

# ASYMPTOTICALLY OPTIMAL BOOLEAN FUNCTIONS

KAI-UWE SCHMIDT

ABSTRACT. The largest Hamming distance between a Boolean function in  $n$  variables and the set of all affine Boolean functions in  $n$  variables is known as the covering radius  $\rho_n$  of the  $[2^n, n+1]$  Reed-Muller code. This number determines how well Boolean functions can be approximated by linear Boolean functions. We prove that

$$\lim_{n \rightarrow \infty} 2^{n/2} - \rho_n / 2^{n/2-1} = 1,$$

which resolves a conjecture due to Patterson and Wiedemann from 1983.

## 1. INTRODUCTION AND RESULTS

The Hamming distance of two Boolean functions  $F, G : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  is

$$d(F, G) = \#\{y \in \mathbb{F}_2^n : F(y) \neq G(y)\}.$$

Put

$$\rho_n = \max_F \min_G d(F, G),$$

where the maximum is over all functions  $F$  from  $\mathbb{F}_2^n$  to  $\mathbb{F}_2$  and the minimum is over all  $2^{n+1}$  affine functions  $G$  from  $\mathbb{F}_2^n$  to  $\mathbb{F}_2$ . Then  $\rho_n$  equals the covering radius of the  $[2^n, n+1]$  Reed-Muller code, whose determination is one of the oldest and most difficult open problems in coding theory [6], [14], [17]. We refer to [4] for background on the covering radius of codes in general and its combinatorial and geometric significance. The determination of  $\rho_n$  also answers the question of how well Boolean functions can be approximated by linear functions, which is of significance in cryptography [3]. One can also interpret  $\rho_n$  in terms of the Fourier coefficients of Boolean functions (see Section 2).

It is convenient to define

$$\mu_n = 2^{n/2} - \rho_n / 2^{n/2-1}.$$

An averaging argument shows that  $\mu_n \geq 1$  (see Section 2) and a simple recursive construction involving functions of the form  $F(y) + uv$  on  $\mathbb{F}_2^{n+2}$  shows that  $\mu_{n+2} \leq \mu_n$ . The fact that  $\mu_2 = 1$  implies that  $\mu_n = 1$  for all even  $n$ ; the functions attaining the minimum are known as *bent* functions and these have been studied extensively for more than forty years [15], [12].

---

*Date:* 17 October 2018.

2010 *Mathematics Subject Classification.* Primary: 11T71; Secondary: 94B05, 06E30.  
K.-U. Schmidt is partly supported by German Research Foundation (DFG).

We are interested in the case that  $n$  is odd. Since  $\mu_1 = \sqrt{2}$ , we have  $1 \leq \mu_n \leq \sqrt{2}$ . It is known that equality holds in the upper bound for  $n = 3$  (trivial), for  $n = 5$  [1], and for  $n = 7$  [13], [7]. It was suggested in [6] that  $\mu_n = \sqrt{2}$  for all odd  $n$ , which was disproved by Patterson and Wiedemann [14], by showing that

$$(1) \quad \mu_n \leq \sqrt{729/512} = 1.19\dots \quad \text{for each } n \geq 15.$$

More recently it was shown by Kavut and Yücel [8] that

$$\mu_n \leq \sqrt{49/32} = 1.23\dots \quad \text{for each } n \geq 9.$$

Patterson and Wiedemann [14] also conjectured that  $\lim_{n \rightarrow \infty} \mu_n = 1$ . However no improvement of (1) for large  $n$  has been found since this conjecture has been posed in 1983. We shall prove that this conjecture is true.

