An Upper Bound for the Number of Uniformly Packed Codes

Natalia Tokareva
Sobolev Institute of Mathematics, 4 Acad. Koptyug avenue
Siberian Branch of the Russian Academy of Sciences
Novosibirsk State University, 2 Pirogova street
630090 Novosibirsk, Russia
E-mail: tokareva@math.nsc.ru

***Abstract*— Binary uniformly packed in the narrow sense codes were introduced in 1971 by Semakov, Zinoviev and Zaitsev. Later more general definitions were proposed by Bassalygo, Zaitsev and Zinoviev (uniformly packed in the wide sense codes) and by Goethals and Tilborg (uniformly packed codes). We consider binary uniformly packed in the wide sense codes. These codes are well known for their remarkable properties and have been intensively studied. In this paper we give an upper bound on the number of distinct uniformly packed in the wide sense codes of length n with constant odd minimum distance d and fixed parameters of packing. In particular, we give nontrivial upper bounds on the numbers of Preparata codes with $d = 5$, primitive BCH codes with d equal to 5 or 7, Goethals codes with $d = 7$, et al. The result obtained generalizes the upper bound for the number of perfect codes with $d = 3$ that was derived by Avgustinovich in 1995.**

I. 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 $C \subset E^n$ of size M with the smallest distance d between two distinct elements of C is called *binary (n,M,d)-code*, where n and d are *length* and *minimum distance* of the code C, respectively. Elements of a code are called *codewords*. By $|A|$ we denote the size of a set A. Let $supp(x)$ be the set of all nonzero components of a vector x.

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 [1], a binary (n, M, 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 the following equality holds:

$$\sum_{i=0}^{\rho} \alpha_i f_i(x) = 1,$$

where $f_i(x)$ is the number of codewords of the code 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 [2]) that for $j = \rho - t$ gives a particular case of the definition [1]. For the case $j = \rho - t = 1$ both definitions [1] and [2] 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 [3]. Note that uniformly packed codes have also close connections with *completely regular* codes, see for instance [2]. Further by "uniformly packed" we mean "uniformly packed in the wide sense".

S. V. Avgustinovich [4] 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 codewords of weight $\frac{n-1}{2}$. Applying this fact S. V. Avgustinovich 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 $\mathbf{L}(n, M, d, \rho; \alpha_0, \ldots, \alpha_\rho)$ of binary uniformly packed (in the wide sense) (n, M, d)-codes with covering radius ρ and packing parameters $\alpha_0, \ldots, \alpha_\rho$. We suppose that d and ρ are constants. Denote by $L_{n,d}$ the number of distinct codes in the class $\mathbf{L}(n, M, d, \rho; \alpha_0, \ldots, \alpha_\rho)$. It should be mentioned that using the sphere packing bound

$$M \le \frac{2^n}{\sum\limits_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}},$$

one can obtain the trivial upper bound:

$$L_{n,d} \le \binom{2^n}{M} \le 2^{2^{n-\frac{d-1}{2}\log n + o(\log n)}},$$

here $\binom{a}{b} = \frac{a!}{b!(a-b)!}$. In this paper we generalize the method [4] for the case of any class $\mathbf{L}(n, M, d, \rho; \alpha_0, \ldots, \alpha_\rho)$. We show that any code from $\mathbf{L}(n, M, d, \rho; \alpha_0, \ldots, \alpha_\rho)$ is uniquely determined by the set of its codewords of weights $\lceil \frac{n}{2} \rceil - \rho, \ldots, \lfloor \frac{n}{2} \rfloor + \rho$. In the case of odd d we derive the following

1-4244-1429-6/07/$25.00 ©2007 IEEE

upper bound:

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

Note that ρ does not entry into the bound expression. In particular, we give nontrivial upper bounds on the numbers of Preparata codes ($d = 5$), primitive BCH codes (d equals 5 or 7), Goethals codes ($d = 7$), et al.

II. Three lemmas

Let x, y be any binary vectors of length n, $d(x, y) = k$. It is known (see, for example, [5]) 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 and equals zero if the corresponding set of vectors z is empty.

Let C be a code from an arbitrary class $\mathbf{L}(n, M, d, \rho; \alpha_0, \ldots, \alpha_\rho)$. 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 $i = 0, 1, \ldots, n$. Let μ_C^i be the size of C_i. The vector $\mu(C) = (\mu_C^0, \mu_C^1, \ldots, \mu_C^n)$ is called a *weight spectrum* of a code C. Numbers μ_C^i, $i = 0, 1, \ldots, n$, are said to be *spectral values* of the code. Weight spectrum of a code is tightly connected with its weight function. In [1] 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 [1]). We prove the following fact.

