The code $C_{29}^3$ has a generator matrix

$$\begin{pmatrix}
01001110111010000000000000000\\
00111011101001000000000000000\\
11010011011000101100000000000\\
10100110000000111010000000000\\
00000001011000110001000000000\\
10011101011000011000100000000\\
10011101110100000000000000000\\
00011111111000011000011000000\\
11011111101000111000010100000\\
10111111100000101000010010000\\
00010010010000100000010001000\\
10010111110000001000010000100\\
00000110011000110000010000010\\
11111100001000010000010000001
\end{pmatrix}.$$

The constructed self-dual codes have a weight enumerator (9). In 21 cases codes with such weight enumerators were not known up to now.

### *F.* $[68, 34, 12]$ *Codes*

The weight enumerator of an extremal self-dual $[68, 34, 12]$ code must be of the form

$$W(y) = 1 + (442 + 4\beta)y^{12} + (10864 - 8\beta)y^{14} + \cdots \quad (10)$$

$$W(y) = 1 + (442 + 4\beta)y^{12} + (14960 - 8\beta - 256\gamma)y^{14} + \cdots. \quad (11)$$

The double circulant self-dual $[68, 34, 12]$ codes have weight enumerators (10) for

$$\beta = 104, 137, 170, 203, 236, 269, 302, 335, 401,$$

and (11) for

$$\gamma = 0, \beta = 34, 68, 102, 136, 170, 204, 238, 272$$

[9]. There also exist codes with weight enumerators (10) for

$$\beta = 122, 125, 126, \cdots, 132, 134, 135, 136, 139$$

and (11) with $\gamma = 0$ and

$$\beta = 40, 44, 45, 47, \cdots, 65, 67, 68, 69,$$

$\gamma = 1$ and

$$\beta = 61, 63, 64, 65, 72, 73, 76,$$

$\gamma = 2$ and $\beta = 65, 71, 77$ [7].

From the quasi-cyclic $[34, 16]$ code with a generator matrix obtained from two circulant $17 \times 16$ matrices with first rows $01000000001010010$ and $11000000001111101$ we construct the extremal self-dual $[68, 34, 12]$ codes listed in Table IX. These codes have weight enumerators (11). Codes with these weight enumerators were not known to exist.

## References


[1] R. A. Brualdi and V. Pless, "Weight enumerators of self-dual codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1222–1225, 1991.

[2] F. C. Bussemaker and V. D. Tonchev, "Extremal doubly-even codes of length 40 derived from Hadamard matrices of order 20," *Discr. Math.*, vol. 82, pp. 317–321, 1990.

[3] S. Buyuklieva, "On the binary self-dual codes with an automorphism of order 2," *Des., Codes Cryptogr.*, to be published.

[4] ——, "Existence of certain extremal self-dual codes of lengths 42 and 44," in *Proc. Int. Workshop OCRT* (Sozopol, Bulgaria, 1995), pp. 29–31.

[5] St.Buyuklieva and V.Yorgov, "Singly-even self-dual codes of length 40," *Des., Codes Cryptogr.*, vol. 9, pp. 131–141, 1996.

[6] J. H. Conway and N. J. A.Sloane, "A new upper bound on the minimal distance of self-dual codes,"*IEEE Trans. Inform. Theory*, vol. 36, pp. 1319–1333, 1990.

[7] S. T. Dougherty and M. Harada, "Extremal dobly-even self-dual codes of length a multiple of 24," preprint.

[8] T. A. Gulliver and M. Harada, "Classification of extremal double circulant self-dual codes of length 64 to 72," preprint.

[9] M. Harada, T. A. Gulliver, and H. Kaneta, "Classification of extremal double circulant self-dual codes of length up to 62," preprint.

[10] M. Harada, "Existence of new extremal double-even codes and extremal singly-even codes," *Des., Codes Cryptogr.*, vol. 8, pp. 1–12, 1996.

[11] M. Harada and H. Kimura, "On extremal self-dual codes," *Math. J. Okayama Univ.*, vol. 37, pp. 1–14, 1995.

[12] M. Harada and V. D. Tonchev, "Singly-even self-dual codes and Hadamard matrices," in *Lecture Notes in Computer Science*, vol. 948. Berlin, Germany: Springer-Verlag, pp. 1995, 279–284.

[13] R. Ruseva and V. Yorgov, "Two extremal codes of length 42 and 44" (in Russian), *Probl. Pered. Inform.*, vol. 29, pp. 99–103, 1993.

[14] E. Spence and V. D. Tonchev, "Extremal self-dual codes from symmetric designs," *Discr. Math.*, vol. 110, pp. 265–268, 1992.

[15] V. Tonchev and V. Yorgov, "The existence of certain extremal $[54, 27, 10]$ self-dual codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1628–1631, 1996.

[16] H. P. Tsai, "Existence of certain extremal self-dual codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 501–504, 1992.

[17] ——, "Existence of some extremal self-dual codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1829–1833, 1992.

[18] V. Y. Yorgov, "New extremal singly-even self-dual codes of length 44," in *Proc. 6th Joint Swedish–Russian Int. Workshop on Information Theory* (Mölle, Sweden), 1993, pp. 372–375.


