Title	On the constructions of constant-composition codes from perfect nonlinear functions
Author(s)	Li, Chao; Li, Qiang; Ling, San
Citation	Li, C., Li, Q., & Ling, S. (2009). On the constructions of constant-composition codes from perfect nonlinear functions. Science in China Series F: Information Sciences, 52(6), 964-973.
Date	2009
URL	http://hdl.handle.net/10220/9388
Rights	© 2009 Science in China Press and Springer. This is the author created version of a work that has been peer reviewed and accepted for publication by Science in China Series F: Information Sciences, Science in China Press and Springer. It incorporates referee's comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [http://dx.doi.org/10.1007/s11432-009-0110-0].

On the constructions of constant-composition codes from perfect nonlinear functions

LI Chao [1,2†] , LI Qiang[1] & LING San[3]

[1] Department of Mathematics and System Sciences, Science College, National University of Defense Technology, Changsha 410073, China;
[2] National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China;
[3] Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637313, Republic of Singapore
[†] Corresponding author (email: lichao_nudt@sina.com)

A new construction of constant-composition codes based on all known perfect nonlinear functions from F_{q^m} to itself is presented, which provides a kind of unified constructions of constant-composition codes based on all known perfect nonlinear functions from F_{q^m} to itself. It is proved that the new constant-composition codes are optimal with respect to the Luo-Fu-Vinck-Chen bound, when *m* is an odd positive integer greater than 1. Finally, we point out that two constructions of constant-composition codes, proposed by Ding Cunsheng et al. in 2005, are equivalent to two special types of the new constant-composition codes.

constant-composition codes, perfect nonlinear functions, quadratic forms

---

Highly nonlinear functions are widely used in cryptography, coding theory and sequences. Let $(A, +)$ and $(B, +)$ be two abelian groups of order n and m, respectively. A function $f: A \to B$ is called perfect nonlinear if $f(x+a) - f(x)$ is a balanced function from A to B for every $a \in A^*$, where $A^* = A\backslash\{0\}$. In particular, if f is a perfect nonlinear function from $(F_{q^m}, +)$ to itself, where F_{q^m} denotes the finite field of order q^m, then $f(x+a) - f(x)$ must be a permutation from F_{q^m} to itself for every $a \in F_{q^m}^*$. It follows that the characteristic of F_{q^m} must be an odd prime. It seems very hard to construct perfect nonlinear functions from F_{q^m} to itself[1]. Up to now, all known perfect nonlinear functions from F_{q^m} to itself are equivalent to one of the following functions in refs. [2, 3], where q is an odd prime power.

(1) $\prod_1(x) = x^{q^t+1}$, where $t \geq 0$ is an integer and $\frac{m}{\gcd(m,t)}$ is odd;

(2) $\prod_2(x) = x^{\frac{3^k+1}{2}}$, where $q = 3$, k is odd and $\gcd(m,k) = 1$;

(3) $\prod_3(x) = x^{10} - ux^6 - u^2x^2$, where $q = 3$, m is odd and $u \in F_{q^m}^*$.

$\prod_1(x) = x^{q^t+1}$, $\prod_2(x) = x^{\frac{3^k+1}{2}}$ and $\prod_3(x) = x^{10} - ux^6 - u^2x^2$ are said to be the first, second and third perfect nonlinear functions, respectively. It is noted that $\prod(x) = x^2$ is a first perfect nonlinear function with $t = 0$ and it is also a second perfect nonlinear

function with k = 1. In this paper, all known perfect nonlinear functions from F_{q^m} to itself are referred to as $\prod_1(x)$, $\prod_2(x)$and $\prod_3(x)$.

Constant-weight codes play an important role in coding theory, and have been extensively studied by many researchers. For good survey papers, see Agrell et al.[4] and Brouwer et al.[5]. As a special type of constant-weight codes, constant-composition codes have attracted much attention[6-10] in recent years, due to their mathematical interest and real applications. It is often very hard to construct optimal constant-composition codes. Recently, Ding et al.[9,10] presented some constructions of optimal constant-composition codes, using some special perfect nonlinear functions from F_{q^m} to itself. A family of optimal q-ary constant-composition codes from $\prod(x) = x^2$ was constructed by using the theory of Gauss Sums in ref. [9], and another family of optimal ternary constant-composition codes from $\prod(x) = x^{10} - ux^6 - u^2x^2$ was constructed by using the skew Hadamard difference set in ref. [10].

In this paper, we present a new construction of constant-composition codes based on all known perfect nonlinear functions from F_{q^m} to itself by using the theory of quadratic forms over finite fields, which gives a kind of unified construction of constant-composition codes for all known perfect nonlinear functions from F_{q^m} to itself. It turns out that the new constant-composition codes are optimal with respect to the Luo-Fu-Vinck-Chen bound[11], when m is an odd positive integer greater than 1. Finally, we point out that two constructions of constant-composition codes, proposed in refs. [9, 10] respectively, are equivalent to two special types of the new constant-composition codes.

1 Preimage distributions of a family of perfect nonlinear functions

Let $\prod(x)$ be a known perfect nonlinear function from F_{q^m} to itself. According to the properties of trace functions (see Theorem 2.23 in ref. [12]), $\mathrm{tr}(a\prod(x))$ must be a perfect nonlinear function from F_{q^m} to F_q for every $a \in F_{q^m}^*$, where $\mathrm{tr}(\cdot)$ denotes the trace function from F_{q^m} to F_q, i.e., $\mathrm{tr}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{m-1}}$ for all $x \in F_{q^m}$. In this section, we will present the properties of preimage distribution of $\mathrm{tr}(a\prod(x))$ for all known perfect nonlinear functions $\prod(x)$ from F_{q^m} to itself.

Lemma 1[12]. Let $f(x_1, x_2, \ldots, x_n)$ be a quadratic form of rank r over F_q, where q is an odd prime power. Then, $f(x_1, x_2, \ldots, x_n)$ is equivalent to a diagonal quadratic form $a_1y_1^2 + a_2y_2^2 + \cdots + a_ry_r^2$, where $a_1, a_2, \ldots, a_r$ are nonzero elements of F_q.

Lemma 2[12]. Let m be a positive integer, q be an odd prime power, η be the quadratic character of F_q, and $b \in F_q$. If $f(x_1, x_2, \ldots, x_n)$ is a nondegenerate quadratic form over F_q, and Δ denotes the determinant of f, then the number of solutions in F_q^n of the equation $f(x_1, x_2, \ldots, x_n) = b$ is given by

$$\begin{cases} q^{n-1} + q^{\frac{n-1}{2}}\eta((-1)^{\frac{n-1}{2}}b\Delta) & \text{when } n \text{ is odd,} \\ q^{n-1} + v(b)q^{\frac{n-2}{2}}\eta((-1)^{\frac{n}{2}}\Delta) & \text{when } n \text{ is even,} \end{cases}$$

where $v(\cdot)$ is defined by $v(b) = -1$ for $b \in F_q^*$ and $v(0) = q - 1$.

Theorem 1. Let q be an odd prime power and let m be a positive integer greater than 1. Then, for every $a \in F_{q^m}^*$, $\mathrm{tr}(a\prod(x))$ is a nondegenerate quadratic form of m indeterminates over F_q for $\prod(x) = \prod_1(x)$ or $\prod_3(x)$, and a homogenous polynomial of degree $k + 1$ of m indeterminates over F_q for $\prod(x) = \prod_2(x)$, where k is the parameter of $\prod_2(x)$.

