WORD-LEVEL POLYNOMIAL ABSTRACTION FROM CIRCUITS USING GRÖBNER BASES

Tim Pruss
A Master's Thesis Proposal
Electrical & Computer Engineering, University of Utah
Spring Semester 2013

Abstract

A combinational circuit with k-inputs and k-outputs implements Boolean functions $f : \mathbb{B}^k \rightarrow \mathbb{B}^k$, where $\mathbb{B} = \{0,1\}$. Such functions can also be construed as a mapping $f : \mathbb{F}_{2^k} \rightarrow \mathbb{F}_{2^k}$, where $\mathbb{F}_{2^k}$ denotes the Galois field of 2^k elements. Every function over $\mathbb{F}_{2^k}$ is a polynomial function — i.e. there exists a unique, minimal, canonical polynomial $\mathcal{F}$ that describes f. In this master's thesis, we propose to investigate computer algebra based methods to derive the canonical (word-level) polynomial representation of the circuit as $Y = \mathcal{F}(A)$ over $\mathbb{F}_{2^k}$, where A and Y denote, respectively, the input and output bit-vectors of the circuit. We show that this can be achieved by computing a Gröbner basis of a set of polynomials derived from the circuit, using a specific elimination term order. Computing Gröbner bases using elimination orders is, however, practically infeasible for large circuits. To overcome this limitation, we propose to investigate the use of the FGLM algorithm — which converts a given Gröbner basis w.r.t. one term order $>_1$ into another w.r.t. an elimination term order $>_2$ — to derive the required polynomial abstraction. The objective of this research is to: i) design an efficient CAD tool based on our approach; and ii) apply it to reverse-engineer hardware implementations of Elliptic Curve Cryptography (ECC) primitives over Galois fields $\mathbb{F}_{2^k}$ — with applications to design verification and function identification.

I. INTRODUCTION

Abstraction of word-level functionality from bit-level descriptions of digital circuits is an important fundamental problem in Electronic Design Automation (EDA) and design verification. Word-level abstractions find applications in high-level/RTL datapath synthesis [1] [2] [3], RTL verification [4] [5] [6], word-level SMT and constraint solving [7] [8] [9], and can also be applied to detect malicious modifications to a circuit – potentially inserted as hardware Trojan horses – by reverse-engineering the function implemented by the circuit. It is further desirable that the obtained word-level abstraction be a *canonical* representation of the function, to facilitate equivalence verification between a specification model and an implementation circuit. This master's thesis proposes the investigation of the problem of deriving word-level, canonical, polynomial representations from circuits over Galois fields using concepts from commutative algebra and algebraic geometry — notably, Gröbner bases [10], Buchberger's algorithm [11], elimination ideals [12], and the FGLM algorithm [13].

The main motivation for this work is to "reverse engineer" or identify the function implemented by a given Galois field arithmetic circuit as used in Elliptic Curve Cryptography (ECC). The main operations of encryption, decryption and authentication in ECC rely on point-addition and point-doubling operations on elliptic curves defined over Galois fields $\mathbb{F}_{2^k}$. These primitive operations are, in turn, implemented as circuits that perform polynomial computations over k-bit vectors [14]. The objective is to apply our approach to a given circuit and *extract the word-level polynomial function* implemented by it for design verification. The mathematical problems addressed in this proposal, and the approaches to solve them, are described below:

Problem Statement: Given a combinational circuit C with k-bit inputs and k-bit outputs, such that the circuit implements Boolean functions that are mappings between k-dimensional Boolean spaces: $f : \mathbb{B}^k \rightarrow \mathbb{B}^k$. Let $\{a_0, \ldots, a_{k-1}\}$ denote the primary inputs of the circuit, and let $\{y_0, \ldots, y_{k-1}\}$ denote the bit-level primary outputs. Suppose that we do not know the function implemented by the circuit. We wish to derive a *word-level, symbolic representation* of the function as $Y = \mathcal{F}(A)$, where $Y = \{y_0, \ldots, y_{k-1}\}$, $A = \{a_0, \ldots, a_{k-1}\}$ are, respectively, the output and input bit-vectors, and $\mathcal{F}$ denotes a polynomial representation of the function f. We wish to further generalize our approach to any circuit with arbitrary number of inputs (n) and outputs (m), as polynomial functions $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^m}$.

Approach: At a Boolean-level, canonical symbolic DAG representations of functions have been extensively investigated; such as decisions diagrams (ROBDDs [15], FDDs [16]), moment diagrams (BMDs [17], K*BMDs [18]) and their word-level variants [4]. However, the decomposition principle behind these representations is based on (variants of) the Shannon's expansion, which is a bit-wise, Boolean decomposition. Such approaches cannot be efficiently applied to word-level abstraction of modulo-arithmetic circuits over Galois extension fields $\mathbb{F}_{2^k}$. Therefore, we approach this problem from a symbolic commutative algebra perspective.

The function $f : \mathbb{B}^k \rightarrow \mathbb{B}^k$ is a mapping among 2^k elements. Therefore, f can also be interpreted, algebraically, in the following two ways: i) as a function $f : \mathbb{Z}_{2^k} \rightarrow \mathbb{Z}_{2^k}$, i.e. as a function over finite integer rings $\pmod{2^k}$; and ii) as a function $f : \mathbb{F}_{2^k} \rightarrow \mathbb{F}_{2^k}$, where $\mathbb{F}_{2^k}$ represents the Galois field of 2^k elements. In this work, we will analyze f as a polynomial function over $\mathbb{F}_{2^k}$, for the following reasons.

First of all, *not every function* of the type $f : \mathbb{Z}_{2^k} \rightarrow \mathbb{Z}_{2^k}$, is a polynomial function; i.e. every function cannot be represented by a polynomial $\mathcal{F} \pmod{2^k}$. In commutative algebra, identification of such polynomial functions is an important problem: i.e. given a function $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$, $n \in \mathbb{N}$, identify if f has a polynomial representation. If so, derive a unique, minimal, canonical polynomial $\mathcal{F}$, such that $f \equiv \mathcal{F} \pmod{n}$. The papers [19] [20] [21] addressed such problems in number theory and algebra. *Shekhar* [22] also addressed RTL verification of polynomial datapaths over k-bit vectors using the above concepts. However, in her work, the RTL datapath was already known to be a polynomial function $\pmod{2^k}$. Unfortunately, an arbitrary k-input/k-output combinational circuit cannot always be modeled as a polynomial function over $\mathbb{Z}_{2^k}$; therefore, the $\mathbb{Z}_{2^k}$ model is not considered in this work.

On the other hand, there is a well-known "textbook" result [23] which states that over Galois fields ($\mathbb{F}_q$) of q elements, *every function* $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ is a polynomial function. Motivated by this fundamental result, we will devise an approach to extract a word-level polynomial function (abstraction) from a circuit. Given the circuit C which represents a function $f : \mathbb{B}^k \rightarrow \mathbb{B}^k$, we will interpret f as a function $f : \mathbb{F}_{2^k} \rightarrow \mathbb{F}_{2^k}$, and derive a unique, minimal, canonical polynomial representation as $Y = \mathcal{F}(A)$ over $\mathbb{F}_{2^k}$, where Y, A are, respectively, the output and input bit-vectors of the circuit C. We will extract a set of polynomials (ideal) from the circuit and employ *Gröbner bases* techniques to abstract the canonical polynomial representation. Our approach can be generalized to a circuit with arbitrary number of inputs and outputs, i.e. to analyze polynomial functions $f : \mathbb{F}_q^d \rightarrow \mathbb{F}_q$, $q = 2^k$, and further to $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^m}$.

