

## СОВЕРШЕННЫЕ КОДЫ ПОЛНОГО РАНГА С ЯДРАМИ БОЛЬШИХ РАЗМЕРНОСТЕЙ\*)

*С. В. Августинович, Ф. И. Соловьева, У. Хеден*

Построены совершенные коды всех допустимых длин  $n > 2^{10} - 1$  полного ранга с ядрами всех возможных размерностей  $K$  от  $(n-1)/2$  до  $U(n)$  — максимально возможной. Такие коды длины  $n$ ,  $31 \leq n \leq 2^{10} - 1$  построены при каждом  $k \in \{(n-1)/2, \dots, U(n)-2\}$ .

*Совершенным двоичным кодом  $C$  длины  $n$  с кодовым расстоянием 3* (далее совершенным кодом) называется такое подмножество  $n$ -мерного векторного пространства  $E^n$  над  $GF(2)$ , что для любого вектора  $y \in E^n$  имеется такое единственное кодовое слово  $x \in C$ , что  $d(x, y) \leq 1$ , где  $d$  — расстояние Хемминга. Совершенные двоичные коды длины  $n$  с расстоянием 3 существуют только при  $n = 2^m - 1, m > 1$ . Размерность подпространства  $\langle C \rangle$  называется *рангом*  $r = r(C)$  кода  $C$ . *Ядром*  $\text{Ker}(C)$  кода  $C$  называется совокупность его *периодов*, т. е. кодовых слов  $x \in C$  таких, что  $x + C = C$ . Размерность ядра обозначим через  $k = k(C)$ .

Ранги и ядра совершенных кодов исследовались в нескольких статьях [1–14]. У. Хеден [8] описал совершенные коды длины 15 с ядрами размера 1, 2, 3. Т. Этцион и А. Варди [6] построили совершенные коды длины  $n \geq 15$  всех допустимых рангов. В [13] доказано существование нелинейного совершенного кода длины  $n \geq 15$  с ядром размерности  $k$ ,  $k = 1, 2, \dots, n - m - 2$ . В [4] для каждого  $n > 127$  были построены несистематические совершенные коды полного ранга с тривиальной группой автоморфизмов (и, следовательно, с тривиальным ядром размерности 1). С. А. Малюгин [10] для каждого  $n > 15$  построил систематические совершенные коды с такими же свойствами. Т. Этцион и А. Варди в [7] поставили вопрос об описании совокупности допустимых пар чисел  $(r, k)$ , для каждой из которых существует совершенный

---

\*) Исследование выполнено при поддержке Шведского института. Исследование С. В. Августиновича выполнено при финансовой поддержке голландско-российской программы NWO (грант 047–008–006), Ф. И. Соловьевой — при финансовой поддержке Российского фонда фундаментальных исследований (проект 00–01–00822).

код длины  $n$  с рангом  $r$  и ядром размерности  $k$ . Там же они доказали, что для каждого  $n \geq 2^m - 1, m > 3$ , верхняя оценка размерности ядра совершенного кода длины  $n$  полного ранга равна  $U(n) = n - m - \delta$ , где  $\delta$  — наименьшее число такое, что  $2^\delta - \delta - 1 \geq m$ ; оценка достижима для каждого  $n \geq 2^{10} - 1$ . К. Фелпсом и М. Виллануевой [14] установлены верхняя и нижняя оценки пар чисел  $(r, k)$ , для которых существуют совершенные коды длины  $n \geq 15$  с рангом  $r$  и размерностью ядра, равной  $k$ . Они же доказали, что эти оценки точны (за исключением верхней оценки для кодов длины 15), и построили совершенные коды длины  $n$  с рангом  $r$  и размерностью ядра  $k$  для каждой допустимой пары  $(r, k)$ , где  $k > n - 2m, r < n$ . В работе [3] построены совершенные коды длины  $n > 15$  для всех возможных пар  $(r, k)$ , где  $r < n$ . В [2] дана классификация кодов рангов  $n - m + 1$  и  $n - m + 2$ . Для  $n = 15$  известны совершенные коды длины 15 с ядрами размерности  $k, 1 \leq k \leq 5$  [7, 8, 11]; для  $k \geq 7$  совершенные коды полного ранга не существуют [7, 15], для  $k = 6$  вопрос о существовании таких кодов остается открытым. Для  $r < 15$  обнаружены совершенные коды длины 15 для всех возможных пар  $(r, k)$  [12].

