ACTA ARITHMETICA
170.2 (2015)

Polynomial quotients: Interpolation, value sets and Waring's problem

by

Zhixiong Chen (Putian) and Arne Winterhof (Linz)

1. Introduction. For an odd prime p and an integer u with $\gcd(u,p)=1$, the *Fermat quotient* $q_p(u)$ is defined as the unique integer

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

and

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

An equivalent definition is

$$q_p(u) \equiv \frac{u^{p-1}-u^{p(p-1)}}{p} \bmod p. \tag{1.1}$$

Many number-theoretic and cryptographic questions as well as measures of pseudorandomness have been studied for Fermat quotients and their generalizations [1–3, 5–7, 9, 11, 13, 15, 17, 20, 21, 24, 28, 30–34].

In particular, for all positive integers w, we extend (1.1) to define

$$q_{p,w}(u) \equiv \frac{u^w-u^{wp}}{p} \bmod p \quad \text{with } 0 \le q_{p,w}(u) \le p-1,\ u \ge 0, \tag{1.2}$$

which is called a *polynomial quotient* in [12]. In fact $q_{p,p-1}(u) = q_p(u)$. We have the following relation between $q_{p,w}(u)$ and $q_p(u)$:

$$q_{p,w}(u) \equiv -u^w w q_p(u) \bmod p \tag{1.3}$$

for all $u \ge 0$ with $\gcd(u,p) = 1$. In particular, we get $q_{p,w}(kp) = 0$ if $w \ge 2$, and $q_{p,w}(kp) = k$ if $w = 1$. We estimated certain character sums of polynomial quotients in [12]. Recently the first author (partly with other coauthors) also applied polynomial quotients to construct pseudorandom sequences with good cryptographic properties [8, 10, 16].

2010 *Mathematics Subject Classification*: Primary 11P05; Secondary 11T06, 11T24.
Key words and phrases: polynomial quotients, Fermat quotients, Waring problem, value set, character sums, Cauchy–Davenport theorem.

DOI: 10.4064/aa170-2-2

In this paper, first we study interpolation polynomials of polynomial quotients (including the number of fixed points of polynomial quotients) and the size of value sets of polynomial quotients defined in (1.2). Then we apply results on the size of value sets to study an analogue of the *Waring problem* for polynomial quotients, that is, the question about the smallest positive integer s, which is called the *Waring number* and denoted by $g(w,N,p)$, such that the equation

$$q_{p,w}(u_1)+\cdots+q_{p,w}(u_s)\equiv c \bmod p,\qquad 0\le u_1,\dots,u_s<N\ (\le p),$$

is solvable for any $c\in\mathbb{F}_p$. If such an s does not exist, or equivalently $q_{p,w}(0)=\cdots=q_{p,w}(N-1)=0$, we set $g(w,N,p)=\infty$. Let ℓ be the smallest value with $q_{p,w}(\ell)\not\equiv 0 \bmod p$. Then the Waring number $g(w,N,p)$ always exists if $N>\ell$. Indeed, it is easy to see that $g(w,N,p)\le p-1$ for $N>\ell$. For $w=p-1$ (and thus for all $w\not\equiv 0 \bmod p$ by (1.3)), ℓ is estimated in [3] by $\ell\le(\log p)^{463/252+o(1)}$ for all p, which has more recently been improved to $(\log p)^{7829/4284+o(1)}$ in [29].

Let us denote by $F(w,N,p;f(x))$ the number of solutions $0\le u<N$ of $q_{p,w}(u)\equiv f(u)$ for $f(x)\in\mathbb{F}_p[x]$:

$$F(w,N,p;f(x))=\#\{u\in\{0,\dots,N-1\}:q_{p,w}(u)\equiv f(u) \bmod p\},\quad N\le p.$$

In particular, $F(w,N,p;x)$ is the number of fixed points of $q_{p,w}$. We prove upper bounds on $F(w,N,p;f(x))$ in Section 2.

Denote by $V(w,N,p)$ the size of the value set of $q_{p,w}(u)$ with $0\le u<N$:

$$V(w,N,p)=\#\{q_{p,w}(u):u=0,\dots,N-1\},\qquad N\le p.$$

If $w=kp$ for any positive integer k, we have $q_{p,kp}(u)=0$ by (1.3), and thus $F(kp,N,p;f(x))\le\min\{N,\deg(f(x))\}$, $V(kp,N,p)=1$ and $g(kp,N,p)=\infty$.

For any positive w with $p\nmid w$, write $w=w_1+w_2(p-1)$ with $1\le w_1\le p-1$ and $w_2\ge 0$. By (1.3) again one can get

$$\begin{aligned}q_{p,w_1+w_2(p-1)}(u)&\equiv -u^{w_1}(w_1-w_2)q_p(u)\\&\equiv w_1^{-1}(w_1-w_2)q_{p,w_1}(u) \bmod p,\qquad 0\le u<p,\end{aligned}$$

and thus for $N\le p$,

$$\begin{aligned}F(w_1+w_2(p-1),N,p;f(x))&=F(w_1,N,p;w_1(w_1-w_2)^{-1}f(x)),\\V(w_1+w_2(p-1),N,p)&=V(w_1,N,p),\\g(w_1+w_2(p-1),N,p)&=g(w_1,N,p).\end{aligned}$$

(Note that $w_1\not\equiv w_2 \bmod p$ since $p\nmid w$.) Hence, we may restrict ourselves to $1\le w\le p-1$ from now on.

