MATHEMATICS OF COMPUTATION
Volume 84, Number 296, November 2015, Pages 2969–2977
http://dx.doi.org/10.1090/mcom/2946
Article electronically published on April 10, 2015

CHARACTER SUMS AND DETERMINISTIC POLYNOMIAL ROOT FINDING IN FINITE FIELDS

JEAN BOURGAIN, SERGEI V. KONYAGIN, AND IGOR E. SHPARLINSKI

Abstract. We obtain a new bound of certain double multiplicative character sums. We use this bound together with some other previously obtained results to obtain new algorithms for finding roots of polynomials modulo a prime p.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of q elements of characteristic p. The classical algorithm of Berlekamp [1] reduces the problem of factoring polynomials of degree n over $\mathbb{F}_q$ to the problem of factoring squarefree polynomials of degree n over $\mathbb{F}_p$ that fully split in $\mathbb{F}_p$; see also [8, Chapter 14]. Shoup [15, Theorem 3.1] has given a deterministic algorithm that fully factors any polynomial of degree n over $\mathbb{F}_p$ in $O(n^{2+o(1)}p^{1/2}(\log p)^2)$ arithmetic operations over $\mathbb{F}_p$; in particular, it runs in time at most $n^2p^{1/2+o(1)}$. Furthermore, Shoup [15, Remark 3.5] has also announced an algorithm of complexity $O(n^{3/2+o(1)}p^{1/2}(\log p)^2)$ for factoring arbitrary univariate polynomials of degree n over $\mathbb{F}_p$.

We remark, that although the efficiency of deterministic polynomial factorisation algorithms falls far behind the fastest probabilistic algorithms (see, for example, [9, 11, 12]), the question is of great theoretic interest.

Here we address a special case of the polynomial factorisation problem when the polynomial f fully splits over $\mathbb{F}_p$ (as we have noticed there is a polynomial time reduction between factoring general polynomials and polynomials that split over $\mathbb{F}_p$). That is, here we deal with the root finding problem. We also note that in order to find a root (or all roots) of a polynomial $f \in \mathbb{F}_p[X]$, it is enough to do the same for the polynomial $\gcd\big(f(X), X^{p-1}-1\big)$ which is squarefree and fully splits over $\mathbb{F}_p$.

We consider two variants of the root finding problem:

- Given a polynomial $f \in \mathbb{F}_p[X]$, find all roots of f in $\mathbb{F}_p$.
- Given a polynomial $f \in \mathbb{F}_p[X]$, find at least one root of f in $\mathbb{F}_p$.

For the case of finding all roots we show that essentially the initial approach of Shoup [15] together with the fast factor refinement procedure of Bernstein [2] leads to an algorithm of complexity $np^{1/2+o(1)}$. In fact this result is already implicit in [15] but here we record it again with a very short proof. We use this as a benchmark for our algorithm for the second problem.

We remark that a natural example of the situation when one has to find a root of a polynomial of large degree arises in the problem of constructing elliptic curves

Received by the editor September 10, 2013 and, in revised form, March 9, 2014.
2010 *Mathematics Subject Classification.* Primary 11L40, 11T06, 11Y16, 68Q25.
Key words and phrases. Finite field, root finding, character sums, multiplicative energy.

over $\mathbb{F}_p$ with a prescribed number of $\mathbb{F}_p$-rational points. In this case one has to find a root of the *Hilbert class polynomial*, we refer to [17, 18] for more details on this and underlying problems.

In the case of finding just one root, we obtain a faster algorithm, which is based on bounds of double multiplicative character sums

$$T_\chi(\mathcal{I}, \mathcal{S}) = \sum_{u \in \mathcal{I}} \left| \sum_{s \in \mathcal{S}} \chi(u+s) \right|^2,$$

where $\mathcal{I} = \{1, \ldots, h\}$ is an interval of h consecutive integers, $\mathcal{S} \subseteq \mathbb{F}_p$ is an arbitrary set and χ is a multiplicative character of $\mathbb{F}_p^*$. More precisely, here we use a new bound on $T_\chi(\mathcal{I}, \mathcal{S})$ to improve the bound $np^{1/2+o(1)}$ in the case when n is large enough, namely if it grows as a power of p. We believe that our new bound of the sums $T_\chi(\mathcal{I}, \mathcal{S})$ as well as several auxiliary results (based on some methods from additive combinatorics) are of independent interest as well.

