Calculabilité et complexité

Université de Montpellier
Examen partiel
9 novembre 2015

Durée 2 heures 30 minutes
Aucun document n'est autorisé
Pas de calculatrice, téléphone portable, montre programmable,
appel à un ami, consultation de l'avis du public, *etc.*

Justifiez vos réponses avec soin !

Exercice 1 échauffement

On note $A + B = \{x + y,\ x \in A \text{ et } y \in B\}$.
Montrez que si A et B sont énumérables, alors $A + B$ l'est aussi.

Exercice 2 archi-classique

Soit $A = \{x,\ [x \mid \cdot] \text{ est une bijection sur les entiers naturels}\}$.

1. En utilisant avec soin le théorème de Rice, montrez que A n'est pas récursif.
2. Sans utiliser le théorème de Rice, montrez que A n'est pas récursif.

Exercice 3 classique

Soit $A = \{x,\ [x \mid 0] \downarrow \text{ et } [x \mid 1] \uparrow\}$.
A et son complémentaire $\bar{A}$ sont-ils récursifs ? énumérables ?

Exercice 4 facile

Soit g une fonction calculable.

1. Montrez qu'il existe une fonction calculable *totale* G telle que $[G(n) \mid \cdot] = n + g(.)$
2. Montrez que $\exists n\ [n \mid \cdot] = n + g(.)$.

Exercice 5 tout aussi aisé

1. Montrez qu'il existe une fonction calculable *totale* f telle que $[f(n) \mid \cdot] = [n \mid \cdot] + 1$
2. Quelles fonctions sont calculées par les points fixes de f ?

Exercice 6 à peine plus dur

1. Montrez qu'il existe 2 programmes consécutifs qui calculent la même fonction.
2. Proposez un système de programmation dans lequel 3 programmes consécutifs ne calculent jamais la même fonction.

Exercice 7 un peu moins dur

On s'intéresse au problème de décision suivant :
Tiling-with-borders
Entrée : Un ensemble fini de tuiles τ et une suite de couleurs s.
Question : Existe-t-il un pavage d'un carré par les tuiles de τ tel que la suite des couleurs des bords du carré soit exactement s ?

Montrez que ce problème est NP-complet.

Exercice 8 Alice prend le tramway

En 2031, dans l'état du Capitaland, Alice est employée comme programmeuse[1] : son travail consiste à réécrire plus clairement, en langage *C+++*, et en utilisant des algorithmes rénovés, des programmes écrits en *Fortran 77* qui datent des années 80. L'entreprise qui emploie Alice est rachetée par Bob. Bob propose au syndicat majoritaire de l'entreprise de négocier un avenant aux contrats des programmeurs : un employé sera licencié si et seulement si Bob parvient à prouver que le programme que l'employé a écrit calcule quelque chose de différent de ce que calculait le programme initial. Dans la négociation, le syndicat exige que les preuves de Bob soient exprimées dans ZFC, ce que Bob accepte. Pour profiter du "seulement si" de la clause, le syndicat signe l'avenant.

Alice paniquée se souvient de l'éxercice suivant, quelle avait résolu à l'automne 2015 en partiel de calculabilité :

1. Montrez qu'il n'existe pas de programme qui prend en entrée $< x, y >$ et qui décide si $[x \mid \cdot] = [y \mid \cdot]$

Elle se précipite alors à l'Université pour consulter son (très) vieux professeur de calculabilité et lui demande si, par hasard il n'aurait pas une idée pour empêcher Bob de la licencier trop facilement. Celui-ci lui répond :
"Ah ah ah, et vous auriez donc suivi mon cours en 2015 ?! Mais si vous aviez correctement composé au partiel, vous sauriez qu'il existe un programme-miracle : quelque soit le programme en *Fortran 77* qu'on vous donne à réécrire, vous pouvez rendre à votre patron ce programme-miracle. Bien sûr, ce programme ne fait pas ce qu'il faut, mais il ne pourra jamais le prouver...".
Alice demande timidement où elle peut trouver le programme-miracle et le vieux professeur hausse les épaules : "Please Alice, use your brain !". Alice réfléchit dans le tramway, oublie de descendre à son arrêt, mais en arrivant au terminus s'écrie : "Nom d'un petit Kleene, j'ai trouvé !".

