AROUND THE COUNTER-EXAMPLES OF PATTERSON–WIEDEMANN

PHILIPPE LANGEVIN, JEAN-PIERRE ZANOTTI

abstract

Let L be an extension of degree m of $\mathbf{F}_2$, the field of order 2. Let μ_L be the canonical additive character of L that applies $z \in L$ onto $(-1)^{\mathrm{tr}_L(z)}$, where $\mathrm{tr}_L(z)$ is the trace of z over $\mathbf{F}_2$. The Fourier coefficient of the boolean function $f\colon L \to \mathbf{F}_2$ at $a \in L$ is defined by :

$$\widehat{f}(a) = \sum_{x\in\mathbf{F}_2^m} (-1)^{f(x)}\mu_L(ax)$$

The non-linearity of f, that is the distance between f and the space of affine functions, writes $2^{m-1} - \frac{1}{2}R(f)$ where $R(f) := \sup_{a\in L} |\widehat{f}(a)|$ is the *spectral magnitude* of f. For this reason, one introduces the *spectral radius* of the space of affine functions of m variables : $R(m) = \inf_f \mathrm{Sp}(f)$, a fundamental number for the cryptographic point of view. Elementary fact from Fourier analysis shows that $2^{m/2} \leq R(m)$ with an equality when m is an even, the corresponding function are the *bent functions* so-called by Rothaus. The spectral magnitude of the quadratic forms are easy to calculate. In particular, when m is odd, the spectral magnitude of a quadratic form of maximal rank is $2^{(m+1)/2}$ therefore

$$2^{m/2} \leq R(m) \leq 2^{(m+1)/2}$$

with equality to the right hand side for $m = 3,\ 5,\ 7$. The demonstration of $R(7) = 64$ is an hard job, done by Mykkelveit, improved by Hou. The equality $R(m) = 2^{(m+1)/2}$ for all odd m was conjectured a time by Mykkelveit is known false since a famous numerical experimentation of Patterson and Wiedemann. In their experience, they look for highly non-linear functions among the space of boolean functions over the field $\mathbf{F}_{2^{15}}$ which are union of cosets of the subgroup of order 217 of multiplicative group of $\mathbf{F}_{2^{15}}$. They have found four functions of 15 variables of spectral magnitude 216 and 232 i.e. exceeding the quadratic bound. However they did not find any structure within these counter-examples.

In that paper, we study the non-linearity of the boolean functions defined over L invariant under the action of a subgroup G of $L^\times$ by means of Gauss sums. We show that some constructions of bent functions by Dillon (partial spread) and by Lachaud and Wolfmann (Kloosterman sums) are related respectively to theorems of Stickelberger and Hasse-Davenport about Gauss sums. Moreover, we construct a function exceeding the quadratic bound over $\mathbf{F}_{2^{15}}$, invariant under the subgroup of order 151 which has a remarkable structure of relative difference set.

sketch of the results.

Let G be a subgroup of order d of $L^\times$. We say that a boolean function f is invariant under G if and only if $F(gz) = F(z)$ for all $g \in G$ and $z \in L$. It is equivalent to say that f is an union of cosets of $L^\times$ modulo G. We want to study the spectral magnitude of the G-invariant boolean functions in order to obtain functions exceeding the quadratic bound. We denote by g the indicating boolean function of the group G so that

$$F(z) = \sum_{\omega \in \Omega} s(\omega) G(\omega z) = \sum_{\omega \in D} G(\omega z),$$

where s is a numerical boolean sequence corresponding to a choice of cosets of G in $L^\times$ whose support denoted by D is a set of cardinality say k. We denote by v the order of the quotient group $\Omega = L^\times/G$ of course $dv = 2^m - 1$. The Fourier coefficient of F at 0 is

$$\widehat{F}(0) = dv + 1 - 2dk.$$

This equality shows that d must be chosen less or equal to $2^t + 1$ to obtain bent functions, and less than 2^{t+1} to have some chance to exceed the quadratic bound. The Fourier coefficient of G at a depends on the class of a modulo G and is given by

$$\widehat{g}(a) = -\frac{2}{v} \sum_{\chi \perp G} \tau_L(\chi) \bar{\chi}(a),$$