Throughout the paper, any implied constants in symbols O and $\ll$ may depend on two real positive parameters, ε and δ, and are absolute otherwise. We recall that the notations $U = O(V)$ and $U \ll V$ are all equivalent to the statement that $|U| \le cV$ holds with some constant $c > 0$. We also use $U \asymp V$ to denote that $U \ll V \ll U$.

2. Bounds on the number solutions to some equations and character sums

2.1. **Uniform distribution and exponential sums.** The following result is well-known and can be found, for example, in [13, Chapter 1, Theorem 1] (which is a more precise form of the celebrated Erdős–Turán inequality).

Lemma 1. *Let $\xi_1, \ldots, \xi_M$ be a sequence of M points of the unit interval $[0,1]$. Then for any integer $K \ge 1$, and an interval $[0,\rho] \subseteq [0,1]$, we have*

$$\#\{m = 1, \ldots, M \ : \xi_m \in [0,\rho]\} - \rho M \ll \frac{M}{K} + \sum_{k=1}^{K} \left(\frac{1}{K} + \min\{\rho, 1/k\} \right) \left| \sum_{m=1}^{M} \exp(2\pi i k \xi_m) \right|.$$

2.2. **Preliminary bounds.** Throughout this section we fix some set $\mathcal{S} \subseteq \mathbb{F}_p$ and an interval $\mathcal{I} = \{1, \ldots, h\}$ of $h \le p^{1/2}$ consecutive integers.

We say that a set $\mathcal{D} \subseteq \mathbb{F}_p$ is Δ-spaced if no elements $d_1, d_2 \in \mathcal{D}$ and positive integer $k \le \Delta$ satisfy the equality $d_1 + k = d_2$.

Here we always assume that the set $\mathcal{S}$ is h-spaced.

Finally, we also fix some L and denote by $\mathcal{L}$ the set of primes of the interval $[L, 2L]$.

We denote

$$\mathcal{W} = \Big\{ (u_1, u_2, \ell_1, \ell_2, s_1, s_2) \in \mathcal{I}^2 \times \mathcal{L}^2 \times \mathcal{S}^2 \ : \ \frac{u_1 + s_1}{\ell_1} \equiv \frac{u_2 + s_2}{\ell_2} \pmod p \Big\}.$$

The following result is based on some ideas of Shao [14].

Lemma 2. *If $L < h$ and $8hL < p$, then*

$$\#\mathcal{W} \ll (\#\mathcal{S} hL)^2 p^{-1} + \#\mathcal{S} hL p^{o(1)}.$$

Proof. Clearly

$$\#\mathcal{W} = \#\mathcal{W}^* + O(\#\mathcal{S}hL), \tag{1}$$

where

$$\mathcal{W}^* = \{(u_1, u_2, \ell_1, \ell_2, s_1, s_2) \in \mathcal{W} \ : \ \ell_1 \neq \ell_2\}.$$

Denote

$$\overline{\mathcal{S}} = \mathcal{S} + \mathcal{I} = \{u + s \ : \ (u, v) \in \mathcal{I} \times \mathcal{S}\}, \quad \overline{\mathcal{I}} = \{-h, \dots, h\}.$$

Clearly,

$$\mathcal{W}^* \ll h^{-2}\Big\{(u_1, u_2, \ell_1, \ell_2, s_1, s_2) \in \overline{\mathcal{I}}^2 \times \mathcal{L}^2 \times \overline{\mathcal{S}}^2 \ : \ \ell_1 \neq \ell_2, \\ \frac{u_1 + s_1}{\ell_1} \equiv \frac{u_2 + s_2}{\ell_2} \pmod p\Big\}.$$

Note that for fixed $\ell_1, \ell_2 \in \mathcal{L}$, $\ell_1 \neq \ell_2$ and integer x, $|x| \le 4hL$, the congruence

$$u_1\ell_2 - u_2\ell_1 \equiv x \pmod p, \qquad u_1, u_2 \in \overline{\mathcal{L}},$$

is equivalent to the equation $u_1\ell_2 - u_2\ell_1 = x$ (since $8hL < p$) and thus has $O\left(h/L\right)$ solutions. We rewrite

$$\frac{u_1 + s_1}{\ell_1} \equiv \frac{u_2 + s_2}{\ell_2} \pmod p$$

as

$$s_1\ell_2 - s_2\ell_1 \equiv x \equiv u_1\ell_2 - u_2\ell_1 \pmod p.$$

One can consider that $x \ge 0$. We now bound the cardinality of

$$\mathcal{U} = \Big\{(x, \ell_1, \ell_2, s_1, s_2) \in [0, 4hL] \times \mathcal{L}^2 \times \overline{\mathcal{S}}^2 \ : \\ s_1\ell_2 - s_2\ell_1 \equiv x \pmod p\Big\}.$$