On rappelle que les théorèmes de ZFC constituent un ensemble énumérable (c'est assez évident : on construit les preuve dans le cadre de systèmes formels à partir d'un nombre fini d'axiomes, et en suivant des règles de déduction ; autrement dit il existe un programme qui permet de vérifer les preuves). L'expression ZFC $\vdash T$ signifie que ZFC permet de prouver la proposition T, ou, autrement dit, elle signifie que T est un théorème de ZFC.

2. En raisonnant par l'absurde, montrez que $\exists \mu \forall q$ ZFC $\nvdash [\mu \mid \cdot] \neq [q \mid \cdot]$. Indication : énumérez les preuves et trouvez une fonction récursive qui à un programme p associe un programme q qui ne calcule pas la même fonction (justifiez qu'on a alors une contradiction).

Un programme μ tel que défini ci-dessus est appelé *proramme-miracle*.

3. Quelles fonctions sont calculées par les programmes-miracles ?

On a ainsi prouvé l'existence d'un programme-miracle μ ; reste à le construire...

4. Proposez une fonction récursive dont les points fixes sont des programmes-miracles. On pourrait remarquer que si $[p \mid x] \neq [q \mid x]$ et que les deux convergent, alors il existe une preuve de ceci dans ZFC.
5. Montrez qu'un programme-miracle peut être trouvé récursivement en fonction du système de preuve considéré.

Epilogue : Alice a pu garder son emploi grâce à son cours de calculabilité d'une part, et son cerveau d'autre part...

1. Je trouve ce terme hideux mais il semble que ce soit le terme politiquement correct...

Calculabilité et complexité

Université de Montpellier
Examen
15 janvier 2016

Durée 3 heures
Aucun document n'est autorisé
Pas de calculatrice, téléphone portable, montre programmable,
appel à un ami, consultation de l'avis du public, *etc.*

Justifiez vos réponses avec soin !

Exercice 1 échauffement

Montrez que $\mathbb{K}$ est énumérable (cours). Montrez que si A et B sont énumérables, alors $A \cup B$ l'est aussi (cours).

Exercice 2 archi-classique

Soit $A = \{x,\ [x \mid \cdot]$ calcule un polynôme à coefficients entiers$\}$.

1. En utilisant avec soin le théorème de Rice, montrez que A n'est pas récursif.
2. Sans utiliser le théorème de Rice, montrez que A n'est pas récursif.
3. Montrez que $\bar{\mathbb{K}}$ se réduit à A. Indication : simuler $[x \mid x]$ sur y étapes et ensuite, si le calcul n'a pas convergé, calculez un polynôme adéquat. Si une convergence est observée, alors diverger.

Exercice 3 classique

Soit $B = \{x,$ si y est une puissance de 2 non nulle alors $[x \mid y] = 2$ sinon si y est une puissance de 3 non nulle alors $[x \mid y] \uparrow$ et dans les autres cas $[x \mid y] = 5\}$.
Montrez que ni B ni son complémentaire $\bar{B}$ ne sont énumérables.

Exercice 4 points fixes faciles

1. Proposez deux fonctions dont les ensembles de points fixes sont disjoints (il faut bien sûr le montrer).
2. Montrez qu'il existe une fonction récursive F qui à x associe un point fixe pour la fonction $[x \mid \cdot]$.

Exercice 5 réductions

Soit $C = \{x,\ \forall y\ [x \mid y] = F(y)\}$ où F est une fonction calculable définie sur un nombre fini non nul de point.

1. Montrez que C est l'ensemble des points fixes d'une fonction récursive qu'on explicitera.
2. Montrez que $\mathbb{K}$ se réduit à C.
3. Montrez que $\bar{\mathbb{K}}$ se réduit à C.
4. En déduire qu'il existe des ensembles de points fixes non énumérables.

Exercice 6 un peu de complexité

Montrez que NP est dans PSPACE (cours)

Exercice 7 tautologies

Soit TAUTO le problème qui prend en entrée une formule et qui cherche à décider si la formule est une tautologie (une tautologie est une formule propositionnelle qui est vraie quelle que soit la valeur de ses variables). Montrez que TAUTO est co-NP-complet.

