Properties and applications of preimage distributions of perfect nonlinear functions

Li, Chao; Li, Qiang; Ling, San

2009

Li, C., Li, Q., & Ling, S. (2009). Properties and Applications of Preimage Distributions of Perfect Nonlinear Functions. IEEE Transactions on Information Theory, 55(1), 64-69.

<https://hdl.handle.net/10356/96299>

<https://doi.org/10.1109/TIT.2008.2008126>

© 2009 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [<http://dx.doi.org/10.1109/TIT.2008.2008126>].

Downloaded on 26 Apr 2023 16:43:29 SGT

Properties and Applications of Preimage Distributions of Perfect Nonlinear Functions

Chao Li, Qiang Li, and San Ling

Abstract—The preimage distributions of perfect nonlinear functions from an Abelian group of order n to an Abelian group of order 3 or 4, respectively, are studied. Based on the properties of the preimage distributions of perfect nonlinear functions from an Abelian group of order 3^r to an Abelian group of order 3, the weight distributions of the ternary linear codes C_Π from the perfect nonlinear functions $\Pi(x)$ from F_{3^r} to itself are determined. These results suggest that two open problems, proposed by Carlet, Ding, and Yuan in 2005 and 2006, respectively, are answered.

Index Terms—Perfect nonlinear functions, preimage distributions, weight distributions.

I. INTRODUCTION

ONE of the techniques for measuring the nonlinearity of a function f from an Abelian group $(A, +)$ to another Abelian group $(B, +)$ is related to differential cryptanalysis [1]: the nonlinearity P_f of f is defined by

$$P_f = \max_{0 \neq a \in A} \max_{b \in B} \frac{|\{x \mid x \in A, f(x+a) - f(x) = b\}|}{|A|}.$$

It is easily seen that $\frac{1}{|B|} \leq P_f \leq 1$. The smaller the value of P_f , the higher the corresponding nonlinearity of f , and then the stronger the capability of f for resisting differential cryptanalysis [2]. In particular, if f is an affine function, then $P_f = 1$. A function f from A to B is called a perfect nonlinear function if $P_f = \frac{1}{|B|}$. Since the maximum of a sequence of positive real numbers equals its mean if and only if the sequence is constant, it follows that a function $f : A \rightarrow B$ is a perfect nonlinear function if and only if for every $a \in A^* = A \setminus \{0\}$ and every $b \in B$, the quantity $|\{x \mid x \in A, f(x+a) - f(x) = b\}|$ is $\frac{|A|}{|B|}$, which suggests that if there exists a perfect nonlinear function from A to B , then $|A|$ must be a multiple of $|B|$. It seems to be very hard to construct perfect nonlinear functions from a general Abelian group $(A, +)$ to another general Abelian group $(B, +)$ [4]–[6]. Let $(A, +)$ and $(B, +)$ be two Abelian groups of orders n and m , respectively, where n is a multiple of m . If f is a perfect nonlinear function from A to B , we let

$k_z = |\{x \mid x \in A, f(x) = z\}|$ for every $z \in B$. The vector $(k_z \mid z \in B)$ is called the preimage distribution of f . Determining the preimage distributions of perfect nonlinear functions is very important for studying the existence of perfect nonlinear functions [2], [5]. A fundamental characteristic of the preimage distributions of perfect nonlinear functions was given in [2] as follows.

Lemma 1: [2] If f is a perfect nonlinear function from an Abelian group $(A, +)$ of order n to an Abelian group $(B, +)$ of order m , where n is a multiple of m . Then, for every nonzero $b \in B$, the preimage distribution $(k_z \mid z \in B)$ of f has the following properties:

$$\begin{cases} \sum_{z \in B} k_z = n \\ \sum_{z \in B} k_z k_{z+b} = \frac{n(n-1)}{m} \\ \sum_{z \in B} k_z^2 = \frac{n^2 + n(m-1)}{m}. \end{cases} \quad (1)$$

Solving the above equations is the open problem in [2]. In this correspondence, we first study the properties of the preimage distributions of perfect nonlinear functions from an Abelian group of order n to an Abelian group of order 3 or 4, respectively. It turns out that the preimage distributions of these perfect nonlinear functions are related to the representations of positive integers in binary quadratic forms. We obtain all the possible preimage distributions for these perfect nonlinear functions, thus answering the first open problem in [3]. Secondly, the weight distributions of the ternary linear codes based on the perfect nonlinear functions from F_{3^r} to itself in [3] are determined by using the properties of the preimage distributions of the perfect nonlinear functions from F_{3^r} to F_3 . This presents a unified treatment for determining the weight distributions of these linear codes, which settles the remaining open case in [9].

The correspondence is organized as follows. In Section II, we describe the properties of the preimage distributions of perfect nonlinear functions from an Abelian group of order n to an Abelian group of order 3 or 4, respectively. In Section III, as an application of the preimage distributions of perfect nonlinear functions from F_{3^r} to F_3 , we determine the weight distributions of the ternary linear codes based on the perfect nonlinear functions from F_{3^r} to itself.

