Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Finite Fields and Their Applications 13 (2007) 713–726
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

Crooked maps in $\mathbb{F}_{2^n}$

Gohar M. Kyureghyan

Department of Mathematics, Otto-von-Guericke University of Magdeburg, Universitätsplatz 2, 39106 Magdeburg, Germany

Received 22 July 2005; revised 8 March 2006

Available online 24 April 2006

Communicated by Gary L. Mullen

Abstract

A map $f:\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called crooked if the set $\{f(x+a)+f(x)\colon x \in \mathbb{F}_{2^n}\}$ is an affine hyperplane for every fixed $a \in \mathbb{F}_{2^n}^*$ (where $\mathbb{F}_{2^n}$ is considered as a vector space over $\mathbb{F}_2$). We prove that the only crooked power maps are the quadratic maps $x^{2^i+2^j}$ with $\gcd(n, i-j)=1$. This is a consequence of the following result of independent interest: for any prime p and almost all exponents $0 \leqslant d \leqslant p^n-2$ the set $\{x^d + \gamma(x+a)^d\colon x \in \mathbb{F}_{p^n}\}$ contains n linearly independent elements, where γ and $a \neq 0$ are arbitrary elements from $\mathbb{F}_{p^n}$.

Keywords: Almost perfect nonlinear map; Crooked map; Bent functions; Quadrics

1. Introduction

A map $f:\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called almost perfect nonlinear if for every $a \in \mathbb{F}_{2^n}^* := \mathbb{F}_{2^n} \setminus \{0\}$ the set

$$D(a) := \left\{f(x+a)+f(x)\colon x \in \mathbb{F}_{2^n}\right\}$$

contains 2^{n-1} elements, i.e. it is as large as possible. We call $D(a)$ the differential set of f at a. Almost perfect nonlinear maps provide the best resistance against the so-called differential cryptanalysis [7]. All known almost perfect nonlinear maps, with the exception of some sporadic examples [11], can be obtained from the almost perfect nonlinear power maps. The known exponents of almost perfect nonlinear power maps (up to factor 2^i) are

E-mail address: gohar.kyureghyan@mathematik.uni-magdeburg.de.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2006.03.003

2^k+1, $\gcd(k,n)=1$ (Gold's exponent [1,12]),

$2^{2k}-2^k+1$, $\gcd(k,n)=1$ (Kasami's exponent [15]),

if $n=5k$ $2^{4k}+2^{3k}+2^{2k}+2^k-1$ (Dobbertin's function [10]),

if $n=2m+1$ also 2^m+3 (Welch's exponent [5,9,14]),

$2^m+2^{\frac{m}{2}}-1$ if m is even, and

$2^m+2^{\frac{3m+1}{2}}-1$ if m is odd (Niho's exponent [8,14]),

2^n-2 (field inverse [22]).

The characterization of almost perfect nonlinear power maps is open and seems to be a very difficult problem.

In [1,24] the almost perfect nonlinear maps with the differential sets being the complements of hyperplanes are studied. Such maps are called crooked. Crooked maps exist only if n is odd. Crooked maps can be used to construct many interesting combinatorial objects [1,23,24]. The only known crooked maps are polynomials with exponents of binary weight 2. We study here the question whether other crooked maps exist. Using combinatorics in the cyclic group of order n, we show that in a class of maps including power maps only the ones with exponents of binary weight 2 can be crooked. This is a generalization of a result in [17]. There are some indications that the complete characterization of crooked maps is difficult. For example, the characterization of crooked binomials is more difficult [3]. Also it was believed that any almost perfect nonlinear polynomial with exponents of binary weight 2 is affinely equivalent to a Gold power map [2]. This was recently disproved [11]. In [11] it is shown that $f(x)=x^3+ux^{36}$ for a suitable $u\in\mathbb{F}_{2^{10}}$ defines an almost perfect nonlinear map from $\mathbb{F}_{2^{10}}$ into $\mathbb{F}_{2^{10}}$, which is not affinely equivalent to any power map.

This paper is organized as follows. In Section 2 we generalize the notion of crooked maps and give some properties of such maps. In Section 3 as an application of the results of Section 2 we give new proofs of some known properties of Gold power maps. In Section 4 we show that for any prime p the set $\{x^d+\gamma(x+a)^d\colon x\in\mathbb{F}_{p^n}\}$ contains n linearly independent elements almost for all exponents d. We also prove a similar result for more general class of maps. As a consequence we characterize the crooked maps in that class.

2. Crooked maps

Let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements, which is also considered as a vector space over $\mathbb{F}_2$. If k divides n, then $\mathbb{F}_{2^k}$ denotes the subfield of 2^k elements in $\mathbb{F}_{2^n}$. The hyperplanes in $\mathbb{F}_{2^n}$ are the subspaces of dimension $n-1$. The affine hyperplanes are the subspaces of dimension $n-1$ and their complements. Let $\mathrm{tr}:\mathbb{F}_{2^n}\to\mathbb{F}_2$ be the absolute trace map. Then the affine hyperplanes are the sets $\{x\in\mathbb{F}_{2^n}\colon \mathrm{tr}(\alpha x)=c\}$ for some $\alpha\in\mathbb{F}_{2^n}^*$ and $c\in\mathbb{F}_2$.

In [1] a map $f:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ is called crooked, if

$$D(a)=\{f(x+a)+f(x)\colon x\in\mathbb{F}_{2^n}\}$$

is the complement of a hyperplane in $\mathbb{F}_{2^n}$ for every $a\in\mathbb{F}_{2^n}^*$. Crooked maps are necessarily bijective, since $0\notin D(a)$ for all $a\in\mathbb{F}_{2^n}^*$. They exist only if n is odd. We extend the definition of crooked maps in the following way.

Definition 1. A map $f:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ is called crooked, if for every $a\in\mathbb{F}_{2^n}^*$ the set

$$D(a)=\left\{f(x+a)+f(x):\ x\in\mathbb{F}_{2^n}\right\}$$

is an affine hyperplane of $\mathbb{F}_{2^n}$.

In this notion crooked maps exist also for even n. For example, every almost perfect nonlinear polynomial with exponents of binary weight 2 is crooked (see Section 3). Moreover, there are crooked maps for odd n, which are not bijective, as the example of $x^{2^i+1}+x$, $\gcd(i,n)=1$, shows.

The maps $f:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ and $g:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ are called affinely equivalent if there are affine maps B_1, B_2 and $b:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ such that B_1, B_2 are bijective and $f=B_1\circ g\circ B_2+b$. A map that is affinely equivalent to a crooked map is also crooked.