Example 1.1: **Motivating Example:** *Consider a 2-bit multiplier circuit over $\mathbb{F}_{2^2}$ given in Fig. 1, which implements a function $f : \mathbb{F}_4 \times \mathbb{F}_4 \rightarrow \mathbb{F}_4$. It implements a* **polynomial function***: $Z = A \times B$, $Z, A, B \in \mathbb{F}_4$. Variables a_0, a_1, b_0, b_1 are primary inputs, z_0, z_1 are primary outputs, and s_0, s_1, s_2, s_3, r_0 are intermediate variables of the circuit. These bit-level variables are in $\mathbb{F}_2 = \{0, 1\}$. Then, we can consider $A = a_0 + a_1\alpha$, $B = b_0 + b_1\alpha$ as the word-level inputs and $Z = z_0 + z_1\alpha$ as the output in $\mathbb{F}_4$. Here $P(x) = x^2 + x + 1$ is the primitive polynomial of $\mathbb{F}_4$ and $P(\alpha) = 0$.*

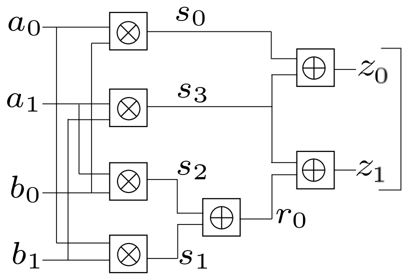

Fig. 1: A 2-bit Multiplier over $\mathbb{F}_{2^2}$. The gate $\otimes$ corresponds to AND-gate, i.e. bit-level multiplication modulo 2. The gate $\oplus$ corresponds to XOR-gate, i.e. addition modulo 2.

The functionality of the entire circuit can be described using the following polynomials derived from the Boolean gate-level operators: $f_1 : z_0 + z_1\alpha + Z$; $f_2 : b_0 + b_1\alpha + B$; $f_3 : a_0 + a_1\alpha + A$; $f_4 : s_0 + a_0 \cdot b_0$; $f_5 : s_1 + a_0 \cdot b_1$; $f_6 : s_2 + a_1 \cdot b_0$; $f_7 : s_3 + a_1 \cdot b_1$; $f_8 : r_0 + s_1 + s_2$; $f_9 : z_0 + s_0 + s_3$; $f_{10} : z_1 + r_0 + s_3$. If we impose the following **elimination** *term order:* **lex term order** *with "circuit variables" > "Output Z" > "Inputs, A, B" and compute a Gröbner basis G of $\{f_1, \dots, f_{10}\}$, we observe the following polynomials in the basis: $g_1 : z_0 + z_1\alpha + Z$; $g_2 : b_0 + b_1\alpha + B$; $g_3 : a_0 + a_1\alpha + A$; $g_4 : s_3 + r_0 + z_1$; $g_5 : s_1 + s_2 + r_0$; $g_6 : s_0 + s_3 + z_0$; $\mathbf{g_7 : Z + AB}$; $g_8 : a_1b_1 + a_1B + b_1A + z_1$; $g_9 : r_0 + a_1b_1 + z_1$; $g_{10} : s_2 + a_1b_0$. Notice that the polynomial $g_7 : Z + AB$ describes $Z = AB$ as the (canonical) polynomial function implemented by the circuit; and we were able to extract this representation using the Gröbner basis computation. We wish to explore such an approach to derive an efficient decision procedure for word-level abstraction.*

Contributions of this Thesis: Our approach to solve this problem, and the contributions of this thesis, can be outlined as follows:

1) Using polynomial abstractions, we analyze the circuit, and model the gate-level Boolean operators as elements of a multivariate polynomial ring with coefficients in $\mathbb{F}_{2^k}$.
2) Based on the concepts of *Strong Nullstellensatz, Gröbner bases, elimination ideals and projections of varieties* [12], we deduce that the polynomial abstraction problem can be formulated as one of *computing a Gröbner basis* of the set of

polynomials derived from the given circuit netlist, using a specific elimination term order $>$.

3) Computing Gröbner bases using elimination term orders is infeasible for large circuits. To overcome this limitation, we will investigate the use of the FGLM algorithm [13] to derive the polynomial representation. The FGLM algorithm takes an *already computed* Gröbner basis (G_1) w.r.t. an arbitrary term order $>_1$, and transforms it into another Gröbner basis (G) w.r.t. an elimination term order $>$. In the PhD thesis of *Lv* [24], it was shown that for any given circuit, there exists a term order $>_1$ that renders the set of polynomials derived from the circuit itself a Gröbner basis. Moreover, $>_1$ can be easily derived by performing a reverse topological traversal of the circuit. Consequently, G_1 is readily available as a Gröbner basis directly by construction. Using FGLM, we can then translate G_1 into the Gröbner basis G w.r.t. the required elimination order $>$.
4) The worst-case complexity of computing a Gröbner basis is known to be doubly exponential in n, the number of variables, and polynomial in d, the degree of the ideal. Most hardware/software verification applications do exhibit such high complexity, as the number of intermediate computations in the Buchbeger's algorithm [11] tend to explode. Therefore, we conjecture that using the FGLM algorithm — which relies on sparse linear algebra concepts — perhaps this complexity can be avoided. In this thesis, we will develop a CAD framework using the above ideas and investigate the scalability of our methods.
5) As an application, we will use our CAD approach to reverse-engineer the function implemented by a given Galois field arithmetic circuits used in ECC implementations. This can be used for function identification from a given circuit for formal verification.

Proposal Organization: The next section reviews previous work in the area of canonical representations functions, word-level abstractions, formal design verification using computer algebra techniques, and also polynomial interpolation literature in symbolic computing. Section III reviews Galois field theory and hardware design. Section IV reviews preliminary computer-algebra concepts related to ideals, varieties, Gröbner bases, elimination ideals and Nullstellensatz. Section V describes our results on polynomial abstraction from circuits, and demonstrates the application of our work using preliminary experiments. The application of the FGLM algorithm is covered in Section **??**. Finally, Section **??** outlines the research plan and concludes the proposal.

II. Review of Previous Work

A. Canonical Decision Diagrams

The problem of canonical representations of Boolean functions has received a lot of attention. The Reduced Ordered Binary Decision Diagram (ROBBD) [15] was the first significant contribution in this area. ROBDDs represent a Boolean function as an implicit set of points on a canonical directed acyclic graph (DAG). The decomposition principle behind BDDs is one of Shannon's expansion, i.e. $f(x,y,\dots) = xf_x + x'f_{x'}$, where $f_x = f(x=1)$ and $f_{x'} = f(x=0)$ denote the positive and negative co-factors of f w.r.t. x, respectively. Motivated by the success of BDDs, variants of the Shannon's decomposition principle (Davio, Reed-Muller, etc.) were explored to develop other functional decision diagrams. These include FDDs [16], ADDs [25], MTBDDs [26], their hybrid and edge-valued counterparts, HDDs [27] and EVBDDs [28]. While these are referred to as *Word-Level Decision Diagrams* [4], the decomposition is still point-wise, binary, w.r.t. each Boolean variable. These representations do not serve the purpose of word-level abstraction from bit-level representations.

Binary Moment Diagrams (BMDs) [17], and its derivatives K*BMDs [18] and *PHDDs [29], depart from the Boolean decomposition and perform the decomposition of a *linear* function based on its two moments. BMDs provide a compact representation for integer arithmetic circuits such as multipliers and squarers. However, these are inapplicable for modulo-arithmetic circuits over Galois fields. Taylor Expansion Diagrams (TEDs) [30] are a canonical representation of a *polynomial expression*, but they do not represent a *polynomial function* canonically. While [22] and [31] provide canonical representations of polynomial functions, they do so over $\mathbb{Z}_{2^k}$ and not over $\mathbb{F}_{2^k}$.

MODDs [32] [33] are a DAG representation of the characteristic function of a circuit over Galois fields $\mathbb{F}_{2^k}$. MODDs come very close to satisfying our requirements as a canonical word-level representation that can be employed over Galois fields, as it essentially interpolates a polynomial from the characteristic function. However, MODDs do not scale very well for large circuits — this is because every node in the DAG can have up to k children and the normalization operations are very complicated for MODDs. They also suffer from the size explosion problem during intermediate computations. They are known to be infeasible beyond 32-bit circuits.

