On Constant-Composition Codes Over Z_q

Yuan Luo, Fang-Wei Fu, A. J. Han Vinck, *Senior Member, IEEE*, and Wende Chen

***Abstract*—A constant-composition code is a special constant-weight code under the restriction that each symbol should appear a given number of times in each codeword. In this correspondence, we give a lower bound for the maximum size of the q-ary constant-composition codes with minimum distance at least 3. This bound is asymptotically optimal and generalizes the Graham–Sloane bound for binary constant-weight codes. In addition, three construction methods of constant-composition codes are presented, and a number of optimum constant-composition codes are obtained by using these constructions.**

***Index Terms*—Code construction, constant-composition code, constant-weight code, Hadamard matrix, Johnson bound, Plotkin bound, simplex code.**

I. Introduction

Constant-weight codes play an important role in coding theory. Binary constant-weight codes have been extensively studied by many authors. For good survey papers, see Agrell *et al.* [2] and Brouwer *et al.* [5]. Nonbinary constant-weight codes and constant-composition codes have not received the same amount of attention, but recently there have been several papers dealing with these two topics (see [4], [8]–[10], [12], [18]–[23]). Research has been done in searching for good codes and finding good lower and upper bounds. Besides being of mathematical interest, nonbinary constant-weight codes and constant-composition codes are also useful in the construction of spherical codes for modulation, see [7].

In this correspondence, we study constant-composition codes. We first give a lower bound for the maximum size of the q-ary constant-composition codes with minimum distance at least 3. This lower bound is shown to be asymptotically optimal and generalizes the Graham–Sloane bound for binary constant-weight codes. Then, by extending and modifying the methods of Fu *et al.* [10] for constructing constant-weight codes, three concatenated constructions of constant-composition codes are presented, and a number of optimum constant-composition codes are obtained by using these concatenated constructions.

This correspondence is organized as follows. In Section II, we introduce some basic definitions and notations. We also review some basic properties which will be used in this correspondence. In Section III, we give a lower bound for the maximum size of the q-ary constant-composition codes with minimum distance at least 3. We show that this bound is asymptotically optimal. In Section IV, we construct a q-ary constant-composition code from a code over Z_m, by using a representation of Z_m as codewords of a q-ary constant-composition code. We show that some q-ary optimum constant-composition codes, which achieve the nonrecursive Johnson bound, can be constructed from some optimum codes over Z_m, which achieve the Plotkin bound. In Section V, we construct a q-ary constant-composition code from a constant-weight code over Z_m, by using a representation of nonzero elements of Z_m as codewords of a constant-composition code over $Z_q^* = \{1, \ldots, q-1\}$, and the zero element as a zero vector. We show that some q-ary optimum constant-composition codes can be constructed by using this method. In Section VI, we construct a q-ary constant-composition code from a constant-weight code over Z_m, by using a representation of nonzero elements of Z_m as codewords of a constant-composition code over Z_q, and the zero element as a repetition vector. We show that some q-ary optimum constant-composition codes can also be constructed by using this modified method. In Section VII, we summarize and conclude this correspondence.

Manuscript received August 30, 2001; revised October 24, 2002. This work was supported in part by the DSTA project (POD 0103223), the National Natural Science Foundation of China under Grant 60172060, the Trans-Century Training Program Foundation for the Talents by the Education Ministry of China, and the Foundation for University Key Teacher by the Education Ministry of China.

Y. Luo is with the Computer Science and Engineering Department, Shanghai Jiao Tong University, Shanghai 200030, China (e-mail: yluo@cs.sjtu.edu.cn).

F.-W. Fu is with the Temasek Laboratories, National University of Singapore, Singapore 119260, on leave from the Department of Mathematics, Nankai University, Tianjin 300071, China (e-mail: tslfufw@nus.edu.sg).

A. J. H. Vinck is with the Institute for Experimental Mathematics, Essen University, 45326 Essen, Germany (e-mail: vinck@exp-math.uni-essen.de).

W. Chen is with the Institute of Systems Science, Academy of Mathematics and System Sciences, Chinese Academy of Sciences, Beijing 100080, China (e-mail: xinmei@public3.bta.net.cn).

Communicated by J. J. Ashley, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2003.819339

II. Preliminary

Let $Z_q = \{0, 1, \ldots, q-1\}$ be the ring of integers modulo q. Let $V_n(q) = Z_q^n$ denote the set of n-tuples over Z_q. For any two n-tuples $\boldsymbol{a}, \boldsymbol{b} \in V_n(q)$, the Hamming distance $d_H(\boldsymbol{a}, \boldsymbol{b})$ is the number of components where they differ. The Hamming weight $w_H(\boldsymbol{a})$ is the number of nonzero components in $\boldsymbol{a}$. An $(n, M, d)_q$ code C is a subset of $V_n(q)$ with size M and Hamming distance at least d between any two distinct elements of C. Denote $A_q(n, d)$ as the maximal size of an $(n, M, d)_q$ code. Let $V_{n,w}(q)$ denote the set of n-tuples over Z_q of Hamming weight w. An $(n, M, d, w)_q$ constant-weight code C is a subset of $V_{n,w}(q)$ with size M and Hamming distance at least d between any two distinct elements of C. Denote $A_q(n, d, w)$ as the maximal size of an $(n, M, d, w)_q$ constant-weight code. Let $V_{[w_0,\ldots,w_{q-1}]}(q)$ denote the set of n-tuples over Z_q of the fixed composition $[w_0, \ldots, w_{q-1}]$, i.e., the number of 0's, 1's, $\ldots$, $(q-1)$'s in the n-tuple over Z_q is given by $w_0, w_1, \ldots, w_{q-1}$, respectively, where $n = w_0 + \cdots + w_{q-1}$. An $(n, M, d, [w_0, \ldots, w_{q-1}])_q$ constant-composition code C is a subset of $V_{[w_0,\ldots,w_{q-1}]}(q)$ with size M and Hamming distance at least d between any two distinct elements of C. Denote $A_q(n, d, [w_0, \ldots, w_{q-1}])$ as the maximal size of an $(n, M, d, [w_0, \ldots, w_{q-1}])_q$ constant-composition code. Note that the definitions of codes, constant-weight codes, and constant-composition codes still work if we use any finite set of size q instead of Z_q.

In order to establish our results in this correspondence, we need the following bounds in coding theory.

Lemma 1: Plotkin bound [17]

$$A_q(n, d) \le \frac{qd}{qd - n(q-1)}, \qquad \text{if } d > n(q-1)/q.$$

Note that, Bogdanova *et al.* (see [3, Theorem 3]) provided a slightly stronger version of Lemma 1.

Lemma 2: The nonrecursive Johnson bound for constant-weight codes [10]

$$A_q(n, d, w) \le \frac{nd}{nd - 2nw + \frac{q}{q-1}w^2}$$

if $nd - 2nw + \frac{q}{q-1}w^2 > 0$.

