A Note on the Kasami Power Function

Doreen HERTEL†

† Institute for Algebra and Geometry, Faculty of Mathematics, Otto-von-Guericke-University Magdeburg, 39016 Magdeburg, Germany
E-mail: †doreen.hertel@mathematik.uni-magdeburg.de

Abstract This work is motivated by the observation that the function $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ defined by $x^d + (x+1)^d + a$ for some $a \in \mathbb{F}_{2^m}$ can be used to construct difference sets. A desired condition is, that the function $\varphi_d(x) := x^d + (x+1)^d$ is a 2^s-to-1 mapping. If $s = 1$, then the function x^d has to be APN. If $s > 1$, then there is up to equivalence only one function known: The function φ_d is a 2^s-to-1 mapping if d is the Gold parameter $d = 2^k + 1$ with $\gcd(k, m) = s$. We show in this paper, that φ_d is also a 2^s-to-1 mapping if d is the Kasami parameter $d = 2^{2k} - 2^k + 1$ with $\gcd(k, m) = s$ and m/s odd. We hope, that this observation can be used to construct more difference sets.

key words: *difference set, finite field, 2^s-to-1 mapping, APN, Kasami power function, Gold power function*

1. Introduction

In this paper we consider the properties of the Kasami exponent. In the first section we list some similarities between the Kasami exponent $d = 2^{2k} - 2^k + 1$ and the Gold exponent $d = 2^k + 1$. In the second section we give a motivation, why considering functions $x^d + (x+1)^d$. In the last part we present our main result.

We denote the finite field with 2^m elements by $\mathbb{F}_{2^m}$ and its multiplicative group by $\mathbb{F}_{2^m}^*$. The reader is referred to [11] for more information on the theory of finite fields.

We define the function $\varphi_d : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ by

$$\varphi_d(x) := x^d + (x+1)^d.$$

Lemma 1: Let the function φ_d be a c-to-1 mapping. Then the function $\varphi_{d'}$ is also a c-to-1 mapping for $d' = 2^i d$ and, since $\gcd(d, 2^m - 1) = 1$, for $d' = 1/d \bmod 2^m - 1$.

A power function x^d on $\mathbb{F}_{2^m}$ is called **almost perfect nonlinear (APN)**, if the function φ_d is a 2-to-1 mapping. If $\gcd(k, m) = 1$, the Gold and the Kasami power functions are both APN. There are more cases of APN functions, see [12]–[14]. So far, there is only one value d known, where the function φ_d is a 2^s-to-1 mapping: Let $s = \gcd(k, m)$. The function φ_{2^k+1} is a 2^s-to-1 mapping. This follows from the fact, that $\varphi_{2^k+1}(x) = x^{2^k} + x + 1$ is an affine function, see [3]. For the Kasami exponent $d = 2^{2k} - 2^k + 1$ it is only known, that 1 has exactly 2^s preimage under φ_d, since $s = \gcd(k, m)$, see [2]. We will shown, that φ_d with d is the Kasami exponent, is a 2^s-to-1 mapping, since m/s is odd. For this propose, we need the following well-known proposition, which also shows an other common property of the Gold and Kasami exponent.

We define the **trace** function $tr : \mathbb{F}_{2^m} \to \mathbb{F}_2$ by $tr(x) = \sum_{i=0}^{r-1} x^{2^i}$ and the **Walsh transform** $\mathcal{W}(f)$ of a function $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ by

$$\mathcal{W}(f)(y) := \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x)+tr(yx)}$$

for all $y \in \mathbb{F}_{2^m}$. The function $f^{(d)}$ is defined by $f^{(d)}(x) = f(x^d)$ for all $x \in \mathbb{F}_{2^m}$.

Proposition 1: Let $s = \gcd(m, k)$ and m/s odd. Let $d = 2^k + 1$ or $d = 2^{2k} - 2^k + 1$. Then $\mathcal{W}(tr^{(d)})$ takes on the following three values:

value	multiplicity
$2^{(m+s)/2}$	$2^{m-s-1} + 2^{(m-s-2)/2}$
0	$2^m - 2^{m-s}$
$-2^{(m+s)/2}$	$2^{m-s-1} - 2^{(m-s-2)/2}$

Let $\gcd(k, m) = s$ and m/s be odd. Note, we have $\gcd(d, 2^m - 1) = 1$ for $d = 2^k + 1$ or $d = 2^{2k} - 2^k + 1$. In this case, $\gcd(d, 2^m - 1)$ does not depend on $\gcd(k, m)$.

