Cryptogr. Commun. (2011) 3:165–174
DOI 10.1007/s12095-011-0043-5

Boolean functions derived from Fermat quotients

Hassan Aly · Arne Winterhof

Received: 17 November 2010 / Accepted: 1 February 2011 / Published online: 23 February 2011

Abstract We study Boolean functions derived from Fermat quotients modulo p using the Legendre symbol. We prove bounds on several complexity measures for these Boolean functions: the nonlinearity, sparsity, average sensitivity, and combinatorial complexity. Our main tools are bounds on character sums of Fermat quotients modulo p.

Keywords Fermat quotients · Boolean functions · Nonlinearity · Sparsity · Average sensitivity · Combinatorial complexity · Cryptography · Legendre symbol

1 Introduction

For a prime p and an integer u with $\gcd(u, p) = 1$ the *Fermat quotient* $q_p(u)$ modulo p is defined as the unique integer that satisfies

$$q_p(u) \equiv \frac{u^{p-1} - 1}{p} \pmod{p}, \quad 0 \le q_p(u) \le p - 1,$$

and we put

$$q_p(kp) = 0, \quad k \in \mathbb{Z}.$$

H. Aly
Department of Mathematics, Faculty of Science, Cairo University,
P.O. Box 12613, Giza, Egypt
e-mail: hassan@sci.cu.edu.eg

A. Winterhof (✉)
Johann Radon Institute for Computational and Applied Mathematics,
Austrian Academy of Sciences, Altenberger Straße 69, 4040 Linz, Austria
e-mail: arne.winterhof@oeaw.ac.at

We note that $q_p(u)$ is p^2-periodic. There are several results which involve the distribution and structure of Fermat quotients $q_p(u)$ modulo p with numerous applications in computational and algebraic number theory, see e.g. [4–8, 11, 14, 15] and references therein. Some characteristics of Fermat quotients which are relevant to their use as pseudorandom number generators for quasi-Monte Carlo methods or cryptography are studied in [4, 6, 11].

In this paper we study Boolean functions derived from Fermat quotients modulo p using the Legendre symbol. For a recent survey on Boolean functions we refer to [2, 3]. For a prime $p > 2$ we define the Boolean function $B(U_1, U_2, \cdots, U_r)$ of $r = \lfloor 2 \log p \rfloor$ variables by

$$B(u_1, \cdots, u_r) = \begin{cases} 0, \text{ if } \left(\dfrac{q_p(x)}{p}\right) = 1, \\ 1, \text{ if } \left(\dfrac{q_p(x)}{p}\right) \neq 1, \end{cases} \tag{1}$$

for any $0 \le x \le 2^r - 1$ where $(u_1, u_2, \cdots, u_r)$ is the binary representation of x, $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol and log is the binary logarithm.

We prove bounds on several complexity measures for $B(U_1, \ldots, U_r)$. (Note that we use capital letters for variables and small letters for integers and their bit representations.)

Let $\mathscr{B}_r = \{0, 1\}^r$. The *Hamming weight* $\|a\|$ of a vector $a \in \mathscr{B}_r$ is the number of its nonzero components. The *Fourier coefficients* (or *Walsh-Hadamard coefficients*) $\widehat{B}(a)$ of $B(U_1, \ldots, U_r)$, where $a \in \mathscr{B}_r$, are defined as

$$\widehat{B}(a) = \sum_{u \in \mathscr{B}_r} (-1)^{B(u) + <a,u>}$$

where $< a, u >= a_1u_1 + a_2u_2 + \cdots + a_ru_r$ denotes the standard inner product. The *nonlinearity* of the Boolean function $B(U_1, \ldots, U_r)$ is defined by

$$N(B) = 2^{r-1} - \frac{1}{2} \max_{a \in \mathscr{B}_r} \left|\widehat{B}(a)\right|.$$

