Devoir de logique: calcul propositionnel

February 18, 2014

Soit $\mathcal{P}_n = \{a_{i,j} \mid 1 \leq i \leq n+1, 1 \leq j \leq n\}$ un ensembe de variables propositionnelles paramétré par $n \in \mathbb{N}, n \geq 1$. On note $\Gamma_n = \{\bigvee_{j=1}^{n} a_{ij} \mid 1 \leq i \leq n+1\}$ et $\Delta_n = \{a_{i_1,j} \wedge a_{i_2,j} \mid 1 \leq j \leq n, 1 \leq i_1 < i_2 \leq n+1\}$.

PHP_n est le séquent $\Gamma_n \vdash \Delta_n$. Montrer que c'est une tautologie.

Sous forme clausale, PHP_n est codé par l'ensemble des clauses $S_n = \Gamma_n \cup \overline{\Delta_n}$ où $\overline{\Delta_n} = \{\neg a_{i_1,j} \vee \neg a_{i_2,j} \mid 1 \leq j \leq n, 1 \leq i_1 < i_2 \leq n+1\}$. Montrer que S_n est insatisfaisable.
La *taille* d'une formule (resp. d'un séquent) ϕ est le nombre de connecteurs logiques et d'occurrences de variables propositionnelles de ϕ.

La *taille* d'une preuve par résolution est le nombre d'applications de la règle de résolution dans la preuve (on ne compte pas les factorisations).

La *taille* d'une preuve en calcul des séquents est le nombre de règles qui sont soit des coupures, soit des règles d'introduction (on ne compte pas les contractions ou affaiblissements).

1 Il n'y a pas de petite preuve de PHP en calcul des séquents sans coupure

Dans toute la question, on ne considère que des séquents $\Gamma \vdash \Delta$ construits sur les variables propositionnelles et les seuls connecteurs logiques $\vee, \wedge$.

Si σ est une application d'un sous-ensemble des variables propositionnelles de $\mathcal{P}$ dans $\{\top, \bot\}$, on note $\Gamma^\sigma \vdash \Delta^\sigma$ le séquent défini comme suit:

- $P^\sigma = \sigma(P)$ si P est dans le domaine de σ
- $(\phi \vee \psi)^\sigma = \top$ si $\phi^\sigma = \top$ ou $\psi^\sigma = \top$. $(\phi \vee \psi)^\sigma = \phi^\sigma$ si $\psi^\sigma = \bot$, $(\phi \vee \psi)^\sigma = \psi^\sigma$ si $\phi^\sigma = \bot$. Dans les autres cas, $(\phi \vee \psi)^\sigma = \phi^\sigma \vee \psi^\sigma$
- $(\phi \wedge \psi)^\sigma = \phi^\sigma$ si $\psi^\sigma = \top$, $(\phi \wedge \psi)^\sigma = \psi^\sigma$ si $\phi^\sigma = \top$, $(\phi \wedge \psi)^\sigma = \bot$ si $\phi^\sigma = \bot$ ou $\psi^\sigma = \bot$. Dans les autres cas, $(\phi \wedge \psi)^\sigma = \phi^\sigma \wedge \psi^\sigma$.
- $(\phi_1, \ldots, \phi_p)^\sigma \vdash (\psi_1, \ldots, \psi_q)^\sigma$ est le séquent $\{\phi_i^\sigma \mid \phi_i^\sigma \neq \top\} \vdash \{\psi_j^\sigma \mid \psi_j^\sigma \neq \bot\}$ si, pour rout j, $\psi_j\sigma \neq \top$ et, pour tout i, $\phi_i^\sigma \neq \bot$. Sinon c'est le séquent $\bot \vdash \top$.

Si π est une application d'un ensemble $\mathcal{P}$ de variables propositonnelles dans un ensemble $\mathcal{Q}$ de variables propositionnelles, π est étendue aux formules de manière compatible avec les connecteurs logiques ($\pi(\phi \vee \psi) = \pi(\phi) \vee \pi(\psi)$ par exemple) et par l'identité sur les variables propositionnelles qui ne sont pas dans $\mathcal{P}$.

On dit que PHP_n *se plonge dans* $\Gamma \vdash \Delta$, s'il existe un sous ensemble σ des variables propositionnelles de $\Gamma \vdash \Delta$ et une injection π de $\mathcal{P}_n$ dans l'ensemble des variables propositionnelles de $\Gamma \vdash \Delta$ telle que $\Gamma^\sigma \vdash \Delta^\sigma = \pi(\Gamma_n \vdash \Delta_n)$.

1. Montrer que, si π est une preuve de $\Gamma \vdash \Delta$ dans le calcul des séquents sans coupure, alors, pour tout σ, il existe une preuve de $\Gamma^\sigma \vdash \Delta^\sigma$ de taille inférieure ou égale à celle de π dans le calcul des séquents sans coupure.

