UDC 517.919

On upper bound for the number of binary uniformly packed codes [1] [2]

Natalia N. Tokareva

We consider binary uniformly packed (in the wide sense) codes of length n with minimum distance d and covering radius ρ. It is shown that any such code is uniquely determined by the set of its codewords of weights $\lceil n/2 \rceil - \rho, \ldots, \lfloor n/2 \rfloor + \rho$. For an odd d the number of distinct such codes is not more than $2^{2^{n-\frac{d}{2}\log_2 n + o(\log_2 n)}}$.

Introduction

Let us consider the metric space E^n on the set of all binary vectors of length n with respect to the Hamming metric $d(\cdot,\cdot)$ (the distance between two vectors equals the number of components for which they differ). The *Hamming weight* $wt(x)$ of a vector $x \in E^n$ is given by $wt(x) = d(x, \mathbf{0})$, where $\mathbf{0}$ is the zero vector. A nonempty set $C \subset E^n$ with the smallest distance d between two its distinct elements is called *binary* (n,d)*-code*, where n and d are *length* and *minimum distance* of the code C, respectively. Elements of a code are called *codewords*. For a binary code C of length n the *covering radius* ρ is given by the equality $\rho = \max_{x \in E^n} d(x, C)$.

According to L. A. Bassalygo, G. V. Zaitsev and V. A. Zinoviev [2], a binary (n,d)-code C with covering radius ρ is called *uniformly packed in the wide sense*, if there exist rational numbers $\alpha_0, \alpha_1, \ldots, \alpha_\rho$ such that for any binary vector x of length n it holds the equality $\sum_{i=0}^{\rho} \alpha_i f_i(x) = 1$, where $f_i(x)$ is the number of codewords of C at distance i from the vector x for $i = 0, 1, \ldots, \rho$. Let $d = 2t+1$. There exists another definition of uniformly packed of jth order codes for $j = 1, \ldots, t$ (see the paper of J. M. Goethals and H. C. A. van Tilborg [7]) that for $j = \rho - t$ gives a particular case of the definition [2]. For the case $j = \rho - t = 1$ both definitions [2] and [7] coincide and determine *strongly uniformly packed codes* or *uniformly packed in the narrow sense codes* introduced in 1971 by N. V. Semakov, V. A. Zinoviev and G. V. Zaitsev [5]. Further by “uniformly packed” we mean “uniformly packed in the wide sense”.

S. V. Avgustinovich [1] showed that any perfect binary code of length n with minimum distance $d = 3$ (known also as 1-perfect code) is uniquely determined by the set of its

[1] The original version is
Tokareva N. N. On upper bound for the number of binary uniformly packed codes // Discrete Analysis and Operation Research, 2007. V. 14, N 3. P. 90–97 [in Russian].
This English translation will be available soon in *J. Applied and Industrial Mathematics*, 2008.

[2] This research was supported by the Siberian Branch of the Russian Academy of Sciences Integration project “Tree-like catalogue of mathematical Internet resources mathtree.ru” (no. 35), by the Russian Foundation for Basic Research (projects 07-01-00248, 08-01-00671) and Russian Science Support Foundation.

codewords of weight $(n-1)/2$. Applying this fact S. V. Avgustinovich [1] proved that the number of distinct perfect binary codes of length n is not more than $2^{2^{n-\frac{3}{2}\log n+o(\log n)}}$ (here and in what follows log is the logarithm to the base 2). This bound has not been improved since 1995.

Consider an arbitrary class $\mathbb{L}(n,d,\rho;\alpha_0,\dots,\alpha_\rho)$ of binary uniformly packed (in the wide sense) (n,d)-codes with covering radius ρ and packing parameters $\alpha_0,\dots,\alpha_\rho$. We suppose that d and ρ are constants. Denote by $L_{n,d}$ the number of distinct codes in the class $\mathbb{L}(n,d,\rho;\alpha_0,\dots,\alpha_\rho)$. It should be mentioned that using the sphere packing bound for the size of a (n,d)-code one can obtain the trivial upper bound: $L_{n,d}\leqslant 2^{2^{n-\frac{d-1}{2}\log n+o(\log n)}}$. In this paper we generalize the method [1] for the case of any class $\mathbb{L}(n,d,\rho;\alpha_0,\dots,\alpha_\rho)$. We show that a code from $\mathbb{L}(n,d,\rho;\alpha_0,\dots,\alpha_\rho)$ is uniquely determined by the set of its codewords of weights $\lceil n/2\rceil-\rho,\dots,\lfloor n/2\rfloor+\rho$. In the case of odd d we derive the following upper bound $L_{n,d}<2^{2^{n-\frac{d}{2}\log n+\log\log n+\delta}}$, where $\delta=d\log d+\log(\rho+1)$ is a constant.