For ternary constant-weight codes, Svanström (see [18, Corollary 3.16]) gave a slightly stronger version of Lemma 2. In the following we have a nonrecursive Johnson bound for constant-composition codes, which is an analog of Lemma 2. For ternary constant-composition

codes, Svanström *et al.* (see [22, Theorem 5]) also gave a slightly stronger version of Lemma 3.

Lemma 3: The nonrecursive Johnson bound for constant-composition codes

$$A_q(n,d,[w_0,\ldots,w_{q-1}]) \le \frac{nd}{nd-n^2+(w_0^2+\cdots+w_{q-1}^2)}$$

if $nd-n^2+(w_0^2+\cdots+w_{q-1}^2)>0$.

Proof: Let C be an $(n,M,d,[w_0,\ldots,w_{q-1}])_q$ constant-composition code. Denote

$$S=\sum_{\boldsymbol{a},\boldsymbol{b}\in C} d_H(\boldsymbol{a},\boldsymbol{b}).$$

Since the distance between any two distinct codewords is at least d, then

$$M(M-1)d \le S. \tag{1}$$

Let k_{ij} be the number of symbols $j\in Z_q$ at the ith $(0\le i\le n-1)$ component of all the codewords of C. Then

$$\sum_{j=0}^{q-1} k_{ij}=M \quad \text{and} \quad \sum_{i=0}^{n-1} k_{ij}=Mw_j. \tag{2}$$

By using the Cauchy–Schwartz inequality, we have

$$\sum_{i=0}^{n-1} k_{ij}^2 \ge \frac{1}{n}\left(\sum_{i=0}^{n-1} k_{ij}\right)^2=\frac{M^2w_j^2}{n}. \tag{3}$$

It is not hard to see that

$$S=\sum_{i=0}^{n-1}\sum_{j=0}^{q-1} k_{ij}(M-k_{ij}). \tag{4}$$

By using (2)–(4), we have

$$S=nM^2-\sum_{j=0}^{q-1}\sum_{i=0}^{n-1} k_{ij}^2 \le nM^2-\sum_{j=0}^{q-1}\frac{M^2w_j^2}{n}. \tag{5}$$

Expressions (1) and (5) yield that

$$(M-1)d \le nM-\sum_{j=0}^{q-1}\frac{Mw_j^2}{n}.$$

Solving this inequality for M, Lemma 3 follows. □

Remark: We know that in Lemmas 1 and 2, if the equalities hold, then the corresponding optimum codes must be equidistant. It is easy to see that the same conclusion is true for Lemma 3.

Lemma 4: The recursive Johnson bound for constant-composition codes [22]

$$A_q(n,d,[w_0,\ldots,w_{q-1}]) \le \frac{n}{w_r}A_q(n-1,d,[w_0^{(r)},\ldots,w_{q-1}^{(r)}])$$

for $0\le r\le q-1$, where $w_j^{(r)}=w_j-1$ if $j=r$, and $w_j^{(r)}=w_j$ if $j\ne r$.

III. A Lower Bound for $A_q(n,3,[w_0,\ldots,w_{q-1}])$

Graham and Sloane [11] derived a lower bound for binary constant-weight codes with minimum distance at least four, i.e.,

$$A_2(n,4,w) \ge \binom{n}{w}/n. \tag{6}$$

This lower bound was improved by van Pul and Etzion [24] and Kløve [15] in some cases. By extending and modifying the methods of Graham and Sloane [11] and Kløve [15], Svanström [20] derived a lower bound for ternary constant-weight codes with minimum distance at least 3. This bound was generalized and improved in some cases by Fu, Kløve, Luo, and Wei [8]. Svanström [18] also derived a lower bound for ternary constant-composition codes with minimum distance at least 3, i.e.,

$$A_3(n,3,[w_0,w_1,w_2]) \ge \binom{n}{w_0,w_1,w_2}/(2n-1).$$

In this section, we derive a lower bound for q-ary constant-composition codes with minimum distance at least 3. This lower bound generalizes the Graham–Sloane bound for binary constant-weight codes and improves the Svanström bound for ternary constant-composition codes. Denote

$$\binom{n}{w_0,\ldots,w_{q-1}}=\frac{n!}{w_0!\cdots w_{q-1}!}$$

as the multinomial coefficient where $n=w_0+\cdots+w_{q-1}$. If $q=2$, denote

$$\binom{n}{w_0}=\binom{n}{w_0,w_1}.$$

Let $\gcd(\alpha,\beta)$ be the greatest common divisor of the positive integers α and β. Denote

$$Q=\prod_{\substack{p \text{ is prime}\\ p\le q-1}} p, \qquad \text{for } q\ge 3 \tag{7}$$

and

$$L(s,q)=\min\{l: l\ge s \text{ and } \gcd(l,Q)=1\}, \qquad \text{for } 0\le s\le Q-1. \tag{8}$$

It is easy to see that $Q-1\ge L(s,q)\ge s$. In particular, for $q=2$, denote $Q=1$ and $L(0,2)=0$.

Theorem 1:

$$A_q(n,3,[w_0,\ldots,w_{q-1}]) \ge \binom{n}{w_0,\ldots,w_{q-1}}/(n+\Gamma(t_n,q)) \tag{9}$$

where t_n is the least nonnegative integer such that $t_n\equiv n \pmod Q$, and $\Gamma(t_n,q)=L(t_n,q)-t_n$.

Proof: Recall that $V_{[w_0,\ldots,w_{q-1}]}(q)$ is the set of n-tuples over Z_q of the fixed composition $[w_0,\ldots,w_{q-1}]$. It is easy to see that $d_H(\boldsymbol{a},\boldsymbol{b})\ge 2$ for any two distinct elements $\boldsymbol{a}$ and $\boldsymbol{b}$ in $V_{[w_0,\ldots,w_{q-1}]}(q)$. We show that $V_{[w_0,\ldots,w_{q-1}]}(q)$ can be partitioned into $n+\Gamma(t_n,q)$ parts C_m $(0\le m<n+\Gamma(t_n,q))$, and the minimum distance of each part C_m is at least 3. The theorem follows from the fact that the right-hand side of (9) is the average size of C_m.