In the realm of theorem-proving and SMT-solving, many automated decision procedures have been devised that can decide satisfiability/validity of word-level formulas represented by a combination of theories, but they do not provide a canonical representation of the function implemented by a "bit-blasted" circuit.

B. Prior work on Verification of Galois field circuits

Symbolic computer algebra techniques have been employed for formal verification of circuits over $\mathbb{Z}_{2^k}$ and also over $\mathbb{F}_{2^k}$. The work of [34] shows how to use Gröbner basis techniques to count the zeros of an ideal J over $\mathbb{F}_q$ (i.e. count $V_{\mathbb{F}_q}(J)$). The authors then follow-up with an approach for *quantifier elimination* over Galois fields $\mathbb{F}_q$ [35]. While the above works present the theory and algorithms, efficiency/improvements in Gröbner basis computation is not addressed. So is also the case with other general verification techniques using Gröbner bases [36] [37] [38], etc. The paper [39] addresses verification of finite-precision integer datapath circuits using the concepts of Gröbner bases over the ring $\mathbb{Z}_{2^k}$. In [40], the authors further show an integration of their approach within an SMT-solver for arithmetic instances.

In [41] [42] [43], the authors present the BLUEVERI tool from IBM for verification of Galois field circuits for error correcting codes against an algorithmic spec. The implementation consists of a set of (pre-designed and verified) circuit blocks that are interconnected to form the error correcting system. The spec is given as a set of design constraints on a "check file". Their objective is to prove the equivalence of the implementation against this check file, for which they employ a Nullstellensatz formulation. For final verification, the polynomial system is given to a computer algebra tool (SINGULAR [44]) to *compute* a reduced Gröbner basis. However, improvements to the core Gröbner basis computational engine are not the subject of their work.

In [24] [45] [46] [47], *Lv et al.* present computer algebra techniques for formal verification of Galois field arithmetic circuits. Given a specification polynomial f, and a circuit C, they formulate the verification problems as an ideal membership test using the Strong Nullstellensatz and Gröbner bases. In [45], the authors show that for any combinational circuit, *there exists a term order $>_1$ that renders the set of polynomials of the circuit itself a Gröbner basis — and this term order can be easily derived by performing a topological traversal of the circuit.* By exploiting this term order, verification can be significantly scaled to 163-bit (NIST-specified) cryptography circuits. In contrast to the work of [24], we are not given a specification polynomial. Given the circuit C, we want to derive (extract) the word-level specification f. In our work, we borrow and further build upon the results of [34] [35] [45] [24].

C. Polynomial Interpolation in Symbolic Computation

The problem of polynomial interpolation is a fundamental problem in symbolic and algebraic computing which finds application in modular algorithms, such as the GCD computation and polynomial factorization. The problem is stated as follows: Given n distinct data points $x_1,\dots,x_n$, and their evaluations at these points $y_1,\dots,y_n$, *interpolate* a polynomial $\mathcal{F}(X)$ of degree $n-1$ (or less) such that $\mathcal{F}(x_i) = y_i$ for $1 \le i \le n$. Let t be the number of non-zero terms in $\mathcal{F}$ and let T be the total number of possible terms. When $\frac{t}{T} << 1$, the polynomial $\mathcal{F}$ is *sparse*, otherwise it is *dense*. Much of the work in polynomial interpolation addresses sparse interpolation using the "black-box" model (also called the algebraic circuit model) as shown in Fig. 2.

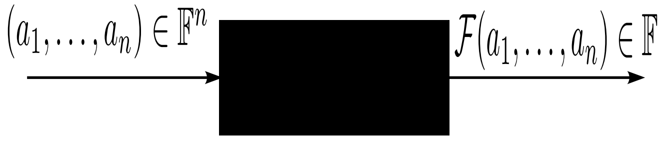
$(a_1,\dots,a_n) \in \mathbb{F}^n$
$\mathcal{F}(a_1,\dots,a_n) \in \mathbb{F}$

Fig. 2: The black-box or the algebraic circuit representation.

Let $\mathcal{F}$ be a multivariate polynomial in n variables $\{x_1,\dots,x_n\}$, with t non-zero terms ($0 < t < T$), represented with a black-box B. On input $(x_1,\dots,x_n)$, the black-box evaluates $y_i = \mathcal{F}(x_1,\dots,x_n)$. Given also a degree bound d on $\mathcal{F}$, the goal is to interpolate the polynomial $\mathcal{F}$ with a minimum number of *probes* to the black-box. The early work of Zippel [48] and Ben-Or/Tiwari [49] require $O(ndt)$ and $O(T\log n)$ probes, respectively, to the black-box. These bounds have since been improved significantly; the recent algorithm of [50] interpolates with $O(nt)$ probes.

Our problem falls into the category of dense interpolation, as we require a polynomial that describes the function at each of the q points of the field $\mathbb{F}_q$. Newton's interpolation technique, with the black-box model, bounds the number of probes by $(d+1)^n$ — which exhibits very high complexity. In the logic synthesis area, the work of [51] investigates dense interpolation. Due to this high-complexity, their approach is feasible only for applications over small fields, *e.g.* computing Reed-Muller forms for multi-valued logic.

We can also employ the black-box model by replacing the black-box (algebraic circuit) by the given circuit C; then every *probe* of the black-box would correspond to a *simulation of the circuit.* As we desire a polynomial representation of the entire function, exhaustive simulation would be required, which is infeasible. Therefore, we propose a *symbolic approach* to polynomial interpolation from a circuit using the Gröbner basis computation. It can be shown that the computational complexity of computing a Gröbner basis for our problem, in the worst case, is $q^{O(n)}$, where $q = 2^k$, k is the datapath width and n is the number of variables in the circuit.

III. Galois Fields, Polynomial Functions & Hardware Design

A Galois field is a field with a finite number of elements. The number of elements q of the field is a power of a prime integer — i.e. $q = p^k$, where p is a prime integer, and $k \geq 1$ is a positive integer [52]. Galois fields are denoted as $\mathbb{F}_q$ and also $GF(q = p^k)$. We are interested in fields where $p = 2$ and $k > 1$ — i.e. *binary Galois extension fields* $\mathbb{F}_{2^k}$ — as they are widely employed in hardware implementations of cryptography primitives.

To construct $\mathbb{F}_{2^k}$, we take the polynomial ring $\mathbb{F}_2[x]$, where $\mathbb{F}_2 = \{0,1\}$, and an irreducible polynomial $P(x) \in \mathbb{F}_2[x]$ of degree k, and construct $\mathbb{F}_{2^k}$ as $\mathbb{F}_2[x] \pmod{P(x)}$. As a result, all field operations are performed modulo the irreducible polynomial $P(x)$ and the coefficients are reduced modulo $p = 2$. Any element $A \in \mathbb{F}_{2^k}$ can be represented in polynomial form as $A = a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1}$, where $a_i \in \mathbb{F}_2, i = 0,\ldots,k-1$, and α is the root of the irreducible polynomial, *i.e.* $P(\alpha) = 0$. The field $\mathbb{F}_{2^k}$ can therefore be construed as a k-dimensional vector space over $\mathbb{F}_2$.

Example 3.1: Let us construct $\mathbb{F}_{2^4}$ as $\mathbb{F}_2[x] \pmod{P(x)}$, where $P(x) = x^4 + x^3 + 1 \in \mathbb{F}_2[x]$ is an irreducible polynomial of degree $k = 4$. Let α be the root of $P(x)$, i.e. $P(\alpha) = 0$. Any element $A \in \mathbb{F}_2[x] \pmod{x^4 + x^3 + 1}$ has a representation of the type: $A = a_3x^3 + a_2x^2 + a_1x + a_0$ where the coefficients $a_3,\ldots,a_0$ are in $\mathbb{F}_2 = \{0,1\}$. Since there are only 16 such polynomials, we obtain 16 elements in the field $\mathbb{F}_{16}$. Each element in can then be viewed as a 4-bit vector over $\mathbb{F}_2$: $\mathbb{F}_{16} = \{(0000),(0001),\ldots(1110),(1111)\}$. Each element also has an exponential representation; all three representations are shown in Table I. For example, consider the element α^{12}. Computing $\alpha^{12} \pmod{\alpha^4 + \alpha^3 + 1} = \alpha + 1 = (0011)$; hence we have the three equivalent representations.