1. Auxiliary statements

Let x,y be any binary vectors of length n, let $d(x,y)=k$. It is known (see, for example, [4, ch. 21]) that the number of vectors $z\in E^n$ such that $d(x,z)=i$ and $d(y,z)=j$ does not depend on the choice of x,y and depend only on i,j,k,n. Denote this number by p_{ijk}. It is clear that

$$p_{ijk}=\binom{k}{(i-j+k)/2}\binom{n-k}{(i+j-k)/2},$$

if $i+j-k$ is even. In the case of odd $i+j-k$ we have $p_{ijk}=0$. Assume that p_{ijk} is defined for any i,j,k, $0\leqslant i,j,k\leqslant n$, and equals zero if the corresponding set of vectors z is empty.

Let C be a code from an arbitrary class $\mathbb{L}(n,d,\rho;\alpha_0,\dots,\alpha_\rho)$. Denote by C_i and E_i the sets of weight i vectors in the code C and in the space E^n, respectively, here $i=0,1,\dots,n$. Let μ_C^i be the size of C_i. The vector $\mu(C)=(\mu_C^0,\mu_C^1,\dots,\mu_C^n)$ is called a *weight spectrum* of a code C. Numbers μ_C^i, $i=0,1,\dots,n$, are said to be *spectral values* of the code. Weight spectrum of a code is tightly connected with its weight function. In [2] formula for the weight function of any uniformly packed code is given. This formula contains ρ unknown constants. In order to determine them it is required to find out any ρ spectral values for which it is possible to solve the corresponding system of linear equations (see for details [2]).

We prove the following fact.

Lemma 1. *The weight spectrum of any code C from a class of uniformly packed codes $\mathbb{L}(n,d,\rho;\alpha_0,\dots,\alpha_\rho)$ is uniquely determined by numbers $\mu_C^0,\dots\mu_C^{\rho-1}$.*

Proof. Let us show how to determine $\mu_C^{j+\rho}$ by known values $\mu_C^0,\dots\mu_C^{j+\rho-1}$ (for any $j=0,1,\dots,n-\rho$). For each $i=0,1,\dots,\rho$ it holds

$$\sum_{x\in E_j} f_i(x)=\sum_{k=\max\{0,j-i\}}^{j+i} p_{ijk}\,\mu_C^k. \tag{1}$$

Indeed, any codeword of weight k is at distance i exactly from p_{ijk} binary vectors of weight j. Note that all spectral values $\mu_C^{\max\{0,j-\rho+1\}},\dots,\mu_C^{j+\rho-1}$ that appear in any equation (1) for

$i = 0, 1, \ldots, \rho - 1$ are known; for $i = \rho$ there is just one unknown value $\mu_C^{j+\rho}$ in the equation (with the coefficient being nonzero). As far as the code C is uniformly packed we have

$$\sum_{x \in E_j} \sum_{i=0}^{\rho} \alpha_i f_i(x) = \binom{n}{j}.$$

Summing in another order and using (1) we get

$$\sum_{i=0}^{\rho} \alpha_i \sum_{k=\max\{0, j-i\}}^{j+i} p_{ijk}\, \mu_C^k = \binom{n}{j}.$$

From this we uniquely determine the value $\mu_C^{j+\rho}$. Thus, we can find out step by step all the values $\mu_C^{\rho}, \ldots, \mu_C^{n}$. $\square$

The following lemma is a generalization of one property of perfect binary codes, which is given in [1].

