Resolving Unknown Component In Finite Field Arithmetic Circuits Using Computer Algebra Methods

Vikas Rao

I. Theory and Procedure

Consider a specification polynomial f and its circuit implementation C, modeled as polynomials $F = \{f_1, \ldots, f_s\} \in \mathbb{F}_q[x_1, \ldots, x_n]$. Generator of polynomials is given as $J = \langle F \rangle$, while J_0 is the set of all vanishing polynomials. Let us consider RTTO>for the circuit. We will assume $f_i : 1 \le i \le s$ to be the unknown component which is of the special form:

$$f_i = x_i + P \tag{1}$$

where x_i is the leading monomial, and P is the tail representing desired solution in variables: x_j s.t. $x_i > x_j$ in the order.

For a correct implementation, specification f should vanish on the variety of ideal generated by the circuit polynomials i.e., f will be in the ideal generated by the circuit:

$$f \in J + J_0; f \in \langle f_1, .., f_s \rangle + \langle x_l^q - x_l \rangle; 1 \le l \le n \tag{2}$$

Using Ideal membership testing, we can rewrite f in terms of its generators as:

$$f = h_s f_s + h_{s-1} f_{s-1} + \cdots + h_i f_i + \cdots + h_1 f_1 + \sum_{l=1}^{n} H_l \langle x_l^q - x_l \rangle$$

where H_l are arbitrary elements from $\mathbb{F}_q$.

From equation 1:

$$f = h_s f_s + h_{s-1} f_{s-1} + \cdots + h_i x_i + h_i P + \cdots + h_1 f_1 + \sum_{l=1}^{n} H_l \langle x_l^q - x_l \rangle$$

$$f - h_s f_s - \cdots - h_i x_i = h_i P + \cdots + h_1 f_1 + \sum_{l=1}^{n} H_l \langle x_l^q - x_l \rangle$$

$$f - h_s f_s - \cdots - h_i x_i \in \langle h_i, f_{i-1}, \ldots, f_1, x_l^q - x_l \rangle$$

We shall call the intermediate remainder computed on the left hand side as g.

$$g \in \langle h_i, f_{i-1}, \ldots, f_1, x_l^q - x_l \rangle \tag{3}$$

Given polynomials $h_i, g, f_{i-1}, \ldots, f_1$, we compute $h_i^{'} = P$ such that:

$$g = h_i^{'} h_i + h_{i-1}^{'} f_{i-1} + \cdots + h_1^{'} f_1 + \sum_{l=1}^{n} H_l^{'} \langle x_l^q - x_l \rangle$$

The computed $h_i^{'} = P$ is a solution to the function implemented by the unknown gate. This linear combination computation is done using $lift$ implementation in SINGULAR[**?**].

A. computing all solutions space of P

Despite being a correct solution, the above approach doesn't guarantee the solution to be in the immediate support variables of f_i due to RTTO>. To determine a solution in immediate support variable set x_j of f_i, we use an elimination term order for the variables x_i followed by x_j. We can then compute a GB using this elimination term order with the intermediate solution P added as tail of f_i. This GB will have one and only one polynomial which is of the form $x_i + \mathcal{F}(x_j)$, where $\mathcal{F}$ is the function implemented by the gate, and is the most desired solution.

Since we found two solutions, it is given that P is not unique. We can explore more such solutions which might satisfy the unknown component functionality. Given P as one of the solutions, under RTTO> we have:

$$g = P * h_i + h_{i-1}^{'} f_{i-1} + \cdots + h_1^{'} f_1 + \sum_{l=1}^{n} H_l^{'} \langle x_l^q - x_l \rangle;$$

Since g can be computed as any linear combination of polynomials, we can rewrite the equation as:

$$P * h_i + h_{i-1}^{'} f_{i-1} + \cdots + h_1^{'} f_1 + \sum_{l=1}^{n} H_l^{'} \langle x_l^q - x_l \rangle = P^{'} * h_i + h_{i-1}^{''} f_{i-1} + \cdots + h_1^{''} f_1 + \sum_{l=1}^{n} H_l^{''} \langle x_l^q - x_l \rangle;$$

Rearranging the terms:

$$(P - P^{'}) h_i = (h_{i-1}^{'} - h_{i-1}^{''}) f_{i-1} + \cdots + (h_1^{'} - h_1^{''}) f_1 + (\sum_{l=1}^{n} H_l^{'} - \sum_{l=1}^{n} H_l^{''}) x_l^q - x_l;$$

$$(P - P^{'}) h_i \in \langle f_{i-1}, \ldots, f_1, x_l^q - x_l \rangle;$$

By definition of Quotient of Ideals:

$$P - P^{'} \in \langle f_{i-1}, \ldots, f_1, x_l^q - x_l \rangle : h_i; \tag{4}$$

There can be many $P^{'}$ which might satisfy the above membership test. We can pick any polynomial from the quotient operation, add the previous solution P and compute a new $P^{'}$. All such $P^{'}$ computed are valid solutions and will satisfy the membership test with specification polynomial f.

We will also have cases, when h_i ends up being a constant, in which case $lift$ returns g itself as a solution $h_i^{'}$. To arrive at a implementable solution, we divide $h_i^{'}$ by the constant h_i(multiply the inverse of h_i) and reduce the result by rest of the input polynomials$\{f_{i-1}, \ldots, f_1\}$.

$$h_i^{'} * h_i^{-1} \xrightarrow{f_{i-1}} \xrightarrow{f_{i-2}} \ldots \xrightarrow{f_1} P \tag{5}$$