COUNTING TROPICALLY DEGENERATE VALUATIONS AND P-ADIC APPROACHES TO THE HARDNESS OF THE PERMANENT

PASCAL KOIRAN, NATACHA PORTIER, AND J. MAURICE ROJAS

Abstract. The Shub-Smale τ-Conjecture is a hitherto unproven statement (on integer roots of polynomials) whose truth implies both a variant of $\mathbf{P} \neq \mathbf{NP}$ (for the BSS model over $\mathbb{C}$) and the hardness of the permanent. We give alternative conjectures, some clearly easier to prove, whose truth still implies the hardness of the permanent. Along the way, we discuss new upper bounds on the number of p-adic valuations of roots of certain sparse polynomial systems, culminating in a connection between quantitative p-adic geometry and complexity theory.

Dedicated to Mike Shub, on his 70$^{\underline{\text{th}}}$ birthday.

1. Introduction

Deep questions from algebraic complexity, cryptology, and arithmetic geometry can be approached through sufficiently sharp upper bounds on the number of roots of structured polynomials in one variable. (We review four such results in Section 1.2 below.) The main focus of this paper is the connection between the number of distinct *norms* of roots of polynomials, over the p-adic rationals $\mathbb{Q}_p$, and separations of complexity classes. Our first main theorem motivates the introduction of p-adic methods.

Definition 1.1. *We define* $\mathrm{SPS}(k,m,t)$ *to be the family of polynomials presentable in the form* $\sum_{i=1}^{k}\prod_{j=1}^{m} f_{i,j}$ *where, for all* i *and* j, $f_{i,j} \in \mathbb{Z}[x_1]\setminus\{0\}$ *and has at most* t *monomial terms. We call such polynomials* SPS *(for* sum-product-sparse*) polynomials.* $\diamond$

Theorem 1.2. *Suppose that there is a prime* p *with the following property: For all* $k,m,t\in\mathbb{N}$ *and* $f\in\mathrm{SPS}(k,m,t)$*, we have that the cardinality of*

$$S_f := \left\{e\in\mathbb{N} \;:\; x\in\mathbb{Z},\ f(x)=0,\ p^e|x,\ \text{and } p^{e+1}\not| x.\right\}$$

is $(kmt)^{O(1)}$*. Then the permanent of* $n\times n$ *matrices cannot be computed by constant-free, division-free arithmetic circuits of size* $n^{O(1)}$*.* ■

The special cases of the hypothesis where $k=1$, $t=1$, or m is a fixed constant are easy to prove (see, e.g., Lemma 1.21 of Section 1.3 below). However, the hypothesis already becomes an open problem for $k=2$ or $t=2$. The greatest e such that p^e divides an integer x is nothing more than the *p-adic valuation* of x, hence our focus on p-adic techniques.

Remark 1.3. *We in fact prove a stronger theorem: the truth of an even weaker hypothesis, easily implied by the famous Shub-Smale τ-Conjecture (see* [Sma98, Sma00] *and Section 1.2 below), still implies the same conclusion. See Theorem 3.3 of Section 3 below. Theorem 3.5 there also shows that an even weaker hypothesis still implies a new complexity lower bound for the permanent.* $\diamond$

We now describe certain families of univariate polynomials, and multivariate polynomial systems, where valuation counts in the direction of Theorem 1.2 can actually be proved. In particular, we give another related hypothesis (in Theorem 1.11 below), entirely within the realm of p-adic geometry, whose truth also implies the hardness of the permanent.

Key words and phrases. sparse polynomial, sum-product, tau conjecture, local field, tropically generic, straight-line program, complexity.

P.K. and N.P. were partially supported by the European Community (7th PCRD Contract: PIOF-GA-2009-236197). J.M.R. was partially supported by NSF MCS grant DMS-0915245 and Labex MILYON.

1.1. **Provable Upper Bounds on the Number of Valuations.**

Definition 1.4. *For any commutative ring R, we let $R^* := R \setminus \{0\}$. The* support *of a polynomial $f \in R\left[x_1^{\pm 1}, \ldots, x_n^{\pm 1}\right]$, denoted* $\mathrm{Supp}(f)$*, is the set of exponent vectors appearing in the monomial term expansion of f. For any prime p and $x \in \mathbb{Z} \setminus \{0\}$ we let* $\mathrm{ord}_p(x)$ *denote the p-adic valuation of x, and we set* $\mathrm{ord}_p(0) := +\infty$*. We then set* $\mathrm{ord}_p(x/y) := \mathrm{ord}_p(x) - \mathrm{ord}_p(y)$ *to extend* $\mathrm{ord}_p(\cdot)$ *to $\mathbb{Q}$, and we let $\mathbb{Q}_p$ denote the completion of $\mathbb{Q}$ with respect to the metric defined by $|u-v|_p := p^{-\mathrm{ord}_p(u-v)}$. The* p-adic complex numbers*, $\mathbb{C}_p$, are then the elements of the completion of the algebraic closure of $\mathbb{Q}_p$. Finally, for any polynomials $f_1, \ldots, f_r \in R\left[x_1^{\pm 1}, \ldots, x_n^{\pm 1}\right]$, we let $Z_R(f_1, \ldots, f_r)$ (resp. $Z_R^*(f_1, \ldots, f_r)$) denote the set of roots of $(f_1, \ldots, f_r)$ in R^n (resp. $(R^*)^n$), and we use $\#S$ to denote the cardinality of a set S.* $\diamond$

In particular, $\mathrm{ord}_p(\cdot)$ and $|\cdot|_p$ extend naturally to $\mathbb{C}_p$, and the algebraic closure of $\mathbb{Q}$ embeds naturally within $\mathbb{C}_p$. [Art67, Wei63, Ser79, Sch84, Rob00, Gou03, Kat07] are some excellent sources for further background on p-adic fields. What will be most important for our setting is that p-adic norms (or, equivalently, p-adic valuations) enable new hypotheses — closer to being provable with current techniques — that imply new separations of complexity classes.

We will ultimately focus on counting valuations of roots of polynomial systems with few monomial terms as a means of understanding the valuations of roots of univariate SPS polynomials. For example, a simple consequence of our main multivariate bounds (Theorems 1.10 and 1.12 below) is the following univariate bound revealing that at least part of the $k=t=2$ case of the hypothesis of Theorem 1.2 is true.

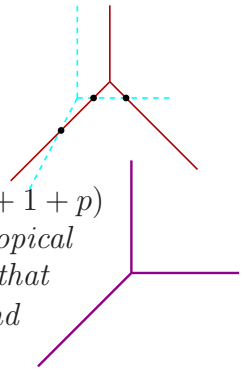
Corollary 1.5. *Suppose $m_1, m_2 \in \mathbb{N}$; $\alpha_i, \beta_i \in \mathbb{C}_p$; $\gamma_{i,j} \in \mathbb{Z}$;*
$$f(x_1) := \left(\textstyle\prod_{i=1}^{m_1} (\alpha_{i,1} + \beta_{i,1} x_1)^{\gamma_{i,1}}\right) + \left(\textstyle\prod_{i=1}^{m_2} (\alpha_{i,2} + \beta_{i,2} x_1)^{\gamma_{i,2}}\right)$$
is not identically zero; and the lower hulls of the p-adic Newton polygons (cf. Definition 1.19 below) of the two products have no common vertices. Then $\#\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(f)\right) \leq m_1 + m_2$, and this bound is tight. Furthermore, any root of f in $\mathbb{C}_p$ not making both products vanish has multiplicity at most $m_1 + m_2$, and this bound is tight as well. ■

Bounds for the number of valuations, independent of the degree, had previously been known only for sparse polynomials, i.e., polynomials in $\mathrm{SPS}(k, 1, t)$: see, e.g., Lemma 1.21 of Section 1.3 and [Wei63]. Note in particular that $\mathrm{SPS}(2, m, 2)$ contains the family of f in our corollary when $\gamma_{i,j} = 1$ for all i, j. Also, our valuation count above is independent of the $\alpha_i, \beta_i, \gamma_i$.

Remark 1.6. *We set* $\mathrm{ord}_p(x_1, \ldots, x_n) := (\mathrm{ord}_p(x_1), \ldots, \mathrm{ord}_p(x_n))$ *henceforth. Clearly then,* $\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(f_1, \ldots, f_r)\right) \subseteq \bigcap_{i=1}^{r} \mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(f_i)\right)$ *but, as revealed below, the containment can be strict.* $\diamond$

Definition 1.7. *For any finite subsets $A_1, \ldots, A_n \subset \mathbb{Z}^n$ we define $\overline{\mathcal{V}}_p(A_1, \ldots, A_n)$ (resp. $\overline{\mathcal{R}}_p(A_, \ldots, A_n)$) to be the maximum of $\#\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(F)\right)$ (resp. $\mathrm{ord}_p\left(Z^*_{\mathbb{Q}_p}(F)\right)$) over all $F := (f_1, \ldots, f_n)$ with $f_i \in \mathbb{C}_p[x_1, \ldots, x_n]$ and $\mathrm{Supp}(f_i) \subseteq A_i$ for all i, and $Z^*_{\mathbb{C}_p}(F)$ finite. We say that F is* tropically generic (over $\mathbb{C}_p$) *iff the closures of $\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(f_1)\right), \ldots, \mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(f_n)\right)$ intersect transversally. We then define $\mathcal{V}_p$ to be the natural analogue of $\overline{\mathcal{V}}_p$ where we restrict further to tropically generic F.* $\diamond$

Kapranov's Non-Archimedean Theorem [EKL06], reviewed in Section 2 below, tells us that the closure of each $\mathrm{ord}_p(Z^*_{\mathbb{C}_p}(f_i))$ is in fact a polyhedral complex of codimension 1 in $\mathbb{R}^n$, so it makes sense to speak of transversality.



