8-6-2007

Polynomial Functions over Rings of Residue Classes of Integers

M Brandon Meredith

POLYNOMIAL FUNCTIONS OVER RINGS OF RESIDUE CLASSES OF INTEGERS

by

M BRANDON MEREDITH

Under the Direction of Florian Enescu

ABSTRACT

In this thesis we discuss how to find equivalent representations of polynomial functions over the ring of integers modulo a power of a prime. Specifically, we look for lower degree representations and representations with fewer variables for which important applications in electrical and computer engineering exist. We present several algorithms for finding these compact formulations.

INDEX WORDS: Polynomial function, Polynomial, Algebra, Electrical circuit, Simplification, Simplifiable. Equivalence verification

POLYNOMIAL FUNCTIONS OVER RINGS OF RESIDUE CLASSES OF INTEGERS

by

M BRANDON MEREDITH

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of

Master of Science

in the College of Arts and Sciences

Georgia State University

2007

POLYNOMIAL FUNCTIONS OVER RINGS OF RESIDUE CLASSES OF INTEGERS

by

M BRANDON MEREDITH

Major Professor:	Florian Enescu
Committee:	Mihaly Bakonyi
	Yongwei Yao

Electronic Version Approved:

Office of Graduate Studies

College of Arts and Sciences

Georgia State University

August 2007

ACKNOWLEDGEMENTS

This work could not have been done without the direction and constant aid of my advisor Dr. Florian Enescu. The motivation behind this work would not have existed without the mathematically minded group in the Electrical Engineering Department at the University of Utah, including Dr. Priyank Kalla, Namrata Shekhar, and Sivaram Gopalakrishnan. Finally, the author was partially supported by the NSF grant CCF-515010.

TABLE OF CONTENTS

1. Introduction

The high technology fields rely on the continued shrinking of electrical circuits for the increase of computing power in an increasingly confined space. Certain among these electrical circuits share a relationship with the polynomials over the ring of integers modulo a power of a prime, that is, $\mathbb{Z}_{p^\alpha}$ [13]. Therefore, methods for "shrinking" polynomials over this ring provide equivalent, but more compact, electrical circuits. "Shrinking" a polynomial can take on the form of finding a lower degree polynomial whose associated polynomial function is equal to the polynomial function of the original polynomial, or it can take the form of decreasing the number of variables of a polynomial by means of linear substitutions, among other forms.

Section 2 deals with equating polynomial functions, and Sections 3 and 4 provides a numerical palliative for the problem of reducing the number of variables of a polynomial.

It should be noted that we will use some age-old notation. Specifically, we will use $\mathbb{Z}$ to mean the set of integers, $\mathbb{Z}_n$ is the set of integers modulo a number n, and $\mathbb{Z}[x]$ is the ring of univariate polynomials over the integers, or more generally if R is some commutative ring then $R[x_1, \dots, x_n]$ is the ring of n-variable polynomials with coefficients in R.

1.1. **Polynomials v. Polynomial Functions.**

One of the first steps of this work must be to call up the difference between a polynomial and the function that it represents. This may sound needlessly nuanced, but the disparity between the two ideas becomes annoyingly salient when one starts to work over domains and ranges that are not necessarily the full set of integers. In fact, much work (though not enough!) has been done explaining exactly what properties these polynomial functions have. For instance, see the work of Chen [4, 5], Hungerbueler and Specker [9], Barghava [1], Frisch [6], Wood [15], and Singmaster [14]. As the distinction will bear quite a bit of weight in a good part of this work, we begin here:

You will remember that a single variable polynomial is an expression of the type $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ where the a_i come from some ring R. A multivariate polynomial can be seen in the same way, if we consider R to be a polynomial ring itself. The important thing to remember is that when we write about polynomials, we are writing about *expressions*, the actual object with coefficients and variables, not the function it can represent.

Having recalled polynomials, we now define polynomial functions for the cases that are pertinent to this work:

Definition 1.1. A function $f : \mathbb{Z} \to \mathbb{Z}_m$ is a *polynomial function* if there exists a polynomial $F \in \mathbb{Z}[x]$ such that $f(a) = F(a) + m\mathbb{Z}$ for all $a \in \mathbb{Z}$.

Notice that in this definition, we used the notation $F(a) + m\mathbb{Z}$ which denotes the coset of $\mathbb{Z}$ in which the integer $F(a)$ is a member. One should keep in mind that f, in the above definition, is actually mapping integers to cosets, not integers to integers. We use this notation as opposed to hats and such to clear up meaning, especially in the multi-variate case.

Definition 1.2. A function $f : \mathbb{Z}_n \to \mathbb{Z}_m$ is also defined to be a *polynomial function* if there exists a polynomial function $f' : \mathbb{Z} \to \mathbb{Z}_m$ such that $f = f' \circ \pi$ where $\pi_n : \mathbb{Z}_n \to \mathbb{Z}$ is defined as $\pi_n(x + n\mathbb{Z}) = a$ for all $x \in \mathbb{Z}$ and $a \in \{0, \ldots, n-1\}$ where $x \equiv a(mod\ n)$.

Note that this definition involves functions that map cosets of $\mathbb{Z}$ to cosets of $\mathbb{Z}$. Note also that whereas every polynomial provides a polynomial function, not every function is a polynomial function.

We can extend this definition to the case where the domain is more complicated. First we will define the multi-variate function $\pi_{\mathbf{n}}$. Define $\pi_{\mathbf{n}} = \pi_{(n_1,n_2,\ldots,n_r)} : \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r} \to \mathbb{Z}^r$ to be $\pi_{\mathbf{n}}(\mathbf{x}) = \pi_{\mathbf{n}}(x_1 + n_1\mathbb{Z}, \ldots, x_r + n_r\mathbb{Z}) = (a_1, \ldots, a_r)$ for all $\mathbf{x} \in \mathbb{Z}^r$ and $a_i \in \{0, \ldots, n_i\}$ and $x_i \equiv a_i(mod\ n_i)$ for $i = 1, \ldots, r$.

Definition 1.3. A function $f : \mathbb{Z}^r \to \mathbb{Z}_m$ is a *polynomial function* if there exists a polynomial $F \in \mathbb{Z}[x_1, \ldots, x_r]$ such that $f(\mathbf{a}) = F(\mathbf{a}) + m\mathbb{Z}$ for all $\mathbf{a} \in \mathbb{Z}^r$.

Definition 1.4. Finally, we would like to define a function $f : \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r} \to \mathbb{Z}_m$ to be a *polynomial function* if there exists a polynomial function $f' : \mathbb{Z}^r \to \mathbb{Z}_m$ such that $f = f' \circ \pi_{\mathbf{n}}$.

There are several different versions of the definition of polynomial functions in papers by, for example, Chen [4, 5], Singmaster [14], and Bhargava [1]. We will now provide the definition given by Chen in [4] and prove the equivalence of notions.

Please note that we have altered the definition some to be precisely correct, though the meaning has not changed.

Definition 1.5. A function $f : \mathbb{Z}_n \to \mathbb{Z}_m$ is said to be a polynomial function, if it is representable by a polynomial $F \in \mathbb{Z}[x]$, i.e.,

$$f(a + n\mathbb{Z}) = F(a) + m\mathbb{Z} \text{ for all } a \in \{0, 1, \ldots, n-1\}.$$

Theorem 1.6. *The definition of a polynomial function by Chen is equivalent to the definition given here.*

Proof. Let $f : \mathbb{Z}_n \to \mathbb{Z}_m$, and let $F \in \mathbb{Z}[x]$ such that

$$f(a+n\mathbb{Z}) = F(a) + m\mathbb{Z} \text{ for all } a \in \{0, 1, \ldots, n-1\}.$$

Then let $f' : \mathbb{Z} \to \mathbb{Z}_m$ where $f'(a) = F(a) + m\mathbb{Z}$ for all $a \in \mathbb{Z}$. So for all $b \in \mathbb{Z}$ we have:

$$\begin{aligned} f' \circ \pi_n(b+n\mathbb{Z}) &= f' \circ \pi_n(a+n\mathbb{Z}) && \text{where } b \equiv a(mod\ n) \text{ and} \\ & && a \in \{0, 1, \ldots, n-1\} \\ &= f'(a) && \text{by definition of } \pi_n \\ &= F(a) + m\mathbb{Z} && \text{by definition of } f' \\ &= f(a+n\mathbb{Z}) && \text{by our assumption about } f \\ &= f(b+n\mathbb{Z}) && \text{since } a+n\mathbb{Z} = b+n\mathbb{Z} \end{aligned}$$

Hence $f = f' \circ \pi_n$.

Conversely, let $f : \mathbb{Z}_n \to \mathbb{Z}_m$, and let $F \in \mathbb{Z}[x]$ and $f' : \mathbb{Z} \to \mathbb{Z}_m$ such that $f'(b) = F(b) + m\mathbb{Z}$ for all $b \in \mathbb{Z}$ and such that $f = f' \circ \pi_n$. Then $f(a+n\mathbb{Z}) = f' \circ \pi(a+n\mathbb{Z}) = f'(a) = F(a) + m\mathbb{Z}$ for all $a \in \{0, 1, \ldots, n-1\}$. □

In [5], Chen has a corresponding multi-variate definition of polynomial functions. In order to prove the equivalence between our definitions, one must make minor changes to the proof above.

We will deliver now one final definition before continuing to the next section. This definition associates a set of polynomials to a polynomial function.