2. Soit $\Gamma \vdash \Delta$ un séquent tel que toutes les formules de Γ sont construites à l'aide des variables propositionnelles et du seul connecteur logique $\vee$ et toutes les formules de Δ sont construites à l'aide des variables propositionnelles et du seul connecteur logique $\wedge$, Supposons que $\Gamma \vdash \Delta$ s'obtient, soit par introduction du $\vee$ à gauche, soit par introduction du $\wedge$ à droite, à partir des séquents $\Gamma' \vdash \Delta'$ et $\Gamma'' \vdash \Delta''$.

   Montrer que, si PHP_{n+1} se plonge dans $\Gamma \vdash \Delta$, alors

   - ou bien $\Gamma_n \vdash \Delta_n$ se plonge dans $\Gamma' \vdash \Delta'$ et $\Gamma_n \vdash \Delta_n$ se plonge dans $\Gamma'' \vdash \Delta''$
   - ou bien $\Gamma_{n+1} \vdash \Delta_{n+1}$ se plonge dans l'un des séquents $\Gamma' \vdash \Delta'$, $\Gamma'' \vdash \Delta''$.

3. Montrer que toute preuve de $\Gamma_n \vdash \Delta_n$ dans le calcul des séquents sans coupure est de taille au moins $2^n - 1$.

2 Simulation du calcul des séquents sans coupure par la résolution

Si ϕ est une formule du calcul propositionnel (qu'on voit ici comme un arbre étiqueté par les connecteurs logiques), on associe à ϕ une variable propositionnelle A_ψ par sous-formule $\psi \notin \mathcal{P} \cup \{\top, \bot\}$. Par convention, $A_P = P$ si $P \in \mathcal{P}$. On note $c(\phi)$ l'ensemble des formules:

- $c(\phi) = \emptyset$ si $\phi \in \mathcal{P} \cup \{\top, \bot\}$
- $c(\neg\phi) = \{\neg A_{\neg\phi} \vee \neg A_\phi, A_\phi \vee A_{\neg\phi}\} \cup c(\phi)$
- $c(\phi \vee \psi) = \{\neg A_{\phi\vee\psi} \vee A_\phi \vee A_\psi, \neg A_\phi \vee A_{\phi\vee\psi}, \neg A_\psi \vee A_{\phi\vee\psi}\} \cup c(\phi) \cup c(\psi)$
- $c(\phi \wedge \psi) = \{A_{\phi\wedge\psi} \vee \neg A_\phi \vee \neg A_\psi, \neg A_{\phi\wedge\psi} \vee A_\phi, \neg A_{\phi\wedge\psi} \vee A_\psi\} \cup c(\phi) \cup c(\psi)$
- $c(\phi \to \psi) = \{\neg A_{\phi\to\psi} \vee \neg A_\phi \vee A_\psi, A_{\phi\to\psi} \vee \neg A_\psi, A_\phi \vee A_{\phi\to\psi}\} \cup c(\phi) \cup c(\psi)$

1. Montrer que, si $\mathcal{E}$ est un ensemble de clauses satisfaisable et π est une preuve par résolution de $\mathcal{E}, L \vdash\bot$ où L est un littéral, alors il existe une preuve par résolution π' de $\mathcal{E} \vdash \overline{L}$, de taille inférieure ou égale à celle de π.

2. Montrer qu'il existe un polynôme P telle que, si π est une preuve de $\Gamma \vdash \Delta$ dans le calcul des séquents sans coupure, alors il existe une preuve π' par résolution de $\{c(\phi) \mid \phi \in \Gamma \cup \Delta\} \cup \{A_\phi \mid \phi \in \Gamma\} \cup \{\neg A_\psi \mid \psi \in \Delta\} \vdash\bot$ telle que la taille de π' est bornée par $P(|\pi|)$.

3 Il n'y a pas de preuve courte de PHP par résolution

On fixe une preuve d'insatisfaisabilité de S_n par résolution et factorisation binaire. On note D_n l'ensemble des clauses dérivées par cette preuve (les clauses étiquetant les noeuds de la preuve). On suppose de plus que D_n est de cardinal minimal.

1. On note $V(C)$ l'ensemble des variables propositionnelles apparaissant dans C et $\widehat{a_{i,j}}$ la clause $a_{1,j} \vee \cdots \vee a_{i-1,j} \vee a_{i+1,j} \vee \cdots \vee a_{n+1,j}$. Si C est une clause, $\widehat{C}$ est la clause obtenue en remplaçant tous les littéraux négatifs $\neg P$ par $\widehat{P}$ dans C.

   On note $\mathcal{I}^-$ l'ensemble des interprétations α telles qu'il existe exactement un indice i tel que:

   - pour tout $k \neq i$, il existe un unique indice j_k, tel que $a_{k,j_k} \in \alpha$
   - $a_{i,1}, \ldots, a_{i,n} \notin \alpha$

   Pour toute clause C on note enfin

   $$w(C) = \min\{|W| \mid W \subseteq \Gamma_n, \forall \alpha \in \mathcal{I}^-, \alpha \models W \text{ entraine } \alpha \models C\}$$

   (a) Montrer que, si $\alpha \in \mathcal{I}^-$, alors $\alpha \models C$ ssi $\alpha \models \widehat{C}$.

