VARGA'S THEOREM IN NUMBER FIELDS

PETE L. CLARK AND LORI D. WATSON

Abstract. We give a number field version of a recent result of Varga on solutions of polynomial equations with binary input variables and relaxed output variables.

1. Introduction

This note gives a contribution to the study of solution sets of systems of polynomial equations over finite local principal rings in the *restricted input / relaxed output* setting. The following recent result should help to explain the setting and scope.

Let $n, a_1, \ldots, a_n \in \mathbb{Z}^+$ and $1 \leq N \leq \sum_{i=1}^n a_i$. Put

$$\mathfrak{m}(a_1, \ldots, a_n; N) = \begin{cases} 1 & \text{if } N < n \\ \min \prod_{i=1}^n y_i & \text{if } n \leq N \leq \sum_{i=1}^n a_i \end{cases};$$

the minimum is over $(y_1, \ldots, y_n) \in \mathbb{Z}^n$ with $1 \leq y_i \leq a_i$ for all i and $\sum_{i=1}^n y_i = N$.

Theorem 1.1. *([Cl18, Thm. 1.7]) Let R be a Dedekind domain, and let $\mathfrak{p}$ be a maximal ideal in R with finite residue field $R/\mathfrak{p} \cong \mathbb{F}_q$. Let $n, r, v_1, \ldots, v_r \in \mathbb{Z}^+$. Let $A_1, \ldots, A_n, B_1, \ldots, B_r \subset R$ be nonempty subsets each having the property that no two distinct elements are congruent modulo $\mathfrak{p}$. Let $r, v_1, \ldots, v_r \in \mathbb{Z}^+$. Let $P_1, \ldots, P_r \in R[t_1, \ldots, t_n]$ be nonzero polynomials, and put*

$$z_{\mathbf{A}}^{\mathbf{B}} := \#\{x \in \prod_{i=1}^n A_i \mid \forall 1 \leq j \leq m \ P_j(x) \in B_j \pmod{\mathfrak{p}^{v_j}}\}.$$

Then $z_{\mathbf{A}}^{\mathbf{B}} = 0$ or

$$z_{\mathbf{A}}^{\mathbf{B}} \geq \mathfrak{m}\left(\#A_1, \ldots, \#A_n; \sum_{i=1}^n \#A_i - \sum_{j=1}^r (q^{v_j} - \#B_j) \deg(P_j)\right).$$

Remark 1.2. For every finite local principal ring $\mathfrak{r}$, there is a number field K, a prime ideal $\mathfrak{p}$ of the ring of integers $\mathbb{Z}_K$ of K, and $v \in \mathbb{Z}^+$ such that $\mathfrak{r} \cong \mathbb{Z}_K/\mathfrak{p}^v$ [Ne71], [BC15]. Henceforth we will work in the setting of residue rings of $\mathbb{Z}_K$.

If in Theorem 1.1 we take $v_1 = \cdots = v_r = 1$, $A_i = \mathbb{F}_q$ for all i and $B_j = \{0\}$ for all j, then we recover a result of E. Warning.

Theorem 1.3. *(Warning's Second Theorem [Wa35])*
Let $P_1, \ldots, P_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ be nonzero polynomials, and let

$$\mathbf{z} = \#\{\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n \mid P_1(\mathbf{x}) = \cdots = P_r(\mathbf{x}) = 0\}.$$

Then $\mathbf{z} = 0$ or $\mathbf{z} \geq q^{n - \sum_{j=1}^n \deg(P_j)}$.

By Remark 1.2, we may write $\mathbb{F}_q$ as $\mathbb{Z}_K/\mathfrak{p}$ for a suitable maximal ideal $\mathfrak{p}$ in the ring of integers $\mathbb{Z}_K$ of a suitable number field K. Having done so, Theorem 1.3 can be interpreted in terms of solutions to a congruence modulo $\mathfrak{p}$, whereas Theorem 1.1 concerns congruences modulo powers of $\mathfrak{p}$. At the same time, we are *restricting* the input variables $x_1, \ldots, x_n$ to lie in certain subsets $A_1, \ldots, A_n$ and also *relaxing* the output variables: we do not require that $P_j(x) = 0$ but only that $P_j(x)$ lies in a certain subset B_j modulo $\mathfrak{p}^{v_j}$.

There is however a tradeoff: Theorem 1.1 contains the hypothesis that no two elements of any A_i (resp. B_j) are congruent modulo $\mathfrak{p}$. Thus, whereas when $v_j = 1$ for all j we are restricting variables *by choice* – e.g. we could take each A_i to be a complete set of coset representatives for $\mathfrak{p}$ in $\mathbb{Z}_K$ as done above – when $v_j > 1$ we are restricting variables *by necessity* – we cannot take A_i to be a complete set of coset representatives for $\mathfrak{p}^{v_j}$ in $\mathbb{Z}_K$.