# On the Constructions of Constant-Weight Codes


Fang-Wei Fu, A. J. Han Vinck, and Shi-Yi Shen



***Abstract*—Two methods of constructing binary constant-weight codes from 1) codes over GF$(q)$ and 2) constant-weight codes over GF$(q)$ are presented. Several classes of binary optimum constant-weight codes are derived from these methods. In general, we show that binary optimum constant-weight codes, which achieve the Johnson bound, can be constructed from optimum codes over GF$(q)$ which achieve the Plotkin bound. Finally, several classes of optimum constant-weight codes over GF$(q)$ are constructed.**

***Index Terms*—Constant-weight codes, Johnson bound, Plotkin bound, simplex codes.**


## I. Introduction

Binary constant-weight codes play an important role in coding theory. Research has been done in searching good constant-weight codes and finding good lower and upper bounds. For a good survey


Manuscript received February 22, 1997; revised July 15, 1997. This work was supported in part by the Chinese Education Ministry, National Natural Science Foundation of China, and the University of Essen. The material in this correspondence was presented in part at the 7th Benelux–Japan Workshop on Information Theory, Eltville, Germany, June 25–27, 1997.



F.-W. Fu is with the Institute for Experimental Mathematics, University of Essen, 4300 Essen, Germany, on leave from the Department of Mathematics, Nankai University, Tianjin, China.

A. J. H. Vinck is with the Institute for Experimental Mathematics, University of Essen, 4300 Essen, Germany.

S.-Y. Shen is with the Department of Mathematics, Nankai University, Tianjin, China.



Publisher Item Identifier S 0018-9448(98)00090-X.

paper, see Brouwer *et al.*, [4]. Nguyen, Györfi, and Massey [1] presented a new construction method of binary cyclic constant-weight codes from $p$-ary linear cyclic codes, where $p$ is a prime. They used a representation of GF$(p)$ as cyclic shifts of a binary $p$-tuple. Based on this method, some asymptotically optimum binary constant-weight codes were obtained. Because of the requirement of "cyclic codes," binary optimum constant-weight codes were not constructed in [1]. In this correspondence, we present two construction methods of binary constant-weight codes, and one construction method of constant-weight codes over GF$(q)$. First, we extend the construction method of [1] in the following two directions:

1) We construct a binary constant-weight code (not necessarily cyclic) from a code over GF$(q)$, by using a representation of GF$(q)$ as codewords of a binary constant-weight code. Actually, this idea already has been explored by Ericson and Zinoviev in [5] and [6]. We show that binary optimum constant-weight codes, which achieve the Johnson bound, can be constructed from optimum codes over GF$(q)$, which achieve the Plotkin bound. The cyclic shifts of a binary vector forms a binary constant-weight code, and thus this construction method can be understood as a generalization of the method as presented in [1], see Section II. Furthermore, two classes of binary optimum constant-weight codes can be constructed from simplex codes over GF$(q)$ by using this generalized method, see Sections II and III.
2) We construct a binary constant-weight code from a constant-weight code over GF$(q)$, by using a representation of nonzero elements of GF$(q)$ as codewords of a binary constant-weight code, and $0 \in$ GF$(q)$ as a zero vector. We show that some binary optimum constant-weight codes can be constructed by using this modified method, see Section IV.

To our knowledge, most research in this field is concerned with binary constant-weight codes. The contruction of constant-weight codes over GF$(q)$ did not receive a lot of attention. For some references, see [13]–[15]. It is easy to see that the Johnson bounds for binary constant-weight codes can be generalized to the $q$-ary case. Here we show that the first construction method can be generalized to construct optimum constant-weight codes over GF$(q)$. Actually, several classes of $q$-ary optimum constant-weight codes, which achieve the Johnson bounds ($q$-ary case), are constructed, see Section V.

## II. Construction A

In this section, we construct a binary constant-weight code from a code over GF$(q)$, by using a representation of GF$(q)$ as codewords of a binary constant-weight code. Actually, this idea already appeared in [5] and [6]. We show that binary optimum constant-weight codes, which achieve the Johnson bound, can be constructed from optimum codes over GF$(q)$ (outer codes), which achieve the Plotkin bound. We use a representation of GF$(q)$ as codewords of a binary optimum constant-weight code (inner code), which achieves the Johnson bound.

Let $A_q(n,d)$ denote the largest number $M$ of codewords in any $q$-ary code of length $n$ and minimum distance at least $d$ (called $q$-ary $(n,M,d)$ code), and $A_q(n,d,w)$ denote the largest number $M$ of codewords in any $q$-ary constant-weight code of length $n$, minimum distance at least $d$, and codeword weight $w$ (called a $q$-ary $(n,M,d,w)$ constant-weight code). In the sequel, we omit the index "2" for the binary case. We use the following lemmas.

*Lemma 2.1 (Plotkin Bound [7]):*

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

*Lemma 2.2 (Johnson Bound I [8]):*

$$A(n,2\delta,w) \le \frac{n\delta}{n\delta - w(n-w)}, \qquad n\delta > w(n-w).$$

*Lemma 2.3 (Johnson Bound II [8]):*

$$A(n,2\delta,w) \le \left[\frac{n}{w}\left[\frac{n-1}{w-1}\cdots\left[\frac{n-w+\delta}{\delta}\right]\cdots\right]\right]$$

where $[x]$ denote the largest integer less than $x$.