Example 1.8. *For any prime p, the polynomials $f_1 := x_1x_2 - p - x_1^2$ and $f_2 := x_2 - 1 - px_1^2$ have $\mathrm{ord}_p(Z^*_{\mathbb{C}_p}(f_1))$ and $\mathrm{ord}_p(Z^*_{\mathbb{C}_p}(f_2))$ intersecting transversally as shown on the right. $\mathrm{ord}_p(Z^*_{\mathbb{C}_p}(f_1))$ (resp. $\mathrm{ord}_p(Z^*_{\mathbb{C}_p}(f_2))$) consists of the rational points on the solid (resp. dashed) curve.* $\diamond$

Example 1.9. *For any prime p, the system $F := (x_1 + x_2 + 1, x_1 + x_2 + 1 + p)$ shows us that having just finitely many roots over $\mathbb{C}_p$ need* not *imply tropical genericity. In particular, while F has no roots at all in $\mathbb{C}_p^2$, we have that $\mathrm{ord}_p(Z^*_{\mathbb{C}_p}(x_1 + x_2 + 1)), \mathrm{ord}_p(Z^*_{\mathbb{C}_p}(x_1 + x_2 + 1 + p)) \subset \mathbb{R}^2$ are identical and exactly the set of rational points on the right-hand union of 3 rays: (So the intersection is non-transversal.) Nevertheless, $\mathrm{ord}_p(Z^*_{\mathbb{C}_p}(F))$ is empty.* $\diamond$

Clearly $\mathcal{V}_p(A_1, \ldots, A_n) \leq \overline{\mathcal{V}}_p(A_1, \ldots, A_n)$ and $\overline{\mathcal{R}}_p(A_1, \ldots, A_n) \leq \overline{\mathcal{V}}_p(A_1, \ldots, A_n)$. While *Smirnov's Theorem* [Smi97, Thm. 3.4] implies that $\mathcal{V}_p(A_1, \ldots, A_n)$ is well-defined and finite for any fixed $(A_1, \ldots, A_n)$, explicit upper bounds for $\overline{\mathcal{V}}_p(A_1, \ldots, A_n)$ appear to be unknown. So we derive such an upper bound for certain $(A_1, \ldots, A_n)$.

Theorem 1.10. *Suppose p is any prime, $A_1, \ldots, A_n \subset \mathbb{Z}^n$, $A := \#\bigcup_i A_i$, $t := \#A$, and e_i denotes the $i^{\underline{th}}$ standard basis vector of $\mathbb{R}^n$. Then:*

(0) $t \leq n \implies \mathcal{V}_p(A_1, \ldots, A_n) = \overline{\mathcal{V}}_p(A_1, \ldots, A_n) = 0$.

(1) $t = n+1 \implies \mathcal{V}_p(A_1, \ldots, A_n) = \overline{\mathcal{V}}_p(A_1, \ldots, A_n) \leq 1$. *In particular,* $\mathcal{V}_p(\{\mathbf{O}, e_1\}, \ldots, \{\mathbf{O}, e_n\}) = 1$.

(2) *[$t = n+2$ and every collection of n distinct pairs of points of A determines an n-tuple of linearly independent vectors]* $\implies \overline{\mathcal{V}}_p(A_1, \ldots, A_n) \leq \max\left\{2, \left\lfloor \frac{n}{2} \right\rfloor^n + n\right\}$. *Also,* $\mathcal{V}_p(\{\mathbf{O}, 2e_1, e_1 + e_2\}, \{\mathbf{O}, 2e_1, e_2 + e_3\}, \ldots, \{\mathbf{O}, 2e_1, e_{n-1} + e_n\}, \{\mathbf{O}, 2e_1, e_n\}) = n + 1$.

We conjecture that the upper bound in Assertion (2) can in fact be improved to $n + 1$. It is easily shown that the general position assumption on A holds for a dense open set of exponents. For instance, if A has convex hull an n-simplex then the hypothesis of Assertion (2) holds automatically.

Whether the equality $\mathcal{V}_p(A_1, \ldots, A_n) = \overline{\mathcal{V}}_p(A_1, \ldots, A_n)$ holds beyond the setting of Assertions (0) and (1) is an intriguing open question. More to the point, proving that the growth of order of $\overline{\mathcal{R}}_p(A_1, \ldots, A_n)$ is at most a constant multiple of the growth order of $\mathcal{V}_p(A_1, \ldots, A_n)$ has deep implications for complexity theory.

Theorem 1.11. *Suppose there is a prime p such that $\overline{\mathcal{R}}_p(A_1, \ldots, A_n) = \mathcal{V}_p(A_1, \ldots, A_n)^{O(1)}$ for all finite $A_1, \ldots, A_n \subset \mathbb{Z}^n$. Then the permanent of $n \times n$ matrices cannot be computed by constant-free, division-free arithmetic circuits of size $n^{O(1)}$.*

We thus obtain an entirely tropical geometric statement implying the hardness of the permanent. In Theorem 1.11 it in fact suffices to restrict to certain families of supports A_i (see Proposition 1.17 below).

Intersection multiplicity is a key subtlety underlying the counting of valuations.

Theorem 1.12. *Suppose K is any algebraically closed field of characteristic 0 and $A \subset \mathbb{Z}^n$ has cardinality at most $n + 2$ and no $n + 1$ points of A lie in a hyperplane. Suppose also that $f_1, \ldots, f_n \in K[x_1, \ldots, x_n]$ have support contained in A and $\#Z^*_K(F)$ is finite. Then the intersection multiplicity of any point of $Z^*_K(F)$ is at most $n + 1$ (resp. 1) when $\#A = n + 2$ (resp. $\#A = n + 1$), and both bounds are sharp.*

The intersection multiplicity considered in our last theorem is the classical definition coming from commutative algebra or differential topology (see, e.g., [Ful08]).

1.2. **Earlier Applications of Root Counts for Univariate Structured Polynomials.** Recall the following classical definitions on the evaluation complexity of univariate polynomials.

Definition 1.13. *For any field K and $f \in K[x_1]$ let $s(f)$ — the* SLP complexity of f — *denote the smallest n such that $f = f_n$ identically where the sequence $(f_{-N}, \ldots, f_{-1}, f_0, \ldots, f_n)$ satisfies the following conditions: $f_{-1}, \ldots, f_{-N} \in K$, $f_0 := x_1$, and, for all $i \geq 1$, f_i is a sum, difference, or product of some pair of elements (f_j, f_k) with $j, k < i$. Finally, for any $f \in \mathbb{Z}[x_1]$, we let $\tau(f)$ denote the obvious analogue of $s(f)$ where the definition is further restricted by assuming $N = 1$ and $f_{-1} := 1$.* $\diamond$

Note that we always have $s(f) \leq \tau(f)$ since s does not count the cost of computing large integers (or any constants). One in fact has $\tau(n) \leq 2 \log_2 n$ for any $n \in \mathbb{N}$ [dMS96, Prop. 1]. See also [Bra39, Mor97] for further background.

We can then summarize some seminal results of Bürgisser, Cheng, Lipton, Shub, and Smale as follows:

Theorem 1.14.

I. (See [BCSS98, Thm. 3, Pg. 127] *and* [Bür09, Thm. 1.1]*.) Suppose that for all nonzero $f \in \mathbb{Z}[x_1]$ we have $\#Z_{\mathbb{Z}}(f) \leq \tau(f)^{O(1)}$. Then (a) $\mathbf{P}_{\mathbb{C}} \neq \mathbf{NP}_{\mathbb{C}}$ and (b) the permanent of $n \times n$ matrices cannot be computed by constant-free, division-free arithmetic circuits of size $n^{O(1)}$.*

II. (Weak inverse to (I) [Lip94]*.*[1]*) If there is an $\varepsilon > 0$ and a sequence $(f_n)_{n \in \mathbb{N}}$ of polynomials in $\mathbb{Z}[x_1]$ satisfying:*

$$\text{(a) } \#Z_{\mathbb{Z}}(f_n) > e^{\tau(f_n)^{\varepsilon}} \text{ for all } n \geq 1 \quad \text{and} \quad \text{(b) } \deg f_n, \max_{\zeta \in Z_{\mathbb{Z}}(f)} |\zeta| \leq 2^{(\log \#Z_{\mathbb{Z}}(f_n))^{O(1)}}$$

then, for infinitely many n, at least $\frac{1}{n^{O(1)}}$ of the n digit integers that are products of exactly two distinct primes (with an equal number of digits) can be factored by a Boolean circuit of size $n^{O(1)}$.

III. (Number field analogue of (I) implies Uniform Boundedness [Che04]*.) Suppose that for any number field K and $f \in K[x_1]$ we have $\#Z_K(f) \leq c_1 1.0096^{s(f)}$, with c_1 depending only on $[K : \mathbb{Q}]$. Then there is a constant $c_2 \in \mathbb{N}$ depending only on $[K : \mathbb{Q}]$ such that for any elliptic curve E over K, the torsion subgroup of $E(K)$ has order at most c_2.* ■

The hypothesis in Part (I) is known as the *(Shub-Smale) τ-Conjecture* and was stated as the fourth problem (still unsolved as of late 2013) on Smale's list of the most important problems for the $21^{\underline{\text{st}}}$ century [Sma98, Sma00]. Via fast multipoint evaluation applied to the polynomial $(x-1)\cdots(x-m^2)$ [vzGG03] one can show that the O-constant from the τ-Conjecture should be at least 2 if the τ-Conjecture is true.

The complexity classes $\mathbf{P}_{\mathbb{C}}$ and $\mathbf{NP}_{\mathbb{C}}$ are respective analogues (for the BSS model over $\mathbb{C}$ [BCSS98]) of the well-known complexity classes $\mathbf{P}$ and $\mathbf{NP}$. (Just as in the famous $\mathbf{P}$ vs. $\mathbf{NP}$ Problem, the equality of $\mathbf{P}_{\mathbb{C}}$ and $\mathbf{NP}_{\mathbb{C}}$ remains an open question.) The assertion on the hardness of the permanent in Theorem 1.14 is also an open problem and its proof would be a major step toward solving the $\mathbf{VP}$ *vs.* $\mathbf{VNP}$ *Problem* — Valiant's algebraic circuit analogue of the $\mathbf{P}$ vs. $\mathbf{NP}$ Problem [Val79, Bür00, Koi11, BLMW11]: The only remaining issue to resolve for a complete solution of this problem would then be the restriction to constant-free circuits in Part (I).

[1] Lipton's main result from [Lip94] is in fact stronger, allowing for rational roots and primes with a mildly differing number of digits.

The hypothesis of Part (II) (also unproved as of late 2013) merely posits a sequence of polynomials violating the τ-Conjecture in a weakly exponential manner. The conclusion in Part (II) would violate a widely-believed version of the cryptographic hardness of integer factorization.

The conclusion in Part (III) is the famous *Uniform Boundedness Theorem*, due to Merel [Mer96]. Cheng's conditional proof (see [Che04, Sec. 5]) is dramatically simpler and would yield effective bounds significantly improving known results (e.g., those of Parent [Par99]). In particular, the $K = \mathbb{Q}$ case of the hypothesis of Part (III) would yield a new proof (less than a page long) of Mazur's landmark result on torsion points [Maz78].

