

NONEQUIVALENT q -ARY PERFECT CODES*

TUVI ETZION†

Abstract. We construct a set of q^{cn} nonequivalent q -ary perfect single error-correcting codes of length n over $GF(q)$ for sufficiently large n and a constant $c = \frac{1}{q} - \epsilon$. The construction is based on a small subcode A of the q -ary Hamming code of length n for which A and $q - 1$ of its cosets A_1, \dots, A_{q-1} cover the same subset V . We show a few isomorphic and nonisomorphic ways in which A can be chosen, and we prove the uniqueness of these ways to choose A .

Key words. Hamming codes, isomorphism, nonequivalent codes, perfect codes

AMS subject classifications. 94B, 05B

1. Introduction. Let F_q^n be a vector space of dimension n over $GF(q)$. A subset of F_q^n is a q -ary code of length n . Two codes $C_1, C_2 \subset F_q^n$, are said to be *isomorphic* if there exists a permutation π such that $C_2 = \{\pi(c) : c \in C_1\}$. They are said to be *equivalent* if there exists a vector v and a permutation π such that $C_2 = \{v + \pi(c) : c \in C_1\}$. The Hamming *distance* between vectors $u, v \in F_q^n$, denoted $d(u, v)$, is the number of coordinates in which u and v differ. Without loss of generality (w.l.o.g.), we shall assume, unless stated otherwise, that the all-zero vector is in C .

A code C of length n is *perfect* if for some integer $r \geq 0$ every $x \in F_q^n$ is within distance r from exactly one codeword of C . The study of perfect codes is one of the most fascinating subjects in coding theory. It is well known [3] that the only parameters for nontrivial perfect codes are those of the two Golay codes and the Hamming codes. The Hamming codes have length $n_m = \frac{q^m - 1}{q - 1}$, $m \geq 2$, and $r = 1$. They are single error-correcting codes, and henceforth when we use the words “perfect code” we will refer to codes with $r = 1$ and length n_m . The Hamming codes are the only linear codes with these parameters [3, p. 77]. For $q = 2$, constructions for nonequivalent perfect codes were presented by Phelps [5], [6], Etzion and Vardy [1], and others. For other q 's, constructions of nonlinear codes were presented by Schönheim [9], Lindström [2], and Mollard [4]. Nonequivalent perfect codes were generated by Phelps [7]. The construction for $q = 2$ given in Etzion and Vardy [1] has the advantage of obtaining the largest known set of nonequivalent perfect codes. It is also possible to obtain from the construction of [1] perfect codes with other properties as different ranks [1] and different kernels [8]. In this paper we generalize the construction of Etzion and Vardy [1] to any alphabet of size q , where q is a power of a prime.

In §2 we present a construction of a set of $q^{\frac{n_m - 1}{q} + 1 - \log_q(n_m(q-1)+1)}$ distinct perfect codes of length n . This set contains at least $q^{\frac{n_m - 1}{q} + 1 - \log_q(n_m(q-1)+1) - n_m(1 + \log_q n_m)}$ nonequivalent codes. This is the largest known set of nonequivalent perfect codes. The construction is based on a small subcode A of the q -ary Hamming code for which A and $q - 1$ of its cosets A_1, \dots, A_{q-1} cover the same subset V . This set A is important

* Received by the editors December 5, 1994; accepted for publication (in revised form) August 25, 1995. This research was supported in part by the EPSRC of the United Kingdom under grant GR/K38847.

† Computer Science Department, Royal Holloway, University of London, Egham, Surrey TW20 0EX, United Kingdom (etzion@cs.technion.ac.il). The author is on leave of absence from the Computer Science Department, Technion - Israel Institute of Technology, Haifa 32000, Israel.

in constructions of perfect codes with different ranks [1] and different kernels [8]. In §3 we show a few isomorphic and nonisomorphic ways in which this set A can be chosen, and we prove the uniqueness of the ways in which A is chosen.

