L2 – Logique 2
Collection d'exercices

1 Introduction à la preuve

Exercice 1

1. Soit n un entier, démontrez par contraposée que si n^2 est un entier naturel pair alors n est un entier naturel pair.
2. Démontrez par l'absurde que $\sqrt{2}$ est irrationnel.
   Indication : vous pourrez vous appuyer sur le résultat démontré au point précédent.

Exercice 2 Démontrez par l'absurde qu'il existe un nombre infini de nombres premiers.

Exercice 3 On souhaite démontrer que pour tout n entier, $n(2n+1)(7n+1)$ est divisible par 2 et 3.

1. Procédez par distinction de cas ;
2. Procédez par récurrence sur les entiers.

Exercice 4 Pour tout entier n non multiple de 5, le nombre $6n+5$ est-il premier ? Quel type de preuve avez-vous fait pour répondre à la question précédente ?

Exercice 5 (CC 2017)

1. Soient 3 ensembles A, B et C, démontrez par contraposée que si $A \cap B = \emptyset$ et $A \cap C = \emptyset$ alors $A \cap (B \cup C) = \emptyset$.
2. Pour fêter les vacances, les 5 enseignants de l'UE "Logique 2" décident de préparer un goûter pour leurs étudiants de L2. Chaque enseignant prépare chez lui un certain nombre de gâteaux. Au final, 8 gâteaux sont offerts au gouter.
   Démontrez qu'il y a nécessairement au moins 2 enseignants qui ont préparé le même nombre de gâteaux.
   Indication : soient n_1, n_2, ..., n_5 les nombres de gâteaux préparés par les enseignants. On pourra, par l'absurde, supposer $n_1 < n_2 < ... < n_5$.

2 Preuve par induction

2.1 Définition inductive

Exercice 6 Comment l'ensemble $S = \{3, 7, 11, 15, 19, 23, ...\}$ peut-il être défini inductivement ?

1. Si x est dans S alors $x+4$ est dans S.
2. 3 est dans S. Si x est dans S alors $x+4$ est dans S.
3. 3 est dans S. 7 est dans S. Si x est dans S alors $x+4$ est dans S.

Exercice 7 Énumérez les 10 premiers entiers appartenant à l'ensemble S défini inductivement de la façon suivante :

- 3 et 4 appartiennent à S ;
- Si x est dans S alors :
  - si x est impair alors $2x-1$ appartient à S ;
  - sinon $x+4$ appartient à S.

Exercice 8 Donnez une définition inductive pour l'ensemble des mots $S = \{a^{n+1}bc^n \mid n \in \mathbb{N}\}$.

Exercice 9 Soient x et y deux variables, f une fonction d'arité 2, a une constante (on rappelle qu'une constante peut être vue comme une fonction d'arité 0), P un prédicat d'arité 1 et R un prédicat d'arité 2.

Pour chacune des propositions suivantes, indiquez si elle constitue un **terme** ou bien une **formule** de la logique des prédicats. Lorsque la proposition n'est ni un terme ni une formule vous expliquerez pourquoi elle n'est pas syntaxiquement correcte.

- $\neg$P(x, a)
- f(a, f(a, a))
- R(a, R(a, a))
- R(a, f(a, a))
- $\exists$a.P(a)
- $\exists$x.P(a)
- $\neg\forall$x.$\neg$R(x, y)
- $\forall$f.$\exists$x.P(f(x, x))

2.2 Fonctions récursives et application du schéma de preuve par induction

Pour les exercices suivants, établissez clairement la base de l'induction. Précisez clairement vos hypothèses d'induction. Établissez clairement l'étape d'induction. Rédigez clairement la conclusion.

Exercice 10 En utilisant la représentation des entiers naturels utilisant 0 et S (succésseur), prouvez les théorèmes suivants par induction :

1. L'addition est associative : $\forall l, m, n.\ (l + m) + n = l + (m + n)$
2. L'addition et la multiplication sont distributives : $\forall l, m, n.\ l \cdot (m + n) = l \cdot m + l \cdot n$

Exercice 11 (Annale de janvier 2017)

1. Considérez la fonction récursive f suivante s'appliquant aux formules de la logique propositionnelle :
   - $f(p) = 0$
   - $f(\bot) = 0$
   - $f(\neg A) = f(A)$
   - $f(A \wedge B) = f(A) + f(B)$
   - $f(A \vee B) = f(A) + f(B)$
   - $f(A \longrightarrow B) = f(A) + f(B) + 1$

   Indiquez ce que calcule f.
2. Définissez la fonction récursive OU qui compte le nombre d'occurrences du connecteur $\vee$ dans une formule quelconque de la logique propositionnelle.
3. Définissez la fonction récursive NF qui transforme une formule en remplaçant toutes les sous-formules de la forme $A \longrightarrow B$ par $\neg A \vee B$.
   Par exemple, $\text{NF}(((\neg p \longrightarrow q) \longrightarrow (r \wedge s))) = (\neg(\neg\neg p \vee q) \vee (r \wedge s))$.
4. Prouvez par induction que pour toute formule A de la logique propositionnelle, on a :

$$\text{OU}(\text{NF}(A)) = \text{OU}(A) + f(A)$$

Exercice 12 (Annale juin 2017) Nous considérons un sous-ensemble de la logique propositionnelle qui contient uniquement des variables propositionnelles, la négation, la conjonction et la disjonction.

