Deciding $GF(2^k)$ Arithmetic over $GF((2^m)^n)$: Exploiting Galois Field Decomposition for Efficient Symbolic Computation.

Priyank Kalla and Jinpeng Lv

I. Introduction

We have been working on verification of multiplier circuits over Galois fields $F_q = GF(q = 2^k)$. This is a practical and challenging problem because such circuits are used in Cryptography and many other computer engineering applications. To solve the verification problems, we have formulated them using some form of Gröbner basis (ideal membership) instance. Given a circuit over $GF(2^k)$, we extract the polynomials from the circuit and model these polynomials as ideal I. Then, for verification we:

- Compute a Gröbner basis G of $\langle I, I_0 \rangle$ over $GF(2^k)$, where I_0 corresponds to the ideal of vanishing polynomials of the field.
- And then we have to perform an ideal membership test: is a given polynomial $f \in \langle I, I_0 \rangle$?

This is the essense of our approach. The main message to take from here is that we need to compute a Gröbner basis of an ideal in $F_q[x_1, \ldots, x_d], q = 2^k$ and perform an ideal membership test $f \in \langle I, I_0 \rangle$?

Unfortunately, in practical applications, the field size (and thus the operand size) is large, e.g. $k = 64, 128, 256, \ldots$, and so on. For large size k, the Gröbner basis computation generates too many polynomials in the basis and runs into memory explosion. For example, if we are given a circuit that computes multiplication over $GF(2^k), k = 128$, then $GB(I, I_0)$ does not terminate, and the computer runs out of memory.

In this document, I want to introduce a research problem which is related to overcoming this limitation, using Composite field decomposition. And these research questions arise from our experience with computing Gröbner basis of ideals corresponding to circuits in $GF(2^k)$, where a non-prime k can be factorized as $k = m \cdot n$.

We had submitted a paper earlier this year, which was rejected for publication, where we were verifying that a (multiplier) circuit over the composite Galois field $GF((2^m)^n)$ was a correct implementation of multiplication $G = A \cdot B \pmod{P(x)}$ over $GF(2^k), k = m \cdot n$. Our observations were that: i) the composite field decomposition introduced a hierarchy that "simplified" the design as well as its verification; and ii) We were able to compute the Gröbner basis of the polynomials corresponding to the circuit over $GF((2^m)^n)$. For example, in one instance, $k = 1024 = 32 \times 32$ and we were able to compute Gröbner basis of the circuit over $GF((2^{32})^{32})$. However, we could not compute Gröbner basis for the corresponding circuit over $GF(2^{1024})$.

So, I am wondering whether there is a way to "exploit" this concept of composite field decomposition, and instead of solving the problem over $GF(2^k)$, *can we solve an equivalent problem over* $GF((2^m)^n)$? I am not exactly sure how to formulate the problem mathematically, but I think it looks like as follows:

Given a set of polynomials (ideal I) with coefficients in $GF(2^k)$, we derive another set of polynomials (ideal J) with coefficients in $GF((2^m)^n), k = mn$, such that $f \in I \iff f \in J$, or perhaps $f \in \langle I, I_0 \rangle \iff f \in \langle J, J_0 \rangle$.

I think it would be better to explain using some examples.

II. Multiplication over $GF(2^k)$ and over $GF((2^m)^n)$

Consider the example circuit design of a multiplier over $GF(2^k) = GF(2^4)$ and its corresponding implementation over $GF((2^2)^2)$.

Example II.1: First, let us consider the field $GF(2^4)$. We take as inputs: $A = a_0 + a_1 \cdot \alpha + a_2 \cdot \alpha^2 + a_3 \cdot \alpha^3$ and $B = b_0 + b_1 \cdot \alpha + b_2 \cdot \alpha^2 + b_3 \cdot \alpha^3$, where $A, B \in GF(2^4)$, along with the irreducible polynomial $P(x) = x^4 + x^3 + 1$. Here α is the primitive root, i.e. $P(\alpha) = 0$. We have to perform the multiplication $G = A \times B \pmod{P(x)}$. The coefficients of $A = \{a_0, \ldots, a_3\}, B = \{b_0, \ldots, b_3\}$ are in $F_2 = \{0, 1\}$. So we can perform this multiplication as shown below:

			a_3	a_2	a_1	a_0
$\times$			b_3	b_2	b_1	b_0
			$a_3 \cdot b_0$	$a_2 \cdot b_0$	$a_1 \cdot b_0$	$a_0 \cdot b_0$
		$a_3 \cdot b_1$	$a_2 \cdot b_1$	$a_1 \cdot b_1$	$a_0 \cdot b_1$	
	$a_3 \cdot b_2$	$a_2 \cdot b_2$	$a_1 \cdot b_2$	$a_0 \cdot b_2$		
$a_3 \cdot b_3$	$a_2 \cdot b_3$	$a_1 \cdot b_3$	$a_0 \cdot b_3$			
s_6	s_5	s_4	s_3	s_2	s_1	s_0

In polynomial expression, we have the result as: $S = s_0 + s_1 \cdot \alpha + s_2 \cdot \alpha^2 + s_3 \cdot \alpha^3 + s_4 \cdot \alpha^4 + s_5 \cdot \alpha^5 + s_6 \cdot \alpha^6$, where,

$$s_0 = a_0 \cdot b_0 \quad (1)$$

$$s_1 = a_0 \cdot b_1 + a_1 \cdot b_0 \quad (2)$$

$$s_2 = a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0 \quad (3)$$

$$s_3 = a_3 \cdot b_0 + a_2 \cdot b_1 + a_1 \cdot b_2 + a_0 \cdot b_3 \quad (4)$$

$$s_4 = a_3 \cdot b_1 + a_2 \cdot b_2 + a_1 \cdot b_3 \quad (5)$$

$$s_5 = a_3 \cdot b_2 + a_2 \cdot b_3 \quad (6)$$

$$s_6 = a_3 \cdot b_3 \quad (7)$$

and so on. Here the multiply "$\cdot$" and add "$+$" operations are performed modulo 2, so they can be implemented in a circuit using AND and XOR gates. However, the result is yet to be reduced modulo the irreducible/primitive polynomial $P(x) = x^4 + x^3 + 1$. This is shown below, where the final output of the circuit is denoted by $G = g_3\alpha^3 + g_2\alpha^2 + g_1\alpha + g_0$.

s_6	s_5	s_4	s_3	s_2	s_1	s_0		
			s_4	0	0	s_4	$\Leftarrow$	$s_4 \cdot \alpha^4 \pmod{P(\alpha)} = s_4 \cdot (\alpha^3 + 1)$
			s_5	0	s_5	s_5	$\Leftarrow$	$s_5 \cdot \alpha^5 \pmod{P(\alpha)} = s_5 \cdot (\alpha^3 + \alpha + 1)$
		$+$	s_6	s_6	s_6	s_6	$\Leftarrow$	$s_6 \cdot \alpha^6 \pmod{P(\alpha)} = s_6 \cdot (\alpha^3 + \alpha^2 + \alpha + 1)$
			g_3	g_2	g_1	g_0		

The final result of the circuit is: $G = g_0 + g_1\alpha + g_2\alpha^2 + g_3\alpha^3$; where

$$g_0 = s_0 + s_4 + s_5 + s_6 \quad (8)$$

$$g_1 = s_1 + s_5 + s_6 \quad (9)$$

$$g_2 = s_2 + s_6 \quad (10)$$

$$g_3 = s_3 + s_4 + s_5 + s_6 \quad (11)$$

To verify that the circuit correctly implements the multiplication, we do the following:

- We need to "extract" the polynomials from the above circuit, and represent them with ideal $I \subset F_{2^4}[A, B, a_0, \ldots, a_3, b_0, \ldots, b_3, s_0, \ldots, s_6, g_0, \ldots, g_3, G]$. In the above example, the ideal I consists of all the following polynomials:

$$
\begin{aligned}
A &+ a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0, && (12)\\
B &+ b_3\alpha^3 + b_2\alpha^2 + b_1\alpha + b_0, && (13)\\
s_0 &+ a_0 \cdot b_0, && (14)\\
s_1 &+ a_0 \cdot b_1 + a_1 \cdot b_0, && (15)\\
s_2 &+ a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0, && (16)\\
s_3 &+ a_3 \cdot b_0 + a_2 \cdot b_1 + a_1 \cdot b_2 + a_0 \cdot b_3, && (17)\\
s_4 &+ a_3 \cdot b_1 + a_2 \cdot b_2 + a_1 \cdot b_3, && (18)\\
s_5 &+ a_3 \cdot b_2 + a_2 \cdot b_3, && (19)\\
s_6 &+ a_3 \cdot b_3, && (20)\\
g_0 &+ s_0 + s_4 + s_5 + s_6, && (21)\\
g_1 &+ s_1 + s_5 + s_6, && (22)\\
g_2 &+ s_2 + s_6, && (23)\\
g_3 &+ s_3 + s_4 + s_5 + s_6, && (24)\\
G &+ g_0 + g_1\alpha + g_2\alpha^2 + g_3\alpha^3 && (25)
\end{aligned}
$$

