Discrete Mathematics 56 (1985) 125–131
North-Holland

GOOD COVERINGS OF HAMMING SPACES WITH SPHERES

Gérard COHEN

Ecole Nationale Supérieure des Télécommunications, 75013 Paris, France

Peter FRANKL

CNRS, 75007 Paris, France

Received December 1984

We give a non-constructive proof ot the existence of good coverings of binary and non binary Hamming spaces by spheres centered on a subspace (linear codes). The results hold for tiles other than spheres.

1. Introduction

We denote by $H(n, q)$ the n dimensional vector space over F_q endowed with the Hamming metric: for $x = (x_i)$, $y = (y_i)$ in $H(n, q)$, $d(x, y) = |\{i: 1 \leqslant i \leqslant n, x_i \neq y_i\}|$. A sphere $S(c, r)$ with center c and radius r has cardinality $S_r = \sum_{i=0}^{r} (q-1)^i \binom{n}{i}$. For an (n, k) linear code C (i.e., a linear k dimensional subspace of $H(n, q)$) denote by $d(C)$ its minimum distance, $\rho(C)$ its covering radius, defined respectively as:

$$d(C) = \min d(c_i, c_j), \quad \text{over all } c_i, c_j \text{ in } C$$

$$\rho(C) = \min r \text{ s.t. } \bigcup_{c \in C} S(c, r) = H(n, q).$$

The covering radius problem has been considered by many authors (e.g. [1, 5, 6]). Finally, let $t(n, k)$ be the minimum possible covering radius for an (n, k) code and $k(n, \rho)$ the minimum possible dimension of a code with covering radius ρ. The study of $t(n, k)$ was initiated by Karpovsky. For a survey of these questions, see [4].

The main goal of this paper is to find good linear coverings.

The unrestricted (nonlinear) case is considered in Section 4, where existence theorems for coverings are given in a generalized setting, namely coverings of association schemes by tiles, using a result of Lovász (based on the greedy algorithm [8]).

Our first result is the following.

Theorem 1.

$$n - \log_q S_\rho \leqslant k(n, \rho) \leqslant n - \log_q' S_\rho + 2 \log_2 n - \log_q n + \mathrm{O}(1). \tag{1}$$

0012-365X/85/$3.30

In the sequel, C_j will denote a (n, j) code and N_j the proportion of elements in $H(n, q)$ at distance more than ρ from C_j. At each step C_j is obtained from C_{j-1} by adding a new element $x \notin C_{j-1}$, chosen so as to minimize N_j (linear greedy algorithm), i.e., $C_j = \langle C_{j-1}; x\rangle$, the subspace spanned by C_{j-1} and x.

2. The binary case

The case $q = 2$, solved in [3], is proved here in a different way, using the following simple lemma, valid for all q.

Lemma 1. *Let Y, Z be subsets of $H(n, q)$, and $Y + x = \{y + x : y \in Y, x \in H(n, q)\}$, then the average value of $|Y + x \cap Z|$ over all x in $H(n, q)$, $E(|Y + x \cap Z|)$, is $q^{-n} |Y| |Z|$.*

Proof.

$$\sum_{x\in H(n,q)} |Y+x\cap Z| = \sum_{x\in H(n,q)} \sum_{y\in Y} \sum_{\substack{z\in Z\\ y+x=z}} 1 = \sum_{y\in Y} \sum_{z\in Z} \sum_{\substack{x\in H(n,q)\\ x=z-y}} 1 = |Y|\,|Z|.$$

When $|Y| = |Z|$, this yields $E(1 - q^{-n} |Y + x \cup Z|) = (1 - q^{-n} |Z|)^2$. Setting $Y = Z = \bigcup_{c\in C_{j-1}} S(c, \rho)$, we have

$$N_j \leqslant (1 - q^{-n} |Z|)^2, \qquad N_j \leqslant N_{j-1}^2 \leqslant N_0^{2^j} = (1 - q^{-n} S_\rho)^{2^j}. \tag{2}$$

(See [11], for $q = 2$.)

For $q = 2$ and j equal to the RHS of (1), $N_j < 2^{-n}$. Hence $N_j = 0$. That is there exists a (n, j) code having covering radius ρ, with j at most equal to the RHS of (1).