Given a map $g:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$, the Fourier transform of g is the map $\mathcal{F}_g:\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}\to\mathbb{C}$ defined by

$$\mathcal{F}_g(\alpha,\beta)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{tr}(\alpha g(x)+\beta x)},\quad (\alpha,\beta)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}.$$

A map $g:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ is called *almost bent*, if $\mathcal{F}_g(\alpha,\beta)\in\{-2^{\frac{n+1}{2}},0,2^{\frac{n+1}{2}}\}$ for all $\alpha\in\mathbb{F}_{2^n}^*$, $\beta\in\mathbb{F}_{2^n}$. Obviously, almost bent maps exist only for odd n.

Let $f:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ be crooked. Consider

$$\begin{aligned}\mathcal{F}_f(\alpha,\beta)^2&=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{tr}(\alpha f(x)+\beta x)}\sum_{y\in\mathbb{F}_{2^n}}(-1)^{\mathrm{tr}(\alpha f(y)+\beta y)}\\&=\sum_{x,y\in\mathbb{F}_{2^n}}(-1)^{\mathrm{tr}(\alpha f(x)+\beta x+\alpha f(y)+\beta y)}\\&=\sum_{a\in\mathbb{F}_{2^n}}(-1)^{\mathrm{tr}(\beta a)}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{tr}(\alpha(f(x)+f(x+a)))}\\&=2^n\sum_{a\in T_f(\alpha)}(-1)^{\mathrm{tr}(\beta a)}-2^n\sum_{a\in\overline{T}_f(\alpha)}(-1)^{\mathrm{tr}(\beta a)},\end{aligned}\tag{1}$$

where

$$T_f(\alpha)=\left\{a\in\mathbb{F}_{2^n}:\ \mathrm{tr}\big(\alpha\big(f(x)+f(x+a)\big)\big)=0\text{ for all }x\in\mathbb{F}_{2^n}\right\}$$

is the set of all a for which $D(a)$ coincides with the hyperplane $\{x\in\mathbb{F}_{2^n}:\ \mathrm{tr}(\alpha x)=0\}$ and

$$\overline{T}_f(\alpha)=\left\{a\in\mathbb{F}_{2^n}^*:\ \mathrm{tr}\big(\alpha\big(f(x)+f(x+a)\big)\big)=1\text{ for all }x\in\mathbb{F}_{2^n}\right\}$$

is the set of all a with $D(a)$ equal to the complement of hyperplane $\{x\in\mathbb{F}_{2^n}:\ \mathrm{tr}(\alpha x)=0\}$. Clearly, $0\in T_f(\alpha)$ for any α.

Proposition 1. *Let $f:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ be crooked and $\alpha\in\mathbb{F}_{2^n}^*$, then $T_f(\alpha)$ is a subspace and $\overline{T}_f(\alpha)$ is either empty or is a coset of $T_f(\alpha)$.*

Proof. Let $a, b \in T_f(\alpha)$ or $a, b \in \overline{T}_f(\alpha)$, then $a+b \in T_f(\alpha)$ too. Indeed,

$$\mathrm{tr}\big(\alpha\big(f(x)+f(x+a)\big)\big) = \mathrm{tr}\big(\alpha\big(f(x)+f(x+b)\big)\big) \quad \text{for all } x \in \mathbb{F}_{2^n},$$

which implies that

$$\mathrm{tr}\big(\alpha\big(f(x+a)+f(x+b)\big)\big) = \mathrm{tr}\big(\alpha\big(f(y)+f(y+a+b)\big)\big) = 0 \quad \text{for all } y \in \mathbb{F}_{2^n}.$$

Similarly, it can be shown, that if $a \in T_f(\alpha)$ and $b \in \overline{T}_f(\alpha)$ then $a+b \in \overline{T}_f(\alpha)$. Thus $\overline{T}_f(\alpha)$ is a coset of $T_f(\alpha)$ if it is not empty. □

Theorem 1. *The squared Fourier spectrum of a crooked map $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ consists of* 0 *and powers of* 2*.*

Proof. From (1)

$$\mathcal{F}_f(\alpha,\beta)^2 = 2^n \sum_{a \in T_f(\alpha)} (-1)^{\mathrm{tr}(\beta a)} - 2^n \sum_{a \in \overline{T}_f(\alpha)} (-1)^{\mathrm{tr}(\beta a)}.$$

Let $\dim T_f(\alpha) = k$. If $\overline{T}_f(\alpha) = \emptyset$, then

$$\mathcal{F}_f(\alpha,\beta)^2 = 2^n \sum_{a \in T_f(\alpha)} (-1)^{\mathrm{tr}(\beta a)} = \begin{cases} 2^{n+k} & \text{if } T_f(\alpha) \subset \{x \in \mathbb{F}_{2^n}\colon \mathrm{tr}(\beta x) = 0\}, \\ 0 & \text{otherwise.} \end{cases}$$

In the case $\overline{T}_f(\alpha) \neq \emptyset$, let $b \in \overline{T}_f(\alpha)$, then

$$\begin{aligned} \mathcal{F}_f(\alpha,\beta)^2 &= 2^n \sum_{a \in T_f(\alpha)} \big((-1)^{\mathrm{tr}(\beta a)} - (-1)^{\mathrm{tr}(\beta(b+a))}\big) \\ &= 2^n\big(1-(-1)^{\mathrm{tr}(\beta b)}\big) \sum_{a \in T_f(\alpha)} (-1)^{\mathrm{tr}(\beta a)} \\ &= \begin{cases} 2^{n+k+1} & \text{if } T_f(\alpha) \subset \{x \in \mathbb{F}_{2^n}\colon \mathrm{tr}(\beta x) = 0\} \text{ and } \mathrm{tr}(\beta b) = 1, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$ □

The Walsh transform of a Boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_2$ at a point $\beta \in \mathbb{F}_{2^n}$ is defined to be

$$\mathcal{W}_F(\beta) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{F(x)+\mathrm{tr}(\beta x)}.$$

A Boolean function is called *plateaued* if the squared Walsh transform of it takes at most three values [26]. The plateaued functions with the Walsh transform taking only two values $\pm 2^{n/2}$ are called bent. The proof of Theorem 1 shows that the Boolean function $\mathrm{tr}(\alpha f(x))$, $\alpha \in \mathbb{F}_{2^n}^*$, is plateaued, if f is crooked. Moreover, we get the following description of such bent functions.

