Designs, Codes and Cryptography, 22, 221–237, 2001.

On Perfect Codes and Related Concepts

R. AHLSWEDE

H.K. AYDINIAN

L.H. KHACHATRIAN

Communicated by: J.H. van Lint

Received September 15, 1998; Revised June 7, 1999; Accepted August 31, 1999

Abstract. The concept of diameter perfect codes, which seems to be a natural generalization of perfect codes (codes attaining the sphere–packing bound) is introduced. This was motivated by the "code–anticode" bound of Delsarte in distance regular graphs. This bound in conjunction with the recent complete solutions of diametric problems in the Hamming graph $\mathcal{H}_q(n)$ and the Johnson graph $J(n,k)$ gives a sharpening of the sphere–packing bound. Some necessary conditions for the existence of diameter perfect codes are given. In the Hamming graph all diameter perfect codes over alphabets of prime power size are characterized. The problem of tiling of the vertex set of $J(n,k)$ with caps (and maximal anticodes) is also examined.

Keywords: Perfect codes, anticodes, tilings, diametric theorems, complete intersection theorem

1. Introduction

Perfect codes are a fascinating structure in coding theory, which again and again attracted attention. They have been studied for different metrics, especially, for the Hamming metric (for a good survey see e.g. [5]). Generally we are given a distance regular graph Γ with vertex set $\mathcal{V}$. A code $\mathcal{C}$ in Γ is a nonempty subset of $\mathcal{V}$. Its minimum distance $d(\mathcal{C})$ is the minimum distance of two distinct codewords, that is

$$d(\mathcal{C}) = \min\{\text{dist}(x,y)\colon\ x,y \in \mathcal{C}, x \neq y\}. \tag{1.1}$$

The set

$$\mathcal{B}_i(u) = \{x \in \mathcal{V}\colon\ \text{dist}(x,u) \leq i\} \tag{1.2}$$

is the ball of radius i and center u.

Now, a code $\mathcal{C}$ is called *e–perfect* if the balls $\{\mathcal{B}_e(u)\colon\ u \in \mathcal{C}\}$ partition $\mathcal{V}$, that is,

$$\dot{\bigcup_{u\in\mathcal{C}}} \mathcal{B}_e(u) = \mathcal{V} \tag{1.3}$$

and consequently with the cardinality b_e of these balls

$$|\mathcal{C}| = |\mathcal{V}| b_e^{-1}. \tag{1.4}$$

Clearly, an e–perfect code $\mathcal{C}$ has minimum distance

$$d(\mathcal{C}) = 2e + 1. \tag{1.5}$$

Conversely, if a code $\mathcal{C}$ satisfies (1.4) and (1.5), then it is e–perfect.

Central in our investigations is a bound which was found by Delsarte in his study of the Bose–Mesner algebra of association schemes:

THEOREM D [6] *Let $\mathcal{X}$ and $\mathcal{Y}$ be subsets of the vertex set $\mathcal{V}$ of a distance regular graph Γ, such that nonzero distances occuring between vertices in $\mathcal{X}$ do not occur between vertices of $\mathcal{Y}$. Then*

$$|\mathcal{X}||\mathcal{Y}| \leq |\mathcal{V}|. \tag{1.6}$$

In particularly, for a code $\mathcal{C}$ with minimum distance $d(\mathcal{C}) = D+1$ and any ball $\mathcal{B}_e(u) \subset \mathcal{V}$

$$|\mathcal{C}||\mathcal{B}_e(u)| \leq |\mathcal{V}|$$

and thus

$$|\mathcal{C}| \leq |\mathcal{V}|b_e^{-1} \text{ for } e = \left\lfloor \frac{D}{2} \right\rfloor. \tag{1.7}$$

This is the well–known so–called "sphere" packing bound.

The present investigation started with the observation that the Diametric Theorems (stated below) of [1] for the Johnson graph $J(n, k)$ and of [2] for the Hamming graph $\mathcal{H}_q(n)$ yield improvements of (1.7).

Indeed, let $D(\mathcal{A})$ be the diameter of any $\mathcal{A} \subset \mathcal{V}$ of a distance regular graph.

$$D(\mathcal{A}) = \max\{\text{dist}(x, y)\colon\ x, y \in \mathcal{A}\}. \tag{1.8}$$

We also say that $\mathcal{A}$ is an *anticode* with diameter $D(\mathcal{A})$.

Let $A^*(D) = \max\{|\mathcal{A}|\colon\ D(\mathcal{A}) \leq D\}$.

Then by Theorem D for any code $\mathcal{C} \subset \mathcal{V}$ with minimum distance $d(\mathcal{C}) = D + 1$

$$|\mathcal{C}| \leq |\mathcal{V}|A^*(D)^{-1}. \tag{1.9}$$

One can use this bound to introduce another and seemingly more natural concept of perfect codes.

Definition. A code $\mathcal{C}$ with $d(\mathcal{C}) = D + 1$ is called D–diameter perfect, if (1.9) holds with equality. We use the word diameter perfect, if the parameter is unspecified.

Clearly, any perfect code is also diameter perfect. In this case an optimal anticode must be a ball! However, in general that is not the case and we get improvements of the sphere packing bound.

The diametric problems in Johnson and Hamming graphs are closely related to intersection problems for systems of finite sets. Recently these two problems were completely solved in [1], [2] by describing all maximal anticodes. We need some further notation:

$\binom{[n]}{k}$ denotes the set of all k–element subsets of the set $[n] \triangleq \{1, \ldots, n\}$.

A system of subsets $\mathcal{A} \subset \binom{[n]}{k}$ is called t–intersecting, if

$$|A_1 \cap A_2| \geq t \quad \text{for all} \quad A_1, A_2 \subset \mathcal{A}.$$

Define the function

$$M(n, k, t) = \max \left\{ |\mathcal{A}|\colon\ \mathcal{A} \text{ is a } t\text{–intersecting system, } \mathcal{A} \subset \binom{[n]}{k} \right\}, 1 \leq t \leq k \leq n.$$

Note that in the language of $0-1$ vectors of length n and weight k this is the maximal size of an anticode of Hamming diameter $2(k-t)$. Define

$$\mathcal{F}_i = \left\{ A \in \binom{[n]}{k}\colon\ |A \cap [1, t+2i]| \geq t+i \right\}$$

for $o \leq i \leq \frac{n-t}{2}$.