Below we present the first concatenated construction method of binary constant-weight codes. We use $q$-ary codes as outer codes, and binary constant-weight codes as inner codes.

*Construction A:* Let $C_1$ be a $q$-ary $(n_1,M,d_1)$ code, $C_2$ be a binary $(n_2,q,d_2,w)$ constant-weight code, $f$: GF$(q) \to C_2$ be a one to one mapping. Let

$$C_A(C_1,C_2,f) = \{(f(c_1),\cdots,f(c_{n_1}))|c = (c_1,\cdots,c_{n_1}) \in C_1\}.$$

It is easy to verify that $C_A(C_1,C_2,f)$ is a binary $(n_1n_2, M, d_1d_2, n_1w)$ constant-weight code.

*Theorem 2.1:* If in Construction A, $C_1$ is an optimum code over GF$(q)$, which achieves the Plotkin bound, i.e.,

$$M = \frac{qd_1}{qd_1 - n_1(q-1)}, \qquad d > n_1(q-1)/q$$

$C_2$ is a binary optimum constant-weight code, which achieves the Johnson bound $I$, i.e.,

$$q = \frac{n_2d_2/2}{n_2d_2/2 - w(n_2-w)}, \qquad n_2d_2/2 > w(n_2-w)$$

then $C_A(C_1,C_2,f)$ is a binary optimum constant-weight code, which achieves the Johnson bound $I$, i.e.,

$$M = \frac{n_1n_2(d_1d_2/2)}{n_1n_2(d_1d_2/2) - n_1w(n_1n_2 - n_1w)}.$$

*Proof:* The proof follows from substituting $q$ into the expression for $M$. □

## III. Two Classes of Binary Optimum Constant-Weight Codes

Nguyen, Györfi, and Massey [1] presented a concatenated construction method of binary cyclic constant-weight codes from $p$-ary linear cyclic codes. By using Reed–Solomon codes and generalized Berlekamp–Justesen codes as outer codes, they obtained four classes of good binary cyclic constant-weight codes, which asymptotically achieve the Johnson upper bound I or the Plotkin upper bound. In this section, we use $q$-ary optimum codes, which achieve the Plotkin bound, as outer codes in the construction method of [1]. This is a special case of Construction A. We construct several classes of optimum binary constant-weight codes, which achieve the Johnson upper bound I.

The cyclic order of

$$v = (v_1,\cdots,v_N) \in [\mathrm{GF}(2)]^N$$

is denoted as $t(v)$, i.e., the smallest positive integer $t$ such that

$$v = S^t(v) = (v_{t+1},\cdots,v_N,v_1,\cdots,v_t).$$

It is clear that

$$\mathcal{E}(v) = \{v, S(v),\cdots,S^{t(v)-1}(v)\}$$

forms a binary constant-weight code with length $N$, cod size $t(v)$, and weight $w(v)$. Its minimum distance is denoted as $d(v)$. Given a $q$-ary $(n,M,d)$ code $C$, $v \in [\mathrm{GF}(2)]^N$ with cyclic order $q$, and a one-to-one mapping $f$: GF$(q) \to \mathcal{E}(v)$, then we have the following proposition.

*Propositon 3.1:* $C_A(C, \mathcal{E}(v), f)$ is a binary constant-weight code with length $nN$, weight $nw(v)$, minimum distance at least $d(v)d$, and code size $M$.

*Proposition 3.2:*

$$A(nN, d(v)d, nw(v)) \geq A_q(n, d).$$

From [1], we know that

- $\alpha_q = (1, 0, \cdots, 0) \in [\mathrm{GF}(2)]^q$, $t(\alpha_q) = q$, $w(\alpha_q) = 1$, $d(\alpha_q) = 2$.
- $q = p$, prime, and $\frac{p-1}{2}$ is odd, $\beta \overset{\text{def}}{=}$ Legendre sequence of length $p$,

$$t(\beta) = p, \quad w(\beta) = \frac{p-1}{2}, \quad d(\beta) = \frac{p+1}{2}$$

where

$$\beta = (0, \beta_1, \cdots, \beta_{p-1}), \qquad \beta_i = 0$$

if $i$ is a quadratic residue modulo $p$ and $\beta_i = 1$ if $i$ is a quadratic nonresidue modulo $p$.

It is easy to verify that $\mathcal{E}(\alpha_q)$ and $\mathcal{E}(\beta_p)$ are binary optimum constant-weight codes, which achieve Johnson bound I. From both examples, we obtain the following proposition.

*Proposition 3.3:*

1) $A(nq, 2d, n) \geq A_q(n, d)$,
2) if $p$ is prime, and $\frac{p-1}{2}$ is odd, then

$$A\left(np, d\frac{p+1}{2}, n\frac{p-1}{2}\right) \geq A_p(n, d).$$

*Remark:* Proposition 3.3 (1) can also be found in [12, Theorem 7, p. 57].

Lower bounds for $A(n', d', w)$ can be obtained from lower bounds for $A_q(n, d)$, e.g., Gilbert–Varshamov bound, and optimum codes in $\mathrm{GF}(q)$, e.g., Hamming codes, Golay codes, R-S codes, MDS codes, and simplex codes.