Definition 1.7. Let $F \in \mathbb{Z}[x_1, \ldots, x_r]$, $f : \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r} \to \mathbb{Z}_m$, and $f' : \mathbb{Z}^r \to \mathbb{Z}_m$ such that f and f' are polynomial functions with $f = f' \circ \pi_{\mathbf{n}}$ where

$n = (n_1, \dots, n_r)$ and $f'(\mathbf{a}) = F(\mathbf{a}) + m\mathbb{Z}$ for all $\mathbf{a} \in \mathbb{Z}^r$. Then f is called *the polynomial function associated to F* (from $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$ to $\mathbb{Z}_m$). Likewise, F is called *a polynomial associated to f*.

Example 1.8. Let $F = x$. Then the polynomial function associated to F from $\mathbb{Z}_2$ to $\mathbb{Z}_3$ is defined by $f(0+2\mathbb{Z}) = F(0)+3\mathbb{Z} = 0+3\mathbb{Z}$, and $f(1+2\mathbb{Z}) = F(1)+3\mathbb{Z} = 1+3\mathbb{Z}$. Alternatively, if we define $f : \mathbb{Z}_2 \to \mathbb{Z}_3$ by $f(0) = 0$ and $f(1) = 1$, then f is a polynomial function where $F(x) = x$ is one of its associated polynomials. Notice that $G(x) = x^2$ is also one of its associated polynomials.

1.2. **Congruent v. Equivalent Polynomials.** The reader may come upon some trouble in the subsequent sections if they fail to remark upon the differences between congruent polynomials and polynomials whose associated polynomial functions are equal.

Borevich and Shafarevich [2] gave a very concise explanation of the difference in question. We would be remiss if we paraphrased (aside from some minor index changes to retain consistency):

"We write $F(x_1, \dots, x_r) \equiv G(x_1, \dots, x_r)(modp)$ and call the polynomials F and G congruent, if the coefficient of corresponding terms on the right and left sides are congruent modulo p. If for any set of values $c_1, \dots, c_r$ we have $F(c_1, \dots, c_r) \equiv G(c_1, \dots, c_r)(modp)$ then we write $F \sim G$ and call F and G [functionally] equivalent. It is clear that if $F \equiv G$, then $F \sim G$, but...the converse is false."

The following is an example of the "converse is false" statement (i.e. we now present a counter-example).

Example 1.9. Let $F = x(x+1)$, and let us consider $\mathbb{Z}_2$. Well, it is clear that $F = x^2 + x \not\equiv 0$ $(mod\ 2)$, but we claim that $F \sim 0$. Since F is equal to a number times one plus that number, $F(a)$ is even for all $a \in \mathbb{Z}$. That is, $F(a) \equiv 0$ $(mod\ 2)$ for all $a \in \mathbb{Z}$. Hence $F \sim 0$, but $F \not\equiv 0$.

Notice that "$\sim$" in the above quote actually is an equivalence relation among polynomials. Let us prove this explicitly.

Definition 1.10. Let $R[x_1, \ldots, x_r]$ be a polynomial ring in n variables. Then we define $(R[x_1, \ldots, x_r], \sim, m, n)$ to be the following relation: Let $F, G \in R[x_1, \ldots, x_n]$ and let $f, g : \mathbb{Z}_n \to \mathbb{Z}_m$ be polynomial functions associated to F and G respectively. Then

$$F \sim G \iff f = g.$$

Theorem 1.11. *The relation $(R[x_1, \ldots, x_r], \sim, m, n)$ is an equivalence relation.*

Proof. In this proof we will use the notation $S = R[x_1, \ldots, x_r]$ to save space.

Reflexivity: Let $F \in S$. Then there exists a polynomial function $f : \mathbb{Z}_n \to \mathbb{Z}_m$ associated to F. Now $f = f \implies F \sim F$. So $F \sim F$ for all $F \in S$.

Symmetry: Let $F, G \in S$. Let $f, g : \mathbb{Z}_n \to \mathbb{Z}_m$ be two polynomial functions associated to F and G respectively. Then $F \sim G \implies f = g \implies g = f \implies G \sim F$.

Transitivity: Let $F, G, H \in S$. Let $f, g, h : \mathbb{Z}_n \to \mathbb{Z}_m$ be their respective polynomial functions. Then $F \sim G$ and $G \sim H \implies f = g$ and $g = h \implies f = h \implies F \sim H$.

□

2. THE DELTA ALGORITHM

2.1. **Introduction.** In this section, we will describe an algorithm for checking if a single-variate polynomial function vanishes. The algorithm works by calculating the coefficients of the polynomial over a convenient basis, that is, the basis of falling factorials ([12], pgs. 85-87). This method is motivated by comments Singmaster made at the end of his paper [14] and by the work of Chen [4]. First, we will describe Newton's interpolation polynomial and explain its utility in our program. We will then discuss the work of Chen, which is used in the proofs. We will then present the main result, which is a characterization of vanishing polynomials that uses the aforementioned interpolation. We will end with an algorithm, based on this result, that will test whether a polynomial vanishes.

It should be noted here that the work on the Delta Algorithm was developed during an intensive time of discussion and intellectual exchanges between the author and his advisor and the several members of the Electrical and Computer Engineering department at the University of Utah, including Dr. Priyank Kalla and his graduate student assistants Namrata Shekhar and Sivaram Gopalakrishnan.

We refer to the positive integers m and n throughout this section. They are only used in the context of describing a polynomial function $f : \mathbb{Z}_n \to \mathbb{Z}_m$.

A polynomial $F \in \mathbb{Z}[x]$ is said to *vanish from* $\mathbb{Z}_n$ *to* $\mathbb{Z}_m$ (or simply to *vanish*) when its associated polynomial function $f : \mathbb{Z}_n \to \mathbb{Z}_m$ is the zero function.

2.2. **Newton's Interpolation Polynomial.** Given a polynomial $F \in \mathbb{Z}[x]$ and its associated polynomial function $f : \mathbb{Z}_n \to \mathbb{Z}_m$ we would like to reinterpret F in a way that would be more fitting for our purposes. Newton gave us this reinterpretation in the form of a polynomial equivalent to our own (found in many numerical methods books and mentioned in the last page of [14]). In order to understand the formula for the interpolation we will first need to discuss the forward difference.

2.3. **Forward Difference.** The forward difference is a discrete analog to the derivative and is defined here by $(\Delta F)(x) = F(x+1) - F(x)$. By iterating this operation we can derive higher orders of Δ. For instance $(\Delta^2 F)(x) = (\Delta F)(x+1) - (\Delta F)(x)$. One immediately wonders about the general form of the k^{th} order of the forward difference. So we present here a well-known formula with proof:

Proposition 2.1. *The k^{th} iteration of the forward difference can be expressed as*

$$(\Delta^k F)(x) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} F(k-i+x). \tag{2.1.1}$$

Proof. This proof is by induction over k:

1. This works trivially for the zeroth order of the forward difference, i.e. $F^0(x) = F(x)$.
2. Induction hypothesis: Assume the formula is true for all orders less than or equal to k.
3. Prove true for $k+1$:

$$(\Delta^{k+1} F)(x) = \Delta^k (\Delta F)(x) = \Delta^k (F(x+1) - F(x))$$

$$=\sum_{i=0}^{k}(-1)^i\binom{k}{i}(F(k-i+x+1)-F(k-i+x))$$

$$=\sum_{i=0}^{k}(-1)^i\binom{k}{i}F(k-i+x+1)-\sum_{i=0}^{k}(-1)^i\binom{k}{i}F(k-i+x)$$

$$=\sum_{i=0}^{k}(-1)^i\binom{k}{i}F(k-i+x+1)-\sum_{i=1}^{k}(-1)^{i-1}\binom{k}{i-1}F(k-i+x+1)$$

$$=\sum_{i=0}^{k}(-1)^i\binom{k}{i}F(k-i+x+1)+\sum_{i=1}^{k}(-1)^{i}\binom{k}{i-1}F(k-i+x+1)$$

$$=F(k+x+1)+\sum_{i=1}^{k}(-1)^i(\binom{k}{i}+\binom{k}{i-1})F(k-i+x+1)$$

$$=\sum_{i=0}^{k+1}(-1)^i\binom{k+1}{i}F(k-i+x+1) \text{ since } \binom{a}{b}+\binom{a}{b+1}=\binom{a+1}{b+1}.$$

Therefore we have our result.

□

Now, we can state the form of Newton's interpolation polynomial.

Proposition 2.2. *Newton's Interpolation Formula: If $F \in \mathbb{Z}[x]$ and d is the degree of F then F can be expressed as*

$$F(x)=\sum_{k=0}^{d}(\Delta^k F)(0)\binom{x}{k} \text{ where } \binom{x}{k}=\frac{x(x-1)\cdots(x-k+1)}{k!}.$$

This proof can be found in [8]. Note that it is well-known that $k!$ divides $x(x-1)\cdots(x-k+1)$ when x is an integer.

2.4. **A Unique Polynomial Representation.** This is as good a time as any to bring up the work of Zhibo Chen [4] in his article "On polynomial functions from $\mathbb{Z}_n$ to $\mathbb{Z}_m$." It is in this paper that Chen discusses how to use the falling factorial $(x)_k$ to find convenient ways to transition between polynomials and polynomial functions. He also delivers a canonical representation for univariate polynomial functions from $\mathbb{Z}_n$ to $\mathbb{Z}_m$ where $n,m \in \mathbb{N}$, but it is the lemmata leading up to this representation that will be useful to us. Before getting to these lemmas, we need a little bit of notation, which Chen also provides in his paper. The following function $\lambda(m)$ has been used in many works over a long period of time. Indeed, Kempner used this function in his paper [10] from 1921.