We would like to have a version of Theorem 1.1 in which the A_i's can be any nonempty finite subsets of $\mathbb{Z}_K$ and the B_j can be any nonempty finite subsets of $\mathbb{Z}_K$ containing $\{0\}$. However, to do so the degree conditions need to be modified in order to take care of the "arithmetic" of the rings $\mathbb{Z}_K/\mathfrak{p}^{d_j}$. In general this seems like a difficult – and worthy – problem.

An interesting special case was resolved in recent work of L. Varga [Va14]. His degree bound comes in terms of a new invariant of a subset $B \subset \mathbb{Z}/p^d\mathbb{Z} \setminus \{0\}$ called the **price of B** and denoted $\operatorname{pr}(B)$ that makes interesting connections to the theory of integer-valued polynomials.

Theorem 1.4. *(Varga* [Va14, Thm. 6]*) Let $P_1, \ldots, P_r \in \mathbb{Z}[t_1, \ldots, t_n] \setminus \{0\}$ be polynomials without constant terms. For $1 \leq j \leq r$, let $d_j \in \mathbb{Z}^+$, and let $B_j \subset \mathbb{Z}/p^{d_j}\mathbb{Z}$ be a subset containing 0. If*

$$\sum_{j=1}^{r} \deg(P_j) \operatorname{pr}(\mathbb{Z}/p^{d_j}\mathbb{Z} \setminus B_j) < n,$$

then

$$\#\{\mathbf{x} \in \{0,1\}^n \mid \forall 1 \leq j \leq r,\ P_j(\mathbf{x}) \in B_j \pmod{p^{d_j}}\} \geq 2.$$

In this note we will revisit and extend Varga's work. Here is our main result.

Theorem 1.5. *Let K be a number field of degree N, and let $e_1, \ldots, e_N$ be a $\mathbb{Z}$-basis for $\mathbb{Z}_K$. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathbb{Z}_K$, and let $d_1, \ldots, d_r \in \mathbb{Z}^+$. Let $P_1, \ldots, P_r \in \mathbb{Z}_K[t_1, \ldots, t_n]$ be nonzero polynomials without constant terms. For each $1 \leq j \leq r$, there are unique $\{\varphi_{j,k}\}_{1 \leq k \leq N} \in \mathbb{Z}[t_1, \ldots, t_n]$ such that*

$$P_j(t) = \sum_{k=1}^{N} \varphi_{j,k} e_j. \tag{1}$$

For $1 \leq j \leq r$, let B_j be a subset of $\mathbb{Z}_K/\mathfrak{p}^{d_j}$ that contains $0 \pmod{\mathfrak{p}^{d_j}}$. Let

$$S := \sum_{j=1}^{r} \left(\sum_{k=1}^{N} \deg(\varphi_{j,k}) \right) \operatorname{pr}(Z_K/\mathfrak{p}^{d_j} \setminus B_j).$$

Then

$$\#\{\mathbf{x} \in \{0,1\}^n \mid \forall 1 \leq j \leq r,\ P_j(\mathbf{x}) \pmod{\mathfrak{p}^{d_j}} \in B_j\} \geq 2^{n-S}.$$

Thus we extend Varga's Theorem 1.4 from $\mathbb{Z}$ to $\mathbb{Z}_K$ and refine the bound on the number of solutions.

In §2 we discuss the price of a subset of $\mathbb{Z}_K/\mathfrak{p}^d$. It seems to us that Varga's definition of the price has minor technical flaws: as we understand it, he tacitly assumes that for an integer-valued polynomial $f \in \mathbb{Q}[t]$ and $m, n \in \mathbb{Z}$, the output $f(n)$ modulo m depends only on the input modulo m. This is not true: for instance if $f(t) = \frac{t(t-1)}{2}$, then $f(n)$ modulo 2 depends on n modulo 4, not just modulo 2. So we take up the discussion from scratch, in the context of residue rings of $\mathbb{Z}_K$.

The proof of Theorem 1.5 occupies §3. After setting notation in §3.1 and developing some preliminaries on multivariate Gregory-Newton expansions in §3.2, the proof proper occurs in §3.3.

