Zero Testing of $p$-adic and Modular Polynomials

Marek Karpinski *  Alf van der Poorten †
Igor Shparlinski ‡

Abstract

We obtain new algorithms to test if a given multivariate polynomial over $p$-adic fields is identical to zero. We also consider zero testing of polynomials in residue rings. The results complement a series of known results about zero testing of polynomials over integers, rationals and finite fields.

*Dept. of Computer Science, University of Bonn, 53117 Bonn, and the International Computer Science Institute, Berkeley, California. Research supported by DFG Grant KA 673/4-1, and by the ESPRIT BR Grants 7097 and EC-US 030, by DIMACS, and by the Max-Planck Research Prize. Email: marek@cs.uni-bonn.de
†School of MPCE, Macquarie University, NSW 2109, Australia.
Email: alf@mpce.mq.edu.au
‡School of MPCE, Macquarie University, NSW 2109, Australia.
Email: igor@mpce.mq.edu.au
1 Introduction

One of the central questions of zero-testing of functions can be formulated as follows.

Assume that a function $f$ from some family of functions $\mathcal{F}$ is given by a black box $B$, that is for each point $x$ from the definition domain of $f$ entered into $B$ it computes the value of $f$ at this point. The task is to design an efficient algorithm testing if $f$ is identical to zero and using as little of calls of $B$ as possible.

In a number of papers this question was considered for polynomials, rational functions and algebraic functions belonging various families of functions over various algebraic domains [1, 2, 3, 4, 5, 6, 7, 8, 14, 16, 18], some additional references can be found in Section 4.4 of [15] and in Chapter 12 of [17].

In this paper we consider similar questions for multivariate polynomials over $p$-adic fields.

As usual $\mathbb{Q}_p$ denotes the $p$-adic completion of the field of rationals, and $\mathbb{C}_p$ the $p$-adic completion of its algebraic closure.

We normalize the additive valuation $\text{ord}_p t$ such that $\text{ord}_p p = 1$.

The ring of $p$-adic integers $\mathbb{Z}_p$ is the set

$$\mathbb{Z}_p = \{t \in \mathbb{Q}_p : \text{ord}_p t \geq 0\}.$$ 

We consider exponential polynomials of the class $\mathcal{P}_p(m, n)$ which consist of the multivariate polynomials of the shape

$$f(X_1, \ldots, X_m) = \sum_{i_1, \ldots, i_m = 0}^{n} a_{i_1, \ldots, i_m} X_1^{i_1} \ldots X_m^{i_m}$$

of degree at most $n$ over $\mathbb{C}_p$ with respect to each variable and such that either $f$ is identical to zero or

$$\min_{0 \leq i_1, \ldots, i_m \leq n} \text{ord}_p a_{i_1, \ldots, i_m} = 0.$$

Generally speaking, two different types of black boxes are possible.

We say that a multivariate polynomial (1) over a ring $R$ is given by an exact black box $B$ of the exact if for any point $x = (x_1, \ldots, x_m) \in R^m$ it outputs the exact value $B(x) = f(x)$ and it does it in time which does not depend on $x$. 

2
For zero testing over finite fields and rings black boxes of this type are quite natural but for infinite algebraic domains they are not.

For example for testing over \( \mathbb{Q}_p \) the following we consider the following weaker but more realistic black boxes.

We say that a multivariate polynomial \( f \) over \( \mathbb{Q}_p \) is given by an approximating black box \( \mathfrak{A} \) if for any point \( x = (x_1, \ldots, x_m) \in \mathbb{Z}_p^m \) and any integer \( k \geq 0 \) it computes a \( p \)-adic approximation \( \mathfrak{A}_k(x) \) to \( f(x) \) of order \( k \), that is

\[
\text{ord}_p \left( \mathfrak{A}_k(x) - f(x) \right) \geq k
\]

and does it in time \( T(k) \) depends on \( k \) polynomially, \( T(k) = k^{O(1)} \).

Informally, an approximating black box can make no miracles but just performs 'honest' computation, its only advantage is that it knows the polynomial \( f(x) \) explicitly.

Here we design a polynomial time algorithms of zero testing of polynomials of class \( \mathcal{P}_p(m, n) \) by using a black box of the aforementioned type. Sparse polynomials are considered as well. Using the Strassman theorem \([9]\) one can apply our result to zero testing of various analytic functions over \( p \)-adic fields, exponential polynomials of the form

\[
E(X) = \sum_{i=1}^{r} f_i(X) \varphi_i^2(X),
\]

where \( \varphi_i \in \mathbb{Q}_p, f_i(X) \in \mathbb{Q}_p[X], g_i(X) \in \mathbb{Z}[X] \), in particular.