The above argument shows that

$$\mathcal{W}^* \ll h^{-2}(h/L)\#\mathcal{U} = h^{-1}L^{-1}\#\mathcal{U}. \tag{2}$$

We now apply Lemma 1 to the sequence of fractional parts

$$\left\{\frac{s_1\ell_2 - s_2\ell_1}{p}\right\}, \qquad (\ell_1, \ell_2, s_1, s_2) \in \mathcal{L}^2 \times \overline{\mathcal{S}}^2,$$

with $M = (\#\mathcal{L})^2(\#\overline{\mathcal{S}})^2$, $\rho = 8hLp^{-1}$ and $K = \lceil \rho^{-1} \rceil$. This yields the bound

$$\begin{aligned}\#\mathcal{U} &\ll (\#\mathcal{L})^2(\#\overline{\mathcal{S}})^2\rho \\ &\qquad + \rho\sum_{k=1}^{K}\left|\sum_{(\ell_1,\ell_2,s_1,s_2)\in\mathcal{L}^2\times\overline{\mathcal{S}}^2} \exp\left(2\pi ik\left(s_1\ell_2 - s_2\ell_1\right)/p\right)\right| \\ &= (\#\mathcal{L})^2(\#\overline{\mathcal{S}})^2\rho + \rho\sum_{k=1}^{K}\left|\sum_{(\ell,s)\in\mathcal{L}\times\overline{\mathcal{S}}} \exp\left(2\pi iks\ell/p\right)\right|^2.\end{aligned}$$

Using the Cauchy inequality, denoting $r = k\ell$ and then using the classical bound on the divisor function, we derive

$$\begin{aligned}\#\mathcal{U} &\ll (\#\mathcal{L})^2(\#\overline{\mathcal{S}})^2\rho + \rho\#\mathcal{L}\sum_{k=1}^{K}\sum_{\ell\in\mathcal{L}}\left|\sum_{s\in\overline{\mathcal{S}}}\exp\left(2\pi iks\ell/p\right)\right|^2\\ &\le (\#\mathcal{L})^2(\#\overline{\mathcal{S}})^2\rho + p^{o(1)}\rho\#\mathcal{L}\sum_{r=0}^{p-1}\left|\sum_{s\in\overline{\mathcal{S}}}\exp\left(2\pi irs/p\right)\right|^2,\end{aligned}$$

since $r \in [1, 2KL] \subseteq [0, p-1]$ provided that p is sufficiently large. Thus, using the Parseval inequality and recalling the values of our parameters, we obtain

$$\#\mathcal{U} \ll hL^3(\#\overline{\mathcal{S}})^2p^{-1} + hL^2\#\overline{\mathcal{S}}p^{o(1)}.$$

Using the trivial bound $\#\overline{\mathcal{S}} \ll \#\mathcal{S}h$, we obtain

$$\#\mathcal{U} \ll h^3L^3(\#\mathcal{S})^2p^{-1} + h^2L^2\#\mathcal{S}p^{o(1)}.$$

Thus, recalling (1) and (2) we conclude the proof. □

Denote

$$W(x,y) = \#\left\{(u,\ell,s,t) \in \mathcal{I}\times\mathcal{L}\times\mathcal{S}^2 \ : \ \frac{u+s}{\ell} = x, \ \frac{u+t}{\ell} = y\right\}. \tag{3}$$

Lemma 3. *We have*

$$\sum_{x,y\in\mathbb{F}_p} W(x,y)^2 \ll (\#S)^3(hL)^2p^{-1} + (\#S)^2hLp^{o(1)}.$$

Proof. Clearly,

$$\begin{aligned}\sum_{x,y\in\mathbb{F}_p} W(x,y)^2 &= \#\Big\{(u_1,u_2,\ell_1,\ell_2,s_1,t_1,s_2,t_2) \in \mathcal{I}^2\times\mathcal{L}^2\times\mathcal{S}^4 \ :\\ &\qquad \frac{u_1+s_1}{\ell_1} = \frac{u_2+s_2}{\ell_2}, \ \frac{u_1+t_1}{\ell_1} = \frac{u_2+t_2}{\ell_2}\Big\}.\end{aligned}$$

For each $(u_1,u_2,\ell_1,\ell_2,s_1,s_2) \in \mathcal{W}$ and $t_1 \in \mathcal{S}$ there is only one possible value for t_2. The result now follows from Lemma 2. □

2.3. **Character sum estimates.** First we recall the following special case of the Weil bound of character sums (see [10, Theorem 11.23]).

