным двоичным кодом с расстоянием 3, если все шары единичного радиуса (в метрике Хемминга) с центрами из C попарно не пересекаются и их объединение покрывает куб $\{0,1\}^{\mathbb{N}}$. Аналогичным образом определяется совершенный двоичный код в нулевом слое $\{0,1\}^{\mathbb{N}}_0$, состоящем из всех векторов куба $\{0,1\}^{\mathbb{N}}$, имеющих конечные носители. В работе доказывается, что мощность множества всех классов эквивалентности совершенных двоичных кодов в нулевом слое $\{0,1\}^{\mathbb{N}}_0$ равна континууму, а мощность множества классов эквивалентности совершенных двоичных кодов во всём кубе — гиперконтинууму.

Ключевые слова: *совершенные двоичные коды, код Хемминга, расстояние Хемминга, коды Васильева, классы эквивалентности, континуум, гиперконтинуум.*

1. Основные определения

Пусть $\mathbb{N}$ — множество натуральных чисел. *Бесконечномерный куб* $\{0,1\}^{\mathbb{N}}$ состоит из всевозможных бесконечных последовательностей $u = (u_1, \ldots, u_n, \ldots)$, где $u_n \in \{0,1\}$; $n \in \mathbb{N}$. Сумма двух элементов $u, v \in \{0,1\}^{\mathbb{N}}$ определяется формулой $u + v = (u_1 \oplus v_1, \ldots, u_n \oplus v_n, \ldots)$, где $u = (u_1, \ldots, u_n, \ldots)$, $v = (v_1, \ldots, v_n, \ldots)$ и $u_n \oplus v_n$ — сумма элементов u_n, v_n в двухэлементном поле Галуа $\mathrm{GF}(2) = \{0,1\}$. Относительно такой операции сложения куб $\{0,1\}^{\mathbb{N}}$ является бесконечномерным векторным пространством над полем $\mathrm{GF}(2)$. Элементы куба $\{0,1\}^{\mathbb{N}}$ далее будем называть векторами. Нулевой вектор обозначаем через $\mathbf{0}$, а базисные векторы с единичной i-й координатой — через $e_i = (0, \ldots, 0, \underset{i}{1}, 0, \ldots)$. *Носитель* вектора $u \in \{0,1\}^{\mathbb{N}}$ (множество индексов i, для которых $u_i = 1$) обозначается через $[u]$. Число ненулевых координат вектора u называется его *весом* и обозначается через $|u|$. В отличие от конечномерного случая вес может

[1]Работа поддержана грантами РФФИ № 13-01-00463; 14-01-00507.

принимать также значение ∞. *Расстояние Хемминга* между векторами $u, v \in \{0,1\}^{\mathbb{N}}$ определяется как $|u+v|$. Расстояние Хемминга задаёт в пространстве $\{0,1\}^{\mathbb{N}}$ «обобщённую» *метрику Хемминга* со значениями в $\mathbb{N} \cup \{\infty\}$.

Определение 1. Подмножество C в бесконечномерном двоичном кубе $\{0,1\}^{\mathbb{N}}$ называется *совершенным двоичным кодом с расстоянием* 3, если все шары единичного радиуса (в метрике Хемминга) с центрами из C попарно не пересекаются и их объединение покрывает куб $\{0,1\}^{\mathbb{N}}$.

Следует отметить, что изучение кодов бесконечной длины (МДР-кодов, задаваемых квазигруппами с бесконечным числом аргументов) впервые было предпринято В. Н. Потаповым в [1]. Рассмотрим в $\{0,1\}^{\mathbb{N}}$ следующее отношение эквивалентности: $u \sim v \iff |u+v| \neq \infty$ $(u, v \in \{0,1\}^{\mathbb{N}})$. Куб $\{0,1\}^{\mathbb{N}}$ относительно этого отношения разбивается на попарно не пересекающиеся классы эквивалентности, которые далее будем называть *слоями* куба $\{0,1\}^{\mathbb{N}}$. Слой, содержащий нулевой вектор, будем обозначать символом $\{0,1\}^{\mathbb{N}}_0$ и называть его *нулевым слоем.* Он состоит из всех векторов конечного веса (такие векторы будем называть *финитными*). Очевидно, что нулевой слой является подпространством в $\{0,1\}^{\mathbb{N}}$, а любой другой слой $\mathcal{L}$ является смежным классом по этому подпространству. Пусть $\mathcal{L}$ — произвольный слой в кубе $\{0,1\}^{\mathbb{N}}$.