2. Construction for nonequivalent perfect codes. The parity check matrix of the Hamming code of length $n_{m+1} = \frac{q^{m+1}-1}{q-1} = q^m + q^{m-1} + \dots + q + 1$, over $GF(q)$, consists of n_{m+1} pairwise linear independent column vectors of length $m + 1$ over $GF(q)$. We will take the n_{m+1} column vectors of the form $(0 \dots 0 1 x_1 \dots x_r)^T$ for all $0 \leq r \leq m$, where for $x_i \in GF(q)$, $1 \leq i \leq r$. Let α be a primitive element in $GF(q)$. Then the $2 \times (q + 1)$ parity check matrix of the Hamming code of length n_2 has the form

$$H_2 = \begin{bmatrix} 0 & 1 & 1 & 1 & \dots & 1 \\ 1 & 0 & \alpha^0 & \alpha^1 & \dots & \alpha^{q-2} \end{bmatrix},$$

and its $(q - 1) \times (q + 1)$ generator matrix has the form

$$G_2 = \begin{bmatrix} 1 & \alpha^{q-1} & -\alpha^{q-1} & 0 & \dots & 0 \\ 1 & \alpha^{q-2} & 0 & -\alpha^{q-2} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha & 0 & 0 & \dots & -\alpha \end{bmatrix} = \begin{bmatrix} 1 & & & & & \\ \vdots & \mathbf{X} & & & & \\ 1 & & & & & \end{bmatrix},$$

where \mathbf{X} is a $(q - 1) \times q$ matrix.

Assume the Hamming code of length $n_m = \frac{q^m-1}{q-1} = q^{m-1} + \dots + q + 1$ with $m \geq 2$ has the $m \times n_m$ parity check matrix H_m of the form

$$H_m = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix} \begin{bmatrix} S_1 & S_2 & \dots & S_{n_m-1} \end{bmatrix},$$

where the S_i 's are column vectors.

Also assume that the $(n_m - m) \times n_m$ generator matrix G_m has the form

$$G_m = \begin{bmatrix} 1 \\ \vdots \\ 1 \\ 1 \\ \vdots \\ 1 \\ \vdots \\ \vdots \\ \vdots \\ 1 \\ \vdots \\ 1 \\ \vdots \\ 1 \end{bmatrix} \begin{bmatrix} \mathbf{X} & \mathbf{0} & \dots & \dots & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{X} & \dots & \dots & \dots & \mathbf{0} \\ \vdots & \vdots & \vdots & \dots & \dots & \vdots \\ \vdots & \vdots & \vdots & \dots & \dots & \vdots \\ \vdots & \vdots & \vdots & \dots & \dots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \dots & \dots & \mathbf{X} \end{bmatrix},$$

$\overbrace{\hspace{15em}}^{\mathbf{F}}$

where F is a $t \times n_m$ matrix with $t = (n_m - m) - (q - 1) \frac{n_m - 1}{q} = n_{m-1} + 1 - m$.

Now, we generate the following $(m + 1) \times (n_m q + 1)$ parity check matrix H_{m+1} :

$$H_{m+1} = \begin{bmatrix} 0 & & & & & & & & & & & 0 & 0 & \cdots & 0 \\ \vdots & S_1 & S_1 & \cdots & S_1 & \cdots & S_{n_m-1} & S_{n_m-1} & \cdots & S_{n_m-1} & \vdots & \vdots & \cdots & \vdots \\ 0 & & & & & & & & & & 0 & 0 & \cdots & 0 \\ 0 & & & & & & & & & & 1 & 1 & \cdots & 1 \\ 1 & 0 & \alpha^0 & \cdots & \alpha^{q-2} & \cdots & 0 & \alpha^0 & \cdots & \alpha^{q-2} & 0 & \alpha^0 & \cdots & \alpha^{q-2} \end{bmatrix}$$

LEMMA 2.1. H_{m+1} is a parity check matrix of the Hamming code of length $n_m q + 1$.