*Proposition 3.4:* If $C$ is an optimum $(n, M, d)$ code over $\mathrm{GF}(q)$, which achieves the Plotkin bound, then $C_A(C, \mathcal{E}(\alpha_q), f)$ and $C_A(C, \mathcal{E}(\beta_p), f)$ are binary optimum constant-weight codes, which achieve the Johnson bound I.

Generalized Hadamard matrix over $\mathrm{GF}(q)$ can be used to construct codes over $\mathrm{GF}(q)$, which achieve the Plotkin bound, see [2]. If we take $C$ to be the $[(q^m - 1)/(q-1), m, q^{m-1}]$ simplex code $S_q(m)$, i.e., the dual code of the Hamming code over $\mathrm{GF}(q)$, we obtain the following two classes of binary optimum constant-weight codes.

*Proposition 3.5:*

1) $A\left(q\frac{q^m-1}{q-1}, 2q^{m-1}, \frac{q^m-1}{q-1}\right) = q^m$.
2) If $p$ is prime, and $\frac{p-1}{2}$ is odd, then

$$A\left(p\frac{p^m-1}{p-1}, p^{m-1}\frac{p+1}{2}, \frac{p^m-1}{2}\right) = p^m.$$

*Remark:* If $C$ is a binary optimum code which achieves the Plotkin bound, then $C_A(C, \mathcal{E}(\alpha_2), f)$ is an optimum balanced error-correcting code. Therefore, we can use the Hadamard matrix to construct optimum balanced error-correcting codes. Barg and Litsyn [9] used the Hadamard matrix to construct good balanced error-correcting codes. In [10], van Tilborg and Blaum also presented a construction method for balanced error-correcting codes.

## IV. Construction B

In this section, we construct a binary constant-weight code from a constant-weight code over $\mathrm{GF}(q)$. We use a representation of the nonzero elements of $\mathrm{GF}(q)$ as codewords of a binary constant-weight code, and $0 \in \mathrm{GF}(q)$ as a zero vector. We show that some binary optimum constant-weight codes can be constructed by using this modified method.

*Construction B:* Let $C_1$ be a $q$-ary $(n_1, M, d_1, w_1)$ constant-weight code, $C_2$ be a binary $(n_2, q-1, d_2, w_2)$ constant-weight code, $\mathbf{0} \in [\mathrm{GF}(2)]^{n_2}$ be the all-zero vector, $f$: $\mathrm{GF}(q) \to C_2 \cup \{\mathbf{0}\}$ be a one-to-one mapping $f(0) = \mathbf{0}$. Let

$$\begin{aligned} C_B(C_1, C_2, f) = \{&(f(c_1), \cdots, f(c_{n_1}))|c \\ &= (c_1, \cdots, c_{n_1}) \in C_1\}. \end{aligned}$$

It is easy to verify that $C_B(C_1, C_2, f)$ is a binary constant-weight code with length $n_1 n_2$, code size $M$, weight $w_1 w_2$.

Given $x, y \in C_1$, $x \neq y$, and $x = (x_1, \cdots, x_{n_1})$, $y = (y_1, \cdots, y_{n_1})$, we denote

$$\begin{aligned} l(x, y) &= |\{i\colon x_i = 0, y_i \neq 0 \text{ or } y_i = 0, x_i \neq 0\}| \\ l^*(x, y) &= |\{i\colon x_i \neq y_i \text{ and } x_i, y_i \neq 0\}|. \end{aligned}$$

Then

$$l(x, y) + l^*(x, y) \geq d_1.$$

Denote

$$d_B = \min\{w_2 l(x, y) + d_2 l^*(x, y) | \forall x, y \in C_1, x \neq y\}.$$

It is not difficult to see that the minimum distance of $C_B(C_1, C_2, f)$ is at least $d_B$.

*Proposition 4.1:*

$$A(q^2 - 1, 2(q-1), q) = q^2 - 1, \qquad q \text{ is a prime power, } q \neq 2.$$

*Proof:* Let $C_1 = S_q(2) - \{\mathbf{0}\}$ (Simplex code $S_q(2)$ deleting the zero vector) and $C_2 = \mathcal{E}(\alpha_{q-1})$ in Construction B. Then

$$\begin{aligned} &n_1 = q + 1, \quad M = q^2 - 1, \quad d_1 = q, \quad w_1 = q, \\ &n_2 = q - 1, \quad d_2 = 2, \quad w_2 = 1, \\ &d_B \geq 1 \times 2 + 2(q-2) = 2(q-1). \end{aligned}$$

Hence

$$C_B(S_q(2) - \{\mathbf{0}\}, \mathcal{E}(\alpha_{q-1}), f)$$

is a binary $(q^2 - 1, q^2 - 1, 2(q-1), q)$ constant-weight code. This yields that

$$A(q^2 - 1, 2(q-1), q) \geq q^2 - 1.$$

From Johnson bound II, we have

$$\begin{aligned} A(q^2 - 1, 2(q-1), q) &\leq \left\lfloor \frac{q^2-1}{q} \left\lfloor \frac{q^2-2}{q-1} \right\rfloor \right\rfloor \\ &= \left\lfloor \frac{q^2-1}{q} \times q \right\rfloor = q^2 - 1. \end{aligned}$$

Therefore,

$$A(q^2 - 1, 2(q-1), q) = q^2 - 1. \qquad \square$$

Actually, we can obtain following results.

