I. Theory and Procedure

Example I.1. Consider the buggy implementation of a 2-bit mastrovito multiplier as shown in Figure 1. The system is modeled over the ring $R = \mathbb{F}_4[a_0, b_0, a_1, b_1, s_0, s_1, s_2, s_3, s_4, s_5, e_0, e_1, e_2, e_3, r_0, z_0, z_1, Z, A, B]$.

The multiplier specification is given as $f : Z + A \cdot B$.

A. Problem setup

1) Field construction: $\mathbb{F}_4 = \mathbb{F}_2[X]$ (mod $\mathcal{P}$); where $\mathcal{P} = X^2 + X + 1$ is the primitive polynomial used.
2) $Z = z_0 + \alpha z_1; A = a_0 + \alpha a_1; B = b_0 + \alpha b_1$; are the word level polynomials, and α is the root of primitive polynomial s.t. $\mathcal{P}(\alpha) = 0$.

Based on the circuit topology, RTTO$>$ with variable order: $\{Z\} > \{A > B\} > \{z_0 > z_1\} > \{r_0\} > \{e_0 > e_1\} > \{e_2\} > \{e_3\} > \{s_0 > s_1 > s_2 > s_3 > s_4 > s_5\} > \{a_0 > a_1 > b_0 > b_1\}$

Let F be the set of all polynomials implementing the circuit which is given as:

$f_1 : Z + z_0 + \alpha z_1$; $f_9 : e_2 + e_3 + s_4$;
$f_2 : A + a_0 + \alpha a_1$; $f_{10} : e_3 + b_0 + s_3$;
$f_3 : B + b_0 + \alpha b_1$; $f_{11} : s_0 + a_0 b_0$;
$f_4 : z_0 + s_0 + e_0$; $f_{12} : s_1 + a_1 b_1$;
$f_5 : z_1 + e_0 + r_0$; $f_{13} : s_2 + a_1 b_0$;
$f_6 : r_0 + e_1 + s_5$; $f_{14} : s_3 + a_0 + b_0 + a_0 b_0$;
$f_7 : e_0 + s_1 e_2$; $f_{15} : s_4 + b_0 + 1$;
$f_8 : e_1 + s_2 e_2$; $f_{16} : s_5 + a_0 b_1$;

For the ease of explanation, we have taken a single gate bug as our fault model. As shown in the Figure 1, the marked gate f_{10} is the buggy XOR gate replacing the original AND gate.

Let $J_0 = \langle x_l^4 - x_l \rangle$ denote the ideal of vanishing polynomials in R. Given the RTTO¿ order, we will have ideal of vanishing polynomials J_0 for primary inputs only.

$f_{17} : a_0^2 + a_0$;
$f_{18} : a_1^2 + a_1$;
$f_{19} : b_0^2 + b_0$;
$f_{20} : b_1^2 + b_1$;

Then $F = \{f_1, \ldots, f_{16}\}, J = \langle F \rangle = \langle f_1, \ldots, f_{16} \rangle$

B. Verification

For a correct implementation, the specification f should be in $J + J_0$.

$f \in \langle f_1, f_2, f_3, \ldots, f_{16} \rangle + J_0$

$f \xrightarrow{GB(J+J_0)} (\alpha+1)a_0a_1b_1b_0 + (\alpha+1)a_0a_1b_1 + (\alpha+1)a_1b_1b_0 + (\alpha)a_1b_0$

Since, the remainder is non zero, the circuit doesn't implement the specification and needs to be debugged.

C. Remainder partition and cone pruning

Given the elimination order under RTTO, the remainder will contain variables only from primary inputs. We will group these monomials based on their coefficients and record all the group coefficients.

$r = (\alpha+1)a_0a_1b_1b_0 + (\alpha+1)a_0a_1b_1 + (\alpha+1)a_1b_1b_0 + (\alpha)a_1b_0$

$r = \alpha*(a_0a_1b_1b_0 + a_0a_1b_1 + a_1b_1b_0 + a_1b_0) + 1*(a_0a_1b_1b_0 + a_0a_1b_1 + a_1b_1b_0)$

$coeffs = \{\alpha, 1\}$

Since the remainder was derived by reducing primary outputs, the the recorded coefficients represent the coefficients of outputs where the bug got propagated. By matching the recorded coefficients with the coefficients of outputs, we will derive the list of all affected outputs.

$coefficient(z_0) = 1$; $coefficient(z_1) = \alpha$

Since we have both $\{1, \alpha\}$ in the coefficient record($coeffs$), all the outputs (z_0, z_1) are affected and their respective cones need to be checked for rectification.