$\lambda(m) =$ the least positive integer λ such that $m|\lambda!$.

$\mu(n,m) = min\{n, \lambda(m)\}$.

And when there is no confusion, we will write these as λ and μ respectively.

Furthermore, there is a basis for $\mathbb{Z}[x]$, the elements of which are falling factorials, denoted by $(x)_k$, where $(x)_0 = 1$ and

$$(x)_k = x(x-1)\cdots(x-k+1) \text{ for all } k = 1,2,\ldots.$$

It should be noted that the binomial term in Newton's Interpolation Formula can be expressed using our chosen basis; that is:

$$\binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!} = \frac{(x)_k}{k!}.$$

In this case the interpolation formula would look like this:

$$F(x) = \sum_{k=0}^{d} \frac{(\Delta^k F)(0)}{k!}(x)_k. \tag{2.2.1}$$

Assertion (5) in Hungerbuehler-Specker [9] implies that if F has integer coefficients, then $\frac{(\Delta^k F)(0)}{k!}$ is an integer for $0 \leq k \leq deg(F)$.

One last bit of notation: The set of polynomials in $\mathbb{Z}[x]$ that have the same associated polynomial function is in fact an equivalence class, and we say that two polynomials in this set are equivalent and denote the equivalence with the symbol "$\sim$".

Chen's main theorem is as follows:

Theorem 2.3. *Let f be a polynomial function from $\mathbb{Z}_n$ to $\mathbb{Z}_m$. Then f can be uniquely represented by a polynomial*

$$F = \sum_{k=0}^{\mu-1} c_k (x)_k \text{ with } 0 \leq c_k < \frac{m}{(m,k!)}.$$

This is a very nice theorem that gives us that if we have a polynomial F in the above form, then it has an associated polynomial function that no other polynomial of the same form has. This theorem is quite nice and it is a reformulation of this that gives us our main result and, indeed, the Delta Algorithm. This last theorem was also the motivation for the following lemmata, which will prove to be very useful.

In [4], Chen provides the following lemmas which we will use in our main result:

Let $b_k \in \mathbb{Z}$ for all $k = 0, 1, 2, \ldots$

Lemma 2.4. *$k!$ divides $(x)_k$ for all integers x and $k \geq 0$.*

Lemma 2.5. *If $k \geq \mu$ then $(x)_k \sim 0$.*

Lemma 2.6. *$\sum_{k=0}^{\mu-1} b_k (x)_k \sim 0$ if and only if $b_k (x)_k \sim 0$ $\forall$ $k = 0, 1, \ldots, \mu - 1$.*

Lemma 2.7. *Let $0 \leq k \leq n-1$. Then $b_k (x)_k \sim 0$ if and only if $(\frac{m}{(m,k!)}) | b_k$.*

2.5. **Main Result.** Let $F \in \mathbb{Z}[x]$. Since $(x)_k$ is a monic polynomial for all $k \in \mathbb{N}$, we can apply the Division-Remainder Theorem to give us:

$$F(x) = Q(x)(x)_\mu + R(x)$$

where $m \in \mathbb{N}$, $deg(R) \leq \mu - 1$, and $Q, R \in \mathbb{Z}[x]$ are unique.

As Chen points out in Lemma 2.5, $(x)_\mu$ vanishes mod m (i.e. $(x)_\mu \sim 0$, which indeed provides the motivation behind our use of this basis). We are now only left with the remainder $R(x)$ to worry about. All this combined leads us to the following lemma:

Lemma 2.8. *Let $F \in \mathbb{Z}[x]$, then F can be expressed as*

$$F(x) = Q(x)(x)_\mu + \sum_{k=0}^{deg(R)} \frac{(\Delta^k R)(0)}{k!}(x)_k$$

where $deg(R) \leq \mu - 1$ and $R(x), Q(x) \in \mathbb{Z}[x]$ are uniquely determined.

Proof. As stated above

$$F(x) = Q(x)(x)_\lambda + R(x), R \in \mathbb{Z}[x]$$

and $deg(R) < \lambda$. Using Newton's interpolation formula on the remainder $R(x)$ we get:

$$R(x) = \sum_{k=0}^{deg(R)} \frac{(\Delta^k R)(0)}{k!}(x)_k$$

□

We can now state our main result:

Theorem 2.9. *Let $F \in \mathbb{Z}[x]$. Then its associated polynomial function $f : \mathbb{Z}_n \to \mathbb{Z}_m$ is the zero function if and only if for all $0 \leq k \leq \mu - 1$*

$$b_k = \frac{(\Delta^k R)(0)}{k!} = \frac{1}{k!}\sum_{i=0}^{k}(-1)^i \binom{k}{i} R(k-i) \equiv 0 \mod \frac{m}{(k!, m)}.$$

Proof. The fact that $\frac{(\Delta^k R)(0)}{k!} = \frac{1}{k!}\sum\limits_{i=0}^{k}(-1)^i\binom{k}{i}R(k-i)$ is a direct consequence of Proposition (2.1). The rest of the proof is carried out in the following way:

$\Longleftarrow$: If for all $0 \leq k \leq \mu - 1$

$$\frac{1}{k!}\sum_{i=0}^{k}(-1)^i\binom{k}{i}R(k-i) \equiv 0 \mod \frac{m}{(k!,m)}.$$

Then by Proposition 2.1

$$\frac{(\Delta^k R)(0)}{k!} \equiv 0 \mod \frac{m}{(k!,m)} \text{ for all } 0 \leq k \leq \mu - 1.$$

But now, by Lemma 2.8 we have that

$$F(x) = Q(x)(x)_\lambda + \sum_{k=0}^{deg(R)} \frac{(\Delta^k R)(0)}{k!}(x)_k.$$

Since by Lemma 2.5 $(x)_\mu \equiv 0 \mod m$ we have then that

$$F(x) \equiv 0 \mod m \text{ for all } x \in \mathbb{Z}.$$

Hence F vanishes, and thus its associated polynomial function $f : \mathbb{Z}_n \to \mathbb{Z}_m$ is the zero function.

$\Longrightarrow$:Lemma 2.8 gives that there exist a unique Q and a unique R in $\mathbb{Z}[x]$ with $deg(R) < \mu$ such that

$$F(x) = Q(x)(x)_\mu + \sum_{k=0}^{deg(R)} \frac{(\Delta^k R)(0)}{k!}(x)_k.$$

Let the associated polynomial function $f : \mathbb{Z}_n \to \mathbb{Z}_m$ be the zero function. (By definition this means that there exists a polynomial function $f' : \mathbb{Z} \to \mathbb{Z}_m$ such that $f = f' \circ \pi_n$ and $f'(a) = F(a) + m\mathbb{Z}$ for all $a \in \mathbb{Z}$ (Recall that $\pi_n : \mathbb{Z}_n \to \mathbb{Z}$ is defined as $\pi_n(x + n\mathbb{Z}) = a$ for all $x \in \mathbb{Z}$ and where $a \in \{0, 1, \ldots, n-1\}$ and $a \equiv x(mod\ n)$). Now, $f' \circ \pi_n$ is also the zero function, which implies that $f'(a) = 0 = F(a) + m\mathbb{Z}$ for all $a \in \{0,1,\dots,n-1\}$.) This implies that

$$F \sim 0.$$

Now since $(x)_\mu \sim 0$ we get that

$$F \sim R \sim 0.$$

Now this implies that $R(x) = \sum_{k=0}^{\mu-1} b_k(x)_k \sim 0$. And by Lemma 2.6 we get that $b_k(x)_k \sim 0$ for all $k = 0,1,\dots,\mu-1$. Then by Lemma 2.7 we have that $\frac{m}{(m,k!)} | b_k$ for all $k = 0,1,\dots,\mu-1$. This implies that $b_k \equiv 0 \mod \frac{m}{(m,k!)}$ for all $k = 0,1,\dots,\mu-1$. □

This theorem lends itself nicely to the creation of an algorithm for testing whether a polynomial vanishes. This algorithm is culled from the various sources that have already been cited including especially Chen [4] and Singmaster [14], and it has been used in an article co-written by the author [13].

Algorithm 1. *The Delta Algorithm*

1. *Compute* $\mu = \min\{n, \lambda(m)\}$.
2. *Divide the polynomial by* $(x)_\mu$. *If the remainder* $R(x)$ *is congruent to 0 mod m, the polynomial vanishes.*
3. *Otherwise, in the basis of falling factorials, compute the coefficients for the remainder using the following formula:* $b_k = \frac{1}{k!} \sum_{i=0}^{k} (-1)^i \binom{k}{i} R(k-i) \mod \frac{m}{(k!,m)}$ *where* $k = 0,1,\dots,\mu-1$.
4. *The polynomial vanishes if and only if all of the* b_k *are congruent to 0.*

One last comment before moving on. This algorithm tells us that in some special cases (specifically the cases that most readily apply to electrical circuits) we must check only a vast minority of the integers less than m to decide whether a polynomial vanishes. In the case where m is a power of a prime, say p^i, we have that $\lambda(p^i)$ is quite small relative to p^i. In fact $\lambda(p^i) \leq ip$ provides a useful upper bound for λ. Based on some numerical evidence, though, as the power increases this upper bound becomes very rough. That is, as i gets larger, the difference between $\lambda(p^i)$ and ip increases.

