Licence STS, semestre 4 — 2013–14
Mathématiques pour l'Informatique (Info 229) — 12 mars 2014
`http://www.lri.fr/~paulin/MathInfo`

Partiel - 12 mars 2014

L'examen dure 2 heures. L'énoncé est composé de 5 pages. Toutes les réponses devront être clairement justifiées. Les seuls documents autorisés sont une page A4 manuscripte recto-verso. Le tableau résumant les règles de déduction du calcul des séquents sont données à la fin du sujet.
NE PAS CACHETER LES COPIES.

Exercice 1 *Enigme, d'après Smullyan, 3 points.*

Trois coffres numérotés de 1 à 3 sont disposés sur une table. Un seul de ces coffres contient un trésor qu'il faut découvrir. Chaque coffre comporte une inscription :

1. Le trésor est dans ce coffre.
2. Le trésor n'est pas dans ce coffre.
3. Si le trésor n'est pas dans le coffre 1 alors il n'est pas dans ce coffre.

Questions. On introduit des variables propositionnelles P_1 pour représenter le fait que le trésor est dans le coffre 1 et P_2 pour représenter le fait que le trésor est dans le coffre 2.

1. Donner une formule (notée P_3) qui utilise les variables P_1 et P_2 et qui est vraie exactement lorsque le trésor est dans le coffre 3.
2. Donner une formule (notée C) qui utilise les variables P_1 et P_2 et qui représente le fait que le trésor est exactement dans un des coffres.
3. Donner des formules I_1, I_2 et I_3 qui utilisent les variables P_1 et P_2 et qui représentent les inscriptions sur chacun des coffres.
4. Donner la table de vérité des formules P_3, C, I_1, I_2 et I_3 en fonction des variables P_1 et P_2.
5. Sachant que C est vrai et qu'au moins deux des formules I_1, I_2 et I_3 sont vraies, en déduire dans quel coffre est caché le trésor.

Correction :

1. *Le tableau sera dans le coffre* 3 *si et seulement si il n'est ni dans le coffre* 1*, ni dans le coffre* 2*, la formule qui exprime cette situation est* $P_3 \stackrel{\text{def}}{=} \neg P_1 \land \neg P_2$.
2. *Plusieurs formulations (équivalentes) sont possibles :*
   - $(P_1 \Rightarrow \neg P_2) \land (P_2 \Rightarrow \neg P_1)$ *: si le tableau est dans le coffre* 1 *alors il n'est pas dans le coffre* 2 *et s'il est dans le coffre* 2 *alors il n'est pas dans* 1 *ce qui s'écrit;*
   - $(P_1 \land \neg P_2) \lor (\neg P_1 \land P_2) \lor (\neg P_1 \land \neg P_2)$ *: soit le tableau est dans le coffre* 1 *et pas dans le coffre 2, soit il n'est pas dans le coffre* 1 *et il est dans le coffre* 2 *soit il n'est ni dans le coffre* 1 *ni dans le coffre* 2 *(auquel cas* P_3 *est vrai par définition) :*
   - $\neg(P_1 \land P_2)$ *: la seule situation à exclure est celle dans laquelle le tableau serait à la fois dans les coffres* 1 *et* 2.
3. $I_1 \stackrel{\text{def}}{=} P_1$, $I_2 \stackrel{\text{def}}{=} \neg P_2$, $I_3 \stackrel{\text{def}}{=} \neg P_1 \Rightarrow P_2$ *ou* $I_3 \stackrel{\text{def}}{=} \neg P_1 \Rightarrow \neg P_3$
4.

P_1	P_2	$P_3 \stackrel{\text{def}}{=} \neg P_1 \land \neg P_2$	$C \stackrel{\text{def}}{=} (P_1 \Rightarrow \neg P_2) \land (P_2 \Rightarrow \neg P_1)$	$I_1 \stackrel{\text{def}}{=} P_1$	$I_2 \stackrel{\text{def}}{=} \neg P_2$	$I_3 \stackrel{\text{def}}{=} \neg P_1 \Rightarrow \neg P_3$
V	V	F	F	V	F	V
V	F	F	V	V	V	V
F	V	F	V	F	F	V
F	F	V	V	F	V	F

5. *La seule situation dans laquelle* C *est vrai et au moins deux affirmations sont vraies est la situation* 2 *dans laquelle toutes les affirmations sont vraies : le trésor est dans le coffre 1.*