II. PREIMAGE DISTRIBUTIONS OF PERFECT NONLINEAR FUNCTIONS

A. Case $|B| = 3$

The only group of order 3 is $(Z_3, +)$, i.e., $(F_3, +)$. If f is a perfect nonlinear function from an Abelian group $(A, +)$ of order n to $(Z_3, +)$, where n is a multiple of 3, then the preimage distribution of f can be denoted by (k_0, k_1, k_2) , where $k_i =$

C. Li and Q. Li are with the Department of Mathematics and System Sciences, Science College, National University of Defence Technology, Changsha 410073, China (e-mail: lichao_nudt@sina.com; lzyuancn@163.com).

S. Ling is with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371, Republic of Singapore (e-mail: lingsan@ntu.edu.sg).

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

Digital Object Identifier 10.1109/TIT.2008.2008126

$|\{x \mid x \in A, f(x) = i\}|, (i = 0, 1, 2)$. In this subcase, the conditions of (1) are equivalent to the following:

$$\begin{cases} k_0 + k_1 + k_2 = n, \\ k_0^2 + k_1^2 + k_2^2 = \frac{n^2 + 2n}{3} \end{cases} \quad (2)$$

since the conditions of (2) imply that

$$k_0 k_1 + k_1 k_2 + k_2 k_0 = k_0 k_2 + k_1 k_0 + k_2 k_1 = \frac{n^2 - n}{3}.$$

Open problem 1 in [3] is to determine all integral solutions (k_0, k_1, k_2) of (2), namely, all the possible preimage distributions of the perfect nonlinear functions from an Abelian group $(A, +)$ of order n to $(Z_3, +)$. Noting that the conditions of (2) are symmetric in k_0, k_1 , and k_2 , two solutions (k_0, k_1, k_2) and (k'_0, k'_1, k'_2) of (2) are said to be equivalent if $\{k_0, k_1, k_2\} = \{k'_0, k'_1, k'_2\}$ as multisets.

The following lemma relates the solvability of the equations in (2) with the representation of positive integers in the binary quadratic form $x^2 + xy + y^2$.

Lemma 2: Let n, l be two positive integers such that $n = 3l$. Then the equations in (2) are solvable if and only if the equation $x^2 + xy + y^2 = l$ is solvable.

Proof: Assume that (2) is solvable. Let (k_0, k_1, k_2) be a solution of (2). Since $n = 3l$, it is clear that (2) is equivalent to the following equations:

$$\begin{cases} k_0 + k_1 + k_2 = 3l \\ k_0^2 + k_1^2 + k_2^2 = 3l^2 + 2l. \end{cases} \quad (3)$$

From the first equation of (3), we have $k_2 = 3l - k_0 - k_1$. Substituting k_2 into the second equation of (3), and setting $x = k_0 - l, y = k_1 - l$, we obtain

$$x^2 + xy + y^2 = l.$$

It follows that $(x, y) = (k_0 - l, k_1 - l)$ is a solution of $x^2 + xy + y^2 = l$. By reversing the above arguments, one sees immediately that the converse is also true. $\square$

It is noted from the proof of Lemma 2 that, for given positive integers n, l such that $n = 3l$, if (a, b) is a solution of $x^2 + xy + y^2 = l$, then $(k_0, k_1, k_2) = (l + a, l + b, l - (a + b))$ is a solution of the equations in (2). On the other hand, if (k_0, k_1, k_2) is a solution of the equations in (2), then $(a, b) = (k_0 - l, k_1 - l)$ is a solution of $x^2 + xy + y^2 = l$. There is therefore a one-to-one correspondence between all the solutions of the equations in (2) and all the solutions of $x^2 + xy + y^2 = l$. Furthermore, this correspondence has the following properties:

- 1) (a, b) is a solution of $x^2 + xy + y^2 = l$ if and only if (b, a) is a solution of $x^2 + xy + y^2 = l$, and the solution of (2) corresponding to (a, b) is $(k_0, k_1, k_2) = (l + a, l + b, l - (a + b))$, while that corresponding to (b, a) is $(k'_0, k'_1, k'_2) = (l + b, l + a, l - (b + a))$. These two solutions of (2) are obviously equivalent.
- 2) If (a, b) is a solution of $x^2 + xy + y^2 = l$, then so are $(-a, -b), (a + b, -a), (a + b, -b), (-a + b, a)$ and $(-a + b, b)$. Furthermore, each of the three solutions $(a, b), (-a + b, a)$ and $(-a + b, b)$ corresponds to a solution of (2) equivalent to $(k_0, k_1, k_2) = (l + a, l + b, l - (a + b))$, while each of the three solutions $(-a, -b), (a + b, -a)$

and $(a + b, -b)$ corresponds to a solution of (2) equivalent to $(k'_0, k'_1, k'_2) = (l - a, l - b, l + (a + b))$. When one of a, b , and $a + b$ is zero, $(k_0, k_1, k_2) = (l + a, l + b, l - (a + b))$ and $(k'_0, k'_1, k'_2) = (l - a, l - b, l + (a + b))$ are equivalent solutions. Otherwise, $(k_0, k_1, k_2) = (l + a, l + b, l - (a + b))$ and $(k'_0, k'_1, k'_2) = (l - a, l - b, l + (a + b))$ are two inequivalent solutions.