**Theorem 1.** *We have  $\lim_{n \rightarrow \infty} \mu_n = 1$ .*

Several researchers (for example in [16], [5], [11]) also investigated

$$\rho'_n = \max_F \min_G d(F, G),$$

where now the maximum is over all *balanced* functions  $F$  from  $\mathbb{F}_2^n$  to  $\mathbb{F}_2$  (which means that  $F$  takes the values 0 and 1 equally often) and the minimum is still over all affine functions  $G$  from  $\mathbb{F}_2^n$  to  $\mathbb{F}_2$ . Put

$$\mu'_n = 2^{n/2} - \rho'_n/2^{n/2-1}.$$

Slight modifications of our proof of Theorem 1 lead to the following result, which proves a conjecture due to Dobbertin [5, Conjecture B] from 1995.

**Theorem 2.** *We have  $\lim_{n \rightarrow \infty} \mu'_n = 1$ .*

## 2. PROOF OF MAIN RESULT

In what follows, we identify  $\mathbb{F}_2^n$  with  $\mathbb{F}_{2^n}$  and consider functions  $f : \mathbb{F}_{2^n} \rightarrow \mathbb{C}$ . Let  $\psi : \mathbb{F}_{2^n} \rightarrow \mathbb{C}$  be the canonical additive character of  $\mathbb{F}_{2^n}$ , which is given by  $\psi(y) = (-1)^{\text{Tr}(y)}$ , where  $\text{Tr}$  is the absolute trace function on  $\mathbb{F}_{2^n}$ . The *Fourier transform* of  $f$  is the function  $\hat{f} : \mathbb{F}_{2^n} \rightarrow \mathbb{C}$  given by

$$\hat{f}(a) = \frac{1}{2^{n/2}} \sum_{y \in \mathbb{F}_{2^n}} f(y) \psi(ay).$$

It is well known [3] and readily verified that

$$\mu_n = \min_f \max_{a \in \mathbb{F}_{2^n}} |\hat{f}(a)|,$$

where the minimum is over all functions  $f : \mathbb{F}_{2^n} \rightarrow \{-1, 1\}$ . From Parseval's identity

$$\sum_{a \in \mathbb{F}_{2^n}} |\hat{f}(a)|^2 = \sum_{y \in \mathbb{F}_{2^n}} |f(y)|^2$$

it follows now that  $\mu_n \geq 1$ .

We shall construct functions  $f$  with image  $\{-1, 1\}$  for which  $|\hat{f}(a)|$  is small for all  $a \in \mathbb{F}_{2^n}$ . Let  $H$  be a (multiplicative) subgroup of  $\mathbb{F}_{2^n}^*$  of index  $v$  and define the indicator function of  $H$  on  $\mathbb{F}_{2^n}$  by

$$\mathbb{1}_H(y) = \begin{cases} 1 & \text{for } y \in H \\ 0 & \text{otherwise.} \end{cases}$$

Let  $h : H \rightarrow \{-1, 1\}$  be a function to be specified later. Let  $T$  be a complete system of coset representatives of  $H$  in  $\mathbb{F}_{2^n}^*$  and let  $g : T \rightarrow \{0, -1, 1\}$  be a function satisfying  $g(z) = 0$  if and only if  $z \in H$  and such that  $g$  is balanced, which means that the images  $-1$  and  $1$  occur equally often. We define  $f : \mathbb{F}_{2^n} \rightarrow \{-1, 1\}$  by  $f(0) = 1$  and

$$f(y) = \mathbb{1}_H(y) h(y) + \sum_{z \in T} \mathbb{1}_H(y/z) g(z) \quad \text{for } y \in \mathbb{F}_{2^n}^*.$$

Note that  $f$  is constant on the cosets of  $H$ , except for  $H$  itself. Such functions were also used by Patterson and Wiedemann [14] in their proof of (1) and have been also studied in several other papers, for example in [2].

Recall that  $\text{ord}_v(a)$  for integers  $v$  and  $a$  with  $v > 0$  and  $\gcd(a, v) = 1$  is the smallest positive integer  $t$  such that  $v \mid a^t - 1$ . Note that for every multiple  $n$  of  $\text{ord}_v(2)$ , there exists a subgroup of  $\mathbb{F}_{2^n}^*$  of index  $v$ .

