



HAL
open science

Crooked Maps in Finite Fields

Gohar Kyureghyan

► **To cite this version:**

Gohar Kyureghyan. Crooked Maps in Finite Fields. 2005 European Conference on Combinatorics, Graph Theory and Applications (EuroComb '05), 2005, Berlin, Germany. pp.167-170, 10.46298/dmtcs.3392 . hal-01184348

HAL Id: hal-01184348

<https://inria.hal.science/hal-01184348v1>

Submitted on 14 Aug 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Crooked Maps in Finite Fields

Gohar Kyureghyan

*Institute for Algebra and Geometry
Otto-von-Guericke-University Magdeburg
D-39016 Magdeburg*

We consider the maps $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ with the property that the set $\{f(x+a) + f(x) : x \in \mathbb{F}_{2^n}\}$ is a hyperplane or a complement of hyperplane for every $a \in \mathbb{F}_{2^n}^*$. The main goal of the talk is to show that almost all maps $f(x) = \sum_{b \in B} c_b(x+b)^d$, where $B \subset \mathbb{F}_{2^n}$ and $\sum_{b \in B} c_b \neq 0$, are not of that type. In particular, the only such power maps have exponents $2^i + 2^j$ with $\gcd(n, i-j) = 1$. We give also a geometrical characterization of this maps.

Keywords: almost perfect maps, Gold power function, quadrics

1 Introduction

For applications in cryptography the maps $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$, which are far from being linear, are important. There are several possibilities to define “being far from linear”. Let $L : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ be a linear map, then the set $\{L(x+a) + L(x) : x \in \mathbb{F}_{2^n}\}$ consists of only one element $L(a)$ for all fixed $a \in \mathbb{F}_{2^n}$. Hence, a function $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ would be far from being linear if the sets $\{f(x+a) + f(x) : x \in \mathbb{F}_{2^n}\}$ are as big as possible. We can also think about $\{L(x+a) + L(x) : x \in \mathbb{F}_{2^n}\}$ as an affine subspace with only one element, and require for $\{f(x+a) + f(x) : x \in \mathbb{F}_{2^n}\}$ to be one of the largest possible affine subspaces. Another possibility is to require that all coordinate functions $\text{tr}(\alpha f(x)) : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ have large Hamming distance from the linear functions $\text{tr}(\beta x)$ (which are the only linear functions from \mathbb{F}_{2^n} into \mathbb{F}_2). There are three classes of maps with good nonlinearity properties ([4], [1]):

Definition 1 A map $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ is called **almost perfect nonlinear**, if for every $a \in \mathbb{F}_{2^n}^*$

$$|\{f(x+a) + f(x) : x \in \mathbb{F}_{2^n}\}| = 2^{n-1};$$

crooked, if for every $a \in \mathbb{F}_{2^n}^*$

$$|\{f(x+a) + f(x) : x \in \mathbb{F}_{2^n}\}|$$

is a hyperplane or a complement of a hyperplane;

almost bent, if n is odd and for all $\alpha \in \mathbb{F}_{2^n}^*, \beta \in \mathbb{F}_{2^n}$

$$\mathcal{F}_f(\alpha, \beta) := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{tr}(\alpha f(x) + \beta x)} \in \{-2^{\frac{n+1}{2}}, 0, 2^{\frac{n+1}{2}}\}.$$

Observe, that we extend the notion of crooked maps introduced in [1]. In [1] a map is called crooked if all sets $\{f(x+a) + f(x) : x \in \mathbb{F}_{2^n}\}$ are complements of hyperplanes. These are in our notion bijective crooked maps. Bijective crooked maps exist only for n odd, while crooked maps exist also for n even ([15], [13]). It can be shown ([4], [15], [13]), that

$$\text{crooked} \Rightarrow \text{almost bent} \Rightarrow \text{almost perfect nonlinear.}$$

All known almost perfect nonlinear functions can be obtained from almost perfect nonlinear power maps using the following construction.