2. The Price

Consider the ring of **integer-valued polynomials**

$$\mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K) = \{f \in K[t] \mid f(\mathbb{Z}_K) \subset \mathbb{Z}_K\}.$$

We have inclusions of rings

$$\mathbb{Z}_K[t] \subset \mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K) \subset K[t].$$

Let

$$\mathfrak{m}(\mathfrak{p}, 0) := \{f \in \mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K) \mid f(0) \equiv 0 \pmod{\mathfrak{p}}\}.$$

Observe that $\mathfrak{m}(\mathfrak{p}, 0)$ is the kernel of a ring homomorphism $\mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K) \to \mathbb{Z}_K/\mathfrak{p}$: first evaluate f at 0 and then reduce modulo $\mathfrak{p}$. So $\mathfrak{m}(\mathfrak{p}, 0)$ is a maximal ideal of $\mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K)$. We put

$$\mathcal{U}(\mathfrak{p}, 0) := \mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K) \setminus \mathfrak{m}(\mathfrak{p}, 0) = \{f \in \mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K) \mid f(0) \notin \mathfrak{p}\}.$$

Let $d \in \mathbb{Z}^+$, and let B be a subset of $\mathbb{Z}_K/\mathfrak{p}^d$. We say that $h \in \mathcal{U}(\mathfrak{p}, 0)$ **covers B** if: for all $b \in \mathbb{Z}_K$ such that $b \pmod{\mathfrak{p}^d} \in B$, we have $h(b) \in \mathfrak{p}$. The **price of B**, denoted $\mathrm{pr}(B)$, is the least degree of a polynomial $h \in \mathcal{U}(\mathfrak{p}, 0)$ that covers B, or ∞ if there is no such polynomial.

Remark 2.1. a) If B_1, B_2 are subsets of $\mathbb{Z}_K/\mathfrak{p}^d \setminus \{0\}$, then

$$\mathrm{pr}(B_1 \cup B_2) \leq \mathrm{pr}(B_1) + \mathrm{pr}(B_2):$$

If for $i = 1, 2$ the polynomial $h_i \in \mathcal{U}(\mathfrak{p}, 0)$ covers B_i and has degree d_i, then $h_1 h_2 \in \mathcal{U}(\mathfrak{p}, 0)$ covers $B_1 \cup B_2$ and has degree $d_1 + d_2$.
b) If $0 \pmod{\mathfrak{p}^d} \in B$, then $\mathrm{pr}(B) = \infty$:
Since $0 \in B$ we need $h(0) \in \mathfrak{p}$, contradicting $h \in \mathcal{U}(\mathfrak{p}, 0)$.
c) If $d = 1$, then for any subset $B \subset \mathbb{Z}_K/\mathfrak{p} \setminus \{0\}$, we have $\mathrm{pr}(B) \leq \#B$:
Let $\tilde{B}$ be any lift of B to $\mathbb{Z}_K$. Then

$$h = \prod_{x \in \tilde{B}} (t - x) \in \mathbb{Z}_K[t] \subset \mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K)$$

covers B and has degree $\#B$. Note that here we use polynoimals with $\mathbb{Z}_K$-coefficients. It is clear that $\#B$ is the minimal degree of a covering polynomial h with $\mathbb{Z}_K$-coefficients: we can then reduce modulo $\mathfrak{p}$ to get a polynomial in $\mathbb{F}_q[t]$ that we want to be 0 at the points of B and nonzero at 0, so of course it must have degree at least $\#B$.
d) If we assume no element of B is 0 modulo $\mathfrak{p}$, let $\overline{B}$ be the image of B under the natural map $\mathbb{Z}_K/\mathfrak{p}^d \to \mathbb{Z}_K/\mathfrak{p} \cong \mathbb{F}_q$; then our assumption gives $0 \notin \overline{B}$. Above we constructed a polynomial $h \in \mathbb{Z}_K[t]$ of degree $\#\overline{B}$ such that $h(0) \notin \mathfrak{p}$ and for all $x \in \mathbb{Z}_K$ such that $x \pmod{\mathfrak{p}} \in B$, we have $h(x) \in \mathfrak{p}$. This same polynomial h covers B and shows that $\mathrm{pr}(B) \leq \mathrm{pr}(\overline{B}) \leq \#B$.

For $B \subset \mathbb{Z}_K/\mathfrak{p}^d \setminus \{0\}$ we define $\kappa(B) \in \mathbb{Z}^+$, as follows. For $1 \leq i \leq d$ we will recursively define $B_i \subset \mathbb{Z}_K/\mathfrak{p}^i \setminus \{0\}$ and $k_{i-1} \in \mathbb{N}$.

- Put $B_d = B$, and let k_{d-1} be the number of elements of B_d that lie in $\mathfrak{p}^{d-1}$.
- Having defined B_i and k_{i-1}, we let B_{i-1} be the set of $x \in \mathbb{Z}_K/\mathfrak{p}^{i-1}$ such that there are more than k_{i-1} elements of B_i mapping to x under reduction modulo $\mathfrak{p}^{i-1}$. We let k_{i-2} be the number of elements of B_{i-1} that lie in $\mathfrak{p}^{i-2}$.

