Finite Fields and Their Applications 18 (2012) 855–862

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

An upper bound for the linearity of Exponential Welch Costas functions ☆

Risto M. Hakala *

Department of Information and Computer Science, Aalto University, P.O. Box 15400, FI-00076 Aalto, Finland

ARTICLE INFO

Article history:
Received 28 December 2011
Accepted 1 May 2012
Available online 7 May 2012
Communicated by Gary L. Mullen

MSC:
11T71
11T23
11T24
94A60
42A16
42A38

Keywords:
Linearity
Nonlinearity
Welch Costas functions
Exponential function
Fourier analysis

ABSTRACT

The maximum correlation between a function and affine functions is often called the linearity of the function. In this paper, we determine an upper bound for the linearity of Exponential Welch Costas functions using Fourier analysis on $\mathbb{Z}_n$. Exponential Welch Costas functions are bijections on $\mathbb{Z}_{p-1}$, where p is an odd prime, defined using an exponential function of $\mathbb{Z}_p$. Their linearity properties were recently studied by Drakakis, Requena, and McGuire (2010) [1] who conjectured that the linearity of an Exponential Welch Costas function on $\mathbb{Z}_{p-1}$ is bounded from above by $O(p^{0.5+\epsilon})$, where ϵ is a small constant. We prove that the linearity is upper bounded by $\frac{2}{\pi}\sqrt{p}\ln p + 4\sqrt{p}$, which is asymptotically strictly less than what was previously conjectured.

1. Introduction

Linear cryptanalysis [2,3] is a prominent cryptanalytic method that is based on finding linear approximations over the nonlinear components of the cipher. Fourier analysis is commonly used in studying the resistance of a component to linear cryptanalysis. It allows us to determine the strongest linear approximation of a function by finding the largest (nontrivial) absolute value of the Fourier

☆ A version entitled "A Lower Bound for the Nonlinearity of Exponential Welch Costas Functions" appeared in the informal proceedings of the Seventh International Workshop on Coding and Cryptography, WCC 2011, pp. 397–404.

* Fax: +358 9 470 23277.
E-mail address: risto.m.hakala@aalto.fi.

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2012.05.001

coefficients of the function. This quantity is called the linearity of the function and it indicates the maximum correlation between the function and affine functions. The nonlinearity of the function is defined as the minimum distance to the set of affine functions: higher distance means lower linearity and better resistance to linear cryptanalysis. Optimal resistance against linear cryptanalysis is achieved by bent functions [4,5], which have a flat Fourier spectrum.

Traditional linear cryptanalysis is based on constructing linear approximations over binary vector spaces. Since some ciphers, such as SAFER [6,7], IDEA [8] and ZUC [9], rely on components that have simple non-binary representations, the use of other algebraic structures in linear cryptanalysis has been studied as well: for example, Carlet and Ding [10] studied non-binary functions that have optimal nonlinearity; Baignères, Stern, and Vaudenay [11] presented several results related to linear cryptanalysis of ciphers containing non-binary functions. The choice of the algebraic structure affects how Fourier analysis is applied: if a binary vector space is used, Fourier analysis is also performed on the same binary vector space. The general notion on linearity and nonlinearity can be defined using a Fourier transform on arbitrary finite groups, where the chosen groups depend on the definition of the studied function.

In this paper, we derive an upper bound for the linearity of Exponential Welch Costas (EWC) functions and their inverses, Logarithmic Welch Costas (LWC) functions, using Fourier analysis on $\mathbb{Z}_n$. EWC and LWC functions are bijections on $\mathbb{Z}_{p-1}$, where p is an odd prime, and they are used as S-boxes in SAFER with $p = 257$. Cryptographic properties of EWC and LWC functions have been previously studied in [12,1]: Drakakis, Gow, and McGuire [12] showed that EWC functions form a class of almost perfect nonlinear bijections; Drakakis, Requena, and McGuire [1] presented results about the linearity of EWC functions and conjectured based on empirical evidence that the linearity of an EWC function on $\mathbb{Z}_{p-1}$ is bounded from above by $O(p^{0.5+\epsilon})$, where ϵ is a small constant. We prove that the linearity of an EWC function is upper bounded by $\frac{2}{\pi}\sqrt{p}\ln p + 4\sqrt{p}$, which is asymptotically strictly less than the conjectured bound. The bound also shows that EWC functions are asymptotically highly nonlinear: the linearity is larger by at most a logarithmic factor than the minimum linearity achieved by generalized bent functions [4,5].