The we consider polynomials \( f \) with coefficients from the residue ring \( \mathbb{Z}/M \) modulo an integer \( M \geq 2 \).

Our methods is based on some ideas of \([10, 11, 12, 13]\) related to \( p \)-adic Lagrange interpolation and estimating of \( p \)-adic orders of some determinants.

## 2 Zero Testing of \( p \)-adic Polynomials

Here we consider the case of general polynomials \( f \in \mathcal{P}_p(m, n) \). It is reasonable to accept the total number of coefficients \((n + 1)^m\) as the measure of the input-size of such polynomials.

We also assume that each polynomial \( f \in \mathcal{P}_p(m, n) \) is given by an approximating black box \( \mathfrak{A} \).
Theorem 1. A polynomial $f \in \mathcal{P}_p(m, n)$ can be zero tested within $N = (n+1)^m$ calls of an approximating black box $\mathfrak{B}_k$ with

$$k = \left\lfloor \frac{(n+1)^m}{p-1} \right\rfloor.$$ 

Proof. First of all we consider the case of univariate polynomials. We set $k = \lceil n/(p-1) \rceil$ and make $n+1$ calls $\mathfrak{B}_k(j)$, $j = 0, \ldots, n$. If $f \in \mathcal{P}_p(1, n)$ is identical to zero then obviously $\text{ord}_p \mathfrak{B}_k(j) \geq k$, $j = 0, \ldots, n$. We show that otherwise for at least one value of $j$ we have $\text{ord}_p \mathfrak{B}_k(j) < k$. Indeed, assuming that this is not true we obtain $\text{ord}_p f(j) \geq k$, $j = 0, \ldots, n$. Using the Lagrange interpolation we obtain

$$f(X) = \prod_{j=0}^{n} \frac{(X - i)}{\prod_{j \neq i}^{n} (j - i)} f(j).$$

Because for every $j = 0, \ldots, n$

$$\text{ord}_p \prod_{i=0}^{n} (j - i) \leq \text{ord}_p j! + \text{ord}_p (n - j)! \leq \frac{n}{p-1} < k$$

we see that all coefficients of $f$ have positive $p$-adic orders which contradicts our assumption $f \in \mathcal{P}_p(1, n)$. This finishes the proof of the theorem for $m = 1$. For $m \geq 2$ for a polynomial $f \in \mathcal{P}_p(m, n)$ we use the substitution

$$X_i = X^{(n+1)^{m-1}}, \nu = 1, \ldots, m$$

and consider the polynomial

$$f \left( X, X^{n+1}, \ldots, X^{(n+1)^{m-1}} \right) \in \mathcal{P}_p(1, (n+1)^m).$$

for which we apply the algorithm above. □

Now we consider a very important subclass $\mathcal{P}_p(m, n, t)$ of $t$-sparse polynomials $f \in \mathcal{P}_p(m, n)$ with at most $t$ non-zero coefficients. It is reasonable to accept the total number of non-zero coefficients times the bit-size of the coding the $m$ corresponding exponents $tm \log n$ as the measure of the input-size of such polynomials.
Theorem 2. A polynomial $f \in \mathcal{P}_p(m, n, t)$ can be zero tested within

$$N = \begin{cases} t, & \text{if } m = 1; \\ mt^3, & \text{if } m \geq 2; \end{cases}$$

calls of an approximating black box $\mathfrak{B}_k$ with

$$k = \begin{cases} \left\lfloor 0.5t^2 \log_p 4n \right\rfloor, & \text{if } m = 1; \\ \left\lfloor t^2 \log_p 8mnt \right\rfloor, & \text{if } m \geq 2. \end{cases}$$

Proof. As in the proof of Theorem 1, first of all we consider the case of univariate polynomials.

Let $g$ be a primitive root modulo $p$ and therefore modulo all power of $p$, if $p \geq 3$ and let $g = 5$ if $p = 2$. In any case the multiplicative order $\tau_s$ of $g$ modulo $p^s$ is at least

$$\tau_s \geq 0.25p^s$$

for any integer $s \geq 1$.

We set $k = \left\lfloor 0.5t^2 \log_p 4n \right\rfloor$ and make $t$ calls $\mathfrak{B}_k(g^j)$, $j = 0, \ldots, t - 1$.