В настоящей статье исследуются совершенные коды длины  $n$  полного ранга с ядрами размерности  $k \geq (n - 1)/2$ . С учетом известных результатов для кодов длин  $2^{10} - 1$  и 15 полного ранга известная итеративная конструкция Васильева [1] позволяет строить совершенные коды длины  $n > 2^{10} - 1$  полного ранга с ядрами размерности  $k$ , где  $k = (n - 1)/2, \dots, U(n)$ , и для каждого  $n, 31 \leq n \leq 2^{10} - 1$ , — коды длины  $n$  полного ранга с ядрами каждой размерности  $k \in \{(n - 1)/2, \dots, U(n) - 2\}$ .

Напомним конструкцию кодов Васильева [1]. Пусть  $C'$  — произвольный совершенный код длины  $(n - 1)/2 = 2^{m-1} - 1, m \geq 2$ ,  $\lambda$  — произвольная функция из  $C'$  в множество  $\{0, 1\}$ .

Множество

$$C = \{(u, u + v, |u| + \lambda(v)) \mid u \in E^{(n-1)/2}, v \in C'\}$$

является совершенным кодом длины  $n$ , где  $|u| = u_1 + \dots + u_{(n-1)/2} \pmod{2}$ .

В дальнейшем потребуется следующая

**Теорема 1** (см. [7], а также [14]). Пусть  $C$  — совершенный код длины  $n$  и ранга  $r(C) = n - m + p$  с ядром размерности  $k(C) = n - m - \delta$ . Тогда  $2^\delta - \delta - 1 \geq p$ .

**Доказательство.** Рассмотрим разложение совершенного кода  $C$  на классы смежности по ядру  $\text{Ker}(C)$ :

$$C = \text{Ker}(C) \cup (v^1 + \text{Ker}(C)) \cup \dots \cup (v^s + \text{Ker}(C)),$$

где  $v^i$  — лидер класса смежности  $v^i + \text{Ker}(C)$ ,  $s = |C|/|\text{Ker}(C)| - 1$ . Так как каждый класс смежности дает самое большее одно линейно независимое слово, то  $r(C) \leq k(C) + s$ . С учетом соотношений  $r(C) = n - m + p$

и  $k(C) = n - m - \delta$  имеем

$$n - m + p \leq n - m - \delta + \frac{2^{n-m}}{2^{n-m-\delta}} - 1.$$

Следовательно,  $2^\delta - \delta - 1 \geq p$ .

**Теорема 2.** Пусть существует совершенный код длины  $(n-1)/2$  полного ранга с ядром максимальной размерности. Тогда существует совершенный код  $C$  длины  $n$  полного ранга с ядром размерности  $k(C)$ , где  $k(C) = (n-1)/2, \dots, U(n)$ .

**Доказательство.** Пусть  $C'$  — совершенный код длины  $(n-1)/2$  полного ранга с ядром максимальной размерности, равной  $U((n-1)/2)$ . Пусть  $B'$  — база пространства  $\langle C' \rangle$  размерности  $(n-1)/2$  и  $B$  — база ядра  $\text{Ker}(C')$  максимальной размерности  $U((n-1)/2)$ ,  $B \subset B'$ . Рассмотрим подпространство  $A$  в ядре  $\text{Ker}(C')$  и определенный выше код Васильева. Будем различать три случая.

**Случай 1.**  $0 \leq |A| < |\text{Ker}(C')|$ . В этом случае определим нелинейную функцию  $\lambda$  для кода  $C$  следующим образом:  $\lambda(v) = 0$  тогда и только тогда, когда  $v \in A$ . Рассмотрим произвольное ненулевое кодовое слово  $v' \in \text{Ker}(C') \setminus A$  и произвольное кодовое слово  $v'' \in B' \setminus B$ . Так как  $v'$  принадлежит ядру кода  $C'$ , то  $v' + v'' \in C'$ . По определению кода  $C$  имеем  $\lambda(v' + v'') = 1$ . Следовательно,

$$w = (0^{(n-1)/2}, v' + v'', 1) \in C,$$

где  $0^{(n-1)/2}$  — нулевое слово длины  $(n-1)/2$ . Пусть  $e_i$  — слово длины  $(n-1)/2$  с единственной  $i$ -й единичной координатой. Нетрудно видеть, что следующие  $n$  кодовых слов кода  $C$  линейно независимы:

$$\begin{cases} (e_i, e_i, 1), \text{ где } i = 1, \dots, (n-1)/2; \\ (0^{(n-1)/2}, v, \lambda(v)), v \in B'; \\ w. \end{cases}$$

Отсюда следует, что  $C$  — код полного ранга.

