Algorithmica
DOI 10.1007/s00453-016-0273-1

Polynomial Interpolation and Identity Testing from High Powers Over Finite Fields

Gábor Ivanyos[1] · Marek Karpinski[2] · Miklos Santha[3,4] · Nitin Saxena[5] · Igor E. Shparlinski[6]

Received: 24 February 2015 / Accepted: 23 December 2016

Abstract We consider the problem of recovering (that is, interpolating) and identity testing of a "hidden" monic polynomial f, given an oracle access to $f(x)^e$ for $x \in \mathbb{F}_q$, where $\mathbb{F}_q$ is finite field of q elements (extension fields access is not permitted). The naive interpolation algorithm needs $O(e \deg f)$ queries and thus requires $e \deg f < q$. We design algorithms that are asymptotically better in certain cases; requiring only $e^{o(1)}$ queries to the oracle. In the randomized (and quantum) setting, we give a substantially better interpolation algorithm, that requires only $O(\deg f \log q)$ queries. Such results have been known before only for the special case of a linear f, called

✉ Igor E. Shparlinski
igor.shparlinski@unsw.edu.au

Gábor Ivanyos
gabor.ivanyos@sztaki.mta.hu

Marek Karpinski
marek@cs.uni-bonn.de

Miklos Santha
santha@irif.fr

Nitin Saxena
nitin@cse.iitk.ac.in

1 Institute for Computer Science and Control, Hungarian Academy of Sciences, Budapest 1111, Hungary

2 Department of Computer Science, Bonn University, 53113 Bonn, Germany

3 CNRS, Université Paris Diderot, 75013 Paris, France

4 CQT, National University of Singapore, Singapore 117543, Singapore

5 Department of Computer Science and Engineering, Indian Institute of Technology, Kanpur, UP 208016, India

6 Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia

Published online: 05 January 2017

the *hidden shifted power* problem. We use techniques from algebra, such as effective versions of Hilbert's Nullstellensatz, and analytic number theory, such as results on the distribution of rational functions in subgroups and character sum estimates.

Keywords Hidden polynomial power · Black-box interpolation · Nullstellensatz · Rational function · Deterministic algorithm · Randomised algorithm · Quantum algorithm

Mathematics Subject Classification 11T06 · 11Y16 · 68Q12 · 68Q25

1 Introduction

1.1 Background and Previous Results

Let $\mathbb{F}_q$ be the finite field of q elements. Here we consider several problems of recovering and identity testing of a "hidden" monic polynomial $f \in \mathbb{F}_q[X]$, given $\mathfrak{O}_{e,f}$ an oracle that on every input $x \in \mathbb{F}_q$ outputs $\mathfrak{O}_{e,f}(x) = f(x)^e$ for some large positive integer $e \mid q-1$.

More precisely, we consider the following problem *Interpolation from Powers*:

given an oracle $\mathfrak{O}_{e,f}$ for some unknown monic polynomial $f \in \mathbb{F}_q[X]$, recover f.

We also consider the following two versions of the *Identity Testing from Powers*:

given an oracle $\mathfrak{O}_{e,f}$ for some unknown monic polynomial $f \in \mathbb{F}_q[X]$ and another known polynomial $g \in \mathbb{F}_q[X]$, decide whether $f = g$,

and

given two oracles $\mathfrak{O}_{e,f}$ and $\mathfrak{O}_{e,g}$ for some unknown monic polynomials $f, g \in \mathbb{F}_q[X]$, decide whether $f = g$.

In particular, for a linear polynomial $f(X) = X + s$, with a 'hidden' $s \in \mathbb{F}_q$, we denote $\mathfrak{O}_{e,f} = \mathcal{O}_{e,s}$. We remark that in this case there are two naive algorithms that work for linear polynomials:

- One can query $\mathcal{O}_{e,s}$ at $e+1$ arbitrary points and then using a fast interpolation algorithm, see [25], get a deterministic algorithm of complexity $e(\log q)^{O(1)}$ (as in [25], we measure the complexity of an algorithm by the number of bit operations in the standard RAM model).
- For probabilistic testing one can query $\mathcal{O}_{e,s}$ (and $\mathcal{O}_{e,t}$) at randomly chosen elements $x \in \mathbb{F}_q$ until the desired level of confidence is achieved (note that the equation $(x+s)^e = (x+t)^e$ has at most e solutions $x \in \mathbb{F}_q$).

These naive algorithms have been improved by Bourgain, Garaev, Konyagin and Shparlinski [5] in several cases (with respect to both the time complexity and the number of queries).

For non-linear monic polynomials $f \in \mathbb{F}_p[X]$ and a prime p, some classical and quantum algorithms for polynomial interpolation, given an oracle oracles $\mathfrak{O}_{e,f}$, with

$e = (p-1)/2$, have been presented by Russell and Shparlinski [16]. We remark that querring $\mathfrak{O}_{(p-1)/2,f}$, is equivalent to asking for the quadratic character of $f(x)$. In particular, by [16, Theorem 6], for a fixed d and a sufficiently large prime p, given such an oracle, one can reconstruct a monic polynomial f of degree d in time $p^{d+o(1)}$. Note that the search space is of size $O(p^{d+o(1)})$ and a naive application of the Weil bound leads to an algorithm that runs in time $p^{d+1/2+o(1)}$, see the discussion in [16, Section 1]. It is also shown in [16, Theorem 6] that the quantum query complexity is at most cd for an absolute constant c, however no nontrivial quantum complexity bounds are known for non-linear polynomials. On the other hand, for linear polynomials $X+s$, Dam, Hallgren and Ip [24] provide a quantum polynomial time algorithm to find s, see also [23].