*Proposition 4.2:* For all $c_1, c_2 \in S_q(m) - \{\mathbf{0}\}, c_1 \neq c_2$

1) if $c_1 \neq \theta c_2, \forall \theta \in F_q$, then

$$l(c_1, c_2) = 2q^{m-2} \qquad l^*(c_1, c_2) = q^{m-1} - 2q^{m-2}$$

2) if there exists $\theta \in F_q, \theta \neq 0$ such that $c_1 = \theta c_2$, then

$$l(c_1, c_2) = 0 \qquad l^*(c_1, c_2) = q^{m-1}.$$

*Proof:* Let $(F_q)^m$ be the $m$-dimensional column vector space over the finite field $F_q$. The scalar multiple class of $a \in (F_q)^m - \{\mathbf{0}\}$ is defined by

$$\overline{a} = \{\theta a | \theta \in F_q,\ \theta \neq 0\}.$$

There are a total of $\frac{q^m-1}{q-1}$ scalar multiple classes. First, pick only one column vector in every scalar multiple class. We obtain the column vectors $h_1, h_2, \cdots, h_n, n = \frac{q^m-1}{q-1}$. The generator matrix of $S_q(m)$ is defined as $H = (h_1, h_2, \cdots, h_n)_{m \times n}$. Denote the row vectors of $H$ as $v_1, v_2, \cdots, v_m$. Then

$$S_q(m) = \{\theta_1 v_1 + \theta_2 v_2 + \cdots + \theta_m v_m \mid \theta_i \in F_q, \\ i = 1, 2, \cdots, m\}.$$

Given $c \in S_q(m) - \{\mathbf{0}\}$, then there exist $\theta_i \in F_q, i = 1, 2, \cdots, m$ (not all zero), such that

$$c = \theta_1 v_1 + \theta_2 v_2 + \cdots + \theta_m v_m$$

and the components of $c$ satisfy

$$c_j = (\theta_1, \theta_2, \cdots, \theta_m) \cdot h_j, \qquad j = 1, 2, \cdots, n.$$

Consider the linear equation $(\theta_1, \theta_2, \cdots, \theta_m)x = 0$, where $x = (x_1, x_2, \cdots, x_m)^T$ is an unknown column vector in $(F_q)^m$. There are $q^{m-1} - 1$ nonzero solution vectors, and thus $\frac{q^{m-1}-1}{q-1}$ scalar multiple classes. Therefore,

$$|\{j | c_j = 0\}| = \frac{q^{m-1} - 1}{q - 1}.$$

The Hamming weight of $c$ is

$$w(c) = \frac{q^m - 1}{q - 1} - \frac{q^{m-1} - 1}{q - 1} = q^{m-1}.$$

It is easy to verify that assertion (2) is true.

Given $c_1, c_2 \in S_q(m) - \{\mathbf{0}\}$, and $c_1$ is not a multiple vector of $c_2$. Let $c_i = (c_{i1}, c_{i2}, \cdots, c_{in}), i = 1, 2$. Using the same argument as above, we have

$$|\{j | c_{1j} = c_{2j} = 0\}| = \frac{q^{m-2} - 1}{q - 1}.$$

Therefore,

$$\begin{aligned} l(c_1, c_2) &= |\{j | c_{1j} = 0\}| + |\{j | c_{2j} = 0\}| - 2|\{j | c_{1j} = c_{2j} = 0\}| \\ &= 2\frac{q^{m-1} - 1}{q - 1} - 2\frac{q^{m-2} - 1}{q - 1} = 2q^{m-2}. \end{aligned}$$

Hence,

$$l^*(c_1, c_2) = d_H(c_1, c_2) - l(c_1, c_2) = q^{m-1} - 2q^{m-2}. \qquad \square$$

Let $C_1 = S_q(m) - \{\mathbf{0}\}$ and $C_2 = \mathcal{E}(\alpha_{q-1})$ in Construction B. We then have the following proposition.

*Proposition 4.3:*

$$A(q^m - 1, 2(q-1)q^{m-2}, q^{m-1}) \geq q^m - 1.$$

*Proposition 4.4:*

$$A(2q, q+1, q-1) = q, \qquad q \text{ is an odd prime power.}$$

*Proof:* Let $Q = (b_{ij})_{q \times q}$ be the Jacobsthal matrix (see [3, p. 47], notifying that quadratic residues are defined to be the nonzero squares in GF$(q)$). From the properties of the Jacobsthal matrix, we know that the row vectors of $Q$ form a ternary $(q, q, (q+3)/2, q-1)$ constant-weight code $C_J$. If in Construction B, we take $C_1 = C_J$, $C_2 = \{10, 01\}$, $f$: $0 \to 00, 1 \to 10, -1 \to 01$, then $d_B = q + 1$. Hence, $C_B(C_J, C_2, f)$ is a binary $(2q, q, q+1, q-1)$ constant-weight code. This yields that $A(2q, q+1, q-1) \geq q$. From Johnson bound I, we have $A(2q, q+1, q-1) \leq q$ and therefore $A(2q, q+1, q-1) = q$. $\square$

If in Contruction A, we take $C_1$ as a $q$-ary optimum $(n, M, d)$ code, which achieves $A_q(n, d)$, and $C_2$ as the binary $(2q, q, q+1, q-1)$ constant-weight code constructed in Proposition 4.4, we have the following proposition.