Exercice 8 NP=co-NP ?

Montrez que NP = co-NP si et seulement si SAT et TAUTO peuvent mutuellement se réduire l'une à l'autre.

Exercice 9 Retour aux points fixes sérieux

Soit $D = \{x,\ \forall y\ [x \mid y] = F(x, y)\}$ où F est une fonction récursive totale. L'objet de l'exercice est de montrer que $\mathbb{K}$ et $\bar{\mathbb{K}}$ se réduisent à D.

1. Si F ne dépend que de y (en d'autres termes si $\forall a, b, y\ F(a, y) = F(b, y)$), expliquez pourquoi vous avez déjà prouvé le résultat recherché.
2. Maintenant, F est une fonction récursive totale qui dépend à la fois de x et de y. Montrez le résultat recherché. Aide : en faisant votre preuve, il est probable que vous ayez besoin comme lemme d'une version du théorème de point fixe avec variable. Vous pouvez seulement énoncer et utiliser le lemme (lucratif), ou alternativement l'énoncer, le prouver puis l'utiliser (très lucratif). Attention à être très précis dans vos preuves.
3. Que se passe-t-il si F est une fonction récursive partielle ?

Logique - Calculabilité - Complexité

Université de Montpellier
Partiel de logique - 2021
13 octobre 2021

Durée 1h30
Aucun document n'est autorisé
Pas de calculatrice, téléphone portable, montre programmable,
appel à un ami, consultation de l'avis du public, *etc.*

Justifiez vos réponses avec grand soin !

Exercice 1 ABC

1. Est-ce que la formule $\forall x \exists y F(x,y) \to \exists y \forall x F(x,y)$ est vraie dans tous les modèles ayant un symbole de prédicat binaire F ? Si oui, expliquez pourquoi. Sinon, proposez un modèle qui fournit un contre-exemple.
2. Est-ce que la formule $\exists y \forall x F(x,y) \to \forall x \exists y F(x,y)$ est vraie dans tous les modèles ayant un symbole de prédicat binaire F ? Si oui, expliquez pourquoi. Sinon, proposez un modèle qui fournit un contre-exemple.

Exercice 2 ABC

1. Qu'est-ce qu'une théorie cohérente ?
2. Donnez un exemple de théorie cohérente et de théorie non cohérente.

Exercice 3 ABC

Soit T une théorie cohérente et A et B deux formules closes. On suppose que $T \vdash A$ et $T \vdash \neg B$. Existe-t-il un modèle de T noté $\mathcal{M}$ tel que $\mathcal{M} \models (B \vee \neg A)$? Justifiez soigneusement en explicitant les théorèmes du cours utilisés.

Exercice 4 ABC

1. Soient T_1, T_2 deux théories. Montrer que si $T_1 \subseteq T_2$ alors les modèles de T_2 sont aussi des modèles de T_1.
2. Soit $\mathcal{M}$ un modèle. Montrer que $\mathcal{M}$ est un modèle de $\mathrm{th}(\mathcal{M})$.

Exercice 5 ABC

Soit T une théorie cohérente. On note $\mathcal{M}_1$ et $\mathcal{M}_2$ deux modèles de T. Définir l'équivalence élémentaire entre $\mathcal{M}_1$ et $\mathcal{M}_2$.

Exercice 6 C

Soit T une théorie cohérente.

1. Donnez une formule qui exprime que tout modèle de T a au moins k éléments.
2. Donnez une formule qui exprime que tout modèle de T a exactement k éléments.
3. Proposez une théorie qui étend T et qui exprime que tout modèle de T est infini.

Exercice 7 BC

Soit F une théorie telle que chaque sous-ensemble fini de F admet un modèle. Soit g une formule close quelconque. On considère maintenant les ensembles de formules $F_1 = F \cup \{g\}$ et $F_2 = F \cup \{\neg g\}$.

1. Est-il possible qu'il existe un modèle $\mathcal{M}$ tel que $\mathcal{M} \models F_1$ et $\mathcal{M} \models F_2$?
2. Montrez qu'au moins l'un des ensembles F_1 et F_2 admet un modèle.
3. Est-il possible que F_1 admette un modèle et F_2 aussi ? Justifiez.