$affected\_outputs = \{z_0, z_1\}$

For a single output function, all the nets in the circuit are potential rectifiable nets since it has single coefficient. In case of multi-output, a single fix rectification might exist only at the intersection of all the buggy cones as the error propagation is affecting all the outputs marked by the remainder coefficients.

logical cones of each outputs are given as $cone_{z_0} = (s_4, s_3, s_1, s_0, e_3, e_2, e_0, z_0)$

$cone_{z_1} = (s_5, s_4, s_3, s_2, s_1, e_3, e_2, e_1, e_0, r_0, z_1)$

$prune\_cone = cone_{z_0} \cap cone_{z_1} = \{s_4, s_3, s_2, s_1, e_3, e_2, e_0\}$

D. Rectification check

We will be checking for a single fix rectification within the pruned cone by sweeping the nets from primary input side in the topological order of the circuit. This is to ensure that we try and find a rectification point as early as possible in the topology. Given the highly irredundant nature of the finite field benchmarks, most of the circuits will allow a rectification fix early in the topology, if one exists.

Based on the circuit topology, we will check for a single fix rectification existence at given nets in the order($\{s_4 > s_3 > s_2 > s_1 > e_3 > e_2 > e_0\}$). We will perform the rectification check in the topological order until we find a net which satisfies the single fix rectification condition or until we exhaust the potential rectifiable nets. In the former case we return the net where a single fix rectification exists, while in the latter case we exit the program indicating the absence of single fix rectification for the given bugs.

For checking the existence of rectification for the net under consideration, we will form two ideals (J_L, J_H) with the net polynomial modified as shown below.

Since (s_4) is the first net to be checked for a fix, we will mark the polynomial f_{15} which has leading term s_4 for modification.

$J_L = \langle f_1, f_2 \ldots f_{15} : s_4 + 1 \ldots f_{16} \rangle$

$J_H = \langle f_1, f_2 \ldots f_{15} : s_4 \ldots f_{16} \rangle$

By reducing spec using the above ideals we derive the remainders for the respective ideals.

$r_L = f \xrightarrow{J_L} (\alpha+1)a_0a_1b_1b_0 + (\alpha+1)a_0a_1b_1$

$r_H = f \xrightarrow{J_H} (\alpha+1)a_0a_1b_1b_0 + (\alpha+1)a_0a_1b_1 + (\alpha+1)a_1b_1 + (\alpha)a_1b_0$

From theorem **??**-

$G_r = Grobner\_basis((r_L * r_H) + J_0)$

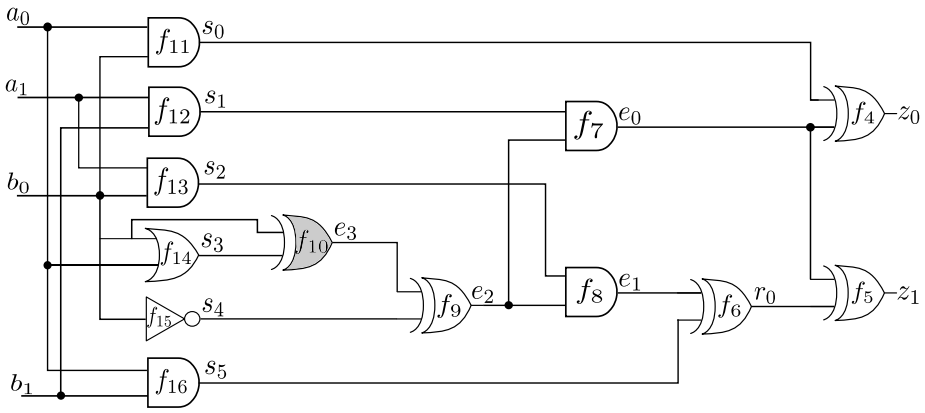

Fig. 1: Buggy 2-bit mastrovito multiplier with redundancy

The computed G_r for rectification check at net s_4 is given as:

$G_r[1] = b_0^2 + b_0; G_r[2] = b_1^2 + b_1;$
$G_r[3] = a_1^2 + a_1; G_r[4] = a_0^2 + a_0$

Since the computed product of ideals is equal to the ideal of vanishing polynomials, a single fix rectification exists at net s_4.