Boolean functions used in cryptography must have high nonlinearity. In Section 2 we show that the Boolean function $B(U_1, \ldots, U_r)$ as defined in (1) yields

$$\max_{a \in \mathscr{B}_r} \left|\widehat{B}(a)\right| \ll p^{15/8} \log^{1/4} p,$$

where $A \ll B$ is equivalent to $|A| \le cB$ for some constant c. (Note that $p^2/4 < 2^{r-1} < p^2/2$.) The proof is based on a recent character sum bound obtained in [6]. Although there are Boolean functions which attain the best possible value

$$\max_{a \in \mathscr{B}_r} \left|\widehat{B}(a)\right| = 2^{r/2-1}$$

(so called *bent functions*, see for example [2, 3]) and asymptotically almost all Boolean functions satisfy

$$\max_{a \in \mathscr{B}_r} \left|\widehat{B}(a)\right| \ll 2^{r/2} \log r,$$

see [12], it is hard to prove nontrivial bounds $o(2^r)$ in general, in particular, if the Boolean function guarantuees some other nice features.

The *sparsity spr* B, or *weight*, of $B(U_1, \dots, U_r)$ is the number of its nonzero coefficients. In Section 3 we show that

$$spr\ B \gg p^{1/4} \log^{-1/2} p.$$

The *average sensitivity* $\sigma_{av}(B)$ of the Boolean function $B(U_1, \dots, U_r)$ is a measure on how the value of $B(U_1, \dots, U_r)$ changes on average if the ith bit of the argument is flipped, i.e.

$$\sigma_{av}(B) = 2^{-r} \sum_{a \in \mathscr{B}_r} \sum_{i=1}^{r} \left| B(a) - B(a^{(i)}) \right|,$$

where $x^{(i)}$ is the vector obtained from x by flipping its ith coordinate. In Section 4 we show that

$$\sigma_{av}(B) \geq 0.5r + o(r).$$

A Boolean function $B(U_1, \cdots, U_r)$ of r variables is said to belong to the class $\mathscr{P}^r_{k,s}$ if for any choice of k integers $1 \leq i_1 < i_2 < \cdots < i_k \leq r$ there are at least s distinct functions obtainable by making all 2^k possible assignments to $U_{i_1}, \cdots, U_{i_k}$. Thus, it is a measure on how many of the variables are independent in some sense. In Section 5 we show that

$$B \in \mathscr{P}^r_{k,2^k}$$

for any $k \leq \frac{1}{3} \log p + O(1)$.

Similar results on the rightmost bit of the discrete logarithm in a finite field can be found in [13, Chapter 1] and [1, 9, 10].

We will need the following well-known property of Fermat quotients. For any integers k, u and v with $\gcd(uv, p) = 1$ we have

$$q_p(u + kp) \equiv q_p(u) - ku^{-1} \pmod{p}, \tag{2}$$

see for example [5, Equation (2)]. Since every integer x such that $0 \leq x \leq p^2 - 1$ can be written uniquely as $x = u + vp$ where $0 \leq u, v \leq p - 1$ and using (2) for $u \neq 0$, the equation

$$q_p(x) = q_p(u + vp) = 0$$

has $O(p)$ solutions.

We also recall a simple consequence of [6, Theorem 1] for the convenience of the reader. We have

$$\sum_{u=0}^{N-1} \left(\frac{q_p(u + d_1) \cdots q_p(u + d_\ell)}{p} \right) \ll \max\{\ell N p^{-1/3}, \ell p^{3/2} \log p\}$$

for any $0 \leq d_1 < \ldots < d_\ell \leq p^2 - 1$ and $1 \leq N \leq p^2$.

2 A bound for the maximum Fourier coefficients

This section gives an upper bound for $\max_{a\in\mathscr{B}_r}\left|\widehat{B}(a)\right|$.

Theorem 1 *Let $B(U_1,\ldots,U_r)$ be defined as in (1). Then the bound*

$$\max_{a\in\mathscr{B}_r}\left|\widehat{B}(a)\right| \ll p^{15/8}\log^{1/4} p$$

holds.

