Optimal Constant Composition Codes From Zero-Difference Balanced Functions

Cunsheng Ding, *Senior Member, IEEE*

***Abstract*—Constant composition codes are a special class of constant weight codes, and include permutation codes as a subclass. They have applications in communications engineering. In this correspondence, a generic construction of optimal constant composition codes using zero-difference balanced functions is introduced. It generalizes the earlier construction of optimal constant composition codes employing perfect nonlinear functions. In addition, two classes of optimal constant composition codes with new parameters are reported.**

***Index Terms*—Constant composition codes, constant weight codes, perfect nonlinear functions, zero-difference balanced functions.**

I. Introduction

An $(n, M, d, w)_q$ constant weight code is a code over an abelian group $\{b_0, b_1, \ldots, b_{q-1}\}$, with length n, size M and minimum distance d such that the Hamming weight of each codeword is w.

An $(n, M, d, [w_0, w_1, \ldots, w_{q-1}])_q$ *constant composition code* (CCC in short) is a code over an abelian group $\{b_0, b_1, \ldots, b_{q-1}\}$, with length n, size M, and minimum Hamming distance d such that in every codeword the element b_i appears exactly w_i times for every i. An $(n, M, d, [w_0, w_1, \ldots, w_{q-1}])_q$ constant composition code is called a *permutation code* if $n = q$ and $w_i = 1$ for all i. Thus, permutation codes are a special class of constant composition codes, and constant composition codes are a subclass of constant weight codes.

Since the class of binary constant composition codes coincides with the class of binary constant weight codes, the study of binary constant composition codes has relatively a long history. Instead of giving a survey of constant composition codes, we will here provide brief information on references regarding permutation codes and nonbinary constant composition codes.

The study of permutation codes goes back to at least 1965 [27]. In the 1970s, Blake [1]–[3], Deza and Vanstone [12], and Frankel and Deza [19] investigated permutation codes. Recently, advances on permutation codes have been made by Chu, Colbourn and Dukes [9], Colbourn, Kløve and Ling [8], Ding, Fu, Kløve, and Wei [14], and Fu and Kløve [20]. Nonbinary constant composition codes were studied already in the 60's. Both algebraic and combinatorial constructions have been presented. For further information, the reader is referred to Bogdanova and Kapralov [4], Chee, Ling, Ling, and Shen [7], Colbourn, Kløve, and Ling [8], Chu, Colbourn, and Dukes [10], [11], Ding and Yin [15]–[17], Ding and Yuan [18], Luo, Fu, Han Vink, and Chen [23], Semakov and Zinoviev [25], Semakov, Zinoviev, and Zaitsev [26], Svanström [29], Svanström, Östergard, and Bogdanova [30], and Zinoviev [31].

The objective of this correspondence is twofold. First of all, we will present a generic construction of optimal constant composition codes using a special class of functions—the zero-difference balanced functions. This generalizes the earlier construction of optimal constant composition codes employing perfect nonlinear functions [15]. Secondly, we will report two classes of optimal constant composition codes with new parameters.

Manuscript received June 12, 2008; revised August 28, 2008. Current version published November 21, 2008.

The author is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China (e-mail: cding@cse.ust.hk).

Communicated by T. Etzion, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2008.2006420

II. A Bound on Constant Composition Codes

Let $A_q(n, d, [w_0, w_1, \ldots, w_{q-1}])$ denote the maximum size of an $(n, M, d, [w_0, w_1, \ldots, w_{q-1}])_q$ constant composition code. Luo, Fu, Han Vinck, and Chen [23] developed the following bound for constant composition codes.

Lemma 1: If $nd - n^2 + (w_0^2 + w_1^2 + \cdots + w_{q-1}^2) > 0$, then

$$A_q(n, d, [w_0, w_1, \ldots, w_{q-1}]) \leq \frac{nd}{nd - n^2 + \left(w_0^2 + w_1^2 + \cdots + w_{q-1}^2\right)}.$$

In the sequel, we will present a generic construction of constant composition codes meeting the upper bound of Lemma 1.

III. Equivalence of Constant Composition Codes

Let q be a power of a prime. An $[n, k, d]_q$ linear code is a subspace of $\mathrm{GF}(q)^n$ with dimension k and minimum Hamming distance d. Two linear codes are said to be *equivalent* if one can be obtained from the other by a combination of operations of the following types:

- permutation of the n coordinates of the codewords;
- multiplication of the symbols appearing in a fixed coordinate by a nonzero scalar.

