JOURNAL OF COMBINATORIAL THEORY, Series A **80**, 247–256 (1997)
ARTICLE NO. TA972805

Intersection of Isomorphic Linear Codes

Eli Bar-Yahalom and Tuvi Etzion

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

Communicated by the Managing Editors

Received November 8, 1996

Given an (n, k) linear code $\mathscr{C}$ over GF(q), the intersection of $\mathscr{C}$ with a code $\pi(\mathscr{C})$, where $\pi \in S_n$, is an (n, k_1) code, where $\max\{0, 2k-n\} \leqslant k_1 \leqslant k$. The intersection problem is to determine which integers in this range are attainable for a given code $\mathscr{C}$. We show that, depending on the structure of the generator matrix of the code, some of the values in this range are attainable. As a consequence we give a complete solution to the intersection problem for most of the interesting linear codes, e.g. cyclic codes, Reed–Muller codes, and most MDS codes. © 1997 Academic Press

1. INTRODUCTION

Let $\mathbf{F}_q^n$ be a vector space of dimension n over GF(q). A linear subspace of dimension k of $\mathbf{F}_q^n$ is a linear code of length n and dimension k over GF(q). An (n, k) code is a linear code of length n and dimension k. Two (n, k) codes $\mathscr{C}_1, \mathscr{C}_2 \subset \mathbf{F}_q^n$ are said to be *isomorphic* if there exists a permutation $\pi \in S_n$, such that $\mathscr{C}_2 = \pi(\mathscr{C}_1) = \{\pi(c): c \in \mathscr{C}_1\}$.

In this paper we consider the problem of finding the possible sizes of intersection between isomorphic linear codes. For a code $\mathscr{C} \subset \mathbf{F}_q^n$ and a permutation $\pi \in S_n$, $\mathscr{C}^\pi$ denotes the intersection $\mathscr{C} \cap \pi(\mathscr{C})$. If $\mathscr{C}$ is an (n, k) code then clearly $\mathscr{C}^\pi$ is an (n, k_1) code for $l \leqslant k_1 \leqslant k$, where $l = \max\{0, n-2r\}$ and $r = n-k$ is the *redundancy* of $\mathscr{C}$. Given two (n, k) codes $\mathscr{C}_1$ and $\mathscr{C}_2$ over GF(q), the *intersection number* of $\mathscr{C}_1$ and $\mathscr{C}_2$ is defined as $\eta(\mathscr{C}_1, \mathscr{C}_2) = \log_q |\mathscr{C}_1 \cap \mathscr{C}_2|$. For a given (n, k) code $\mathscr{C}$, the *intersection problem* is to determine which values in the range between l and k are attainable as intersection numbers of $\mathscr{C}$ and its isomorphic codes; these integers are called the *intersection numbers* of $\mathscr{C}$. It was shown in [1] that for the binary $(2^m-1, 2^m-m-1)$ Hamming code all the values in this range are attainable, by considering the dimension of the matrix

$$H = \begin{bmatrix} H_1 \\ \hline H_2 \end{bmatrix},$$

0097-3165/97 $25.00

which is the parity check matrix of the intersection between $\mathscr{C}_1$ and $\mathscr{C}_2$, where H_i, $i=1, 2$, is the parity check matrix of $\mathscr{C}_i$.

In this paper we will use a different approach which enables us to give a complete solution to the intersection problem for most interesting codes, e.g., cyclic codes, Reed–Muller codes, and most MDS codes. This approach is based on a partition of the columns of the generator matrix of the code into two sets $I(\mathscr{C})$ and $R(\mathscr{C})$, where $I(\mathscr{C})$ is the *information set* which consists of k linearly independent columns, and $R(\mathscr{C})$ is the *redundant set* which consists of $n-k$ columns, among which at most t are linearly independent. We will choose a partition in which t gets its maximum value. A code with such a partition is called a *t-independent redundancy* (*t-IR*) *code*, and an *independent redundancy* (*IR*) *code* if $t=r$.

