Long Nonbinary Codes Exceeding the Gilbert–Varshamov Bound for any Fixed Distance

Sergey Yekhanin and Ilya Dumer, *Senior Member, IEEE*

***Abstract*—Let $A(q,n,d)$ denote the maximum size of a q-ary code of length n and distance d. We study the minimum asymptotic redundancy**

$$\rho(q,n,d) = n - \log_q A(q,n,d)$$

as n grows while q and d are fixed. For any d and $q \geq d-1$, long algebraic codes are designed that improve on the Bose–Chaudhuri–Hocquenghem (BCH) codes and have the lowest asymptotic redundancy

$$\rho(q,n,d) \lesssim ((d-3) + 1/(d-2)) \log_q n$$

known to date. Prior to this work, codes of fixed distance that asymptotically surpass BCH codes and the Gilbert–Varshamov bound were designed only for distances $4, 5$, and 6.

***Index Terms*—Affine lines, Bose–Chaudhuri–Hocquenghem (BCH) code, Bezout's theorem, norm.**

I. Introduction

Let $A(q,n,d)$ denote the maximum size of a q-ary code of length n and distance d. We study the asymptotic size $A(q,n,d)$ if q and d are fixed as $n \to \infty$, and introduce a related quantity

$$c(q,d) = \underline{\lim}_{n\to\infty} \frac{n - \log_q A(q,n,d)}{\log_q n}$$

which we call the *redundancy coefficient.*

The Hamming upper bound

$$A(q,n,d) \leq q^n \Big/ \sum_{i=0}^{\lfloor (d-1)/2 \rfloor} (q-1)^i \binom{n}{i}$$

leads to the lower bound

$$c(q,d) \geq \lfloor (d-1)/2 \rfloor \tag{1}$$

Manuscript received February 28, 2004; revised June 23, 2004. The work of S. Yekhanin was supported in part by NTT Award MIT 2001-04 and by the National Science Foundation under Grant CCR–0219218. The work of I. Dumer was supported by the National Science Foundation under Grant CCR–0097125.

S. Yekhanin is with the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139 USA (e-mail: yekhanin@mit.edu).

I. Dumer is with the College of Engineering, University of California, Riverside, CA 92521, USA (e-mail: dumer@ee.ucr.edu).

Communicated by C. Carlet, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2004.834744

which is the best bound on $c(q,d)$ known to date for arbitrary values of q and d. On the other hand, the Varshamov existence bound admits any linear $[n,k,d]_q$ code of dimension

$$k \leq n - 1 - \left\lfloor \log_q \sum_{i=0}^{d-2} (q-1)^i \binom{n-1}{i} \right\rfloor.$$

This leads to the redundancy coefficient

$$c(q,d) \leq d-2. \tag{2}$$

(Note that the Gilbert bound results in a weaker inequality $c(q,d) \leq d-1$.)

Let e be a primitive element of the Galois field F_{q^m}. Consider (see [20]) the narrow-sense Bose–Chaudhuri–Hocquenghem (BCH) code defined by the generator polynomial with *zeros* $e^1, \ldots, e^{d-2}$. Let $C_q^m(d)$ denote the extended BCH code obtained by adding the overall parity check. Code $C_q^m(d)$ has length q^m, *constructive* distance d, and redundancy coefficient

$$c(q,d) \leq \left\lceil \frac{(d-2)(q-1)}{q} \right\rceil. \tag{3}$$

Note that the above BCH bound (3) is better than the Varshamov bound (2) for $q < d-1$ and coincides with (2) for $q \geq d-1$. Note also that (3) meets the Hamming bound (1) if $q = 2$ or $d = 3$. Therefore,

$$c(2,d) = \lfloor (d-1)/2 \rfloor \quad \text{and} \quad c(q,3) = 1.$$

For distances $4, 5$, and 6, infinite families of nonbinary linear codes are constructed in [5] and [6] that reduce asymptotic redundancy (3). Open Problem 2 from [6] also raises the question if the BCH bound (3) can be improved for larger values of d. Our main result is an algebraic construction of codes that gives an affirmative answer to this problem for all $q \geq d-1$. In terms of redundancy, the new bound is expressed by the following.