2.6. **The Multivariate Delta Algorithm.** In this section we present a sketch of the multivariate case of the Delta algorithm from the last section. We use in the section the multivariate notation used by Hungerbuehler and Specker ([9], pgs. 2, 3) and by Chen ([5], pg. 72).

For $\mathbf{k} = (k_1, \ldots, k_d) \in \mathbb{N}^d$ and $\mathbf{x} := (x_1, \ldots, x_d)$, let

$$\mathbf{x}^{\mathbf{k}} := \prod_{i=1}^{d} x_i^{k_i}$$

and

$$\mathbf{k}! := \prod_{i=1}^{d} k_i!.$$

Furthermore, we write

$$|\mathbf{k}| := \sum_{i=1}^{d} k_i$$

and

$$\binom{\mathbf{x}}{\mathbf{k}} := \prod_{i=1}^{d} \binom{x_i}{k_i}.$$

Let $\mathbf{e}_i := (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{Z}_n^d$, with the 1 at place i. Then, we define the (forward) partial difference operator Δ by

$$\Delta_i g(\mathbf{x}) := g(\mathbf{x} + \mathbf{e}_i) - g(\mathbf{x})$$

$$\Delta_i^0 := \text{ identity}$$

$$\Delta_i^k := \Delta_i \circ \Delta_i^{k-1}.$$

For a multi-index **k**, let

$$\Delta^{\mathbf{k}} := \Delta_1^{k_1} \circ \cdots \circ \Delta_d^{k_d}.$$

Notice that the Δ operators commute and that $\Delta^{\mathbf{k}_1} \circ \Delta^{\mathbf{k}_2} = \Delta^{\mathbf{k}_1 + \mathbf{k}_2}$.

2.6.1. *Newton's Interpolation Formula for Several Variables.* According to assertion (3) of Hungerbuehler and Specker in [9], a polynomial $F(\mathbf{x})$ equals its "discrete Taylor expansion" or, as we will call it here, its Newton's Interpolation Polynomial:

$$F(\mathbf{x}) = \sum_{|\mathbf{k}| \leq degF} (\Delta^{\mathbf{k}} F)(\mathbf{0}) \binom{\mathbf{x}}{\mathbf{k}}$$

$$= \sum_{|\mathbf{k}| \leq degF} \frac{(\Delta^{\mathbf{k}} F)(\mathbf{0})}{k_1! \ldots k_d!} \prod_{i=1}^{d} (x_i)_{k_i}$$

$$= \sum_{|\mathbf{k}| \leq degF} \frac{(\Delta^{\mathbf{k}} F)(\mathbf{0})}{\mathbf{k}!} (\mathbf{x})_{\mathbf{k}}$$

A proof of this can be found in [8].

If we set $b_{\mathbf{k}}$ equal to the coefficients $\frac{(\Delta^{\mathbf{k}} F)(\mathbf{0})}{\mathbf{k}!}$ in the above summation, we can determine, based solely on these $b_{\mathbf{k}}$, if F vanishes. The following algorithm details how to do this. The formulation of this algorithm represents an extension of the Delta algorithm presented earlier for the univariate case and is a consequence of the work of Hungerbuehler-Specker and Chen [9, 5].

Algorithm 2. *The Multivariate Delta Algorithm*

1. *Choose only the* $\mathbf{k} = (k_1, \ldots, k_d)$ *where* $k_i < \lambda(n)$. *(The fact that these* $\mathbf{k}$*'s are sufficient is given by Lemma 6 of* [5].
2. *Compute* $b_{\mathbf{k}}$ *for each* $\mathbf{k}$ *chosen in the last step.*
3. *Check whether* $b_{\mathbf{k}} \equiv 0 \mod \frac{m}{(m,\mathbf{k}!)}$ *for all* $b_{\mathbf{k}}$ *from the first step. If one of these* $b_{\mathbf{k}}$ *is not congruent to zero, then the function F fails to vanish. (Given by Lemma 5 of* [5].*)*

2.6.2. *Computing* $b_{\mathbf{k}}$. By assertion (2) of [9] we have that

$$(\Delta^{\mathbf{k}}F)(\mathbf{0}) = \sum_{\mathbf{r}\leq\mathbf{k}} F(\mathbf{k}-\mathbf{r})(-1)^{|\mathbf{r}|}\binom{\mathbf{k}}{\mathbf{r}}$$

And so

$$b_{\mathbf{k}} = \frac{(\Delta^{\mathbf{k}}F)(\mathbf{0})}{\mathbf{k}!} = \frac{\sum_{\mathbf{r}\leq\mathbf{k}} F(\mathbf{k}-\mathbf{r})(-1)^{|\mathbf{r}|}\binom{\mathbf{k}}{\mathbf{r}}}{\mathbf{k}!}.$$

3. Simplification

In this section, we tackle the problem of whether one can decrease the number of variables of a polynomial by applying linear substitutions.

It turns out that this question has been answered completely in the case of fields of characteristic zero by Enrico Carlini in his chapter entitled *Reducing the number of variables of a polynomial* in [3]. Carlini claims also that his methods work over fields of positive characteristic, but little justification is given for this.

Due to the lack of previous work on this subject, the following two sections are an original attempt by the author to solve this problem over the ring $\mathbb{Z}_q$ where q is a power of a prime, which is not a field (unless q is prime) but rather a local commutative ring with zero divisors. These special circumstances provide challenges as well as unique opportunities.

Now, this idea of *decreasing* the number of variables in a polynomial hearkens back to the theme of this thesis, which is the *simplification* of polynomials. With this in mind we create a natural definition: that of a “simplifiable” polynomial.

If a polynomial expression has exactly n variables, then the polynomial is simplifiable if, by a linear change of variable, the polynomial may be expressed with fewer variables.

We will now make this definition more precise in the case where $n = 2$, i.e. when f is a bivariate polynomial. We will extend my results to the multi-variate case later on.

Definition 3.1. Let f be a bivariate polynomial, then f is *simplifiable* (or simp) if there exists a linear bivariate polynomial u and a univariate polynomial g such that

$$f = g(u) = g \circ u.$$

Furthermore, when u is known, f is called *u-simplifiable* (or u-simp). Also u will sometimes be called a *simplifying element for f*.

In the definition above you can see that we are *simplifying* the two-variable polynomial f to a one-variable polynomial g.

Example 3.2. Let $f = 4 + 4x + x^2 + 4xy + 4y^2$ in $\mathbb{Z}_8$. Then if we set $u = 2 + x + 2y$ we get

$$f = u^2 = (2 + x + 2y)^2 = 4 + 4x + x^2 + 4xy + 4y^2.$$

And hence f is u-simplifiable.

Often it is preferable to work exclusively with polynomials that do not have constant terms. That is, it can be much nicer to work with the polynomial $f = a_nx^n + \cdots + a_1x$ rather than $g = b_nx^n + \cdots + b_1x + b_0$. With this in mind, note the following:

Proposition 3.3. *If f is simplifiable, then f is u-simp where u is a linear form, i.e. $u = ax + by$ with $a, b \in R$.*

Proof. Let f be simplifiable. Then there exists

$$h = b_0 + b_1x + b_2y \text{ where } b_0, b_1, b_2 \in R$$

such that

$$f = g \circ h \text{ for some } g \in R[x]$$

that is

$$f = a_0 + a_1h + \cdots + x_nh^n \text{ where } a_0, \ldots, a_n \in R.$$

Let $u = b_1x + b_2y$. Then $h = b_0 + u$. This implies

$$f = a_0 + a_1(b_0 + u) + \cdots + a_n(b_0 + u)^n.$$

If we define the polynomial $i \in R[x]$ as

$$i = a_0 + a_1(b_0 + x) + \cdots + a_n(b_0 + x)^n$$

we clearly have that

$$f = i \circ u.$$

And hence f is u-simp. □

Given the above property, we will from this point on choose the simplifying element u to be a linear form.

As a point of notation, when we refer to an "n-variable polynomial" or something similar, we am referring to a polynomial that has at least n distinct variables in one or more monomials that do not have zero coefficients. For example, a bivariate polynomial would have exactly two visible variables such as $x+3xy$ but not $7x+0y$.

Next, we would like to present one of the featured characters of this work, the reduced linear form. Before this we point out that when we refer to the "linear part" of a polynomial f, we are referring to the sum of degree one terms in f, and we do consider the zero polynomial to be the linear part of a polynomial with no degree one terms.

Definition 3.4. Let f be a bivariate polynomial. Then a *reduced linear form* (or RLF) of f is a monic linear form that divides the linear part of f.

In particular, if $f = a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + \cdots + a_{mn}x^m y^n$ where $a_{ij} \in R$, and if $b_1, b_2 \in R$ and $u = b_1x + b_2y$ is an RLF of f, then $b_1 \neq 1 \implies b_2 = 1$, and $u | a_{10}x + a_{01}y$.

Notation: we will use the notation $lp(f)$ to stand for the linear part of f. In other words, if f is as in the above definition, then $lp(f) = a_{10}x + a_{01}y$.

Furthermore, for the rest of this section, we will refer to the the rings in which we will be working as $R = \mathbb{Z}_{p^\alpha}$ where p is a prime number and $\alpha \in \mathbb{N}$. The electrical engineering application for this work requires us only to work over the rings $\mathbb{Z}_{2^\alpha}$, but the results extend so readily to where p is any prime number, that we have written this work in that more general case.