The lower bound in (1) is an immediate consequence of the sphere covering bound $2^k S_\rho \geqslant 2^n$. $\square$

3. The non binary case

We use the same method: construct a $(n, j + 1)$ code C_{j+1} from C_j by adding a generator x 'optimally', but we don't get an analogous result (namely $N_{j+1} \leqslant N_j^q$), because for v in $\mathbb{F}_q^n$, the events constituting the set $\{v : v \in Z_j + \alpha x, \alpha \in \mathbb{F}_q\}$ can no longer be viewed as independent. Still it will 'almost' be true for a while: namely, as long as $N_j < 1 - (qn)^{-1}$, and this we prove now.

Lemma 2. *For $Z \subset \mathbb{F}_q^n$ s.t. $|Z|\, q^{-n} = \varepsilon < (qn)^{-1}$, one has*

$$P = E\left(1 - q^{-n} \left|\bigcup_{\alpha\in F_q} Z + \alpha x\right|\right) \leqslant (1 - \varepsilon)^{q(1-(2n)^{-1})}.$$

Proof. By the principle of inclusion–exclusion.

$$\begin{aligned} P &\leqslant 1 - q\varepsilon + \binom{q}{2}\varepsilon^2 \\ &\leqslant 1 - q(1 - q\varepsilon/2)\varepsilon \\ &\leqslant (1-\varepsilon)^{q(1+q\varepsilon/2)} \quad \text{(Bernouilli's inequality).} \end{aligned}$$

Setting as in Lemma 1, $Z = \bigcup_{c \in C_j} S(c, \rho)$, for $|Z| < q^{n-1}/n$, $N_{j+1} \leqslant N_j^{q(1-(2n)^{-1})}$. That is

$$N_{j+1} \leqslant (1 - q^{-n}S_\rho)^{(q(1-(2n)^{-1}))^j} \leqslant (1 - q^{-n}S_\rho)^{e^{-0.5}q^j}$$

since $(1-(2n)^{-1})^j \geqslant (1-(2n)^{-1})^{n-1} \geqslant e^{-1/2}$. □

Lemma 3. *The minimum value j_1 of j s.t. $N_j \leqslant 1-(qn)^{-1}$ satisfies:*

$$j_1 \leqslant n - \log_q S_\rho - \log_q n + \mathrm{O}(1). \tag{3}$$

Proof. According to Lemma 2, one has

$$1-(qn)^1 \leqslant N_{j-1} \leqslant (1-q^n S_\rho)^{q^{j_1-1}e^{-1/2}} \tag{4}$$

Comparing the two extreme sides in this double inequality, one gets (3). □

Now we start with a (n, j_1) code C. We have $N_{j+1} \leqslant N_j^2$ by (2) and next we are looking for the minimum number j_2 of generators x that must be added to C to get a (n, j_1+j_2) code with $N_{j_1+j_2} \leqslant q^{-n}$. But $N_{j_1} \leqslant 1-(qn)^{-1}$, so by (4) we only need $(1-(qn)^{-1})^{2^{j_2}} \leqslant q^{-n}$ which is realized for $j_2 = 2\log_2 n + \mathrm{O}(1)$. Hence there exist codes (n, j) with $j \leqslant j_1 + j_2$ having covering radius at most ρ, proving the upper bound in (1).

Like for the binary case, the lower bound comes from the sphere covering bound $q^k S_\rho \geqslant q^n$.

Defining $E_q(x) = x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x)$ for $0 \leqslant x \leqslant 1/2$ (q-ary entropy function), it is well known that

$$\lambda n^{-1/2} q^{nE_q(c)} \leqslant \sum_{i=0}^{cn} (q-1)^i \binom{n}{i} \leqslant q^{nE_q(c)},$$

$0 < c < 1/2$, c, λ, constant, which gives:

Corollary 1.

$$n(1 - E_q(\rho/n)) \leqslant k(n, \rho) \leqslant n(1 - E_q(\rho/n)) + \mathrm{O}(\log n),$$

and for $k/n = R$ fixed,

$$\lim_{n\to\infty} n^{-1} t(n, Rn) = E_q^{-1}(1-R),$$

because $nE_q^{-1}(1-R) \leqslant t(n, nR) \leqslant nE_q^{-1}(1-R) + \mathrm{O}(\log n)$.