The above questions appear naturally in understanding the pseudorandomness of the *Legendre symbol* $\left(\frac{f(x)}{p}\right)$. In particular, this has applications in the cryptanalysis of certain homomorphic cryptosystems. See [2,3,9,15] for further details.

1.2 New Results

Here we concentrate on the case of small and medium values of e (in particular, this is different from the scenario of [16]) and consider both classical and quantum algorithms. In particular, we extend the results of [5, Section 3.3] to arbitrary monic polynomials $f \in \mathbb{F}_p[X]$ for a prime p. These deterministic algorithms are very simple are based on a straightforward search. The proofs of correctness are however more difficult. They are based on quite involved estimates on the size of the product sets and subgroups generated by samples of values of rational functions on several consecutive integers.

In Sect. 4 we also indicate how one can obtain similar results in the case finite fields of small characteristic. However the case of arbitrary finite fields remains open.

We also observe that the above naive interpolation and random sampling algorithms both fail if $e \deg f > q$. Indeed, note that queries from an extension field are not permitted, and $\mathbb{F}_q$ may not have enough elements to make these algorithms correct.

Further, we also consider quantum and randomised algorithms. We emphasise that in the case of quantum algorithms, our setting is quite different from those of [16, 23,24] as we do not assume that the values of f are given by a quantum oracle, rather the algorithm works with the classical oracle $\mathfrak{O}_{e,f}$. These algorithms are based on that initially we query the oracle for a sufficiently large set of points and then combine a quantum or classical search over all the eth roots of the returned values with interpolation. We also discuss the possibility of derandomisation in Sect. 3.5.

Note that the above questions are closely related to the general problem of oracle (also sometimes called "black-box") polynomial interpolation and identity testing for arbitrary polynomials (though forbidding the use of extensions of the ground field makes the problems harder), see [17,18,22] and the references therein.

1.3 Notation

Throughout the paper, any implied constants in the symbols O, $\ll$ and $\gg$ may occasionally, where obvious, depend on the degree d of the polynomial f (and, occa-

sionally, on an integer parameter ν which appears in our arguments), and are absolute otherwise. We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that the inequality $|U| \le cV$ holds with some constant $c > 0$.

2 Identity Testing on Classical Computers

2.1 Main Results

Here we consider the identity testing case of two unknown *monic* polynomials $f, g \in \mathbb{F}_q[X]$ of degree d given the oracles $\mathfrak{O}_{e,f}$ and $\mathfrak{O}_{e,g}$. We remark that if f/g is an $(q-1)/e$-th power of a nonconstant rational function over $\mathbb{F}_q$ then it is impossible to distinguish between f and g from the oracles $\mathfrak{O}_{e,f}$ and $\mathfrak{O}_{e,g}$. We write $f \sim_e g$ in this case, and $f \nsim_e g$ otherwise.

We note that it is shown in the proof of [16, Theorem 6] that the Weil bound of multiplicative character sums (see [13, Theorem 11.23]) implies that given two oracles $\mathfrak{O}_{e,f}$ and $\mathfrak{O}_{e,g}$ for some unknown monic polynomials $f, g \in \mathbb{F}_q[X]$ with $f \nsim_e g$ one can decide whether $f = g$ in time $q^{1/2+o(1)}$. Note that the result of [16] is stated only for prime fields $\mathbb{F}_p$ but it can be extended to arbitrary fields at the cost of only typographical changes. The same holds for the results of Sect. 3 but the results of Sect. 2 hold only for prime fields.

For "small" values of e, over prime fields $\mathbb{F}_p$, we have a stronger result.

Theorem 1 (Small e) *For a prime p and a positive integer $e \mid p-1$, with $e \le p^{\delta}$ for some fixed $\delta > 0$, given two oracles $\mathfrak{O}_{e,f}$ and $\mathfrak{O}_{e,g}$ for some unknown monic polynomials $f, g \in \mathbb{F}_p[X]$ of degree d with $f \nsim_e g$, there is a deterministic algorithm to decide whether $f = g$ in at most $e^{c_0 \delta^{1/(2d)}}$ queries to the oracles $\mathfrak{O}_{e,f}$ and $\mathfrak{O}_{e,g}$, where c_0 is an absolute constant.*

We note that taking $d = 1$ in Theorem 1 we obtain a stronger version of [5, Theorem 51] with $\delta^{1/2}$ instead of $\delta^{1/3}$. This is due to the use of a stronger version of Hilbert's Nullstellensatz given by D'Andrea et al. [10], see Lemma 3 below.

For intermediate values of e, the following result complements both Theorem 1 and the result of [16]. We, however, have to assume that the polynomials f and g are *irreducible*.

Theorem 2 (Medium e) *For a prime p and a positive integer $e \mid p-1$, with $e \le p^{\eta-\delta}$ for some fixed $\delta > 0$, given two oracles $\mathfrak{O}_{e,f}$ and $\mathfrak{O}_{e,g}$ for some unknown monic irreducible polynomials $f, g \in \mathbb{F}_p[X]$ of degree $d \ge 1$ with $f \nsim_e g$, there is a deterministic algorithm to decide whether $f = g$ in at most $e^{\kappa+\delta}$ queries to the oracles $\mathfrak{O}_{e,f}$ and $\mathfrak{O}_{e,g}$, where*

$$\eta = \frac{4d-1}{4d^2(d+1)^2} \quad \text{and} \quad \kappa = \frac{2d}{4d-1}.$$

The proofs of Theorems 1 and 2 are given below in Sects. 2.5 and 2.6, respectively. The underlying algorithms are quite simple and based on querring the oracles $\mathfrak{O}_{e,f}$

and $\mathfrak{O}_{e,g}$ on a short sequences of consecutive elements $x = 1, \ldots, h$ and comparing the outputs.