Proof. We only give the proofs for $\prod(x) = \prod_1(x)$ and $\prod_2(x)$, the case of $\prod(x) = \prod_3(x)$ is verified in a way similar to that of $\prod(x) = \prod_1(x)$.

Case 1. $\prod(x) = \prod_1(x)$.

Let $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ be a basis of F_{q^m} over F_q, and denote the coordinates of x with respect to the basis $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ by $(x_1, x_2, \dots, x_m) \in F_q^m$ for every $x \in F_{q^m}$, i.e., $x = \sum_{i=1}^m \alpha_i x_i$. Then,

$$\mathrm{tr}(x^{q^t+1}) = \mathrm{tr}\left(a\left(\sum_{i=1}^m \alpha_i x_i\right)^{q^t+1}\right)$$

$$= \mathrm{tr}\left(a\left(\sum_{i=1}^m \alpha_i^{q^t} x_i\right)\left(\sum_{j=1}^m \alpha_j x_j\right)\right)$$

$$= \sum_{i,j=1}^m \mathrm{tr}(a\alpha_i^{q^t}\alpha_j)x_i x_j.$$

It follows that $\mathrm{tr}(ax^{q^t+1})$ is a quadratic form over F_q.

If the rank of $\mathrm{tr}(ax^{q^t+1})$ is r, it follows from Lemma 1 that $\mathrm{tr}(ax^{q^t+1})$ is independent of $m - r$ coordinates. Therefore, the rank r of $\mathrm{tr}(ax^{q^t+1})$ can be determined by

$$q^{m-r} = |\{z \in F_{q^m} \mid f_a(x+z) = f_a(x) \text{ for all } x \in F_{q^m}\}|,$$

where $f_a(\mathrm{x}) = \mathrm{tr}(ax^{q^t+1})$, which implies that $f_a(\mathrm{x})$ is a nondegenerate quadratic form of m indeterminates over F_q if and only if there is only the zero element of F_{q^m} such that $f_a(x+z) = f_a(x)$ for all $x \in F_{q^m}$. Note that $f_a(x+z) = f_a(x)$ if and only if $\mathrm{tr}(a(\prod(x+z) - \prod(x))) = 0$. If $z \neq 0$, then $\prod(x+z) - \prod(x)$ is a permutation from F_{q^m} to itself as x ranges over all elements of F_{q^m}, since $\prod(x)$ is a perfect nonlinear

function from F_{q^m} to itself. It follows that it is impossible that $\mathrm{tr}(a(\prod(x+z)-\prod(x)))=0$ for all $x \in F_{q^m}$ when $z \neq 0$, which implies that there is only the zero element such that $f_a(x+z)=f_a(x)$ for all $x \in F_{q^m}$. Therefore $f_a(x)=\mathrm{tr}(a\prod(x))$ is a nondegenerate quadratic form of m indeterminates over F_q.

Case 2. $\prod(x)=\prod_2(x)$.

Let $\{\alpha_1,\alpha_2,\ldots,\alpha_m\}$ be a basis of F_{3^m} over F_3, and denote the coordinates of x with respect to the basis $\{\alpha_1,\alpha_2,\ldots,\alpha_m\}$ by $(x_1,x_2,\ldots,x_m) \in F_3^m$ for every $x \in F_{3^m}$. Then,

$$
\begin{aligned}
&\mathrm{tr}\left(ax^{\frac{3^k+1}{2}}\right)\\
&=\mathrm{tr}\left(a\left(\sum_{i=1}^{m}\alpha_i x_i\right)^{2+3^{k-1}+3^{k-2}+\cdots+3^1}\right)\\
&=\mathrm{tr}\left(a\left(\sum_{i_1=1}^{m}\alpha_{i_1}x_{i_1}\right)\left(\sum_{i_2=1}^{m}\alpha_{i_2}x_{i_2}\right)\right.\\
&\quad\cdot\left(\sum_{i_3=1}^{m}\alpha_{i_3}^{3^{k-1}}x_{i_3}\right)\left(\sum_{i_4=1}^{m}\alpha_{i_4}^{3^{k-2}}x_{i_4}\right)\\
&\quad\left.\cdots\left(\sum_{i_{k+1}=1}^{m}\alpha_{i_{k+1}}^{3}x_{i_{k+1}}\right)\right)\\
&=\mathrm{tr}\left(a\left(\sum_{i_1,i_2,\cdots,i_{k+1}=1}^{m}\alpha_{i_1}\alpha_{i_2}\alpha_{i_3}^{3^{k-1}}\cdots\right.\right.\\
&\qquad\left.\left.\alpha_{i_{k+1}}^{3}x_{i_1}x_{i_2}\cdots x_{i_{k+1}}\right)\right)\\
&=\sum_{i_1,i_2,\cdots,i_{k+1}=1}^{m}\mathrm{tr}(a\alpha_{i_1}\alpha_{i_2}\alpha_{i_3}^{3^{k-1}}\cdots\alpha_{i_{k+1}}^{3})x_{i_1}x_{i_2}\\
&\quad\cdots x_{i_{k+1}}.
\end{aligned}
$$

Hence, $\mathrm{tr}(ax^{\frac{3^k+1}{2}})$ is a homogeneous polynomial of degree $k+1$ in $F_3[x_1,x_2,\cdots,x_m]$.

For simplicity in notation, we denote

$$F_q=\{0,\beta^1,\beta^2,\cdots,\beta^{q-2},\beta^{q-1}\},$$

where β is a primitive element of F_q, and let

$$\begin{aligned} k_0 &= |\{x \in F_{q^m} \mid \mathrm{tr}(a\Pi(x)) = 0\}|, \\ k_i &= |\{x \in F_{q^m} \mid \mathrm{tr}(a\Pi(x)) = \beta^i\}|, \\ & i = 1, 2, \cdots, q-1. \end{aligned} \tag{1}$$

where $\prod(x)$ is a known perfect nonlinear function from F_{q^m} to itself. $(k_0, k_1, \ldots, k_{q-1})$ is called the preimage distribution of $\mathrm{tr}(a\prod(x))$. According to Theorem 1, $\mathrm{tr}(a\prod_2(x))$ is a quadratic form over F_3 only when $k = 1$, where k is the parameter of $\prod_2(x)$. However, we find out that the preimage distributions of $\mathrm{tr}(a\prod(x))$ for $\prod(x) = \prod_1(x)$ or $\prod_2(x)$ are the same as that of $\mathrm{tr}(ax^2)$.

Lemma 3. (1) If m is a positive integer and t is a nonnegative integer such that $\frac{m}{\gcd(m,t)}$ is odd, then $\gcd(q^t + 1, q^m - 1) = 2$, where q is an odd prime power.

(2) If m is a positive integer and k is an odd positive integer such that $\gcd(m, k) = 1$, then $\gcd\left(\frac{3^k+1}{2}, 3^m - 1\right) = 2$.

Proof. (1) Set $u = \gcd(m, t), m = um_1, t = ut_1$. Then $\gcd(m_1, t_1) = 1$ and m_1 is odd. Note that

$$\begin{aligned} &\gcd(q^{2t} - 1, q^m - 1) = q^{\gcd(2t,m)} - 1 \\ &= q^{u\cdot\gcd(2t_1,m_1)} - 1 = q^u - 1. \end{aligned}$$

Let $d = \gcd(q^t + 1, q^m - 1)$. Clearly, d is a multiple of 2. On the other hand, noting that $d \mid \gcd(q^{2t} - 1, q^m - 1) = q^u - 1$ and $(q^u - 1) \mid (q^t - 1)$, we obtain $d \mid \gcd(q^t + 1, q^t - 1) = 2$. Therefore $d = 2$, i.e., $\gcd(q^t + 1, q^m - 1) = 2$.

