NEWTON-HENSEL INTERPOLATION LIFTING

MARTÍN AVENDAÑO, TERESA KRICK, AND ARIEL PACETTI

Abstract. The main result of this paper is a new version of Newton-Hensel lifting that relates to interpolation questions. It allows one to lift polynomials in $\mathbb{Z}[x]$ from information modulo a prime number $p \neq 2$ to a power p^k for any k, and its originality is that it is a mixed version that not only lifts the coefficients of the polynomial but also its exponents. We show that this result corresponds exactly to a Newton-Hensel lifting of a system of $2t$ generalized equations in $2t$ unknowns in the ring of p-adic integers $\mathbb{Z}_p$. Finally we apply our results to sparse polynomial interpolation in $\mathbb{Z}[x]$.

Introduction

Quoting [BCSS98, p.10], Newton's method has been considered *"the search algorithm" sine qua non* of numerical analysis and scientific computation. Since its origins probably by Viète around 1580, its description by Newton in 1669, simplification by Raphson in 1690 and actual formulation by Simpson in 1740, Newton's method has been widely studied, applied and generalized. For instance we mention here the crucial development by S. Smale of the alpha theory, emphasizing conditions on the input approximate zero (i.e., where can we start the Newton's method) instead of hypotheses with regard to estimates on the unknown zero, and of the gamma theory that estimates the size of a ball of approximate zeros around the zero [Sma86] and [BCSS98, Ch. 8 and 14]. Another important issue is the search for algorithms for finding approximate zeros in [ShSm94, CuSm99] (the search of a polynomial time uniform algorithm for such an approximate zero is one of the mathematical problems for next century proposed in [Sma98]), and the generalizations of Newton's method for over-determined systems, for instance in [DeSh00], and recently for systems with multiplicities in [Lec02].

The non-archimedean counterpart of Newton's method, introduced by Hensel around 1900, is the basis of the construction of the p-adic numbers and their applications as in the local-global Hasse-Minkowski principle for quadratic forms. Since then, "Newton-Hensel lifting" in its non-archimedean versions is primordially present in exact symbolic computation: for example in univariate rational polynomial factorization in [Zas69] and the breakthrough LLL-polynomial time factorization algorithm [LLL82], in multivariate polynomial factorization [ChGr82, Chi84, Gri84, Kal85]. Also for multivariate polynomial systems solving in the Gröbner basis setting in [Tri85, Win88] and in the primitive element setting in [ChGr83, Chi84, Gri84] and in [GHMMP98, GHHMMP97, HKPSW00, JKSS04].

The main result of this paper is a new version of Newton-Hensel lifting that relates to interpolation questions. It allows to lift polynomials in $\mathbb{Z}[x]$ from information modulo a prime number $p \neq 2$ to a power p^k for any k, and its originality is that it is a mixed version that not only lifts the coefficients of the polynomial but also its *exponents*.

2000 *Mathematics Subject Classification.* Primary: 41A05; Secondary: 11S05, 68W30.

Key words and phrases. Newton-Hensel lifting, p-adic integers, sparse polynomial interpolation.

The first and third author are partially supported by CONICET fellowships.

The second author is supported by research grants UBACYT X-112 and CONICET PIP 2461/01, Argentina.

Theorem 1. *Let p be an odd prime number, and $t \in \mathbb{N}$, $1 \le t \le p-1$.*
Set $y_1, \dots, y_{2t} \in \mathbb{Z}$. Let $f := \sum_{j=1}^{t} a_j x^{\alpha_j} \in \mathbb{Z}[x]$ and $x_1, \dots, x_{2t} \in \mathbb{Z}$ satisfy that

- $f(x_i) \equiv y_i \pmod{p}$, $1 \le i \le 2t$,
- $\det \begin{pmatrix} x_1^{\alpha_1} & \dots & x_1^{\alpha_t} & a_1\, e_p(x_1) x_1^{\alpha_1} & \dots & a_t\, e_p(x_1) x_1^{\alpha_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ x_{2t}^{\alpha_1} & \dots & x_{2t}^{\alpha_t} & a_1\, e_p(x_{2t}) x_{2t}^{\alpha_1} & \dots & a_t\, e_p(x_{2t}) x_{2t}^{\alpha_t} \end{pmatrix} \not\equiv 0 \pmod{p}$,

  where $e_p : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is the map defined by $x^{p-1} \equiv 1 + p\, e_p(x) \pmod{p^2}$ for $p \nmid x$ and $e_p(x) = 0$ for $p \mid x$ (see Definition 1.1 and Notation 1.4).

Then for every $k \in \mathbb{N}_0$ there exists $f_k := \sum_{j=1}^{t} a_{k,j} x^{\alpha_{k,j}} \in \mathbb{Z}[x]$, that satisfies simultaneously:

- $f_k(x_i) \equiv y_i \pmod{p^{2^k}}$ *for* $1 \le i \le 2t$,
- $a_{k,j} \equiv a_j \pmod{p}$ *and* $\alpha_{k,j} \equiv \alpha_j \pmod{(p-1)}$, $1 \le j \le t$.

Furthermore, if $f_k := \sum_{j=1}^{t} a_{k,j} x^{\alpha_{k,j}}, g_k := \sum_{j=1}^{t} b_{k,j} x^{\beta_{k,j}} \in \mathbb{Z}[x]$ are two such polynomials, then

$$a_{k,j} \equiv b_{k,j} \pmod{p^{2^k}} \quad \text{and} \quad \alpha_{k,j} \equiv \beta_{k,j} \pmod{\varphi(p^{2^k})}, \ 1 \le j \le t,$$

where φ denotes the Euler map.

In fact we show in this paper that this result corresponds exactly to a Newton-Hensel lifting of a system of $2t$ generalized equations in $2t$ unknowns, where the unknowns are the t coefficients of f in the p-adic integers $\mathbb{Z}_p$ and the t exponents of f in some suitable set $\mathcal{E}_p$ (see Definition 2.1), and where the condition that the defined determinant does not vanish modulo p is the corresponding classical condition on the Jacobian determinant of the system: the map e_p plays the role of a logarithmic function that enables us to lower the exponents to the floor level.

For this purpose we introduce the ring $\mathcal{E}_p$ of "allowed exponents" (whose additive group is isomorphic to the p-adic unit group $\mathbb{Z}_p^\times$), where "allowed" means that for $x \in \mathbb{Z}_p^\times$ and $\alpha \in \mathcal{E}_p$, $x^\alpha \in \mathbb{Z}_p^\times$, and we study systems of generalized polynomial expressions in $\mathbb{Z}_p$, where the variables belong to $\mathbb{Z}_p^\times$ and the exponents belong to $\mathcal{E}_p$.

Here, among all the equivalent descriptions of $\mathbb{Z}_p$ we adopt the following one that we consider more suitable for our formulations:

$$\mathbb{Z}_p = \left\{ (a_k)_{k \in \mathbb{N}} \in \mathbb{Z}^{\mathbb{N}} \ : \ a_{k+1} \equiv a_k \pmod{p^k} \ \forall\, k \in \mathbb{N} \right\} / \sim,$$

where $(a_k)_{k\in\mathbb{N}} \sim (b_k)_{k\in\mathbb{N}} \ \Leftrightarrow \ a_k \equiv b_k \pmod{p^k}, \ \forall\, k \in \mathbb{N}$. Similarly, we have

$$\mathcal{E}_p = \left\{ (\alpha_k)_{k \in \mathbb{N}} \in \mathbb{Z}^{\mathbb{N}} \ : \ \alpha_{k+1} \equiv \alpha_k \pmod{\varphi(p^k)} \ \forall\, k \in \mathbb{N} \right\} / \approx,$$

where $(\alpha_k)_{k\in\mathbb{N}} \approx (\beta_k)_{k\in\mathbb{N}} \ \Leftrightarrow \ \alpha_k \equiv \beta_k \pmod{\varphi(p^k)}, \ \forall\, k \in \mathbb{N}$. (In the sequel $\overline{(a_k)}_k$ or $\overline{(\alpha_k)}_k$ denote the class in the corresponding ring.)

We consider systems of equations where the unknowns are the variables in $\mathbb{Z}_p^\times$ or the exponents in $\mathcal{E}_p$, switching from one formulation to the other by a logarithmic argument, and obtain in Propositions 2.11 and 2.12 below the generalizations of the following Newton-Hensel univariate lifting statements:

Proposition 2. *Set $t \in \mathbb{N}$, y, $a_j \in \mathbb{Z}_p$ and $\alpha_j := \overline{(\alpha_{jk})}_k \in \mathcal{E}_p$, $1 \le j \le t$. Let $x_1 \in \mathbb{Z}$, $p \nmid x_1$, be such that*

- $f(x_1) := \sum_{j=1}^{t} a_j\, x_1^{\alpha_j} \equiv y \pmod{p}$,
- $\sum_{j=1}^{t} a_j\, \alpha_{j2}\, x_1^{\alpha_j - 1} \not\equiv 0 \pmod{p}$,

then there exists a unique $x = \overline{(x_1, x_2, \dots)} \in \mathbb{Z}_p^\times$ *such that* $f(x) = y$ *in* $\mathbb{Z}_p$ *.*

Proposition 3. *Set* $t \in \mathbb{N}$, y, $a_j \in \mathbb{Z}_p$ *and* $x_j := \overline{(x_{jk})}_k \in \mathbb{Z}_p^\times$ *,* $1 \le j \le t$ *. Let* $\alpha_1 \in \mathbb{Z}$ *be such that*

- $g(\alpha_1) := \sum_{j=1}^t a_j\, x_j^{\alpha_1} \equiv y \pmod p$ *,*
- $\sum_{j=1}^t a_j\, e_p(x_{j2})\, x_j^{\alpha_1} \not\equiv 0 \pmod p$ *,*
  where $e_p : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ *is the map defined by* $x^{p-1} \equiv 1 + p\, e_p(x) \pmod{p^2}$ *for* $p \nmid x$ *and* $e_p(x) = 0$ *for* $p \mid x$ *,*

then there exists a unique $\alpha = \overline{(\alpha_1, \alpha_2, \dots)} \in \mathcal{E}_p$ *such that* $g(\alpha) = y$ *in* $\mathbb{Z}_p$ *.*

We observe that the map e_p used in the hypotheses of Theorem 1 and Proposition 3 is a group homomorphism $(\mathbb{Z}/p^2\mathbb{Z})^\times \to \mathbb{Z}/p\mathbb{Z}$ that appears widely in the literature, even if not explicitly stated in the way we do in Proposition 1.2 below. It arises naturally when looking for generators of the cyclic multiplicative group $\mathbb{Z}/p^k\mathbb{Z}$ for p an odd prime number [Apo76, Th.10.6] or considering the filtration of the group of p-adic units $\mathbb{Z}_p^\times$ [Ser70, Ch.II §3.1]. As explained in [Car14, p.101] the properties $e(2) = 0$ and $e(3) = 0$ are also intimately related to special cases of Fermat's last theorem. It seems that at least until 1999, it was still unknown if there were infinitely many prime numbers p such that $e_p(2) \neq 0$ without assuming the ABC conjecture [EsMu99, p.8]. Finally, let us mention that numerical experiments we made suggest that the behavior of the map $e_p(x)/p - 1$ for a fixed integer x and a variable prime number p seems to follow a uniform distribution in the $[0, 1]$ interval.

Our initial motivation and a possible useful application for the Newton-Hensel lifting result presented in Theorem 1 above was the search of an efficient interpolation algorithm for integer univariate polynomials, where the number of interpolation points depends on the number of non-zero terms and not on the degree. A polynomial is called *t-sparse* if it has at most t non-zero terms. The problem of interpolating a t-sparse polynomial from its values in a list of specific interpolation points where the number of these points does not depend on the degree but on t is called "sparse interpolation". It received a lot of attention around 1990 and again recently, for instance in [BeTi88, Zip90, KaLa88, KLW90, KLL00, Lee01, KaLe03], [BoTi91], [DrGr91, GKS91], [GKS90, CDGK91] and [GKS94].

It is a well-known fact that, as a consequence of Descartes rule of signs, a t-sparse polynomial $f \in \mathbb{R}[x]$ (one variable) has at most $t-1$ distinct real positive roots. Therefore, any univariate t-sparse polynomial in $\mathbb{C}[x]$ is uniquely determined by its value in $2t$ different positive values in $\mathbb{R}$ (since for two such polynomials, the difference $f - g$ of their real parts (or their imaginary parts) is a $2t$-sparse polynomial which has at most $2t-1$ different real positive roots). In [BeTi88], M. Ben-Or and P. Tiwari produced a beautiful deterministic algorithm that recovers such a t-sparse polynomial $f \in \mathbb{C}[x]$ from its value in the $2t$ interpolation points

$$x_1 := 1,\, x_2 := a,\, x_3 := a^2, \dots, x_{2t} := a^{2t-1},$$

where a is not a root of unity of small order. They also raised the problem of producing an algorithm that interpolates a t-sparse polynomial in $\mathbb{C}[x]$ from $2t$ arbitrary different real positive values, to emulate in some sense Lagrange or Newton interpolation algorithms that do not require specific interpolation input values, instead of imposing the starting points as they do.

Although we are not able to answer this question in generality, we produce in Proposition 1.14 families $\{x_1, \dots, x_{2t}\}$ of starting points where the non-vanishing determinant hypothesis holds under a good reduction property of the input t-sparse polynomial modulo the prime number p (Proposition 1.10). Therefore, applying Theorem 1 we obtain a very fast algorithm for sparse interpolation of t-sparse polynomials in $\mathbb{Z}[x]$ that reduce well modulo p (Algorithm 3.16). The algorithm does not require to know in advance the degree of the polynomial although it needs to know its exact number t of non-zero terms. In order to make this algorithm work for any polynomial $f \in \mathbb{Z}[x]$, we still idealistically need a criterion to choose, in terms of the evaluation values $y_i = f(x_i)$, a (small) prime number p such that f reduces well modulo p. This would be the analog of the choice of the prime in the univariate rational polynomial factorization algorithms (the condition in this case is given by the non-vanishing of a discriminant modulo p), and in the archimedean setting, a (still unknown) criterion for the choice of an approximate zero. More realistically, we would at least need a satisfactory probabilistic argument for the choice of such a prime in a given range (that we are still unable to produce).

The paper is organized as follows.
Section 1 is mainly devoted to the proof of Theorem 1. For this purpose we introduce a generalization of the e_p group homomorphism mentioned above (Definition 1.2). Then we prove the theorem (Theorem 1.6) and present an equivalence of the uniqueness condition (Proposition 1.10). Finally we analyze the existence of good starting sets $\{x_1, \dots, x_{2t}\}$ as inputs of Theorem 1 (Definition 1.12 and Proposition 1.14).
In Section 2, we focus on the Hensel lemma character of our Theorem 1 in the ring of p-adic integers $\mathbb{Z}_p$. We introduce the set $\mathcal{E}_p$ of allowed exponents (Definition 2.1), the generalized polynomial equations and their dual exponential equations (Observation 2.7) and we present the proofs of Propositions 1 and 2 above (Propositions 2.8 and 2.9) and their generalizations to systems of generalized polynomial and exponential equations (Propositions 2.11 and 2.12).
Finally Section 3 deals with the sparse interpolation problem mentioned above, first focusing in univariate t-sparse polynomials with coefficients in finite rings and then in univariate integer t-sparse polynomials.

Acknowledgments. Teresa Krick thanks Wen-shin Lee for bringing her into the sparse interpolation subject and Michael Singer for wonderful discussions. We are also grateful to Felipe Cucker, Arieh Iserles, Erich Kaltofen and Mike Shub for their advice, and to the referees for their careful reading and clarifying comments.

1. Newton-Hensel lifting

This section is mainly devoted to the proof of Theorem 1, the Newton-Hensel interpolation lifting theorem stated in the introduction.

During the paper p denotes an odd prime number. Given an integer ρ prime to p, we denote by $o_{p^k}(\rho)$ the order of ρ in the multiplicative cyclic group $(\mathbb{Z}/p^k\mathbb{Z})^\times$. We recall that $\rho \in \mathbb{Z}$ is a primitive root modulo p^k if its class in $\mathbb{Z}/p^k\mathbb{Z}$ generates this cyclic group, that is if $o_{p^k}(\rho) = \varphi(p^k) = (p-1)p^{k-1}$.

The crucial tool in this paper is a family of group homomorphisms that relates the multiplicative group $(\mathbb{Z}/p^k\mathbb{Z})^\times$ with the additive group $\mathbb{Z}/p^{k-\ell}\mathbb{Z}$ for $\ell \le k \le 2\ell$. This morphism enables us to linearize polynomial expressions.

Definition 1.1. Let p be an odd prime number, k, ℓ positive integers with $\ell \le k \le 2\ell$. Define the morphism $e_{p,k,\ell} : (\mathbb{Z}/p^k\mathbb{Z})^\times \to \mathbb{Z}/p^{k-\ell}\mathbb{Z}$ by

$$e_{p,k,\ell}(x) := \frac{x^{\varphi(p^\ell)} - 1}{p^\ell} \pmod{p^{k-\ell}}$$

Proposition 1.2. *The map $e_{p,k,\ell}$ defined above is a group epimorphism.*

Proof. The map is clearly well-defined since $x^{\varphi(p^\ell)} \equiv 1 + p^\ell e_{p,k,\ell}(x) \pmod{p^k}$. Hence we must prove it is a group homomorphism. It is enough to prove:

- $e_{p,k,\ell}(1) = 0$ (clear from the definition).
- $e_{p,k,\ell}(x\,y) = e_{p,k,\ell}(x) + e_{p,k,\ell}(y)$. Since $x^{\varphi(p^\ell)} \equiv 1 + p^\ell\, e_{p,k,\ell}(x) \pmod{p^k}$ and $y^{\varphi(p^\ell)} \equiv 1 + p^\ell\, e_{p,k,\ell}(y) \pmod{p^k}$, it follows $(x\,y)^{\varphi(p^\ell)} \equiv (1 + p^\ell\, e_{p,k,\ell}(x))(1 + p^\ell\, e_{p,k,\ell}(y)) \equiv 1 + p^\ell\,(e_{p,k,\ell}(x) + e_{p,k,\ell}(y)) \pmod{p^k}$ (here we use the condition $k \le 2\ell$).

