Satisfiabilité d'ensembles de clauses avec compteurs

Correction.

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 $\rho \models L_1, \ldots, L_n/1$.

   $\rho \models L_1 \vee \ldots \vee L_n$ si et seulement si au moins un des L_i est vrai dans ρ; cette condition est équivalente au fait que $|\{L_i, 1 \leq i \leq k \mid \rho \models L_i\}| \geq 1$.

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.

   Prenons $k = n$, alors $\rho \models L_1, \ldots, L_n/n$ si et seulement si au moins n des n littéraux $L_1, \ldots, L_n$ sont vrais dans ρ, si et seulement si tous les L_i, $1 \leq i \leq n$, sont vrais dans ρ.

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.

   Le nombre de littéraux vrais dans ρ parmi $L_1, \ldots, L_n$ est nécessairement ≥ 0, donc $\geq k$ si $k \leq 0$; donc toute tautologie est valide. D'autre part, si $\rho \models L_1, \ldots, L_n/k$, $k > n$, alors le nombre de littéraux vrais dans ρ parmi $L_1, \ldots, L_n$ est au moins k, ce qui est absurde puisqu'il n'y a que n littéraux dans la clause.

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.

Résolution : si ρ satisfait les prémisses, alors ρ rend vrai au moins k des m littéraux $L_1,\ldots,L_p,L_{p+1},\ldots,L_m$, et au moins k' des n littéraux $\neg L_1,\ldots,\neg L_p,L'_{p+1},\ldots,L'_n$. Supposons que ρ satisfait q littéraux ($0 \leq q \leq p$) parmi L_1, ..., L_p. Alors ρ rend vrai au moins $k-q$ littéraux parmi $L_{p+1},\ldots,L_m$, et au moins $k'-(p-q)$ littéraux parmi $L'_{p+1},\ldots,L'_n$. Donc ρ rend vrai au moins $k-q+k'-(p-q) = k+k'-p$ littéraux dans la conclusion.

Factorisation : si ρ satisfait la prémisse, alors ρ rend vrai au moins k des $p+n$ littéraux de la prémisse. Si ρ rend vrai L, alors ρ vérifie trivialement la conclusion. Sinon, c'est que ρ satisfait au moins k des n littéraux $L_1,\ldots,L_n$. Alors, étant donné un sous-multi-ensemble E quelconque de $L_1,\ldots,L_n$ de cardinal $n+1-k$, si ρ rendait tous les littéraux de E faux, alors E serait disjoint du multi-ensemble des $\geq k$ littéraux satisfaits par ρ dans $L_1,\ldots,L_n$, donc $L_1,\ldots,L_n$ contiendrait au moins $(n+1-k)+k = n+1 > n$ littéraux, ce qui est impossible. Donc ρ rend au moins un littéral de E vrai, donc satisfait la conclusion.

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.)

   Si $\rho \models C$, alors au moins k des n littéraux $L_1,\ldots,L_n$ sont vrais dans ρ. Étant donnée une clause $L_{i_1} \vee \ldots \vee L_{i_{n-k+1}}$, si ρ la rendait fausse, c'est que $n-k+1$ littéraux seraient faux dans ρ; comme au moins k sont vrais, il faudrait que nous ayons au moins $(n-k+1)+k = n+1$ littéraux, mais il n'y en a que n parmi $L_1,\ldots,L_n$. Donc ρ satisfait toutes les clauses de S_C.

   Réciproquement, supposons que ρ ne satisfasse pas C. Il y a donc strictement moins de k littéraux parmi $L_1,\ldots,L_n$ qui sont vrais dans ρ. Les autres, qui sont donc au moins $n-k+1$, sont faux dans ρ. Choisissons donc $n-k+1$ littéraux faux L_{i_1}, ..., $L_{i_{n-k+1}}$ dans ρ, alors la clause $L_{i_1} \vee \ldots \vee L_{i_{n-k+1}}$ est fausse dans ρ. Cette clause étant l'une de celles de S_C, $\rho \not\models S_C$.

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.