Proof. Assume H_m has all the n column vectors of length m of the form $(0 \cdots 0 1 x_1 \cdots x_r)^T$ for all r , $0 \leq r \leq m - 1$, where $x_i \in GF(q)$, $1 \leq i \leq r$. By induction starting from the basis H_2 , we can easily prove that H_{m+1} is a parity check matrix of the Hamming code of length n_{m+1} . \square

Now, let G_{m+1} be the following $(n_m q - m) \times (n_m q + 1)$ matrix:

$$G_{m+1} = \left[\begin{array}{cccccccccccc} 1 & & & & & & & & & & & & & & & & & \\ \vdots & X & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & & & & & & & & 0 \\ 1 & & & & & & & & & & & & & & & & & \\ 1 & & & & & & & & & & & & & & & & & \\ \vdots & 0 & X & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & & & & & & & & 0 \\ 1 & & & & & & & & & & & & & & & & & \\ \vdots & \vdots & \vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & & & & & & & & \vdots \\ \vdots & \vdots & \vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & & & & & & & & \vdots \\ \vdots & \vdots & \vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & & & & & & & & \vdots \\ 1 & & & & & & & & & & & & & & & & & \\ \vdots & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & & & & & & & & X \\ 1 & & & & & & & & & & & & & & & & & \end{array} \right],$$

\hline
 F'

where F' is some $t' \times (n_m q + 1)$ matrix; $t' = n_m - m$.

LEMMA 2.2. The generator matrix of the Hamming code with parity check matrix H_{m+1} has the form of G_{m+1} .

Proof. From the form of H_2 and G_2 it follows that the matrix

$$\begin{bmatrix} 0 & S & S & S & \cdots & S \\ 1 & 0 & \alpha^0 & \alpha^1 & \cdots & \alpha^{q-2} \end{bmatrix},$$

for any given column vector S , is orthogonal to the matrix

$$\begin{bmatrix} 1 & & \\ \vdots & X & \\ 1 & & \end{bmatrix}.$$

Taking this fact into account the claim follows directly from the form of H_{m+1} and G_{m+1} . \square

We say that a vector v covers the set U if for any $u \in U$ we have $d(v, u) \leq 1$. A code C covers a set U if for every element $u \in U$ there exists a codeword $c \in C$ such that $d(c, u) \leq 1$. Let $C(G)$ denote the code generated by a generator matrix G .

LEMMA 2.3. *If G_{m+1}^1 is the matrix consisting of the first $n_m(q-1)$ rows of G_{m+1} , then $C(G_{m+1}^1)$ and $(\alpha^j:0 \cdots 0) + C(G_{m+1}^1)$, $j \geq 0$, cover the same subset of $F_q^{n_m q+1}$.*

Proof. Since $G_2 = G_2^1$ and $C(G_2)$ is a perfect code, it follows that its coset $(\alpha^j:0 \cdots 0) + C(G_2)$ is also a perfect code and thus $C(G_2^1)$ and $(\alpha^j:0 \cdots 0) + C(G_2^1)$ cover the same subset of F_q^{q+1} . Let $v = (\gamma:u_1, \dots, u_{n_m}) \in C(G_{m+1}^1)$, where $(\delta_i:u_i) \in C(G_2)$, $u_i \in F_q^q$, $\delta_i \in GF(q)$, and $\gamma = \sum_{i=1}^{n_m} \delta_i$. This is the form of codewords from $C(G_{m+1}^1)$ as follows from the form of G_2 and G_{m+1}^1 . We will show that every vector which is covered by v is also covered by a codeword of $(\alpha^j:0 \cdots 0) + C(G_{m+1}^1)$. Obviously, $v + (\beta:0 \cdots 0)$, $\beta \in GF(q)$, is covered by $v + (\alpha^j:0 \cdots 0) \in (\alpha^j:0 \cdots 0) + C(G_{m+1}^1)$. So, we only have to show that any word of the form $(\gamma:u_1 \cdots u_{i-1}u'_i u_{i+1} \cdots u_{n_m})$, where u_i and u'_i differ in exactly one position, is covered by a codeword of $(\alpha^j:0 \cdots 0) + C(G_{m+1}^1)$. We know that the vector $(\delta_i:u'_i)$ is covered by a codeword $v'_i \in (\alpha^j:0 \cdots 0) + C(G_2)$ because $(\alpha^j:0 \cdots 0) + C(G_2)$ is a perfect code. Since $(\delta_i:u_i) \in C(G_2)$ and since the minimum distance of $C(G_2)$ is 3, it follows that a vector of the form $(x:u'_i)$ is not in $C(G_2)$ and hence also not in $(\alpha^j:0 \cdots 0) + C(G_2)$. Therefore, $v'_i = (\delta_i:u''_i)$, where u''_i differs in exactly one position from u'_i and in exactly two positions from u_i . Since $(\delta_i:u''_i) \in (\alpha^j:0 \cdots 0) + C(G_2)$, it follows that $(\delta_i - \alpha^j:u''_i) \in C(G_2)$ and hence $(\gamma - \alpha^j:u_1 \cdots u_{i-1}u''_i u_{i+1} \cdots u_{n_m}) \in C(G_{m+1}^1)$. Hence, $(\gamma:u_1 \cdots u_{i-1}u'_i u_{i+1} \cdots u_{n_m})$ is covered by $(\gamma:u_1 \cdots u_{i-1}u''_i u_{i+1} \cdots u_{n_m}) \in (\alpha^j:0 \cdots 0) + C(G_{m+1}^1)$. Thus, every vector which is covered by $C(G_{m+1}^1)$ is also covered by $(\alpha^j:0 \cdots 0) + C(G_{m+1}^1)$ and since $C(G_{m+1}^1)$ and $(\alpha^j:0 \cdots 0) + C(G_{m+1}^1)$ have the same size the lemma follows. \square