Suppose $q\ge 3$. Let $Z_{n+\Gamma(t_n,q)}$ be the residue classes modulo $n+\Gamma(t_n,q)$. Let T be the map

$$T: V_{[w_0,\ldots,w_{q-1}]}(q) \longrightarrow Z_{n+\Gamma(t_n,q)}$$

such that for $\boldsymbol{a}=(a_0,\ldots,a_{n-1})\in V_{[w_0,\ldots,w_{q-1}]}(q)$

$$T(\boldsymbol{a})\equiv \sum_{r=1}^{q-1} r\sum_{a_j=r} j \pmod{n+\Gamma(t_n,q)}.$$

For any $m\in Z_{n+\Gamma(t_n,q)}$, denote $C_m=T^{-1}(m)$. Below we show that the minimum distance of C_m is at least 3, i.e., $d_H(\boldsymbol{a},\boldsymbol{b})\ge 3$ for any two distinct elements $\boldsymbol{a}=(a_0,\ldots,a_{n-1})$, $\boldsymbol{b}=(b_0,\ldots,b_{n-1})\in C_m$. Hence, C_m is an $(n,|C_m|,3,[w_0,\ldots,w_{q-1}])_q$ constant-composition code.

Suppose $d_H(\boldsymbol{a},\boldsymbol{b})=2$, then $\boldsymbol{a}$ and $\boldsymbol{b}$ differ in exactly two positions i and j $(i<j)$. Without loss of generality we may assume that $a_i<b_i$. Hence, one of the following two cases occurs:

a) $(a_i,a_j)=(0,u),(b_i,b_j)=(u,0)$ where $u>0$;

b) $(a_i,a_j)=(u,v),(b_i,b_j)=(v,u)$ where $v>u>0$.

It follows from $T(\boldsymbol{a}) = T(\boldsymbol{b}) = m$ that in case a)

$$u(j-i) \equiv 0 \pmod{n + \Gamma(t_n, q)}$$

and in case b)

$$(v-u)(j-i) \equiv 0 \pmod{n + \Gamma(t_n, q)}.$$

Since

$$\begin{aligned}\gcd(n + \Gamma(t_n, q), Q) &= \gcd(t_n + \Gamma(t_n, q), Q) \\ &= \gcd(L(t_n, q), Q) \\ &= 1\end{aligned}$$

and $0 < u < v \leq q-1$, we have

$$\gcd(n + \Gamma(t_n, q), u) = \gcd(n + \Gamma(t_n, q), v-u) = 1.$$

Hence, in both cases, $n + \Gamma(t_n, q) | (j-i)$, which is impossible. Therefore, $d_H(\boldsymbol{a}, \boldsymbol{b}) \geq 3$.

For $q = 2$, denote $Q = 1$ and $L(0, 2) = 0$. By using the same arguments as above, the corresponding result is obtained, which is given by the Graham–Sloane bound (see (6)). Note that, for $q = 2$, the case b) does not exist. □

From the proof of Theorem 1, it is easy to get the following corollary.

Corollary 1:

$$A_q(n, 3, [w_0, \ldots, w_{q-1}]) \geq \max_{m \in Z_{n+\Gamma(t_n, q)}} |C_m|. \tag{10}$$

The Bound (10) is, in general, stronger than the bound (9), but it is less explicit and requires more computation to determine. The following corollaries can be obtained from Theorem 1 immediately.

Corollary 2: Let Q be given by (7). If $gcd(n, Q) = 1$, then

$$A_q(n, 3, [w_0, \ldots, w_{q-1}]) \geq \binom{n}{w_0, \ldots, w_{q-1}} / n. \tag{11}$$

Proof: Since $\gcd(n, Q) = 1$, we have

$$\gcd(t_n, Q) = \gcd(n, Q) = 1.$$

It follows from (8) that $L(t_n, q) = t_n$. Hence, $\Gamma(t_n, q) = L(t_n, q) - t_n = 0$ and Corollary 2 follows from Theorem 1. □

Corollary 3: Let Q be given by (7). If there is an integer r such that $1 \leq r < q$ and $n \equiv -r \pmod{Q}$, then

$$A_q(n, 3, [w_0, \ldots, w_{q-1}]) \geq \binom{n}{w_0, \ldots, w_{q-1}} / (n + r - 1). \tag{12}$$

Proof: For $1 \leq r < q$, we have $L(Q-r, q) = Q-1$ since

$$\gcd(l, Q) = \gcd(Q-l, Q) \neq 1 \text{ for } Q-1 > l \geq Q-r.$$

Thus, $\Gamma(Q-r, q) = r-1$. Therefore, $\Gamma(t_n, q) = r-1$ since $t_n = Q-r$. □

Corollary 4: For $q = 3$

$$A_3(n, 3, [w_0, w_1, w_2]) \geq \begin{cases} \binom{n}{w_0, w_1, w_2} / n, & n = 2k+1 \\ \binom{n}{w_0, w_1, w_2} / (n+1), & n = 2k. \end{cases}$$

Proof: For $q = 3$, we have $Q = 2$. Then this corollary follows from Corollary 3. □

Corollary 5: For $q = 4$

$$A_4(n, 3, [w_0, w_1, w_2, w_3]) \geq \begin{cases} \binom{n}{w_0, w_1, w_2, w_3} / n, & n = 6k+1 \text{ or } 6k+5 \\ \binom{n}{w_0, w_1, w_2, w_3} / (n+1), & n = 6k \text{ or } 6k+4 \\ \binom{n}{w_0, w_1, w_2, w_3} / (n+2), & n = 6k+3 \\ \binom{n}{w_0, w_1, w_2, w_3} / (n+3), & n = 6k+2. \end{cases}$$

Proof: For $q = 4$, we have $Q = 6$. For the cases of $n = 6k+5$, $6k+4$, or $6k+3$, the proof follows from Corollary 3. For other cases of n, the proof follows from $\Gamma(0, 4) = 1$, $\Gamma(1, 4) = 0$, and $\Gamma(2, 4) = 3$, respectively. □

Remark: Since $n + Q - 1 \geq n + \Gamma(t_n, q)$, it follows from Theorem 1 that

$$A_q(n, 3, [w_0, \ldots, w_{q-1}]) \geq \binom{n}{w_0, \ldots, w_{q-1}} / (n + Q - 1). \tag{13}$$

This explicit bound is used below to show that the lower bound (9) in Theorem 1 coincides asymptotically with the true value $A_q(n, 3, [w_0, \ldots, w_{q-1}])$ as $n \to \infty$.

For a constant-composition code with length n, minimum distance at least d, and constant composition $[w_0, \ldots, w_{q-1}]$, denote $\delta = \lfloor (d-1)/2 \rfloor$. Then $\delta < w_1 + \cdots + w_{q-1}$. Let $\delta_{0,0}, \ldots, \delta_{0,q-1}$ be the nonnegative integers such that $\delta_{0,0} = 0$, $\delta_{0,0} + \cdots + \delta_{0,q-1} = \delta$, and $\delta_{0,l} \leq w_l$ for $0 \leq l \leq q-1$. Note that

$$A_q(w_0 + \delta, d, [w_0, \delta_{0,1}, \ldots, \delta_{0,q-1}]) = 1.$$

It follows from Lemma 4 that

$$\begin{aligned} &A_q(n, d, [w_0, \ldots, w_{q-1}]) \\ &\quad \leq \frac{n(n-1)\cdots(w_0+\delta+1)}{\prod_{l=1}^{q-1} w_l(w_l-1)\cdots(\delta_{0,l}+1)} \\ &\qquad \times A_q(w_0+\delta, d, [w_0, \delta_{0,1}, \ldots, \delta_{0,q-1}]) \\ &\quad = \frac{n(n-1)\cdots(w_0+\delta+1)}{\prod_{l=1}^{q-1} w_l(w_l-1)\cdots(\delta_{0,l}+1)} \\ &\quad = \frac{n!}{(w_0+\delta)!} \prod_{l=1}^{q-1} \frac{\delta_{0,l}!}{w_l!} \\ &\quad = \binom{n}{w_0, \ldots, w_{q-1}} \Big/ \binom{w_0+\delta}{w_0, \delta_{0,0}, \ldots, \delta_{0,q-1}}. \end{aligned} \tag{14}$$

By using the same arguments for proving (14), we have the following.