Corollary 1. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a crooked map and $\alpha \in \mathbb{F}_{2^n}^*$, then* $\mathrm{tr}(\alpha f(x))$ *is bent if and only if $T_f(\alpha) \cup \overline{T}_f(\alpha) = \{0\}$.*

Proposition 2. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a crooked map and n be odd. Then for every $\alpha \in \mathbb{F}_{2^n}^*$ there is a unique $a \in \mathbb{F}_{2^n}^*$ with $D(a) = \{x \in \mathbb{F}_{2^n}\colon \operatorname{tr}(\alpha x) = 0\}$ or $D(a) = \{x \in \mathbb{F}_{2^n}\colon \operatorname{tr}(\alpha x) = 1\}$.*

Proof. If for some α the hyperplane $\{x \in \mathbb{F}_{2^n}\colon \operatorname{tr}(\alpha x) = 0\}$ and its complement $\{x \in \mathbb{F}_{2^n}\colon \operatorname{tr}(\alpha x) = 1\}$ are not a differential set of f, then by (1)

$$\mathcal{F}_f(\alpha, \beta)^2 = 2^n \quad \text{for all } \beta,$$

and this contradicts to n odd. The uniqueness follows from counting. $\square$

As a consequence of the proposition above we get the following result proved for bijective crooked maps in [24].

Theorem 2. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a crooked map and n be odd. Then f is almost bent.*

Proof. Using Proposition 2 and (1), we obtain

$$\mathcal{F}_f(\alpha, \beta)^2 \in \{0, 2^{n+1}\}. \qquad \square$$

Theorem 3. *There are no bijective crooked maps in $\mathbb{F}_{2^n}$ if n is even.*

Proof. If f is a bijective crooked map, then $T_f(\alpha) = \{0\}$ and thus $|\overline{T}_f(\alpha)| \leqslant 1$ by Proposition 1. On the other side, for every $a \in \mathbb{F}_{2^n}^*$ there is an $\alpha \in \mathbb{F}_{2^n}^*$ such that $a \in \overline{T}_f(\alpha)$, and thus by counting $|\overline{T}_f(\alpha)| = 1$ for every $\alpha \in \mathbb{F}_{2^n}^*$. This implies that $\mathcal{F}_f(\alpha, \beta)^2 \in \{0, 2^{n+1}\}$ and therefore n must be odd. $\square$

3. Gold power maps

A map $Q : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called quadratic if it is defined by a polynomial with exponents of binary weight 2, i.e.

$$Q(x) = \sum_{0 \leqslant i \leqslant j \leqslant n-1} \delta_{ij} x^{2^i + 2^j}.$$

It is easy to see that $Q(x) + Q(y) + Q(x + y)$ is bilinear, and therefore the differential sets of a quadratic map are affine subspaces. In particular, a quadratic function is crooked if and only if it is almost perfect nonlinear. Theorem 2 implies that a quadratic almost perfect nonlinear map in $\mathbb{F}_{2^n}$ is almost bent in the case of odd n. This was proved in [6] using other methods.

Let us consider the quadratic power maps x^{2^i+1}. Observe, that $D(a) = \{x^{2^i+1} + (x + a)^{2^i+1}\colon x \in \mathbb{F}_{2^n}\} = \{a^{2^i+1} z\colon z \in D(1)\} =: a^{2^i+1} D(1)$, implying that either all differential sets of a quadratic power map are subspaces or they are all cosets. The differential sets are cosets if and only if x^{2^i+1} is a permutation, which is the case when $\gcd(2^i + 1, 2^n - 1) = 1$ or, equivalently, if $\frac{n}{\gcd(n,i)}$ is odd. Indeed, let $s = \gcd(n, i)$. Then

$$\gcd\bigl(2^n - 1, 2^i + 1\bigr) = \frac{\gcd(2^n - 1, 2^{2i} - 1)}{\gcd(2^n - 1, 2^i - 1)} = \frac{2^{\gcd(n,2i)} - 1}{2^{\gcd(n,i)} - 1}.$$

At last note, that

$$\frac{2^{\gcd(n,2i)}-1}{2^s-1}=\begin{cases}1 & \text{if } \frac{n}{s} \text{ is odd},\\ 2^s+1 & \text{otherwise.}\end{cases}$$

It is not difficult to show that $x^{2^i+1}+(x+a)^{2^i+1}$ is a 2^s-to-one map [22]. Thus we get the following proposition.

Proposition 3. *Let* $\gcd(n,i)=s$ *and* $f(x)=x^{2^i+1}$. *Then*

(i) *if* $\frac{n}{s}$ *is odd, then* $f(x)$ *is a permutation and* $\{f(x)+f(x+a)\colon x\in\mathbb{F}_{2^n}\}$ *are cosets of an* $(n-s)$*-dimensional subspace*;
(ii) *if* $\frac{n}{s}$ *is even, then* $f(x)$ *is a* (2^s+1)*-to-one map and* $\{x^{2^i+1}+(x+a)^{2^i+1}\colon x\in\mathbb{F}_{2^n}\}$ *are* $(n-s)$*-dimensional subspaces.*

Our next goal is, for a given $\alpha\in\mathbb{F}_{2^n}^*$, to find the set of $a\in\mathbb{F}_{2^n}$ such that the set $D(a)$ is contained in the hyperplane $\{x\in\mathbb{F}_{2^n}\colon \operatorname{tr}(\alpha x)=0\}$. Set

$$T_i(\alpha):=\bigl\{a\in\mathbb{F}_{2^n}\colon \operatorname{tr}\bigl(\alpha\bigl(x^{2^i+1}+(x+a)^{2^i+1}\bigr)\bigr)=0 \text{ for all } x\in\mathbb{F}_{2^n}\bigr\}.$$

Proposition 4.

$$T_i(1)=\bigl\{a\in\mathbb{F}_{2^{\gcd(2i,n)}}\colon \operatorname{tr}\bigl(a^{2^i+1}\bigr)=0\bigr\}.$$

Proof. We look for $a\in\mathbb{F}_{2^n}$ with

$$\operatorname{tr}\bigl(x^{2^i+1}+(x+a)^{2^i+1}\bigr)=0 \quad \text{for all } x\in\mathbb{F}_{2^n},$$

or, equivalently,

$$\operatorname{tr}\bigl(ax^{2^i}+a^{2^i}x\bigr)=\operatorname{tr}\bigl(\bigl(a^{2^{n-i}}+a^{2^i}\bigr)x\bigr)=\operatorname{tr}\bigl(a^{2^i+1}\bigr).$$

The last identity is possible only if

$$\operatorname{tr}\bigl(a^{2^i+1}\bigr)=0 \quad \text{and} \quad a^{2^{n-i}}+a^{2^i}=0.$$

The condition $a^{2^{n-i}}=a^{2^i}$ implies that $a\in\mathbb{F}_{2^n}\cap\mathbb{F}_{2^{2i}}=\mathbb{F}_{2^{\gcd(2i,n)}}$, completing the proof. □

Corollary 2. *Let* $\gcd(n,i)=s$ *and* $\frac{n}{s}$ *be odd. Then*

$$T_i(\alpha)=\alpha^{-\frac{1}{2^i+1}}\bigl\{a\in\mathbb{F}_{2^s}\colon \operatorname{tr}\bigl(a^{2^i+1}\bigr)=0\bigr\}.$$

Proof. Note, that $T_i(\alpha)=\alpha^{-1/(2^i+1)}T_i(1)$ and $\gcd(n,i)=\gcd(n,2i)$, since $\frac{n}{s}$ is odd. □

Using the discussion above we can find the Fourier spectra of the quadratic power maps [12,15,25].