**Proposition 3.** *Let  $e$  be a positive integer and let  $v = 7^e$ . Then there exists an odd multiple  $n$  of  $\text{ord}_v(2)$  and a function  $h : H \rightarrow \{-1, 1\}$  such that the function  $f : \mathbb{F}_{2^n} \rightarrow \{-1, 1\}$ , defined above, satisfies*

$$\max_{a \in \mathbb{F}_{2^n}} |\hat{f}(a)| \leq 1 + 12 \sqrt{\frac{\log(2v)}{v}}.$$

Since  $\text{ord}_7(2) = 3$  and  $2$  is a square modulo  $7^e$ , Euler's theorem can be used to show that  $\text{ord}_{7^e}(2)$  equals  $\phi(7^d)/2 = 3 \cdot 7^{d-1}$  for some positive integer  $d$  (where  $\phi$  is the Euler totient function). Indeed, using  $\text{ord}_{7^2}(2) = 21$ , a routine induction involving the binomial theorem shows that  $\text{ord}_{7^e}(2)$  equals  $\phi(7^e)/2$ .

Therefore  $\text{ord}_{7^e}(2)$  is odd for all positive integers  $e$ . Now let  $e$  tend to infinity in Proposition 3 and use  $\mu_n = 1$  for all even  $n$  and the inequality  $1 \leq \mu_{n+2} \leq \mu_n$  for all  $n$  to deduce Theorem 1 from Proposition 3.

**Remark.** Proposition 3 remains true if  $7$  is replaced by an arbitrary prime  $q$  satisfying  $q \equiv 3 \pmod{4}$  and  $\text{ord}_{q^e}(2) = \phi(q^e)/2$  for each  $e \in \{1, 2\}$  (as for  $q = 7$ , this ensures that this identity holds for all positive integers  $e$ ). The first primes of this form are  $7, 23, 47, 71, 79$ , but it is not known whether there are infinitely many such primes. We choose  $q = 7$  to keep our proof simple.

To prove Proposition 3, we define functions  $f_1, f_2 : \mathbb{F}_{2^n} \rightarrow \{0, -1, 1\}$  by

$$\begin{aligned} f_1(y) &= \mathbb{1}_H(y) h(y), \\ f_2(y) &= \sum_{z \in T} \mathbb{1}_H(y/z) g(z), \end{aligned}$$

so that  $f(y) = f_1(y) + f_2(y)$  for all  $y \in \mathbb{F}_{2^n}^*$  and  $\hat{f}(a) = 2^{-n/2} + \hat{f}_1(a) + \hat{f}_2(a)$  for all  $a \in \mathbb{F}_{2^n}$ . We shall see that bounding  $|\hat{f}_1(a)|$  is not difficult using known results from probabilistic combinatorics. Bounding  $|\hat{f}_2(a)|$  requires a little more work.

For a multiplicative character  $\chi$  of  $\mathbb{F}_{2^n}$ , the *Gauss sum*  $G(\chi)$  is defined to be

$$G(\chi) = \sum_{y \in \mathbb{F}_{2^n}^*} \psi(y) \chi(y).$$

It is well known that  $|G(\chi)| = 2^{n/2}$  if  $\chi$  is nontrivial (which means that  $\chi(y) \neq 1$  for some  $y \in \mathbb{F}_{2^n}^*$ ) [10, Theorem 5.11].

We begin with the following elementary lemma.

