HIGHLY NONLINEAR FUNCTIONS

KAI-UWE SCHMIDT

ABSTRACT. Let f be a function from $\mathbb{Z}_q^m$ to $\mathbb{Z}_q$. Such a function f is bent if all values of its Fourier transform have absolute value 1. Bent functions are known to exist for all pairs (m, q) except when m is odd and $q \equiv 2 \pmod 4$ and there is overwhelming evidence that no bent function exists in the latter case. In this paper the following problem is studied: how closely can the largest absolute value of the Fourier transform of f approach 1? For $q = 2$, this problem is equivalent to the old and difficult open problem of determining the covering radius of the first order Reed-Muller code. The main result is, loosely speaking, that the largest absolute value of the Fourier transform of f can be made arbitrarily close to 1 for q large enough.

1. Introduction and Results

Let f be a function from $\mathbb{Z}_q^m$ to $\mathbb{Z}_q$ and write $\omega = e^{2\pi i/q}$. The *Fourier* (or *Walsh*) *transform* of f is the function $\widehat{f} : \mathbb{Z}_q^m \to \mathbb{C}$ given by

$$\widehat{f}(\lambda) = \frac{1}{q^{m/2}} \sum_{x \in \mathbb{Z}_q^m} \omega^{f(x) - \lambda x^T}.$$

Kumar, Scholtz, and Welch [9] defined f to be *bent* if

$$\left|\widehat{f}(\lambda)\right| = 1 \quad \text{for all } \lambda \in \mathbb{Z}_q^m.$$

This generalises the classical definition of bent functions (arising for $q = 2$) by Rothaus [14]. The value

$$\max_{\lambda \in \mathbb{Z}_q^m} \left|\widehat{f}(\lambda)\right| \tag{1}$$

equals the largest magnitude of an Hermitian inner product of ω^f with ω^ℓ, where ℓ is a linear function from $\mathbb{Z}_q^m$ to $\mathbb{Z}_q$. Hence (1) is a measure of nonlinearity of f. Notice that (1) is at least 1 by Parseval's identity and thus bent functions have largest possible nonlinearity in this context.

Date: 23 April 2013 (revised 02 September 2013).

2010 *Mathematics Subject Classification.* 06E75, 42A16, 05D40.

Key words and phrases. Generalised bent function, Nonlinearity, Fourier coefficient, Probabilistic method.

The author is with Faculty of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany. Email: kaiuwe.schmidt@ovgu.de.

Constructions of bent functions are known [9] for all pairs (m,q) except when m is odd and $q \equiv 2 \pmod 4$. For $q=2$, the values of $q^{m/2}\widehat{f}(\lambda)$ must be real and integral and hence bent functions cannot exist for $q=2$ and odd m. Several authors have established the nonexistence of bent functions for odd m and infinitely many values of q [9], [13], [1], [7], [5] [10], providing overwhelming evidence that no bent function exists when m is odd and $q \equiv 2 \pmod 4$.

For integers $q \geq 2$ and $m \geq 1$, define

$$\mu(q,m) = \min_{f} \max_{\lambda \in \mathbb{Z}_q^m} \big|\widehat{f}(\lambda)\big|,$$

where the minimum is over all functions f from $\mathbb{Z}_q^m$ to $\mathbb{Z}_q$. Then

$$1 \leq \mu(q,m) \leq \sqrt{q}. \tag{2}$$

Due to the existence of bent functions, the lower bound is an equality except possibly when m is odd and $q \equiv 2 \pmod 4$. The upper bound in (2) is trivial for $m=1$ and, for odd $m \geq 3$, arises by "lifting" a bent function on $\mathbb{Z}_q^{m-1}$ to a function on $\mathbb{Z}_q^m$.