Exercice 2 *Arbre de dérivation, 2 points*

Construire un arbre de dérivation (preuve en calcul des séquents) pour montrer les formules suivantes :

1. $\neg Q(a) \Rightarrow \neg(\forall x, Q(x))$

2. $(\forall x, (P(x) \vee \neg Q(x))) \Rightarrow \neg P(a) \Rightarrow \neg Q(a)$

Correction :

1.

$$\Rightarrow I\;\dfrac{\Rightarrow I\;\dfrac{\forall H\;\dfrac{\neg H\;\dfrac{\mathit{hyp}\;\dfrac{}{(\forall x, Q(x)), Q(a) \vdash Q(a)}}{\neg Q(a), (\forall x, Q(x)), Q(a) \vdash \bot}}{\neg Q(a), (\forall x, Q(x)) \vdash \bot}}{\neg Q(a) \vdash \neg(\forall x, Q(x))}}{\vdash \neg Q(a) \Rightarrow \neg(\forall x, Q(x))}$$

2.

$$\Rightarrow I\;\dfrac{\Rightarrow I\;\dfrac{\forall H\;\dfrac{\forall H\;\dfrac{\neg H\;\dfrac{\mathit{hyp}\;\dfrac{}{(\forall x, (P(x) \vee \neg Q(x))), P(a) \vdash P(a)}}{(\forall x, (P(x) \vee \neg Q(x))), P(a), \neg P(a) \vdash \neg Q(a)} \quad \mathit{hyp}\;\dfrac{}{(\forall x, (P(x) \vee \neg Q(x))), \neg Q(a), \neg P(a) \vdash \neg Q(a)}}{(\forall x, (P(x) \vee \neg Q(x))), (P(a) \vee \neg Q(a)), \neg P(a) \vdash \neg Q(a)}}{(\forall x, (P(x) \vee \neg Q(x))), \neg P(a) \vdash \neg Q(a)}}{(\forall x, (P(x) \vee \neg Q(x))) \vdash \neg P(a) \Rightarrow \neg Q(a)}}{\vdash (\forall x, (P(x) \vee \neg Q(x))) \Rightarrow \neg P(a) \Rightarrow \neg Q(a)}$$

Exercice 3 *Cardinaux, 2 points*

Soit X un ensemble de cardinal 4 et Y un ensemble de cardinal 5. On pourra donner les résultats sous forme d'expression arithmétique sans calculer.

1. Quel est le cardinal de l'ensemble des applications de X dans Y ? de l'ensemble des parties de $X \times Y$?
2. Quel est le cardinal de l'ensemble des applications surjectives de X dans Y ? de l'ensemble des applications bijectives ?

Correction :

1. $|X \to Y| = |Y|^{|X|} = 5^4$, $\wp(X \times Y) = 2^{|X \times Y|} = 2^{20}$

2. *Il n'y a pas d'application surjective (et a fortiori bijective) de X dans Y car le cardinal de Y est strictement supérieur à celui de X. Le cardinal de ces deux ensembles est donc* 0.

Exercice 4 *Modélisation, 5 points*

On cherche à modéliser un système bancaire. Dans le système, il y a des clients et des comptes. La banque garde comme information une *base des comptes ouverts* qui associe un client et un compte. Un client peut avoir plusieurs comptes et un compte peut être associé à plusieurs clients (cas d'un compte joint). La banque garde également trace de l'historique des *soldes des comptes* : à un compte et un jour est associé la somme d'argent disponible sur le compte. Cette somme est un entier qui peut être positif (le compte est approvisionné) ou bien négatif (le compte est à découvert).

On suppose donnés trois ensembles X, C et D qui sont des sous-ensembles de l'ensemble des entiers naturels $\mathbb{N}$ et qui représentent l'ensemble des clients (X), des comptes (C) et des jours (D). La base des comptes ouverts est représentée par un ensemble $B \subseteq X \times C$. L'historique du solde des comptes est représenté par une fonction $H \in C \times D \to \mathbb{Z}$, qui associe à un compte et une date un entier relatif (élément de l'ensemble $\mathbb{Z}$).