Notice that $0 \notin B_i$ for all i: indeed, B_i is defined as the set of elements x such that the fiber under the map $\mathbb{Z}_K/\mathfrak{p}^{i+1} \to \mathbb{Z}_K/\mathfrak{p}_i$ has more elements of B_{i+1} than does the fiber over 0. We put

$$\kappa(B) := \sum_{i=0}^{d-1} k_i q^i.$$

Lemma 2.2. *We have $\kappa(B) \leq q^d - 1$.*

Proof. Each k_i is a set of elements in a fiber of a q-to-1 map, so certainly $k_i \leq q$. In order to have $k_i = q$, then B_{i+1} would need to contain the entire fiber over $0 \in \mathbb{Z}_K/\mathfrak{p}^i$, but this fiber includes $0 \in \mathbb{Z}_K/\mathfrak{p}^{i+1}$, which as above does not lie in B_{i+1}. So

$$\kappa(B) = \sum_{i=0}^{d-1} k_i q^i \leq \sum_{i=0}^{d-1} (q-1)q^i = q^d - 1. \qquad \square$$

Theorem 2.3. *For any subset $B \subset \mathbb{Z}_K/\mathfrak{p}^d \setminus \{0\}$, we have $\mathrm{pr}(B) \leq \kappa(B)$.*

Proof. Step 1: For $r \geq 1$, let $A = \{a_1, \ldots, a_{q^{d-1}}\} \subset \mathbb{Z}_K/\mathfrak{p}^d$ be a complete residue system modulo $\mathfrak{p}^{d-1}$ none of whose elements lie in $\mathfrak{p}^d$. We will show how to cover A with $f \in \mathcal{U}(\mathfrak{p}, 0)$ of degree q^{d-1}. We denote by $v_\mathfrak{p}$ the $\mathfrak{p}$-adic valuation on K. Let $\lambda \in \mathbb{Z}_K$ be an element with $v_\mathfrak{p}(\lambda) = \sum_{j=0}^{d-2} q^j$, and let $\beta \in \mathbb{Z}_K$ be an element such that $v_\mathfrak{p}(\beta) = 0$ and for all nonzero prime ideals $\mathfrak{q} \neq \mathfrak{p}$ of $\mathbb{Z}_K$, we have $v_\mathfrak{q}(\beta) \geq v_\mathfrak{q}(\lambda)$. (Such elements exist by the Chinese Remainder Theorem.) Put

$$g_A(t) := \prod_{j=1}^{q^{d-1}} (t - a_j) \in \mathbb{Z}_K[t], \ h_A(t) := \frac{\beta}{\lambda} g_A(t) \in K[t].$$

For all $x \in \mathbb{Z}_K$, $\{x - a_1, \ldots, x - a_{q^{d-1}}\}$ is a complete residue system modulo $\mathfrak{p}^{d-1}$, so in $\prod_{j=1}^{q^{d-1}} (x - a_j)$, for all $0 \leq j \leq d-1$ there are q^{d-1-j} factors in $\mathfrak{p}^j$, so $v_\mathfrak{p}(g_A(x)) \geq \sum_{j=0}^{d-2} q^j$ and thus $v_\mathfrak{p}(h_A(x)) \geq 0$. For any prime ideal $\mathfrak{q} \neq \mathfrak{p}$ of $\mathbb{Z}_K$, both $v_\mathfrak{q}(g_A(x))$ and $v_\mathfrak{q}(\frac{\beta}{\lambda})$ are non-negative, so $v_\mathfrak{q}(h_A(x)) \geq 0$. Thus $h_A \in \mathrm{Int}\,\mathbb{Z}_K$. Moreover the condition that no a_j lies in $\mathfrak{p}^d$ ensures that $v_\mathfrak{p}(g_A(0)) = \sum_{j=0}^{d-2} q^j$, so $h_A \in \mathcal{U}(\mathfrak{p}, 0)$. If $x \in \mathbb{Z}_K$ is such that $x \equiv a_j \pmod{\mathfrak{p}^d}$ for some j, then $v_\mathfrak{p}(x - a_j) \geq d$. Since in the above lower bounds of $v_\mathfrak{p}(g_A(x))$ we obtained a lower bound of at most $d-1$ on the $\mathfrak{p}$-adic valuation of each factor, this gives an extra divisibility and shows that $v_\mathfrak{p}(h_A(x)) \geq 0$. Thus h_A covers A with price at most q^{d-1}.
Step 2: Now let $B \subset \mathbb{Z}_K/\mathfrak{p}^d \setminus \{0\}$. The number of elements of B that lie in $\mathfrak{p}^{d-1}$ is k_{d-1}. For each of these elements x_i we choose a complete residue system A_i modulo $\mathfrak{p}^{d-1}$ containing it; since no x_i lies in $\mathfrak{p}^d$ this system satisfies the hypothesis of Step 1, so we can cover each A_i with price at most q^{d-1} and thus (using Remark 2.1a)) all of the A_i's with price at most $k_{d-1}q^{d-1}$. However, by suitably choosing the A_i's we can cover many other elements as well. Indeed, because we are choosing k_{d-1} complete residue systems modulo $\mathfrak{p}^{d-1}$, we can cover every element x that is congruent modulo $\mathfrak{p}^{d-1}$ to at most k_{d-1} elements of B. By definition of B_{d-1}, this means that we can cover all elements of B that do not map modulo $\mathfrak{p}^{d-1}$ into B_{d-1}. Now suppose that we can cover B_{d-1} by $h \in \mathcal{U}(\mathfrak{p}, 0)$ of degree κ'. This means that for every $x \in \mathbb{Z}_K$ such that $x \pmod{\mathfrak{p}^{d-1}}$ lies in B_{d-1}, $h(x) \in \mathfrak{p}$. But then every element of B whose image in $\mathfrak{p}^{d-1}$ lies in B_{d-1} is covered by h, so altogether we get