Example 3.5. Let $f = 3 + 2x + 3y + 2x^2$ in $\mathbb{Z}_4[x]$. The linear part of f is $lp(f) = 2x + 3y$. Now $2x + y$ is monic and divides $2x + 3y$, since $3(2x + y) = 6x + 3y \equiv 2x + 3y \mod 4$. Hence $2x + y$ is an RLF of f.

Example 3.6. Let $f = 2x + 4y^2 + 3xy$ in $\mathbb{Z}_4[x]$. Then $lp(f) = 2x$. Now notice that both x and $x + 2y$ are RLFs of f.

Now, two important questions arise:

1) Can we determine when f is simplifiable?

2) Can we determine the simplifying element for f?

We will present an algorithm that answers both of these questions. The notion of an RLF becomes important in the algorithm, and the following propositions explains why:

Proposition 3.7. *The polynomial $f \in R[x,y]$ is simplifiable if and only if there is an RLF of f that is a simplifying element for f.*

Proof. Let $R = \mathbb{Z}_{p^\alpha}$ where p is prime and α is an integer greater than 0. Let $f = a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + \cdots + a_{mn}x^m y^n$ where $a_{ij} \in R$ be simplifiable. Then by Proposition 3.3 there exists a linear form u such that f is u-simp, i.e. $f = b_0 + b_1 u + \cdots + b_r u^r$. Let $u = ax + by$ where $a, b \in R$. Then if we set $d = (a,b)$, the greatest common divisor of a and b (this exists because R is a principal ideal ring), we get

$$\frac{u}{d} = \frac{a}{d}x + \frac{b}{d}y.$$

Since $\frac{a}{d}, \frac{b}{d}$, or both must not be divisible by p, by symmetry we may assume without loss of generality that $e := \frac{a}{d}$ is not divisible by p (and hence invertible in R). Then define the monic linear form

$$v := e^{-1}\frac{u}{d} = x + e^{-1}\frac{b}{d}y.$$

Now since $edv = u$ we get that $f = b_0 + b_1 edv + \cdots + b_r(edv)^r$, which implies that f is v-simp. Furthermore, since $lp(f) = b_1 edv$, we have that v

divides the linear part of f. Hence v is an RLF of f and v is a simplifying element for f. □

This proposition leads us to an algorithm that can determine if a polynomial is simplifiable and what the simplifying element is. Basically, the above proposition has narrowed our search for a simplifying element to the set of reduced linear forms of a polynomial. If we check each of these RLFs and none simplify the polynomial, then the polynomial is not simplifiable. Alternatively, if an RLF does simplify the polynomial, then obviously the polynomial is simplifiable. So now we need a method for testing whether a given linear form simplifies a polynomial.

Let $f \in R[x,y]$ be a u-simplifiable polynomial. Then we can express f as $f = a_0 + a_1 u + \cdots + a_n u^n$. Now, there is an alternative way to express a single-variable polynomial that will be useful to us. We can express f as:

$$f = a_0 + (a_1 + (a_2 + \cdots + (a_{n-1} + a_n u)u)\cdots)u.$$

Notice that this gives us that if f is u-simp, then $f - a_0$ is divisible by u. We also have that $\frac{f-a_0}{u} - a_1$ is also divisible by u. We can carry on like this until the powers of u have been used up. That is f is u-simp if and only if

$$\frac{\frac{\frac{\frac{f-a_0}{u}-a_1}{u}-a_2}{\cdots}}{u} - a_{n-1} \text{ makes sense and is divisible by } u.$$

This is summed up in the following proposition (for this specific proposition, R may be any commutative ring):

Proposition 3.8. *Let $f \in R[x,y]$ and let u be a linear form. Then f is u-simp if and only if there exists $a \in R$ such that $u|f - a$ and $\frac{f-a}{u}$ is u-simp.*

These last two proposition gives us an iterative process for testing which (if any) linear form is a simplifying element for a polynomial.

We now state the algorithm. Remember here that $R = \mathbb{Z}_{p^\alpha}$ where p is a prime number and $\alpha \in \mathbb{N}$.

Algorithm 3. *Let $f \in R[x_1, x_2]$ of degree $n \geq 1$, and let S be the set of RLFs of f. Then:*

```
1. If $S = \emptyset$
       Return "$f$ is not simplifiable."
2. Let $u \in S$ where $u$ is monic for the variable $x_i$.
3. Let $j = 0$.
4. If $j = n$
       Return "$f$ is simplifiable".
5. Divide $f$ by $u$ to get $f = q_{j+1}u + q_j$ where $q_j \in R[x_k]$ and $k \neq i$.
6. If $q_j$ is a constant then
       Let $j = j + 1$.
       Let $f = \frac{f - q_j}{u} = q_{j+1}$.
       Go to line 4.
7. Else
       Let $S = S - \{u\}$.
       Go to line 1.
```

This algorithm gives us all of the information for which we have been looking. Namely:

Proposition 3.9. *Algorithm 1 will output whether f is simplifiable, and if f is simplifiable, it will output a simplifying element u of f as well as the coefficients $q_0, \ldots, q_n$ such that $f = q_0 + q_1 u + \cdots q_n u^n$.*

Proof. That the desired information will be found via this algorithm is given by Propositions 3.7 and 3.8. It remains to show that this algorithm ends. Since there are only ever a finite number of RLFs of a polynomial, we may assume there are $m \in \mathbb{N}$ such elements. So in a worst case scenario, the algorithm will check all m RLFs, and for each RLF the algorithm will move on after a maximum of n divisions (where $n = deg(f)$). So this algorithm will end after a maximum of $m \cdot n$ divisions. □

4. Multivariate Simplification

In this section, we generalize to the multivariate case the results of the previous section. First, we will generalize the definitions, then we will build carefully the elements needed to generalize the main theorem.

Let R be a commutative ring.

Definition 4.1. Let $f \in R[x_1, \ldots, x_n]$. A *reduced linear form* (RLF) of f is a monic linear form in $R[x_1, \ldots, x_n]$ that divides the linear part of f.

Recall from Section 3 that when we refer to an n-variable polynomial, we mean that exactly n variables appear in nonzero monomials of the polynomial.

Definition 4.2. Let f is an n-variable polynomial. Then f is *simplifiable* if there exist an m-variable polynomial g where $m < n$ and a set of linear polynomials $U = \{u_1, \ldots, u_m\}$ such that

$$f = g(u_1, \ldots, u_m).$$

Furthermore when U is known, f is called U*-simplifiable* (or U-simp). Also, U will sometimes be referred to as the *simplifying set for* f.

Notation: when we refer to an n-variable set of polynomials F, we mean that there are exactly n different variables such that each appears in at least one nonzero monomial of an element of F. That is, n is the number of all "visible" variables in the entire set of polynomials, regardless of the (potentially larger) polynomial ring in which the set lies.

Definition 4.3. Let $F = \{f_1, \dots, f_r\}$ be an n-variable set of polynomials. Then F is a *simplifiable set* if there exists a set $U = \{u_1, \dots, u_m\}$ of linear polynomials with $m < n$ such that $F \subseteq R[U]$. When it is clear, we may say simply that F is *simplifiable* (simp) or *U-simplifiable* (U-simp). Also, U may be referred to as the *simplifying set for F*.

The following theorem tells us, similar to Proposition 3.3, that we can always assume that our simplifying set is made up of linear forms, that is, linear polynomials without constant terms.

Theorem 4.4. *A finite polynomial set F is simplifiable if and only if F is U-simp for some set of linear forms U.*

Proof. $\Longleftarrow$: If F is U-simp then it obviously simplifiable.

$\Longrightarrow$: Let F be an n-variable polynomial set. If F is simplifiable, then there exists a set $H = \{h_1, \dots, h_m\}$ of linear polynomials such that $m < n$ and F is H-simplifiable. Let a_i be the constant term for h_i for all $i \in \{1, \dots, m\}$. Then set $u_i = h_i - a_i$ for all $i \in \{1, \dots, m\}$. Since F is H-simp, we have that

$$F \subseteq R[H] = R[h_1, \dots, h_m] = R[a_1 + u_1, \dots, a_m + u_m] \subseteq R[u_1, \dots, u_m].$$

Hence F is U-simp for the set $U = \{u_1, \dots, u_m\}$. □

NOTE: From here on, we will denote by R the ring of integers mod p^{α} where p prime and α a positive integer. That is,

$$R = \mathbb{Z}_{p^{\alpha}}.$$

Also, for the rest of this write-up, we will refer to the set of non-zero linear forms in $R[x_1,\ldots,x_n]$ as X. That is,

$$X = \{u \in R[x_1,\ldots,x_n] : u \neq 0 \text{ is a linear form}\}.$$

Definition 4.5. Let $U \subseteq X$ have m elements. Let $u \in U$. We say that x_i is a *distinct variable for u in U* if u is the only element of U that has a term with x_i, i.e. if $U - \{u\} \subseteq R[x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n]$. When it is unambiguous to do so, we will refer to x_i as a *distinct variable*.

First we start with a few properties of $R[U]$ where U is a set of nonzero linear forms.

In the following, the operator $|\cdot|$ is the operator that gives the number of elements in a set.

Proposition 4.6. *Let $U \subseteq X$ have m elements.*

(1) For each $u \in U$ there exists a $v \in R[x_1,\ldots,x_n]$ monic such that v divides u. We then have that $R[U] \subseteq R[(U-\{u\}) \cup \{v\}]$.

(2) Let U have an element u_i monic for x_j. Then there exists $U' \subseteq R[x_1,\ldots,x_n]$ such that $R[U] \subseteq R[U']$ where $|U'| \leq |U|$, $u_i \in U'$, and x_j is a distinct variable for u_i in U'.