The determination of $\mu(2,m)$ is equivalent to the difficult open problem of finding the covering radius of the first order Reed-Muller code [17]. It is known [3], [11], [6] that equality holds in the upper bound of (2) for $q=2$ and $m \in \{3,5,7\}$. It is also known that

$$\mu(2,m) \leq \begin{cases} \sqrt{49/32} & \text{for } m \geq 9 \text{ (see [8])} \\ \sqrt{729/512} & \text{for } m \geq 15 \text{ (see [12])}. \end{cases}$$

Patterson and Wiedemann [12] conjectured that

$$\lim_{m\to\infty} \mu(2,m) = 1. \tag{3}$$

An appropriate generalisation of the conjecture (3) is

$$\lim_{m\to\infty} \mu(q,m) = 1$$

for each $q \geq 2$. For fixed $q > 2$ satisfying $q \equiv 2 \pmod 4$, this conjecture however does not seem to be easier to resolve than the original conjecture (3).

In this paper we prove that

$$\lim_{q\to\infty} \mu(q,m) = 1.$$

for each $m \geq 1$, which is implied by the following more precise result.

Theorem 1. *For all sufficiently large q^m, we have*

$$\mu(q,m) < \cos\frac{\pi}{q} + 15\sin\frac{\pi}{q}.$$

Notice that, for all $q \geq 16$, the bound of Theorem 1 is strictly better than the upper bound in (2).

To prove Theorem 1, we generalise the notion of bent functions to functions from $\mathbb{Z}_q^m$ to $\mathbb{Z}_{2q}$ (these generalise at the same time the bent functions

from $\mathbb{Z}_q^m$ to $\mathbb{Z}_q$, as defined by Kumar, Scholtz, and Welch [9], and the bent functions from $\mathbb{Z}_2^m$ to $\mathbb{Z}_4$, as defined by the author [15]). We give a construction of such generalised bent functions for all m and all even q. To establish Theorem 1, we apply a random modification to this construction, using a method of Beck [2].

2. A generalised bent function

Let $\zeta = e^{\pi i/q}$ be a primitive $(2q)$-th root of unity and write $\omega = \zeta^2$. We say that a function $f : \mathbb{Z}_q^m \to \mathbb{Z}_{2q}$ is *bent* if

$$\frac{1}{q^{m/2}} \left| \sum_{x \in \mathbb{Z}_q^m} \zeta^{f(x)}\, \omega^{-\lambda x^T} \right| = 1 \quad \text{for all } \lambda \in \mathbb{Z}_q^m.$$

We provide a construction of such bent functions for all even q, generalising [15, Construction 5.7].

Proposition 2. *Let q be an even positive integer. The function $g : \mathbb{Z}^m \to \mathbb{Z}$, given by*

$$g(x_1, \ldots, x_m) = x_1^2 + \cdots + x_m^2,$$

induces a function f from $\mathbb{Z}_q^m$ to $\mathbb{Z}_{2q}$ that is bent.

Proof. The function g induces a function from $\mathbb{Z}_q^m$ to $\mathbb{Z}_{2q}$ because q is even, and thus

$$(x+q)^2 \equiv x^2 \pmod{2q} \quad \text{for all } x \in \mathbb{Z}. \tag{4}$$

To verify the bent property of f, let $\lambda = (\lambda_1, \ldots, \lambda_m)$ be an element of $\mathbb{Z}^m$. Then

$$\begin{aligned}
\sum_{x \in \mathbb{Z}_q^m} \zeta^{f(x)} \omega^{-\lambda x^T} &= \sum_{x_1, \ldots, x_m = 0}^{q-1} \zeta^{x_1^2 + \cdots + x_m^2 - 2\lambda_1 x_1 - \cdots - 2\lambda_m x_m} \\
&= \prod_{k=1}^{m} \sum_{x_k=0}^{q-1} \zeta^{x_k^2 - 2\lambda_k x_k} \\
&= \prod_{k=1}^{m} \sum_{y_k=0}^{q-1} \zeta^{y_k^2 - \lambda_k^2}
\end{aligned}$$

by setting $x_k = y_k + \lambda_k$ and using (4). Therefore,

$$\sum_{x \in \mathbb{Z}_q^m} \zeta^{f(x)} \omega^{-\lambda x^T} = \left(\prod_{k=1}^{m} e^{-\pi i \lambda_k^2/q} \right) \left(\sum_{y=0}^{q-1} e^{\pi i y^2/q} \right)^m$$

