TECHNION - Israel Institute of Technology
Computer Science Department

TILING CODES IN HAMMING SCHEMES

by

R.M. Roth and A. Lempel

Technical Report #434
September 1986
TILING CODES IN HAMMING SCHEMES

RON M. ROTH AND ABRÅHAM LEMPÉL

Department of Computer Science
Technion, Israel Institute of Technology
Haifa 32000 - Israel

ABSTRACT

A code $C$ of length $n$, even minimum Hamming distance $d$, and covering radius $R$, over an alphabet $\mathcal{Q}$ of $q$ elements is called a tiling code if (i) $R = \frac{d}{2}$, and (ii) for every two words $u$ and $v$ in $\mathcal{Q}^n$ of distance 1 apart there exists a codeword $c \in C$ such that both $u$ and $v$ are contained in the sphere of radius $R$ around $c$.

Tiling codes are analogous to the well-known perfect codes, which are defined by $R = \frac{d-1}{2}$, and which attain the sphere-packing bound. In a similar manner, tiling codes attain a so-called sphere-tiling bound, which is the analogue of the sphere-packing bound for even minimum distances.

As might be expected from the said analogy, there exist only a handful of tiling codes over finite fields. A complete characterization of all linear tiling codes is presented. In particular, it is shown that, with the exception of the $[q+2,q-1,4]$ MDS code when $q$ is even, there exist no linear extensions of Hamming codes over $GF(q)$ for $q > 2$ which increment both the length and the minimum distance of the code.
I. INTRODUCTION

Let $Q$ be an alphabet of $q$ elements. An $(n,M,d)$ code $C$ over $Q$ is a set of $M$ $n$-tuples over $Q$, with $d$ being the minimum distance between a pair of distinct words of $C$. When $Q$ is a finite field $GF(q)$, an $(n,q^k,d)$ code $C$ is called a linear $[n,k,d]$ code if its codewords form a $k$-dimensional linear subspace of $GF(q)^n$.

Let $dist(u,v)$ denote the Hamming distance between two words $u$ and $v$ in $Q^n$ (the latter will be referred to as an $n$-dimensional Hamming scheme). The distance of a word $v \in Q^n$ from a code $C$ is defined by

$$dist(v; C) = \min_{c \in C} dist(v,c),$$

and the covering radius $R$ of a code $C$ is defined by [9, p. 172]

$$R = \max_{v \in Q^n} dist(v; C).$$

It is easy to verify, that the covering radius and the minimum distance satisfy the following inequality:

$$R \geq \left\lfloor \frac{d}{2} \right\rfloor,$$

(1)

Definition. A code $C$ is called a minimum covering radius (in short, MCR) code, if it satisfies Eq. (1) with equality.

Example 1. The $[7,4,3]$ binary Hamming code $C_1$ whose parity-check matrix is given by

$$H_1 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

is an MCR code with $d = 3$ and $R = 1$. Since the minimum distance of $C_1$ is odd, it will be referred to as an odd MCR code.

\[ \left\lfloor x \right\rfloor \] denotes the largest integer not greater than $x$. 
The [8,4,4] extended binary Hamming code, $C_1^*$, obtained from $C_1$ by adding an overall parity bit in each codeword, is an even MCR code having $d = 4$ and $R = 2$.

Example 2. The linear binary code $C_2$, generated by the matrix

$$G_2 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

is an even MCR code with $d = 2$ and $R = 1$.

Consider the case of odd $d$, and let $t = \frac{d-1}{2}$. Let $S(u; r)$ denote the sphere of radius $r$ around a word $u \in Q^n$, that is,

$$S(u; r) = \{ v \in Q^n | dist(v,u) \leq r \} .$$

Also, denote by $E(u; r)$ the surface of $S(u; r)$, i.e., the set of words at distance $r$ from $u$. Since the minimum distance of the code, is $2t+1$, the spheres $S(c; t)$, $c \in C$, are pairwise disjoint. However, if $R = \left\lfloor \frac{d}{2} \right\rfloor = t$, those spheres cover the entire space $Q^n$. Hence, a code of odd minimum distance is MCR if and only if it is a perfect code [9, p. 19], i.e., if and only if it satisfies the sphere-packing bound

$$M \cdot \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq q^n$$

with equality. This observation confirms that the [7,4,3] binary Hamming code $C_1$ of Example 1 is indeed an odd MCR code.

