The unknown component problem

Given specification polynomial $f \in \mathbb{F}_q[x_1 \dots x_n] = R$, $q = 2^k$, and a ckt C with 's' gates.

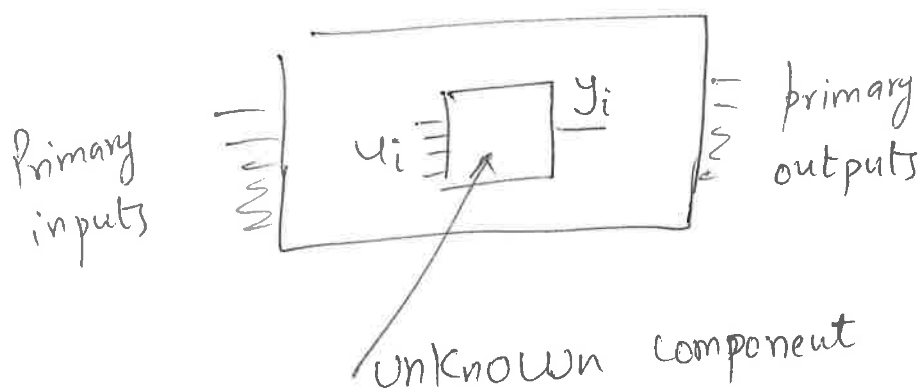
Write the gates as polynomials in R as $F := \{f_1, \dots, f_i, \dots f_s\}$. $J = \langle f_1 \dots, f_i, \dots f_s \rangle$

Assume the circuit C correctly implements f.

Then $f \in I(V_{\mathbb{F}_q}(J)) = J + J_0 \quad (J_0 = \langle x_i^q - x_i \rangle)$

Assume $\underline{J \supset J_0}$.

So $f \in J \Rightarrow f = h_1 f_1 + \cdots + h_i f_i + \cdots + h_s f_s$.



$$f_i = y_i + P_i(u_i)$$

$y_i > u_i$ in our term order.

$$h_i f_i = f + h_1 f_1 + \cdots + h_{i-1} f_{i-1} + h_{i+1} f_{i+1} + \cdots + h_s f_s.$$

or $h_i f_i \in \langle \underbrace{f, f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_s}_{\text{ideal } J'} \rangle$.

<u>Now</u> $f_i = y_i + \underbrace{P(u_i)}_{\text{some polynomial in } u_i}$

but $h_i \in R$ is arbitrary.

Our question was, what if we project the variety of J' on y_i & u_i coordinates? Can we recover f_i?

Is $h_i f_i \in J' \cap \mathbb{F}_q[y_i, u_i]$?

Yes, but that does not always help us recover f_i. Sometimes it does, but not always.

Here is an example that shows that some information is missing.

See Fig 1.

Specification $f: z + ac + a + b + bc + c$.