For constant composition codes, the situation is quite different. A multiplication of the symbols appearing in a fixed coordinate may transform a constant composition code into a non-constant-composition code. In view of this, two constant composition codes are said to be *equivalent* if one can be obtained from the other by coordinate permutations. Hence, equivalent CCCs have the same codeword length n, the same number M of codewords, the same minimum Hamming distance d, and the same frequencies w_i.

IV. A Generic Construction of Optimal CCCs Using Zero-Difference Balanced Functions

A. Zero-Difference Balanced Functions and Their Properties

Let $(A, +)$ and $(B, +)$ be two abelian groups with orders n and ℓ respectively. A function f from A to B is called *zero-difference balanced* (ZDB) if

$$|\{x \in A : f(x + a) - f(x) = 0\}| = \lambda$$

for every nonzero $a \in A$, where λ is a positive integer.

The following proposition follows directly from the definition of zero-difference balanced functions.

Proposition 2: Let f be a ZDB function from $(A, +)$ to $(B, +)$. Define $\lambda_b = |\{x \in A : f(x) = b\}|$ for every $b \in B$. Then

$$\sum_{b \in B} \lambda_b(\lambda_b - 1) = \lambda(|A| - 1).$$

Zero-difference balanced functions were first defined and used to construct difference systems of sets in [13]. In this correspondence, we employ them to construct optimal constant composition codes.

B. The Construction of Optimal CCCs Using Zero-Difference Balanced Functions

In this section, we introduce a construction of $(n, M, d, [w_0, \ldots, w_{q-1}])_q$ CCCs that meet the Luo–Fu–Vinck–Chen

bound of Lemma 1. Our construction is based on zero-difference balanced functions and is a generalization of the one in [15].

Let Π be a function from an Abelian group $(A,+)$ to an Abelian group $(B,+)$. Let

$$A=\{a_0,a_1,\ldots,a_{n-1}\},\ B=\{b_0,b_1,\ldots,b_{\ell-1}\}.$$

Define

$$w_i=|\{x\in A:\Pi(x)=b_i\}|$$

for each i.

Now we define

$$\mathcal{C}_\Pi=\{(\Pi(a_0+a_i),\ldots,\Pi(a_{n-1}+a_i)):0\le i\le n-1\}. \quad (1)$$

Proposition 3: If Π is a zero-difference balanced function, then the $\mathcal{C}_\Pi$ of (1) is an $(n,n,n-\lambda,[w_0,w_1,\ldots,w_{\ell-1}])_\ell$ CCC over B, and is optimal with respect to the Luo–Fu–Vinck–Chen bound of Lemma 1.

Proof: By definition, $\mathcal{C}_\Pi$ is a constant composition code with frequencies w_i for any function Π. Since Π is zero-difference balanced, the Hamming distance between any pair of distinct codewords is $n-\lambda$. By Proposition 2

$$\sum_{i=0}^{\ell-1}w_i^2=\lambda(n-1)+n.$$

Hence

$$nd-n^2+\sum_{i=0}^{\ell-1}w_i^2=d>0.$$

So the Luo–Fu–Vinck–Chen bound is met. □

The construction of optimal constant composition codes is generic in the sense that any zero-difference balanced function yields an optimal CCC. It will be seen later that it is a generalization of the earlier one in [15].

V. Optimal Constant Composition Codes From Zero-Difference Balanced Functions

A. Optimal Constant Composition Codes From Perfect Nonlinear Functions

A function f from an abelian group $(A,+)$ to an abelian group $(B,+)$ is called *linear* if and only if $f(x+y)=f(x)+f(y)$ for all $x,y\in A$. A function g from $(A,+)$ to $(B,+)$ is called *affine* if and only if $g=f+b$, where f is linear and $b\in B$ is a constant. Obviously, the zero function is linear.

There are different ways to measure nonlinearity [5]. A robust measure of nonlinearity of functions is defined by

$$P_f=\max_{0\ne a\in A}\max_{b\in B}\frac{|\{x\in A:f(x+a)-f(x)=b\}|}{|A|}. \quad (2)$$

The smaller the value of P_f, the higher the corresponding nonlinearity of f (if f is linear, then $P_f=1$).

It is easily seen that $P_f\ge\frac{1}{|B|}$. For applications in coding theory and cryptography we wish to find functions with the smallest possible P_f. A function $f:A\to B$ has perfect nonlinearity if $P_f=\frac{1}{|B|}$.