Lemma 4. *For any polynomial $F(X) \in \mathbb{F}_p[X]$ with N distinct zeros in the algebraic closure of $\mathbb{F}_p$ and which is not a perfect dth power in the ring of polynomials over $\mathbb{F}_p$, and a nonprincipal multiplicative character χ of $\mathbb{F}_p^*$ of order d, we have*

$$\left|\sum_{x\in\mathbb{F}_p}\chi\left(F(x)\right)\right| \le Np^{1/2}.$$

The following estimate improves and generalises [4, Lemma 14] and also [7, Theorem 8]. Its proof is based on the classical “amplification” argument of Burgess [5,6].

Lemma 5. *For any positive $\delta > 0$ there is some $\eta > 0$ such that for an interval $\mathcal{I} = \{1, \dots, h\}$ of $h \le p^{1/2}$ consecutive integers and any h-spaced set $\mathcal{S} \subseteq \mathbb{F}_p$ with*

$$\#\mathcal{S}h > p^{1/2+\delta},$$

for any nontrivial multiplicative character χ of $\mathbb{F}_p^*$ we have

$$T_\chi(\mathcal{I}, \mathcal{S}) \ll (\#S)^2 hp^{-\eta}.$$

Proof. We choose a sufficiently small ε and define

$$L = \left\lfloor hp^{-2\varepsilon} \right\rfloor \qquad \text{and} \qquad T = \lfloor p^\varepsilon \rfloor .$$

As in Section 2.2, we denote by $\mathcal{L}$ the set of primes of the interval $[L, 2L]$. Note that

$$(\#\mathcal{S})^2 \, TL \ll (\#S)^2 hp^{-\varepsilon}.$$

Then

$$\begin{aligned} T_\chi(\mathcal{I}, \mathcal{S}) &= \frac{1}{(T+1)\#\mathcal{L}}\sigma + O\left((\#\mathcal{S})^2 \, TL\right) \\ &= \frac{1}{(T+1)\#\mathcal{L}}\sigma + O\left((\#S)^2 hp^{-\varepsilon}\right), \end{aligned} \tag{4}$$

where

$$\begin{aligned} \sigma &= \sum_{\ell\in\mathcal{L}} \sum_{t=0}^{T} \sum_{u\in\widetilde{\mathcal{I}}} \sum_{s_1,s_2\in\mathcal{S}} \chi(u+s_1+t\ell)\overline{\chi}(u+s_2+t\ell) \\ &= \sum_{u\in\widetilde{\mathcal{I}}} \sum_{\ell\in\mathcal{L}} \sum_{s_1,s_2\in\mathcal{S}} \sum_{t=0}^{T} \chi\left(\frac{u+s_1}{\ell}+t\right)\overline{\chi}\left(\frac{u+s_2}{\ell}+t\right). \end{aligned}$$

Furthermore,

$$\sigma = \sum_{x,y\in\mathbb{F}_p} W(x,y) \sum_{t=0}^{T} \chi\left(x+t\right)\overline{\chi}\left(y+t\right),$$

where $W(x, y)$ is defined by (3).

Therefore, for any integer $\nu \ge 1$ by the Hölder inequality, we have

$$\begin{aligned} \sigma^{2\nu} \le \sum_{x,y\in\mathbb{F}_p} W(x,y)^2 &\left(\sum_{x,y\in\mathbb{F}_p} W(x,y)\right)^{2\nu-2} \\ &\sum_{x,y\in\mathbb{F}_p} \left|\sum_{t=0}^{T} \chi\left(x+t\right)\overline{\chi}\left(y+t\right)\right|^{2\nu}. \end{aligned} \tag{5}$$

Clearly,

$$\sum_{x,y\in\mathbb{F}_p} W(x,y) \ll \#\mathcal{I}\#\mathcal{L}\left(\#\mathcal{S}\right)^2 \ll (\#S)^2 hL. \tag{6}$$