Now, we can write G_m as

$$G_m = \begin{bmatrix} G_m^1 \\ F \end{bmatrix}, \text{ where } F = \begin{bmatrix} f_1 \\ \vdots \\ f_t \end{bmatrix},$$

where f_i is a $1 \times n$ matrix. Let c_j , $1 \leq j \leq q^t$, be the q^t codewords formed from F . By Lemma 2.3 we have that $c_j + C(G_m^1)$ and $(\alpha^j:0 \cdots 0) + c_j + C(G_m^1)$ cover the same subset of $F_q^{n_m}$.

LEMMA 2.4. *Given the vector $(g_1, g_2, \dots, g_{q^t})$, $g_i \in GF(q)$, $1 \leq i \leq q^t$, the code*

$$C = \bigcup_{i=1}^{q^t} ((g_i:0 \cdots 0) + c_i + C(G_m^1))$$

forms a q -ary perfect code.

Proof. If $g_i = 0$ for all i , then C is the Hamming code. The lemma now follows from the fact that $c_i + C(G_m^1)$ and $(g_i:0 \cdots 0) + c_i + C(G_m^1)$ cover the same subset of $F_q^{n_m}$. \square

Let $\Omega(n_m)$ be the set of perfect codes constructed in Lemma 2.4. Obviously $|\Omega(n_m)| = q^{q^t} = q^{q^{n_m-1}+1-m} = q^{q^{\frac{n_m-1}{q}+1-\log_q(n_m(q-1)+1)}}$. Given a perfect code C of length n_m , there are at most $q^{n_m} n_m! \leq q^{n_m} q^{n_m \cdot \log_q n_m} = q^{n_m(1+\log_q n_m)}$ different perfect codes equivalent to C . Hence we have Theorem 2.5.

THEOREM 2.5. $\Omega(n_m)$ contains at least $q^{q^{\frac{n_m-1}{q}+1-\log_q(n_m(q-1)+1)}-n_m(1+\log_q n_m)}$ nonequivalent perfect codes.

A more precise enumeration will slightly improve the result of Theorem 2.5. Finally, we would like to mention that given a perfect code C one might permute symbols independently in each position to obtain another perfect code. If we consider these perfect codes as equivalent we will have that there are at most $q^{n_m} n_m! (q!)^n$ different perfect codes equivalent to C . But, this will hardly influence the result of Theorem 2.5.