$$\mathrm{pr}(B) \leq k_{d-1}q^{d-1} + \mathrm{pr}(B_{d-1}).$$

Now applying the same argument successively to $B_{d-1}, \ldots, B_1$ gives

$$\mathrm{pr}(B_i) \leq k_{i-1}q^{i-1} + \mathrm{pr}(B_{i-1})$$

and thus

$$\mathrm{pr}(B) \leq \sum_{i=0}^{d-1} k_i q^i = \kappa(B). \qquad \square$$

3. Proof of the Main Theorem

3.1. **Notation.** Let K be a number field of degree N, and let $e_1, \ldots, e_N$ be a $\mathbb{Z}$-basis for $\mathbb{Z}_K$. A $\mathbb{Z}$-basis for $\mathbb{Z}_K[t_1, \ldots, t_n]$ is given by $e_j \underline{t}^I$ as j ranges over elements of $\{1, \ldots, N\}$ and I ranges over elements of $\mathbb{N}^n$. So for any $f \in \mathbb{Z}_K[t_1, \ldots, t_n]$, we may write

$$f = \varphi_1(t_1, \ldots, t_n)e_1 + \ldots + \varphi_N(t_1, \ldots, t_n)e_N, \ \varphi_i \in \mathbb{Z}[t_1, \ldots, t_n]. \tag{2}$$

Then we have

$$\deg f = \max_i \deg \varphi_i.$$

For a subset $B \subset \mathbb{Z}_K/\mathfrak{p}^d$, we put

$$\overline{B} = \mathbb{Z}_K/\mathfrak{p}^d \setminus B.$$

3.2. **Multivariable Newton Expansions.**

Lemma 3.1.
If $f \in \mathbb{Q}[t]$ is a polynomial and $f(\mathbb{N}) \subset \mathbb{Z}$, then $f(\mathbb{Z}) \subset \mathbb{Z}$.

Proof. See e.g. [CC, p. 2]. $\square$

Theorem 3.2.
Let $f \in K[t]$.
a) There is a unique function $\alpha_\bullet(f) : \mathbb{N}^N \to K$, $\underline{r} \mapsto \alpha_{\underline{r}}(f)$ such that
(i) we have $\alpha_{\underline{r}}(f) = 0$ for all but finitely many $\underline{r} \in \mathbb{N}^N$, and
(ii) for all $x = x_1 e_1 + \ldots + x_N e_N \in \mathbb{Z}_K$, we have

$$f(x) = \sum_{\underline{r} \in \mathbb{N}^N} \alpha_{\underline{r}}(f) \binom{x_1}{r_1} \cdots \binom{x_N}{r_N}. \tag{3}$$

b) The following are equivalent:
(i) We have $f \in \mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K)$.
(ii) For all $r \in \mathbb{N}^N$, $\alpha_{\underline{r}}(f) \in \mathbb{Z}_K$.
*We call the $\alpha_{\underline{r}}(f)$ the **Gregory-Newton coefficients** of f.*

Proof. Step 1: Let $f \in K[t]$. Let $e_1, \ldots, e_N$ be a $\mathbb{Z}$-basis for $\mathbb{Z}_K$. We introduce new independent indeterminates $t_1, \ldots, t_N$ and make the substitution

$$t = \sum_{k=1}^{N} e_k t_k$$

to get a polynomial

$$\tilde{f} \in K[\underline{t}].$$

This polynomial induces a map $K^N \to K$ hence, by restriction, a map $\mathbb{Z}^N \to K$. For $\underline{x} = (x_1, \ldots, x_N) \in \mathbb{Z}^N$, write $x = x_1 e_1 + \ldots + x_N e_N \in \mathbb{Z}_K$. Then we have

$$\tilde{f}(\underline{x}) = f(x).$$

Let $\mathcal{M} = \mathrm{Maps}(\mathbb{Z}^N, K)$ be the set of all such functions, and let $\mathcal{P}$ be the K-subspace of $\mathcal{M}$ consisting of functions obtained by evaluating a polynomial in $K[\underline{t}]$ on $\mathbb{Z}^N$, as above. By the CATS Lemma [Cl14, Thm. 12], the map $K[\underline{t}] \to \mathcal{P}$ is an isomorphism of K-vector spaces. Henceforth we will identify $K[\underline{t}]$ with $\mathcal{P}$ inside $\mathcal{M}$.