Lemma 2. *The set $X = C_{\lceil n/2 \rceil - \rho} \cup \cdots \cup C_{\lfloor n/2 \rfloor + \rho}$ uniquely determines the code C from a class $\mathbb{L}(n, d, \rho; \alpha_0, \ldots, \alpha_\rho)$ of uniformly packed codes.*

Proof. For a code C denote by A and B the following sets of codewords:

$$A = C_0 \cup \cdots \cup C_{\lceil n/2 \rceil - \rho - 1}, \quad B = C_{\lfloor n/2 \rfloor + \rho + 1} \cup \cdots \cup C_n.$$

We have $C = A \cup X \cup B$. It is easy to see that distance between A and B is not less than $2\rho + 1$ and hence is not less than d. Assume that there exists another code $C' = A' \cup X \cup B'$ in the class $\mathbb{L}(n, d, \rho; \alpha_0, \ldots, \alpha_\rho)$ such that $B \neq B'$. In this case the code C'' obtained from C by a substitution the set B' for the set B is also a code of length n and minimum distance d. Let us show that C'' belongs to the class $\mathbb{L}(n, d, \rho; \alpha_0, \ldots, \alpha_\rho)$, i. e. that C'' is uniformly packed with packing parameters $\alpha_0, \ldots, \alpha_\rho$. By definition, let us take a vector $x \in E^n$ and find the value of the sum

$$\sum_{i=0}^{\rho} \alpha_i f_i(x), \tag{2}$$

where $f_i(x)$ is the number of codewords of the code C'' at distance i from the vector x. For a code D of length n denote by $T_\rho^D(x)$ the set of all its codewords contained in the ball of radius ρ centered in the vector x, i. e. $T_\rho^D(x) = \{\, y \in D : d(x, y) \leqslant \rho \,\}$. By construction of the code C'', it is true

$$T_\rho^{C''}(x) = \begin{cases} T_\rho^{C}(x), & \text{if } wt(x) \leqslant \lfloor n/2 \rfloor, \\ \\ T_\rho^{C'}(x), & \text{if } wt(x) \geqslant \lceil n/2 \rceil. \end{cases}$$

By assumption, codes C and C' are uniformly packed with packing parameters mentioned above. Therefore the sum (2) equals 1 for any vector $x \in E^n$. And hence C'' belongs to the class $\mathbb{L}(n, d, \rho; \alpha_0, \ldots, \alpha_\rho)$ of uniformly packed codes.

As far as $B \neq B'$, we assume without loss of generality that there exists a vector $y \in E^n$ such that $y \in B$ and $y \notin B'$. Let $z = y \oplus \mathbf{1}$, where $\mathbf{1}$ is the all-one vector and $\oplus$ is the

componentwise sum by modulo 2. It is easy to see that it holds $wt(z) \leqslant \lceil n/2 \rceil - \rho - 1$, and hence

$$T_\rho^C(z) = T_\rho^{C''}(z).$$

Then for uniformly packed codes $z \oplus C$ and $z \oplus C''$ (shifts of codes C and C'' by the vector z) the first $\rho + 1$ spectral values coincide, i. e.

$$\mu^0_{z\oplus C} = \mu^0_{z\oplus C''}, \ldots, \mu^\rho_{z\oplus C} = \mu^\rho_{z\oplus C''}.$$

Therefore by lemma 1 codes $z \oplus C$ and $z \oplus C''$ have the same weight spectra. But since $\mathbf{1} \in z \oplus C$ and $\mathbf{1} \notin z \oplus C''$, we have $\mu^n_{z\oplus C} \neq \mu^n_{z\oplus C''}$. This contradiction concludes the proof. $\square$

Now we prove a simple (but appropriate for our purposes) bound for the number of weight i codewords of any binary code C. We note that there exist appreciably better bounds for the value $|C_i|$ (see, for example [4, ch. 17]).

Lemma 3. *Let C be a binary code of length n and minimum distance $d = 2t + 1$. For any $i = t, \ldots, n - t$ it is true*

$$|C_i| \leqslant \frac{2^t t!}{n^t} \binom{n}{i}.$$

Proof. Let $i \leqslant \lfloor n/2 \rfloor$. For a vector $x \in E^n$ of weight i define the following set:

$$V_x = \{\ z \in E^n : wt(z) = i - t,\ supp(z) \subset supp(x)\ \},$$

where $supp(z)$ is the set of all nonzero components of a vector z. Note that $|V_x| = \binom{i}{t}$. As far as for any two codewords x and y from C_i sets V_x and V_y do not intersect (otherwise $d(x, y) < d$), we have

$$|C_i| \leqslant \frac{|E_{i-t}|}{|V_x|} \leqslant \frac{\binom{n}{i-t}}{\binom{i}{t}}.$$

This inequality after a small transformation gives us the bound we need. The case $i \geqslant \lceil n/2 \rceil$ is analogous. $\square$

2. Upper bound

The main result is the following.