TABLE I: Bit-vector, Exponential and Polynomial representation of elements in $\mathbb{F}_{2^4} = \mathbb{F}_2[x] \pmod{x^4 + x^3 + 1}$

$a_3a_2a_1a_0$	Exponential	Polynomial	$a_3a_2a_1a_0$	Exponential	Polynomial
0000	0	0	1000	α^3	α^3
0001	1	1	1001	α^4	α^3+1
0010	α	α	1010	α^{10}	$\alpha^3+\alpha$
0011	α^{12}	$\alpha+1$	1011	α^5	$\alpha^3+\alpha+1$
0100	α^2	α^2	1100	α^{14}	$\alpha^3+\alpha^2$
0101	α^9	α^2+1	1101	α^{11}	$\alpha^3+\alpha^2+1$
0110	α^{13}	$\alpha^2+\alpha$	1110	α^8	$\alpha^3+\alpha^2+\alpha$
0111	α^7	$\alpha^2+\alpha+1$	1111	α^6	$\alpha^3+\alpha^2+\alpha+1$

Polynomial Functions $f : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$: Arbitrary mappings among k-bit vectors can be constructed; each such mapping generates a function $f : \mathbb{B}^k \to \mathbb{B}^k$. Since every k-bit vector can be construed as an element in $\mathbb{F}_{2^k}$ (as shown in the above example), every such function corresponds to a function over Galois fields: $f : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$. Every such function is also a polynomial function.

Theorem 3.1: From [23]: Let $\mathbb{F}_q$ be a Galois field of q elements where q is a power of a prime integer. Any function $f : \mathbb{F}_q \to \mathbb{F}_q$ is a polynomial function over $\mathbb{F}_q$, that is there exists a polynomial $\mathcal{F} \in \mathbb{F}_q[x]$ such that $f(a) = \mathcal{F}(a)$, for all $a \in \mathbb{F}_q$.

By analyzing f over each of the q points, one can apply **Langrange's interpolation formula** and interpolate a polynomial $\mathcal{F}(x) = \sum_{k=1}^{q} \frac{\prod_{i\neq k}(x-x_i)}{\prod_{i\neq k}(x_k-x_i)} \cdot f(x_k)$, which is a polynomial of degree at most $q-1$ in x. One can easily see that $\mathcal{F}(a) = f(a)$ for all $a \in \mathbb{F}_q$, and $\mathcal{F}(x)$ is therefore the polynomial function representation of f.

Example 3.2: Let $A = \{a_2,a_1,a_0\}$ and $Y = \{y_2,y_1,y_0\}$ be 3-bit vectors. Consider the function $Y[2:0] = A[2:0] >> 1$, i.e. a **bit-vector right shift** *operation on A. The function maps as follows:*

$\{a_2a_1a_0\}$	A	$\to$	$\{y_2y_1y_0\}$	Y	$\{a_2a_1a_0\}$	A	$\to$	$\{y_2y_1y_0\}$	Y
000	0	$\to$	000	0	100	α^2	$\to$	010	α
001	1	$\to$	000	0	101	α^2+1	$\to$	010	α
010	α	$\to$	001	1	110	$\alpha^2+\alpha$	$\to$	011	$\alpha+1$
011	$\alpha+1$	$\to$	001	1	111	$\alpha^2+\alpha+1$	$\to$	011	$\alpha+1$

If we model this function as $f : \mathbb{Z}_8 \to \mathbb{Z}_8$, then using the results of [19] [20] [21], we deduce that this function is not a polynomial function over $\mathbb{Z}_8$. However, applying Largange's interpolation formula over $\mathbb{F}_{2^3}$, we obtain the following polynomial function representation, $Y = (\alpha^2+1)A^4 + (\alpha^2+1)A^2$, where $P(\alpha) = \alpha^3 + \alpha + 1 = 0$.

An important property of Galois fields is that for all elements $A \in \mathbb{F}_q, A^q = A$, and hence $A^q - A = 0$. Therefore, the polynomial $x^q - x$ *vanishes* on all points in $\mathbb{F}_q$. Consequently, any polynomial $\mathcal{F}(X)$ can be reduced $\pmod{X^q - X}$ to obtain a canonical representation $\mathcal{F}(X) \pmod{X^q - X}$ with degree at most $q-1$. Such *vanishing polynomials* will form an important part of our ideal membership formulation.

Definition 3.1: Any function $f : \mathbb{F}_q^d \rightarrow \mathbb{F}_q$ has a unique canonical representation (UCR) as polynomial $\mathcal{F} \in \mathbb{F}_q[x_1, \ldots, x_d]$ such that all its nonzero monomials are of the form $x_1^{i_1} \cdots x_d^{i_d}$ where $0 \le i_j \le q-1$, for all $j = 1, \ldots d$.

A. Hardware Implementations of Galois Field Arithmetic

Point Addition over Elliptic Curves: The main operations of encryption, decryption and authentication in elliptic curve cryptography (ECC) rely on *point additions* and *doubling* operations on elliptic curves designed over Galois fields. In general, this requires computation of multiplicative inverses over the field - which is expensive. Modern approaches represent the points in projective coordinate systems, *e.g.*, the López-Dahab (LD) projective coordinate [14], which eliminates the need for multiplicative inverses and improves the efficiency of these operations.

Example 3.3: Consider point doubling in LD projective coordinate system. Given an elliptic curve: $Y^2 + XYZ = X^3Z + aX^2Z^2 + bZ^4$. *Let ($X_3$, Y_3, Z_3) = 2(X_1, Y_1, Z_1), then* X_3, Y_3, Z_3 *can be computed as:* $X_3 = X_1^4 + b \cdot Z_1^4$; $Z_3 = X_1^2 \cdot Z_1^2$; $Y_3 = bZ_1^4 \cdot Z_3 + X_3 \cdot (aZ_3 + Y_1^2 + bZ_1^4)$.

The multiplication and iterative squaring operations in the above computation are usually implemented using custom-designed Galois field multipliers, such as the Mastrovito [53], Montgomery [54], Barrett multipliers [55], or composite-field multipliers [56] — which are, in turn, hierarchically designed. For example, Montgomery reduction (MR) computes: $MR(A,B) = A \cdot B \cdot R^{-1} \pmod{P(x)}$, where A, B are k-bit inputs, R is suitably chosen as $R = \alpha^k$, R^{-1} is multiplicative inverse of R in $\mathbb{F}_{2^k}$, and $P(x)$ is the irreducible polynomial. Since Montgomery reduction cannot directly compute $A \cdot B \pmod{P(x)}$, we need to pre-compute $A \cdot R$ and $B \cdot R$, as shown in Figure 3.

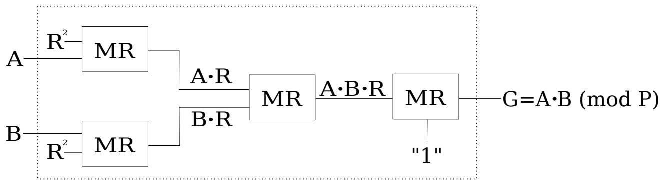

Fig. 3: *Montgomery* multiplication over $\mathbb{F}_{2^k}$ using four Montgomery reductions.

Given a hierarchically designed Montgomery multiplier, we will first extract polynomials AR, BR, ABR from the sub-circuit blocks. By analyzing the interconnection of these sub-circuits at word-level, we can then apply our approach at a higher-level, to extract the function of the entire circuit. Performing such operations hierarchically, we will apply our approach to reverse-engineer point-addition circuits designed using a variety of such Galois field adder and multiplier circuits.