We recall that the classical Waring problem is an important research field in number theory that investigates the smallest s such that every element of $\mathcal{R}$ is a sum of s kth powers in $\mathcal{R}$, where $\mathcal{R}$ is an algebraic structure such as the integers, a finite field, the residue ring modulo m, a polynomial ring, a function field, etc. (see e.g. [23, 36–38]). Recently, the second author and other coauthors considered the Waring problem for Dickson polynomials in finite fields [19, 25, 26].

2. Interpolation of polynomial quotients. In this section we prove bounds on $F(w,N,p;f(x))$. We start with a result which is nontrivial if either w is very large, or $\gcd(w,p-1)$ is moderately large.

THEOREM 2.1. *For $1 \le w < p$ and $f(x) \in \mathbb{F}_p[x]$ of degree d, let*

$$F(w,N,p;f(x)) = \#\{u \in \{0,\ldots,N-1\} : q_{p,w}(u) \equiv f(u) \bmod p\}, \qquad N \le p.$$

Then

$$\begin{aligned} &F(w,N,p;f(x)) \\ &\quad \ll \min\Big\{(p-1-w+d)^{1/4}N^{1/2}p^{1/3}, (p-1-w+d)^{1/8}N^{1/2}p^{3/8}, \\ &\qquad\qquad \frac{1}{\gcd(w,p-1)}d^{1/4}N^{1/2}p^{4/3}, \frac{1}{\gcd(w,p-1)}d^{1/8}N^{1/2}p^{11/8}\Big\}. \end{aligned}$$

Proof. By applying (1.3) we reduce the problem for any w to the case $w = p-1$ (the interpolation of Fermat quotients), i.e., we only need to estimate the number of $0 \le u < N$ satisfying

$$-u^w w q_p(u) \equiv f(u) \bmod p. \tag{2.1}$$

We prove two different bounds.

BOUND 1. By (2.1) we have $q_p(u) \equiv -w^{-1}u^{p-1-w}f(u) \bmod p$. We get

$$\begin{aligned} &F(w,N,p;f(x)) \\ &\quad \ll \big\{\big(\deg(x^{p-1-w}f(x))\big)^{1/4}N^{1/2}p^{1/3}, 1 \le \deg(x^{p-1-w}f(x)) \le p^{1/3}, \\ &\qquad\qquad \big(\deg(x^{p-1-w}f(x))\big)^{1/8}N^{1/2}p^{3/8}, p^{1/3} < \deg(x^{p-1-w}f(x)) < p\big\}, \end{aligned}$$

by [14, Theorem 1]. We remark that the proof of [14, Lemma 1] (which deals only with $N = p$) can be easily extended to $N \le p$. The bound is nontrivial only for $p - w = o(p)$.

BOUND 2. The values attained by $u^w \bmod p$ for all $0 \le u < p$ are the same as the values $u^{\gcd(w,p-1)} \bmod p$. For a fixed primitive element $\gamma \in \mathbb{F}_p$, we consider the cyclotomic classes of order $\frac{p-1}{\gcd(w,p-1)}$:

$$C_j = \{\gamma^{j+\frac{i(p-1)}{\gcd(w,p-1)}} \bmod p : 0 \le i < \gcd(w,p-1)\}, \tag{2.2}$$

where $j = 0,1,\ldots,\frac{p-1}{\gcd(w,p-1)} - 1$. In fact, the C_j's give a partition of $\mathbb{F}_p^*$. For each $u \in C_j$, we always have $u^w = \gamma^{jw}$, and the number of solutions

$u \in C_j \cap \{0, \ldots, N-1\}$ of (2.1) (hence $q_p(u) \equiv -w^{-1}\gamma^{-jw} f(u) \bmod p$) is bounded by

$$\ll \big\{ \big(\deg(f(x))\big)^{1/4} N^{1/2} p^{1/3}, 1 \le \deg(f(x)) \le p^{1/3}, \\ \big(\deg(f(x))\big)^{1/8} N^{1/2} p^{3/8}, p^{1/3} < \deg(f(x)) < p \big\}$$

by [14, Theorem 1] again. So we have

$$\begin{aligned} & F(w,N,p;f(x)) \\ & \quad \ll \frac{p-1}{\gcd(w,p-1)} \min\big\{ \big(\deg(f(x))\big)^{1/4} N^{1/2} p^{1/3}, \big(\deg(f(x))\big)^{1/8} N^{1/2} p^{3/8} \big\} \\ & \quad \ll \frac{1}{\gcd(w,p-1)} \min\big\{ \big(\deg(f(x))\big)^{1/4} N^{1/2} p^{4/3}, \big(\deg(f(x))\big)^{1/8} N^{1/2} p^{11/8} \big\} \end{aligned}$$

since there are $\frac{p-1}{\gcd(w,p-1)}$ C_j's. This bound is nontrivial only if $\gcd(w, p-1) \ge p^{5/6}$. ∎