Exercice 8 B

Nous nous plaçons dans le modèle $(\mathbb{N}, S(x), 0)$ où $S(x)$ est la fonction unaire successeur.

1. Ecrivez une formule qui, interprétée dans ce modèle, exprime que chaque entier strictement positif est le successeur d'un autre entier.

Nous ajoutons au modèle un prédicat binaire $<$ représentant l'ordre strict.

2. Qu'exprime la formule $\forall x\ x < S(x)$?
3. Proposez un ordre sur $\mathbb{N}$ tel que $\neg(\forall x\ x < S(x))$ mais où l'une des formules $F_n = \forall x\ x < S(S(\ldots S(x)))$ – où le symbole S apparait n fois – est vraie.

Exercice 9 BC

1. Inventez un ensemble de deux formules closes dont chacune a un modèle mais qui n'ont pas de modèle quand on les considère ensemble.
2. Inventez un ensemble de trois formules closes dont chaque paire a un modèle mais qui n'ont pas de modèle quand on les considère ensemble.

Exercice 10 A

On considère $\mathcal{M} = (\mathbb{Z}, <)$ les entiers relatifs avec l'ordre habituel. On note $T = \mathrm{th}(\mathcal{M})$. On ajoute maintenant deux symboles de constante a et b et on obtient $\mathcal{M}' = (\mathbb{Z}, a, b, <)$.

1. Ecrivez une formule f_n qui exprime qu'il y a au moins n éléments entre a et b.
2. Montrez que $T \cup \{f_n, n \in \mathbb{N}\}$ a un modèle qu'on notera $\mathcal{M}'_1$.
3. On définit $\mathcal{M}_1$ en enlevant les symboles de constante a et b du langage du modèle. Montrez que $\mathcal{M}_1 \models T$.
4. Montrez que $\mathcal{M}$ et $\mathcal{M}_1$ son élémentairement équivalents mais non isomorphes.

Exercice 11 A

Soit T une théorie de l'ordre total strict et dense sans maximum ni minimum noté $<$, avec une constante 0. On note $\mathcal{M} = (\mathbb{Q}, 0_{\mathbb{Q}}, <_{\mathbb{Q}})$ le modèle classique de T d'univers $\mathbb{Q}$. Montrez qu'il n'existe pas de formule $A(x, y, z)$ qui exprimerait dans $\mathbb{Q}$ que $|x - y| = |y - z|$.

Logique - Calculabilité - Complexité

Université de Montpellier

Partiel de logique - 2022
2 décembre 2022

Durée 1h30
Aucun document n'est autorisé
Pas de calculatrice, téléphone portable, montre programmable, appel à un ami, consultation de l'avis du public, *etc.*

Justifiez vos réponses avec grand soin !

Nous nous plaçons dans le cadre de la logique classique du premier ordre, avec égalité.

Exercice 1 cohérences et modèles

Soit T une théorie cohérente et A et B deux formules closes.
On suppose que $T \vdash A$ et $T \vdash \neg B$.
Existe-t-il un modèle de T noté $\mathcal{M}$ tel que $\mathcal{M} \models (B \vee \neg A)$?
Justifiez soigneusement en explicitant les théorèmes du cours utilisés.

Exercice 2 la cohérence et la preuve

Soit T une théorie et f une formule.

1. Montrez que $T \vdash f$ si et seulement si $T \cup \{\neg f\}$ est incohérente.
2. Montrez que si T est cohérente, alors il en est de même d'au moins une des extensions $T \cup \{f\}$ et $T \cup \{\neg f\}$

Exercice 3 les constantes

Soit T une théorie, f une formule à une seule variable libre et c un symbole de constante n'apparaissanit ni dans f ni dans T.

1. Montrez que $T \vdash f(c)$ entraine $T \vdash \forall x\ f(x)$.
2. Montrez que si $T \cup \{\exists x\ f(x)\}$ est cohérent, alors il en est de même de $T \cup \{f(c)\}$

Exercice 4 tailles des modèles

Soit T une théorie sur le langage $\mathcal{L}$ admettant des modèles de taille arbitrairement grande (on rappelle que la taille d'un modèle est la taille de son univers). Soit $\mathcal{L}'$ le langage obtenu en ajoutant à $\mathcal{L}$ les symboles de constante $(c_n)_{n\in\mathbb{N}}$. Soit T' la théorie obtenue en ajoutant à T les formules $c_i \neq c_j$ pour $i < j$.