**Lemma 4.** *Let  $\epsilon > 0$  and suppose that, for all nontrivial multiplicative characters  $\chi$  of  $\mathbb{F}_{2^n}$  of order dividing  $v$ , we have*

$$\left| \frac{G(\chi)}{2^{n/2}} - 1 \right| \leq \epsilon.$$

Then we have

$$\max_{a \in \mathbb{F}_{2^n}} |\hat{f}_2(a)| \leq 1 + \epsilon v.$$

*Proof.* Since  $g$  is balanced, we have  $\hat{f}_2(0) = 0$ , so let  $a \in \mathbb{F}_{2^n}^*$ . Let  $\chi$  be a multiplicative character of  $\mathbb{F}_{2^n}$  of order  $v$ . Then the indicator function  $\mathbb{1}_H$  satisfies

$$(2) \quad \mathbb{1}_H(y) = \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(y) \quad \text{for each } y \in \mathbb{F}_{2^n}^*.$$

Therefore we have

$$\begin{aligned} \sum_{y \in \mathbb{F}_{2^n}^*} \mathbb{1}_H(y) \psi(ay) &= \frac{1}{v} \sum_{j=0}^{v-1} \sum_{y \in \mathbb{F}_{2^n}^*} \psi(ay) \chi^j(y) \\ &= \frac{1}{v} \sum_{j=0}^{v-1} \chi^j(a^{-1}) \sum_{y \in \mathbb{F}_{2^n}^*} \psi(y) \chi^j(y) \\ &= \frac{1}{v} \sum_{j=0}^{v-1} \bar{\chi}^j(a) G(\chi^j), \end{aligned}$$

which we use to obtain

$$\begin{aligned}
2^{n/2} \hat{f}_2(a) &= \sum_{y \in \mathbb{F}_{2^n}} \sum_{z \in T} \mathbb{1}_H(y/z) g(z) \psi(ay) \\
&= \sum_{z \in T} g(z) \sum_{y \in \mathbb{F}_{2^n}} \mathbb{1}_H(y) \psi(ayz) \\
&= \frac{1}{v} \sum_{z \in T} g(z) \sum_{j=0}^{v-1} \bar{\chi}^j(az) G(\chi^j) \\
&= \frac{1}{v} \sum_{j=0}^{v-1} G(\chi^j) \bar{\chi}^j(a) \sum_{z \in T} g(z) \bar{\chi}^j(z).
\end{aligned}$$

Now write  $G(\chi^j) = 2^{n/2}(1 + \gamma_j)$ , so that  $|\gamma_j| \leq \epsilon$  for all  $j \in \{1, \dots, v-1\}$  by our assumption. Since  $G(\chi^0) = -1$ , we obtain  $\hat{f}_2(a) = M(a) + E(a)$ , where

$$\begin{aligned}
M(a) &= \frac{1}{v} \sum_{j=1}^{v-1} \bar{\chi}^j(a) \sum_{z \in T} g(z) \bar{\chi}^j(z) - \frac{1}{2^{n/2}v} \sum_{z \in T} g(z) \\
&= \frac{1}{v} \sum_{z \in T} g(z) \sum_{j=1}^{v-1} \bar{\chi}^j(az) \\
&= \frac{1}{v} \sum_{z \in T} g(z) \sum_{j=0}^{v-1} \bar{\chi}^j(az) - \frac{1}{v} \sum_{z \in T} g(z) \\
&= g(b) \quad \text{for } b \in T \text{ such that } ab \in H,
\end{aligned}$$

using that  $g$  is balanced and (2) again, and

$$|E(a)| = \left| \frac{1}{v} \sum_{j=1}^{v-1} \gamma_j \bar{\chi}^j(a) \sum_{z \in T} g(z) \bar{\chi}^j(z) \right| \leq \epsilon v.$$

This gives the required result.  $\square$

The following explicit evaluation of certain Gauss sums [9, Proposition 4.2] (see also [20, Theorem 4.1]) will help us to control the error term in Lemma 4.