Perfect codes (or, rather, odd MCR codes) have been widely discussed in the literature ([2, §2.8, §3.7], [5], [6], [9, ch. 6]). In particular, when $q$ is a power of a prime (in which case we may assume that $Q = GF(q)$), almost all perfect codes are known, as stated in the following theorems:

**Theorem 1.** [5], [7], [8], [10], [9, pp. 180-186]. Every $(n,M,d)$ perfect code (odd MCR code) with $d \neq 3$ over $GF(q)$ is equivalent \(^2\) to one of the following codes:

\(^2\) Two codes are said to be equivalent if one is obtained from the other by permuting the codeword coordinates or by permuting the alpha-
1) the \([n,1,n]\) repetition code over \(GF(2)\) for odd \(n\),

2) the \([23,12,7]\) binary Golay code,

3) the \([11,6,5]\) ternary Golay code,

or

4) the \([n,n,1]\) entire space \(GF(q)^n\).

Theorem 2. [9, p. 182], Every \((n,M,3)\) perfect code [odd MCR code] over \(GF(q)\) has the same

length, size and distance distribution as an \([n=q^m-1, k=n-m, 3]\) Hamming codes over \(GF(q)\) \((m \geq 2)\).

Hence, the linear perfect codes are fully characterized:

Corollary 1. Every linear \([n,k,d]\) perfect code over \(GF(q)\) is equivalent to one of the codes

specified in Theorem 1 or to a Hamming code over \(GF(q)\).

In this paper, we investigate the case of even \(d\). We introduce a family of codes which, like the perfect ones, satisfy a certain bound with equality. These codes are strongly related to perfect codes and since most of the results about the latter ones pertain to the case where \(q\) is a power of a prime, we too assume that \(Q = GF(q)\) (although the definitions and some of the theorems given below apply in general).

Definition. Two words \(u, v \in Q^n\) are said to be adjacent if \(\text{dist}(u,v) = 1\).

Definition. An \((n,M,d)\) code \(C\) over \(Q = GF(q)\) with \(d = 2\tau\) is called a tiling code if

(i) \(C\) is an even MCR code, i.e., \(R = \frac{d}{2}\),

and

(ii) for any two adjacent words \(u, v \in Q^n\) there exists a codeword \(c \in C\) such that \(u, v \in S(c; \tau)\).

It can be readily verified, that the extended binary Hamming code \(C_1^*\) of Example 1 is a tiling code.

This, however, is not true for \(C_2\) of Example 2, as there exists no \(c \in C_2\) whose sphere \(S(c; 1)\) contains
both $(1,1,1,0,0)$ and $(1,1,1,1,0)$.

In Section II we derive a sphere-tiling bound, which is the analogue, for codes of even minimum distances, of the sphere-packing bound. The sphere-tiling bound is satisfied with equality by a code $C$ if and only if the code $C$ is a tiling code. This is due to the fact, that the spheres $S(c; \tau)$ of a tiling code $C$ "tile" the entire scheme $Q^n$, that is, each $u \in Q^n$ is contained in at least one sphere, and if $u \in E(c; \tau)$ (i.e., $u$ is a surface point), then $u$ is a common point of exactly $\frac{n}{\tau}$ surfaces.

In Section III we refine the analogy between tiling codes and perfect codes. More specifically, we show, that an $(n,M,d)$ code $C$ of an even minimum distance $d$ over $Q$ is a tiling code if and only if the deletion of one of its coordinates results in an $(n-1,M,d-1)$ perfect code. Note that the existence of an $(n-1,M,d-1)$ perfect code does not necessarily imply the existence of an $(n,M,d)$ tiling code (as a matter of fact, in Section IV we show that there exist linear perfect codes with no corresponding linear tiling codes). However, the existence of an $(n-1,M,d-1)$ perfect code over $GF(2)$ does imply the existence of a corresponding $(n,M,d)$ tiling code, since the addition of a parity bit to a binary code of an odd minimum distance increases both the length of the code and its minimum distance by 1. The above results lead to the conclusion that, like their perfect counterparts, tiling codes are very scarce [1].