Studying nonlinearities using Fourier analysis reduces into determining the maximum absolute value of the exponential sum defined by the Fourier transform. The exponential sum studied in this paper is closely related to the exponential sum introduced and studied by Mordell [13]. The main difference between these sums is that Mordell's sum is incomplete and taken over pth roots of unity, while the sum in this paper is complete and taken over $(p-1)$th roots of unity. Our analysis is also different, but contains analogical elements since the results depend on similar trigonometric sums. A fundamental lemma in our analysis is related to the linearity of mappings from $\mathbb{Z}_n$ into $\mathbb{Z}_{n-1}$, where n is any integer with $n \geqslant 3$. The lemma is not exclusive to the analysis in this paper and can be applied in other similar cases as well. The linearity of mappings between $\mathbb{Z}_n$ and $\mathbb{Z}_{n-1}$ has also been considered by Zhou, Feng, and Wu [14] who focused on studying binary linear approximations of addition modulo $2^m - 1$ using known results on binary linear approximations of addition modulo 2^m. Their results can be applied for binary linear cryptanalysis of ZUC which uses addition modulo $2^m - 1$ as a basic arithmetic operation with $m = 31$.

2. Preliminaries

In this section, we recall some definitions from [12,1] and set up the notation. Let n be a positive integer. We use $\mathbb{Z}_n$ to denote the ring of integers modulo n, p to denote an odd prime, and g to denote a generator of the multiplicative group $\mathbb{Z}_p^*$. We also denote $e(z) = \exp(2\pi i z)$ and $e_n(z) = e(z/n)$ for a real number z. The exponential function of $\mathbb{Z}_p$ is a mapping from $\mathbb{Z}_{p-1}$ to $\mathbb{Z}_p^*$ defined as $x \mapsto g^x \bmod p$. If we consider $\mathbb{Z}_{p-1}$ to be the set $\{0, 1, \ldots, p-2\}$ and $\mathbb{Z}_p^*$ to be the set $\mathbb{Z}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$, then EWC functions can be defined as follows:

Definition 1. An Exponential Welch Costas function is a mapping $f : \mathbb{Z}_{p-1} \to \mathbb{Z}_{p-1}$ defined as

$$f(x) = \left(g^x \bmod p\right) - 1.$$

Its inverse function $f^{-1}(x) = \log_g(x+1)$ is called a Logarithmic Welch Costas function.

The linearity and nonlinearity of a function can be defined using its Fourier transform in the following way:

Definition 2. The Fourier transform of $f : \mathbb{Z}_n \to \mathbb{Z}_m$ at $\alpha \in \mathbb{Z}_n$ and $\beta \in \mathbb{Z}_m$ is defined by

$$\hat{f}(\alpha, \beta) = \sum_{x \in \mathbb{Z}_n} e_m\big(\beta f(x)\big) e_n(\alpha x).$$

Definition 3. The linearity of $f : \mathbb{Z}_n \to \mathbb{Z}_m$ is defined by

$$\mathcal{L}(f) = \max_{\alpha \in \mathbb{Z}_n} \max_{\substack{\beta \in \mathbb{Z}_m \\ \beta \neq 0}} \big|\hat{f}(\alpha, \beta)\big|.$$

Definition 4. The nonlinearity of $f : \mathbb{Z}_n \to \mathbb{Z}_m$ is defined by

$$\mathcal{NL}(f) = \frac{n - \mathcal{L}(f)}{m}.$$

It is not hard to show that a bijection and its inverse have the same nonlinearity [1, Theorem 2]. Also, the nonlinearity of an EWC function depends only on the prime p, not on the generator g of $\mathbb{Z}_p^*$ [1, Theorem 3]. It follows that all EWC and LWC functions over $\mathbb{Z}_{p-1}$ have the same nonlinearity.