(3) If $W \subseteq U$, then if there is a W' such that $R[W] \subseteq R[W']$, for $U' = (U-W) \cup W'$ we have $R[U] \subseteq R[U']$.

(4) $R[U] = R[U']$ where $U' = (U - \{u_i\}) \cup \{u_i'\}$ where $u_i' = a_1u_1 + a_2u_2 + \ldots + a_mu_m$, $a_1,a_2,\ldots,a_m \in R$, and a_i is invertible in R.

Proof. (1) Let $u \in R[x_1, \ldots, x_n]$ where $R = \mathbb{Z}_{p^n}$ be a linear form. One can factor out the greatest common divisor a of the coefficients of $u = a_1x_1 + \cdots + a_nx_n$ giving $u = a(b_1x_1 + \cdots + b_nx_n)$. Now, if one of the b_i is 1 we are done. Otherwise, if none of the b_i are 1, then one of the b_i is not divisible by p since if they all were divisible by p then that factor would have been part of the greatest common divisor. Say b_j is the coefficient not divisible by p, then in our ring it is invertible. So $u' = b_1x_1 + \cdots + b_nx_n = b_j({b_j}^{-1}b_1x_1 + \cdots + x_j + \cdots + {b_j}^{-1}b_nx_n)$. Setting $v = {b_j}^{-1}b_1x_1 + \cdots + x_j + \cdots + {b_j}^{-1}b_nx_n$, we now have $u = au' = ab_jv$ and hence v is a monic divisor of u.

If $f \in R[u_1, \ldots, u_i, \ldots, u_m]$ and if $u_i = av$, then $f(u_1, \ldots, u_i, \ldots, u_m) = f(u_1, \ldots, av, \ldots, u_m) \in R[u_1, \ldots, v, \ldots, u_m] = R[(U - \{u_i\}) \cup v]$.

(2) For all $k \neq i$ divide u_k by u_i in terms of x_j to get by the division-remainder theorem $u_k = q_ku_i + r_k$ where q_k is a constant and $r_k \in R[U]$ is a polynomial without a u_i term. Now it is clear that in this case $R[u_1, \ldots, u_i, \ldots, u_m] = R[q_1u_i + r_1, \ldots, u_i, \ldots, q_mu_i + r_m] \subseteq R[r_1, \ldots, u'_j, \ldots, r_m]$ for any ring R.

(3) Let S be the set of elements in U that are not in W. One can view $R[U]$ as $R[W][S]$. That is, as polynomials in S with coefficients in $R[W]$. Now $R[W] \subseteq R[W']$. So clearly $R[W][S] \subseteq R[W'][S] = R[W', S] = R[U']$ since all the polynomials in S with coefficients in $R[W]$ are also polynomials with coefficients in $R[W']$.

(4) Note that that the following only shows that $R[U] \subseteq R[U']$ the opposite inclusion comes from the fact that the replacement given in (5) can be reversed. Claims: $R[U] = R[U']$ where U' is the same as U except that one element of U, say u_i is replaced by:

i) by a_iu_i, where $a_i \in R$ is a unit.

This is easily seen after noticing $u_i = a_i^{-1}u_i'$.

ii) by $u_i + a_ju_j$ where $j \neq i$ and $a_j \in R$. Let $f \in R[U]$. Rearrange f to get $f = \sum_{k=0}^{d} f_k * (u_i + a_ju_j)^k$ where $d = deg_{u_i}(f)$ and where each f_i is a polynomial in $W = U - \{u_1\}$. Viewing f in this way makes it clear that f is also in $R[U']$.

iii) by $a_iu_i + a_ju_j$ where $j \neq i$ $a_i, b_j \in R$ and a_i is invertible in R. This is a corollary of i) and ii).

iv) Finally, the statement of (5) gotten by induction on iii).

□

The following lemma provides us with the interesting fact that if a set F of polynomial functions is simplifiable, then it is simplifiable by a set where each element has a distinct variable for which that element is monic.

Lemma 4.7. *Let $U \subseteq X$ be a finite set. Then there exists a set $V \subseteq X$ where each $v \in V$ has a distinct variable for which it is monic, $|U| \geq |V|$, and $R[U] \subseteq R[V]$.*

Proof. Do this by induction on the number of terms in U.

i) The trivial case: Let $U = \{u\}$ have only one element. By property 1 of Proposition 4.6 there is a linear form v that divides u and that is monic. Say that $u = av$ where $a \in R$. If $f \in R[U]$ then $f(u) = f(av) \in R[v]$; so $R[U] \subseteq R[v]$. It is clear that $|U| \geq |\{v\}|$.

ii) Induction Hypothesis: Let U have $k-1$ elements. Assume there exists a V where V is as stated.

iii) Prove true for U having k elements:

By property 1 of Proposition 4.6 there exists a $U' \subseteq X$ with $|U'| \leq |U|$ and at least one monic element such that $R[U] \subseteq R[U']$. Say that monic element is u'_i and that it is monic for x_j. Then by property 2 of Proposition 4.6 there exists $U'' \subseteq X$ with $|U''| \leq |U'|$ and $u'_i \in U''$ as the only element with an x_j term such that $R[U'] \subseteq R[U'']$. Consider $W = U'' - \{u'_i\}$. Now W has $k-1$ or fewer elements. So by the induction hypothesis, there exists W' of the desired form with the same or fewer number of elements as W where $R[W] \subseteq R[W']$. By property 3 of Proposition 4.6, if $V = \{u'_i\} \cup W'$, then $R[U''] \subseteq R[V]$. Say that W' has l elements, then since each one is monic for a distinct variable (distinct even from the x_j of u'_i), applying property 2 of Proposition 4.6 a total of l times to V (once for each distinct variable in W') we will arrive at a V' with the desired properties such that $R[U] \subseteq R[V']$.

□

Definition 4.8. Let $v \in X$ and let $U = \{u_1, \ldots, u_m\} \subseteq X$. Then v is called a *replacer for u_i in $R[U]$* (or simply *a replacer in $R[U]$*) if $v = a_1u_1 + \cdots + a_mu_m$ where $\{a_1, \ldots, a_m\} \in R$ and $a_i = 1$ for some $i \in \{1, \ldots, n\}$.

Theorem 4.9. *Let $v \in X$ and let $U = \{u_1, \ldots, u_m\} \subseteq X$. If v is a replacer for u_i in $R[U]$, then*

$$R[U] = R[u_1, \ldots, u_{i-1}, v, u_{i+1}, \ldots, u_m\}.$$

Proof. This theorem is a direct consequence of property (4)of Proposition 4.6 and the above definition. □

Lemma 4.10. *Let $U \in X$ be a finite set where each $u \in U$ has a distinct variable for which u is monic. Let $f \in R[U]$. Let S be the set of all reduced linear forms of f. Then there exists $v \in S$ such that v is a replacer in $R[U]$.*

Proof. We will denote from here on out the linear part of f as $LP(f)$. Let $U = \{u_1, \ldots, u_m\}$.

Case I: $LP(f) \neq 0$.

We have that $LP(f) = a_1u_1 + ... + a_nu_m$ for $a_i \in R$ and $u_i \in U$ for all $i = 1, \ldots, m$. Then $LP(f) = a(a'_1u_1 + ... + u_k + ... + a'_mu_m)$ for some $a, a'_1, \ldots, a'_m \in R$. Let $v = \frac{LP(f)}{a} = a'_1u_1 + ... + u_k + ... + a'_mu_m$. Notice that the term containing u_k in v has the coefficient 1 in front of it.

Now from our hypothesis we know that u_k is monic for, say, x_l. Then v expands to $v = b_1x_1 + ... + x_l + ... + b_nx_n$ for some $b_1, \ldots, b_n \in R$. So v, seen as a polynomial in the variables $x_1, \ldots, x_n$ is a monic linear form that divides $LP(f)$ and hence is an RLF of f, i.e. $v \in S$. Now v is also a linear combination of the elements of U with a coefficient of 1 in front of the u_k term. Hence $v \in S$ is a replacer for u_k in $R[U]$.

Case II: $LP(f) = 0$.

In this case, the first element of U divides $LP(f)$ since everything divides zero. So that element is an RLF of f and is a linear combination of elements in U with a coefficient of 1 in front of the first element of U. Hence this element is in S and is a replacer in $R[U]$. □

The next two lemmas come straight from Serge Lang's book [11], but they are well known results. They are respectively univariate and multivariate Division Remainder Theorems. These division theorems, along with their uniqueness properties, will be useful in creating (and proving the effectiveness of) a multivariate simplification algorithm.

Lemma 4.11. *(Division Remainder Theorem) Let $\mathcal{R}$ be a ring with identity and $\mathcal{R}[x]$ a polynomial ring over $\mathcal{R}$. Let $F(x)$, $G(x) \in \mathcal{R}[x]$ and $G(x)$ be monic. Then there exist polynomials $Q(x)$ and $R(x)$ such that $F(x) = Q(x)G(x) + R(x)$ with $degR(x) < degG(x)$ and such that $Q(x)$ and $R(x)$ are uniquely determined. (Note that the degree of the zero polynomial is assigned to be minus infinity).*

Lemma 4.12. *Let $\mathcal{R}$ be a ring with identity. Given two polynomials F and G in $\mathcal{R}[x_1,\ldots,x_n]$ where G is a polynomial that is monic for a variable x_i then*

$$F = \sum_{j=0}^{d} F_j(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n)[G(x_1,\ldots,x_n)]^j$$

where d is the degree of F in x_i, and $F_j(x_1,\ldots,\, x_{i-1},\, x_{i+1},\ldots,x_n) \in \mathcal{R}[x_1,\, \ldots,\, x_{i-1},\, x_{i+1},\ldots,x_n]$ for all j.

