[6] G.J. Pottie and D.P. Taylor, "Multilevel codes based on partitioning," *IEEE Trans. Inform. Theory*, vol. 35, pp. 87–98, Jan. 1989.
[7] A.R. Calderbank and L.H. Ozarow, "Nonequiprobable signaling on the Guassian channel," *IEEE Trans. Inform. Theory*, vol. 36, pp. 726–740, July 1990.
[8] M.V. Eyuboglu and G.D. Forney, Jr., "Trellis precoding: Combined coding, precoding, and shaping for intersymbol interference channels," in *IEEE Trans. Inform. Theory*, vol.38, pp. 301–314, Mar. 1992.
[9] R.J. McEliece, E.R. Rodemich, H. Rumsey, Jr., and L.R. Welch, "New upper bounds on the rate of a code via the Delsarte–MacWilliams inequality," *IEEE Trans. Inform. Theory*, vol. IT-23, pp. 157–166, Mar. 1977.
[10] G.D. Forney, Jr., R. G. Gallager, G. R. Lang, F. M. Longstaff, and S. U. Qureshi, "Efficient modulation for band-limited channels," *IEEE J. Select. Areas Commun.*, vol. SAC-2, pp. 832–646, 1984.

On the Nonperiodic Cyclic Equivalence Classes of Reed–Solomon Codes

H. Y. Song, *Member, IEEE*, I. S. Reed, *Fellow, IEEE*, and S. W. Golomb, *Fellow, IEEE*

***Abstract*—Picking up exactly one member from each of the nonperiodic cyclic equivalence classes of an $(n, k+1)$ Reed–Solomon code E over $GF(q)$ gives a code, E'', which has bounded Hamming correlation values and the self-synchronizing property. The exact size of E'' is shown to be $\frac{1}{n}\sum_{d|n}\mu(d)q^{1+\lfloor\frac{k}{d}\rfloor}$, where $\mu(d)$ is the Möbius function, $[x]$ is the integer part of x, and the summation is over all the divisors d of $n = q-1$. A construction for a subset V of E is given to prove that $|E''| \geq |V| = (q^{k+1} - q^{k+1-N})/(q-1)$ where N is the number of integers from 1 to k which are relatively prime to $q-1$. A necessary and sufficient condition for $|E''| = |V|$ is proved and some special cases are presented with examples. Furthermore, for all possible values of $q > 2$, a number $B(q)$ is determined such that $|E''| = |V|$ for $1 \leq k \leq B(q)$ and $|E''| > |V|$ for $k > B(q)$.**

***Index Terms*—Reed–Solomon codes, frequency-hopping patterns, combinatorial enumeration.**

I. Introduction

In recent times, communication requirements have evolved for symbol alphabets that are noncoherent self-synchronizable [1], [6], [12], [15], [16]. Applications include frequency-hopping spread-spectrum communications, pulse position modulation in radio and optical channels [3]–[5], [7]–[9], [13], etc. The $(n, k+1)$ Reed–Solomon codes over $GF(q)$ studied here are maximal kth-order near-orthogonal codes [1], and self-synchronizable in the sense that the picking up of exactly one member from each of the nonperiodic cyclic equivalence classes of such a Reed–Solomon code E gives a code, call it E'', which satisfies the following.

1) k is the maximum number of occurrences of any symbol in a codeword (see Proposition 2.1).
2) k is the maximum number of overlaps between two distinct cyclic shifts of a single codeword (the Hamming autocorrelation property, [1]).
3) k is the maximum number of overlaps between the cyclic shifts of any two distinct codewords (the Hamming crosscorrelation property, [1]).
4) If $(a_1, \cdots, a_n)$ and $(b_1, \cdots, b_n)$ are two codewords, then any subsequence of n consecutive digits of the sequence $a_2, \cdots, a_n, b_1, \cdots, b_{n-1}$ is at a (Hamming) distance of at least $n-2k$ from any other codeword (comma-free of degree $n-2k$). Hence, it has the self-synchronization property [2].