To see it is surjective we compute the order of its kernel. $\mathrm{Ker}(e_{p,k,\ell}) = \{x \in (\mathbb{Z}/p^k\mathbb{Z})^\times : x^{\varphi(p^\ell)} \equiv 1 \pmod{p^k}\} = \{x \in (\mathbb{Z}/p^k\mathbb{Z})^\times : o_{p^k}(x) \,|\, \varphi(p^\ell) = (p-1)p^{\ell-1}\}$. Then $|\mathrm{Ker}(e_{p,k,\ell})| = (p-1)p^{\ell-1}$, $|\mathrm{Im}(e_{p,k,\ell})| = p^{k-\ell}$ and $e_{p,k,\ell}$ is surjective. □

Remark 1.3. If ρ is a primitive root modulo p^k then $e_{p,k,\ell}(\rho) \neq 0$.

Notation 1.4. Abusing notation we will denote $e_{p,k,\ell}$ the map from $\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^{k-\ell}\mathbb{Z}$ defined as in Definition 1.1 on elements prime to p and by zero on other elements. In the case $k = 2$ we will denote $e_{p,2}(x) := e_{p,2,1}(x)$ (or just $e_2(x)$ if the prime is clear from the context).

Definition 1.5. Let p be an odd prime number, and $t \in \mathbb{N}$, $1 \le t \le p-1$. Let $f = \sum_{j=1}^t a_j x^{\alpha_j} \in \mathbb{Z}[x]$. For $x_1, \ldots, x_{2t} \in \mathbb{Z}$, we define:

$$\Delta_p\, f(x_1, \ldots, x_{2t}) := \det \begin{pmatrix} x_1^{\alpha_1} & \ldots & x_1^{\alpha_t} & a_1\, e_2(x_1) x_1^{\alpha_1} & \ldots & a_t\, e_2(x_1) x_1^{\alpha_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ x_{2t}^{\alpha_1} & \ldots & x_{2t}^{\alpha_t} & a_1\, e_2(x_{2t}) x_{2t}^{\alpha_1} & \ldots & a_t\, e_2(x_{2t}) x_{2t}^{\alpha_t} \end{pmatrix} \pmod{p} \tag{1}$$

where $e_2(x_i) : \mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is the map of Notation 1.4.

Quantity (1) plays the role of the usual jacobian in our version of Newton-Hensel interpolation lifting. In the next section, using the analysis in the p-adic context, the relation will become clear. For that reason we refer to it as the *interpolating pseudo-jacobian modulo p of f on $x_1, \ldots, x_{2t}$*.

Theorem 1.6. (Newton-Hensel interpolation lifting) *Let p be an odd prime number, and $t \in \mathbb{N}$, $1 \le t \le p-1$. Set $y_1, \ldots, y_{2t} \in \mathbb{Z}$. Let $f := \sum_{j=1}^t a_j x^{\alpha_j} \in \mathbb{Z}[x]$ and $x_1, \ldots, x_{2t} \in \mathbb{Z}$ satisfy*

- $f(x_i) \equiv y_i \pmod{p}$, $1 \le i \le 2t$,
- $\Delta_p\, f(x_1, \ldots, x_{2t}) \not\equiv 0 \pmod{p}$, *where $\Delta_p\, f$ is given by Formula (1).*

Then for every $k \in \mathbb{N}_0$ there exists $f_k := \sum_{j=1}^t a_{k,j} x^{\alpha_{k,j}} \in \mathbb{Z}[x]$, that satisfies simultaneously:

- $f_k(x_i) \equiv y_i \pmod{p^{2^k}}$ *for* $1 \le i \le 2t$,
- $a_{k,j} \equiv a_j \pmod{p}$ *and* $\alpha_{k,j} \equiv \alpha_j \pmod{(p-1)}$, $1 \le j \le t$.

Furthermore, if $f_k := \sum_{j=1}^t a_{k,j} x^{\alpha_{k,j}}, g_k := \sum_{j=1}^t b_{k,j} x^{\beta_{k,j}} \in \mathbb{Z}[x]$ are two such polynomials, then

$$a_{k,j} \equiv b_{k,j} \pmod{p^{2^k}} \quad \text{and} \quad \alpha_{k,j} \equiv \beta_{k,j} \pmod{\varphi(p^{2^k})}, \; 1 \le j \le t. \tag{2}$$

Proof. We define $f_0 := f$, which is clearly the only possible definition for f_0. Assume now $f_k = \sum_{j=1}^t a_{k,j} x^{\alpha_{k,j}}$ is uniquely defined under Condition (2), with $f_k(x_i) \equiv y_i \pmod{p^{2^k}}$ for $1 \le i \le 2t$, and $a_{k,j} \equiv a_j \pmod{p}$, $\alpha_{k,j} \equiv \alpha_j \pmod{(p-1)}$.
We look for f_{k+1} such that $f_{k+1}(x_i) \equiv y_i \bmod p^{2^{k+1}}$ for $1 \le i \le 2t$. In particular $f_{k+1}(x_i) \equiv y_i \pmod{p^{2^k}}$ for $1 \le i \le 2t$, and therefore f_{k+1} is of the form

$$f_{k+1} := \sum_{j=1}^t (a_{k,j} + p^{2^k} d_j) x^{(\alpha_{k,j} + \varphi(p^{2^k})\delta_j)}$$

and d_j, δ_j have to be determined such that $f_{k+1}(x_i) \equiv y_i \pmod{p^{2^{k+1}}}$ for $1 \le i \le 2t$.

For notational simplicity, for the rest of the proof we set $b_j := a_{k,j}$ and $\beta_j := \alpha_{k,j}$.

Since $x_i \not\equiv 0 \pmod p$, $x_i^{\varphi(p^{2^k})} \equiv 1 \pmod{p^{2^k}}$. Let $e_{2^{k+1}}(x_i), \ell_{2^{k+1}}(x_i) \in \{0, \dots, p^{2^k} - 1\}$ be such that

$$x_i^{\varphi(p^{2^k})} \equiv 1 + p^{2^k} e_{2^{k+1}}(x_i) \pmod{p^{2^{k+1}}} \quad \text{and} \quad y_i \equiv f_k(x_i) + p^{2^k} \ell_{2^{k+1}}(x_i) \pmod{p^{2^{k+1}}} \tag{3}$$

i.e. $e_{2^{k+1}}(x_i) = e_{p,2^{k+1},2^k}(x_i)$. Then

$$\begin{aligned}
y_i &\equiv f_{k+1}(x_i) \pmod{p^{2^{k+1}}} \\
&\equiv \sum_{j=1}^{t} (b_j + p^{2^k} d_j) x_i^{(\beta_j + \varphi(p^{2^k})\delta_j)} \pmod{p^{2^{k+1}}} \\
&\equiv \sum_{j=1}^{t} (b_j + p^{2^k} d_j) x_i^{\beta_j} (1 + p^{2^k} e_{2^{k+1}}(x_i))^{\delta_j} \pmod{p^{2^{k+1}}} \\
&\equiv \sum_{j=1}^{t} (b_j + p^{2^k} d_j) x_i^{\beta_j} (1 + p^{2^k} e_{2^{k+1}}(x_i)\delta_j) \pmod{p^{2^{k+1}}} \\
&\equiv \sum_{j=1}^{t} (b_j x_i^{\beta_j} + p^{2^k} (x_i^{\beta_j} d_j + b_j e_{2^{k+1}}(x_i) x_i^{\beta_j} \delta_j)) \pmod{p^{2^{k+1}}} \\
&\equiv f_k(x_i) + p^{2^k} \sum_{j=1}^{t} (x_i^{\beta_j} d_j + b_j e_{2^{k+1}}(x_i) x_i^{\beta_j} \delta_j) \pmod{p^{2^{k+1}}} \\
&\equiv y_i - p^{2^k} \ell_{2^{k+1}}(x_i) + p^{2^k} \sum_{j=1}^{t} (x_i^{\beta_j} d_j + b_j e_{2^{k+1}}(x_i) x_i^{\beta_j} \delta_j) \pmod{p^{2^{k+1}}}.
\end{aligned}$$

Then

$$-p^{2^k} \ell_{2^{k+1}}(x_i) + p^{2^k} \sum_{j=1}^{t} (x_i^{\beta_j} d_j + b_j e_{2^{k+1}}(x_i) x_i^{\beta_j} \delta_j) \equiv 0 \pmod{p^{2^{k+1}}}$$

Dividing by p^{2^k} we get

$$-\ell_{2^{k+1}}(x_i) + \sum_{j=1}^{t} (x_i^{\beta_j} d_j + b_j e_{2^{k+1}}(x_i) x_i^{\beta_j} \delta_j) \equiv 0 \pmod{p^{2^k}} \quad \text{for } 1 \le i \le 2t.$$

Thus, one has to solve modulo p^{2^k} the linear system of equations

(4)

$$\begin{pmatrix} x_1^{\beta_1} & \dots & x_1^{\beta_t} & b_1 e_{2^{k+1}}(x_1) x_1^{\beta_1} & \dots & b_t e_{2^{k+1}}(x_1) x_1^{\beta_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ x_{2t}^{\beta_1} & \dots & x_{2t}^{\beta_t} & b_1 e_{2^{k+1}}(x_{2t}) x_{2t}^{\beta_1} & \dots & b_t e_{2^{k+1}}(x_{2t}) x_{2t}^{\beta_t} \end{pmatrix} \begin{pmatrix} d_1 \\ \vdots \\ d_t \\ \delta_1 \\ \vdots \\ \delta_t \end{pmatrix} = \begin{pmatrix} \ell_{2^{k+1}}(x_1) \\ \vdots \\ \ell_{2^{k+1}}(x_{2t}) \end{pmatrix}$$

Let M_k denote the $2t$ square matrix on the left hand side of System (4), that is the matrix of the $(k+1)$-iteration step of our construction. Our aim is to show that this matrix is invertible modulo p^{2^k}, i.e. that $\det(M_k) \not\equiv 0 \pmod p$. As the next lemma shows all matrices reduce to M_0 modulo p, then we can restrict ourselves to study $\det(M_0)$.

Lemma 1.7. *With the same notation as above* $M_k \equiv M_0 \pmod p$ *term by term.*

Proof. By construction it is clear that $b_j \equiv a_j \mod p$ and $x_i^{\beta_j} \equiv x_i^{\alpha_j} \pmod p$.

Hence we are left to prove that for any $x \in \mathbb{Z}$ prime to p, $e_{p,2^{k+1},2^k}(x) \equiv e_{p,2^{k+2},2^{k+1}}(x) \pmod{p^{2^k}}$. Let $e := e_{p,2^{k+1},2^k}(x)$ and $e' := e_{p,2^{k+2},2^{k+1}}(x)$. Then $x^{\varphi(p^{2^k})} \equiv 1 + p^{2^k} e \pmod{p^{2^{k+1}}}$ and $x^{\varphi(p^{2^{k+1}})} \equiv 1 + p^{2^{k+1}} e' \pmod{p^{2^{k+2}}}$. Since $\varphi(p^{2^{k+1}}) = \varphi(p^{2^k}) p^{2^k}$, we have:

$$\begin{aligned}
x^{\varphi(p^{2^{k+1}})} &= (x^{\varphi(p^{2^k})})^{p^{2^k}} \\
&= (1 + p^{2^k}(e + p^{2^k} r))^{p^{2^k}} \\
&= 1 + p^{2^k} p^{2^k}(e + p^{2^k} r) + \binom{p^{2^k}}{2}(p^{2^k})^2 (e + p^{2^k} r)^2 + \binom{p^{2^k}}{3}(p^{2^k})^3 (e + p^{2^k} r)^3 + \cdots \\
&= 1 + p^{2^{k+1}}(e + p^{2^k} r) + p^{2^k + 2^{k+1}} \frac{p^{2^k} - 1}{2}(e + p^{2^k} r)^2 + p^{3\,2^k}\binom{p^{2^k}}{3}(e + p^{2^k} r)^3 + \cdots \\
&= 1 + p^{2^{k+1}}\Big(e + p^{2^k}(r + \frac{p^{2^k} - 1}{2}(e + p^{2^k} r)^2 + \binom{p^{2^k}}{3}(e + p^{2^k} r)^3 + \cdots)\Big) \\
&\equiv 1 + p^{2^{k+1}}\Big(e + p^{2^k} r'\Big) \pmod{p^{2^{k+2}}},
\end{aligned}$$

where $r' := r + \ldots$. Then $e' \equiv e + p^{2^k} r' \equiv e \mod p^{2^k}$. □

We continue with the proof of the theorem. We can restrict to compute $\det(M_0)$. By definition,

$$M_0 = \begin{pmatrix} x_1^{\alpha_1} & \ldots & x_1^{\alpha_t} & a_1 e_2(x_1) x_1^{\alpha_1} & \ldots & a_t e_2(x_1) x_1^{\alpha_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ x_{2t}^{\alpha_1} & \ldots & x_{2t}^{\alpha_t} & a_1 e_2(x_{2t}) x_{2t}^{\alpha_1} & \ldots & a_t e_2(x_{2t}) x_{2t}^{\alpha_t} \end{pmatrix},$$

so that $\det(M_0) \equiv \Delta_p\, f(x_1, \ldots, x_{2t}) \not\equiv 0 \pmod p$ by the second hypothesis of the theorem.

Since $\det(M_k) \equiv \det(M_0) \not\equiv 0 \pmod p$, M_k is invertible and System (4) has a unique solution modulo p^{2^k}, namely:

$$\begin{pmatrix} d_1 \\ \vdots \\ d_t \\ \delta_1 \\ \vdots \\ \delta_t \end{pmatrix} = M_k^{-1} \begin{pmatrix} \ell_{2^{k+1}}(x_1) \\ \vdots \\ \ell_{2^{k+1}}(x_{2t}) \end{pmatrix}.$$

This shows the existence of f_{k+1} and its uniqueness property. □

Observation 1.8. *The statement of Theorem 1.6 also holds modulo* p^k. *We stated and proved it modulo* p^{2^k} *to get quadratic convergence as well as in the classic Newton-Hensel lifting.*

We observe that the hypothesis $\Delta_p\, f(x_1, \ldots, x_{2t}) \not\equiv 0 \pmod p$ of Theorem 1.6 implies in particular that $p \nmid x_i$, $p \nmid a_j$ and also that $p - 1 \nmid \alpha_j - \alpha_\ell$, $1 \le i \le 2t, 1 \le j \ne \ell \le t$ (otherwise, x_i being prime to p would force two columns of M_0 to coincide). Thus f has exactly the same number t of terms when reduced modulo p than in $\mathbb{Z}[x]$, and no two exponents reduce to the same modulo $(p-1)$. In view of this we give the following definition

Definition 1.9. Let p be an odd prime number. We say that a polynomial $f=\sum_j a_jx^{\alpha_j}\in\mathbb{Z}[x]$ with $a_j\neq 0$, $\forall j$, *reduces well modulo* p if $p\nmid a_j$ for any j, and $p-1\nmid \alpha_j-\alpha_\ell$ for any $j\neq\ell$.