This partition with an additional enumeration method will enable us to show which integers between $n-r-t+1$ and k are intersection numbers of $\mathscr{C}$. If an additional condition holds, we show that $n-r-t$ is also an intersection number. In Section 2 we will present the necessary definitions and the enumeration technique. In Section 3 we will apply the method to the classes of codes mentioned before.

2. THE ENUMERATION METHOD

As said above, the approach for finding intersection numbers is based on the structure of the generator matrix of the code. If $\mathscr{C}$ is an (n, k) t-IR code, for which $t \leqslant k$, then the set of t linearly independent columns in $R(\mathscr{C})$ can be extended with $k-t$ columns from $I(\mathscr{C})$ to obtain a set of k linearly independent columns. This set of k linearly independent columns is called a *free set*; we will use a definite free set in every instance, and refer to it as "the" free set without abuse of terminology. The first enumeration lemma is well known and easily verified:

LEMMA 1. *If $\mathscr{C}$ is an (n, k) code and T is a set of linearly independent columns in its generator matrix, $|T|=t$, then in $\mathscr{C}$ each t-tuple appears in the columns of T exactly in $|C|/q^t$ codewords.*

DEFINITION 1. Let $\pi \in S_n$.

1. A decomposition of π into non-intersecting cycles, of length greater than 1, will be called *canonical*.

2. We shall use the following notation for a canonical decomposition:

$$\pi = \underbrace{(v^2_{1,1}v^2_{1,2})(v^2_{2,1}v^2_{2,2})\cdots(v^2_{k_2,1}v^2_{k_2,2})}_{\text{transpositions (2-cycles)}}\underbrace{(v^3_{1,1}v^3_{1,2}v^3_{1,3})(v^3_{2,1}v^3_{2,2}v^3_{2,3})\cdots(v^3_{k_3,1}v^3_{k_3,2}v^3_{k_3,3})}_{\text{3-cycles}}\cdots$$

where k_j denotes the number of j-cycles in the decomposition of π.

3. The number of cycles will be denoted by $\kappa(\pi)$.

4. For a cycle $\theta = (v^l_{p,1}v^l_{p,2}\cdots v^l_{p,l})$ of length l in π, l will be denoted by $\lambda(\theta)$. The sum of all lengths of the cycles in π will be denoted by $\lambda(\pi)$.

5. With respect to an (n, k) code $\mathscr{C}$, π will be called *free* if all the columns it permutes belong to the free set of $\mathscr{C}$.

Next, we are going to state a necessary and sufficient condition for a codeword of $\mathscr{C}$ to be in $\mathscr{C}^\pi$ for a given permutation π.

DEFINITION 2. For $h \in \mathscr{C}$, $(I - \Pi)h$ (where Π is the permutation matrix which represents π) will be called the π-*index* of h and denoted for short by h_π. Given an index x, a word h such that $x = h_\pi$ will be said to be *attached* to x.

LEMMA 2. If $\mathscr{C}$ is a linear code, $h \in \mathscr{C}$ and $\pi \in S_n$, then $\pi(h) \in \mathscr{C}^\pi$ if and only if $h_\pi \in \mathscr{C}$.

Proof.

$$(I - \Pi)h \in \mathscr{C} \Leftrightarrow h - \pi(h) \in \mathscr{C} \Leftrightarrow \pi(h) \in \mathscr{C} \Leftrightarrow \pi(h) \in \mathscr{C}^\pi. \quad \blacksquare$$

Remark. It may be of use to have an intuition about how h_π actually looks: let $h = (h_1, h_2, ..., h_n)$ be a word in $\mathbf{F}_q^n$, and $\pi \in S_n$. For each cycle $(v^l_{p,1}v^l_{p,2}\cdots v^l_{p,l})$ in the canonical decomposition of π define:

$$\begin{aligned}
x_{v^l_{p,2}} &= h_{v^l_{p,1}} - h_{v^l_{p,2}} \\
x_{v^l_{p,3}} &= h_{v^l_{p,2}} - h_{v^l_{p,3}} \\
&\cdots \\
x_{v^l_{p,l}} &= h_{v^l_{p,l-1}} - h_{v^l_{p,l}} \\
x_{v^l_{p,1}} &= h_{v^l_{p,l}} - h_{v^l_{p,1}}
\end{aligned}$$