Proof First note that for $0\le x\le 2^r-1$ we have

$$\left(\frac{q_p(x)}{p}\right)=\begin{cases}(-1)^{B(u_1,\cdots,u_r)}, & \text{if } q_p(x)\not\equiv 0 \bmod p,\\ 0, & \text{if } q_p(x)\equiv 0 \bmod p,\end{cases}$$

where $(u_1,\cdots,u_r)$ is the binary representation of x. Then for $a=(a_1,\cdots,a_r)\in\mathscr{B}_r$ we have

$$\widehat{B}(a)=S(a)+O(p)$$

where

$$S(a)=\sum_{x=0}^{2^r-1}\left(\frac{q_p(x)}{p}\right)(-1)^{<x,a>}$$

and $<x,a>=u_1a_1+\cdots+u_ra_r$. Put $k=\left\lceil\log\left(p^{7/4}\log^{1/2}p\right)\right\rceil$, $N=2^k$, and $M=2^{r-k}$. Then we obtain

$$S(a)=\sum_{y=0}^{N-1}\sum_{z=0}^{M-1}\left(\frac{q_p(y+Nz)}{p}\right)(-1)^{<y,b>+<z,c>}$$

where $b=(a_1,a_2,\cdots,a_k)$ and $c=(a_{k+1},a_{k+2},\cdots,a_r)$. Therefore,

$$|S(a)|\le\sum_{y=0}^{N-1}\left|\sum_{z=0}^{M-1}\left(\frac{q_p(y+Nz)}{p}\right)(-1)^{<z,c>}\right|$$

and the Cauchy–Schwarz inequality implies

$$\begin{aligned}|S(a)|^2 &\le N\sum_{y=0}^{N-1}\left|\sum_{z=0}^{M-1}\left(\frac{q_p(y+Nz)}{p}\right)(-1)^{<z,c>}\right|^2\\ &= N\sum_{y=0}^{N-1}\sum_{z_1,z_2=0}^{M-1}\left(\frac{q_p(y+Nz_1)q_p(y+Nz_2)}{p}\right)(-1)^{<z_1,c>+<z_2,c>}\\ &\le N\sum_{z_1,z_2=0}^{M-1}|W(z_1,z_2)|,\end{aligned}$$

where

$$W(z_1, z_2) = \sum_{y=0}^{N-1} \left(\frac{q_p(y + Nz_1) q_p(y + Nz_2)}{p} \right).$$

For M pairs (z_1, z_2) with $z_1 = z_2$ we use the trivial bound $|W(z_1, z_2)| \le N$. For $M(M-1)$ pairs (z_1, z_2) with $z_1 \ne z_2$ we apply [6, Theorem 14] to obtain

$$|W(z_1, z_2)| \ll Np^{-1/3} + p^{3/2} \log p \ll p^{3/2} \log p$$

because of the choice of k. (The main ideas of the proof of [6, Theorem 1] will be recalled in the proof of Theorem 4 below.) Therefore,

$$\begin{aligned} |S(a)|^2 &\ll N \left(MN + M(M-1) p^{3/2} \log p \right) \\ &\ll N \left(p^2 + \frac{p^4 p^{3/2} \log p}{N^2} \right) \ll p^{15/4} \log^{1/2} p \end{aligned}$$

because of the choice of k again. □

3 A bound on the sparsity

The number of non-zero terms in any Boolean function $B(U_1, \ldots, U_r)$ is denoted by *spr* B.

Theorem 2 *Let $B(U_1, \ldots, U_r)$ be defined as in (1). Then the bound*

$$spr\ B \gg p^{1/4} \log^{-1/2} p$$

holds.