Conjecture. Corollary 1 holds for almost all codes, i.e., when n goes to infinity, the proportion of (n, nR) codes C whose covering radius $\rho(C)$ satisfies

$$nE_q^{-1}(1-R) \leq \rho(C) \leq nE_q^{-1}(1-R) + \mathrm{O}(\log n)$$

goes to one for fixed R.

Depending on this conjecture, we present another 'proof' of the following known result [7].

Theorem 2. *For almost all codes, the Varshamov–Gilbert* (VG) *bound is tight, namely* $d \leq nE_q^{-1}(1-k/n)$.

Proof. The proof uses the following lemma's.

Lemma 4 ('Supercode' lemma). *If* $C \subsetneq C'$, *then* $\rho(C) \geq d(C')$.

The proof is easy: take $v \in C' \setminus C$, then $\rho(C) \geq d(v, C) \geq d(C')$.

Lemma 5. *Let* $\mathscr{C}_i$ *be the family of* (n, i) *codes. Then* $p\,|\mathscr{C}_{k+1}|$ *codes* $(n, k+1)$ *contain at least* $p\,|\mathscr{C}_k|$ *codes* (n, k); $0 \leq p \leq 1$.

Proof. Let G be the bipartite graph with vertex set $\mathscr{C}_k \cup \mathscr{C}_{k+1}$ and with an edge between $C \in \mathscr{C}_k$ and $C' \in \mathscr{C}_{k+1}$ if $C \subset C'$. G is 'regular' with degrees a and b for vertices of $\mathscr{C}_k$ and $\mathscr{C}_{k+1}$ respectively and $a\,|\mathscr{C}_k| = b\,|\mathscr{C}_{k+1}|$.

Now consider the subgraph H induced by a subfamily $\mathscr{C}'_{k+1}$ of $\mathscr{C}_{k+1}$ with cardinality $p\,|\mathscr{C}_{k+1}|$. Let $\mathscr{C}'_k$ be the subfamily of $\mathscr{C}_k$ contained by elements of $\mathscr{C}'_{k+1}$. then in H every vertex in $\mathscr{C}'_{k+1}$ has degree b and every vertex in $\mathscr{C}'_k$ has degree $\leq a$, yielding $|\mathscr{C}'_{k+1}|b \leq |\mathscr{C}'_k|\,a$, i.e., $|\mathscr{C}'_k| \geq p\,|\mathscr{C}_{k+1}|\,(b/a) = p\,|\mathscr{C}_k|$. $\square$

Back to the theorem now. The VG bound [9, p. 557] states that there exists an (n, k) code with minimum distance d and $S_{d-1} \geq q^{n-k}$ or equivalently $d/n \geq E_q^{-1}(1-k/n)$.

Let $\mathscr{C}'_{k+1}$ be the family of $(n, k+1)$ codes C', with $n^{-1}(k+1) = R$, above this bound, i.e., satisfying $n^{-1}d(C') \geq E_q^{-1}(1-R) + f(R)$ for some positive function f. Then the associated family $\mathscr{C}'_k$ contains (n, k) codes whose covering radius satisfy the same lower bound by Lemma 4. Hence by the conjecture, p goes to 0 when n goes to ∞. On the other hand it has recently been proved [10] that there exist codes better than the VG bound. $\square$

4. The non linear case

The problem of determining the minimum number $K(n, \rho)$ of code words in a non linear code with covering radius ρ, can also be formulated in the form: What is the minimum number of spheres of radius ρ which cover the Hamming space $\mathbb{F}_q^n$?

Using a result of Lovász [8] we deduce the following.

Theorem 3. *Suppose for every $x \in \mathbb{F}_q^n$ we are given a set $B(x) \subset \mathbb{F}_q^n$ such that:*

(i) $|B(x)| = |B(y)| = b$, $\forall x, y \in \mathbb{F}_q^n$,

(ii) $|\{y \in \mathbb{F}_q^n : x \in B(y)\}| = b$, $\forall x \in \mathbb{F}_q^n$

(i.e., $\mathcal{B} = \{B(x): x \in \mathbb{F}_q^n\}$ is a b-uniform, regular hypergraph [12]*). Then there exists a code $C \subset \mathbb{F}_q^n$, such that $\bigcup_{x \in G} B(x) = \mathbb{F}_q^n$, and $|C| \leq (q^n/b)(1 + \log_2 b)$.*