We also have

$$\sum_{x,y\in\mathbb{F}_p}\left|\sum_{t=0}^{T}\chi(x+t)\overline{\chi}(y+t)\right|^{2\nu} = \sum_{t_1,\ldots,t_{2\nu}=0}^{T}\left|\sum_{x\in\mathbb{F}_p}\prod_{i=1}^{\nu}\chi(x+t_i)\prod_{i=\nu+1}^{2\nu}\overline{\chi}(x+t_i)\right|^2.$$

Using the Weil bound in the form of Lemma 4 if $(t_1,\ldots,t_\nu)$ is not a permutation of $(t_{\nu+1},\ldots,t_{2\nu})$, and the trivial bound otherwise, we derive

$$\sum_{x,y\in\mathbb{F}_p}\left|\sum_{t=0}^{T}\chi(x+t)\overline{\chi}(y+t)\right|^{2\nu} \ll T^{2\nu}p+T^{\nu}p^2$$

(see also [10, Lemma 12.8] that underlies the Burgess method). Taking ν to be large enough so that $T^{2\nu}p > T^{\nu}p^2$ we obtain

$$\sum_{x,y\in\mathbb{F}_p}\left|\sum_{t=0}^{T}\chi(x+t)\overline{\chi}(y+t)\right|^{2\nu} \ll T^{2\nu}p. \tag{7}$$

Substituting (6) and (7) in (5) we obtain

$$\sigma^{2\nu} \ll T^{2\nu}p\left((\#S)^2hL\right)^{2\nu-2}\sum_{x,y\in\mathbb{F}_p}W(x,y)^2.$$

We now apply Lemma 3 to derive

$$\begin{aligned}\sigma^{2\nu} &\ll T^{2\nu}p\left((\#S)^2hL\right)^{2\nu-2}\left((\#S)^3(hL)^2p^{-1}+(\#S)^2hLp^{o(1)}\right)\\ &\ll T^{2\nu}p^{1+o(1)}\left((\#S)^2hL\right)^{2\nu}\left((\#\mathcal{S})^{-1}p^{-1}+(\#S)^{-2}h^{-1}L^{-1}\right).\end{aligned}\tag{8}$$

Taking a sufficiently small $\varepsilon>0$, we obtain

$$(\#S)^2hL > p^{1+\delta}$$

which together with (4) concludes the proof. □

3. Root finding algorithms

3.1. **Finding all roots.** Here we address the question of finding all roots of a polynomial $f\in\mathbb{F}_p[X]$.

We refer to [8] for a description of efficient (in particular, polynomial time) algorithms of polynomial arithmetic over finite fields such as multiplication, division with remainder and computing the greatest common divisor.

Theorem 6. *There is a deterministic algorithm that, given a squarefree polynomial $f\in\mathbb{F}_p[X]$ of degree n that fully splits over $\mathbb{F}_p$, finds all roots of f in time $np^{1/2+o(1)}$.*

Proof. We set

$$h=\left\lfloor p^{1/2}(\log p)^2\right\rfloor.$$

We now compute the polynomials

$$g_u(X)=\gcd\left(f(X),(X+u)^{(p-1)/2}-1\right),\quad u=0,\ldots,h. \tag{9}$$

We remark that to compute the greatest common divisor in (9) we first use repeated squaring to compute the residue

$$H_u(X) \equiv (X+u)^{(p-1)/2} \pmod{f(X)}, \qquad \deg H_u < n,$$

and then compute

$$g_u(X) = \gcd\left(f(X), H_u(X)\right).$$

If $a \in \mathbb{F}_p$ is a root of f, then $(X-a) \mid g_u(X)$ if and only if $a+u \neq 0$ and $a+u$ is a quadratic residue in $\mathbb{F}_p$.

We now note that the Weil bound on incomplete character sums implies that for any two roots $a, b \in \mathbb{F}_p$ of f there is $u \in [0,h]$ such that

$$(X-a) \mid g_u(X) \qquad \text{and} \qquad (X-b) \nmid g_u(X). \tag{10}$$

Note that the argument of [16, Theorem 1.1] shows that one can take $h = \left\lfloor Cp^{1/2} \right\rfloor$ for some absolute constant $C > 0$ just by getting some minor speed up for this and the original algorithm of Shoup [15].

