I. Rectification of finite field arithmetic circuits using the Strong Nullstellensatz

Let $R = \mathbb{F}_q[x_1, \dots, x_n], q = 2^k$, and let f be a polynomial in R that acts as a specification of a circuit. Let C be a circuit with logic gates that is supposed to implement f. If C correctly implements f, then f vanishes on $V_{\mathbb{F}_q}(J)$, or $f \in I(V_{\mathbb{F}_q}(J))$.

Recall the following theorem:

Theorem I.1 (The Strong Nullstellensatz over $\mathbb{F}_q$)**.** *Let ideal $J \subseteq R = \mathbb{F}_q[x_1, \dots, x_n]$, and $J_0 = \langle x_i^q - x_i : i = 1, \dots, n\rangle$ be the ideal of all vanishing polynomials in R. Then, $I(V_{\mathbb{F}_q}(J)) = J + J_0$, as $I(V_{\mathbb{F}_q}(J)) = I(V_{\overline{\mathbb{F}_q}}(J + J_0)) = \sqrt{J + J_0} = J + J_0$.*

Using this approach based on the Strong Nullstellensatz over $\mathbb{F}_q$, we consider correction of buggy arithmetic circuits. If C has a bug and it does not correctly implement f, then $f \xrightarrow{GB(J+J_0)}_+ r$ where $r \neq 0$. Also recall that for any given circuit, we can derive a term order $>$ based on a reverse topological traversal of the circuit that makes the set of polynomials of the circuit itself a Gröbner basis. Call this term order the reverse topological term order (RTTO). Then if $F = \{f_1, \dots, f_s\}$ denotes the set of polynomials of the circuit, and $F_0 = \{x_i^q - x_i\}$, then $F \cup F_0$ constitutes a Gröbner basis under RTTO. For a correct circuit, $f \xrightarrow{F \cup F_0}_+ r = 0$, and for a buggy circuit $f \xrightarrow{F \cup F_0}_+ r$ where $r \neq 0$.

We tried to translate the rectification problem for buggy circuits from the Weak Nullstellensatz to the Strong Nullstellensatz, and seem to have discovered the following concepts via experiments and also intuitively. Can you prove or disprove our conjectures?

Conjecture I.1. *Let $f \in R$ be a specification polynomial. Let C be a circuit, described by a set of polynomials $F = \{f_1, \dots, f_s\}, J = \langle F\rangle$, and $J_0 = \langle F_0\rangle$ be the ideal of vanishing polynomials. Let the circuit contain any (set of) bugs that make the circuit implementation C not match the specification f. Our objective is to ascertain whether the circuit under the presence of the (set of) bugs can be rectified at one location x_i. This is called* **single-fix rectification** *in literature; as opposed to multi-fix rectification that may require corrections at multiple gate output locations. We consider only single-fix rectification for now.*

Using RTTO $>$, construct two ideals:

- *$J_L = \langle G_L\rangle$ where $G_L = \{f_1, \dots, f_{i-1}, f_i : x_i + 1, f_{i+1}, \dots, f_s\}$,*
- *$J_H = \langle G_H\rangle$, where $G_H = \{f_1, \dots, f_{i-1}, f_i : x_i, f_{i+1}, \dots, f_s\}$,*

where the polynomials $f_1, \dots, f_{i-1}, f_{i+1}, \dots, f_s$ are the same as from the generators of J (circuit), and f_i is replaced with $f_i = x + 1$ in J_L and $f_i = x_i$ in J_H.

Compute:

- *$f \xrightarrow{J_L + J_0}_+ r_L$*
- *$f \xrightarrow{J_H + J_0}_+ r_H$*

Let $V_{\mathbb{F}_q}(r_L), V_{\mathbb{F}_q}(r_H)$ denote the varieties of r_L and r_H, and $\overline{V_{\mathbb{F}_q}(r_L)}, \overline{V_{\mathbb{F}_q}(r_H)}$ the complement of the varities, i.e. $\overline{V_{\mathbb{F}_q}(r_L)} = \mathbb{F}_q^n - V_{\mathbb{F}_q}(r_L) = V_{\mathbb{F}_q}(J_0 : \langle r_L\rangle)$. We conjecture that the buggy circuit C admits a single-fix rectification at the gate output x_i if and only if $\overline{V_{\mathbb{F}_q}(r_L)} \cap \overline{V_{\mathbb{F}_q}(r_H)} = \emptyset$.

We will describe the application of our conjecture through the following example.