IV. Computer Algebra Preliminaries

We denote a Galois field of q elements by $\mathbb{F}_q$, where $q = 2^k$ in our case. Let $\mathbb{F}_q[x_1, \ldots, x_d]$ be the polynomial ring over $\mathbb{F}_q$ with indeterminates $x_1, \ldots, x_d$. A *monomial* in variables $x_1, \cdots, x_d$ is a product of the form $X = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_d^{\alpha_d}$, where $\alpha_i \ge 0, i \in \{1, \ldots, d\}$. A *polynomial* $f \in \mathbb{F}_q[x_1, \ldots, x_d], f \neq 0$, is written as a finite sum of terms $f = c_1X_1 + c_2X_2 + \cdots + c_tX_t$. Here $c_1, \ldots, c_t$ are coefficients and $X_1, \ldots, X_t$ are monomials. To systematically manipulate the polynomials, a *monomial ordering* $>$ is imposed such that $X_1 > X_2 > \cdots > X_t$. Subject to such an ordering, $lt(f) = c_1X_1$, $lm(f) = X_1$, $lc(f) = c_1$, are the *leading term*, *leading monomial* and *leading coefficient* of f, respectively. Similarly, tail(f) = $c_2X_2 + \cdots + c_tX_t$. Division of a polynomial f by polynomial g gives remainder polynomial r, denoted $f \xrightarrow{g}_+ r$. Similarly, f can be reduced (divided) w.r.t. a set of polynomials $F = \{f_1, \ldots, f_s\}$ to obtain a remainder r, denoted $f \xrightarrow{F}_+ r$, such that no term in r is divisible by the leading term of any polynomial in F.

Ideals and varieties: An *ideal* J generated by polynomials $f_1, \ldots, f_s \in \mathbb{F}_q[x_1, \ldots, x_d]$ is: $J = \langle f_1, \ldots, f_s \rangle = \{\sum_{i=1}^{s} h_i \cdot f_i : \ h_i \in \mathbb{F}[x_1, \ldots, x_d]\}$. The polynomials $f_1, \ldots, f_s$ form the basis or generators of J.

Let $\mathbf{a} = (a_1, \ldots, a_d) \in \mathbb{F}_q^d$ be a point, and $f \in \mathbb{F}_q[x_1, \ldots, x_d]$ be a polynomial. We say that f *vanishes* on $\mathbf{a}$ if $f(\mathbf{a}) = 0$. For any ideal $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}_q[x_1, \ldots, x_d]$, the *affine variety* of J over $\mathbb{F}_q$ is: $V(J) = \{\mathbf{a} \in \mathbb{F}^d : \forall f \in J, f(\mathbf{a}) = 0\}$. In other words, the variety corresponds to the set of all solutions to $f_1 = \ldots f_s = 0$.

For any subset V of $\mathbb{F}_q^d$, the ideal of polynomials that vanish on V, called the *vanishing ideal of* V, is defined as: $I(V) = \{f \in \mathbb{F}_q[x_1,\dots,x_d] : \forall \mathbf{a} \in V, f(\mathbf{a}) = 0\}$. If a polynomial f vanishes on a variety V, then $f \in I(V)$.

A. Strong Nullstellensatz over Galois Fields

Our problem formulation is derived from Nullstellensatz, which admits a special form over Galois fields. We state the following results of Nullstellensatz over Galois fields, proofs of which can be found in [34].

Let $\mathbb{F}_q$ be a Galois field of q elements. For all elements $A \in \mathbb{F}_q$, we have $A^q - A = 0$. Therefore, for a polynomial $x^q - x$, we have $V(x^q - x) = \mathbb{F}_q$. The polynomials of the form $\{x^q - x\}$ are called the *vanishing polynomials* of the field. Let $F_0 = \{x_1^q - x_1, \dots,\ x_d^q - x_d\}$, then $J_0 = \langle x_1^q - x_1, \dots, x_d^q - x_d\rangle$ is the ideal of all vanishing polynomials in $\mathbb{F}_q[x_1,\dots,x_d]$. Below, we use the concept of sum of ideals: given ideals $I_1 = \langle f_1,\dots,f_s\rangle$ and $I_2 = \langle g_1,\dots,g_t\rangle$, then ideal $I_1 + I_2 = \langle f_1,\dots,f_s,g_1,\dots,g_t\rangle$.

Theorem 4.1: Strong Nullstellensatz over $\mathbb{F}_q$: For any Galois field $\mathbb{F}_q$, let $J \subseteq \mathbb{F}_q[x_1,\dots,x_d]$ be an ideal, and let $J_0 = \langle x_1^q - x_1,\dots,x_d^q - x_d\rangle$ be the ideal of all vanishing polynomials. Let $V_{\mathbb{F}_q}(J)$ denote the variety of J over $\mathbb{F}_q$. Then, $I(V_{\mathbb{F}_q}(J)) = J + J_0 = J + \langle x_1^q - x_1,\dots,\ x_d^q - x_d\rangle$.

B. Gröbner Basis of Ideals

An ideal J may have many different generators: it is possible to have sets of polynomials $F = \{f_1,\dots,f_s\}$ and $G = \{g_1,\dots,g_t\}$ such that $J = \langle f_1,\dots,f_s\rangle = \langle g_1,\dots,g_t\rangle$ and $V(J) = V(f_1,\dots,f_s) = V(g_1,\dots,g_t)$. Some generating sets are "better" than others, i.e. they are a better representation of the ideal. A *Gröbner basis* is one such representation which allows to solve many polynomial decision questions.

Definition 4.1: [**Gröbner Basis**] [From [10]] For a monomial ordering $>$, a set of non-zero polynomials $G = \{g_1, g_2, \cdots, g_t\}$ contained in an ideal J, is called a Gröbner basis for $J \iff \forall f \in J,\ f \neq 0$, there exists $i \in \{1,\cdots,t\}$ such that $lm(g_i)$ divides $lm(f)$; i.e., $G = GB(J) \Leftrightarrow\ \forall f \in J : f \neq 0, \exists g_i \in G : lm(g_i) \mid lm(f)$.

Gröbner bases theory provides a *decision procedure to test for membership in an ideal*. As a consequence of Definition 4.1, the set G is a Gröbner basis of ideal J, if and only if for all $f \in J$, dividing f by polynomials of G gives 0 remainder: $G = GB(J) \iff \forall f \in J, f \xrightarrow{G}_+ 0$.

Buchberger's algorithm [11], shown in Algorithm 1, computes a Gröbner basis over a field. Given polynomials $F = \{f_1,\dots,f_s\}$, the algorithm computes the Gröbner basis $G = \{g_1,\dots,g_t\}$. In the algorithm,

$$Spoly(f,g) = \frac{L}{lt(f)} \cdot f - \frac{L}{lt(g)} \cdot g$$

where $L = \mathrm{LCM}(lm(f), lm(g))$, where $lm(f)$ is the leading monomial of f, and $lt(f)$ is the leading term of f.

ALGORITHM 1: Buchberger's Algorithm

```
Input: $F = \{f_1,\dots,f_s\}$
Output: $G = \{g_1,\dots,g_t\}$
$G := F$;
repeat
    $G' := G$;
    for each pair $\{f,g\}, f \neq g$ in $G'$ do
        $Spoly(f,g) \xrightarrow{G'}_+ r$ ;
        if $r \neq 0$ then
            $G := G \cup \{r\}$ ;
        end
    end
until $G = G'$;
```

We now describe our word-level abstraction problem formulation using Strong Nullstellensatz over $\mathbb{F}_{2^k}$, and its solution using Gröbner bases and Buchberger's algorithm.