For all indices i, $1 \leqslant i \leqslant n$, not used above, define $x_i = 0$. Then

$$h_\pi = (x_1, x_2, ..., x_n).$$

Let $h=(h_1, h_2, ..., h_n)\in \mathbf{F}_q^n$ and $J=\{i_1, i_2, ..., i_j\}\subseteq\{1, 2, ..., n\}$. The *projection* $h|_J$ is defined by $h|_J=(h_{i_1}, h_{i_2}, ..., h_{i_j})$, where $i_s<i_{s+1}$, $1\leqslant s\leqslant j-1$. For a permutation $\pi\in S_n$, $h|_\pi$ is a vector of length $\lambda(\pi)$.

THEOREM 1. *Let $\pi\in S_n$ be a free permutation with respect to an (n, k) code $\mathscr{C}$. Then*:

1. *The set of all indices X_π (i.e., the set of all vectors which are indices to at least one word in $\mathbf{F}_q^n$) is the set of all vectors $x\in\mathbf{F}_q^n$ which satisfy*:

   (a) *For every cycle $(v_{p,1}^l v_{p,2}^l\cdots v_{p,l}^l)$ in π, $\sum_{i=1}^l x_{v_{p,i}^l}=0$.*

   (b) *For every s which is not a $v_{e,j}^i$ for any i, e, j, $x_s=0$.*

2. *Every word is attached to one index only, and every index in $\mathscr{C}\cap X_\pi$ has exactly $q^{k-\lambda(\pi)+\kappa(\pi)}$ codewords attached to it.*

Proof. (1) First we prove that all indices satisfy these properties. If we sum the equations from Definition 2, we get

$$\sum_{i=1}^{l} x_{v_{p,i}^l}=\sum_{i=1}^{l-1}(h_{v_{p,i}^l}-h_{v_{p,i+1}^l})+h_{v_{p,l}^l}-h_{v_{p,1}^l}=\sum_{i=1}^{l} h_{v_{p,i}^l}-\sum_{i=1}^{l} h_{v_{p,i}^l}=0.$$

Property 1(b) follows immediately from Definition 2.

On the contrary, let x be a vector which satisfies 1(a) and 1(b); we shall show that x is an index by constructing a word h such that $x=h_\pi$. The values of h_s, for s which is not a $v_{e,j}^i$, may be chosen arbitrarily. For a cycle $\theta=(v_{p,1}^l v_{p,2}^l\cdots v_{p,l}^l)$ in π, select an arbitrary value for $h_{v_{p,1}^l}$, then proceed by the formula

$$\forall j,\quad 2\leqslant j\leqslant l,\qquad h_{v_{p,j}^l}=h_{v_{p,j-1}^l}-x_{v_{p,j}^l}.$$

Since $\sum_{i=1}^l x_{v_{p,i}^l}=0$ it follows that

$$h_{v_{p,1}^l}=h_{v_{p,l}^l}-x_{v_{p,1}^l}.$$

From these formulae we have that

$$\forall i,\quad 1\leqslant i\leqslant n,\qquad x_i=h_i-h_{\pi(i)},$$

i.e., $x=h-\pi(h)$, or $x=h_\pi$ by Definition 2.

(2) By Definition 2, a word h is attached to the index $x=h-\pi(h)$.