The following two lemmas about perfect nonlinear functions were proved in [5].

Lemma 4: Let $(A,+)$ and $(B,+)$ be abelian groups of orders n and ℓ respectively, where ℓ divides n. Then f is a perfect nonlinear function from A to B iff

$$|\{x\in A:f(x+a)-f(x)=b\}|=\frac{n}{\ell}$$

for every nonzero $a\in A$ and every $b\in B$.

Lemma 5: Let $(A,+)$ and $(B,+)$ be abelian groups of orders n and ℓ respectively, where ℓ divides n. If f is a perfect nonlinear mapping from A to B, then for any nonzero $b\in B$

$$\begin{cases}\sum_{z\in B}\lambda_z^2=\frac{n^2+(\ell-1)n}{\ell}\\ \sum_{z\in B}\lambda_z\lambda_{z+b}=\frac{n(n-1)}{\ell}\\ \sum_{z\in B}\lambda_z=n\end{cases} \quad (3)$$

where $\lambda_z=|\{x\in A:f(x)=z\}|$ for each $z\in B$.

Lemma 4 shows that perfect nonlinear functions are zero-difference balanced functions. However, zero-difference balanced functions may not be perfect nonlinear functions. This will be justified subsequently. So the construction of optimal constant composition codes of Section IV-B is indeed a generalization of the one using perfect nonlinear functions presented in [15].

It follows from Lemma 5 that the distance $d=(\ell-1)n/\ell$ for the CCC $\mathcal{C}_\Pi$ of (1) if Π is perfect nonlinear [15]. However, the frequencies $w_i=\lambda_i$ may not be determined by the set of equations in (3) in some cases, as (3) may have more than one solution in some cases. For information on perfect nonlinear functions, the reader is referred to [5], [6], [15], [21], [22].

B. A Class of Optimal Constant Composition Codes With New Parameters

The following lemma is proved in [13].

Lemma 6: Let q be a power of a prime, and let N be a positive integer such that $q\equiv 1\pmod N$. Let ω be a generator of $\mathrm{GF}(q^m)^*$, where m is a positive integer. Define $\alpha=\omega^N$, $n=(q^m-1)/N$, and a function Π from $(\mathbf{Z}_n,+)$ to $(\mathrm{GF}(q),+)$ by

$$\Pi(x)=\mathrm{Tr}_{q^m/q}(\alpha^x),\ x\in\mathbf{Z}_n \quad (4)$$

where $\mathrm{Tr}_{q^m/q}$ is the trace function from $\mathrm{GF}(q^m)$ to $\mathrm{GF}(q)$, and $\mathbf{Z}_n=\{0,1,\ldots,n-1\}$.

If $\gcd(m,N)=1$, the function Π is zero-difference balanced. Furthermore

$$|\{x\in\mathbf{Z}_n:\Pi(x+t)-\Pi(x)=0\}|=\frac{q^{m-1}-1}{N}$$

for every nonzero $t\in\mathbf{Z}_n$.

The function Π of (4) is zero-difference balanced, but not perfect nonlinear as q does not divide n. Hence zero-difference balanced functions may not be perfect nonlinear.

Proposition 7: Let $\gcd(m,N)=1$, and let Π be the function of (4). Then the $\mathcal{C}_\Pi$ of (1) is an optimal cyclic CCC over $\mathrm{GF}(q)$ with parameters

$$\left(\frac{q^m-1}{N},\frac{q^m-1}{N},\frac{q^{m-1}(q-1)}{N},[w_0,w_1,\ldots,w_{q-1}]\right)_q$$

where $w_i=|\{x\in\mathbf{Z}_n:\Pi(x)=y_i\}|$ and $y_0,y_1,\ldots,y_{q-1}$ are all the elements of $\mathrm{GF}(q)$.

Proof: It follows from Lemma 6 and Proposition 3. □

Example 1: When $q=3,m=3$ and $N=2$, the $\mathcal{C}_\Pi$ of (1) is an optimal cyclic CCC over $\mathrm{GF}(3)$ with parameters $(13,13,9,[4,3,6])_3$.

Example 2: When $q=13,m=2$ and $N=3$, the $\mathcal{C}_\Pi$ of (1) is an optimal cyclic CCC over $\mathrm{GF}(13)$ with parameters $(56,56,52,[4,6,5,5,2,6,2,2,6,2,5,5,6])_{13}$.