*Proposition 4.5:*

$$A(2qn, (q+1)d, (q-1)n) \geq A_q(n, d), \quad q \text{ is an odd prime power.}$$

Furthermore, if we take $C_1$ as $S_q(m)$, we have the following proposition.

*Proposition 4.6:*

$$A\left(2q\frac{q^m - 1}{q - 1}, (q+1)q^{m-1}, q^m - 1\right) = q^m, \\ q \text{ is an odd prime power.}$$

## V. Optimum Constant-Weight Codes Over GF$(q)$

To our knowledge, most research in this field is concerned with binary constant-weight codes. The contruction of constant-weight codes over GF$(q)$ did not receive a lot of attention in literature. In this section, we show that the first construction method can be generalized to construct optimum constant-weight codes over GF$(q)$. Actually, several classes of $q$-ary optimum constant-weight codes, which achieve the Johnson bound ($q$-ary case), are constructed. It is easy to see that the Johnson bounds for binary constant-weight codes can be generalized to the $q$-ary case.

Johnson bound I for binary constant-weight codes can be generalized as follows.

*Lemma 5.1 (Generalized Johnson Bound I):*

$$A_q(n, d, w) \leq \frac{n(q-1)d}{qw^2 - 2(q-1)nw + n(q-1)d}, \\ qw^2 - 2(q-1)nw + n(q-1)d > 0.$$

It is easy to see that

$$A_q(n, d, w) \leq \frac{n(q-1)}{w} A_q(n-1, d, w-1)$$

$$A_q(n, 2\delta+1, \delta) = 1 \qquad A_q(n, 2\delta, \delta) = \left[\frac{n}{\delta}\right].$$

Therefore, Johnson bound II for binary constant-weight codes can be generalized as follows.

*Lemma 5.2 (Generalized Johnson Bound II):*

If $d = 2\delta + 1$, and $\delta + 1 \leq w$, then

$$A_q(n, 2\delta+1, w) \leq \left[\frac{(q-1)n}{w}\left[\frac{(q-1)(n-1)}{w-1} \cdots \left[\frac{(q-1)(n-w+\delta+1)}{\delta+1}\right]\cdots\right]\right].$$

If $d = 2\delta$, and $\delta \le w$, then

$$A_q(n, 2\delta, w) \le \left\lfloor \frac{(q-1)n}{w} \left\lfloor \frac{(q-1)(n-1)}{w-1} \cdots \left\lfloor \frac{(q-1)(n-w+\delta+1)}{\delta+1} \cdot \left\lfloor \frac{n-w+\delta}{\delta} \right\rfloor \right\rfloor \cdots \right\rfloor \right\rfloor.$$

*Remark:* The generalized Johnson bound II was given in [13] and [14], but the case $d = 2\delta$ was not separated as was done here. Generalized Steiner systems (see [15]) are a subclass of codes which attain the generalized Johnson bound II.

The method in Construction A can be generalized to construct optimum constant-weight codes over GF$(q)$.

*Construction A′:* Let $C_1$ be a $q_1$-ary $(n_1, M, d_1)$ code, $C_2$ be a $q$-ary $(n_2, q_1, d_2, w)$ constant-weight code over GF$(q)$, $f$: GF$(q_1) \to C_2$ be a one-to-one mapping. Let

$$C_{A'}(C_1, C_2, f) = \{(f(c_1), \cdots, f(c_{n_1}))|c = (c_1, \cdots, c_{n_1}) \in C_1\}.$$

It is easy to verify that $C_{A'}(C_1, C_2, f)$ is a $q$-ary $(n_1n_2, M, d_1d_2, n_1w)$ constant-weight code over GF$(q)$.

*Theorem 5.1:* If in Construction A′ $C_1$ is an optimum code over GF$(q_1)$, which achieves the Plotkin bound, i.e.,

$$M = \frac{q_1 d_1}{q_1 d_1 - n_1(q_1 - 1)}, \qquad d > n_1(q_1-1)/q_1$$

$C_2$ is an optimum constant-weight code over GF$(q)$, which achieves the generalized Johnson bound I, i.e.,

$$q_1 = \frac{n_2(q-1)d_2}{qw^2 - 2(q-1)n_2 w + n_2(q-1)d_2}, \quad qw^2 - 2(q-1)n_2w + n_2(q-1)d_2 > 0$$

then $C_{A'}(C_1, C_2, f)$ is an optimum constant-weight code over GF$(q)$, which achieves the generalized Johnson bound I, i.e.,

$$M = \frac{n_1 n_2 (q-1) d_1 d_2}{q(n_1 w)^2 - 2(q-1)(n_1n_2)(n_1 w) + n_1 n_2 (q-1) d_1 d_2}.$$

Below we present several classes of optimum constant-weight codes over GF$(q)$.