For the sake of comparison if a similar check was performed at net s_1, then the rectification check results would be as shown:

$J_L = \langle f_1, f_2 \dots f_{12} : s_1 + 1 \dots f_{16} \rangle$
$J_H = \langle f_1, f_2 \dots f_{12} : s_1 4 \dots f_{16} \rangle$
$r_L = f \xrightarrow{J_L} (\alpha+1)(a_0b_0 + a_0 + a_1b_1 + b_0 + 1) + (\alpha)a_1b_0$
$r_H = f \xrightarrow{J_H} (\alpha+1)a_1b_1 + (\alpha)a_1b_0$
$G_r = Grobner\_basis((r_L * r_H) + J_0)$

The computed G_r for check at net s_1 is given as:

$G_r[1] = b_0^2 + b_0; G_r[2] = b_1^2 + b_1;$
$G_r[3] = a_1b_0; G_r[4] = a_1^2 + a_1;$
$G_r[5] = a_0a_1b_1 + (\alpha+1)a_0a_1b_0^2 + a_0a_1b_0;$
$G_r[6] = a_0^2 + a_0$

Since the computed product of ideals is not equal to the ideal of vanishing polynomials, a single fix rectification does not exist at net s_1.

E. Correction function computation

For the sake of simplicity, this example will show the correction function computation at net(e_3). To start with, we will mark the gate f_{10} as the *unknown component* in the design which is of the form $f_{10} = e_3 + P$, where P is the unknown function to be implemented by the gate. We know that under RTTO $>$, the given set of circuit polynomials F itself form a GB. Hence to compute r, we start reducing the specification polynomial f using polynomials from $\langle J + J_0 \rangle$.

We will use the following notations for reduction: '[]' to represent quotient-h_j's, '()' to represent divisor-f_j's, and '{}' to represent the partial remainder of every reduction step-fp_j's.

$$f \xrightarrow{f_1} [1](Z + z_0 + \alpha z_1) + \underbrace{\{AB + z_0 + \alpha z_1\}}_{fp_1}$$

$$fp_1 \xrightarrow{f_2} [B](A + a_0 + \alpha a_1) + \underbrace{\{Ba_0 + \alpha Ba_1 + z_0 + \alpha z_1\}}_{fp_2}$$

$$\underbrace{fp_2 \xrightarrow{f_3} [a_0 + \alpha a_1](B + b_0 + \alpha b_1) + \{z_0 + \alpha z_1 + \alpha a_0 b_1 + a_0 b_0 + (\alpha+1)a_1 b_1 + \alpha a_1 b_0\}}_{fp_3}$$

$$fp_3 \xrightarrow{f_4} [1](z_0 + e_0 + s_0) + \underbrace{\{\alpha z_1 + e_0 + s_0 + \alpha a_0 b_1 + a_0 b_0 + (\alpha+1)a_1 b_1 + \alpha a_1 b_0\}}_{fp_4}$$

$$fp_4 \xrightarrow{f_5} [\alpha](z_1 + r_0 + e_0) + \underbrace{\{\alpha z_1 + e_0 + s_0 + \alpha a_0 b_1 + a_0 b_0 + (\alpha+1)a_1 b_1 + \alpha a_1 b_0\}}_{fp_5}$$

$$\underbrace{fp_5 \xrightarrow{f_6} [\alpha](r_0 + e_1 + s_5) + \{(\alpha+1)e_0 + \alpha e_1 + s_0 + \alpha s_5 + \alpha a_0 b_1 + a_0 b_0 + (\alpha+1)a_1 b_1 + \alpha a_1 b_0\}}_{fp_6}$$

$$\underbrace{fp_6 \xrightarrow{f_7} [\alpha + 1](e_0 + e_2 * s_1) + \{\alpha e_1 + (\alpha+1)e_2 s_1 + s_0 + \alpha s_5 + \alpha a_0 b_1 + a_0 b_0 + (\alpha+1)a_1 b_1 + \alpha a_1 b_0\}}_{fp_7}$$

$$\underbrace{fp_7 \xrightarrow{f_8} [\alpha](e_1 + e_2 * s_2) + \{(\alpha+1)e_2 s_1 + \alpha e_2 s_2 + s_0 + \alpha s_5 + \alpha a_0 b_1 + a_0 b_0 + (\alpha+1)a_1 b_1 + \alpha a_1 b_0\}}_{fp_8}$$

$$\underbrace{fp_8 \xrightarrow{f_9} [(\alpha+1)s_1 + \alpha s_2](e_2 + e_3 + s_4) + \{(\alpha+1)e_3 s_1 + \alpha e_3 s_2 + s_0 + (\alpha+1)s_1 s_4 + \alpha s_2 s_4 + \alpha s_5 + \alpha a_0 b_1 + a_0 b_0 + (\alpha+1)a_1 b_1 + \alpha a_1 b_0\}}_{fp_9}$$

$$fp_9 \xrightarrow{lt(f_{10})} \underbrace{[(\alpha+1)s_1 + \alpha s_2]}_{h_{10}}(e_3) + \underbrace{\{s_0 + (\alpha+1)s_1 s_4 + \alpha s_2 s_4 + \alpha s_5 + \alpha a_0 b_1 + a_0 b_0 + (\alpha+1)a_1 b_1 + \alpha a_1 b_0\}}_{r}$$