(Gauss sum connection) where $\tau_L(\chi) = \sum_{z \in L^\times} \chi(z) \mu_L(z)$ is the Gauss sum associated to the multiplicative character χ and the additive character μ_L. Those of F, is equal to the intercorrelation of F by $\widehat{G}$ and is given by :

$$\widehat{F}(a) = \sum_{\omega \in \Omega} s(\omega) \widehat{G}(a\omega) = \sum_{\omega \in D} \widehat{G}(a\omega) = -\frac{2}{v} \sum_{\chi \perp G} \tau_L(\chi) D(\chi) \bar{\chi}(a).$$

In that last equality, we identify $G^\perp$ with the dual of Ω, whence $D(\chi)$ is the (multiplicative) Fourier transform of D at χ. The main question is : what kind of D could make small the absolute value of the $\widehat{F}(a)$'s ?

m even : new proofs of known results.

Proposition 1 (Dillon). *Let G be the subgroup of order $2^t - 1$ in $L^\times$. If D is a set of 2^{t-1} cosets of the group G in $L^\times$ then the corresponding function is bent.*

Proof. It will be shown as a consequence of Stickelberger theorem claiming that the Gauss sums of order $2^{m/2} + 1$ are equal to $2^{m/2}$. $\square$

Proposition 2 (Lachaud-Wolfmann). *Let G be the subgroup of order $2^t + 1$ in $L^\times$. For any $c \in K^\times$, the set $D_c = \{z \mid \mathrm{tr}_K(c/z) = 1\}$ defines a bent function.*

Proof. This will be shown as a consequence of the Hasse-Davenport theorem about Gauss sums. $\square$

m odd : a remarkable example.

As Patterson and Wiedemann did for the group of order 217, we have looked for invariant boolean functions under the action of the group of order 151. There are 2^{217} such functions but only 2^{23} are also invariant by the Frobenius automorphism. Four of them exceed the quadratic bound with spectral magnitude : 248, 234, 232, and 246. It is worst than in the case of the group of order 217 but one of these functions has a remarkable structure since the corresponding set D is a $(7.31, 108, 100, 46)$ relative difference. Moreover, this difference set can be obtained via a construction proposed by Arasu, Haemers, Jungnickel and Pott combining the Singer sets $(7, 3, 1)$ and $(31, 15, 7)$.

Acknowledgments

Special thanks to K. T. Arasu and J. Wolfmann for pointing us the references [1] and [7].

References

[1] Arasu K. T., Haemers W. H., Jungnickel D., Pott A. Matrix constructions of divisible designs. *Linear of Algebra and its Applications*, 153, 1991.

[2] Berlekamp E. R., Welch L. R. Distributions of the cosets of the $(32, 6)$ Reed-Muller code. *IEEE Transactions on Information Theory*, 13(1):203–207, 1972.

[3] Constantin J., Courteau B., Wolfmann J. Numerical experiments related to the covering radius of some Reed-Muller codes. In Lecture Notes in Computer Science, editor, *Algebraic Algorithms and Error-Correcting Codes*, volume 229, pages 69–75. 3rd International Conference AAECC, 1986.

[4] Dillon J. F. *Elementary Hadamard Difference Sets*. PhD thesis, University of Maryland, 1974.

[5] Dillon J. F. Elementary Hadamard difference sets. In *sixth SECCGTC*, 1975.

[6] Hou X.-D. Covering radius of the Reed-Muller code $R(1, 7)$ — a simpler proof. *Journal of Combinatorial Theory*, 74, 1996.

[7] 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.

[8] Lidl R., Niederreiter H. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley, 1983.

[9] Mykkelveit J. J. The covering radius of the $(128, 8)$ Reed-Muller codes is 56. *IEEE Transactions on Information Theory*, 26(3):359–362, 1980.

[10] Patterson N. J., Wiedemann D. H. The covering radius of the $(1, 15)$ Reed-Muller code is at least 16276. *IEEE Transactions on Information Theory*, 29:354–356, 1983.

[11] Rothaus O. S. On bent functions. *Journal of Combinatorial Theory (A)*, 20:300–305, 1976.

GRIM, Université de Toulon, 83957 La Garde, France.