More recently, Koiran has suggested real analytic methods (i.e., upper bounds on the number of real roots) as a means of establishing the desired upper bounds on the number of integer roots [Koi11], and Rojas has suggested p-adic methods [PR13]. In particular, the following variation on the hypothesis from Theorem 1.2 appears in slightly more refined form in [PR13, Sec. 2]:[2]

Simplified Adelic SPS-Conjecture. *For any $k, m, t \in \mathbb{N}$ and $f \in \mathrm{SPS}(k, m, t)$, there is a field $L \in \{\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \dots\}$ such that f has no more than $(kmt)^{O(1)}$ distinct roots in L.*

Theorem 1.15. *If the Simplified Adelic SPS-Conjecture is true then the permanent of $n \times n$ matrices cannot be computed by constant-free, division-free arithmetic circuits of size $n^{O(1)}$.*

Proof of Theorem 1.15: The truth of the Simplified Adelic SPS-Conjecture clearly implies that the number of integer roots of any $f \in \mathrm{SPS}(k, m, t)$ is $(kmt)^{O(1)}$. The latter statement in turn implies the hypothesis of Theorem 1.2, so by the conclusion of Theorem 1.2 we are done. ■

Note that the preceding conjecture can not be further simplified to counting just the valuations: *any* fixed polynomial in $\mathbb{Z}[x_1] \setminus \{0\}$ will have exactly *one* p-adic valuation for its roots in $\mathbb{C}_p$ for sufficiently large p. (This follows easily from, e.g., Lemma 1.21 of the next section.) An alternative simplification (and stronger hypothesis) would be to ask for a *single* field $L \in \{\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \dots\}$ where the number of roots in L of any $f \in \mathrm{SPS}(k, m, t)$ is $(kmt)^{O(1)}$. The latter simplification is an open problem, although it is now known that one can not ask for too much more: the stronger statement that the number of roots in L of any $f \in \mathbb{Z}[x_1]$ is $\tau(f)^{O(1)}$ is known to be false. Counter-examples are already known over $\mathbb{R}$ (see, e.g., [BC76]), and over $\mathbb{Q}_p$ for any prime p [PR13, Example 2.5 & Sec. 4.5].

The latter examples are much more recent, so for the convenience of the reader we summarize them here: Recall that the p-adic *integers*, $\mathbb{Z}_p$, are those elements of $\mathbb{Q}_p$ with nonnegative valuation. (So $\mathbb{Z} \subsetneqq \mathbb{Z}_p$ in particular.)

Example 1.16. *Consider the recurrence $h_1 := x_1(1 - x_1)$ and $h_{n+1} := (p^{3^{n-1}} - h_n)h_n$ for all $n \geq 1$. Then h_n has degree 2^n, exactly 2^n roots in $\mathbb{Z}_p$, and $\tau(h_n) = O(n)$. However, the only integer roots of h_n are $\{0, 1\}$ (see* [PR13, Sec. 4.5]*). Note also that h_n has just n distinct valuations for its roots in $\mathbb{C}_p$. The last fact follows easily from Lemma 1.21, stated in the next section.* ⋄

Note, however, that it is far from obvious if the polynomial h_n above is in $\mathrm{SPS}(k, m, t)$ for some triple (k, m, t) of functions growing polynomially in n.

[2]The simplified conjecture here implies the refined version appearing in [PR13, Sec. 2].

1.3. **From Univariate SPS to Multivariate Sparse.** Perhaps the simplest reduction of root counts for univariate SPS polynomial to root counts for multivariate sparse polynomial systems is the following.

Proposition 1.17. *Suppose $f \in \mathrm{SPS}(k,m,t)$ is written $\sum_{i=1}^{k}\prod_{j=1}^{m} f_{i,j}$ as in Definition 1.1. Let $F := (f_1,\ldots,f_{km+1})$ be the polynomial system defined by $f_{km+1}(x_1,\ldots,y_{i,j},\ldots) := \sum_{i=1}^{k}\prod_{j=1}^{m} y_{i,j}$ and $f_{(i-1)m+j}(x_1,y_{i,j}) := y_{i,j} - f_{i,j}(x_1)$ for all $(i,j)\in\{1,\ldots,k\}\times\{1,\ldots,m\}$. (Note that F involves exactly $km+1$ variables; $f_1,\ldots,f_{km}$ each have at most $t+1$ monomial terms; and f_{km+1} involves exactly k monomial terms.) Then f not identically zero implies that F has only finitely many roots in $\mathbb{C}_p$, and the x_1-coordinates of the roots of F in $\mathbb{C}_p$ are exactly the roots of f in $\mathbb{C}_p$.* ■

Upper bounds for the number of valuations of the roots of multivariate sparse polynomials can then, in some cases, yield useful upper bounds for the number of valuations of the roots of univariate SPS polynomials.

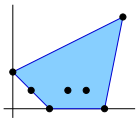
Lemma 1.18. *Following the notation of Proposition 1.17, suppose F is tropically generic. Then $\#\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(F)\right) \leq k(k-1)(2km(t-1)+1)/2 = O(k^3mt)$.*

The crux of our paper is whether a similar bound can hold for $\#\mathrm{ord}_p\left(Z^*_{\mathbb{Q}_p}(F)\right)$, without tropical genericity. We prove Lemma 1.18 in Section 2 below.

We will need to review some polyhedral geometric tools, the first being the p-adic Newton polygon (see, e.g., [Wei63, Gou03]).

Definition 1.19. *Given any prime p and a polynomial $f(x_1) := \sum_{i=1}^{t} c_i x_1^{a_i} \in \mathbb{C}_p[x_1]$, we define its* p-adic Newton polygon*, $\mathrm{Newt}_p(f)$, to be the convex hull of[3] the points $\{(a_i,\mathrm{ord}_p c_i) \mid i \in \{1,\ldots,t\}\}$. Also, a face of a polygon $Q\subset\mathbb{R}^2$ is called* lower *if and only if it has an inner normal with positive last coordinate, and the* lower hull *of Q is simply the union of all its lower edges. Finally, the polynomial associated to summing the terms of f corresponding to points of the form $(a_i,\mathrm{ord}_p c_i)$ lying on some lower face of $\mathrm{Newt}_p(f)$ is called a* (p-adic) lower polynomial. ⋄

Example 1.20. *For $f(x_1) := 36 - 8868x_1 + 29305x_1^2 - 35310x_1^3 + 18240x_1^4 - 3646x_1^5 + 243x_1^6$, the polygon $\mathrm{Newt}_3(f)$ has exactly 3 lower edges and can easily be verified to resemble the illustration to the right. The polynomial f thus has exactly 2 lower binomials, and 1 lower trinomial over $\mathbb{C}_3$.* ⋄



p-adic Newton polygons allow us to easily count valuations (or norms) of p-adic complex roots when the monomial term expansion is known.

Lemma 1.21. *(See, e.g.,* [Wei63, Prop. 3.1.1]*.) The number of roots of f in $\mathbb{C}_p$ with valuation v, counting multiplicities, is* exactly *the horizontal length of the lower face of $\mathrm{Newt}_p(f)$ with inner normal $(v,1)$.* ■

Example 1.22. *In Example 1.20, note that the 3 lower edges have respective horizontal lengths 2, 3, and 1, and inner normals $(1,1)$, $(0,1)$, and $(-5,1)$. Lemma 1.21 then tells us that f has exactly 6 roots in $\mathbb{C}_3$: 2 with 3-adic valuation 1, 3 with 3-adic valuation 0, and 1 with 3-adic valuation -5. Indeed, one can check that the roots of f are exactly 6, 1, and $\frac{1}{243}$, with respective multiplicities 2, 3, and 1.* ⋄

[3] i.e., smallest convex set containing...

Note that while we would truly like to know if the number of valuations of the p-adic complex roots of arbitrary $f \in \mathrm{SPS}(k,m,t)$ admit an upper bound of $(kmt)^{O(1)}$, Lemma 1.21 (applied to the full monomial term expansion of f) easily implies an upper bound of kt^m.

To prove Theorem 1.11 we will need to review p-adic Newton *polytopes*.

2. Background on p-adic Tropical Geometry

The definitive extension of p-adic Newton polygons to arbitrary dimension (and general non-Archimedean, algebraically closed fields) is due to Kapranov.

Definition 2.1. *For any polynomial $f \in \mathbb{C}_p[x_1,\ldots,x_n]$ written $\sum_{a\in A} c_a x^a$ (with $x^a = x_1^{a_1}\cdots x_n^{a_n}$ understood) we define its* p-adic Newton polytope, $\mathrm{Newt}_p(f)$, *to be the convex hull of the point set $\{(a, \mathrm{ord}_p(c_a)) \mid a \in A\}$. We also define the* p-adic tropical variety of f *(or* p-adic amoeba of f*),* $\mathrm{Trop}_p(f)$, *to be $\{v \in \mathbb{R}^n \mid (v,1)$ is an inner normal of a positive-dimensional face of $\mathrm{Newt}_p(f)\}$.* $\diamond$

We note that in [EKL06], the p-adic tropical variety of f was defined via a *Legendre transform* (a.k.a. *support function* [Zie95]) of the lower hull of $\mathrm{Newt}_p(f)$. It is easy to see that both defintions are equivalent.

Kapranov's Non-Archimedean Amoeba Theorem (special case). [EKL06] *Following the notation above,* $\mathrm{ord}_p\Big(Z^*_{\mathbb{C}_p}(f)\Big) = \mathrm{Trop}_p(f) \cap \mathbb{Q}^n$. ■

A simple consequence of Kapranov's Theorem is that counting valuations is most interesting for zero-dimensional algebraic sets.