When $N=1$, $w_0=q^{m-1}-1$ and $w_i=q^{m-1}$ for all $1\le i\le q-1$. When $N=2$, the CCC becomes one of the optimal CCCs described in

[15]. For $N \geq 3$, it is hard to determine these w_i. However, it is known that [13]

$$\frac{q^{m-1} - Nq^{(m-2)/2} - 1}{N} \leq w_i \leq \frac{q^{m-1} + Nq^{(m-2)/2} - 1}{N}.$$

For every N with N dividing $q-1$, it is known that

$$w_0 = q^{m-1} - 1.$$

It seems that the parameters of the CCC $\mathcal{C}_\Pi$ described in Proposition 7 are new when $N \geq 3$.

C. Another Class of Optimal Constant Composition Codes With New Parameters

Before describing the class of optimal CCCs with new parameters, we need to introduce cyclotomy.

Throughout this section, let $q = p^s$ and $r = q^m$, where p is a prime, s and m are positive integers. Let $r - 1 = nN$ for two positive integers $n > 1$ and $N > 1$, and let α be a fixed generator of GF$(r)^*$. Define $C_i^{(N,r)} = \alpha^i \langle \alpha^N \rangle$ for $i = 0, 1, \ldots, N-1$, where $\langle \alpha^N \rangle$ denotes the subgroup of GF$(r)^*$ generated by α^N. The cosets $C_i^{(N,r)}$ are called the *cyclotomic classes* of order N in GF(r). The *cyclotomic numbers* of order N are defined by

$$(i,j)^{(N,r)} = \left| \left(C_i^{(N,r)} + 1 \right) \cap C_j^{(N,r)} \right|$$

for all $0 \leq i \leq N-1$ and $0 \leq j \leq N-1$.

The *Gaussian periods* are defined by

$$\eta_i^{(N,r)} = \sum_{x \in C_i^{(N,r)}} \chi(x), \quad i = 0, 1, \ldots, N-1$$

where $\chi(x) := \epsilon_p^{\mathrm{Tr}_{r/p}(x)}$ is the canonical additive character of GF(r), and ϵ_p is a primitive complex pth root of unity.

The following lemma presents well-known formulas on Gaussian periods [28].

Lemma 8: Let notations be the same as before. Then

$$\eta_i^{(N,r)} \eta_{i+k}^{(N,r)} = \sum_{h=0}^{N-1} (i-h, i-h+k)^{(N,r)} \eta_h^{(N,r)} + n\theta_k$$

where $\theta_k = 1$ if $k = 0$ and $\theta_k = 0$, otherwise.

In general, the values of the Gaussian periods cannot be determined by the relations described in Lemma 8. However, they can be computed in certain cases.

In the sequel, we will need the following lemma [24].

Lemma 9: Assume there exists a positive integer j such that $p^j \equiv -1 (\mathrm{mod}\ N)$, and assume that j is the least such. Let $r = p^{ms}$, where $ms = 2j\gamma$. Then the Gaussian periods are given below.

1) If γ, p and $(p^j+1)/N$ are all odd, then $\eta_{N/2}^{(N,r)} = ((N-1)p^{j\gamma} - 1)/N$ and $\eta_i^{(N,r)} = (-p^{j\gamma} - 1)/N$ for all $i \neq N/2$.
2) In all other cases, $\eta_0^{(N,r)} = ((-1)^{\gamma+1}(N-1)p^{j\gamma} - 1)/N$ and $\eta_i^{(N,r)} = ((-1)^\gamma p^{j\gamma} - 1)/N$ for all $i \neq 0$.

We are now ready to describe the class of optimal CCCs.

Proposition 10: Let $p = 2, m = 4$ and $N = q^2 - 1$. Then $n = q^2 + 1$. Let α be a generator of GF$(r)^*$ and $g = \alpha^N$. Define a function $\Pi(x)$ from $(\mathbf{Z}_n, +)$ to $(\mathrm{GF}(q), +)$ by

$$\Pi(x) = \mathrm{Tr}_{r/q}(g^x), x \in \mathbf{Z}_n.$$

Then Π is zero-difference balanced and the $\mathcal{C}_\Pi$ of (1) is an optimal cyclic CCC over GF(q) with parameters

$$(q^2+1, q^2+1, q^2-q, [w_0, w_1, \ldots, w_{q-1}])_q$$

where $w_i = |\{x \in \mathbf{Z}_n : \Pi(x) = y_i\}|$ and $y_0, y_1, \ldots, y_{q-1}$ are all the elements of GF(q).