In particular, we see from Theorem 1 that for a fixed d and $e \to \infty$ if $e = p^{o(1)}$ then we can test whether $f = g$ in time $e^{o(1)}(\log p)^{O(1)}$ in $e^{o(1)}$ oracle calls.

2.2 Background from Arithmetic Algebraic Geometry

Our argument makes use of a slight modification of [5, Lemma 23]. It is based on a quantitative version of effective Hilbert's Nullstellensatz given by D'Andrea et al. [10], which improved the previous estimates due to Krick, Pardo and Sombra [14].

As usual, we define the *logarithmic height* of a nonzero polynomial $P \in \mathbb{Z}[Z_1, \ldots, Z_n]$ as the maximum natural logarithm of the largest (by absolute value) coefficient of P.

The next statement is a simplified form of [10, Theorem 2].

Lemma 3 *Let $P_1, \ldots, P_N \in \mathbb{Z}[Z_1, \ldots, Z_n]$ be $N \geq 2$ polynomials in n variables of degree at most $D \geq 3$ and of logarithmic height at most H and let $R \in \mathbb{Z}[Z_1, \ldots, Z_n]$ be a polynomial in n variables of degree at most $d \geq 3$ and of logarithmic height at most h such that R vanishes on the variety*

$$P_1(Z_1, \ldots, Z_n) = \ldots = P_N(Z_1, \ldots, Z_n) = 0.$$

There are polynomials $Q_1, \ldots, Q_N \in \mathbb{Z}[Z_1, \ldots, Z_n]$ and positive integers A and r with

$$\log A \leq 2(n+1)dD^n H + 3D^{n+1}h + C(d, D, n, N),$$

such that

$$P_1 Q_1 + \ldots + P_N Q_N = AR^r,$$

where $C(d, D, n, N)$ depends only on d, D, n and N.

We now define the logarithmic height of an algebraic number $\alpha \neq 0$ as the logarithmic height of its minimal polynomial.

We need a slightly more general form of a result of Chang [6]. In fact, this is exactly the statement that is established in the proof of [6, Lemma 2.14], see [6, Equation (2.15)].

Lemma 4 *Let $P_1, \ldots, P_N, R \in \mathbb{Z}[Z_1, \ldots, Z_n]$ be $N + 1 \geq 2$ polynomials in n variables of degree at most D and of logarithmic height at most $H \geq 1$. If the zero-set*

$$P_1(Z_1, \ldots, Z_n) = \ldots = P_N(Z_1, \ldots, Z_n) = 0 \quad \text{and} \quad R(Z_1, \ldots, Z_n) \neq 0$$

is not empty then it has a point $(\beta_1, \ldots, \beta_n)$ in an extension $\mathbb{K}$ of $\mathbb{Q}$ of degree $[\mathbb{K} : \mathbb{Q}] \leq C_1(D, n)$ such that its logarithmic height is at most $C_2(D, n, N)H$, where $C_1(D, n)$ depends only on D, n and $C_2(D, n, N)$ depends only on D, n and N.

2.3 Product Sets in Number Fields

For a set $\mathcal{A}$ in an arbitrary semi-group, we use $\mathcal{A}^{(\nu)}$ to denote the *ν-fold product set*, that is

$$\mathcal{A}^{(\nu)} = \{a_1 \dots a_\nu \ : \ a_1, \dots, a_\nu \in \mathcal{A}\}.$$

We recall the following result given in [5, Lemma 29] (see also [4, Corollary 3] for the case of field of rational numbers).

Lemma 5 *Let $\mathbb{K}$ be a finite extension of $\mathbb{Q}$ of degree $D = [\mathbb{K} : \mathbb{Q}]$. Let $\mathcal{C} \subseteq \mathbb{K}$ be a finite set with elements of logarithmic height at most $H \geq 2$. Then we have*

$$\#\mathcal{C}^{(\nu)} > \exp\left(-c(D, \nu)\frac{H}{\sqrt{\log H}}\right)(\#\mathcal{C})^\nu,$$

where $c(D, \nu)$ depends only on D and ν.

2.4 Product Sets of Consecutive Values of Rational Functions in Prime Fields

We now show that for a nontrivial rational function $f/g \in \mathbb{F}_p(X)$ and an integer $h \geq 1$, the set formed by h consecutive values of f/g cannot be all inside a small multiplicative subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$. For the linear fractional function $(X + s)/(X + t)$ this has been obtained in [5, Lemma 35] (see also [21, Theorem 6]).

Lemma 6 *There is a absolute constant $c > 0$ such that if for some fixed integer such that if for some fixed integer $\nu \geq 1$, sufficiently large positive integer h and prime p we have*

$$h < p^{(c/\nu)^{2d+1}},$$

then the following holds. For any two distinct monic polynomials $f, g \in \mathbb{F}_p[X]$ of degree d for the set

$$\mathcal{A} = \left\{\frac{f(x)}{g(x)} \ : \ 1 \leq x \leq h\right\} \subseteq \mathbb{F}_p.$$

we have

$$\#\mathcal{A}^{(\nu)} > \exp\left(-c(d, \nu)\frac{\log h}{\sqrt{\log\log h}}\right)h^\nu,$$

where $c(d, \nu)$ depends only on ν and d.