In Section IV we characterize several classes of tiling codes, concentrating mainly on linear ones. Given the complete set of linear perfect codes, we specify all classes of linear tiling codes. We show, that every linear tiling code over $GF(q)$ (as well as every nonlinear tiling code with $d>4$) is equivalent to one of the following codes:

1) the $[n,1,n]$ repetition code over $GF(2)$ for even $n$,
2) the $[24,12,8]$ extended binary Golay code,
3) the $[12,6,6]$ extended ternary Golay code,
4) the $[n,n-1,2]$ parity code over $GF(q)$,
5) the $[n=2^m,k=n-m-1,4]$ extended binary Hamming code for $m \geq 2$,
or
6) a $[q+2,q-1,4]$ maximum distance separable (MDS) code $^3$ [9, ch. 11] over $GF(q)$ when $q$ is even.

Technion - Computer Science Department - Technical Report CS0434 - 1986
An example of an MDS code is the so-called *triply-extended Reed-Solomon* code: let \( \alpha \) be a primitive element of \( GF(q) \) for even \( q \). It is well known that the code with the parity-check matrix

\[
H = \begin{bmatrix}
1 & 0 & 0 & 1 & 1 & \cdots & 1 \\
0 & 1 & 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\
0 & 0 & 1 & 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(q-2)}
\end{bmatrix}
\]

is a \([q+2, q-l, 4]\) MDS code. However, there are \([q+2, q-l, 4]\) MDS codes which are not equivalent to the triply-extended Reed-Solomon code, and which are not fully characterized \([4, \text{ch. 8}]\) yet. This family of codes is the only class of linear tiling codes which is not completely specified yet.

Note, that there are "less" linear tiling codes than linear perfect ones; it is due to the fact, that no linear Hamming code over \( GF(q) \), except for \( q = 2 \), or \( m = 2 \) when \( q \) is even, has a corresponding linear tiling code. This result is proved in Theorem 10.

II. THE SPHERE- TILING BOUND

Lemma 1. Let \( C \) be an \((n,M,d)\) code over \( Q = GF(q) \), where \( d = 2^\tau \), and let \( w \) be a word of \( Q^n \). Define the set \( W \) as follows:

\[
W = \{ c \in C | \text{dist}(w,c) = \tau \}.
\]

Then,

\[
|W| \leq \frac{n}{\tau}.
\]

Proof. If \(|W| \leq 1\) the lemma is trivial. Otherwise, let \( c_1, c_2 \in W \) be any two distinct codewords of \( C \). Then,

\[
\text{dist}(c_1,c_2) \geq 2\tau.
\]

\footnote{An \([n,k,d]\) code \( C \) is called maximum distance separable if \( d = n-k+1 \).}
By the triangle inequality, we have
\[ \text{dist}(c_1, c_2) \leq \text{dist}(c_1, w) + \text{dist}(w, c_2) = 2\tau. \]  
(3)

Hence,
\[ \text{dist}(c_1, c_2) = \text{dist}(c_1, w) + \text{dist}(c_2, w) = 2\tau, \]
which implies that the supports of $c_1 - w$ and of $c_2 - w$ must be disjoint. The lemma now follows immediately. $\square$

**Theorem 3.** (The sphere-tiling bound). *Let $C$ be an $(n, M, d)$ code over $Q = GF(q)$, where $d = 2\tau$. Then,

\[ M \cdot \left[ \sum_{i=0}^{\tau-1} \left( \begin{array}{c} \frac{n}{\tau} \end{array} \right) (q-1)^i + \frac{\tau}{n} \left( \begin{array}{c} \frac{n}{\tau} \end{array} \right) (q-1)^{\tau} \right] \leq q^n. \]  
(4)

Proof. In analogy with the proof of the sphere-packing bound, the volume of the union of the spheres $S(c; \tau-1)$ for all $c \in C$ equals to

\[ | \bigcup_{c \in C} S(c; \tau-1) | = M \cdot \sum_{i=0}^{\tau-1} \left( \begin{array}{c} \frac{n}{\tau} \end{array} \right) (q-1)^i. \]  
(5)

The sum of the areas of all the surfaces of radius $\tau$ surrounding the codewords of $C$ is given by

\[ M \cdot \left( \frac{n}{\tau} \right) (q-1)^{\tau}. \]