Theorem 1: For all q and $d \geq 3$

$$c(q,d) \leq (d-3) + 1/(d-2). \tag{4}$$

Combining (3) and (4), we obtain

$$c(q,d) \leq \min\left(\left\lceil \frac{(d-2)(q-1)}{q} \right\rceil, (d-3) + \frac{1}{(d-2)} \right).$$

Note that the above bound is better than the Varshamov existence bound for arbitrary q and $d \geq 4$.

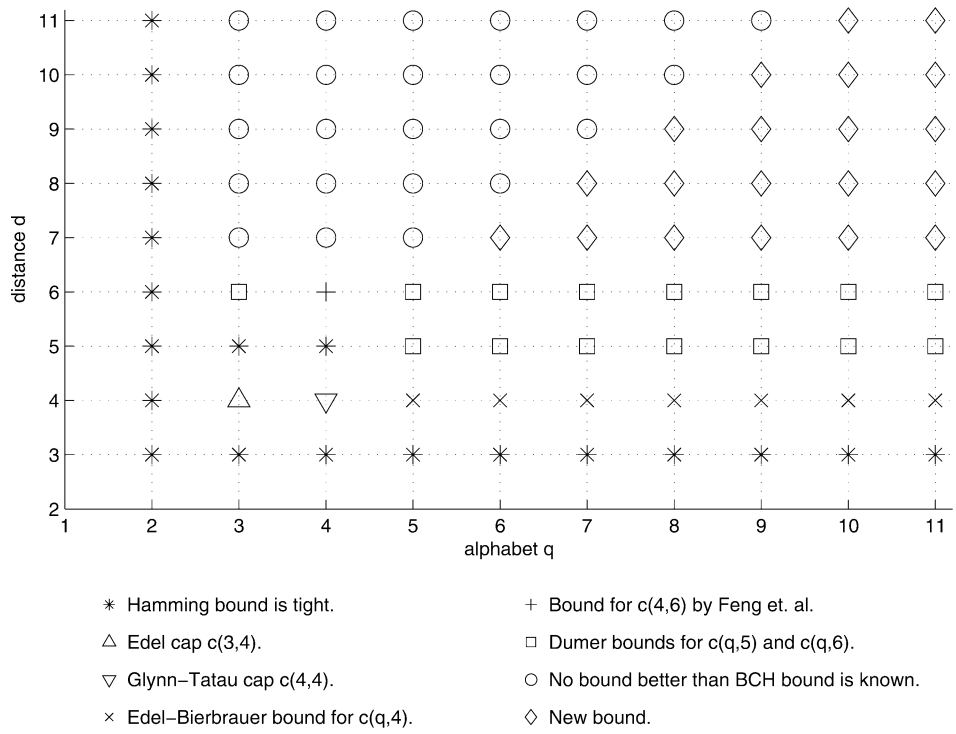

Fig. 1. A taxonomy of best known upper bounds for $c(q,d)$.

The rest of the paper is organized as follows. In Section II, we review the upper bounds for $c(q,d)$ that surpass the BCH bound (3) for small values of d. In Section III, we present our code construction and prove the new bound (4). This proof rests on important Theorem 4, which is proven in Section IV. Finally, we make some concluding remarks in Section V.

II. Previous Work

Prior to this work, codes that asymptotically exceed the BCH bound (3) were known only for $d \leq 6$. We start with the bounds for $c(q,4)$. Linear $[n, n-\rho, 4]_q$ codes are equivalent to *caps* in projective geometries PG$(\rho-1, q)$ and have been studied extensively under this name. See [18] for a review. However, the exact values of $c(q,4)$ remain unknown for all $q \geq 3$, and the gaps between the upper and the lower bounds are still large.

The Hamming bound yields $c(q,4) \geq 1$. Mukhopadhyay [22] obtained the upper bound $c(q,4) \leq 1.5$. For all values of q, this was later improved by Edel and Bierbrauer [7] to

$$c(q,4) \leq \frac{6}{\log_q (q^4+q^2-1)}. \tag{5}$$

Note that for large values of q, the right-hand side of (5) tends to 1.5. The case of $q=3$ has been of special interest, and general bound (5) has been improved in a few papers (see [17], [11], [2], [8]). The current record

$$c(3,4) \leq 1.3796$$

due to Edel [8] slightly improves on the previous record $c(3,4) \leq 1.3855$ obtained by Calderbank and Fishburn [2]. For $q=4$, the construction of [14] also improves (5). Namely, $c(4,4) \leq 1.45$.