Step 2: For all $1 \leq k \leq N$, we define a K-linear endomorphism Δ_k of $\mathcal{M}$, the **kth partial difference operator**:

$$\Delta_k(g) : x \in \mathbb{Z}^N \mapsto g(x+e_k) - g(x).$$

These endomorphisms all commute with each other:

$$(\Delta_i \circ \Delta_j)(g) = g(x+e_i+e_j) - g(x+e_j) - g(x+e_i) + g(x) = (\Delta_j \circ \Delta_i)(g).$$

Let Δ_k^0 be the identity operator on $\mathcal{M}$, and for $i \in \mathbb{Z}^+$, let Δ_k^i be the i-fold composition of Δ_k. For $I = (i_1, \ldots, i_N) \in \mathbb{N}^N$, put

$$\Delta^I = \Delta^{i_1} \circ \ldots \circ \Delta^{i_N} \in \operatorname{End}_K(\mathcal{M}).$$

When we apply Δ_k to a monomial $\underline{t}^I$, we get another polynomial. More precisely, if $\deg_{t_k}(\underline{t}^I) = 0$ then $\Delta_k \underline{t}^I$ is the zero polynomial; otherwise

$$\deg_{t_k}(\Delta_k \underline{t}^I) = (\deg_{t_k} \underline{t}^I) - 1;\ \forall l \neq k, \deg_{t_l}(\Delta_k \underline{t}^I) = \deg_{t_l} \underline{t}^I.$$

Thus for each $f \in \mathcal{P}$, for all but finitely many $I \in \mathbb{N}^N$, we have that $\Delta^I(f) = 0$.

For the one variable difference operator, we have

$$\Delta \binom{x}{r} = \binom{x+1}{r} - \binom{x}{r} = \binom{x}{r-1}.$$

From this it follows that for $I, \underline{r} \in \mathbb{N}^N$ we have

$$\Delta^I \left(\binom{x_1}{r_1} \cdots \binom{x_N}{r_N} \right) (\underline{0}) = \binom{0}{r_1 - i_1} \cdots \binom{0}{r_N - i_N} = \delta_{\underline{r}, I} \tag{4}$$

So if $\beta_\bullet : \mathbb{N}^N \to K$ is any finitely nonzero function then for all $I \in \mathbb{N}^N$ we have

$$\Delta^I \Big(\sum_{\underline{r} \in \mathbb{N}^N} \beta_{\underline{r}} \binom{x_1}{r_1} \cdots \binom{x_N}{r_N} \Big)(\underline{0}) = \beta_I, \tag{5}$$

and thus there is at most one such function satisfying (3), namely

$$\alpha_\bullet(f) : \underline{r} \mapsto \Delta^{\underline{r}}(f)(\underline{0}).$$

So for any $f \in \mathcal{M}$ and $\underline{r} \in \mathbb{N}^N$, we define the **Gregory-Newton coefficient**

$$\alpha_{\underline{r}}(f) := \Delta^{\underline{r}}(f)(\underline{0}) \in K.$$

We may view the assignment of the package $\{\alpha_{\underline{r}}(f)\}_{\underline{r} \in \mathbb{N}^N}$ of Gregory-Newton coefficients to $f \in \mathcal{M}$ as a K-linear mapping

$$\mathcal{M} \to K^{\mathbb{N}^N}.$$

If we put $\mathcal{M}^+ = \operatorname{Maps}(\mathbb{N}^N, K)$, then we get a factorization

$$\mathcal{M} \to \mathcal{M}^+ \stackrel{\alpha}{\to} K^{\mathbb{N}^N},$$

where the first map restricts from $\mathbb{Z}^N$ to $\mathbb{N}^N$, and the factorization occurs because the Gregory-Newton coefficients depend only on the values of f on $\mathbb{N}^N$. We make several observations:
First Observation: The map α is an isomorphism. Indeed, knowing all the successive differences at 0 is equivalent to knowing all the values on $\mathbb{N}^N$, and all possible packages of Gregory-Newton coefficients arise. Namely, let S_n be the assertion that for all $x \in \mathbb{N}^N$ with $\sum_k x_k = n$ and all $f \in \mathcal{M}$, then $f(x)$ is a $\mathbb{Z}$-linear combination of its Gregory-Newton coefficients. The case $n = 0$ is clear: $f(0) = \alpha_0(f)$. Suppose S_n holds for n, let $x \in \mathbb{N}^N$ be such that $\sum_k x_k = n+1$, and choose k such that $x = y + e_k$; thus $\sum_k y_k = n$. Then

$$f(x) = f(y) + \Delta_k f(y).$$

By induction, $f(y)$ is a $\mathbb{Z}$-linear combination of the Gregory-Newton coefficients of f and $\Delta_k f(y)$ is a $\mathbb{Z}$-linear combination of the Gregory-Newton coefficients of $\Delta_k f$. But every Gregory-Newton coefficient of $\Delta_k f$ is also a Gregory-Newton coefficient of f, completing the induction.