and the proposition is proved by showing that

$$\left| \sum_{y=0}^{q-1} e^{\pi i y^2/q} \right| = \sqrt{q}.$$

We have

$$\left|\sum_{y=0}^{q-1} e^{\pi i y^2/q}\right|^2 = \sum_{y,z=0}^{q-1} e^{\pi i y^2/q}\, e^{-\pi i z^2/q}$$
$$= \sum_{y,w=0}^{q-1} e^{\pi i y^2/q}\, e^{-\pi i (y+w)^2/q},$$

using (4) again. Therefore

$$\left|\sum_{y=0}^{q-1} e^{\pi i y^2/q}\right|^2 = \sum_{w=0}^{q-1} e^{-\pi i w^2/q} \sum_{y=0}^{q-1} e^{-2\pi i y w/q}.$$

The inner sum is zero, unless $w \equiv 0 \pmod q$, in which case the inner sum, and hence the total sum, equals q, as required. □

3. Bounding linear transformations

In this section we elaborate on a result due to Spencer [18] and a refinement due to Sharif and Hassibi [16].

We define a norm on $\mathbb{C}^n$ by

$$\|(x_1,\dots,x_n)\| = \max\{|x_1|,\dots,|x_n|\}.$$

Lemma 3 ([18, Theorem 7], [16, Lemma 3])**.** *Let A be a matrix of size $\ell \times m$ satisfying $\ell \le m$ with real-valued entries of absolute value at most 1. Then there exists a nondecreasing function $K : (0,1] \to \mathbb{R}$ satisfying*

(i) $K(\alpha) \le 11\sqrt{\alpha \log(2/\alpha)}$*, and*

(ii) $K(\alpha) \le t\sqrt{\alpha} + K\big(\sqrt{-3.05\alpha Q(t)\,\log_2(0.39Q(t))}\big)$ *for all real $t > 3$, where*

$$Q(t) = \frac{1}{\sqrt{2\pi}} \int_t^\infty e^{-x^2/2}\,dx,$$

such that the following holds. For all sufficiently large ℓ, there exists $u \in \{-1,1\}^\ell$ such that

$$\|uA\| \le K(\ell/m)\sqrt{m}.$$

We use Lemma 3 to deduce the following lemma.

Lemma 4. *Let K be as in Lemma 3 and let $h \ge 2$ be an integer. Let B be a matrix of size $\ell \times n$ satisfying $\ell \le hn$ with complex-valued entries of absolute value at most 1. Then, for all sufficiently large ℓ, there exists $u \in \{-1,1\}^\ell$ such that*

$$\|uB\| \le \sec\Big(\frac{\pi}{2h}\Big) K\Big(\frac{\ell}{hn}\Big)\sqrt{hn}.$$

Proof. For complex z, we have the elementary geometric inequality

$$|z| \le \sec\Big(\frac{\pi}{2h}\Big) \max_{j\in\{0,\dots,h-1\}} \big|\operatorname{Re}(ze^{\pi ij/h})\big|. \tag{5}$$

Construct a matrix of size $\ell \times hn$ with real-valued entries by

$$A = \begin{bmatrix}\operatorname{Re}(B) & \operatorname{Re}(Be^{\pi i/h}) & \operatorname{Re}(Be^{\pi i2/h}) & \dots & \operatorname{Re}(Be^{\pi i(h-1)/h})\end{bmatrix}.$$

By Lemma 3 applied with $m = hn$, we see that there exists $u \in \{-1,1\}^\ell$ such that

$$\|uA\| \le K\Big(\frac{\ell}{hn}\Big)\sqrt{hn}$$

and the lemma follows from (5). □

We shall apply Lemma 4 in the following equivalent form.

Lemma 5. *Let K be as in Lemma 3 and let $h \ge 2$ be an integer. Let B be a matrix of size $\ell \times n$ satisfying $\ell \le hn$ with complex-valued entries of absolute value at most 1. Let $\epsilon_1, \dots, \epsilon_\ell$ be complex numbers of absolute value at most r. Then, for all sufficiently large ℓ, there exists $v_k \in \{-\epsilon_k, \epsilon_k\}$ for all $k \in \{1, \dots, \ell\}$ such that $v = (v_1, \dots, v_\ell)$ satisfies*

$$\|vB\| \le r \sec\Big(\frac{\pi}{2h}\Big) K\Big(\frac{\ell}{hn}\Big)\sqrt{hn}.$$

We shall apply Lemma 5 with $h = 8$ and ℓ equal to either n or $n/2$, so that we require upper bounds for $K(1/8)$ and $K(1/16)$.