In these conditions the uniqueness property of Theorem 1.6 has an equivalent formulation in terms of how the polynomials coincide as functions on $(\mathbb{Z}/p^{2^k}\mathbb{Z})^\times$:

Proposition 1.10. *Let $f=\sum_j a_jx^{\alpha_j}, g=\sum_\ell b_\ell x^{\beta_\ell}\in\mathbb{Z}[x]$ be two polynomials that reduce well modulo p. Then, for any $k\in\mathbb{N}$, the two following conditions are equivalent:*

- *f and g have the same number t of non-zero terms, and up to an index permutation, $a_j\equiv b_j \pmod{p^k}$ and $\alpha_j\equiv\beta_j \pmod{\varphi(p^k)}$.*
- *$f(x)\equiv g(x) \pmod{p^k}$ for all $x\in(\mathbb{Z}/p^k\mathbb{Z})^\times$.*

Before giving the proof, we need the following:

Observation 1.11. *Any primitive root modulo p^k is also a primitive root modulo p.*

Proof. Since $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is a cyclic group, the number of elements in $(\mathbb{Z}/p^k\mathbb{Z})^\times$ of order divisible by $(p-1)$ is $p^{k-1}\varphi(p-1)$. Clearly this set must contain the p^{k-1} lifts of any primitive root of $(\mathbb{Z}/p\mathbb{Z})^\times$ to $(\mathbb{Z}/p^k\mathbb{Z})^\times$. By cardinality they are the same. ☐

Proof. of Proposition 1.10.–
$(\Downarrow)$ is clear.
$(\Uparrow)$ by induction in k:
• Case $k=1$: Write $f=\sum_{j=0}^{p-2}a_jx^{j+(p-1)k_j}$ and $g=\sum_{j=0}^{p-2}b_jx^{j+(p-1)k'_j}$. Since $x^{p-1}\equiv 1 \pmod p$ and $f(x)\equiv g(x) \pmod p$ for $1\le x\le p-1$,

$$\sum_{j=0}^{p-2}(a_j-b_j)x^j\equiv 0 \pmod p \quad \text{for } 1\le x\le p-1,$$

but a degree $p-2$ polynomial has at most $p-2$ different roots modulo p hence $a_j\equiv b_j \mod p$.
• Assume it is true for k.
Let f,g be two polynomials satisfying the hypothesis and such that $f(x)\equiv g(x) \pmod{p^{k+1}}$ for all $x\in(\mathbb{Z}/p^{k+1}\mathbb{Z})^\times$. In particular $f(x)\equiv g(x) \pmod p$ and by the $k=1$ case they have both exactly t non-zero terms modulo p for some $1\le t\le p-1$.
If $f:=\sum_{j=1}^t a_jx^{\alpha_j}$ and $g:=\sum_{j=1}^t b_jx^{\beta_j}$, by inductive hypothesis (up to a permutation of indexes) $a_j\equiv b_j \pmod{p^k}$ and $\alpha_j\equiv\beta_j \pmod{\varphi(p^k)}$. Let a_j^{-1} denote the inverse of a_j in the multiplicative group $(\mathbb{Z}/p^{k+1}\mathbb{Z})^\times$, and $0\le c_j,\gamma_j<p$ be such that

$$a_j^{-1}b_j\equiv 1+p^kc_j \pmod{p^{k+1}} \quad\text{and}\quad \beta_j-\alpha_j\equiv\varphi(p^k)\gamma_j \pmod{\varphi(p^{k+1})}.$$

For all $x\in(\mathbb{Z}/p^{k+1}\mathbb{Z})^\times$:

$$\begin{aligned}
0 &\equiv (f-g)(x) \pmod{p^{k+1}}\\
&\equiv \sum_{j=1}^t(a_jx^{\alpha_j}-b_jx^{\beta_j}) \pmod{p^{k+1}}\\
&\equiv \sum_{j=1}^t a_jx^{\alpha_j}(1-a_j^{-1}b_jx^{\beta_j-\alpha_j}) \pmod{p^{k+1}}\\
&\equiv \sum_{j=1}^t a_jx^{\alpha_j}(1-(1+p^kc_j)x^{\varphi(p^k)\gamma_j}) \pmod{p^{k+1}}
\end{aligned}$$

But $x^{\varphi(p^k)} \equiv 1 + p^k e_{p,k+1,k}(x) \pmod{p^{k+1}}$ for $e_{p,k+1,k}$ defined in Notation 1.4, thus

$$\begin{aligned} 0 &\equiv \sum_{j=1}^{t} a_j x^{\alpha_j}(1-(1+p^k c_j)(1+p^k e_{p,k+1,k}(x))^{\gamma_j}) \pmod{p^{k+1}} \\ &\equiv \sum_{j=1}^{t} a_j x^{\alpha_j}(1-(1+p^k c_j)(1+p^k e_{p,k+1,k}(x)\gamma_j) \pmod{p^{k+1}} \\ &\equiv \sum_{j=1}^{t} -a_j x^{\alpha_j} p^k (c_j + e_{p,k+1,k}(x)\gamma_j) \pmod{p^{k+1}} \end{aligned}$$

Therefore,

$$\sum_{j=1}^{t} a_j x^{\alpha_j}(c_j + e_{p,k+1,k}(x)\gamma_j) \equiv 0 \pmod{p}. \tag{5}$$

Let $\rho \in \mathbb{Z}$ be a primitive root $\bmod\, p^{k+1}$. Then $x_1 := 1, x_2 := \rho^p, \ldots, x_t := \rho^{(t-1)p}$ are all different modulo p by Observation 1.11, and $e_{p,k+1,k}(x_i) = e_{p,k+1,k}(\rho^{(i-1)p}) \equiv 0 \pmod{p}$ since $e_{p,k+1,k}$ is a group homomorphism. Substituting in (5):

$$\sum_{j=1}^{t} a_j \rho^{(i-1)p\,\alpha_j} c_j \equiv 0 \pmod{p} \quad \text{for } 1 \le i \le t.$$

That is

$$\begin{pmatrix} a_1 & \ldots & a_t \\ a_1\rho^{p\alpha_1} & \ldots & a_t\rho^{p\alpha_t} \\ \vdots & & \vdots \\ a_1\rho^{(t-1)p\alpha_1} & \ldots & a_t\rho^{(t-1)p\alpha_t} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_t \end{pmatrix} \equiv \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \pmod{p}.$$

The Vandermonde determinant of this linear system is

$$a_1 \cdots a_t \prod_{j<\ell} (\rho^{p\,\alpha_\ell} - \rho^{p\,\alpha_j}) \not\equiv 0 \pmod{p},$$

since $\alpha_j \not\equiv \alpha_\ell \mod (p-1)$. Therefore $c_j \equiv 0 \pmod{p}$ and $a_j \equiv b_j \pmod{p^{k+1}}$ for $1 \le j \le t$. In a similar way, taking $x_1 := \rho, x_2 := \rho^2, \ldots, x_t := \rho^t$ in (5) knowing that $c_j = 0$ and $e_{p,k+1,k}$ is a group homomorphism we get for $e_\rho := e_{p,k+1,k}(\rho)$:

$$\sum_{j=1}^{t} a_j \rho^{i\alpha_j}(i\, e_\rho)\gamma_j \equiv 0 \pmod{p} \quad \text{for } 1 \le i \le t,$$

that leads to a Vandermonde linear system with determinant equal to

$$t!\, a_1 \cdots a_t\, e_\rho^t \rho^{\alpha_1} \prod_{j<\ell} (\rho^{\alpha_\ell} - \rho^{\alpha_j}) \not\equiv 0 \pmod{p},$$

since $e_\rho \not\equiv 0 \pmod{p}$. We conclude that $\gamma_j \equiv 0 \pmod{p}$ and therefore $\alpha_j \equiv \beta_j \pmod{\varphi(p^{k+1})}$. ☐

The question in order to apply Theorem 1.6 is whether, given a polynomial $f = \sum_{j=1}^{t} a_j x^{\alpha_j} \in \mathbb{Z}[x]$ and an odd prime number p such that f reduces well modulo p, there exist starting interpolating sets $\{x_1, \ldots, x_{2t}\} \subset \mathbb{Z}$ satisfying the assumption that $\Delta_p f(x_1, \ldots, x_{2t}) \not\equiv 0 \pmod{p}$.
The condition is independent from the polynomial coefficients a_i since we can factor out $a_1 \cdots a_t$ from $\Delta_p f$ and f reducing well modulo p implies that $a_i \not\equiv 0 \pmod{p}$. Proposition 1.14 below

gives examples of good starting sets modulo p independent from f (i.e. they are good for any polynomial $f \in \mathbb{Z}[x]$ with exactly t terms that reduces well modulo p).

Definition 1.12. Let p be an odd prime number, and $t \in \mathbb{N}$, $1 \le t \le p-1$. We say that $\{x_1, \dots, x_{2t}\} \subset \mathbb{Z}$ is a *good starting set modulo* p (for Newton-Hensel interpolation) if for every subset $\{\alpha_1, \dots, \alpha_t\} \subseteq \{0, \dots, p-2\}$, the quantity

$$\det \begin{pmatrix} x_1^{\alpha_1} & \dots & x_1^{\alpha_t} & e_2(x_1)x_1^{\alpha_1} & \dots & e_2(x_1)x_1^{\alpha_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ x_{2t}^{\alpha_1} & \dots & x_{2t}^{\alpha_t} & e_2(x_{2t})x_{2t}^{\alpha_1} & \dots & e_2(x_{2t})x_{2t}^{\alpha_t} \end{pmatrix} \not\equiv 0 \pmod{p}, \tag{6}$$

where $e_2 : \mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is the map of Notation 1.4.

Remark 1.13. While the previous determinant depends on the order chosen for the points x_i and the exponents α_j, the condition of being zero (respectively non-zero) does not.

Proposition 1.14. *The following sets $\{x_1, \dots, x_{2t}\} \subset \mathbb{Z}$ are good starting sets modulo p:*

(1) $\{x_1, \dots, x_{2t}\}$ *where* $x_i \equiv \rho^{i-1} \pmod{p^2}$, $1 \le i \le 2t$, *for* $\rho \in \mathbb{Z}$ *a primitive root modulo* p^2, *or, more generally, where* $x_i \equiv \rho^{a+i-1} \pmod{p^2}$, $1 \le i \le 2t$, *for* $\rho \in \mathbb{Z}$ *a primitive root modulo* p^2 *and* $a \in \mathbb{Z}$ *(*$2t$ *consecutive powers of a primitive root modulo* p^2*).*

(2) $\{x_1, \dots, x_{2t}\}$ *where* $x_i \equiv \rho^{i-1} \pmod{p}$ *and* $x_{t+i} = x_i + p$, $1 \le i \le t$, *for* $\rho \in \mathbb{Z}$ *a primitive root modulo* p, *or , more generally, where* $x_i, x_{t+i} \equiv \rho^{a+i-1} \pmod{p}$ *and* $x_{t+i} \not\equiv x_i \pmod{p^2}$, $1 \le i \le t$, *for* $\rho \in \mathbb{Z}$ *a primitive root modulo* p *and* $a \in \mathbb{Z}$ *(any set* $x_1, \dots, x_{2t}$ *where you choose 2 sets of* t *consecutive powers of a primitive root modulo* p*, formed by different elements modulo* p^2*).*

Proof. We show the main cases of the two items, since their generalizations are straight-forward. We denote by Δ_p the determinant modulo p defined in (6).

In the first case $x_i \equiv \rho^{i-1}$ modulo p^2 for $1 \le i \le 2t$. Denote $e := e_2(\rho)$, then $e \ne 0$ since ρ is a primitive root modulo p^2 and $e_2(x_i) = e_2(\rho^{i-1}) = (i-1)e_2(\rho) = (i-1)e$. Substituting in the definition we get

$$\begin{aligned} \Delta_p = \ & \det \begin{pmatrix} 1 & \dots & 1 & 0 & \dots & 0 \\ \rho^{\alpha_1} & \dots & \rho^{\alpha_t} & e\rho^{\alpha_1} & \dots & e\rho^{\alpha_t} \\ \rho^{2\alpha_1} & \dots & \rho^{2\alpha_t} & 2e\rho^{2\alpha_1} & \dots & 2e\rho^{2\alpha_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ \rho^{(2t-1)\alpha_1} & \dots & \rho^{(2t-1)\alpha_t} & (2t-1)e\rho^{(2t-1)\alpha_1} & \dots & (2t-1)e\rho^{(2t-1)\alpha_t} \end{pmatrix} \\ = \ & e^t \det \begin{pmatrix} 1 & \dots & 1 & 0 & \dots & 0 \\ \rho^{\alpha_1} & \dots & \rho^{\alpha_t} & \rho^{\alpha_1} & \dots & \rho^{\alpha_t} \\ \rho^{2\alpha_1} & \dots & \rho^{2\alpha_t} & 2\rho^{2\alpha_1} & \dots & 2\rho^{2\alpha_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ \rho^{(2t-1)\alpha_1} & \dots & \rho^{(2t-1)\alpha_t} & (2t-1)\rho^{(2t-1)\alpha_1} & \dots & (2t-1)\rho^{(2t-1)\alpha_t} \end{pmatrix} \end{aligned}$$

If we denote $z_i := \rho^{\alpha_i}$ for $1 \le i \le t$, then

$$\Delta_p = e^t \det \begin{pmatrix} 1 & \dots & 1 & 0 & \dots & 0 \\ z_1 & \dots & z_t & z_1 & \dots & z_t \\ z_1^2 & \dots & z_t^2 & 2z_1^2 & \dots & 2z_t^2 \\ \vdots & & \vdots & \vdots & & \vdots \\ z_1^{2t-1} & \dots & z_t^{2t-1} & (2t-1)z_1^{2t-1} & \dots & (2t-1)z_t^{2t-1} \end{pmatrix} \pmod{p}$$

The transpose of this last matrix is well-known. It arises in the Hermite interpolation problem while trying to interpolate a function by a polynomial f such that $f(z_i) = y_i$ and $f'(z_i) = y_i'$ for $1 \le i \le t$. Its determinant equals

$$(-1)^{t(t-1)/2} z_1 \cdots z_t \prod_{1\le i<j\le t} (z_j - z_i)^4.$$

Hence

$$\Delta_p = (-1)^{t(t-1)/2} e^t \rho^{\alpha_1+\cdots+\alpha_t} \prod_{1\le i<j\le t} (\rho^{\alpha_j} - \rho^{\alpha_i})^4 \pmod p.$$

Since $1 \le \alpha_i \le p-2$ are all distinct and ρ is a primitive root modulo p (by Observation 1.11), $\rho^{\alpha_i} \not\equiv \rho^{\alpha_j} \pmod p$ if $i \ne j$, hence $\Delta_p \not\equiv 0 \pmod p$ as wanted.
The general case reduces to this one factoring out from the determinant the (non-zero) term $\rho^{2a(\alpha_1+\cdots+\alpha_t)}$.

In the second case $x_i \equiv \rho^{i-1}$ modulo p and $x_{t+i} = x_i + p$ for $1 \le i \le t$. Then $e_2(x_{t+i}) \equiv e_2(x_i) - x_i^{-1} \pmod p$ for $1 \le i \le t$ since

$$(x_i+p)^{p-1} \equiv x_i^{p-1} + (p-1)\, p\, x_i^{p-2} \equiv 1 + p\,(e_2(x_i) - x_i^{-1}) \pmod{p^2}.$$

Thus, since $x_{t+i} \equiv x_i \pmod p$, we have modulo p:

$$\begin{aligned}
\Delta_p &= \det \begin{pmatrix} x_1^{\alpha_1} & \dots & x_1^{\alpha_t} & e_2(x_1)x_1^{\alpha_1} & \dots & e_2(x_1)x_1^{\alpha_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ x_t^{\alpha_1} & \dots & x_t^{\alpha_t} & e_2(x_t)x_t^{\alpha_1} & \dots & e_2(x_t)x_t^{\alpha_t} \\ x_1^{\alpha_1} & \dots & x_1^{\alpha_t} & (e_2(x_1)-x_1^{-1})x_1^{\alpha_1} & \dots & (e_2(x_1)-x_1^{-1})x_1^{\alpha_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ x_t^{\alpha_1} & \dots & x_t^{\alpha_t} & (e_2(x_t)-x_t^{-1})x_t^{\alpha_1} & \dots & (e_2(x_t)-x_t^{-1})x_t^{\alpha_t} \end{pmatrix} && \pmod p \\
&= \det \begin{pmatrix} x_1^{\alpha_1} & \dots & x_1^{\alpha_t} & e_2(x_1)x_1^{\alpha_1} & \dots & e_2(x_1)x_1^{\alpha_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ x_t^{\alpha_1} & \dots & x_t^{\alpha_t} & e_2(x_t)x_t^{\alpha_1} & \dots & e_2(x_t)x_t^{\alpha_t} \\ 0 & \dots & 0 & -x_1^{\alpha_1-1} & \dots & -x_1^{\alpha_t-1} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & -x_t^{\alpha_1-1} & \dots & -x_t^{\alpha_t-1} \end{pmatrix} && \pmod p \\
&= (-1)^t x_1^{-1} \dots x_t^{-1} \textstyle\prod_{1\le i<j\le t} (\rho^{\alpha_j} - \rho^{\alpha_i})^2 \not\equiv 0 && \pmod p.
\end{aligned}$$

For the general case observe that for $1 \le i \le t$, $x_{t+i} \equiv x_i + k_i p \pmod{p^2}$ for some k_i prime to p. ☐

Unfortunately, not every set $\{x_1, \dots, x_{2t}\}$ with $x_i \not\equiv 0 \pmod p$ is a good starting set modulo p:

Example 1.15. *Take $p := 7$, $\rho := 3$ and $t = 2$, $x_1 \equiv 3^0 \pmod 7$, $x_2 \equiv 3^1 \pmod 7$, $x_2 :\equiv 3^2 \pmod 7$ and $x_3 \equiv 3^4 \pmod 7$, then $e_2(3) = 6 \equiv -1 \pmod 7$, for $\alpha_1 := 0$ and $\alpha_2 := 3$ we obtain:*

$$\Delta_p \equiv \det \begin{pmatrix} 1 & 1 & 0 & 0 \\ 3^0 & 3^3 & -3^0 & -3^3 \\ 3^{2\cdot 0} & 3^{2\cdot 3} & -2\cdot 3^{2\cdot 0} & -2\cdot 3^{2\cdot 3} \\ 3^{4\cdot 0} & 3^{4\cdot 3} & -4\cdot 3^{4\cdot 0} & -4\cdot 3^{4\cdot 3} \end{pmatrix} \equiv \det \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -2 & -2 \\ 1 & 1 & -4 & -4 \end{pmatrix} \equiv 0 \pmod 7.$$

In particular, Proposition 1.14 implies that for any polynomial $f \in \mathbb{Z}[x]$ that reduces well modulo p and with exactly t non-zero terms , there exists a subset of size $2t$ in $\{1, \dots, 2p-1\}$, $x_1, \dots, x_{2t}$, that satisfies the hypothesis of Theorem 1.6, i.e. such that $\Delta_p f(x_1, \dots, x_{2t}) \not\equiv 0 \pmod{p}$. In the case of a binomial, this result can be sharpened: for any prime $p \geq 5$, there exists a subset $\{x_1, \dots, x_4\} \subset \{1, \dots, p-1\}$ with $\Delta_p f(x_1, \dots, x_4) \not\equiv 0 \pmod{p}$.

Proposition 1.16. *Let $p \geq 5$ be a prime number and $0 \leq \alpha < \beta < p-1$. Then*

$$\begin{pmatrix} 1^\alpha & 1^\beta & e_2(1)1^\alpha & e_2(1)1^\beta \\ 2^\alpha & 2^\beta & e_2(2)2^\alpha & e_2(2)2^\beta \\ \vdots & \vdots & \vdots & \vdots \\ (p-1)^\alpha & (p-1)^\beta & e_2(p-1)\,(p-1)^\alpha & e_2(p-1)\,(p-1)^\beta \end{pmatrix} \pmod{p}$$

has rank four, where $e_2 : \mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is the map of Notation 1.4.