Theorem 4. *Let* $\gcd(n,i)=s$, $\frac{n}{s}$ *be odd and* $f(x)=x^{2^i+1}$. *Then*

$$\mathcal{F}_f(\alpha,\beta)\in\left\{0,\pm 2^{\frac{n+s}{2}}\right\},$$

for all $(\alpha,\beta)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}\setminus\{(0,0)\}$.

Proof. Since x^{2^i+1} is a permutation then $|T_i(\alpha)|=2^{s-1}$ and $\overline{T_i}(\alpha)\neq\emptyset$. The rest of the proof is similar to the proof of Theorem 1. □

Corollary 3. *Let* $\gcd(n,i)=s$ *and* $\frac{n}{s}$ *be even. Then*

$$T_i(\alpha)=\begin{cases}\alpha^{-\frac{1}{2^i+1}}\mathbb{F}_{2^{2s}} & \text{if } \alpha \text{ is a } 2^i+1 \text{ power},\\ \{0\} & \text{otherwise.}\end{cases}$$

Proof. Observe, that the hyperplane $\{x\in\mathbb{F}_{2^n}\colon \operatorname{tr}(\beta x)=0\}$ contains the differential set $D(1)$ of x^{2^i+1} if and only if $\beta\in\mathbb{F}_{2^s}$. Indeed, $\operatorname{tr}(\beta(x^{2^i+1}+(x+1)^{2^i+1}))=0$ is possible only if $\operatorname{tr}(\beta)=0$ and $\beta^{2^{n-i}}=\beta$, implying $\beta\in\mathbb{F}_{2^s}$. Now, if

$$D(a)=a^{2^i+1}D(1)\subset\left\{x\in\mathbb{F}_{2^n}\colon \operatorname{tr}(\alpha x)=0\right\},$$

then

$$D(1)\subset\left\{a^{-(2^i+1)}x\colon x\in\mathbb{F}_{2^n},\ \operatorname{tr}(\alpha x)=0\right\}=\left\{y\in\mathbb{F}_{2^n}\colon \operatorname{tr}\left(a^{2^i+1}\alpha y\right)=0\right\},$$

and therefore $a^{2^i+1}\alpha\in\mathbb{F}_{2^s}$. Hence, if $T_i(\alpha)\neq\{0\}$ then $\alpha\in\bigcup_{a\in\mathbb{F}_{2^n}}a^{-(2^i+1)}\mathbb{F}_{2^s}$. (Observe, that $\bigcup_{a\in\mathbb{F}^*_{2^n}}a^{-(2^i+1)}\mathbb{F}_{2^s}=\langle\gamma^{2^i+1}\rangle$, since $\mathbb{F}^*_{2^s}$ is a subgroup of $\langle\gamma^{2^i+1}\rangle$, where γ is a primitive element of $\mathbb{F}_{2^n}$.) Further, using Proposition 4 we get

$$T_i(\alpha)=\alpha^{\frac{1}{2^i+1}}T_i(1)=\alpha^{\frac{1}{2^i+1}}\left\{a\in\mathbb{F}_{2^{2s}}\colon \operatorname{tr}\left(a^{2^i+1}\right)=0\right\}=\alpha^{\frac{1}{2^i+1}}\mathbb{F}_{2^{2s}},$$

since $a^{2^i+1}\in\mathbb{F}_{2^s}$ for all $a\in\mathbb{F}_{2^s}$, implying $\operatorname{tr}(a^{2^i+1})=0$. □

Theorem 5. *Let* $\gcd(n,i)=s$, $\frac{n}{s}$ *be even and* $f(x)=x^{2^i+1}$. *Then*

$$\mathcal{F}_f(\alpha,\beta)\in\left\{0,\pm 2^{\frac{n}{2}},\pm 2^{\frac{n+2s}{2}}\right\},$$

for all $(\alpha,\beta)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}\setminus\{(0,0)\}$.

Proof. Clearly, $\overline{T_i}(\alpha)=\emptyset$ for all $\alpha\in\mathbb{F}^*_{2^n}$. The proof can be completed using Corollary 3 and the steps of the proof of Theorem 1. □

Corollary 4. *Let* $\gcd(n,i)=s$ *and* $\frac{n}{s}$ *be even. Then the Boolean function* $\operatorname{tr}(\alpha x^{2^i+1})$ $x\in\mathbb{F}_{2^n}$ *is bent if and only if* α *is not a* 2^i+1 *power in* $\mathbb{F}_{2^n}$.

Proof. Follows from Corollaries 3 and 1. □

The obtained results can be used to determine the type of quadratic form $\mathrm{tr}(\alpha x^{2^i+1})$. At first, we repeat briefly some definitions and facts about quadratic forms [20,21].

Given a basis $\{\gamma_1, \ldots, \gamma_n\}$ of $\mathbb{F}_2^n$, every polynomial $P \in \mathbb{F}_2[x_1, \ldots, x_n]$ determines a map $P : \mathbb{F}_2^n \to \mathbb{F}_2$ by $\sum_{i=1}^n a_i\gamma_i \mapsto P(a_1, \ldots, a_n)$. The maps arising from a homogeneous polynomial of degree 2 are called quadratic forms. Thus, the quadratic forms are determined by

$$Q(x_1, \ldots, x_n) = \sum_{i \leqslant j} c_{ij} x_i x_j, \quad c_{ij} \in F_2.$$