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

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

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

Indeed, any codeword of weight k is at distance i exactly from p_{ijk} binary vectors of weight j. Note that in any equation (1) for $i = 0, 1, \ldots, \rho - 1$ only known spectral values $\mu_C^{\max\{0, j-\rho+1\}}, \ldots, \mu_C^{j+\rho-1}$ appear and for $i = \rho$ there is unique unknown value $\mu_C^{j+\rho}$ in it (with 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 $\mu_C^\rho, \ldots, \mu_C^n$. ■

The following lemma is a generalization of the property of perfect binary codes, which is given in [4].

Lemma 2: The set $X = C_{\lceil n/2 \rceil - \rho} \cup \ldots \cup C_{\lfloor n/2 \rfloor + \rho}$ uniquely determines the code C from a class $\mathbf{L}(n, M, d, \rho; \alpha_0, \ldots, \alpha_\rho)$.

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

$$A = C_0 \cup \ldots \cup C_{\lceil n/2 \rceil - \rho - 1},$$

$$B = C_{\lfloor n/2 \rfloor + \rho + 1} \cup \ldots \cup C_n.$$

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 $\mathbf{L}(n, M, d, \rho; \alpha_0, \ldots, \alpha_\rho)$ 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 $\mathbf{L}(n, M, d, \rho; \alpha_0, \ldots, \alpha_\rho)$, 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

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

where $f_i(x)$ is the number of codewords of the code C'' at distance i from the vector x. Denote by $T_\rho^D(x)$ the set of all codewords of a code D contained in the ball of radius ρ centered in the vector x, i. e.

$$T_\rho^D(x) = \{\, y \in D : d(x, y) \leq \rho \,\}.$$

Note that by the construction of the code C'', it is true

$$T_\rho^{C''}(x) = \begin{cases} T_\rho^C(x), & \text{if } wt(x) \leq \lfloor \frac{n}{2} \rfloor, \\ T_\rho^{C'}(x), & \text{if } wt(x) \geq \lceil \frac{n}{2} \rceil. \end{cases} \qquad (3)$$

By assumption, codes C and C' are uniformly packed with packing parameters mentioned above. Therefore by (3), the sum (2) equals 1 for any vector $x \in E^n$.

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 $wt(z) \le \lceil n/2 \rceil - \rho - 1$, 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 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 $\mu^n_{z\oplus C} \ne \mu^n_{z\oplus C''}$. This contradiction concludes the proof. ■

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

$$|C_i| \le \frac{2^t t!}{n^t} \left(\begin{array}{c} n \\ i \end{array} \right).$$

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

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

Note that $|V_x| = \left(\begin{array}{c} i \\ t \end{array} \right)$. As far as for any two codewords x and y from C_i the sets V_x and V_y do not intersect (otherwise $d(x,y) < d$), we have

$$|C_i| \le \frac{|E_{i-t}|}{|V_x|} \le \frac{\left(\begin{array}{c} n \\ i-t \end{array} \right)}{\left(\begin{array}{c} i \\ t \end{array} \right)}.$$

This inequality after a little transformation gives us the bound we need. The case $i \ge \lceil \frac{n}{2} \rceil$ is analogous. ■

III. Upper bound

The main result is the following.

Theorem 1: Let $L_{n,d}$ be the number of distinct codes from a class $\mathbf{L}(n, M, d, \rho; \alpha_0, \ldots, \alpha_\rho)$ of uniformly packed codes with odd d. Then

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

Proof: According to Lemma 2, it is true that

$$L_{n,d} \le \left(\begin{array}{c} |E_{\lceil n/2 \rceil - \rho}| + \ldots + |E_{\lfloor n/2 \rfloor + \rho}| \\ |C_{\lceil n/2 \rceil - \rho}| + \ldots + |C_{\lfloor n/2 \rfloor + \rho}| \end{array} \right). \quad (4)$$

Then we have

$$|E_{\lceil n/2 \rceil - \rho}| + \ldots + |E_{\lfloor n/2 \rfloor + \rho}| \le (2\rho+1) \left(\begin{array}{c} n \\ \lfloor n/2 \rfloor \end{array} \right). \quad (5)$$

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

$$|C_{\lceil n/2 \rceil - \rho}| + \ldots + |C_{\lfloor n/2 \rfloor + \rho}| \le \frac{\lambda}{n^t} \left(\begin{array}{c} n \\ \lfloor n/2 \rfloor \end{array} \right), \quad (6)$$

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

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

it is not difficult to get

$$\left(\begin{array}{c} n \\ \lfloor n/2 \rfloor \end{array} \right) \le 2^{n - \frac{1}{2}\log n + 2}. \quad (7)$$

Then by (4-7), we have $L_{n,d} < \left(\begin{array}{c} 2^{n - \frac{1}{2}\log n + (2 + \log(2\rho+1))} \\ 2^{n - \frac{d}{2}\log n + (2 + \log \lambda)} \end{array} \right)$. As far as d and ρ are constants, using the well known inequalities

$$\left(\begin{array}{c} a \\ b \end{array} \right) < \left(\frac{3a}{b} \right)^b \text{ for any } a > b > 1$$

and

$$a! \le \left(\frac{a+1}{2} \right)^a \text{ for any } a \ge 1,$$

we obtain

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

■

IV. Examples

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

The case $d = 3$

1) Binary *perfect codes* of length $n = 2^m - 1$, $m \ge 2$, 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 [3]. This particular case of Theorem 1 was proved in [4].