Proof Put $t = spr\ B$ and define k by the inequalities

$$2^k > t + 1 \ge 2^{k-1}.$$

For each $m = 1, 2, \cdots, 2^k - 1$ we consider the function

$$B_m(V_1, \cdots, V_{r-k}) = B(V_1, \cdots, V_{r-k}, e_1, \cdots, e_k),$$

where $m = (e_1, \cdots, e_k)$ is the bit representation of m. The total number of distinct monomials in $V_1, \cdots, V_{r-k}$ occurring in all these functions does not exceed t. Therefore, one can find a non-trivial linear combination

$$\sum_{m=1}^{2^k-1} c_m B_m(V_1, \cdots, V_{r-k}), \quad c_1, \cdots, c_{2^k-1} \in \mathbb{F}_2,$$

which vanishes identically. From the definition of $B(U_1, \ldots, U_r)$ we see that

$$\left(\frac{q_p(x)}{p} \right) = \begin{cases} (-1)^{B(u_1, \cdots, u_r)}, & \text{if } q_p(x) \not\equiv 0 \bmod p, \\ 0, & \text{if } q_p(x) \equiv 0 \bmod p, \end{cases}$$

where $(u_1, \cdots, u_r)$ is the bit representation of x. Therefore, we have

$$\prod_{m=1}^{2^k-1} \left(\frac{q_p(2^k y + m)}{p} \right)^{c_m} = (-1)^{\sum_{m=1}^{2^k-1} c_m B_m(v_1, \cdots, v_{r-k})} = 1,$$

for all $0 \le y \le 2^{r-k} - 1$ with $q_p(2^k y + m) \neq 0$ for all $m = 1, \ldots, 2^k - 1$, where $(v_1, \cdots, v_{r-k})$ is the bit representation of y. There are $O(2^k p)$ values of y with $q_p(2^k y + m) = 0$ for some m. Combining this result with [6, Theorem 1] we obtain

$$\begin{aligned} p^2 2^{-k} \ll 2^{r-k} &\ll \sum_{y=0}^{2^{r-k}-1} \prod_{m=1}^{2^k-1} \left(\frac{q_p(2^k y + m)}{p} \right)^{c_m} + 2^k p \\ &\ll 2^k \max\left\{ 2^{r-k} p^{-1/3}, p^{3/2} \log p \right\} \ll \max\left\{ p^{5/3}, 2^k p^{3/2} \log p \right\}. \end{aligned}$$

If the maximum on the right hand side is $p^{5/3}$ we get $t + 1 \ge 2^{k-1} \gg p^{1/3}$ and $(t+1)^2 \ge 2^{2k-2} \gg p^{1/2}/\log p$ otherwise, and the result follows. □

4 A bound on the average sensitivity

Theorem 3 *Let $B(U_1, \ldots, U_r)$ be defined as in (1). Then the bound*

$$\sigma_{av}(B) \ge 0.5r + o(r)$$

holds.

Proof Put $m = \lfloor r^{1/2} \rfloor$, $k = 2m + 1$, $l = \lfloor r - r^{1/2} \rfloor$, and $R = 2^r - k2^l$. For $0 \le i \le l$ and $0 \le x \le R - 1$ the vector $\left(B(x + j2^i)\right)_{j=1}^{k}$ is defined. Over the range of x, the vector takes on the value of each possible binary k-tuple $T = (t_1, \cdots, t_k)$ with multiplicity

$$N(T) = 2^{-k} \sum_{x=0}^{R-1} \prod_{j=1}^{k} \left(\left(\frac{q_p(x + j2^i)}{p} \right) (-1)^{t_j} + 1 \right) + O(kp/2^k).$$

The term $O(kp)$ estimates the number of values x such that $q_p(x + j2^i) = 0$ for some j. Then we have one main term $R2^{-k}$ and $2^k - 1$ terms of the form

$$\pm 2^{-k} \sum_{x=0}^{R-1} \left(\frac{q_p(x + j_1 2^i) \cdots q_p(x + j_s 2^i)}{p} \right) \ll s p^{5/3}$$

by [6, Theorem 1], where $s \le k$ and $1 \le j_1 \le \cdots \le j_s \le k$. Thus,

$$\begin{aligned} N(T) &= R2^{-k} + O\left(kp^{5/3}\right) \\ &= R2^{-k} + O\left(r^{1/2} 2^{5r/6}\right) \\ &= R2^{-k} + o(R2^{-k}). \end{aligned}$$

It follows from probabilistic arguments that for $2^k + o(2^k)$ binary k-tuples $T = (t_1, \cdots, t_k)$, both of the following statements are true:

1. $t_{2j} \neq t_{2j+1}$ for $\frac{m}{2} + o(m)$ values of $j = 1, 2, \cdots, m$,
2. $t_{2j} \neq t_{2j-1}$ for $\frac{m}{2} + o(m)$ values of $j = 1, 2, \cdots, m$.