Proof: The proof is divided into several parts. We first prove that

$$\cup_{y \in \mathrm{GF}(q)^*} y C_0^{(N,r)} = C_0^{(q+1,r)}.$$

Note that any $y \in \mathrm{GF}(q)^*$ can be expressed as

$$y = \alpha^{(q^3+q^2+q+1)t} = \alpha^{(q^2-1)(q+1)t + 2(q+1)t}$$

for some t with $0 \leq t \leq q-2$. Hence

$$\cup_{y \in \mathrm{GF}(q)^*} y C_0^{(N,r)} \subseteq C_0^{(q+1,r)}.$$

On the other hand, since $\gcd(2, q-1) = 1$, we have

$$\mathrm{GF}(q)^* \cap C_0^{(N,r)} = \{1\}.$$

It then follows that $\cup_{y \in \mathrm{GF}(q)^*} y C_0^{(N,r)} = C_0^{(q+1,r)}$.

By Lemma 9, we have

$$\eta_i^{(q+1,r)} = q - 1 \text{ for all } i \neq 0, \eta_0^{(q+1,r)} = -q^2 + q - 1.$$

Finally, define

$$\Delta_\tau = |\{i \in \mathbf{Z}_n : \Pi(i+\tau) - \Pi(i) = 0\}|$$

for each nonzero $\tau \in \mathbf{Z}_n$.

Note that $\Pi(i+\tau) - \Pi(i) = \mathrm{Tr}_{r/q}((g^\tau - 1)g^i)$. Furthermore, for any subset S of GF(r), we define

$$\chi(S) = \sum_{y \in S} \chi(y)$$

where χ is the additive group character on GF(r) defined before.

For any $0 \leq \tau \leq n-1$, using the results proved above we have then

$$\begin{aligned}
\Delta_\tau &= \frac{1}{q} \sum_{i=0}^{n-1} \sum_{y \in \mathrm{GF}(q)} (-1)^{\mathrm{Tr}_{q/p}[y \mathrm{Tr}_{r/q}((g^\tau - 1)g^i)]} \\
&= \frac{1}{q} \sum_{i=0}^{n-1} \sum_{y \in \mathrm{GF}(q)} \chi(y(g^\tau - 1)g^i) \\
&= \frac{1}{q} \left[n + \sum_{y \in \mathrm{GF}(q)^*} \chi\left((g^\tau - 1) y C_0^{(N,r)} \right) \right] \\
&= \frac{1}{q} \left[n + \chi\left((g^\tau - 1) C_0^{(q+1,r)} \right) \right] \\
&= \begin{cases} 1, & \text{if } g^\tau - 1 \in C_0^{(q+1,r)} \\ q+1, & \text{otherwise.} \end{cases}
\end{aligned} \tag{5}$$

Now we prove that $g^\tau - 1 \notin C_0^{(q+1,r)}$ for all $0 \leq \tau \leq n-1$. On the contrary, suppose that $g^\tau - 1 \in C_0^{(q+1,r)}$ for some $1 \leq \tau \leq q^2$. Then there would exist an integer θ such that $0 \leq \theta < (q-1)(q^2+1)$ and

$$g^\tau - 1 = \alpha^{(q+1)\theta}. \tag{6}$$

Define $h = g^\tau$ and $\beta = \alpha^{(q+1)\theta}$. We have then $h = 1 + \beta$.

Since $g = \alpha^{q^2-1}$, we have

$$1 = h^{q^2+1} = (1+\beta)^{q^2+1} = 1 + \beta + \beta^{q^2} + \beta^{q^2+1}.$$

It follows then that

$$\beta + \beta^{q^2} = \beta^{q^2+1}. \tag{7}$$

Note that $\beta^{q^2+1} = \alpha^{(q+1)(q^2+1)\theta} \in \mathrm{GF}(q)$. We have

$$\left(\beta + \beta^{q^2}\right)^q = \beta + \beta^{q^2}.$$

This means that $\mathrm{Tr}_{q^4/q}(\beta) = 0$. It then follows that $\mathrm{Tr}_{q^4/q}(h) = \mathrm{Tr}_{q^4/q}(1+\beta) = 0$, that is

$$h + h^q + h^{q^2} + h^{q^3} = 0. \tag{8}$$

Note that $g^{q^2} = g^{-1}$. We have $h^{q^2} = h^{-1}$. It then follows from (8) that