Proof. Let $\mathcal{H}$ be the dual hypergraph of $\mathcal{B}$, i.e., the vertices of $\mathcal{H}$ are the edges of $\mathcal{B}$, and for every vertex of $\mathcal{B}$ we have an edge of $\mathcal{H}$, consisting of those edges of $\mathcal{B}$ which contain this vertex. Then $\mathcal{H}$ is b-uniform and b-regular, as well. Applying Corollary 2 of Lovász [8] we obtain that there exists a set A of vertices of $\mathcal{H}$ with $|A| = a \leq (q^n/b)(1 + \log_2 b)$, such that every edge $H \in \mathcal{H}$ satisfies $H \cap A \neq \emptyset$. By the definition of $\mathcal{H}$ we have $A = \{B(x_1), \ldots, B(x_a)\}$.

Now the condition $H \cap A \neq \emptyset$ is equivalent to $\bigcup_{i=1}^a B(x_i) = \mathbb{F}_q^n$, i.e., choose $C = \{x_1, \ldots, x_a\}$ and the theorem is proved. $\square$

Remark. Of course, by taking $B(x) = S(x, \rho)$ in Theorem 3, we get:

$$K(n, \rho) \leq q^n S_\rho^{-1}(1 + \log_2 S_\rho). \tag{5}$$

Theorem 3 can be generalized to any association scheme A with relations $R_0, R_1, \ldots, R_n$ by defining for all x in A: $B(x, r) = \{y \in A : \exists i, 0 \leq i \leq r, xR_iy\}$. In particular, it holds for the Johnson scheme $J(n, q, w)$, set of all q-ary n-tuples having exactly w non-zero coordinates. This answers a question of Csiszàr. Namely

$$\exists C = \{c_i\} \subset J(n, q, w), \quad \text{s.t.} \bigcup B(c_i, r) \supset J(n, q, w)$$

and

$$|C| \leq \frac{(q-1)^w \binom{n}{w}}{b}(1 + \log_2 b),$$

where $b = \sum_{i=0}^r \binom{w}{i}\binom{n-w}{i} = |B(c, 2r)|$.

Wyner and Ziv consider a related question in [13], and get the weaker expression $K(n, \rho) \leq q^n S_\rho^{-1} \cdot o(q^n)$ instead of (5).

5. The value of $t(n, n - [c \log_q n])$, for fixed c

We want to give a more precise estimation of j_2 (see proof of Lemma 3). To that end, we notice that we only need to reach $N_k < q^{-n+k}$, because if for a given (n, k) code C, there exists a v at distance more than ρ from C, then the whole coset $C + v$ has the same property. Hence $N_k < q^{-n+k}$ implies $N_k = 0$.

For fixed c, $n-k \leqslant \log_q S_c$ (Theorem 1) implies $n-k \leqslant c \log_q n + O(1)$, so we want $N_k \leqslant \lambda n^{-c}$. We shall reach $N_k < \lambda n^{-c}$ in three steps:

(1) For small $j: N_j < N_{j-1}^{q(1-(qn)^{-1})}$,

(2) For intermediate $j: N_j < N_{j-1}^{q-1}$,

(3) For larger $j: N_j < N_{j-1}^2$.

Lemma 6. *Suppose $q \geqslant 3$, then*

$$N_{j_1} < 1-(qn)^{-1} \qquad \text{for } j_1 = n - \log_q S_c - \log_q n + O(1), \tag{6}$$

$$N_{j_3+j_1} < 1-q^{-2} \qquad \text{for } j_3 = \log_{q-1} n + O(1), \tag{7}$$

$$N_{j_1+j_3+j_4} < \lambda n^{-c} \qquad \text{for } j_4 = c \log_2 \log_2 n + O(1). \tag{8}$$

Proof. (6) is already proved in Lemma 3. For (7) we use the fact that $\varepsilon < q^{-2}$ and deduce like in Lemma 2 $N_{j+1} < N_j^{q(1-0.5q\varepsilon)} < N_j^{q-1}$, for $j_1 \leqslant j < j_3$. Hence j_3 is the minimal integer s.t. $(1-(qn)^{-1})^{(q-1)^{j_3}} < 1-q^2$, yielding (7).