   (b) Calculer $w(C)$ pour $C \in \Gamma_n$, $C \in \overline{\Delta_n}$ et $C = \perp$.

   (c) Montrer que, si C s'obtient à partir de C_1, C_2 par une étape de résolution binaire, alors $w(C) \leq w(C_1) + w(C_2)$.

   (d) En déduire qu'il existe $C_0 \in D_n$ telle que $\frac{n+1}{3} \leq w(C_0) \leq 2 \times \frac{n+1}{3}$.

   (e) Montrer que, pour toute clause C, $|V(\widehat{C})| \geq w(C) \times (n + 1 - w(C))$.

   (f) En déduire le lemme de Haken: D_n contient une clause C_0 telle que $|V(\widehat{C_0})| \geq 2 \times \frac{(n+1)^2}{9}$.

2. Soit $L_n = \{\widehat{C} \mid C \in D_n, |V(\widehat{C})| \geq \frac{(n+1)^2}{8}\}$.

   (a) Montrer qu'il existe une variable $a_{i,j}$ qui apparaît dans au moins $\frac{|L_n|}{8}$ clauses de L_n.

   (b) Montrer qu'il existe une preuve d'insatisfaisabilité de S_{n-1} par résolution binaire telle que $|L_{n-1}| \leq \frac{7}{8}|L_n|$.

   (c) En utilisant la question 1f (et l'inégalité $(\frac{8}{7})^6 \geq 2$) montrer que $|L_n| \geq 2^{\frac{n+1}{24}}$.
   Et donc que toute preuve d'insatisfaisabilité de S_n par résolution et factorisation binaire contient au moins $2^{\frac{n+1}{24}}$ noeuds distincts...

4 Il existe une preuve courte de PHP dans le calcul des séquents avec coupure

C'est l'objet d'un autre DM...

Solution

Il n'y a pas de petite preuve de PHP en calcul des séquents sans coupure

1. On montre ce résultat par récurrence sur la taille de π:

   - Si π est réduite à un axiome, alors $\bot \in \Gamma$ ou $\top \in \Delta$, ou $\Gamma \cap \Delta \neq \emptyset$. Dans les deux premiers cas, la situation est inchangée pour $\Gamma^\sigma, \Delta^\sigma$.

     Dans le dernier cas, si $P \in \Gamma \cap \Delta$, ou bien P n'est pas dans le domaine de σ et dans ce cas $P^\sigma \in \Gamma^\sigma \cap \Delta^\sigma$. ou bien $\sigma(P) = \top$ et dans ce cas $\top = \Delta^\sigma$, ou bien $\sigma(P) = \bot$ et dans ce cas $\Gamma^\sigma = \bot$.

     Dans tous les cas $\Gamma^\sigma \vdash \Delta^\sigma$ s'obtient grâce à un axiome.

   - Si π n'est pas réduit à une feuille, 4 cas se présentent suivant la dernière règle d'inférence appliquée:

     – introduction du $\vee$ à gauche

     $$\dfrac{\dfrac{\pi_1}{\Gamma, \phi \vdash \Delta} \qquad \dfrac{\pi_2}{\Gamma, \psi \vdash \Delta}}{\Gamma, \phi \vee \psi \vdash \Delta}$$

     Par hypothèse de récurrence, il existe des preuves π_1^σ et π_2^σ de $(\Gamma, \phi)^\sigma \vdash \Delta^\sigma$ et $(\Gamma, \psi)^\sigma \vdash \Delta^\sigma$ respectivement, telles que $|\pi_1^\sigma| \leq |\pi_1|$ et $|\pi_2^\sigma| \leq |\pi_2|$.
     Si $(\phi \vee \psi)^\sigma = \phi^\sigma \vee \psi^\sigma$, alors il suffit de choisir pour π^σ la preuve obtenue en appliquant une introduction gauche de $\vee$ aux deux séquents $(\Gamma, \phi)^\sigma \vdash \Delta^\sigma$ et $(\Gamma, \psi)^\sigma \vdash \Delta^\sigma$. La preuve obtenue est de taille $1 + |\pi_1^\sigma| + |\pi_2^\sigma| \leq |\pi|$.
     Si $\phi^\sigma = \bot$ alors $(\phi \vee \psi)^\sigma = \psi^\sigma$ et il suffit de choisir $\pi^\sigma = \pi_2^\sigma$: $|\pi^\sigma| \leq |\pi_2| < |\pi|$.
     Si $\psi^\sigma = \bot$, il suffit de choisir $\pi^\sigma = \pi_1^\sigma$.
     Si $(\phi \vee \psi)^\sigma = \top$, alors $\phi^\sigma = \top$ ou $\psi^\sigma = \top$ et il suffit à nouveau de choisir π_1^σ ou π_2^σ pour π^σ.