(2) Since k is odd, we have

$$3^k + 1 = (3 + 1)(3^{k-1} - 3^{k-2} + 3^{k-3} - \cdots - 3 + 1).$$

Hence, we have $\frac{3^k+1}{2} = 2s$, where $s = 3^{k-1} - 3^{k-2} + 3^{k-3} - \cdots - 3 + 1$ is an odd positive integer. Let $d = \gcd(\frac{3^k+1}{2}, 3^m - 1)$. Clearly, d is a multiple of 2. If p is any prime factor of d, then

$$p \mid \gcd(3^{2k}-1, 3^m-1) = 3^{\gcd(2k,m)}-1 = 3^{\gcd(2,m)}-1$$

due to $3^{2k} - 1 = (3^k + 1)(3^k - 1)$ and $\gcd(m, k) = 1$. It follows that $p = 2$, which

implies that $d = 2^l$, where l is a positive integer. Note that $d \mid \frac{3^k+1}{2} = 2s$ and s is odd. Then $d = 2$, i.e., $\gcd(\frac{3^k+1}{2}, 3^m - 1) = 2$.

Lemma 4. Let q be an odd prime power and let m be a positive integer greater than 1. If $\prod(x) = \prod_1(x)$ or $\prod_2(x)$, then for every $a \in F_{q^m}^*$, the preimage distribution of $\mathrm{tr}(a\prod(x))$ is the same as that of $\mathrm{tr}(ax^2)$.

Proof. We only give the proof for $\prod(x) = \prod_1(x)$, the other cases are similarly verified.

Let $b \in F_{q^m}$. When $b = 0$, $x^{q^t+1} = b$ and $x^2 = b$ both have only the zero solution in F_{q^m}. Next, assume $b \neq 0$. Let α be a primitive element of F_{q^m}. Then $b = \alpha^j$ for some integer j. The equation $x^{q^t+1} = b$ has a solution $\gamma = \alpha^i \in F_{q^m}$ if and only if $i(q^t + 1) \equiv j \bmod q^m - 1$. Similarly, $x^2 = b$ has a solution $\delta = \alpha^k \in F_{q^m}$ if and only if $2k \equiv j \bmod q^m - 1$. Since $\gcd(q^t + 1, q^m - 1) = 2$ from Lemma 3, $i(q^t + 1) \equiv j \bmod q^m - 1$ has a solution for i if and only if $2k \equiv j \bmod q^m - 1$ has a solution for k, and, in this case, the number of solutions for each congruence is 2. Hence, for each $b \neq 0$, the number of solutions of $x^{q^t+1} = b$ in F_{q^m} is equal to that of $x^2 = b$ in F_{q^m}, which suggests that

$$\begin{aligned}&\sharp\{x \mid x \in F_{q^m},\ \mathrm{tr}(ax^{q^t+1}) = c\}\\ =&\sharp\{x \mid x \in F_{q^m},\ \mathrm{tr}(ax^2) = c\},\end{aligned}$$

for every $c \in F_q$.

For every $a \in F_{q^m}^*$, we use Δ_a to denote the determinant of quadratic form $\mathrm{tr}(a\prod(x))$, where $\prod(x) = x^2$ or $x^{10} - ux^6 - u^2x^2$, $u \neq 0$.

Lemma 5. Let q be an odd prime power, let m be a positive integer greater than 1 and let η be the quadratic character of F_q. If $\prod(x) = x^2$, then $\eta(\Delta_a)$ is the same for all nonzero squares $a \in F_{q^m}$, and $\eta(\Delta_a)$ is also the same for all non-squares $a \in F_{q^m}$. Furthermore, $\eta(\Delta_a) = 1$ (resp -1) for nonzero squares if and only if $\eta(\Delta_a) = -1$ (resp 1) for nonsquares.

Proof. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ be a basis of F_{q^m} over F_q, and for every $x \in F_{q^m}$, the coordinates of x with respect to $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ is denoted by $(x_1, x_2, \ldots, x_m)$. Then, the determinant of $\mathrm{tr}(ax^2) = \sum_{i,j=1}^m \mathrm{tr}(a\alpha_i\alpha_j)x_ix_j$, where $a \in F_{q^m}^*$, is given by

$$\Delta_a = \begin{vmatrix} \mathrm{tr}(a\alpha_1\alpha_1) & \mathrm{tr}(a\alpha_1\alpha_2) & \cdots & \mathrm{tr}(a\alpha_1\alpha_m) \\ \mathrm{tr}(a\alpha_2\alpha_1) & \mathrm{tr}(a\alpha_2\alpha_2) & \cdots & \mathrm{tr}(a\alpha_2\alpha_m) \\ \vdots & \vdots & & \vdots \\ \mathrm{tr}(a\alpha_m\alpha_1) & \mathrm{tr}(a\alpha_m\alpha_2) & \cdots & \mathrm{tr}(a\alpha_m\alpha_m) \end{vmatrix}$$

$$= \begin{vmatrix} a\alpha_1 & (a\alpha_1)^q & \cdots & (a\alpha_1)^{q^{m-1}} \\ a\alpha_2 & (a\alpha_2)^q & \cdots & (a\alpha_2)^{q^{m-1}} \\ \vdots & \vdots & & \vdots \\ a\alpha_m & (a\alpha_m)^q & \cdots & (a\alpha_m)^{q^{m-1}} \end{vmatrix}$$

$$\cdot \begin{vmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_m^q \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \cdots & \alpha_m^{q^{m-1}} \end{vmatrix}$$

$$= a^{\frac{q^m-1}{q-1}}$$

$$\cdot \begin{vmatrix} \mathrm{tr}(\alpha_1\alpha_1) & \mathrm{tr}(\alpha_1\alpha_2) & \cdots & \mathrm{tr}(\alpha_1\alpha_m) \\ \mathrm{tr}(\alpha_2\alpha_1) & \mathrm{tr}(\alpha_2\alpha_2) & \cdots & \mathrm{tr}(\alpha_2\alpha_m) \\ \vdots & \vdots & & \vdots \\ \mathrm{tr}(\alpha_m\alpha_1) & \mathrm{tr}(\alpha_m\alpha_2) & \cdots & \mathrm{tr}(\alpha_m\alpha_m) \end{vmatrix}$$

$$= a^{\frac{q^m-1}{q-1}} \cdot \Delta(\alpha_1, \alpha_2, \cdots, \alpha_m),$$

where

$$\Delta(\alpha_1, \alpha_2, \cdots, \alpha_m) =$$

$$\begin{vmatrix} \mathrm{tr}(\alpha_1\alpha_1) & \mathrm{tr}(\alpha_1\alpha_2) & \cdots & \mathrm{tr}(\alpha_1\alpha_m) \\ \mathrm{tr}(\alpha_2\alpha_1) & \mathrm{tr}(\alpha_2\alpha_2) & \cdots & \mathrm{tr}(\alpha_2\alpha_m) \\ \vdots & \vdots & & \vdots \\ \mathrm{tr}(\alpha_m\alpha_1) & \mathrm{tr}(\alpha_m\alpha_2) & \cdots & \mathrm{tr}(\alpha_m\alpha_m) \end{vmatrix}$$

is the discriminant of the elements $\alpha_1, \alpha_2, \ldots, \alpha_m$. Since $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ is a basis of F_{q^m} over F_q, $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_m)$ is a nonzero element of F_q (see Theorem 2.37 in ref. [12]). Let