We omit the proof of this fact since it is quite tedious and is based on a smart choice of the four elements x_i depending on congruences of $\alpha - \beta$ modulo 2 , modulo $(p-1)$ and on the behavior of $e_2(x_i)$. □

Unfortunately this result is not true in general since for $p := 11$, the polynomial $f = a_1 + a_2\, x + a_3\, x^3 + a_4\, x^5 + a_5 x^8$ has five non-zero terms but $\Delta_p\, f(1, \dots, 10) \equiv 0 \pmod{11}$. Surprisingly, computer experiments performed with [PARI/GP] did not show any counter-example for trinomials (with any prime) nor polynomials with 5 terms for a prime different from 11 .

For an arbitrary odd prime number p , there may be more good starting sets modulo p for a given t than the sets described in Proposition 1.14 but we are still unable to prove their existence in general. For instance for $p = 7$ and $t = 2$, the set $\{1, 2, 3, 6\}$ is good but is neither of type (1) nor of type (2). Actually in that case the total number of sets is 10626 , from which 1640 are good but only 560 are of type (1) or (2).

In what follows, we compute the number of different good starting sets as in Proposition 1.14 on the interval $\{1, \dots, p^2-1\}$ in order to estimate (at least from below) the probability of having a good starting set modulo p when choosing any subset of $\{1, \dots, p^2-1\}$.
A first question we have to deal with is whether the sets described of type (1) and type (2) of Proposition 1.14 are distinct when choosing arbitrarily a primitive root modulo p^2 or modulo p and a starting exponent a . To make this analysis we need to distinguish the case $t = p-1$ from $t < p-1$.

Observation 1.17. *If $t = p-1$, the good starting sets modulo p of type (1) in Proposition 1.14 are contained in type (2) while if $t < p-1$ type (1) and (2) define different good starting sets.*

Proof. For $t = p-1$, this is clear since the set of $p-1$ consecutive powers of a primitive root modulo p coincides with the set $\{1, \dots, p-1\}$ and a primitive root modulo p^2 is a primitive root modulo p . For $t < p-1$, in a set $\{\rho^a, \rho^{a+2t-1}\}$ of type (1) there are more than t consecutive primitive roots modulo p that cannot appear in a set of type (2). □

Proposition 1.18. *For $t = p-1$ there are at least $\binom{p}{2}^{p-1}$ good starting sets modulo p in the set $\{1, \dots, p^2-1\}$.*

Proof. We simply choose for each i , $1 \leq i \leq p-1$, two different elements congruent to i modulo p . There are $\binom{p}{2}^{p-1}$ such choices. □

Taking into account that the number of subsets of size $2(p-1)$ in $\{1,\dots,p^2-1\}$, avoiding the multiples of p, equals $\binom{p(p-1)}{2(p-1)}$, this gives a ratio of

$$\frac{\binom{p}{2}^{p-1}}{\binom{p(p-1)}{2(p-1)}} \approx \frac{1}{p(p-1)^{p-1}}$$

good starting sets modulo p, which is obviously a very small quantity.

For $t < p-1$ we need to perform a more careful analysis:

Lemma 1.19. *Let $n \in \mathbb{N}, n > 2$ and $\mathcal{C} := \{0,1,\dots,s\} \subset \mathbb{Z}/n\mathbb{Z}$ where $1 \le s < n-1$. If $\sigma(x) = m\,x + a$ is a bijective map of $\mathbb{Z}/n\mathbb{Z}$ into itself such that $\sigma(\mathcal{C}) = \mathcal{C}$, then $\sigma = Id$ or $\sigma = -Id + s$.*

Proof. Without loss of generality we may suppose $1 \le m < n$ and $0 \le a < n$. Furthermore we may restrict to the case $s < n/2$ since if not $\overline{\mathcal{C}} = \{s+1,\dots,n-1\}$ is also fixed by σ. Then the bijective map $\tau(x) = \sigma(x+s+1) - (s+1)$ fixes $\{0,1,\dots,n-s-2\}$ (where $n-s-2 < n/2$) and satisfies that $\sigma = Id \Leftrightarrow \tau = Id$ and $\sigma = -Id + s \Leftrightarrow \tau = -Id + (n-s-2)$. We consider two different cases:

- Case $a = 0$. Note that in this case $m < n/2$ since $\sigma(1) = m \in \mathcal{C}$. We need to show that $\sigma = Id$. Assume that $m > 1$, then by the Euclidean algorithm $s = qm + r$ with $0 \le r < m$. In particular $q < s$ since $m > 1$, therefore $q+1 \in \mathcal{C}$ and $\sigma(q+1) \in \mathcal{C}$, i.e. $\sigma(q+1) \le s$. But $0 \le (q+1)m \le s+m < n/2+n/2 = n$ implies that $\sigma(q+1) = (q+1)m$, and, on the other side, $(q+1)m > qm + r = s$. Contradiction.
- Case $a > 0$. Assuming $m > 1$ we will prove that $m = n-1$ and $a = s$.

  Note that $m > s$ since if not let $\mathcal{A} := \{0 \le x \le n-1 : mx + a \le s\}$. Clearly $\mathcal{A}$ is non-empty ($0 \in \mathcal{A}$), denote by y its maximum element, i.e. $my + a \le s$ and $m(y+1)+a > s$. Since $m \le s$, $0 \le m(y+1) + a \le 2s < n$, then $\sigma(y+1) = m(y+1) + a$. Since $m > 1$ and $my + a \le s$, $y < s$ thus $y+1 \in \mathcal{C}$. But then $\sigma(y+1) \le s$ and also $m(y+1)+a > s$, a contradiction. Then $s < m \le n-1$.

  In that case, $\sigma(s) = 0$ since if $\sigma(y) = 0$ for $y < s$, then $\sigma(y+1) = m \le s$ (σ is bijective on $\mathcal{C}$), which is not the case. Thus there exists $z < s$ such that $\sigma(z) = 1$ and $\sigma(z+1) = m+1 \in \mathcal{C}$. That is, $s+1 < m+1 \le n$ belongs to $\mathcal{C}$ $\bmod n$. That means that $m+1 \equiv 0 \mod n$ and $m = n-1$. We conclude, since $0 = \sigma(s) = -s + a$, that $a = s$.

∎

Corollary 1.20. *Let $\rho, \varrho \in \mathbb{Z}$ be two different primitive roots $\bmod p^k$. Then, for any s, $1 \le s < \varphi(p^k)$, the sets $\rho^a\{1,\rho,\dots,\rho^{s-1}\}$ and $\varrho^b\{1,\varrho,\dots,\varrho^{s-1}\}$ coincide modulo p^k if and only if $\varrho \equiv \rho \pmod{p^k}$ and $b \equiv a \pmod{\varphi(p^k)}$ or $\varrho \equiv \rho^{-1} \pmod{p^k}$ and $b \equiv -(a+s-1) \pmod{\varphi(p^k)}$.*

Proof. Without loss of generality we may assume $\varrho = \rho^m$ for some m prime to $\varphi(p^k)$. Then the two sets coincide if and only if $\{1,\rho,\dots,\rho^{s-1}\}$ and $\rho^{mb-a}\{1,\rho^m,\dots,\rho^{m\,s-1}\}$ coincide, i.e. if the bijective map $\sigma(x) = m\,x + (mb-a)$ of $\mathbb{Z}/\varphi(p^k)\mathbb{Z}$ fixes the set $\{0,1,\dots,s-1\}$. We apply Lemma 1.19 to conclude that $\sigma = Id$, that is $m \equiv 1 \pmod{\varphi(p^k)}$, and $a \equiv b \pmod{\varphi(p^k)}$ or $\sigma = -Id + s$, that is $m \equiv -1 \pmod{\varphi(p^k)}$ and $b \equiv -(a+s-1) \pmod{\varphi(p^k)}$. ∎

As an immediate consequence we can compute the number of good sets of type (1) and (2) in Proposition 1.14 for $t < p-1$:

Corollary 1.21. *Let p be an odd prime number and set $1 \le t < p-1$. There are at least*

$$p\,\varphi(p-1)(p-1)^2/2 + \binom{p}{2}^t \varphi(p-1)(p-1)/2$$

good starting sets modulo p in the set $\{1,\dots,p^2-1\}$.

Proof. First we count the sets of type (1) in Proposition 1.14: We choose a primitive root ρ modulo p^2, there are $\varphi(\varphi(p^2))$ such choices, and we choose $0 \le a < \varphi(p^2)$. Since $t < p-1$, $2t < \varphi(p^2)$ we can apply the previous lemma and divide the total number by 2.
Next we count the sets of type (2): We first compute the number of sets modulo p, i.e. the number of different sets $\left\{\rho^{a+i-1} \pmod p \ : \ 1 \le i \le t\right\}$ in the set $\{1,\dots,p-1\}$. Applying the previous lemma, there are $\varphi(p)\varphi(\varphi(p))/2$ such different choices. Then for $1 \le i \le t$ we freely choose x_i, x_{t+i} congruent to ρ^{a+i-1} but different. There are $\binom{p}{2}^t$ such choices. □

Like in the case $t = p-1$, the ratio is again very deceptive: given p and t the probability of choosing randomly a good starting set modulo p is very low and tends to *zero* when p grows. However, a more realistic probability estimation would be to compute, given an odd prime number p and $f \in \mathbb{Z}[x]$ a polynomial with exactly $t < p$ non zero terms that reduces well modulo p, the probability that randomly chosen $\{x_1,\dots,x_{2t}\} \subset \{0,\dots,p^2-1\}$ satisfy that Determinant (6) does not vanish modulo p. Unfortunately we are still not able to give a sharp estimation for that probability.

2. p-adic equations

This section shows how Newton-Hensel construction of Theorem 1.6 corresponds to an usual Hensel lemma on the p-adic integers $\mathbb{Z}_p$. It explains the role played by the e_2 group homomorphism of Proposition 1.2 and why starting sets modulo p need to contain a primitive root modulo p^2. We begin by recalling some definitions and properties of $\mathbb{Z}_p$. We refer to [Ser70, Ch.II] for the details.

For a prime integer p, the set of p-adic integers $\mathbb{Z}_p$ is the inverse limit of the diagram

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\phi_1} Z/p^2\mathbb{Z} \xleftarrow{\phi_2} \mathbb{Z}/p^3\mathbb{Z} \xleftarrow{\phi_3} \cdots,$$

where $\phi_k : \mathbb{Z}/p^{k+1}\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ is the canonical projection. Here we will view $\mathbb{Z}_p$ as the equivalent construction

$$\mathbb{Z}_p = \left\{(a_k)_{k\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}} \ : \ a_{k+1} \equiv a_k \pmod{p^k} \ \forall k \in \mathbb{N}\right\} / \sim$$

where $\sim$ is the equivalence relation defined by

$$(a_k)_{k\in\mathbb{N}} \sim (b_k)_{k\in\mathbb{N}} \iff a_k \equiv b_k \pmod{p^k} \ \forall k \in \mathbb{N}.$$

and the operations are coordinate-wise, i.e.:

$$\overline{(a_k)}_{k\in\mathbb{N}} + \overline{(b_k)}_{k\in\mathbb{N}} := \overline{(a_k+b_k)}_{k\in\mathbb{N}} \quad \text{and} \quad \overline{(a_k)}_{k\in\mathbb{N}} \cdot \overline{(b_k)}_{k\in\mathbb{N}} := \overline{(a_k \cdot b_k)}_{k\in\mathbb{N}}.$$

In this formulation, $a := \overline{(a_k)}_{k\in\mathbb{N}} \in \mathbb{Z}_p^\times$, the multiplicative group of p-adic units, if and only if $p \nmid a_1$.

From now on p will denote an odd prime number. In this case the multiplicative group $\mathbb{Z}_p^\times$ and the additive group $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ are isomorphic. This last additive group can be viewed in another additive way, closely related to the changes of exponents we allow in Theorem 1.6 and that justifies a convenient exponentiation in $\mathbb{Z}_p^\times$. For that purpose, we construct the ring of *exponents* that we will denote $\mathcal{E}_p$:

Definition 2.1. Let p be an odd prime number. We define $\mathcal{E}_p$ as the inverse limit of the following diagram:

$$\mathbb{Z}/\varphi(p)\mathbb{Z} \xleftarrow{\rho_1} Z/\varphi(p^2)\mathbb{Z} \xleftarrow{\rho_2} \mathbb{Z}/\varphi(p^3)\mathbb{Z} \xleftarrow{\rho_3} \cdots,$$

where, since $\varphi(p^k) \mid \varphi(p^{k+1})$, $\rho_k : \mathbb{Z}/\varphi(p^{k+1})\mathbb{Z} \to \mathbb{Z}/\varphi(p^k)\mathbb{Z}$ is the well-defined canonical projection.

Equivalently, $\mathcal{E}_p$ can be seen as the ring

$$\mathcal{E}_p = \left\{(\alpha_k)_{k\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}} \; : \; \alpha_{k+1} \equiv \alpha_k \pmod{\varphi(p^k)} \; \forall\, k \in \mathbb{N}\right\} / \approx$$

where $\approx$ is the equivalence relation defined by

$$(\alpha_k)_{k\in\mathbb{N}} \approx (\beta_k)_{k\in\mathbb{N}} \iff \alpha_k \equiv \beta_k \pmod{\varphi(p^k)} \; \forall\, k \in \mathbb{N}.$$

where the operations are coordinate-wise, i.e.:

$$\overline{(\alpha_k)}_{k\in\mathbb{N}} + \overline{(\beta_k)}_{k\in\mathbb{N}} := \overline{(\alpha_k+\beta_k)}_{k\in\mathbb{N}} \quad \text{and} \quad \overline{(\alpha_k)}_{k\in\mathbb{N}} \cdot \overline{(\beta_k)}_{k\in\mathbb{N}} := \overline{(\alpha_k\cdot\beta_k)}_{k\in\mathbb{N}}.$$

In this formulation, $\alpha := \overline{(\alpha_k)}_{k\in\mathbb{N}} \in \mathcal{E}_p^\times$ if and only if $\gcd(\alpha_2, \varphi(p^2)) = 1$, and we have the ring isomorphism

$$\mathcal{E}_p \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p : \quad \overline{(\alpha_k)}_{k\in\mathbb{N}} \mapsto (\alpha_1, \overline{(\alpha_k)}_{k\geq 2}).$$

Next proposition shows that $\mathcal{E}_p$ is a natural set of exponents for $\mathbb{Z}/p\mathbb{Z}^\times$:

Proposition 2.2. *Let* $a := \overline{(a_k)}_{k\in\mathbb{N}} \in \mathbb{Z}_p^\times$ *and* $\alpha := \overline{(\alpha_k)}_{k\in\mathbb{N}} \in \mathcal{E}_p$, *then* $a^\alpha := \overline{(a_k^{\alpha_k})}_{k\in\mathbb{N}} \in \mathbb{Z}_p^\times$.

Proof.

- It is immediate that $a_k \equiv a'_k \pmod{p^k}$ and $\alpha_k \equiv \alpha'_k \pmod{\varphi(p^k)}$ implies $a_k^{\alpha_k} \equiv (a'_k)^{\alpha_k} \equiv (a'_k)^{\alpha'_k} \pmod{p^k}$ since $a_k \not\equiv 0 \pmod{p}$.
- Similarly, $a_{k+1} \equiv a_k \pmod{p^k}$ and $\alpha_{k+1} \equiv \alpha_k \pmod{\varphi(p^k)}$ implies $a_{k+1}^{\alpha_{k+1}} \equiv a_{k+1}^{\alpha_k} \equiv a_k^{\alpha_k} \pmod{p^k}$.

□

Corollary 2.3. *For a given* $\alpha \in \mathcal{E}_p$, *the map* $\mathbb{Z}_p^\times \to \mathbb{Z}_p^\times : a \mapsto a^\alpha$ *is a group homomorphism. Moreover if* $\alpha \in \mathcal{E}_p$ *is invertible, this map is an isomorphism since* $b = a^\alpha \Leftrightarrow a = b^{\alpha^{-1}}$.

Lemma 2.4. *For a given* $a \in \mathbb{Z}_p^\times$, *the map* $(\mathcal{E}_p, +) \to (\mathbb{Z}_p^\times, \cdot) : \alpha \mapsto a^\alpha$ *is a group homomorphism. Moreover, this map is an isomorphism if and only if* $a := \overline{(a_k)}_{k\in\mathbb{N}}$ *is such that* a_2 *is a primitive root modulo* p^2. *We call such* a a good basis for taking logarithms*.*

Proof. Note that if $a := \overline{(a_k)}_{k\in\mathbb{N}}$ is such that a_2 is a primitive root modulo p^2, then a_k is a primitive root modulo p^k for all $k \in \mathbb{N}$ (see for instance [Apo76, Th.10.6]). Now for $b := \overline{(b_k)}_{k\in\mathbb{N}} \in \mathbb{Z}_p^\times$, we let α_k be such that $a_k^{\alpha_k} \equiv b_k \pmod{p^k}$ and we define $\alpha := \overline{(\alpha_k)}_{k\in\mathbb{N}}$. It is easy to check that $\alpha \in \mathcal{E}_p$, and $a^\alpha = b$.
Conversely, we want to check that a_2 is a primitive root modulo p^2 if the map is onto. For each $1 \leq b_2 < p^2$, with $\gcd(b_2, p) = 1$, let $b := \overline{(b_2)}_{k\in\mathbb{N}} \in \mathbb{Z}_p^\times$ (the natural injection of $\mathbb{Z}$ into $\mathbb{Z}_p$), and let α be such that $a^\alpha = b$. In particular $a_2^{\alpha_2} \equiv b_2 \pmod{p^2}$, i.e. the powers of a_2 span $(\mathbb{Z}/p^2\mathbb{Z})^\times$ then a_2 is a primitive root. □

In particular, if $\rho \in \mathbb{Z}$ is a primitive root modulo p^2, then $\rho := \overline{(\rho)}_{k\in\mathbb{N}} \in \mathbb{Z}_p^\times$ is a good basis for taking logarithms.