     – introduction de $\wedge$ à gauche.

     $$\dfrac{\dfrac{\pi_1}{\Gamma, \phi, \psi \vdash \Delta}}{\Gamma, \phi \wedge \psi \vdash \Delta}$$

     De même que dans le cas précédent: si $\phi^\sigma = \top$ ou $\psi^\sigma = \top$, il suffit de choisir $\pi^\sigma = \pi_1^\sigma$. Si $\phi^\sigma = \bot$ ou $\psi^\sigma = \bot$, on a une preuve triviale (de taille 1). Dans les autres cas, on peut appliquer la règle d'introduction de $\wedge$ à gauche à π_1^σ et on obtient une preuve π^σ de taille inférieure ou égale à celle de π.

     – introduction de $\wedge$ à droite

     $$\dfrac{\dfrac{\pi_1}{\Gamma \vdash \Delta, \phi} \qquad \dfrac{\pi_2}{\Gamma \vdash \Delta, \psi}}{\Gamma \vdash \Delta, \phi \wedge \psi}$$

     Si $\phi^\sigma = \top$ (resp. $\psi^\sigma = \top$), il suffit de choisir $\pi^\sigma = \pi_2^\sigma$ (resp. $\pi^\sigma = \pi_1^\sigma$). Si $\phi^\sigma = \bot$ (resp. $\psi^\sigma = \bot$), il suffit de choisir $\pi^\sigma = \pi_1^\sigma$ (resp. $\pi^\sigma = \pi_2^\sigma$).
     Dans les autres cas, $(\phi \wedge \psi, \Delta)^\sigma = \phi^\sigma \wedge \psi^\sigma, \Delta^\sigma$ et il suffit de choisir π^σ comme la preuve obtenue à partir de π_1^σ et π_2^σ par introduction du $\wedge$ à droite.

– introduction de $\vee$ à droite

$$\dfrac{\dfrac{\pi_1}{\Gamma \vdash \Delta, \phi, \psi}}{\Gamma \vdash \Delta, \phi \vee \psi}$$

Si $\phi^\sigma = \perp$ ou $\psi^\sigma = \perp$, on choisit $\pi^\sigma = \pi_1^\sigma$. Si $\phi^\sigma = \top$ ou $\psi^\sigma = \top$, on a une preuve triviale (en une étape). Sinon, il suffit d'appliquer $\vee$-r à π_1^σ.

2. soient σ et π tels que $\Gamma^\sigma \vdash \Delta^\sigma = \pi(\Gamma_{n+1} \vdash \Delta_{n+1})$,

- Si la dernière règle est une introduction gauche:

$$\frac{\Gamma, \phi \vdash \Delta \quad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \vee \psi \vdash \Delta}$$

– Si $(\phi \vee \psi)^\sigma = \top$ alors Γ_{n+1} se plonge dans $\Gamma, \phi \vdash \Delta$ (cas où $\phi^\sigma = \top$) ou dans $\Gamma, \psi \vdash \Delta$ (cas où $\psi^\sigma = \top$). Dans les deux cas on utilise les mêmes σ, π.

– Sinon, on montre que $\Gamma_n \vdash \Delta_n$ se plonge dans les deux prémisses. Par symétrie, il suffit de considérer $\Gamma, \phi \vdash \Delta$. Comme $\phi^\sigma \neq \top$, les variables propositionnelles de ϕ ne sont pas dans σ. Soit P l'une d'elles.
Par injectivité de π, il existe au plus une variable $a_{i_0,j_0} \in \mathcal{P}_n$ telle que $\pi(a_{i_0,j_0}) = P$. On définit π' par $\pi'(a_{i,j}) = \pi(a_{i+\epsilon(i),j+\theta(j)})$ où $\epsilon(i) = \begin{cases} 0 \text{ Si } i < i_0 \\ 1 \text{ Sinon} \end{cases}$ et $\theta(j) = \begin{cases} 0 \text{ Si } j < j_0 \\ 1 \text{ Sinon} \end{cases}$

$$\Gamma^\sigma = \{\bigvee_{j=1}^{n+1} \pi(a_{i,j}) \mid 1 \leq i \leq n+2\}$$

On considère σ' définie par:

  * si Q est dans le domaine de σ, alors $\sigma'(Q) = \sigma(Q)$
  * $\sigma(P) = \top$
  * $\sigma(Q) = \perp$ si $\pi(a_{i,j_0}) = Q$ et $i \neq i_0$ ou si $\pi(a_{i_0,j}) = Q$ et $j \neq j_0$.