2. Motivation

Let G be a finite abelian additive group with $n_1 n_2$ elements. Let D be a k-subset of the group G, such that every element outside a subgroup N of order n_2 has exactly λ_2 representations as a difference $d - d'$ with elements $d, d' \in D$. Elements in N different from the identity have exactly λ_1 such representations. Any set with this property is called an $(n_1, n_2, k, \lambda_1, \lambda_2)$-**divisible difference set** in G relative to N. If $\lambda_1 = 0$, we call it a **relative difference set**. Note, if $n_2 = 1$, we speak about (n_1, k, λ)-**difference sets**. The reader is referred to [4] for more information on difference sets.

Difference sets with parameter $(2^m - 1, 2^{m-1}, 2^{m-2})$ or $(2^m - 1, 2^{m-1} - 1, 2^{m-2} - 1)$ are called **Singer difference sets**. Singer difference sets correpond to binary sequences with ideal two-level autocorrelation, see [7] for example.

We define for $a \in \mathbb{F}_{2^m}$ the set

$$D_{a,d} := \{ \varphi_d(x) + a \mid x \in \mathbb{F}_{2^m}, \varphi_d(x) \neq a \}.$$

Result 1: The set $D_{a,d}$ is a Singer difference set in $\mathbb{F}_{2^m}^*$ for

1. $d = 2^k + 1$ or $d = 1/(2^k + 1)$ with $\gcd(k, m) = 1$ and $a = 0$. It is easy to show, that in this cases $D_{a,d}$ is the classical Singer difference set.
2. $d = 2^{2k} - 2^k + 1$ with $m = 3k \pm 1$ and $a = 0$. This was conjectured by No, Chung and Yun in [9] and proved by Dillon and Dobbertin in [5], [6].
3. $d = 2^{2k} - 2^k + 1$ with $\gcd(k, m) = 1$ and $a = 1$. This was shown by Dillon and Dobbertin in [6].

This result shows, that the Gold and the Kasami exponent may give difference sets in the case $\gcd(k, m) = 1$. Now let us look at the case $\gcd(k, m) > 1$.

Result 2: Let $\gcd(k, m) = s$ and m/s be odd and $a = 0$. Then the set $D_{a,d}$ is a $(\frac{2^m-1}{2^s-1}, 2^s - 1, 2^{m-s}, 0, 2^{m-2s})$-relative difference set in $\mathbb{F}_{2^m}^*$ for $d = 2^k + 1$ resp. $d = 1/(2^k + 1)$.

As above, this set is the classical affine Singer relative difference set, see [1].

Such $(\frac{2^m-1}{2^s-1}, 2^s-1, 2^{m-s}, 0, 2^{m-2s})$-relative difference sets can be used to construct Singer difference sets by the GMW method, see [1].

We have tried to construct such relative difference sets in a similar way using the Kasami exponent. To get the desired parameters of the relative difference set, we look for 2^s-to-1 mappings φ_d. The function φ_d with d is the Kasami parameter satisfies this property. But computer results indicate, that in this case $D_{a,d}$ is not a relative difference set for $a = 0$ and $a = 1$.

Question 1: Let $d = 2^{2k} - 2^k + 1$ and $\gcd(k, m) > 1$. Do there exists $a \in \mathbb{F}_{2^m}$ such that $D_{a,d}$ is a relative difference set in $\mathbb{F}_{2^m}^*$?

3. Main Theorem

Theorem 1: Let $\gcd(k, m) = s$ and m/s odd. Then the function $\varphi_d : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ with $\varphi_d(x) = x^d + (x + 1)^d$ and $d = 2^{2k} - 2^k + 1$ is a 2^s-to-1 mapping.

To prove this, we need the following proposition. Let $I := \{\varphi_d(x) | x \in \mathbb{F}_{2^m}\}$ be the image of φ_d. If $|\{x \in \mathbb{F}_{2^m} | \varphi_d(x) = y\}| \geq c$ for all $y \in I$, then we say φ_d is at least a c-to-1 mapping.

Proposition 2: Let the function φ_d be at least a 2^s-to-1 mapping and let the Walsh transform of $tr^{(d)}$ take just the values $\pm 2^{(m+s)/2}$ and 0. Then the function φ_d is a 2^s-to-1 mapping.