THEOREM AK 1 [1] *For $1 \leq t \leq k \leq n$ with*

(i) $(k-t+1)\left(2+\frac{t-1}{r+1}\right) < n < (k-t+1)\left(2+\frac{t-1}{r}\right)$ *for some $r \in \mathbb{N} \cup \{0\}$ we have*

$$M(n, k, t) = |\mathcal{F}_r|$$

and $\mathcal{F}_r$ is—up to permutation—the unique optimum. By convention $\frac{t-1}{r} = \infty$ for $r = 0$.

(ii) $(k-t+1)\left(2+\frac{t-1}{r+1}\right) = n$ *for $r \in \mathbb{N} \cup \{0\}$ we have*

$$M(n, k, t) = |\mathcal{F}_r| = |\mathcal{F}_{r+1}|$$

and an optimal system equals up to permutations—either $\mathcal{F}_r$ or $\mathcal{F}_{r+1}$.

We denote the maximal cardinality of an anticode in $J(n, k)$ of diameter D by

$$A^*(n, D, k) = M(n, k, t), \quad \text{if} \quad D = 2k - 2t. \tag{1.10}$$

In the Hamming space $\mathcal{H}(n, q)$ we have a second concept of intersection.

Let $F = \{0, 1, \ldots, q-1\}$ and let $\mathcal{A} \subset F^n$ be a set of sequences $(a_1, \ldots, a_n)$, $a_i \in F$. We say that $\mathcal{A}$ is t–intersecting if, for any $a^n, b^n \in \mathcal{A}$

$$\text{int}(a^n, b^n) \triangleq |\{i \in [n]\colon\ a_i = b_i\}| \geq t.$$

Equivalently we say that $\mathcal{A}$ has a diameter $n-t$. Define

$$N_q(n, t) \triangleq \max\{|\mathcal{A}|\colon\ \mathcal{A} \text{ is a } t\text{–intersecting system in } F^n\}.$$

Denote now the maximal cardinality of an anticode in $\mathcal{H}_q(n)$ of diameter D by

$$A_q^*(n, D) = N_q(n, t), \quad \text{if } D = n - t. \tag{1.11}$$

THEOREM AK 2 [2] *For $q \geq 2$, $D < n$ we have*

$$A_q^*(n, D) = \left|B_r^{n-D+2r}(u)\right| \cdot q^{D-2r}, \tag{1.12}$$

where $B_r^{n-D+2r}(u)$ is a ball in $\mathcal{H}_q(n - D + 2r)$ of radius r and

$$r = \begin{cases} \left\lfloor \frac{D}{2} \right\rfloor, & \text{if } (D+1)q \leq 2n \\ \left\lfloor \frac{n-D+1}{q-2} \right\rfloor, & \text{if } (D+1)q > 2n. \end{cases} \tag{1.13}$$

Remark 1. In [2] this Theorem is formulated in terms of intersection. It can be seen from (1.11) that an optimal anticode is a Cartesian product of a ball and cube with parameters determined by (1.13).

Obviously these theorems give a sharpening of the sphere packing bound in the Johnson graph and the Hamming graph.

Besides improving the sphere packing bound we investigate D–diameter perfectness and tiling with optimal anticodes.

But first we report classical results on e–perfectness for most familiar distance regular graphs.

1. Hamming Graphs

The vertex set of the Hamming graph $\mathcal{H}_q(n)$ is the set $V^n = \{0, 1, \ldots, q-1\}^n$. The distance for any two vertices is the Hamming distance d_H (counting the number of different components). Two vertices are adjacent, if their Hamming distance is 1.

It was proved by van Lint [16], Tietäväinen [17], and independently by Zinoviev and Leontiev [18], that all e–perfect codes in $\mathcal{H}_q(n)$ (q is a prime power) must have the same parameters as one of the Hamming or Golay codes.

However, the problem of existence of e–perfect codes is still open, if q is not a power of a prime. Another direction of research has been to find non–isomorphic e–perfect codes with the same parameters. A recent survey is [5, ch. 11].

2. Johnson Graphs

The vertex set of the Johnson graph $J(n, k)$ is $V_k^n = \{x \in \{0, 1\}^n\colon x \text{ has } k \text{ ones}\}$. Two vertices x, y are adjacent, if they have $k-1$ ones in common or, equivalently, if $d_H(x, y) = 2$. Thus the Johnson distance between $x, y \in V_k^n$ is defined to be $d_J(x, y) = \frac{1}{2} d_H(x, y)$.

Delsarte [6] conjectured in 1973 that no nontrivial e–perfect codes exist in $J(n, k)$. Until now none has been found. However, Roos [15] established a necessary condition for their existence.

THEOREM R [15] *If an e–perfect code in* $J(n,k)$, $n \geq 2k$ *exists then*

$$n \leq \frac{(k-1)(2e+1)}{e}. \tag{1.14}$$

(The case $n < 2k$ gives nothing new, because exchanging zeros and ones gives an isometry.)

Another significant nonexistence result is due to Etzion [7] (see also [3], [9]).

THEOREM E [7] *There are no perfect codes in* $J(2k+e+1, e+1)$, $J(2k+p,k)$, $J(2k+2p,k)$; $p \neq 3$, $J(2k+3p,k)$; $p \neq 2,3,5$ *where* p *is a prime.*

3. Grassmann Graph

Among the distance regular graphs the Grassmann graph $G_q(n,k)$ seems also to be interesting to our direction of research. Its vertex set is the set of all k–dimensional subspaces of $GF(q)^n$. Two such subspaces are adjacent iff they intersect in a $(k-1)$–dimensional subspace.

The diametric problem in the Grassman graph (in terms of intersections) is solved by Frankl and Wilson in [8].

We mention now our main results.

In Section 2 Theorem 1 generalizes Delsarte's Theorem for $J(n,k)$ to a local inequality, which in particular implies Johnson's bound. A similar inequality holds for $\mathcal{H}_q(n)$ and $G_q(n,k)$.