If $f \in \mathcal{P}_p(1, n, t)$ is identical to zero then obviously $\text{ord}_p \mathfrak{B}_k(g^j) \geq k$, $j = 0, \ldots, t - 1$. We show that otherwise for at least one value of $j$ we have $\text{ord}_p \mathfrak{B}_k(g^j) < k$.

Indeed, assuming that this is not true we obtain $\text{ord}_p f(g^j) \geq k$, $j = 0, \ldots, t - 1$.

Let

$$f(X) = \sum_{i=1}^{t} A_i X^{r_i},$$

where $0 \leq r_1 < \ldots < r_t \leq n$. Recalling that

$$\min_{i \leq i \leq t} \text{ord}_p A_i = 0,$$

from the identities

$$\sum_{i=1}^{t} z_i g^{r_i} = f(g^j), \quad j = 0, \ldots, t - 1$$

and the Cramer rule we derive that

$$\text{ord}_p \Delta \geq \min_{0 \leq j \leq t-1} \text{ord}_p f(g^j) \geq k,$$ (4)
where $\Delta$ is the following determinant

$$ \Delta = \det \left( g^{(j-1)r_i} \right)_{i,j=1}^t. $$

Therefore

$$ \Delta = \prod_{1 \leq i < j \leq t} (g^{r_i} - g^{r_j}). $$

Because $g^{r_i} - g^{r_j} \in \mathbb{Z}$ its $p$-adic order is just the largest power $p^s$ of $p$ which divides this number. Therefore the multiplicative order $\tau_s$ of $g$ modulo $p^s$ divides $r_i - r_j$. Recalling the inequality (3) we obtain $0.25p^s \leq |r_i - r_j| \leq n$. Hence, obtain

$$ \text{ord}_p (g^{r_i} - g^{r_j}) \leq \log_p 4n, \quad 1 \leq i < j \leq t. $$

Finally we derive

$$ \text{ord}_p \Delta \leq 0.5t(t-1) \log_p 4n < k $$

which contradicts the inequality (4).

For $m \geq 2$ we use the reduction to the univariate case which for the first time was used in [6].

Let $l$ be the smallest prime number exceeding $mt(t-1)$. Obviously

$$ l \leq 2mt(t-1). $$

Integers $0 \leq c_{uv} \leq l - 1$ we define from the congruences

$$ c_{uv} \equiv \frac{1}{u + v} \pmod{l}, \quad u, v = 1, \ldots, (l - 1)/2. $$

The matrix

$$ C = (c_{ij})_{i,j=1}^{l-1} $$

is a Cauchy matrix which has the property that each its minor is non-singular modulo $l$, and therefore over integers. We claim that if $f$ is a non identical to zero polynomial then so is at least one of the polynomials

$$ f(X^{c_{v1}}, \ldots, X^{c_{vm}}), \quad v = 1, \ldots, (l - 1)/2. \quad (5) $$

Let

$$ f(X_1, \ldots, X_m) = \sum_{i=1}^t A_i X_1^{r_{i1}} \ldots X_m^{r_{mi}} $$

with some integers $r_{ij}$, $i = 1, \ldots, t$, $j = 1, \ldots, m$. We show that for at least one $j = 1, \ldots, l - 1$ the powers of the monomials appearing in the
polynomials (5) are pairwise different. Indeed, for each pair of distinct exponents \((r_{1i}, \ldots, r_{mi})\) and \((r_{1j}, \ldots, r_{mj})\), \(1 \leq i < j \leq t\), there are at most \(m - 1\) values of \(v = 1, \ldots, (l - 1)/2\) satisfying
\[
c_{1v}r_{1i} + \cdots + c_{mv}r_{mi} = c_{1v}r_{1j} + \cdots + c_{mv}r_{mj}. \tag{6}
\]
Therefore the total number of \(v = 1, \ldots, (l - 1)/2\) for which (6) happens for at least one pair of exponents is at most \(0.5(m - 1)t(t - 1) < (l - 1)/2\). Thus if \(f\) is not identical to zero then at least one of the polynomials (5) is not identical to zero polynomial of with at most \(t\) monomials and of degree at most \((l - 1)mn \leq 2m^2nt^2 \leq 2m^2n^2t^2\). Thus each of them can be tested within \(t\) calls of \(\mathcal{B}_k\) with \(k = \lceil t^2 \log_2 8mnt \rceil\) and the total number of calls is \(t(l - 1)/2 \leq mt^3\).