Notice, in the above polynomials, $A, B, G \in F_{2^4}$ whereas $a_0, \ldots, a_3, b_0, \ldots, b_3, s_0, \ldots, s_6, g_0, \ldots, g_3 \in F_2 \subset F_{2^4}$, and α is the primitive root of F_{2^4}. The coefficients are therefore in F_{2^4}.

- Then we generate ideal $I_0 = \langle A^q - A, B^q - B, a_0^q - a_0, \ldots, G^q - G \rangle$.
- The polynomial $f = G + A \cdot B$ is our specification polynomial.
- We need to test if f vanishes over the variety $V(I)$; or if $f \in I(V(I)) = \langle I, I_0 \rangle$.
- For this, we need to compute the Gröbner basis of $\langle I, I_0 \rangle$ so that we can perform this membership test.
- Now assume that this problem is too large because F_q is very large and the Gröbner basis cannot be computed.

A. Composite Field Decomposition

Instead of performing the multiplication over $GF(2^4)$, we can now design the circuit over $GF((2^2)^2)$. While we have discussed this before, just for reference, I am describing the construction of the composite field multiplier again.

Recall that to construct a finite field $GF(2^k)$, we need a primitive polynomial $P(x) \in F_2[x]$ of degree k. Similarly, to construct $GF((2^m)^n)$, we require a primitive polynomial, of degree n, with coefficients from the ground field $GF(2^m)$. Given $GF(2^k)$ and $P(x)$, the primitive polynomial of the composite field can be easily derived. We will use the following notation:

- Let $P(x)$ denote the given primitive polynomial of general field GF(2^k), and α be the primitive root, i.e. $P(\alpha) = 0$.
- Let $Q(x)$ denote the primitive polynomial of ground field GF(2^m), and β be the primitive root of $GF(2^m)$, i.e. $Q(\beta) = 0$. Note that $Q(x)$ is a degree m primitive polynomial over $GF(2)$ so it is also known.
- Let $R(x)$ denote the primitive polynomial of composite field GF($(2^m)^n$), and γ be the primitive root, i.e. $R(\gamma) = 0$. This polynomial $R(x)$ has to be derived.

Lemma 1: From [1]: Let $GF(2^k)$ be decomposed as $GF((2^m)^n)$ where $k = m \cdot n$. Let γ be the primitive root of the field $GF((2^m)^n)$. Then

$$R(x) = \prod_{i=0}^{i=n-1} (x + \gamma^{2^{m \cdot i}}) \tag{26}$$

Since $GF(2^k)$ is isomorphic to $GF((2^m)^n)$, α and γ are actually the same elements. Therefore $P(x)$ and $R(x)$ are minimal polynomials of the same element, but w.r.t. different ground fields, $GF(2)$ and $GF(2^m)$ respectively [1]. Now let us consider the representation of an element A in $GF(2^k)$ and its corresponding representation in the composite field.

- Any element $A \in GF(2^k)$ is represented as:

$$A = \sum_{i=0}^{i=k-1} a_i \cdot \alpha^i, a_i \in GF(2), \text{and} P(\alpha) = 0 \tag{27}$$

- The same element $A \in GF((2^m)^n)$ is represented as:

$$A = \sum_{i=0}^{i=n-1} A_i \cdot \gamma^i, A_i \in GF(2^m), \text{and} R(\gamma) = 0 \tag{28}$$

- Now we have to represent the element A_i from above in the ground field $GF(2^m)$:

$$A_i = \sum_{j=0}^{j=m-1} a_{ij} \cdot \beta^j, a_{ij} \in GF(2), \text{and} Q(\beta) = 0 \tag{29}$$

