A Note of Perfect Nonlinear Functions

Xiyong Zhang[1,2], Hua Guo[3], and Jinjiang Yuan[1]

[1] Department of Mathematics, Zhengzhou University,
450052 Zhengzhou, China
xyzhxy3711@sina.com, yuanjj@zzu.edu.cn
[2] Department of Applied Mathematics, Information Engineering University,
450002 Zhengzhou, China
xyzhxy3711@sina.com
[3] School of Computer Science Engineering, Beihang University,
100083 Beijing, China
hua.g@hotmail.com

Abstract. Perfect nonlinear functions are of importance in cryptography. By using Galois rings and investigating the character values of corresponding relative difference sets, we construct a perfect nonlinear function from $\mathbb{Z}_{p^2}^n$ to $\mathbb{Z}_{p^2}^m$ where $2m$ is possibly larger than the largest divisor of n. Meanwhile we prove that there exists a perfect nonlinear function from $\mathbb{Z}_{2p}^2$ to $\mathbb{Z}_{2p}$ if and only if $p = 2$, and that there doesn't exist a perfect nonlinear function from $\mathbb{Z}_{2^k l}^{2n}$ to $\mathbb{Z}_{2^k l}^m$ if $m > n$ and $l(l$ is odd) is *self-conjugate* modulo $2^k (k \geq 1)$.

1 Introduction

Let n, m, q, k, λ be positive integers, p be prime, and $\mathbb{Z}_q$ be the ring of rediue class modulo q. A perfect nonlinear function(abbr.PNF) $f(x)$ is a map from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q^m$ such that the number of the solutions $x \in \mathbb{Z}_q^n$ of the equation $f(x + w) - f(x) = y$ is exact q^{n-m} for $w \neq 0 \in \mathbb{Z}_q^n, y \in \mathbb{Z}_q^m$. The original motivations for the introduction of the notion [11] were the study of S-boxes for block ciphers and the construction of cryptographic functions. It was also revealed in [14] that perfect nonlinear functions may be used to design word-oriented stream cipher based on S-boxes with high efficiency. Furthermore the notion is also relevant to other topics, such as combinatorics (for example relative difference sets ([12,14])), finite geometries(affine and projective planes) and coding theory([3]).

Assume R is a $k-$element subset of a finite multiplicative group G of order mn with a normal subgroup N of order n, R is called an $(m, n, k, \lambda)-$relative difference set (abbr. RDS) in G relative to N provided that the multiset $r_1 r_2^{-1} (r_1 \neq r_2 \in R)$ replicates each element of $G \setminus N$ exactly λ times and replicates no element of N. If $G \cong G/N \oplus N$, then R is called splitting. If $k = n\lambda$, then R is called semi-regular.

Group ring $\mathbb{Z}[G]$ is the standard setting for studying difference sets. In general, a subset D of a finite group G can be regarded as an element $\sum_{g \in D} g$ in $\mathbb{Z}[G]$.

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 259–269, 2006.

Let G^* be the character group of $G \to \mathbb{C}$, where $\mathbb{C}$ is the complex number field. Suppose $\chi \in G^*, D = \sum_g g \in \mathbb{Z}[G]$, we define $\chi(D) = \sum_{g\in D} \chi(g)$, $D^{(-1)} = \sum_{g\in D} g^{-1}$.

Throughout this paper, χ_0 denotes the principal character of G, ξ_q is a primitive $q-$th root of unity, and all groups will be limited to be abelian and finite.

In the following, we list a well-known definition and some basic results which will be needed in the further sections.

Definition 1. *Let p be a prime number, m a positive integer and $m = p^a m'$ with $(m', p) = 1$. p is called self-conjugate modulo m if there exists a positive integer i with $p^i \equiv -1(\mathrm{mod}\ m')$. If every prime divisor p of n is self-conjugate modulo m,then n is called self-conjugate modulo m.*

Lemma 1. *[13] Let m be a positive integer and p a prime number which is self-conjugate modulo m. Let $X \in \mathbb{Z}[\xi_m]$ such that $X\overline{X} \equiv 0(mod\ p^{2a})$ where $\overline{X}$ is the complex conjugate of X, then we have*

$$X \equiv 0(mod\ p^a).$$

Lemma 1 is frequently used in connection with the following so-called Ma Lemma, which is an important tool in the theory of difference sets.

Lemma 2. *[9] Let A be an element in $\mathbb{Z}[G]$ where G is an abelian group with a cyclic Sylow $p-$group P. Let P_1 denote the unique subgroup of order p . If $\chi(A) \equiv 0(mod\ p^a)$ for all nonprincipal characters of G, then*

$$A = P_1 X + p^a Y$$

for suitable X and Y in $\mathbb{Z}[G]$, where the coefficients of X and Y can be chosen to be nonnegative if the coefficients of A are nonnegative.

Lemma 3. *Let G be a finite abelian group of order mn with a subgroup N of order n. Then a k-element subset R of G is an $(m, n, k, \lambda)-RDS$ in G relative to N if and only if for every nonprincipal character χ of G,*

$$|\chi(R)| = \begin{cases} \sqrt{k - \lambda n} & if\ \chi\ is\ principal\ on\ N; \\ \sqrt{k} & if\ \chi\ is\ nonprincipal\ on\ N. \end{cases}$$

Lemma 4. *Let R be an $(m, n, k, \lambda)-RDS$ in G relative to N and let $\rho : G \to G/U$ denote the canonical epimorphism, where U is a subgroup of G and $|U| = u$, then we have*

$$\rho(R)\rho(R^{(-1)}) = k + u\lambda \cdot G/U - |U \cap N|\lambda \cdot N/U.$$

If U is a subgroup of N, then $\rho(R)$ is an $(m, n/u, k, \lambda u)-RDS$ in G/U relative to N/U.

The following theorem establishes the equivalent connection between perfect nonlinear functions and a kind of relative difference sets.