3 Zero Testing of Sparse \(p\)-adic Polynomials

Let \(\mathcal{Q}(M, m, n)\) denote the class of multivariate polynomials (1) with coefficients from \(\mathbb{Z}/M\) and such that either \(f\) is identical to zero in \(\mathbb{Z}/M\) or its coefficients are jointly relatively prime to \(M\).

We also assume that each polynomial \(f \in \mathcal{Q}(M, m, n)\) is given by an exact black box \(\mathcal{B}\).

We remark that as the polynomial
\[
f(X_1, \ldots, X_m) = \prod_{i=1}^{m} X_i(X_i - 1) \cdots (X_i - n + 1)
\]
shows there are non-zero polynomials of degree \(n\) which are identical to zero as functions modulo \(M = n!\). So one of the necessary conditions to make such zero testing possible is
\[
M \geq (n!)^m. \tag{7}
\]

We obtain an algorithm which works for such \(M\) if \(m = 1\) but unfortunately only for substantially large \(M\) if \(m \geq 1\).

**Theorem 3.** A polynomial \(f \in \mathcal{Q}(M, m, n)\) with \(M > ((n + 1)^m)!\) can be zero tested within \(N = (n + 1)^m\) calls of an approximating black box \(\mathcal{B}\).
Proof. First of all we consider the case of univariate polynomials. We make $n+1$ calls $B(j)$, $j = 0, \ldots, n$.

If $f \in \mathcal{Q}(M, 1, n)$ is identical to zero in $\mathbb{Z}/M$ then obviously $B(j) \equiv 0 \pmod{M}$, $j = 0, \ldots, n$. We show that otherwise for at least one value of $j$ we have $B(j) \not\equiv 0 \pmod{M}$.

Indeed, assuming that this is not true we obtain $f(j) \equiv 0 \pmod{M}$, $j = 0, \ldots, n$.

Using the Lagrange interpolation we obtain

$$f(X) \equiv \sum_{j=0}^{n} \frac{\prod_{i \neq j}^{n} (X - i)}{\prod_{i \neq j}^{n} (j - i)} f(j) \pmod{M}$$

Because for every $j = 0, \ldots, n$

$$\gcd\left(M, \prod_{i \neq j}^{n} (j - i)\right) = \gcd\left(M, j!(n-j)!\right) \mid \gcd(M, n!).$$

we see that all coefficients of $f$ are divisible by $M/\gcd(M, n!) > 1$ which finishes the proof of the theorem for $m = 1$.

For $m \geq 2$ for a polynomial $f \in \mathcal{P}_p(m, n)$ we use the substitution

$$X_i = X^{(n+1)^{\nu-1}}, \nu = 1, \ldots, m$$

and consider the polynomial

$$f\left(X, X^{n+1}, \ldots, X^{(n+1)^{m-1}}\right) \in \mathcal{P}_p(1, (n+1)^m).$$

for which we apply the algorithm above. \qed

4 Some Remarks and Further Applications

The Strassman’s theorem claim that if a function $F(X)$ is given by a power series

$$F(X) = \sum_{h=0}^{\infty} a_h X^h \in \mathbb{C}_p[[X]]$$

8
converging on some disk

\[ D = \{ x \in \mathbb{C}_p : \text{ord}_p x \geq \delta \} \]

with

\[ \min_{h=0,1,\ldots} \text{ord}_p a_h = 0 \]

and \( n \) is defined by

\[ n = \max \{ h : \text{ord}_p a_h = 0 \} \]

then

\[ F(X) = f(X)U(X) \]

where \( f(X) \in \mathbb{C}_p[X] \) is a polynomial of degree at most \( n \) and the power series \( U(X) \in \mathbb{C}_p[[X]] \) satisfies \( \text{ord}_p U(x) = 0 \) for all \( x \in D \).

Thus an estimate on the growth of coefficients of \( F(X) \) is known then one can bound \( M \) and then apply our results to zero testing of \( F \). In particular, for exponential polynomials (2 such a bound of \( n \) (under some additional conditions) can be found in [13] (see also [10, 12]).

We also remark that it would be interesting to obtain an algorithm of zero testing of \( t \)-sparse polynomials.

Finally, the lower bound on \( M \geq ((n + 1)^m)! \) in Theorem 3 can probably be weaken and could be make closer to the lower bound (7). In fact we conjecture that essentially smaller \( M \) can be dealt with if one considers polynomials which are either identical to zero or take at least one value relatively prime to \( M \).

References