3. Linearity of Exponential Welch Costas functions

In this section, we derive an upper bound for the linearity of an EWC function. The bound can be used to obtain a lower bound for the nonlinearity. Let p be an odd prime and $f : \mathbb{Z}_{p-1} \to \mathbb{Z}_{p-1}$ be an EWC function defined by

$$f(x) = \big(g^x \bmod p\big) - 1.$$

We obtain an upper bound for

$$\big|\hat{f}(\alpha, \beta)\big| = \left| \sum_{x=0}^{p-2} e_{p-1}\big(\beta f(x)\big) e_{p-1}(\alpha x) \right|$$

for $\alpha, \beta \in \mathbb{Z}_{p-1}$ with $\beta \neq 0$. The analysis of this sum is problematic since two different modulo operations, mod p and mod $p-1$, are mixed in the term $e_{p-1}(\beta f(x))$. Thus, in the proof of Theorem 1, we formulate $e_{p-1}(\beta f(x))$ as a sum, where $f(x)$ is given as an argument for $e_p(\cdot)$ instead of $e_{p-1}(\cdot)$. The final expression consists of two sums that can be bounded individually using the results of Lemmas 1 and 2. Lemma 1 was shown by Drakakis et al. [1] and used to approximate the average linearity of f, but we also present the proof here for completeness. It gives an upper bound for the linearity of the mapping from $\mathbb{Z}_{p-1}$ to $\mathbb{Z}_p$ defined by $x \mapsto (g^x \bmod p) - 1$. Lemma 2 gives crucial information about the linearity of the mapping from $\mathbb{Z}_p$ into $\mathbb{Z}_{p-1}$ defined by $x \mapsto x \bmod p - 1$.

Lemma 1. *For any integers $\alpha \in \mathbb{Z}_{p-1}$ and $r \in \mathbb{Z}_p$ with $r \neq 0$, we have*

$$\left| \sum_{x=0}^{p-2} e_p\big(r f(x)\big) e_{p-1}(\alpha x) \right| \leqslant \sqrt{p}.$$

Proof. Denote

$$W = \sum_{x=0}^{p-2} e_p\big(rf(x)\big)e_{p-1}(\alpha x).$$

We get

$$\begin{aligned}|W|^2 &= \sum_{x,y=0}^{p-2} e_p\big(r\big(g^x - g^y\big)\big)e_{p-1}\big(\alpha(x-y)\big)\\ &= \sum_{z=0}^{p-2} e_{p-1}(\alpha z)\sum_{y=0}^{p-2} e_p\big(rg^y\big(g^z-1\big)\big).\end{aligned}$$

Since

$$\sum_{y=0}^{p-2} e_p\big(rg^y\big(g^z-1\big)\big) = \begin{cases} p-1 & \text{if } z=0 \text{ or } r=0,\\ -1 & \text{otherwise,}\end{cases}$$

we obtain

$$|W|^2 = \begin{cases} (p-1)^2 & \text{if } \alpha = r = 0,\\ 0 & \text{if } \alpha \neq 0, r = 0,\\ 1 & \text{if } \alpha = 0, r \neq 0,\\ p & \text{if } \alpha, r \neq 0,\end{cases}$$

and the result follows. □

We use the ideas presented in the proof of Lemma 8.80 in [15] to prove the following result:

Lemma 2. *For any integers $p \geqslant 3$ and $\beta \in \mathbb{Z}_{p-1}$ with $\beta \neq 0$, we have*

$$\sum_{r=0}^{p-1}\left|\sum_{y=0}^{p-2} e_{p-1}(\beta y)e_p(-ry)\right| < \frac{2}{\pi}p\ln p + 4p.$$