Proposition 1 ([3]) *Let $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ be an almost perfect nonlinear map and $l_1, l_2 : \mathbb{F}_{2^n}^2 \rightarrow \mathbb{F}_{2^n}$ be linear maps. Assume that (l_1, l_2) is a permutation on $\mathbb{F}_{2^n}^2$ and $f_2 = l_2(f(x), x)$ is a permutation on \mathbb{F}_{2^n} . Then, the map $f_1 \circ f_2^{-1}$, where $f_1(x) = l_1(f(x), x)$, is almost perfect nonlinear.*

The known exponents of power almost nonlinear maps (up to factor 2^i) are

- $2^k + 1$, $\gcd(k, n) = 1$ (Gold's exponent [9],[1]);
- $2^{2k} - 2^k + 1$, $\gcd(k, n) = 1$ (Kasami's exponent [12])
- $2^{4k} + 2^{3k} + 2^{2k} + 2^k - 1$, if $n = 5k$ (Dobbertin's function [7])
- if $n = 2m + 1$ also
 - $2^m + 3$ (Welch's exponent [6], [2], [11])
 - $2^m + 2^{\frac{m}{2}} - 1$, if m is even, and
 - $2^m + 2^{\frac{3m+1}{2}} - 1$, if m is odd (Niho's exponent [5], [11]);
 - $2^n - 2$ (field inverse [14]).

This list is conjectured to be complete.

The main goal of our talk is to show that the only crooked power maps are the ones with Gold exponents. Denote by C_k the cyclotomic coset modulo $2^n - 1$ containing k , more precisely,

$$C_k = \{k, 2k, \dots, 2^{n-1}k\} \pmod{2^n - 1}.$$

If $|C_k| = l$, then $\{x^k : x \in \mathbb{F}_{2^n}\} \subset \mathbb{F}_{2^l}$ and l is the smallest such number. The binary weight of k is the number of ones in its binary representation. For two integers i and j we write $i \prec j$ if $i \neq j$ and in the binary representations of these integers every digit of i is less or equal to the corresponding digit of j .

We call the integers in the cyclotomic class of $\sum_{j=0}^{\frac{n}{g}-2} 2^{jg}$ exceptional, where g is a divisor of n .

The following results imply that the only crooked power maps are the Gold power maps.

Lemma 1 *Let an integer $0 \leq d \leq 2^n - 2$ have binary weight > 2 and $|C_d| = n$. If for every i with $2^i \prec d$ there exist $j(i)$ and $0 < s(i) < n$ such that $2^{j(i)} \prec d$ and $(d - 2^i) \equiv 2^{s(i)}(d - 2^{j(i)}) \pmod{2^n - 1}$, then d is exceptional.*

Corollary 1 *Let $1 \leq d \leq 2^n - 2$ be an unexceptional integer of binary weight > 2 , $|C_d| = n$. If $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ is given by $f(x) = \sum_{b \in B} c_b(x+b)^d$, where $B \subset \mathbb{F}_{2^n}$ and $\sum_{b \in B} c_b \neq 0$, then the set $\{f(x) + f(x+a) : x \in \mathbb{F}_{2^n}\}$ contains n linearly independent vectors for every $a \in \mathbb{F}_{2^n}^*$.*

Theorem 1 *If $1 \leq d \leq 2^n - 2$ is an unexceptional integer of binary weight > 2 and $|C_d| = n$, then $f(x) = \sum_{b \in B} c_b(x+b)^d$, where $B \subset \mathbb{F}_{2^n}$ and $\sum_{b \in B} c_b \neq 0$, is not crooked.*

In the case $B = \{0\}$ the exceptional exponents can be excluded as well.

Theorem 2 *The only crooked power maps in \mathbb{F}_{2^n} are the ones with exponent $2^i + 2^j$, $\gcd(i - j, n) = 1$.*

It is conjectured [13], that all crooked maps contain only monomials with exponents of binary weight 2 in their polynomial representation. The following observation strengthens this conjecture.

