Résolution de Formules Booléennes en Temps Polynomial

Mohamed Hamlil

Octobre 2023

1 Introduction

Notre approche consiste à transformer toutes les formules de logique propositionnelle en un système d'équations polynomiales sur $\mathbb{Z}_2$ qui peut être résolu (c'est-à-dire déterminer s'il existe une assignation des variables propositionnelles qui rend la formule vraie) en temps polynomial.

2 Prérequis

- Le Corps de Galois $\mathbb{F}_2$
- Solutions d'un Système d'Équations
- Systèmes d'Équations Polynomiales
- Élimination Gaussienne et Substitution de Variables
- Algèbre Booléenne

Notes :

- L'opération **and** est abrégée par $(\cdot)$.
- L'opération **xor** est notée $\oplus$.

3 Transformation d'une Formule de Logique Propositionnelle en un Système Polynomial sur $\mathbb{Z}_2$

Une formule de logique propositionnelle est écrite en fonction des opérations **or**, **and**, **not**.
Transformations des opérations logiques :

- not x est équivalent à $x \oplus 1$.

- x or y est équivalent à :

$$\begin{aligned} x \text{ or } y &= \text{not}(\text{not } x \text{ and not } y) \\ &= \text{not}((\text{not } x) \cdot (\text{not } y)) \\ &= 1 \oplus [(1 \oplus x)(1 \oplus y)] \\ &= x \oplus y \oplus (x \cdot y) \end{aligned}$$

En conclusion, avec **true** $= 1$ et **false** $= 0$, toutes les formules de logique propositionnelle peuvent être écrites sous forme d'équations polynomiales sur $\mathbb{Z}_2$.

4 Résolution d'une Équation Polynomiale sur $\mathbb{Z}_2$

Considérons les équations polynomiales sur $\mathbb{Z}_2$ écrites sous la forme :

$$f(x_0, x_1, \ldots, x_n) = a_0 x_0 \oplus a_1 x_1 \oplus \cdots \oplus a_i(x_0 x_1) \oplus a_{i+1}(x_0 x_2) \oplus \cdots \oplus a_n(x_0 x_1 \ldots x_n)$$

Exemple :

$$x_0 \oplus x_2 \oplus (x_0 x_1) \oplus (x_0 x_1 x_2) = f(x_0, x_1, x_2)$$

Notre approche consiste à isoler le terme $x_0 x_1 x_2$, c'est-à-dire le terme avec le plus haut degré dans l'équation.

Procédure Générale

Pour b un nombre binaire, en isolant le terme avec le plus haut degré, nous avons les cas suivants :

Cas 0 : Écrire le terme avec le plus haut degré en fonction des termes de plus bas degré.

Cas 1 : Identifier les situations où le terme avec le plus haut degré doit être égal à 1. La multiplication de x_i de i jusqu'à n :

$$\prod_i^n x_i = 1$$

implique que tous les x_i sont égaux à 1.

Cas 2 : Après avoir identifié le cas où le terme doit être égal à 1, pour les autres cas (tant que ce n'est pas $1 = 0$), les solutions pour les variables sont soit 0 (obligatoire dans le cas où un **or** est faux, ce qui est équivalent au **not** du Cas 1), soit 1 (optionnel). Par précaution, on choisira 0 quand on ne peut plus simplifier un système.

5 Complexité Temporelle de la Résolution d'un Système Polynomial sur $\mathbb{Z}_2$

Considérons le système :

$$\begin{aligned} f_0(x_0, x_1, \ldots, x_n) &= b_0 \\ f_1(x_0, x_1, \ldots, x_n) &= b_1 \\ &\vdots \\ f_j(x_0, x_1, \ldots, x_n) &= b_j \\ &\vdots \\ f_m(x_0, x_1, \ldots, x_n) &= b_m \end{aligned}$$

où b est un nombre binaire.

La simplification d'une équation polynomiale se fait en temps polynomial (puisque $a \oplus a = 0$, $b \cdot b = b$), et la substitution est également en temps polynomial. Le nombre de variables n ne dépassera pas $n^{(\text{degré maximal})}$, qui est 3 dans notre cas.

Étapes de la résolution :

- Isolation des termes.
- Itérer sur les variables x_i dans une équation.
- Identifier les cas et les substituer dans notre système.

Ce processus sera répété m fois, ce qui est polynomial. Une fois que nos substitutions et l'identification des cas seront terminées, nous nous retrouverons avec un système réduit :

- Un système cohérent (consistent) ou incohérent (inconsistent).
- Un système indéterminé ou déterminé.

6 Exemple

Soient x, y des variables propositionnelles, et considérons la formule :

$$(x \text{ or } x \text{ or } y) \text{ and } (\neg x \text{ or } \neg y \text{ or } \neg y) \text{ and } (\neg x \text{ or } y \text{ or } y) = \text{true}$$

C'est l'équivalent de :

$$\begin{aligned} (x \text{ or } y \text{ or } y) &= 1 \\ (\neg x \text{ or } \neg y \text{ or } \neg y) &= 1 \\ (\neg x \text{ or } y \text{ or } y) &= 1 \end{aligned}$$

Écriture en termes de $\cdot$ et $\oplus$:

1. Transformons les opérations :

$$\begin{aligned} x \oplus y \oplus y \oplus (xy) \oplus yy \oplus xy \oplus xyy = 1 \\ (1 \oplus x) \oplus (1 \oplus y) \oplus (1 \oplus y) \oplus (1 \oplus x)(1 \oplus y) \\ \oplus (1 \oplus y)(1 \oplus y) \oplus (1 \oplus x)(1 \oplus y) \\ \oplus (1 \oplus x)(1 \oplus y)(1 \oplus y) = 1 \end{aligned}$$

2. Simplifions en utilisant les propriétés $(a \oplus a = 0)$:

$$x \oplus y \oplus (xy) = 1$$

3. Équations supplémentaires :

$$xy = 0$$

$$x \oplus (xy) = 0$$

Résolution :

- Élimination gaussienne de xy :

$$x \oplus y = 1 \quad \Rightarrow \quad x = 1 \oplus y$$

- Substitution :

$$xy = x(1 \oplus x) = x(1 \oplus x) = 0$$

- Conclusion :

$$x = 0 \quad \Rightarrow \quad y = 1$$

Notre système est cohérent et déterminé :

$$x = \text{false}, \quad y = \text{true}$$