Proof. Denote

$$S(r) = \sum_{y=0}^{p-2} e_{p-1}(\beta y)e_p(-ry).$$

For an integer $r \in \mathbb{Z}_p$, we have

$$\begin{aligned}S(r) &= \sum_{y=0}^{p-2} e_{p-1}(\beta y)e_p(-ry) = \sum_{y=0}^{p-2} e\left(\frac{\beta y}{p-1} - \frac{ry}{p}\right)\\ &= \sum_{y=0}^{p-2} e\left(\left(\frac{\beta}{p-1} - \frac{r}{p}\right)y\right) = \frac{e(\varphi(r)(p-1)) - 1}{e(\varphi(r)) - 1},\end{aligned}$$

where we denote

$$\varphi(r) = \frac{\beta}{p-1} - \frac{r}{p}.$$

Thus,

$$\big|S(r)\big| = \frac{|\sin \pi\varphi(r)(p-1)|}{|\sin \pi\varphi(r)|}.$$

Let R' denote the set $\{\beta-1, \beta, \beta+1, \beta+2\} \subseteq \mathbb{Z}_p$. We will find an upper bound for $\sum_{r=0}^{p-1} |S(r)|$ by comparing sums with integrals. For this purpose, we first find individual upper bounds for $|S(r)|$, $r \in R'$, since the divisor $|\sin \pi\varphi(r)|$ in $|S(r)|$ is close to zero when $r \in R'$. For $s \geqslant 6$, we have

$$\left(\frac{\pi}{s}\right)^{-1} \sin\left(\frac{\pi}{s}\right) \geqslant \left(\frac{\pi}{6}\right)^{-1} \sin\left(\frac{\pi}{6}\right), \quad \text{so} \quad \sin\left(\frac{\pi}{s}\right) \geqslant \frac{3}{s}.$$

It follows that

$$\frac{1}{|\sin \pi\varphi(r)|} = \frac{1}{\sin \pi|\varphi(r)|} \leqslant \frac{1}{3|\varphi(r)|} \tag{1}$$

holds if $|\varphi(r)| \leqslant 1/6$. Since $1 \leqslant \beta \leqslant p-2$, we have $|\varphi(r)| < 2/p$ for all $r \in R'$. Therefore, (1) holds for $p \geqslant 12$ and $r \in R'$. Since also $|\sin\theta| \leqslant |\theta|$ for all θ, we get

$$\big|S(r)\big| = \frac{|\sin \pi\varphi(r)(p-1)|}{|\sin \pi\varphi(r)|} \leqslant \frac{|\pi\varphi(r)(p-1)|}{3|\varphi(r)|} = \frac{\pi}{3}(p-1) \tag{2}$$

for $p \geqslant 12$ and $r \in R'$. We then estimate the remaining part of the sum. Suppose that $p \geqslant 5$ and let R denote the set $\mathbb{Z}_p \setminus R'$. Since $|\sin\theta| = |\sin(-\theta)| = |\sin(\pi-\theta)|$ for all θ, we obtain

$$\begin{aligned}
\sum_{r\in R}\big|S(r)\big| &= \sum_{r=0}^{\beta-2}\big|S(r)\big| + \sum_{r=\beta+3}^{p-1}\big|S(r)\big| \\
&= \sum_{r=p}^{\beta+p-2}\big|S(r)\big| + \sum_{r=\beta+3}^{p-1}\big|S(r)\big| = \sum_{r=\beta+3}^{\beta+p-2}\big|S(r)\big| \\
&\leqslant \sum_{r=\beta+3}^{\beta+p-2} \frac{1}{|\sin \pi\varphi(r)|} = \sum_{r=\beta+3}^{\beta+p-2} \big|\csc \pi\varphi(r)\big| \\
&= \sum_{r=\beta+3}^{\beta+p-2} \csc\left(\pi\left(\frac{r}{p} - \frac{\beta}{p-1}\right)\right) \\
&\leqslant \int_{\beta+2}^{\beta+p-1} \csc\left(\pi\left(\frac{t}{p} - \frac{\beta}{p-1}\right)\right) dt.
\end{aligned}$$