$(\Gamma, \phi)^{\sigma'} \vdash \Delta^{\sigma'} = \Gamma^{\sigma'} \vdash \Delta^{\sigma'}$.

$$\Gamma^{\sigma'} = \{\bigvee_{1 \leq j \leq n+1, j \neq j_0} \pi(a_{i,j}) \mid 1 \leq i \leq n+2, i \neq i_0\} = \{\bigvee_{j=1}^{n} \pi'(a_{i,j}) \mid \ \leq i \leq n+1\}$$

De plus, comme $(\pi(a_{i_0,j}) \wedge \pi(a_{i_1,j}))^{\sigma'} = \perp$ si $i_1 \neq i_0$

$$\begin{aligned} \Delta^{\sigma'} &= \{\pi(a_{i_1,j}) \wedge \pi(a_{i_2,j}) \mid 1 \leq i_1 < i_2 \leq n+2, i_1 \neq i_0, i_2 \neq i_0, j \neq j_0\} \\ &= \{\pi'(a_{i_1,j}) \wedge \pi'(a_{i_2,j}) \mid 1 \leq i_1 < i_2 \leq n+1, 1 \leq j \leq n\} \end{aligned}$$

- Si la dernière règle est une introduction droite,

$$\frac{\Gamma \vdash \phi, \Delta \quad \Gamma \vdash \psi, \Delta}{\Gamma \vdash \phi \wedge \psi, \Delta}$$

La preuve est très semblable au cas précédent:

– Si $(\phi \wedge \psi)^\sigma =\perp$, alors $\Gamma_{n+1} \vdash \Delta_{n+1}$ se plonge dans $\Gamma \vdash \Delta, \phi$ (cas où $\phi^\sigma =\perp$) ou dans $\Gamma \vdash \Delta, \psi$ (cas où $\psi^\sigma =\perp$).
– Sinon, $\phi^\sigma = \pi(a_{i_1,j_0})$ et $\psi^] sigma = \pi(a_{i_2,j_0})$ avec $i_1 \neq i_2$. Pour le séquent $\Gamma \vdash \phi, \Delta$, on étend σ en affectant a_{i_2,j_0} à $\top$, et $a_{i_2,j}$, $j \neq j_0$ à $\perp$ et a_{i,j_0}, $i \neq i_2$ à $\perp$. De cette manière, $\phi^{\sigma'} =\perp$.
  On construit ensuite π' comme dans le premier cas, et on obtient un plongement de $\Gamma_n \vdash \Delta_n$

3. On montre ce résultat par récurrence sur n: pour $n = 1$, la preuve de $a_{1,2}, a_{2,2} \vdash a_{1,2} \wedge a_{2,2}$ utile une règle d'introduction et un axiome. Sa taille est $1 = 2^1 - 1$.

   Si Π_{n+1} est une preuve de taille minimale de $\Gamma_{n+1} \vdash \Delta_{n+1}$ dans le calcul des séquents sans coupure, soit $\Gamma' \vdash \Delta'$ et $\Gamma'' \vdash \Delta''$ les deux prémisses de la dernière règle de Π_{n+1}. D'après la question précédente, $\Gamma_{n+1} \vdash \Delta_{n+1}$ se plonge dans l'une des deux prémisses (disons $\Gamma' \vdash \Delta'$) ou $\Gamma_n \vdash \Delta_n$ se plonge dans les deux séquents.

   Supposons d'abord $\pi(\Gamma_{n+1} \vdash \Delta_{n+1}) = \Gamma'^\sigma \vdash \Delta'^\sigma$. D'après la première question, il existe une preuve de $\Gamma'^\sigma \vdash \Delta'^\sigma$ de taille infŕieure à la preuve de $\Gamma' \vdash \Delta'$ et donc strictement inférieure à la taille de Π. Mais dans ce cas $\pi^{-1}(\Pi)$ est une preuve de $\Gamma_{n+1} \vdash \Delta_{n+1}$, contredisant la minimalité de Π. (Noter que π est une injection, mais comme il y a égalité des séquents, c'est aussi une surjection sur l'ensemble des variables propositionnelles de $\Gamma'^\sigma \vdash \Delta'^\sigma$, donc π^{-1} est bien définie et l'image de la preuve est une preuve).

   Si maintenant $\pi_1(\Gamma_n \vdash \Delta_n) = \Gamma'^{\sigma_1} \vdash \Delta'^{\sigma_1}$ et $\pi_2(\Gamma_n \vdash \Delta_n) = \Gamma''^{\sigma_2} \vdash \Delta''^{\sigma_2}$. D'après la première question les preuves $\Pi_1^{\sigma_1}$ de $\Gamma'^{\sigma_1} \vdash \Delta'^{\sigma_1}$ et $\Pi_2^{\sigma_2}$ de $\Gamma''^{\sigma_2} \vdash \delta''^{\sigma_2}$ sont de taille respectivement inférieures aux tailles des preuves Π_1 de $\Gamma' \vdash \Delta'$ et Π_2 de $\Gamma'' \vdash \Delta''$.