Lemma 5: For any fixed i where $0 \leq i \leq q-1$, we have

$$\begin{aligned} &A_q(n, d, [w_0, \ldots, w_{q-1}]) \\ &\qquad \leq \binom{n}{w_0, \ldots, w_{q-1}} \Big/ \binom{w_i+\delta}{w_i, \delta_{i,0}, \ldots, \delta_{i,q-1}} \end{aligned} \tag{15}$$

where $\delta_{i,0}, \ldots, \delta_{i,q-1}$ are nonnegative integers such that $\delta_{i,i} = 0$, $\delta_{i,0} + \cdots + \delta_{i,q-1} = \delta$, and $\delta_{i,l} \leq w_l$ for $0 \leq l \leq q-1$. In particular, for $d = 3$, we have

$$A_q(n, 3, [w_0, \ldots, w_{q-1}]) \leq \binom{n}{w_0, \ldots, w_{q-1}} / (w_i + 1). \tag{16}$$

Proposition 1: If we fix any $q-1$ components of the q-tuple $[w_0,\ldots,w_{q-1}]$, then the lower bound in Theorem 1 coincides asymptotically with $A_q(n,3,[w_0,\ldots,w_{q-1}])$ as $n\to\infty$.

Proof: Without loss of generality, we may assume that $w_1,\ldots,w_{q-1}$ are fixed. It follows from (13), (16), and Theorem 1 that

$$\begin{aligned}1 &\geq \frac{\binom{n}{w_0,\ldots,w_{q-1}}/(n+\Gamma(t_n,q))}{A_q(n,3,[w_0,\ldots,w_{q-1}])}\\ &\geq \frac{\binom{n}{w_0,\ldots,w_{q-1}}/(n+Q-1)}{A_q(n,3,[w_0,\ldots,w_{q-1}])}\\ &\geq \frac{w_0+1}{n+Q-1}\\ &= \frac{n-(w_1+\cdots+w_{q-1})+1}{n+Q-1}.\end{aligned}$$

Therefore,

$$\lim_{n\to\infty}\frac{\binom{n}{w_0,\ldots,w_{q-1}}/(n+\Gamma(t_n,q))}{A_q(n,3,[w_0,\ldots,w_{q-1}])}=1.$$

This completes the proof. □

IV. Construction A

In this section, a concatenated Construction A is presented to build constant-composition codes. We construct a q-ary constant-composition code from a code over Z_m, by using a representation of Z_m as codewords of a q-ary constant-composition code. We show that some q-ary optimum constant-composition codes, which achieve the nonrecursive Johnson bound, can be constructed from optimum codes over Z_m, which achieve the Plotkin bound.

Construction A: Let C^1 be an $(n_1,M,d_1)_m$ code over Z_m and C^2 be an $(n_2,m,d_2,[w_0,\ldots,w_{q-1}])_q$ constant-composition code over Z_q. Let $f: Z_m\to C^2$ be a one-to-one mapping. Denote

$$C(C^1,C^2,f)=\{(f(c_0),\ldots,f(c_{n_1-1})):(c_0,\ldots,c_{n_1-1})\in C^1\}.$$

Then it is easy to verify that $C(C^1,C^2,f)$ is an

$$(n_1n_2,M,d_1d_2,[n_1w_0,\ldots,n_1w_{q-1}])_q$$

constant-composition code over Z_q.

By using Construction A, a relation between the maximum size of an unrestricted code and the maximum size of a constant-composition code can be obtained as immediately follows.

Proposition 2: If $A_q(n_2,d_2,[w_0,\ldots,w_{q-1}])\geq m$, then

$$A_m(n_1,d_1)\leq A_q(n_1n_2,d_1d_2,[n_1w_0,\ldots,n_1w_{q-1}]).$$

It is easy to see that a number of optimum constant-composition codes achieving the nonrecursive Johnson bound can be obtained by using Construction A.

Theorem 2: In Construction A, if the outer code C^1 is an optimum code achieving the Plotkin bound (see Lemma 1), and the inner code C^2 is an optimum constant-composition code achieving the nonrecursive Johnson bound (see Lemma 3), then $C(C^1,C^2,f)$ is an

$$(n_1n_2,M,d_1d_2,[n_1w_0,\ldots,n_1w_{q-1}])_q$$

optimum constant-composition code achieving the nonrecursive Johnson bound.

Then how to select the inner codes and the outer codes in Theorem 2? In this section, we use the following optimum constant-composition codes, which achieve the nonrecursive Johnson bound, as the inner codes in Construction A. These codes were given by Svanström,Östergård, and Bogdanova (see [18] and [22]).

Lemma 6 (see [18] and [22]):

1)
$$\begin{aligned}A_3(9,6,[5,2,2])&=9\\ A_3(8,6,[3,3,2])&=8\\ A_3(10,7,[6,2,2])&=5.\end{aligned}$$

2) $A_q(q,q,[1,\ldots,1])=q$.

3) $A_3(q,\frac{q+3}{2},[\frac{q-1}{2},\frac{q-1}{2},1])=q$, where q is an odd prime power.

Note that the ternary constant-composition code in item 3) is constructed by using the row vectors of the Jacobsthal matrix (see [16, p. 47]).

It is known that the $\left[\frac{q^k-1}{q-1},k,q^{k-1}\right]$ simplex code over GF(q), i.e., the dual code of the Hamming code over GF(q), achieves the Plotkin bound. By using the $\left[\frac{q^k-1}{q-1},k,q^{k-1}\right]$ simplex code over GF(q) as the outer code, and the codes in Lemma 6 as the inner codes, the following proposition follows from Theorem 2.

Proposition 3:

1) $A_3(9n,\,6\cdot 9^{k-1},[5n,2n,2n])=9^k$, where $n=(9^k-1)/8$;
$A_3(8n,\,6\cdot 8^{k-1},[3n,3n,2n])=8^k$, where $n=(8^k-1)/7$;
$A_3(10n,\,7\cdot 5^{k-1},[6n,2n,2n])=5^k$, where $n=(5^k-1)/4$.