Corollary 2.2. *For $1 \le w < p$, the number*

$$F(w,N,p) = \#\{u \in \{0,\ldots,N-1\} : q_{p,w}(u) \equiv u \bmod p\}, \qquad N \le p,$$

of fixed points of polynomial quotients satisfies

$$F(w,N,p) \ll \min\bigg\{ (p-w)^{1/4} N^{1/2} p^{1/3}, (p-w)^{1/8} N^{1/2} p^{3/8}, \frac{N^{1/2} p^{4/3}}{\gcd(w,p-1)} \bigg\}.$$

Besides the cases when $p - w = o(p)$ and $\gcd(w, p-1) \ge p^{5/6}$, there is another nontrivial result if $\gcd(w-1, p-1) \ge p^{1/2+\varepsilon}$, which includes the important case $w = 1$.

Theorem 2.3. *For $1 \le w < p$,*

$$F(w,N,p) \ll \frac{p^{3/2+\varepsilon}}{\gcd(w-1,p-1)}, \qquad N \le p.$$

Proof. Define

$$\widetilde{C}_j = \{\gamma^{j + \frac{i(p-1)}{\gcd(w-1,p-1)}} \bmod p : 0 \le i < \gcd(w-1,p-1)\},$$

where $j = 0, 1, \ldots, \frac{p-1}{\gcd(w-1,p-1)} - 1$. The number of solutions $u \in \widetilde{C}_j \cap \{0, \ldots, N-1\}$ of

$$q_p(u) \equiv -w^{-1} u^{-(w-1)} \equiv -w^{-1} \gamma^{-j(w-1)} \bmod p$$

is bounded by $O(p^{1/2+\varepsilon})$ by [18, Proposition 2.1]. So we have

$$F(w,N,p) \ll \frac{p-1}{\gcd(w-1,p-1)} p^{1/2+\varepsilon},$$

which completes the proof. ∎

Remark. The bound is nontrivial only for $\gcd(w-1,p-1) \gg p^{1/2+\varepsilon}$ and $N \gg p^{1/2+\varepsilon}$. However, if $N < p^{2/s}$ for some integer $s \geq 3$, the proof of [18, Proposition 2.1] can be easily modified, and the bound $O(p^{1/2+\varepsilon})$ on the number of solutions $0 \leq u < N$ with $q_p(u) = c$ can be improved to $O(p^{1/s+\varepsilon})$. Using this in the proof of Theorem 2.3 we get

$$F(w,N,p) \ll \frac{p^{1+1/s+\varepsilon}}{\gcd(w-1,p-1)}, \quad N < p^{2/s}.$$

3. Size of value sets. First we prove a bound on $V(p-1,N,p)$, the size of the value set of Fermat quotients q_p (see [24, Theorem 13]) for $N = p$. Then we estimate $V(w,N,p)$ for general $1 \leq w \leq p-2$ in terms of $V(p-1,N,p)$ by (1.3).

Lemma 3.1. *Let $V(p-1,N,p) = \#\{q_p(u) : u = 0,\dots,N-1\}$. Then*

$$V(p-1,N,p) \gg \frac{N^2}{p\log^2 N}, \quad N \leq p.$$

Proof. For $N < p$, one can get the desired result the same way as for $N = p$; see the proof of [24, Theorem 13]. For the convenience of the reader, we sketch the proof here.

Let $Q(N,a)$ be the number of primes l smaller than N with $q_p(l) = a$. Clearly

$$\sum_{a=0}^{p-1} Q(N,a) = \pi(N-1),$$

where $\pi(x)$ denotes the number of primes $l \leq x$. The number of prime number pairs (l,r) with $0 \leq l,r \leq N-1$ and $q_p(l) = q_p(r)$ is $\sum_{a=0}^{p-1} Q(N,a)^2$.

According to the fact that $q_p : \mathbb{Z}_{p^2}^* \to \mathbb{Z}_p$ is a group homomorphism with kernel $\ker(q_p)$ of size $p-1$, we see that $l/r \in \ker(q_p)$ for each pair (l,r) above. Now for each $u \in \ker(q_p)$, there are $\pi(N-1)$ pairs (l,l) such that $1 \equiv l/l \bmod p^2$ if $u = 1$, and at most one pair (l,r) such that $u \equiv l/r \bmod p^2$ if $u \neq 1$, since otherwise $u \equiv l_1/r_1 \equiv l_2/r_2 \bmod p^2$ leads to $l_1 = r_1$, $l_2 = r_2$ or $l_1 = l_2$, $r_1 = r_2$. So we get

$$\sum_{a=0}^{p-1} Q(N,a)^2 \leq \pi(N-1) + \#\ker(q_p) - 1 = \pi(N-1) + p - 2.$$