   Comme $\pi_1^{-1}(\Pi_1^{\sigma_1})$ et $\pi_2^{-1}(\Pi_2^{\sigma_2})$ sont des preuves de $\Gamma_n \vdash \Delta_n$, par hypothèse de récurrence, $|\Pi_1^{\sigma_1}| \geq 2^n - 1$ et $|\Pi_2^{\sigma_2}| \geq 2^{n-1}$. Par conséquent,

$$|\Pi| = 1 + |\Pi_1| + |\Pi_2| \geq 1 + |\Pi_1^{\sigma_1}| + |\Pi_2^{\sigma_2}| \geq 1 + 2^n - 1 + 2^n - 1 = 2^{n+1} - 1$$

2. Simulation du calcul des séquents sans coupure par la résolution

1. On montre par récurrence sur la longueur d'une preuve de taille $n \geq 1$ que, pour toute clause C, si $\mathcal{E}, \overline{L} \vdash C$, alors ou bien $\mathcal{E} \vdash C$, ou bien $\mathcal{E} \vdash C \vee L$, et, dans le dernier cas, la preuve est de taille au plus n.

   - Dans le cas de base, trois situations se présentent:
     – il existe deux clauses $C_1, C_2 \in \mathcal{E}$ telles que, par résolution, $C_1, C_2 \vdash C$. Dans ce cas $\mathcal{E} \vdash C$
     – il existe une clause $C_1 \in \mathcal{E}$ telle que $C_1 \vdash C$ et, à nouveau $\mathcal{E} \vdash C$
     – il existe une clause $C \vee L \in \mathcal{E}$ et $C \vee L, \overline{L} \vdash C$. Dans ce dernier cas $C \vee L \in \mathcal{E}$ et donc $\mathcal{E} \vdash C \vee L$ et la preuve obtenue est de taille 0 (donc inférieure à 1).
   - Supposons que la propriété est vraie pour des preuves de taille $n \geq 1$ et considérons une preuve de taille $n + 1$. On distingue alors deux cas, selon la dernière règle appliquée:

– C'est une résolution entre C_1 et C_2:

$$\dfrac{\dfrac{\pi_1}{C_1} \quad \dfrac{\pi_2}{C_2}}{C}$$

Par hypothèse de récurrence, ou bien $\mathcal{E} \vdash C_1$ et $\mathcal{E} \vdash C_2$, et dans ce cas $\mathcal{E} \vdash C_1 \vee C_2$, ou bien pour l'un des indices au moins (par exemple $i = 1$), il existe une preuve π'_i de $C_i \vee L$ telle que $|\pi'_i| \leq |\pi_i|$. On obtient alors la preuve de $C \vee L$:

$$\dfrac{\dfrac{\pi'_1}{C_1 \vee L} \quad \dfrac{\pi_2}{C_2}}{C \vee L}$$

Dont la taille est inférieure à $|\pi_1| + |\pi_2| + 1$.

– ** cas a revoir ** C'est une factorisation de C_1: $E, \neg P \vdash C_1 \vdash_{fact} C$. Par hypothèse de récurrence, $E \vdash C_1$ ou $E \vdash C_1 \vee P$, dans les deux cas, par factorisation, on obtient $E \vdash C$ ou $E \vdash C \vee P$.

Il suffit alors d'appliquer ce résultat avec $C = \perp$: comme $\mathcal{E}$ est satisfaisable, si $\mathcal{E}, \overline{L} \vdash \perp$, on obtient une preuve de taille inférieure de $\mathcal{E} \vdash L$.

2. On prend pour polynome $P(n) = 3n$. ** question a terminer ** On note $c(\Gamma) = \{c(\phi)\ \phi \in \Gamma\} \cup \{A_\phi, \phi \in \Gamma\}$ et $c(\Delta) = \{c(\phi), \phi \in \Delta\} \cup \{\neg A_\phi, \phi \in \Delta\}$

On raisonne par récurrence sur la taille de la preuve. Par exemple, dans le cas d'une introduction de $\vee$ à gauche, par HR, soit π_1 une preuve de contradiction de $c(\Gamma), c(\phi), c(\Delta), A_\phi$ et π_2 une preuve de contradiction de $c(\Gamma), c(\psi), c(\Delta), A_\psi$ telles que $|\pi_1| + |\pi_2| \leq 3 \times (|\pi| - 1)$.

Par la première question, on a des preuves π'_1, π'_2 par résolution de $c(\Gamma), c(\Delta), c(\phi), \vdash \neg A_\phi$ et $c(\Gamma), c(\Delta), c(\psi) \vdash \neg A_\psi$.

$$\dfrac{\dfrac{\dfrac{A_{\phi\vee\psi} \quad \neg A_{\phi\vee\psi} \vee A_\phi \vee A_\psi}{A_\phi \vee A_\psi} \quad \dfrac{\pi'_1}{\neg A_\phi}}{A_\psi} \quad \dfrac{\pi'_2}{\neg A_\psi}}{\perp}$$

La preuve obtenue est de taille inférieure à $3(|\pi| - 1) + 3$...