α be a primitive element of F_{q^m} . Then $\beta = \alpha^{\frac{q^m-1}{q-1}}$ is a primitive element of F_q. If a is a nonzero square of F_{q^m}, then $a = \alpha^{2l}$, l bing some integer. It follows that

$$\begin{aligned}\Delta_a &= a^{\frac{q^m-1}{q-1}} \cdot \Delta(\alpha_1, \alpha_2, \cdots, \alpha_m) \\ &= \beta^{2l} \cdot \Delta(\alpha_1, \alpha_2, \cdots, \alpha_m).\end{aligned}$$

If a is a nonsquare of F_{q^m}, then $a = \alpha^{2l+1}$,, where l is some integer. It follows that

$$\begin{aligned}\Delta_a &= a^{\frac{q^m-1}{q-1}} \cdot \Delta(\alpha_1, \alpha_2, \cdots, \alpha_m) \\ &= \beta^{2l+1} \cdot \Delta(\alpha_1, \alpha_2, \cdots, \alpha_m).\end{aligned}$$

Therefore, $\eta(\Delta_a) = \eta(\Delta(\alpha_1, \alpha_2, \ldots, \alpha_m))$ for every nonzero square of F_{q^m}, while $\eta(\Delta_a) = -\eta(\Delta(\alpha_1, \alpha_2, \ldots, \alpha_m))$for every nonsquare of F_{q^m}.

Theorem 2. Let q be an odd prime power, let m be a positive integer greater than 1 and let η be the quadratic character of F_q. Then, for every nonzero $a \in F_{q^m}$, the preimage distributions $(k_0, k_1, k_2, \ldots, k_{q-1})$ of $\mathrm{tr}(a\prod(x))$ have the following properties, where $\prod(x)$ is a known perfect nonlinear function.

(1) If m is odd, then

$$\begin{aligned}&(k_0, k_1, k_2, \cdots, k_{q-1}) = (q^{m-1}, q^{m-1} - q^{\frac{m-1}{2}}, \\ &q^{m-1} + q^{\frac{m-1}{2}}, \cdots, q^{m-1} - q^{\frac{m-1}{2}}, q^{m-1} + q^{\frac{m-1}{2}}),\end{aligned}$$

or

$$\begin{aligned}&(k_0, k_1, k_2, \cdots, k_{q-1}) = (q^{m-1}, q^{m-1} + q^{\frac{m-1}{2}}, \\ &q^{m-1} - q^{\frac{m-1}{2}}, \cdots, q^{m-1} + q^{\frac{m-1}{2}}, q^{m-1} - q^{\frac{m-1}{2}}).\end{aligned}$$

(2) If m is even, then

$$\begin{aligned}&(k_0, k_1, k_2, \cdots, k_{q-1}) = (q^{m-1} + (q-1)q^{\frac{m-2}{2}}, \\ &q^{m-1} - q^{\frac{m-2}{2}}, q^{m-1} - q^{\frac{m-2}{2}}, \cdots, q^{m-1} - q^{\frac{m-2}{2}}),\end{aligned}$$

or

$$\begin{aligned}&(k_0, k_1, k_2, \cdots, k_{q-1}) = (q^{m-1} - (q-1)q^{\frac{m-2}{2}}, \\ &q^{m-1} + q^{\frac{m-2}{2}}, q^{m-1} + q^{\frac{m-2}{2}}, \cdots, q^{m-1} + q^{\frac{m-2}{2}}).\end{aligned}$$

Proof. We give the proof for the case of m odd, the case of m even is similarly verified.

Note that q is an odd prime power. It follows that $\eta(-1) = 1$ if $q \equiv 1 \pmod 4$ and $\eta(-1) = -1$ if $q \equiv 3 \pmod 4$. According to Lemma 4, we only need to consider the preimage distributions of $\mathrm{tr}(a\prod(x))$ for $\prod(x) = x^2$ and $x^{10} - ux^6 - u^2x^2$. If m is odd, from Theorem 1 and Lemma 2, for any $b \in F_q$, the number n_b of solutions in F_{q^m} of equation $\mathrm{tr}(a\prod(x)) = b$ is given by

$$n_b = q^{m-1} + q^{\frac{m-1}{2}}\eta((-1)^{\frac{m-1}{2}}b\Delta_a),$$

where Δ_a is denoted as above.
If $\eta(\Delta_a) = 1$, then

$$\begin{cases} n_0 = q^{m-1}, \\ n_{\beta^{2l}} = q^{m-1} + q^{\frac{m-1}{2}}\eta((-1)^{\frac{m-1}{2}}), \\ \qquad l = 1, 2, \cdots, \frac{q-1}{2}, \\ n_{\beta^{2l+1}} = q^{m-1} - q^{\frac{m-1}{2}}\eta((-1)^{\frac{m-1}{2}}), \\ \qquad l = 0, 1, \cdots, \frac{q-3}{2}. \end{cases}$$

It follows that

$$(k_0, k_1, k_2, \cdots, k_{q-1}) = (q^{m-1}, q^{m-1} - q^{\frac{m-1}{2}}, \\ q^{m-1} + q^{\frac{m-1}{2}}, \cdots, q^{m-1} - q^{\frac{m-1}{2}}, q^{m-1} + q^{\frac{m-1}{2}})$$

in the case where $m \equiv 1 \pmod 4$, or $m \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$, and

$$(k_0, k_1, k_2, \cdots, k_{q-1}) = (q^{m-1}, q^{m-1} + q^{\frac{m-1}{2}}, \\ q^{m-1} - q^{\frac{m-1}{2}}, \cdots, q^{m-1} + q^{\frac{m-1}{2}}, q^{m-1} - q^{\frac{m-1}{2}})$$

in the case where $m \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$.
If $\eta(\Delta_a) = -1$, then

$$\begin{cases} n_0 = q^{m-1}, \\ n_{\beta^{2l}} = q^{m-1} - q^{\frac{m-1}{2}}\eta((-1)^{\frac{m-1}{2}}), \\ \qquad l = 1, 2, \cdots, \frac{q-1}{2}, \\ n_{\beta^{2l+1}} = q^{m-1} + q^{\frac{m-1}{2}}\eta((-1)^{\frac{m-1}{2}}), \\ \qquad l = 0, 1, \cdots, \frac{q-3}{2}. \end{cases}$$

It follows that

$$(k_0, k_1, k_2, \cdots, k_{q-1}) = (q^{m-1}, q^{m-1} + q^{\frac{m-1}{2}}, \\ q^{m-1} - q^{\frac{m-1}{2}}, \cdots, q^{m-1} + q^{\frac{m-1}{2}}, q^{m-1} - q^{\frac{m-1}{2}}),$$

in the case where $m \equiv 1 \pmod 4$, or $m \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$, and

$$(k_0, k_1, k_2, \cdots, k_{q-1}) = (q^{m-1}, q^{m-1} - q^{\frac{m-1}{2}}, \\ q^{m-1} + q^{\frac{m-1}{2}}, \cdots, q^{m-1} - q^{\frac{m-1}{2}}, q^{m-1} + q^{\frac{m-1}{2}}),$$

in the case where $m \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$.