Now we proceed to the bounds for $c(q,5)$. The Hamming bound yields $c(q,5) \geq 2$. Several families of linear codes constructed in [6] reach the bound

$$c(q,5) \leq 7/3 \tag{6}$$

for all values of q. Later, alternative constructions of codes with the same asymptotic redundancy were considered in [9]. Similarly to the case of $d=4$, there exist better bounds for small alphabets. Namely, Goppa pointed out that ternary double error-correcting BCH codes asymptotically meet the Hamming bound (1). For $q=4$ and $d=5$, two different constructions that asymptotically meet the Hamming bound were proposed in [12] and [4]. Thus,

$$c(3,5) = c(4,5) = 2.$$

For $d=6$, the infinite families of linear codes designed in [5] and [6] reach the upper bound

$$c(q,6) \leq 3 \tag{7}$$

for all q. The constructions are rather complex and the resulting linear codes are not cyclic. Later, a simpler construction of a cyclic code with the same asymptotic redundancy was proposed in [3]. Again, better bounds exist for small values of q. Namely, $c(3,6) \leq 2.5$ [6] and $c(4,6) \leq 17/6$ [10].

We summarize the bounds described so far in Fig. 1.

The following Lemma 2 due to Gevorkyan [13] shows that redundancy $c(q,d)$ cannot increase when the alphabet size is reduced.

Lemma 2: For arbitrary value of distance d

$$q_1 \leq q_2 \Rightarrow c(q_1,d) \leq c(q_2,d).$$

Proof: Given a code V of length n over the q_2-ary alphabet we prove the existence of a code V' of the same length over q_1-ary alphabet with the same redundancy coefficient. Let q_2-ary alphabet be an additive group E_{q_2}, and q_1-ary alphabet form a subset $E_{q_1} \subseteq E_{q_2}$. Define the componentwise shift $V_v = V + v$ of code V by an arbitrary vector $v \in E_{q_2}^n$. Note that any vector $f \in E_{q_1}^n$ belongs to exactly $|V|$ codes among all q_2^n codes V_v, as v runs through $E_{q_2}^n$. Hence, codes V_v include on average $q_1^n|V|/q_2^n$ vectors of the subset $E_{q_1}^n \subseteq E_{q_2}^n$. Therefore, some set $V_v \cap E_{q_1}^n$ has at least this average size. Denote this set by V'. Clearly, V' is a q_1-ary code with the same distance as code V. It remains to note that

$$\frac{n - \log_{q_1}(q_1^n|V|/q_2^n)}{\log_{q_1} n} = \frac{n - \log_{q_2}|V|}{\log_{q_2} n}.$$

The proof is completed. □

Corollary 3: Let $\{q_i\}$ be an infinite sequence of growing alphabet sizes. Assume there exist $c^\star$ and d such that for all i, $c(q_i, d) \le c^\star$. Then $c(q, d) \le c^\star$ for all values of q.

Proof: This follows trivially from Lemma 2. □

III. Code Construction

In the sequel, the elements of the field F_q are denoted by Greek letters, while the elements of extension fields F_{q^i} are denoted by Latin letters.

We start with an extended BCH code $C = C_q^m(d-1)$ of length $n = q^m$ and constructive distance $d-1$. Here for any position $j \in [1, q^m]$, we define its *locator* e_j, where $e_j = e^j$ for $j < n$ and $e_n = 0$. Then the parity-check matrix of code C has the form

$$H_q^m(d-1) = \begin{pmatrix} 1 & \dots & 1 & 1 \\ e_1 & \dots & e_{n-1} & 0 \\ \vdots & \dots & \vdots & \vdots \\ e_1^{d-3} & \dots & e_{n-1}^{d-3} & 0 \end{pmatrix}. \tag{8}$$

Here the powers of locators e_j are represented with respect to some basis of F_{q^m} over F_q. Note that the redundancy of C is at most $(d-3)m+1$. Also, we assume in the sequel that q does not divide $d-2$, since code C has constructive distance d instead of $d-1$ otherwise.

Consider any nonzero codeword $c \in C$ of weight w with nonzero symbols in positions $j_1, \dots, j_w$. Let $X(c) = \{x_1, \dots, x_w\}$ denote its *locator set*, where we use notation $x_i = e_{j_i}$ for all $i = 1, \dots, w$. We say that $X(c)$ lies on an affine line $L(a, b)$ over F_q if there exist $a, b \in F_{q^m}$ such that

$$x_i = a + \lambda_i b \tag{9}$$

where $\lambda_i \in F_q$ for all values of $i = 1, \dots, w$.