Let n be odd. The almost bent permutations $f(x)$ can be characterized as maps with coordinate functions $\text{tr}(\alpha f(x))$ having the same distances from the hyperplanes as nondegenerate quadrics ([8]). More precisely, let $\alpha, \beta \in \mathbb{F}_{2^n}^*$

$$F_\alpha := \{x \in \mathbb{F}_{2^n} : \text{tr}(\alpha f(x)) = 1\} \text{ and } H_i(\beta) := \{x \in \mathbb{F}_{2^n} : \text{tr}(\beta x) = i\}, \quad i = 0, 1.$$

Then a permutation $f(x)$ is almost bent if and only if

$$F_\alpha \cap H_i(\beta) \in \{2^{n-2}, 2^{n-2} \pm 2^{\frac{n-3}{2}}\}, \quad i = 0, 1,$$

for all $\alpha, \beta \in \mathbb{F}_{2^n}^*$. The following Theorem shows that the coordinate functions of crooked maps behave like quadrics also with the affine subspaces of dimension $n - 2$.

Theorem 3 *Let f be an almost bent permutation with $f(0) = 0$. Then f is crooked if and only if*

$$F_\alpha \cap H_i(\beta_1) \cap H_j(\beta_2) \in \{2^{n-3}, 2^{n-3} \pm 2^{\frac{n-3}{2}}\}, \quad i, j \in \{0, 1\},$$

where $\alpha, \beta_1 \neq \beta_2 \in \mathbb{F}_{2^n}^*$.

Last Theorem was proved using the arguments of the proof for a similar result about power maps in [10].

References

- [1] T. Bending, D. Fon-Der-Flaass, Crooked functions, bent functions, and distance regular graphs, *Electron.J.Comb.* **5** (R34), **14** (1998).
- [2] A. Canteaut, P. Charpin, H. Dobbertin, Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture, *IEEE Trans. Inform. Theory* **46** (2000), 4-8.
- [3] C. Carlet, P. Charpin, V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Desings, Codes and Cryptography* **15** (1998), 125-156.
- [4] F. Chabaud and S. Vaudenay, Links between differential and linear cryptanalysis, Advances in Cryptology, EUROCRYPT'94, *Lecture Notes in Computer Science* **950** (1995), 356-365.
- [5] H. Dobbertin, Almost perfectly nonlinear power functions on $\text{GF}(2^n)$: the Niho case, *Information and Computation* **151**, (1999), 57-72.
- [6] H. Dobbertin, Almost perfectly nonlinear power functions on $\text{GF}(2^n)$: the Welch case, *IEEE Transactions on Information Theory* **45** (1999), 1271-1275.
- [7] H. Dobbertin, Almost perfect nonlinear functions on $\text{GF}(2^n)$: a new case for n divisible by 5, in *Finite Fields and Applications*, D. Jungnickel and H. Niederreiter (Eds.), Springer, Berlin 2001, 113-121.

- [8] R.A. Games, The geometry of quadrics and correlations of sequences, *IEEE Trans. Inform. Theory* **32(3)** (1986), 423-426.
- [9] R. Gold, Maximal recursive sequences with 3-valued recursive crosscorrelation functions, *IEEE Trans. Inform. Theory* **14** (1968), 154-156.
- [10] D. Hertel and A. Pott, A characterization of a class of maximum nonlinear functions, submitted.
- [11] H.D.L. Hollmann, Q. Xing, A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences, *Finite Fields Appl.* **7** (2001), 253-286.
- [12] T. Kasami, The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes, *Inform. Control.* **18** (1971), 369-394.
- [13] G.M. Kyureghyan, Differentially affine maps, WCC2005, Bergen, Norway pp.296-305 .
- [14] K. Nyberg, Differentially uniform mappings for cryptography, Advances in Cryptology, EURO-CRYPT'93, *Lecture Notes in Computer Science* **765** (1994), 55-64.
- [15] E.R. van Dam and D. Fon-Der-Flaass, Codes, graphs, and schemes from nonlinear functions, *European J. Comb.* **24** (2003), 85-98, doi:10.1016/S0195-6698(02)00116-6.