3. Splitting submatrices of the Hamming code. In Lemma 2.3 we have proved that $C(G_{m+1}^1)$ and $(\alpha^j:0 \cdots 0) + C(G_{m+1}^1)$, $j \geq 0$, cover the same subset of $F_q^{n_m q+1}$. The following question is of interest and importance. For a given i , $2 \leq i \leq n_m q+1$, does there exist an $n_m(q-1) \times (n_m q+1)$ submatrix G_{m+1}^i of G_{m+1} such that $C(G_{m+1}^i)$ and $\alpha^j e_i + C(G_{m+1}^i)$, $j \geq 0$, where $e_i = (0 \cdots 010 \cdots 0)$ with the 1 in position i , cover the same subset of $F_q^{n_m q+1}$? For $q = 2$ these submatrices exist as proved in [1]. These subcodes together with $C(G_{m+1}^1)$ were used in [1] to construct codes with various ranks and in [8] to construct codes with various kernels. This submatrix, G_{m+1}^i , $1 \leq i \leq n_{m+1}$, will be called a *splitting submatrix* of G_{m+1} and these submatrices are the subject of this section.

In this section we will prove that for each i , $1 \leq i \leq n_{m+1}$, a splitting submatrix G_{m+1}^i of G_{m+1} exists. We will also prove the uniqueness of these submatrices. In order to simplify the understanding of the construction for G_{m+1}^i we will permute the columns of the code such that column i will become the first column.

We start by considering the Hamming code of length $q+1$. As shown in §2, a parity check matrix of the code H_2 has the form

$$H_2 = \begin{bmatrix} 0 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 0 & \alpha^0 & \alpha^1 & \cdots & \alpha^{q-2} \end{bmatrix},$$

the generator matrix of the code has the form

$$\begin{bmatrix} \alpha^0 - 0 & 1 & -1 & 0 & \cdots & 0 & 0 \\ \alpha^1 - \alpha^0 & 0 & 1 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha^{q-2} - \alpha^{q-3} & 0 & 0 & 0 & \cdots & 1 & -1 \end{bmatrix},$$

and from this matrix we can immediately compute

$$G_2 = \begin{bmatrix} 1 & & \\ \vdots & X & \\ 1 & & \end{bmatrix}$$

as given is §2.

If $q = p$ then we can take instead of H_2 the check matrix

$$\begin{bmatrix} 0 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & 2 & \cdots & p-1 \end{bmatrix},$$

and its generator matrix has the form

$$\begin{bmatrix} 1 & 1 & -1 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 1 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & 0 & 0 & \cdots & 1 & -1 \end{bmatrix}.$$

For a given $\beta \in GF(q)$, if the parity check matrix has the column $\binom{1}{\beta}$ as the first column then we take the parity check matrix

$$H_2^* = \begin{bmatrix} 1 & 0 & 1 & 1 & \dots & 1 \\ \beta & 1 & \beta + \alpha^0 & \beta + \alpha^1 & \dots & \beta + \alpha^{q-2} \end{bmatrix},$$

and its generator matrix is

$$G_2^* = \begin{bmatrix} 1 & \alpha^0 & -1 & 0 & \dots & 0 \\ 1 & \alpha^1 & 0 & -1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{q-2} & 0 & 0 & \dots & -1 \end{bmatrix} = \begin{bmatrix} 1 & & & & & \\ \vdots & & & & & \\ 1 & & & & & \end{bmatrix} \begin{matrix} \\ \\ Y \\ \\ \end{matrix},$$

where Y is a $(q-1) \times q$ matrix.

The proof that H_2^* is a parity check matrix of the Hamming code is based on the following simple lemma.

LEMMA 3.1. *If β is an element in $GF(q)$ then the set of elements $\{\beta + \alpha^i : 0 \leq i \leq q-2\}$ consists of all the elements of $GF(q)$.*

We will make extensive use of this lemma in our constructions to prove that the parity check matrix of the codes, which we will construct, has all the columns of length $m+1$ and the form $(0 \dots 01x_1 \dots x_r)^T$ for all $r, 0 \leq r \leq m$, where $x_i \in GF(q), 1 \leq i \leq r$.