**Lemma 5** ([9, Proposition 4.2]). *Let  $q > 3$  be a prime satisfying  $q \equiv 3 \pmod{4}$ . Let  $d$  be a positive integer, write  $k = \phi(q^d)/2$ , and let  $p$  be a prime such that  $\text{ord}_{q^d}(p) = k$ . Let  $\tau$  be a multiplicative character of  $\mathbb{F}_{p^k}$  of order  $q^d$  and let  $h$  be the class number of  $\mathbb{Q}(\sqrt{-q})$ . Then*

$$G(\tau) = \frac{1}{2} (a + b\sqrt{-q}) p^{(k-h)/2},$$

where  $a$  and  $b$  are integers satisfying  $a, b \not\equiv 0 \pmod{p}$ ,  $a^2 + b^2q = 4p^h$ , and  $ap^{(k-h)/2} \equiv -2 \pmod{q}$ .

We shall apply Lemma 5 with  $p = 2$  and  $q = 7$ . Since the class number of  $\mathbb{Q}(\sqrt{-7})$  equals 1 and

$$2^{(\phi(7^d)/2-1)/2} \equiv 2 \pmod{7}$$

for all positive integers  $d$ , we find that  $a = -1$  and  $b^2 = 1$  in this case. As noted after Proposition 3, we have  $\text{ord}_{7^d}(2) = \phi(7^d)/2$  for all positive integers  $d$ , so that the hypothesis in Lemma 5 is satisfied for  $p = 2$  and  $q = 7$ .

As a corollary to Lemma 5, we obtain the following lemma.

**Lemma 6.** *Let  $e$  and  $d$  be integers satisfying  $1 \leq d \leq e$  and write  $m = \text{ord}_{7^e}(2)$ . Let  $\chi$  be a multiplicative character of  $\mathbb{F}_{2^{sm}}$  of order  $7^d$ . Then*

$$\frac{G(\chi)}{2^{sm/2}} = -(-1)^s \left( \frac{-1 \pm \sqrt{-7}}{2^{3/2}} \right)^{7^{e-d}s},$$

where the sign depends on  $\chi$ .

*Proof.* Write  $k = \text{ord}_{7^d}(2)$  and let  $\tau$  be the multiplicative character of  $\mathbb{F}_{2^k}$  such that  $\chi$  is the lifted character of  $\tau$ , by which we mean that  $\chi = \tau \circ N$ , where  $N$  is the field norm from  $\mathbb{F}_{2^{sm}}$  to  $\mathbb{F}_{2^k}$ . Lemma 5 and the preceding discussion implies that

$$G(\tau) = 2^{(k-3)/2}(-1 \pm \sqrt{-7}).$$

From the Davenport-Hasse theorem [10, Theorem 5.14] we find that

$$G(\chi) = -(-1)^{sm/k} \left[ 2^{(k-3)/2}(-1 \pm \sqrt{-7}) \right]^{sm/k},$$

and the lemma follows since  $m/k = \phi(7^e)/\phi(7^d) = 7^{e-d}$ .  $\square$

The next lemma gives the desired control for the error term in Lemma 4.

**Lemma 7.** *Let  $e$  be a positive integer, let  $v = 7^e$ , and write  $m = \text{ord}_v(2)$ . Let  $\epsilon > 0$ . Then there is an infinite set  $S$  of odd positive integers such that, for all  $s \in S$  and all nontrivial multiplicative characters  $\chi$  of  $\mathbb{F}_{2^{sm}}$  of order dividing  $v$ , we have*

$$|\arg G(\chi)| \leq \epsilon.$$

Here,  $\arg(\xi) \in (-\pi, \pi]$  is the principal angle of a nonzero complex number  $\xi$ .

*Proof.* Let  $\tau$  be a multiplicative character of  $\mathbb{F}_{2^m}$  of order  $v$ . Since the units of the ring of algebraic integers in  $\mathbb{Q}(\sqrt{-7})$  are  $\pm 1$ , we find from Lemma 6 that  $G(\tau)/2^{m/2}$  is not a root of unity. Therefore Weyl's uniform distribution theorem [19, Satz 2] implies that  $([G(\tau)/2^{m/2}]^{2i})_{i \in \mathbb{N}}$ , and therefore also  $([G(\tau)/2^{m/2}]^{2i+1})_{i \in \mathbb{N}}$ , is uniformly distributed on the complex unit circle. Hence there is an infinite set  $S$  of odd positive integers such that

$$|\arg(G(\tau)^s)| \leq \frac{\epsilon}{7^{e-1}}$$

for all  $s \in S$ .