The following lemma from [7] gives a necessary and sufficient condition for determining whether the equation $x^2 + xy + y^2 = l$ is solvable for a given positive integer l .

Lemma 3: [7] Let l be a positive integer. Then the equation $x^2 + xy + y^2 = l$ is solvable if and only if, for every prime p dividing l such that $p \neq 3$ and $p \not\equiv 1 \pmod{6}$, an even power of p exactly divides l .

Based on Lemmas 2, 3, and the observations after Lemma 2, we can easily obtain the following theorem.

Theorem 1: Let n, l be two positive integers such that $n = 3l$. Then the equations in (2) are solvable if and only if l is a positive integer with the following form:

$$l = u^2 \cdot 3^v \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_t^{\alpha_t} \quad (4)$$

where u is a positive integer with no prime factor of the form $6k + 1$, $t, v, \alpha_1, \alpha_2, \dots, \alpha_t$ are some nonnegative integers, and $p_1, p_2, \dots, p_t$ are distinct primes of the form $6k + 1$. When the equations in (2) are solvable, all the inequivalent solutions of (2) can be given as follows:

$$(l + a, l + b, l - (a + b)), (l - a, l - b, l + (a + b)) \quad (5)$$

where a, b are nonnegative integers such that $a \geq b$ and $a^2 + ab + b^2 = l$.

Theorem 1 suggests that we can find all the integral solutions of (2) if we can obtain all the nonnegative solutions of $x^2 + xy + y^2 = l$ when l has the form (4). However, from [7], this latter task seems hard in general. Nonetheless, for some special values of n , we can obtain all the inequivalent solutions of (2). Theorem 2 presents all the inequivalent solutions of (2) for $n = 3^r$, where r is a positive integer. This result is useful for determining the weight distributions of ternary linear codes C_{Π} based on the perfect nonlinear functions $\Pi(x)$ from F_{3^r} to itself in Section III.

Theorem 2: Let $n = 3^r$, where r is a positive integer. Then,

- 1) if r is odd, the equations in (2) have exactly one inequivalent solution:

$$\left(3^{r-1} - 3^{\frac{r-1}{2}}, 3^{r-1}, 3^{r-1} + 3^{\frac{r-1}{2}}\right)$$

- 2) if r is even, the equations in (2) have exactly two inequivalent solutions:

$$\begin{aligned} &\left(3^{r-1} + 3^{\frac{r-2}{2}}, 3^{r-1} + 3^{\frac{r-2}{2}}, 3^{r-1} - 2 \cdot 3^{\frac{r-2}{2}}\right) \\ &\left(3^{r-1} - 3^{\frac{r-2}{2}}, 3^{r-1} - 3^{\frac{r-2}{2}}, 3^{r-1} + 2 \cdot 3^{\frac{r-2}{2}}\right). \end{aligned}$$

Proof: By Theorem 1, it is sufficient to find all the nonnegative solutions of $x^2 + xy + y^2 = l$, where $l = 3^{r-1}$. Solving the equation $x^2 + xy + y^2 = l$ is equivalent to solving the equation

$x^2 + 3y^2 = 4l$. Indeed, (a, b) is a solution of $x^2 + xy + y^2 = l$ if and only if $(2a + b, b)$ is a solution of $x^2 + 3y^2 = 4l$. Hence, we only need to solve the equation $x^2 + 3y^2 = 4l$, i.e.

$$x^2 + 3y^2 = 4 \cdot 3^{r-1}. \quad (6)$$

In the following, we only give the proof of the case r odd, the other case is similarly verified.

It is easily seen that the first assertion is true for $r = 1$. Now we assume that r is an odd positive integer greater than 1. If $r - 1 \geq 2$, we know from (6) that x must be a multiple of 3. Setting $x = 3x_1$, where x_1 is an integer, and replacing x by $3x_1$ in (6), we obtain

$$9x_1^2 + 3y^2 = 4 \cdot 3^{r-1}. \quad (7)$$

Therefore y is also a multiple of 3 since $r - 1 \geq 2$. Setting $y = 3y_1$, where y_1 is an integer, and replacing y by $3y_1$ in (7), then

$$x_1^2 + 3y_1^2 = 4 \cdot 3^{r-3}. \quad (8)$$

If $r - 3 \geq 2$, we can similarly obtain from (8)

$$x_2^2 + 3y_2^2 = 4 \cdot 3^{r-5}.$$

Since r is odd, proceeding as above, we finally obtain

$$x_k^2 + 3y_k^2 = 4$$

where $k = \frac{r-1}{2}$, x_k, y_k are integers such that

$$\begin{aligned} x &= 3x_1 = 3^2x_2 = \dots = 3^{\frac{r-1}{2}}x_k \\ y &= 3y_1 = 3^2y_2 = \dots = 3^{\frac{r-1}{2}}y_k. \end{aligned}$$