2) $A_q(q\,n,\,q^k,[n,\ldots,n])=q^k$, where $n=\frac{q^k-1}{q-1}$ and q is a prime power.

3) $A_3(qn,\frac{q+3}{2}\cdot q^{k-1},[\frac{q-1}{2}n,\frac{q-1}{2}n,n])=q^k$, where $n=\frac{q^k-1}{q-1}$ and q is an odd prime power.

One way to construct optimum codes, which achieve the Plotkin bound, is to use the generalized Hadamard matrix introduced by Drake [6]. Let G be an Abelian group of order s and $H=[h_{i,j}]$ be a square matrix of order r whose entries are elements of G. The matrix H is called a generalized Hadamard matrix GH(r,s) if for $i\neq l$, the sequence $\{h_{i,j}-h_{l,j}:1\leq j\leq r\}$ contains every element of G equally often. Suppose $r=ts$, then every element of G occurs t times in the above sequence. Jungnickel [14] showed that the columns of GH(r,s) also have the same property as its rows. If there exists a generalized Hadamard matrix GH(r,s), then every entry of the first row and column can be taken as 0. By removing the first column, the row vectors of the corresponding matrix consist of an $(r-1,r,r-t)_s$ code. Note that $r=ts$, it is easy to verify that this code achieves the Plotkin bound. Hence, $A_s(r-1,r-t)=r$ if GH(r,s) exists.

Now two kinds of GH(r,s) matrices (see [6] and [14]) are useful here. One is GH$(2^mp^k,p)$, where p is prime, $0\leq m\leq k$, and $k\neq 0$. Another is GH$(2q,q)$, where q is an odd prime power. From the preceding discussion, we obtain two classes of codes achieving the Plotkin bound.

Lemma 7:

1) $A_p(n,(1-p^{-1})(n+1))=n+1$, where $n=2^mp^k-1$, p is prime, $0\leq m\leq k$, and $k\neq 0$.

2) $A_q(n,(1-q^{-1})(n+1))=n+1$, where q is an odd prime power and $n=2q-1$.

By using the codes in Lemma 7 as the outer codes, and the codes in Lemma 6 as the inner codes, the following proposition follows from Theorem 2.

Proposition 4:

1) $A_3(10n, 28(n+1)/5, [6n, 2n, 2n]) = n+1$, where $n = 2^m 5^k - 1$, $0 \le m \le k$, and $k \ne 0$; $A_3(153, 96, [85, 34, 34]) = 18$
2) $A_p(pn, (p-1)(n+1), [n, \ldots, n]) = n+1$, where $n = 2^m p^k - 1$, p is prime, $0 \le m \le k$, and $k \ne 0$.
3) $A_q(qn, (q-1)(n+1), [n, \ldots, n]) = n+1$, where $n = 2q-1$ and q is an odd prime power.
4) $A_3(pn, \frac{p+3}{2}(1-p^{-1})(n+1), [\frac{p-1}{2}n, \frac{p-1}{2}n, n]) = n+1$, where $n = 2^m p^k - 1$, p is an odd prime, $0 \le m \le k$, and $k \ne 0$.
5) $A_3(qn, \frac{q+3}{2}(1-q^{-1})(n+1), [\frac{q-1}{2}n, \frac{q-1}{2}n, n]) = n+1$, where $n = 2q-1$ and q is an odd prime power.

Note that, in Proposition 4, item 3) is not a special case of item 2). Item 5) is also not a special case of item 4).

V. Construction B

The second concatenated construction for constant-composition codes is given in this section. We construct a q-ary constant-composition code from a constant-weight code over Z_m, by using a representation of nonzero elements of Z_m as codewords of a constant-composition code over $Z_q^* = \{1, \ldots, q-1\}$, and the zero element as a zero vector. We show that some q-ary optimum constant-composition codes can be constructed by using this method.

Construction B: Let C^3 be an $(n_1, M, d_1, w)_m$ constant-weight code over Z_m, and C^4 be an $(n_2, m-1, d_2, [w_1, \ldots, w_{q-1}])_{q-1}$ constant-composition code over $Z_q^* = \{1, \ldots, q-1\}$. Let $f: \{1, \ldots, m-1\} \to C^4$ be a one-to-one mapping. Denote

$$C(C^3, C^4, f) = \{(g(c_0), \ldots, g(c_{n_1-1})) : (c_0, \ldots, c_{n_1-1}) \in C^3\}$$

where $g(\alpha) = f(\alpha)$ for $\alpha \in \{1, \ldots, m-1\}$, and $g(0) = [0]^{n_2}$. Then it is easy to verify that $C(C^3, C^4, f)$ is a q-ary constant-composition code with size M, length $n_1 n_2$, and constant-composition $[(n_1 - w)n_2, ww_1, \ldots, ww_{q-1}]$.

For any two vectors $\boldsymbol{x}, \boldsymbol{y}$, let

$$l(\boldsymbol{x}, \boldsymbol{y}) = |\{i : x_i = 0, y_i \ne 0\}|$$
$$l^*(\boldsymbol{x}, \boldsymbol{y}) = |\{i : x_i \ne 0, y_i \ne 0, x_i \ne y_i\}|.$$

Since C^3 is a constant-weight code, then for $\boldsymbol{x}, \boldsymbol{y} \in C^3$, we have $l(\boldsymbol{x}, \boldsymbol{y}) = l(\boldsymbol{y}, \boldsymbol{x})$ and

$$d_H(\boldsymbol{x}, \boldsymbol{y}) = l(\boldsymbol{x}, \boldsymbol{y}) + l(\boldsymbol{y}, \boldsymbol{x}) + l^*(\boldsymbol{x}, \boldsymbol{y}) = 2l(\boldsymbol{x}, \boldsymbol{y}) + l^*(\boldsymbol{x}, \boldsymbol{y}).$$

Denote

$$\begin{aligned} d_B &= \min\{2l(\boldsymbol{x}, \boldsymbol{y})n_2 + l^*(\boldsymbol{x}, \boldsymbol{y})d_2 : \boldsymbol{x} \ne \boldsymbol{y} \in C^3\} \\ &= \min\{2l(\boldsymbol{x}, \boldsymbol{y})(n_2 - d_2) + d_H(\boldsymbol{x}, \boldsymbol{y})d_2 : \boldsymbol{x} \ne \boldsymbol{y} \in C^3\}. \end{aligned}$$