Second Observation: The composite map

$$K[\underline{t}] \to \mathcal{M} \to \mathcal{M}^+ \stackrel{\alpha}{\to} K^{\mathbb{N}^N}$$

is an injection. Indeed, the kernel of $\mathcal{M} \to K^{\mathbb{N}^N}$ is the set of functions that vanish on $\mathbb{Z}^N \setminus \mathbb{N}^N$. In particular, any element of the kernel vanishes on the infinite Cartesian subset $(\mathbb{Z}^{<0})^N$ and thus by the CATS Lemma is the zero polynomial.

Third Observation: For a subring $R \subset K$ and $f \in \mathcal{M}$, we have $f(\mathbb{N}^N) \subset R$ iff all of the Gregory-Newton coefficients of f lie in R. This is a consequence of the First Observation: the Gregory-Newton coefficients are $\mathbb{Z}$-linear combinations of the values of f on $\mathbb{N}^N$ and conversely.

Step 3: For $F \in K[\underline{t}]$, we define the **Newton expansion**

$$T(F) = \sum_{\underline{r} \in \mathbb{N}^N} \alpha_{\underline{r}}(F) \binom{t_1}{r_1} \cdots \binom{t_N}{r_N} \in K[\underline{t}].$$

This is a finite sum. Moreover, by definition of $\alpha_{\underline{r}}(F)$ and by (5) we get that for all $r \in \mathbb{N}^N$,

$$\alpha_{\underline{r}}(T(F)) = \alpha_{\underline{r}}(F).$$

It now follows from Step 2 that $T(F) = F \in K[\underline{t}]$. Applying this to the $\tilde{f}$ associated to $f \in K[t]$ in Step 1 completes the proof of part a).

Step 4: If we assume that $f \in \operatorname{Int}(\mathbb{Z}_K, \mathbb{Z}_K)$ then $\tilde{f}(\mathbb{Z}^N) \subset \mathbb{Z}_K$ so all the Gregory-Newton coefficents lie in $\mathbb{Z}_K$. Conversely, if all the Gregory-Newton coefficients of $\tilde{f}$ lie in $\mathbb{Z}_K$, then for $x = x_1 e_1 + \ldots + x_N e_N \in \mathbb{Z}_K$, by Lemma 3.1 and (3) we have $f(x) = \tilde{f}(x_1, \ldots, x_N) \in \mathbb{Z}_K$, so $f \in \operatorname{Int}(\mathbb{Z}_K, \mathbb{Z}_K)$. □

3.3. **Proof of Theorem 1.5.** We begin by recalling the following result.

Theorem 3.3. *Let F be a field, and let $P \in F[t_1, \ldots, t_n]$ be a polynomial. Let*

$$\mathcal{U} := \{\mathbf{x} \in \{0,1\}^n \mid P(\mathbf{x}) \neq 0\}.$$

Then either $\#\mathcal{U} = 0$ or $\#\mathcal{U} \geq 2^{n-\deg(P)}$.

Proof. This is a special case of a result of Alon-Füredi [AF93, Thm. 5]. □

We now turn to the proof of Theorem 1.5. Put

$$Z := \{x \in \{0,1\}^n \mid \forall 1 \leq j \leq r,\ P_j(x) \pmod{\mathfrak{p}^{d_j}} \in B_j\}.$$

Step 0: If $q = \#\mathbb{Z}_K/\mathfrak{p}$ is a power of p, then we have $p^d \in \mathfrak{p}^d$. Therefore in (1) if we modify any coefficient of $\varphi_{j,k}(t)$ by a multiple of p^d, it does not change P_j modulo $\mathfrak{p}^d$ and thus does not change the set Z. We may thus assume that every coefficient of every $\varphi_{j,k}$ is non-negative.