In view of the previous discussion, for $a_j \in \mathbb{Z}_p^\times, \alpha_j \in \mathcal{E}_p, 1 \leq j \leq t$, the specialization

$$\mathbb{Z}_p^\times \to \mathbb{Z}_p : \quad x \mapsto f(x) := \sum_{j=1}^{t} a_j x^{\alpha_j}$$

is a well-defined map. As a consequence of Proposition 1.10, two such maps $f = \sum_{j=1}^t a_j x^{\alpha_j}$ and $g = \sum_{j=1}^t b_j x^{\beta_j}$ coincide on $\mathbb{Z}_p^\times$ if and only if $a_j = b_j$ in $\mathbb{Z}_p^\times$ and $\alpha_j = \beta_j$ in $\mathcal{E}_p$, $1 \leq j \leq t$, i.e. $f = g$. In this setting Theorem 1.6 admits the following formulation:

Theorem 2.5. (Newton-Hensel interpolation lifting on $\mathbb{Z}_p$)
Let p be an odd prime number, and $t \in \mathbb{N}$, $1 \le t \le p-1$. Set $y_1, \dots, y_{2t} \in \mathbb{Z}_p$. Let $f_1 := \sum_{j=1}^t a_{j1} x^{\alpha_{j1}} \in \mathbb{Z}[x]$ and $x_1 = \overline{(x_{1k})_k}, \dots, x_{2t} = \overline{(x_{(2t)k})_k} \in \mathbb{Z}_p^\times$ satisfy

- $f_1(x_i) \equiv y_i \pmod p$, $1 \le i \le 2t$,
- $\det \begin{pmatrix} x_1^{\alpha_1} & \dots & x_1^{\alpha_t} & a_1 e_2(x_{12}) x_1^{\alpha_1} & \dots & a_t e_2(x_{12}) x_1^{\alpha_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ x_{2t}^{\alpha_1} & \dots & x_{2t}^{\alpha_t} & a_1 e_2(x_{(2t)2}) x_{2t}^{\alpha_1} & \dots & a_t e_2(x_{(2t)2}) x_{2t}^{\alpha_t} \end{pmatrix} \not\equiv 0 \pmod p$,

  where $e_2(x_i) : (\mathbb{Z}/p^2\mathbb{Z})^\times \to \mathbb{Z}/p\mathbb{Z}$ is the group homomorphism of Definition 1.1.

Then there exists a unique $f := \sum_{j=1}^t a_j x^{\alpha_j}$ with $a_j \in \mathbb{Z}_p^\times$ and $\alpha_j \in \mathcal{E}_p$, $1 \le j \le t$, that satisfies simultaneously:

- *$f(x_i) = y_i$ in $\mathbb{Z}_p$, $1 \le i \le 2t$.*
- *$a_j = \overline{(a_{j1}, \dots)}, \alpha_j = \overline{(\alpha_{j1}, \dots)}$, $1 \le j \le t$.*

In fact, this theorem is a particular case of a more general type of equations in $\mathbb{Z}_p$. We deal now with two types of equations: generalized polynomial ones and exponential ones, and we exhibit the duality they inherit from Lemma 2.4.

Definition 2.6.

- A *generalized polynomial equation in* $\mathbb{Z}_p^\times$ is
$$f(x) := \sum_{j=1}^t a_j x^{\alpha_j}$$
where $t \in \mathbb{N}, a_j \in \mathbb{Z}_p$ and $\alpha_j \in \mathcal{E}_p$, $1 \le j \le t$, are given, and $x \in \mathbb{Z}_p^\times$ is the unknown.
- An *exponential equation in* $\mathcal{E}_p$ is
$$g(\alpha) := \sum_{j=1}^t a_j x_j^\alpha$$
where $t \in \mathbb{N}, a_j \in \mathbb{Z}_p$ and $x_j \in \mathbb{Z}_p^\times$, $1 \le j \le t$, are given, and $\alpha \in \mathcal{E}_p$ is the unknown.

Observation 2.7. *Solving a generalized polynomial equation in $\mathbb{Z}_p^\times$ or an exponential equation in $\mathcal{E}_p$ are essentially the same problem, since if $a \in \mathbb{Z}_p^\times$ is a good basis for taking logarithms, setting $x = a^\alpha$ and $x_i = a^{\alpha_i}$ we obtain*
$$\sum_{j=1}^t a_j \, x^{\alpha_j} = \sum_{j=1}^t a_j \, x_j^\alpha.$$

The two next propositions generalize Hensel's lemma, traditionally for polynomials in $\mathbb{Z}[x]$ or $\mathbb{Z}_p[x]$, to the previous equations. We state them before giving their proofs to highlight their dual character.

Proposition 2.8. *Set $t \in \mathbb{N}$, $y, a_j \in \mathbb{Z}_p$ and $\alpha_j := \overline{(\alpha_{jk})_k} \in \mathcal{E}_p$, $1 \le j \le t$. Let $x_1 \in \mathbb{Z}$, $p \nmid x_1$, be such that*

- $f(x_1) := \sum_{j=1}^t a_j \, x_1^{\alpha_j} \equiv y \pmod p$,
- $\sum_{j=1}^t a_j \, \alpha_{j2} \, x_1^{\alpha_j - 1} \not\equiv 0 \pmod p$,

then there exists a unique $x = \overline{(x_1, x_2, \dots)} \in \mathbb{Z}_p^\times$ such that $f(x) = y$ in $\mathbb{Z}_p$.

Proposition 2.9. *Set $t \in \mathbb{N}$, $y, a_j \in \mathbb{Z}_p$ and $x_j := \overline{(x_{jk})_k} \in \mathbb{Z}_p^\times$, $1 \le j \le t$. Let $\alpha_1 \in \mathbb{Z}$ be such that*

- $g(\alpha_1) := \sum_{j=1}^{t} a_j\, x_j^{\alpha_1} \equiv y \pmod{p}$,
- $\sum_{j=1}^{t} a_j\, e_2(x_{j2})\, x_j^{\alpha_1} \not\equiv 0 \pmod{p}$ *where* e_2 *is the group homomorphism defined in Definition 1.1,*

then there exists a unique $\alpha = \overline{(\alpha_1, \alpha_2, \dots)} \in \mathcal{E}_p$ *such that* $g(\alpha) = y$ *in* $\mathbb{Z}_p$.

Proof. (of Proposition 2.8)
We are looking for $x := \overline{(x_k)}_k \in \mathbb{Z}_p^\times$ such that

$$f(x_k) = \sum_{j=1}^{t} a_j\, x_k^{\alpha_j} \equiv \sum_{j=1}^{t} a_{jk}\, x_k^{\alpha_{jk}} \equiv y_k \pmod{p^k}.$$

We construct it inductively starting from the given x_1 . The condition $p \nmid x_1$ guarantees that $x \in \mathbb{Z}_p^\times$. Let $k \in \mathbb{N}$ and assume there is a unique x_k such that $x_k \equiv x_1 \pmod{p}$ and $f(x_k) \equiv y_k \pmod{p^k}$. If we denote $a_j := \overline{(a_{jk})}_k$, $y := \overline{(y_k)}_k$, we are looking for x_{k+1} such that $f(x_{k+1}) \equiv y_{k+1} \pmod{p^{k+1}}$. This implies $f(x_{k+1}) \equiv y_k \pmod{p^k}$ and thus $x_{k+1} = x_k + p^k \xi$ where ξ is to be uniquely determined modulo p . We use the same arguments as in the proof of Theorem 1.6. Since $a_{j(k+1)} \equiv a_{jk} \pmod{p^k}$, $y_{k+1} \equiv y_k \pmod{p^k}$ and $\alpha_{j(k+1)} \equiv \alpha_{jk} \pmod{\varphi(p^k)}$, using the fact that $f(x_k) \equiv y_k \pmod{p^k}$ there exists $z \in \mathbb{Z}$ such that

$$y_{k+1} - \sum_{j=1}^{t} a_{j(k+1)} x_k^{\alpha_{j(k+1)}} \equiv p^k\, z \pmod{p^{k+1}}.$$

We obtain, by Newton expansion,

$$\begin{array}{rrcll} & f(x_{k+1}) & \equiv & \sum_{j=1}^{t} a_{j(k+1)}(x_k + p^k \xi)^{\alpha_{j(k+1)}} & \pmod{p^{k+1}} \\ & & \equiv & \sum_{j=1}^{t} (a_{j(k+1)} x_k^{\alpha_{j(k+1)}} + p^k\, \alpha_{j(k+1)}\, x_k^{\alpha_{j(k+1)}-1}\, \xi) & \pmod{p^{k+1}} \\ & & \equiv & y_{k+1} & \pmod{p^{k+1}} \\ \iff & p^k\, z & \equiv & p^k \sum_{j=1}^{t} a_{j(k+1)}\, \alpha_{j(k+1)}\, x_k^{\alpha_{j(k+1)}-1} \xi & \pmod{p^{k+1}} \\ \iff & z & \equiv & (\sum_{j=1}^{t} a_{j(k+1)}\, \alpha_{j(k+1)}\, x_k^{\alpha_{j(k+1)}-1})\, \xi & \pmod{p}. \end{array}$$

Now, by hypothesis, since $\alpha_{j(k+1)} \equiv \alpha_{j2} \pmod{p}$ for $p \mid \varphi(p^2)$, we conclude:

$$\begin{array}{rcll} 0 & \not\equiv & \sum_{j=1}^{t} a_j\, \alpha_{j2}\, x_1^{\alpha_j - 1} & \pmod{p} \\ 0 & \not\equiv & \sum_{j=1}^{t} a_{j(k+1)}\, \alpha_{j(k+1)} x_1^{\alpha_{j(k+1)}-1} & \pmod{p}, \end{array}$$

and therefore, there exists a unique ξ modulo p that solves the problem. □

Proof. (of Proposition 2.9) The exponential equation $g(\alpha) = \sum_{j=1}^{t} a_j x_j^{\alpha} = y$ has a unique solution $\alpha \in \mathcal{E}_p$ such that $\alpha \equiv \alpha_1 \pmod{(p-1)}$ if and only if the generalized polynomial equation $f(\xi) = \sum_{j=1}^{t} a_j \xi^{\beta_j} = y$ has a unique solution $\xi \in \mathbb{Z}_p^\times$ such that $\xi \equiv \xi_1 \pmod{p}$, where $\xi := b^{\alpha}$ and $x_j := b^{\beta_j}$, $1 \le j \le t$, for a good basis b for taking logarithms.
We check the assumption of Proposition 2.8:

$$\begin{aligned} \sum_{j=1}^{t} a_{j1}\, \beta_{j2}\, \xi_1^{\beta_{j1}-1} \not\equiv 0 \pmod{p} \quad &\iff \quad \sum_{j=1}^{t} a_{j1}\, \beta_{j2}\, b_1^{\alpha_1(\beta_{j1}-1)} \not\equiv 0 \pmod{p} \\ &\iff \quad \sum_{j=1}^{t} a_{j1}\, \beta_{j2}\, x_{j1}^{\alpha_1} \not\equiv 0 \pmod{p}. \end{aligned}$$

Here we used $b_1^{-\alpha_1} \not\equiv 0 \pmod{p}$ since $p - 1 \nmid \alpha_1$ and b_1 is a primitive root modulo p .

Now, we apply the group homomorphism e_2 to $x_{j2} = b_2^{\beta_{j2}}$: $e_2(x_{j2}) \equiv \beta_{j2}\, e_2(b_2) \pmod p$. Moreover, since b_2 is a primitive root $\bmod\, p^2$, $e_2(b_2) \not\equiv 0 \pmod p$. Thus

$$\sum_{j=1}^{t} a_{j1}\,\beta_{j2}\,x_{j1}^{\alpha_1} \not\equiv 0 \pmod p \Longleftrightarrow \sum_{j=1}^{t} a_{j1}\,e_2(x_{j2})\,x_{j1}^{\alpha_1} \not\equiv 0 \pmod p.$$

$\square$

We observe that in both propositions, the second assumption on x_1 and α_1 respectively is the one that corresponds to the usual $f'(x_1) \not\equiv 0 \pmod p$ in the classical Newton-Hensel lemma. Here, taking derivatives is not a closed operation (because $\alpha_2 \not\equiv \alpha_1 \pmod p$ but modulo $(p-1)$) and the assumption on the second order is the natural replacement of the derivative. Therefore, both for a generalized polynomial equation $f(x) = \sum_j a_j x^{\alpha_j}$ and for an exponential equation $g(\alpha) = \sum_j a_j x_j^{\alpha}$, we call the expressions

$$(7) \qquad \Delta_p\, f(x) := \sum_j a_j\,\alpha_{j2}\,x^{\alpha_j - 1} \pmod p \quad \text{and} \quad \Delta_p\, g(\alpha) := \sum_j a_j\,e_2(x_{j2})\,x_j^{\alpha_1} \pmod p$$

their *pseudo-derivatives* modulo p.

Like the usual Newton-Hensel lemma, Propositions 2.8 and 2.9 generalize to their Implicit Function Theorem versions for *systems of generalized polynomial* and *exponential equations* in $\mathbb{Z}_p$. We set a couple of notations.

Notation 2.10. We fix $m, n \in \mathbb{N}, t_1, \dots, t_m \in \mathbb{N}$, and for each $1 \le i \le m$ a multivariate generalized polynomial equation and a multivariate exponential equation

$$f_i(x_1, \dots, x_n) := \sum_{j=1}^{t_i} a_j^{(i)} x_1^{\alpha_j^{(i1)}} \cdots x_n^{\alpha_j^{(in)}} \quad \text{and} \quad g_i(\alpha_1, \dots, \alpha_n) := \sum_{j=1}^{t_i} a_j^{(i)} (x_j^{(i1)})^{\alpha_1} \cdots (x_j^{(in)})^{\alpha_n},$$

where $a_j^{(i)} \in \mathbb{Z}_p, \alpha_j^{(i\ell)} \in \mathcal{E}_p, x_j^{(i\ell)} \in \mathbb{Z}_p^\times$, are given.

- For a *system of m generalized polynomial equations in n unknowns* $x_1, \dots, x_n \in \mathbb{Z}_p^\times$:
$$\mathbf{f}(\mathbf{x}) = (f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)),$$
we denote by $J_p\, \mathbf{f}(\mathbf{x})$ its *pseudo-jacobian* matrix modulo p:
$$J_p\, \mathbf{f}(\mathbf{x}) := \begin{pmatrix} \Delta_p\, f_1(x_1) & \dots & \Delta_p\, f_1(x_n) \\ \vdots & & \vdots \\ \Delta_p\, f_m(x_1) & \dots & \Delta_p\, f_m(x_n) \end{pmatrix} \in (\mathbb{Z}/p\mathbb{Z})^{m \times n}.$$
- For a *system of m exponential equations in n unknowns* $\alpha_1, \dots, \alpha_n \in \mathcal{E}_p$:
$$\mathbf{g}(\alpha) = (g_1(\alpha_1, \dots, \alpha_n), \dots, g_m(\alpha_1, \dots, \alpha_n)),$$
we denote by $J_p\, \mathbf{g}(\alpha)$ its *pseudo-jacobian* matrix modulo p:
$$J_p\, \mathbf{g}(\alpha) := \begin{pmatrix} \Delta_p\, g_1(\alpha_1) & \dots & \Delta_p\, g_1(\alpha_n) \\ \vdots & & \vdots \\ \Delta_p\, g_m(\alpha_1) & \dots & \Delta_p\, g_m(\alpha_n) \end{pmatrix} \in (\mathbb{Z}/p\mathbb{Z})^{m \times n},$$

where $\Delta_p\, f_i(x_\ell)$ and $\Delta_p\, g_i(\alpha_\ell)$ are the corresponding generalizations of Formula (7):

$$\begin{aligned} \Delta_p\, f_i(x_\ell) \quad &:= \quad \textstyle\sum_j a_j^{(i)}\,\alpha_{j2}^{(i\ell)}\,x_\ell^{-1}\,x_1^{\alpha_j^{(i1)}} \cdots x_n^{\alpha_j^{(in)}} && \pmod p \\ \Delta_p\, g_i(\alpha_\ell) \quad &:= \quad \textstyle\sum_j a_j^{(i)}\,e_2(x_{j2}^{(i\ell)})\,(x_j^{(i1)})^{\alpha_1} \cdots (x_j^{(in)})^{\alpha_n} && \pmod p. \end{aligned}$$

Proposition 2.11. *For $m \le n$, let $\mathbf{f}(\mathbf{x})$ denote a system of m generalized polynomial equations in $\mathbb{Z}_p$ in n unknowns $x_1, \dots, x_n \in \mathbb{Z}_p^\times$, and let $\mathbf{y} := (y_1, \dots, y_m) \in \mathbb{Z}_p^m$. Let $\mathbf{x}_1 = (x_{11}, \dots, x_{n1}) \in \mathbb{Z}^n$, $p \nmid x_{\ell 1}$, $1 \le \ell \le n$, be such that*

- $\mathbf{f}(\mathbf{x}_1) \equiv \mathbf{y} \pmod{p}$,
- $J_p\,\mathbf{f}(\mathbf{x}_1) \pmod{p}$ *has rank* m,

then there exists $\mathbf{x} = (x_1, \dots, x_n) \in (\mathbb{Z}_p^\times)^n$ such that $x_\ell = \overline{(x_{\ell 1}, \dots)}$, $1 \le \ell \le n$, and $\mathbf{f}(\mathbf{x}) = \mathbf{y}$ in $\mathbb{Z}_p$.