While a word on the surface of a sphere may be shared by a number of such surfaces, it follows from Lemma 1 that this number cannot exceed $\frac{n}{\tau}$. Hence, the area of the union of all surfaces is lower-bounded by

\[ | \bigcup_{c \in C} E(c; \tau) | \geq M \cdot \frac{\tau}{n} \cdot \left( \begin{array}{c} \frac{n}{\tau} \end{array} \right) (q-1)^{\tau}. \]  
(6)

The theorem follows by combining Eqs. (5) and (6). $\square$

*The support of a vector is the set of coordinates at which the vector elements are nonzero.*
Theorem 4. An \((n,M,d=2t)\) code \(C\) over \(Q = GF(q)\) is a tiling code if and only if it attains the sphere-tiling bound.

Proof. (i) Assume \(C\) is a tiling code. Then the distance of each \(v \in Q^n\) from \(C\) is \(\tau\) or less, and it remains to be shown, that each word at distance \(\tau\) from \(C\) is contained in exactly \(\frac{n}{\tau}\) surfaces \(E(c_i ; \tau), i = 1, 2, \ldots, \frac{n}{\tau}\). Assume, to the contrary, that a word \(v\) of distance \(\tau\) from \(C\) is contained in \(m\) surfaces, where \(0 < m < \frac{n}{\tau}\), and let \(W = \{ c_1, c_2, \ldots, c_m \} \subseteq C\) be the corresponding set of nearest codewords to \(v\) (all at distance \(\tau\) from \(v\)). Then there exists a coordinate, say the \(l\)-th one, at which all the members of \(W\) as well as \(v\) have the same value. Consider a word \(u\), which differs from \(v\) only at its \(l\)-th coordinate. Clearly, \(dist(u,v) = 1\), and

\[ u \not\in \bigcup_{i=1}^{m} S(c_i ; \tau). \]

Hence, there is no codeword in \(C\) whose surrounding sphere of radius \(\tau\) contains both \(u\) and \(v\), thus contradicting the definition of a tiling code.

(ii) Assume now that \(C\) satisfies the sphere-tiling bound with equality. First, this implies \(R = \tau\). Second, for every \(v \in Q^n\) at distance \(\tau - 1\) or less from \(C\), there exists a codeword \(c \in C\), whose surrounding sphere \(S(c ; \tau)\) contains \(v\) together with all the words adjacent to \(v\) in \(Q^n\). Hence, it remains to consider the case where \(dist(v ; C) = \tau\). By the sphere-tiling bound, \(v\) is contained in exactly \(\frac{n}{\tau}\) surfaces \(E(c_i ; \tau), i = 1, 2, \ldots, \frac{n}{\tau}\). Moreover, by the triangle inequality, the supports of \(c_i - v\) and \(c_j - v\) must be disjoint whenever \(i \neq j\). Hence, the union of the supports for \(c_i - v, i = 1, 2, \ldots, \frac{n}{\tau}\), covers all the \(n\) coordinates. Consequently, for each \(u\) adjacent to \(v\), there exists a codeword \(c_i \in C, 1 \leq i \leq \frac{n}{\tau}\), such that the support of \(c_i - v\) contains the coordinate in which \(u\) and \(v\) differ. This puts \(u\) at distance \(\tau\) or less from \(c_i\), making \(S(c_i ; \tau)\) a common sphere for both \(u\) and \(v\). \(\Box\)
III. THE CORRESPONDENCE BETWEEN TILING CODES AND PERFECT CODES

Definition. An \((n,M,d=2^r)\) code \(C\) over \(Q=GF(q)\) is called an even extension of an \((n-1,M,d-1)\) code \(C'\), if it is obtained from the latter by adjoining an extra coordinate to each codeword of \(C'\).

For example, the \([8,4,4]\) extended binary Hamming code \(C_1^*\) of Example 1 is an even extension of the \([7,4,3]\) binary Hamming code \(C_1\).

The following theorem establishes the correspondence between tiling codes and perfect codes:

**Theorem 5.** A given \((n,M,d=2^r)\) code \(C\) over \(Q=GF(q)\) is a tiling code if and only if it is an even extension of a perfect code.