V. Word-Level Abstraction using Gröbner basis

We are given a circuit C with k-bit inputs and outputs that performs a polynomial computation $Y = \mathcal{F}(A)$ over $\mathbb{F}_q = \mathbb{F}_{2^k}$. Let $P(x)$ be the *given* irreducible or primitive polynomial used for field construction, and let α be its root, i.e. $P(\alpha) = 0$. Note that we do not know the polynomial representation $\mathcal{F}(A)$ and our objective is to identify (the coefficients of) $\mathcal{F}(A)$. Let $\{a_0, \dots, a_{k-1}\}$ denote the primary inputs and let $\{y_0, \dots, y_{k-1}\}$ be the primary outputs of C. Then, the word-level and bit-level correspondences are:

$$A = a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1}; \quad Y = y_0 + y_1\alpha + \cdots + y_{k-1}\alpha^{k-1}; \tag{1}$$

We analyze the circuit and model all the gate-level Boolean operators as polynomials in $\mathbb{F}_2 \subset \mathbb{F}_{2^k}$. To this set of Boolean polynomials, we append the polynomials of Eqn (1) that relate the word-level and bit-level variables. We model this set of polynomials as $F = \{f_1, \dots, f_s\}$ over the ring $R = \mathbb{F}_q[x_1, \dots, x_d, Y, A]$. Here $x_1, \dots, x_d$ denote, collectively, all the bit-level variables of the circuit — i.e. primary inputs, primary outputs and the intermediate circuit variables — and Y, A the word-level variables. Denote the generated ideal as $J = \langle F \rangle \subset R$. As $Y = \mathcal{F}(A)$ is a polynomial representation of the circuit, represent this (unknown) "specification" as a polynomial $f : Y - \mathcal{F}(A)$, or as $f : Y + \mathcal{F}(A)$ and $-1 = +1$ over $\mathbb{F}_{2^k}$.

As the circuit C implements the function f, clearly f *agrees with the solutions* to $f_1 = \cdots = f_s = 0$. In computer algebra terminology, this means that f *vanishes on the variety* $V_{\mathbb{F}_q}(J)$. If f vanishes on $V_{\mathbb{F}_q}(J)$, then f is a member of the ideal $I(V_{\mathbb{F}_q}(J))$. Strong Nullstellensatz over Galois fields (Theorem 4.1) tells us that $I(V_{\mathbb{F}_q}(J)) = J + J_0$, where $J_0 = \langle x_1^q - x_1, \dots, x_d^q - x_d, Y^q - Y, A^q - A \rangle$ is the ideal of vanishing polynomials in R. Consolidating these results, we deduce that the specification polynomial $f \in (J + J_0)$.

If the specification polynomial is known, then the verification problem can be solved using membership testing of f in the ideal $(J + J_0)$ ([45] used such a formulation). We will now show that by computing a Gröbner basis of $(J + J_0)$, using a specific elimination term order, we can also identify the polynomial f which represents the function implemented by the circuit.

Reverse-Engineering f from C: The variety $V_{\mathbb{F}_q}(J)$ is the set of all consistent assignments to the nets (signals) in the circuit C. If we *project this variety on the word-level input and output variables of the circuit C, we essentially generate the function f implemented by the circuit.* Projection of varieties from d-dimensional space $\mathbb{F}_q^d$ onto a lower dimensional subspace $\mathbb{F}_q^{d-l}$ is equivalent to *eliminating l variables* from the corresponding ideal.

Definition 5.1: (**Elimination Ideal**) From [12]: Given $J = \langle f_1, \dots, f_s \rangle \subset \mathbb{F}_q[x_1, \dots, x_d]$, the lth **elimination ideal** J_l is the ideal of $\mathbb{F}_q[x_{j+1}, \dots, x_d]$ defined by

$$J_l = J \cap \mathbb{F}_q[x_{l+1}, \dots, x_d] \tag{2}$$

In other words, the lth elimination ideal does not contain variables $x_1, \dots, x_l$, nor do the generators of it. This can aid in solving systems of polynomial equations by isolating variables in a set of constraints, as is the purpose of techniques such as Gaussian elimination. Moreover, Gröbner bases may be used to generate an elimination ideal by using an "elimination order." One such ordering is a pure lexicographic ordering, which features into a theorem:

Theorem 5.1: (**Elimination Theorem**) From [12]: Let $J \subset \mathbb{F}_q[x_1, \dots, x_d]$ be an ideal and let G be a Gröbner basis of J with respect to a lex ordering where $x_1 > x_2 > \cdots > x_d$. Then for every $0 \le l \le d$, the set

$$G_l = G \cap \mathbb{F}_q[x_{l+1}, \dots, x_d] \tag{3}$$

is a Gröbner basis of the lth elimination ideal J_l.

We describe the application of elimination ideals using the following example, borrowed from [12].

Example 5.1: Consider polynomials $f_1 : x^2 - y - z - 1$; $f_2 : x - y^2 - z - 1$; $f_3 : x - y - z^2 - 1$ and ideal $J = \langle f_1, f_2, f_3 \rangle \subset \mathbb{C}[x, y, z]$. Let us compute a Gröbner basis G of J w.r.t. lex term order with $x > y > z$. Then $G = \{g_1, \dots, g_4\}$ is obtained as: $g_1 : x - y - z^2 - 1$; $g_2 : y^2 - y - z^2 - z$; $g_3 : 2yz^2 - z^4 - z^2$; $g_4 : z^6 - 4z^4 - 4z^3 - z^2$. Notice that the polynomial g_4 contains only the variable z, and it **eliminates** *variables x, y. Similarly, polynomials g_2, g_3, g_4, contain variables y, z and eliminate x. According to Theorem 5.1, $G_1 = G \cap \mathbb{C}[y, z] = \{g_2, g_3, g_4\}$ and $G_2 = G \cap \mathbb{C}[z] = \{g_4\}$ are the Gröbner bases of the 1^{st} and 2^{nd} elimination ideals of J, respectively.*

In conclusion, Gröbner basis computations w.r.t. pure lexicographic term orders can be used to eliminate variables from an ideal. The above example motivates our approach: Since we want to derive a polynomial representation from a circuit in variables Y, A, we can compute a Gröbner basis of $J + J_0$ w.r.t. an elimination order that eliminates all the (d) bit-level variables of the circuit. Then, the Gröbner basis $G_d = G \cap \mathbb{F}_q[x_1, \dots, x_d, Y, A]$ of the d^{th} elimination ideal of $(J + J_0)$ will contain polynomials in only Y, A. We now prove that the required polynomial representation will be found in G_d. First, let us formally "setup" the abstraction problem:

Problem Setup 5.1: Given a circuit C with k-bit inputs and outputs which computes a polyfunction $f : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$. Let $\{a_0, \ldots, a_{k-1}\}$ be the bit-level primary inputs and $\{y_0, \ldots, y_{k-1}\}$ be the primary outputs. Let A, Y denote the word-level input and output variables of the circuit, respectively, such that $A = a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1}$ and $Y = y_0 + \cdots + y_{k-1}\alpha^{k-1}$, where α is a primitive element of $\mathbb{F}_{2^k}$. Let $\mathcal{F}(A)$ be the (unknown) polynomial representation of the function implemented by the circuit such that $Y = \mathcal{F}(A)$.

Denote by $x_i, i = 1, \ldots, d$ all the Boolean variables of the circuit – i.e. the input, output and the intermediate variables. Let $R = \mathbb{F}_{2^k}[x_i, Y, A : i = 1, \ldots d]$ denote the ring to model the polynomials that describe the circuit functionality. Let ideal $J \subset \mathbb{F}_{2^k}[x_i, Y, A : i = 1 \ldots d]$ be generated by the bit-level and word-level polynomials of the circuit. Let $J_0 = \langle x_i^2 - x_i, Y^{2^k} - Y, A^{2^k} - A : i = 1, \ldots, d \rangle$ denote the ideal of vanishing polynomials in R. $\square$

Now, we will impose the following elimination order used for abstraction:

Definition 5.2: **Abstraction Term Order $>$:** Using the variable order $x_1 > x_2 > \cdots > x_d > Y > A$, impose a lex term order $>$ on the polynomial ring $R = \mathbb{F}_q[x_1, \ldots, x_d, Y, A]$. This elimination term order $>$ is defined as the **Abstraction Term Order**.