Given an index $x\in X_\pi\cap\mathscr{C}$, we consider all the codewords of $\mathscr{C}$ which are attached to it, i.e., all the codewords h such that $x=h_\pi$. For every cycle $\theta=(v_{p,1}^l v_{p,2}^l\cdots v_{p,l}^l)$ in π, and for each initial choice of $h_{v_{p,1}^l}$, $h|_\theta$ is determined uniquely. Thus for every θ there are q possible values for the l entries $h|_\theta$. Therefore, for π there are $q^{\kappa(\pi)}$ possible values for the $\lambda(\pi)$ entries $h|_\pi$.

Since π is a free permutation, it follows by Lemma 1 that for each value of $h|_\pi$ there are exactly $|\mathscr{C}|/q^{\lambda(\pi)}$ codewords. Altogether x is attached to $q^{\kappa(\pi)} \cdot |\mathscr{C}|/q^{\lambda(\pi)} = q^{k-\lambda(\pi)+\kappa(\pi)}$ codewords. ∎

As a consequence of Lemma 2 and Theorem 1 we obtain

COROLLARY 1. *If $\pi \in S_n$ is a free permutation with respect to an (n, k) code $\mathscr{C}$, then $|\mathscr{C}^\pi| = |\mathscr{C} \cap X_\pi| q^{k-\lambda(\pi)+\kappa(\pi)}$.*

DEFINITION 3. For a word $x = (x_1, x_2, ..., x_n) \in \mathbf{F}_q^n$ the *generalized parity* of x, $\mathrm{gp}(x)$, is defined as the sum of the entries of x, i.e., $\mathrm{gp}(x) = \sum_{i=1}^n x_i$, where this sum is computed in $\mathrm{GF}(q)$.

Let $\mathbf{0}$ denote the all-zeroes word, and $\mathbf{1}$ the all-ones word.

THEOREM 2. *If $\mathscr{C}$ is an (n, k) t-IR code, then for each ρ, $0 \leqslant \rho \leqslant t-1$, there exists a permutation π_ρ, for which $|\mathscr{C}^{\pi_\rho}| = q^{k-\rho}$.*

Proof. Let $r = n-k$ and assume that $R(\mathscr{C}) = \{1, 2, ..., r\}$, $I(\mathscr{C}) = \{r+1, r+2, ..., n\}$, and columns 1 through t of the generator matrix of $\mathscr{C}$ are linearly independent. Given $0 \leqslant \rho \leqslant t-1$, let π_ρ be the permutation which consists of the single cycle $(1, 2, ..., \rho+1)$; here $\kappa(\pi_\rho) = 1$, $\lambda(\pi_\rho) = \rho+1$. By Theorem 1, X_{π_ρ} is the set of vectors with generalized parity 0 in columns 1 through $\rho+1$, and zeroes in columns $\rho+2$ through n. Since $\rho+2 \leqslant r+1$ and the only codeword of $\mathscr{C}$ which has zeroes in columns $r+1$ through n is $\mathbf{0}$, it follows that $\mathscr{C} \cap X_\pi = \{\mathbf{0}\}$. Hence,

$$|\mathscr{C}^\pi| = |\mathscr{C} \cap X_{\pi_\rho}|\, q^{k-\lambda(\pi)+\kappa(\pi)} = q^{k-\rho}. \quad \blacksquare$$

THEOREM 3. *Let $\mathscr{C}$ be an (n, k) t-IR code and G its generator matrix, where $I(\mathscr{C}) = \{n-k+1, n-k+2, ..., n\}$, columns $1, 2, ..., t, n-k+1$ are linearly independent, the first row of G doesn't have generalized parity 0, and the last $k-1$ entries in this row are zeroes. Then there exists a permutation π such that $|\mathscr{C}^\pi| = q^{k-t}$.*

Proof. Let π be the permutation which consists of the single cycle $(1, 2, ..., t, n-k+1)$; here $\kappa(\pi) = 1$, $\lambda(\pi) = t+1$. Since columns $1, 2, ..., t$, $n-k+1$ are linearly independent, it follows that π is a free permutation. Thus, by Theorem 1, X_π is the set of vectors with generalized parity 0 in entries $1, 2, ..., t, n-k+1$, and zeroes in all other entries, in particular the last $k-1$. Since the last $k-1$ entries of the first row are zeroes it follows that the only codewords with zeroes in the last $k-1$ columns are multiples of its first row. However, the first row has generalized parity different from