2) Binary codes of length $n = 2^{m+1} - 2$, $m \ge 2$, with size $2^{n - 2\log(n+2) + 2}$, minimum distance $d = 3$, covering radius $\rho = 2$ and packing parameters

$$\alpha_0 = 1, \alpha_1 = \frac{2-n}{4}, \alpha_2 = 1.$$

For instance, these codes can be constructed by applying the doubling construction to arbitrary perfect codes of length $2^m - 1$, see [1].

3) Let H_a be a parity check matrix of the binary linear perfect code of length $2^m - 1$, $m \ge 3$. Let H_b be a parity check matrix of the binary repetition code of length $\ell \ge 3$. Assume $2^m \ge \ell$. According to J. Rifa and V. A. Zinoviev [6], the code with parity check matrix $H = H_a \otimes H_b$ (the Kronecker product of H_a and H_b) is a uniformly packed code of length $n = \ell(2^m - 1)$ with size $2^{n - m(\ell-1)}$, minimum distance $d = 3$ and covering radius $\rho = \ell - 1$. For ℓ equal to 3 or 4 we have two families of uniformly packed codes with $\rho \le d$.

Each family induces the class of codes with the same packing parameters.

Other series of uniformly packed codes with minimum distance $d = 3$ can be found in [2].

The case $d = 5$

4) Binary *Preparata codes* of length $n = 2^m - 1$ ($m \geq 4$ 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 determined by n, M, d. They are $\rho = 3$ and

$$\alpha_0 = \alpha_1 = 1, \alpha_2 = \alpha_3 = \frac{3}{n},$$

see [3] and [1].

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 [7] (see Corollary 2), the number of nonequivalent quaternary linear Preparata codes of length n with minimum distance 6 is not more than $2^{n \log n}$.

5) Binary primitive *BCH-like codes* of length $n = 2^m - 1$ ($m \geq 5$ is odd) with size $2^{n-2\log(n+1)}$, minimum distance $d = 5$, covering radius $\rho = 3$ and packing parameters [1]:

$$\alpha_0 = \alpha_1 = 1, \alpha_2 = \alpha_3 = \frac{6}{n-1}.$$

The case $d = 7$

6) Binary *Goethals codes* of length $n = 2^m - 1$ ($m \geq 4$ 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 [2] and [8] (these codes are also known as *Goethals-like codes*).

Corollary 2: The number of distinct binary Goethals codes of length n with minimum distance 7 is not more than

$$2^{2^{n-\frac{7}{2}\log n + o(\log n)}}.$$

7) Binary primitive *BCH-like codes* of length $n = 2^m - 1$ ($m \geq 5$ is odd) with size $2^{n-3\log(n+1)}$, designed minimum distance $d = 7$, covering radius $\rho = 5$ and packing parameters, see [2],

$$\alpha_0 = \alpha_1 = 1, -\alpha_2 = -\alpha_3 = \alpha_4 = \alpha_5 = \frac{120}{(n-1)(n-7)}.$$

ACKNOWLEDGMENT

The author is grateful to D. S. Krotov for essential remarks that help to extend the area of codes for which Theorem 1 takes place. This research was supported by the Siberian Branch of the Russian Academy of Sciences Integration project "Tree-like catalogue of mathematical Internet resources" (no. 35) and by the Russian Foundation for Basic Research (project 07-01-00248).

REFERENCES

[1] L. A. Bassalygo, G. V. Zaitsev, and V. A. Zinoviev, "Uniformly Packed Codes," *Probl. Inform. Trans.*, vol. 10, no. 1, pp. 6–9, 1974.
[2] J. M. Goethals and H. C. A Van Tilborg, "Uniformly packed codes," *Philips Res. Repts.*, vol. 30, pp. 9–36, 1975.
[3] N. V. Semakov, V. A. Zinoviev, and Zaitsev G. V., "Uniformly Packed Codes," *Probl. Inform. Trans.*, vol. 7, no. 1, pp. 30–39, 1971.
[4] 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].
[5] F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," *North-Holland: Amsterdam*, 1977.
[6] J. Rifa and 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.
[7] N. N. Tokareva, "Representation of Z_4-Linear Preparata Codes Using Vector Fields," *Probl. Inform. Trans.*, vol. 41, no. 2, pp. 113–124, 2004.
[8] V. A. Zinoviev and T. Helleseth, "On Weight Distributions of Shifts of Goethals-like Codes," *Probl. Inform. Trans.*, vol. 40, no. 2, pp. 19–36, 2004.