1. Exprimer les contraintes suivantes comme des formules faisant intervenir les ensembles X, C, D, les relations B et H, les notations ensemblistes ainsi que les opérations arithmétiques usuelles (on supposera que des entiers consécutifs représentent des jours successifs).
   (a) chaque compte est associé à au moins un client
   (b) chaque jour, un client doit avoir au moins un compte dont le solde est positif
   (c) chaque client doit avoir au moins un compte dont le solde reste toujours positif
   (d) aucun compte ne peut rester strictement négatif plus de 7 jours de suite
2. que peut-on dire des contraintes (b) et (c) de la question précédente, est-ce qu'il y en a une qui implique l'autre ?

3. Donner des expressions ensemblistes utilisant les ensembles introduits précédemment ainsi que les constantes `j` et `m` correspondant aux ensembles suivants :
   (a) l'ensemble `contact` des clients qui ont un compte dont le solde le jour `j` est supérieur à 3000 €.
   (b) l'ensemble des comptes de Madame Machin (client `m`) sur lesquels il y a au jour `j` une somme supérieure à 1000 €. A quelle condition sur cet ensemble Mme Machin peut-elle effectuer un retrait de 1000€ sur un de ses comptes sans être à découvert ?

Correction :

1. (a) $\forall c \in C, \exists x \in X, B(x, c)$
   (b) $\forall d \in D, \forall x \in X, \exists c \in C, B(x, c) \wedge H(c, d) \geq 0$
   (c) $\forall x \in X, \exists c \in C, B(x, c) \wedge (\forall d \in D, H(c, d) \geq 0)$
   (d) $\forall c \in C, \forall d \in D, H(c, d) < 0 \Rightarrow \exists d', d < d' \wedge d' \leq d + 7 \wedge H(c, d) \geq 0$

2. la condition c implique la condition b mais elle ne sont pas équivalentes, un client peut avoir deux comptes différents qui sont alternativement négatifs.

3. (a) $\texttt{contact} \stackrel{\text{def}}{=} \{x \in X | \exists c \in C, B(x, c) \wedge H(c, j) \geq 3000\}$
   (b) $\texttt{machin} \stackrel{\text{def}}{=} \{c \in C | B(m, c) \wedge H(c, j) \geq 1000\}$, *Mme Machin peut effectuer le retrait si cet ensemble est non vide (elle a au moins un compte suffisament alimenté).*

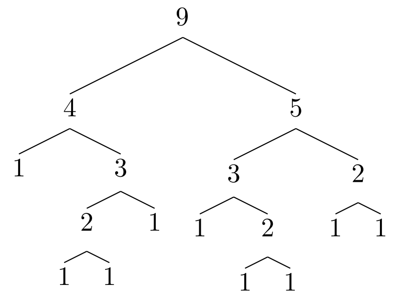
Exercice 5 Récurrence (4 points)

On considère le jeu suivant : on part d'un entier $n \geq 2$, on le décompose en une somme $p + q$ avec $p, q \geq 1$, puis tant que p ou q est strictement plus grand que 1 on recommence en le décomposant à nouveau en une somme de deux nombres plus petits.

Par exemple, en partant de $n = 9$ on peut faire la décomposition suivante : $9 = 4 + 5 = (1 + 3) + (3 + 2) = (1 + (2 + 1)) + ((1 + 2) + (1 + 1)) = (1 + ((1 + 1) + 1)) + ((1 + (1 + 1)) + (1 + 1))$

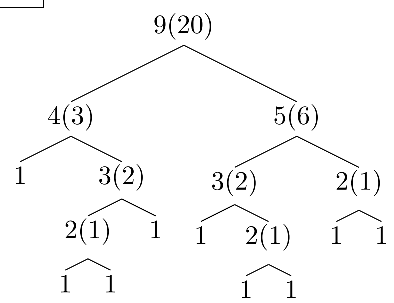
On représente la décomposition sous forme d'arbre : la transformation de n en $p+q$ devient le nœud $\boxed{\begin{array}{c} \text{n} \\ \frown \\ \text{p} \quad \text{q} \end{array}}$.

Dans le cas de l'exemple, on obtient l'arbre suivant :



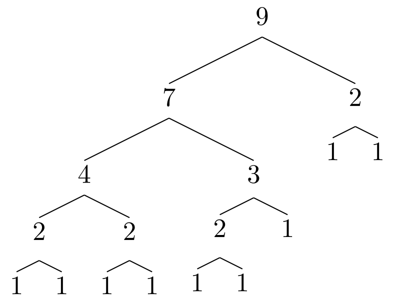
On fait ensuite la somme de tous les produits $p \times q$ ainsi créés. Pour cela, on commence par ajouter les produits dans les arbres entre parenthèses, en écrivant $\boxed{\begin{array}{c} n(p \times q) \\ \frown \\ \text{p} \quad \text{q} \end{array}}$.

