Satisfiabilité d'ensembles de clauses avec compteurs

Documents autorisés (en particulier le poly).

Les questions sont annotées par un niveau de difficulté, variant de (0) (facile) à (3) (difficile).

En comptant 5 minutes passées par problème facile, 10 minutes par problème de difficulté (1), 15 minutes par problème de difficulté (2), et 20 minutes par problème de difficulté (3), vous aurez besoin de 1h55 pour tout faire.

On note $|A|$ le cardinal d'un ensemble fini A.

On considère des *clauses étendues* C/k, où C est un multi-ensemble $L_1, \ldots, L_n$ de littéraux, et k est un entier relatif, c'est-à-dire dans $\mathbb{Z}$. (On note $\Box$ le multi-ensemble $L_1, \ldots, L_n$ lorsque $n = 0$.) La sémantique d'une telle clause étendue est :

$$\rho \models L_1, \ldots, L_n/k \text{ ssi } |\{i \mid 1 \leq i \leq n \text{ et } \rho \models L_i\}| \geq k$$

autrement dit, ρ satisfait la clause s'il satisfait au moins k littéraux de la clause.

On dit qu'un ensemble S de clauses étendues est *satisfiable* si et seulement s'il existe ρ telle que $\rho \models S$, autrement dit $\rho \models C$ pour toute clause étendue $C \in S$. Le but du problème est d'examiner deux méthodes de test d'insatisfiabilité de tels ensembles de clauses étendues.

On notera par une virgule l'union multi-ensembliste : si $E \hat{=} L_1, \ldots, L_n$ et $E' \hat{=} L_{n+1}, \ldots, L_m$, alors $E, E' \hat{=} L_1, \ldots, L_m$. De plus, un littéral L désignera aussi de façon ambiguë le multi-ensemble singleton contenant exactement L.

Préliminaires

1. (0) Justifier que les clauses étendues généralisent les clauses usuelles, en montrant que $\rho \models L_1 \vee \ldots \vee L_n$ (sémantique usuelle) si et seulement si $\rho \models L_1, \ldots, L_n/1$.
2. (1) Montrer que $L_1, \ldots, L_n/k$ a la même sémantique que $L_1 \wedge \ldots \wedge L_n$ pour un certain entier k à trouver.
3. (0) Vérifier que toute clause, dite *tautologique*, de la forme $L_1, \ldots, L_n/k$, $k \leq 0$, est vraie dans toute interprétation ρ; et que toute clause, dite *antilogique*, de la forme $L_1, \ldots, L_n/k$, $k > n$, est fausse dans toute interprétation ρ.

Résolution avec compteurs

Dans cette partie, on va considérer que toutes les clauses étendues sont normalisées, au sens où dans $L_1, \ldots, L_n/k$, on aura toujours $0 \leq k \leq n+1$. Noter en effet que si $k \leq 0$, on obtient une clause équivalente en remplaçant k par 0; et si $k > n+1$, on obtient une clause équivalente en remplaçant k par $n+1$. On considérera d'autre part que toutes les clauses étendues engendrées par les règles à venir sont implicitement normalisées. Ceci a pour but de simplifier les raisonnements à venir.

1. (2) On considère la règle de *résolution* :

$$\frac{L_1, \ldots, L_p, L_{p+1}, \ldots, L_m/k \qquad \neg L_1, \ldots, \neg L_p, L'_{p+1}, \ldots, L'_n/k'}{L_{p+1}, \ldots, L_m, L'_{p+1}, \ldots, L'_n/(k+k'-p)}$$

   où $p \geq 1$ et le *complémentaire* $\neg L$ d'un littéral L est défini comme $\neg A$ si $L = A$, comme A si $L = \neg A$; on considère d'autre part la règle de *factorisation* :

$$\frac{\overbrace{L, \ldots, L}^{p \text{ fois}}, L_1, \ldots, L_n/k}{L, L_{i_1}, \ldots, L_{i_{n+1-k}}/1}$$

où $p \geq 1$, $1 \leq i_1 < i_2 < \ldots < i_{n+1-k} \leq n$ est n'importe quel sous-multi-ensemble de $1, \ldots, n$ de cardinal $n+1-k$.

Montrer que ces règles sont correctes : si ρ satisfait toutes les prémisses (au-dessus de la barre), alors ρ satisfait la conclusion, pour chacune de ces règles. En particulier, si une clause antilogique est déductible de S par résolution et factorisation, alors S est insatisfiable.