Proof We closely follow the proof of [5, Lemma 35]. Let

$$f(X) = X^d + \sum_{k=0}^{d-1} a_{d-k} x^k \quad \text{and} \quad g(X) = X^d + \sum_{\ell=0}^{d-1} b_{d-\ell} X^\ell.$$

The idea is to move from the finite field to a number field, where we are in a position to apply Lemma 5.

We consider the collection $\mathcal{P} \subseteq \mathbb{Z}[\mathbf{U}, \mathbf{V}]$, where

$$\mathbf{U} = (U_1, \ldots, U_d) \quad \text{and} \quad \mathbf{V} = (V_1, \ldots, V_d),$$

of polynomials

$$P_{\mathbf{x},\mathbf{y}}(\mathbf{U}, \mathbf{V}) = \prod_{i=1}^{\nu} \left(x_i^d + \sum_{k=0}^{d-1} U_{d-k} x_i^k \right) \left(y_i^d + \sum_{\ell=0}^{d-1} V_{d-\ell} y_i^\ell \right) - \prod_{i=1}^{\nu} \left(x_i^d + \sum_{\ell=0}^{d-1} V_{d-\ell} x_i^\ell \right) \left(y_i^d + \sum_{k=0}^{d-1} U_{d-k} y_i^k \right),$$

where $\mathbf{x} = (x_1, \ldots, x_\nu)$ and $\mathbf{y} = (y_1, \ldots, y_\nu)$ are integral vectors with entries in $\mathcal{I} = [1, h]$ and such that

$$P_{\mathbf{x},\mathbf{y}}(a_1, \ldots, a_d, b_1, \ldots, b_d) \equiv 0 \pmod{p}.$$

Note that

$$P_{\mathbf{x},\mathbf{y}}(a_1, \ldots, a_d, b_1, \ldots, b_d) \equiv \prod_{i=1}^{\nu} f(x_i) g(y_i) - \prod_{i=1}^{\nu} f(y_i) g(x_i) \pmod{p}.$$

Clearly if the polynomial $P_{\mathbf{x},\mathbf{y}}(\mathbf{U}, \mathbf{V})$ is identical to zero modulo p then, by the uniqueness of polynomial factorisation in the ring $\mathbb{F}_p[\mathbf{U}, \mathbf{V}]$, we see that for every $i = 1, \ldots, \nu$, for the linear form

$$L_{x_i}(\mathbf{U}) = x_i^d + U_{d-1} x_i^{d-1} + \cdots U_1 x_i + U_0$$

there should be an equal (over $\mathbb{F}_p$) linear form

$$L_{y_j}(\mathbf{U}) = y_j^d + U_{d-1} y_j^{d-1} + \cdots U_1 y_j + U_0$$

with some $j = 1, \ldots, \nu$. Hence, if $P_{\mathbf{x},\mathbf{y}}(\mathbf{U}, \mathbf{V})$ vanishes then $\mathbf{x}$ and $\mathbf{y}$ can be obtained from each other by a permutation of their components. Therefore, if $\mathcal{P}$ contains no non-zero polynomials then each value $\lambda \in \mathbb{F}_p$, given by the product

$$\lambda \equiv \prod_{i=1}^{\nu} f(x_i)/g(x_i) \pmod{p},$$

appears no more than $\nu!$ times. In turn this impleis that

$$\#\mathcal{A}^{(\nu)} \ge \frac{1}{\nu!}\,(\#\mathcal{A})^{\nu} \gg h^{\nu}.$$

Thus, we now assume that $\mathcal{P}$ contains non-zero polynomials.

Clearly, every polynomial $P(\mathbf{U}, \mathbf{V}) \in \mathcal{P}$ is of degree at most 2ν and of logarithmic height at most $c_1 \nu \log h$.

We take a family $\mathcal{P}_0$ containing the largest possible number

$$N \le (d+1)^{2\nu} - 1$$

of linearly independent polynomials $P_1, \ldots, P_N \in \mathcal{P}$, and consider the variety

$$\mathcal{V} : \{(\mathbf{U}, \mathbf{V}) \in \mathbb{C}^{2d} \ : \ P_1(\mathbf{U}, \mathbf{V}) = \ldots = P_N(\mathbf{U}, \mathbf{V}) = 0\}.$$

Clearly $\mathcal{V} \ne \emptyset$ as it contains the diagonal $\mathbf{U} = \mathbf{V}$.

We claim that $\mathcal{V}$ contains a point outside of the diagonal, that is, there is a point $(\boldsymbol{\beta}, \boldsymbol{\gamma})$ with $\boldsymbol{\beta}, \boldsymbol{\gamma} \in \mathbb{C}^d$ and $\boldsymbol{\beta} \ne \boldsymbol{\gamma}$.

Assume that $\mathcal{V}$ does not contain a point outside of the diagonal. Then for every $k = 1, \ldots, d$, the polynomial

$$R_k(U_1, \ldots, U_d, V_1, \ldots, V_d) = U_k - V_k$$

vanishes on $\mathcal{V}$.