So whatever the $(i+1)$th bit of x is, if the vector $\left(B(x+j2^{i+1})\right)_{j=1}^{k}$ is such a k-tuple T, then among the m values $B(x+j2^i)$, $j=1,2,\cdots,m$ about half differ from their respective

$$B\left((x+j2^{i+1})^{(i)}\right)=B(x+j2^{i+1}\pm 2^i)=B\left(x+(2j\pm 1)2^i\right).$$

So we have

$$\sum_{i=0}^{l}\sum_{x=0}^{R-1}\sum_{\substack{j=0\\ B(x+j2^{i+1})\neq B((x+j2^{i+1})^{(i)})}}^{m} 1\geq (l+1)\left(R2^{-k}+o(R2^{-k})\right)\left(2^k+o(2^k)\right)(0.5m+o(m))$$

$$=0.5Rlm+o(Rlm).$$

For every $0\leq i\leq l$ and $1\leq j\leq m$, we find

$$\left|\sum_{\substack{x=0\\ B(x+j2^{i+1})\neq B((x+j2^{i+1})^{(i)})}}^{R-1} 1-\sum_{\substack{x=0\\ B(x)\neq B(x^{(i)})}}^{2^r-1} 1\right|\leq m2^{l+1}=o(2^r).$$

Therefore

$$\sigma_{av}(B)=2^{-r}\sum_{i=0}^{l}\sum_{\substack{x=0\\ B(x)\neq B(x^{(i)})}}^{2^r-1} 1\geq 0.5l+o(l)=0.5r+o(r),$$

and we are done. □

5 A bound on the combinatorial complexity

Theorem 4 *Let $B(U_1,\ldots,U_r)$ be defined as in (1). Then*

$$B\in\mathscr{P}^r_{k,2^k}\quad \textit{for any } k\leq\frac{1}{3}\log p+O(1).$$

Proof Fix k integers $1\leq i_1<\cdots<i_k\leq r$. We consider the set $\mathscr{U}$ of r-bit integers $x=(u_1,\cdots,u_r)$ such that the digits at the positions i_j, $j=1,2,\cdots,k$ are fixed in an arbitrary way. We also put $i_0=0$ and $i_{k+1}=r+1$. Then we have

$$\mathscr{U}=\left\{A+\sum_{j=0}^{k}x_j2^{i_j}\mid\quad 0\leq x_j\leq 2^{i_{j+1}-i_{j-1}-1},\ j=0,1,\cdots,k\right\},$$

where A depends on the fixed digits of x. Put

$$h_j=\lceil 2^{i_{j+1}-i_j-2}\rceil,\quad j=0,1,\cdots,k,$$

and define

$$D=A+\sum_{j=0}^{k}h_j2^{i_j},\quad \mathscr{V}=\left\{\sum_{j=0}^{k}x_j2^{i_j}\mid\quad 0\leq x_j\leq h_j-1,\ j=0,\cdots,k\right\}.$$

We see that $D + v - w \in \mathscr{U}$ for all $u, w \in \mathscr{V}$. Note also that for distinct selections of the digits of x at the positions $i_1, \cdots, i_k$ we get distinct values of D. Now we will show that for any $0 \le D_1 < D_2 < p^2$ we have

$$\left| \sum_{v,w \in \mathscr{V}} \left(\frac{q_p(D_1 + v - w) q_p(D_2 + v - w)}{p} \right) \right| < |\mathscr{V}|^2 - 2(2p - 1).$$