On the other hand, only at most $V(p-1,N,p)$ of the $Q(N,a)$ are nonzero for $0 \leq a \leq p-1$, so by the Cauchy–Schwarz inequality we have

$$\Big(\sum_{a=0}^{p-1} Q(N,a)\Big)^2 \leq V(p-1,N,p) \sum_{a=0}^{p-1} Q(N,a)^2.$$

Putting everything together, we obtain

$$V(p-1,N,p) \gg \pi(N-1)^2 p^{-1},$$

which concludes the proof. ∎

Remark. For $N<p^{1/s}$ we can also study the number of primes $l_1,\dots,l_s$, $r_1,\dots,r_s<N$ with $q_p(l_1)=\dots=q_p(l_s)=q_p(r_1)=\dots=q_p(r_s)$ to improve Lemma 3.1.

As in Section 2, we prove different bounds on $V(w,N,p)$ which are nontrivial if either $\gcd(w,p-1)$, or $\gcd(w-1,p-1)$ is large enough.

Theorem 3.2. *For* $1\le w<p$ *let* $V(w,N,p)=\#\{q_{p,w}(u): u=0,\dots,N-1\}$. *Then*

$$V(w,N,p) \gg \gcd(w,p-1)\left(\frac{N}{p\log N}\right)^2, \qquad N\le p.$$

Proof. The values assumed by $u^w \bmod p$ for all $0\le u<p$ are the same as the values $u^{\gcd(w,p-1)} \bmod p$. For a fixed primitive element $\gamma\in\mathbb{F}_p$, we consider the cyclotomic classes of order $\frac{p-1}{\gcd(w,p-1)}$ defined by (2.2). Let U be the biggest subset of $\{0,\dots,N-1\}$ such that $q_p(u)\ne q_p(v)$ for any $u\ne v\in U$. It is easy to see that $\#U=V(p-1,N,p)$. Then for any $u_1,u_2\in(C_j\cap U)$ and any j, using (1.3) we always have

$$u_1^w\equiv u_2^w \bmod p \quad\text{and}\quad q_{p,w}(u_1)\ne q_{p,w}(u_2).$$

By the pigeonhole principle we see that there exists some j with

$$C_j\cap U \ge \frac{\#U}{(p-1)/\gcd(w,p-1)}.$$

So we have

$$V(w,N,p)\ge \frac{\#U}{(p-1)/\gcd(w,p-1)} \gg \frac{\gcd(w,p-1)N^2}{p^2\log^2 N}$$

by Lemma 3.1. ∎

The bound in Theorem 3.2 is trivial if $\gcd(w,p-1)\ll \log^2 N$. Below we consider the cases of large $\gcd(w-1,p-1)$ (including $w=1$) and get a nontrivial bound using a different method.

Theorem 3.3. *For* $1\le w<p$,

$$V(w,N,p)\gg \gcd(w-1,p-1)\frac{N^{1/2}}{p^{4/3}}, \qquad N\le p.$$

Proof. We first prove the case $w=1$, and then reduce to it the general case $w>1$. The proof follows [14, Section 2], which deals with the case

$N = p$. Define

$$M_d = \#\{u \in \{0, \ldots, N-1\} : q_{p,1}(u) = d\}$$

for some d. We first give an upper bound on M_d.

For $0 \le a < N$ and $1 \le b < N$, suppose that $(a, a+b \bmod N)$ is a pair of points satisfying

$$q_{p,1}(a) = q_{p,1}(a+b \bmod N) = d.$$

We note that there are $M_d(M_d-1)$ such pairs. (Note that $M_d = 1$ if no such b exists.) Now we fix any $1 \le b < N$ and estimate the number of a. For each pair (a, b), set $c = b$ if $a + b < N$, and $c = b - N$ otherwise. Hence for a given b there are two possible choices of c such that $(a, a+c)$ satisfy

$$q_{p,1}(a) = q_{p,1}(a+c) = d \tag{3.1}$$

for some a. For given c we estimate the number of a.

If $(a, a+c)$ is a pair satisfying (3.1), using (1.3) and the definition of $q_p(u)$ we get

$$d = q_{p,1}(a+c) \equiv -(a+c)q_p(a+c) \equiv -aq_p(a) - cq_p(c) - c\sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p}(ac^{-1})^i$$
$$\equiv q_{p,1}(a) + q_{p,1}(c) + c\sum_{i=1}^{p-1} \frac{(-ac^{-1})^i}{i} \bmod p,$$

and thus

$$q_{p,1}(c) + c\sum_{i=1}^{p-1} \frac{(-a^{-1}c)^i}{i} \equiv 0 \bmod p.$$

Substituting $a \equiv -cx \bmod p$ for $x \in \mathbb{F}_p$ we get

$$q_{p,1}(c)c^{-1} + \sum_{i=1}^{p-1} \frac{x^i}{i} \equiv 0 \bmod p.$$

Now by [22, Lemma 4] the number of x (which is not smaller than the number of a since $0 \le a < N$) for fixed c is bounded by $O(p^{2/3})$, and we obtain