We now recall the factor refinement algorithm of Bernstein [2] that, in particular, for any set of N polynomials $G_1, \ldots, G_N \in \mathbb{F}_p[X]$ of degree n over $\mathbb{F}_p$ in time $O(nNp^{o(1)})$ finds a set of relatively prime polynomials $H_1, \ldots, H_M \in \mathbb{F}_p[X]$ such that any polynomial G_i, $i = 1, \ldots, N$, is a product of powers of the polynomials $H_1, \ldots, H_M$. Applying this algorithm to the family of polynomials g_u, $u = 0, \ldots, h$, and recalling (10), we see that it outputs the set of polynomials with

$$\{H_1, \ldots, H_M\} = \{X - a \ : \ f(a) = 0\},$$

which concludes the proof. □

3.2. **Finding one root.**

Here we give an algorithm that finds one root of a polynomial over $\mathbb{F}_p$. It is easy to see that up to a logarithmic factor this problem is equivalent to a problem of finding any nontrivial factor of a polynomial.

Lemma 7. *There is a deterministic algorithm that, given a squarefree polynomial $f \in \mathbb{F}_p[X]$ of degree $n > 1$ that fully splits over $\mathbb{F}_p$, finds in time $(n + p^{1/2})p^{o(1)}$ a factor $g \mid f$ of degree $1 \leq \deg g < n$.*

Proof. It suffices to prove that for any $\delta > 0$ there is a desirable algorithm with running time at most $(n + p^{1/2})p^{\delta + o(1)}$. If $n \leq p^{\delta}$, then the result follows from Theorem 6. Now assume that δ is small and $n > p^{\delta}$. Let

$$h = \left\lfloor (1 + n^{-1}p^{1/2})p^{\delta/2} \right\rfloor.$$

We start with computing the polynomials

$$\gcd\left(f(X), f(X+u)\right), \quad u = 1, \ldots, h; \tag{11}$$

see [8] for fast greatest common divisor algorithms. Clearly, if f has two distinct roots a and b with $|a - b| \leq h$, then one of the polynomials (11) gives a nontrivial factor of f. It is also easy to see that the complexity of this step is at most $nhp^{o(1)}$.

If this step does not produce any nontrivial factor of f, then we note that the set $\mathcal{S}$ of the roots of f is h-spaced. We now again compute the polynomials $g_u(X)$, given by (9), for every $u \in \mathcal{I}$.

So, we see that for the above choice of h the condition of Lemma 5 holds and implies that there is $u \in \mathcal{I}$ with

$$\left|\sum_{s\in\mathcal{S}} \left(\frac{s+u}{p}\right)\right| \ll \#\mathcal{S}p^{-\eta} = np^{-\eta},$$

for some $\eta > 0$ that depends only on δ, and thus the sequence of Legendre symbols $((s+u)/p)$, $s \in \mathcal{S}$, cannot be constant.

Therefore, at least one of the polynomials (9) gives a nontrivial factor of f. As in [15], we see that the complexity of this algorithm is again $O\left(nh(\log p)^{O(1)}\right)$. Since $\delta > 0$ is arbitrary, we obtain the desired result. □

Theorem 8. *There is a deterministic algorithm that, given a squarefree polynomial $f \in \mathbb{F}_p[X]$ of degree n that fully splits over $\mathbb{F}_p$, finds in time $(n + p^{1/2})p^{o(1)}$ a root of f.*

Proof. We use Lemma 7 to find a polynomial factor g_1 of f with $1 \le \deg g \le 0.5 \deg f$. Next, we find a polynomial factor g_2 of g_1 with $1 \le \deg g_2 \le 0.5 \deg g_1$, and so on. The number of iterations is $O(\log n)$, and the complexity of each iteration, by Lemma 7, does not exceed $(n + p^{1/2})p^{o(1)}$. This completes the proof. □

4. Comments

It is certainly natural to expect that the condition of Lemma 5 can be relaxed, however, proving such a result seems to be presently out of reach (even under the standard number theoretic conjectures). Furthermore, such an improvement does not immediately propagate into improvements of Theorems 6 and 8. It seems that within the method of Shoup [15] the only plausible way to reduce the complexity below $p^{1/2}$ is to obtain nontrivial bounds of single sums of Legendre symbols

$$\left|\sum_{x=1}^{H} \left(\frac{(x+s_1)(x+s_2)}{p}\right)\right| \le Hp^{-\eta}$$

for intervals of length $H \ge p^\alpha$ with some fixed $\alpha < 1/2$, uniformly over $s_1, s_2 \in \mathbb{F}_p$, $s_1 \ne s_2$. It seems that even the Generalised Riemann Hypothesis (GRH) does not immediately imply such a statement. In fact, even in the case of linear polynomials, it is not known how to use the GRH to get an improvement of the Burgess bound [5, 6] (for intervals away from the origin).