Theorem 1. *Let $L_{n,d}$ be the number of distinct codes from a class $\mathbb{L}(n, d, \rho; \alpha_0, \ldots, \alpha_\rho)$ of uniformly packed codes with $n \geqslant 3$ and odd $d \geqslant 3$. Then $L_{n,d} < 2^{2^{n - \frac{d}{2}\log n + \log\log n + \delta}}$, where $\delta = d \log d + \log(\rho + 1)$ is a constant.*

Proof. According to Lemma 2, it is true that

$$L_{n,d} \leqslant \begin{pmatrix} |E_{\lceil n/2\rceil-\rho}| + \cdots + |E_{\lfloor n/2\rfloor+\rho}| \\ |C_{\lceil n/2\rceil-\rho}| + \cdots + |C_{\lfloor n/2\rfloor+\rho}| \end{pmatrix}. \tag{3}$$

Then we have

$$|E_{\lceil n/2\rceil-\rho}| + \cdots + |E_{\lfloor n/2\rfloor+\rho}| \leqslant (2\rho+1)\binom{n}{\lfloor n/2\rfloor}. \tag{4}$$

By Lemma 3, for any binary code C of length n with minimum distance d it holds

$$|C_{\lceil n/2\rceil-\rho}| + \cdots + |C_{\lfloor n/2\rfloor+\rho}| \leqslant \frac{\lambda}{n^t}\binom{n}{\lfloor n/2\rfloor}, \tag{5}$$

where $\lambda = (2\rho+1)\cdot 2^t \cdot t!$ and $t = (d-1)/2$. Applying the Stirling's formula

$$n^n e^{-n}\sqrt{2\pi n} \leqslant n! \leqslant n^n e^{1-n}\sqrt{2\pi n},$$

it is not difficult to get $\binom{n}{\lfloor n/2\rfloor} \leqslant 2^{n-\frac{1}{2}\log n+2}$. Then by (3-5), we have

$$L_{n,d} < \begin{pmatrix} 2^{n-\frac{1}{2}\log n+(2+\log(2\rho+1))} \\ 2^{n-\frac{d}{2}\log n+(2+\log\lambda)} \end{pmatrix}.$$

By the inequality $\binom{a}{b} < \left(\frac{3a}{b}\right)^b$ for any $a > b > 1$ it follows that

$$L_{n,d} < 2^{2^{n-\frac{d}{2}\log n+\log\log n+(\log\lambda+\log d+1)}}.$$

By using $c! \geqslant \left(\frac{c+1}{2}\right)^c$ for any $c \geqslant 1$, it is easy to obtain $\log\lambda + \log d + 1 \leqslant d\log d + \log(\rho+1)$, and hence

$$L_{n,d} < 2^{2^{n-\frac{d}{2}\log n+\log\log n+\delta}}.$$

□

The following classes of codes can be taken for $\mathbb{L}(n, d, \rho; \alpha_0, \ldots, \alpha_\rho)$ and hence the upper bound of Theorem 1 takes place for all of them:

1) Binary *perfect codes* of length $n = 2^m - 1$ ($m \geqslant 2$) with size $2^{n-\log(n+1)}$ and minimum distance $d = 3$. The covering radius of these codes is $\rho = 1$ and packing parameters are $\alpha_0 = \alpha_1 = 1$, see [5]. This particular case of Theorem 1 was proved in [1].

Other series of uniformly packed codes with minimum distance $d = 3$ can be found in [7] (see also [2, 8]).

2) Binary *Preparata codes* of length $n = 2^m - 1$ ($m \geqslant 4$ is even) with size $2^{n-2\log(n+1)+1}$ and minimum distance $d = 5$ (sometimes these codes are called *Preparata-like codes*). Covering radius and packing parameters of these codes are $\rho = 3$ and $\alpha_0 = \alpha_1 = 1, \alpha_2 = \alpha_3 = 3/n$, see [5, 2].