2 Constructions of constant-composition codes from perfect nonlinear functions

A $(n, M, d, [\omega_0, \omega_1, \ldots, \omega_{q-1}]; q)$ constant-composition code is a code over an additive group $G = \{a_i \mid i = 0, 1, 2, \ldots, q-1\}$ of order q with length n, size M, and minimum distance d such that the element a_i appears exactly ω_i times in every code-word for every i. In 2003, Luo, Fu, Vinck and Chen[11] developed the following upper bound for constant-composition codes:

$$A_q(n, d, [\omega_0, \omega_1, \cdots, \omega_{q-1}]) \\ \leqslant \frac{nd}{nd - n^2 + (\omega_0^2 + \omega_1^2 + \cdots + \omega_{q-1}^2)}, \qquad (2)$$

if $nd - n^2 + (\omega_0^2 + \omega_1^2 + \cdots + \omega_{q-1}^2) > 0$, where $A_q(n, d, [\omega_0, \omega_1, \ldots, \omega_{q-1}])$ denotes the maximum size of a constant-composition code of length n, minimum distance d and composition $\omega_0, \omega_1, \ldots, \omega_{q-1}$.

A constant-composition code is called optimal with respect to the Luo-Fu-Vinck-Chen bound, if it can attain the upper bound given in (2). In this section, we present a new construction of constant-composition codes based on all known perfect nonlinear functions from F_{q^m} to itself, and demonstrate that some of them are optimal with respect to the Luo-Fu-Vinck-Chen bound. First of all, we define a class of q-ary linear codes as follows:

$$C_{(\Pi,q)} = \{c_a = (\mathrm{tr}(a\Pi(\gamma_1)), \mathrm{tr}(a\Pi(\gamma_2)), \\ \cdots, \mathrm{tr}(a\Pi(\gamma_{q^m-1}))) \mid a \in F_{q^m}\}, \qquad (3)$$

where $\gamma_1, \gamma_2, \ldots, \gamma_{q^m-1}$ are all nonzero elements of F_{q^m}, $\prod(x)$ is a known perfect nonlinear function from F_{q^m} to itself, and $\mathrm{tr}(\cdot)$ denotes the trace function from F_{q^m} to F_q.

Let β be the primitive element of F_q and denote the number of $0, \beta^1, \beta^2, \dots, \beta^{q-1}$ in the codeword c_a by $\omega_0, \omega_1, \omega_2, \dots, \omega_{q-1}$, respectively. We call $(\omega_0, \omega_1, \omega_2, \dots, \omega_{q-1})$ the frequency distribution of codeword c_a. It is easily known that $(\omega_0, \omega_1, \omega_2, \dots, \omega_{q-1}) = (k_0 - 1, k_1, k_2, \dots, k_{q-1})$, since $\mathrm{tr}(a\prod(0)) = 0$ for $\prod(x) = \prod_1(x), \prod_2(x)$ and $\prod_3(x)$. It follows from Theorem 2 that

$$(\omega_0, \omega_1, \omega_2, \dots, \omega_{q-1}) = \left(q^{m-1} - 1, q^{m-1} - q^{\frac{m-1}{2}}, q^{m-1} + q^{\frac{m-1}{2}}, \dots, q^{m-1} - q^{\frac{m-1}{2}}, q^{m-1} + q^{\frac{m-1}{2}}\right),$$

or $\left(q^{m-1} - 1, q^{m-1} + q^{\frac{m-1}{2}}, q^{m-1} - q^{\frac{m-1}{2}}, \dots, q^{m-1} + q^{\frac{m-1}{2}}, q^{m-1} - q^{\frac{m-1}{2}}\right)$ if m is odd, and

$$(\omega_0, \omega_1, \omega_2, \dots, \omega_{q-1}) = \left(q^{m-1} + (q-1)q^{\frac{m-2}{2}} - 1, q^{m-1} - q^{\frac{m-2}{2}}, q^{m-1} - q^{\frac{m-2}{2}}, \dots, q^{m-1} - q^{\frac{m-2}{2}}\right),$$

or $\left(q^{m-1} - (q-1)q^{\frac{m-2}{2}} - 1, q^{m-1} + q^{\frac{m-2}{2}}, q^{m-1} + q^{\frac{m-2}{2}}, \dots, q^{m-1} + q^{\frac{m-2}{2}}\right)$ if m is even.

A codeword c_a in $C_{(\Pi,q)}$ is called I-codeword if

$$(\omega_0, \omega_1, \omega_2, \dots, \omega_{q-1}) = \left(q^{m-1} - 1, q^{m-1} - q^{\frac{m-1}{2}}, q^{m-1} + q^{\frac{m-1}{2}}, \dots, q^{m-1} - q^{\frac{m-1}{2}}, q^{m-1} + q^{\frac{m-1}{2}}\right)$$

in the case where *m* is odd, or

$$(\omega_0, \omega_1, \omega_2, \dots, \omega_{q-1}) = \left(q^{m-1} + (q-1)q^{\frac{m-2}{2}} - 1, q^{m-1} - q^{\frac{m-2}{2}}, q^{m-1} - q^{\frac{m-2}{2}}, \dots, q^{m-1} - q^{\frac{m-2}{2}}\right)$$

in the case where *m* is even.

And a codeword c_a in $C_{(\Pi,q)}$ is called II-codeword if

$$(\omega_0, \omega_1, \omega_2, \dots, \omega_{q-1}) = \left(q^{m-1} - 1, q^{m-1} + q^{\frac{m-1}{2}}, q^{m-1} - q^{\frac{m-1}{2}}, \dots, q^{m-1} + q^{\frac{m-1}{2}}, q^{m-1} - q^{\frac{m-1}{2}}\right)$$

in the case where *m* is odd, or

$$(\omega_0, \omega_1, \omega_2, \dots, \omega_{q-1}) = \left(q^{m-1} - (q-1)q^{\frac{m-2}{2}} - 1, q^{m-1} + q^{\frac{m-2}{2}}, q^{m-1} + q^{\frac{m-2}{2}}, \dots, q^{m-1} + q^{\frac{m-2}{2}}\right)$$

in the case where *m* is even.

In the following, we demonstrate that the number of I-codewords is equal to that of II-codewords in $C_{(\Pi,q)}$ for all known perfect nonlinear functions from F_{q^m} to itself.

Theorem 3. Let *q* be an odd prime power and let *m* be a positive integer greater than 1. If $\prod(x)$ is a known perfect nonlinear function from F_{q^m} to itself, then the number of I-codewords is equal to that of II-codewords in $C_{(\Pi,q)}$.

Proof. From Lemma 4, we only need to prove the assertions for $\prod(x) = x^2$ and $x^{10} - ux^6 - u^2x^2$.

When $\prod(x) = x^2$, according to Lemma 5 and the proof of Theorem 2, the frequency distribution of the codewords c_a is the same for all the nonzero squares of F_{q^m}, and the frequency distribution of the codewords c_a is also the same for all the nonsquares of F_{q^m}. Furthermore, the codewords for nonzero squares are I-codewords if and only if the codewords for the nonsquares are II-codewords. Note that the number of the nonzero squares of F_{q^m} is equal to that of the nonsquares of F_{q^m}, which are both $\frac{q^m-1}{2}$. We conclude that the number of I-codewords is equal to that of II-codewords in $C_{(\Pi,q)}$ for$\prod(x) = x^2$.