Then by Lemma 3 we see that there are polynomials $Q_{k,1}, \ldots, Q_{k,N} \in \mathbb{Z}[\mathbf{U}, \mathbf{V}]$ and positive integers A_k and r_k with

$$\log A_k \le c_2 d (2\nu)^{2d+1} \log h \tag{1}$$

for some absolute constant c_2 (provided that h is large enough) and such that

$$P_1 Q_{k,1} + \cdots + P_N Q_{k,N} = A_k (U_k - V_k)^{r_k}. \tag{2}$$

Since $f \ne g$, there is $k \in \{1, \ldots, d\}$ for which $a_k \not\equiv b_k \pmod p$. For this k we substitute

$$(\mathbf{U}, \mathbf{V}) = (a_1, \ldots, a_d, b_1, \ldots, b_d)$$

in (2). Recalling the definition of the set $\mathcal{P}$ we now derive that $p \mid A_k$ and thus $A_k \ge p$. Taking

$$c = \max_{d \ge 1} \left(\frac{1}{c_2 d 2^{2d+1} + 1} \right)^{1/(2d+1)}$$

in the condition of the lemma, we see from (1) that this is impossible.

Hence the set

$$\mathcal{U} = \mathcal{V} \cap [\mathbf{U} - \mathbf{V} \neq 0]$$

is nonempty. Applying Lemma 4 we see that it has a point $(\boldsymbol{\beta}, \boldsymbol{\gamma})$ with components of logarithmic height $O(\log h)$ in an extension $\mathbb{K}$ of $\mathbb{Q}$ of degree $[\mathbb{K} : \mathbb{Q}] \le \Delta(d, \nu)$, where $\Delta(d, \nu)$ depends only on d and ν.

Consider the maps $\Phi : \mathcal{I}^\nu \to \mathbb{F}_p$ given by

$$\Phi : \mathbf{x} = (x_1, \ldots, x_\nu) \mapsto \prod_{j=1}^{\nu} \frac{f(x_j)}{g(x_j)}$$

and $\Psi : \mathcal{I}^\nu \to \mathbb{K}$ given by

$$\Psi : \mathbf{x} = (x_1, \ldots, x_\nu) \mapsto \prod_{j=1}^{\nu} \frac{F_{\boldsymbol{\beta}}(x_j)}{G_{\boldsymbol{\gamma}}(x_j)},$$

where

$$F_{\boldsymbol{\beta}}(X) = X^d + \sum_{k=0}^{d-1} \beta_{d-k} x^k \qquad \text{and} \qquad G_{\boldsymbol{\gamma}}(X) = X^d + \sum_{\ell=0}^{d-1} \gamma_{d-\ell} X^\ell.$$

By construction of $(\boldsymbol{\beta}, \boldsymbol{\gamma})$ we have that $\Psi(\mathbf{x}) = \Psi(\mathbf{y})$ if $\Phi(\mathbf{x}) = \Phi(\mathbf{y})$. Hence

$$\#\mathcal{A}^{(\nu)} \ge \operatorname{Im}\Psi = \#\mathcal{C}^{(\nu)},$$

where $\operatorname{Im}\Psi$ is the image set of the map Ψ and

$$\mathcal{C} = \left\{ \frac{F_{\boldsymbol{\beta}}(x)}{G_{\boldsymbol{\gamma}}(x)} \ : \ 1 \le x \le h \right\} \subseteq \mathbb{K}.$$

Using Lemma 5, we derive the result. □

Given a rational function

$$\psi(X) = \frac{f(X)}{g(X)} \in \mathbb{F}_p(X)$$

where $f, g \in \mathbb{F}_p[X]$ are relatively prime polynomials, and a set $\mathcal{S} \subseteq \mathbb{F}_p$, we consider the value set

$$\psi(\mathcal{S}) = \{\psi(x) \ : \ x \in \mathcal{S}, \ g(x) \neq 0\}.$$

We also recall the following bound on the size of the interesection of an image of an interval under a rational map and a subgroup, which is given by [11, Theorem 7] (we also recall the definition of the symbol '$\ll$' given in Sect. 1.3).

Lemma 7 *Let $\psi(X) = f(X)/g(X)$ where $f, g \in \mathbb{F}_p[X]$ relatively prime polynomials of degree d and e respectively with $d + e \geq 1$. We define*

$$\ell = \min\{d, e\}, \qquad m = \max\{d, e\}$$

and set

$$k = (\ell + 1)\left(\ell m - \ell^2 + m^2 + m\right) \qquad \text{and} \qquad s = 2m\ell + 2m - \ell^2.$$

Assume that ψ is not a perfect power of another rational function over the algebraic closure of $\mathbb{F}_p$. Then for any interval $\mathcal{I}$ of h consecutive integers and a subgroup $\mathcal{G}$ of $\mathbb{F}_p^*$ of order T, we have

$$\#\left(\psi(\mathcal{I}) \cap \mathcal{G}\right) \ll (1 + h^{\rho} p^{-\vartheta}) h^{\tau + o(1)} T^{1/2},$$

where

$$\vartheta = \frac{1}{2s}, \qquad \rho = \frac{k}{2s}, \qquad \tau = \frac{1}{2(\ell + m)},$$

and the implied constant depends on d and e.

Note that for quadratic polynomials $\psi(X)$ (that is, $d = 2$ and $e = 0$) a bound which is better than that of Lemma 7 is given by [21, Theorem 7].

We now derive:

Lemma 8 *Suppose for two relatively prime monic polynomials $f, g \in \mathbb{F}_p[X]$ of degree $d \geq 1$, an interval $\mathcal{I}$ with positive integer h and a multiplicative subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ we have*

$$\psi(\mathcal{I}) \subseteq \mathcal{G},$$

where $\psi(X) = f(X)/g(X)$. Then

$$\#\mathcal{G} \gg \min\{h^{2(1-\tau)+o(1)}, h^{2(1-\rho-\tau)+o(1)} p^{2\vartheta}\},$$

where

$$\vartheta = \frac{1}{2d(d+2)}, \qquad \rho = \frac{(d+1)^2}{2(d+2)}, \qquad \tau = \frac{1}{4d},$$

and the implied constant depends on d.