In the application of designing hopping patterns for frequency-hopping multiple-access communications, it is desirable to use each of the available frequency slots as nearly equally often as possible in each period. In an ideal situation, each pattern (user) would make use of each frequency slot the same number of times in every period so that the carrier frequency of the transmitted signal could be hopped as randomly as possible. Here, the code E'' is shown to have the property that k is the maximum number of occurrences of any symbol(frequency) in one period (see Proposition 2.1). Thus, for code E'' the number of visits to each frequency slot in one period is limited by k. Furthermore, the Hamming correlation properties 2) and 3) given for E'' are essential in order to guarantee a certain level of system performance [13]. Also code E'' can be used to design the sequence needed to establish frame synchronization in a pulse-position modulation communications system for optical channels [12]. In such a case a symbol of a codeword corresponds to a specific position in one frame interval. The fact in code E'' that the number of overlaps between any cyclic shifts of two codewords (or distinct cyclic shifts of a single codeword) is limited by k is most desirable in both of the above applications.

In Section II, the $(n, k+1)$ Reed–Solomon code E is briefly reviewed, and the fact that the code E is MDS(maximum-distance-separable) is used to prove Proposition 2.1. Nonperiodic cyclic equivalence classes of E are formally defined, and their number is counted in Theorem 2.2.

Reed and Wolverton [2] gave a "reasonably" systematic method for generating all of the codewords of E', which (by the definition in [2]) represents both the periodic and nonperiodic cyclic equivalence classes of E. Hence, the problem of finding an algorithm which generates all of the nonperiodic classes (only) exactly once still awaits a better solution. Such an algorithm would generally depend on the structure of the prime factorization of the number $n = q-1$ and as a consequence seems to defy any straightforward solution.

In Section III, a constructive lower bound is given in Theorem 3.3, and examples are given for the cases in which this bound is attained. Some parts of Theorem 3.3 are implicitly proved in either [1] or [2]. It should be emphasized at this point that the lower bound given in Theorem 3.3 provides not only a "reasonably good" bound on $|E''|$ for the number of elements in E'', but also the exact value of $|E''|$ in many cases. The cases in which the bound is attained are classified completely for any prime power $q > 2$ in Corollary 3.2. Finally, the construction leading to (3.8) provides an easy method for generating the nonperiodic classes needed for practical applications.

II. Cyclic Equivalence Classes of the RS Codes

Let α be a primitive element of $GF(q)$, where q is a prime power, and define $k+1$ vectors of n-tuples, where $n = q-1$, over $GF(q)$

Manuscript received April 9, 1992. This work was supported in part by the NSF under Grant NCR-9016340 and in part by the United States Office of Naval Research under Grant N00014-90-J-1341.

The authors are with the Communication Sciences Institute, Department of EE-Systems, University of Southern California, Los Angeles, CA 90089-2565.

IEEE Log Number 9209596.

as follows:

$$\boldsymbol{e}_i = (\alpha^i, \alpha^{2i}, \cdots, \alpha^{ni}), \qquad \text{for } i = 0, 1, 2, \cdots, k. \tag{2.1}$$

Then, the $(k+1)$-dimensional vector space E over $GF(q)$, which is defined in [1] by

$$E = \{\sum_{i=0}^{k} x_i \boldsymbol{e}_i \mid x_i \in GF(q)\} \tag{2.2}$$

is an $(n, k+1)$ Reed–Solomon code with minimum distance $n-k$, and hence, is a maximum kth-order near-orthogonal code, i.e. no two members of the code overlap in more than k places.

Proposition 2.1: Except for the constant vectors, each symbol occurs at most k times in each codeword of E.

Proof: Recall that E is given explicitly in (2.2). Thus, E contains q constant vectors of length n. If any symbol v occurs more than k times in some non-constant codeword $\boldsymbol{x} \in E$, then the (Hamming) distance between $\boldsymbol{x}$ and $\boldsymbol{v} = (v, v, \cdots, v)$ is less than $n-k$. On the other hand, since this code is MDS (maximum-distance-separable), the minimum (Hamming) distance is exactly $n-k$. □

Define the following cyclic permutation ρ of an element $\boldsymbol{x} = (v_1, v_2, \cdots, v_n)$ of E as $\rho\boldsymbol{x} = (v_2, \cdots, v_n, v_1)$. For any $\boldsymbol{x}$, $\boldsymbol{y}$ in E, if $\boldsymbol{x} = \rho^m \boldsymbol{y}$ for some integer m, then $\boldsymbol{x}$ and $\boldsymbol{y}$ are said to be ρ-equivalent. ρ-equivalence gives a partition of E into disjoint subsets, called cyclic equivalence classes. Thus picking up one element from each equivalence class gives a subcode of E, say E', which has the property that the cyclic shifts of two distinct codewords of E' do not overlap in more than k places. The exact size of the code E' is given in [1].