Proposition 2.2. *Suppose $f_1,\ldots,f_r \in \mathbb{C}_p\big[x_1^{\pm 1},\ldots,x_n^{\pm 1}\big]$, $F := (f_1,\ldots,f_r)$, and $Z^*_{\mathbb{C}_p}(F)$ is infinite. Then* $\mathrm{ord}_p\Big(Z^*_{\mathbb{C}_p}(F)\Big)$ *is infinite.*

Proof: By the definition of dimension for algebraic sets over an algebraically closed field, there must be a linear projection $\pi : \mathbb{C}_p^n \longrightarrow I$, for some coordinate subspace I of positive dimension k, with $\pi\Big(Z^*_{\mathbb{C}_p}(F)\Big)$ dense. Taking valuations, and applying Kapranov's Theorem, this implies that $\mathrm{ord}_p\Big(\pi\Big(Z^*_{\mathbb{C}_p}(F)\Big)\Big)$ must be linearly isomorphic to $\mathbb{Q}^k$ minus a (codimension 1) polyhedral complex. In other words, $\mathrm{ord}_p\Big(Z^*_{\mathbb{C}_p}(F)\Big)$ must be infinite. ■

Another consequence of Kapranov's Theorem is a simple characterization of $\mathrm{ord}_p(Z^*_{\mathbb{C}_p}(F))$ when $F := (f_1,\ldots,f_n)$ is over-determined in a certain sense. This is based on a trick commonly used in toric geometry, ultimately reducing to an old matrix factorization: For any matrix $M = [M_{i,j}] \in \mathbb{Z}^{n\times n}$ and $x \in (\mathbb{C}_p^*)^n$, we define $x^M := \Big(x_1^{M_{1,1}}\cdots x^{M_{n,1}}, \ldots, x_1^{M_{1,n}}\cdots x^{M_{n,n}}\Big)$. We then call the map $m_M : (\mathbb{C}_p^*)^n \longrightarrow (\mathbb{C}_p^*)^n$ defined by $m_M(x) := x^M$ a *monomial change of variables.*

Lemma 2.3. *Given any finite set $A = \{a_1,\ldots,a_n\} \subset \mathbb{Z}^n$ lying in a hyperplane in $\mathbb{R}^n$, there is a matrix $U \in \mathbb{Z}^{n\times n}$, with determinant ± 1, satisfying the following conditions:*

1. *$Ua_i \in \mathbb{Z}^i \times \{0\}^{n-i}$ for all $i \in \{1,\ldots,n\}$.*
2. *Left (or right) multiplication by U induces a linear bijection of $\mathbb{Z}^n$.*
3. *m_U is an automorphism of the multiplicative group $(\mathbb{C}_p^*)^n$, with inverse $m_{U^{-1}}$. In particular, the map sending $\mathrm{ord}_p(x) \mapsto \mathrm{ord}_p(m_U(x))$ for all $x \in (\mathbb{C}_p^*)^n$ is a linear automorphism of $\mathbb{Q}^n$.* ■

Lemma 2.3 follows immediately from the existence of *Hermite factorization* for matrices with integer entries (see, e.g., [Her56, Sto00]). In fact, the matrix U above can be constructed efficiently, but this need not concern us here. The characterization of $\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(F)\right)$ for over-determined F is the following statement.

Proposition 2.4. *Suppose $A_1,\ldots,A_n\subseteq A\subset\mathbb{Z}^n$ and A lies in some $(n-1)$-flat of $\mathbb{R}^n$. Then $\mathcal{V}_p(A_1,\ldots,A_n)=\overline{\mathcal{V}}_p(A_1,\ldots,A_n)=0$.*

Proof: Suppose $F:=(f_1,\ldots,f_n)$ where $\mathrm{Supp}(f_i)\subseteq A_i$ for all i. By Lemma 2.3 we may assume that $A\subset\mathbb{Z}^{n-k}\times\{0\}^k$ for some $k\geq 1$. Clearly then, $Z^*_{\mathbb{C}_p}(F)$ is either empty or contains a coordinate k-flat. So $\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(F)\right)$ must either be empty or infinite, and we are done. ■

Another consequence of Kapranov's Theorem is the following characterization of $\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(f)\right)$ for certain trinomials. Recall that $\mathbb{R}_+$ is the set of positive real numbers and that $\mathbb{R}_+v$, for any vector $v\in\mathbb{R}^N\setminus\{\mathbf{O}\}$, is the *open ray* generated by all positive multiples of v.

Lemma 2.5. *Suppose $g\in\mathbb{C}_p[x_1]$ has exactly t monomial terms, the lower hull of $\mathrm{Newt}_p(g)$ consists of exactly t' edges, and $f(x_1,y_i):=y_i-g(x_1)$ is considered as a polynomial in $\mathbb{C}_p[x_1,y_1,\ldots,y_N]$ with $N\geq i$. Then $\mathrm{ord}_p(Z^*_{\mathbb{C}_p}(f))$ is the set of rational points of a polyhedral complex Σ_f of the following form: a union of* **(a)** *an open $(N-1)$-dimensional half-space parallel to $(\mathbb{R}_+(-1,\deg(g)))\times\mathbb{R}^{N-1}$,* **(b)** *$t'$ "vertical" open half-spaces parallel to $(\mathbb{R}_+(0,1))\times\mathbb{R}^{N-1}$,* **(c)** *$t'-1$ strips of the form $L\times\mathbb{R}^{N-2}$ where $L\subset\mathbb{R}^2$ is a line segment missing one of its vertices, and* **(d)** *a closed $(N-1)$-dimensional half-space parallel to $(\mathbb{R}_+\cup\{0\})\times\{0\}\times\mathbb{R}^{N-1}$.*

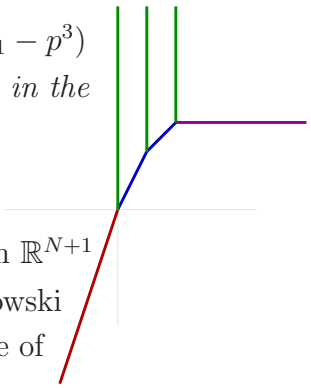
Example 2.6. *For any prime p, the polynomial*

$$f(x_1,y_1):=y_1-(x_1^3-(1+p+p^2)x_1^2+(p+p^2+p^3)x_1-p^3)$$

has $\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(f)\right)$ resembling the diagram to the right. In particular, in the notation of Lemma 2.5, we have

$$g(x_1):=x_1^3-(1+p+p^2)x_1^2+(p+p^2+p^3)x_1-p^3,$$

$N=1$, $t=4$, and $t'=3$. ◇



Proof of Lemma 2.5: By construction, $\mathrm{Newt}(f)$ lies in a 2-plane in $\mathbb{R}^{N+1}$ and thus, thanks to Kapranov's Theorem, $\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(f)\right)$ is the Minkowski sum of a 1-dimensional tropical variety and a complementary subspace of dimension $N-1$. In particular, it suffices to prove the $N=1$ case.

The $N=1$ case follows easily: the ray of type (a) (resp. (d)) is parallel to the inner normal ray to the edge with vertices $(0,1)$ and $(\deg g,0)$ (resp. $(0,1)$ and $(0,0)$) of $\mathrm{Newt}(f)$. The vertical rays correspond to the inner normals corresponding to the lower edges of $\mathrm{Newt}_p(g)$ (alternatively, the edges of $\mathrm{Newt}_p(f)$ not incident to $(0,1,0)$). Finally, the "strips" are merely the segments connecting the points v with $(v,1)$ a lower facet normal of $\mathrm{Newt}_p(f)$. ■

Proof of Lemma 1.18: Let $n=km+1$ be the number of variables in the system constructed in Proposition 1.17. Lemma 2.5 (applied to each $y_{i,j}-f_{i,j}$) induces a natural finite partition of $\mathbb{R}^n$ into half-open slabs of the form $(-\infty,v_1)\times\mathbb{R}^{n-1}$, $[v_\ell,v_{\ell+1})\times\mathbb{R}^{n-1}$ for $\ell\in\{1,\ldots,M-1\}$, or $[v_M,+\infty)\times\mathbb{R}^{n-1}$, with $M\leq km(t-1)-1$. (Note, in particular, that the boundaries of the slabs coming from different $f_{i,j}$ can not intersect, thanks to tropical genericity.) Note also that within the interior of each slab, any non-empty intersection

of $\mathrm{ord}_p\Big(Z^*_{\mathbb{C}_p}(f_1)\Big),\ldots,\mathrm{ord}_p\Big(Z^*_{\mathbb{C}_p}(f_n)\Big)$ must be a transversal intersection of n hyperplanes, thanks to tropical genericity.

In particular, for the left-most (resp. right-most) slab, we obtain a transversal intersection of $n-1$ type (a) (resp. type (d)) $(n-1)$-cells coming from $f_1,\ldots,f_{n-1}$ (in the notation of Lemma 2.5) and an $(n-1)$-cell of $\mathrm{ord}_p\Big(Z^*_{\mathbb{C}_p}(f_n)\Big)$. Each $(n-1)$-cell of $\mathrm{ord}_p\Big(Z^*_{\mathbb{C}_p}(f_n)\Big)$, by definition, is dual to an edge of the lower hull of $\mathrm{Newt}_p(f_n)$. So there are no more than $\binom{k}{2}$ such $(n-1)$-cells. Thus, there are at most $\binom{k}{2}$ intersections of $\mathrm{ord}_p\Big(Z^*_{\mathbb{C}_p}(f_1)\Big),\ldots,\mathrm{ord}_p\Big(Z^*_{\mathbb{C}_p}(f_n)\Big)$ occuring in the interior of the left-most (resp. right-most) slab.

Similarly, the number of intersections of $\mathrm{ord}_p\Big(Z^*_{\mathbb{C}_p}(f_1)\Big),\ldots,\mathrm{ord}_p\Big(Z^*_{\mathbb{C}_p}(f_n)\Big)$ occuring in any other slab interior is $\binom{k}{2}$. Also, within any of the $M+1$ slab boundaries, there are clearly at most $\binom{k}{2}$ intersections of $\mathrm{ord}_p\Big(Z^*_{\mathbb{C}_p}(f_1)\Big),\ldots,\mathrm{ord}_p\Big(Z^*_{\mathbb{C}_p}(f_n)\Big)$.

So we obtain no more than $\binom{k}{2}(2+M+M+1)\leq\binom{k}{2}(2km(t-1)+1)=O(k^3mt)$ intersections for the underlying p-adic tropical varieties and we are done. ■

3. Proving, and Improving, Theorem 1.2

Thanks to a result from [Koi11], paraphrased in Theorem 3.4 below, we easily obtain a strengthening of Theorem 1.2. However, let us first review some background.

Recall that the *counting hierarchy* **CH** is a hierarchy of complexity classes built on top of the counting class $\#\mathbf{P}$; it contains the entire polynomial hierarchy **PH** and is contained in **PSPACE**. A detailed understanding of **CH** is not necessary here since we will need only one fact (Theorem 3.4 below) related to **CH**. The curious reader can consult [Bür09, Koi11] and the references therein for more information on the counting hierarchy.