$$M_d(M_d-1) \ll (N-1)\min\{p^{2/3}, N\},$$

and thus $M_d \ll N^{1/2}p^{1/3}$ if $N \gg p^{2/3}$, which implies that

$$V(1, N, p) \gg \frac{N^{1/2}}{p^{1/3}}.$$

From (1.3) again, we have

$$q_{p,w}(u) \equiv -u^w w q_p(u) \equiv u^{w-1} w q_{p,1}(u) \bmod p,$$

and hence

$$V(w,N,p) \geq \frac{V(1,N,p)}{(p-1)/\gcd(w-1,p-1)}$$

following the proof of Theorem 3.2. ∎

REMARK. Ostafe and Shparlinski [24] stated the problem of finding a nontrivial lower bound on $V(1,N,p)$ for $N \leq p$. In particular, Theorem 3.3 implies

$$V(1,N,p) \gg N^{1/2}p^{-1/3},$$

which is nontrivial for $N \gg p^{2/3}$.

4. Bounds on the Waring number

4.1. Bound derived from additive character sums. We first present a bound on character sums of polynomial quotients, which is a special case of [12, Theorem 3]. In this subsection, we will exploit these character sums to estimate the Waring number $g(w,N,p)$.

LEMMA 4.1. *Let $q_{p,w}(u)$ be defined by (1.2) with $1 \leq w < p$. For any nontrivial additive character ψ of $\mathbb{F}_p$ we have*

$$\Big|\sum_{u=0}^{N-1} \psi(q_{p,w}(u))\Big| \ll \frac{1}{\gcd(w,p-1)} N^{1/2}p^{11/8}, \qquad N \leq p.$$

As noted in [22, Theorem 2], the exponent ε in [12, Theorem 3] can be removed when the modulus k of (multiplicative) characters equals p^2 since the Burgess bound contains a factor $k^{3/16+\varepsilon}$ (see [4, Theorems 2 and 3]). Lemma 4.1 is only nontrivial for $N \geq p^{3/4}$. However, using the precise Theorem 3 in [12] we can derive bounds which are nontrivial for $N \geq p^{1/2+o(1)}$.

THEOREM 4.2. *For $1 \leq w < p$, we have*

$$g(w,N,p) \leq s$$

if $\gcd(w,p-1)^{s-1} \gg p^{11s/8+1/4}N^{-s/2-1}\log^2 N$, *$s \geq 3$ and $N \leq p$.*

Proof. Without loss of generality we restrict ourselves to the case $g(w,N,p) \geq 3$.

Let ψ be a nontrivial additive character of $\mathbb{F}_p$. For $s \geq 3$ and $y \in \mathbb{F}_p$, the number $N_s(y)$ of solutions $(v_1, v_2, u_1, \ldots, u_{s-2})$ of the equation

$$y \equiv v_1 + v_2 + q_{p,w}(u_1) + \cdots + q_{p,w}(u_{s-2}) \bmod p,$$

where $v_1, v_2 \in V(w,N,p)$, $0 \le u_1, \ldots, u_{s-2} < N$, is

$$N_s(y) = \frac{1}{p} \sum_{a \in \mathbb{F}_p} \sum_{v_1,v_2 \in V(w,N,p)} \sum_{\substack{0 \le u_j < N \\ 1 \le j \le s-2}} \psi\Big(a\Big(v_1 + v_2 + \sum_{i=1}^{s-2} q_{p,w}(u_i) - y\Big)\Big)$$

$$= \frac{V(w,N,p)^2 N^{s-2}}{p} + \frac{1}{p} \sum_{a \in \mathbb{F}_p^*} \psi(-ay) \sum_{v_1,v_2 \in V(w,N,p)} \psi(a(v_1+v_2))$$

$$\times \sum_{\substack{0 \le u_j < N \\ 1 \le j \le s-2}} \psi\Big(a \sum_{i=1}^{s-2} q_{p,w}(u_i)\Big).$$

By Lemma 4.1, we have

$$\left| N_s(y) - \frac{V(w,N,p)^2 N^{s-2}}{p} \right|$$

$$\le \frac{1}{p} \sum_{a \in \mathbb{F}_p^*} \Big| \sum_{v \in V(w,N,p)} \psi(av) \Big|^2 \Big| \sum_{0 \le u < N} \psi\left(a q_{p,w}(u)\right) \Big|^{s-2}$$

$$\ll \frac{1}{p} \bigg(\frac{N^{1/2} p^{11/8}}{\gcd(w,p-1)} \bigg)^{s-2} \sum_{a \in \mathbb{F}_p^*} \Big| \sum_{v \in V(w,N,p)} \psi(av) \Big|^2$$

$$\le \frac{1}{p} \bigg(\frac{N^{1/2} p^{11/8}}{\gcd(w,p-1)} \bigg)^{s-2} \sum_{a \in \mathbb{F}_p} \sum_{v_1,v_2 \in V(w,N,p)} \psi(a(v_1 - v_2))$$