When $\prod(x) = x^{10} - ux^6 - u^2x^2$, in the subcase, $q = 3$ and m is odd. For every $a \in F_{3^m}^*$, if c_a is a I-codeword, then the frequency distribution of the codeword

$$c_a = (\mathrm{tr}(a\Pi(\gamma_1)), \mathrm{tr}(a\Pi(\gamma_2)), \cdots, \mathrm{tr}(a\Pi(\gamma_{3^m-1})))$$

is $(\omega_0, \omega_1, \omega_2) = (3^{m-1} - 1, 3^{m-1} - 3^{\frac{m-1}{2}}, 3^{m-1} + 3^{\frac{m-1}{2}})$, and hence the frequency distribution of the codeword

$$c_{-a} = (\mathrm{tr}(-a\Pi(\gamma_1)), \mathrm{tr}(-a\Pi(\gamma_2)), \cdots, \mathrm{tr}(-a\Pi(\gamma_{3^m-1})))$$

is $(\omega_0, \omega_1, \omega_2) = \left(3^{m-1} - 1, 3^{m-1} + 3^{\frac{m-1}{2}}, 3^{m-1} - 3^{\frac{m-1}{2}}\right)$, which implies that c_{-a} is a II-codeword. Similarly, the converse is also true. Therefore, the number of I-codewords is equal to that of II-codewords in $C_{(\Pi,q))}$ for $\prod(x) = x^{10} - ux^6 - u^2x^2$.

Corollary 1. (1) If m is odd, then the weight distribution $\{A_0, A_1, \cdots, A_{q^m-1}\}$ of $C_{(\Pi,q)}$ is given as follows: all $A_i = 0$ except that

$$\begin{cases} A_0 = 1, \\ A_{(q-1)q^{m-1}} = q^m - 1. \end{cases}$$

(2) If m is even, then the weight distribution $\{A_0, A_1, \cdots, A_{q^m-1}\}$ of $C_{(\Pi,q)}$ is given as follows: all $A_i = 0$ except that

$$\begin{cases} A_0 = 1, \\ A_{(q-1)(q^{m-1}+q^{\frac{m-2}{2}})} = \dfrac{q^m-1}{2}, \\ A_{(q-1)(q^{m-1}-q^{\frac{m-2}{2}})} = \dfrac{q^m-1}{2}. \end{cases}$$

Let $C^1_{(\Pi,q)}$ and $C^2_{(\Pi,q)}$ be the set of all the I-codewords and II-codewords in $C_{(\Pi,q)}$, respectively.
Then, we have

Theorem 4. Let q be an odd prime power and let m be a positive integer greater than 1. If $\prod(x)$ is a known perfect nonlinear function from F_{q^m} to itself, then

(1) when m is odd, $C^1_{(\Pi,q)}$ is a

$$(n, M, d_1, [q^{m-1}-1, q^{m-1}-q^{\frac{m-1}{2}}, q^{m-1}+q^{\frac{m-1}{2}}, \\ \cdots, q^{m-1}-q^{\frac{m-1}{2}}, q^{m-1}+q^{\frac{m-1}{2}}]; q)$$

constant-composition code, and $C^2_{(\Pi,q)}$ is a

$$(n, M, d_1, [q^{m-1}-1, q^{m-1}+q^{\frac{m-1}{2}}, q^{m-1}-q^{\frac{m-1}{2}}, \\ \cdots, q^{m-1}+q^{\frac{m-1}{2}}, q^{m-1}-q^{\frac{m-1}{2}}]; q)$$

constant-composition code, where

$$n = q^m-1, M = \frac{q^m-1}{2}, d_1 = (q-1)q^{m-1};$$

(2) when m is even, $C^1_{(\Pi,q)}$is a

$$(n, M, d_2, [q^{m-1}+(q-1)q^{\frac{m-2}{2}}-1, \\ q^{m-1}-q^{\frac{m-2}{2}}, \cdots, q^{m-1}-q^{\frac{m-2}{2}}]; q)$$

constant-composition code, and $C^2_{(\Pi,q)}$ is a

$$(n,\ M,\ d_2,\ [q^{m-1}-(q-1)q^{\frac{m-2}{2}}-1, \\ q^{m-1}+q^{\frac{m-2}{2}}, \cdots, q^{m-1}+q^{\frac{m-2}{2}}]; q)$$

constant-composition code, where

$$n = q^m - 1,\ M = \frac{q^m - 1}{2},$$
$$d_2 = (q-1)(q^{m-1} - q^{\frac{m-2}{2}}).$$

Proof. It is clear that the lengths of the codes $C^1_{(\Pi,q)}$ and $C^2_{(\Pi,q)}$ are $q^m - 1$. Since $\mathrm{tr}(a(\prod(x)))$ is a perfect nonlinear function from F_{q^m} to F_q for every $a \in F^*_{q^m}$, we have $c_a \neq c_b$ for any $a, b \in F_{q^m}$ and $a \neq b$, which implies that the size of $C_{(\Pi,q)}$ is q^m. It follows from Theorem 3 that the size of $C^1_{(\Pi,q)}$ and $C^2_{(\Pi,q)}$ are both $\frac{q^m-1}{2}$. When m is odd, the weight of every nonzero codeword in $C_{(\Pi,q)}$ is $(q-1)q^{m-1}$. From Corollary 1, it follows that the minimum distances of $C^1_{(\Pi,q)}$ and $C^2_{(\Pi,q)}$ are both $(q-1)q^{m-1}$ in the case of m bing odd. When m is even, the weight of every codeword in $C^1_{(\Pi,q)}$ is $(q-1)(q^{m-1} - q^{\frac{m-2}{2}})$, and the weight of every codeword in $C^2_{(\Pi,q)}$ is $(q-1)(q^{m-1} + q^{\frac{m-2}{2}})$. Note that the difference of any two nonzero squares in F_{q^m} can be either square or nonsquare when $m \geq 2$, and similarly for the difference of any two nonsquares in F_{q^m} (see Lemma 6.24 in ref. [12]). Then the minimum distances of $C^1_{(\Pi,q)}$ and $C^2_{(\Pi,q)}$ are both $(q-1)(q^{m-1} - q^{\frac{m-2}{2}})$ in the case of m bing even. Finally, the frequency distributions of the codewords in the codes $C^1_{(\Pi,q)}$ and $C^2_{(\Pi,q)}$ are easily known from the definitions of $C^1_{(\Pi,q)}$ and $C^2_{(\Pi,q)}$.

Corollary 2. If m is an odd positive integer greater than 1, then both $C^1_{(\Pi,q)}$ and $C^2_{(\Pi,q)}$ are optimal constant-composition codes with respect to the Luo-Fu-Vinck-Chen bound.

Proof. We only check that the Luo-Fu-Vinck-Chen bound can be met by $C^1_{(\Pi,q)}$, while the other cases are similarly checked. The parameters of the code $C^1_{(\Pi,q)}$ are given by

$$n = q^m - 1, M = \frac{q^m - 1}{2}, d = (q-1)q^{m-1},$$
$$[\omega_0, \omega_1, \cdots, \omega_{q-1}] = [q^{m-1} - 1, q^{m-1} - q^{\frac{m-1}{2}},$$
$$q^{m-1} + q^{\frac{m-1}{2}} \cdots, q^{m-1} - q^{\frac{m-1}{2}}, q^{m-1} + q^{\frac{m-1}{2}}],$$

then we obtain

$$nd - n^2 + \omega_0^2 + \omega_1^2 + \cdots + \omega_{q-1}^2 = 2q^m - 2q^{m-1} > 0,$$

and

$$\frac{nd}{nd - n^2 + \omega_0^2 + \omega_1^2 + \cdots + \omega_{q-1}^2} = \frac{(q^m - 1)(q-1)q^{m-1}}{2q^m - 2q^{m-1}} = \frac{q^m - 1}{2} = M.$$

Therefore C_{Π}^1 is optimal with respect to the Luo-Fu-Vinck-Chen bound.