We denote $u = \pi(t/p - \beta/(p-1))$, so $t = pu/\pi + \beta p/(p-1)$ and $dt = (p/\pi)\,du$. Let

$$\theta_1 = \pi\left(\frac{\beta+2}{p} - \frac{\beta}{p-1}\right) = \pi\left(\frac{2p-2-\beta}{p(p-1)}\right)$$

and

$$\theta_2 = \pi\left(\frac{\beta+p-1}{p} - \frac{\beta}{p-1}\right) = \pi\left(1 - \frac{p-1+\beta}{p(p-1)}\right).$$

Since $1 \leqslant \beta \leqslant p-2$, we have $\theta_1 \geqslant \pi/(p-1)$ and $\pi - \theta_2 \geqslant \pi/(p-1)$. Therefore,

$$\begin{aligned}\sum_{r\in R}\left|S(r)\right| &\leqslant \frac{p}{\pi}\int_{\theta_1}^{\theta_2} \csc u\,du \leqslant \frac{2p}{\pi}\int_{\pi/(p-1)}^{\pi/2} \csc u\,du \\ &= -\frac{2p}{\pi}\ln\tan\frac{\pi}{2(p-1)} = \frac{2p}{\pi}\ln\cot\frac{\pi}{2(p-1)} \\ &\leqslant \frac{2p}{\pi}\ln\frac{2(p-1)}{\pi} = \frac{2p}{\pi}\ln\frac{2}{\pi} + \frac{2p}{\pi}\ln(p-1) \qquad (3)\end{aligned}$$

for $p \geqslant 5$. From (2) and (3), we get

$$\begin{aligned}\sum_{r=0}^{p-1}\left|S(r)\right| &\leqslant \frac{4\pi}{3}(p-1) + \frac{2p}{\pi}\ln\frac{2}{\pi} + \frac{2p}{\pi}\ln(p-1) \\ &= \left(\frac{4\pi}{3} + \frac{2}{\pi}\ln\frac{2}{\pi}\right)p + \frac{2p}{\pi}\ln(p-1) - \frac{4\pi}{3} \\ &< \frac{2}{\pi}p\ln p + 4p\end{aligned}$$

for $p \geqslant 12$. This inequality can be quickly checked for $3 \leqslant p \leqslant 11$, so the result follows. □

Theorem 1. *Let f be an EWC function and p be an odd prime. Then*

$$\mathcal{L}(f) < \frac{2}{\pi}\sqrt{p}\ln p + 4\sqrt{p}.$$

Proof. Let $\alpha, \beta \in \mathbb{Z}_{p-1}$ be integers with $\beta \neq 0$. We have

$$\hat{f}(\alpha,\beta) = \sum_{x=0}^{p-2} e_{p-1}\big(\beta f(x)\big)e_{p-1}(\alpha x).$$

For integers z, y, and n with $n \geqslant 2$, we have

$$\sum_{r=0}^{n-1} e_n\big(r(z-y)\big) = \begin{cases} n & \text{if } y \equiv z \bmod n, \\ 0 & \text{if } y \not\equiv z \bmod n, \end{cases}$$

so

$$e_{p-1}\big(\beta f(x)\big) = \frac{1}{p}\sum_{y=0}^{p-2} e_{p-1}(\beta y)\sum_{r=0}^{p-1} e_p\big(r\big(f(x)-y\big)\big)$$
$$= \frac{1}{p}\sum_{r=0}^{p-1}\sum_{y=0}^{p-2} e_{p-1}(\beta y)e_p\big(rf(x)\big)e_p(-ry).$$

The value $r=0$ can be omitted from the sum above since $\sum_{y=0}^{p-2} e_{p-1}(\beta y)=0$. By Lemmas 1 and 2, we obtain

$$\big|\hat{f}(\alpha,\beta)\big| = \left|\sum_{x=0}^{p-2}\frac{1}{p}\sum_{r=1}^{p-1}\sum_{y=0}^{p-2} e_{p-1}(\beta y)e_p\big(rf(x)\big)e_p(-ry)e_{p-1}(\alpha x)\right|$$
$$\leqslant \frac{1}{p}\sum_{r=1}^{p-1}\left|\sum_{y=0}^{p-2} e_{p-1}(\beta y)e_p(-ry)\right|\left|\sum_{x=0}^{p-2} e_p\big(rf(x)\big)e_{p-1}(\alpha x)\right|$$
$$< \frac{2}{\pi}\sqrt{p}\ln p + 4\sqrt{p}. \qquad \square$$