It is well known that all the integral values of (x_k, y_k) such that $x_k^2 + 3y_k^2 = 4$ are

$$(2, 0), (-2, 0), (1, 1), (1, -1), (-1, 1), (-1, -1).$$

It therefore follows that all the integral values of (x, y) such that $x^2 + 3y^2 = 4l$ are

$$\begin{aligned} &\left(2 \cdot 3^{\frac{r-1}{2}}, 0\right), \left(-2 \cdot 3^{\frac{r-1}{2}}, 0\right), \left(3^{\frac{r-1}{2}}, 3^{\frac{r-1}{2}}\right) \\ &\left(3^{\frac{r-1}{2}}, -3^{\frac{r-1}{2}}\right), \left(-3^{\frac{r-1}{2}}, 3^{\frac{r-1}{2}}\right), \left(-3^{\frac{r-1}{2}}, -3^{\frac{r-1}{2}}\right). \end{aligned}$$

The nonnegative solutions of $x^2 + xy + y^2 = l$ are then given by $(3^{\frac{r-1}{2}}, 0)$ and $(0, 3^{\frac{r-1}{2}})$. From Theorem 1, the only inequivalent solution of (2) is

$$\left(3^{r-1} - 3^{\frac{r-1}{2}}, 3^{r-1}, 3^{r-1} + 3^{\frac{r-1}{2}}\right).$$

This completes the proof. $\square$

B. Case $|B| = 4$

Up to isomorphism, the only Abelian groups of order 4 are $(Z_4, +)$ and $(Z_2 \times Z_2, +)$. The preimage distributions based on these two Abelian groups have different properties. Indeed, the

conditions of (2) are equivalent to the following conditions in the case when $B = Z_4$:

$$\begin{cases} k_0k_2 + k_1k_3 = \frac{n(n-1)}{8} \\ k_0 + k_1 + k_2 + k_3 = n \\ k_0^2 + k_1^2 + k_2^2 + k_3^2 = \frac{n^2+3n}{4} \end{cases} \quad (9)$$

where $k_i = |\{x \mid x \in A, f(x) = i\}|$, for $0 \leq i \leq 3$, since

$$\begin{aligned} &2(k_0k_1 + k_1k_2 + k_2k_3 + k_3k_0) \\ &= 2(k_0k_3 + k_1k_0 + k_2k_1 + k_3k_2) \\ &= (k_0 + k_1 + k_2 + k_3)^2 - (k_0^2 + k_1^2 + k_2^2 + k_3^2) \\ &\quad - 2(k_0k_2 + k_1k_3). \end{aligned}$$

On the other hand, the conditions of (2) are equivalent to the following conditions in the case when $B = Z_2 \times Z_2$:

$$\begin{cases} k_0k_1 + k_2k_3 = \frac{n(n-1)}{8} \\ k_0k_3 + k_1k_2 = \frac{n(n-1)}{8} \\ k_0k_2 + k_1k_3 = \frac{n(n-1)}{8} \\ k_0 + k_1 + k_2 + k_3 = n \\ k_0^2 + k_1^2 + k_2^2 + k_3^2 = \frac{n^2+3n}{4} \end{cases} \quad (10)$$

where

$$\begin{aligned} k_0 &= |\{x \mid x \in A, f(x) = (0, 0)\}| \\ k_1 &= |\{x \mid x \in A, f(x) = (0, 1)\}| \\ k_2 &= |\{x \mid x \in A, f(x) = (1, 0)\}| \\ k_3 &= |\{x \mid x \in A, f(x) = (1, 1)\}|. \end{aligned}$$

It is noted that the solutions of (10) must also be solutions of (9). Hence, if we can find all the solutions of (9), then we can obtain all the solutions of (10) by checking against the additional conditions in (10), so we only need to solve (9).

Considering the symmetry of the conditions of (9) in k_0, k_1, k_2 and k_3 , two solutions (k_0, k_1, k_2, k_3) and (k'_0, k'_1, k'_2, k'_3) of (9) are said to be equivalent if, as multisets, we have $\{k_0, k_2\} = \{k'_0, k'_2\}$ and $\{k_1, k_3\} = \{k'_1, k'_3\}$, or $\{k_0, k_2\} = \{k'_1, k'_3\}$ and $\{k_1, k_3\} = \{k'_0, k'_2\}$.

Theorem 3: Suppose that n is a positive integer which is a multiple of 4. Then, the equations in (9) are solvable if and only if $n = 16l^2$, where l is a positive integer, and when the equations in (9) are solvable, all the inequivalent solutions of (9) are given as follows:

$$(4l^2 + l + a, 4l^2 - l + b, 4l^2 + l - a, 4l^2 - l - b)$$

where a, b are nonnegative integers such that $4l^2 = a^2 + b^2$.