Consider a buggy circuit implementation C as shown in figure 1 on the right (the correct circuit is depicted on the left) modeled as polynomials $F = \{f_1, \dots, f_s\} \in \mathbb{F}_2[x_1, \dots, x_n]$, with $J = \langle F\rangle$, and $J_0 = \langle x^2 - x : \forall x\rangle$ is the set of all vanishing polynomials. Let's consider a single faulty gate with original AND gate f_4 replaced with a buggy XOR gate.

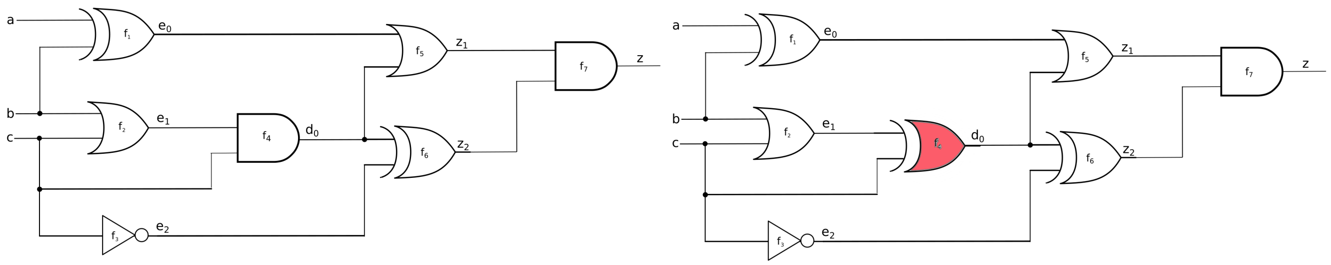

Fig. 1: Correct (left) and buggy (right) logic circuits

Specification polynomial for the circuit is: $f : z + ac + a + bc + b + c$.

Based on the circuit topology, RTTO $>$ with variable order is given as:

$$\{z\} > \{z_2 > z_1\} > \{d_0\} > \{e_2 > e_1 > e_0\} > \{a > b > c\}$$

Polynomials implementing the given circuit:

$$\begin{aligned} f_1 &= e_0 + a + b; & f_5 &= z_1 + e_0 \cdot d_0 + e_0 + d_0; \\ f_2 &= e_1 + b \cdot c + b + c; & f_6 &= z_2 + d_0 + e_2; \\ f_3 &= e_2 + c + 1; & f_7 &= z + z_1 \cdot z_2; \\ f_4b &= d_0 + e_1 + c; \end{aligned} \tag{1}$$

Here f_4b is the polynomial for the buggy gate.

$$\begin{aligned} F &= \{f_1, f_2, f_3, f_4, f_4b, f_5, f_6, f_7\}; \\ J = \langle F \rangle &= \langle f_1, f_2, f_3, f_4, f_4b, f_5, f_6, f_7 \rangle; \end{aligned} \tag{2}$$

We shall add the ideal of vanishing polynomials J_0 for primary inputs. Actually, given the term RTTO order, the vanishing polynomials for only the primary inputs are needed.

$$\begin{aligned} f_8 : a^2 + a; f_9 : b^2 + b; f_{10} : c^2 + c; \\ F_0 = \{f_8, f_9, f_{10}\}; \\ J_0 = \langle F_0 \rangle; \end{aligned}$$

Under RTTO, $F \cup F_0$ forms a Gröbner basis for $J + J_0$.
Computing $f \xrightarrow{F \cup F_0}_+ r = abc + ab + bc + b + c$. Since $r \neq 0$, the circuit is buggy.

A. Rectification at the bug location

Given the setup, let us check if the circuit can be rectified at location d_0 while bug is also at d_0. This is, of course, possible. Consider the following ideals with net d_0 forced to ’1’ and ’0’ respectively.

$$\begin{aligned} J_L &= \langle f_1, f_2, f_3, f_4b : d_0 + 1, f_5, f_6, f_7, f_8, f_9, f_{10} \rangle \\ J_H &= \langle f_1, f_2, f_3, f_4b : d_0, f_5, f_6, f_7, f_8, f_9, f_{10} \rangle \end{aligned}$$

Note that the generators of J_L, J_H still constitute a Gröbner basis due to RTTO $>$. Let us analyze the variety of the circuit with respect to these two ideals as shown in table I. The first 2 columns show the function implemented by the specification. The next 2 columns show the function of the circuit when d_0 is forced to 1 in J_L. Last 2 columns likewise show the evaluation of the circuit output when $d_0 = 0$ in J_H.