0, and since by Theorem 1 every index has generalized parity 0, it follows that the only possible index is **0**. Hence,

$$|\mathscr{C}^{\pi}| = |\mathscr{C} \cap X_{\pi}|\, q^{k-\lambda(\pi)+\kappa(\pi)} = q^{k-t}. \quad \blacksquare$$

Finally, we present three additional results concerning the intersection number of linear codes. The first one is a simple observation.

THEOREM 4. *Let $\mathscr{C}$ be an (n, k) code over* GF(q). *If* $\mathbf{1} \in \mathscr{C}$ *then* 0 *is not an intersection number of* $\mathscr{C}$.

For an (n, k) code $\mathscr{C}$, the *dual code* $\mathscr{C}^{\perp}$ is an $(n, n-k)$ code which is the subspace of $\mathbf{F}_q^n$ orthogonal to $\mathscr{C}$, i.e., the parity check matrix of $\mathscr{C}$ is the generator matrix of $\mathscr{C}^{\perp}$.

THEOREM 5. *k_1 is an intersection number of an (n, k) code $\mathscr{C}$ if and only if $n-2k+k_1$ is an intersection number of $\mathscr{C}^{\perp}$.*

Proof. Let G be the generator matrix of $\mathscr{C}$ and H be the parity check matrix of $\mathscr{C}$. If for $\pi \in S_n$, $\log_q |\mathscr{C}^{\pi}| = k_1$ then the dimension of

$$\left[\frac{H}{\pi(H)}\right],$$

which is the parity check matrix of $\mathscr{C}^{\pi}$, is $n-k_1$. If k_2 is the dimension of $\pi(\mathscr{C}^{\perp}) \cap \mathscr{C}^{\perp}$ then $n-k_1 = k_2 + 2(n-k-k_2)$ and hence $k_2 = n-2k+k_1$ is an intersection number of $\mathscr{C}^{\perp}$. Similarly if $k_2 = n-2k+k_1$ is an intersection number of $\mathscr{C}^{\perp}$ then $n-2(n-k)+k_2 = k_1$ is an intersection number of $\mathscr{C}$. $\blacksquare$

The last result is a consequence of Theorems 4 and 5 and the fact that **1** is orthogonal to all the words of generalized parity 0.

COROLLARY 2. *If $\mathscr{C}$ is an (n, k) code, $k \geqslant n-k$, all of whose codewords have generalized parity* 0, *then $2k-n$ is not an intersection number of $\mathscr{C}$.*

3. APPLICATIONS OF THE RESULTS

Theorems 2 through 5 and Corollary 2 can provide a complete answer to the intersection problem for many (n, k) codes. In this section we will show that this answer can be given to most of the interesting codes.

3.1. *Cyclic Codes*

The most studied class of codes is the cyclic codes [2, p. 188]. The generator matrix of an (n, k) cyclic code $\mathscr{C}$ has the form

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_r & & & 0 \\ & g_0 & g_1 & g_2 & \cdots & g_r & & \\ & & \cdots & \cdots & \cdots & \cdots & & \\ & & & \cdots & \cdots & \cdots & \cdots & \\ 0 & & & & g_0 & g_1 & g_2 \quad \cdots & g_r \end{bmatrix},$$

where $g(x) = g_0 + g_1 x + \cdots + g_r x^r$ is the generator polynomial of $\mathscr{C}$ [2, p. 190], $r = n - k$, $g_i \in \mathrm{GF}(q)$, $0 \leqslant i \leqslant r$, $g_0 \neq 0$, and $g_r \neq 0$. Clearly the first k columns of G are linearly independent and the last k columns of G are also linearly independent. Hence, $\mathscr{C}$ is a t-IR code for $t = \min\{k, r\}$. Thus by Theorem 2, all integers between $\max\{1, n - 2r + 1\}$ and $n - r$ are intersection numbers of $\mathscr{C}$.