Definition 3.1. *A* hitting set *H for a family $\mathcal{F}$ of polynomials is a finite set of points such that, for any $f\in\mathcal{F}\setminus\{0\}$, there is at least one $x\in H$ such that $f(x)\neq 0$. Also, a* **CH**-algebraic number generator *is a sequence of polynomials $G:=(g_i)_{i\in\mathbb{N}}$ satisfying the following conditions: (1) There is a positive integer c such that we can write $g_i(x_1):=\sum_{\alpha=0}^{i^c}a(\alpha,i)x_1^\alpha$, with $a(\alpha,i)\in\mathbb{Z}$ of absolute value no greater than 2^{i^c}, for all i. (2) The language $L(G):=\big\{(\alpha,i,j,b)\mid$ the $j^{\underline{th}}$ bit of $a(\alpha,i)$ is equal to $b\big\}$ is in* **CH**. ⋄

Hitting sets are sometimes called *correct test sequences*, as in [HS82]. In particular, the deterministic construction of hitting sets is equivalent to the older problem of deterministic identity testing for polynomials given in the *black-box* model.

To state our strengthening of Theorem 1.2, we will first need to refine our notion of SPS polynomials to take coefficient and degree size into account as well.

Definition 3.2. *(See* [Koi11, Sec. 3]*.) Let us define* $\mathrm{SPS}(k,m,t,d,\delta)$ *to be the family of non-constant polynomials presentable in the form $\sum_{i=1}^k\prod_{j=1}^m f_{i,j}$ where, for all i and j,*

(1) $f_{i,j}\in\mathbb{Z}[x_1]\setminus\{0\}$ has degree $\leq d$ and $\leq t$ monomial terms

(2) each coefficient of $f_{i,j}$ has absolute value $\leq 2^d$, and is the difference of two nonnegative integers with at most δ nonzero digits in their binary expansions. ⋄

It is easily checked that there is an absolute constant C such that $\tau(f)=(1+kmt+\delta+\log d)^C$ for all $f\in\mathrm{SPS}(k,m,t,d,\delta)$. (Recall that $\tau(f)$ is the constant-free evaluation complexity of f, from Definition 1.13.)

Theorem 3.3. *Suppose that there is a prime p with the following property: For all $k, m, t, d, \delta \in \mathbb{N}$ and $f \in \mathrm{SPS}(k, m, t, d, \delta)$, we have that the cardinality of*

$$S'_f := \{e \in \mathbb{N} \mid f(p^e) = 0\}$$

is $(kmt + \delta + \log d)^{O(1)}$. Then the permanent of $n \times n$ matrices cannot be computed by constant-free, division-free arithmetic circuits of size $n^{O(1)}$.

The Shub-Smale τ-Conjecture thus implies the hypothesis of Theorem 3.3. Note also that the hypothesis of Theorem 1.2 trivially implies the hypothesis of Theorem 3.3.

The main technical fact we need now is the following:

Theorem 3.4. *(See* [Koi11, Thm. 7]*.) Let $G := (g_i)$ be a* **CH***-algebraic number generator and let $Z(G, m)$ be the set of all roots of the polynomials g_i for all $i \leq m$. If there is a polynomial q such that $Z(G, q(kmt + \delta + \log d))$ is a hitting set for $\mathrm{SPS}(k, m, t, d, \delta)$ then the permanent of $n \times n$ matrices cannot be computed by constant-free, division-free arithmetic circuits of size $n^{O(1)}$.* ■

The last result shows that the construction of explicit hitting sets of polynomial size for sums of products of sparse polynomials implies a lower bound for the permanent.

Proof of Theorem 3.3: Suppose there is a constant $c \geq 1$ such that any $f \in \mathrm{SPS}(k, m, t, d, \delta)$ has at most $(1 + kmt + \delta + \log d)^c$ integer roots that are powers of p. The set S'_f would then form a polynomial-size hitting set for $\mathrm{SPS}(k, m, t, d, \delta)$. By Theorem 3.4, it just remains to check that the sequence of polynomials $(x_1 - p^i)_{i \in \mathbb{N}}$ forms a **CH**-algebraic number generator. We must therefore show that the following problem belongs to **CH**: given two integers i and j in binary notation, compute the j-th bit of p^i. Note that this problem would be solvable in polynomial time if i was given in unary notation (by performing the $i - 1$ multiplications in the most naive way). To deal with the binary notation underlying our setting, we apply Theorem 3.10 of [Bür09]: iterated multiplication of exponentially many integers can be done within the counting hierarchy. Here we have to multiply together exponentially many (in the binary size of i) copies of the same integer p. We note that Theorem 3.10 of [Bür09] applies to a very wide class of integer sequences: the numbers to be multiplied must be computable in the counting hierarchy. In our case we only have to deal with a constant sequence (consisting of i copies of p) so the elements of this sequence are computable in polynomial time (and actually in constant time since p is constant). So we are done. ■

It is interesting to note that even a weakly exponential upper bound on the number of valuations would still suffice to prove new hardness results for the permanent: from the development of Sections 5 and 6 of [Koi11], and our development here, one has the following fall-back version of Theorem 3.3.

Theorem 3.5. *Suppose that there is a prime p with the following property: For all $k, m, t, d, \delta \in \mathbb{N}$ and $f \in \mathrm{SPS}(k, m, t, d, \delta)$, we have that $\#S'_f \leq 2^{(kmt+\delta+\log d)^{o(1)}}$. Then the permanent of $n \times n$ matrices cannot be computed by polynomial size depth 4 circuits using polynomial size integer constants.* ■

Note the *little*-"oh" in the exponent. In particular, a super-polynomial upper bound like $2^{(\log(kmt+\delta+\log d))^{1000}}$ would suffice to yield the conclusion of Theorem 3.5, but a bound like $2^{(kmt+\delta+\log d)^{1/1000}}$ would not. While the conclusion is weaker than that of Theorems 1.2 or 3.3, the truth of the hypothesis of Theorem 3.5 nevertheless yields a hitherto unknown complexity lower bound for the permanent.

4. Proving Theorem 1.10

For the sake of disambiguation, we recall the following basic definition.

Definition 4.1. *Fix any field K. We say that a matrix $E=[E_{i,j}]\in K^{m\times n}$ is in* reduced row echelon form *if and only if the following conditions hold:*

1. *The left-most nonzero entry of each row of E is 1, called the* leading 1 *of the row.*
2. *Every leading 1 is the unique nonzero element of its column.*
3. *The index j such that $E_{i,j}$ is a leading 1 of row i is a strictly increasing function of i.* $\diamond$

Note that in Condition (1), we allow a row to consist entirely of zeroes. Also, by Condition (3), all rows below a row of zeroes must also consist solely of zeroes. For example, the matrix $\begin{bmatrix} \boxed{1} & 0 & 0 & 3 & 0 & 2 \\ 0 & 0 & \boxed{1} & 12 & 0 & -5 \\ 0 & 0 & 0 & 0 & \boxed{1} & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$ is in reduced row echelon form, and we have boxed the leading 1s.

By *Gauss-Jordan Elimination* we mean the well-known classical algorithm that, given any matrix $M\in K^{m\times n}$, yields the factorization $UM=E$ with $U\in\mathbb{GL}_m(K)$ and E in reduced row echelon form (see, e.g., [Pra04, Str09]). In what follows, we use $(\cdot)^\top$ to denote the operation of matrix tranpose.

Definition 4.2. *Given any Laurent polynomials $f_1,\ldots,f_r\in K\left[x_1^{\pm 1},\ldots,x_n^{\pm 1}\right]$ with supports contained in a set $A=\{a_1,\ldots,a_t\}\subset\mathbb{Z}^n$ of cardinality t,* applying Gauss-Jordan Elimination to $(f_1,\ldots,f_r)$ *means the following: (a) we identify the row vector $(f_1,\ldots,f_r)$ with the vector-matrix product $(x^{a_1},\ldots,x^{a_t})C$ where $C\in K^{t\times r}$ and the entries of C are suitably chosen coefficients of the f_i, and (b) we replace $(f_1,\ldots,f_r)$ by $(g_1,\ldots,g_r)$ where $(g_1,\ldots,g_r)=(x^{a_1},\ldots,x^{a_t})E$ and $E^\top$ is the reduced row echelon form of $C^\top$.* $\diamond$

Note in particular that the ideals $\langle f_1,\ldots,f_r\rangle$ and $\langle g_1,\ldots,g_r\rangle$ are identical. As a concrete example, one can observe that applying Gauss-Jordan Elimination to the pair (x^3-y-1,x^3-2y+2) means that one instead works with the pair $(x^3-4,-y+3)$.

We now proceed with the proof of Theorem 1.10. In what follows, we set $A:=\bigcup_i A_i$, $t:=\#A$, and let $F:=(f_1,\ldots,f_n)$ be any polynomial system with $f_i\in\mathbb{C}_p\left[x_1^{\pm 1},\ldots,x_n^{\pm 1}\right]$ and $\mathrm{Supp}(f_i)\subseteq A_i$ for all i.

4.1. **Proving Assertions (0) and (1).** Assume $t\leq n+1$. If any f_i is a single monomial term then $Z^*_{\mathbb{C}_p}(F)$ is empty. Also, if any f_i is identically 0 then $\#Z^*_{\mathbb{C}_p}(F)$ is infinite, so (by Proposition 2.2) $\mathrm{ord}_p\Big(\#Z^*_{\mathbb{C}_p}(F)\Big)=+\infty$. So we may assume that no f_i is identically zero or a monomial term. Also, dividing all the f_i by a suitable monomial term, we may assume that $\mathbf{O}\in A$.

Assertion (0) then follows immediately from Proposition 2.4. So we may now assume that A does *not* lie in any $(n-1)$-flat (and $t=n+1$ in particular).

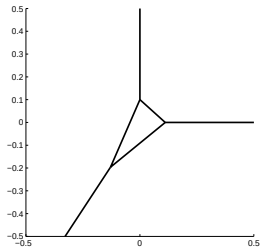
Our remaining case is then folkloric: by Gauss-Jordan Elimination (as in Definition 4.2, ordering so that the last monomial is $x^{\mathbf{O}}$), we can reduce to the case where each polynomial has 2 or fewer terms, and $\mathrm{Supp}(f_i)\cap\mathrm{Supp}(f_j)=\mathbf{O}$ for all $i\neq j$. In particular, should Gauss-Jordan Elimination not yield the preceding form, then some f_i is either identically zero or a monomial term, thus falling into one of our earlier cases. So assume F is a binomial system with $\mathrm{Supp}(f_i)\cap\mathrm{Supp}(f_j)=\mathbf{O}$ for all $i\neq j$. Since no $n+1$ points of A lie on a hyperplane, $\mathrm{Newt}(f_1),\ldots,\mathrm{Newt}(f_n)$ define n linearly independent vectors in $\mathbb{R}^n$. The underlying tropical varieties are then hyperplanes intersecting transversally, and the number of valuations is thus clearly 1.