On dit qu'une formule est en forme normale négative (*NNF*) si les négations apparaissent uniquement devant les variables propositionnelles. Par exemple, $\neg(p \wedge q) \vee \neg\neg p$ n'est pas en *NNF* mais $(\neg p \vee \neg q) \vee p$ l'est. Ces deux formules sont pourtant équivalentes ; on peut même montrer que toute formule a une formule en *NNF* qui lui est équivalente.

Pour cela, on définit la fonction *nnf* suivante. Elle prend deux arguments : un entier ($+1$ ou -1) et la formule à convertir. La définition (partielle) de la fonction est la suivante :

$$\begin{array}{lcl} nnf(+1,p) & = & p \\ nnf(-1,p) & = & \neg p \\ nnf(+1,\neg A) & = & nnf(-1,A) \\ nnf(-1,\neg A) & = & nnf(+1,A) \\ nnf(+1,A\wedge B) & = & nnf(+1,A)\wedge nnf(+1,B) \end{array}$$

1. Complétez la définition précédente en rajoutant les clauses manquantes (à savoir pour : $nnf(-1, A\wedge B)$, $nnf(+1, A\vee B)$, et $nnf(-1, A\vee B)$) pour obtenir une fonction dont la correction fera l'objet de la question 3.
2. Tracez l'exécution de $nnf(+1, \neg(p\wedge q)\vee\neg\neg p)$
(c'est-à-dire, donnez les étapes intermédiaires lors du calcul du résultat)
3. Montrez, par induction sur la formule F, la propriété suivante :

$$nnf(+1,F) \text{ et } nnf(-1,F) \text{ sont en NNF} \quad \text{et} \quad nnf(+1,F)\equiv F \quad \text{et} \quad nnf(-1,F)\equiv\neg F$$

Exercice 13

1. Donnez des définitions récursives de $nc(A)$, $ncu(A)$, $ncb(A)$, $nsf(A)$ respectivement nombre de connecteurs, nombre de connecteurs unaires, nombre de connecteurs binaires et nombre d'occurrences de sous-formules d'une formule A.
2. Combien (d'occurrences) de sous-formules a une formule avec n connecteurs binaires (et sans négation) ? Prouvez le résultat par induction.
3. Combien (d'occurrences) de sous-formules a une formule avec n connecteurs (binaires et unaires) ? Prouvez le résultat par induction.
4. Soit $n\geq 0$ un entier quelconque, et $B, A_0, \ldots, A_n$ des formules du langage de la logique des propositions. Définissez récursivement les abréviations $\Delta_n = A_n\wedge(A_{n-1}\wedge(\ldots\wedge(A_1\wedge A_0)))$ et $\Gamma_n(B) = A_n\longrightarrow(A_{n-1}\longrightarrow(\ldots\longrightarrow(A_0\longrightarrow B)))$.
5. Soit A une formule quelconque. On définit, par récursion, la profondeur $pf(A)$ de A de la manière suivante : $pf(\bot)=0; pf(p)=0$ (pour $p\in PROP$) ; $pf((\neg B))=pf(B)+1; pf((C*B))=max(pf(C),pf(B))+1$
Exemple : $nsf((\neg(p\vee((\neg\bot)\wedge(\neg q)))))=8$ et $pf((\neg(p\vee((\neg\bot)\wedge(\neg q)))))=4$
Montrez par induction sur A que : $nsf(A)\leq 2^{pf(A)+1}-1$ où $nsf(A)$ est la fonction définie sous le point 1.
6. Montrez que $\Delta_n\longrightarrow B$ et $\Gamma_n(B)$ (voir point 4) sont logiquement équivalentes.
7. Soit E l'ensemble des formules écrites avec la proposition p, les connecteurs $\wedge$, $\vee$, le $\bot$ et les parenthèses uniquement. Montrez que pour toute valuation v et toute formule A de E, on a v(A)=0 ou v(A)=v(p). En déduire que E ne contient aucune tautologie.
8. Soit E l'ensemble des formules écrites avec toute proposition, les connecteurs $\wedge$, $\vee$, $\longrightarrow$ et les parenthèses. Soit v une valuation telle que $v(p)=1$ pour tout p. Montrez que si $A\in E$ alors $v(A)=1$. En déduire que pour toute formule A de E, il n'y a pas de formule B de E équivalente à $\neg A$.