As an application of Theorem AK 1 we give a comparison of upper bounds obtained in Theorem D for constant weight codes.

In Section 3 we give examples of diameter perfect codes in $J(n,k)$. We also give necessary conditions which include the known one stated above.

In Section 4 we show that MDS codes are diameter perfect in $\mathcal{H}_q(n)$ and so are extended Hamming codes and extended Golay codes. Recall that the perfect codes are automatically diameter perfect. We prove that there are no others!

In Section 5 we show that the problem of existence of diameter perfect codes in $J(n,k)$ can be reduced in all cases to the problem of tiling of vertex set V_k^n with caps.

Finally, we prove that there are no tilings of V_k^n with optimal anticodes, which are not balls. (Compare Delsarte's conjecture above.)

2. A Local Inequality

In standard notation an $(n, 2\delta, k)$–code in $J(n,k)$ has blocklength n, constant weight k, and minimum distance $d_H = 2\delta$ (or $d_J = \delta$). The maximum size of such codes is denoted by $A(n, 2\delta, k)$.

In $\mathcal{H}_q(n)$ the corresponding notions are $(n,d)_q$–codes and maximum sizes $A(n,d)_q$.

The following statement is a generalization of Theorem D for the graphs mentioned above.

THEOREM 1 *Let $\mathcal{C}_{\mathcal{D}}$ be a code in Γ ($\Gamma = J(n,k)$, $\mathcal{H}_q(n)$ or $G_q(n,k)$) with distances from $\mathcal{D} = \{d_1, \ldots, d_s\} \subset \{1, 2, \ldots, n\}$. Further let $\mathcal{L}_{\mathcal{D}}(B)$ be a maximal code in $B \subset \Gamma$ with distances from $\mathcal{D}$. Then one has*

$$\frac{|\mathcal{C}_{\mathcal{D}}|}{|\Gamma|} \leq \frac{|\mathcal{L}_{\mathcal{D}}(B)|}{|B|}. \tag{2.1}$$

Proof. Let $\Gamma = J(n,k)$. Count in two ways the number of pairs (a, π), where $a \in C_D$, π is a permutation of $\{1, 2, \ldots, n\}$ with $\pi(a) \in B$. For a fixed $a \in \mathcal{C}_{\mathcal{D}}$ and $b \in B$ there are exactly $k!(n-k)!$ choices for π; hence the number of such pairs equal $|\mathcal{C}_{\mathcal{D}}||B|k!(n-k)!$.

On the other hand no permutation can transfer elements of $\mathcal{C}_{\mathcal{D}}$ into more than $|\mathcal{L}_{\mathcal{D}}(B)|$ elements of B. Then we have

$$|\mathcal{C}_{\mathcal{D}}||B|k!(n-k)! \leq |\mathcal{L}_{\mathcal{D}}(B)|n!$$

as desired.

In fact the following much more general statement is valid. ∎

THEOREM 1′ *With the conditions of Theorem 1 inequality (2.1) holds for any graph Γ, which admits a transitive group of automorphisms.*

This can be easily proved using the same argument as in the proof above.

Remark 2. For the Hamming graph this extends the Elias–Bassalygo inequality (see [5, ch. 12]). Such an extension for the Hamming graph was already observed (stated in an even more general form) by Levenshtein [13].

Theorem D (for $J(n,k)$, $\mathcal{H}_q(n)$, $G_q(n,k)$ follows from (2.1) by choosing for B a subset with distances from $\{1, \ldots, n\} \backslash D$. Then clearly $|\mathcal{L}_D(B)| = 1$ and we get (1.6).

In $J(n,k)$ (2.1) implies

$$A(n, 2\delta, k) \leq \binom{n}{k} |L(B)||B|^{-1}, \tag{2.2}$$

where $L(B)$ is a maximal code in B with minimum distance 2δ.

Inequality (2.2) can be very useful to get various kinds of upper and lower bounds for constant weight codes by choosing B in a suitable way. For example (2.2) can be viewed as a generalization of the well known Johnson bound (see [14]).

COROLLARY 1

$$A(n, 2\delta, k) \leq \left\lfloor \frac{n}{k} A(n-1, 2\delta, k-1) \right\rfloor \tag{2.3}$$

$$A(n, 2\delta, k) \leq \left\lfloor \frac{n}{n-k} A(n-1, 2\delta, k) \right\rfloor. \tag{2.4}$$

Indeed take as B in (2.1) all vectors in V_k^n with a 1 (resp. 0) in a fixed component and get (2.3) (resp. (2.4)).

Another application of (2.2) gives the bound due to Zinoviev [19] (see also [12]).

THEOREM Z [19] *If* $0 \le g \le \min\{k, \delta\}$ *and* $0 \le \ell < n$, *then*

$$A(n, 2\delta, k) \le \frac{\binom{n}{\ell}}{\sum_{i=0}^{g} \binom{k}{i}\binom{n-k}{\ell-i}} A(n-\ell, 2\delta - 2g, k-g). \tag{2.5}$$

Proof. Take as a B the set of all vectors in V_k^n with weight at most g in the first ℓ positions. Then by (2.2) we have

$$A(n, 2\delta, k) \le \frac{\binom{n}{k}|L(B)|}{|B|} = \frac{\binom{n}{k}|L(B)|}{\sum_{i=0}^{g} \binom{\ell}{i}\binom{n-\ell}{k-i}}.$$

Note that $|L(B)| \le A(n-\ell, 2\delta - 2g, k-g)$. This follows from the easy observation, that deletion of the first ℓ positions and change of arbitrary i 1's to 0's in the last $n-\ell$ positions in every vector from $L(B)$ with weight $k-g+i$ $(i = 1, \ldots, g)$ (in the remaining positions) gives an $(n-\ell, 2\delta - 2g, k-g)$–code.

Finally we get (2.5) using the following identity, which can be easily verified

$$\frac{\binom{n}{k}}{\sum_{i=0}^{g} \binom{\ell}{i}\binom{n-\ell}{k-i}} = \frac{\binom{n}{\ell}}{\sum_{i=0}^{g} \binom{k}{i}\binom{n-k}{\ell-i}} \tag{2.6}$$

for $0 < k, \ell \le n$. ∎

Theorem 1 gives also the following necessary condition for existance of a diameter perfect code in $J(n, k)$ $(\mathcal{H}_q(n), G_q(n, k))$.

