Solving Boolean Equation Systems over $\mathbb{C}$ valentinpi, Last Change: April 1, 2025

The following notes are based on [1]. Let $X = \{x_1, ..., x_n\}$ be a set of variables and $\mathcal{F} = \{f_1, ..., f_r\} \subseteq \mathbb{F}_2[X]$ be a set of Boolean multivariate polynomials with $n, r \in \mathbb{N}_{\geq 1}$. We assume all polynomials have no redundant terms and omit the explicit indexing in the following. Denote by $\mathbb{V}_F(\mathcal{F}) = \bigcap_{i=1}^r f_i|_F^{F^{-1}}(0)$ the *variety* of $\mathcal{F}$ over a field F, where $f_i|_F^F \colon F \to F$ is the polynomial function over F associated with f_i and $t_i \in \mathbb{N}_{\geq 1}$ the number of (monomial) summands in f_i for each i.

The overall goal is to solve $\mathcal{F}$ over $\mathbb{F}_2$ by solving it over $\mathbb{C}$. In general, $\mathbb{V}_{\mathbb{F}_2}(\mathcal{F}) \neq \mathbb{V}_{\mathbb{C}}(\mathcal{F})$. For instance, for the system $\mathcal{F} = \{x_1 x_2\}$, we have $\mathbb{V}_{\mathbb{F}_2}(\mathcal{F}) = \{(0,0), (0,1), (1,0)\} \neq \mathbb{C} \times \{0\} \cup \{0\} \times \mathbb{C} = \mathbb{V}_{\mathbb{C}}(\mathcal{F})$.

The first step is to restrict the variables in the solution to $\mathbb{F}_2$. Thus, consider the system $\mathcal{F} \cup \{x_i^2 - x_i\}_i$. Over $\mathbb{C}$, the added polynomials suffice $x_i^2 - x_i = x_i(x_i - 1)$ for each i, so the solution has to restrict the variables to 0 or 1.

However, this is not sufficient. Consider the system $\mathcal{F} = x_1^2 + x_1 x_2$. We have $\mathbb{V}_{\mathbb{F}_2}(\mathcal{F}) = \{(0,0), (0,1), (1,1)\}$, but $\mathbb{V}_{\mathbb{C}}(\mathcal{F} \cup \{x_1^2 - x_1, x_2^2 - x_2\}) = \{(0,0), (0,1)\}$. So we adjust the general system by introducing

$$C(f_i) \coloneqq \prod_{k = f_i|_{\mathbb{F}_2}^{\mathbb{F}_2}(0)}^{\lfloor t_i/2 \rfloor} (f_i - 2k) \tag{1}$$

for each i and letting

$$C(\mathcal{F}) \coloneqq \{C(f_i)\}_i. \tag{2}$$

Lemma 1 ([1, p. 23]). We have $\mathbb{V}_{\mathbb{F}_2}(\mathcal{F}) = \mathbb{V}_{\mathbb{C}}(C(\mathcal{F}))$.

Proof. ($\subseteq$) Let $f_i = \sum_{k=1}^{t_i} m_{ik}$ with monomials $m_{ik} \in \mathbb{F}_2[X]$, i be arbitrarily chosen, and $a \in \mathbb{V}_{\mathbb{F}_2}(\mathcal{F})$. Thus $f_i|_{\mathbb{C}}^{\mathbb{C}}(a) \in [f_i|_{\mathbb{F}_2}^{\mathbb{F}_2}(0), t_i]_{\mathbb{N}} \cap 2\mathbb{N}$, implying $C(f_i)(a) = 0$.
($\supseteq$) On the other hand, let i be arbitrary and $a \in \mathbb{V}_{\mathbb{C}}(C(\mathcal{F}))$. Then $f_i|_{\mathbb{C}}^{\mathbb{C}}(a) = 2k$ for a $k \in [f_i|_{\mathbb{F}_2}^{\mathbb{F}_2}(0), \lfloor t_i/2 \rfloor]_{\mathbb{N}}$, so $a \in \mathbb{V}_{\mathbb{F}_2}(\mathcal{F})$. ∎

References

[1] Y.-A. Chen and X.-S. Gao, "Quantum algorithm for boolean equation solving and quantum algebraic attack on cryptosystems," *Journal of Systems Science and Complexity*, vol. 35, no. 1, pp. 373–412, Jan. 2021, ISSN: 1559-7067. DOI: 10.1007/s11424-020-0028-6.