So the upper bound from Assertion (1) is proved. The final equality follows immediately from the polynomial system $(x_1-1,\ldots,x_n-1)$. ■

Remark 4.3. *Note that in our proof, Gauss-Jordan Elimination allowed us to replace any tropically non-generic F by a new,* tropically generic *system with the same roots over $\mathbb{C}_p$. Recalling standard height bounds for linear equations (see, e.g.,* [Sto00]*), another consequence of our proof is that, when $t\leq n+1$, we can decide whether $\#\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(F)\right)$ is 0, 1, or ∞ in polynomial-time.* ⋄

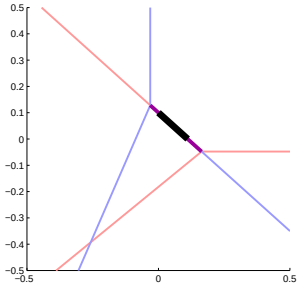
4.2. **Proving Assertion (2).** Let us first see an example illustrating a trick underlying our proof.

Example 4.4. *Consider, for any prime $p\neq 2$, the polynomial system* $F:=(f_1,f_2):=\left\{\begin{array}{l} px_2^{21}-px_1^{32}+p+x_1^9x_2^{10} \\ -(p+p^2)x_2^{21}+(p+p^3)x_1^{32}+p+p^4+(1+p)x_1^9x_2^{10}\end{array}\right.$. *The tropical varieties $\mathrm{Trop}_p(f_1)$ and $\mathrm{Trop}_p(f_2)$ turn out to be identical and equal to a polyhedral complex with exactly 3 0-dimensional cells and 6 1-dimensional cells (a truncation of which is shown on the right).*



How can we prove that $\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(F)\right)$ in fact has small cardinality?

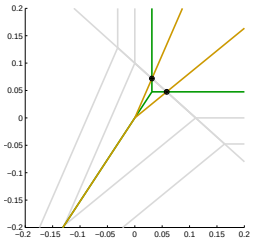
While it is not hard to apply Bernstein's Theorem (as in [Ber75]*) to see that F has only finitely many roots in $(\mathbb{C}_p^*)^2$, there is a simpler approach to proving $\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(F)\right)$ is finite: First note that via Gauss-Jordan Elimination (and a suitable ordering of monomials), F has the same roots in $(\mathbb{C}_p^*)^2$ as*



$F^{(1,2)}:=\left(f_1^{(1,2)},f_2^{(1,2)}\right):=\left\{\begin{array}{l} x_2^{21}+\frac{2+p^2+p^3}{p(p-1)}+\frac{2+p+p^2}{p^2(p-1)}x_1^9x_2^{10} \\ (p+p^3)x_1^{32}+\frac{2+p+p^3}{p(p-1)}+\frac{2(1+p)}{p^2(p-1)}x_1^9x_2^{10}\end{array}\right.$.

We then obtain that the tropical varieties $\mathrm{Trop}_p\left(f_1^{(1,2)}\right)$ and $\mathrm{Trop}_p\left(f_2^{(1,2)}\right)$ intersect (in a small interval) along a single 1*-dimensional cell, drawn more thickly, as shown to the right of the definition of $F^{(1,2)}$. (The intersection $\mathrm{Trop}(f_1)\cap\mathrm{Trop}(f_2)\cap\mathrm{Trop}\left(f_1^{(1,2)}\right)\cap\mathrm{Trop}\left(f_2^{(1,2)}\right)$ is drawn still more thickly.) From the definition of $\mathrm{Trop}_p(\cdot)$, it is not hard to check that the degenerately intersecting 1-cells of $\mathrm{Trop}_p\left(f_1^{(1,2)}\right)$ and $\mathrm{Trop}_p\left(f_2^{(1,2)}\right)$ correspond to parallel lower edges of $\mathrm{Newt}_p\left(f_1^{(1,2)}\right)$ and $\mathrm{Newt}_p\left(f_2^{(1,2)}\right)$, which in turn correspond to the binomials $\frac{2+p^2+p^3}{p(p-1)}+\frac{2+p+p^2}{p^2(p-1)}x_1^9x_2^{10}$ and $\frac{2+p+p^3}{p(p-1)}+\frac{2(1+p)}{p^2(p-1)}x_1^9x_2^{10}$. (Note that the intersecting 1-cells of the $\mathrm{Trop}\left(f_i^{(1,2)}\right)$ are each perpendicular to the resulting Newton polytopes of the preceding binomials.)*

So to contend with this remaining degenerate intersection, we simply apply Gauss-Jordan Elimination with the monomials ordered so that the aforementioned pair of binomials becomes a pair of monomials. More precisely, we obtain that F has the same roots in $(\mathbb{C}_p^*)^2$ as



$F^{(3,4)}:=\left(f_1^{(3,4)},f_2^{(3,4)}\right):=\left\{\begin{array}{l} -\frac{2}{p(p-1)}x_2^{21}+\frac{2+p+p^2}{p(p^2-1)}x_1^{32}+1 \\ \frac{2-p+p^2}{p(p-1)}x_2^{21}+\frac{2+p^2+p^3}{p^2-1}x_1^{32}+x_1^9x_2^{10}\end{array}\right.$.

$\mathrm{Trop}_p\Big(f_1^{(3,4)}\Big)$ *and* $\mathrm{Trop}_p\Big(f_2^{(3,4)}\Big)$ *then intersect transversally precisely within the overlapping* 1*-cells of* $\mathrm{Trop}_p(f_1)\cap\mathrm{Trop}_p(f_2)$ *and* $\mathrm{Trop}_p\Big(f_1^{(1,2)}\Big)\cap\mathrm{Trop}_p\Big(f_2^{(1,2)}\Big)$*. In particular, the intersection of the tropical varieties of the* f_i*,* $f_i^{(1,2)}$*, and* $f_i^{(3,4)}$ *consists of exactly* 2 *points:* $\big(\frac{1}{32},\frac{23}{320}\big)$ *and* $\big(\frac{11}{189},\frac{1}{21}\big)$*. So, thanks to Kapranov's Theorem,* $\mathrm{ord}_p\Big(Z^*_{\mathbb{C}_p}(F)\Big)$ *in fact has cardinality at most* 2*.* $\diamond$

A simple observation used in our example above is the following consequence of the basic ideal/variety correspondence.

Proposition 4.5. *Given any* $f_1,\ldots,f_r\in\mathbb{C}_p\big[x_1^{\pm1},\ldots,x_n^{\pm1}\big]$ *and* $F:=(f_1,\ldots,f_r)$*, we have* $\mathrm{ord}_p\Big(Z^*_{\mathbb{C}_p}(F)\Big)\subseteq\bigcap_{f\in\langle f_1,\ldots,f_r\rangle}\mathrm{ord}_p\Big(Z^*_{\mathbb{C}_p}(f)\Big)$*, where* $\langle f_1,\ldots,f_r\rangle\subseteq\mathbb{C}_p\big[x_1^{\pm1},\ldots,x_n^{\pm1}\big]$ *denotes the ideal generated by* $f_1,\ldots,f_r$*.* ■

The reverse inclusion also holds, but is far less trivial to prove (see, e.g., [MS12]). In particular, Example 4.4 shows us that restricting the intersection to a *finite* set of generators can sometimes result in strict containment.

Proof of Assertion (2) of Theorem 1.10: The case $n=1$ is immediate from Lemma 1.21 and the example $(A_1,f)=(\{0,1,2\},(x_1-1)(x_1-2))$. So we assume henceforth that $n\geq 2$.

Recall from last section that $t=n+2$ and $A:=\bigcup_\ell A_\ell$. For any distinct $i,j\in\{1,\ldots,n+2\}$ let us then define $F^{(i,j)}$ by applying Gauss-Jordan Elimination, as in Definition 4.2, where we order monomials so that the last exponents are a_i and a_j. In particular, F and $F^{(i,j)}$ clearly have the same roots in $(\mathbb{C}_p^*)^n$ for all distinct i,j. We will show that *every* $F^{(i,j)}$ can be assumed to be a trinomial system of a particular form.

First note that we may assume that $\mathrm{Supp}\Big(f_\ell^{(n+1,n+2)}\Big)\subseteq\{a_{r_\ell},a_{s_\ell},a_{n+2}\}$ for all ℓ, where $(r_\ell)_\ell$ is a strictly increasing sequence of integers in $\{1,\ldots,n\}$ satisfying $s_\ell\geq r_\ell\geq\ell$ for all ℓ. This is because, similar to our last proof, we may assume that each $f_\ell^{(n+1,n+2)}$ has at least 2 monomial terms, thus implying that $r_n\in\{n,n+1\}$. In particular, no $f_\ell^{(n+1,n+2)}$ can have 4 or more terms, by the positioning of the leading 1s in reduced row echelon form.

By dividing by a suitable monomial term, we may assume that $a_{n+2}=\mathbf{O}$. Also, by Lemma 2.3, we may assume that $a_\ell\in\mathbb{Z}^\ell\times\{0\}^{n-\ell}$ for all $\ell\in\{1,\ldots,n\}$. (Our general position assumption on A also implies that the $\ell^{\underline{\text{th}}}$ coordinate of a_ℓ is nonzero.) Now, should $f_n^{(n+1,n+2)}$ have exactly 2 monomial terms, then $f_n^{(n+1,n+2)}$ must be of one of the following forms: (a) $x^{a_n}+\alpha_n x^{a_{n+1}}$, (b) $x^{a_n}+\alpha_n x^{a_{n+2}}$, or (c) $x^{a_{n+1}}+\alpha_n x^{a_{n+2}}$, for some $\alpha_n\in\mathbb{C}_p^*$. In Case (c), we could then replace all occurences of $x^{a_{n+1}}$ in $f_1^{(n+1,n+2)},\ldots,f_{n-1}^{(n+1,n+2)}$ by a nonzero multiple of $x^{a_{n+2}}$. We would thus reduce to the setting of Assertion (1), in which case, the maximal finite number of valuations would be 1. In Cases (a) and (b), we obtain either that some x_i vanishes, or that $\mathrm{ord}_p x_n$ is a linear function of $\mathrm{ord}_p x_1,\ldots,\mathrm{ord}_p x_{n-1}$. So we could then reduce to a case one dimension lower.