Определение 1′. Подмножество $C \subset \mathcal{L}$ называем совершенным двоичным кодом слоя $\mathcal{L}$, если все шары единичного радиуса с центрами из C попарно не пересекаются и их объединение покрывает слой $\mathcal{L}$.

Легко видеть, что изучение совершенных кодов в кубе $\{0,1\}^{\mathbb{N}}$ фактически сводится к изучению совершенных кодов в нулевом слое $\{0,1\}^{\mathbb{N}}_0$.

Совершенный код в $\{0,1\}^{\mathbb{N}}_0$ называется *кодом Хемминга*, если он является линейным подпространством в $\{0,1\}^{\mathbb{N}}_0$. Код Хемминга H^∞ можно определить следующим образом. Для конечных n код Хемминга H^n длины $n = 2^k - 1$ $(k > 1)$ определяется стандартным образом. Добавляя справа к векторам $u \in H^n$ бесконечное число нулевых координат, можно вложить код H^n в нулевой слой $\{0,1\}^{\mathbb{N}}_0$. Это вложение будем обозначать символом $\widetilde{H}^n$. Тогда, так как $\widetilde{H}^n \subset \widetilde{H}^{2n+1}$ $(n = 2^k - 1)$, можно положить $H^\infty = \bigcup\limits_{k=2}^{\infty} \widetilde{H}^{2^k-1}$.

2. Эквивалентность линейных совершенных кодов в нулевом слое и их группа автоморфизмов

Как и в конечномерном случае, для любой изометрии $A : \{0,1\}^{\mathbb{N}}_0 \to \{0,1\}^{\mathbb{N}}_0$ существует вектор $a \in \{0,1\}^{\mathbb{N}}_0$ и перестановка $\pi : \mathbb{N} \to \mathbb{N}$, такие, что $A(u) = \widetilde{\pi}(u) + a$, где $\widetilde{\pi}((u_1, \ldots, u_n, \ldots)) = (u_{\pi^{-1}(1)}, \ldots, u_{\pi^{-1}(n)}, \ldots)$.

Определение 2. Два совершенных двоичных кода $C_1, C_2 \subset \{0,1\}^{\mathbb{N}}_0$ называются эквивалентными, если существует изометрия A нулевого слоя $\{0,1\}^{\mathbb{N}}_0$, такая, что $A(C_1) = C_2$. Два совершенных двоичных кода $C_1, C_2 \subset \{0,1\}^{\infty}_0$ называются изоморфными, если существует перестановка $\pi : \mathbb{N} \to \mathbb{N}$, такая, что $\widetilde{\pi}(C_1) = C_2$.

Лемма 1. Все коды Хемминга в слое $\{0,1\}^{\mathbb{N}}_0$ эквивалентны между собой.

3. Континуальность множества классов эквивалентности совершенных двоичных кодов бесконечной длины

В коде Хемминга H^∞ рассмотрим подпространство R_i, порождённое всеми векторами веса 3 с i-й координатой равной единице. Всевозможные смежные классы вида

$R_i^u = R_i + u$ $(u \in H^\infty)$ называются *i-компонентами* кода H^∞, $i \in \mathbb{N}$. Рассмотрим некоторое семейство $\mathcal{B} = \left\{R_{i_1}^{u_1}, R_{i_2}^{u_2}, \dots\right\}$, состоящее из конечного или бесконечного числа попарно не пересекающихся i_p-компонент, где $\mathbf{u}_p \in H^\infty$, $1 \leqslant p < m+1$ $(m \in \mathbb{N} \cup \{\infty\})$. Одна из основных конструкций нелинейных совершенных двоичных кодов состоит в том, что в коде H^n сдвигаются по координатам i_p все компоненты из семейства $\mathcal{B}$. Доказательство этого факта в точности такое же, как и в случае кодов конечной длины [2–5]. Далее будем говорить, что код $H^\infty(\mathcal{B})$ построен из кода Хемминга H^∞ *сдвигами* (или *свитчингами*) компонент из семейства $\mathcal{B}$. Если при фиксированном индексе i имеем $i_p = i$ для всех p, то код $H^\infty(\mathcal{B})$ называем *кодом Васильева* бесконечной длины. Такие коды конечной длины впервые были построены в [6]. Для нахождения мощности множества всех классов эквивалентности кодов бесконечной длины достаточно ограничиться рассмотрением кодов Васильева.