   Supposons S insatisfiable, alors $\bigcup_{C \in S} S_C$ est un ensemble insatisfiable de clauses (usuelles), donc la clause vide (usuelle) est déductible de $\bigcup_{C \in S} S_C$ par résolution (usuelle). Il suffit donc de montrer que : (1) si $c \vee A \in S_C$ et $c' \vee \neg A \in S_{C'}$ sont deux clauses (usuelles) et c, c' leur résolvant (usuel), alors $c \vee c' \in S_{C''}$, où C'' est une clause étendue déductible à partir de $\{C, C'\}$ par résolution et factorisation; et : (2) les seules clauses étendues (normalisées) C telles que S_C contienne la clause vide $\Box$ sont des clauses antilogiques.

Commençons par (2): supposons que $C \hat{=} L_1, \ldots, L_n/k$, $1 \leq k \leq n+1$, soit telle que $\Box \in S_C$. Donc $\Box$ est de la forme $L_{i_1} \vee \ldots \vee L_{i_{n-k+1}}$, donc $n-k+1=0$, soit $k=n+1$: mais alors C est une antilogie.

Montrons maintenant (1). Écrivons C sous la forme $L_1, \ldots, L_m/k$. Alors la clause (usuelle) $c \vee A \in S_C$ est une disjonction de $m-k+1$ littéraux $L_{i_1}, \ldots, L_{i_{m-k+1}}$ parmi $L_1, \ldots, L_m$. Supposons sans perte de généralité, d'une part, que $L_{i_1}, \ldots, L_{i_{m-k+1}}$ sont $L_1, \ldots, L_{m-k+1}$, et d'autre part que parmi ces derniers, ceux qui valent exactement A sont $L_1, \ldots, L_p$, $1 \leq p \leq m-k+1$. La clause (usuelle) c est donc $L_{p+1} \vee \ldots \vee L_{m-k+1}$. Or on peut aussi former un facteur de $C = \overbrace{A, \ldots, A}^{p \text{ fois}}, L_{p+1}, \ldots, L_{m-k+1}, L_{m-k+2}, \ldots, L_m/k$ qui est $C_0 \hat{=} A, L_{p+1}, \ldots, L_{m+1-k}/1$: mais S_{C_0} est alors réduit à exactement une clause, qui est exactement $c \vee A$.

Par un raisonnement similaire, il existe un facteur $C'_0 \hat{=} \neg A, L'_{p+1}, \ldots, L'_{n+1-k'}/1$ de C' tel que $S_{C'_0}$ est réduit à une clause, qui est exactement $c' \vee \neg A$.

Si on résout C_0 avec C'_0 sur A et $\neg A$, on obtient alors la clause étendue $C'' \hat{=} L_{p+1}, \ldots, L_{m+1-k}, L'_{p+1}, \ldots, L'_{n+1-k'}/1$, et $S_{C''}$ est alors réduit à une clause, qui est exactement le résolvant (usuel) $c \vee c'$.

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.

   Notons d'abord que : $(*)$ comme aucun L_i, $q+1 \leq i \leq n$, n'est ni A ni $\neg A$, $\rho \models L_i$ si et seulement si $\rho[A := \top] \models L_i$.

   Si $\rho \models C[A := \mathbf{1}]$, alors le nombre m de littéraux L_i avec $i \geq q+1$ rendus vrais par ρ est $\geq k-p$. Par $(*)$ m est aussi le nombre de littéraux L_i avec $i \geq q+1$ rendus vrais par $\rho[A := \top]$. Or le nombre de littéraux de C rendus vrais par $\rho[A := \top]$ est exactement p de plus, soit $m+p$. Comme $m \geq k-p$, $m+p \geq k$, donc $\rho[A := \top] \models C$.

   Réciproquement, si $\rho[A := \top] \models C$, alors le nombre m de littéraux de C rendus vrais par $\rho[A := \top]$ est $\geq k$. Mais aucun littéral parmi $L_{p+1}, \ldots, L_q$ n'est rendu vrai par $\rho[A := \top]$ puisque $L_{p+1} = \ldots = L_q = \neg A$, donc les $m-p$ littéraux autres que $L_1, \ldots, L_p$ dans C rendus vrais par $\rho[A := \top]$ sont dans $C[A := \mathbf{1}]$. Par $(*)$, ce sont les mêmes qui sont vrais dans ρ, donc il y a $m-p \geq k-p$ littéraux de $C[A := \mathbf{1}]$ rendus vrais par ρ, c'est-à-dire $\rho \models C[A := \mathbf{1}]$.

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.