Proof: Assume that (9) is solvable and let (k_0, k_1, k_2, k_3) be a solution of (9). From the third equation of (9), we obtain

$$(k_0 + k_2)^2 + (k_1 + k_3)^2 - 2(k_0k_2 + k_1k_3) = \frac{n^2 + 3n}{4}.$$

Combined with the first equation of (9), we have

$$(k_0 + k_2)^2 + (k_1 + k_3)^2 = \frac{n^2 + n}{2}. \quad (11)$$

The following equations are obtained from (11) and the second equation of (9):

$$\begin{cases} k_0 + k_2 = \xi \\ k_1 + k_3 = \zeta \end{cases} \quad (12)$$

where

$$\xi = \frac{n + \sqrt{n}}{2}, \quad \zeta = \frac{n - \sqrt{n}}{2}$$

or

$$\xi = \frac{n - \sqrt{n}}{2}, \quad \zeta = \frac{n + \sqrt{n}}{2}.$$

We only give the proof for the case when $\xi = \frac{n + \sqrt{n}}{2}$ and $\zeta = \frac{n - \sqrt{n}}{2}$, the proof for the other case is similar.

Since ξ, ζ are integers and n is a multiple of 4, we have $n = 4t^2$, where t is a positive integer. Note that

$$k_0 k_2 + k_1 k_3 = k_0(\xi - k_0) + k_1(\zeta - k_1) = \frac{n(n-1)}{8}$$

which is equivalent to

$$\left(k_0 - \frac{\xi}{2}\right)^2 + \left(k_1 - \frac{\zeta}{2}\right)^2 = \frac{n}{4}. \quad (13)$$

Replacing ξ, ζ of (13) by $\xi = \frac{n + \sqrt{n}}{2} = 2t^2 + t$ and $\zeta = \frac{n - \sqrt{n}}{2} = 2t^2 - t$, respectively, we obtain

$$(k_0 - t^2)^2 - t(k_0 - t^2) + (k_1 - t^2)^2 + t(k_1 - t^2) = \frac{t^2}{2}.$$

Since k_0, k_1, t are integers, t must be a multiple of 2. Letting $t = 2l$, where l is a positive integer, it follows that $n = 4t^2 = 16l^2$.

Conversely, if $n = 16l^2$, where l is a positive integer, it is easily verified that $(k_0, k_1, k_2, k_3) = (4l^2 + 3l, 4l^2 - l, 4l^2 - l, 4l^2 - l)$ is a solution of (9).

It follows that the first assertion of the theorem is true. In the following, we prove the second assertion.

When $n = 16l^2$ and a, b are nonnegative integers such that $4l^2 = a^2 + b^2$, we know that $(4l^2 + l + a, 4l^2 - l + b, 4l^2 + l - a, 4l^2 - l - b)$ is a solution of (9) by a straightforward verification. Taking $a = 2l$ and $b = 0$, we see that $(k_0, k_1, k_2, k_3) = (4l^2 + 3l, 4l^2 - l, 4l^2 - l, 4l^2 - l)$ is particular solution of (9). Now suppose that (x_0, x_1, x_2, x_3) is any solution of (9) and let $t_i = x_i - k_i, i = 0, 1, 2, 3$.

First, since (x_0, x_1, x_2, x_3) and (k_0, k_1, k_2, k_3) both satisfy the second condition of (9), we obtain

$$t_0 + t_1 + t_2 + t_3 = 0. \quad (14)$$

Second, noting that

$$\begin{aligned} x_0^2 + x_1^2 + x_2^2 + x_3^2 &= (k_0 + t_0)^2 + (k_1 + t_1)^2 + (k_2 + t_2)^2 + (k_3 + t_3)^2 \\ &= (k_0^2 + k_1^2 + k_2^2 + k_3^2) + (2k_0 t_0 + 2k_1 t_1 + 2k_2 t_2 + 2k_3 t_3) \\ &\quad + (t_0^2 + t_1^2 + t_2^2 + t_3^2) \end{aligned}$$

and (x_0, x_1, x_2, x_3) and $(k_0, k_1, k_2, k_3) = (4l^2 + 3l, 4l^2 - l, 4l^2 - l, 4l^2 - l)$ both satisfy the third condition of (9), then

$$\begin{aligned} 0 &= 2(4l^2 + 3l)t_0 + 2(4l^2 - l)t_1 + 2(4l^2 - l)t_2 \\ &\quad + 2(4l^2 - l)t_3 + (t_0^2 + t_1^2 + t_2^2 + t_3^2) \end{aligned}$$

i.e.

$$\begin{aligned} 0 &= 8l^2(t_0 + t_1 + t_2 + t_3) - 2l(t_0 + t_1 + t_2 + t_3) \\ &\quad + 8lt_0 + (t_0^2 + t_1^2 + t_2^2 + t_3^2). \end{aligned}$$