Ring $\mathbb{F}_2[z, z_1, z_2, e_0, e_2, a, b, d_0, e_1, c]$

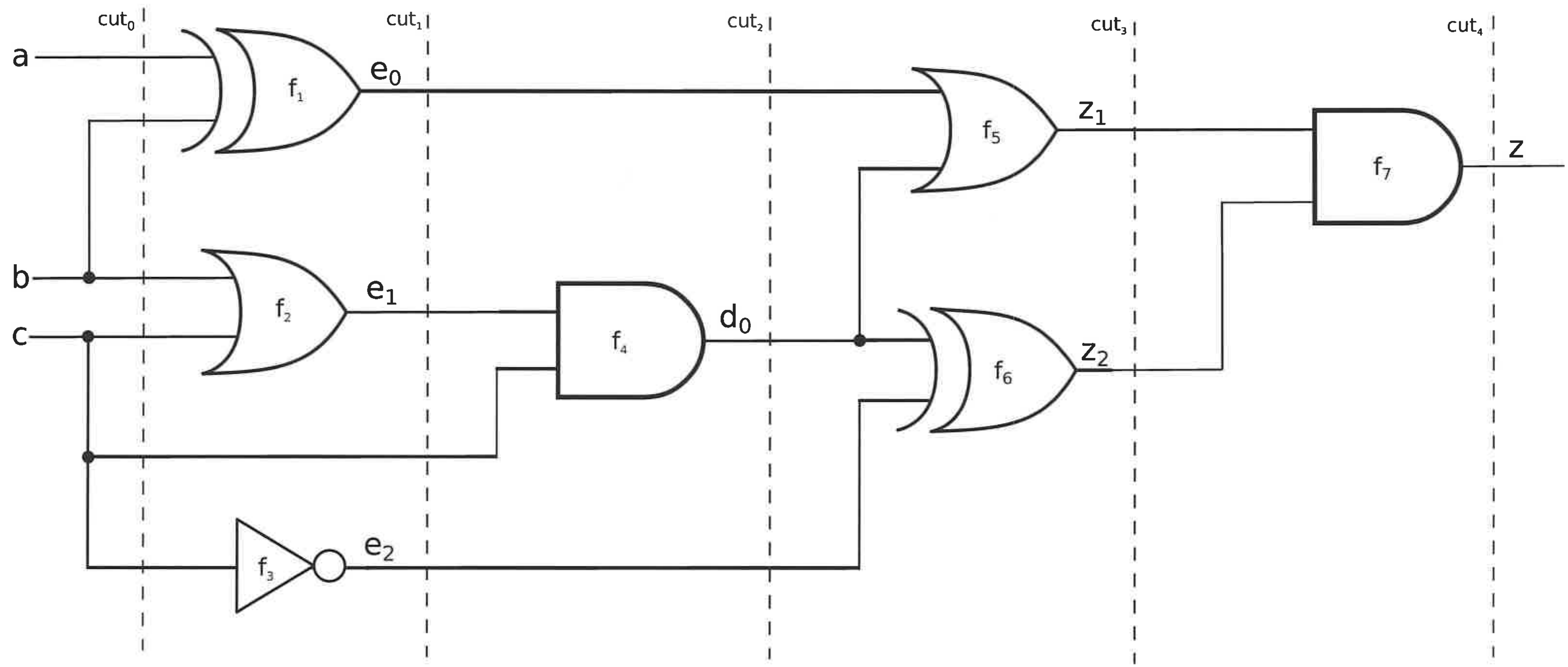


Fig 1.

Assume $f_4 : d_0 = e_1 \wedge c$ is the unknown component.

$[d_0 + e_1 \cdot c$ in $\mathbb{F}_2]$

3

Polynomials of this ckt.

$f_1 : e_0 + a + b$

$f_2 : e_1 + bc + b + c$

$f_3 : e_2 + c + 1$

$f_4 : d_0 + e_1 \cdot c$ [unknown gate]

$f_5 : z_1 + e_0 d_0 + e_0 + d_0$

$f_6 : z_2 + d_0 e_2$

$f_7 : z_0 + z_1 \cdot z_2$

$$\frac{+}{J_0}.$$

$f \in \langle f_1, f_2, \underline{\underline{f_4}}, f_7 \rangle$

↳ unknown.

Let $f_4 = \underline{d_0 + P(e_1, c)}$

what is P?

Notice the function implemented by f_4:

e_1	c	$\rightarrow d_0$
0	0	0
0	1	0
1	0	0
1	1	1

$d_0 = AND(e_1, c)$.

$P(e_1, c) = \underline{\underline{e_1 \cdot c}}$

$h_4 f_4 \in \underbrace{\langle f, f_1, \cdots f_3, f_5, \cdots f_7 \rangle}_{J'}$

Compute reduced Gröbner Basis of

$$J_L = J' \cap \mathbb{F}_2[d_0, e_1, c]$$

J_L = elimination ideal that eliminates everything but d_0, e_1, c.

$$GB(J_L + J_0) = G = \{g_1, g_2 \cdots g_5\}$$ 6

$$= g_1 : c^2 + c$$
$$g_2 : e_1 c + c$$
$$g_3 : e_1^2 + e_1$$
$$g_4 : d_0 c + c$$
$$g_5 : d_0^2 + d_0$$

$V(G) =$ ~~$e_1 c d_0$~~

$$\left.\begin{array}{cccc} & e_1 & c & d_0 \\ \checkmark & 0 & 0 & 0 \\ & 0 & 0 & 1 \\ \checkmark & 1 & 0 & 0 \\ & 1 & 0 & 1 \\ \checkmark & 1 & 1 & 1 \end{array}\right\}$$

$\checkmark$ = pts in $V(f_4)$

Recall $h_4 f_4 \in J'$ $(J' \supset J_0)$

$V(h_4 f_4) \supset V(J')$. Now project variety on e_1, c, d_0.

Projection is also a variety

So. $V(h_4 f_4)|_{e_1, c, d_0} \supset V(J_L + J_0)$

$$\boxed{V(h_4) \cup V(f_4) \supset V(J_L + J_0)} \quad - 1$$

Notice the point $e_1\ c\ d_0 = (0\,1\,0) \in V(f_4)$

but is <u>not</u> in $V(J_L + J_0)$.

From this information, do you think

$V(f_4)$ can be found?

Notice $f_4 = d_0 + P(e_1, c)$

$\exists\ h_4$ s.t. $h_4 \cdot f_4 \in J_L + J_0$.

If $\underline{h_4 = c}$, then

$$c \cdot [d_0 + P(e_1, c)] = \underbrace{g_2 + g_4}_{\in G}$$

$$= \underline{e_1 c + d_0 c}.$$

then $P(e_1, c) = e_1 \cdot c$

but how do we guess h_4?