Exercice 14

1. Donner une définition par récursion sur A de l'opération $A[B/p]$ qui remplace toute occurrence de la proposition p dans la formule propositionnelle A par la formule propositionnelle B. *Exemple* : $((p\wedge q)\longrightarrow p)[(a\vee b)/p] = ((a\vee b)\wedge q)\longrightarrow(a\vee b)$.
2. Définir la fonction $nbocc(p, A)$ qui calcule le nombre d'occurrences d'une variable propositionnelle p dans une formule A
3. A quoi est égal $A[B/p]$ lorsque $nbocc(p, A)=0$? Justifiez votre réponse.

4. On appelle taille d'une formule le nombre de nœuds de l'arbre syntaxique associé à cette formule. Définir une fonction $taille(A)$ qui calcule la taille d'une formule propositionnelle.
5. Quel est la relation entre $taille(A)$, $taille(B)$, $nbocc(p, A)$ et $taille(A[B/p])$? Prouvez cette relation par induction.

3 Déduction naturelle

3.1 Cas de la logique minimale

Exercice 15 Prouvez les séquents suivants dans le calcul de la logique minimale :

1. $\vdash p \longrightarrow p$
2. $\vdash (p \longrightarrow p) \longrightarrow (p \longrightarrow p)$
3. $\vdash (p \longrightarrow q) \longrightarrow (q \longrightarrow r) \longrightarrow p \longrightarrow r$
4. $p \longrightarrow q \longrightarrow r \vdash q \longrightarrow p \longrightarrow r$
5. $p \longrightarrow r \vdash p \longrightarrow q \longrightarrow r$
6. $p \longrightarrow p \longrightarrow q \vdash p \longrightarrow q$
7. $p \longrightarrow q, p \longrightarrow r, q \longrightarrow r \longrightarrow t \vdash p \longrightarrow t$

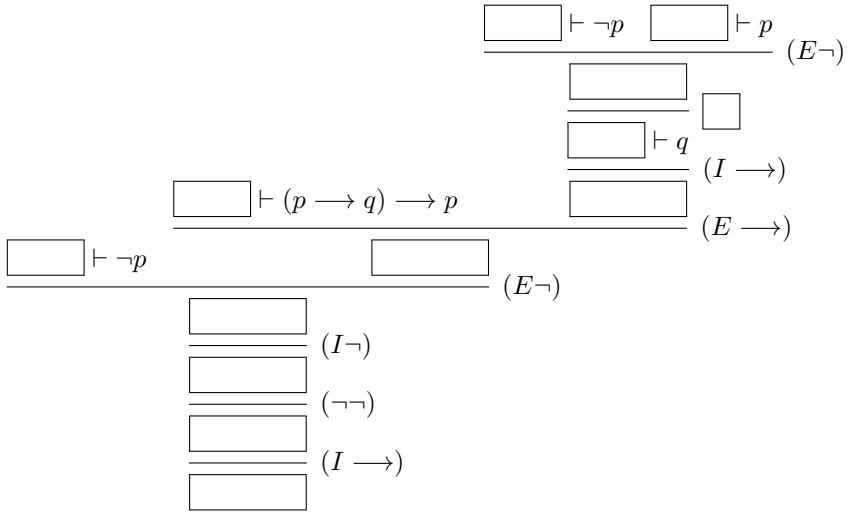
Exercice 16

1. Supposons que l'on doive prouver le séquent $\Gamma \vdash B$. De plus, on suppose qu'on préfère se ramener à prouver le séquent $\Gamma \vdash A_1 \longrightarrow A_2 \longrightarrow ... \longrightarrow A_n \longrightarrow B$. Proposez une règle dérivée s'appuyant sur une utilisation répétée de la règle de l'élimination de l'implication.
2. Utilisez la règle dérivée précédente pour prouver immédiatement : $p \longrightarrow q \longrightarrow r, p, q \vdash r$
3. Utilisez la règle dérivée précédente pour prouver : $p \longrightarrow q \longrightarrow r \longrightarrow s \longrightarrow t, p, q \vdash r \longrightarrow s \longrightarrow t$