It follows from (14) that

$$t_0^2 + t_1^2 + t_2^2 + t_3^2 + 8lt_0 = 0. \quad (15)$$

Third, since (x_0, x_1, x_2, x_3) and (k_0, k_1, k_2, k_3) both satisfy the first condition of (11), we can obtain the following equation by using a similar argument:

$$t_0 t_2 + t_1 t_3 + 4lt_2 = 0. \quad (16)$$

From (14) and (16), we have

$$\begin{aligned} t_1^2 + t_3^2 &= (t_1 + t_3)^2 - 2t_1 t_3 \\ &= (-t_0 - t_2)^2 - 2(-4lt_2 - t_0 t_2) \\ &= t_0^2 + t_2^2 + 4t_0 t_2 + 8lt_2. \end{aligned}$$

Combined with (15), we obtain

$$t_0^2 + t_2^2 + 2t_0 t_2 + 4lt_0 + 4lt_2 = 0$$

which can be reformulated as

$$(t_0 + t_2)^2 = -4l(t_0 + t_2).$$

Therefore $t_2 = -t_0$ or $t_2 = -4l - t_0$.

When $t_2 = -t_0$, the conditions of (14), (15), and (16) are equivalent to the following:

$$\begin{cases} t_1 + t_3 = 0 \\ t_1^2 + t_3^2 = -8lt_0 - 2t_0^2 \\ t_1 t_3 = 4lt_0 + t_0^2. \end{cases} \quad (17)$$

By solving (17), we obtain

$$t_1 = \pm \sqrt{4l^2 - (t_0 + 2l)^2}, \quad t_3 = \mp \sqrt{4l^2 - (t_0 + 2l)^2}.$$

In this subcase, (x_0, x_1, x_2, x_3) is represented as follows:

$$\begin{cases} x_0 = 4l^2 + 3l + t_0 \\ x_1 = 4l^2 - l \pm \sqrt{4l^2 - (t_0 + 2l)^2} \\ x_2 = 4l^2 - l - t_0 \\ x_3 = 4l^2 - l \mp \sqrt{4l^2 - (t_0 + 2l)^2} \end{cases} \quad (18)$$

where t_0 is an integer such that $-4l \leq t_0 \leq 0$ and $4l^2 - (t_0 + 2l)^2$ is a square. Letting $a = |t_0 + 2l|$ and $b = \sqrt{4l^2 - (t_0 + 2l)^2}$, then a, b are nonnegative integers such that $4l^2 = a^2 + b^2$, and (18) is equivalent to the following:

$$\begin{cases} x_0 = 4l^2 + l \pm a \\ x_1 = 4l^2 - l \pm b \\ x_2 = 4l^2 + l \mp a \\ x_3 = 4l^2 - l \mp b. \end{cases} \quad (19)$$

Therefore, up to equivalence, (x_0, x_1, x_2, x_3) can be expressed in the following form:

$$\begin{cases} x_0 = 4l^2 + l + a \\ x_1 = 4l^2 - l + b \\ x_2 = 4l^2 + l - a \\ x_3 = 4l^2 - l - b. \end{cases} \quad (20)$$

When $t_2 = -4l - t_0$, using the same technique as above, we obtain that (x_0, x_1, x_2, x_3) can be expressed as follows:

$$\begin{cases} x_0 = 4l^2 - l + a \\ x_1 = 4l^2 + l + b \\ x_2 = 4l^2 - l - a \\ x_3 = 4l^2 + l - b \end{cases} \quad (21)$$

which is equivalent to (20), since the equation $4l^2 = a^2 + b^2$ is symmetric in a and b . This completes the proof. $\square$

Corollary 1: Let n, l be two positive integers such that $n = 16l^2$, then the equations in (10) have exactly the following two inequivalent solutions:

$$\begin{aligned} & (4l^2 + 3l, 4l^2 - l, 4l^2 - l, 4l^2 - l) \\ &= \left(\frac{n + 3\sqrt{n}}{4}, \frac{n - \sqrt{n}}{4}, \frac{n - \sqrt{n}}{4}, \frac{n - \sqrt{n}}{4} \right) \\ & (4l^2 - 3l, 4l^2 + l, 4l^2 + l, 4l^2 + l) \\ &= \left(\frac{n - 3\sqrt{n}}{4}, \frac{n + \sqrt{n}}{4}, \frac{n + \sqrt{n}}{4}, \frac{n + \sqrt{n}}{4} \right). \end{aligned}$$

Remark: The results in Corollary 1 coincide with the results on the solutions of (10) in [3].

III. WEIGHT DISTRIBUTIONS OF TERNARY LINEAR CODES FROM PERFECT NONLINEAR FUNCTIONS

The paper [3] constructed a class of linear codes based on perfect nonlinear functions from F_q to itself as follows, where $q = p^r$, p is a prime and r is a positive integer:

$$C_\Pi = \{c_{a,b} = (f_{a,b}(\gamma_1), f_{a,b}(\gamma_2), \dots, f_{a,b}(\gamma_{q-1})) \mid a, b \in F_q\} \quad (22)$$

where $\gamma_1, \gamma_2, \dots, \gamma_{q-1}$ are all the nonzero elements of F_q , and $f_{a,b}(x) = \text{tr}(a\Pi(x) + bx)$, $a, b \in F_q$, is a function from F_q to F_p , where $\text{tr}(\cdot)$ denotes the trace function from F_q to F_p , and $\Pi(x)$ is a perfect nonlinear function from F_q to itself.