The number $2(2p - 1)$ counts the number of possible zero values for which the function D is defined in an arbitrary way. Put $e_q(z) = \exp(2\pi i z/q)$ for any integers z and $q > 1$. Now we have

$$\begin{aligned}
\delta_{D_1, D_2} &= \left| \sum_{v,w \in \mathscr{V}} \left(\frac{q_p(D_1 + v - w) q_p(D_2 + v - w)}{p} \right) \right| \\
&= \frac{1}{p^2} \left| \sum_{z=0}^{p^2-1} \left(\frac{q_p(D_1 + z) q_p(D_2 + z)}{p} \right) \sum_{c=0}^{p^2-1} \sum_{v,w} e_{p^2}(c(z - v + w)) \right| \\
&\le \frac{1}{p^2} \sum_{c=0}^{p^2-1} \left| \sum_{z=0}^{p^2-1} \left(\frac{q_p(D_1 + z) q_p(D_2 + z)}{p} \right) e_{p^2}(cz) \right| \left| \sum_{v \in \mathscr{V}} e_{p^2}(cv) \right|^2.
\end{aligned}$$

Now put

$$\Delta_c(D_1, D_2) = \left| \sum_{z=0}^{p^2-1} \left(\frac{q_p(D_1 + z) q_p(D_2 + z)}{p} \right) e_{p^2}(cz) \right|.$$

Since every integer z such that $0 \le z \le p^2 - 1$ can be written uniquely as $z = x + py$ where $0 \le x, y \le p - 1$, we have

$$\begin{aligned}
\Delta_c(D_1, D_2) &\le \sum_{x=0}^{p-1} \left| \sum_{y=0}^{p-1} \left(\frac{q_p(D_1 + x + yp) q_p(D_2 + x + yp)}{p} \right) e_{p^2}(c(x + yp)) \right| \\
&= \sum_{\substack{x=0 \\ x \ne p - D_1, p - D_2}}^{p-1} |\sigma(x)| + O(p),
\end{aligned}$$

where

$$\sigma(x) = \sum_{y=0}^{p-1} \left(\frac{(q_p(D_1 + x) - (D_1 + x)^{-1} y)(q_p(D_2 + x) - (D_2 + x)^{-1} y)}{p} \right) e_p(cy).$$

If $c \not\equiv 0 \bmod p$ we can estimate the absolute value of the inner sum $\sigma(x)$ by $p^{1/2}$ using the Weil bound getting

$$\Delta_c(D_1, D_2) \ll p^{3/2}.$$

If $c \equiv 0 \bmod p$ we can apply the Weil bound only if

$$q_p(D_1 + x)(D_1 + x) \not\equiv q_p(D_2 + x)(D_2 + x) \tag{3}$$

and have to use the trivial bound p otherwise. We will show that the number of solutions $0 \le x < p$ of (3) is $O(p^{2/3})$ which implies

$$\Delta_c(D_1, D_2) \ll p^{2/3}p + pp^{1/2} \ll p^{5/3}.$$

If $D_1 \equiv D_2 \bmod p$ but $D_1 \not\equiv D_2 \bmod p^2$, (2) and (3) with $K = (D_2 - D_1)/p$ imply $x + D_1 \equiv 0 \bmod p$. Hence we may assume $D_1 = 0$ and $1 \le D_2 < p$ since the function defined by $f(x) = q_p(x)x - q_p(x + D_2)(x + D_2)$ if $\gcd(x, p) = \gcd(x + D_2, p) = 1$ and $f(x) = 0$ otherwise is p-periodic.

Using

$$q_p(D_1w) \equiv q_p(D_1) + q_p(w) \bmod p, \quad \gcd(D_1w, p) = 1,$$

and substituting $x = D_1(w - 1)$ in (3) we get for $2 \le w < p$

$$0 \equiv q_p(w)D_1w - q_p(w - 1)D_1(w - 1) + q_p(D_1)D_1 \bmod p.$$

This can be transformed to (cf. [6])

$$\sum_{i=1}^{p-1} \frac{w^i}{i} \equiv q_p(D_1) \bmod p.$$

The number of solutions w is $O(p^{2/3})$ by [8, Lemma 4].