With $Q(t)$ defined as in Lemma 3, we have

$$Q(t) \le \frac{1}{\sqrt{2\pi}\,t}\, e^{-t^2/2}$$

(see [4, Theorem 1.2.3], for example). Applying the implicit bound (ii) for K in Lemma 3, first with $t = 5$ and then with $t = 7$, we find that

$$\begin{aligned} K(1/8) &\le 5\sqrt{1/8} + K(1.617 \times 10^{-3}) \\ &\le 5\sqrt{1/8} + 7\sqrt{1.617 \times 10^{-3}} + K(5.127 \times 10^{-7}). \end{aligned}$$

Then, using the explicit bound (i) for K in Lemma 3, we conclude that $K(1/8) < 2.08$ and therefore,

$$\sec(\pi/16)K(1/8)\sqrt{8} < 6. \tag{6}$$

Likewise (by taking the same parameters), we have $K(1/16) < 1.52$ and

$$\sec(\pi/16)K(1/16)\sqrt{8} < 4.4. \tag{7}$$

4. Proof of Theorem 1

Write $\omega = e^{2\pi i/q}$ and let $B = (b_{kj})$ be the $q^m \times q^m$ matrix whose elements are given by

$$b_{kj} = \omega^{-(j_1k_1+\cdots+j_mk_m)},$$

where

$$j = 1 + j_1 + j_2q + \cdots + j_mq^{m-1}$$
$$k = 1 + k_1 + k_2q + \cdots + k_mq^{m-1}$$

and $j_\ell, k_\ell \in \{0, \ldots, q-1\}$ for all $\ell \in \{1, \ldots, m\}$. Given a function $f : \mathbb{Z}_q^m \to \mathbb{Z}_q$, there exists a uniquely determined vector $z = (z_1, \ldots, z_{q^m})$ such that

$$\omega^{f(k_1,\ldots,k_m)} = z_{1+k_1+k_2q+\cdots+k_mq^{m-1}} \quad \text{for each } (k_1, \ldots, k_m) \in \mathbb{Z}_q^m,$$

where the index is computed in $\mathbb{Z}$. Thus the theorem is proved by showing the existence of a vector $z \in \mathbb{C}^{q^m}$ whose entries are q-th roots of unity such that

$$\|zB\| < \left(\cos\frac{\pi}{q} + 15\sin\frac{\pi}{q}\right)q^{m/2} \tag{8}$$

for all sufficiently large q^m.

Since bent functions from $\mathbb{Z}_q^m$ to $\mathbb{Z}_q$ always exist when q is odd and the expression in the bracket of (8) is strictly greater than 1 for all $q \geq 2$, we may assume that q is even. Then, by the above discussion and by Proposition 2, there exists a vector $x \in \mathbb{C}^{q^m}$ (induced by the bent function in Proposition 2) whose entries are $(2q)$-th roots of unity such that

$$\|xB\| = q^{m/2}. \tag{9}$$

By multiplying x with $e^{\pi i/q}$ if necessary, we may also assume that

(10) at least half of the entries of x are not q-th roots of unity.

We obtain a vector z satisfying (8) by rounding the entries of x to q-th roots of unity, using a refined version of a method due to Beck [2].

Write $\rho = \cos(\pi/q)$, so that ρ is the radius of the inscribed circle of the regular q-sided polygon whose vertices are the q-th roots of unity. Write $x = (x_1, \ldots, x_{q^m})$ and let $k \in \{1, \ldots, q^m\}$. Then $x_k = e^{\pi i(2j)/q}$ or $x_k = e^{\pi i(2j+1)/q}$ for some j satisfying $0 \leq j < q$. In either case, ρx_k lies within the triangle Δ_k with vertices

$$(e^{2\pi i(j-1)/q} + e^{2\pi ij/q})/2,\ e^{2\pi ij/q},\ (e^{2\pi i(j+1)/q} + e^{2\pi ij/q})/2. \tag{11}$$