Now, we want to form the Hamming code of length n_{m+1} , which has as the first column in the parity check matrix the column vector of length $m+1, (0 \dots 01a_1 \dots a_r)^T$ for some $r, 0 \leq r \leq m$, and some a_i 's, $a_i \in GF(q), 1 \leq i \leq r$. We start with the parity check matrix H_{m+1-r} and the splitting submatrix G_{m+1-r}^1 given in §2. For $r = m$ we take $H_1 = [1]$ and G_1^1 is an empty matrix. Now, let $H_{m+1-r}^* = H_{m+1-r}$ and $G_{m+1-r}^* = G_{m+1-r}^1$. Assume we have constructed the $i \times n_i$ parity check matrix $H_i^*, i \geq m+1-r$, where $S = (0 \dots 01a_1 \dots a_{i-m-1+r})^T$ is the first column of H_i^* , and the $(q^{i-1} - 1) \times n_i$ splitting submatrix G_i^* which is a submatrix of the generator matrix of the Hamming code with the parity check matrix H_i^* . Assume further that G_i^* has the form

$$G_i^* = \begin{bmatrix} 1 & & & & & & & \\ \vdots & Z_1 & \mathbf{0} & \dots & \dots & \dots & \mathbf{0} & \\ 1 & & & & & & & \\ 1 & & & & & & & \\ \vdots & \mathbf{0} & Z_2 & \dots & \dots & \dots & \mathbf{0} & \\ 1 & & & & & & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ 1 & & & & & & & \\ \vdots & \mathbf{0} & \mathbf{0} & \dots & \dots & \dots & Z_{n_{i-1}} & \\ 1 & & & & & & & \end{bmatrix},$$

where Z_i is either the $(q-1) \times q$ matrix X given in §2 or the $(q-1) \times q$ matrix Y given in this section. W.l.o.g. we will further assume that there exists an integer l ,

$0 \leq l \leq n_{i-1}$, such that for each j , $1 \leq j \leq l$, $\mathbf{Z}_j = \mathbf{X}$, and for each j , $l+1 \leq j \leq n_{i-1}$, $\mathbf{Z}_j = \mathbf{Y}$. Now, assume H_i^* has the form

$$H_i^* = \left[\begin{array}{cccc} S & T_1 & T_2 & \cdots & T_{n_{i-1}} \end{array} \right],$$

where T_j , $1 \leq j \leq n_{i-1}$ is an $i \times q$ matrix.

We distinguish between two cases.

Case 1. If $a_{i-m+r} = 0$, we generate the following $(i + 1) \times n_{i+1}$ parity check matrix H_{i+1}^* :

$$H_{i+1}^* = \left[\begin{array}{cccccccc} S & \cdots & T_j & T_j & \cdots & T_j & & \\ 0 & \cdots & 0 \cdot L & \alpha^0 \cdot L & \cdots & \alpha^{q-2} \cdot L & & \\ & & & & & & 0 & \\ \cdots & T_k & T_k & \cdots & T_k & \cdots & \vdots & S & S & \cdots & S \\ & & & & & & 0 & & & & \\ \cdots & 0 \cdot K & \alpha^0 \cdot K & \cdots & \alpha^{q-2} \cdot K & \cdots & 1 & \alpha^0 & \alpha^1 & \cdots & \alpha^{q-2} \end{array} \right],$$

where $1 \leq j \leq l$, $l + 1 \leq k \leq n_{i-1}$, L is an $1 \times q$ matrix of the form $L = [1 \cdots 1]$, and K is a $1 \times q$ matrix of the form $K = [\alpha^0 \alpha^0 \alpha^1 \cdots \alpha^{q-2}]$.

Case 2. If $a_{i-m+r} = \alpha^c$, we generate the following $(i + 1) \times n_{i+1}$ parity check matrix H_{i+1}^* :

$$H_{i+1}^* = \left[\begin{array}{cccccccc} S & \cdots & T_j & T_j & \cdots & T_j & \cdots & T_k & T_k \\ \alpha^c & \cdots & M + 0 & M + \alpha^0 & \cdots & M + \alpha^{q-2} & \cdots & N + 0 \cdot K & N + \alpha^0 \cdot K \\ & & & & & & & & & & \\ \cdots & & T_k & \cdots & \vdots & S & S & \cdots & S \\ & & & & & & 0 & & & & \\ \cdots & N + \alpha^{q-2} \cdot K & \cdots & 1 & \alpha^c + \alpha^0 & \alpha^c + \alpha^1 & \cdots & \alpha^c + \alpha^{q-2} \end{array} \right],$$

where $1 \leq j \leq l$, $l + 1 \leq k \leq n_{i-1}$, M is an $1 \times q$ matrix of the form $M = [0 \alpha^c \alpha^{c+1} \cdots \alpha^{c+q-2}]$, and N is a $1 \times q$ matrix of the form $N = [0 \alpha^c \cdots \alpha^c]$.