3. Il n'y a pas de preuve courte de PHP par résolution

1. (a) Montrons d'abord que, pour $\alpha \in \mathcal{I}^-$, $\alpha \models \neg a_{i,j}$ ssi $\alpha \models a_{1,j} \vee \ldots \vee a_{i-1,j} \vee a_{i+1,j} \vee \ldots \vee a_{n+1,j}$. Les interprétations $\alpha \in \mathcal{I}^-$ sont caractérisées par un indice $i_\alpha \in \{1, ..., n+1\}$ et une bijection θ_α de $\{1, ..., n+1\} \setminus \{i_\alpha\}$ dans $\{1, \ldots, n\}$: $a_{j,\ell} \in \alpha$ ssi $\ell = \theta_\alpha(j)$. $\alpha \models \neg a_{i,j}$ ssi $i \neq \theta_\alpha^{-1}(j)$ ssi $a_{\theta^{-1}(j),j} \in \{a_{1,j}, \ldots, a_{i-1,j}, a_{i+1,j}, \ldots, a_{n+1,j}\}$ ssi $\alpha \models a_{1,j} \vee \ldots \vee a_{i-1,j} \vee a_{i+1,j} \vee \ldots \vee a_{n+1,j}$.

Il en résulte que, pour tout $\alpha \in \mathcal{I}^-$ et toute clause C, $\alpha \models \neg a_{i,j} \vee C$ ssi $\alpha \models \widehat{a_{i,j}} \vee C$. Par récurrence sur le nombre de littéraux négatifs de C on obtient le résultat voulu.

(b) Si $C \in \Gamma_n$, il suffit de choisir $W = \{C\}$ $\alpha \models W$ entraine $\alpha \models C$. Par ailleurs, il existe un $\alpha \in \mathcal{I}^-$ qui falsifie C. Donc $w(C) = 1$.

Si $C \in \overline{\Delta_n}$, alors comme α induit une bijection θ_α de $\{1, \ldots, n+1\} \setminus \{i_\alpha\}$ dans $\{1, \ldots, n\}$, $\alpha \models C$. Il en résulte que $w(C) = 0$.

Si W est un sous-ensemble à n éléments de Γ_n, il existe un indice i tel que $a_{i,1} \vee \cdots \vee a_{i,n} \notin W$. Les interprétations de $\mathcal{I}^-$ ne contenant aucun $a_{i,j}, i = 1, ..., n$ satisfont alors W: $w(\perp) > n$. D'autre part, aucune interprétation de $\mathcal{I}^-$ ne satisfait Γ_n, puisqu'elles satisfont toutes les clauses de $\overline{\Delta_n}$ et S_n est insatisfaisable d'après la question précédente. Il en résulte que $w(\perp) = n + 1$.

(c) Soient W_i, $i = 1, 2$ des sous-ensemble de Γ_n de cardinal minimal tel que, pour tout $\alpha \in \mathcal{I}^-$, $\alpha \models W_i$ entraine $\alpha \models C_i$. Alors, si $W = W_1 \cup W_2$, $\alpha \models W$ entraine que $\alpha \models C_1$ et $\alpha \models C_2$. Soit $C_1 = C'_1 \vee a_{i,j}$ et $C_2 = C'_2 \vee \neg a_{i,j}$. $\alpha \models C_1 \wedge C_2$ entraine que $\alpha \models C'_1$ ou bien $a_{i,j} \in \alpha$ et, dans ce dernier cas, $\alpha \models C'_2$. Dans tous les cas $\alpha \models C'_1 \vee C'_2$. Il en résulte que $w(C'_1 \vee C'_2) \leq |W_1 \cup W_2| \leq w(C_1) + w(C_2)$.

(d) Considérons un arbre t_0 de preuve par résolution binaire et factorisation, qui conduit à la clause vide et dont les noeuds sont étiquetés par des éléments de D_n. Associons à chaque noeud d'étiquette C l'entier $w(C)$. On extrait un sous-arbre de t_0 de la manière suivante: soit $e(t)$ définie sur les arbres de preuves par:

- Si C étiquette la racine de t et $w(C) \leq 2 \times \frac{n+1}{3}$, alors retourner t.
- Sinon, l'arbre n'est pas réduit à une feuille d'après (b). Si la dernie̊re règle est une factorisation, retourner $e(t')$ où t' est l'unique fils de la racine de t.
- Sinon soient t_1, t_2 les fils de la racine de t, étiquetés respectivement par C_1, C_2. Retourner $e(t_i)$ tel que $w(C_i) = \max\{w(C_1).w(C_2)\}$.

Par (b), $e(t_0) \neq t_0$. $e(t_0)$ a une racine étiquetée par C_1 telle que $w(C_1) \leq 2 \times \frac{n+1}{3}$. Son père est étiqueté par C tel que $w(C) > 2 \times \frac{n+1}{3}$ et son frère unique est étiqueté par C_2 telle que $w(C_2) \leq w(C_1)$. Or, d'après (c), $w(C_1)+w(C_2) \geq w(C) > 2\times \frac{n+1}{3}$. Donc $w(C_1) > \frac{n+1}{3}$ et C_1 est la clause cherchée.