The following proposition and two lemmas provide one of the more nuanced parts of this section. It gives that if f is U-simp and if $u \in U$ has a distinct variable x_i for which u is monic, then the polynomial coefficients of f in $R[U - \{u\}][u]$ are unique, and one can find these coefficients by dividing f by u in terms of x_i according to the multivariate Division Remainder Theorem.

Proposition 4.13. *Let $F \subseteq R[x_1,\ldots,x_n]$ be a finite, n-variable polynomial set, and let $U \subseteq X$ such that $|U| < n$ and such that U contains an element u with a distinct variable for which u is monic. If F is U-simp and if we divide $f \in F$ by u to get $f = q_1 \cdot u + q_0$ where $q_1 \in R[x_1,\ldots,x_n]$ and $q_0 \in R[x_1,\ldots,x_{k-1},x_{k+1},\ldots,x_n]$ then $q_1 \in R[U]$ and $q_0 \in R[U - \{u\}]$ (that is, $(F - \{f\}) \cup \{q_1, q_0\}$ is U-simp).*

Proof. Let u be monic for the distinct variable x_k. Let $f \in F$ have x_k as a visible variable. Then as in the previous proof, $R[U] = R[U - \{u\}][u]$ and hence f can be expressed as $f = h_1 \cdot u + h_0$ where $h_1 \in R[U]$ and $h_0 \in R[U - \{u\}]$. Now since u has a distinct variable, $h_0 \in R[U - \{u\}]$ implies that $h_0 \in R[x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n]$. By the uniqueness of the division-remainder theorem, we have that $q_1 = h_1$ and $q_0 = h_0 \in R[U - \{u\}]$. □

Lemma 4.14. *Let $f \in R[x_1, \ldots, x_n]$ be an n-variable polynomial, and let f be U-simp for some $U \subseteq X$ such that $|U| < n$ and such that U contains an element u with a distinct variable x_k for which u is monic. Let $f = \sum_{j=0}^{d} q_j u^j$, where $d = deg_{x_k}(f)$ and each q_j is in $R[x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n]$. If $Q = \{q_0, q_1, \ldots, q_d\}$ then Q is $(U - \{u\})$-simp.*

Proof. This proof is done by induction on the degree of f in terms of x_k.

Trivial case: Prove the lemma true in the case where $deg_{x_k}(f) = 1$.

In this case, we have that $f = q_1 \cdot u + q_0$ where q_1, $q_0 \in R[x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n]$ as in the hypothesis. By the previous proposition, we have also that $q_1 \in R[U]$ and $q_0 \in R[U - \{u\}]$. This case will be proved if we can show that $q_1 \in R[U - \{u\}]$. Assume that this is not the case, but that $q_1 \in R[U]$ and $q_1 \notin R[U - \{u\}]$. Then q_1 can be written as a polynomial in u with coefficient from $R[U - \{u\}]$ (i.e. $q_1 \in R[U - \{u\}][u]$). So we can write $q_1 = a_r u^r + \cdots + a_1 u + a_0$ where $r \in \mathbb{Z}$, $a_r \neq 0$, and $a_i \in R[U - \{u\}]$ for $i = 0, 1, \ldots, r$. Now, since u is monic for x_k then $a_r x_k$ is a term of q_1, and since $a_r \neq 0$ and since x_k is a distinct variable for u, the term $a_r x_k$ does not cancel out with any other term. But this contradicts the fact that $q_1 \in R[x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n]$. Hence our assumption that $q_1 \notin R[U - \{u\}]$ is false. So $q_1 \in R[U - \{u\}]$.

Induction Hypothesis: Assume the lemma is true in the case where $deg(f) < k$. Assume that for any polynomial f that is U-simp and such that $d = deg_{x_k}(f) < k$ and where $f = \sum_{j=0}^{d} q_j u^j$ and each q_j is in $R[x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n]$ has the property that $\{g_1, \ldots, g_d\} \in R[U - \{u\}]$.

Inductive Step: Prove the lemma in the case where $deg(f) = k$.

In this case we have that $f = \sum_{j=0}^{k} q_j u^j$ where each q_j is in $R[x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n]$. This implies that $f = \sum_{j=0}^{k} q_j u^j = (\sum_{j=1}^{k} q_j u^{j-1})u + q_0$. By the previous proposition we have that $\sum_{j=1}^{k} q_j u^{j-1} \in R[U]$ and $q_0 \in R[U - \{u\}]$. Since $\sum_{j=1}^{k} q_j u^{j-1}$ has degree $k-1$ in terms of x_k, by the induction hypothesis $\{q_1, \ldots, q_k\} \in R[U - \{u\}]$. And hence we have our proof.

□

Lemma 4.15. *Let $F \subseteq R[x_1, \ldots, x_n]$ be a finite, n-variable polynomial set, and let F be U-simp for some $U \subseteq X$ such that $|U| < n$ and such that U contains an element u with a distinct variable x_k for which u is monic. Let $f = \sum_{j=1}^{d_f} g_{fj} u^j$ for all $f \in F$, where $d_f = deg_{x_k}(f)$ and each g_{fj} is in $R[x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n]$ (by the division-remainder theorem, each g_{fj} is uniquely determined). If $G = \{g_{fj} : f \in F, j = 1, \ldots, d_f\}$ then G is (U-$\{u\}$)-simp.*

Proof. If we apply the previous lemma to each element of F, we have the desired result. □

4.1. **Multivariate Simplification Algorithm.** We present now the Multivariate Simplification Algorithm.

Algorithm 4. *Multivariate Simplification Algorithm*

Let $F \subseteq R[x_1,\ldots,x_n]$ be a finite, n-variable set of polynomials where each polynomial has at least 2 variables (and hence n must be greater than or equal to 2). Let $U = \emptyset$. Let $t = 0$. Let $F_0 = \{f_1,\ldots,f_r\}$. Then:

```
1. Let $S_f = RLFset(f)$ for all $f \in F_t$.
2. Let $T_t = S_f$ where $|S_f|$ is minimal for all $f \in F$.
3. While $T_t \neq \emptyset$, do the following:
   a. Let $u_t \in T_t$ where $u_t$ is monic for the variable $x_k$.
   b. By Lemma 4.12 we can compute: $f = \sum_{j=1}^{d_f} g_{fj} u_t^j$ for all $f \in F_t$, where
      $d_f = deg_{x_k}(f)$ and each $g_{fj}$ is in $R[x_1,\ldots,x_{k-1},x_{k+1},\ldots,x_n]$.
   c. Let $F_{t+1} = \{g_{fj} : f \in F_t$ and $j = 1,\ldots,d_f\}$.
   d. If $F_{t+1}$ is an $(n-t-2)$-variable set, then
      $U = U \cup \{u_t\} \cup \{$set of "visible" variables in $F_{t+1}\}$.
      Return "F is simplifiable."
   e. If $|U| = n-1$
      Let $T_t = T_t - \{u_t\}$.
      Go to Step 3.
   f. If $|U| < n-1$
      Let $t = t+1$.
      Let $U = U \cup \{u\}$.
      Go to Step 1.
4. If $t = 0$ then
      Return "F is not simplifiable."
5. Else (if $t > 0$)
      Let $U_t = U_t - \{u_t\}$.
      Go to Step 3.
```

In the preceding algorithm, we input a set of polynomials $F \subset R[x_1, \ldots, x_n]$, and a set U of monic linear forms is output, where every polynomial in F can be expressed as an element of $R[U]$. In practice, when using this algorithm, we will usually input just one polynomial at the beginning. The algorithm will work just fine in this case. We chose to generalize to a set of polynomials because the algorithm can be written out more succinctly in its present form.

What the above algorithm accomplishes can be summed up in the following way: if a polynomial set is simplifiable, then there are a handful of sets that can simplify the polynomial set. At least one of these sets can be found by checking possible combinations of RLFs of polynomials found in an iterative fashion. This algorithm checks all of the relevant possible combinations of RLFs to see if they provide a simplifying set. If none of the combinations is a simplifying set for F, then, in fact, F is not simplifiable.

In particular, let F be simplifiable. Then Lemma 4.7 gives that F is V-simp for some set $V \in X$ where each element has a distinct variable and is monic for that variable. Now, unfortunately, though we know that this simplifying set V exists, we do not yet know explicitly a single element in V. We arrange in the following to find linear forms, explicitly, that will be replacers in $R[V]$ for each of the elements in V. That is, we will derive a set U made up of RLFs of polynomials found in an iterative fashion such that $R[V] = R[U]$, which implies moreover that F is U-simp.