1. Soit $\mathcal{M}$ un modèle de T sur le langage $\mathcal{L}$. comment faut-il modifier $\mathcal{M}$ pour construire $\mathcal{M}'$ qui soit un modèle de T sur le langage $\mathcal{L}'$.
2. Soit T_f une partie finie (quelconque) de la théorie T. Montrez en utilisant la question précédente qu'elle a un modèle dans le langage $\mathcal{L}'$.
3. Replaçons-nous dans le langage $\mathcal{L}$. Montrez que soit il existe un entier naturel n tel que tous les modèles de T ont une taille bornée par n, soit T a des modèles infinis.

Exercice 5 (in)-complétude

Soit T une théorie énumérable assez puissante (hypothèse du théorème de Gödel). Soit g une formule close quelconque. On considère maintenant les ensembles de formules $T_1 = T \cup \{g\}$ et $T_2 = T \cup \{\neg g\}$.

1. Supposons que $T \nvdash g$. Est-ce qu'il existe un modèle $\mathcal{M}$ tel que $\mathcal{M} \models T_2$?
2. Soit g une formule indécidable de Gödel. Montrez que si T est cohérente alors les théories T_1 et T_2 ont chacune un modèle. Peuvent-elles avoir le même ?

On considère le programme a qui ignore son entrée, énumère les théorèmes d'un côté, les énoncés réfutables de l'autre (ces deux processus en parallèle), et si jamais il trouve un énoncé à la fois prouvable et réfutable, s'arrête. On remarque que ce programme s'arrête si et seulement si la théorie est incohérente.

3. En utilisant le lemme de codage de Gödel (pour la fonction step) montrez qu'il existe une formule ψ qui exprime que a ne s'arrête pas.

On considère le programme b qui prend un entier n en entrée, énumère les théorèmes et les énoncés réfutables comme le faisait a mais seulement sur n pas. Ensuite, il donne en sortie la formule de plus petit numéro qui n'a pas ainsi été énumérée.

4. Montrez que $[b|.]$ est une fonction croissante (au sens large).
5. Est-ce que $[b|.]$ tend vers l'infini ? est bornée ? (justifiez).

Logique - Calculabilité - Complexité

Université de Montpellier
Examen - 2022-2023
10 janvier 2023

Durée 2h
Aucun document n'est autorisé
Pas de calculatrice, téléphone portable, montre programmable,
appel à un ami, consultation de l'avis du public, *etc.*

Justifiez vos réponses avec grand soin !

Dans tout ce qui suit, comme dans le cours, le symbole $\prec$ désigne la *réduction many-one* ; les ensembles considérés sont des ensembles d'entiers, qu'ils contiennent des données ou des programmes.

Exercice 1 mise en jambes

1. Montrez que $\mathbb{K}$ et son complémentaire $\overline{\mathbb{K}}$ ne sont pas comparables par $\prec$.
2. Montrez que si un ensemble est énumérable par une fonction récursive totale strictement croissante, alors il est infini et récursif.

Exercice 2 réductions

Soit A l'ensemble des programmes x dont l'ensemble de convergence (*i. e.* $\{y, [x|y]\downarrow\}$) est un ensemble récursif.

1. Un ensemble de convergence peut-il être récursif ? non récursif ? énumérable ? non énumérable ? Pour chaque cas, donnez un exemple si votre réponse est oui, une justification si la réponse est non.
2. En utilisant avec soin le théorème de Rice, montrez que A n'est pas récursif.
3. Montrez que $\mathbb{K} \prec A$.
4. Montrez que $\mathbb{K} \prec \overline{A}$.
5. Montrez que ni A ni $\overline{A}$ ne sont énumérables.

Exercice 3 la cohérence et la preuve

Soit T une théorie sur le langage $\mathcal{L}_T$ et f une formule de $\mathcal{L}_T$.