(e) Soit $W \subseteq \Gamma_n$ tel que $|W| = w(C)$. Si $w(C) = 0$, le résultat est démontré, de même si $w(C) = n+1$. Supposons désormais $n \geq w(C) \geq 1$. Soit $C_i = a_{i,1} \vee \cdots \vee a_{i,n+1} \in W$ et $C_j = a_{j,1} \vee \cdots \vee a_{j,n+1} \notin W$. Soit $\alpha_i \in \mathcal{I}^-$ telle que $\alpha_i \not\models C$ et $\alpha_i \not\models C_i$. Une telle affectation existe, par minimalité de W. Soit θ_i la bijection induite, de $\{1, \ldots, n+1\} \setminus \{i\}$ dans $\{1, \ldots, n\}$.

Soit α_j l'affectation obtenue à partir de α_i en échangeant les rôles de i et j: $a_{i,k} \in \alpha_j$ ssi $a_{j,k} \in \alpha_i$, $\forall \ell, a_{j,\ell} \notin \alpha_j$ et, pour tout $k \neq i, j$, $a_{k,\ell} \in \alpha_j$ ssi $a_{k,\ell} \in \alpha_i$. Autrement dit α_j définit une bijection de $\{1, \ldots, n+1\} \setminus \{j\}$ dans $\{1, \ldots, n\}$ par $\theta_j(i) = \theta_i(j)$ et et $\theta_j(k) = \theta_i(k)$ pour $k \neq i, j$.

$\alpha_j \models W$ puisque $C_j \notin W$. Donc, par définition, $\alpha_j \models C$. Mais par ailleurs $\alpha_i \not\models C$. D'après (a), $\alpha_i \not\models \widehat{C}$ et $\alpha_j \models \widehat{C}$.

Or α_i et α_j ne diffèrent que dans l'interprétation des variables $a_{i,k}, a_{j,k}$ (qui sont échangées). Donc $a_{i,\theta_i(j)} \in V(\widehat{C})$.

Maintenant, j peut être choisie de $n+1-w(C)$ manières distinctes: $V(\widehat{C})$ contient donc $n + 1 - w(C)$ variables $a_{i,k}$ distinctes. Comme i peut par ailleurs être choisi de $w(C)$ façons distinctes, on a $|V(\widehat{C})| \geq w(C) \times (n + 1 - w(C))$.

(f) On remarque (par un raisonnement élémentaire sur les fonctions de variable réelle) que la fonction $x \mapsto x \times (n+1-x)$ atteint son minimum sur un intervalle $[a,b]$ à l'une des extrémités de l'intervalle. En utilisant les questions 1d et 1e, D_n contient une clause C_0 telle que $|V(\widehat{C_0})| \geq \min\{\frac{n+1}{3} \times (n+1-\frac{n+1}{3}), 2 \times \frac{n+1}{3} \times (n+1-2 \times \frac{n+1}{3})\} = 2 \times \frac{(n+1)^2}{9}$.

2. (a) Considérons l'application de l'ensemble $\{(C,P) \,|\, C \in L_n, P \in V(C)\}$ qui Il y a une paire (C,P) associe P. C'est une application d'un ensemble de cardinal au moins $|L_n| \times \frac{(n+1)^2}{8}$ dans un ensemble de cardinal $n(n+1)$. Comme $(n+1)^2 > n(n+1)$ (et d'après le principe des tiroirs et des chaussettes), au moins $\frac{|L_n|}{8}$ éléments ont la même image, ce qui est exactement le résultat souhaité.

   (b) D'après la question 2a, il existe une variable propositionnelle qui apparait dans au moins $\frac{|L_n|}{8}$ clauses de L_n. Soit $a_{i,j}$ cette variable. Affectons cette variable à $\top$ et toutes les variables $a_{i,k}, k \neq j$, $a_{k,j}, k \neq i$ à $\bot$,et simplifions l'ensemble des clauses: après renommage des variables (on a retiré un tiroir et une chaussette), on obtient une instance de S_{n-1} et une preuve d'insatisfaisabilité dans laquelle les clauses contenant $a_{i,j}$ ont disparu: $|L_{n-1}| \leq \frac{7}{8}|L_n|$.

   (c) On itère le résultat de la question précédente $\frac{n+1}{4}$ fois: $|L_{3 \times \frac{n+1}{4}}| \leq (\frac{7}{8})^{\frac{n+1}{4}}|L_n|$. Par ailleurs, d'après la question 1f, $D_{3 \times \frac{n+1}{4}}$ contient une clause C_0 telle que $|V(\widehat{C_0})| \geq 2 \times (3 \times \frac{n+1}{4})^2 \times \frac{1}{9} = \frac{(n+1)^2}{8}$. Autrement dit $|L_{3 \times \frac{n+1}{4}}| \geq 1$, et donc $|L_n| \geq (\frac{8}{7})^{\frac{n+1}{4}} \geq 2^{\frac{n+1}{24}}$ (car $(\frac{8}{7})^6 \geq 2$).