Положим $i = 1$. Компонента R_1 порождается всеми векторами v_p веса 3 с носителями $[v_p] = \{1, 2p, 2p+1\}$, $p \in \mathbb{N}$. Рассмотрим векторы $w_1 = 0$, $w_p = e_8 + e_9 + \dots + e_{2^{p+2}-2}$, $p \in \mathbb{N}$, $p \geqslant 2$. Из определения проверочной матрицы следует, что $w_p \in H^\infty$, $p \in \mathbb{N}$. Для бесконечного семейства компонент $\mathcal{B}_1 = \{R_1^{w_p}\}_{p=1}^\infty$ и любого $\varepsilon \in \{0,1\}^\mathbb{N}$ $(\varepsilon = (\varepsilon_1, \varepsilon_2, \dots))$ рассмотрим следующий код Васильева:

$$H^\infty(\mathcal{B}_1, \varepsilon) = \left(H^\infty \setminus \bigcup_{p=1}^{\infty} R_1^{w_p}\right) \cup \left(\bigcup_{p=1}^{\infty} \left(R_1^{w_p} + \varepsilon_p e_1\right)\right).$$

То есть код $H^\infty(\mathcal{B}_1, \varepsilon)$ получается из кода Хемминга H^∞ сдвигами только тех компонент $R_1^{u_p}$ из семейства $\mathcal{B}_1$, для которых $\varepsilon_p = 1$.

Лемма 2. Пусть L — любое линейное пространство над полем GF(2) и $H \subset L$ — его подпространство. Пусть $A : L \to L$ — аффинный изоморфизм пространства L и $F : L \to \{0,1\}^3$ — линейное отображение, такое, что $F(H) = \{0,1\}^3$ и $F \circ A(H) = \{0,1\}^3$. Рассмотрим два подмножества $C_1, C_2 \subset L$, удовлетворяющих условиям

$$C_1 \setminus \mathrm{Ker} F = C_2 \setminus \mathrm{Ker} F = H \setminus \mathrm{Ker} F,$$
$$C_1 \setminus H \subset \mathrm{Ker} F, \quad C_2 \setminus H \subset \mathrm{Ker} F.$$

Тогда если $A(C_1) = C_2$, то $A(H) \subseteq H$ и $a \in H$.

Эта лемма позволяет доказать следующий ключевой факт.

Теорема 1. Если $\varepsilon, \varepsilon' \in \{0,1\}^\mathbb{N}$, $\varepsilon \neq \varepsilon'$ $\varepsilon_1 = \varepsilon'_1 = 1$, то коды Васильева $H^\infty(\mathcal{B}_1, \varepsilon)$, $H^\infty(\mathcal{B}_1, \varepsilon')$ не эквивалентны.

Мы построили континуум попарно не эквивалентных кодов Васильева бесконечной длины. Так как в счётном множестве $\{0,1\}_0^\mathbb{N}$ может быть не более континуума различных кодов, то из теоремы 1 сразу получается

Следствие 1. Мощность множества всех классов эквивалентности совершенных двоичных кодов бесконечной длины равна континууму.

4. Совершенные двоичные коды в кубе $\{0,1\}^\mathbb{N}$

Существование совершенных двоичных кодов в кубе $\{0,1\}^\mathbb{N}$ сразу следует из существования таких кодов в слое $\{0,1\}_0^\mathbb{N}$. Для этого пронумеруем все слои числами из отрезка $[0,1]$, т. е. каждому числу $\alpha \in [0,1]$ сопоставляем слой $\mathcal{L}_\alpha \subset \{0,1\}^\mathbb{N}$, при этом $\{0,1\}^\mathbb{N} = \bigcup\limits_{\alpha \in [0,1]} \mathcal{L}_\alpha$. Выберем в каждом слое по одному элементу u_α и для любого совершенного кода $C_0 \subset \mathcal{L}_0 = \{0,1\}_0^\mathbb{N}$ полагаем $C = \bigcup\limits_{\alpha \in [0,1]} (C_0 + u_\alpha)$. Очевидно, множество C

является совершенным двоичным кодом в $\{0,1\}^{\mathbb{N}}$. Отметим, что при построении кода C была применена аксиома выбора.