COROLLARY 2 *A D–diameter perfect code in $J(n, k)$ with minimum distance d exists only if for every $B \subset V_k^n$ and every maximal code $L(B) \subseteq B$ with minimum distance d holds*

$$A^*(n, d-2, k) \ge |B||L(B)|^{-1}.$$

The same holds in $\mathcal{H}_q(n)$ and $G_q(n, k)$.

Another condition, which easily can be derived with Theorem 1, is as follows.

COROLLARY 3 *$\mathcal{C}$ is a D–diameter perfect code in $J(n, k)$ $(\mathcal{H}_q(n), G_q(n, k))$ with $d(C) \ge D+1$ iff each maximal anticode $\mathcal{A}(D)$ contains a codeword.*

The next result compares the upper bounds of Theorem D for constant weight codes (with the same minimum distance), using Theorem AK 1.

THEOREM 2 *Let m, k, D, n be integers with $2k \le n$, $0 < m < k$. Then*

$$\frac{\binom{n}{k}}{A^*(n, D, k)} > \frac{\binom{n}{m}}{A^*(n, D, m)}. \tag{2.7}$$

Proof. Note first, that it suffices to prove the inequality

$$\frac{A^*(n, D, k)}{A^*(n, D, k-1)} < \frac{n-k+1}{k}. \tag{2.8}$$

Indeed applying (2.8) $k-m$ times we will get the desired relation. Let $r \ge 0$ be determined from relation (i) of Theorem AK 1, where $t = \frac{2k-D}{2}$.

Then by Theorem AK 1

$$A^*(n, D, k) = \sum_{i=0}^{r} \binom{t+2r}{t+r+i} \binom{n-t-2r}{k-t-r-i}.$$

Further, since

$$A^*(n, D, k-1) = M(n, k-1, t-1) \ge \sum_{j=0}^{r} \binom{t+2r-1}{t+r+j-1} \binom{n-t-2r+1}{k-t-r-j},$$

we have

$$\frac{A^*(n, D, k)}{A^*(n, D, k-1)} \le \frac{\sum_{i=0}^{r} \binom{t+2r}{t+r+i}\binom{n-t-2r}{k-t-r-i}}{\sum_{j=0}^{r} \binom{t+2r-1}{t+r+j-1}\binom{n-t-2r+1}{k-t-r-j}}.$$

Set

$$f(i) = \frac{\binom{t+2r}{t+r+i}\binom{n-t-2r}{k-t-r-i}}{\binom{t+2r-1}{t+r+i-1}\binom{n-t-2r+1}{k-t-r-i}} = \frac{(t+2r)(n-k-r+i+1)}{(t+r+i)(n-t-2r+1)}.$$

From the relation

$$n < (k-t+1)\left(2 + \frac{t-1}{r}\right)$$

with $2k \le n$ we get $t + 2r \le k$. This implies

$$n - k - r + i + 1 > t + r + i.$$

Thus $f(i)$ is monotone decreasing and it suffices to show that

$$\frac{(t+2r)(n-k-r+1)}{(t+r)(n-t-2r+1)} < \frac{n-k+1}{k}$$

or equivalently

$$n + \frac{r(k-t-r)}{n-k-r+1} > \frac{k(t+2r)}{t+r} + t + r - 1. \tag{2.9}$$

Denote the LHS of (2.9) by $g(n)$. The function $g(n)$ is increasing for $n \geq n_m = \sqrt{r(k-t-r)} + k + r - 1$. We have

$$(k-t+1)\left(2+\frac{t-1}{r+1}\right) = n_1 \leq n.$$

One can check that $n_m < n_1$. Hence it is sufficient to show the desired relation for $n = n_1$. That is, we have to verify the following inequality

$$\frac{(t+2r+1)(k-t+1)}{r+1} + \frac{r(r+1)(k-t-r)}{(t+r)(k-t-r)+2(r+1)} - \frac{k(t+2r)}{t+r} - t - r + 1 > 0. \tag{2.10}$$

We distinguish two cases: (i) $k \geq t+2r+1$ and (ii) $k = t+2r$.

Denote the LHS of (2.10) by $h(k)$. One can check now that $h(t+2r+1) > 0$ and $h(t+r) < 0$.

On the other hand it can be easily seen that there exists $0 \leq k_0 < t+r$ such that $h(k_0) > 0$. Hence $h(k)$ monotonically increases when $k \geq t+2r+1$ i.e. $h(k) > 0$ as desired.

The case (ii) $k = t+2r$ needs slightly a more delicate estimation. In this case we have

$$n_m < n_1 = (k-t+1)\left(2+\frac{t-1}{r+1}\right) = 4r + 2t - \frac{t-1}{r+1} = 2k - \frac{t-1}{r+1} < 2k \leq n.$$

Hence for the case (ii) it suffices to show (2.9) for $n = 2k = 2(t+2r)$, which easily can be verified.

Remark 3. The following example shows that in general (2.7) cannot be improved even by a constant factor $c > 1$ in the RHS. Let $n = 2k$, $m = k-1$, $D = 4$ (in fact one can take any D). Then in view of Theorem AK1, if $k > 3$ the maximal anticode of diameter 4 in $J(2k, k)$ and $J(2k, k-1)$ is a ball of Hamming radius 2. Hence $A^*(2k, 4, k) = k^2 + 1$, $A^*(2k, 4, k-1) = k^2$. By (2.7) we have

$$\frac{\binom{2k}{k}}{k^2+1} > \frac{\binom{2k}{k-1}}{k^2}$$

and clearly RHS/LHS goes to 1 as $k \to \infty$.

3. Examples of D–Diameter Perfect Codes in $J(n, k)$

We have from (2.2) and Theorem AK 1 in the Introduction that

$$A(n, 2\delta, k) \leq \frac{\binom{n}{k}}{|\mathcal{F}_r|}, \tag{3.1}$$

with $r \in \mathbb{N} \cup \{0\}$ as specified there.