Let  $s \in S$  and let  $\tau'$  be the lifted character of  $\tau$  to  $\mathbb{F}_{2^{sm}}$ , namely  $\tau' = \tau \circ N$ , where  $N$  is the field norm from  $\mathbb{F}_{2^{sm}}$  to  $\mathbb{F}_{2^m}$ . Then  $\tau'$  has order  $v = 7^e$  and

the Davenport-Hasse theorem [10, Theorem 5.14] states  $G(\tau') = G(\tau)^s$ , so that

$$|\arg G(\tau')| \leq \frac{\epsilon}{7^{e-1}}.$$

Now let  $\chi$  be a multiplicative character of  $\mathbb{F}_{2^{sm}}$  of order  $7^d$ , where  $1 \leq d \leq e$ . Then by Lemma 6 we have

$$|\arg G(\chi)| \leq 7^{e-d} |\arg G(\tau')|,$$

which completes the proof.  $\square$

We need one more classical result from probabilistic combinatorics due to Spencer [18].

**Lemma 8** ([18, Theorem 7]). *Let  $A$  be a matrix of size  $M \times N$  satisfying  $M \geq N$  with real-valued entries of absolute value at most 1. Then, for all sufficiently large  $N$ , there exists  $u \in \{-1, 1\}^N$  such that*

$$\|Au\| \leq 11\sqrt{N \log(2M/N)},$$

where  $\|\cdot\|$  is the maximum norm on  $\mathbb{R}^M$ .

We now prove Proposition 3.

*Proof of Proposition 3.* Write  $m = \text{ord}_v(2)$ . Lemma 7 implies that, for all  $\epsilon > 0$ , there is an infinite set  $S$  of odd positive integers such that

$$\left| \frac{G(\chi)}{2^{sm/2}} - 1 \right| \leq \epsilon$$

for all  $s \in S$  and all nontrivial multiplicative characters  $\chi$  of  $\mathbb{F}_{2^{sm}}$  of order dividing  $v$ . Writing  $n = sm$  and taking  $\epsilon = \frac{1}{2}\sqrt{\log(2v)/v^3}$ , Lemma 4 then implies that

$$\max_{a \in \mathbb{F}_{2^n}} |\hat{f}_2(a)| \leq 1 + \frac{1}{2}\sqrt{\frac{\log(2v)}{v}}$$

for infinitely many odd positive integers  $n$ .

It remains to consider  $\hat{f}_1$ . Since

$$\hat{f}_1(a) = \frac{1}{2^{n/2}} \sum_{y \in H} h(y)\psi(ay),$$

we find from Lemma 8 with  $M = 2^n$  and  $N = (2^n - 1)/v$  that, for all sufficiently large  $n$ , there exists  $h : H \rightarrow \{-1, 1\}$  such that

$$\max_{a \in \mathbb{F}_{2^n}} |\hat{f}_1(a)| \leq 11\sqrt{\frac{\log(2v)}{v}}.$$