Let d be the diameter of the triangles Δ_k, so that

$$d = 2\cos(\pi/q)\,\sin(\pi/q). \tag{12}$$

For a real number λ and a triangle Δ, let $\lambda\Delta$ be the triangle obtained by a uniform scaling of Δ with scaling factor λ. Using the barycentric

decomposition of a triangle, we have the chain of partitions

$$\Delta_k = \bigcup_{s=1}^{4} \Delta_k(1,s) = \bigcup_{s=1}^{4^2} \Delta_k(2,s) = \cdots = \bigcup_{s=1}^{4^\ell} \Delta_k(\ell,s) = \cdots,$$

where, for each $s \in \{1,\dots,4^\ell\}$, the triangle $\Delta_k(\ell,s)$ is congruent to $2^{-\ell}\Delta_k$. Notice that the diameter of the triangles $\Delta_k(\ell,s)$ equals $2^{-\ell}d$.

Let $t>1$ be an integer to be determined later. Then there exist integers $s_1,\dots,s_t$ satisfying $s_\ell \in \{1,\dots,4^\ell\}$ for all $\ell \in \{1,\dots,t\}$ such that

$$\rho x_k \in \Delta_k(t,s_t) \subset \Delta_k(t-1,s_{t-1}) \subset \cdots \subset \Delta_k(1,s_1) \subset \Delta_k.$$

Let $y^{(t)}$ be a vector in $\mathbb{C}^{q^m}$ whose k-th entry is obtained by rounding ρx_k to a nearest vertex of the small triangle $\Delta_k(t,s_t)$. Then

$$\|\rho x - y^{(t)}\| \le 2^{-t} d/2$$

and so

$$\|\rho x B - y^{(t)} B\| \le q^m 2^{-t} d/2. \tag{13}$$

In the next step, we round the k-th entry of $y^{(t)}$ to a vertex of the big triangle Δ_k. By virtue of the definition of Δ_k, we see from (10) that at least $q^m/2$ entries of $y^{(t)}$ are already vertices of the corresponding big triangle. Now, each vertex of $\Delta_k(t,s_t)$ is either a vertex of $\Delta_k(t-1,s_{t-1})$ or lies exactly in the centre between two vertices of $\Delta_k(t-1,s_{t-1})$. We apply Lemma 5 with $r = 2^{-(t-1)}d/2$, $\ell = q^m/2$, $n = q^m$, and $h = 8$ and use (7) to conclude that there exists a vector $y^{(t-1)}$ whose entries are vertices of $\Delta_k(t-1,s_{t-1})$ such that

$$\|y^{(t)}B - y^{(t-1)}B\| < 4.4 \cdot 2^{-t} d\, q^{m/2}$$

for all sufficiently large q^m. Continuing this process, there exist vectors $y^{(t-2)},\dots,y^{(1)},y^{(0)}$ whose entries are vertices of $\Delta_k(t-2,s_{t-2}),\dots,\Delta_k(1,s_1)$, Δ_k, respectively, such that

$$\|y^{(\ell)}B - y^{(\ell-1)}B\| < 4.4 \cdot 2^{-\ell} d\, q^{m/2} \quad \text{for each } \ell \in \{1,\dots,t\}$$

and all sufficiently large q^m. Hence, by the triangle inequality,

$$\begin{aligned} \|y^{(t)}B - y^{(0)}B\| &\le \sum_{\ell=1}^{t} \|y^{(\ell)}B - y^{(\ell-1)}B\| \\ &< \sum_{\ell=1}^{t} 4.4 \cdot 2^{-\ell} d\, q^{m/2} \\ &< 4.4\, d\, q^{m/2}. \end{aligned} \tag{14}$$

The k-th entry in $y^{(0)}$ is a vertex of Δ_k, so equals one of the points in (11). Notice that the length of the two equal sides of the triangle Δ_k equals $\sin(\pi/q)$. We apply Lemma 5 once more with $r = \sin(\pi/q)$, $\ell = n = q^m$,

and $h = 8$ and use (6) to conclude that there exists a vector $z \in \mathbb{C}^{q^m}$ whose entries are q-th roots of unity such that

$$\|zB - y^{(0)}B\| < 6\sin(\pi/q)\, q^{m/2} \tag{15}$$

for all sufficiently large q^m.