So we may assume that $\mathrm{Supp}\Big(f_n^{(n+1,n+2)}\Big)=\{a_n,a_{n+1},a_{n+2}\}$, which in turn forces $a_\ell\in\mathrm{Supp}\Big(f_\ell^{(n+1,n+2)}\Big)\subseteq\{a_\ell,a_{n+1},a_{n+2}\}$ for all $\ell\in\{1,\ldots,n-1\}$. Moreover, by repeating the arguments of Cases (a) and (b) above, we may in fact assume $\mathrm{Supp}\Big(f_\ell^{(n+1,n+2)}\Big)=\{a_\ell,a_{n+1},a_{n+2}\}$ for all $\ell\in\{1,\ldots,n\}$.

Permuting indices, we can then repeat the last 3 paragraphs and assume further that, for any distinct $i,j\in\{1,\ldots,n+2\}$, we have

$(\star)$ $\quad \mathrm{Supp}\left(f_\ell^{(i,j)}\right)=\{a_{k_\ell},a_i,a_j\}$ for all $\ell\in\{1,\ldots,n\}$, where $\{k_\ell\}_\ell=A\setminus\{i,j\}$.

Let us now fix (i,j) and set $G=(g_1,\ldots,g_n):=F^{(i,j)}$. Thanks to $(\star)$ and Lemma 2.5 (mimicking the proof of Lemma 1.18), the $\mathrm{Trop}_p(g_i)$ each contain a half-plane parallel to a common hyperplane. We then obtain a finite partition of $\mathbb{R}^n$ into half-open slabs of a form linearly isomorphic (over $\mathbb{Q}$) to $(-\infty,u_1)\times\mathbb{R}^{n-1}$, $[u_\ell,u_{\ell+1})\times\mathbb{R}^{n-1}$ for $\ell\in\{1,\ldots,m_{i,j}-1\}$, or $[u_{m_{i,j}},+\infty)\times\mathbb{R}^{n-1}$, with $m_{i,j}\leq n$. More precisely, the boundaries of the cells of our partition are hyperplanes of the form $H_\ell^{(i,j)}:=\{v\in\mathbb{R}^n \mid (a_i-a_j)\cdot v=\mathrm{ord}_p(\gamma_\ell^{(i,j)})\}$ for $\ell\in\{1,\ldots,m_{i,j}\}$, where $\gamma_\ell^{(i,j)}$ is a ratio of coefficients of $f_\ell^{(i,j)}$.

In particular, Lemma 2.5 and our genericity hypothesis tell us that, within any slab, any non-empty intersection of $\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(f_1)\right),\ldots,\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(f_n)\right)$ must be a *transversal* intersection of n hyperplanes, unless it includes the intersection of two or more $H_k^{(i,j)}$. So if G is tropically generic, we have by Proposition 4.5 that $\#\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(F)\right)\leq n+1$.

Otherwise, any non-transversal intersection must occur within an intersection of slab boundaries $H_k^{(i,j)}$. So to finish this case, consider $n-1$ more distinct pairs $(i_2,j_2),\ldots,(i_n,j_n)$, i.e., $i_\ell\neq j_\ell$ for all ℓ and $\#\{i_\ell,j_\ell,i_{\ell'},j_{\ell'}\}\leq 3$ for all $\ell\neq\ell'$.

Just as for G, the genericity of the exponent set A implies that any non-transversal intersection for $\mathrm{Trop}_p(f_1^{(i_\ell,j_\ell)}),\ldots,\mathrm{Trop}_p(f_n^{(i_\ell,j_\ell)})$ must occur within the intersection of at least two coincident slab boundaries $H_k^{(i_\ell,j_\ell)}$. In particular, we may assume that none of $F^{(i_2,j_2)},\ldots,F^{(i_n,j_n)}$ are tropically generic (for $\#\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(F)\right)\leq n+1$ otherwise).

By our assumption on the genericity of the exponent set A, we have that $H_{\ell_1}^{(i,j)},H_{\ell_2}^{(i_2,j_2)},\ldots,H_{\ell_n}^{(i_n,j_n)}$ intersect transversally, for any choice of n-tuples $(\ell_1,\ldots,\ell_n)$. In particular, we have embedded the non-transversal intersections of $\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(F)\right)$ into a (finite) intersection of $m_{i,j}\prod_{\ell=2}^n m_{i_\ell,j_\ell}$ many tropical varieties. In particular, to count the non-transversal intersections, we may assume $m_{i,j},m_{i_2,j_2},\ldots,m_{i_n,j_n}\leq\left\lfloor\frac{n}{2}\right\rfloor$.

From our earlier observations on slab decomposition, there can be at most n intersections occuring away from an intersection of slab boundaries (since we are assuming G and the $F^{(i_\ell,j_\ell)}$ all fail to be tropically generic). The number of distinct points of $\mathrm{ord}_p\left(Z^*_{\mathbb{C}_p}(F)\right)$ lying in intersections of the form $H_{\ell_1}^{(i,j)}\cap H_{\ell_2}^{(i_2,j_2)}\cap\cdots\cap H_{\ell_n}^{(i_n,j_n)}$ is no greater than $\left\lfloor\frac{n}{2}\right\rfloor^n$. So our upper bound is proved.

That $\mathcal{V}_p(\{\mathbf{O},2e_1,e_1+e_2\},\{\mathbf{O},2e_1,e_2+e_3\},\ldots,\{\mathbf{O},2e_1,e_{n-1}+e_n\},\{\mathbf{O},2e_1,e_n\})\geq n+1$ follows directly from [PR13, Thm. 1.6]. To be more precise, the polynomial system

$$\left(x_1x_2-p\left(1+\frac{x_1^2}{p}\right),x_2x_3-\left(1+px_1^2\right),x_3x_4-\left(1+p^3x_1^2\right),\ldots,x_{n-1}x_n-\left(1+p^{2n-5}x_1^2\right),x_n-\left(1+p^{2n-3}x_1^2\right)\right)$$

has exactly $n+1$ valuation vectors for its roots over $\mathbb{C}_p$, and tropical genericity follows directly from [PR13, Lemma 3.7]. The reverse inequality then follows from our earlier observations on slab decomposition. In particular, via our earlier reductions, Assertions (0) and (1) easily imply that any F with smaller support has no more than n valuation vectors for its roots. ■

Remark 4.6. *Our proof thus reveals various supports A_i where $\#A_i=3$ for all i, $\#\left(\bigcup_i A_i\right)=n+2$, and $\mathcal{V}_p(A_1,\ldots,A_n)\leq n+1$.* ⋄

5. Proving Theorem 1.11

By Theorem 1.2 and Proposition 1.17 it is enough to show that, for $n := km + 1$ and $A_1, \ldots, A_n$ the supports of the polynomial system F from the proposition, we have $\mathcal{V}_p(A_1, \ldots, A_n) = (kmt)^{O(1)}$. By Lemma 1.18 we are done. ■

Since $\overline{\mathcal{R}}_p(A_1, \ldots, A_n) \leq \overline{\mathcal{V}}_p(A_1, \ldots, A_n)$, it is tempting to also conjecture that $\overline{\mathcal{V}}_p(A_1, \ldots, A_n) = \mathcal{V}_p(A_1, \ldots, A_n)^{O(1)}$. The latter bound clearly implies the hypothesis of Theorem 1.11, and thus also implies the hardness of the permanent. Unfortunately, the latter bound is too strong to be true beyond $n=1$.

Example 5.1. *Consider the polynomial system* $F := \left(x_1 - x_2 + 1, x_2^{p^r} - 1\right)$ *with supports* $A_1 = \{0, e_1, e_2\}$ *and* $A_2 = \{0, p^r e_2\}$. *It is then easily checked that* $\mathcal{V}_p(A_1, A_2) = 1$ *and, via* [Rob00, Pg. 107] *that* $\operatorname{ord}_p\left(Z^*_{\mathbb{C}_p}(F)\right) = \left\{\left(\frac{1}{p-1}, 0\right), \ldots, \left(\frac{1}{p^{r-1}(p-1)}, 0\right)\right\}$. *So* $\overline{\mathcal{V}}_p(A_1, A_2)$ *is bounded from below by a logarithmic function of the coordinates of the* A_i *and thus* $\overline{\mathcal{V}}_p(A_1, A_2)$ *can not be bounded from above by any constant power of* $\mathcal{V}_p(A_1, A_2)$. *Note in particular that the general position assumption of Assertion (2) of Theorem 1.10 is violated, since* $A_1 \cup A_2$ *contains* 3 *colinear points. Note, however, that this* F *has no roots at all in* $(\mathbb{Q}^*_p)^2$. ⋄

Similarly, the underlying tropical genericity assumption in Corollary 1.5 is necessary, as revealed by the r distinct valuations of the roots of the polynomial $(x_1 + 1)^{p^r} - 1$ in $\mathbb{C}^*_p$. (Nevertheless, note that the number of valuations is logarithmic in the number of factors $m = p^r$, and is thus still $(kmt)^{O(1)}$.) We are indebted to Kiran Kedlaya for pointing out the basic properties of p-adic $p^{r\underline{\text{th}}}$ roots of unity inspiring these last two examples.

6. Proving Theorem 1.12

First note that we can divide our equations by a suitable monomial term so that $\mathbf{O} \in A$.

The case where A has cardinality $n + 1$ can be easily handled just as in the proof of Theorem 1.10: F can be reduced to a binomial system via Gauss-Jordan Elimination, and then by Lemma 2.3 we can easily reduce to a *triangular* binomial system. In particular, all the roots of F in $(K^*)^n$ are non-degenerate and thus have multiplicity 1, so the sharpness of the bound is immediate as well.

So let us now assume that A has cardinality $n + 2$. By Gauss-Jordan Elimination and a monomial change of variables again, we may assume that F is of the form $(x^{a_1} - \alpha_1 - x^{a_{n+1}}/c, \ldots, x^{a_n} - \alpha_n - x^{a_{n+1}}/c)$ for some $c \in K^*$.

Consider now the matrix $\hat{A}$ obtained by appending a rows of 1s to the matrix with columns $\mathbf{O}, a_1, \ldots, a_{n+1}$. By construction, $\hat{A}$ has right-kernel generated by a single vector $b = (b_0, \ldots, b_{n+1}) \in \mathbb{Z}^{n+2}$ with *no* zero coordinates. So the identity $1^{b_0} (x^{a_1})^{b_1} \cdots (x^{a_{n+1}})^{b_{n+1}} = 1$ clearly holds for any $x \in (K^*)^n$. Letting $u := x^{a_{n+1}}$ we then clearly obtain a bijection between the roots of F in $(K^*)^n$ and the roots of $g(u) := u^{b_{n+1}} \left(\prod_{i=1}^n (\alpha_i + u)^{b_i}\right) - C$ where $C := c^{b_1 + \cdots + b_n}$. Furthermore, intersection multiplicity is preserved under this univariate reduction since each x_i is a radical of a linear function of a root of g. We thus need only determine the maximum intersection multiplicity of a root of g in K^*.