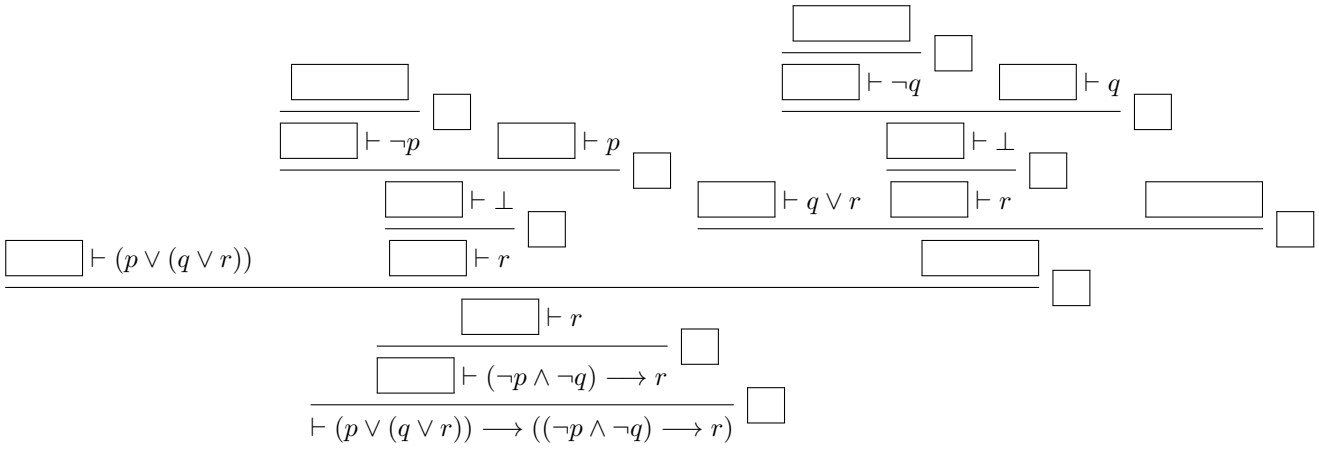
3.2 Cas de la logique propositionnelle

Exercice 17 Compléter les preuves suivantes en précisant (c'est signalé par des $\square$), la règle appliquée, les formules obtenues et la, ou les, hypothèses déchargées. De quoi sont-elles la preuve (quelles hypothèses pour quelle conclusion) ?

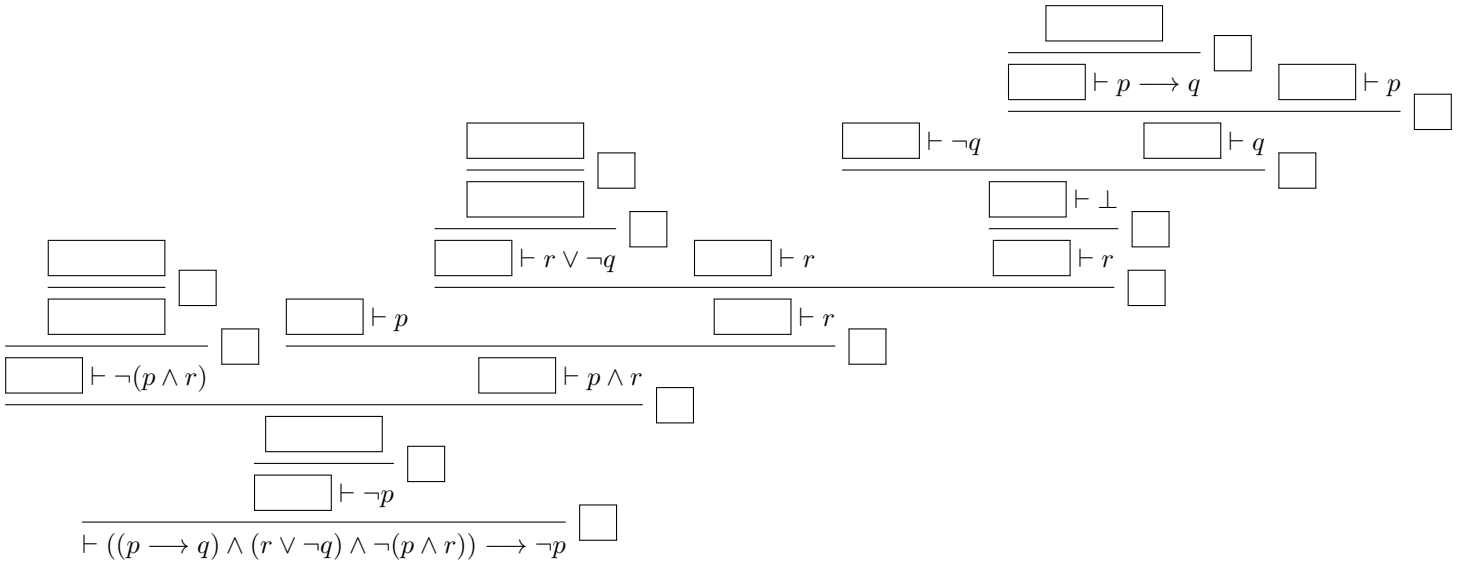
1.