Лемма 3. В кубе $\{0,1\}^{\mathbb{N}}$ существуют линейные совершенные двоичные коды.

Посмотрим, как устроены изометрии куба $\{0,1\}^{\mathbb{N}}$. Так как разные слои этого куба находятся на бесконечном расстоянии Хемминга друг от друга, то изометрия допускает, во-первых, произвольную перестановку (континуального) множества всех слоев. Далее, в каждом слое $\mathcal{L}_\alpha$ допускается (независимо от других слоёв) перестановка координат π_α и перенос на вектор $a_\alpha \in \{0,1\}^{\mathbb{N}}_0$. Изометрия может не быть аффинным преобразованием всего куба. На этом основании вводим два различных определения.

Определение 3. Два совершенных кода $C_1, C_2 \subset \{0,1\}^{\mathbb{N}}$ называются *изометричными* (соответственно, *эквивалентными*), если существует изометрия A пространства $\{0,1\}^{\mathbb{N}}$ (соответственно, изометрия, являющаяся аффинным преобразованием пространства $\{0,1\}^{\mathbb{N}}$), такая, что $A(C_1) = C_2$.

Лемма 4. Все линейные совершенные коды в $\{0,1\}^{\mathbb{N}}$ эквивалентны между собой.

Мощность континуума принято обозначать символом $\mathfrak{c}$. Мощность всех подмножеств континуального множества будем обозначать символом $2^{\mathfrak{c}}$. Эту мощность называют также *гиперконтинуумом*.

Пример 1. В пространстве $\{0,1\}^{\mathbb{N}}$ строится гиперконтинуальное семейство линейных совершенных двоичных кодов $\mathcal{H} = \{H_\gamma\}_{\gamma\in\Gamma}$, такое, что для любых $H_{\gamma_1}, H_{\gamma_2} \in \mathcal{H}$ $(\gamma_1 \neq \gamma_2)$ не существует ни одной перестановки $\pi : \mathbb{N} \to \mathbb{N}$, такой, что $H_{\gamma_2} = \widetilde{\pi}(H_{\gamma_1})$.

Теорема 2. Мощность множества всех классов эквивалентности совершенных двоичных кодов в пространстве $\{0,1\}^{\mathbb{N}}$ равна гиперконтинууму $2^{\mathfrak{c}}$.

ЛИТЕРАТУРА

1. *Потапов В. Н.* Бесконечномерные квазигруппы конечных порядков // Матем. заметки. 2013. Т. 93. Вып. 3. С. 457–460.
2. *Августинович С. В., Соловьева Ф. И.* Построение совершенных двоичных кодов последовательными сдвигами $\widetilde{\alpha}$-компонент // Проблемы передачи информации. 1997. Т. 33. Вып. 3. С. 15–21.
3. *Романов А. М.* О построении совершенных нелинейных двоичных кодов инверсией символов // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4. №1. С. 46–52.
4. *Phelps K. T. and LeVan M. J.* Kernels of nonlinear Hamming codes // Designs, Codes and Cryptogr. 1995. V. 6. No. 3. P. 247–257.
5. *Solov'eva F. I.* Switchings and perfect codes // Numbers, Information and Complexity. Dordrecht: Kluver Acad. Publ., 2000. P. 311–324.
6. *Васильев Ю. Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. М.: Физматгиз, 1962. Вып. 8. С. 75–78.

УДК 512.6 DOI 10.17223/2226308X/8/46

ЭНЕРГОСБЕРЕГАЮЩЕЕ ПРОТИВОГОНОЧНОЕ КОДИРОВАНИЕ СОСТОЯНИЙ АСИНХРОННОГО АВТОМАТА

Ю. В. Поттосин

Рассматривается задача противогоночного кодирования состояний асинхронного автомата, где наряду с минимизацией длины кода состояния минимизируется