Now we need to find the relationship between the primitive roots α and β (or between γ and β, since $\alpha = \gamma$), so as to be able to map the elements from $GF(2^k)$ to $GF((2^m)^n)$. We have the following result [1]:

Theorem 1: For $\gamma \in GF((2^m)^n)$, and $\beta = \gamma^\omega$, where $\omega = (2^{m \cdot n} - 1)/(2^m - 1)$, then we have $\beta \in GF(2^m)$. In other words:

$$\beta = \alpha^{(2^{m \cdot n}-1)/(2^m-1)} = \gamma^{(2^{m \cdot n}-1)/(2^m-1)} \tag{30}$$

The above result states the following: Since γ is a primitive root, it can be used to generate all the non-zero elements of $GF((2^m)^n)$. Moreover, β is a primitive root of the ground field $GF(2^m)$, which is a sub-field of $GF((2^m)^n)$ (i.e. $GF(2^m) \subset GF((2^m)^n)$); so $\beta \in GF((2^m)^n)$. Therefore an exponent of γ can be used to generate β as $\beta = \gamma^\omega$, where ω is given in Theorem 1. Now we know all the relationships between α, β, γ, and we are ready to perform the decomposition.

Example II.2: As an example, let us reconsider the field $GF(2^4)$ and decompose it as $GF((2^2)^2)$. Let $P(x) = x^4 + x^3 + 1$ and $P(\alpha) = 0$. We need to perform the following steps:

1. Derivation of $R(x)$:

$$\begin{aligned} R(x) &= \prod_{i=0}^{i=1}(x + \gamma^{2^{2 \cdot i}}) \\ &= (x + \gamma) \cdot (x + \gamma^{2^2}) \\ &= x^2 + (\gamma^4 + \gamma) \cdot x + \gamma^5 \end{aligned} \tag{31}$$

Notice that $R(\gamma) = \gamma^2 + (\gamma^4 + \gamma) \cdot \gamma + \gamma^5 = 0$.

2. Representation of element $A \in GF((2^2)^2)$:

$$\begin{aligned} A &= \sum_{i=0}^{i=1} A_i \cdot \gamma^i, A_i \in GF(2^2) \\ &= A_0 + A_1 \cdot \gamma \end{aligned} \tag{32}$$

3. Representation of A_0, A_1 in $GF(2^2)$:

$$A_0 = a_{00} + a_{01} \cdot \beta$$
$$A_1 = a_{10} + a_{11} \cdot \beta \tag{33}$$

where $a_{ij} \in GF(2)$. $Q(x)$ can be any degree $m = 2$ primitive polynomial in the ground field GF(2^2). Let us take $Q(x) = x^2 + x + 1$.

4. Now we can substitute A_0, A_1 into A as follows:

$$\begin{aligned} A &= \sum_{i=0}^{i=1}(\sum_{j=0}^{j=1} a_{ij} \cdot \beta^j) \cdot \gamma^i \\ &= a_{00} + a_{01} \cdot \beta + (a_{10} + a_{11} \cdot \beta) \cdot \gamma \end{aligned} \tag{34}$$

where each $a_{ij} \in GF(2)$. From Eqn. (30), we have: $\beta = \alpha^5 = \gamma^5$. We then substitute β and γ with α to obtain:

$$\begin{aligned} A &= \sum_{i=0}^{i=1}(\sum_{j=0}^{j=1} a_{ij} \cdot \beta^j) \cdot \gamma^i \\ &= a_{00} + a_{01} \cdot \alpha^5 + (a_{10} + a_{11} \cdot \alpha^5) \cdot \alpha \end{aligned}$$

Since $P(x) = x^4 + x^3 + 1$ with $P(\alpha) = 0$, we have

$$A \pmod{P(\alpha)} = a_{00} + a_{01} + a_{11} + (a_{01} + a_{10} + a_{11}) \cdot \alpha + a_{11} \cdot \alpha^2 + (a_{01} + a_{11}) \cdot \alpha^3 \tag{35}$$

5. The same element $A \in GF(2^4)$ is represented as:

$$A = a_0 + a_1 \cdot \alpha + a_2 \cdot \alpha^2 + a_3 \cdot \alpha^3 \tag{36}$$

6. Since Eqns. 35 and 36 represent the same element, we can match the coefficients of the the polynomials to obtain:

$$\begin{aligned} a_0 &= a_{00} + a_{01} + a_{11} \\ a_1 &= a_{01} + a_{10} + a_{11} \\ a_2 &= a_{11} \\ a_3 &= a_{01} + a_{11} \end{aligned}$$