Reduction order for f :

$f \xrightarrow{f_1} \xrightarrow{f_2} \xrightarrow{f_3} \xrightarrow{f_4} \xrightarrow{f_5} \xrightarrow{f_6} \xrightarrow{f_7} \xrightarrow{f_8} \xrightarrow{f_9} \xrightarrow{lt(f_{10})} r$

Given: $r, h_{10}, f_{11}, f_{12}, f_{13}, f_{14}, f_{15}, f_{16}, J_0$, the problem can be formulated as an ideal membership test using (**??**) such that:

$$r \in \langle h_{10}, f_{11}, f_{12}, f_{13}, f_{14}, f_{15}, f_{16} \rangle + \langle J_0 \rangle$$

The above ideal membership can be solved by expressing r as a linear combination of the ideal members (**??**). $r = Ph_{10} + h_{11}f_{11} + h_{12}f_{12} + h_{13}f_{13} + h_{14}f_{14} + h_{15}f_{15} + h_{16}f_{16}$

In our example, polynomial r can be expressed as

$r = [b_0]h_{10} + [1]f_{11} + [\alpha+1]f_{12} + [\alpha s_4 + \alpha b_0]f_{13} + [0]f_{14} + [(\alpha+1)s_1 + \alpha a_1 b_0]f_{15} + [\alpha]f_{16} + [0]f_{17} + [0]f_{18} + [0]f_{19} + [0]f_{20};$

Thus computed $P = b_0$ is a solution to the *unknown component* f_{10}; i.e. $f_{10} : e_3 + b_0$.

Given a solution P, we can explore the solution space for the gate f_i in terms of variables x_j such that $x_i > x_j$ in the variable order. In our example, r can be written as:

$$\begin{aligned} r &= Ph_{10} + h_{11}f_{11} + h_{12}f_{12} + h_{13}f_{13} + h_{14}f_{14} \\ &\quad + h_{15}f_{15} + h_{16}f_{16} + HJ_0 \\ r &= P'h_{10} + h'_{11}f_{11} + h'_{12}f_{12} + h'_{13}f_{13} + h'_{14}f_{14} \\ &\quad + h'_{15}f_{15} + h'_{16}f_{16} + H'J_0 \end{aligned}$$

Re-writing the above two equations:

$$\begin{aligned} (P - P')h_{10} = (h_{11} - h'_{11})f_{11} + (h_{12} - h'_{12})f_{12} \\ + \cdots + (h_{16} - h'_{16})f_{16} + (H - H')J_0 \end{aligned} \tag{1}$$

$$(P - P')h_{10} \in \langle f_{11}, f_{12}, \ldots, f_{16}, J_0 \rangle \tag{2}$$

$$(P - P') \in \langle f_{11}, f_{12}, \ldots, f_{16}, J_0 \rangle : h_{10} \tag{3}$$

$$(P - P') \in J_Q \tag{4}$$

The above expression for J_Q represents the quotient of ideals operation (**??**). We can pick any polynomial within desired variable subset x_j from the result of J_Q and add it to the computed solution P to arrive at a new solution.

Under the current $RTTO >$ variable order, the quotient of ideals operation results in the following polynomials:

$g[1] = b_1b_0 + b_1 + b_0 + 1$
$g[2] = (\alpha + 1)b_1 + (\alpha + 1) * b_1 * b_0 + (\alpha + 1) * b_0 + (\alpha + 1)$
$g[3] = a_1 + 1$
$g[4] = s_5 + a_0b_1$
$g[5] = s_4 + b_0 + 1$
$g[6] = s_3 + a_0b_0 + a_0 + b_0$
$g[7] = s_2 + b_0$
$g[8] = s_1 + b_1$
$g[9] = s_0 + a_0b_0$

Any $P + g[k]$, where $1 < k < 9$, will work as a solution for the *unknown component* f_{10}.

Now assume that we know the immediate input variables of the polynomial f_{10} as $X_{im} = (b_0, s_3)$, we can compute a solution in terms of these variables by using the elimination ideal $J_Q \cap \mathbb{F}_q[b_0, s_3]$. The quotient operation with the elimination ideal results in:

$g[1] = s_3b_0 + b_0$

Since, there is only one g from the operation, $P + g[1] = s_3b_0$ also works as a solution for the *unknown component*: $f_{10} : e_3 + s_3b_0$.