**Proof.** Assume \(C\) is an \((n,M,d=2^r)\) tiling code. We show that the deletion of any one of its coordinates results in a perfect code \(C'\). By Theorem 4, \(C\) satisfies the sphere-tiling bound with equality. Thus, using the identities \(\sum_{i=0}^{n} \binom{n}{i} = q^n\) and \(\sum_{i=0}^{n} \binom{n}{i} = M\), we have:

\[
q^n = M \cdot \left[ \sum_{i=0}^{n-1} \binom{n}{i} (q-1)^i + \binom{n-1}{i-1} (q-1)^{i-1} \right]
\]

\[
= M \cdot \left[ 1 + \sum_{i=1}^{n-1} \binom{n-1}{i} (q-1)^i + \sum_{i=1}^{n-1} \binom{n-1}{i-1} (q-1)^{i-1} \right]
\]

\[
= M \cdot q \sum_{i=1}^{n-1} \binom{n-1}{i} (q-1)^i
\]

Dividing both sides by \(q\) yields

\[
M \cdot \sum_{i=0}^{\tau-1} \binom{n-1}{i} (q-1)^i = q^{n-1},
\]

which is satisfied by every \((n-1,M,d')\) code \(C'\), obtained from \(C\) by deleting any one of its coordinates.

Clearly, \(d' = 2(\tau-1) + 1 = d - 1\), and \(C'\) is a perfect code, by virtue of attaining the sphere-packing bound.
The "if" part of the theorem is obtained by reversing the steps of the "only if" part.

Note that Theorem 5 first assumes the existence of an \((n,M,d=2t)\) code and then specifies the necessary and sufficient condition for it to be a tiling code. The existence of an \((n-1,M,d-1)\) perfect code, does not in itself imply the existence of a tiling even extension thereof. In the next section, we show that there are linear perfect codes with no linear even extensions and, hence, no corresponding linear tiling codes.

The above remark does not apply to the binary \((q = 2)\) case. Indeed, if we add a parity bit to the codewords of a binary \((n-1,M,2t-1)\) code \(C\), an \((n,M,2t)\) code \(C\) is obtained. Therefore, in the binary case, there exists an \((n,M,d)\) tiling code if and only if there exists an \((n-1,M,d-1)\) perfect code ([3], [9, p. 27]). As it turns out, the binary case is exceptional in this respect.

According to Theorems 1 and 2, perfect codes are quite scarce over \(Q = GF(q)\). Due to Theorem 5, we conclude that tiling codes are even scarcer.

IV. CHARACTERIZATION OF CLASSES OF TILING CODES

Theorems 1 and 2 specify all perfect codes with \(d \geq 3\). Together with Theorem 5, we can determine all candidates for tiling codes with \(d > 4\):

Theorem 6. Every \((n,M,d)\) tiling code with \(d > 4\) over \(GF(q)\) is equivalent to one of the following codes:

1) the \([n,1,n]\) repetition code over \(GF(2)\) for even \(n\),
2) the \([24,12,8]\) extended binary Golay code,
   or
3) the \([12,6,6]\) extended ternary Golay code.

Proof. 1) There is only one possible equivalence class of even extensions to the \([n,1,n]\) binary code with odd \(n\), and this class contains the linear repetition code of even length. 2) It is well known [9, p. 646], that there exists only one equivalence class of \([24,2^{12},8]\) codes (not necessarily linear), containing...
the [24,12,8] extended binary Golay code. 3) The same holds for the extended ternary Golay code [9, p. 648]. □

The case of linear tiling codes with \( d=2 \) is covered by the following theorem:

Theorem 7. Every linear \([n, n-1,2]\) tiling code over GF(\( q \)) is equivalent to the parity code, having \( H = [1 \ 1 \ \cdots \ 1] \) as its parity-check matrix.