Proof Since the result improves when d decreases, we can assume that $\psi(X)$ is not a perfect power of another rational function over the algebraic closure of $\mathbb{F}_p$.

By Lemma 7 applied with $d = e$ (and thus with $k = d(d+1)^2$, $s = d^2 + 2d$ and hence the above values of ϑ, ρ and τ), we have

$$h - d \le \#\psi(\mathcal{I}) = \#\left(\psi(\mathcal{I}) \cap \mathcal{G}\right) \le \left(1 + h^{\rho} p^{-\vartheta}\right) h^{\tau + o(1)} T^{1/2}$$

where $T = \#\mathcal{G}$ and the result follows. □

2.5 Proof of Theorem 1

We set

$$\nu = \left\lfloor \frac{c^{1+1/(2d)}}{(2\delta)^{1/(2d)}} \right\rfloor \qquad \text{and} \qquad h = \left\lfloor e^{2/\nu} \right\rfloor,$$

where c is the constant of Lemma 6. We note that

$$\frac{2\delta}{\nu} \le \left(\frac{c}{\nu}\right)^{2d+1}$$

so we have

$$h \le e^{2/\nu} \le p^{2\delta/\nu} \le p^{(c/\nu)^{2d+1}}. \tag{3}$$

We now query the oracles $\mathfrak{O}_{e,f}$ and $\mathfrak{O}_{e,g}$ for $x = 1, \ldots, h$.
If the oracles return two distinct values then clearly $f \ne g$. Now assume

$$f(x)^e = g(x)^e, \qquad x = 1, \ldots, h.$$

Therefore, the values $f(x)/g(x)$, $x = 1, \ldots, h$ belong to the subgroup $\mathcal{G}_e$ of $\mathbb{F}_p^*$ of order e. Hence for the set

$$\mathcal{A} = \left\{ \frac{f(x)}{g(x)} \ : \ 1 \le x \le h \right\} \subseteq \mathbb{F}_p \tag{4}$$

for any integer $\nu \ge 1$ we have

$$\mathcal{A}^{(\nu)} = \{a_1 \ldots a_\nu \ : \ a_1, \ldots, a_\nu \in \mathcal{A}\} \subseteq \mathcal{G}_e. \tag{5}$$

We see from (3) that Lemma 6 applies and yields $e \ge h^{\nu + o(1)}$, which contradicts (5) since we have $h^\nu > e^{2 + o(1)}$ as $e \to \infty$ for the above choice of the parameters. We also also note that with the above choice of ν we have $h \le e^{c_0 \delta^{1/(2d)}}$ for an absolute constant c_0. This concludes the proof.

2.6 Proof of Theorem 2

We define ϑ, ρ and τ as in Lemma 8.

We fix some $\varepsilon > 0$ and set

$$h = \left\lceil e^{(1+\varepsilon)/(2-2\tau)} \right\rceil.$$

We also note that for the above choice of h and for

$$e^{1+\varepsilon} \le e^{(1-\rho-\tau)(1+\varepsilon)/(1-\tau)} p^{\vartheta} \tag{6}$$

we have

$$\min\{h^{2(1-\tau)}, h^{2(1-\rho-\tau)} p^{2\vartheta}\} \ge e^{1+\varepsilon}.$$

Therefore, under the condition (6), we derive from Lemma 8 that for the set $\mathcal{A}$ given by (4) we have $\mathcal{A} \nsubseteq \mathcal{G}_e$. Proceeding as in the proof of Theorem 1, we obtain an algorithm that requires h queries.

Clearly, for the above choice of h, the condition (6) is satisfied if

$$e^{(1+\varepsilon)\rho/(1-\tau)} \le p^{\vartheta}. \tag{7}$$

Taking

$$\eta = \frac{\vartheta(1-\tau)}{\rho} \quad \text{and} \quad \kappa = \frac{1}{2-2\tau}$$

we see that the condition (7) is equivalent to $e \le p^{\eta/(1+\varepsilon)}$, under which we get an algorithm which requires $h = O\left(e^{(1+\varepsilon)\kappa}\right)$ queries. Since $\varepsilon > 0$ is arbitrary, the result now follows.

3 Quantum and Randomized Interpolation

3.1 Main Results

Here we present a quantum algorithm for the interpolation problem of finding an unknown monic polynomial $f \in \mathbb{F}_q[X]$ of degree d given the oracle $\mathfrak{O}_{e,f}$. We emphasise the difference between our settings where the oracle is classical and only the algorithm is quantum and the settings of [23,24] which employ the quantum analogue of the oracle $\mathfrak{O}_{e,f}$.

We recall that the oracle $\mathfrak{O}_{e,f}$ does not accept queries from field extensions of $\mathbb{F}_q$, and therefore, if $de > q$, we *cannot* interpolate f^e from queries to $\mathfrak{O}_{e,f}$.

Theorem 9 *Given an oracle $\mathfrak{O}_{e,f}$ for some unknown monic polynomial f of degree at most d, for any $\varepsilon > 0$ there is a quantum algorithm to find with probability $1-\varepsilon$ a polynomial g such that $g \sim_e f$ in time $e^{d/2}\,(d \log q \log(1/\varepsilon))^{O(1)}$ and $O\,(d \log q \log(1/\varepsilon))$ calls to $\mathfrak{O}_{e,f}$.*

Replacing quantum parts of the algorithm above with classical (randomized) methods, we obtain the following.