Example 1. Let $k, n \in \mathbb{N}$ and $k|n$. Obviously there exists an $(n, 2k, k)$–code $\mathcal{C}$ with $|\mathcal{C}| = \frac{n}{k}$. We have

$$|\mathcal{C}| = \frac{n}{k} = \frac{\binom{n}{k}}{A^*\big(n, 2(k-1), k\big)} = \frac{\binom{n}{k}}{M(n,k,1)} = \frac{\binom{n}{k}}{\binom{n-1}{k-1}}.$$

Thus $\mathcal{C}$ is a D–diameter perfect code with $D = D_H = 2(k-1)$. This is also e–perfect (the trivial code) in the case $n = 2k$, k odd, $e = \frac{k-1}{2}$.

This example is a special case of a class of diameter perfect codes obtained from Steiner systems.

A Steiner system $S(n, t, k)$ is a collection of k–subsets (called blocks) taken from an n–set such that for each t–subset of the n–set there exists exactly one block containing this t–subset. The number b of blocks is

$$b = \binom{n}{t} \Big/ \binom{k}{t}. \tag{3.2}$$

A necessary condition for a Steiner system to exists is that

$$\binom{n-i}{t-i} \Big/ \binom{k-i}{t-i} \in \mathbb{N} \text{ for } 0 \le i \le t. \tag{3.3}$$

Representing blocks by $0-1$–vectors one sees that a Steiner system $S(t, k, n)$ is equivalent to a constant weight code with parameters $\big(n, 2(k-t+1), k\big)$, because any two vectors have at most $t-1$ ones in common.

LEMMA 1 *Any Steiner system $S(t, k, n)$ forms a diameter perfect code.*

Proof. Let $\mathcal{C}$ be an $\big(n, 2(k-t+1), k\big)$–code corresponding to a $S(t, k, n)$. Then

$$|\mathcal{C}| = \frac{\binom{n}{t}}{\binom{k}{t}} = \frac{\binom{n}{k}}{\binom{n-t}{k-t}}.$$

On the other hand $|\mathcal{C}| \le \dfrac{\binom{n}{k}}{A^*\left(n, 2(k-t), k\right)}$ and therefore $A^*\big(n, 2(k-t), k\big) \le \binom{n-t}{k-t}$.

Since there exists an anticode of size $\binom{n-t}{k-t}$ the statement follows. ∎

Next we return to e–perfect codes in $J(n, k)$. Suppose that $\mathcal{C}$ is an $(n, 2\delta, k)$–code which is e–perfect. Then clearly $\delta = 2e + 1$ and

$$|\mathcal{C}| = \binom{n}{k} \left(\sum_{i=0}^{e} \binom{k}{i} \binom{n-k}{i} \right)^{-1}.$$

The parameters of a maximal anticode of diameter $D_H = 2(\delta - 1)$ can be found (see Theorem AK 1) from the relation

$$\delta\left(2 + \frac{k-\delta}{r+1}\right) \leq n < \delta\left(2 + \frac{k-\delta}{r}\right). \tag{3.4}$$

We must have $k - \delta + 1 + 2r = k$ and therefore $r = \frac{\delta-1}{2} = e$. Hence

$$n \leq (2e+1)(k-1)/e,$$

which is Roos's result reported in the Introduction.

The following necessary condition for the existence of e–perfect codes [7] inspired us to obtain a similar condition for D–diameter perfect codes:

THEOREM 3 [7] *If an e–perfect code in $J(n, k)$ exists then Steiner systems $S(e+1, 2e+1, k)$ and $S(e+1, 2e+1, n-k)$ exist.*

THEOREM 4 *Assume that there exists a diameter perfect $(n, 2\delta, k)$–code $\mathcal{C}$ and $r \in \mathbb{N} \cup \{0\}$ is the parameter obtained from (3.4). Then Steiner systems $S(\delta - r, \delta, k)$ and $S(r+1, \delta, n-k)$ exist.*

Proof. Let b_0 be a codeword. Partition the set of coordinates $\{1, \ldots, n\}$ into two parts N_1 and N_2, such that N_1 is the position of 1's in b_0. We will say that x is an (i, j)–vector, if it has weight i in part N_1 and weight j in N_2.

Consider now all codewords, which are at distance $2\delta = 2(k - t + 1)$ from b_0, and the vectors of weight $t + 2r$, which are at distance $k - t + 2$ from b_0. That is, we consider all $(t-1, k-t+1)$–code vectors B and all $(t + r - 1, r + 1)$–vectors.

In view of Theorem AK 1 each maximal anticode (in $J(n, k)$) of diameter $D = 2(\delta - 1)$ can be represented as a vector of weight $t + 2r$, where r is obtained from (3.4). Moreover, Corollary 3 implies that for any $u \in V^n_{t+2r}$ there exists a $v \in \mathcal{C}$, such that $d(u, v) \leq k - t$. This means that for each $(t + r - 1, r + 1)$–vector u there exists precisely one codeword $v \in B$, such that v is covered by u (is contained in u as a set) in part N_1 and v covers u in part N_2. Transform now B into B' by inverting 0's and 1's in vectors of B, in part N_1.

Clearly we obtain $(k - t + 1, k - t + 1)$–vectors. It is easily seen that B' forms a "two part Steiner" system. That is any $(k - t - r + 1, r + 1)$–vector is covered by exactly one $(k - t + 1, k - t + 1)$–vector from B', and no $k - t + 2$–vector is covered by two different vectors from B'.

Since $\delta = k - t + 1$ this clearly enforces

$$|B| = |B'| = \frac{\binom{k}{\delta-r}\binom{n-k}{r+1}}{\binom{\delta}{\delta-r}\binom{\delta}{r+1}}.$$

A Steiner system $S(\delta - r, \delta, k)$ ($S(r+1, \delta, n-k)$) can be obtained from B' in part N_1 (resp. N_2) by taking all vectors of B' with fixed $r + 1$ 1's in N_2 (resp. $\delta - r$ 1's in N_1). ∎

Example 2. There exists a Steiner system $S(5, 8, 24)$, which is a diameter perfect (24,8,8)–code. Since $(k - t + 1)(t + 1) = 4 \cdot 6 = 24$, by Theorem AK 1 we have two choices of $r : r = 0$, or $r = 1$. Therefore by Theorem 4 (with $r = 1$) we obtain two Steiner systems, $S(3, 4, 8)$ and $S(2, 4, 16)$.