To finish, we only use $N_{j+1} \leqslant N_j^2$, which is always true, and get (8). $\square$

Hence for c fixed, $k(n, c) \leqslant j_1 + j_3 + j_4$, i.e., for n large

$$k(n, c) \leqslant n - (c-1)\log_q n$$

from which follows

$$t(n, n - \lceil (c-1)\log_q n \rceil) \leqslant t(n, k(n, c)) = c. \tag{9}$$

Now the left-hand side of (9) is strictly greater than $c-1$ (this follows from the sphere-covering bound $q^k S_\rho \geqslant q^n$). We thus have proved:

Theorem 4. *For $c \geqslant 2$ and integer, n large enough:*

$$t(n, n - \lceil (c-1)\log_q n \rceil) = c.$$

Remark. The case $q=2$ is simpler. We use $N_{j+1} \leqslant N_j^2$ and reach $N_0^{2^j} \leqslant n^{-c}$ for $j = n - \log_2 S_c + \log_2 \log_2 n + O(1)$. The proof goes then like for general q.

Example. $n = 2^m - 1$, $q = 2$, $e \in \mathbb{N} - \{0, 1\}$. For large enough n, $t(2^m-1, 2^m-1-me) = e+1$, i.e., BCH codes with $e > 2$ are not optimal for covering radius.

6. Conclusion

We exhibit here by non constructive methods efficient coverings of the Hamming space, using 'reasonable' tiles (not necessarily spheres). One can define the efficiency of a covering C of $H(n, q)$ by tiles B_i of cardinality b by

$$\Delta = n^{-1} \log_q |\bigcup B_i| - 1.$$

Then we get lattice (or linear) coverings with

$$0 \leqslant \Delta \leqslant 2n^{-1} \log_2 n$$

and non lattice coverings with

$$0 \leqslant \Delta \leqslant n^{-1} \log_q \log_2 b.$$

For q and the diameter d of the tiles fixed, $b \leqslant O(n^d)$, q-ary or even binary lattice coverings exist with

$$0 \leqslant \Delta \leqslant cn^{-1} \log \log n = c(\log(H(n, q)))^{-1} \log \log \log(H(n, q)),$$

for some constants c, d.

On the other hand, it is known that coverings with $\Delta = 0$ (perfect codes) almost never exist [2].

Acknowledgment

We are very grateful to the referee for his helpful comments and detection of an error in a previous paper.

References

[1] E.F. Assmus Jr. and H.F. Mattson Jr., Some 3-error-correcting BCH codes have covering radius 5, IEEE Trans. Inform. Theory 22 (1976) 348–349.
[2] M.R. Best, Optimal codes, Math. Centre Tracts 106 (1979) 119–140.
[3] G. Cohen, A non constructive upper bound on covering radius, IEEE Trans. Inform. Theory 29 (1983) 352–353.
[4] G. Cohen, M. Karpovsky, H.F. Mattson, Jr. and J.R. Schatz, A survey of covering radius, IEEE Trans. Inform. Theory (1985) to appear.
[5] P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, Inform. and Control 23 (1973) 407–438.
[6] T. Helleseth, T. Klove and J. Mykkeltveit, On the covering radius of binary codes, IEEE Trans. Inform. Theory 24 (1978) 627–628.
[7] V.N. Koshelev, On some properties of random group codes of great length, Problems Inform. Transmission 1(4) (1965) 35–38.
[8] L. Lovász, On the ratio of optimal integral and fractional covers, Discrete Math. 13 (1975) 383–390.
[9] J. MacWilliams and N.J. Sloane, The Theory of Error-correcting Codes (North-Holland, Amsterdam, 1977).
[10] M.A. Tsfasman, S.G. Vladut and Th. Zink, Modular curves, Shimura curves, and Goppa codes, better than the Varshamov–Gilbert bound, Math. Nachr., 104 (1982) 13–28.
[11] T. Berger, Rate-Distortion Theory (Prentice-Hall, Englewood Cliffs, NJ, 1971).
[12] C. Berge, Graphs and Hypergraphs (North-Holland, Amsterdam, 1973).
[13] A.D. Wyner, and J. Ziv, On communication of analog data from a bounded source space, Bell System Tech. J. 48 (10) (1969) 3139–3172.