Proposition 2.12. *For $m \le n$, let $\mathbf{g}(\alpha)$ denote a system of m exponential equations in $\mathbb{Z}_p$ in n unknowns $\alpha_1, \dots, \alpha_n \in \mathcal{E}_p$, and let $\mathbf{y} := (y_1, \dots, y_m) \in \mathbb{Z}_p^m$. Let $\alpha_1 = (\alpha_{11}, \dots, \alpha_{n1}) \in \mathbb{Z}^n$, be such that*

- $\mathbf{g}(\alpha_1) \equiv \mathbf{y} \pmod{p}$,
- $J_p\,\mathbf{g}(\alpha_1) \pmod{p}$ *has rank* m,

then there exists $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathcal{E}_p^n$ such that $\alpha_\ell = \overline{(\alpha_{\ell 1}, \dots)}$, $1 \le \ell \le n$, and $\mathbf{g}(\alpha) = \mathbf{y}$ in $\mathbb{Z}_p$.

We prove here Proposition 2.11 since the other one has exactly the same proof as Proposition 2.9.

Proof. (Proposition 2.11) We set $\mathbf{f}(\mathbf{x}) = (f_1(\mathbf{x}), \dots, f_m(\mathbf{x}))$ where

$$f_i(x_1, \dots, x_n) := \sum_{j=1}^{t_i} a_j^{(i)} x_1^{\alpha_j^{(i1)}} \cdots x_n^{\alpha_j^{(in)}}, \ 1 \le i \le m.$$

Following the proof of Proposition 2.8, we assume that $\mathbf{x}_k := (x_{1k}, \dots, x_{nk}) \in \mathbb{Z}^n$ is constructed such that $\mathbf{f}(\mathbf{x}_k) \equiv \mathbf{y}_k \pmod{p^k}$ with $\mathbf{x}_k \equiv \mathbf{x}_1 \pmod{p}$ coordinate-wise. We need $x_{\ell(k+1)} = x_{\ell k} + p^k \xi_\ell$ with ξ_ℓ to be determined for $1 \le \ell \le n$ such that $\mathbf{f}(\mathbf{x}_{k+1}) \equiv \mathbf{y}_{k+1} \pmod{p^{k+1}}$. By assumption, for $1 \le i \le m$,

$$y_{i(k+1)} - \sum_{j=1}^{t_i} a_{j(k+1)}^{(i)} x_{1k}^{\alpha_{j(k+1)}^{(i1)}} \cdots x_{nk}^{\alpha_{j(k+1)}^{(in)}} \equiv p^k z_i \pmod{p^{k+1}}.$$

Now,

$$\begin{aligned}
y_{i(k+1)} &\equiv \textstyle\sum_{j=1}^{t_i} a_{j(k+1)}^{(i)} \prod_{\ell=1}^n (x_{\ell k} + p^k \xi_\ell)^{\alpha_{j(k+1)}^{(i\ell)}} && \pmod{p^{k+1}} \\
&\equiv \textstyle\sum_{j=1}^{t_i} a_{j(k+1)}^{(i)} \prod_{\ell=1}^n (x_{\ell k}^{\alpha_{j(k+1)}^{(i\ell)}} + p^k\, \alpha_{j(k+1)}^{(i\ell)}\, x_{\ell k}^{\alpha_{j(k+1)}^{(i\ell)}-1} \xi_\ell) && \pmod{p^{k+1}} \\
&\equiv \textstyle\sum_{j=1}^{t_i} a_{j(k+1)}^{(i)} \big[\prod_{\ell=1}^n x_{\ell k}^{\alpha_{j(k+1)}^{(i\ell)}} \\
&\quad + p^k \textstyle\sum_{\ell=1}^n \alpha_{j(k+1)}^{(i\ell)} (\prod_{\ell' \ne \ell} x_{\ell' k}^{\alpha_{j(k+1)}^{(i\ell')}}) x_{\ell k}^{\alpha_{j(k+1)}^{(i\ell)}-1} \xi_\ell \,\big] && \pmod{p^{k+1}}.
\end{aligned}$$

Hence we need to solve

$$\begin{aligned}
p^k z_i &\equiv p^k \textstyle\sum_{\ell=1}^n \big[\sum_{j=1}^{t_i} a_{j(k+1)}^{(i)} \alpha_{j(k+1)}^{(i\ell)} (\prod_{\ell' \ne \ell} x_{\ell' k}^{\alpha_{j(k+1)}^{(i\ell')}}) x_{\ell k}^{\alpha_{j(k+1)}^{(i\ell)}-1} \big] \xi_\ell && \pmod{p^{k+1}} \\
\iff \quad z_i &\equiv \textstyle\sum_{\ell=1}^n \big[\sum_{j=1}^{t_i} a_{j(k+1)}^{(i)} \alpha_{j(k+1)}^{(i\ell)} (\prod_{\ell' \ne \ell} x_{\ell' k}^{\alpha_{j(k+1)}^{(i\ell')}}) x_{\ell k}^{\alpha_{j(k+1)}^{(i\ell)}-1} \big] \xi_\ell && \pmod{p} \\
\iff \quad z_i &\equiv \textstyle\sum_{\ell=1}^n \Delta_p\, f_i(x_{\ell 1})\, \xi_\ell && \pmod{p}.
\end{aligned}$$

Therefore, since by hypothesis, $J_p(\mathbf{f}(\mathbf{x}_1)) = (\Delta_p\, f_i(x_{\ell 1}))_{i\ell}$ has maximal rank m, the system has a solution $(\xi_1, \dots, \xi_n)$ modulo p. $\square$

Proposition 2.12 yields immediately, as a particular case, another proof of Theorem 2.5:

Proof. (Second Proof of Theorem 2.5) Let $b \in \mathbb{Z}_p^\times$ be a good basis for taking logarithms, $a_j := b^{\beta_j}$, and consider the exponential system of $2t$ equations in $2t$ unknowns given by: $\mathbf{g}(\beta, \alpha) = (f_1(\beta, \alpha), \ldots, f_{2t}(\beta, \alpha))$ where

$$f_i(\beta, \alpha) = \sum_{j=1}^{t} b^{\beta_j} x_i^{\alpha_j}, 1 \le i \le 2t.$$

By Proposition 2.12, this exponential square system has a solution in $\mathcal{E}_p$ if Rank $J_p\,\mathbf{g}(\beta, \alpha)) = 2t$, or equivalently that $\det(J_p\,\mathbf{g}(\beta, \alpha)) \not\equiv 0 \pmod p$. Furthermore, on this hypothesis the solution is unique. Now,

$$\Delta_p\, f_i(\beta_\ell) = e_2(b_2) b^{\beta_\ell} x_i^{\alpha_\ell} = a_\ell e_2(b_2) x_i^{\alpha_\ell} \quad \text{and} \quad \Delta_p\, f_i(\alpha_\ell) = e_2(x_{i2}) b^{\beta_\ell} x_i^{\alpha_\ell} = a_\ell\, e_2(x_{i2}) x_i^{\alpha_\ell}.$$

Therefore, since b_2 is a primitive root $\bmod\, p^2$, $e_2(b_2) \not\equiv 0 \pmod p$,

$$\det \begin{pmatrix} a_1 e_2(b_2) x_1^{\alpha_1} & \ldots & a_t e_2(b_2) x_1^{\alpha_t} & a_1 e_2(x_{12}) x_1^{\alpha_1} & \ldots & a_t\, e_2(x_{12}) x_1^{\alpha_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_1 e_2(b_2) x_{2t}^{\alpha_1} & \ldots & a_t e_2(b_2) x_{2t}^{\alpha_t} & a_1 e_2(x_{(2t)2}) x_{2t}^{\alpha_1} & \ldots & a_t\, e_2(x_{(2t)2}) x_{2t}^{\alpha_t} \end{pmatrix} \equiv$$

$$\equiv a_1 \cdots a_t\, e_2(b_2)^t \det \begin{pmatrix} x_1^{\alpha_1} & \ldots & x_1^{\alpha_t} & a_1\, e_2(x_{12}) x_1^{\alpha_1} & \ldots & a_t\, e_2(x_{12}) x_1^{\alpha_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ x_{2t}^{\alpha_1} & \ldots & x_{2t}^{\alpha_t} & a_1\, e_2(x_{(2t)2}) x_{2t}^{\alpha_1} & \ldots & a_t\, e_2(x_{(2t)2}) x_{2t}^{\alpha_t} \end{pmatrix} \not\equiv 0 \pmod p$$

by hypothesis. □

3. Sparse interpolation

A polynomial $f = \sum_{j=0}^{d} a_j x^j \in A[x]$, with A an arbitrary ring, is usually called a *sparse polynomial* or a *fewnomial* if we focus on its number of non-zero terms, i.e. the number of j 's s.t. $a_j \neq 0$. If it has at most t non-zero terms, i.e. $f = \sum_{j=1}^{t} a_j x^{\alpha_j}$, f is called a t*-sparse polynomial*. Here we choose to name such a fewnomial a t*-nomial* to avoid confusion with the other usual notions of sparsity. Also we refer to a polynomial with exactly t non-zero terms as an *exact* t*-nomial*.

As mentioned in the introduction, any univariate t-nomial in $\mathbb{C}[x]$ is uniquely determined by its value in $2t$ different positive values in $\mathbb{R}$, and in [BeTi88], M. Ben-Or and P. Tiwari produced a beautiful deterministic algorithm that recovers such a t-nomial $f \in \mathbb{C}[x]$ from its value in the $2t$ interpolation points $x_1 := 1$, $x_2 := a$, $x_3 := a^2$, ..., $x_{2t} := a^{2t-1}$, where a is not a root of unity of small order.

Furthermore, their algorithm works for a n-multivariate t-nomial $f \in \mathbb{C}[x_1, \ldots, x_n]$, using as input interpolation points

$$\mathbf{x}_1 := (1, \ldots, 1), \mathbf{x}_2 := (p_1, \ldots, p_n), \mathbf{x}_3 := (p_1^2, \ldots, p_n^2), \ldots, \mathbf{x}_{2t} := (p_1^{2t-1}, \ldots, p_n^{2t-1}),$$

where $p_1, \ldots, p_n$ are different integer prime numbers. The number of arithmetic operations in $\mathbb{C}$ it performs equals $t^2(\log t + \log(nd))$ where log denotes the base 2 logarithm. In case the t-nomial has integer coefficients, the bit size of the algorithm is also polynomial in the maximal bit size h of the coefficients of f.

A lot of work has been done in sparse polynomial and rational interpolation, in different bases of monomials and models. Let us mention again here some of these, mostly for polynomial interpolation in the standard monomial basis and the black box model, meaning you are allowed to choose your interpolation starting points: the work of M. Ben-Or and P. Tiwari in [BeTi88], of R.E. Zippel in [Zip90], of A. Borodin and P. Tiwari in [BoTi91], the series of papers of D. Grigoriev, M. Karpinski and M. Singer in [GKS90] on finite fields, as well as [CDGK91], the conceptually unifying paper [GKS91] following [DrGr91], and [GKS94] on rational interpolation. Also [KaLa88, KLW90, KLL00, Lee01, KaLe03] that improve Ben-Or-Tiwari algorithms in different ways (producing probabilistic algorithm that reduce the explosion of size of intermediate integers or get rid of the assumption that a bound t for the number of terms is known).

First let us mention a result that holds when the black-box representation of the polynomial is in fact a straight-line program, that is a program of evaluation that allows constants, and the $+$, $-$ and $*$ operations. This result does not seem to appear in the literature although it should be naturally contained in [GKS91]. The proof we present here is the fruit of a discussion with Michael Singer. It is based on the fact that taking derivatives linearizes exponents, the same effect than the e_p "logarithmic" map we used in the p-adic context, and works for straight-line programs because of Baur and Strassen derivative inequality [BCS97, (7.7)].

Theorem 3.1. *There is a deterministic algorithm that takes as input a straight-line program of length L representing a t-nomial $f \in \mathbb{C}[x]$ and returns (the monomial expansion of) f. The complexity of the algorithm is of order $O(t^4 L)$.*

Proof. For $f = \sum_{j=1}^t a_j x^{\alpha_j} \in \mathbb{C}[x]$ we set $Df(x) := xf'(x)$ so that $D(x^\alpha) = \alpha x^\alpha$, the k-iteration $D^{(k)}(x^\alpha) = \alpha_j^k x^\alpha$, and finally for $k \in \mathbb{N}$, $D^{(k)} f = \sum_j a_j \alpha^k x^{\alpha_j}$.
Since f is represented by a straight-line program of length L, $\{D^{(k)} f, 0 \leq k \leq t\}$ are given by $t+1$ straight-line programs of length $O(L)$, that can all be constructed from the straight-line program for f in time $O(tL)$ [BCS97, (7.7)].
We fix different positive $x_1, \ldots, x_t \in \mathbb{R}$ and we construct the matrix

$$C(f) := \begin{pmatrix} f(x_1) & \ldots & f(x_t) \\ Df(x_1) & \ldots & Df(x_t) \\ \vdots & & \vdots \\ D^{(t-1)} f(x_1) & \ldots & D^{(t-1)} f(x_t) \end{pmatrix} \in \mathbb{C}^{t \times t}$$

and observe that

$$C(f) = V(f)\, A(f)\, W(f),$$

where

$$V(f) := \begin{pmatrix} \alpha_1^0 & \ldots & \alpha_t^0 \\ \vdots & & \vdots \\ \alpha_1^{t-1} & \ldots & \alpha_t^{t-1} \end{pmatrix}, \; A(f) := \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_t \end{pmatrix}, \; W(f) := \begin{pmatrix} x_1^{\alpha_1} & \ldots & x_t^{\alpha_1} \\ \vdots & & \vdots \\ x_1^{\alpha_t} & \ldots & x_t^{\alpha_t} \end{pmatrix}.$$

Therefore the rank of $C(f)$ gives the exact number of non-zero coefficients a_j and we can assume f is an exact t-nomial, so that $C(f)$ is invertible.
Now we observe that if we set $g := Df = \sum_{j=1}^t a_j \, \alpha_j \, x^{\alpha_j}$, then $C(g) = V(g)A(g)W(g)$ where $V(g) = V(f)$, $W(g) = W(f)$ and $A(g)$ is the diagonal matrix with diagonal terms $a_j \alpha_j$. Therefore

$$C(g)C(f)^{-1} = V(f) \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_t \end{pmatrix} V(f)^{-1},$$

and to compute the exponents α_j, $1 \leq j \leq t$, is is enough to compute the characteristic polynomial of $C(g)C(f)^{-1}$ and its (integer) roots. The coefficients are then recovered by solving a linear system. ☐

In next section we investigate univariate fewnomials over finite fields, in particular in $(\mathbb{Z}/p\mathbb{Z})[x]$, and over the finite rings $\mathbb{Z}/p^k\mathbb{Z}$, where p is an odd prime number.

We then switch to univariate integer polynomials, trying to produce an answer to the question raised by Ben-Or and Tiwari on how to interpolate a t-nomial in $\mathbb{Z}[x]$ from $2t$ arbitrary different real positive values.

In the sequel we denote by $\deg f$ the degree of a non-zero polynomial $f \in A[x]$, A a ring, and by $h(f)$ its binary length when $A = \mathbb{Z}$, i.e. the maximum (base 2) logarithm $\log$ of the absolute value of its coefficients.

3.1. **Fewnomial interpolation in $(\mathbb{Z}/p\mathbb{Z})[x]$ and $(\mathbb{Z}/p^k\mathbb{Z})[x]$.**
Here we impose conditions on the exponents of the polynomial, since for example, every $x \in (\mathbb{Z}/p\mathbb{Z})[x]$ is a root of the binomial $f = x^p - x$. We first recall the proof of a well-known result (see for instance [CDGK91, Th 4.2] for a more general context): any t-nomial of degree strictly bounded by $p-1$ in $(\mathbb{Z}/p\mathbb{Z})[x]$ is uniquely determined by its values in $2t$ points of the form $x_i = \rho^{i-1}$ for $1 \le i \le 2t$, where ρ is a primitive root modulo p. (Of course this statement makes sense only if t is small with respect to p, i.e. if $2t \le p-2$, since if not standard interpolation suffices.) In some sense this is an analogous statement than that of a t-nomial in $\mathbb{C}[x]$ being uniquely determined by its value in $2t$ positive points. This condition can not be arbitrarily relaxed since for example a binomial modulo 7 of degree < 6 is not uniquely determined by its values in $1, 2, 3$ and 4: $f = x^4 + 3$ and $g = 3x^3 + x$ coincide modulo 7 but are different (observe that in this example we may take $\rho = 3$, and therefore 1, 3, 2 and 6 are good interpolation points: $f(6) \ne g(6)$).