Now we ask whether $\max\{0, n - 2r\}$ is also an intersection number. This question can be solved by considering whether $g(1) = 0$ or $g(1) \neq 0$. It is well known [2, p. 201] that $g(1) \neq 0$ if and only if $\mathbf{1} \in \mathscr{C}$.

If $g(1) \neq 0$ then $\sum_{i=0}^{r} g_i \neq 0$, and we distinguish between two cases:

Case 1.1. If $k > n - k$, then the conditions of Theorem 3 are satisfied and hence $n - 2r$ is an intersection number.

Case 1.2. If $k \leqslant n - k$, then since $g(1) \neq 0$ it follows that $\mathbf{1} \in \mathscr{C}$ and hence by Theorem 4, $0 = \max\{0, n - 2r\}$ is not an intersection number.

If $g(1) = 0$ then $\sum_{i=0}^{r} g_i = 0$, i.e., all the codewords have generalized parity 0, and we distinguish between two cases:

Case 2.1. If $k \geqslant n - k$, then by Corollary 2 we have that $n - 2r$ is not an intersection number.

Case 2.2. If $k < n - k$, then let H be the parity check matrix of $\mathscr{C}$. $G^{\perp} = H$ is the generator matrix of the (n, k') code $\mathscr{C}^{\perp}$, where $k' = n - k$. It is well known [2], that $\mathscr{C}^{\perp}$ is also a cyclic code and for its generator polynomial $g^{\perp}(x)$ we have $g^{\perp}(1) \neq 0$. Since $k' > n - k'$, it follows from Case 1.1 that $n - 2k$ is an intersection number for $\mathscr{C}^{\perp}$. Therefore by Theorem 5 we have that 0 is an intersection number of $\mathscr{C}$.

3.2. *Extended Cyclic Codes*

For an (n, k) code $\mathscr{C}$ with at least one codeword whose generalized parity is different from 0, the *extended code* $\mathscr{C}^*$ is an $(n + 1, k)$ code whose last column is an overall parity check, i.e., if $c = (c_1, c_2, \ldots, c_n, c_{n+1}) \in \mathscr{C}^*$ then $(c_1, c_2, \ldots, c_n) \in \mathscr{C}$ and $c_{n+1} = 0 - \sum_{i=1}^{n} c_i$.

Let $\mathscr{C}$ be an (n, k) cyclic code with generator polynomial $g(x)$. If $g(1) \neq 0$ then some codewords of $\mathscr{C}$ have generalized parity different from 0, and we form the extended code $\mathscr{C}^*$. Clearly all the intersection numbers of $\mathscr{C}$ are also intersection numbers of $\mathscr{C}^*$. Now, we distinguish between two cases:

Case 1. If $k > n-k$ then, as said before, all the integers between $2k-n$ and k are intersection numbers of $\mathscr{C}$ and hence also intersection numbers of $\mathscr{C}^*$. By Corollary 2, $2k-n-1$ is not an intersection number of $\mathscr{C}^*$.

Case 2. If $k \leqslant n-k$ then, as said before, all the integers between 1 and k are intersection numbers of $\mathscr{C}$ and hence also intersection numbers of $\mathscr{C}^*$. If $\mathbf{1} \in \mathscr{C}^*$ (which is the case in codes like the extended binary BCH codes and the Reed–Muller codes), then by Theorem 4, 0 is not an intersection number of $\mathscr{C}^*$. If $\mathbf{1} \notin \mathscr{C}^*$ we cannot give a definite answer whether 0 is an intersection number of $\mathscr{C}^*$ or not.