Theorem 2.1 ([1, Theorem 2]): Assume the same parameters and notation n, k, q as previously defined. Then the number $|E'|$ of cyclic equivalence classes in E is

$$|E'| = \frac{1}{n} \sum_{d|n} \phi(d) q^{1+\left[\frac{k}{d}\right]}, \tag{2.3}$$

where $\phi(d)$ is the Euler ϕ-function, $[x]$ is the integer part of x, and the summation is over all the divisors d of $n = q-1$.

Next, define a subset E'' of E' as follows:

Definition 2.1: E'' consists of those codewords $\boldsymbol{x} \in E'$ such that $\rho^j \boldsymbol{x} \neq \boldsymbol{x}$ for $j = 1, 2, \cdots, n-1$.

Thus, E'' represents each of the nonperiodic cyclic equivalence classes (which are the ρ-equivalence classes which have the maximum period $q-1$) exactly once. It is evident that E'' has the additional property that any two distinct cyclic shifts of a single codeword in E'' overlap in no more than k places.

Theorem 2.2: Assume the same parameters and notation n, k, q as previously defined. Then the number $|E''|$ of nonperiodic cyclic equivalence classes in E is

$$|E''| = \frac{1}{n} \sum_{d|n} \mu(d) q^{1+\left[\frac{k}{d}\right]}, \tag{2.4}$$

where $\mu(d)$ is the Möbius function, $[x]$ is the integer part of x, and the summation is over all the divisors d of $n = q-1$.

Proof: Consider the cyclic group $G = \{\rho^j | 1 \leq j \leq n\}$ of order n and its action on the elements of E. The number of orbits in E under G is the size of E'. Let C_d be the total number of codewords in E which have a maximum subperiod d for each divisor d of the codeword length n. Clearly, a codeword $\boldsymbol{x}$ has a maximum subperiod d if and only if d is the smallest positive integer such that $\rho^d \boldsymbol{x} = \boldsymbol{x}$. The problem is to find $C_n = |E''|$.

Since each codeword with a maximum subperiod d contributes exactly d times in E, one evidently has the following relation:

$$\sum_{d|n} dC_d = |E| = q^{k+1}. \tag{2.5}$$

To apply the Möbius Inversion Formula, one needs to express the right-hand side of (2.5) as a function of n.

Let $I(\rho^d)$ be the number of codewords of E which are left fixed by $\rho^d \in G$. Note that $\rho^d \boldsymbol{x} = \sum_{i=0}^{k} x_i \rho^d \boldsymbol{e}_i = \sum_{i=0}^{k} x_i \alpha^{id} \boldsymbol{e}_i$. Therefore, $\boldsymbol{x}$ is fixed by ρ^d if and only if $\alpha^{id} = 1$ for any nonzero coefficients x_i of $\boldsymbol{x}$. But $\alpha^{id} = 1$ if and only if id is a multiple of $q-1$ or i is a multiple of $\frac{q-1}{d}$, the number of which from 0 to k is given by $1 + [\frac{kd}{q-1}]$. Therefore,

$$I(\rho^d) = q^{1+\left[\frac{kd}{q-1}\right]}. \tag{2.6}$$

Substitution of $I(\rho^n)$ from (2.6) into (2.5) yields $|E|$ as a function of n, namely the result,

$$\sum_{d|n} dC_d = q^{1+[\frac{kn}{q-1}]}. \tag{2.7}$$

Finally, application of the Möbius Inversion Formula [14, 15] produces

$$nC_n = \sum_{d|n} \mu(\frac{n}{d}) q^{1+[\frac{kd}{q-1}]} = \sum_{d|n} \mu(d) q^{1+[\frac{k}{d}]},$$

the desired result. □

Example 2.1: Let $q = 2^6 = 64$, $q-1 = n = 63 = 3^2 \cdot 7$. Then, for each k between 1 and 62, the number of codewords in E'' is $\frac{1}{63}(64^{1+k} - 64^{1+[\frac{k}{3}]} - 64^{1+[\frac{k}{7}]} + 64^{1+[\frac{k}{21}]})$. The exact values of $|E|$, $|E'|$, and $|E''|$ are calculated for small values of k, and are given in Table I.