Theorem 10 *Given an oracle $\mathfrak{O}_{e,f}$ for some unknown monic polynomial f of degree at most d, for any $\varepsilon > 0$ there is a* randomized *algorithm to find with probability $1-\varepsilon$ a polynomial g such that $g \sim_e f$ in time $e^d\,(d\log q\log(1/\varepsilon))^{O(1)}$ and $O\,(d\log q\log(1/\varepsilon))$ calls to $\mathfrak{O}_{e,f}$.*

The proofs of Theorems 9 and 10 are given below in Sects. 3.3 and 3.4, respectively.

3.2 Coincidences Among *e*th Powers of Polynomials

The following result is immediate from the Weil bound on multiplicative character sums, see [13, Theorem 11.23].

Lemma 11 *Let $g_1, g_2 \in \mathbb{F}_q[X]$ be two monic polynomials of degree at most d with $g_1 \nsim_e g_2$. Then*

$$\#\{x \in \mathbb{F}_q \;:\; g_1(x)^e = g_2(x)^e\} = \frac{q}{e} + O(dq^{1/2}).$$

We now immediately conclude.

Corollary 12 *Let $g_1, g_2 \in \mathbb{F}_q[X]$ be two monic polynomials of degree $o(q^{1/2})$ with $g_1 \nsim_e g_2$. Then for any $e \le (q-1)/2$ and a sufficiently large q*

$$\#\{x \in \mathbb{F}_q \;:\; g_1(x)^e \neq g_2(x)^e\} \ge \frac{1}{3}q.$$

3.3 Proof of Theorem 9

Let $\mathcal{S}$ stand for the monic polynomials of degree at most d. By Corollary 12, a random choice of elements $x \in \mathbb{F}_q$ gives with probability at least 0.99 a set T of size $O(\log|\mathcal{S}|) = O(d\log q)$ such that for every pair $f, g \in \mathcal{S}$ we have $f(a)^e = g(a)^e$ for every $a \in T$ if and only if $f \sim_e g$.

We continue with picking d different elements $a_1, \ldots, a_d$ and use the oracle $\mathfrak{O}_{e,f}$ to obtain the values $b_j = f(a_j)^e$, $j = 1, \ldots, d$, as well as to get the values $b(a) = f(a)^e$ for every $a \in T$.

Using Shor's order finding and discrete logarithm algorithms [19] we can also compute a generator ζ_e for the multiplicative subgroup $\{u \in \mathbb{F}_q : u^e = 1\}$ and for every j an element $z_j \in \mathbb{F}_q$ such that $z_j^e = b_j$.

The cost of the steps performed so far is polynomial in $\log q$ and d. Let $E = \{0, \ldots, e-1\}$. For a tuple $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d)$ from E^d, let $f_{\boldsymbol{\alpha}}$ be the monic polynomial of degree at most d such that $f_{\boldsymbol{\alpha}}(a_j) = z_j\zeta_e^{\alpha_j}$, $j = 1, \ldots, d$. For any specific tuple α, the polynomial $f_{\boldsymbol{\alpha}}$ can be computed by simple interpolation in time polynomial in $d\log q$.

We use Grover's search [12] over E^d to find a tuple $\boldsymbol{\alpha}$ with probablity at least 0.99 such that $f_{\boldsymbol{\alpha}}^e(a) = b(a)$ for every $a \in T$. The cost of this part is bounded by $O(e^{d/2})$ times a polynomial in $\log q$ and d. Repeating the whole procedure $O(\log(1/\varepsilon))$ times we achieve the desired probability level, which concludes the proof.

3.4 Proof of Theorem 10

Observe that a generator for the group $\{u \in \mathbb{F}_q : u^e = 1\}$ as well as elements z_j with $z_j^e = b_j$ can be found by simple classical algorithms of complexity bounded by $e^{1/2}(\log q)^{O(1)}$, that is, even within the complexity bound of Theorem 9. Indeed, assume that for every prime r diving e we have an element $g_r \in \mathbb{F}_q$ which is not an rth power of an $\mathbb{F}_q$ element. Such elements can be found in time $(\log q)^{O(1)}$ using random choices. The product of appropriate powers of the elements g_r is a generator for the group of the eth roots of unity.

For computing an eth roots of b_j it is sufficient to be able to take rth root of an arbitrary field element y for every prime divisor r of e. This task can be accomplished in time $\sqrt{r}(\log q)^{O(1)}$ as in the algorithm of Adleman, Manders and Miller [1] instead of the brute force one that uses Shanks' baby step-giant step method for computing discrete logarithms in groups of order r, see [8, Section 5.3].

Therefore, if we replace Grover's search [12] over E^d with a classical search we obtain a classical randomised algorithm of complexity $e^d(d \log q \log(1/\varepsilon))^{O(1)}$.

3.5 Further Remarks

Under Generalised Riemann Hypothesis we can derandomize the proof of Theorem 10. If $q = p$ is a prime then a generator for the group of eth roots of unity can be found in deterministic polynomial time. If, furthermore, $e \le p^{\delta}$ or $e \le p^{\eta-\delta}$ for some fixed $\delta > 0$, then we could use the test of Theorem 1 or Theorem 2 to obtain a deterministic algorithm of complexity $e^{d+c_0\delta^{1/(2d)}}(d \log p)^{O(1)}$ or $e^{d+\kappa+o(1)}(d \log p)^{O(1)}$, respectively.