Obviously, $d_B \ge d_1 d_2$. It is not difficult to see that the minimum distance of $C(C^3, C^4, f)$ is at least d_B. If C^4 is equidistant, i.e., $d_2 = d_H(\boldsymbol{a}, \boldsymbol{b})$ for any $\boldsymbol{a} \ne \boldsymbol{b} \in C^4$, then the minimum distance of $C(C^3, C^4, f)$ is given by

$$d_B = \min\{2l(\boldsymbol{x}, \boldsymbol{y})(n_2 - d_2) + d_H(\boldsymbol{x}, \boldsymbol{y})d_2 : \boldsymbol{x} \ne \boldsymbol{y} \in C^3\}. \quad (17)$$

Furthermore, if C^3 is also equidistant, i.e., $d_1 = d_H(\boldsymbol{x}, \boldsymbol{y})$ for any $\boldsymbol{x} \ne \boldsymbol{y} \in C^3$, then the minimum distance of $C(C^3, C^4, f)$ is given by

$$d_B = d_1 d_2 + 2(n_2 - d_2)\min\{l(\boldsymbol{x}, \boldsymbol{y}) : \boldsymbol{x} \ne \boldsymbol{y} \in C^3\}. \quad (18)$$

Example 1: Suppose m is a prime power. In Construction B, let $C^3 = S_m(k)\backslash\{\boldsymbol{0}\}$ where $S_m(k)$ is the $[\frac{m^k-1}{m-1}, k, m^{k-1}]$ simplex code over GF(m). Then C^3 is an

$$\left(\frac{m^k - 1}{m-1}, m^k - 1, m^{k-1}, m^{k-1}\right)_m$$

constant-weight code over GF(m). Let C^4 consist of all cyclic shifts of the vector $(1, 2, \ldots, 2)$ with length $m-1$. Then C^4 is an $(m-1, m-1, 2, [1, m-2])_2$ constant-composition code over $\{1, 2\}$. It is easy to see that both C^3 and C^4 are equidistant codes. Hence, $C(C^3, C^4, f)$ is a ternary constant-composition code with length $m^k - 1$, size $m^k - 1$, and constant-composition $[m^{k-1} - 1, m^{k-1}, (m-2)m^{k-1}]$. Since the simplex code $S_m(k)$ is linear, then

$$\min\{l(\boldsymbol{x}, \boldsymbol{y}) : \boldsymbol{x} \ne \boldsymbol{y} \in C^3\} = 0.$$

Since C^3 and C^4 are equidistant codes, it follows from (18) that the minimum distance of $C(C^3, C^4, f)$ is $d_B = 2m^{k-1}$.

Example 2: Suppose $q = 2^m$ such that $q - 1$ is a prime. In Construction B, let $C^3 = S_q(k)\backslash\{\boldsymbol{0}\}$ where $S_q(k)$ is the $[\frac{q^k-1}{q-1}, k, q^{k-1}]$ simplex code over GF(q). Then C^3 is a

$$\left(\frac{q^k - 1}{q-1}, q^k - 1, q^{k-1}, q^{k-1}\right)_q$$

constant-weight code over GF(q). Let C^4 consist of the row vectors of the $(q-1) \times (q-1)$ Jacobsthal matrix (see [16, p. 47]). Then C^4 can be considered as a

$$\left(q-1, q-1, \frac{q+2}{2}, \left[\frac{q-2}{2}, \frac{q-2}{2}, 1\right]\right)_3$$

constant-composition code over $\{1, 2, 3\}$. It is easy to see that both C^3 and C^4 are equidistant codes. Hence, $C(C^3, C^4, f)$ is a quaternary constant-composition code with length $q^k - 1$, size $q^k - 1$, and constant composition

$$\left[q^{k-1} - 1, \frac{q-2}{2}q^{k-1}, \frac{q-2}{2}q^{k-1}, q^{k-1}\right].$$

In the same way as Example 1, the minimum distance of $C(C^3, C^4, f)$ is given by $d_B = \frac{q+2}{2}q^{k-1}$.

From Construction B, a relation between the maximum size of a constant-weight code and the maximum size of a constant-composition code can be obtained immediately.

Proposition 5: If $A_{q-1}(n_2, d_2, [w_1, \ldots, w_{q-1}]) \ge m-1$, then

$$A_m(n_1, d_1, w) \le A_q(n_1 n_2, d_1 d_2, [(n_1 - w)n_2, ww_1, \ldots, ww_{q-1}]).$$

In the following, we show that some optimum constant-composition codes can be obtained by using Construction B.

Theorem 3: In Construction B, if the outer code C^3 is an optimum constant-weight code achieving the nonrecursive Johnson bound (see Lemma 2), and the inner code C^4 is an optimum constant-composition code achieving the nonrecursive Johnson bound (see Lemma 3), then for $n_2 = d_2$, $C(C^3, C^4, f)$ is an

$$(n_1 n_2, M, d_1 d_2, [(n_1 - w)n_2, ww_1, \ldots, ww_{q-1}])_q$$

constant-composition code achieving the nonrecursive Johnson bound.

Proof: Since C^3 and C^4 achieve the nonrecursive Johnson bounds for constant-weight codes and constant-composition codes, respectively, then we have an expression for the size M and an expression for the size $m-1$, respectively. The proof follows from substituting m into the expression for M.

Note that C^3 and C^4 are both equidistant. Hence, by using (18), $C(C^3, C^4, f)$ is also an equidistant code with minimum distance $d_B = d_1 d_2$ since $n_2 = d_2$. □

By using Theorem 3, we can also get some optimum constant-composition codes which achieve the nonrecursive Johnson bound.

Proposition 6:

$$A_q(q^k - 1, q^{k-1}(q-1), [q^{k-1} - 1, q^{k-1}, \ldots, q^{k-1}]) = q^k - 1$$

where q is a prime power.

Proof: In Construction B, let $C^3 = S_q(k) \backslash \{\mathbf{0}\}$ where $S_q(k)$ is the $\left[\frac{q^k-1}{q-1}, k, q^{k-1}\right]$ simplex code over GF (q). Then C^3 is a

$$\left(\frac{q^k-1}{q-1}, q^k - 1, q^{k-1}, q^{k-1}\right)_q$$

constant-weight code over GF (q), which achieves the nonrecursive Johnson bound (see Lemma 2). Let C^4 consist of the cyclic shifts of the vector $(1, 2, \ldots, q-1)$. Then C^4 is a

$$(q-1, q-1, q-1, [1, 1, \ldots, 1])_{q-1}$$

constant-composition code over $\{1, 2, \ldots, q-1\}$, which achieves the nonrecursive Johnson bound (see Lemma 3). By using Theorem 3, we obtain an optimum constant-composition code over GF (q) with length $q^k - 1$, size $q^k - 1$, minimum distance $q^{k-1}(q-1)$, and constant composition $[q^{k-1} - 1, q^{k-1}, \ldots, q^{k-1}]$. □

VI. Construction C

The third concatenated construction for constant-composition codes is presented here. We construct a q-ary constant-composition code from a constant-weight code over Z_m, by using a representation of nonzero elements of Z_m as codewords of a constant-composition code over Z_q, and the zero element as a repetition vector. We show that some q-ary optimum constant-composition codes can also be constructed by using this modified method.