$$h + \frac{1}{h} = \left(h + \frac{1}{h}\right)^q$$

which implies that

$$\frac{\beta^2}{1+\beta} = \frac{\beta^{2q}}{(1+\beta)^q}.$$

Simplifying this equation, we obtain

$$(\beta + \beta^q)^2 = \beta^{q+1}(\beta + \beta^q). \tag{9}$$

We now consider the following two cases. In the first case, we assume that $\beta + \beta^q \neq 0$. In this case, it follows from (9) that

$$\beta + \beta^q = \beta^{q+1}. \tag{10}$$

Adding (7) and (10) together gives

$$\beta^q + \beta^{q^2} = \beta\left(\beta^q + \beta^{q^2}\right).$$

Since $\beta + \beta^q \neq 0$, we have $\beta = 1$. It follows that $h = 0$, which is impossible.

In the second case, we assume that $\beta + \beta^q = 0$. Then we have $\beta \in \mathrm{GF}(q)$. Therefore $h = 1 + \beta$ also belongs to $\mathrm{GF}(q)$. This means that $\alpha^{(q^2-1)(q-1)\tau} = 1$. Hence

$$(q^4 - 1) | (q^2 - 1)(q-1)\tau$$

which holds if and only if

$$(q^2 + 1) | (q-1)\tau.$$

Since q is even, $\gcd(q^2+1, q-1) = 1$. It then follows that $(q^2+1)|\tau$, which is possible, since $1 \leq \tau \leq q^2$.

Thus, $g^\tau - 1 \notin C_0^{(q+1,r)}$ for all $0 \leq \tau \leq n-1$. Hence Π is a zero-difference balanced function and the other conclusions of this proposition follow from Proposition 3. □

Similar to the derivation of (5), we can obtain that

$$w_0 = \frac{1}{q}\left[n + \chi\left(C_0^{(q+1,r)}\right)\right] = 1.$$

However, the author was not able to compute the other frequencies w_i for $i \geq 1$. The reader is invited to solve this problem. Numerical examples show that the construction of CCCs of this section may not work if $(p, m) \neq (2, 4)$.

Example 3: Let $q = 2^2$. Then the code of Proposition 10 is an optimal CCC over $\mathrm{GF}(4)$ with parameters $(17, 17, 12, [1, 4, 4, 8])_4$.

VI. Concluding Remarks

There are other known zero-difference balanced functions [13]. But they do not give optimal constant composition codes with new parameters. An interesting problem is to search for new zero-difference balanced functions leading to optimal constant composition codes with new parameters under the framework of this correspondence. The reader is invited to attack this problem.

Acknowledgment

The author would thank the reviewers for their detailed comments and suggestions that much improved the quality of this correspondence, and Qing Xiang for the help of the proof of Proposition 10.

References

[1] I. F. Blake, "Permutation codes for discrete channels," *IEEE Trans. Inf. Theory*, vol. 20, no. 1, pp. 138–140, 1974.
[2] I. F. Blake, "Configuration matrices of group codes," *IEEE Trans. Inf. Theory*, vol. 20, no. 1, pp. 95–100, 1974.
[3] I. F. Blake, "Coding with permutations," *Inf. Contr.*, vol. 43, pp. 1–19, 1979.
[4] G. T. Bogdanova and S. N. Kapralov, "Enumeration of optimal ternary constant-composition codes," *Probl. Inf. Transm.*, vol. 39, no. 4, pp. 346–351, 2003.
[5] C. Carlet and C. Ding, "Highly nonlinear mappings," *J. Complex.*, vol. 20, no. 2, pp. 205–244, 2004.
[6] C. Carlet and S. Dubuc, "On generalized bent and q-ary perfect nonlinear functions," in *Proc. Fq5, Finite Fields Applic.*, D. Jungnickel and H. Niederreiter, Eds. New York: Springer Verlag, 2000, pp. 81–94.
[7] Y. M. Chee, A. C. H. Ling, S. Ling, and H. Shen, "The PBD-closure of constant composition codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2685–2692, 2007.
[8] C. J. Colbourn, T. Kløve, and A. C. H. Ling, "Permutation arrays for powerline communication and mutually orthogonal Latin squares," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1289–1291, June 2004.
[9] W. Chu, C. J. Colbourn, and P. Dukes, "Constructions for permutation codes in powerline communications," *Designs, Codes, Cryptogr.*, vol. 32, pp. 51–64, 2004.
[10] W. Chu, C. J. Colbourn, and P. Dukes, "On constant composition codes," *Discr. Appl. Math.*, vol. 154, no. 6, pp. 912–929, Apr. 2006.
[11] W. Chu, C. J. Colbourn, and P. Dukes, "Tables for constant composition codes," *J. Combin. Math. Combin. Comput.*, vol. 54, pp. 57–65, 2005.
[12] M. Deza and S. A. Vanstone, "Bounds for permutation arrays," *J. Statist. Planning Inference*, vol. 2, pp. 197–209, 1978.
[13] C. Ding, "Optimal and perfect difference systems of sets," *J. Comb. Theory Ser. A*, to be published.
[14] C. Ding, F. W. Fu, T. Kløve, and V. W. K. Wei, "Constructions of permutation arrays," *IEEE Trans. Inf. Theory*, vol. 48, no. 4, pp. 977–980, Apr. 2002.
[15] C. Ding and J. Yin, "Algebraic constructions of constant composition codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1585–1589, 2005.
[16] C. Ding and J. Yin, "Combinatorial constructions of constant composition codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3671–3674, 2005.
[17] C. Ding and J. Yin, "A construction of optimal constant composition codes," *Designs, Codes Cryptogr.*, vol. 40, no. 2, pp. 157–165, 2006.
[18] C. Ding and J. Yuan, "A family of optimal constant composition codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3668–3671, 2005.
[19] P. Frankl and M. Deza, "On the maximum number of permutations with given maximal or minimal distance," *J. Combin. Theory Ser. A*, vol. 22, pp. 352–360, 1977.
[20] F. W. Fu and T. Kløve, "Two constructions of permutation arrays," *IEEE Trans. Inf. Theory*, vol. 50, no. 5, pp. 881–883, 2004.