Let $V = \{v_1, \ldots, v_m\}$ where $m < n$. Then we restate that

$$F \text{ is } \{v_1, \ldots, v_m\}\text{-simplifiable.}$$

Now, Lemma 4.10 gives that if $f \in F$, then an RLF u_1 of f is a replacer for an element, say v_1 in V. This gives that $R[V] = R[u_1, v_2, \ldots, v_m]$ giving also that

$$F \text{ is } \{u_1, v_2 \ldots, v_m\}\text{-simplifiable.}$$

Now Lemma 4.15 provides a set Q that is $(V - \{v_1\})$-simp from whence the rest of the replacement elements can be found. That is, plugging Q in for F and $V - \{v_1\}$ for V in the last paragraph provides us with: Lemma 4.10 gives that if $q \in Q$, then an RLF u_2 of q is a replacer for an element, say v_2 in $V - \{v_1\}$. This gives that $R[V - \{v_1\}] = R[u_2, v_3, \ldots, v_m]$, which in turn implies that $R[V] = R[u_1, u_2, v_3, \ldots, v_m]$. That is,

$$F \text{ is } \{u_1, u_2, v_3, \ldots, v_m\}\text{-simplifiable.}$$

Now Lemma 4.15 provides a set Q' that is $(V - \{v_1, v_2\})$-simp from whence the rest of the replacement elements can be found. One should note that the cardinality of Q can be larger than that of F: when we pass from $f \in F$ to a collection of $q \in Q$ we do this by adding at most $N + 1$ polynomials (as in Lemma 4.15), where N is the total degree of f. However, these new polynomials are in a fewer number of variables than f. This is what guarantees that the algorithm will stop in a finite number of steps.

We can continue in this way until we have replaced each of the unknown elements in V with a list of known elements. We will call this new set of known elements U, and knowing that $R[V] = R[U]$, we will conclude that

$$F \text{ is } \{u_1, u_2, u_3, \ldots, u_m\}\text{-simplifiable.}$$

Theorem 4.16. *Let $F = \{f_1, \dots, f_r\} \subseteq R[x_1, \dots, x_n]$. Algorithm 4 will output whether F is simplifiable, and, if so, it will output the polynomials $g_1, \dots, g_r$ and the simplifying set $U = \{u_1, \dots, u_m\}$ such that $f_i = g_i(u_1, \dots, u_m)$.*

Proof. All of the previous lemmas assure us that the output will be as stated. We have only now to prove that the algorithm stops. In the worst case scenario for this algorithm, the polynomial set which is input into the algorithm will not be simplifiable. In this case, each possible simplifying set (constrained to the RLFs of the polynomials) must be tested. In order to count how many calculations this will take, we notice that t will increase one-by-one to $n-2$. Then there will be $|T_{n-2}|$ RLFs to check. After all of these are checked, t will decrease to $n-3$, one element of T_{n-3} will be discarded, and we will check a new element of T_{n-3}. This will increase t to $n-2$ again, and we will need to check a new set T_{n-2} for simplifying elements. We will carry on in this way until all of the elements of T_{n-3} are used up. Then we will decrease the number of elements in T_{n-4} by one and follow the algorithm again.

Now, an upper bound for the number of RLFs for an i-variable polynomial is $q^i = |\{\text{the set of linear forms with at most } i \text{ variables over } R\}|$. But note that by Lemma 4.15 the set F_t will be an $(n-t)$-variable polynomial set (notice that this is why t cannot progress beyond $n-2$ as in Step 3e). So when $t = n-2$ there are fewer than q^2 possible RLFs to check (i.e. $|T_{n-2}| < q^2$). When we have exhausted these, there are fewer than q^3 possible RLFs when $t = n-3$ to check, each having fewer than a possible q^2 RLFs to check after each RLF at the $n-3$ level is discarded. That total is $q^3 \cdot q^2$.

Continuing in this way we get $q^2q^3q^4\dots q^n = q^{\sum\limits_{i=2}^{n} i} = q^{\frac{n(n+1)}{2}-1}$. This is an upper bound for the total number of possible simplifying sets the algorithm will have to check.

Hence the algorithm ends. □

This first example is that of a single polynomial that is input into the algorithm and found to be simplifiable.

Example 4.17. Let us work over $R = \mathbb{Z}_4$, and let $f = x+y+2z+x^2+y^2$.

Now, the only RLF of f is $u = x+y+2z$. Divide f once by u in terms of x to get $f = (x+3y+2z+1)u+2y^2$. Now, divide $x+3y+2z+1$ by u so that we get $f = (u+2y+1)u+2y^2 = u^2+(2y+1)u+2y^2 = g_2u^2+g_1u+g_0$ where $g_2 = 1$, $g_1 = 2y+1$, and $g_0 = 2y^2$. So f is now in the form of the multivariate Division Remainder Theorem. Let $F_1 = \{g_0, g_1, g_2\}$.

At this point we need to take a step back and look at what we have. Notice that F_1 is a 1-variable polynomial set. That is, the only "visible" variable in F_1 is y. So f can be expressed as a polynomial in u and y. And hence f is simplifiable by $U = \{u, y\}$, and $f = u^2+(2y+1)u+2y^2$ is the polynomial in u and y for which we were searching.

The next example is that of a single polynomial that is input into the algorithm and found to not be simplifiable.

Example 4.18. Let us work again in $R = \mathbb{Z}_4$. Let $f = x+y+y^2+z^2$. Let us assume that f is simplifiable (we will eventually disprove this). Then by Lemma 4.7 f is V-simp for some $V \subseteq X$ such that each element of V has a distinct variable for which that element is monic. Let us examine the size of

V. For f to be V-simp, $|V|$ must be less than $n = 3$, the number of variables in f. So $|V| = 1$ or 2.

Now, the only RLF of f is $u_1 = x + y$. By Lemma 4.10 we know that u is a replacer for, say, v in $R[V]$. So f is $(V - \{v\}) \cup \{u_1\} = V'$-simp. That is, if f is indeed simplifiable, we have just found an element that is in a simplifying set for f. Divide f once by u_1 in terms of x to get $f = u_1 + y^2 + z^2 = g_1 u_1 + g_0$ where $g_1 = 1$ and $g_0 = y^2 + z^2$. So f is now in the form of the multivariate Division Remainder Theorem. Let $F_1 = \{g_0, g_1\}$.

Let us take a step back, now. Unfortunately, since F_1 is a 2-variable polynomial set, we can not claim the "visible" variables as the rest of the simplifying set, since this would leave us with a simplifying set of 3 variables (u, y, and z), which would be no better than the three original variables x, y, and z.

So it remains to find a replacer for the other element in V. By Lemma 4.15 we know that F_1 is $(V' - \{u_1\}) - simp$ (note that there is only one element in $V' - \{u_1\}$). And so, again, by Lemma 4.10 we know that an RLF of one of the elements of F_1 is a replacer for the element in $V' - \{u_1\}$. That is F_1 is simplifiable by *one* RLF of an element of F_1. Well, both of the elements of F_1 have a complete set of RLFs; so we must check the entire set $\{y, z, y+z, y+2z, y+3z, 2y+z, 3y+z, \}$. We can discount y and z, though, since using one of these elements in the simplifying set would imply that the other must also be in the simplifying set, making the simplifying set too large.

Now divide g_0 by $y+z$ to get $g_0 = (y+3z)(y+z) + 2z^2$. Divide g_0 by $y+2z$ to get $g_0 = (y+3z)(y+2z) + z^2$. Divide g_0 by $y+3z$ to get

$g_0 = (y+z)(y+3z)+2z^2$. The remainders in each of these divisions are non-constant. By symmetry, dividing similarly by the rest of the RLFs will leave remainders that are non-constant. But this contradicts the fact that F_1 is simplifiable by one of its RLFs. Hence f is not simplifiable.

REFERENCES

[1] M. Bhargava, *P-orderings and polynomial functions on arbitrary subsets of Dedekind rings*, J. Reine Angew Math 490 (1997), 101-127.

[2] Z.I. Borevich, I.R. Shafarevich, *Number Theory*, Academic Press 1986.

[3] M. Elkadi, et. al., eds., *Algebraic Geometry and Geometric Modeling*, Series: Mathematics and Visualization, Springer 2006.

[4] Z. Chen, *On polynomial functions from Z_n to Z_m*, Discrete Mathematics 137 (1995) 137-145.

[5] Z. Chen, *On polynomial functions from $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ to $\mathbb{Z}_m$*, Discrete Mathematics 162 (1996) 67-76.

[6] S. Frisch, *Polynomial Functions on Finite Commutative Rings*, Advances in Ring Theory (Fes III Conf. 1997) (1999) 323-336.

[7] S. Gopalakrishnan, P. Kalla, M.B. Meredith, and F. Enescu, *Finding Linear Building-Blocks for RTL Synthesis of Polynomial Datapaths with Fixed-Size Bit-Vectors*, Accepted. To appear in Proc. Intl. Conf. on CAD (ICCAD) 2007.

[8] L.K. Hua, *Introduction to Number Theory*, Springer, 1982.

[9] N. Hungerbuehler and E. Specker, *A generalization of the Smarandache function to several variables*, Integers: Electronic J. Combinatorial Number Theory, 6 (2006), #A23.

[10] A. J. Kempner, *Polynomials and their residue systems*, Amer. Math. Soc. Trans 22 (1921) 240-288.

[11] S. Lang, *Algebra*, Springer, 2002.

[12] V. Prasolov, *Polynomials*, Springer, Berlin 2000.

[13] N. Shekhar, P. Kalla, M.B. Meredith, and F. Enescu, *Simulation Bounds for Equivalence Verification of Polynomial Datapaths using Finite Ring Algebra*, Accepted. To appear in IEEE Trans. on VLSI, special section on Design Validation and Verification.

[14] D. Singmaster, *On Polynomial Functions (mod m)*, J. Number Theory 6 (1974) 345-352.

[15] M. Wood, *P-orderings: a metric viewpoint and the non-existence of simultaneous orderings*, J. Number Theory 99 (2003) 36-56.