4 Comments and Open Problems

It is very plausible that one can obtain analogues of Theorems 1 and 2 in the settings of high degree extensions of finite fields. More precisely, if $q = p^n$ for a fixed p and growing n, we write $\mathbb{F}_q \cong \mathbb{F}_p[X]/\langle\psi(X)\rangle$ for a fixed irreducible polynomial $\psi \in \mathbb{F}_p[X]$ of degree n. Then one can attempt to transfer the technique used in the proofs of Theorems 1 and 2 to this case where a role of a short interval of length h is now played by the set of polynomials of degree at most h. This approach has been used in [7,20] for several related problems. We also note that a version of effective Hilbert's Nullstellensatz for function fields, which is needed for this approach, has recently been given by D'Andrea et al. [10]. However working out concrete technical details may require some nontrivial efforts.

We remark that we do not know how to take any advantage of actually knowing g, and get stronger version of Theorems 1 and 2 in this case, like, for example, in [5, Section 3.2].

Acknowledgements The authors are very grateful to the referees for the very careful reading of the manuscipt which helped to remove some imprecisions and also improved the quality of the exposition. This research was supported in part by the Hungarian Scientific Research Fund (OTKA) Grant NK105645 (for G.I.); Singapore Ministry of Education and the National Research Foundation Tier 3 Grant MOE2012-T3-1-009 (for G.I. and M.S.); the Hausdorff Grant EXC-59 (for M.K.); European Commission IST STREP Project QALGO 600700 and the French ANR Blanc Program Contract ANR-12-BS02-005 (for M.S.); Research-I Foundation CSE and Hausdorff Center Bonn (for N.S.); the Australian Research Council Grant DP140100118 (for I.S.).

Compliance with Ethical Standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Adleman, L., Manders, K., Miller, G.: On taking roots in finite fields. In: 2013 IEEE 54th Annual Symposium on Foundations of Computer Science, IEEE, pp. 175–178 (1997)
2. Blum, M., Micali, S.: How to generate cryptographically strong sequences of pseudorandom bits. SIAM J. Comput. **13**(4), 850–864 (1984)
3. Boneh, D., Lipton, R.J.: Algorithms for black-box fields and their application to cryptography. In: Koblitz, N. (ed.) Advances in Cryptology CRYPTO 96, pp. 283–297. Springer, Berlin (1996)
4. Bourgain, J., Konyagin, S.V., Shparlinski, I.E.: Product sets of rationals, multiplicative translates of subgroups in residue rings, and fixed points of the discrete logarithm. Int. Math. Res. Not. **2008**, 1–29 (2008)
5. Bourgain, J., Garaev, M.Z., Konyagin, S.V., Shparlinski, I.E.: On the hidden shifted power problem. SIAM J. Comput. **41**(6), 1524–1557 (2012)
6. Chang, M.-C.: Factorization in generalized arithmetic progressions and application to the Erdős-Szemerédi sum-product problems. Geom. Funct. Anal. **13**(4), 720–736 (2003)
7. Cilleruelo, J., Shparlinski, I.: Concentration of points on curves in finite fields. Monatshefte Math. **171**(3–4), 315–327 (2013)
8. Crandall, R., Pomerance, C.: Prime numbers: a computational perspective. Springer, New York (2001)
9. Damgård, I.B.: On the randomness of legendre and jacobi sequences. In: Advances In: Goldwasser, S. (ed.) Cryptology CRYPTO 88, pp. 163–172. Springer, Berlin (1990)
10. D'Andrea, C., Krick, T., Sombra, M.: Heights of varieties in multiprojective spaces and arithmetic nullstellensätze. Ann. Sci. l'ENS **46**, 549–627 (2013)
11. Gómez-Pérez, D., Shparlinski, I.E.: Subgroups generated by rational functions in finite fields. Monat. Math. **176**, 241–253 (2015)
12. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing, pp. 212–219. ACM (1996)
13. Iwaniec, H., Kowalski, E.: Analytic Number Theory. American Mathematical Society, Providence (2004)
14. Krick, T., Pardo, L.T., Sombra, M.: Sharp estimates for the arithmetic nullstellensatz. Duke Math. J. **109**(3), 521–598 (2001)
15. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press, Boco Raton (2010)
16. Russell, A., Shparlinski, I.E.: Classical and quantum function reconstruction via character evaluation. J. Complex. **20**(2), 404–422 (2004)
17. Saxena, N.: Progress on polynomial identity testing. Bull. EATCS **99**, 49–79 (2009)
18. Saxena, N.: Progress on Polynomial Identity Testing - 2, Perspectives in Computational Complexity. Springer, Berlin (2014)

19. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997)
20. Shparlinski, I.E.: Products with variables from low-dimensional affine spaces and shifted power identity testing in finite fields. J. Symb. Comput. **64**, 35–41 (2014)
21. Shparlinski, I.E.: Polynomial values in small subgroups of finite fields. Rev. Mat. Iberoam. **32**, 1127–1136 (2016)
22. Shpilka, A., Yehudayoff, A.: Arithmetic circuits: a survey of recent results and open questions. Found. Trends Theor. Comput. Sci. **5**(3–4), 207–388 (2010)
23. van Dam, W.: Quantum algorithms for weighing matrices and quadratic residues. Algorithmica **34**(4), 413–428 (2002)
24. van Dam, W., Hallgren, S., Ip, L.: Quantum algorithms for some hidden shift problems. SIAM J. Comput. **36**(3), 763–778 (2006)
25. von zur Gathen, J., Gerhard, J.: Modern Computer Algebra. Cambridge University Press, Cambridge (2013)