TABLE I
SOME EXACT NUMERICAL VALUES OF $|E''|$ FOR $n = 63$

k	$n-2k$	$\lvert E\rvert$	$\lvert E'\rvert$	$\lvert E''\rvert$
1	61	4096	128	64
2	59	262144	4224	4160
3	57	16777216	266496	266240
4	55	1073741824	17043712	17043456
⋮				

Corollary 2.1: Given q and k such that $1 \leq k \leq q-2$, let N be the number of integers from 1 to k which are relatively prime to $q-1$. If $q-1 = p^t$ for some prime p and $t = 1, 2, \cdots$, then $|E''| = (q^{k+1} - q^{k+1-N})/(q-1)$.

Proof: Since $\mu(1) = 1$, $\mu(p) = -1$, and $\mu(p^s) = 0$ for $s \geq 2$, (2.4) yields

$$\begin{aligned} |E''| &= (\mu(1) q^{1+k} + \mu(p) q^{1+\left[\frac{k}{p}\right]})/(q-1) \\ &= (q^{1+k} - q^{1+\left[\frac{k}{p}\right]})/(q-1) \\ &= (q^{1+k} - q^{1+k-N})/(q-1) \end{aligned}$$

where $\left[\frac{k}{p}\right] = k - N$ since $\left[\frac{k}{p}\right]$ counts the number of integers from 1 to k that are multiples of p. □

III. A Constructive Lower Bound on $|E''|$

Let $P = \{i_1 = 1 < i_2 < \cdots < i_N\}$ be the set of N integers from 1 to k which are relatively prime to $q-1$. Also let $b_1, b_2, \cdots, b_N$ be any N nonzero elements of $GF(q)$. Now, make a recursive construction of N subsets $V(1), V(2), \cdots, V(N)$ of E in accordance with the following rule:

$$V(1) = \{\boldsymbol{x} \in E | x_1 = b_1\},$$
$$V(2) = \{\boldsymbol{x} \in E | x_{i_2} = b_2, x_1 = 0\},$$
$$\vdots$$
$$V(N) = \{\boldsymbol{x} \in E | x_{i_N} = b_N, x_{i_1} = x_{i_2} = \cdots = x_{i_{(N-1)}} = 0\}.$$

Next, form the union V of the $V(i)$'s, i.e.,

$$V = \bigcup_{i=1}^{N} V(i). \tag{3.8}$$

Theorem 3.3: For any i from 1 to $q-1$, let $\boldsymbol{e}_i$ be the vectors as given in (2.1). Then, the integer $p_i = \frac{q-1}{(i,q-1)}$ is the period of $\boldsymbol{e}_i$ where $(i, q-1)$ denotes the greatest common divisor of i and $q-1$. For any given k between 0 and $q-2$, let Q be the set of integers from 0 to k which are not relatively prime to $q-1$ (i.e., the complement of P in $\{0 \le i \le k\}$). Let V be the subset of E constructed in (3.8). Then

$$|E''| \ge |V| = \frac{q^{k+1} - q^{k+1-N}}{q-1}, \tag{3.9}$$

where the equality holds, if and only if there exists no subset Q' of Q such that the least common multiple of the p_i's for $i \in Q'$ is $q-1$.

Proof: Recall that $\boldsymbol{e}_i = (\alpha^i, \alpha^{2i}, \cdots, \alpha^{ni})$, and that $\rho^d \boldsymbol{e}_i = \alpha^{id} \boldsymbol{e}_i$. Therefore, the period of $\boldsymbol{e}_i$ is the multiplicative order of α^i, which is clearly given by $\frac{q-1}{(i,q-1)}$ where α is the primitive element of $GF(q)$.

