Suppose the unknown component is the i^{th} gate in the circuit with the leading term x_i. Let the RTTO order for the circuit be $x_1 > x_2 > \cdots > x_n$. Also assuming that the specification polynomial is f_{spec}, we can write

$$f_{spec} = h_1 f_1 + h_2 f_2 + \cdots + h_i(x_i + P) + h_{i+1} f_{i+1} + \cdots + h_n f_n \tag{1}$$

Since we know f_{spec} polynomial and f_1 polynomial, we can obtain the polynomial h_1 as the quotient of the reduction $f_{spec} \xrightarrow{f_1}_+$. The remainder of this reduction can be reduced by f_2 to obtain h_2. Performing quotient computations in a similar fashion, we can obtain the polynomial h_i. Notice that we cannot obtain h_{i+1} as the tail or P part of the polynomial f_i is unknown. We can rearrange the terms in Eqn. 1 to obtain the following equation.

$$f_{spec} - h_1 f_1 - h_2 f_2 - \cdots - h_i x_i = h_i P + h_{i+1} f_{i+1} + \cdots + h_n f_n \tag{2}$$

In the Eqn. 2, the L.H.S. is known. We can compute the polynomial P using the $lift$ operation in SINGULAR. The $lift$ operation returns a list of polynomial coefficients $T_1 \ldots T_s$ for a list of polynomials $p_1, \ldots, p_s$ such that the linear combination $T_1 p_1 + \cdots + T_s p_s$ is equal to some given polynomial f. Using the $lift$ operation with inputs $f_{spec} - h_1 f_1 - h_2 f_2 - \cdots - h_i x_i$ as f and $h_i, f_{i+1}, \ldots, f_n$ as $p_1, \ldots, p_s$, we can obtain the polynomial coefficients $T_1 \ldots T_s$ such that $T_1 h_i + \cdots + T_s f_n = f_{spec} - h_1 f_1 - h_2 f_2 - \cdots - h_i x_i$. Then the polynomial T_1 can be construed as the polynomial P in our formulation.

The computed polynomial P, can contain any variable *i.e.* it can contain the immediate input variables of the unknown component or it may even contain variables that are not the immediate inputs. In other words, there is no guarantee about the variables that P consists of. But we know from the circuit topology, that there must be at least one polynomial P only in the immediate input variables of gate i, that can be used in the polynomial $f_i = x_i + P$ to solve the problem. Let us denote this polynomial by P'.

Using the Eqn. 2, we can write,

$$f_{spec} - h_1 f_1 - h_2 f_2 - \cdots - h_i x_i = h_i P' + h'_{i+1} f_{i+1} + \cdots + h'_n f_n \tag{3}$$

The polynomials $h'_{i+1}, \ldots, h'_n$ in Eqn. 3 need not be same as $h_{i+1}, \ldots, h_n$ in Eqn. 2 as their computation is dependent on two different polynomials P and P' respectively. Subtracting the Eqn. 2 and Eqn. 3, we get,

$$\begin{aligned} h_i(P' - P) &= (h_{i+1} - h'_{i+1}) f_{i+1} + \cdots + (h_n - h'_n) f_n \\ h_i(P' - P) &\in \langle f_{i+1}, \ldots, f_n \rangle \\ P' - P &\in \langle f_{i+1}, \ldots, f_n \rangle : h_i \end{aligned}$$

We denote the quotient (or colon) ideal $\langle f_{i+1}, \ldots, f_n \rangle : h_i$ by C. Therefore,

$$P' - P \in C \tag{4}$$

From remainder arithmetic and Eqn. 4, we can say that the remainder of the reduction $P \xrightarrow{GB(C)}_+$ and the remainder of the reduction $P' \xrightarrow{GB(C)}_+$ will be equal. Let this remainder be r.

Now consider a term order similar to RTTO where the variables x_i (the output of the unknown component) and the immediate inputs of gate i are placed at the end in the lexicographic ordering. The $GB(C)$ with this order will contain the first few polynomials only in the variables x_i and immediate inputs of gate i (as this term order is an elimination term order). So the reduction $P' \xrightarrow{GB(C)}_+ r$ will produce r consisting of only the immediate inputs of gate i. The reason is that P' is assumed to contain only the immediate inputs of gate i, and therefore, it will only be reduced by the first few polynomials of GB(C) that contain the same variables as P'. After computing P (using the $lift$ operation) and $GB(C)$ with the new term order, we can perform the reduction $P \xrightarrow{C}_+$ to obtain r which will only contain the immediate inputs of gate i as variables. Therefore, $x_i + r$ can used a replacement for the unknown component.

We can also pick a polynomial $p \in GB(C)$ such that p contains only the immediate inputs of gate i and use $x_i + (r + p)$ as another replacement for the unknown component. This is due to the fact that $r + p \xrightarrow{GB(C)}_+ r$.