Observation 3.2. *Let p be a prime number and $\rho \in \mathbb{Z}$ be a primitive root modulo p. Let $f = \sum_{j=1}^t a_j x^{\alpha_j} \in (\mathbb{Z}/p\mathbb{Z})[x]$ be a t-nomial satisfying that for $j \ne \ell$, $\alpha_j \not\equiv \alpha_\ell \pmod{(p-1)}$. Then $f(\rho^i) = 0$ for $0 \le i \le t-1$ implies $f = 0$.*

Proof. We have
$$\begin{pmatrix} 1^{\alpha_1} & \dots & 1^{\alpha_t} \\ \rho^{\alpha_1} & \dots & \rho^{\alpha_t} \\ \vdots & & \vdots \\ \rho^{(t-1)\alpha_1} & \dots & \rho^{(t-1)\alpha_t} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_t \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$
But the Vandermonde determinant of the left-hand side matrix
$$\prod_{1 \le j < \ell \le t} (\rho^{\alpha_\ell} - \rho^{\alpha_j})$$
does not vanish modulo p since ρ is a primitive root modulo p and $p-1 \nmid \alpha_\ell - \alpha_j$. Thus the unique solution of the system is $a_j = 0$ for $1 \le j \le t$. ☐

Corollary 3.3. *Set p a prime number. A t-nomial in $(\mathbb{Z}/p\mathbb{Z})[x]$ of degree strictly bounded by $p-1$ is uniquely determined by its values at ρ^i, $0 \le i \le 2t-1$, where ρ is a primitive root modulo p.*

Proof. Let $f := \sum_{j=0}^{p-2} a_j x^j, g := \sum_{j=0}^{p-2} b_j x^j$ be two t-nomials in $(\mathbb{Z}/p\mathbb{Z})[x]$ such that $f(\rho^i) = g(\rho^i)$, $0 \le i \le 2t-1$. Then $h := \sum_{j=0}^{p-2}(a_j - b_j)x^j$ is a $2t$-nomial modulo p that satisfies $h(\rho^i) \equiv 0 \pmod{p}$ for $0 \le i \le 2t-1$, and we apply the previous observation. ☐

In the paper mentioned above, M. Ben-Or and P. Tiwari raised the problem of generalizing their procedure for finite fields. As a partial answer, it is straight-forward that the determination of the unique t-nomial in $(\mathbb{Z}/p\mathbb{Z})[x]$ of degree strictly bounded by $p-1$ and with prescribed values in $1, \rho, \dots, \rho^{2t-1}$ —when it exists— can be easily done copying their algorithm for this case. This gives an alternative simple proof in this particular case of the multivariate result of [CDGK91, Th. 4.2].

Algorithm 3.4. (Ben-Or/Tiwari)
Set p a prime number and $\rho \in \mathbb{Z}$ a primitive root modulo p. Let $f \in (\mathbb{Z}/p\mathbb{Z})[x]$ be a t-nomial of degree strictly bounded by $p-1$. Then there is a deterministic algorithm that takes as inputs the values $y_1 := f(1), y_2 := f(\rho), \dots, y_{2t} = f(\rho^{2t-1})$ and returns f. The binary running time of the algorithm equals $O((t^2+p)\log p)$

Proof. The proof copies [BeTi88]. Let $f = \sum_{j=1}^{t} a_j x^{\alpha_j} \in (\mathbb{Z}/p\mathbb{Z})[x]$, $0 \le \alpha_j \le p-2$. The algorithm first computes the exact number $\tilde{t}$ of terms of f, then it determines the exponents $\alpha_1, \dots, \alpha_{\tilde{t}}$ associated to non-zero coefficients and finally it recovers the coefficients $a_1, \dots, a_{\tilde{t}}$.

Let us first assume that $\tilde{t} = t$. The core of the procedure is the same previous fact that since ρ is a primitive root modulo p, $\rho^\alpha \neq \rho^\beta$ in $\mathbb{Z}/p\mathbb{Z}$ for $0 \le \alpha \neq \beta \le p-2$.
As in [BeTi88], we construct a polynomial $F \in (\mathbb{Z}/p\mathbb{Z})[\lambda]$ of degree t whose roots are exactly ρ^{α_j}, and then we recover α_j, $1 \le j \le t$, by simple inspection.
The polynomial $F = \prod_{j=1}^{t}(\lambda - \rho^{\alpha_j}) = \sum_{k=0}^{t} b_k \lambda^k$, $b_t = 1$, is constructed in the following way: For $0 \le \ell \le t-1$, $1 \le j \le t$:

$$\begin{aligned}
0 &= a_j \rho^{\alpha_j \ell} F(\rho^{\alpha_j}) = a_j(b_0 \rho^{\alpha_j \ell} + b_1 \rho^{\alpha_j(\ell+1)} + \dots + b_t \rho^{\alpha_j(\ell+t)}) \quad \Longrightarrow \\
0 &= \sum_{j=1}^{t} a_j \rho^{\alpha_j \ell} F(\rho^{\alpha_j}) \\
&= b_0 \sum_{j=1}^{t} a_j \rho^{\alpha_j \ell} + b_1 \sum_{j=1}^{t} a_j \rho^{\alpha_j(\ell+1)} + \dots + b_t \sum_{j=1}^{t} a_j \rho^{\alpha_j(\ell+t)} \\
&= b_0 f(\rho^\ell) + b_1 f(\rho^{\ell+1}) + \dots + b_{t-1} f(\rho^{\ell+t-1}) + f(\rho^{\ell+t}) \\
&= b_0 y_{\ell+1} + \dots + b_{t-1} y_{\ell+t} + y_{\ell+t+1}.
\end{aligned}$$

This yields the following system

$$\begin{pmatrix} y_1 & \dots & y_t \\ \vdots & & \vdots \\ y_t & \dots & y_{2t-1} \end{pmatrix} \begin{pmatrix} b_0 \\ \vdots \\ b_{t-1} \end{pmatrix} = - \begin{pmatrix} y_{t+1} \\ \vdots \\ y_{2t} \end{pmatrix}$$

which is clearly solvable since

$$\begin{pmatrix} y_1 & \dots & y_t \\ \vdots & & \vdots \\ y_t & \dots & y_{2t-1} \end{pmatrix} = \begin{pmatrix} 1 & \dots & 1 \\ \rho^{\alpha_1} & \dots & \rho^{\alpha_t} \\ \vdots & & \vdots \\ \rho^{\alpha_1(t-1)} & \dots & \rho^{\alpha_t(t-1)} \end{pmatrix} \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_t \end{pmatrix} \begin{pmatrix} 1 & \dots & \rho^{\alpha_1(t-1)} \\ 1 & \dots & \rho^{\alpha_2(t-1)} \\ \vdots & & \vdots \\ 1 & \dots & \rho^{\alpha_t(t-1)} \end{pmatrix}$$

whose determinant $a_1 \dots a_t \prod_{1 \le i < j \le t} (\rho^{\alpha_j} - \rho^{\alpha_i})^2 \not\equiv 0 \pmod p$.
Now it is easy to recover $a_1, \dots, a_t$ by solving the Vandermonde system:

$$\begin{pmatrix} 1 & \dots & 1 \\ \rho^{\alpha_1} & \dots & \rho^{\alpha_t} \\ \vdots & & \vdots \\ \rho^{\alpha_1(t-1)} & \dots & \rho^{\alpha_t(t-1)} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_t \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_t \end{pmatrix}$$

When the exact number of terms $\tilde{t}$ is not known, but strictly bounded by t, we compute it by considering for $1 \leq \ell \leq t$ the matrices

$$V_\ell := \begin{pmatrix} y_1 & \cdots & y_\ell \\ \vdots & & \vdots \\ y_\ell & \cdots & y_{2\ell-1} \end{pmatrix},$$

that satisfy that $\det(V_\ell) = 0$ for all $\tilde{t} < \ell \leq t$ while $\det(V_{\tilde{t}}) \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. Thus, computing $\tilde{t}$ is equivalent here to compute the rank of the matrix V_t.

Let us check the complexity of this algorithm: all integers are bounded by p, and $t < p$. As in [BeTi88], computing the exact number $\tilde{t}$ of terms of the t-nomial requires $O(t^2 \log p)$ binary operations, and bounds the complexity of solving the linear system to determine the polynomial F. The simplest way of computing the exponents α_j, $1 \leq j \leq t$, of f seems to be by simple inspection: computing ρ^i, $1 \leq i \leq p-2$ and checking which of those are roots of F. This takes $O(p \log p)$ steps. Finally, recovering the coefficients does not modify the overall complexity. □

Corollary 3.5. *An analogous algorithm holds in a finite field $\mathbb{F}_q$ for $q = p^n$, since the multiplicative group of a finite field is cyclic of order $q-1$. Any t-nomial in $\mathbb{F}_q[x]$ of degree strictly bounded by $q-1$ can be recovered from its values in the interpolation points ρ^i, $0 \leq i \leq 2t-1$, where ρ is a generator of the field $\mathbb{F}_q$ over $\mathbb{Z}/p\mathbb{Z}$.*

Now we turn to polynomials with coefficients in the ring $\mathbb{Z}/p^k\mathbb{Z}$, where all usual arguments fail for it is not even a domain. However combining Theorem 1.6 and Algorithm 3.4, we are able to obtain some results for p an odd prime number and $k \in \mathbb{N}$, $k \geq 2$. We introduce for polynomials in $(\mathbb{Z}/p^k\mathbb{Z})[x]$ the analogue of Definition 1.9:

Definition 3.6. Let p be an odd prime number and $k \in \mathbb{N}$. We say that a polynomial $f = \sum_j a_j x^{\alpha_j} \in (\mathbb{Z}/p^k\mathbb{Z})[x]$ with $a_j \neq 0$, $\forall j$, *reduces well modulo* p if $p \nmid a_j$ for any j, and $p-1 \nmid \alpha_j - \alpha_\ell$ for any $j \neq \ell$.

Corollary 3.7. *Set p an odd prime number and $k \in \mathbb{N}$ with $k \geq 2$. A t-nomial in $(\mathbb{Z}/p^k\mathbb{Z})[x]$ of degree strictly bounded by $\varphi(p^k)$ that reduces well modulo p is uniquely determined by its values at ρ^i, $0 \leq i \leq 2t-1$, where ρ is a primitive root $\mathrm{mod}\, p^2$.*

Proof. Let $f = \sum_{j=1}^t a_j x^{\alpha_j + (p-1)k_j} \in (\mathbb{Z}/p^k\mathbb{Z})[x]$ be such a t-nomial, where $a_j \not\equiv 0 \pmod p$ and $0 \leq \alpha_j < p-1$ are all distinct since f reduces well modulo p. Since ρ is also a primitive root modulo p, by Corollary 3.3, $\sum_j a_j x^{\alpha_j} \in (\mathbb{Z}/p\mathbb{Z})[x]$ is the unique (exact) t-nomial of degree bounded by $p-1$ with the prescribed values in ρ^i, $0 \leq i \leq 2t-1$. Applying Theorem 1.6, since $\{\rho^i, 0 \leq i \leq 2t-1\}$ is a good starting set (Proposition 1.14), there exists a unique g such that $g(\rho^i) \equiv f(\rho^i) \pmod{p^k}$, $0 \leq i \leq 2t-1$, under the condition that the coefficients coincide modulo p^k and the exponents $\mathrm{mod}\, \varphi(p^k)$. Therefore, since f is such a polynomial, $f \in (\mathbb{Z}/p^k\mathbb{Z})[x]$ is the unique t-nomial of degree bounded by $\varphi(p^k)$ that reduces well modulo p. □

Algorithm 3.8. *Set p an odd prime number, $\rho \in \mathbb{Z}$ a primitive root $\mathrm{mod}\, p^2$ and $k \in \mathbb{N}$ with $k \geq 2$. Let $f \in (\mathbb{Z}/p^k\mathbb{Z})[x]$ be a t-nomial of degree strictly bounded by $\varphi(p^k)$ that reduces well modulo p. Then there is a deterministic algorithm that takes as inputs the values $y_1 := f(1), y_2 := f(\rho), \ldots, y_{2t} = f(\rho^{2t-1})$ in $\mathbb{Z}/p^k\mathbb{Z}$ and returns f. The binary running time of the algorithm is of order $O(t^3 k^2 \log^2 p + p \log p)$.*

Proof. We first apply Algorithm 3.4 to compute the unique exact t-nomial $f_0 \in (\mathbb{Z}/p\mathbb{Z})[x]$ of degree strictly bounded by $p-1$ such that $f_0(\rho^{i-1}) \equiv y_i \pmod p$ for $0 \leq i \leq 2t-1$. Then we apply Theorem 1.6 to lift f_0 to f.

Now we check the complexity of the algorithm. First we reduce y_i and $\rho^{i-1} \pmod p$, $1 \le i \le 2t$ to construct f_0. This takes $O(t\,k\log p + (t^2+p)\log p)$ binary operations. Next, there are at most $\log\log\varphi(p^k) = O(\log k + \log\log p)$ lifting steps, each of them solves a system of size $2t$ with entries bounded by p^k, that takes $O((\log k + \log\log p)t^3 k\log p)$ binary operations. The overall complexity is then of order $O(t^3 k\log k\log p + t^3 k\log p\log\log p + p\log p)$. □

A final observation for this section is that, with the same proof than that of Corollary 3.7, Proposition 1.10 can be reformulated as follows:

Corollary 3.9. *Set p an odd prime number. Let $f = \sum_j a_j x^{\alpha_j}, g = \sum_\ell b_\ell x^{\beta_\ell} \in \mathbb{Z}[x]$ be two polynomials that reduce well modulo p. Then, for any $k \in \mathbb{N}$, the three following conditions are equivalent:*

- *f and g have the same number t of non-zero terms, and up to an index permutation, $a_j \equiv b_j \pmod{p^k}$ and $\alpha_j \equiv \beta_j \pmod{\varphi(p^k)}$.*
- *$f(x) \equiv g(x) \pmod{p^k}$ for all $x \in \mathbb{Z}$ prime to p.*
- *$f(\rho^{i-1}) \equiv g(\rho^{i-1}) \pmod{p^k}$ for $1 \le i \le 2t$ and $\rho \in \mathbb{Z}$ a primitive root modulo p^2.*

For the previous results we used the fact that for $\rho \in \mathbb{Z}$ a primitive root modulo p^2, $\{1, \rho, \dots, \rho^{2t-1}\}$ is a good starting set (of type (1) of Proposition 1.14). For good starting sets of type (2), for instance $\{1, \rho, \dots, \rho^{t-1}, p+1, p+\rho, \dots, p+\rho^{t-1}\}$ for $\rho \in \mathbb{Z}$ a primitive root modulo p, we do not have analogous of Corollary 3.3 and Algorithm 3.4, and the best we can obtain are the following statements:

Corollary 3.10. *Set p an odd prime number and $k \in \mathbb{N}$, $k \ge 2$. A t-nomial in $(\mathbb{Z}/p^k\mathbb{Z})[x]$ of degree strictly bounded by $\varphi(p^k)$ that reduces well modulo p is uniquely determined by its values in $\{1, \dots, p-1, p+1, \dots, 2p-1\}$.*

Proof. This is simply due to the fact that the first $p-1$ points decide which is the t-nomial modulo p and then we apply Theorem 1.6 for the over-constrained compatible system we have, using that the given set contains a good starting set of type (2). □

Algorithm 3.11. *Set p an odd prime number and $k \in \mathbb{N}$, $k \ge 2$. Let $f \in (\mathbb{Z}/p^k\mathbb{Z})[x]$ be a t-nomial of degree strictly bounded by $\varphi(p^k)$ that reduces well modulo p. Then there is a deterministic algorithm that takes as inputs the values $f(1), \dots, f(p-1), f(p+1), \dots, f(2p-1)$ in $\mathbb{Z}/p^k\mathbb{Z}$ and returns f. The binary running time of the algorithm is of order $O(p^4 k\log k)$.*

Corollary 3.12. *Set p an odd prime number. Let $f = \sum_j a_j x^{\alpha_j}, g = \sum_\ell b_\ell x^{\beta_\ell} \in \mathbb{Z}[x]$ be two polynomials that reduce well modulo p. Then, for any $k \in \mathbb{N}$, the three following conditions are equivalent:*

- *f and g have the same number t of non-zero terms, and up to an index permutation, $a_j \equiv b_j \pmod{p^k}$ and $\alpha_j \equiv \beta_j \pmod{\varphi(p^k)}$.*
- *$f(x) \equiv g(x) \pmod{p^k}$ for all $x \in \mathbb{Z}$ prime to p.*
- *$f(i) \equiv g(i) \pmod{p^k}$ for $1 \le i \le p-1$ and $p+1 \le i \le 2p-1$.*

3.2. **Fewnomial interpolation in $\mathbb{Z}[x]$.**

In their paper, M. Ben-Or and P. Tiwari also raised the problem of producing an algorithm that interpolates a t-nomial in $\mathbb{C}[x]$ from $2t$ arbitrary different real positive values. Here we restrict to polynomials in $\mathbb{Z}[x]$. On one hand we observe that applying a bound by A. Borodin and P. Tiwari [BoTi91, Thm.4.3] we can restrict ourselves to $t+1$ interpolation points, t of them being almost arbitrary, but the last one imposed and huge. On the other hand, Theorem 1.6 enables us to reduce the size of the starting interpolation points for t-nomials in $\mathbb{Z}[x]$ that reduce well mod p for some small enough prime number p.