Corollary 3. If m is an even positive integer, then neither $C_{(\Pi,q)}^1$ nor $C_{(\Pi,q)}^2$ meets the conditions about the Luo-Fu-Vinck-Chen bound, but the following lower bound are obtained:

$$A_q(n, d, [q^{m-1} + (q-1)q^{\frac{m-2}{2}} - 1, q^{m-1} - q^{\frac{m-2}{2}}, \cdots, q^{m-1} - q^{\frac{m-2}{2}}]) \geqslant \frac{q^m - 1}{2},$$

$$A_q(n,\ d,\ [q^{m-1} - (q-1)q^{\frac{m-2}{2}} - 1, q^{m-1} + q^{\frac{m-2}{2}}, \cdots, q^{m-1} + q^{\frac{m-2}{2}}]) \geqslant \frac{q^m - 1}{2}, \quad (4)$$

where

$$n = q^m - 1, d = (q-1)(q^{m-1} - q^{\frac{m-2}{2}}).$$

Proof. We only check the conditions for the code $C_{(\Pi,q)}^1$. It is similarly checked for the code $C_{(\Pi,q)}^2$. Since

$$n = q^m - 1, M = \frac{q^m - 1}{2},$$
$$d = (q-1)(q^{m-1} - q^{\frac{m-2}{2}}),$$
$$[\omega_0, \omega_1, \cdots, \omega_{q-1}] = [q^{m-1} + (q-1)q^{\frac{m-2}{2}} - 1, q^{m-1} - q^{\frac{m-2}{2}}, \cdots, q^{m-1} - q^{\frac{m-2}{2}}],$$

we obtain

$$nd - n^2 + \omega_0^2 + \omega_1^2 + \cdots + \omega_{q-1}^2 = (1-q)(4q^{\frac{3m-2}{2}} + 4q^{\frac{m-2}{2}} - 8q^{m-1}) < 0.$$

Therefore it does not meet the condition about the Luo-Fu-Vinck-Chen bound. According to the definition of $A_q(n, d, [\omega_0, \omega_1 \cdots, \omega_{q-1}])$, (4) follows from Theorem 4.

In order to demonstrate that two constructions of constant-composition codes from $\prod(x) = x^2$ and $\prod(x) = x^{10} - ux^6 - u^2x^2$, proposed in refs. [9,10] respectively, are equivalent to two special types of our new constant-composition codes. From now on, we assume that $\gamma_1 = \alpha^0, \gamma_2 = \alpha^1, \gamma_3 = \alpha^2, \ldots, \gamma_{q^m-1} = \alpha^{q^m-2}$ in $C_{(\Pi,q)}$ defined by eq. (3), i.e., every codeword c_a in $C_{(\Pi,q)}$ can be represented in the following form:

$$c_a = (\mathrm{tr}(a\Pi(\alpha^0)), \mathrm{tr}(a\Pi(\alpha^1)), \mathrm{tr}(a\Pi(\alpha^2)), \cdots, \mathrm{tr}(a\Pi(\alpha^{q^m-2}))), \quad a \in F_{q^m}, \tag{5}$$

where α is the primitive element of F_{q^m}, $\prod(x)$ is a known perfect nonlinear function from F_{q^m} to itself, and $\mathrm{tr}(\cdot)$ denotes the trace function from F_{q^m} to F_q.

Lemma 6. Every nonzero codeword in $C_{(\Pi,q)}$ defined by eq. (5) is of period $\frac{q^m-1}{2}$.

Proof. When $\prod(x) = \prod_1(x)$, the general term of code sequence in eq. (5) is

$$\mathrm{tr}(a\Pi(\alpha^i)) = \mathrm{tr}(a\alpha^{(q^t+1)i}), \quad i = 0, 1, 2, \cdots q^m - 2.$$

According to the trace representation of sequences, the period of the code sequence

$$c_a = (\mathrm{tr}(a\Pi(\alpha^0)), \mathrm{tr}(a\Pi(\alpha^1)), \mathrm{tr}(a\Pi(\alpha^2)), \cdots, \mathrm{tr}(a\Pi(\alpha^{q^m-2})))$$

is equal to the order of the element α^{q^t+1} in F_{q^m}. By Lemma 3, $\gcd(q^t + 1, q^m - 1) = 2$, and then the order of α^{q^t+1} in F_{q^m} is $\frac{q^m-1}{2}$, which implies that the period of the code sequence c_a in $C_{(\Pi,q)}$ is $\frac{q^m-1}{2}$ for $\prod(x) = \prod_1(x)$. Similarly, the case of $\prod(x) = \prod_2(x)$ is also true. Now, we consider the case of $\prod(x) = \prod_3(x)$. In this subcase, the general term of code sequence c_a is

$$\mathrm{tr}(a\Pi(\alpha^i)) = \mathrm{tr}(a\alpha^{10i}) - \mathrm{tr}(ua\alpha^{6i}) - \mathrm{tr}(u^2a\alpha^{2i}), \quad i = 0, 1, 2, \cdots.$$

Note that $\gcd(10, 3^m - 1) = \gcd(6, 3^m - 1) = \gcd(2, 3^m - 1) = 2$, since m is odd. It follows that the codeword c_a is the sum of three sequences with period $\frac{3^m-1}{2}$. Therefore, c_a is of period $\frac{3^m-1}{2}$.

Denoting $c_a = (c_a^L, c_a^R)$ for every codeword in the linear code $C_{(\Pi,q)}$, namely c_a^L is the left $\frac{q^m-1}{2}$ elements and c_a^R is the right $\frac{q^m-1}{2}$ elements, we have $c_a^L = c_a^R$ from Lemma 6. Therefore, we can construct the following two classes of q-ary

codes:

$$C_{(\Pi,q)}^{1L} = \{c_a^L \mid c_a \in C_{(\Pi,q)}^1\},$$
$$C_{(\Pi,q)}^{2L} = \{c_a^L \mid c_a \in C_{(\Pi,q)}^2\}.$$

Theorem 5. Let q be an odd prime power and let m be a positive integer greater than 1. If $\prod(x)$ is a known perfect nonlinear function from F_{q^m} to itself, then

(1) when m is odd, $C_{(\Pi,q)}^{1L}$ is a

$$(n, M, d_1, [r, s, t, \cdots, s, t]; q)$$

constant-composition code, and $C_{(\Pi,q)}^{2L}$ is a

$$(n, M, d_1, [r, t, s, \cdots, t, s]; q)$$

constant-composition code, where

$$n = \frac{q^m - 1}{2},\ M = \frac{q^m - 1}{2},\ d_1 = \frac{(q-1)q^{m-1}}{2},$$
$$r = \frac{q^{m-1} - 1}{2},\ s = \frac{q^{m-1} - q^{\frac{m-1}{2}}}{2},$$
$$t = \frac{q^{m-1} + q^{\frac{m-1}{2}}}{2};$$

(2) when m is even, $C_{(\Pi,q)}^{1L}$ is a

$$\left(n, M, d_2, \left[\frac{q^{m-1} + (q-1)q^{\frac{m-2}{2}} - 1}{2}, \frac{q^{m-1} - q^{\frac{m-2}{2}}}{2}, \cdots, \frac{q^{m-1} - q^{\frac{m-2}{2}}}{2}\right]; q\right)$$

constant-composition code, and $C_{(\Pi,q)}^{2L}$ is a

$$\left(n, M, d_2, \left[\frac{q^{m-1}-(q-1)q^{\frac{m-2}{2}}-1}{2}, \frac{q^{m-1}+q^{\frac{m-2}{2}}}{2}, \cdots, \frac{q^{m-1}+q^{\frac{m-2}{2}}}{2}\right]; q\right)$$

constant-composition code, where

$$n=\frac{q^m-1}{2},\ M=\frac{q^m-1}{2},$$
$$d_2=\frac{(q-1)(q^{m-1}-q^{\frac{m-2}{2}})}{2}.$$

Proof. It is easily seen from Theorem 4 and Lemma 6.