Since Q is the complement of P in $\{0 \le i \le k\}$, the mth-cyclic shift of $\boldsymbol{x} \in E$ for any integer m can be expressed by

$$\begin{aligned}\rho^m \boldsymbol{x} &= \rho^m (x_{i_1} \boldsymbol{e}_{i_1} + \cdots + x_{i_N} \boldsymbol{e}_{i_N} + \sum_{i \in Q} x_i \boldsymbol{e}_i) \\ &= x_{i_1} \rho^m \boldsymbol{e}_{i_1} + \cdots + x_{i_N} \rho^m \boldsymbol{e}_{i_N} + \sum_{i \in Q} x_i \rho^m \boldsymbol{e}_i \\ &= x_{i_1} \alpha^{m i_1} \boldsymbol{e}_{i_1} + \cdots + x_{i_N} \alpha^{m i_N} \boldsymbol{e}_{i_N} + \sum_{i \in Q} x_i \alpha^{mi} \boldsymbol{e}_i.\end{aligned}$$

The period of $\boldsymbol{x}$ is the least common multiple of the p_i's for which $x_i \neq 0$. Therefore, any $\boldsymbol{x} \in V$ must have the maximum period $q-1$ since it has at least one index i such that $x_i \neq 0$ and $p_i = q-1$.

Suppose $\rho^m \boldsymbol{x} = \boldsymbol{y}$ for some m. If $\boldsymbol{x} \in V(s)$ and $\boldsymbol{y} \in V(t)$ where $s < t$, then since $y_{i_s} = 0$ by the construction leading to (3.8), the coefficient of $\boldsymbol{e}_{i_s}$ in $\rho^m \boldsymbol{x}$ is $\alpha^{m i_s} b_s = y_{i_s} = 0$. But, this is impossible since $b_s \neq 0$ and $\alpha^{m i_s} \neq 0$. If both $\boldsymbol{x}$ and $\boldsymbol{y}$ are in $V(s)$, then since $y_{i_s} = b_s$, one has by the same construction $\alpha^{m i_s} b_s = b_s$, which yields $(\alpha^{i_s})^m = 1$. But this implies $m \equiv 0 \pmod{q-1}$. Therefore, no two codewords in V are ρ-equivalent, and hence V is a disjoint union. Therefore, since $V(j)$ is a subspace of dimension $k+1-j$ for $j = 1, 2, \cdots, N$, one obtains

$$\begin{aligned}|V| &= |V(1)| + |V(2)| + \cdots + |V(N)| \\ &= q^k + q^{k-1} + \cdots + q^{k-(N-1)} \\ &= (q^{k+1} - q^{k+1-N})/(q-1).\end{aligned}$$

To find the condition for equality in (3.9), consider the following: For any $i_s (\in P)$ relatively prime to $q-1$ and for any nonzero b_s, if $x_{i_s} \neq 0$, then there is some m such that $\alpha^{i_s m} x_{i_s} = b_s$. Therefore, for any $\boldsymbol{x} \in E''$ such that $x_{i_s} \neq 0$ for $i_s \in P$, vector $\boldsymbol{x}$ must be ρ-equivalent to some vector in V. This implies that if there is some $\boldsymbol{x}$ which has the maximum period $q-1$ and which is not ρ-equivalent to any codeword in V, then one must have that $x_i = 0$ for all $i \in P$. In this case, the period of $\boldsymbol{x}$ is $q-1$, if and only if there exists some subset Q' of Q such that the lcm of the p_i's for $i \in Q'$ is $q-1$. □

It is easy to see that the term q^{k+1} on the right sides of both (3.9) and (2.4) becomes more dominant as q gets larger for fixed k. Indeed, the two expressions have values which are of the same order of magnitude even for small values of q. Moreover, these values are exactly the same for some k between 0 and $q-2$.

To see this, reconsider Example 2.1 where $q-1 = 63 = 3^2 \cdot 7$. In this case, $|E''| = |V|$ for the values of k from 1 to 6. For $k = 7$ the values of $|E''|$ and $|V|$ are different for the first time. But these values have the order of $64^7 \sim 4.4 \times 10^{12}$. Next, it can be verified that $|V| < |E''|$ for $7 < k \le 61$. Therefore, the above construction provides not only a "reasonably good" lower bound on $|E''|$, but also it gives the exact value of $|E''|$ for some integer k. The following corollary gives all the integer k for which $|E''| = |V|$.