2.



3.



Exercice 18

1. Donnez une interprétation intuitive de la règle d'inférence suivante dite, d'*affaiblissement* :

$$\frac{\Gamma \vdash B}{\Gamma, A \vdash B}\ (\text{aff})$$

2. Une façon de prouver A est de prouver, d'une part, $A \vee B$ et, d'autre part, $\neg B$. Donnez une règle d'inférence correspondant à cette démarche de preuve.
3. Montrez que la règle proposée à la question précédente peut être dérivée à partir des règles de la déduction naturelle pour la logique intuitionniste ainsi que de la règle d'affaiblissement discutée à la première question.

Exercice 19 On rappelle que l'équivalence $A \leftrightarrow B$ peut être définie comme : $(A \longrightarrow B) \wedge (B \longrightarrow A)$. Dérivez les règles $(I \leftrightarrow)$ suivantes :

$$\frac{\Gamma, A \vdash B \quad \Gamma, B \vdash A}{\Gamma \vdash A \leftrightarrow B}\ (I \leftrightarrow)$$

et $(E \leftrightarrow_1)$, $(E \leftrightarrow_2)$:

$$\frac{\Gamma \vdash A \leftrightarrow B}{\Gamma \vdash A \to B}\ (E \leftrightarrow_1) \qquad \frac{\Gamma \vdash A \leftrightarrow B}{\Gamma \vdash B \to A}\ (E \leftrightarrow_2)$$

Exercice 20 Donnez une preuve en déduction naturelle des formules suivantes

1. Règles utilisées : $(E\wedge)$, $(I\wedge)$, $(E \longrightarrow)$, $(I \longrightarrow)$, $(I\vee)$
   (a) $(p \longrightarrow (q \longrightarrow r)) \longrightarrow (q \longrightarrow (p \longrightarrow r))$
   (b) $(p \longrightarrow (q \longrightarrow r)) \longrightarrow ((p \longrightarrow q) \longrightarrow (p \longrightarrow r))$
   (c) $(r \longrightarrow p) \longrightarrow ((r \longrightarrow q) \longrightarrow (r \longrightarrow (p \wedge q)))$
   (d) $(p \wedge (p \vee q)) \leftrightarrow p$
   (e) $(p \longrightarrow q) \leftrightarrow ((p \wedge q) \leftrightarrow p)$
   (f) $(r \longrightarrow (p \wedge q)) \leftrightarrow ((r \longrightarrow p) \wedge (r \longrightarrow q))$
2. Règles utilisées : les mêmes qu'en 1 plus $(E\vee)$
   (a) $(p \longrightarrow q) \leftrightarrow ((p \vee q) \leftrightarrow q)$
   (b) $(p \longrightarrow r) \longrightarrow ((q \longrightarrow r) \longrightarrow ((p \vee q) \longrightarrow r))$
   (c) $(p \wedge (q \vee r)) \longrightarrow ((p \wedge q) \vee (p \wedge r))$
   (d) $((p \longrightarrow r) \wedge (q \longrightarrow r)) \longrightarrow ((p \vee q) \longrightarrow r)$
   (e) $(p \vee (q \wedge r)) \longrightarrow ((p \vee q) \wedge (p \vee r))$
   (f) $(p \vee (p \wedge q)) \longrightarrow p$
3. Règles utilisées : les mêmes qu'en 2 plus $(I\neg)$, $(E\neg)$, $(I\bot)$, $(E\bot)$. Il s'agit essentiellement de preuves par l'absurde.
   (a) $p \leftrightarrow \neg\neg p$
   (b) $(p \longrightarrow q) \longrightarrow (\neg q \longrightarrow \neg p)$
   (c) $(p \vee q) \leftrightarrow \neg(\neg p \wedge \neg q)$
   (d) $(p \wedge q) \leftrightarrow \neg(\neg p \vee \neg q)$
   (e) $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$
   (f) $(p \longrightarrow q) \leftrightarrow \neg(p \wedge \neg q)$
   (g) $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$
   (h) $(p \longrightarrow q) \leftrightarrow (\neg p \vee q)$

Exercice 21 Après une course hippique entre chevaux noir et blanc, le cheval gagnant fut celui qui avait une robe noire et une crinière blanche. Il s'agissait de PetitGris, de Qristal ou de Rikita. Or PetitGris a une crinière noire et une queue blanche, Qristal a une robe noire et une queue blanche, et enfin Rikita a une robe noire. Enfin le gagnant avait sa crinière et sa queue de couleur opposées. C'est donc Rikita le gagnant.