This mapping can also be reversed and represented as a matrix T:

$$\begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Now we have successfully derived the composite field representation $GF((2^2)^2)$ from $GF(2^4)$. The element $A \in GF(2^4)$ is represented as $A = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$, where $P(\alpha) = 0$. The same element A is represented in $GF((2^2)^2)$ as:

$$\begin{aligned} A &= A_0 + A_1 \cdot \alpha \\ A_0 &= a_{00} + a_{01} \cdot \alpha^5 \\ A_1 &= a_{10} + a_{11} \cdot \alpha^5 \\ a_{00} &= a_0 + a_3 \\ a_{01} &= a_2 + a_3 \\ a_{10} &= a_1 + a_3 \\ a_{11} &= a_2 \end{aligned}$$

In the above equations, $\alpha = \gamma$ and $R(\gamma) = 0$.

Multiplication $A \cdot B \pmod{P(x)}$ over $GF(2^4)$ can now be performed over the decomposition $GF((2^2)^2)$, where $A = A_0 + A_1\gamma, B = B_0 + B_1\gamma$ and the modulus is taken over $R(\gamma)$. Such a design is shown in Fig. 1, where $a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3$ are primary inputs. After a suitable transformation, *composite field* inputs are obtained as $a_{00}, a_{01}, a_{10}, a_{11}, b_{00}, b_{01}, b_{10}, b_{11}$. A_0, A_1, B_0, B_1 are 2-bit buses. Correspondingly, each block in Fig.1 internally represents a 2-bit operation: $\times$ represents 2-bit *multiplication* and $+$ represents 2-bit *addition* over the ground field.

B. Verification of the composite field multiplier

We can now verify whether the implementation of Fig. 1 correctly implements the multiplication $A \cdot B \pmod{P(x)}$. We can do this hierarchically. First we can verify the computation at the high-level at $GF((2^2)^2)$, and then verify the adders and multipliers over the ground field. We will analyze the multiplication over $GF((2^2)^2)$ as follows:

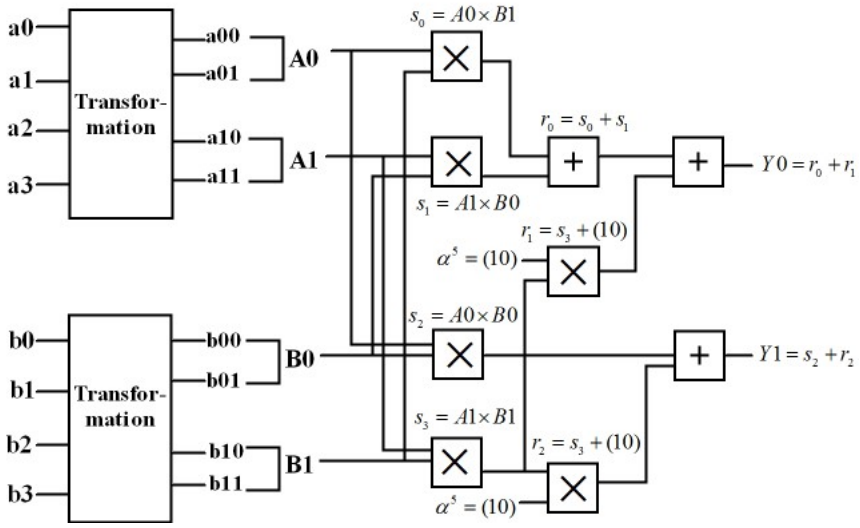

Fig. 1. *Mastrovito* multiplier over GF($(2^2)^2$)

$$\begin{array}{ccc} & A_1 & A_0 \\ \times & B_1 & B_0 \\ \hline & A_1 \cdot B_0 & A_0 \cdot B_0 \\ A_1 \cdot B_1 & A_0 \cdot B_1 & \times \\ \hline S_2 & S_1 & S_0 \end{array}$$

Here, $S_0 = A_0 \cdot B_0,\ S_1 = A_0 \cdot B_1 + A_1 \cdot B_0,\ S_2 = A_1 \cdot B_1$, and $S = S_0 + S_1\gamma + S_2\gamma^2$. Now reduce S modulo the primitive polynomial R of the composite field, where $R(x) = x^2 + (\gamma^4 + \gamma) \cdot x + \gamma^5$ and $R(\gamma) = 0$. Then we have the circuit output $Y = Y_0 + Y_1\gamma$, where $Y_0 = S_0 + S_2\gamma^5$ and $Y_1 = S_1 + S_2(\gamma^4 + \gamma)$.