Set $\mathbf{x} = (x_1, \ldots, x_n)$. Then $Q(\mathbf{x})$ can be represented also as

$$Q(\mathbf{x}) = \mathbf{x}^t B\mathbf{x} + \mathbf{c}^t\mathbf{x},$$

where B is an $n \times n$ upper triangular matrix with zeros along the diagonal and $\mathbf{c} \in \mathbb{F}_2^n$. The rank $2h$ $(1 \leqslant h \leqslant \frac{n}{2})$ of the symmetric matrix $B + B^t$ is called the rank of the quadratic form. Two quadratic forms are called equivalent if they can be transformed each into the other by means of a nonsingular linear substitution of indeterminates. It is well known that a quadratic form of rank $2h$ is equivalent to one of the following quadratic forms:

$$x_1x_2 + \cdots + x_{2h-1}x_{2h} \quad \text{(hyperbolic)},$$
$$x_1x_2 + \cdots + x_{2h-1}x_{2h} + x_{2h-1} + x_{2h} \quad \text{(elliptic)},$$
$$x_1x_2 + \cdots + x_{2h-1}x_{2h} + x_{2h-1}x_{2h} + x_{2h+1} \quad \text{(parabolic)},$$

and its Walsh transform takes values $0, \pm 2^{n-h}$ if $h \neq \frac{n}{2}$, and $\pm 2^{n/2}$, if $h = \frac{n}{2}$. The cardinality $N := |\{\mathbf{x} \in V\colon\ Q(\mathbf{x}) = 0\}|$ allows to determine the kind of a quadratic form. More precisely, a quadratic form is

$$\begin{array}{ll} \text{hyperbolic} & \text{if } N = 2^{n-2h}\big((2^h - 1)(2^{h-1} + 1) + 1\big), \\ \text{elliptic} & \text{if } N = 2^{n-2h}\big((2^h + 1)(2^{h-1} - 1) + 1\big), \\ \text{parabolic} & \text{if } N = 2^{n-2h-1}2^{2h}. \end{array}$$

Equivalently,

$$\mathcal{W}_Q(0) = \begin{cases} -2^{n-h} & \text{if } Q(\mathbf{x}) \text{ is hyperbolic}, \\ 2^{n-h} & \text{if } Q(\mathbf{x}) \text{ is elliptic}, \\ 0 & \text{if } Q(\mathbf{x}) \text{ is parabolic}. \end{cases} \tag{2}$$

Any quadratic form from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$ has also a univariate polynomial representation $\mathrm{tr}(x\sum_{i=0}^{\lfloor n/2\rfloor} a_i x^{2^i+1})$ with $a_i \in \mathbb{F}_{2^n}$. In general it is difficult to find the type or the rank of $\mathrm{tr}(x\sum_{i=0}^{\lfloor n/2\rfloor} a_i x^{2^i+1})$. In [16] types of the monomial quadratic forms are determined. We give another proof of this result using the properties of the Gold power maps obtained above. Let $\mathcal{W}_\alpha(\beta)$ denote the value of Walsh transform of $\mathrm{tr}(\alpha x^{2^i+1})$ at β and P be the set of the $2^i + 1$

powers in $\mathbb{F}_{2^n}$. Further, let $\gcd(n,i)=s$ and thus $\gcd(2^n-1,2^i+1)=2^s+1$ in the case $\frac{n}{s}$ is even. By Theorem 5 $\mathcal{W}_\alpha(0)\in\{\pm 2^{n/2},\pm 2^{n/2+s}\}$. It was observed in [19] that

$$\mathcal{W}_\alpha(0)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{tr}(\alpha x^{2^i+1})}=1+\left(2^s+1\right)\sum_{y\in G}(-1)^{\mathrm{tr}(\alpha y^{2^i+1})},$$

where G is the subgroup of $\mathbb{F}_{2^n}^*$ generated by a primitive element to the power 2^s+1, and therefore $\mathcal{W}_\alpha(0)$ is congruent 1 modulo 2^s+1. This remark implies

$$\mathcal{W}_\alpha(0)=\begin{cases}-2^{\frac{n}{2}} & \frac{n}{2s}\text{ if odd,}\\ 2^{\frac{n}{2}} & \frac{n}{2s}\text{ if even,}\end{cases}$$

in the case $\alpha\notin P$, and

$$\mathcal{W}_\alpha(0)=\begin{cases}2^{\frac{n}{2}+s} & \frac{n}{2s}\text{ if odd,}\\ -2^{\frac{n}{2}+s} & \frac{n}{2s}\text{ if even,}\end{cases}$$

in the case $\alpha\in P$.

So the following theorem is immediate.

Theorem 6. *(See [16].) Let* $\gcd(n,i)=s$ *and* $\alpha\in\mathbb{F}_{2^n}^*$.

(i) *If* $\frac{n}{s}$ *is odd, then the quadratic form* $\mathrm{tr}(\alpha x^{2^i+1})$ *in* $\mathbb{F}_{2^n}$ *is parabolic of rank* $n-s$.
(ii) *If* $\frac{n}{2s}$ *is odd, then the quadratic form* $\mathrm{tr}(\alpha x^{2^i+1})$ *in* $\mathbb{F}_{2^n}$ *is elliptic of rank* $n-2s$ *if* α *is a* 2^i+1 *power in* $\mathbb{F}_{2^n}$ *and hyperbolic of rank* n *otherwise.*
(iii) *If* $\frac{n}{2s}$ *is even, then the quadratic form* $\mathrm{tr}(\alpha x^{2^i+1})$ *in* $\mathbb{F}_{2^n}$ *is hyperbolic of rank* $n-2s$ *if* α *is a* 2^i+1 *power in* $\mathbb{F}_{2^n}$ *and elliptic of rank* n *otherwise.*

4. On the image set of $x^d+\gamma(x+a)^d$ in $\mathbb{F}_{p^n}$

In this section p is an arbitrary prime. Let $0\leqslant k\leqslant p^n-2$. We denote by C_k the cyclotomic coset modulo p^n-1 containing k, i.e.

$$C_k=\left\{k,pk,\ldots,p^{n-1}k\right\}\pmod{p^n-1}.$$

Further, let $\mathcal{C}$ be the set of all cyclotomic cosets modulo p^n-1, i.e.

$$\mathcal{C}=\left\{C_k\colon\ 0\leqslant k\leqslant p^n-2\right\}.$$

If $|C_k|=l$, then $\{x^k\colon\ x\in\mathbb{F}_{p^n}\}\subset\mathbb{F}_{p^l}$ and $\mathbb{F}_{p^l}$ is the smallest subfield with this property. Let k and k' have base p representation $(k_{n-1}\ldots k_0)_p$ and $(k'_{n-1}\ldots k'_0)_p$, respectively. Let $0<i<n$. We say that $(k_{n-1}\ldots k_0)_p$ is the ith shift of $(k'_{n-1}\ldots k'_0)_p$ if $k_j=k'_{j+i}$ for every j, where indices are taken modulo n. Observe, that k and k' are in the same cyclotomic coset modulo p^n-1 if and only if $(k_{n-1}\ldots k_0)_p$ is a shift of $(k'_{n-1}\ldots k'_0)_p$. The p-weight of k is the number of nonzero

digits in its base p representation. The support $s_p(k)$ of k is the binary sequence $(s_{n-1}\dots s_0)$ that records the nonzero positions of $(k_{n-1}\dots k_0)_p$, i.e.

$$s_i = \begin{cases} 1 & \text{if } k_i \neq 0, \\ 0 & \text{if } k_i = 0. \end{cases}$$

If k and k' are in the same cyclotomic coset then $s_p(k)$ and $s_p(k')$ are shifts of each other. We say that k covers k' and write $k' \prec k$ if $k \neq k'$ and $s_p(k)$ covers $s_p(k')$.