The proof is straightforward and, therefore, omitted. Note, however, that when \( q = p^r \), \( p \) a prime and \( r > 1 \), there are \((n, q^{n-1},2)\) codes over GF(\( q \)), \( n > 2 \), which are not equivalent to the parity code. Consider the alphabet \( Q = \{0, 1, 2, \cdots, q-1\} \) (\( q \geq 2 \) and not necessarily a power of a prime), and let \( \hat{C} \) be the \((n, q^{n-1},2)\) code consisting of all \( c = (c_1, c_2, \cdots, c_{n-1}, c_n) \in Q^n \) such that \( c_n = -\sum_{i=1}^{n-1} c_i \mod q \). We show in the Appendix that when \( n > 2 \) and \( q = p^r \) with \( r > 1 \), the resulting code \( \hat{C} \) is not equivalent to any linear code over GF(\( q \)).

It remains to examine the extensions of Hamming codes.

Lemma 2. All weights of the codewords of an \((n, M, 2\tau)\) binary tiling code have the same parity.

Proof. Let \( C \) be an \((n, M, 2\tau)\) binary tiling code containing the all-zero codeword \((0, 0, \cdots, 0)\). We show that each codeword of \( C \) has even weight. The lemma will follow immediately. Assume, to the contrary, that \( C \) contains a codeword of odd weight and let \( c_1 \in C \) have the least odd weight \( w > 2\tau \). Let \( v \) be a word of \( \{0, 1\}^n \) of weight \( w - \tau \) located on the surface \( E(c_1 ; \tau) \). Since \( v \) is a surface word, it is contained in exactly \( \frac{n}{\tau} \) surfaces \( E(c_i ; \tau) \), \( i = 1, 2, \cdots, \frac{n}{\tau} \). The weight of each of these \( c_i \)-s must be odd and, due to the minimality of \( w \), each must have weight \( w \). Furthermore, the support of each \( c_i \) contains that of \( v \) and the supports of \( c_i - v \) (which are of size \( \tau \)) are pairwise disjoint. This implies that \( v \) must be the all-zero word, thus leading to a contradiction. □

Theorem 8. Every \([n,k,4]\) linear tiling code over GF(2) is equivalent to one of the \([n=2^m, k=n-m-1,4]\) extended binary Hamming codes.
Proof. By Corollary 1, Theorem 5 and Lemma 2, all the \([n,k,4]\) linear binary tiling codes are obtained by adding an overall parity bit to one of the binary Hamming codes. \(\square\)

**Theorem 9.** Every \((n,M,4)\) tiling code over \(GF(2)\) has the same length, size and distance distribution as those of one of the \([n=2^m,k=n-m-1,4]\) extended binary Hamming codes \((m \geq 2)\).

Proof. Without loss of generality, we may assume, that such a tiling code \(C\) contains the all-zero codeword. By Theorem 5 and Lemma 2, \(C\) is an even extension of an \((n-1,M,3)\) binary perfect code (say, by adjoining the \(n\)-th coordinate), where the last coordinate in each codeword of \(C\) has the parity value of the original codeword. An application of Theorem 2 completes this proof. \(\square\)

As noted before, the binary case is exceptional in the context of linear even extensions of Hamming codes. As a matter of fact, when \(q > 2\), there exists only one class of linear \([n,k,4]\) tiling codes, namely, the class of the \([q+2,q-1,4]\) MDS codes with even \(q\), which are even extensions of the \([n=q^m-1,q-1,n-m,3]\) Hamming codes with \(m=2\). It is interesting to point out that these extension codes with even \(q\) are also a singular phenomenon among the MDS codes. In particular, there exist no \([q+2,q-1,4]\) MDS codes over \(GF(q)\) with odd \(q\), nor \([q+2,q-2,5]\) MDS codes over any finite field. The nonexistence of linear even extensions of Hamming codes for \(q > 2\) (except when \(m=2\) and \(q\) is even) is established in Theorem 10 below, which requires the following lemmas:

**Lemma 3.** [9, p. 33]. Let \(H\) be the parity-check matrix of an \([n,k,d]\) linear code \(C\). Then every \(d-1\) columns of \(H\) are linearly independent.

**Lemma 4.** [2, p. 49]. Let \(C\) be an \([n,k,d]\) linear code over \(GF(q)\), whose generator matrix does not contain an all-zero column. Then, each column of the \(q^k \times n\) matrix \(B\), whose rows are the codewords of \(C\), contains each element of \(GF(q)\) exactly \(q^{k-1}\) times.