Theorem 3.13. ([BoTi91, Thm.4.3])
Let $f\in\mathbb{Z}[x]$ be a t-nomial, and $(x_i,y_i)\in\mathbb{Z}^2$, $1\le i\le t$, that satisfy that $x_i\ge 2$ and $f(x_i)=y_i$ for $1\le i\le t$. Then
$$\deg f\le \max_i \log x_i + t^2\max_i \log y_i + 2.$$

This bound for the degree of such a t-nomial f in term of the height of its evaluation points immediately yields a bound for the height $h(f)$ of f:

Corollary 3.14. *Let $f\in\mathbb{Z}[x]$ be a t-nomial, and $(x_i,y_i)\in\mathbb{Z}^2$, $1\le i\le t$, that satisfy that $x_i\ge 2$ and $f(x_i)=y_i$ for $1\le i\le t$. Then*
$$h(f)\le \max_i \log|y_i| + 2t(\log t+\max_i \log x_i) + t\max_i{}^2 \log x_i + t^3\max_i \log x_i \max_i \log|y_i|.$$

Proof. Set $D:=\max_i\log x_i + t^2\max_i \log y_i + 2$. As $f=\sum_{j=1}^t a_j x^{\alpha_j}$ where $\alpha_j\le D$, when solving the linear system induced by $f(x_i)=y_i$ for $1\le i\le t$, we deal with an integer matrix of size t and entries of absolute height bounded by $H:=t\max_i {x_i}^D$ and a vector with entries of absolute height bounded by $\max_i|y_i|$. Applying Cramer's rule and the fact that $a_i\in\mathbb{Z}$, we obtain $|a_i|\le t!\,H^{t-1}\max_i|y_i|$. This gives the announced bound. □

Now we remark that an a priori bound for the height of a t-nomial $f\in\mathbb{Z}[x]$ immediately yields the polynomial by interpolation in one single huge value:

Observation 3.15. *Let $f\in\mathbb{Z}[x]$ be a t-nomial and let H be a bound for the maximum absolute value of the coefficients of f.*
Then, for any odd number $\widetilde{H}\ge 2H+1$, there is a deterministic algorithm that takes as input the value $f(\widetilde{H})$ and returns the t-nomial f in $\mathbb{Z}[x]$.
The binary running time of the algorithm is polynomial in t, $\log(\widetilde{H})$ and $\log(f(\widetilde{H}))$.

Proof. It is enough to write $f(\widetilde{H})=\sum_{i\ge1}\tilde a_i\widetilde{H}^i$ in base $\widetilde{H}$ with coefficients in $[-\frac{\widetilde{H}-1}{2},\frac{\widetilde{H}-1}{2}]$ to recover the exponents and coefficients of f by simple inspection. □

Combining these two facts, we conclude that to obtain f we can restrict ourselves to $t+1$ interpolation points $x_1,\dots,x_{t+1}$, where $x_i\ge 2$ are arbitrary for $1\le i\le t$ but x_{t+1} satisfies the condition of the previous observation.

Now we come back to Ben-Or/Tiwari type algorithms to recover t-nomials. We remind that in the sequel a bound t for the number of non-zero terms is always given as an input. An inconvenient in the original algorithm by [BeTi88] is the explosion of intermediate integers: one has to deal with a polynomial F —see proof of Algorithm 3.4 above— where a coefficient equals at least $2^{\alpha_1+\cdots+\alpha_t}$. This problem has been solved in [KaLa88, KLW90], where the authors propose a probabilistic algorithm that keeps the intermediate integers small by employing the traditional Hensel lifting of roots. They choose a "lucky" prime p and $k\in\mathbb{N}$ big enough (essentially s.t. $p^k\ge\deg f$), compute the crucial polynomial F modulo p^k and lift its roots modulo p to roots modulo p^k. These algorithms require a degree bound as input, mostly to control the probability of unlucky reduction modulo p.
Here we present an alternative algorithm to recover a t-nomial $f\in\mathbb{Z}[x]$ from its interpolation in $2t$ points of size bounded by p^2, provided we know in advance that it reduces well modulo the odd prime number p. Since we are still not able to produce a probability analysis for the choice of a good prime p such that f reduces well modulo p, our algorithm only yields an heuristic for arbitrary t-nomials.
We de not intend here to compare the speed of our method with that of [KLW90]: no serious implementation has been done yet. However, since both methods are different in nature, we think that it can be useful to have them both in mind.

Algorithm 3.16. *Let $f \in \mathbb{Z}[x]$ be a t-nomial and let $p > t$ be an odd prime number such that f reduces well modulo p. Set $\rho \in \mathbb{Z}$ a primitive root modulo p^2 and let $x_1, \dots, x_{2t} \in \mathbb{N}$ be such that $x_i \equiv \rho^{i-1} \pmod{p^2}$.*
Then there is a deterministic algorithm that takes as input the values $y_1 := f(x_1), \dots, y_{2t} := f(x_{2t})$ and returns the t-nomial f in $\mathbb{Z}[x]$.
The binary running time of the algorithm is polynomial in p, $\log d$, h and $\tilde{h}$, where $d := \deg f$, $h := h(f)$ and $\tilde{h} := \max\{h(y_i), 1 \le i \le 2t\}$.
The algorithm computes $m \le \max\{\lceil \log\log d \rceil, \lceil \log h \rceil\}$ t-nomials $f_0, \dots, f_m \in \mathbb{Z}[x]$ until matching f. The termination of the procedure is given by the condition $f_m(x_i) = y_i$ for $1 \le i \le 2t$.

Proof. We first compute by Algorithm 3.4 the unique exact $\tilde{t}$-nomial $f_0 \in \mathbb{Z}[x]$, where $\tilde{t} \le t$, of degree $\le p-2$ and integer coefficients in $[-\frac{p-1}{2}, \frac{p-1}{2}]$, determined by the conditions

$$f_0(x_i) \equiv y_i \pmod{p} \quad \text{for } 1 \le i \le 2t.$$

This $\tilde{t}$-nomial must exist since it coincides with $\sum_{j=1}^{t} a_j x^{\alpha_j}$ if $f := \sum_{j=1}^{t} (a_j + p\, d_j) x^{(\alpha_j + (p-1)\delta_j)}$, with $a_j \in [-\frac{p-1}{2}, \frac{p-1}{2}], \beta_j \in [0, p-2]$.
We observe that if $f_0(x_i) = y_i$ in $\mathbb{Z}$, the procedure stops and $f = f_0$, since f is uniquely determined by its value in the $2t$ positive values $x_1, \dots, x_{2t}$.

W.l.o.g. we can assume now that $\tilde{t} = t$. To continue the procedure we apply Theorem 1.6 to compute recursively the unique exact t-nomial $f_k = \sum_{j=1}^{t} b_j x^{\beta_j}$ of degree strictly bounded by $\varphi(p^{2^k})$ and with integer coefficients in $[-\frac{p^{2^k}-1}{2}, \frac{p^{2^k}-1}{2}]$ that satisfies $f_k(x_i) \equiv y_i \pmod{p^{2^k}}$ for $1 \le i \le 2t$.

The termination of the procedure occurs at most for $f_m = f$, i.e m such that $\frac{p^{2^m}-1}{2} \ge 2^h$ and $\varphi(p^{2^m}) > d$, that is

$$m = \max\{\lceil \log h \rceil, \lceil \log\log d \rceil\}.$$

Now let us compute the binary complexity of the algorithm. The running time needed to compute f_0 is of order $O((t^2 + p)\log p)$.
To compute f_{k+1} from f_k:
First we compute $\bmod\, p^{2^k}$ the entries of matrix M_k: we need to compute $e_{2^{k+1}}(x_i)$ and $\ell_{2^{k+1}}(x_i)$ defined in Identity (3), that require $O(t\,(\log(p^{2^{k+1}}) + \tilde{h})) = O(t(2^{k+1}\log p + \tilde{h}))$ bit operations. To compute $x_i^{\beta_j}$ modulo p^{2^k} requires $O(\log(p^{2^k})) = O(2^k \log p)$ operations. The computation of the determinant of M_k and of its inverse modulo p^{2^k} requires $O(t^3 2^k \log p)$ more operations. Thus, computing f_{k+1} from f_k requires $O(t^3(2^{k+1}\log p + \tilde{h}))$ bit operations.
Thus, the total number of bit operations of the algorithm is bounded by

$$O(t^3(\max\{h, \log d\}\log p + \tilde{h}) + p\log p).$$

(We kept the complexity in terms of p and $\log p$ since the only place where it seems to depend on p is in the computation of the starting polynomial f_0). □

Since under our conditions, the bound of [BoTi91, Thm.4.3] gives $\deg f \le 2\log p + t^2\tilde{h} + 2$, we obtain the following heuristic for the case we do not know in advance that f reduces well modulo p.

Heuristic 3.17.

- **Input:** $f \in \mathbb{Z}[x]$ given by a black-box, $t \in \mathbb{N}$ a bound for the number of terms of f.
- **Output:** Luckily, the monomial basis representation of f.
- **Heuristic:**
  - Pick $p > t$ an odd prime number.
  - Pick $\rho \in \mathbb{Z}$ a primitive root modulo p^2.

– Pick $x_1, \dots, x_{2t} \in \mathbb{N}$ such that $x_i \equiv \rho^{i-1} \pmod{p^2}$.
– Compute $y_i := f(x_i)$ for $1 \le i \le 2t$ from the black box.
– Compute f_0, the unique exact $\tilde{t}$-nomial modulo p such that $f_0(x_i) \equiv y_i \pmod{p}$ for $1 \le i \le 2t$ (we observe that $\tilde{t} \le t$ must occur).
– Lift, Applying Theorem 1.6, f_0 to $f_m = \sum_{i=1}^{\tilde{t}} a_i x^{\alpha_i}$ such that

$$\varphi(p^{2^{m-1}}) \le 2\log p + t^2\tilde{h} + 2 < \varphi(p^{2^m}).$$

(This yields the possible exponents $\alpha_1, \dots, \alpha_{\tilde{t}}$ of f.)
– Set $\tilde{f} = \sum_{i=1}^{\tilde{t}} z_i x^{\alpha_i}$ and try to interpolate $\tilde{f}(x_i) = y_i$ for $1 \le i \le 2t$ in $\mathbb{Z}[x]$ solving a simple Vandermonde system.
– If the interpolation problem has a solution, then $\tilde{f} = f$ and output $\tilde{f}$.
– If there is no solution, it was because f was not an exact $\tilde{t}$-nomial (and in fact the exact number of terms of f is strictly greater than $\tilde{t}$). In that case pick another prime $q > t$ and start the procedure again. (If the exact number of terms of the new starting polynomial f_0 is not greater than $\tilde{t}$, pick another prime.) □

Final comment: The problem of finding an algorithm that, given an (unknown) t-nomial f in $\mathbb{Z}[x]$ and $2t$ starting evaluation points, finds the monomial structure of f has proven very hard. If one can find an algorithm that solves the (easier) problem over the finite field $\mathbb{Z}/p\mathbb{Z}$ (where there may be no solution or more than one), our method for lifting the coefficients and the exponents can be used under the assumption of the existence of a "good" (relatively small) prime p, i.e. a prime p such that f reduces well modulo p, and the pseudo-jacobian of f is invertible. A probability analysis for good reduction of t-nomials modulo p is still lacking. We are trying to give an answer to these problems.

References

[Apo76] T. Apostol, *Introduction to analytic number theory.* Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg (1976).

[BeTi88] M. Ben-Or, P. Tiwari, *A deterministic algorithm for sparse multivariate polynomial interpolation. Extended abstract.* STOC (1988) 301–309.

[BCS97] P. Bürgisser, M. Clausen, M. Shokrollahi, *Algebraic complexity theory.* Springer Vol. **317** (1997).

[BCSS98] L. Blum, F. Cucker, M. Shub, S. Smale, *Complexity and real computation.* Springer-Verlag New York, Inc. 1998.

[BoTi91] A. Borodin, P. Tiwari, *On the decidability of sparse univariate polynomial interpolation.* Comput. Complexity **1** (1991) 67–90. STOC (1988) 301–309.

[Car14] R. Carmichael, *The theory of numbers.* Dover Publications Inc, Copyright 1914 and 1915 by R. Carmichael, New York (1959).

[Chi84] A. Chistov, *Factoring polynomials over a finite field and solution of systems of algebraic equations.* (Russian. English summary.) Theory of the complexity of computations, II. Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **137** (1984) 124-188.

[ChGr82] A. Chistov, D. Grigoriev, *Polynomial time factoring of the multivariate polynomials over a global field.* Preprint LOMI E-5-82 (1982) 39 p.

[ChGr83] A. Chistov, D. Grigoriev, *Subexponential-time solving systems of algebraic equations I,II.* Preprint LOMI E-9-83, E-10-83 (1983) 119 p.

[CDGK91] M. Clausen, A. Dress, J. Grabmeier, M. Karpinski, *On zero-testing and interpolation of k-sparse multivariate polynomials over finite fields.* Theoretical Computer Science **84** (1991) 151–164.

[CuSm99] F. Cucker, S. Smale, *Complexity Estimates depending on Condition and Round-off Error.* Journal of the A.C.M. **46** (1999) 113–184.

[DeSh00] J.-P. Dedieu, M. Shub, *Newton's Method for Overdetermined Systems of Equations.* Math of Comp. Vol. **69** (2000) 1099-1115.

[DrGr91] A. Dress, J. Grabmeier, *The interpolation problem for k-sparse polynomials and character sums.* Adv. in Appl. Math. **12** (1991) 57–75.

[EsMu99] J. Esmonde, M. R. Murty, *Problems in Algebraic Number Theory.* Graduate texts in Mathematics **190**, Springer New York (1999).

[GHHMMP97] M. Giusti, K. Hägele, J. Heintz, J.E. Morais, L.M. Pardo, *Lower bounds for diophantine approximations.* J. Pure Appl. Algebra **117 & 118** (1997) 277–317.

[GHMMP98] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, L.M. Pardo, *Straight-line programs in geometric elimination theory.* J. Pure Appl. Algebra **124** (1998) 101-146.

[Gri84] D. Grigoriev, *Factoring polynomials over a finite field and solution of systems of algebraic equations.* (Russian. English summary.) Theory of the complexity of computations, II. Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **137** (1984) 20–79.

[GKS90] D. Grigoriev, M. Karpinski, M. Singer, *Fast parallel algorithms for sparse multivariate polynomial interpolation over finite fields.* Siam J. Comput. Vol. **19** No. 6 (1990) 1059–1063.

[GKS91] D. Grigoriev, M. Karpinski, M. Singer, *The interpolation problem for k-sparse sums of eigenfunctions of operators.* Adv. in Appl. Math. **12** (1991) 76–81.

[GKS94] D. Grigoriev, M. Karpinski, M. Singer, *Computational complexity of sparse rational function interpolation.* SIAM J. Comput. **23** (1995) 1–11.

[HKPSW00] J. Heintz, T. Krick, S. Puddu, J. Sabia, A. Waissbein, *Deformation techniques for efficient polynomial equation solving.* J. Complexity **16** (2000) 70–109.

[JKSS04] G. Jeronimo, T. Krick, J. Sabia, M. Sombra, *The computational complexity of the Chow form.* Found. Comput. Math. **4**(2004) 41–117.

[Kal85] E. Kaltofen, *Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization.* SIAM J. Comput., 14(2) (1985) 469-489.

[KaLa88] E. Kaltofen, Y.N. Lakshman *Improved sparse multivariate polynomial interpolation algorithms.* ISSAC'88, Proc. 1988 Internat. Symp. Symbolic Algebraic Comput., Lecture Notes in Comput. Sci **358**, Springer-Verlag, New York (1988) 467–474.

[KLW90] E. Kaltofen, Y.N. Lakshman, J.-M. Wiley *Modular rational sparse multivariate polynomial interpolation.* ISSAC'90, Proc. 1990 Internat. Symp. Symbolic Algebraic Comput. (S. Watanabe and M. Nagata, eds.), ACM Press, New York (1990) 135–139.

[KaLe03] E. Kaltofen, W.-s Lee *Early termination in sparse interpolation algorithms.* J. Symbolic Computation **40** (2003).

[KLL00] E. Kaltofen, A. Lobo, W.-s Lee *Early termination in Ben-Or/Tiwari sparse interpolation and a hybrid of Zippel's algorithm.* ISSAC'00, Proc. 2000 Internat. Symp. Symbolic Algebraic Comput. (C. Travero, ed.), ACM Press, New York (2000) 192–201.

[Lec02] G. Lecerf, *Quadratic Newton iteration for systems with multiplicity.* Found. Comput. Math. **2**(2002) 247-293.

[Lee01] W.-s. Lee, *Early Termination Strategies in Sparse Interpolation Algorithms.* Ph.D. Dissertation, North Carolina State University (2001).

[LLL82] A.K.Lenstra, H.W.Lenstra, L.Lovász *Factoring polynomials with rational coefficients.* Math. Ann. 261 (1982) 515–534.

[PARI/GP] PARI/GP, version 2.2.8 2004 Webpage `http://pari.math.u-bordeaux.fr/`

[Ser70] J.-P. Serre, *Cours d'arith'métique.* Presses Universitaires de France, 1970.

[ShSm94] M.Shub, S.Smale, *Complexity of Bezout's theorem V : polynomial time.* Theoret. Comp. Sci **133** (1994) 141–164.

[Sma86] S. Smale, *Newton's method estimates from data at one point.* The merging of disciplines: new directions in pure, applied and computational mathematics (R. Erwing, K. Gross, C. Martin, Eds.), Springer-Verlag (1986).

[Sma98] S. Smale, *Mathematical problems for the next century.* Math. Intelligencer **20** (1998) 7–15.

[Tri85] W. Trinks, *On improving approximate results of Buchberger's algorithm by Newton's method.* L. N. Comput. Sci. **204**, Springer-Verlag (1985) 608-611.

[Win88] F. Winkler, *A p-adic approach to the computation of Gröbner bases.* J. Symb. Comput. **6** (1988) 287-304.

[Zas69] H.Zassenhaus, *On Hensel Factorization I.* J. Number Theory 1 (1969) 291–311.

[Zip90] R. Zippel, *Interpolating polynomials from their values.* J. Symbolic Computation **9**(1990) 375–403.

Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Pabellón I Ciudad Universitaria 1428 Buenos Aires, Argentina
E-mail address: mavendar@yahoo.com.ar

Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Pabellón I Ciudad Universitaria 1428 Buenos Aires, Argentina
E-mail address: krick@dm.uba.ar

Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Pabellón I Ciudad Universitaria 1428 Buenos Aires, Argentina
E-mail address: apacetti@dm.uba.ar