Since  $\hat{f}(a) = 2^{-n/2} + \hat{f}_1(a) + \hat{f}_2(a)$  for all  $a \in \mathbb{F}_{2^n}$ , there is an odd integer  $n$  that is a multiple of  $m = \text{ord}_v(2)$  such that

$$\max_{a \in \mathbb{F}_{2^n}} |\hat{f}(a)| \leq 1 + 12\sqrt{\frac{\log(2v)}{v}},$$

as required.  $\square$

We now comment on the required modifications of our proof to prove Theorem 2. The function  $h$  identified in the proof of Proposition 3 satisfies

$$\left| \sum_{y \in H} h(y) \right| \leq 11 \sqrt{2^n \frac{\log(2v)}{v}}.$$

Therefore we have to change at most  $6\sqrt{2^n \log(2v)/v}$  values of the function  $h$  to get

$$\sum_{y \in H} h(y) = -1.$$

This increases  $|\hat{f}_1(a)|$  by at most  $12\sqrt{\log(2v)/v}$ . The resulting function  $f$  is balanced and satisfies

$$\max_{a \in \mathbb{F}_{2^n}} |\hat{f}(a)| \leq 1 + 24\sqrt{\frac{\log(2v)}{v}}.$$

Using  $1 \leq \mu'_{n+2} \leq \mu'_n$ , this shows that  $\lim_{i \rightarrow \infty} \mu'_{2i+1} = 1$ . We combine this with  $\lim_{i \rightarrow \infty} \mu'_{2i} = 1$ , which was already shown in [5], but also follows from our argument using further slight modifications, to obtain a proof of Theorem 2.

#### ACKNOWLEDGEMENTS

I would like to thank James A. Davis for many valuable discussions in the early stage of this research.

#### REFERENCES

- [1] 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.
- [2] J. Bringer, V. Gillot, and P. Langevin. Exponential sums and Boolean functions. In *Proceedings of Boolean Functions: Cryptography and Applications*, pages 177–185, Rouen, 2005.
- [3] C. Carlet. Boolean functions for cryptography and error-correcting codes. In Y. Crama and P. L. Hammer, editors, *Boolean models and methods in mathematics, computer science, and engineering*, pages 257–397. 2010.
- [4] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein. *Covering codes*, volume 54 of *North-Holland Mathematical Library*. North-Holland Publishing Co., Amsterdam, 1997.
- [5] H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. In B. Preneel, editor, *Fast Software Encryption: Second International Workshop Leuven, Belgium, December 14–16, 1994 Proceedings*, pages 61–74. Springer Berlin Heidelberg, 1995.
- [6] T. Helleseeth, T. Kløve, and J. Mykkeltveit. On the covering radius of binary codes. *IEEE Trans. Inform. Theory*, 24(5):627–628, 1978.
- [7] 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.
- [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. Langevin. Calculs de certaines sommes de Gauss. *J. Number Theory*, 63(1):59–64, 1997.



- [10] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2nd edition, 1997.
- [11] S. Maitra and P. Sarkar. Modifications of Patterson-Wiedemann functions for cryptographic applications. *IEEE Trans. Inform. Theory*, 48(1):278–284, 2002.
- [12] S. Mesnager. *Bent functions: Fundamentals and results*. Springer, 2016.
- [13] J. J. Mykkeltveit. The covering radius of the (128, 8) Reed-Muller code is 56. *IEEE Trans. Inform. Theory*, 26(3):359–362, 1980.
- [14] 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.
- [15] O. S. Rothaus. On “bent” functions. *J. Combin. Theory Ser. A*, 20(3), 1976.
- [16] J. Seberry, Z. M. Zhang, and Y. Zheng. Nonlinearity and propagation characteristics of balanced Boolean functions. *Inform. and Comput.*, 119(1):1–13, 1995.
- [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.
- [19] H. Weyl. Über die Gleichverteilung von Zahlen mod. Eins. *Math. Ann.*, 77(3):313–352, 1916.
- [20] J. Yang and L. Xia. Complete solving of explicit evaluation of Gauss sums in the index 2 case. *Sci. China Math.*, 53(9):2525–2542, 2010.

DEPARTMENT OF MATHEMATICS, PADERBORN UNIVERSITY, WARBURGER STR. 100,  
33098 PADERBORN, GERMANY.

*E-mail address*, K.-U. Schmidt: kus@math.upb.de