Soit dans notre exemple :



Lorsque l'on fait la somme des produits ainsi obtenus $20 + 3 + 6 + 2 + 2 + 1 + 1 + 1$, on obtient le nombre 36.

1. On se donne une autre décomposition de l'entier 9



Ajouter les produits dans l'arbre de décomposition et montrer que la somme de ces produits est aussi 36.

2. On cherche maintenant à montrer que cette somme ne dépend que de n et pas de la décomposition. On appelle $s(n)$ la somme des produits d'une décomposition de n.
   (a) Si n est décomposé en $p+q$, exprimer la valeur de $s(n)$ en fonction des valeurs de $s(p)$ $s(q)$ et du produit $p \times q$.
   (b) Montrer par une récurrence généralisée sur n que pour tout $n \geq 2$ on a

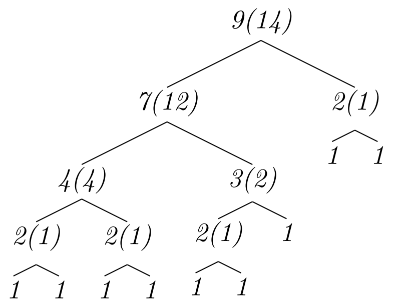
$$s(n) = \frac{n(n-1)}{2}$$

   Rappel : *la récurrence généralisée consiste lorsque l'on montre l'étape d'hérédité $P(n+1)$ pour n quelconque, à supposer non seulement que $P(n)$ est vrai mais plus généralement que $P(k)$ est vrai pour tout $k \leq n$.*

3. Un magicien demande à une personne dans la salle de choisir sans le dévoiler un nombre n, d'appliquer une décomposition suivant le principe précédent et de lui donner le résultat de la somme des produits obtenus, la réponse est 78. Le magicien "devine" alors le nombre n de départ. Quel est ce nombre ?

Correction :

1.



14+12+1+4+2+1+1+1=36

2. *(a) La somme cumulée en un nœud de l'arbre $n = p + q$ est égale à la somme $s(p)$ du sous-arbre sous p plus la somme $s(q)$ du sous-arbre sous q plus le produit $p \times q$. On a donc $s(n) = s(p) + s(q) + p \times q$.*
   (b) – *initialisation : on commence à $n = 2$ la seule décomposition est $(1+1)$ dont le produit est 1 donc $s(2) = 1 = \frac{2\times(2-1)}{2}$*
   – *hérédité : on se donne n quelconque, on suppose que la formule $s(k) = \frac{k(k-1)}{2}$ est vraie pour tous les entiers $k \leq n$ et on veut montrer $s(n+1) = \frac{(n+1)n}{2}$. Pour tout découpage $n+1 = p+q$ on a (question précédente) $s(n+1) = s(p) + s(q) + p \times q$. Comme $p \geq 1$ et $q \geq 1$ on a $p \leq n$ et $q \leq n$, donc l'hypothèse de récurrence s'applique à p et à q. Donc*

$$s(n{+}1) = \frac{p(p-1)}{2} + \frac{q(q-1)}{2} + p\times q = \frac{p^2 - p + q^2 - q + 2pq}{2} = \frac{(p+q)^2 - (p+q)}{2} = \frac{(n+1)^2 - (n+1)}{2}$$

   – *la propriété $s(n) = \frac{n(n-1)}{2}$ est donc vérifiée pour tout n.*

3. Il suffit de trouver n tel que $s(n) = \frac{n(n-1)}{2} = 78$ soit $n = 13$.

Exercice 6 *Règles d'inférence, 4 points*

On se donne le système d'inférence suivant

$$(a)\frac{}{R(0,1,0)} \qquad (b)\frac{R(x,y,n)}{R(x+y, y+2, n+1)}$$

1. Montrer que l'on a $R(1,3,1)$ et $R(4,5,2)$. Trouver x et y tels que $R(x,y,4)$ et construire l'arbre de dérivation correspondant.
2. Énoncer le principe d'induction associé à la définition de R.
3. Utiliser ce principe pour montrer que pour tout x, y, n, on a $R(x,y,n) \Rightarrow x = n^2 \wedge y = 2n+1$.
4. On admettra sans le démontrer que pour tout n, il existe un unique x et un unique y tel que $R(x,y,n)$. On note x_n la valeur de x pour laquelle $R(x,y,n)$.