[21] W. M. Kantor, "Commutative semifields and symplectic spreads," *J. of Algebra*, vol. 270, pp. 96–114, 2003.
[22] W. M. Kantor, "Finite semifields," in *Finite Geometries, Groups, and Computation (Proc. Conf. Pingree Park, CO Sep. 2005)*, Berlin, Germany, Sept. 2006, pp. 103–114, de Gruyter.
[23] Y. Luo, F.-W. Fu, A. J. Han Vinck, and W. Chen, "On constant composition codes over Z_q," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 3010–3016, Nov. 2003.
[24] G. Myerson, "Period polynomials and Gauss sums for finite fields," *Acta. Arithmetica*, vol. XXXIX, pp. 251–264, 1981.
[25] N. V. Semakov and V. A. Zinoviev, "Equidistant q-ary codes with maximal distance and resolvable balanced incomplete block designs," *Probl. Inf. Transm.*, vol. 4, no. 2, pp. 1–7, 1968.
[26] N. V. Semakov, V. A. Zinoviev, and G. V. Zaitsev, "A class of maximal equidistant codes," *Probl. Inf. Transm.*, vol. 5, no. 2, pp. 65–68, 1969.
[27] D. Slepian, "Permutation modulation," *Proc. IEEE*, vol. 53, pp. 228–236, 1965.
[28] T. Storer, *Cyclotomy and Difference Sets*. Chicago, IL: Markham, 1967.
[29] M. Svanström, "Construction of ternary constant-composition codes with weight three," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2644–2647, 2000.
[30] M. Svanström, P. R. J. Östergard, and G. T. Bogdanova, "Bounds and constructions for ternary constant-composition codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 1, pp. 101–111, Jan. 2002.
[31] V. A. Zinoviev, "Cascade equal-weight codes and maximal packings," *Probl. Contr. Inf. Theory*, vol. 12, no. 1, pp. 3–10, 1983.

An Explicit Construction of 2-Generator Quasi-Twisted Codes

Eric Z. Chen

***Abstract*—Quasi-twisted (QT) codes are a generalization of quasi-cyclic (QC) codes. Based on consta-cyclic simplex codes, a new explicit construction of a family of 2-generator quasi-twisted (QT) two-weight codes is presented. It is also shown that many codes in the family meet the Griesmer bound and therefore are length-optimal. New distance-optimal binary QC $[195, 8, 96]$, $[210, 8, 104]$, and $[240, 8, 120]$ codes, and good ternary QC $[208, 6, 135]$ and $[221, 6, 144]$codes are also obtained by the construction.**

***Index Terms*—Linear codes, optimal codes, quasi-cyclic codes, quasi-twisted codes, simplex codes.**

I. Introduction

As a generalization to cyclic codes, quasi-cyclic (QC) codes and quasi-twisted (QT) codes have been shown to contain many good linear codes. Many researchers have been using modern computers to search for good QC or QT codes, and many record-breaking codes are found [1]–[12]. The problem with this method is that it becomes intractable when the dimension and the length of the code become large. Unfortunately, very little is known on explicit constructions of good QC or QT codes. For 2-generator QC or QT codes, even fewer results are known [13], [14].