The key observation underlining our code construction is that under some restrictions on extension m and characteristic $\operatorname{char} F_q$ of the field F_q, any code vector $c \in C$ of weight $d-1$ has its locator set $X(c)$ lying on some affine line.[1] Formally, this is expressed by the following.

[1]We shall also see that code $C_q^m(d-1)$ does have minimum distance $d-1$ under these restrictions.

Theorem 4: Let m be a prime, $m > (d-3)!$ and $\operatorname{char} F_q > d-3$. Consider the extended BCH code $C_q^m(d-1)$ of constructive distance $d-1$. Then, any codeword c of minimum weight $d-1$ has its locator set $X(c)$ lying on some affine line $L(a, b)$ over F_q.

We defer the proof of Theorem 4 till Section IV and proceed with the code construction. Let

$$s = \lceil m/(d-2) \rceil, \qquad \mu = s(d-2).$$

Consider the field F_{q^μ} and its subfield F_{q^s}. Let $g = \{g_1, \dots, g_\mu\}$ be the basis of F_{q^μ} over F_q such that F_{q^s} is spanned by $\{g_1, \dots, g_s\}$. Let $h = \{h_1, \dots, h_m\}$ be an arbitrary basis of F_{q^m} over F_q. In what follows, we map each element $x = \sum_{i=1}^m \alpha_i h_i$ of the field F_{q^m} onto the element

$$\hat{x} = \sum_{i=1}^m \alpha_i g_i \tag{10}$$

of the field F_{q^μ}. It is readily seen that for arbitrary $a, b \in F_{q^m}$ and $\lambda \in F_q$

$$\widehat{a + \lambda b} = \hat{a} + \lambda \hat{b}. \tag{11}$$

Recall that the *norm* [15] of $\hat{x} \in F_{q^\mu}$

$$N_{F_{q^\mu}/F_{q^s}}(\hat{x}) = N_{d-2}(\hat{x}) = \hat{x}^{q^{(d-3)s} + \dots + q^s + 1} \tag{12}$$

is a classical mapping from F_{q^μ} to F_{q^s}.

Now we are ready to present our code construction. Consider the q-ary code $C'(n, k', d')$ of length $n = q^m$ with the parity-check matrix

$$\hat{H}_q^m = \begin{pmatrix} 1 & \dots & 1 & 1 \\ e_1 & \dots & e_{n-1} & 0 \\ \vdots & \dots & \vdots & \vdots \\ e_1^{d-3} & \dots & e_{n-1}^{d-3} & 0 \\ N_{d-2}(\hat{e}_1) & \dots & N_{d-2}(\hat{e}_{n-1}) & 0 \end{pmatrix} \tag{13}$$

where the locators e_j and their powers are represented in F_q with respect to the basis h and values of N_{d-2} are represented in F_q with respect to g. Recall that $N_{d-2}(x)$ takes values in F_{q^s}. Therefore, the redundancy of C' does not exceed $(d-3)m + s + 1$.

Theorem 5 is the main theorem of the paper.

Theorem 5: Suppose $m > (d-3)!$ is a prime, and $\operatorname{char} F_q > d-3$; then code $C'(n, k', d')$ defined by (13) has parameters

$$[q^m, k' \ge q^m - (d-3)m - \lceil m/(d-2) \rceil - 1, d' \ge d]_q.$$

Proof: Note that $d' \ge d-1$, since C' is a subcode of the extended BCH code C defined in (8). Let $C_{d-1} \subseteq C$ be the set of all codewords of weight exactly $d-1$. It remains to prove that $C' \cap C_{d-1} = \emptyset$.

Assume the converse. Let $c \in C'$ be a codeword of weight $d-1$ with locator set $X(c) = (x_1, \dots, x_{d-1})$. This implies that for some nonzero symbols $\xi_1, \dots, \xi_{d-1} \in F_q$

$$\begin{cases} \sum\limits_{i=1}^{d-1} \xi_i x_i^t = 0, & t = 0, \dots, d-3 \\ \sum\limits_{i=1}^{d-1} \xi_i N_{d-2}(\hat{x}_i) = 0. \end{cases} \tag{14}$$