Очевидно, что в этом случае

$$\text{Ker}(C) = \{(u, u, |u|) \mid u \in E^{(n-1)/2}\} + \{0^{(n-1)/2}, v, 0 \mid v \in A\}.$$

Следовательно,

$$k(C) = (n-1)/2 + k', \quad (1)$$

где  $k' = |A|$ ,  $0 \leq k' < U((n-1)/2)$ .

**Случай 2.**  $|A| = |\text{Ker}(C')|$ , где  $\text{Ker}(C')$  максимально и  $2^\delta - \delta - 1 > \log(n+1)/2$  для кода  $C'$ . В этом случае по теореме 1 число классов

смежности кода  $C'$  строго больше  $r(C') - k(C') + 1$ . Следовательно, существует слово  $v' \in C'$ , не принадлежащее ни одному классу смежности с представителями из  $B'$ . Положим  $\lambda(v) = 1$  тогда и только тогда, когда  $v \in v' + \text{Ker}(C')$ . По определению кода  $C$  имеем  $(0^{(n-1)/2}, v', 1) \in C$ . Кодовые слова  $(e_i, e_i, 1)$ , где  $i = 1, \dots, (n-1)/2$ ;  $(0^{(n-1)/2}, v, 0)$ ,  $v \in B'$ , и  $(0^{(n-1)/2}, v', 1)$  кода  $C$  определяют базу  $\langle C \rangle$  размерности  $n$ . Отсюда вытекает, что  $C$  — код полного ранга.

Из  $2^\delta - \delta - 1 > \log(n+1)/2$  вытекает неравенство  $2^\delta - \delta - 1 \geq \log(n+1)$  для длины кода. Следовательно, по теореме 1 размерность максимального ядра произвольного совершенного кода полного ранга длины  $n$ , удовлетворяющей последнему неравенству, должна быть равна  $n - m - \delta$ .

Ядро кода  $C$  равно

$$\text{Ker}(C) = \{(u, u, |u|) \mid u \in E^{(n-1)/2}\} + \{0^{(n-1)/2}, v, 0 \mid v \in \text{Ker}(C')\}.$$

Следовательно,  $k(C) = (n-1)/2 + U((n-1)/2) = n - m - \delta$ , т. е. ядро максимально.

**Случай 3.**  $|A| = \text{Ker}(C')$ , где  $\text{Ker}(C')$  максимально и

$$2^\delta - \delta - 1 = \log(n+1)/2 \quad (2)$$

для кода  $C'$ . В этом случае по теореме 1 число классов смежности кода  $C'$  в точности равно  $r(C') - k(C') + 1$ . Положим  $\lambda(v) = 0$  тогда и только тогда, когда  $v \in A'$ , где  $A'$  — подпространство  $\text{Ker}(C')$  размерности  $k(C') - 1$ . Далее рассуждения относительно ранга кода  $C$  проводим аналогично рассуждениям, рассматриваемым в случае 1.

Покажем, что размерность  $k(C)$  ядра кода  $C$  максимальна. Из равенства (2) имеем  $2^\delta - \delta = \log(n+1)$ , и, следовательно, для  $\delta' = \delta + 1$  справедливо неравенство  $2^{\delta'} - \delta' - 1 \geq \log(n+1)$ . По теореме 1 это означает, что максимальное значение размерности ядра произвольного совершенного кода длины  $n$ , удовлетворяющей последнему неравенству, равно  $n - m - \delta' = n - m - \delta - 1$ . С другой стороны, из равенства (1) для кода  $C$  следует, что

$$k(C) = (n-1)/2 + (n-1)/2 - \log\left(\frac{n+1}{2}\right) - \delta - 1 = n - m - \delta - 1,$$

т. е.  $C$  — код полного ранга с максимальным ядром. Теорема доказана.

