Preuve formelle mécanisée
Correction de l'examen final

ÉNSIIE, semestre 5

mardi 25 octobre 2022

Exercice 1 : Démonstration automatique

1. On travaille sur des entiers, et on a des produits entre variable (ab par exemple). On est donc en arithmétique non-linéaire sans quantificateur (`QF_NIA`).
2. On va utiliser les variables propositionnelles suivantes pour abstaires les formules atomiques :

$$\begin{aligned} a + b \leq 6 &\mapsto V \\ a \leq -1 &\mapsto W \\ b \leq -2 &\mapsto X \\ a \leq b &\mapsto Y \\ ab \leq ab^2 &\mapsto Z \end{aligned}$$

   On a alors les formules propositionnelles :

$$V \Rightarrow (W \vee X) \tag{1}$$
$$W \Rightarrow (X \wedge Y) \tag{2}$$
$$X \Rightarrow \neg V \tag{3}$$
$$Z \Rightarrow (W \wedge X) \tag{4}$$

   avec le but

$$X \wedge Y \tag{5}$$

3. On nie le but, on remplace $A \Rightarrow B$ par $\neg A \vee B$, on distribue les $\wedge$ sur les $\vee$, on obtient :

$$\neg V \vee W \vee X \tag{6}$$
$$\neg W \vee X \tag{7}$$
$$\neg W \vee Y \tag{8}$$
$$\neg X \vee \neg V \tag{9}$$
$$\neg Z \vee W \tag{10}$$
$$\neg Z \vee X \tag{11}$$
$$\neg X \vee \neg Y \tag{12}$$

4. En associant les entiers 1 2 3 4 et 5 à V W X Y et Z, on obtient pour le format DIMACS le fichier d'entrée suivant :

```
p cnf 5 7
-1 -2 3 0
-2 3 0
-2 4 0
-3 -1 0
-5 2 0
-5 3 0
-3 -4 0
```

5. On n'a pas de propagation unitaires à faire au début.
   - On décide que V est vrai.
     On propage que X est faux. $(\neg X \vee \neg V)$
     On propage que W est vrai. $(\neg V \vee W \vee X)$
     On a un conflit. $(\neg W \vee X)$
   - On décide que V est faux.
     On n'a pas de propagation unitaires à faire
     - On décide que W est vrai.
       On propage que X est vrai. $(\neg W \vee X)$
       On propage que Y est vrai. $(\neg W \vee Y)$
       On a un conflit. $(\neg X \vee \neg Y)$
     - On décide que W est faux.
       On propage que Z est faux. $(\neg Z \vee W)$
       - On décide que X est vrai.
         On propage que Y est faux. $(\neg X \vee \neg Y)$
         On a un modèle.

6. - On décide que V est vrai.
     On propage que X est faux. $(\neg X \vee \neg V)$
     On propage que W est vrai. $(\neg V \vee W \vee X)$
     On a un conflit. $(\neg W \vee X)$
     On calcule la clause de conflit :

$$\textsf{Resolution}\ \dfrac{\textsf{Resolution}\ \dfrac{\neg W \vee X \qquad \neg V \vee W \vee X}{\neg V \vee X} \qquad \neg X \vee \neg V}{\neg V}$$

     On rajoute la clause de conflit $\neg V$ et on backjump au tout début.

   On propage que V est faux. $(\neg V)$
   - On décide que W est vrai.
     On propage que X est vrai. $(\neg W \vee X)$
     On propage que Y est vrai. $(\neg W \vee Y)$
     On a un conflit. $(\neg X \vee \neg Y)$
     On calcule la clause de conflit :

$$\textsf{Resolution}\ \dfrac{\textsf{Resolution}\ \dfrac{\neg X \vee \neg Y \qquad \neg W \vee Y}{\neg X \vee \neg W} \qquad \neg W \vee X}{\neg W}$$

On ajoute la clause de conflit $\neg W$ et on revient avant la décision de W.

On propage que W est faux. ($\neg W$)
On propage que Z est faux. ($\neg Z \vee W$)

— On décide que X est vrai.
On propage que Y est faux. ($\neg X \vee \neg Y$)
On a un modèle.

7. Du point de vue de la théorie, ce modèle correspond à :

$$a + b > 6 \quad \wedge \quad a > -1 \quad \wedge \quad b \leq -2 \quad \wedge \quad a > b \quad \wedge \quad ab > ab^2$$

Si $a = 0$, alors on ne peut pas avoir $ab > ab^2$.
Si $a > 0$, alors $ab > ab^2$ implique $b > b^2$ ce qui n'est pas possible sur $\mathbb{Z}$.
Ce n'est donc pas un modèle pour la théorie.
On doit rajouter la clause $V \vee W \vee \neg X \vee Y \vee Z$.
(On pourrait se contenter de $W \vee Z$ parce qu'on a pas utilisé les autres.)

8. Si on reprend CDCL, à la place d'avoir le modèle, on aura un conflit avec la nouvelle clause $V \vee W \vee \neg X \vee Y \vee Z$
La clause apprise est alors :

$$\textsf{Resolution}\ \dfrac{\textsf{Resolution}\ \dfrac{\textsf{Resolution}\ \dfrac{\textsf{Resolution}\ \dfrac{V \vee W \vee \neg X \vee Y \vee Z \qquad \neg X \vee \neg Y}{V \vee W \vee \neg X \vee Z} \qquad \neg Z \vee W}{V \vee W \vee \neg X} \qquad \neg W}{V \vee \neg X} \qquad \neg V}{\neg X}$$

On backjump avant la décision de X.
On propage $\neg X$.
On a un modèle. (Quelle que soit la valeur de Y.)
Du point de vue de la théorie, ce modèle correspond à :

$$a + b > 6 \quad \wedge \quad a > -1 \quad \wedge \quad b > -2 \quad \wedge \quad ab > ab^2$$

Ce n'est pas un modèle non plus.
L'ensemble de clauses de départ est donc insatisfiable.

9. (5) est bien une conséquence de {(1), (2), (3), (4)}.
10. Avec une version online de DPLL(T), dès que W et Z sont affectés à faux, le solveur de théorie detecte un conflit sans avoir faire d'autres décisions/propagations.
11. Sur $\mathbb{R}$, en prenant par exemple $a = 6$ et $b = \frac{1}{2}$, on a donc $a + b > 6$, $a > -1$, $b > -2$, $a > b$ et $ab = 3 > 1,5 = ab^2$. On obtient donc bien un modèle de toutes les clauses.