*Proposition 5.1:*

$$A_q(n, 2, w) = \binom{n}{w} (q-1)^{w-1}.$$

*Proof:* Assume $C = \{(c_1, c_2, \cdots, c_n) \in [\mathrm{GF}(q)]^n|$ there are only $w$ nonzero components $c_{i_1}, c_{i_2}, \cdots, c_{i_{w-1}}, c_{i_w}, 1 \le i_1 < i_2 < \cdots < i_{w-1} < i_w \le n$, such that $c_{i_w} = c_{i_1}c_{i_2}\cdots c_{i_{w-1}}\}$. It is easy to verify that $C$ is a $q$-ary $(n, 2, w)$ constant-weight code over GF$(q)$, and

$$|C| = \binom{n}{w}(q-1)^{w-1}.$$

Therefore,

$$A_q(n, 2, w) \ge |C| = \binom{n}{w} (q-1)^{w-1}.$$

By using the generalized Johnson bound II, we have

$$A_q(n, 2, w) \le \left\lfloor \frac{(q-1)n}{w} \left\lfloor \frac{(q-1)(n-1)}{w-1} \cdots \left\lfloor \frac{(q-1)(n-w+2)}{2} \left\lfloor \frac{n-w+1}{1} \right\rfloor \right\rfloor \cdots \right\rfloor \right\rfloor = \binom{n}{w} (q-1)^{w-1}.$$

This yields

$$A_q(n, 2, w) = \binom{n}{w}(q-1)^{w-1}.$$ □

*Proposition 5.2:*

$$A_q\left(\frac{q^m-1}{q-1}, q^{m-1}, q^{m-1}\right) = q^m - 1.$$

*Proof:* It is easy to see that $S_q(m) - \{\mathbf{0}\}$ is an optimum $q$-ary $(\frac{q^m-1}{q-1}, q^m-1, q^{m-1}, q^{m-1})$ constant-weight code, which achieves the generalized Johnson bound I. □

*Proposition 5.3:*

$$A_3\left(q, \frac{q+3}{2}, q-1\right) = q, \qquad \text{is an odd prime power.}$$

*Proof:* From the proof of Proposition 4.4, we know that the row vectors of the Jacobsthal matrix form a ternary optimum $(q, q, \frac{q+3}{2}, q-1)$ constant-weight code $C_J$, which achieves the generalized Johnson bound I. □

*Proposition 5.4:*

$$A_3\left(q\frac{q^m-1}{q-1}, q^{m-1}\frac{q+3}{2}, q^m-1\right) = q^m, \quad q \text{ is an odd prime power.}$$

*Proof:* In Theorem 5.1, set $C_1 = S_q(m)$, and $C_2 = C_J$ (in Proposition 5.3). From this we obtain a ternary optimum $(q\frac{q^m-1}{q-1}, q^m, q^{m-1}\frac{q+3}{2}, q^m - 1)$ constant-weight code, which achieves the generalized Johnson bound I. □

If in Contruction A′, we take $C_1$ as a $q$-ary optimum $(n, M, d)$ code, which achieves $A_q(n, d)$, and $C_2$ as $C_J$, we have the following proposition.

*Proposition 5.5:*

$$A_3\left(nq, d\,\frac{q+3}{2}, n(q-1)\right) \ge A_q(n, d), \; q \text{ is an odd prime power.}$$

*Proposition 5.6:*

$$A_q\left(\frac{q^m-1}{q-1}, 3, 3\right) = \frac{(q^m-1)(q^m-q)}{6}.$$

*Proof:* From the generalized Johnson bound II, we have

$$A_q(n, 3, 3) \le \frac{(q-1)^2 n(n-1)}{6}.$$

The codewords with weight 3 in the $q$-ary Hamming code $\mathrm{Ham}(m, q)$ form an optimum $q$-ary $(\frac{q^m-1}{q-1}, \frac{(q^m-1)(q^m-q)}{6}, 3, 3)$ constant-weight code, which achieves the generalized Johnson bound II. □

*Proposition 5.7:*

$$A_3(11, 5, 5) = 132 \qquad A_3(12, 6, 6) = 264.$$

*Proof:* The codewords with weight 5 in the ternary [11, 6, 5] Golay code form an optimum ternary $(11, 132, 5, 5)$ constant-weight code, which achieves the generalized Johnson bound II. The codewords with weight 6 in the ternary [12, 6, 6] extended Golay code form an optimum ternary $(12, 264, 6, 6)$ constant-weight code, which achieves the generalized Johnson bound II. □

*Remark:* As pointed out by one referee, Proposition 5.6 and the first part of Proposition 5.7 are among the results which are mentioned in [14]. For completeness, we still include these results here.

Ericson and Zinoviev [6] studied the asymptotic behavior of $A(n, d, w)$. By using the well-known bound of Tsfasman, Vlăduţ, and Zink [11] and the fact $A(nq, 2d, n) \geq A_q(n, d)$, they obtained an improvement of the Gilbert bound for binary constant-weight codes. It is worthy to point out that we can obtain new lower bounds for asymptotic values of $A(n, d, w)$ and $A_3(n, d, w)$ in the same way, by using the fact

$$A(2qn, (q+1)d, (q-1)n) \geq A_q(n, d)$$
$$A_3(nq, d\frac{q+3}{2}, n(q-1)) \geq A_q(n, d)$$

$q$ is an odd prime power, respectively.