Acknowledgements

The authors are grateful to Andrew Sutherland for patient explanations of several issues related to Hilbert class polynomials.

The research of J. B. was supported by National Science Foundation Grant DMS-0808042, that of S. V. K. by Russian Fund for Basic Research Grant N. 14-01-00332, and Program Supporting Leading Scientific Schools Grant Nsh-3082.2014.1, and that of I. E. S. by Australian Research Council Grant DP130100237.

References

[1] E. R. Berlekamp, *Factoring polynomials over large finite fields*, Math. Comp. **24** (1970), 713–735. MR0276200 (43 #1948)

[2] D. J. Bernstein, *Factoring into coprimes in essentially linear time*, J. Algorithms **54** (2005), no. 1, 1–30, DOI 10.1016/j.jalgor.2004.04.009. MR2108417 (2006e:68058)

[3] J. Bourgain, *Sum-product theorems and applications*, Additive number theory, Springer, New York, 2010, pp. 9–38, DOI 10.1007/978-0-387-68361-4_2. MR2744741 (2012c:11164)

[4] J. Bourgain, M. Z. Garaev, S. V. Konyagin, and I. E. Shparlinski, *On the hidden shifted power problem*, SIAM J. Comput. **41** (2012), no. 6, 1524–1557, DOI 10.1137/110850414. MR3023803

[5] D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika **4** (1957), 106–112. MR0093504 (20 #28)

[6] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. (3) **12** (1962), 179–192. MR0132732 (24 #A2569)

[7] M.-C. Chang, *On a question of Davenport and Lewis and new character sum bounds in finite fields*, Duke Math. J. **145** (2008), no. 3, 409–442, DOI 10.1215/00127094-2008-056. MR2462111 (2009i:11099)

[8] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, 3rd ed., Cambridge University Press, Cambridge, 2013. MR3087522

[9] J. von zur Gathen and V. Shoup, *Computing Frobenius maps and factoring polynomials*, Comput. Complexity **2** (1992), no. 3, 187–224, DOI 10.1007/BF01272074. MR1220071 (94d:12011)

[10] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004. MR2061214 (2005h:11005)

[11] E. Kaltofen and V. Shoup, *Subquadratic-time factoring of polynomials over finite fields*, Math. Comp. **67** (1998), no. 223, 1179–1197, DOI 10.1090/S0025-5718-98-00944-2. MR1459389 (99m:68097)

[12] K. S. Kedlaya and C. Umans, *Fast polynomial factorization and modular composition*, SIAM J. Comput. **40** (2011), no. 6, 1767–1802, DOI 10.1137/08073408X. MR2863194

[13] H. L. Montgomery, *Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis*, CBMS Regional Conference Series in Mathematics, vol. 84, Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1994. MR1297543 (96i:11002)

[14] X. Shao, *Character sums over unions of intervals*, Forum Math., (to appear).

[15] V. Shoup, *On the deterministic complexity of factoring polynomials over finite fields*, Inform. Process. Lett. **33** (1990), no. 5, 261–267, DOI 10.1016/0020-0190(90)90195-4. MR1049276 (91f:11088)

[16] I. E. Shparlinski, *Finite Fields: Theory and Computation*: *The meeting point of number theory, computer science, coding theory and cryptography*, Mathematics and its Applications, vol. 477, Kluwer Academic Publishers, Dordrecht, 1999. MR1745660 (2001g:11188)

[17] A. V. Sutherland, *Computing Hilbert class polynomials with the Chinese remainder theorem*, Math. Comp. **80** (2011), no. 273, 501–538, DOI 10.1090/S0025-5718-2010-02373-7. MR2728992 (2011k:11177)

[18] A. V. Sutherland, *Accelerating the CM method*, LMS J. Comput. Math. **15** (2012), 172–204, DOI 10.1112/S1461157012001015. MR2970725

Institute for Advanced Study, Princeton, New Jersey 08540
E-mail address: bourgain@ias.edu

Steklov Mathematical Institute, 8, Gubkin Street, Moscow, 119991, Russia
E-mail address: konyagin@mi.ras.ru

Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia
E-mail address: igor.shparlinski@unsw.edu.au