Proof: We transform

$$\sum_{x \in \mathbb{F}_{2^m}} \left(\mathcal{W}(tr^{(d)})(x)\right)^4 =$$

$$= \sum_{y,z,v,w \in \mathbb{F}_{2^m}} (-1)^{tr(y^d + z^d + v^d + w^d)} \underbrace{\sum_{x \in \mathbb{F}_{2^m}} (-1)^{tr(x(y+z+v+w))}}_{= \begin{cases} 2^m & w = y+z+v \\ 0 & \text{otherwise} \end{cases}}$$

$$= 2^m \sum_{y,z,v \in \mathbb{F}_{2^m}} (-1)^{tr(y^d + z^d + v^d + (y+z+v)^d)}$$

$$= 2^m \sum_{y,z \in \mathbb{F}_{2^m}} \sum_{v \in \mathbb{F}_{2^m}} (-1)^{tr(y^d + (y+v)^d + z^d + (z+v)^d)}$$

$$= 2^m \sum_{y,z \in \mathbb{F}_{2^m}} \sum_{v \in \mathbb{F}_{2^m}} (-1)^{tr(v(y^d + (y+1)^d + z^d + (z+1)^d))}$$

This sum over all $v \in \mathbb{F}_{2^m}$ is 2^m if $y^d + (y + 1)^d = z^d + (z + 1)^d$ and 0 otherwise, thus

$$\sum_{x \in \mathbb{F}_{2^m}} \left(\mathcal{W}(tr^{(d)})(x)\right)^4 =$$
$$= 2^{2m} |\{ (y, z) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \mid \varphi_d(y) = \varphi_d(z) \}|. \quad (1)$$

From Proposition 1 we get $(\mathcal{W}(tr^{(d)})(x))^2 = 2^{m+s}$ exactly 2^{m-1} times and $(\mathcal{W}(tr^{(d)})(x))^2 = 0$ exactly 2^{m-1} times. Therefore, for the left hand side of (1) we calculate $\sum_{x \in \mathbb{F}_{2^m}} (\mathcal{W}(tr^{(d)})(x))^4 = (2^{m+s})^2 \cdot 2^{m-s} = 2^{3m+s}$. For the right hand side of (1) we have $|\{(y, z) | \varphi_d(y) = \varphi_d(z)\}| \geq 2^m \cdot 2^s$, since φ_d maps at least 2^s to 1. The right side is minimal, if φ_d is a 2^s-to-1 mapping. □

Proof of Theorem 1: We define $\phi_d : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ by

$$\phi_d(x) := \frac{1 + x^d}{(1 + x)^d}$$

for all $x \in \mathbb{F}_{2^m} \backslash \{1\}$ and $\phi_d(1) := 1$. If the mapping ϕ_d is at least a 2^s-to-1 mapping, then the mapping φ_d is also at least a 2^s-to-1 mapping, since

$$\varphi_d(x) = \phi_d(x^{-1} + 1) \quad (2)$$

for all $x \in \mathbb{F}_{2^m}^*$ and $\varphi_d(0) = \phi_d(1)$.

We show, that the mapping $\phi_{2^{2k}-2^k+1}$ is at least a 2^s-to-1 mapping. Let $x^* \in \mathbb{F}_{2^s}$, then $\phi_{2^{2k}-2^k+1}(x^*) = 1$, since $(x^*)^{2^s} = x$ and therefore $(x^*)^{2^{2k}-2^k+1} = x^*$. Now let $x^* \in \mathbb{F}_{2^m} \backslash \mathbb{F}_{2^s}$. We have

$$\left(\phi_{2^{2k}-2^k+1}(x^{2^k+1})\right)^{2^k+1} = \frac{(1 + x^{2^{3k}+1})^{2^k+1}}{(1 + x^{2^k+1})^{2^{3k}+1}}. \quad (3)$$

Note, the function φ_{2^l+1} is at least a 2^s-to-1 mapping, since $s | ggT(l, m)$ and $\varphi_{2^l+1}(x) = x^{2^l} + x + 1$. Thus, all elements $x + u, u \in \mathbb{F}_{2^s}$, with $x \in \mathbb{F}_{2^m}$ have the same image under φ_{2^l+1}. We define

$$v := (x^*)^{2^k} + x^* + 1 \quad \text{and} \quad w := (x^*)^{2^{3k}} + x^* + 1.$$

We express v and w by the function ϕ_d. Since (2) holds, we

get for all $y^* := (x^* + u)^{-1} + 1, u \in \mathbb{F}_{2^s}$

$$v = \frac{1 + (y^*)^{2^k+1}}{(1 + y^*)^{2^k+1}} \quad \text{and} \quad w = \frac{1 + (y^*)^{2^{3k}+1}}{(1 + y^*)^{2^{3k}+1}}. \quad (4)$$