TABLE I: Variety evaluation of J_L & J_H with rectification at bug location

input	**specification output**	**circuit evaluation**			
		J_L		J_H	
abc	z	**force** d_0 **to 1**	z	**force** d_0 **to 0**	z
000	0	1	0	0	0
001	1	1	1	0	*0
010	1	1	*0	0	1
011	1	1	1	0	*0
100	1	1	*0	0	1
101	1	1	1	0	*0
110	0	1	0	0	0
111	1	1	1	0	*0

The evaluations marked with a ’*’ indicate the points where circuit output z differs from specification z with net d_0 forced to values {0,1}. This table is presented here just to show the different functions.

We need to consider these varieties in our setup as follows:
$f \xrightarrow{J_L}_+ r_L = a \cdot c + a + b \cdot c + b;$
$V(r_L) = (abc) : \{000, 001, 011, 101, 110, 111\}; \overline{V(r_L)} = (abc) : \{010, 100\};$

$f \xrightarrow{J_H}_+ r_H = c;$
$V(r_H) = (abc) : \{000, 010, 100, 110\}; \overline{V(r_H)} = (abc) : \{001, 011, 101, 111\};$
Given our earlier conjuncture, a circuit can be rectified at a given location if and only if

$$\begin{aligned} \overline{V(r_L)} \cap \overline{V(r_H)} = \emptyset \\ \{010, 100\} \cap \{001, 011, 101, 111\} = \emptyset \end{aligned}$$

Since the intersection is empty, the circuit can be corrected at location d_0. This demonstrates the “if case” of our conjecture.

B. *Rectification at a different location where correction is not possible*

Given the setup, let us demonstrate the “only if” case of our conjecture. Let us check if the circuit can be rectified at location z_1 with bug located at d_0. Actually, it should not possible to apply a single-fix rectification at z_1 to fix a bug at d_0.

Consider the following ideals with net z_1 forced to ’1’ and ’0’ respectively.

$$J_L = \langle f_1, f_2, f_3, f_4b, f_5 : z_1 + 1, f_6, f_7, f_8, f_9, f_{10}\rangle$$
$$J_H = \langle f_1, f_2, f_3, f_4b, f_5 : z_1, f_6, f_7, f_8, f_9, f_{10}\rangle$$

Let us analyze the variety of the circuit with respect to these two ideals as shown in table II.

TABLE II: Variety evaluation of J_L & J_H with rectification at different locations

input	**specification output**	**circuit evaluation**			
		J_L		J_H	
abc	z	**force** z_1 **to 1**	z	**force** z_1 **to 0**	z
000	0	1	*1	0	0
001	1	1	*0	0	*0
010	1	1	*0	0	*0
011	1	1	*0	0	*0
100	1	1	1	0	*0
101	1	1	*0	0	*0
110	0	1	0	0	0
111	1	1	*0	0	*0

The evaluations marked with a ’*’ indicates the point where circuit output z differs from specification z with net z_1 forced to values {0,1}. Just as in the previous case, consider the Gröbner basis reductions:

$f \xrightarrow{J_L}_+ \underbrace{a\cdot c+a+1}_{r_L};$

$V(r_L) = \{100, 110\}; \overline{V(r_L)} = V(E_L) = \{000, 001, 010, 011, 101, 111\};$

$f \xrightarrow{J_H}_+ \underbrace{a\cdot c+a+b\cdot c+b+c}_{r_H};$

$V(r_H) = \{000, 110\}; \overline{V(r_H)} = V(E_H) = \{001, 010, 011, 100, 101, 111\};$

$$\overline{V(r_L)} \cap \overline{V(r_H)} = \{000, 001, 010, 011, 101, 111\} \cap \{001, 010, 011, 100, 101, 111\} \neq \emptyset$$

Since, the intersection is not empty, the circuit cannot be corrected at location z_1. We have tried this concept on a few more circuits, and the conjecture seem to hold well.

Also, we extrapolated these results from our analysis of the same problem that we carried out a couple of weeks ago using the Weak Nullstellensatz and Interpolants. However, for now I have refrained from describing the relationship between these two works. As the ideals in the two formulations are constructed slightly differently (J_{miter} versus $J_{implementation}$), I did not want to confuse the two issues. If you would still like to see the relationship, let me know. Also, I wanted to see if we can prove this result without explicitly making use of interpolants!

If we can prove this result, then we have a complete problem formulation using the strong Nullstellensatz. We formulate the verification problem using the Strong Nullstellensatz ($f \in J + J0$?). If $f \pmod{J + J0} = r \neq 0$, then apply the conjecture to see if f can be rectified at gate x_i. If so, then we identify a correction using our *unknown component problem*, which is also based on the Strong Nullstellensatz.