Donnez une preuve en déduction naturelle des affirmations suivantes :
— PetitGris n'a pas gagné ;
— Qristal n'a pas gagné ;
— Rikita a gagné.

Exercice 22 Pour obtenir la logique classique, on a ajouté la règle du *tertium non datur* suivante :

$$\frac{}{\Gamma \vdash A \vee \neg A}\ (TND)$$

Dans la littérature, on trouve deux autres formulations :

$$\frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}\ (\neg\neg)$$

et

$$\frac{\Gamma, \neg A \vdash A}{\Gamma \vdash A}\ (clas.)$$

On souhaiter montrer que toutes ces formulations sont équivalentes. Pour cela, montrez que depuis (TND) on peut dériver $(\neg\neg)$; depuis $(\neg\neg)$ on peut dériver $(clas.)$; et enfin depuis $(clas.)$, on peut dériver (TND).

3.3 Cas de la logique des prédicats

Exercice 23 *Définitions :* Soit R une relation binaire (on écrira xRy plutôt que $R(x, y)$)

- R est réflexive ssi $\forall x.xRx$
- R est sérielle ssi $\forall x.\exists y.xRy$
- R est dense ssi $\forall x.\forall y.xRy \longrightarrow \exists z.xRz \wedge zRy$
- R est irréflexive ssi $\forall x.\neg xRx$
- R est transitive ssi $\forall x.\forall y.\forall z.xRy \wedge yRz \longrightarrow xRz$
- R est symétrique ssi $\forall x.\forall y.xRy \longrightarrow yRx$
- R est asymétrique ssi $\forall x.\forall y.xRy \longrightarrow \neg yRx$
- R est confluente ssi $\forall x.\forall y.\forall z.xRy \wedge xRz \longrightarrow \exists u.yRu \wedge zRu$
- R est euclidienne ssi $\forall x.\forall y.\forall z.xRy \wedge xRz \longrightarrow yRz$

1. Que pensez-vous de l'affirmation suivante : si R est transitive et symétrique alors R est réflexive ? (Vérifiez-le sans déduction naturelle, puis avec)
2. Donnez une preuve en déduction naturelle des énoncés suivants :
   (a) Si R est réflexive alors R est sérielle
   (b) Si R est réflexive alors R est dense
   (c) Si R est asymétrique alors R est irréflexive
   (d) Si R est irréflexive et transitive alors R est asymétrique
   (e) Si R est symétrique alors R est confluente
   (f) Si R est symétrique et transitive alors R est euclidienne
   (g) Si R est sérielle, symétrique et transitive alors R est réflexive
   (h) Si R est réflexive et euclidienne alors R est symétrique
   (i) Si R est réflexive et euclidienne alors R est transitive

Exercice 24 Donnez une dérivation en déduction naturelle des jugements suivants :

1. $R(c, c) \vdash \exists y.R(c, y)$
2. $H(socrate), \forall x.H(x) \longrightarrow M(x) \vdash M(socrate)$ où $socrate$ est une constante
3. $\forall x.P(x) \longrightarrow Q(x), P(y) \vdash Q(y)$
4. $\vdash \forall z.P(z) \longrightarrow Q(z) \vee P(z)$
5. $\exists x.P(x), \forall x.P(x) \longrightarrow Q(x) \vdash \exists x.Q(x)$
6. $\vdash (\forall x.\forall y.P(x, y)) \longrightarrow \forall y.\forall x.P(x, y)$
7. $\vdash (\exists x.\exists y.P(x, y)) \longrightarrow \exists y\exists x.P(x, y)$
8. $\exists x.E(x), \forall x.E(x) \longrightarrow H(x) \vdash \exists x.H(x)$
9. $\forall x.P(x) \vee Q(x), \forall x.\neg P(x) \vdash \forall x.Q(x)$