COROLLARY 4 *A diameter perfect* $(n, 2\delta, k)$*–code exists only if* $k \geq (r + 1)(\delta - r + 1)$.

Proof. This follows from the known fact that for any Steiner system $S(t, k, n)$ necessarily $n \geq (k - t + 1)(t + 1)$. Note that this immediately follows from Theorem AK 1 using Theorem D.

One can also obtain additional necessary conditions using divisibility conditions (3.3). ■

4. Examples of D–Diameter Perfect Codes in $\mathcal{H}_q(n)$

An $(n, d)_q$–code $\mathcal{C}$ is called MDS–code (maximum distance separable code), if it meets the Singleton bound, that is,

$$|\mathcal{C}| = q^{n-d+1}.$$

Reed–Solomon codes [14] are an example of MDS–codes.

LEMMA 2 *Any MDS–code is diameter perfect.*

Proof. The set of all vectors with fixed $n - d + 1$ coordinates forms an anticode of diameter $d - 1$ and size q^{d-1}. Thus $|\mathcal{C}|q^{d-1} = q^n$ and the result follows. ■

We say that $\mathcal{C}'$ is an extended code if it is obtained from a code $\mathcal{C}$ by adding an extra symbol to every codeword, such that $d(\mathcal{C}') = d(\mathcal{C}) + 1$.

LEMMA 3 *If* $\mathcal{C}$ *is a diameter perfect code in* $\mathcal{H}_q(n)$*, then the extended code* $\mathcal{C}'$ *is also diameter perfect.*

Proof. Let $\mathcal{C}$ be a diameter perfect code with minimum distance d and let $\mathcal{A}$ be a maximal anticode of diameter $d - 1$. Set

$$\mathcal{A}' = \left\{ b^{n+1} \triangleq (a^n, \alpha) \colon a^n \in \mathcal{A}, \alpha \in \{0, 1, \ldots, q - 1\} \right\}.$$

Clearly $\operatorname{diam}(\mathcal{A}') \leq d$ and $|\mathcal{A}'| = q|\mathcal{A}|$. Then $|\mathcal{A}'||\mathcal{C}'| = q^{n+1}$ and the statement follows. ■

COROLLARY 5 *The extended Hamming and Golay codes are diameter perfect.*

Remark 4. Using standard notation we denote by $[n, k, d]_q$ a q–ary linear code of length n, dimension k and minimum distance d. It is known (see [14]), that there exist extended Golay codes ([24, 12, 8]–code and $[12, 6, 6]_3$–code) and extended binary Hamming code ($[2^m, 2^m, -m - 1, 4]$–code).

There are also q–ary extended Hamming $[q+2, q-1, 4]_q$–codes in the case when $q = 2^r$, $q \geq 2$, which are also MDS codes. On the other hand one can show that there are no other extended Hamming codes. (This follows e.g. from a result in [10] (Theorem 5.3).)

However we do not know whether there are extensions of nonlinear q–ary perfect codes (which have the same parameters as Hamming codes).

THEOREM 5 *In $\mathcal{H}_q(n)$ (q is a prime power) there are no diameter perfect codes except for the codes having the parameters of the Hamming and extended Hamming codes, Golay and extended Golay codes, MDS codes.*

Proof. Let $\mathcal{C}$ be a D–diameter perfect $(n, d)_q$–code and let r be the parameter obtained from relation (1.13). Suppose also that $r \neq \frac{d-1}{2}$ (i.e. $\mathcal{C}$ is not an e–perfect code) and $r > 0$ (if $r = 0$ we have an MDS code).

We have

$$|\mathcal{C}| = q^n / A_q^*(n, d-1),$$

and in view of Theorem AK 2

$$A_q^*(n, d-1) = |B_r^{n-d+2r+1}(u)| \cdot q^{d-2r-1}.$$

Then puncturing some position in $\mathcal{C}$ we obtain an $(n-1, d-1)_q$–code $\mathcal{C}_1$ with $|\mathcal{C}_1| = |\mathcal{C}|$.

Clearly $\mathcal{C}_1$ is a $(D-1)$–diameter perfect code, because there exists an anticode (in $\mathcal{H}_q(n-1)$) of diameter $d-2$ and of size $|B_r^{n-d+2r+1}(u)| \cdot q^{d-2r-2}$.

Repeating this procedure we will finally get a diameter perfect code with parameters $n^* = n - d + 2r + 1$, $d^* = 2r + 1$ and this is a perfect code with parameters of Hamming or Golay codes. Next clearly on the length $n^* + 1$ we have extended Golay codes or a code with parameters of an extended Hamming code.

On the other hand one can easily show that there are no doubly extended Golay codes, or codes with parmeters of possible doubly extended Hamming codes.

Namely $(25, 9)_2$–code with cardinality $M = 2^{12}$, $(13, 7)_3$–code with $M = 3^6$ and $(\frac{q^m-1}{q-1} + 2, 5)_q$–code with $M = q^{n-m}$ ($n = \frac{q^m-1}{q-1}$, $m > 2$). This completes the proof. ∎

Remark 5. Note that MDS–codes include also trivial perfect codes. That is a q–ary code containing just one codeword $a \in \mathcal{H}_q(n)$ (by convention here $d = n+1$), the whole space, and an $(n, n)_q$ "repetition" code with q codewords.

5. Tiling in $J(n, k)$ with Caps

For $n, m, k, \ell \in \mathbb{N}$, $\ell \leq k$, $m < n$ and $E \in \binom{[n]}{m}$ define

$$\mathcal{F}_E = \left\{ A \subset \binom{[n]}{k} : |A \cap E| \geq \ell \right\}. \tag{5.1}$$

We say, that $\mathcal{B} \subset \binom{[n]}{m}$ forms a partition of $\binom{[n]}{k}$ if

$$\binom{[n]}{k} = \dot{\bigcup_{E \in \mathcal{B}}} \mathcal{F}_E.$$

Let $B_{r_1}(x)$ be the ball (in Hamming space) of radius r_1 and center x and let $S_{r_2}(y)$ be a "sphere" of radius r_2 centered at y (the boundary points of $B_{r_2}(y)$). Denote by $C(x)$ the cap

$$B_{r_1}(x) \cap S_{r_2}(y).$$

Clearly the characteristic vectors of $\mathcal{F}_E$, defined above form a cap $C(x) \subset V_k^n$, where $wt(x) = m$, $wt(y) = 0$, $r_1 = m + k - 2\ell$ and $r_2 = k$.