Since the multiplicity of a root ζ over a field of characteristic 0 is characterized by the derivative of least order not vanishing at ζ, let us suppose, to derive a contradiction, that $f(\zeta) = f'(\zeta) = \cdots = f^{(n+1)}(\zeta) = 0$, i.e., ζ is a root of multiplicity $\geq n + 2$. An elementary calculation then reveals that we must have

$$\frac{b'_1}{\alpha'_1+\zeta}+\cdots+\frac{b'_{m+1}}{\alpha'_{m+1}+\zeta}=\cdots=\frac{b'_1}{(\alpha'_1+\zeta)^{n+1}}+\cdots+\frac{b'_{m+1}}{(\alpha'_{m+1}+\zeta)^{n+1}}=0,$$

where $m\leq n$, the α'_i are distinct and comprise all the α_i, $\alpha'_{m+1}=0$, $b'_i:=\sum_{\alpha_j=\alpha'_i} b_j$, $b'_{m+1}:=b_{n+1}$, we set $\alpha'_{m+1}:=0$, and $\zeta\notin\{-\alpha_i\}$. In other words, $[b'_1,\ldots,b'_{m+1}]^\top$ is a right-null vector of a Vandermonde matrix with non-vanishing determinant. Since $[b'_1,\ldots,b'_{m+1}]$ has nonzero coordinates, we thus obtain a contradiction. So our upper bound is proved.

To prove that our final bound is tight, let $\zeta_1,\ldots,\zeta_{n+1}$ denote the (distinct) $(n+1)^{\underline{\text{st}}}$ roots of unity in K and set $g(u):=u\left(\prod_{i=1}^{n}(u+\zeta_{n+1}-\zeta_i)\right)+1$. Since $g(u-\zeta_{n+1})=u^{n+1}$, it is clear that g has $-\zeta_{n+1}$ as a root of multiplicity $n+1$. Furthermore, g is nothing more than the univariate reduction argument of our proof applied to the system $\left(\theta x_1-\zeta_{n+1}+\zeta_1-\frac{1}{x_1\cdots x_n}\ ,\ \ldots\ ,\ \theta x_n-\zeta_{n+1}+\zeta_n-\frac{1}{x_1\cdots x_n}\right)$ where θ is any $n^{\underline{\text{th}}}$ root of -1. ■

Acknowledgements

We thank Henry Cohn for his wonderful hospitality at Microsoft Research New England (where Rojas presented a preliminary version of Lemma 1.18 on July 30, 2012), and Kiran Kedlaya and Daqing Wan for useful p-adic discussions. We also thank Martín Avendano, Bruno Grenet, and Korben Rusek for useful discussions on an earlier version of Lemma 2.5, and Jeff Lagarias for insightful comments on an earlier version of this paper.

Most importantly, however, we would like to congratulate Mike Shub on his $70^{\underline{\text{th}}}$ birthday: he has truly blessed us with his friendship and his beautiful mathematics. We hope this paper will serve as a small but nice gift for Mike.

References

[Art67] Artin, Emil, *Algebraic Numbers and Algebraic Functions,* Gordon and Breach, New York, 1967.

[Ber75] Bernshtein, David N., *"The Number of Roots of a System of Equations,"* Functional Analysis and its Applications (translated from Russian), Vol. 9, No. 2, (1975), pp. 183–185.

[BCSS98] Blum, Lenore; Cucker, Felipe; Shub, Mike; and Smale, Steve, *Complexity and Real Computation,* Springer-Verlag, 1998.

[BC76] Borodin, Alan and Cook, Steve, *"On the number of additions to compute specific polynomials,"* SIAM Journal on Computing, 5(1):146–157, 1976.

[Bra39] Brauer, Alfred, *"On addition chains,"* Bull. Amer. Math. Soc. 45, (1939), pp. 736–739.

[Bür00] Bürgisser, Peter, *"Cook's versus Valiant's Hypothesis,"* Theor. Comp. Sci., 235:71–88, 2000.

[Bür09] _____, *"On defining integers and proving arithmetic circuit lower bounds,"* Computational Complexity, 18:81–103, 2009.

[BLMW11] Bürgisser, Peter; Landsberg, J. M.; Manivel, Laurent; and Weyman, Jerzy, *"An Overview of Mathematical Issues Arising in the Geometric Complexity Theory Approach to* $\mathbf{VP}\neq\mathbf{VNP}$*,"* SIAM J. Comput. **40**, pp. 1179-1209, 2011.

[Che04] Cheng, Qi, *"Straight Line Programs and Torsion Points on Elliptic Curves,"* Computational Complexity, Vol. 12, no. 3–4 (sept. 2004), pp. 150–161.

[EKL06] Einsiedler, Manfred; Kapranov, Mikhail; and Lind, Douglas, *"Non-archimedean amoebas and tropical varieties,"* Journal für die reine und angewandte Mathematik (Crelles Journal), Vol. 2006, no. 601, pp. 139–157, December 2006.

[Ful08] Fulton, William, *Intersection Theory,* $2^{\underline{\text{nd}}}$ ed., Ergebnisse der Mathematik und ihrer Grenzgebiete 3, **2**, Springer-Verlag, 2008.

[vzGG03] von zur Gathen, Joachim and Gerhard, Jürgen, *"Modern Computer Algebra,"* 2nd ed., Cambridge University Press, 2003.

[Gou03] Gouvêa, Fernando Q., *p-adic Numbers,* Universitext, 2nd ed., Springer-Verlag, 2003.

[HS82] Heintz, Joos and Schnorr, C.-P., *"Testing polynomials which are easy to compute,"* in Logic and Algorithmic (international symposium in honor of Ernst Specker), pp. 237–254, monograph no. 30 of L'Enseignement Mathématique, 1982.

[Her56] Hermite, Charles, *"Sur le nombres des racines d'une équation algébrique comprisé entre des limites donn'es,"* J. Reine Angew. Math. 52 (1856) 39–51; also: Oeuvres, Vol. I (Gauthier-Villars, Paris, 1905) pp. 397–414; English translation: P. C. Parks, Internat. J. Control 26 (1977), pp. 183–195.

[Kat07] Katok, Svetlana, *p-adic Analysis Compared with Real,* Student Mathematical Library, vol. 37, American Mathematical Society, 2007.

[Koi11] Koiran, Pascal, *"Shallow Circuits with High-Powered Inputs,"* in Proceedings of Innovations in Computer Science (ICS 2011, Jan. 6–9, 2011, Beijing China), pp. 309–320, Tsinghua University Press, Beijing.

[Lip94] Lipton, Richard, *"Straight-line complexity and integer factorization,"* Algorithmic number theory (Ithaca, NY, 1994), pp. 71–79, Lecture Notes in Comput. Sci., 877, Springer, Berlin, 1994.

[MS12] Maclagan, Diane and Sturmfels, Bernd, *Introduction to Tropical Geometry,* in progress.

[Maz78] Mazur, Barry, *"Rational Isogenies of Prime Degree,"* Invent. Math., 44, 1978.

[dMS96] de Melo, W. and Svaiter, B. F., *"The cost of computing integers,"* Proc. Amer. Math. Soc. **124** (1996), pp. 1377–1378.

[Mer96] Merel, Loic, *"Bounds for the torsion of elliptic curves over number fields,"* Invent. Math., 124(1–3):437–449, 1996.

[Mor97] T. de Araujo Moreira, Gustavo, *"On asymptotic estimates for arithmetic cost functions,"* Proccedings of the American Mathematical Society, Vol. 125, no. 2, Feb. 1997, pp. 347–353.

[Par99] Parent, Philippe, *"Effective Bounds for the torsion of elliptic curves over number fields,"* J. Reine Angew. Math, 508:65–116, 1999.

[PR13] Phillipson, Kaitlyn and Rojas, J. Maurice, *"Fewnomial Systems with Many Roots, and an Adelic Tau Conjecture,"* in proceedings of Bellairs workshop on tropical and non-Archimedean geometry (May 6–13, 2011, Barbados), Contemporary Mathematics, vol. 605, pp. 45–71, AMS Press, to appear.

[Pra04] Prasolov, V. V., *Problems and Theorems in Linear Algebra,* translations of mathematical monographs, vol. 134, AMS Press, 2004.

[Rob00] Robert, Alain M., *A course in p-adic analysis,* Graduate Texts in Mathematics, 198, Springer-Verlag, New York, 2000.

[Sch84] Schikhof, W. H., *Ultrametric Calculus, An Introduction to p-adic Analysis,* Cambridge Studies in Adv. Math. 4, Cambridge Univ. Press, 1984.

[Ser79] Serre, Jean-Pierre, *Local fields,* Graduate Texts in Mathematics, 67, Springer-Verlag, New York-Berlin, 1979.

[Shu93] Shub, Mike, *"Some Remarks on Bézout's Theorem and Complexity Theory,"* From Topology to Computation: Proceedings of the Smalefest (Berkeley, 1990), pp. 443–455, Springer-Verlag, 1993.

[Sma98] Smale, Steve, *"Mathematical Problems for the Next Century,"* Math. Intelligencer 20 (1998), no. 2, pp. 7–15.

[Sma00] _____, *"Mathematical Problems for the Next Century,"* Mathematics: Frontiers and Perspectives, pp. 271–294, Amer. Math. Soc., Providence, RI, 2000.

[Smi97] Smirnov, A. L., *"Torus Schemes Over a Discrete Valuation Ring,"* St. Petersburg Math. J. **8** (1997), no. 4, pp. 651–659.

[Sto00] Storjohann, Arne, *"Algorithms for matrix canonical forms,"* doctoral dissertation, Swiss Federal Institute of Technology, Zurich, 2000.

[Str09] Strang, Gilbert, *Introduction to Linear Algebra,* $4^{\underline{\text{th}}}$ edition, Wellesley-Cambridge Press, 2009.

[Val79] Valiant, Leslie G., *"The complexity of computing the permanent,"* Theoret. Comp. Sci., 8:189–201, 1979.

[Wei63] Weiss, Edwin, *Algebraic Number Theory*, McGraw-Hill, 1963.

[Zie95] Ziegler, Gunter M., *Lectures on Polytopes*, Graduate Texts in Mathematics, Springer Verlag, 1995.

E-mail address: pascal.koiran@ens-lyon.fr

E-mail address: natacha.portier@gmail.com

E-mail address: rojas@math.tamu.edu