10. $\vdash (\exists x.P(x) \longrightarrow Q(x)) \longrightarrow \forall x.P(x) \longrightarrow \exists x.Q(x)$
11. $\forall y.P(y) \longrightarrow Q(y), \forall z.Q(z) \longrightarrow R(z) \vdash \forall y.P(y) \longrightarrow R(y)$
12. $x+1 = 1+x, x+1 > 1 \longrightarrow x+1 > 0 \vdash 1+x > 1 \longrightarrow 1+x > 0$
13. $t_1 = t_2 \vdash t_2 = t_1$
14. $t_1 = t_2, t_2 = t_3 \vdash t_1 = t_3$
15. $\vdash R(a,c) \wedge (a = b) \longrightarrow R(b,c)$
16. $\exists x.P(x) \vee Q(x) \vdash (\exists x.P(x)) \vee \exists x.Q(x)$
17. $(\exists x.P(x)) \vee \exists x.Q(x) \vdash \exists x.P(x) \vee Q(x)$
18. $(\forall x.P(x)) \vee \forall x.Q(x) \vdash \forall x.P(x) \vee Q(x)$
19. $\forall x.P(x) \wedge Q(x) \vdash (\forall x.P(x)) \wedge \forall x.Q(x)$
20. $(\forall x.P(x)) \wedge \forall x.Q(x) \vdash \forall x.P(x) \wedge Q(x)$
21. $\exists x.P(x) \wedge Q(x) \vdash (\exists x.P(x)) \wedge \exists x.Q(x)$
22. $\neg\exists x.P(x) \vdash \forall x.\neg P(x)$
23. $\forall x.\neg P(x) \vdash \neg\exists x.P(x)$
24. $\neg\forall x.P(x) \vdash \exists x.\neg P(x)$
25. $\exists x.\neg P(x) \vdash \neg\forall x.P(x)$
26. $P(0), \forall x.P(x) \longrightarrow P(s(s(x))) \vdash P(s(s(s(s(0)))))$

Exercice 25

1. Le paradoxe du buveur est le suivant : dans tout pub non vide (c'est-à-dire, au moins une personne est présente), il existe une personne qui, si elle boit, alors tout le monde boit. Cet énoncé peut être modélisé de la façon suivante :

   $$\exists x.(B(x) \longrightarrow \forall y.B(y))$$

   Démontrez que cet énoncé est vrai en vous appuyant sur le calcul de la déduction naturelle pour la logique classique.
2. Modélisez et démontrez la variante suivante : dans un pub non vide, il y a une personne telle que si elle boit, son meilleur ami boit également.

4 Unification

Exercice 26 Déterminer le *mgu* des problèmes d'unification suivants, ou justifier pourquoi les termes ne sont pas unifiables syntaxiquement. On suppose que les symboles en minuscule (f, g, h, a, b, c) sont des noms de fonctions ou constantes et les symboles en majuscules(X, Y, Z) des variables. Les fonctions 0-aires (= constantes) s'écrivent sans parenthèses : c au lieu de $c()$.

1. $f(g(X)) \stackrel{?}{=} f(Y)$
2. $f(g(Y)) \stackrel{?}{=} f(Y)$
3. $h(X, g(X)) \stackrel{?}{=} h(Y, g(X))$
4. $h(X, g(c)) \stackrel{?}{=} h(Y, g(X))$
5. $h(X, g(c)) \stackrel{?}{=} h(Y, Y)$
6. $h(X, g(c)) \stackrel{?}{=} h(g(c), Y)$
7. $h(X, g(c)) \stackrel{?}{=} h(g(a), Y)$

Exercice 27 Appliquez l'algorithme d'unification aux termes suivants. Montrez clairement les différentes étapes de l'algorithme ; il ne suffit pas d'afficher l'unificateur.

1. $pair(a, crypt(Z, b)) \stackrel{?}{=} pair(X, Y)$
2. $pair(crypt(X, b), crypt(Y, b)) \stackrel{?}{=} pair(crypt(a, b), Z)$
3. $crypt(pair(Z, a), X) \stackrel{?}{=} crypt(pair(Y, crypt(X, b)), b)$
4. $crypt(pair(a, Z), X) \stackrel{?}{=} crypt(pair(Y, crypt(X, b)), b)$

5 Résolution pour la logique des prédicats

Exercice 28 Donnez la forme prénexe des formules suivantes :

1. $\forall x.\forall y.P(x, y) \longrightarrow \exists z.Q(x, z)$
2. $\forall x.(\exists y.P(x, y)) \longrightarrow Q(x)$
3. $(\exists x.P(x)) \wedge \forall x.\exists y.Q(y) \longrightarrow R(x)$

Exercice 29 Donnez la skolémisation des formules suivantes :

1. $\forall x.\forall y.\exists z.\neg P(x, y) \vee R(x, z)$
2. $\forall x.\exists u.\forall y.\forall z.\neg P(x, u) \vee Q(u, y) \wedge R(y, z)$

Exercice 30 (Forme prénexe et skolémisation)

1. L'algorithme pour calculer la forme prénexe d'une formule n'est pas déterministe : Montrez que vous pouvez l'appliquer de deux manières différentes à la formule $(\forall x.P(x)) \vee (\exists y.Q(y))$.
2. Skolémisez les deux formules ainsi obtenues. Laquelle vous semble préférable (en termes de taille de la formule skolémisée) ?
3. Tirez-en la conclusion pour trouver la forme prénexe skolémisée optimale des formules suivantes :
   (a) $(\forall x.\exists y.R(x, y)) \wedge (\exists u.\forall v.R(u, v))$
   (b) $(\forall x.(\forall y.S(x, y)) \longrightarrow (\forall v.T(x, v)))$