Corollary 4. If m is an odd positive integer greater than 1, then both $C_{(\Pi,q)}^{1L}$ and $C_{(\Pi,q)}^{2L}$ are optimal constant-composition codes with respect to the Luo-Fu-Vinck-Chen bound.

Proof. It can be straightly checked similarly to the proof of Corollary 2.

Corollary 5. If m is an even positive integer, then neither $C_{(\Pi,q)}^{1L}$ nor $C_{(\Pi,q)}^{2L}$ meets the conditions about the Luo-Fu-Vinck-Chen bound, but the following lower bounds are obtained,

$$A_q\left(n, d, \left[\frac{q^{m-1}+(q-1)q^{\frac{m-2}{2}}-1}{2}, \frac{q^{m-1}-q^{\frac{m-2}{2}}}{2}, \cdots, \frac{q^{m-1}-q^{\frac{m-2}{2}}}{2}\right]\right) \geqslant \frac{q^m-1}{2},$$

$$A_q\left(n, d, \left[\frac{q^{m-1}-(q-1)q^{\frac{m-2}{2}}-1}{2}, \frac{q^{m-1}+q^{\frac{m-2}{2}}}{2}, \cdots, \frac{q^{m-1}+q^{\frac{m-2}{2}}}{2}\right]\right) \geqslant \frac{q^m-1}{2},$$

where

$$n = \frac{q^m - 1}{2}, \quad d = \frac{(q-1)(q^{m-1} - q^{\frac{m-2}{2}})}{2}.$$

Proof. It can be straightly checked similarly to the proof of Corollary 3.

From Theorem 5, we can obtain some new constant-composition codes compared with the results in refs. [5,7]. For example, when $q = 3$, the first six new ternary constant-composition codes are given in Table 1. By Corollary 4, the codes corresponding to odd m are optimal.

Finally, we point out that the q-ary constant-composition code from $\prod(x) = x^2$, proposed in ref. [9], is one of the codes $C^{1L}_{(\Pi,q)}$ and $C^{2L}_{(\Pi,q)}$ with $\prod(x) = x^2$ and odd m, and the ternary constant-composition codes from $\prod(x) = x^{10} - ux^6 - u^2x^2$ proposed in ref. [10], are equivalent to one of the codes $C^{1L}_{(\Pi,3)}$ and $C^{2L}_{(\Pi,3)}$ with $\prod(x) = x^{10} - ux^6 - u^2x^2$.

In fact, from the constructions of the codes in ref. [9], the constant-composition codes in ref. [9] are given as follows:

$$C = \{(\mathrm{tr}(a), \mathrm{tr}(a\alpha^2), \cdots, \mathrm{tr}(a\alpha^{q^m-1})) \\ |a \in (F^*_{q^m})^2\}, \quad (6)$$

where α is the primitive element of F_{q^m} and $(F^*_{q^m})^2$ denotes the set of all nonzero squares of F_{q^m}. It is easily seen that the constant-composition code defined by eq. (6) is one of the codes $C^{1L}_{(\Pi,q)}$ and $C^{2L}_{(\Pi,q)}$ with $\prod(x) = x^2$ and odd m. From the constructions of the constant-composition codes in ref. [10], we know that all the codewords of the following codes presented in ref. [10]:

$$C = \{\big(\mathrm{tr}(a\Pi(1)), \mathrm{tr}(a\Pi(\alpha^2)), \cdots, \mathrm{tr}(a\Pi(\alpha^{3^m-1}))\big) \\ |a \in F_{3^m}\},$$

where α is the primitive element of F_{3^m} and $\prod(x) = x^{10} - ux^6 - u^2x^2$, are exactly the 2-decimation of all the codewords of $C_{(\Pi,3)}$ with $\prod(x) = x^{10} - ux^6 - u^2x^2$. Note that every nonzero codeword in the code $C_{(\Pi,3)}$ is of period $\frac{3^m-1}{2}$, and $\frac{3^m-1}{2}$ is an odd positive integer since m is odd. It follows that every codeword in the constant-composition code proposed in ref. [10] is actually the rearrangement of elements of the codeword in the code $C^L_{(\Pi,q)}$ with $\prod(x) = x^{10} - ux^6 - u^2x^2$.

References

1 Carlet C, Ding C S. Highly nonlinear mappings. J Complex, 2004, 20(2): 205–244
2 Carlet C, Ding C S, Yuan J. Linear codes from perfect nonlinear mapping and their secret sharing schemes. IEEE Trans Inf Theory, 2005, 51(6): 2089–2102
3 Ding C S, Yuan J. A family of skew Hadamard difference sets. J Comb Theory Ser A, 2006, 113: 1526–1535
4 Agrell E, Vardy A, Zeger K. Upper bounds for constant-weight codes. IEEE Trans Inf Theory, 2000, 46(11): 2373–2395
5 Brouwer A E, Shearea J B, Sloane N J A, et al. A new table of constant-weight codes. IEEE Trans Inf Theory, 1990, 36(6): 1344–1380
6 Bogdanova G T, Kapralov S N. Enumeration of optimal ternary constant-composition codes. Probl Peredachi Inf, 2003, 39(4): 35–40
7 Svanström M. Constructions of ternary constant-composition codes with weight three. IEEE Trans Inf Theory, 2000, 46(7): 2644–2647
8 Svanström M, östergård P J, Bogdanova G T. Bounds and constructions for ternary constant-composition codes. IEEE Trans Inf Theory, 2002, 48(1): 101–111
9 Ding C S, Yin J. Algebraic constructions of constant-composition codes. IEEE Trans Inf Theory, 2005, 51(4): 1585– 1589
10 Ding C S, Yuan J. A family of optimal constant-composition codes. IEEE Trans Inf Theory, 2005, 51(10): 3668–3671
11 Luo Y, Fu F W, Vinck H, et al. On constant-composition codes over Z_q. IEEE Trans Inf Theory, 2003, 49(11): 3010–3016
12 Lidl R, Niederreiter H. Finite Fields. Cambridge, UK: Cambridge Univ. Press, 1997

List of Tables

Table 1

m	C_{Π}^{1L}	C_{Π}^{2L}
2	$(4, 4, 2, [2, 1, 1])$	$(4, 4, 2, [0, 2, 2])$
3	$(13, 13, 9, [4, 6, 3])$	$(13, 13, 9, [4, 3, 6])$
4	$(40, 40, 24, [16, 12, 12])$	$(40, 40, 24, [10, 15, 15])$
5	$(141, 141, 81, [40, 36, 45])$	$(141, 141, 81, [40, 45, 36])$
6	$(364, 364, 234, [130, 117, 117])$	$(364, 364, 234, [162, 126, 126])$
7	$(1093, 1093, 729, [364, 378, 351])$	$(1093, 1093, 729, [364, 351, 378])$