Note that $c \in C_{d-1}$. Therefore according to Theorem 4, there exist $a, b \neq 0$ from F_{q^m} and pairwise distinct $\{\lambda_i\} \in F_q$ such that $x_i = a + \lambda_i b$. Consider the affine permutation $\pi(x) = A + Bx$ of the entire locator set F_{q^m}, where $A = -ab^{-1}$ and $B = b^{-1}$. Clearly, π maps each x_i onto λ_i, i.e.,

$$\lambda_i = A + Bx_i.$$

It is well known ([1], [20]) that the extended BCH code C is invariant under any affine permutation of the locators, so that $\{\lambda_i\}$ is also a locator set in C_{d-1}. Indeed, for any $t \in [0, d-3]$, we have an equality

$$\sum_{i=1}^{d-1} \xi_i \lambda_i^t = \sum_{i=1}^{d-1} \xi_i (A + Bx_i)^t = \sum_{j=0}^{t} A^{t-j} B^j \binom{t}{j} \sum_{i=1}^{d-1} \xi_i x_i^j = 0. \tag{15}$$

We shall now demonstrate that (14) yields one more equation

$$\sum_{i=1}^{d-1} \xi_i \lambda_i^{d-2} = 0. \tag{16}$$

Indeed, we use (11) and (12) to obtain

$$\begin{aligned} N_{d-2}\left(\hat{a} + \lambda_i \hat{b}\right) &= \left(\hat{a} + \lambda_i \hat{b}\right)^{q^{(d-3)s} + \cdots + q^s + 1} \\ &= \prod_{t=0}^{d-3} \left(\hat{a}^{q^{ts}} + \lambda_i \hat{b}^{q^{ts}}\right) \\ &= \sum_{t=0}^{d-2} C_t(\hat{a}, \hat{b}) \lambda_i^t \end{aligned} \tag{17}$$

where C_t are some polynomials in $\hat{a}$ and $\hat{b}$. Now the last equation in (14) can be rewritten as

$$\sum_{i=1}^{d-1} \xi_i \sum_{t=0}^{d-2} C_t(\hat{a}, \hat{b}) \lambda_i^t = \sum_{t=0}^{d-2} C_t(\hat{a}, \hat{b}) \sum_{i=1}^{d-1} \xi_i \lambda_i^t = 0.$$

This gives (16), due to the two facts:

- $\sum_{i=1}^{d-1} \xi_i \lambda_i^t = 0$ for all $t = 0, \ldots, d-3$, according to (15).
- $C_{d-2}(\hat{a}, \hat{b}) = N_{d-2}(\hat{b})$ and is nonzero, since b is nonzero and norm is a degree.

Equations (15) and (16) form the linear system

$$\sum_{i=1}^{d-1} \xi_i \lambda_i^t = 0, \qquad t = 0, \ldots, d-2$$

in variables ξ_i with the Vandermonde matrix (λ_i^t). Recall that $\{\xi_i\}$ are nonzero and $\{\lambda_i\}$ are pairwise distinct. Therefore, these $d-1$ equations hold only if $\xi_i = 0$ simultaneously. Thus, our initial assumption that c has weight $d-1$ does not hold. This completes the proof. □

Lemma 6: Suppose $\operatorname{char} F_q > d-3$; then

$$c(q, d) \leq (d-3) + 1/(d-2).$$

Proof: We estimate the asymptotic redundancy of the family of codes presented in Theorem 5. Here q and d are fixed, while $m > (d-3)!$ runs to infinity over primes. Then

$$\begin{aligned} c(q, d) &\leq \lim_{m \to \infty} \frac{(d-3)m + \lceil m/(d-2) \rceil + 1}{m} \\ &= (d-3) + 1/(d-2). \end{aligned} \tag{18}$$

The proof is completed. □

It is obvious that for every $d \geq 3$ there exists an infinite family $\{q_i\}$ of growing alphabets such that $\operatorname{char} F_{q_i} > d-3$. Combining Lemma 6 with Corollary 3, we get Theorem 1. The proof is completed. □

To conclude, we would like to note that our construction of code C' (13) generalizes the construction of nonbinary double error-correcting codes from Theorem 7 in [6].