Let \(\{A_i\}_{i=0}^n\) be the weight distribution of \(C\), i.e., \(A_i\) is the number of codewords of \(C\) having Hamming weight \(i\).
Lemma 5. Let $C$ be an $[n,k,d]$ linear code, whose generator matrix does not contain an all-zero column. Then the weight-distribution $\{A_i\}_{i=0}^{n}$ satisfies the following two equalities:

\[
\sum_{i=1}^{n} A_i = q^k - 1, \quad (7)
\]

and

\[
\sum_{i=1}^{n} i \cdot A_i = n \cdot q^{x-1}(q-1). \quad (8)
\]

Proof. Eq. (7) simply states that the weight distribution components add up to the number of code-words of $C$. Eq. (8) is obtained by counting the nonzero elements of the matrix $B$ both in row order and in column order. □

Lemma 6. [9, ch. 11]. There is no $[q+3,q,4]$ linear MDS code over $GF(q)$, and there is no $[q+2,q-1,4]$ MDS code over $GF(q)$ for odd $q$.

Theorem 10. The $[n=q^{m-1}/q-1,n'-m,3]$ Hamming code over $GF(q)$ does not have a linear even extension when $q > 2$ and $m > 2$. Furthermore, when $q$ is odd, there exists no such extension even if $m=2$.

Proof. We prove by induction on $m$ that there is no $[n,n-m-1,4]$ code $C$ over $GF(q)$ with $n = \frac{q^{m-1}}{q-1} + 1$ for the specified values of $q$ and $m$.

Induction base. The case of odd $q$ and $m=2$ is covered by Lemma 6. For the sake of clarity, we postpone the proof of the case of $q > 2$ and $m=3$ until after the induction step is dealt with.

Induction step (for all $q$). Assume, to the contrary, that there exists an $[n,n-m-1,4]$ code $C$ with $n = \frac{q^{m-1}}{q-1} + 1 = \sum_{i=0}^{m-1} q^i + 1$, and let $H$ be the $(m+1) \times n$ parity-check matrix of $C$. Let $d^\perp$ be the minimum distance of the dual code $C^\perp$ of $C$ (i.e., $C^\perp$ is the code generated by $H$). We may assume, without loss of generality, that $H$ is of the form
and deduce that \( d^L \leq q^{m-1} \). Otherwise, there must be two columns among the first \( d^L \) columns of \( H \) with identical values in each of the first \( m \) rows which, together with the last column of \( H \), form a linearly dependent triple of columns. By Lemma 3, this is clearly impossible as the minimum distance of \( C \) is 4.

Having established that \( d^L \leq q^{m-1} \), \( H \) may be rewritten as

\[
H = \begin{bmatrix}
1 & \cdots & 1 & 0 & \cdots & 0 & 0 \\
a_1 & \cdots & a_{d^L} & a_{d^L+1} & \cdots & a_{n-1} & 0 \\
\vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\vdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
\vdots & \cdots & \cdots & \cdots & \cdots & \cdots & 1
\end{bmatrix},
\]

where \( H_1 \) is an \( m \times n_1 \) matrix with \( n_1 = d^L \leq q^{m-1} \), and \( H_0 \) is an \( m \times n_0 \) matrix with \( n_0 = n - n_1 \geq \sum_{i=0}^{m-2} q^i + 1 \). Since every three columns of \( H_0 \) must be linearly independent, \( H_0 \) serves as a parity-check matrix for a linear \([n_0, n_0 - m_0 - 1, 4]\) code with \( m_0 \leq m - 1 \), contradicting the induction hypothesis.

We turn now to prove the induction base for even \( q \).

**Induction base (continued):** \( m = 3, q > 2 \). Assume, to the contrary, that there exists a linear \([n = q^2 + q + 2, n - 4, 4]\) code \( C \). Let \( H \) be the parity-check matrix of \( C \), and let \( C^\perp \) be the dual code of \( C \) with minimum distance \( d^L \). Our assumption implies the following claims:

**Claim (i):** \( d^L \geq q^2 \). Otherwise, referring to the form of \( H \) as given in Eq. (9), \( H_0 \) is a \( 3 \times n_0 \) matrix with \( n_0 > q + 2 \). Since every three columns of \( H_0 \) must be linearly independent, \( H_0 \) serves as a parity-check matrix of an MDS code of length greater than \( q + 2 \), thus contradicting Lemma 6.