Now from (13), (14), and (15), for all sufficiently large q^m, we have by the triangle inequality

$$\begin{aligned}\|zB - \rho xB\| &< 6\sin(\pi/q)q^{m/2} + 4.4\, d\, q^{m/2} + q^m\, 2^{-t} d/2 \\ &= \sin(\pi/q)q^{m/2}\big(6 + 8.8\cos(\pi/q) + q^{m/2}\, 2^{-t}\cos(\pi/q)\big)\end{aligned}$$

using (12). Hence, by choosing t large enough, we have

$$\|zB - \rho xB\| < 15\sin(\pi/q)\, q^{m/2}.$$

From (9) we have $\|\rho xB\| = \cos(\pi/q)\, q^{m/2}$, which shows that z satisfies (8), as required. □

References

[1] E. Akyildiz, I. Ş. Güloğlu, and M. İkeda. A note of generalized bent functions. *J. Pure Appl. Algebra*, 106(1):1–9, 1996.

[2] J. Beck. Flat polynomials on the unit circle—note on a problem of Littlewood. *Bull. London Math. Soc.*, 23(3):269–277, 1991.

[3] E. R. Berlekamp and L. R. Welch. Weight distributions of the cosets of the (32, 6) Reed-Muller code. *IEEE Trans. Inform. Theory*, IT-18(1):203–207, 1972.

[4] R. Durrett. *Probability: Theory and Examples*. Cambridge University Press, 4th edition, 2010.

[5] K. Feng and F. Liu. New results on the nonexistence of generalized bent functions. *IEEE Trans. Inform. Theory*, 49(11):3066–3071, 2003.

[6] X.-D. Hou. Covering radius of the Reed-Muller code $R(1, 7)$—a simpler proof. *J. Combin. Theory Ser. A*, 74(2):337–341, 1996.

[7] M. İkeda. A remark on the non-existence of generalized bent functions. In *Number theory and its applications (Ankara, 1996)*, volume 204 of *Lecture Notes in Pure and Appl. Math.*, pages 109–119. Dekker, New York, 1999.

[8] S. Kavut and M. D. Yücel. 9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class. *Inform. and Comput.*, 208(4):341–350, 2010.

[9] P. V. Kumar, R. A. Scholtz, and L. R. Welch. Generalized bent functions and their properties. *J. Combin. Theory Ser. A*, 40(1):90–107, 1985.

[10] F. M. Liu and Q. Yue. The relationship between the nonexistence of generalized bent functions and Diophantine equations. *Acta Math. Sin. (Engl. Ser.)*, 27(6):1173–1186, 2011.

[11] J. J. Mykkeltveit. The covering radius of the (128, 8) Reed-Muller code is 56. *IEEE Trans. Inform. Theory*, 26(3):359–362, 1980.

[12] N. J. Patterson and D. H. Wiedemann. The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16 276. *IEEE Trans. Inform. Theory*, 29(3):354–356, 1983. Corrected in: IEEE Trans. Inform. Theory, 36(2):443, 1990.

[13] D. Y. Pei. On nonexistence of generalized bent functions. In *Finite fields, coding theory, and advances in communications and computing (Las Vegas, NV, 1991)*, volume 141 of *Lecture Notes in Pure and Appl. Math.*, pages 165–172. Dekker, New York, 1993.

[14] O. S. Rothaus. On "bent" functions. *J. Combin. Theory Ser. A*, 20(3), 1976.

[15] K.-U. Schmidt. Quaternary constant-amplitude codes for multicode CDMA. *IEEE Trans. Inform. Theory*, 55(4):1824–1832, 2009.

[16] M. Sharif and B. Hassibi. Existence of codes with constant PMEPR and related design. *IEEE Trans. Signal Proces.*, 52(10):2836–2846, 2004.

[17] N. Sloane. Unsolved problems related to the covering radius of codes. In T. Cover and B. Gopinath, editors, *Open Problems in Communication and Computation*, pages 51–56. Springer New York, 1987.

[18] J. Spencer. Six standard deviations suffice. *Trans. Amer. Math. Soc.*, 289(2):679–706, 1985.