LEMMA 3.2. H_{i+1}^* is a parity check matrix for the Hamming code.

Proof. This is an immediate consequence from the fact that H_i^* is a parity check matrix of the Hamming code, Lemma 3.1, and the observation that in the four $q \times q$ matrices,

$$\left[\begin{array}{c} 0 \cdot L \\ \alpha^0 \cdot L \\ \vdots \\ \alpha^{q-2} \cdot L \end{array} \right], \left[\begin{array}{c} 0 \cdot K \\ \alpha^0 \cdot K \\ \vdots \\ \alpha^{q-2} \cdot K \end{array} \right], \left[\begin{array}{c} M + 0 \\ M + \alpha^0 \\ \vdots \\ M + \alpha^{q-2} \end{array} \right], \text{ and } \left[\begin{array}{c} N + 0 \cdot K \\ N + \alpha^0 \cdot K \\ \vdots \\ N + \alpha^{q-2} \cdot K \end{array} \right],$$

each column is a permutation of the elements of $GF(q)$. \square

$$(4) \quad (1 : \beta, \beta\alpha^0 + 1, \dots, \beta\alpha^{q-2} + 1), \quad \beta \in GF(q).$$

For a row $v = (\gamma : u_1 u_2 \dots u_r)$, $\gamma \in GF(q)$, $u_i \in F_q^q$, $1 \leq i \leq r$, of the Hamming code, we say that $(\gamma : u_i)$ is a subrow of v for $1 \leq i \leq r$. Now, assume that we are constructing the parity check matrix H of the Hamming code of length n_{m+1} which have as a first column in the parity check matrix the column vector of length $m + 1$, $S = (0 \dots 0 1 a_1 \dots a_r)^T = (s_1 \dots s_{m+1})^T$ for some r , $0 \leq r \leq m$, and some a_i 's, $a_i \in GF(q)$, $1 \leq i \leq r$. Now, we distinguish between two cases.

Case 1. $s_1 = 1$. Since the first row of H consists only of 0's and 1's, it follows that only subrows of type (4) with $\beta = 0$ appear in the first row of H and hence only

$$G = \begin{bmatrix} 1 \\ \vdots \\ 1 \\ 1 \\ \vdots \\ 1 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ 1 \\ \vdots \\ 1 \end{bmatrix} \begin{bmatrix} Y & 0 & \dots & \dots & \dots & 0 \\ 0 & Y & \dots & \dots & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & \dots & Y \end{bmatrix}$$

can be a splitting submatrix of the generator matrix of the code.

Case 2. $s_1 = 0$. All the 1's in the first row of H must participate in subrows of type (1). This implies that we can write any splitting submatrix of the code as

$$G = \begin{bmatrix} 1 \\ \vdots \\ 1 \\ 1 \\ \vdots \\ 1 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ 1 \\ \vdots \\ 1 \end{bmatrix} \begin{bmatrix} Z_1 & 0 & \dots & \dots & \dots & 0 \\ 0 & Z_2 & \dots & \dots & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & \dots & Z_{n_m} \end{bmatrix},$$

where $Z_i = X$, $1 \leq i \leq q^{m-1}$, and H has the form

$$H = \begin{bmatrix} 0 & 1 & \cdots & 1 & 0 & \cdots & 0 \\ s_2 & & & & & & \\ \vdots & & \tilde{H}_1 & & \tilde{H}_2 & & \\ s_{m+1} & & & & & & \end{bmatrix}.$$