4. Conclusion

We derived an upper bound for the linearity of EWC (and LWC) functions. The bound shows that EWC functions are asymptotically more nonlinear than previously conjectured in [1]. We can also conclude that the asymptotic nonlinearity of EWC functions is high: their linearity is larger by at most a logarithmic factor than the minimum linearity achieved by generalized bent functions [4,5].

The techniques involved in the paper and specifically the result of Lemma 2 are not exclusive to the analysis of EWC functions: they can be used when two different modulo operations are mixed in a similar manner as in EWC functions.

Acknowledgments

The author would like to thank Gary McGuire for bringing [1] to his attention and Kaisa Nyberg for helpful suggestions. The research work has been supported by Helsinki Doctoral Programme in Computer Science – Advanced Computing and Intelligent Systems, Academy of Finland (project #122736), Nokia Foundation, and KAUTE Foundation.

References

[1] K. Drakakis, V. Requena, G. McGuire, On the nonlinearity of Exponential Welch Costas functions, IEEE Trans. Inform. Theory 56 (2010) 1230–1238.
[2] M. Matsui, A. Yamagishi, A new method for known plaintext attack of FEAL cipher, in: EUROCRYPT 1992, in: Lecture Notes in Comput. Sci., vol. 658, Springer, 1993, pp. 81–91.
[3] M. Matsui, Linear cryptanalysis method for DES cipher, in: EUROCRYPT 1993, in: Lecture Notes in Comput. Sci., vol. 765, Springer, 1994, pp. 386–397.
[4] O.S. Rothaus, On "bent" functions, J. Combin. Theory Ser. A 20 (1976) 300–305.
[5] P.V. Kumar, R.A. Scholtz, L.R. Welch, Generalized bent functions and their properties, J. Combin. Theory Ser. A 40 (1985) 90–107.
[6] J.L. Massey, SAFER K-64: A byte-oriented block-ciphering algorithm, in: FSE 1993, in: Lecture Notes in Comput. Sci., vol. 809, Springer, 1994, pp. 1–17.
[7] J.L. Massey, SAFER K-64: One year later, in: FSE 1994, in: Lecture Notes in Comput. Sci., vol. 1008, Springer, 1995, pp. 212–241.
[8] X. Lai, J.L. Massey, A proposal for a new block encryption standard, in: EUROCRYPT 1990, in: Lecture Notes in Comput. Sci., vol. 473, Springer, 1991, pp. 389–404.
[9] ETSI/SAGE, Specification of the 3GPP confidentiality and integrity algorithms 128-EEA3 & 128-EIA3. Document 2: ZUC specification. Version 1.6, Technical report, 2011.

[10] C. Carlet, C. Ding, Highly nonlinear mappings, J. Complexity 20 (2004) 205–244.
[11] T. Baignères, J. Stern, S. Vaudenay, Linear cryptanalysis of non binary ciphers, in: SAC 2007, in: Lecture Notes in Comput. Sci., vol. 4876, Springer, 2007, pp. 184–211.
[12] K. Drakakis, R. Gow, G. McGuire, APN permutations on $\mathbb{Z}_n$ and Costas arrays, Discrete Appl. Math. 157 (2009) 3320–3326.
[13] L.J. Mordell, On the exponential sum $\sum_{x=1}^{X} \exp(2\pi i(ax + bg^x)/p)$, Mathematika 19 (1972) 84–87.
[14] C. Zhou, X. Feng, C. Wu, Linear approximations of addition modulo $2^n - 1$, in: FSE 2011, in: Lecture Notes in Comput. Sci., vol. 6733, Springer, 2011, pp. 359–377.
[15] R. Lidl, H. Niederreiter, Finite Fields, 2nd edition, Encyclopedia Math. Appl., vol. 20, Cambridge University Press, 1997.