Corollary 1. *The number of distinct binary Preparata codes of length* n *with minimum distance* 5 *is not more than*
$$2^{2^{n-\frac{5}{2}\log n+o(\log n)}}.$$

Remark. Let us note that we have a better bound for the number of codes from one special subclass of Preparata codes. According to [6, corollary 2] the number of nonequivalent quaternary linear Preparata codes of length n with minimum distance 6 is not more than $2^{n\log n}$.

3) Binary primitive *BCH-like codes* of length $n = 2^m - 1$ ($m \geqslant 5$ is odd) with size $2^{n-2\log(n+1)}$, minimum distance $d = 5$, covering radius $\rho = 3$ and packing parameters $\alpha_0 = \alpha_1 = 1, \alpha_2 = \alpha_3 = \frac{6}{n-1}$ (see [2]).

4) Binary *Goethals codes* (these codes are also known as *Goethals-like codes*) of length $n = 2^m - 1$ ($m \geqslant 4$ is even) with size $2^{n-3\log(n+1)+2}$, minimum distance $d = 7$, covering radius $\rho = 5$ and packing parameters $\alpha_0 = \alpha_1 = 1, \alpha_2 = \alpha_3 = \frac{15}{2n}, \alpha_4 = \alpha_5 = \frac{30}{n(n-3)}$ (see [7, 3]) .

Corollary 2. *The number of distinct binary Goethals codes of length* n *with minimum distance* 7 *is not more than*
$$2^{2^{n-\frac{7}{2}\log n+o(\log n)}}.$$

5) Binary primitive *BCH-like codes* of length $n = 2^m - 1$ ($m \geqslant 5$ is odd) with size $2^{n-3\log(n+1)}$, minimum distance $d = 7$, covering radius $\rho = 5$ and packing parameters $\alpha_0 = \alpha_1 = 1, -\alpha_2 = -\alpha_3 = \alpha_4 = \alpha_5 = \frac{120}{(n-1)(n-7)}$ (see [7]).

The author is grateful to Denis S. Krotov for essential remarks that help to extend the area of codes for which Theorem 1 takes place.

References

[1] S. V. Avgustinovich, “On one property of the perfect binary codes,” *Discrete Analysis and Operation Research*, vol. 2, no. 1, pp. 4–6, 1995 [in Russian].

[2] L. A. Bassalygo, G. V. Zaitsev, and V. A. Zinoviev, “Uniformly Packed Codes,” *Probl. Inform. Trans.*, vol. 10, no. 1, pp. 6–9, 1974.

[3] V. A. Zinoviev and T. Helleseth, “On Weight Distributions of Shifts of Goethals-like Codes,” *Probl. Inform. Trans.*, vol. 40, no. 2, pp. 118–134, 2004.

[4] F. J. MacWilliams and N. J. A. Sloane, “The Theory of Error-Correcting Codes,” *North-Holland: Amsterdam*, 1977.

[5] N. V. Semakov, V. A. Zinoviev, and Zaitsev G. V., “Uniformly Packed Codes,” *Probl. Inform. Trans.*, vol. 7, no. 1, pp. 30–39, 1971.

[6] N. N. Tokareva, “Representation of $\mathbb{Z}_4$-Linear Preparata Codes Using Vector Fields,” *Probl. Inform. Trans.*, vol. 41, no. 2, pp. 113–124, 2004.

[7] J. M. Goethals and H. C. A. Van Tilborg, “Uniformly packed codes,” *Philips Res. Repts.*, vol. 30, pp. 9–36, 1975.

[8] J. Rifa, V. A. Zinoviev, "On completely regular codes from perfect codes," *Proc. Tenth Int. Workshop «Algebraic and Combinatorial Coding Theory», Zvenigorod, Russia*, pp. 225–229, September, 3–9, 2006.

Sobolev Institute of mathematics SB RAS, ac. Koptyug av., 4,
Novosibirsk State University, Pirogova st., 2
630090 Novosibirsk, Russian Federation.
E-mail: tokareva@math.nsc.ru
Web: www.math.nsc.ru/∼tokareva

Paper submitted March 14, 2007.