The matrix

$$\tilde{H} = \begin{bmatrix} s_2 & & \\ \vdots & & \tilde{H}_2 \\ s_{m+1} & & \end{bmatrix}$$

is the parity check matrix of the Hamming code of length n_m , with a splitting submatrix

$$\tilde{G} = \begin{bmatrix} 1 & & & & & & \\ \vdots & Z_{q^{m-1}+1} & 0 & \cdots & \cdots & \cdots & 0 \\ 1 & & & & & & \\ 1 & & & & & & \\ \vdots & 0 & Z_{q^{m-1}+2} & \cdots & \cdots & \cdots & 0 \\ 1 & & & & & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & & & & & & \\ \vdots & 0 & 0 & \cdots & \cdots & \cdots & Z_{n_m} \\ 1 & & & & & & \end{bmatrix}.$$

We proceed to examine \tilde{H} and \tilde{G} inductively in the same manner until we reach $s_j = 1$, $j = m + 1 - r$, using Cases 1 and 2. This process and the constructions of §2 and this section lead to Theorem 3.5.

THEOREM 3.5. *Given the parity check matrix*

$$H_{m+1}^* = \begin{bmatrix} S & H' \end{bmatrix}$$

of the Hamming code, then by ordering the columns of H' we can obtain the unique splitting submatrix of the generator matrix of the code. This unique splitting submatrix G_{m+1}^ has the form*

$$G_{m+1}^* = \begin{bmatrix} 1 & & & & & & & \\ \vdots & Z_1 & 0 & \dots & \dots & \dots & 0 & \\ 1 & & & & & & & \\ 1 & & & & & & & \\ \vdots & 0 & Z_2 & \dots & \dots & \dots & 0 & \\ 1 & & & & & & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ 1 & & & & & & & \\ \vdots & 0 & 0 & \dots & \dots & \dots & Z_{n_m} & \\ 1 & & & & & & & \end{bmatrix},$$

where $Z_i = X$ for $1 \leq i \leq l$ and $Z_i = Y$ for $l + 1 \leq i \leq n_m$, $l = \sum_{j=r}^{m-1} q^j$.

Finally, we will mention that the intersection between $C(G_{m+1}^{i_1})$ and $C(G_{m+1}^{i_2})$ for $i_1 \neq i_2$ is not empty since the zero codeword belongs to both of them. Also, $C(G_{m+1}^{i_1}) \neq C(G_{m+1}^{i_2})$ and the proof is done by a careful analysis of the codewords of weight 3 in the codes. But finding $C(G_{m+1}^{i_1}) \cap C(G_{m+1}^{i_2})$ is not easy, except for the case $q = 2$ which was dealt with in [1].

Acknowledgment. The author would like to thank Alexander Vardy for his constructive comments.

REFERENCES

- [1] T. ETZION AND A. VARDY, *Perfect codes: Constructions, properties and enumeration*, IEEE Trans. Inform. Theory, 40 (1994), pp. 754–763.
- [2] B. LINDSTRÖM, *On group and non-group perfect codes in q symbols*, Math. Scand., 25 (1969), pp. 149–158.
- [3] F. J. MACWILLIAMS AND N. J. A. SLOANE, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, 1977.
- [4] M. MOLLARD, *A generalized parity function and its use in the construction of perfect codes*, SIAM J. Alg. Disc. Meth., 7 (1986), pp. 113–115.
- [5] K. T. PHELPS, *A combinatorial construction of perfect codes*, SIAM J. Alg. Disc. Meth., 4 (1983), pp. 398–403.
- [6] ———, *A general product construction for error-correcting codes*, SIAM J. Alg. Disc. Meth., 5 (1984), pp. 224–228.
- [7] ———, *A product construction for perfect codes over arbitrary alphabets*, IEEE Trans. Inform. Theory, 30 (1984), pp. 769–771.
- [8] K. T. PHELPS AND M. LEVAN, *Kernels of nonlinear hamming codes*, Des. Codes Cryptogr., 6 (1995), pp. 247–257.
- [9] J. SCHÖNHEIM, *On linear and nonlinear single-error-correcting q -ary perfect codes*, Inform. and Control, 12 (1968), pp. 23–26.