Corresponding to the computation in the figure, we can generate an ideal J which is much "simpler" than the ideal I generated earlier. The ideal J (in the composite field) is:

$$A + A_0 + A_1 \cdot \gamma, \tag{37}$$

$$B + B_0 + B_1\gamma, \tag{38}$$

$$S_0 + A_0 \cdot B_0, \tag{39}$$

$$S_1 + A_0 \cdot B_1 + A_1 \cdot B_0, \tag{40}$$

$$S_2 + A_1 \cdot B_1, \tag{41}$$

$$Y_0 + S_0 + S_2\gamma^5, \tag{42}$$

$$Y_1 + S_1 + S_2(\gamma^4 + \gamma), \tag{43}$$

$$Y + Y_0 + Y_1\gamma \tag{44}$$

This ideal $J \subset F_q[A, B, Y, A_0, A_1, B_0, B_1, S_0, S_1, S_2, Y_0, Y_1]$ where $F_q = GF((2^m)^n)$. In my view, this ideal J "looks simpler" and smaller, and our experiments have shown that the Gröbner basis of such an ideal can be computed over $GF((2^m)^n)$. So our verification problem is now formulated as testing whether the specification polynomial $f : Y + A \cdot B$ is a member of the ideal $I(V(J)) = \langle J, J_0 \rangle$ over $GF((2^m)^n)$ with $R(x)$ as the primitive polynomial of the composite field and $R(\gamma) = 0$.

III. So what is the research problem?

In the above example, we actually generated, or derived, a multiplier circuit (and hence a set of polynomial equations) over $GF((2^m)^n)$. I would like to solve a somewhat opposite problem, which I re-state here.

Given a set of polynomials (ideal I) with coefficients in $GF(2^k)$, we derive another set of polynomials (ideal J) with coefficients in $GF((2^m)^n), k = mn$, such that $f \in I \iff f \in J$, or perhaps $f \in \langle I, I_0 \rangle \iff f \in \langle J, J_0 \rangle$.

Corresponding to the above examples of ideals I and J, if I were to give you Equations (12)-(25) corresponding to ideal I over the field representation $GF(2^k)$, would you be able to derive corresponding Equations (37)-(44) for ideal J over the field representation $GF((2^m)^n)$?

You may assume that the ideals correspond to some circuit. The circuit will have inputs $A, B \in F_q$ and an output $G \in F_q$, where $q = 2^k = 2^{mn}$. You may also assume that the primitive polynomials $P(x), R(x)$ of $GF((2^k)), GF((2^m)^n)$, respectively, are given, along with primitive

roots α, γ. So, we will have: $A = a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1} = A_0 + A_1\gamma + \cdots + A_{n-1}\gamma^{n-1}$. Similarly for the other input B and the output G we will have corresponding representations w.r.t. the ground fields. However, we will have to derive the rest of the polynomials that connect the inputs to the outputs – and represent them over the composite field. Ideal I will be given. Variable A, B, G will be common to both ideals, but it looks like the rest of the variables may be different.

Do you think such a problem is solvable? This problem sparked my interest in understanding the concept of sub-algebra. If $GF(2^m) \subset GF((2^m)^n)$, or a "sub-field", is it also a sub-algebra? And, by the way, I still haven't understood the concept of sub-algebra. In an email, you have given me a mathematical explanation of it – but I think I need a more intuitive explanation of it. We should talk sometime soon.

REFERENCES

[1] Berk Sunar, Erkay Savas, and etin K. Ko, "Constructing Composite Field Representations for Efficient Conversion", *IEEE Transactions on Computers*, vol. 52, pp. 1391–1398, November 2003.

[2] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties and Algorithms* An Introduction to Computational Algebraic Geometry and Commutative Algebra, Springer-Verlag, 1997.

[3] S. Gao, "Counting Zeros over Finite Fields with Gröbner Bases", Master's thesis, Carnegie Mellon University, 2009.