We transform (4) and obtain

$$\begin{aligned}
&(1 + (y^*)^{2^{3k}+1})^{2^k+1} = \\
&= (w(1 + y^*)^{2^{3k}+1})^{2^k+1} \\
&= w^{2^k+1}((1 + y^*)^{2^k+1})^{2^{3k}+1} \\
&= w^{2^k+1}(v^{-1}(1 + (y^*)^{2^k+1}))^{2^{3k}+1} \\
&= w^{2^k+1}v^{-(2^{3k}+1)}(1 + (y^*)^{2^k+1})^{2^{3k}+1}.
\end{aligned}$$

We rewrite this equation and get

$$\frac{(1 + (y^*)^{2^{3k}+1})^{2^k+1}}{(1 + (y^*)^{2^k+1})^{2^{3k}+1}} = w^{2^k+1}v^{-(2^{3k}+1)}.$$

Therefore, by (3) we obtain

$$\phi_{2^{2k}-2^k+1}(z^*) = wv^{-d}$$

for all $z^* = ((x^*+u)^{-1}+1)^{1/(2^k+1)}, u \in \mathbb{F}_{2^s}$, since m/s is odd and therefore $\gcd(d, 2^m-1) = 1$. Thus, we have shown that the function $\phi_{2^{2k}-2^k+1}$ is at least a 2^s-to-1 mapping.

Therefore, the function $\varphi_{2^{2k}-2^k+1}$ is also at least a 2^s-to-1 maping. Proposition 1 together with Proposition 2 completes the proof. □

References

[1] A. Pott, "Finite Geometry and Character Theory" Lecture Notes in Mathematics 1601. Berlin: Springer-Verlag, 1995

[2] T. Helleseth, J. Lahtonen, P. Rosendahl, "On certain Equations over Finite Fields and Cross-Correlations of m-Sequences" In: K. Feng, H. Niederreiter and C. Xing, editors, Coding, Cryptograhpy and Combinatorics, Progress in Computer Science and Applied Logic, Vol. 23, pp. 169-176, 2004

[3] K. Nyberg, "Differentially Uniform Mappings for Crytography", Advance in Cryptology, EURO-CRYPT'93, Lecture Notes in Computer Science, Vol.765, pp. 55-64, 1994

[4] T. Beth, D. Jungnickel, H. Lenz, Design Theory. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Vol. 1, 2nd ed., Cambridge, 1999.

[5] J.F. Dillon, "Multiplicative Difference Sets via Additive Charakters", Designs, Codes and Cryptography, Vol.17, No.1-3, pp.225-235, 1999.

[6] J.F. Dillon, H. Dobbertin, "New Cyclic Difference Sets with Singer Parameters", Finite Fields Appl. 10, No.3, pp.342-389, 2004.

[7] T. Helleseth, P.V. Kumar, "Sequences with low correlation", In: Handbook of Coding Theory, Vol.1,2, North-Holland, pp.1065-1138, Amsterdam, 1998.

[8] D. Jungnickel, A. Pott, "Perfect and almost perfect sequences", Discrete Applied Mathematics, Vol.95, pp.331-359, 1999.

[9] J.S. No, H. Chung, M.S. Yun, "Binary Pseudorandom Sequences of Period $2^m - 1$ with Ideal Autocorrelation Generated by the Polynomial $z^d + (z + 1)^d$", IEEE Transactions on Information Theory, Vol.44, pp.1278-1282, 1998.

[10] T. Hellseth, "On the Cross-Correlation of m-Sequences and related Sequences with ideal Autocorrelation", Proceedings of the 2nd International Conference, Sequences and Their Applications (SETA'01), Bergen, Norway, May, 2001. Springer, Discrete Mathematics and Theoretical Computer Science, pp.34-45, 2002.

[11] R. Lidl, H. Niederreiter, "Finite Fields", 2nd ed., Encyclopedia of Mathematics and its Applications, Vol. 20, Cambridge University Press, 1996,

[12] H. Dobbertin, "Almost perfect nonlinear power functions on GF(2^n): A new case for n divisible by 5." Jungnickel, Dieter (ed.) et al., Finite fields and applications. Proceedings of the fifth international conference on finite fields and applications F_q5, University of Augsburg, Germany, August 2-6, 1999. Berlin: Springer-Verlag, pp. 113-121, 2001

[13] H. Dobbertin, "Almost perfect nonlinear power functions on GF(2^n): The Niho case." Inf. Comput., Vol. 151, No.1-2, pp. 57-72, 1999

[14] H. Dobbertin, "Almost perfect nonlinear power functions on GF(2^n): the Welch case." IEEE Trans. Inf. Theory, Vol. 45, No.4, pp. 1271-1275, 1999