$$\le V(w,N,p) \bigg(\frac{N^{1/2} p^{11/8}}{\gcd(w,p-1)} \bigg)^{s-2}.$$

The number $N_s(y)$ is positive for all $y \in \mathbb{F}_p$ if

$$V(w,N,p) > p \bigg(\frac{p^{11/8}}{\gcd(w,p-1) N^{1/2}} \bigg)^{s-2},$$

and thus $g(w,N,p) \le s$ under this condition. ∎

Remark. It is clear that $g(p-1,p,p) \le 3$, which is the Waring number for Fermat quotients. Theorem 4.2 is only nontrivial if $\gcd(w,p-1) \gg p^{7/8}$ and $N \ge p^{3/4}$. Very recently, Harman and Shparlinski [21] proved $g(p-1,N,p) \le 9$ for any $N \ge p^{1/(2e^{1/2})+\varepsilon}$ and sufficiently large p.

4.2. Bound derived from the Cauchy–Davenport theorem. In this subsection we prove a bound on $g(w,N,p)$ based on the Cauchy–Davenport theorem (see e.g., [35, Theorem 5.4]), which is rather moderate but nontrivial if $\gcd(w,p-1) \gg \log^2 p$ or $\gcd(w-1,p-1) \gg p^{5/6}$.

Lemma 4.3 (Cauchy–Davenport theorem). *Let A, B be nonempty subsets of $\mathbb{F}_p$. Then*

$$\#(A+B) \geq \min\{\#A + \#B - 1, p\},$$

where $A + B = \{a + b : a \in A,\ b \in B\}$.

Theorem 4.4. *For $1 \leq w < p$, we have*

$$g(w, N, p) \ll \min\left\{\frac{p^3 \log^2 p}{N^2 \gcd(w, p-1)}, \frac{p^{7/3}}{N^{1/2} \gcd(w-1, p-1)}\right\}, \qquad N \leq p.$$

Proof. For $s \geq 1$ define

$$W_s = \{q_{p,w}(u_1) + \cdots + q_{p,w}(u_s) : 0 \leq u_1, \ldots, u_s < N\}.$$

Since $W_s = W_{s-1} + W_1$ for $s \geq 2$, by Lemma 4.3 we have

$$\#W_s \geq \min\{\#W_{s-1} + \#W_1 - 1, p\}, \qquad s \geq 2,$$

and get by induction

$$\#W_s \geq \min\{s(\#W_1 - 1) + 1, p\}, \qquad s \geq 1.$$

Hence

$$s \leq \left\lceil \frac{p-1}{\#W_1 - 1} \right\rceil,$$

and then the desired result follows from Theorems 3.2 and 3.3. ∎

5. Final remarks. 1. The bounds in this paper are nontrivial if $\gcd(w, p-1)$ or $\gcd(w-1, p-1)$ is "large". It is challenging to study general w.

2. The bound in Lemma 4.1 does not cover the cases of small w. In particular, it is an interesting problem to estimate the character sums

$$\sum_{u=0}^{N-1} \psi(q_{p,1}(u)).$$

3. In [32], Shparlinski considered for Fermat quotients the smallest number Λ_p such that

$$\{q_p(u) : u \in \{1, \ldots, \Lambda_p\}\} = \mathbb{F}_p$$

by estimating $\Lambda_p \leq p^{463/252+o(1)}$. It would be interesting to extend this result to $q_{p,w}$.

4. In [34], Shparlinski and the second author introduced the *polynomial Fermat quotients* in polynomial rings over finite fields. Let $\mathbb{F}_q$ be a finite field of prime power order $q = p^r$. Then for a fixed irreducible polynomial $P \in \mathbb{F}_q[X]$ of degree $n \geq 2$ and $A \in \mathbb{F}_q[X]$, the polynomial Fermat quotient is defined by

$$q_P(A) \equiv \frac{A^{q^n-1} - 1}{P} \bmod P, \quad \deg(q_P(A)) < n, \qquad \text{if } \gcd(A, P) = 1,$$

and $q_P(A) = 0$ if $\gcd(A, P) = P$. The properties, such as the number of fixed points and the image size, of the polynomial Fermat quotient are investigated in [34].

Like the definition of polynomial quotients modulo p, one can define

$$q_{P,w}(A) \equiv \frac{A^w - A^{wq^n}}{P} \bmod P, \qquad \deg(q_{P,w}(A)) < n,$$

for integers $w \geq 1$. In particular, $-q_{P,1}(A)$ has been introduced in [27]. Since $q_{P,1}$ is a linear map with kernel of dimension $\lceil n/p \rceil$, we have

$$\#\{A : q_{P,1}(A) = B,\ \deg(A) < n\} = q^{\lceil n/p \rceil}$$

for any fixed $B = q_{P,1}(A_0)$ for some A_0, and hence

$$\#\{q_{P,1}(A) : \deg(A) < n\} = q^{n - \lceil n/p \rceil}.$$

(See also the proof of [34, Lemma 6].)