2. (2) Montrer que toute clause étendue $C \hat{=} L_1, \ldots, L_n/k$ ($0 \leq k \leq n+1$) est équivalente à la conjonction S_C des clauses (usuelles) $L_{i_1} \vee \ldots \vee L_{i_{n-k+1}}$, où $\{i_1, i_2, \ldots, i_{n-k+1}\}$, $1 \leq i_1 < i_2 < \ldots < i_{n-k+1} \leq n$, parcourt l'ensemble des parties à $n-k+1$ éléments de $\{1, \ldots, n\}$, autrement dit que $\rho \models C$ si et seulement si $\rho \models S_C$. (Pour résumer, et de façon légèrement imprécise, S_C est la conjonction de toutes les disjonctions de $n-k+1$ littéraux parmi les n de C.)

3. (3) Montrer que les règles de résolution et de factorisation sont complètes, autrement dit : si S est un ensemble insatisfiable de clauses étendues, alors il existe une dérivation finie d'une clause antilogique par les règles de résolution et de factorisation. On pourra utiliser la complétude de la résolution propositionnelle et utiliser une technique de relèvement similaire à celle utilisée pour montrer la complétude de la résolution au premier ordre.

Méthode de Davis-Putnam avec compteurs

1. (1) Étant donné un atome A, et une clause étendue $C \hat{=} L_1, \ldots, L_n/k$ on note $C[A := \mathbf{1}]$ la clause définie comme suit. Sans perte de généralité, on peut supposer que les L_i tels que $L_i = A$ sont $L_1, \ldots, L_p$, $p \geq 0$, que ceux tels que $L_i = \neg A$ sont $L_{p+1}, \ldots, L_q$, $q \geq p$, et que les autres sont $L_{q+1}, \ldots, L_n$, $n \geq q$. On pose alors $C[A := \mathbf{1}] \hat{=} L_{q+1}, \ldots, L_n/(k-p)$.

   Montrer que $\rho \models C[A := \mathbf{1}]$ si et seulement si $\rho[A := \top] \models C$, où $\top$ est le booléen vrai.

2. (1) Définir de même une opération $C[A := \mathbf{0}]$ telle que $\rho \models C[A := \mathbf{0}]$ si et seulement si $\rho[A := \bot] \models C$, où $\bot$ est le booléen faux.

3. (2) On note $S[A := \mathbf{1}]$ l'ensemble $\{C[A := \mathbf{1}] \mid C \in S, C[A := \mathbf{1}] \text{ non tautologique}\}$, et $S[A := \mathbf{0}]$ l'ensemble $\{C[A := \mathbf{0}] \mid C \in S, C[A := \mathbf{0}] \text{ non tautologique}\}$

   Montrer que l'algorithme suivant, en pseudo-Caml, est correct et complet, au sens où `dp(S)` termine, et que `dp(S)` retourne `true` si et seulement si S est satisfiable :

```
let dp (S) =
    if S ne contient que des tautologies  (* incluant le cas S = ∅ *)
       then true
    else if S contient une antilogie
            then false
    else let A = un atome quelconque libre dans S
           in dp (S[A := 0]) || dp (S[A := 1])
```

   où `||` est le ou logique en Caml.

4. (1) On cherche à généraliser la notion de résolution unitaire. Posons $S[L := \mathbf{1}] \hat{=} S[A := \mathbf{1}]$ si $L = A$, $S[A := \mathbf{0}]$ si $L = \neg A$, et de même $S[L := \mathbf{0}] \hat{=} S[A := \mathbf{0}]$ si $L = A$, $S[A := \mathbf{1}]$ si $L = \neg A$.

   Appelons *clause pleine* toute clause étendue de la forme $L_1, \ldots, L_n/n$. Montrer que, dès que S contient une clause pleine $L_1, \ldots, L_n/n$, alors S est satisfiable si et seulement si $S[L_1 := \mathbf{1}] \ldots [L_n := \mathbf{1}]$ l'est. En déduire que l'on peut ajouter les lignes suivantes juste avant le `let` de la définition précédente de `dp` :

```
else if S contient une clause pleine L1, ..., Ln/n, n ≥ 1
      then dp (S[L1 := 1]...[Ln := 1])
```

L'intérêt du formalisme des clauses avec compteurs, ainsi que de la procédure de résolution opérant dessus, est de pouvoir résoudre des problèmes combinatoires complexes. Notamment, Benhamou, Sais et Siegel, qui ont introduit ces notions (Belaid Benhamou, Lakhdar Sais et Pierre Siegel, Two Proof Procedures for a Cardinality Based Language in Propositional Calculus, *STACS'94*, Springer Verlag LNCS 775, pp.71–82, Caen, France, 1994) ont montré que la résolution sur clauses étendues permettait de résoudre en temps polynomial en n le problème des pigeons : étant donné $n + 1$ pigeons et n trous, montrer qu'on ne peut pas mettre chaque pigeon dans exactement un trou sans qu'un trou contienne au moins deux pigeons. Ce problème en apparence trivial requiert un temps exponentiel en n pour la plupart des méthodes de calcul propositionnel (Davis-Putnam, résolution, tableaux, BDD, même Davis-Putnam sur les clauses étendues).