Construction C: Let C^5 be an $(n_1, M, d_1, w)_m$ constant-weight code over Z_m, and C^6 be an $(n_2, m-1, d_2, [w_0, \ldots, w_{q-1}])_q$ constant-composition code over Z_q. Let $f : \{1, \ldots, m-1\} \to C^6$ be a one-to-one mapping. For fixed $l \in Z_q$, denote

$$C(C^5, C^6, f) = \{(g(c_0), \ldots, g(c_{n_1-1})) : (c_0, \ldots, c_{n_1-1}) \in C^5\}$$

where $g(\alpha) = f(\alpha)$ for $\alpha \in \{1, \ldots, m-1\}$, and $g(0) = [l]^{n_2}$. Then it is easy to verify that $C(C^5, C^6, f)$ is a q-ary constant-composition code with length $n_1 n_2$, size M, and constant composition

$$[ww_0, \ldots, ww_{l-1}, (n_1 - w)n_2 + ww_l, ww_{l+1}, \ldots, ww_{q-1}].$$

Since C^5 is a constant-weight code, then for $\boldsymbol{x}, \boldsymbol{y} \in C^5$, we have $d_H(\boldsymbol{x}, \boldsymbol{y}) = 2l(\boldsymbol{x}, \boldsymbol{y}) + l^*(\boldsymbol{x}, \boldsymbol{y})$. Denote

$$\begin{aligned} d_C &= \min\{2l(\boldsymbol{x}, \boldsymbol{y})(n_2 - w_l) + l^*(\boldsymbol{x}, \boldsymbol{y})d_2 : \boldsymbol{x} \neq \boldsymbol{y} \in C^5\} \\ &= \min\{2l(\boldsymbol{x}, \boldsymbol{y})(n_2 - d_2 - w_l) + d_H(\boldsymbol{x}, \boldsymbol{y})d_2 : \boldsymbol{x} \neq \boldsymbol{y} \in C^5\}. \end{aligned} \tag{19}$$

It is not difficult to see that the minimum distance of $C(C^5, C^6, f)$ is at least d_C. If C^6 is equidistant, i.e., $d_2 = d_H(\boldsymbol{a}, \boldsymbol{b})$ for any $\boldsymbol{a} \neq \boldsymbol{b} \in C^6$, then the minimum distance of $C(C^5, C^6, f)$ is given by

$$d_C = \min\{2l(\boldsymbol{x}, \boldsymbol{y})(n_2 - d_2 - w_l) + d_H(\boldsymbol{x}, \boldsymbol{y})d_2 : \boldsymbol{x} \neq \boldsymbol{y} \in C^5\}. \tag{20}$$

Furthermore, if C^5 is also equidistant, i.e., $d_1 = d_H(\boldsymbol{x}, \boldsymbol{y})$ for any $\boldsymbol{x} \neq \boldsymbol{y} \in C^5$, then the minimum distance of $C(C^5, C^6, f)$ is given by

$$d_C = d_1 d_2 + 2(n_2 - d_2 - w_l)\min\{l(\boldsymbol{x}, \boldsymbol{y}) : \boldsymbol{x} \neq \boldsymbol{y} \in C^5\}. \tag{21}$$

If $n_2 \geq d_2 + w_l$, then by (19), we have $d_C \geq d_1 d_2$. From Construction C, a relation between the maximum size of a constant-weight code and the maximum size of a constant-composition code can be obtained as follows.

Proposition 7: If $A_q(n_2, d_2, [w_0, \ldots, w_{q-1}]) \geq m-1$ and $n_2 \geq d_2 + w_l$, then

$$\begin{aligned} A_m(n_1, d_1, w) \leq A_q(n_1 n_2, d_1 d_2, [&ww_0, \ldots, ww_{l-1}, \\ &(n_1 - w)n_2 + ww_l, ww_{l+1}, \ldots, ww_{q-1}]). \end{aligned}$$

In what follows, we show that some optimum constant-composition codes can be obtained by using Construction C.

Theorem 4: In Construction C, if the outer code C^5 is an optimum constant-weight code achieving the nonrecursive Johnson bound (see Lemma 2), and the inner code C^6 is an optimum constant-composition code achieving the nonrecursive Johnson bound (see Lemma 3), then for $n_2 = d_2 + w_l$ where $l \in Z_q$ is fixed, $C(C^5, C^6, f)$ is an

$$\begin{aligned} (n_1 n_2, M, d_1 d_2, [&ww_0, \ldots, ww_{l-1}, \\ &(n_1 - w)n_2 + ww_l, ww_{l+1}, \ldots, ww_{q-1}])_q \end{aligned}$$

constant-composition code achieving the nonrecursive Johnson bound.

Proof: The proof is similar to the proof of Theorem 3. Note that C^5 and C^6 are both equidistant. By using (21), it is easy to verify that $C(C^5, C^6, f)$ is also an equidistant code with minimum distance $d_C = d_1 d_2$ since $n_2 = d_2 + w_l$. □

Example 3: $A_4(15, 12, [6, 3, 3, 3]) = 10$.

Proof: We know from [12] and Proposition 6 that $A_4(5, 4, 3) = 10$ and $A_4(3, 3, [0, 1, 1, 1]) = 3$. In Construction C, if C^5 is taken as a quaternary $(5, 10, 4, 3)_4$ constant-weight code achieving the nonrecursive Johnson bound, and C^6 is taken as a quaternary $(3, 3, 3, [0, 1, 1, 1])_4$ constant-composition code achieving the nonrecursive Johnson bound, then this example follows from Theorem 4 and the fact $n_2 = d_2 + w_0 = 3$. □

VII. Conclusion

In this correspondence, we study the problem of determining the maximum size of a q-ary constant-composition code, given its length, minimum distance and composition. We derive a lower bound for the maximum size of a q-ary constant-composition code with minimum distance at least 3. Furthermore, the recursive and nonrecursive Johnson bounds for q-ary constant-composition codes are given. By comparison with the recursive Johnson bound, we show that our lower bound is asymptotically optimal in a certain sense. We further study the construction methods of q-ary constant-composition codes in this correspondence. Three concatenated constructions of constant-composition codes are presented, and a number of optimum constant-composition codes are obtained by using these concatenated constructions.

Acknowledgment

The authors would like to thank the anonymous reviewers, Editor-in-Chief Paul H. Siegel, and Associate Editor Jonathan J. Ashley for their comments and suggestions that helped to improve this correspondence.

References

[1] S. S. Agaian, *Hadamard Matrices and Their Applications (Lecture Notes in Mathematics).* Berlin, Germany: Springer-Verlag, 1985, vol. 1168.