Here we present some lower bounds on the image size of $q_{P,w}$ for $w > 1$. We only consider the case $p \nmid w$, since otherwise $q_{P,w}$ is a zero map. Firstly from

$$q_{P,w}(A) \equiv -wA^w q_P(A) \bmod P,$$

we reduce the problem to the image size of q_P (see [34, Theorem 5]) and obtain

$$\#\{q_{P,w}(A) : \deg(A) < n\} \gg \frac{\gcd(w, q^n - 1)}{qn^2}$$

by using the proof technique of Theorem 3.2. Secondly from

$$q_{P,w}(A) \equiv wA^{w-1} q_{P,1}(A) \bmod P \tag{5.1}$$

we obtain a lower bound similarly in terms of the image size of $q_{P,1}$ above:

$$\#\{q_{P,w}(A) : \deg(A) < n\} \gg \frac{\gcd(w - 1, q^n - 1)}{q^{\lceil n/p \rceil}}.$$

Finally from (5.1) again, since there are exactly $\frac{q^n - 1}{\gcd(w-1, q^n-1)} + 1$ different A^{w-1} modulo P for all A with $\deg(A) < n$, we see that there exists a B such that at least $\big(\frac{q^n-1}{\gcd(w-1,q^n-1)} + 1\big)/q^{n-\lceil n/p \rceil}$ A satisfy $q_{P,1}(A) = B$, but $A^{w-1} \bmod P$ are different for all such A. Thus we obtain another lower bound:

$$\#\{q_{P,w}(A) : \deg(A) < n\} \gg \frac{q^{\lceil n/p \rceil}}{\gcd(w - 1, q^n - 1)}.$$

About the Waring problem for $q_{P,w}$ we cannot say anything more. The Cauchy–Davenport theorem is not true for arbitrary finite fields in general and we do not have any results on character sums of $q_{P,w}$, so we cannot deal with the Waring problem using the methods in Section 4. But for $q_{P,1}$ the Waring number does not exist, since $q_{P,1}$ is a linear map with kernel of dimension $\lceil n/p \rceil$, and hence the image of $q_{P,1}$ is a proper linear subspace of

$\mathbb{F}_q[X]/\langle P\rangle$. That is, there does exist an element in $\mathbb{F}_q[X]/\langle P\rangle$ which cannot be represented as a sum of $q_{P,1}$.

Acknowledgements. The authors thank the referee for providing some ideas how to extend the range of nontriviality of N, and Igor Shparlinski for mentioning reference [21]. The authors also thank Alina Ostafe for pointing to Waring's problem for Fermat quotients.

Z.X.C. was partially supported by the National Natural Science Foundation of China under grants No. 61373140 and No. 61170246. A.W. was partially supported by the Austrian Science Fund (FWF), Project F5511-N26, which is part of the Special Research Program "Quasi-Monte Carlo Method: Theory and Applications".

Parts of this paper were written during pleasant mutual visits of the authors to RICAM, Austrian Academy of Sciences in Linz and Putian University. They wish to thank for the hospitality and financial support.

References

[1] T. Agoh, K. Dilcher and L. Skula, *Fermat quotients for composite moduli*, J. Number Theory 66 (1997), 29–50.

[2] H. Aly and A. Winterhof, *Boolean functions derived from Fermat quotients*, Cryptogr. Commun. 3 (2011), 165–174.

[3] J. Bourgain, K. Ford, S. Konyagin and I. E. Shparlinski, *On the divisibility of Fermat quotients*, Michigan Math. J. 59 (2010), 313–328.

[4] D. A. Burgess, *On character sums and L-series, II*, Proc. London Math. Soc. 13 (1963), 524–536.

[5] M. C. Chang, *Short character sums with Fermat quotients*, Acta Arith. 152 (2012), 23–38.

[6] Z. X. Chen, *Trace representation and linear complexity of binary sequences derived from Fermat quotients*, Sci. China Inf. Sci. 57 (2014), no. 11, 112109, 10 pp.

[7] Z. X. Chen and X. N. Du, *On the linear complexity of binary threshold sequences derived from Fermat quotients*, Des. Codes Cryptogr. 67 (2013), 317–323.

[8] Z. X. Chen and D. Gómez-Pérez, *Linear complexity of binary sequences derived from polynomial quotients*, in: Sequences and Their Applications—SETA 2012, Lecture Notes in Comput. Sci. 7280, Springer, Berlin, 2012, 181–189.

[9] Z. X. Chen, L. Hu and X. N. Du, *Linear complexity of some binary sequences derived from Fermat quotients*, China Commun. 9 (2012), 105–108.

[10] Z. X. Chen, Z. H. Niu and C. H. Wu, *On the k-error linear complexity of binary sequences derived from polynomial quotients*, Sci. China Inf. Sci. 58 (2015), no. 9, 092107, 15 pp.

