ON THE NONLINEARITY OF POWER FUNCTIONS

PHILIPPE LANGEVIN, GRIM UNIVERSITÉ DE TOULON.

Let L be an extension of degree m of the field $\mathbf{F}_2$. Let μ be the canonical additive character of L. The *Fourier coefficient* of the polynomial $f(X) \in L[X]$ at the point $a \in L$ is defined by $\widehat{f}(a) = \sum_{x\in L} \mu(f(x) + a.x)$. The *spectral magnitude* of f, $R(f) := \sup_{a\in\mathbf{F}_2^m} |\widehat{f}(a)|$, is one of the most important cryptographic parameters associated to f [10]. The determination of the spectral magnitude of power functions $x \mapsto x^s$ is an old open problem from different frameworks [5, 9] : two zeros cyclic codes (Kasami, Charpin), correlation of sequences (Gold, Niho, Welch) and boolean functions (Canteaut, Dobbertin). The main questions are : what is the spectral magnitude, say $L(s,m)$ of the power function $x \mapsto x^s$, what is the minimal value $L(m)$ of the $L(s,m)$ and what are the *good* exponents s such that $L(s,m) = L(m)$? Most of the papers on the subject use McEliece's theorem on the divisibility of weight of cyclic codes whose the proof [2, 3, 6] is very similar to those of the Ax 's theorem on the divisibility of the number of zeros of algebraic equations [8]. Here we apply Stickelberger's congruences on Gauss sums [7] to explore the non-linearity of power functions.

Conjecture 1 (Welch)**.** *If m is even then $L(m) = 2^{(m+2)/2}$.*

Let m be an odd integer. By Sidelnikov, we know that $L(m) = 2^{(m+1)/2}$. The set of good exponents is closed under the action of the group generated by the transformations $s \mapsto s^{-1}$ and $s \mapsto 2s$ modulo $q - 1$. We say that two exponents are equivalent if they are in the same orbit. Up to equivalence, all the known good exponents are summarized in the table (1). They share out in four class and usually one conjectures that all the good exponents are known. The Stickelberger's congruences on Gauss sums suggests the introduction of the mapping

$$V : j \mapsto S(-j) + S(j/s)$$

type	s	condition	proof	date
Gold	$2^k + 1$	$(k,m) = 1$	folklore	1968
Kasami	$2^{2k} - 2^k + 1$	$(k,m) = 1$	Kasami.	1971
Welch	$2^t + 3$		DCC(†)	1999
Niho	$2^t + 2^{(m-1)/4} - 1$	$m \equiv 1\,(4)$	DHX(‡)	2000
Niho	$2^t + 2^{(3m-1)/4} - 1$	$m \equiv 3\,(4)$		

TABLE 1. Good exponents, (†)Canteaut, Charpin, Dobbertin, (‡) Dobbertin, Hollmann, Xiang.

where $S(k)$ denotes the sum of the bits of $k \mod q-1$ when j ranges $[0, q-2]$. In particular, we introduce the following notations

$$W_s = \min_{1 \leq j \leq q-2} V(j), \quad J_s = \{j \mid V(j) = W_s\}, \quad P_s(X) = \sum_{j \in J_s} X^j.$$

Proposition 1. *The Fourier coefficients of x^s have a dyadic valuation greater or equal to W_s. Moreover, the multiplicative isomorphism $a \mapsto \bar{a} = \chi(a^s) \mod 2$ shows that $\widehat{f}(a) \equiv 0 \mod 2^{W_s+1} \Leftrightarrow P(\bar{a}) = 0$.*

Theorem 1. *If $W_s = \frac{m+1}{2}$ and $P_s(X)$ has 2^{m-1} roots in L then s is a good exponent.*

Corollary 1. *If $W_s = \frac{m+1}{2}$ and $\sum_{j \in J_s} X^j$ is a permutation polynomial then s is a good exponent.*

The corollary gives a strategy to eventually find new good exponents. Indeed it suffice for example to look for among the s such that J_s reduces to a single cyclotomic class. On the basis of numerical experiments :

Conjecture 2. *An integer s has Gold type if and only if $W_s = t+1$ and $J_s = \{1, 2, \ldots, 2^{m-1}\}$.*

References

[1] W.-C. W. Li et B. Poonen A.R. Calderbank. A 2-adic approach to the analysis of cyclic codes. *IEEE trans. Inf. th.*, 43(3):977–986, 1997.

[2] P. Delsarte. Weight of p-ary abelian codes. *Philips Res. Rep.*, 26:145–153, 1971.

[3] P. Delsarte et R.J. McEliece. Zeros of functions in finite abelian group algebras. *Amer. Journal of Math.*, 98:197–224, 226.

[4] A.R. Calderbank G. McGuire. Proof of a conjecture of sarwate and pursley regarding pairs of binary m-sequence. *IEEE transactions on Inf. Theory*, 41(4):1153–1155, 1995.

[5] D.V. Sarwate M.B. Pursley. Cross correlation properties of pseudo-random and related sequences. *Proc. IEEE*, 68:593–619, 1980.

[6] R.J. McEliece. Weight congruences for p-ary cyclic codes. *Discr. Math.*, 3:177–192, 1972.

[7] J. Stickelberger. Uber eine verallgemeinerung der kreistheilung. *Math. Ann.*, 37:321–367, 1890.

[8] Ax J. Zeroes of polynomials over finite fields. *American Journal of Mathematics*, 86:256–261, 1964.

[9] Canteaut A., Charpin P. and Dobbertin H. Weight divisibility of cyclic codes, highly nonlinear functions and crosscorrelation of maximum-length sequences. *SIAM J. Discrete Math.*, 13:105–138, 2000.

[10] Chabaud F., Vaudenay S. Links between diffrential and linear cryptanalysis. *Eurocrypt 94*, 950:356–365, 1994.

[11] Cusick T., Dobbertin H. Some new 3-valued crosscorrelation functions of binary m-sequences. *IEEE Transactions on Information Theory*, 42:1238–1240, 1996.

[12] Dobbertin H. one-to-one highly non-linear power functions on finite fields. *AAECC*, AECC 9 2:139–152, 1998.

[13] Gold R. Maximal recursive sequences with 3-valued crosscorrelation functions. *IEEE transactions on Information Theory*, 14:154–156, 1968.

[14] Kasami T. The weight enumerators for several classes of subcodes of the 2-nd reed-muller codes. *Information and Control*, 18:369–394, 1971.

[15] Lachaud G., Wolfmann J. Sommes de kloosterman, courbes elliptiques et codes cycliques en caractéristique 2. *Comptes rendus de l'académie des sciences*, 305:881–883, 1987.

[16] Niho Y. *Multi-valued cross correlation functions between two maximal linear recursive sequences.* PhD thesis, University of Southern California, 1972.