Theorem 5.2: **Abstraction Theorem:** Using the setup and notations from Problem Setup 5.1 above, compute a Gröbner basis G of ideal $(J + J_0)$ using the abstraction term order $>$. Then:
(i) G must contain the vanishing polynomial $A^q - A$ as the only polynomial with only A as the support variable;
(ii) G must contain a polynomial of the form $Y + \mathcal{G}(A)$; and
(iii) $Y + \mathcal{G}(A)$ is such that $\mathcal{F}(A) = \mathcal{G}(A), \forall A \in \mathbb{F}_q$. In other words, $\mathcal{G}(A)$ and $\mathcal{F}(A)$ are equal as polynomial functions over $\mathbb{F}_q$.

Proof: (i) $A^q - A$ is a given generator of J_0. Variable A is also the last variable in the abstraction term order. Moreover, A is an input to the circuit, so A is an independent variable which can take any and all values in $\mathbb{F}_{2^k}$. As a result, $G_{d+1} = G \cap \mathbb{F}_{2^k}[A] = \{A^q - A\}$.

(ii) Since $f : Y + \mathcal{F}(A)$ is a polynomial representation of the function of the circuit, $Y + \mathcal{F}(A) \in J + J_0$, as described above. Therefore, according to the definition of a Gröbner basis (Definition 4.1), the leading term of $Y + \mathcal{F}(A)$ (which is Y) should be divisible by the leading term of some polynomial $g_i \in G$. The only way $lt(g_i)$ can divide Y is when $lt(g_i) = Y$ itself. Moreover, due to our abstraction (lex) term order, $Y > A$, so this polynomial must be of the form $Y + \mathcal{G}(A)$.

(iii) As $Y = \mathcal{F}(A)$ represents the function of the circuit, $Y + \mathcal{F}(A) \in J + J_0$. Moreover, $V(J + J_0) \subset V(Y + \mathcal{F}(A))$. Project this variety $V(J + J_0)$ onto the co-ordinates corresponding to (A, Y). What we obtain is the *graph of the function* $(A) \mapsto \mathcal{F}(A)$ from $\mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$. Since $Y + \mathcal{G}(A)$ is an element of the Gröbner basis of $J + J_0$, $V(J + J_0) \subset V(Y + \mathcal{G}(A))$ too. Therefore, $Y = \mathcal{G}(A)$ gives the same function as $Y = \mathcal{F}(A)$, for all $A \in \mathbb{F}_{2^k}$. $\blacksquare$

As a consequence of Theorem 5.2, if we compute a Gröbner basis G of $J + J_0$ using the abstraction term order, we will find a polynomial of the form $Y + \mathcal{G}(A)$ in the Gröbner basis, such that $Y = \mathcal{G}(A)$ is a polynomial representation of the circuit. However, if the Gröbner basis is not reduced, it is possible to obtain multiple polynomials in G of the form $Y + \mathcal{G}_1(A), Y + \mathcal{G}_2(A), \ldots,$; all of which correspond to the same function.

Corollary 5.1: Computing a **reduced** Gröbner basis G_r of $J + J_0$, we will obtain **one and only one polynomial** in G_r of the form $Y + \mathcal{G}(A)$, such that $Y = \mathcal{G}(A)$ is the **unique, minimal, canonical** representation of the function f implemented by the circuit.

The above results trivially extend to circuits with multiple word-level input variables $A^1, \ldots, A^n$, and the canonical polynomial representation obtained by computing a reduced Gröbner basis G_r of $J + J_0$ using $>$ is of the form $Y = \mathcal{F}(A^1, \ldots, A^n)$.

VI. Research to be conducted further....

Gröbner basis Complexity: To compute a Gröbner basis for $J + J_0$ over $\mathbb{F}_q$, the following result is known [34]:

Theorem 6.1: Let $J = \langle f_1, \ldots, f_s,\ x_1^q - x_1, \ldots, x_d^q - x_d \rangle \subset \mathbb{F}_q[x_1, \ldots, x_d]$ be an ideal. The time and space complexity of Buchberger's algorithm to compute a Gröbner basis of J is bounded by $q^{O(d)}$. assuming that the length of input $f_1, \ldots, f_s$ is dominated by $q^{O(d)}$.

In our case, $q = 2^k$, and when k and d are large, this complexity may make verification infeasible. Therefore, I wish to conduct research to make this approach scalable. Talk about FGLM here, and maybe show an example corresponding to the same 2-bit multiplier circuit....... You take it up from here....

References

[1] J. Smith and G. DeMicheli, "Polynomial methods for component matching and verification", *in In Proc. ICCAD*, 1998.
[2] J. Smith and G. DeMicheli, "Polynomial methods for allocating complex components", *in Proc. Des. Auto. Test in Europe*, 1999.
[3] A. Peymandoust and G. DeMicheli, "Application of Symbolic Computer Algebra in High-Level Data-Flow Synthesis", *IEEE Trans. CAD*, vol. 22, pp. 1154–11656, 2003.

[4] S. Horeth and Drechsler, “Formal Verification of Word-Level Specifications”, *in DATE*, pp. 52–58, 1999.

[5] L. Arditi, “*BMDs can Delay the use of Theorem Proving for Verifying Arithmetic Assembly Instructions”, in Srivas, editor, *In Proc. Formal methods in CAD*. Springer-Verlag, 1996.

[6] Z. Zeng, P. Kalla, and M. J. Ciesielski, “LPSAT: A Unified Approach to RTL Satisfiability”, *in Proc. DATE*, 2001.

[7] D. Babic and M. Musuvathi, “Modular Arithmetic Decision Procedure”, Technical Report TR-2005-114, Microsoft Research, 2005.

[8] R. Brummayer and A. Biere, “Boolector: An Efficient SMT Solver for Bit-Vectors and Arrays”, *in TACAS 09, Volume 5505 of LNCS*. Springer, 2009.

[9] N. Tew, P. Kalla, N. Shekhar, and S. Gopalakrishnan, “Verification of Arithmetic Datapaths using Polynomial Function Models and Congruence Solving”, *in Proc. Intl. Conf. on Computer-Aided Design (ICCAD)*, pp. 122–128, 2008.

[10] W. W. Adams and P. Loustaunau, *An Introduction to Grobner Bases*, American Mathematical Society, 1994.

[11] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, PhD thesis, Philosophiesche Fakultät an der Leopold-Franzens-Universität, Austria, 1965.

[12] D. Cox, J. Little, and D. O’Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer, 2007.

[13] J. C. Faugére, P. Gianni, D. Lazard, and T. Mora, “Efficient computation of zero-dimentional Gröbner Basis by change of ordering”, *Journal of Symbolic Computation*, vol. 16, pp. 329–344, 1993.

[14] J. López and R. Dahab, “Improved Algorithms for Elliptic Curve Arithmetic in GF(2^n)”, *in Proceedings of the Selected Areas in Cryptography*, pp. 201–212, London, UK, UK, 1999. Springer-Verlag.

[15] R. E. Bryant, “Graph Based Algorithms for Boolean Function Manipulation”, *IEEE Trans. on Computers*, vol. C-35, pp. 677–691, August 1986.

[16] R. Drechsler, A. Sarabi, M. Theobald, B. Becker, and M.A. Perkowski, “Efficient Representation and Manipulation of Switching Functions based on Ordered Kronecker Functional Decision Diagrams”, *in Design Automation Conference*, pp. 415–419, 1994.

[17] R. E. Bryant and Y-A. Chen, “Verification of Arithmetic Functions with Binary Moment Diagrams”, *in DAC*, 95.

[18] R. Dreschler, B. Becker, and S. Ruppertz, “The K*BMD: A Verification Data Structure”, *IEEE Design & Test*, vol. 14, pp. 51–59, 1997.