Lemma 1. *Let an integer $d = (d_{n-1}\dots d_0)_p$ have p-weight > 2 and $|C_d| = n$. Suppose that for every i with $p^i \prec d$ there exists $j \neq i$ such that $p^j \prec d$ and $d - d_i p^i$ is a shift of $d - d_j p^j$. Then d is in the cyclotomic coset of $\sum_{l=0}^{n/g-2} tp^{gl}$, where g a divisor of n and $1 \leqslant t \leqslant p-1$.*

Proof. Let $(s_{n-1}\dots s_0)$ be the support of d. Note, that all integers in C_d satisfy the assumption of this lemma, and therefore we can assume that $s_0 = 1$ and $\min\{i - j\colon s_i = 1,\ s_j = 1,\ i \neq j\} = \min\{i\colon s_i = 1,\ i \neq 0\}$. Observe that if $i \neq 0$ and $(d - d_i p^i)$ is the mth shift of $(d - d_j p^j)$ then $d_0 = d_m$, and in particular $s_m = 1$. Let $i \neq i'$. Then $|C_d| = n$ implies that if $(d - d_i p^i)$ is the mth shift of $(d - d_j p^j)$, and $(d - d_{i'} p^{i'})$ is the m'th shift of $(d - d_{j'} p^{j'})$, then $m \neq m'$. Hence, by counting, for every $m \neq 0$ with $s_m = 1$ there are $i \neq 0$ and j such that $(d - d_i p^i)$ is the mth shift of $(d - d_j p^j)$. Take $g = \min\{i\colon s_i = 1, i \neq 0\}$. Let $f \neq 0$ be such that $s_f = 1$ and $(d - d_f p^f)$ is the gth shift of some $(d - d_i p^i)$. Then, in particular, $s_p(d - d_f p^f)$ is the gth shift of $s_p(d - d_i p^i)$, implying

$$\begin{aligned}\{k\colon 0 \leqslant k \leqslant n-1,\ s_k = 1\} &= \bigl\{k\colon p^k \prec d\bigr\} \\ &= \bigl\{0, g, 2g, \dots, fg, fg + h, (f+1)g + h, \dots, \\ &\qquad (f+r)g + h = n - g\bigr\}.\end{aligned}$$

Again, replacing d by an appropriate integer from C_d we can assume that $\{k\colon p^k \prec d\} = \{0, g, 2g, \dots, (w-1)g\}$, where w is the p-weight of d. Note that $n - (w-1)g$ must be equal to $2g$. Indeed, otherwise $|\{k\colon p^k \prec d\} \cap \{k'\colon p^{k'} \prec p^{2g} d\}| \leqslant w - 2$, contradicting to the fact that there are i, j such that $s_p(d - d_i p^i)$ is the $2g$th shift of $s_p(d - d_j p^j)$. $\square$

We call the integers of type $\sum_{l=0}^{n/g-2} tp^{gl}$ exceptional, where g a divisor of n and $1 \leqslant t \leqslant p-1$, otherwise unexceptional.

Corollary 5. *Let $d = (d_{n-1}\dots d_0)_p$ be unexceptional and $|C_d| = n$. Then there is a k such that $p^k \prec d$, $|C_{d - d_k p^k}| = n$ and $C_{d - d_k p^k} \cap \{d - d_j p^j\colon p^j \prec d,\ j \neq i\} = \emptyset$.*

Proof. Observe, that if $|C_{d - d_i p^i}| = l < n$ for some i with $p^i \prec d$ then $(d - d_i p^i) \equiv p^l (d - d_i p^i) \pmod{p^n - 1}$ and therefore Lemma 1 guarantees the existence of such a k. $\square$

Further we need the following well-known facts.

Proposition 5. *Let $1 \leqslant d \leqslant p^n - 2$ and $|C_d| = n$. Then $\operatorname{tr}(\alpha x^d)$ is constantly 0 if and only if $\alpha = 0$.*

Theorem 7 *(Lucas theorem). Let $d = (d_{n-1} \dots d_0)_p$ and $m = (m_{n-1} \dots m_0)_p$. Then*

$$\binom{d}{m} \equiv \binom{d_{n-1}}{m_{n-1}} \cdots \binom{d_0}{m_0} \pmod{p}.$$

In particular, if $\binom{d}{m} \not\equiv 0 \pmod{p}$ then $m \prec d$.

Lemma 2. *If $1 \leqslant d \leqslant p^n - 2$ has p-weight larger than 2 and $|C_d| = n$, then the function $\operatorname{tr}(\delta(x^d + \gamma(x+1)^d))$, $\delta, \gamma \in \mathbb{F}_{p^n}$, is a constant function if and only if $\delta = 0$.*

Proof. Let $\delta' = \delta\gamma$. Using Lucas theorem we get

$$\begin{aligned}
\operatorname{tr}\bigl(\delta\bigl(x^d + \gamma(x+1)^d\bigr)\bigr) &= \operatorname{tr}\bigl(\delta(1+\gamma)x^d\bigr) + \operatorname{tr}\left(\delta'\left(\sum_{m=0}^{d-1} \binom{d}{m} x^m\right)\right) \\
&= \operatorname{tr}\bigl(\delta(1+\gamma)x^d\bigr) + \operatorname{tr}\left(\delta'\left(\sum_{m \prec d} \binom{d}{m} x^m\right)\right) \\
&= \operatorname{tr}\bigl(\delta(1+\gamma)x^d\bigr) + \sum_{C \in \mathcal{C}} \sum_{m \in C,\, m \prec d} \operatorname{tr}\left(\delta' \binom{d}{m} x^m\right),
\end{aligned}$$

where in the last sum the monomials with exponents from the same cyclotomic cosets are collected together. Let K be the set of the smallest representatives of the cyclotomic cosets. Further for $k \in K$ let $I(k) := \{i \in \{0, \dots, n-1\}\colon\ p^i k \prec d\}$. Then the above sum can written as follows:

$$\begin{aligned}
&\operatorname{tr}\bigl(\delta(1+\gamma)x^d\bigr) + \sum_{k \in K} \sum_{i \in I(k)} \operatorname{tr}\left(\delta' \binom{d}{p^i k} x^{p^i k}\right) \\
&\quad = \operatorname{tr}\bigl(\delta(1+\gamma)x^d\bigr) + \sum_{k \in K} \sum_{i \in I(k)} \operatorname{tr}\left(\left(\binom{d}{p^i k} (\delta')^{p^{n-i}} x^k\right)^{p^i}\right) \\
&\quad = \operatorname{tr}\bigl(\delta(1+\gamma)x^d\bigr) + \sum_{k \in K} \operatorname{tr}\left(\left(\sum_{i \in I(k)} \binom{d}{p^i k} (\delta')^{p^{n-i}}\right) x^k\right) \\
&\quad = \operatorname{tr}\bigl(\delta(1+\gamma)x^d\bigr) + \sum_{k \in K} \operatorname{tr}\bigl(\delta(k)x^k\bigr),
\end{aligned}$$

where $\delta(k) = \sum_{i \in I(k)} \binom{d}{p^i k} (\delta')^{p^{n-i}}$. Since $\operatorname{tr}(\delta(x^d + \gamma(x+1)^d))$ is a polynomial of degree less than $p^n - 1$, it will be a constant on $\mathbb{F}_{p^n}$ only if it is the zero polynomial. The exponents k belong to different cyclotomic cosets, so every summand $\operatorname{tr}(\delta(k)x^k)$ must be constantly 0. By Proposition 5, it must hold $\gamma = -1$ and $\delta(k) = 0$ for every k with $|C_k| = n$. By Corollary 5 if d is unexceptional, then there is a $k \in K$ with $|C_k| = n$ and $|I(k)| = 1$. Let $\gamma = -1$ and d be in the same cyclotomic coset with $\sum_{l=0}^{n/g-2} tp^{gl}$ for some $1 \leqslant t \leqslant p-1$ and a divisor g of d. Remark that n/g is at least 4 because of weight of d. In that case $I(t) = \{0, g, \dots, n-2g\}$ and thus

$$\delta(t) = \sum_{i \in I(t)} \binom{d}{p^i t} (-\delta)^{p^{n-i}} = \sum_{l=0}^{n/g-2} (-\delta)^{p^{n-lg}},$$

where the last equation follows from Lucas lemma. Consider the exponent $t + tp^g$. Then $I(t + tp^g) = \{0, g, \dots, n-3g\}$, implying

$$\delta\bigl(t + tp^g\bigr) = \sum_{i \in I(t+tp^g)} \binom{d}{p^i(t + tp^g)} (-\delta)^{p^{n-i}} = \sum_{l=0}^{n/g-3} (-\delta)^{p^{n-lg}}.$$

Note that $\delta(t) - \delta(t + tp^g) = (-\delta)^{p^{2g}}$. Moreover, $|C_t| = |C_{t+tp^g}| = n$ thus both $\delta(t)$ and $\delta(t + tp^g)$ must be 0, yielding $\delta = 0$. $\square$

Corollary 6. *Let $1 \leqslant d \leqslant p^n - 2$ be of p-weight larger than 2, $|C_d| = n$ and $a \in \mathbb{F}_{p^n}^*$. Then the function $\operatorname{tr}(\delta(x^d + \gamma(x+a)^d))$, where $\delta, \gamma \in \mathbb{F}_{p^n}$, is a constant function if and only if $\delta = 0$.*

A special case of Lemma 2 with $p = 2$, odd n and $\delta = \gamma = 1$ was proved in [13,18].

The statement of Corollary 6 can be generalized for the following class of maps.

Lemma 3. *Let d be an unexceptional integer of p-weight at least 3 and with $|C_d| = n$. Further, let $B \subset \mathbb{F}_{p^n}$ and $a \in \mathbb{F}_{p^n}$. Define $f(x) = \sum_{b \in B} c_b (x+b)^d$, where $c_b \in \mathbb{F}_{p^n}$ and $\sum_{b \in B} c_b \neq 0$. Then $\operatorname{tr}(\delta(f(x) - f(x+a)))$ is a constant function if and only if $\delta = 0$.*

Proof. It is enough to consider the case $a = 1$. We have

$$\begin{aligned}
\sum_{b \in B} c_b (x+b)^d - \sum_{b \in B} c_b (x+b+1)^d &= \sum_{b \in B} c_b \bigl((x+b)^d - (x+b+1)^d\bigr) \\
&= \sum_{b \in B} c_b \biggl(\sum_{m \prec d} \binom{d}{m} \bigl(b^{d-m} - (b+1)^{d-m}\bigr) x^m\biggr) \\
&= \sum_{m \prec d} \binom{d}{m} x^m \biggl(\sum_{b \in B} c_b \bigl(b^{d-m} - (b+1)^{d-m}\bigr)\biggr).
\end{aligned}$$

Using the notation of the proof of Lemma 2, we get

$$\begin{aligned}
&\operatorname{tr}\biggl(\delta\biggl(\sum_{m \prec d} \binom{d}{m} x^m \biggl(\sum_{b \in B} c_b \bigl(b^{d-m} - (b+1)^{d-m}\bigr)\biggr)\biggr)\biggr) \\
&\quad = \sum_{m \prec d} \operatorname{tr}\biggl(\delta \binom{d}{m} \biggl(\sum_{b \in B} c_b \bigl(b^{d-m} - (b+1)^{d-m}\bigr)\biggr) x^m\biggr) \\
&\quad = \sum_{k \in K} \operatorname{tr}\biggl(\sum_{i \in I(k)} \biggl(\delta \binom{d}{p^i k} \biggl(\sum_{b \in B} c_b \bigl(b^{d-p^i k} - (b+1)^{d-p^i k}\bigr)\biggr)\biggr)^{p^{n-i}} x^k\biggr).
\end{aligned}$$

By Corollary 5 there is a k_0 such that $d - k_0 = p^l$, $|C_{k_0}| = n$ and $|I(k_0)| = 1$. The summand corresponding to that k_0 is

$$\mathrm{tr}\left(\delta\binom{d}{k_0}\left(\sum_{b\in B} c_b\left(b^{p^l} - (b+1)^{p^l}\right)\right)x^{k_0}\right) = \mathrm{tr}\left(\delta\binom{d}{k_0}\left(\sum_{b\in B} c_b\right)x^{k_0}\right),$$

which is constantly 0 only if $\delta = 0$. $\square$

For $p = 2$ Lemma 3 implies the following result.