**Claim (ii):** Let \( \{A_i^\perp\}_{i=0}^\infty \) be the weight distribution of \( C^\perp \). Then, \( A_i^\perp = 0 \) for \( q^2 < i < q^2 + q + 2 \). Otherwise, we may assume the following form for \( H \)}
where \( q^2 < w < q^2 + q + 2 \). This implies, that among the first \( w \) columns of \( H \) there exist two which may differ only in their last row which, in turn, implies the existence of three linearly dependent columns in \( H \).

Hence, \( d^\perp = q^2 \), and the only nonzero elements of the weight distribution of \( C^\perp \) are \( A_0^\perp \), \( A_2^\perp \) and, possibly, \( A_{n_2}^\perp \). By Lemma 5:

\[
A_{d^\perp} + A_{n_1}^\perp = q^4 - 1 ,
\]

and

\[
d^\perp A_{d^\perp} + n A_{n_1}^\perp = n \cdot q^3(q-1) .
\]

Substituting the values of \( d^\perp \) and \( n \) in the above equations and solving for \( A_{n_1}^\perp \) yields,

\[
A_{n_1}^\perp = \frac{q^2(q-1)^2}{q+2} .
\]

Hence, for \( q > 2 \), \( A_{n_1}^\perp > q-1 \), which implies that \( C^\perp \) contains at least two independent codewords, \( c_1 \) and \( c_2 \), both of weight \( n \). Without loss of generality, we may assume that \( c_1 = (1,1, \ldots, 1) \). Since \( c_2 \) is not a multiple of \( c_1 \) and for all \( a \in GF(q) \), \( a \cdot c_1 + c_2 \in C^\perp \), it follows that no element of \( GF(q) \) may appear in \( c_2 \) more than \( q+2 \) times, or else, \( 0 < \text{dist}(c_1, a \cdot c_1 + c_2) < q^2 \) for some \( a \in GF(q) \).

Therefore,

\[
n \leq \frac{(q+2)(q-1)}{q+2} = q^2 + q - 2 ,
\]

which provides the required contradiction.  \( \square \)
APPENDIX

Let $q = p^r$ for some prime $p$ and $r > 1$. Let $\hat{\mathcal{Q}}$ be the alphabet containing the $q$ integers \{0, 1, \ldots, q-1\}, and let $\hat{C}$ be the $(n, q^{n-1}, 2)$ code, $n > 2$, consisting of all $c = (c_1, c_2, \ldots, c_{n-1}, c_n) \in \hat{\mathcal{Q}}^n$ such that $c_n = -\sum_{i=0}^{n-1} c_i \mod q$. We claim that $\hat{C}$ is not equivalent to the linear $(n, n-1, 2)$ parity code $C$ over $GF(q)$. Assume, to the contrary, that the codes are equivalent. Then there exist $n$ one-to-one transformations $\phi_j : \hat{\mathcal{Q}} \to GF(q)$, $j = 1, 2, \ldots, n$, such that for all $c \in \hat{C}$, $\sum_{i=1}^n \phi_j(c_j) = 0$. Consider the $2p$ codewords of $\hat{C}$ defined by \{(0, 0, 0, \ldots, 0, q-i)\}_{i=1}^p$ and \{(1, 0, 0, \ldots, 0, q-i-1)\}_{i=1}^p$. Then, for their equivalents in $C$, we must have

$$\sum_{i=1}^p \left[ \phi_1(0) + \phi_2(i) + \sum_{j=3}^{n-1} \phi_j(0) + \phi_n(q-i) \right] = 0,$$

and

$$\sum_{i=1}^p \left[ \phi_1(1) + \phi_2(i) + \sum_{j=3}^{n-1} \phi_j(0) + \phi_n(q-1-i) \right] = 0.$$ 

Since $\sum_{i=1}^n a = 0$ for all $a \in GF(q)$, the difference between the above equations yields

$$\phi_n(q-p-1) - \phi_n(q-1) = 0.$$

This contradicts the 'one-to-one' property of $\phi_n$, since for $r > 1$, $-p \neq 0 \mod q$. 

Technion - Computer Science Department - Technical Report CS0434 - 1986
REFERENCES