In order to determine the weight distributions of C_Π based on the perfect nonlinear functions from F_{3^r} to itself, we need the following two results.

Lemma 4: [3] Let $\Pi(x)$ be a perfect nonlinear function from F_{3^r} to itself such that $\Pi(x) = \Pi(-x)$ for all $x \in F_{3^r}$ and $\Pi(x) = 0$ if and only if $x = 0$. Then C_Π is a $[3^r - 1, 2r; 3]$ -code with minimal distance $d \geq \frac{2}{3}(3^r - 3^{\frac{r}{2}})$, and the dual code $C_\Pi^\perp$ of C_Π is a $[3^r - 1, 3^r - 1 - 2r; 3]$ -code with minimal distance $d^\perp = 4$.

Lemma 5: [8] Suppose that $\{A_0, A_1, \dots, A_n\}$ and $\{B_0, B_1, \dots, B_n\}$ denote the weight distributions of an

$[n, k; q]$ -code C and its dual code $C^\perp$, respectively. Then, for every nonnegative integer t

$$\sum_{j=0}^n j^t A_j = \sum_{j=0}^{\min\{n,t\}} (-1)^j B_j \cdot \left(\sum_{v=j}^t v! s(t, v) q^{k-v} (q-1)^{v-j} \binom{n-j}{n-v} \right)$$

where $s(t, v) = \frac{1}{v!} \sum_{i=0}^v (-1)^{v-i} \binom{v}{i} i^t$ is the second kind of Stirling number.

Theorem 4: Let r be a positive integer and let $\Pi(x)$ be a perfect nonlinear function from F_{3^r} to itself such that $\Pi(x) = \Pi(-x)$ for all $x \in F_{3^r}$ and $\Pi(x) = 0$ if and only if $x = 0$. Then,

i) if r is odd, the weight distribution of C_Π is as follows: all $A_i = 0$ except that

$$\begin{cases} A_0 = 1 \\ A_{2 \cdot 3^{r-1} - 3^{\frac{r-1}{2}}} = 3^{\frac{r-1}{2}} (3^r - 1) (3^{\frac{r-1}{2}} + 1) \\ A_{2 \cdot 3^{r-1}} = (3^{r-1} + 1) (3^r - 1) \\ A_{2 \cdot 3^{r-1} + 3^{\frac{r-1}{2}}} = 3^{\frac{r-1}{2}} (3^r - 1) (3^{\frac{r-1}{2}} - 1) \end{cases} \quad (23)$$

ii) if r is even, the weight distribution of C_Π is as follows: all $A_i = 0$ except that

$$\begin{cases} A_0 = 1 \\ A_{2 \cdot 3^{r-1} - 2 \cdot 3^{\frac{r-2}{2}}} = \frac{1}{6} (3^r - 1) (3^r + 2 \cdot 3^{\frac{r}{2}}) \\ A_{2 \cdot 3^{r-1} - 3^{\frac{r-2}{2}}} = \frac{1}{3} (3^r - 1) (3^r + 3^{\frac{r}{2}}) \\ A_{2 \cdot 3^{r-1}} = 3^r - 1 \\ A_{2 \cdot 3^{r-1} + 3^{\frac{r-2}{2}}} = \frac{1}{3} (3^r - 1) (3^r - 3^{\frac{r}{2}}) \\ A_{2 \cdot 3^{r-1} + 2 \cdot 3^{\frac{r-2}{2}}} = \frac{1}{6} (3^r - 1) (3^r - 2 \cdot 3^{\frac{r}{2}}). \end{cases} \quad (24)$$

Proof: Since $\Pi(x)$ is a perfect nonlinear function from F_{3^r} to itself, from the definition of perfect nonlinear functions and the properties of the trace function, it is easy to see that $f_{a,b}(x) = \text{tr}(a\Pi(x) + bx)$ is a perfect nonlinear function from F_{3^r} to F_3 for any $a \in F_{3^r}^*$ and $b \in F_{3^r}$. In the following, we only give the proof of the case r odd, the other case is similarly verified.

When $a = 0$, $f_{a,b}(x) = \text{tr}(bx)$ is a linear function from F_{3^r} to F_3 . If $b = 0$, then for every $x \in F_{3^r}$, $f_{0,0}(x) = 0$, the codeword $c_{0,0}$ is the zero codeword. If $b \neq 0$, then $f_{a,b}(x) = \text{tr}(bx)$ is a nonzero linear function. It follows that the weight of the codeword $c_{0,b}$ is $2 \cdot 3^{r-1}$ by using the properties of the trace function.