1. Montrez que $T \vdash f$ si et seulement si $T \cup \{\neg f\} \vdash f \wedge \neg f$.
2. Montrez que si T est cohérente, alors il en est de même d'au moins une des extensions $T \cup \{f\}$ et $T \cup \{\neg f\}$

Exercice 4 cours - incomplétude

On se place dans une théorie énumérable assez puissante (au sens du cours) qu'on note T sur le langage $\mathcal{L}_T$. L'exercice consiste à re-prouver des résultats du cours. Répondre "c'est traité dans le cours" ne rapporte pas de points.

1. Énoncez un lemme de codage pour la fonction *step* de la calculabilité puis utilisez-le pour montrer qu'il existe une formule de $\mathcal{L}_T$ (qu'on note $f(x)$) qui exprime $[x|0]\downarrow$.
2. Montrez qu'il existe a tel que $T \nvdash f(a)$ et $T \nvdash \neg f(a)$. Pour la suite on en choisit un, noté a_0.
3. Est-ce que $[a_0|0]\downarrow$ (au sens du cours de calculabilité) ?
4. Expliquez où et sous quelle forme la cohérence de T a été utilisée pour prouver le résultat de la question précédente.
5. Montrez qu'il existe une formule g, logiquement équivalente à la cohérence de T, telle que $T \nvdash g$ et $T \nvdash \neg g$.

Calculabilité et complexité

Université de Montpellier
Examen
30 mars 2016

Durée 2 heures
Aucun document n'est autorisé
Pas de calculatrice, téléphone portable, montre programmable,
appel à un ami, consultation de l'avis du public, *etc.*

Justifiez vos réponses avec soin !

Exercice 1 échauffement

1. Montrez que $\mathbb{K}$ est énumérable.
2. Montrez que si A et B sont énumérables, alors $A * B = \{x * y,\ x \in A$ et $y \in B\}$ l'est aussi.

Exercice 2 archi-classique

Soit $A = \{x,\ [x \mid \cdot]$ calcule un polynôme à coefficients premiers supérieurs à 2$\}$.

1. En utilisant avec soin le théorème de Rice, montrez que A n'est pas récursif.
2. Sans utiliser le théorème de Rice, montrez que A n'est pas récursif.
3. Montrez que $\bar{\mathbb{K}}$ se réduit à A.

Exercice 3 classique

Soit $B = \{x,$ si y est pair alors $[x \mid y] = 0$ sinon si y est non null et divisible par 3 alors $[x \mid y] \uparrow$ et dans les autres cas $[x \mid y] = 1\}$. Montrez que ni B ni son complémentaire ne sont énumérables.

Exercice 4 points fixes faciles

Proposez un ensemble énumérable infini de programmes qui calculent des fonctions dont les ensembles de points fixes sont disjoints deux à deux (il faut bien sûr le montrer).

Exercice 5 réductions

Soit $C = \{x, \forall y\ [x \mid y] = F(y)\}$ où F est une fonction calculable définie sur les nombres pairs.

1. Montrez que $\mathbb{K}$ se réduit à C.
2. Montrez que $\bar{\mathbb{K}}$ se réduit à C.
3. En déduire qu'il existe des ensembles de points fixes non énumérables.

Exercice 6 un peu de complexité

Au niveau des classes de complexité que vous connaissez, que se passe-t-il si P=NP ? On déterminera celles qui deviennent égales, celles qui restent distinctes et celles pour lesquelles la question de l'égalité reste ouverte.

Exercice 7 Sommes

Soit SubsetSum le problème où on donne en entrée un nombre fini d'entiers relatifs non nuls, et où on se demande si tous les sous-ensembles non vides de cette entrée ont une somme différente de zéro.

1. Montrez que SubsetSum est co-NP-complet.
2. Montrez que NP = co-NP si et seulement si Sat et SubsetSum peuvent mutuellement se réduire l'une à l'autre.

Calculabilité et complexité

Université de Montpellier
Examen partiel
9 novembre 2016

Durée 3 heures
Aucun document n'est autorisé
Pas de calculatrice, téléphone portable, montre programmable, appel à un ami, consultation de l'avis du public, *etc.*

Justifiez vos réponses avec soin !

Exercice 1 échauffement

Soit f une fonction récursive totale à deux arguments.
On note $\widehat{fAB} = \{f(x,y),\ x \in A \text{ et } y \in B\}$.