   Sans perte de généralité, on peut encore 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 $C[A := \mathbf{0}] \hat{=} L_{q+1}, \ldots, L_n/k-(q-p)$. La preuve est essentiellement identique à celle de la question précédente.

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.

Soit $\#(S)$ le nombre de variables propositionnelles libres dans S. Il est clair que $\#(S[A := \mathbf{0}])$ et $\#(S[A := \mathbf{1}])$ valent au plus $\#(S) - 1$, donc $\#(S)$ décroît à chaque appel récursif à `dp` *: donc* `dp` *termine.*

Montrons maintenant que `dp(S)` *retourne* `true` *si et seulement si S est satisfiable, par récurrence sur $\#(S)$. Observons d'abord que si S ne contient que des tautologies, alors* `dp(S)` *retourne* `true` *et S est satisfiable (S est satisfaite par n'importe quelle interprétation). D'autre part, si S contient une antilogie, alors* `dp(S)` *retourne* `false` *et S est insatisfiable.*

Plaçons-nous donc dans le cas où S ne contient pas que des tautologies, et ne contient pas d'antilogie. Si $\#(S) = 0$, alors S ne contient que des clauses de la forme $\Box/k$, qui sont toutes soit des tautologies ($k \leq 0$) soit des antilogies ($k > 0$), donc ce cas ne se présente pas. Soit A l'atome choisi par `dp` *dans le* `let`*, et soit ρ une interprétation satisfaisant S. Si $\rho(A) = \bot$, alors par les questions précédentes $\rho \models S[A := \mathbf{0}]$, donc $S[A := \mathbf{0}]$ est satisfiable, et par hypothèse de récurrence* `dp(S[A :=` $\mathbf{0}$`])` *retourne* `true`*. Sinon, $S[A := \mathbf{1}]$ est satisfiable, donc par hypothèse de récurrence* `dp(S[A :=` $\mathbf{1}$`])` *retourne* `true`*.*

Réciproquement, supposons que `dp(S)` *retourne* `true`*. Alors* `dp(S[A :=` $\mathbf{0}$`])` *ou* `dp(S[A :=` $\mathbf{1}$`])` *retourne* `true`*. Par hypothèse de récurrence, ceci implique que $S[A := \mathbf{0}]$ ou $S[A := \mathbf{1}]$ est satisfiable. Mais par les questions précédentes, ceci implique que S est satisfiable.*

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 $L_1, \ldots, L_n/n$, $n \geq 1$
         `then dp` $(S[L_1 := \mathbf{1}] \ldots [L_n := \mathbf{1}])$

   Supposons que S contienne une clause pleine $L_1, \ldots, L_n/n$, alors si ρ satisfait S, $\rho \models L_1, \ldots, L_n/n$, donc le nombre de littéraux parmi $L_1, \ldots, L_n$ rendus vrais par ρ est exactement n. C'est donc que ρ rend chaque L_i vrai. Or, que les L_i soient des A_i ou des $\neg A_i$, par les questions 1 et 2, ρ satisfait donc aussi $S[L_1 := \mathbf{1}] \ldots [L_n := \mathbf{1}]$. Réciproquement, si ρ satisfait donc aussi $S[L_1 := \mathbf{1}] \ldots [L_n := \mathbf{1}]$, alors $\rho[L_1 := \top] \ldots [L_n := \top]$ satisfait S, par les questions 1 et 2, où la notation $\rho[L := \top]$ dénote $\rho[A := \top]$ si $L = A$ et $\rho[A := \bot]$ si $L = \neg A$.

   L'algorithme reste correct si on ajoute les lignes mentionnées. Le seul point délicat est de vérifier que la terminaison est préservée. Mais comme le test est fait sur les clauses pleines de cardinal $n \geq 1$, comme au cas précédent, le nombre $\#(S)$ d'atomes libres dans S décroît toujours strictement à chaque appel récursif de `dp`*.*

   En pratique, on élimine évidemment le cas pathologique des tautologies, incluant les $\Box/0$, de S avant l'appel à `dp`*, sachant qu'il ne sera plus jamais recréé (vu que ni $S[A := \mathbf{0}]$ ni $S[A := \mathbf{1}]$ ne contient de tautologie par construction). On peut alors remplacer le premier test* `if` *de* `dp` *par le test plus simple $S = \emptyset$.*

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).