Therefore,

$$\delta_{D_1,D_2} \ll \frac{p^{5/3}}{p^2} \sum_{c=0}^{p^2-1} \left| \sum_{v \in \mathscr{V}} e_{p^2}(cv) \right|^2 \ll p^{5/3}|\mathscr{V}|.$$

Taking into account that $|\mathscr{V}| \ge \prod_{j=0}^{k} 2^{i_{j+1}-i_j-2} = 2^{r-2k-2} \ge p^2 2^{-2k-3}$, we obtain

$$p^{5/3}|\mathscr{V}| < |\mathscr{V}|^2 - 2(2p - 1)$$

for any $k \le \frac{1}{3}\log p + O(1)$. □

Acknowledgements The authors wish to thank Igor Shparlinski for pointing to the problem of estimating the nonlinearity of these Boolean functions. This work was written during a visit of the first author to RICAM. He wishes to thank the Austrian Academy of Sciences for hospitality and financial support.

References

1. Brandstätter, N., Lange, T., Winterhof, A.: On the non-linearity and sparsity of Boolean functions related to the discrete logarithm in finite fields of characteristic two. In: Coding and Cryptography. Lect. Notes Comput. Sci., vol. 3969, pp. 135–143. Springer, Berlin (2006)
2. Carlet, C.: Boolean functions for cryptography and error correcting codes. In: Crama, Y., Hammer, P.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge University Press (2010)
3. Carlet, C., Helleseth, T.: Sequences, Boolean functions, and cryptography. In: Boztas, S., et al. (eds.) CRC Handbook of Sequences, Codes and Applications. Chapman and Hall/CRC Press (to appear)
4. Chen, Z., Ostafe, A., Winterhof, A.: Structure of pseudorandom numbers derived from Fermat quotients. In: Hasan, M.A., Helleseth, T. (eds.) WAIFI 2010. Lect. Notes Comput. Sci. vol. 6087, pp. 73–85. Springer, Berlin (2010)

5. Ernvall, R., Metsänkylä, T.: On the p-divisibility of Fermat quotients. Math. Comput. **66**(219), 1353–1365 (1997)
6. Gomez, D., Winterhof, A.: Multiplicative character sums of Fermat quotients and pseudorandomness. Period. Math. Hung. (to appear)
7. Granville, A.: Some conjectures related to Fermat's last theorem. Number Theory, pp. 177–192. W. de Gruyter, NY (1990)
8. Heath-Brown, D.: An estimate for Heilbronn's exponential sum. In: Analytic Number Theory, Proc. Conf. in Honor of Heini Halberstam, pp. 541–463. Birkhäuser, Boston (1996)
9. Lange, T., Winterhof, A.: Interpolation of the discrete logarithm in $\mathbf{F}_q$ by Boolean functions and by polynomials in several variables modulo a divisor of $q-1$. International Workshop on Coding and Cryptography (WCC 2001) (Paris). Discrete Appl. Math. **128**(1), 193–206 (2003)
10. Lange, T., Winterhof, A.: Incomplete character sums over finite fields and their application to the interpolation of the discrete logarithm by Boolean functions. Acta Arith. **101**(3), 223–229 (2002)
11. Ostafe, A., Shparlinski, I.: Pseudorandomness and dynamics of Fermat quotients. SIAM J. Discrete Math. **25**, 50–71 (2011)
12. Rodier, F.: Asymptotic nonlinearity of Boolean functions. Des. Codes Cryptogr. **40**(1), 59–70 (2006)
13. Shparlinski, I.E.: Cryptographic Applications of Analytic Number Theory: Complexity Lower Bounds and Pseudorandomness. Birkhäuser (2003)
14. Shparlinski, I.E.: Character sums of Fermat quotients. Quart. J. Math. (to appear)
15. Shparlinski, I.E.: Bounds of multiplicative character sums with Fermat quotients of primes. Bull. Aust. Math. Soc. (to appear)