IV. Affine Lines

Before we proceed to the proof of Theorem 4, let us introduce some standard concepts and theorems of algebraic geometry. Let F be an algebraically closed field and r, t be two positive integers. Let $f_1, \ldots, f_r \in F[x_1, \ldots, x_t]$. For any $x = (a_1, \ldots, a_t) \in F^t$, the matrix

$$J_x(f_1, \ldots, f_r) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1}\big|_x & \cdots & \frac{\partial f_1}{\partial x_t}\big|_x \\ \vdots & \ddots & \vdots \\ \frac{\partial f_r}{\partial x_1}\big|_x & \cdots & \frac{\partial f_r}{\partial x_t}\big|_x \end{pmatrix} \tag{19}$$

is called the *Jacobian* of functions f_i at point x.

The set V of common roots to the system of equations

$$\begin{cases} f_1(x_1, \ldots, x_t) &= 0 \\ \quad \vdots & \\ f_r(x_1, \ldots, x_t) &= 0 \end{cases} \tag{20}$$

is called an affine variety. The ideal $I(V)$ is the set of all polynomials $f \in F[x_1, \ldots, x_t]$ such that $f(x) = 0$ for all $x \in V$. One important characteristic of a variety is its dimension $\dim V$. Dimension of a nonempty variety is a nonnegative integer. Let $x = (a_1, \ldots, a_t) \in V$ be an arbitrary point on V. The dimension of a variety V at a point x, denoted $\dim_x V$, is the maximum dimension of an irreducible component of V containing x. A point $x \in V$ such that $\dim_x V = 0$ is called an *isolated* point.

We shall need the following lemma ([19, p. 166]).

Lemma 7: Let V be an affine variety with the ideal

$$I(V) \subset F[x_1, \ldots, x_t].$$

Then for any $x = (a_1, \ldots, a_t) \in V$ and $f_1, \ldots, f_r \in I(V)$

$$\operatorname{rank} J_x(f) \leq t - \dim_x V.$$

The next lemma is a corollary to the classical Bezout's theorem ([16, p. 53]).

Lemma 8: Let V be an affine variety defined by (20). Then the number of isolated points on V does not exceed

$$\prod_{i=1}^{r} \deg f_i.$$

Let $\xi_1, \ldots, \xi_{t+1}$ be fixed nonzero elements of some finite field F_q. Consider a variety V in the algebraic closure of F_q defined by the following system of equations:

$$\begin{cases} \xi_1 x_1 + \ldots + \xi_t x_t + \xi_{t+1} = 0 \\ \xi_1 x_1^2 + \ldots + \xi_t x_t^2 + \xi_{t+1} = 0 \\ \qquad\qquad \vdots \\ \xi_1 x_1^t + \ldots + \xi_t x_t^t + \xi_{t+1} = 0. \end{cases} \tag{21}$$

Let $x = (a_1, \ldots, a_t)$ be an arbitrary point on V. We say that x is an *interesting* point if $a_i \neq a_j$ for all $i \neq j$.

Lemma 9: Let V be the variety defined by (21). Suppose $\operatorname{char} F_q > t$; then every interesting point on V is isolated.

Proof: Let $x = (a_1, \ldots, a_t)$ be an arbitrary interesting point on V. Let $f_i(x_1, \ldots, x_t)$ denote the left-hand side of the ith equation of (21). Consider the Jacobian of $\{f_i\}$ at point x

$$J_x(f_1, \ldots, f_t) = \begin{pmatrix} \xi_1 & \cdots & \xi_t \\ 2\xi_1 a_1 & \ldots & 2\xi_t a_t \\ \vdots & \ddots & \vdots \\ t\xi_1 a_1^{t-1} & \ldots & t\xi_t a_t^{t-1} \end{pmatrix}.$$

Thus, we have

$$\det J_x(f_1, \ldots, f_t) = t! \prod_{i=1}^{t} \xi_i \begin{vmatrix} 1 & \ldots & 1 \\ a_1 & \ldots & a_t \\ \vdots & \ddots & \vdots \\ a_1^{t-1} & \ldots & a_t^{t-1} \end{vmatrix}.$$

Using standard properties of the Vandermonde determinant and the facts that ξ_i are nonzero and $\operatorname{char} F_q > t$, we get

$$\operatorname{rank} J_x(f_1, \ldots, f_t) = t. \tag{22}$$

It is easy to see that $f_1, \ldots, f_t \in I(V)$. Combining (22) with Lemma 7, we obtain $\dim_x V = 0$. The proof is completed. □

Lemma 10: Let m be a prime $m > t!$. Assume $\operatorname{char} F_q > t$. Let V be the variety defined by (21). Suppose $x \in F_{q^m}^t$ is an interesting point on V; then $x \in F_q^t$. In other words, every interesting point on V that is rational over F_{q^m} is rational over F_q.