1. Montrez que si A et B sont énumérables, alors $\widehat{fAB}$ l'est aussi.
2. Que se passe-t-il si f est seulement récursive (partielle) ?

Exercice 2 archi-classique

Le symbole $\prec$ représente ici la réduction (many-one) entre ensembles d'entiers.
Soit $A = \{x,\ [x \mid \cdot] \text{ calcule une fonction totale}\}$.

1. En utilisant avec soin le théorème de Rice, montrez que A n'est pas récursif.
2. Sans utiliser le théorème de Rice, montrez que $\mathbb{K} \prec A$.

Soit $B = \{x,\ [x \mid \cdot] \text{ a un domaine infini}\}$.

3. En utilisant avec soin le théorème de Rice, montrez que B n'est pas récursif.
4. Sans utiliser le théorème de Rice, montrez que $\mathbb{K} \prec B$.
5. Est-ce que $\overline{\mathbb{K}} \prec A$?
6. Est-ce que $\overline{\mathbb{K}} \prec B$?
7. Est-ce que $A \prec B$?
8. Est-ce que $B \prec A$?
9. Est-ce que $A \prec \overline{\mathbb{K}}$?
10. Est-ce que $B \prec \mathbb{K}$?

Exercice 3 facile

Soit g une fonction calculable.

1. Montrez qu'il existe une fonction calculable *totale* G telle que $[G(n) \mid \cdot] = n + g(.)$
2. Montrez que $\exists n\ [n \mid \cdot] = n + g(.)$.

Exercice 4 toujours facile

1. Montrez qu'il existe une fonction calculable *totale* f telle que $[f(n) \mid \cdot] = [n \mid \cdot] + 1$
2. Quelles fonctions sont calculées par les points fixes de f ?

Exercice 5 classique

1. Montrez qu'il existe deux programmes dont le premier écrit (quelle que soit son entrée) 2 fois le texte du second et dont le second écrit (quelle que soit son entrée) 3 fois le texte du premier.
2. En utilisant uniquement le premier théorème de point fixe, montrez qu'il existe deux programmes dont le premier écrit (quelle que soit son entrée) 2 fois le texte du second et le second écrit (quelle que soit son entrée) 2 fois le texte du premier.
3. Montrez qu'il existe deux programmes différents dont le premier écrit (quelle que soit son entrée) son propre texte suivi par le miroir du texte du second et dont le second écrit (quelle que soit son entrée) son propre texte suivi par le mirroir du texte du premier.
4. En utilisant uniquement le premier théorème de point fixe, montrez qu'il existe deux programmes dont le premier écrit (quelle que soit son entrée) son propre texte suivi par le miroir du texte du second et dont le second écrit (quelle que soit son entrée) son propre texte suivi par le mirroir du texte du premier.

Exercice 6 plus intéressant

On note par W_x le domaine de la fonction calculée par le programme x : $W_x = \{y,\ [x \mid y] \downarrow\}$. On définit $A = \{x,\ W_x \subset \overline{\mathbb{K}}\}$.

1. Montrez que $A \subset \overline{\mathbb{K}}$.
2. Montrez qu'il existe x tel que $W_x = \overline{\{x\}}$.
3. Montrez que $A \neq \overline{\mathbb{K}}$.

Calculabilité et complexité

Université de Montpellier

Examen

9 janvier 2017

Durée 2 heures

Aucun document n'est autorisé

Pas de calculatrice, téléphone portable, montre programmable, appel à un ami, consultation de l'avis du public, *etc.*

Justifiez vos réponses avec soin !

Exercice 1 échauffement

1. Montrez que $\mathbb{K}$ est énumérable.
2. Montrez que si A et B sont énumérables, si $\mathbb{K} \prec A$ et $\mathbb{K} \prec B$, alors $C = \{2^x 3^y,\ x \in A \text{ et } y \in B\}$ est énumérable et vérifie $\mathbb{K} \prec C$.

Exercice 2 archi-classique

Soit $A_{p,q} = \{x,\ [x \mid p] = 0 \text{ et } [x \mid q] \text{ diverge}\}$, où $p \neq q$.