3.3. *MDS Codes*

The next interesting class of codes is that of the MDS codes. In an (n, k) MDS code $\mathscr{C}$, every k columns of the generator matrix G are linearly independent. Since each k-tuple appears exactly once in any projection of k columns of $\mathscr{C}$ it follows that a generator matrix of $\mathscr{C}$ has either the form

$$G = \begin{bmatrix} a_1 & \overbrace{0 \quad \cdots \quad 0}^{k-1} & b_1 & \cdots\cdots\cdots\cdots \\ & a_2 & \overbrace{0 \quad \cdots \quad 0}^{k-1} & b_2 & \cdots\cdots\cdots \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ & & a_k & \overbrace{0 \quad \cdots \quad 0}^{k-1} & b_k & \cdots \end{bmatrix} \quad \text{if} \quad k \leqslant n-k,$$

or the form

$$G = \begin{bmatrix} a_1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & b_1 & \cdots & \cdots & \cdots \\ \cdots & a_2 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & b_2 & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & a_r & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & b_r \\ b_{r+1} & \cdots & \cdots & \cdots & a_{r+1} & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & 0 & b_k & \cdots & \cdots & \cdots & a_k & 0 & \cdots & \cdots \end{bmatrix}$$

if $k > r = n - k$, where $a_i \neq 0$, $b_i \neq 0$, $1 \leqslant i \leqslant k$, and all visible chains of zeroes start after a_i and end before b_i, being of overall length $k - 1$.

Similarly to the cyclic codes it is easy to verify that $\mathscr{C}$ is a t-IR code for $t = \min\{k, r\}$, $r = n - k$. Thus by Theorem 2 all integers between $\max\{1, n - 2r + 1\}$ and $n - r$ are intersection numbers of $\mathscr{C}$. The last possible intersection number of $\mathscr{C}$ is $\max\{0, n - 2r\}$. For this value we search G for a row with generalized parity different from 0.

If G has a row with generalized parity different from 0 we distinguish between three cases:

Case 1.1. If $k > n - k$, then it is easy to verify that by a suitable permutation of rows and columns we can satisfy the conditions of Theorem 3 and hence $n - 2r$ is an intersection number.

Case 1.2. $k < n - k$. If $\mathbf{1} \in \mathscr{C}$ then by Theorem 4, $0 = \max\{0, n - 2r\}$ is not an intersection number of $\mathscr{C}$. If $\mathbf{1} \notin \mathscr{C}$, then let H be the parity check matrix of $\mathscr{C}$. $G^{\perp} = H$ is the generator matrix of the (n, k') code $\mathscr{C}^{\perp}$, where $k' = n - k$. It is well known [2] that $\mathscr{C}^{\perp}$ is also an MDS code and since $\mathbf{1} \notin \mathscr{C}$, there exists a row in $G^{\perp}$ which has generalized parity different from 0. Since $k' > n - k'$, it follows from Case 1.1 that $n - 2k$ is an intersection number for $\mathscr{C}^{\perp}$. Therefore by Theorem 5 we have that 0 is an intersection number of $\mathscr{C}$.

Case 1.3. If $k = n - k$ we cannot give a definite answer whether 0 is an intersection number of $\mathscr{C}$ or not.

If all the rows of G have generalized parity 0, then again we distinguish between two cases:

Case 2.1. If $k \geqslant n - k$ then by Corollary 2 we have that $n - 2r$ is not an intersection number of $\mathscr{C}$.

Case 2.2. If $k < n - k$ then this case is handled exactly as Case 1.2.

The analysis given for cyclic codes, extended cyclic codes, and MDS codes completes the answer to the intersection problem for most interesting codes. This includes among others the Hamming codes, BCH codes, punctured Reed–Muller codes, quadratic-residue codes, and double-error correcting Goppa codes, which are all cyclic codes [2] and their extended codes.

ACKNOWLEDGMENTS

The authors thank Alexander Vardy and an anonymous referee for their constructive comments.

REFERENCES

1. T. Etzion and A. Vardy, On perfect codes and tilings: Problems and solutions, *SIAM J. Discrete Math.*, to appear.
2. F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1977.