Further we will use the notation $C(x, \ell)$ to indicate the parameter ℓ in (5.1), that is

$$C(x, \ell) = \{u \in V_k^n \colon \langle x, u \rangle \geq \ell\},$$

where $\langle x, y \rangle$ is the number of common 1's in x and u.

Thus we can speak about the problem of tiling of V_n^k by caps. The problem of tiling of $H_2(n)$ by different balls is considered in [11]. Remind that Theorem AK 1 says that the maximal anticode in $J(n, k)$ of given diameter $2(k - t)$ is always a cap $C(x, t + r)$, $x \in V_{t+2r}^n$, with parameter r determined by the relation

$$(k - t + 1)\left(2 + \frac{t-1}{r+1}\right) \leq n < (k - t + 1)\left(2 + \frac{t-1}{r}\right). \tag{5.2}$$

Later we will associate with an $(n, 2\delta, k)$–code the parameters t and r, where $t - 1$ is the "maximal intersection" (the number of common 1's) between codewords (i.e. $t = k - \delta + 1$) and r is the parameter determined by relation (5.2).

THEOREM 6

(i) *If $\mathcal{C} \subset V_m^n$ is a D–diameter perfect code, then there exists a partition of V_{t+2r}^n by caps $C(x, t + r)$, $x \in \mathcal{C}$.*

(ii) *if V_k^n is partitioned by caps $C(x, \ell)$, $x \in \mathcal{C} \subset V_m^n$, then $\mathcal{C}$ is a diameter perfect code with minimum distance $2(m + k - 2\ell + 1)$.*

Proof. The idea of proof for part (i) is clear and we already used it in the proof of Theorem 4. However we give a formally complete proof. Let t, r be the parameters (defined above) of a D–diameter perfect code $\mathcal{C}$. We know that each anticode can be represented as vector of weight $t + 2r$.

Consider now the set of anticodes (taken as $t + 2r$–vectors) containing a given codeword x. Clearly this is a cap $C(x, t + r) \subset V_{t+2r}^n$. We claim that $V_{t+2r}^n = \dot{\bigcup}_{x \in \mathcal{C}} C(x, t + r)$.

Indeed, using a modification of identity (2.6) we get

$$|\mathcal{C}| = \frac{\binom{n}{m}}{A^*(n, D, m)} = \frac{\binom{n}{m}}{\sum_{i=0}^{m-t-r}\binom{t+2r}{t+r+i}\binom{n-t-2r}{m-t-r-i}} = \frac{\binom{n}{t+2r}}{\sum_{i=0}^{r}\binom{m}{t+r+i}\binom{n-m}{r-i}}$$

$$= \frac{\binom{n}{r+2r}}{|C(x, t+r)|}.$$

(ii) Assume now that there exists a partition of V_k^n by caps $C(x, \ell)$, $x \in \mathcal{C} \subset V_m^n$. One readily veryfies that two caps $C(x_1, \ell)$ and $C(x_2, \ell)$ are disjoint only if $2\ell > k$. Moreover if $x_1, x_2 \in \mathcal{C}$ they must have less than $2\ell - k$ common 1's. This means that for any $x_1, x_2 \in \mathcal{C}$

$$d_H(x_1, x_2) \geq 2(m + k - 2\ell + 1).$$

By condition (ii) of the Theorem together with (2.6) we get

$$|\mathcal{C}| = \frac{\binom{n}{k}}{\sum_{i=0}^{m-\ell}\binom{m}{\ell+i}\binom{n-m}{k+\ell-i}} = \frac{\binom{n}{m}}{\sum_{i=0}^{k-\ell}\binom{k}{\ell+i}\binom{n-k}{m-\ell-i}}.$$

Consider now a cap $C(u, \ell)$, $u \in V_k^n$. Clearly it is an anticode with $\operatorname{diam} C(u, \ell) = 2(m + k - 2\ell)$. Therefore by the code–anticode condition we have

$$|\mathcal{C}| \leq \frac{\binom{n}{m}}{|C(u, \ell)|} = \frac{\binom{n}{m}}{\sum_{i=0}^{k-\ell}\binom{k}{\ell+i}\binom{n-k}{m-\ell-i}}.$$

Hence $\mathcal{C}$ is a diameter perfect code and $C(u, \ell)$ is a maximal anticode.

The following question seems to be natural. Does the existence of a D–diameter perfect code in all cases imply a partition of the whole space by maximal anticodes as for e–perfect codes? The next theorem gives a negative answer. ■

THEOREM 7 *For given n, k, D there is no partition of V_k^n by maximal anticodes of diameter D, if the maximal anticode is not a ball in $J(n, k)$.*

Proof. By Theorem AK 1 the maximal anticode is a cap $C(x, t + r)$, $x \in V_{t+2r}^n$, where $t = \frac{2k-D}{2}$, and (by the condition of the Theorem) $t + 2r \neq k$.

Assume to the opposite that there is a partition

$$V_k^n = \dot{\bigcup_{x \in \mathcal{C}}} C(x, t + r), \mathcal{C} \subset V_{t+2r}^n.$$

W.l.o.g. we can assume that $2k \leq n$. This (with (5.2)) gives $k > t + 2r$.