[11] Z. X. Chen, A. Ostafe and A. Winterhof, *Structure of pseudorandom numbers derived from Fermat quotients*, in: Arithmetic of Finite Fields—WAIFI 2010, Lecture Notes in Comput. Sci. 6087, Springer, Berlin, 2010, 73–85.

[12] Z. X. Chen and A. Winterhof, *Additive character sums of polynomial quotients*, in: Theory and Applications of Finite Fields, Contemp. Math. 579, Amer. Math. Soc., Providence, RI, 2012, 67–73.

[13] Z. X. Chen and A. Winterhof, *On the distribution of pseudorandom numbers and vectors derived from Euler–Fermat quotients*, Int. J. Number Theory 8 (2012), 631–641.

[14] Z. X. Chen and A. Winterhof, *Interpolation of Fermat quotients*, SIAM J. Discrete Math. 28 (2014), 1–7.

[15] X. N. Du, Z. X. Chen and L. Hu, *Linear complexity of binary sequences derived from Euler quotients with prime-power modulus*, Inform. Process. Lett. 112 (2012), 604–609.

[16] X. N. Du, A. Klapper and Z. X. Chen, *Linear complexity of pseudorandom sequences generated by Fermat quotients and their generalizations*, Inform. Process. Lett. 112 (2012), 233–237.

[17] R. Ernvall and T. Metsänkylä, *On the p-divisibility of Fermat quotients*, Math. Comp. 66 (1997), 1353–1365.

[18] W. L. Fouché, *On the Kummer–Mirimanoff congruences*, Quart. J. Math. Oxford Ser. (2) 37 (1986), 257–261.

[19] D. Gómez-Pérez and A. Winterhof, *Waring's problem in finite fields with Dickson polynomials*, in: Finite Fields: Theory and Applications, Contemp. Math. 518, Amer. Math. Soc., Providence, RI, 2010, 185–192.

[20] D. Gómez-Pérez and A. Winterhof, *Multiplicative character sums of Fermat quotients and pseudorandom sequences*, Period. Math. Hungar. 64 (2012), 161–168.

[21] G. Harman and I. E. Shparlinski, *Products of small integers in residue classes and additive properties of Fermat quotients*, Int. Math. Res. Notices (2015), online.

[22] R. Heath-Brown, *An estimate for Heilbronn's exponential sum*, in: Analytic Number Theory: Proc. Conf. in Honor of Heini Halberstam, Birkhäuser, Boston, 1996, 451–463.

[23] Y. R. Liu and T. D. Wooley, *Waring's problem in function fields*, J. Reine Angew. Math. 638 (2010), 1–67.

[24] A. Ostafe and I. E. Shparlinski, *Pseudorandomness and dynamics of Fermat quotients*, SIAM J. Discrete Math. 25 (2011), 50–71.

[25] A. Ostafe and I. E. Shparlinski, *On the Waring problem with Dickson polynomials in finite fields*, Proc. Amer. Math. Soc. 139 (2011), 3815–3820.

[26] A. Ostafe, D. Thomson and A. Winterhof, *On the Waring problem with multivariate Dickson polynomials*, in: Theory and Applications of Finite Fields, Contemp. Math. 579, Amer. Math. Soc., Providence, RI, 2012, 153–161.

[27] J. Sauerberg and L. Shu, *Fermat quotients over function fields*, Finite Fields Appl. 3 (1997), 275–286.

[28] M. Sha, *The arithmetic of Carmichael quotients*, Period. Math. Hungar. (2015), online.

[29] I. D. Shkredov, *On Heilbronn's exponential sum*, Quart. J. Math. 64 (2013), 1221–1230.

[30] I. E. Shparlinski, *Character sums with Fermat quotients*, Quart. J. Math. 62 (2011), 1031–1043.

[31] I. E. Shparlinski, *Bounds of multiplicative character sums with Fermat quotients of primes*, Bull. Austral. Math. Soc. 83 (2011), 456–462.

[32] I. E. Shparlinski, *On the value set of Fermat quotients*, Proc. Amer. Math. Soc. 140 (2012), 1199–1206.

[33] I. E. Shparlinski, *Fermat quotients: Exponential sums, value set and primitive roots*, Bull. London Math. Soc. 43 (2011), 1228–1238.

[34] I. E. Shparlinski and A. Winterhof, *Distribution of values of polynomial Fermat quotients*, Finite Fields Appl. 19 (2013), 93–104.

[35] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge Univ. Press, Cambridge, 2006.
[36] A. Winterhof, *On Waring's problem in finite fields*, Acta Arith. 87 (1998), 171–177.
[37] A. Winterhof, *A note on Waring's problem in finite fields*, Acta Arith. 96 (2001), 365–368.
[38] A. Winterhof and C. van de Woestijne, *Exact solutions to Waring's problem for finite fields*, Acta Arith. 141 (2010), 171–190.

Zhixiong Chen
Provincial Key Laboratory of
Applied Mathematics
Putian University
Putian, Fujian 351100, P.R. China
E-mail: ptczx@126.com

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

Received on 8.7.2014
and in revised form on 19.5.2015 (7868)