Corollary 3.2: Consider the code E'' defined earlier and V which is constructed according to the steps leading to (3.8). For any prime power $q > 2$, there exists a number $B(q)$ between 1 and $q-2$ such that $|E''| = |V|$ for $1 \le k \le B(q)$ and $|E''| > |V|$ for $k > B(q)$. Furthermore, $B(q)$ is explicitly given as follows: (1) If $q-1$ is divisible by only one prime, then $B(q) = q-2$. (2) If $q-1$ is divisible by at least two distinct primes, then $B(q)$ is one less than the second smallest prime factor of $q-1$.

Proof: It is sufficient to prove (2), since (1) is exactly the case covered by Corollary 2.1. Let $q-1 = a^s b^t M$ where a and b are the smallest and the second smallest prime factors of $q-1$, respectively, for $s \ge 1$ and $t \ge 1$ and where $M = 1$ or M contains only prime factors larger than b. Then, any integer i less than b, which is not relatively prime to $q-1$, must be a multiple of a. For any such i one has

$$p_i = \frac{a^s b^t M}{(i, a^s b^t M)} = \frac{a^s b^t M}{a^u} = a^{s-u} b^t M$$

where u cannot be zero. Therefore, the lcm of any such p_i can never be $q-1$. This proves that $|V| = |E''|$ for $1 \le k \le b-1$. If $b \le k \le q-2$, then

$$p_b = \frac{a^s b^t M}{(b, a^s b^t M)} = a^s b^{t-1} M \quad \text{and}$$
$$p_a = \frac{a^s b^t M}{(a, a^s b^t M)} = a^{s-1} b^t M.$$

Hence, the lcm of p_a and p_b is $q-1$. Since both a and b are not relatively prime to $q-1$, this proves that $|V| < |E''|$ for $k \ge b$. □

Example 3.2: Let $q = 7$. In this case, $B(7) = 3 - 1 = 2$ and Corollary 3.2 says $|E''| = |V|$ for $k = 1, 2$. Take $k = 2$. The primitive roots of the integers (mod 7) are 3 and 5. Choose $\alpha = 3$. Then code E has $q^{(k+1)} = 7^3 = 343$ codewords, $|E'| = 70$, and $|E''| = |V| = 49$. Table II shows both codes E' and E'' explicitly for this example where E'' is constructed from $V = V(1) = \{\boldsymbol{x} | x_1 = b_1 = 1\}$. Since $k = 2$, one has $p_0 = 1$, $p_1 = 6$, and $p_2 = 3$. Thus code E'' does not contain any representatives from the classes of period 2.

TABLE II
WHEN $q = 7$ AND $k = 2$ (IN EXAMPLE 3.2), CODE E' CONSISTS OF ALL OF THE CODEWORDS. CODE E'' CONSISTS ONLY OF THOSE HAVING PERIOD 6

Classes of period 1:						
(000000)	(111111)	(222222)	(333333)	(444444)	(555555)	(666666)
Classes of period 3:						
(241241)	(352352)	(463463)	(504504)	(615615)	(026026)	(130130)
(653653)	(064064)	(105105)	(216216)	(320320)	(431431)	(542542)
Classes of period 6 (Nonperiodic classes):						
(326451)	(430562)	(541603)	(652014)	(063125)	(104236)	(215340)
(560622)	(601033)	(012144)	(123255)	(234366)	(345400)	(456511)
(031163)	(142204)	(253315)	(364426)	(405530)	(516641)	(620052)
(202334)	(313445)	(424556)	(535660)	(646001)	(050112)	(161223)
(443505)	(554616)	(665020)	(006131)	(110242)	(221353)	(332464)
(614046)	(025150)	(136261)	(240302)	(351413)	(462524)	(503635)
(155210)	(266321)	(300432)	(411543)	(522654)	(633065)	(044106)

Example 3.3: Let $q = 17$ and $q - 1 = 16 = 2^4$, then for any k from 1 to 14, Q contains all of the even integers from 0 to k. Hence, for any $i \in Q$, $p_i = 2^4/(i, 2^4) = 2^s$ for some $s < 4$. Also the l.c.m. of such p_i's can never equal 2^4. Therefore, $|E''| = |V|$ for all integers k from 1 to 15.