Further by Theorem 6 $\mathcal{C}$ is a D–diameter perfect code (with minimum distance $2(k-t+1)$). Therefore

$$|\mathcal{C}| = \frac{\binom{n}{t+2r}}{A^*(n, D, t+2r)} = \frac{\binom{n}{k}}{|C(x, t+r)|}$$

$$= \frac{\binom{n}{k}}{\sum_{i=0}^{r}\binom{t+2r}{t+r+i}\binom{n-t-2r}{k-t-r-i}} = \frac{\binom{n}{t+2r}}{\sum_{i=0}^{k-t-r}\binom{k}{t+r+i}\binom{n-k}{r+i}}. \tag{5.3}$$

Hence the maximal anticode in V_{t+2r}^n of diameter D is a cap $\mathcal{C}(u, t+r)$, $u \in V_k^n$. Thus we have $k = t' + 2r'$, where $t' = 2t + 2r - k$ and the parameter r' is obtained from the relation

$$(t+2r-t'+1)\left(2+\frac{t'-1}{r'+1}\right) \le n < (t+2r-t'+1)\left(2+\frac{t'-1}{r'}\right).$$

This implies $t' + 2r' \le t + 2r$, which is a contradiction. ■

6. Open Problems

1. Of course one of the main problem left is to clarify, whether there exist diameter perfect codes in $J(n, k)$ aside from Steiner systems.

   More generally one can ask about the existence of perfect sets in $J(n, k)$. That is a pair of sets $X, Y \subset V_k^n$ satisfying the condition of Theorem D and $|X||Y| = \binom{n}{k}$. The analogous question can be asked for $\mathcal{H}_q(n)$.

2. Are there diameter perfect codes in $G_q(n, k)$? Let V be an n–dimensional vector space over $GF(q)$. For $k \ge 0$ we denote by $\begin{bmatrix} V \\ k \end{bmatrix}_q$ the set of all k–dimensional subspace of V. A family $\mathcal{F} \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$ is called t–intersecting iff $\dim(F_1 \cap F_1) \ge t$ for all $F_1, F_2 \in \mathcal{F}$ or, equivalently, $\operatorname{dist}(F_1, F_2) \triangleq \dim(F_1) + \dim(F_2) - 2\dim(F_1 \cap F_2) \le 2(k-t)$. Frankl and Wilson [8] proved:

   For every t–intersecting family $\mathcal{F} \subset \begin{bmatrix} V \\ k \end{bmatrix}_q$ holds

$$|\mathcal{F}| \le \begin{cases} \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q, & \text{if } n \ge 2k \\ \begin{bmatrix} 2k-t \\ k \end{bmatrix}_q, & \text{if } 2k-t < n < 2k. \end{cases}$$

   This result together with Theorem D implies that in $G_q(n, k)$ only "Steiner system type" diameter perfect codes can exist. Here $\mathcal{F} \subset \begin{bmatrix} V \\ k \end{bmatrix}_q$ is called a Steiner system $S(t, k, n)_q$

if each t–space from V is contained in exactly one k–space from $\mathcal{F}$. We know only $S(1, k, n)_q$ (k divides n) Steiner systems in $G_q(n, k)$, which are just partitiones of $V \setminus \{0\}$ into k–spaces (with excluded 0–vector).

3. In section 5 we have shown that V_k^n cannot be partitioned into maximal anticodes, if the maximal anticode is not a ball. Now, we ask whether V_k^n can be nontrivially partitioned into diameter perfect codes?

   In one case it is possible, namely, by Baranyai's theorem V_k^n (k divides n) can be partitioned into $\binom{n-1}{k-1}$ classes of $S(1, k, n)$ Steiner systems (see [4]).

References

1. R. Ahlswede and L.H. Khachatrian, The complete intersection theorem for systems of finite sets, *European J. Combin.*, Vol. 18 (1997) pp. 125–136.
2. R. Ahlswede and L.H. Khachatrian, The diametric theorem in Hamming spaces—optimal anticodes, *Advances in Applied Mathematics*, Vol. 20 (1998) pp. 429–449.
3. E. Bannai, Codes in bi–partite distance–regular graphs, *J. of London Math. Soc.*, (2), Vol. 16 (1982) pp. 197–202.
4. Z. Baranyai and A.E. Brouwer, Extension of colourings of the edges of a complete (uniform) hypergraph, *Math. Centrum Dep. Pure Math. ZW.*, Vol. 91 (1977).
5. G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering codes*, Elsevier (1997).
6. P. Delsarte, An algebraic approach to association schemes of coding theory, *Phillips J. Res.*, Vol. 10 (1973).
7. T. Etzion, On the nonexistence of perfect codes in the Johnson scheme, *SIAM J. Discrete Mathematics*, Vol. 9 (1996) pp. 201–209.
8. P. Frankl and R.M. Wilson, The Erdös–Ko–Rado theorem for vector spaces, *J. Combin. Theory Ser. A*, Vol. 43 (1986) pp. 228–236.
9. P. Hammond, On the non–existence of perfect and nearly perfect codes, *Discrete Math*, Vol. 39 (1982) pp. 105–109.
10. R. Hill, Caps and codes, *Discrete Math.*, Vol. 22 (1978) pp. 111–137.
11. H.D.L. Hollmann, J. Körner and S. Litsyn, Tiling Hamming space with few spheres, *J. Combinatorial Th., Ser. A*, Vol. 80 (1997) pp. 388–393.
12. I. Honkala, H. Hamalainen and M. Kaikkonen, A modification of the Zinoviev lower bound for constant weight codes, *Discrete Applied Mathematics*, Vol. 11 (1985) pp. 307–310.
13. V. Levenshtein, On the minimal redundancy of binary error–correcting codes, *Information and Control*, Vol. 28 (1975) pp. 268–291.
14. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error Correcting Codes*, North–Holland, Amsterdam (1977).
15. C. Roos, A note on the existence of perfect constant weight codes, *Discrete Math.*, Vol. 47 (1983) pp. 121–123.
16. J.H. van Lint, On the nonexistence of certain perfect codes, in *Computers in Number Theory* (Atkin and Birch, Eds.), Acad. Press, New York (1971) pp. 227–282.
17. A. Tietäväinen, On the nonexistence of perfect codes over finite fields, *SIAM J. Appl. Math.*, Vol. 24 (1973) pp. 88–96.
18. V.A. Zinov'ev and V.K. Leont'ev, The nonexistence of perfect codes over Galois fields, *Probl. Control and Inform. Theory*, Vol. 2 (1973) pp. 123–132.
19. V. Zinoviev, On a generalization of the Johnson bound, *Problemy Peredachi Informatsii*, Vol. 20, No. 3 (1984) pp. 105–108.