   Montrer que pour tout réel positif a, il existe un unique n tel que $x_n \leq a$, $x_{n+1} > a$, et que n est alors la partie entière de la racine carrée de a (on a ainsi un algorithme pour calculer la racine carrée entière qui n'utilise que des additions).

Correction :

1. *On a $R(16,9,4)$. L'arbre de dérivation est*

$$
\begin{array}{rc}
(a) & \overline{} \\
(b, n=0, y=1, x=0) & \underline{R(0,1,0)} \\
(b, n=1, y=3, x=1) & \underline{R(1,3,1)} \\
(b, n=2, y=5, x=4) & \underline{R(4,5,2)} \\
(b, n=3, y=7, x=9) & \underline{R(9,7,3)} \\
 & R(16,9,4)
\end{array}
$$

   Cet arbre inclut les dérivations de $R(1,3,1)$ et $R(4,5,2)$.

2. *Soit $P(x,y,n)$ une propriété quelconque si*
   (a) $P(0,1,0)$
   (b) pour tout x, y et n, si $P(x,y,n)$ alors $P(x+y, y+2, n+1)$

   alors $\forall x\, y\, n, R(x,y,n) \Rightarrow P(x,y,n)$

3. *on prend comme formule $P(x,y,n) \stackrel{\text{def}}{=} (x = n^2 \wedge y = 2n+1)$, on vérifie*
   – $P(0,1,0) \equiv 0 = 0^2 \wedge 1 = 2 \times 0 + 1$ *qui est trivial*
   – *on suppose soit x, y et n quelconques, on suppose $P(x,y,n)$ c'est-à-dire $x = n^2 \wedge y = 2n+1$, et on doit montrer $P(x+y, y+2, n+1)$, c'est-à-dire $x + y = (n+1)^2 \wedge y + 2 = 2(n+1) + 1$.*
     on a par hypothèse de récurrence $x + y = n^2 + 2n + 1 = (n+1)^2$ et $y + 2 = 2n + 1 + 2 = 2(n+1) + 1$ donc le résultat est bien vérifié

   On en déduit $\forall x\, y\, n, R(x,y,n) \Rightarrow x = n^2 \wedge y = 2n+1$.

4. *La suite x_n est une suite d'entiers strictement croissante qui démarre à 0, il existe donc un unique n tel que $x_n \leq a < x_{n+1}$. D'après la question précédente, on a $x_n = n^2$ et donc $n^2 \leq a < n + 1^2$ et donc n est bien la racine carrée entière de a.*

Rappel des règles logiques

Hypothèse	Classique	Coupure
$\dfrac{A \in \Gamma}{\Gamma \vdash A}$	$\dfrac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}$	$\dfrac{\Gamma, A \vdash B \qquad \Gamma \vdash A}{\Gamma \vdash B}$

	Introduction(I)	Elimination hypothèse(H)
$\bot$		$\dfrac{}{\Gamma, \bot \vdash C}$
$\neg$	$\dfrac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}$	$\dfrac{\Gamma, \neg A \vdash A}{\Gamma, \neg A \vdash C}$
$\wedge$	$\dfrac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$	$\dfrac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C}$
$\vee$	$\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \qquad \dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$	$\dfrac{\Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}$
$\Rightarrow$	$\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}$	$\dfrac{\Gamma, B \vdash C \qquad \Gamma, A \Rightarrow B \vdash A}{\Gamma, A \Rightarrow B \vdash C}$
$\forall$	$\dfrac{\Gamma \vdash P}{\Gamma \vdash \forall x, P} \quad x \notin \mathsf{Vl}(\Gamma)$	$\dfrac{\Gamma, (\forall x, P), P[x \leftarrow t] \vdash C}{\Gamma, (\forall x, P) \vdash C}$
$\exists$	$\dfrac{\Gamma \vdash P[x \leftarrow t]}{\Gamma \vdash \exists x, P}$	$\dfrac{\Gamma, P \vdash C}{\Gamma, (\exists x, P) \vdash C} \quad x \notin \mathsf{Vl}(\Gamma, C)$

$\mathsf{Vl}(\Gamma)$ désigne l'ensemble des variables libres de Γ, c'est-à-dire les variables qui apparaissent dans une des formules de Γ sans être liées par un quantificateur.