1 Complement set for varieties of ideals with single generator

Note: we only care about varieties (value that circuit variables can take)! Variety is solution to equation *poly generator* $= 0$, it is a set of elements within Galois field. The only reason we adopt ideal representation is: it is convenient to represent the varieties using ideal (set of generator polynomials).

Back to our example. The universal set is $V(U) = \{0, 1, \alpha, 1+\alpha\}$, where $U =< T^4 + T >=< f >$; and *reached* is another set of values we can take, assume it is $V(J) = \{1 + \alpha\}$, then $J =< T + 1 + \alpha >=< g >$. Now our objective is to find an ideal I, whose variety is $V(I) = V(U) - V(J)$. Let's assume I is ideal quotient of U and J, i.e. $I = U : J$. Check again the definition of ideal quotient:

Definition 1 If I, J are ideals in $k[x_1, ..., x_n]$, then $I : J$ is the set $\{f \in k[x_1, ..., x_n] : fg \in I \ for \ all \ g \in J\}$.

Let h^* be a polynomial in I. Then there exists one polynomial $g^* = c_1 g$ from J and another polynomial $f^* = c_2 f$, satisfying $c_2 f = h^* \cdot c_1 g$, i.e.

$$h^* = \frac{c_2}{c_1}\frac{f}{g}$$

So ideal I only have one generator h where $h = f/g$. Find varieties of I: make $h = 0$, which means $f = 0 \ and \ g \neq 0$. Interpret this specification: $f = 0 \rightarrow V(U), and \rightarrow \bigcap, g \neq 0 \rightarrow \overline{V(J)}$. It means $V(U) \bigcap \overline{V(J)}$, which equals to $V(U) - V(J)$! Proof completed for single generator ideal quotient.

Theorem 1 If I, J are ideals with only one generator, we have $V(I : J) = V(I) - V(J)$.