Exercice 31 (Skolémisation, compréhension)

1. Dans l'arithmétique sur les nombres naturels, on peut définir la relation de divisibilité ("d divise n") par : $(d|n) \equiv (\exists k.\, n = d * k)$. Soit F la formule

$$\forall a.\forall b.\, \exists m.\, (m|a) \wedge (m|b) \wedge (\forall d.(d|a) \wedge (d|b) \longrightarrow m \geq d)$$

   (a) Donnez la forme prénexe F' de la formule F.
   (b) Donnez la skolémisation de la formule F'.
   (c) A quel algorithme correspond la fonction de skolémisation que vous avez introduite ?
2. Aussi dans l'arithmétique sur les nombres naturels, définissons la formule G par :

$$\forall a.\forall b.\, \exists q.\exists r.\, a = q * b + r \wedge 0 \leq r \wedge r < b$$

   (a) Donnez la skolémisation de la formule G.
   (b) Quelles sont les fonctions de skolémisation que vous avez introduites ?
   Note : Supposons que vous remplacez la variable q par la fonction $f_q(a, b)$ et la variable r par la fonction $f_r(a, b)$. Vous pourrez définir $f_q(a, b) = fst(de(a, b))$ et $f_r(a, b) = snd(de(a, b))$ où de est un algorithme bien connu (lequel ?) qui calcule un couple de valeurs et fst respectivement snd renvoient le premier respectivement deuxième composant de ce couple.

Exercice 32 Donnez la forme clausale des formules suivantes :

1. $\forall x.\exists u.\forall y.\forall z.P(x,u) \longrightarrow Q(u,y) \wedge R(y,z)$ (sa skolémisation a été obtenue à un exercice précédent)
2. $\forall x.\exists y.P(x,y) \longrightarrow \exists z.Q(z,x)$
3. $(\exists y.R(x,y) \vee \forall z.Q(z,z)) \wedge (\neg\forall x.P(x)) \wedge P(a)$

Exercice 33 Construisez une dérivation pour les ensembles de clauses suivants permettant de démontrer que la formule associée à chaque forme clause est insatisfiable.

1. $\{\{P(x,x)\},\{\neg P(y,z),\neg P(z,u),P(u,y)\},\{P(a,b)\},\{\neg P(b,a)\}\}$
2. $\{\{P(0)\},\{\neg P(x),Q(s(x))\},\{\neg Q(y),P(s(y))\},\{\neg Q(s(s(s(0))))\}\}$

Exercice 34 On souhaite démontrer, à l'aide du principe de résolution, le syllogisme suivant :

$$H(socrate) \wedge (\forall x.H(x) \longrightarrow M(x)) \longrightarrow M(socrate)$$

— Skolémiser la négation du syllogisme.
— Transformer le résultat obtenu à la question précédente en forme clausale.
— Appliquez le principe de résolution et déduisez-en que la négation du syllogisme est insatisfiable.

Exercice 35 Montrez à l'aide du principe de résolution que la formule suivante est valide :

$$(\forall x.P(x) \longrightarrow Q(x)) \longrightarrow (\forall x.P(x)) \longrightarrow \forall x.Q(x)$$

Exercice 36 Considérez les formules suivantes :
— $H_1 = (\exists x.P(x)) \longrightarrow \forall x.P(x)$
— $H_2 = \forall x.P(x) \vee Q(x)$
— $C = (\exists x.\neg Q(x)) \longrightarrow \forall x.P(x)$
Démontrez à l'aide du principe de résolution que C est une conséquence logique de H_1 et H_2

Exercice 37 (Modèles et contre-modèles)

1. Refaites quelques preuves de l'exercice 23 avec le calcul de la résolution.
2. Une relation confluente n'est pas forcément symétrique (donnez un contre-modèle pour le montrer). Tentez une preuve en résolution de l'énoncé "si R est confluente, alors R est symétrique" et montrez comment l'échec de la preuve met en évidence un contre-modèle de l'énoncé.
3. Soit 0 une constante, s une fonction unaire et $<$ une relation binaire. Vous reconnaissez sans doute le vocabulaire de l'arithmétique de Peano. Étant données les hypothèses :
   — $H_1 = \forall x.x < s(x)$
   — $H_2 =$ "relation $<$ est transitive"
   essayez de montrer la conclusion $\neg\exists x.x < 0$. Vous vous rendez compte que la conclusion n'est pas une conséquence logique des hypothèses (donnez un contre-modèle). Est-ce que la preuve par résolution termine, vous permettant ainsi d'extraire un contre-modèle ?