Step 1: For $w = \sum_{i=1}^k \underline{t}^{I_i}$ a sum of monomials and $0 \leq r \leq k$, we put

$$\Psi_r(w) := \sum_{1 \leq i_1 < i_2 < \ldots < i_r \leq k} \underline{t}^{I_{i_1}} \cdots \underline{t}^{I_{i_r}}.$$

For $x \in \{0,1\}^n$, we have $w(x) = \#\{1 \leq i \leq k \mid x^{I_i} = 1\}$, so

$$\Psi_r(w)(x) = \binom{w(x)}{r}.$$

For $f \in \mathbb{Z}_K[t_1, \ldots, t_n]$, write $f = \sum_{k=1}^N \varphi_k(t) e_k$ and suppose that all the coefficients of each φ_k are non-negative – equivalently, each $\varphi_k(t)$ is a sum of monomials. For $\underline{r} \in \mathbb{N}^N$, we put

$$\Psi_{\underline{r}}(f) := \Psi_{r_1}(\varphi_1) \cdots \Psi_{r_N}(\varphi_N) \in \mathbb{Z}[\underline{t}].$$

For $h \in \mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K)$ with Gregory-Newton coefficients $\alpha_{\underline{r}}$, we put

$$\Psi^h(f) := \sum_{\underline{r} \in \mathbb{N}^N} \alpha_{\underline{r}} \Psi_{\underline{r}}(f) \in \mathbb{Z}_K[\underline{t}].$$

For $x \in \{0,1\}^n$, we have

$$\Psi_{\underline{r}}(x) = \prod_{k=1}^{N} \binom{\varphi_k(x)}{r_k},$$

so using (2) we get

$$\Psi^h(f)(x) = \sum_{\underline{r}} \alpha_{\underline{r}} \Psi_{\underline{r}}(f)(x) = \sum_{\underline{r}} \alpha_{\underline{r}} \binom{\varphi_1(x)}{r_1} \cdots \binom{\varphi_N(x)}{r_N}$$
$$= h(\varphi_1(x)e_1 + \ldots + \varphi_N(x)e_N) = h(f(x)).$$

Step 2: For $1 \leq j \leq r$, let $h_j \in \mathrm{Int}(\mathbb{Z}_K, \mathbb{Z}_K)$ have degree $\mathrm{pr}(\overline{B_j})$ and cover $\overline{B_j}$. Put

$$F := \prod_{j=1}^{r} \Psi^{h_j}(P_j) \pmod{\mathfrak{p}} \in \mathbb{Z}_K/\mathfrak{p}[\underline{t}] = \mathbb{F}_q[\underline{t}].$$

Note that

$$\deg(F) \leq \sum_{j=1}^{r} \deg \Psi^{h_j}(P_j) \leq \sum_{j=1}^{r} \left(\deg(h_j) \sum_{k=1}^{n} \deg(\varphi_{j,k}) \right) = S.$$

Here is the key observation: for $x \in \{0,1\}^n$, if $F(x) \neq 0$, then for all $1 \leq j \leq r$ we have $\mathfrak{p} \nmid \Psi^{h_j}(P_j)(x) = h_j(P_j(x))$, so $P_j(x) \pmod{\mathfrak{p}^{d_j}} \notin \overline{B_j}$, and thus $x \in Z$.

Step 3: For all $1 \leq j \leq r$ we have $P_j(0) = 0$ and $h_j \in \mathcal{U}(\mathfrak{p}, 0)$, so $h_j(0) \notin \mathfrak{p}$, so

$$F(0) = \prod_{j=1}^{r} \Psi_j^h(P_j(0)) = \prod_{j=1}^{r} h_j(P_j(0)) \pmod{\mathfrak{p}} = \prod_{j=1}^{r} h_j(0) \pmod{\mathfrak{p}} \neq 0.$$

Applying Alon-Füredi to F, we get

$$\#Z \geq \#\{x \in \{0,1\}^n \mid F(x) \neq 0\} \geq 2^{n - \deg F} \geq 2^{n-S},$$

completing the proof of Theorem 1.5.

References

[AF93] N. Alon and Z. Füredi, *Covering the cube by affine hyperplanes.* Eur. J. Comb. 14 (1993), 79–83.

[BC15] A. Brunyate and P.L. Clark, *Extending the Zolotarev-Frobenius approach to quadratic reciprocity.* Ramanujan J. 37 (2015), 25-50.

[CC] P.-J. Cahen and J.-L. Chabert, *Integer-valued polynomials.* Mathematical Surveys and Monographs, 48. American Mathematical Society, Providence, RI, 1997.

[CFS14] P.L. Clark, A. Forrow and J.R. Schmitt, *Warning's Second Theorem with restricted variables.* Combinatorica 37 (2017), 397-417.

[Cl14] P.L. Clark, *The Combinatorial Nullstellensätze Revisited.* Electronic Journal of Combinatorics. Volume 21, Issue 4 (2014). Paper #P4.15.

[Cl18] P.L. Clark, *Fattening up Warning's Second Theorem.* `http://alpha.math.uga.edu/~pete/Main_Theorem.pdf`

[Ne71] A.A. Nečaev, *The structure of finite commutative rings with unity.* Mat. Zametki 10 (1971), 679–688.

[Va14] L. Varga, *Combinatorial Nullstellensatz modulo prime powers and the parity argument.* Electron. J. Combin. 21 (2014), no. 4, Paper 4.44, 17 pp.

[Wa35] E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley.* Abh. Math. Sem. Hamburg 11 (1935), 76–83.