Theorem 8. *Let d be an unexceptional integer of binary weight at least 3 and with $|C_d| = n$. Further, let $B \subset \mathbb{F}_{2^n}$ and $c_b \in \mathbb{F}_{2^n}$ be such that $\sum_{b\in B} c_b \neq 0$. Then $f(x) = \sum_{b\in B} c_b(x+b)^d$ is not crooked.*

Proof. The proof follows from Lemma 3. Indeed, if $f(x)$ is crooked, then for a given $a \in \mathbb{F}_{2^n}^*$ there exists a $\delta \in \mathbb{F}_{2^n}^*$ such that $\mathrm{tr}(\delta(f(x) + f(x+a)))$ is a constant Boolean function. $\square$

For a particular case of the power maps it holds:

Theorem 9. *The only crooked power maps in $\mathbb{F}_{2^n}$ are the ones with exponent $2^i + 2^j$, $\gcd(i - j, n) = 1$.*

Proof. If $D(a)$ is an affine hyperplane then there is a unique $\delta \in \mathbb{F}_{2^n}^*$ such that $D(a) = \{y \in \mathbb{F}_{2^n}: \mathrm{tr}(\delta y) = c\}$, where $c \in \mathbb{F}_2$. Thus, by Lemma 2, d has weight 2 or $|C_d| < n$. If $|C_d| = l < n$ then $D(a) \subset \mathbb{F}_{2^l}$, implying $|D(a)| < 2^{n-1}$. Application of Proposition 3 completes the proof. $\square$

We believe that the statement of Theorem 9 is true for all maps.

Conjecture 1. *All crooked maps are quadratic.*

Another consequence of Corollary 6 is the characterization of integers s for which the bent function $f: \mathbb{F}_{2^n}^2 \to \mathbb{F}_2$

$$f(x, y) = \mathrm{tr}\left(xy^s\right) + h(y),$$

where $h: \mathbb{F}_{2^n} \to \mathbb{F}_2$ is arbitrary, admits a decomposition into four bent functions. A bent function $g: \mathbb{F}_{2^n} \to \mathbb{F}_2$ admits a decomposition into four bent functions if there is an $(n-2)$-dimensional subspace V of $\mathbb{F}_{2^n}$ such that the restrictions of g to cosets of V are bent [4]. In [4] it is shown that $f(x, y)$ admits such a decomposition if and only if there are $a, \delta \in \mathbb{F}_{2^n}^*$ such that $\mathrm{tr}(\delta((x+a)^d + x^d)) = 1$, where d is the multiplicative inverse of s modulo $2^n - 1$. Hence using Corollary 6 the following theorem is immediate.

Theorem 10. *The only bent functions $f(x, y) = \mathrm{tr}(xy^s) + h(y)$, where $h: \mathbb{F}_{2^n} \to \mathbb{F}_2$ is arbitrary and n odd, admitting a decomposition into four bent functions, are the ones having s in the same cyclotomic coset with $\sum_{k=0}^{(n-1)/2} 2^{2ik}$ for some i coprime to n.*

Proof. As in [22] it is shown $\sum_{k=0}^{(n-1)/2} 2^{2ik}$ is the inverse of $2^i + 1$. $\square$

References

[1] T.D. Bending, D. Fon-Der-Flaass, Crooked functions, bent functions, and distance regular graphs, Electron. J. Combin. 5 (1) (1998) R34.

[2] T. Berger, A. Canteaut, P. Charpin, Y. Laigle-Chapuy, On almost perfect nonlinear mappings over F_2^n, IEEE Trans. Inform. Theory, in press.

[3] J. Bierbrauer, G. Kyureghyan, Crooked binomials, manuscript, 2005.

[4] A. Canteaut, P. Charpin, Decomposing bent functions, IEEE Trans. Inform. Theory 49 (8) (2003) 2004–2019.

[5] A. Canteaut, P. Charpin, H. Dobbertin, Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture, IEEE Trans. Inform. Theory 46 (1) (2000) 4–8.

[6] C. Carlet, P. Charpin, V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, Des. Codes Cryptogr. 15 (2) (1998) 125–156.

[7] F. Chabaud, S. Vaudenay, Links between differential and linear cryptanalysis, in: Proc. Advances in Cryptology – EUROCRYPT '94, in: Lecture Notes in Comput. Sci., vol. 950, Springer, Berlin, 1995, pp. 356–365.

[8] H. Dobbertin, Almost perfect nonlinear power functions on GF(2^n): The Niho case, Inform. and Comput. 151 (1–2) (1999) 57–72.

[9] H. Dobbertin, Almost perfect nonlinear power functions on GF(2^n): The Welch case, IEEE Trans. Inform. Theory 45 (4) (1999) 1271–1275.

[10] H. Dobbertin, Almost perfect nonlinear power functions on GF(2^n): A new case for n divisible by 5, in: Proc. Finite Fields and Applications F_q5, Springer, Berlin, 2001, pp. 113–121.

[11] Y. Edel, G. Kyureghyan, A. Pott, A new APN function which is not equivalent to a power mapping, IEEE Trans. Inform. Theory 52 (2) (2006) 744–747.

[12] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, IEEE Trans. Inform. Theory 14 (1968) 154–156.

[13] D. Hertel, A. Pott, A characterization of a class of maximum nonlinear functions, 2004, submitted for publication.

[14] H.D.L. Hollmann, Q. Xiang, A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences, Finite Fields Appl. 7 (2) (2001) 253–286.

[15] T. Kasami, The weight enumerators for several classes of subcodes of the 2nd order binary Reed–Muller codes, Inform. Control 18 (1971) 369–394.

[16] A. Klapper, Cross-correlations of geometric sequences in characteristic two, Des. Codes Cryptogr. 3 (4) (1993) 347–377.

[17] G. Kyureghyan, The only crooked power functions are $2^k + 2^l$, European J. Combin., in press.

[18] Ph. Langevin, P. Véron, On the non-linearity of power function, Des. Codes Cryptogr. 37 (1) (2005) 31–43.

[19] N.G. Leander, Normality of bent functions. Monomial- and binomial-bent functions, PhD thesis, Ruhr Univ. Bochum, Fakultät für Mathematik, Bochum, 2004.

[20] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997.

[21] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.

[22] K. Nyberg, Differentially uniform mappings for cryptography, in: Advances in Cryptology – EUROCRYPT '93, in: Lecture Notes in Comput. Sci., vol. 765, Springer, Berlin, 1994, pp. 55–64.

[23] E.R. van Dam, D. Fon-Der-Flaass, Uniformly packed codes and more distance regular graphs from crooked functions, J. Algebraic Combin. 12 (2) (2000) 115–121.

[24] E.R. van Dam, D. Fon-Der-Flaass, Codes, graphs, and schemes from nonlinear functions, European J. Combin. 24 (1) (2003) 85–98.

[25] J. Wolfmann, Codes projectifs à deux ou trois poids associés aux hyperquadriques d'une géométrie finie, Discrete Math. 13 (2) (1975) 185–211.

[26] Y. Zheng, X.-M. Zhang, Plateaued functions, in: ICICS '99, in: Lecture Notes in Comput. Sci., vol. 1726, Springer, Berlin, 1999, pp. 284–300.