Manuscript received June 12, 2008; revised August 28, 2008. Current version published November 21, 2008. The material in this correspondence was presented in part at the IEEE ISIT2007, Nice, France, June 2007.

The author is with the Department of Computer Science, Kristianstad University College, 291 88 Kristianstad, Sweden (e-mail: eric.chen@hkr.se).

Communicated by I. Dumer, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2008.2006420

A linear code is called projective if any two of its coordinates are linearly independent, or in other words, if the minimum distance of its dual code is at least three. A code is said to be two-weight if it has only two nonzero weights. Projective two-weight codes are closely related to strongly regular graphs [15].

In this paper, a new explicit construction of a family of 2-generator QT two-weight codes is presented. It is the first time that a family of 2-generator QT codes is constructed systematically. It is also shown that many codes of this family are good and optimal. Examples are given to show the construction and the modular structure of the codes.

II. Quasi-Twisted Codes and Two-Weight Codes

A. Consta-Cyclic Codes

The codes discussed in the following sections are linear. A q-ary linear code is a k-dimensional subspace of an n-dimensional vector space over the finite field F_q, with minimum distance d between any two codewords. We denote a q-ary code as an $[n, k, d]_q$ code, or a binary $[n, k, d]$ code if $q = 2$. A linear $[n, k, d]_q$ code is said to be λ-consta-cyclic if there is a nonzero element λ of F_q such that for any codeword $(a_0, a_1, \ldots, a_{n-1})$, a consta-cyclic shift by one position or $(\lambda a_{n-1}, a_0, \ldots, a_{n-2})$ is also a codeword [16]. Therefore, the consta-cyclic code is a generalization of the cyclic code, and a cyclic code is a λ-consta-cyclic code with $\lambda = 1$. A consta-cyclic code can be defined by a generator polynomial.

B. Hamming Codes and Simplex Codes

Hamming codes are a family of linear single error correcting codes. For any positive integer $t > 1$ and prime power q, we have a Hamming $[n, n-t, 3]_q$ code, where $n = (q^t - 1)/(q-1)$. Further, if t and $q-1$ are relatively prime, then the Hamming code is equivalent to a cyclic code.

The dual code of a Hamming code is called the simplex code. So for any integer $t > 1$ and prime power q, there is a simplex $[(q^t - 1)/(q-1), t, q^{t-1}]_q$ code. It should be noted that a simplex code is an equidistance code, where $q^t - 1$ nonzero codewords have a weight of q^{t-1}. Let $h(x)$ be a primitive polynomial of degree t over F_q. A λ-consta-cyclic simplex $[(q^t-1)/(q-1), t, q^{t-1}]_q$ code can be defined by the generator polynomial $g(x) = (x^n - \lambda)/h(x)$, where $n = (q^t - 1)/(q-1)$ and λ has order of $q-1$ [16]. Further, a simplex code is equivalent to a cyclic code if t and$q-1$ are relatively prime.

C. Quasi-Twisted Codes

A code is said to be quasi-twisted (QT) if a consta-cyclic shift of any codeword by p positions is still a codeword. Thus a consta-cyclic code is a QT code with $p = 1$, and a quasi-cyclic (QC) code is a QT code with $\lambda = 1$. The length n of a QT code is a multiple of p, i.e., $n = pm$.

The consta-cyclic matrices are also called twistulant matrices. They are basic components in the generator matrix for a QT code. An $m \times m$ consta-cyclic matrix is defined as

$$C = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{m-1} \\ \lambda c_{m-1} & c_0 & c_1 & \cdots & c_{m-2} \\ \lambda c_{m-2} & \lambda c_{m-1} & c_0 & \cdots & c_{m-3} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \lambda c_1 & \lambda c_2 & \lambda c_3 & \cdots & c_0 \end{bmatrix} \quad (1)$$

and the algebra of $m \times m$ consta-cyclic matrices over F_q is isomorphic to the algebra in the ring $f[x]/(x^m - \lambda)$ if C is mapped onto the polynomial formed by the elements of its first row, $c(x) = c_0 + c_1 x + \ldots + c_{m-1} x^{m-1}$, with the least significant coefficient on the left. The