[2] E. Agrell, A. Vardy, and K. Zeger, "Upper bounds for constant-weight codes," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2373–2395, Nov. 2000.
[3] G. T. Bogdanova, A. E. Brouwer, S. N. Kapralov, and P. R. J. Östergård, "Error-correcting codes over an alphabet of four elements," *Des., Codes Cryptogr.*, vol. 23, pp. 333–342, 2001.
[4] G. T. Bogdanova and D. S. Ocetarova, "Some ternary constant-composition codes," in *Proc. 6th Int. Workshop on Algebraic and Combinatorial Coding Theory*, Pskov, Russia, Sept. 1998, pp. 41–45.
[5] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, "A new table of constant-weight codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1344–1380, Nov. 1990.
[6] D. A. Drake, "Partial $\boldsymbol{\lambda}$ -geometries and generalized matrices over groups," *Canad. J. Math.*, vol. 31, pp. 617–627, 1979.
[7] T. Ericson and V. Zinoviev, "Spherical codes generated by binary partitions of symmetric point sets," *IEEE Trans. Inform. Theory*, vol. 41, pp. 107–129, Jan. 1995.
[8] F.-W. Fu, T. Kløve, Y. Luo, and V. K. Wei, "On the svanström bound for ternary constant weight codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2061–2064, July 2001.
[9] ——, "On equidistant constant weight codes," *Discr. Appl. Math.*, vol. 128, pp. 157–164, 2003.
[10] F.-W. Fu, A. J. H. Vinck, and S.-Y. Shen, "On the constructions of constant-weight codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 328–333, Jan. 1998.
[11] R. L. Graham and N. J. A. Sloane, "Lower bounds for constant weight codes," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 37–43, Jan. 1980.
[12] W. Heise and T. Honold. Some equidistant constant weight codes. [Online]. Available: http://fatman. mathematik.tu-muenchen.de/~heise/MAT/code_ oval.html
[13] S. M. Johnson, "A new upper bound for error-correcting codes," *IRE Trans. Inform. Theory*, vol. IT-8, pp. 203–207, Apr. 1962.
[14] D. Jungnickel, "On difference matrices, resolvable TD's and generalized hadamard matrices," *Math. Zeit.*, vol. 167, pp. 49–60, 1979.
[15] T. Kløve, "A lower bound for $\boldsymbol{A(n,4,w)}$," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 257–258, Mar. 1981.
[16] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 3rd. ed. Amsterdam, The Netherlands: North-Holland, 1981.
[17] M. Plotkin, "Binary codes with specified minimum distances," *IEEE Trans. Inform. Theory*, vol. PGIT-6, pp. 445–450, Sept. 1960.
[18] M. Svanström, "Ternary Codes with Weight Constraints," Ph.D. dissertation, Dept. Elec. Eng., Linköping Univ., Linköping, Sweden, 1999.
[19] ——, "Constructions of ternary constant-composition codes with weight three," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2644–2647, Nov. 2000.
[20] ——, "A lower bound for ternary constant weight codes," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1630–1632, Sept. 1997.
[21] ——, "A class of perfect ternary constant weight codes," *Des. Codes Cryptogr.*, vol. 18, pp. 223–229, 1999.
[22] M. Svanström, P. R. J. Östergård, and G. T. Bogdanova, "Bounds and constructions for ternary constant-composition codes," *IEEE Trans. Inform. Theory*, vol. 48, pp. 101–111, Jan. 2002.
[23] J. H. van Lint and L. Tolhuizen, "On perfect ternary constant weight codes," *Des. Codes Cryptogr.*, vol. 18, pp. 231–234, 1999.
[24] C. L. M. van Pul and T. Etzion, "New lower bounds for constant weight codes," *IEEE Trans. Inform. Theory*, vol. 35, pp. 1324–1329, Nov. 1989.

Isometries for Rank Distance and Permutation Group of Gabidulin Codes

Thierry P. Berger

***Abstract*—The rank distance was introduced in 1985 by Gabidulin. He determined an upper bound for the minimum rank distance of a code. Moreover, he constructed a class of codes which meet this bound: the so-called Gabidulin codes.**

In this correspondence, we first characterize the linear and semilinear isometries for the rank distance. Then we determine the isometry group and the permutation group of Gabidulin codes of any length. We give a characterization of equivalent Gabidulin codes. Finally, we prove that the number of equivalence classes of Gabidulin codes is exactly the number of equivalence classes of vector spaces of dimension $\boldsymbol{n}$ contained in $\mathrm{GF}(\boldsymbol{p}^m)$ under some particular relations.

***Index Terms*—Automorphism, Gabidulin codes, isometry, permutation, rank metric.**

I. Isometries for Rank Distance

A. The Rank Distance

Let $\mathbb{K} = \mathrm{GF}(q^m)$ be an extension of degree m of the finite field $\mathrm{GF}(q)$. Note that $q = p^r$ is not necessary a prime, however, the field $\mathbb{F} = \mathrm{GF}(q)$ is considered as the "base field" in this correspondence. Let $E = \mathbb{K}^n$ be the vector space of dimension n over $\mathbb{K}$.

Definition 1: For $a \in E$, $a = (a_1, \ldots, a_n)$, the rank $rk(a)$ of a is the dimension of the $\mathbb{F}$-vector space generated by $\{a_1, \ldots, a_n\}$.

Let a and b be two elements of E. The relation $d_r(a,b) = rk(a-b)$ defines a distance over E. Following this definition, it is natural to define the minimum rank distance d_r of a code C. Moreover, if d_h denotes the classical Hamming distance, then for all a, b in E, the rank distance satisfies the inequality $d_r(a,b) \leq d_h(a,b)$.

The rank distance was introduced by Gabidulin in 1985. For more details on this metric, the reader can refer to [2].

B. Isometries for the Hamming Distance

In the coding literature, there are three kinds of automorphism groups for a code relatively to the Hamming metric (cf.[4]).

- The permutations $\sigma \in Sym(n)$ of the support $\{1, \ldots, n\}$ of codewords. Clearly, such a permutation preserves both the Hamming distance and the rank distance.
- The linear isometries for the Hamming distance. It is well known that this group is the monomial group $\mathcal{M}_n$ of $n \times n$ matrices over $\mathbb{K}$ with one and only one nonzero element on each row and each column [4]. This group is generated by the permutations of the support and the scalar multiplications by invertible elements on each coordinate. Clearly, these transformations are not always isometries for the rank distance, as soon as the entries of the matrix are not in the base field $\mathbb{F}$.

Manuscript received February 5, 2003; revised May 26, 2003. The material in this correspondence was presented in part at the 8th International Workshop on Algebraic and Combinatorial Coding Theory, St. Petersburg, Russia, September 2002.

The author is with the LACO, UMR CNRS 6090, University of Limoges, 87060 Limoges Cedex, France (e-mail: thierry.berger@unilim.fr).

Communicated by C. Carlet, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2003.819322