IV. CONCLUSION

Two simpler constructions than the one leading to (3.8) were found recently which give a slightly smaller number of codewords than V in (3.8). N. Q. A, L. Györfi and J. L. Massey constructed a code (see [11, Theorem 2]) which is precisely $V(1)$ in (3.8) with $b_1 = 1$. Note that $|V(1)| = q^k$, and hence $\frac{|V|}{|V(1)|} = (q - q^{1-N})/(q-1)$. Therefore, $|V| = |V(1)|$ for $N = 1$, and $|V(1)| < |V| < |V(1)|q/(q-1)$ for $N > 1$. This implies that $|V(1)|$ and $|V|$ are asymtotically equal.

We remark further that I. Vajda and G. Einarsson [10] made use in a frequency-hopping scheme of the precise form of set $V(1)$ with $k + 1 = 3$ and $b_1 = 1$ so that $V(1) = \{\boldsymbol{x} \in E | \boldsymbol{x} = x_0\boldsymbol{e}_0 + \boldsymbol{e}_1 + x_2\boldsymbol{e}_2\}$ where x_0 is the message and x_2 is the user's address. As a consequence, they obtained a desirable resynchronization property.

ACKNOWLEDGMENT

The authors are grateful to the anonymous referees for bringing [10] and [11] to their attention and for helpful comments.

REFERENCES

[1] I. S. Reed, "kth-order near-orthogonal codes," *IEEE Trans. Inform. Theory*, vol. IT-17, pp. 116–117, Jan. 1971.
[2] I. S. Reed and C. T. Wolverton, "The systematic selection of cyclically equivalent codes," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 304–307, Mar. 1972.
[3] D. V. Sarwate and M. B. Pursley, "Hopping patterns for frequency-hopped multiple-access communication," *Proc. IEEE Int. Conf. Commun.*, 1978.
[4] G. R. Cooper and R W. Nettleton, "A spread-spectrum technique for high-capacity mobil communications," *IEEE Trans. Vehicular Technol.*, vol. 27, no. 4, pp. 264–275, 1978.
[5] T. S. Seay, "Hopping patterns for bounded mutual interference in frequency hopping multiple access," in *MILCOM*, sec. 22.3, Oct. 1982.
[6] A. Lempel and H. Greenberger, "Families of sequences with optimal hamming correlation properties," *IEEE Trans. Inform. Theory*, vol. IT-20, no. 1, pp. 90–94, Jan. 1974.
[7] R. J. McEliece, "Some combinatorial aspects of spread-spectrun communication systems," in *New Concepts in Multi-User Communication*, J. K. Skwirzynski, Ed. Rockville, MD: Sijthoff and Noordhoff, 1981, pp. 199–211.
[8] A. A. Sharr and P. A. Davies, "Prime sequences: Quasi-optimal sequences for OR channel code division multiplexing," *Electron. Lett.*, vol. 19, no. 21, pp. 888–890, 1983.
[9] ——, "A survey of one-coincidence sequences for frequency-hopped spread-spectrum systems," *IEE Proc.*, vol. 131, no. 7, pp. 719–724, 1984.
[10] I. Vajda and G. Einarsson, "Code acquisition for a frequency-hopping system," *IEEE Trans. Commun.*, vol. COM-35, no. 5, pp. 566–568, May 1987.
[11] N. Q. A, L. Györfi, and J. L. Massey, "Construction of binary constant-weight cyclic codes and cyclically permutable codes," *IEEE Trans. Inform. Theory*, vol. 38, no. 3, pp. 940–949, May 1992.
[12] R. Gagliardi, J. Robbins, and H. Taylor, "Acquisition sequences in PPM communications," *IEEE Trans. Inform. Theory*, vol. IT-33, no. 5, pp. 738–744, Sept. 1987.
[13] A. W. Lam and D. V. Sarwate, "Time-hopping and frequency-hopping multiple-access packet communications," *IEEE Trans. Commun.*, vol. 38, no. 6, pp. 875–888, June 1990.
[14] S. W. Golomb, "A mathematical theory of discrete classification," in *Fourth London Symposium on Information Theory*. London: Butterworths, 1961.
[15] S. W. Golomb, B. Gordon and L. R. Welch, "Comma-free codes," *Canadian J. Math.*, vol. 10, pp. 202–209, 1958.
[16] S. W. Golomb and B. Gordon, "Codes with bounded synchronization delay," *Inform. Contr.*, vol. 8, pp. 355–372, 1965.
[17] F. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
[18] D. M. Burton, *Elementary Number Theory*. Boston, MA: Allyn and Bacon Inc., 1980.