Из теоремы 2 с учетом существования совершенного кода длины  $2^{10} - 1$  с максимальным ядром и совершенного кода длины 15 с ядром размерности 5 получаем приведенные ниже следствия.

**Следствие 1.** Существуют совершенные коды длины  $n > 2^{10} - 1$  полного ранга с ядрами каждой размерности  $k \in \{(n-1)/2, \dots, U(n)\}$ .

**Следствие 2.** Существуют совершенные коды длины  $n$ ,  $31 \leq n \leq 2^{10} - 1$ , полного ранга с ядрами каждой размерности  $k \in \{(n-1)/2, \dots, U(n) - 2\}$ .

**Замечание 1.** Аналогичный подход с использованием кодов Васильева позволяет строить совершенные коды длины  $n$ ,  $n > 15$ , ранга  $r$ ,  $n - m + 1 \leq r \leq n - 1$ , с ядром размерности  $k$  для каждого  $k$  от  $(n-1)/2$  до максимального значения включительно [3].

**Замечание 2.** Интересно выяснить эквивалентность кодов полного ранга с максимальным ядром, полученных из теоремы 2 и следствия 1, и кодов с такими же свойствами из [7], а также выяснить существование совершенных кодов полного ранга с не указанными в следствиях 1 и 2 размерностями ядер.

## ЛИТЕРАТУРА

1. **Васильев Ю. Л.** О негрупповых плотно упакованных кодах // Проблемы кибернетики. М.: Физматгиз, 1962. Вып. 8. С. 337–339.
2. **Avgustinovich S. V., Heden O., Solov'eva F. I.** The classsification of some perfect codes. Stockholm: Royal Inst. of Technology, 2001. (Preprint / Trita-mat.-2001-9).
3. **Avgustinovich S. V., Heden O., Solov'eva F. I.** On ranks and kernels of perfect codes. (submitted).
4. **Avgustinovich S. V., Solov'eva F. I.** Perfect binary codes with trivial automorphism group // Proc. of IEEE Intern. Workshop on Inform. Theory. Killarney, Ireland, 1998 (June). P. 114–115.
5. **Bauer H., Ganter B., Hergert F.** Algebraic techniques for nonlinear codes // Combinatorica. 1983. V. 3, N 1. P. 21–33.
6. **Etzion T., Vardy A.** Perfect binary codes: constructions, properties and enumeration // IEEE Trans. Inform. Theory. 1994. V. 40, N 3. P. 754–763.
7. **Etzion T., Vardy A.** On perfect codes and tilings: problems and solutions // SIAM J. Discrete Math. 1998. V. 11, N 2. P. 205–223.
8. **Heden O.** A binary perfect code of length 15 and codimension 0 // Des. Codes Cryptogr. 1994. V. 4, N 3. P. 213–220.
9. **Hergert F.** Algebraische Methoden fur nichtlineare Codes. Thesis Darmstadt, 1985.
10. **Malyugin S. A.** Perfect codes with trivial automorphism group // Proc. Second Intern. Workshop on Optimal Codes and Related Topics. Sozopol, Bulgaria, 1998 (June). P. 163–167.
11. **Näslund M.** Steiner triple systems and perfect codes. Master of Sci. Thesis. Stockholm: Royal Inst. of Technology, 1993.

12. Phelps K. T. An enumeration of 1-perfect binary codes of length 15 // Australas. J. Combin. 2000. V. 21. P. 287–298.
13. Phelps K. T., LeVan M. J. Kernels of nonlinear Hamming codes // Des. Codes Cryptogr. 1995. V. 6, N 3. P. 247–257.
14. Phelps K.T., Villanueva M. On perfect codes: rank and kernel // Des. Codes Cryptogr. (to appear).
15. Vardy A. Частное сообщение.

Адреса авторов:

Статья поступила  
25 июля 2001 г.

*С. В. Августинович,*  
*Ф. И. Соловьева*

Институт математики  
им. С. Л. Соболева СО РАН,  
пр. Академика Коптюга, 4,  
630090 Новосибирск, Россия.  
E-mail: avgust@math.nsc.ru,  
sol@math.nsc.ru

*О. Heden*  
Royal Institute of Technology,  
10044 Stockholm, Sweden.  
E-mail: olohed@math.kth.su