Proof: Assume the converse. Let $x = (a_1, \ldots, a_t)$ be an interesting point on V such that $x \in F_{q^m}^t \setminus F_q^t$. Consider the following m conjugate points:

$$p_i = (a_1^{q^i}, \ldots, a_t^{q^i}), \qquad \text{for all } 0 \leq i \leq m-1.$$

Each of the above points is interesting. Since m is a prime, the points are pairwise distinct. However, according to Lemma 9, every interesting point on V is isolated. Thus, we have $m > t!$ isolated point on V. This contradicts Lemma 8. □

Remark 11: Note that we can slightly weaken the condition of Lemma 10 replacing

$$m \text{ prime} \quad \text{and} \quad m > t!$$

with the following condition: $\forall s \neq 1$, $s | m$ implies $s > t!$.

Now we are ready to prove Theorem 4.

Proof: Assume C_{d-1} is nonempty (this fact will be proven later) and consider the locator set $X(c) = (x_1, \ldots, x_{d-1})$ for any $c \in C_{d-1}$. Recall that $X(c)$ satisfies the first $d-2$ equations in (14) where $\xi_i \neq 0$ for all i. Consider an affine permutation $\pi(x) = a + bx$ of the locator set F_{q^m} of the code C. Let $a, b \neq 0 \in F_{q^m}$ be such that

$$\pi(x_{d-2}) = 1 \quad \text{and} \quad \pi(x_{d-1}) = 0. \tag{23}$$

Let y_i denote $\pi(x_i)$. Now we again use the fact that code C (8) is invariant under affine permutations. Therefore, the new locator set $y(c) = (y_1, \ldots, y_{d-3}, 1, 0)$ satisfies similar equations

$$\begin{cases} \xi_1 + \cdots + \xi_{d-3} + \xi_{d-2} = -\xi_{d-1} \\ \xi_1 y_1 + \cdots + \xi_{d-3} y_{d-3} + \xi_{d-2} = 0 \\ \xi_1 y_1^2 + \cdots + \xi_{d-3} y_{d-3}^2 + \xi_{d-2} = 0 \\ \qquad\qquad \vdots \\ \xi_1 y_1^{d-3} + \cdots + \xi_{d-3} y_{d-3}^{d-3} + \xi_{d-2} = 0. \end{cases} \tag{24}$$

Now we remove the first equation (which does not include variables y_i) from (24), and obtain the system of equations, which is identical to system (21) for $t = d-3$. Recall that $x_1, \ldots, x_{d-1}$ are pairwise distinct elements of F_{q^m}. Therefore, $y_1, \ldots, y_{d-3}, 1, 0$ are also pairwise distinct. Thus, $y_1, \ldots, y_{d-3}$ is an interesting solution to the above system.

It is straightforward to verify that all the conditions of Lemma 10 hold. This yields

$$y_i = a + bx_i = \lambda_i \in F_q, \qquad \forall i \in [1, d-1].$$

Thus, we obtain all locators x_i on the affine line

$$x_i = -\frac{a}{b} + \frac{\lambda_i}{b}, \qquad \lambda_i \in F_q.$$

Finally, we prove that C_{d-1} is nonempty. Note that $\operatorname{char} F_q \geq d-2$. Also, recall that we consider codes $C_q^m(d-1)$ with constructive distance $d-1$, in which case q does not divide $d-2$. Thus, we now assume that $q \geq d-1$. Then we consider (24) taking $\xi_{d-1} = 1$ and arbitrarily choosing $d-3$ different locators $y_1, \ldots, y_{d-3}$ from $F_q \setminus \{0, 1\}$. Obviously, the resulting system of linear equations has nonzero solution $\xi_1, \ldots, \xi_{d-2}$. This gives the codeword of weight $d-1$ and completes the proof of Theorem 4. □

V. Conclusion

We have constructed an infinite family of nonbinary codes that reduce the asymptotic redundancy of BCH codes for any given alphabet size q and distance d if $q \geq d-1$. Families with such a property were earlier known only for distances $4, 5$, and 6 [6]. Even the shortest codes in our family have very big length $n \approx q^{(d-3)!}$, therefore, the construction is of theoretical interest.

The main question (i.e., the determination of the exact values of $c(q, d)$) remains open.