When $a \neq 0$, $f_{a,b}(x) = \text{tr}(a\Pi(x) + bx)$ is a perfect nonlinear function from F_{3^r} to F_3 . According to Theorem 2, the preimage distribution (k_0, k_1, k_2) of $f_{a,b}(x)$ satisfies

$$\{k_0, k_1, k_2\} = \left\{ 3^{r-1} - 3^{\frac{r-1}{2}}, 3^{r-1}, 3^{r-1} + 3^{\frac{r-1}{2}} \right\}.$$

It follows that all the possible weights of C_Π are

$$0, 2 \cdot 3^{r-1} - 3^{\frac{r-1}{2}}, 2 \cdot 3^{r-1}, 2 \cdot 3^{r-1} + 3^{\frac{r-1}{2}}.$$

It is clear that $A_0 = 1$, so we only need to calculate the frequencies of the three nonzero weights. For convenience, set

$$\alpha = 2 \cdot 3^{r-1} - 3^{\frac{r-1}{2}}, \beta = 2 \cdot 3^{r-1}, \gamma = 2 \cdot 3^{r-1} + 3^{\frac{r-1}{2}}.$$

From Lemmas 4 and 5, we have

$$\begin{cases} 1 + A_\alpha + A_\beta + A_\gamma &= 3^{2r} \\ \alpha A_\alpha + \beta A_\beta + \gamma A_\gamma &= 2 \cdot 3^{2r-1}(3^r - 1) \\ \alpha^2 A_\alpha + \beta^2 A_\beta + \gamma^2 A_\gamma &= 2 \cdot 3^{2r-2}(3^r - 1)(2 \cdot 3^r - 1) \\ \alpha^3 A_\alpha + \beta^3 A_\beta + \gamma^3 A_\gamma &= 2 \cdot 3^{2r-3}(3^r - 1)(3^r - 2) \\ &\quad \times (4 \cdot 3^r + 15). \end{cases} \quad (25)$$

Solving (25) yields the results of (23). This completes the proof. $\square$

Theorem 4 suggests the open problem in [9] is solved.

ACKNOWLEDGMENT

The authors would like to thank the anonymous referees and the Associate Editor for invaluable suggestions that have helped to improve the organization of the paper and the exposition.

REFERENCES

- [1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Crypt.*, vol. 4, no. 1, pp. 3–72, 1991.
- [2] C. Carlet and C. Ding, "Highly nonlinear mappings," *J. Complex.*, vol. 20, no. 2, pp. 205–244, 2004.
- [3] C. Carlet, C. Ding, and J. Yuan, "Linear codes from perfect nonlinear mappings and their secret sharing schemes," *IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 2089–2102, 2005.
- [4] C. Carlet and S. Dubuc, "On generalized bent and q -ary perfect nonlinear functions," in *Proc. Fifth Int. Conf. Finite Fields Applications*, Augsburg, Germany, 1999, pp. 2–6.
- [5] C. Ding and J. Yuan, "A family of skew hadamard difference sets," *J. Comb. Theory*, ser. Series A, vol. 113, pp. 1526–1535, 2006.
- [6] W. Kantor, "Finite semifields, in: Finite geometries, groups and computation," in *Proc. Conf. Pingree Park*, Berlin-New York, 2006, pp. 103–114.
- [7] U. P. Nair, "Elementary results on the binary quadratic form $a^2 + ab + b^2$," 2004 [Online]. Available: <http://arxiv.org/abs/math/0408107>
- [8] V. S. Pless and W. C. Huffman, Eds., *Handbook of Coding Theory*. Amsterdam, The Netherlands: North-Holland, 1998, vol. 1.
- [9] J. Yuan, C. Carlet, and C. Ding, "The weight distribution of a class of linear codes from perfect nonlinear functions," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 712–717, 2006.

Chao Li received the B.A. degree in mathematics in 1987 from the University of Information Engineering of China, the M.S. degree in mathematics in 1990 from the University of Science and Technology of China, and the Ph.D. degree in engineering in 2002 from the National University of Defense Technology of China.

Since December 2001, he has been a Professor with the Department of Mathematics and System Science, National University of Defense Technology of China. His research fields include: coding theory, cryptography and sequences.

Qiang Li received the B.A. degree in 2002 and the M.S. degree in mathematics in 2004 from the National University of Defense Technology of China. He is currently working towards the Ph.D. degree in the Department of Mathematics and System Science, National University of Defense Technology of China.

His research fields include: cryptography and information security.

San Ling received the B.A. degree in mathematics in 1985 from the University of Cambridge, Cambridge, U.K., in 1989 and the Ph.D. degree in mathematics in 1990 from the University of California, Berkeley.

Since April 2005, he has been a Professor with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, in the Nanyang Technological University, Singapore. Prior to that, he was with the Department of Mathematics, National University of Singapore. His research fields include: arithmetic of modular curves and application of number theory to combinatorial designs, coding theory, cryptography, and sequences.