## VI. Conclusion

Motivated by the construction method of binary cyclic constant-weight codes by Nguyen, Györfi, and Massey [1], we study the concatenated construction methods of constant-weight codes. In Construction A, we use codes over GF$(q)$ as outer codes and binary constant-weight codes as inner codes. In Construction B, we use constant-weight codes over GF$(q)$ as outer codes and binary constant-weight codes as inner codes, with the zero element in GF$(q)$ is represented as zero vector. We show that binary optimum constant-weight codes can be constructed from Constructions A and B by using different inner codes and outer codes. We also establish some interesting relations between $A(n, 2\delta, w)$ and $A_q(n, d)$. Furthermore, Construction A is generalized to construct constant-weight codes over GF$(q)$. In Construction A$'$, we use codes over GF$(q_1)$ as outer codes and constant-weight codes over GF$(q)$ as inner codes. Finally, several classes of optimum constant-weight codes over GF$(q)$ are constructed.

## Acknowledgment

The authors wish to thank the Editor and the referees for their comments and suggestions that helped to improve the correspondence.

## References

[1] Q. A. Nguyen, L. Györfi, and J. L. Massey, "Constructions of binary constant-weight cyclic codes and cyclically permutable codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 940–949, May 1992.

[2] G. Mackenzie and J. Seberry, "Maximal ternary codes and Plotkin's bound," *Ars Combin.*, vol. 17A, pp. 251–270, 1984.

[3] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error–Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1981 (3rd printing).

[4] 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, 1990.

[5] V. A. Zinoviev, "Cascade equal-weight codes and maximal packings," *Probl. Contr. Inform. Theory*, vol. 12, pp. 3–10, 1983.

[6] T. Ericson and V. A. Zinoviev, "An improvement of the Gilbert bound for constant-weight codes," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 720–723, 1987.

[7] M. Plotkin, "Binary codes with specified minimum distances," *IEEE Trans. Inform. Theory*, vol. IT-6, pp. 445–450, 1960.

[8] S. M. Johnson, "A new upper bound for error-correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-8, pp. 203–207, 1962.

[9] A. Barg and S. Litsyn, "DC-constrained codes from Hadamard matrices," *IEEE Trans. Inform. Theory*, vol. 37, pp. 801–807, 1991.

[10] H. van Tilborg and M. Blaum, "On error-correcting balanced codes," *IEEE Trans. Inform. Theory*, vol. 35, pp. 1091–1095, 1989.

[11] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink, "Modular curves, Shimura curves and Goppa codes better than the Varshamov-Gilbert bound," *Math. Nachrichten.*, vol. 104, pp. 13–28, 1982.

[12] T. Ericson, "Bounds on the size of a code, " in *Topics in Coding Theory, Lecture Notes in Control and Information Sciences*, vol. 128. Berlin, Germany: Springer-Verlag, 1989, ch. 2.

[13] R. J. M. Vaessens, E. H. L. Aarts, and J. H. van Lint, "Genetic algorithms in coding theory—A table for $A_3(n, d)$," *Discr. Appl. Math.*, vol. 45, pp. 71–87, 1993.

[14] T. Etzion, "Optimal constant-weight codes over $Z_k$ and generalized designs," *Discr. Math.*, 1997, to be published.

[15] K. Phelps and C. Yin, "Generalized Steiner systems," *J. Comb. Des.*, to be published.

# Maximum Disjoint Bases and Constant-Weight Codes

Vladimir D. Tonchev

***Abstract*—The following lower bound for binary constant weight codes are derived by an explicit construction:**

$$A(17, 4, 5) \geq 441.$$

**The construction exploits maximal sets of bases in the four-dimensional binary vector space pairwise intersecting in at most two vectors.**

***Index Terms*—Affine geometry, constant-weight code, Steiner system.**

## I. Introduction

We follow the notation of [2]. For the parameters $n = 2^{2m} + 1$, $w = 5$, $d = 2\delta = 4$ of a binary constant-weight code, the Schönheim upper bound is

$$A(2^{2m}+1, 4, 5) \leq \frac{(2^{2m}+1)(2^{2m})(2^{2m}-1)(2^{2m}-2)}{5 \cdot 4 \cdot 3 \cdot 2}$$

with equality if and only if a Steiner system $S(4, 5, 2^{2m}+1)$ exists. Apart from the trivial case $m = 1$, no such system is known presently. An "approximation" of such a Steiner system, being a Steiner 4-design with two block sizes, 5 and 6, can be derived from the Preparata code [4]. The best known lower bound for the smallest nontrivial case $m = 2$ is $A(17, 4, 5) \geq 424$, obtained by the partitioning construction in [2].

In this note, a binary constant-weight code $C$ of length $n = 17$, weight $w = 5$, minimum distance $d = 4$, and containing 441 words is constructed as a "partial extension" of the Steiner system $S(3, 4, 16)$ formed by the planes in the four-dimensional binary affine space AG$(4, 2)$.

## II. Bases in 4-Space

Let $S = S(3, 4, 16)$ be the Steiner system with blocks the 140 planes in the four-dimensional binary affine space AG$(4, 2)$. The point set of $S$ is the four-dimensional binary vector space

$$V_4 = \{\overline{0} = (0, 0, 0, 0), (0, 0, 0, 1), \cdots, (1, 1, 1, 1)\}$$

Manuscript received June 17, 1997; revised July 24, 1997.

The author is with the Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931 USA.

Publisher Item Identifier S 0018-9448(98)00068-6.