Acknowledgment

S. Yekhanin would like to express his deep gratitude to M. Sudan for introducing the problem to him and many helpful

discussions during this work. He would also like to thank J. Kelner for valuable advice.

REFERENCES

[1] R. Blahut, *Algebraic Codes for Data Transmission*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[2] A. R. Calderbank and P. C. Fishburn, "Maximal three-independent subsets of $\{0, 1, 2\}^n$," *Des., Codes Cryptogr.*, vol. 4, pp. 203–211, 1994.

[3] D. Danev and J. Olsson, "On a sequence of cyclic codes with minimum distance six," *IEEE Trans. Inform Theory*, vol. 46, pp. 673–674, Mar. 2000.

[4] I. I. Dumer and V. V. Zinoviev, "New maximal codes over Galois field GF(4)," *Probl. Pered. Inform. (Probl. Inform. Transm.)*, vol. 14, no. 3, pp. 24–34, 1978.

[5] I. I. Dumer, "Nonbinary codes with distances 4, 5, and 6 of cardinality greater than the BCH codes," *Probl. Pered. Inform. (Probl. Inform. Transm.)*, vol. 24, no. 3, pp. 42–54, 1988.

[6] ——, "Nonbinary double error-correcting codes designed by means of algebraic varieties," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1657–1666, Nov. 1995.

[7] Y. Edel and J. Bierbrauer, "Recursive constructions for large caps," *Bull. Belgian Math. Soc.—Simon Stevin*, vol. 6, pp. 249–258, 1999.

[8] Y. Edel, "Extensions of generalized product caps," *Des., Codes Cryptogr.*, vol. 31, pp. 5–14, 2004.

[9] G. L. Feng, X. Wu, and T. R. N. Rao, "New double-byte error-correcting codes for memory systems," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1152–1169, May 1998.

[10] ——, "New DbeC-TbeD codes better than Gilbert-Varshamov bound," in *Proc. IEEE Int. Symp. Information Theory*, Sorrento, Italy, June 2000, p. 32.

[11] P. Frankl, R. L. Graham, and V. Rödl, "On subsets of Abelian groups with no 3-term arithmetic progression," *J. Comb. Theory Ser. A*, vol. 45, pp. 157–161, 1987.

[12] D. N. Gevorkyan, A. M. Avetisyan, and V. A. Tigranyan, "On the construction of codes correcting two errors in Hamming metric over Galois fields" (in Russian), in *Vychislitel'naya Technika*. Kuibyshev, U.S.S.R.: Izvestiya Vuzov, 1975, pp. 19–21.

[13] D. N. Gevorkyan, "On nonbinary codes with fixed code distance" (in Russian), in *Proc. 5th Int. Symp. Information Theory*, Moscow–Tbilisi, U.S.S.R., 1979, pp. 93–96.

[14] D. Glynn and T. T. Tatau, "A 126-cap of PG(5,4) and its corresponding [126, 6, 88]-code," *Utilas Math.*, vol. 55, pp. 201–210, 1999.

[15] R. Lidl and H. Niederrieter, *Finite Fields*. Cambridge, U.K.: Cambridge Univ. Press, 1985.

[16] R. Hartshorne, *Algebraic Geometry*. New York: Springer, 1977.

[17] R. Hill, "On the largest size caps in $S_{5,3}$," *Rened. Acad. Naz. Lincei*, vol. 54, pp. 378–384, 1973.

[18] J. W. P. Hirschfeld and L. Storme, "The packing problem in statistics, coding theory and finite projective spaces: Update 2001," in *Developments in Mathematics*. Norwell, MA: Kluwer (Academic), vol. 3, Finite Geometries, pp. 201–246.

[19] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*. Boston, MA: Birkhäuser, 1985.

[20] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[21] R. Meshulam, "On subsets of finite abelian groups with no three term arithmetic progressions," *Journal of Comb. Theory A*, vol. 71, pp. 169–172, 1995.

[22] A. C. Mukhopadhyay, "Lower bounds for $m_t(r, s)$," *J. Comb. Theory A*, vol. 25, pp. 1–13, 1978.

[23] C. Roos, "A new lower bound for the minimum distance of a cyclic code," *IEEE Trans. Inform Theory*, vol. IT-29, pp. 330–332, May 1983.

[24] J. H. Van Lint and R. Wilson, "On the minimum distance of cyclic codes," *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 23–40, Jan. 1986.