[19] D. Singmaster, “On Polynomial Functions (mod m)”, *J. Number Theory*, vol. 6, pp. 345–352, 1974.

[20] Z. Chen, “On polynomial functions from Z_n to Z_m”, *Discrete Math.*, vol. 137, pp. 137–145, 1995.

[21] Z. Chen, “On polynomial functions from $Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_r}$ to Z_m”, *Discrete Math.*, vol. 162, pp. 67–76, 1996.

[22] N. Shekhar, *Equivalence Verification of Arithmetic Datapaths using Finite Ring Algebra*, PhD thesis, University of Utah, 2007.

[23] Rudolf Lidl and Harald Niederreiter, *Finite Fields*, Cambridge University Press, 1997.

[24] J. Lv, *Scalable Formal Verification of Finite Field Arithmetic Circuits using Computer Algebra Techniques*, PhD thesis, Univ. of Utah, Aug. 2012.

[25] I. Bahar, E. A. Frohm, C. M. Gaona, G. D. Hachtel, E. Macii, A. Pardo, and F. Somenzi, “Algebraic Decision Diagrams and their Applications”, *in ICCAD*, pp. 188–191, Nov. 93.

[26] E. M. Clarke, K. L. McMillan, X. Zhao, M. Fujita, and J. Yang, “Spectral Transforms for Large Boolean Functions with Applications to Technology Mapping”, *in DAC*, pp. 54–60, 93.

[27] E. M. Clarke, M. Fujita, and X. Zhao, “Hybrid Decision Diagrams - Overcoming the Limitation of MTBDDs and BMDs”, *in ICCAD*, 95.

[28] Y-T. Lai, M. Pedram, and S. B. Vrudhula, “FGILP: An ILP Solver based on Function Graphs”, *in ICCAD*, pp. 685–689, 93.

[29] Y. A. Chen and R. E. Bryant, “*PHDD: An Efficient Graph Representation for Floating Point Verification”, *in Proc. ICCAD*, 1997.

[30] M. Ciesielski, P. Kalla, and S. Askar, “Taylor Expansion Diagrams: A Canonical Representation for Verification of Data-Flow Designs”, *IEEE Transactions on Computers*, vol. 55, pp. 1188–1201, 2006.

[31] B. Alizadeh and M. Fujita, “Modular Datapath Optimization and Verification based on Modular-HED”, *IEEE Transactions CAD*, pp. 1422–1435, Sept. 2010.

[32] A. Jabir and Pradhan D., “MODD: A New Decision Diagram and Representation for Multiple Output Binary Functions”, *in Design, Automation and Test in Europe, DATE*, 2004.

[33] A. Jabir, D. Pradhan, T. Rajaprabhu, and A. Singh, “A Technique for Representing Multiple Output Binary Functions with Applications to Verification and Simulation”, *IEEE Transactions on Computers*, vol. 56, pp. 1133–1145, 2007.

[34] S. Gao, “Counting Zeros over Finite Fields with Gröbner Bases”, Master’s thesis, Carnegie Mellon University, 2009.

[35] S. Gao, A. Platzer, and E. Clarke, “Quantifier Elimination over Finite Fields with Gröbner Bases”, *in Intl. Conf. Algebraic Informatics*, 2011.

[36] G. Avrunin, “Symbolic Model Checking using Algebraic Geometry”, *in Computer Aided Verification Conference*, pp. 26–37, 1996.

[37] Y. Watanabe, N. Homma, T. Aoki, and T. Higuchi, “Application of Symbolic Computer Algebra to Arithmetic Circuit Verification”, *in International Conference on Computer Design*, pp. 25–32, October 2007.

[38] S. Sankaranarayanan, H. B. Sipma, and Z. Manna, “Non-linear Loop Invariant Generation using Grobner Bases”, *SIGPLAN Not.*, vol. 39, pp. 318–329, 2004.

[39] O. Wienand, M. Wedler, D. Stoffel, W. Kunz, and G. Gruel, “An Algebraic Approach to Proving Data Correctness in Arithmetic Datapaths”, *in Computer Aided Verification Conference*, pp. 473–486, 2008.

[40] E. Pavlenko, M. Wedler, D. Stoffel, W. Kunz, A. Dreyer, F. Seelisch, and G.-M. Greuel, “STABLE: A New QBF-BV SMT Solver for Hard Verification Problems Combining Boolean Reasoning with Computer Algebra”, *in IEEE Design, Automation and Test in Europe Conference*, pp. 155–160, 2011.

[41] L. Lastras-Montaño, P. Meany, E. Stephens, B. Trager, J. O’Conner, and L. Alves, “A new class of array codes for memory storage”, *in Proc. Information Theory and Applications Workshop*, pp. 1–10, 2011.

[42] L. Lastras, A. Lvov, B. Trager, S. Winograd, V. Paruthi, A. El-Zhein, R. Shadowen, and G. Janssen, “New Formal Verification Techniques for Algorithms over Finite Fields”, Presented at Intl. Workshop on Internation Theory and Applications. Abstract of the paper available at: http://ita.ucsd.edu/workshop/12/talks, 2012.

[43] A. Lvov, L. Lastras-Montaño, V. Paruthi, R. Shadowen, and A. El-Zein, “Formal Verification of Error Correcting Circuits using Computational Algebraic Geometry”, *in Proc. Formal Methods in Computer-Aided Design (FMCAD)*, pp. 141–148, 2012.

[44] W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann, “SINGULAR 3-1-3 — A computer algebra system for polynomial computations”, 2011, http://www.singular.uni-kl.de.

[45] J. Lv, P. Kalla, and F. Enescu, “Efficient Groebner Basis Reductions for Formal Verification of Galois Field Multipliers”, *in IEEE Design, Automation and Test in Europe*, 2012.

[46] J. Lv, P. Kalla, and F. Enescu, "Verification of Composite Galois Field Multipliers over GF($(2^m)^n$) using Computer Algebra Techniques", *in IEEE High-Level Design Validation and Test Workshop*, pp. 136–143, 2011.

[47] J. Lv, P. Kalla, and F. Enescu, "Formal Verification of Galois Field Multipliers using Computer Algebra", *in 25th IEEE International Conference on VLSI Design*, 2012.

[48] R. Zippel, "Probabilistic algorithms for sparse interpolation", *in Proc. Symp. Symbolic and Algebraic Computation*, pp. 216–226, 1979.

[49] M. Ben-Or and P. Tiwari, "A deterministic algorithm for sparse multivariate polynomial interpolation", *in Proc. Symp. Theory of Computing*, pp. 301–309, 1988.

[50] S. Javadi and M. Monagan, "On sparse polynomial interpolation over finite fields", *in Intl. Symp. Symbolic and Algebraic Computing*, 2010.

[51] Z. Zilic and Z. Vranesic, "A deterministic multivariate interpolation algorithm for small finite fields", *IEEE Trans. Computers*, vol. 51, Sept. 2002.

[52] Robert J. McEliece, *Finite Fields for Computer Scientists and Engineers*, Kluwer Academic Publishers, 1987.

[53] E. Mastrovito, "VLSI Designs for Multiplication Over Finite Fields GF(2^m)", *Lecture Notes in Computer Science*, vol. 357, pp. 297–309, 1989.

[54] Cetin K. Koc and Tolga Acar, "Montgomery Multiplication in GF(2^k)", *Designs, Codes and Cryptography*, vol. 14, pp. 57–69, April 1998.

[55] M. Knežević, K. Sakiyama, J. Fan, and I. Verbauwhede, "Modular Reduction in GF(2^n) Without Pre-Computational Phase", *in Proceedings of the International Workshop on Arithmetic of Finite Fields*, pp. 77–87, 2008.

[56] Christof Paar, "A new architecture for a parallel finite field multiplier with low complexity based on composite fields", *IEEE Transactions on Computers*, vol. 45, pp. 856–861, July 1996.