1. $A_{p,q} \prec \mathbb{K}$, $A_{p,q} \prec \overline{\mathbb{K}}$, $\mathbb{K} \prec A_{p,q}$, $\overline{\mathbb{K}} \prec A_{p,q}$?
2. Si p, q, r sont distincts, est-ce que $A_{p,q}$ et $A_{p,q}$ sont récursivement séparables ?

Exercice 3 toujours facile

1. Montrez qu'il existe une fonction calculable *totale* f telle que $[f(n) \mid \cdot] = [n \mid \cdot] + [2^n \mid \cdot] + 2n + 1$
2. Quelles fonctions sont calculées par les points fixes de f ?

Exercice 4 un zeste d'oracle

1. Existe-t-il un oracle A tel que $PSPACE^A \neq EXP^A$?
2. Existe-t-il un oracle A tel que $PSPACE^A = EXP^A$?

Exercice 5 beaucoup d'effondrements

1. Montrez que si $NP = coNP$, alors
$$\Sigma_2^p = NP \ .$$
2. Montrez que si $NP = coNP$, alors pour tout $n \geq 1$
$$\Sigma_n^p = \Pi_n^p = NP \ .$$
3. Montrez que si le problème SAT est dans $coNP$, alors toutes les classes Σ_n^p et Π_n^p coincident avec NP.

Exercice 6 une goutte de preuves interactives

Montrez que le langage suivant est dans IP

$$NQR = \{(k,p) \mid p \text{ est premier, et il n'existe pas } m \text{ vérifiant } m^3 = k \bmod p\} \ .$$

Calculabilité et complexité

UNIVERSITÉ DE MONTPELLIER
Examen
9 janvier 2017

Durée 3 heures
Aucun document n'est autorisé
Pas de calculatrice, téléphone portable, montre programmable, appel à un ami, consultation de l'avis du public, *etc.*

Justifiez vos réponses avec soin !

Exercice 1 échauffement

1. Montrez que $\mathbb{K}$ est énumérable.
2. Montrez que si A et B sont énumérables, alors $A^B = \{x^y,\ x \in A \text{ et } y \in B\}$ l'est aussi.

Exercice 2 archi-classique

Le symbole $\prec$ représente ici la réduction (many-one) entre ensembles d'entiers.
Soit $A = \{x,\ x \text{ diverge sur au moins une entrée}\}$.

1. En utilisant avec soin le théorème de Rice, montrez que A n'est pas récursif.
2. Est-ce que $\mathbb{K} \prec A$?
3. Est-ce que $\overline{\mathbb{K}} \prec A$?
4. Est-ce que $A \prec \overline{\mathbb{K}}$?
5. Est-ce que $A \prec \mathbb{K}$?

Exercice 3 toujours facile

1. Montrez qu'il existe une fonction calculable *totale* f telle que
$[f(n) \mid \cdot] = [n \mid \cdot] + [n+1 \mid \cdot] + n + 1$
2. Quelles fonctions sont calculées par les points fixes de f ?

Exercice 4 stratégie

Si, dans la suite de votre Master, on vous demande de montrer qu'un problème est NP-complet, comment procèderez-vous ?

Exercice 5 une idée de BPP

Montrez que si SAT est dans BPP, alors $NP \subset BPP$.

Exercice 6 un zeste d'oracle

Montrez qu'il existe un oracle A tel que

$$PSPACE^A \neq EXP^A \quad .$$

Exercice 7 un peu de $coNP$

On rappelle qu'un problème A est $coNP$-complet s'il est dans $coNP$, et si pour tout autre problème $B \in coNP$ on a $B \leq_m^p A$. Donnez un exemple de problème $coNP$-complet.

Exercice 8 beaucoup d'effondrements

1. Montrez que si $NP = coNP$, alors

$$\Sigma_2^p = NP \ .$$

2. Montrez que si $NP = coNP$, alors pour tout $n \geq 1$

$$\Sigma_n^p = \Pi_n^p = NP \ .$$

3. Montrez que si le problème SAT est dans $coNP$, alors toutes les classes Σ_n^p et Π_n^p coincident avec NP.

Exercice 9 une goutte de preuves interactives

Montrez que le langage suivant est dans IP

$$NQR = \{(k, p) \mid p \text{ est premier, et il n'existe pas } m \text{ vérifiant } m^2 = k \ mod \ p\} \ .$$