Computational Complexity

Course of Pascal KOIRAN

Notes and LaTeX figures by A. Mazoyer

M1

ÉCOLE
NORMALE
SUPÉRIEURE
DE LYON

Contents

Chapter 1

Machines de Turing

On travaille avec des machines de Turing à $k \geqslant 1$ rubans. Les rubans sont semi-infinis à droite. Sur chaque ruban, on a une tête de lecture qui lit le contenu d'une case.

A chaque étape :

1. M lit les k caractères situés sous les têtes de lecture $(a_1, \cdots, a_k)$
2. En fonction des caractères $(a_1, \cdots, a_k)$ et de son état interne $q \in Q$, M remplace chaque a_i par un nouveau caractère a_i', M passe dans un nouvel état q', et déplace les têtes de lecture d'au plus une case vers la gauche ou vers la droite

1.1 Définitions

Definition 1.1 (Machine de Turing)

Plus formellement, on a un triplet (Γ, Q, δ) avec Γ l'alphabet du ruban, Q un ensemble fini d'états et $\delta : Q \times \Gamma^k \to Q \times \Gamma^k \to \{G, D, I\}^k$

On calcule des fonctions $f : \{0,1\}^* \to \{0,1\}^*$ (ou $f : \Sigma^* \to \Sigma^*$).

Definition 1.2 (Reconnaître un language)

Pour reconnaître un language $L \subseteq \{0,1\}^*$, on calcule $\mathbf{1}_L : \{0,1\}^* \to \{0,1\}$. On peut ainsi avoir un état acceptant (q_a) et un état de rejet (q_r).

On va supposer que Γ contient au moins :

- le symbole blanc B ($\square$ dans Arone-Rajak ?)
- le symbole de départ $\triangle$, et $0, 1$ (ou en général $\Sigma \subseteq \Gamma$)

Definition 1.3

On a un *ruban d'entrée*, un *ruban de sortie*, des *rubans de travail*, un *état initial* q_a et un *état final* q_f.

Au départ, M est dans l'état q_a, le ruban d'entrée contient $\triangle x B^\infty$ avec $x \in \Sigma^*$ l'entrée $(B \notin \Sigma)$.

Definition 1.4
On dit que M calcule la fonction $f : \Sigma^* \to \Sigma^*$ si pour toute entrée $x \in \Sigma^*$, le calcul de M se termine, avec $f(x)$ écrit sur le ruban de sortie.

Remarks :

▷ le ruban d'entrée est souvent en lecture uniquement

▷ le ruban de sortie est souvent en écriture uniquement

Variantes du modèle

1. rubans bi-infinis
2. on peut simuler une machine avec l'alphabet $0, 1, 2, 3, B, \triangle$ par une machine avec l'alphabet $0, 1, B, \triangle$: $0 \mapsto 00, 1 \mapsto 01, 2 \mapsto 10, 3 \mapsto 11$, facteur 2 en espace (et en temps)

Definition 1.5 (Complexité en temps)
Un language $L \subseteq \Sigma^*$ est *reconnu* en temps $T(n)$ par une machine M si :

- M reconnaît L
- sur toute entrée x de taille L, M s'arrête en au plus $T(n)$ étapes de calcul

Definition 1.6 (classe DTIME)
L est dans $\mathrm{DTIME}(f(n))$ s'il existe une machine (à plusieurs rubans) qui reconnaît L en temps $O(f(n))$.
On supposera toujours $f(n) \geqslant n + 1$.

Proposition 1.7

$$P = \bigcup_{\alpha \geqslant 1} n^\alpha$$

Theorem 1.8
Si $L \in \mathrm{DTIME}(f(n))$, alors L peut être résolu en temps $\Omega(f(n)^2)$ sur une machine à 1 ruban.

Theorem 1.9 (Théorème de simulation efficace)
Pour toute machien M fonctionnant en temps $T(n)$, il existe une machine M' à 2 rubans qui fonctionne en temps $O(T(n \log T(n)))$ telle que $M(x) = M'(x)$ pour toute entrée $x \in \Sigma^*$.

Definition 1.10 (Machine de Turing universelle)
Une *machine universelle* U prend en entrée des couples $\langle x, \alpha \rangle$ avec $x \in \{0,1\}^*$ et $\alpha \in \{0,1\}^*$ et simule code d'une machine de Turing M_α, c'est-à-dire pour tout x et tout α, on doit avoir $U(\langle x, \alpha \rangle) = M_\alpha(x)$.

Theorem 1.11
Il existe une machine de Turing universelle U telle que sur toute entrée $\langle x, \alpha \rangle$, si M_α s'arrête sur l'entrée x en T étapes, alors U s'arrête en au plus $c \cdot T \log T$ avec c une constante dépendant de x.

Proof
Construction de U:
On montre d'abord que si M_α est une machine à 2 rubans, U peut simuler M_α en temps linéaire.
M_β a 2 rubans et l'alphabet est $\triangle, 0, 1, B$. U a 4 rubans :

- 2 rubans stockent les rubans de M_β
- un ruban stocke l'état de M_β
- le ruban d'entrée contient $\langle x, \beta \rangle$

Pour faire une étape de calcul de M_β, U doit déterminer $\delta(q, a, b)$. La complexité de cette opération est cachée dans la constante.

Complexité
construire M_β prend un temps indépendant de x

Cas général:

1. sur l'entrée $\langle x, \alpha \rangle$, construire la machine M_β à 2 rubans donnée par le théorème de simulation efficace
2. simuler la machine M_β en temps linéaire

□

1.2 Non déterminisme

Definition 1.12 (Machine de Turing non déterministe)
La définition est la même que celle d'une machine de Turing déterministe, mais on remplace δ par

$$\delta : Q \times \Gamma^k \to \mathcal{P}(Q \times \Gamma^k \times \{G, D, I\}^k)$$

On a deux états finaux q_a et q_r.
Une entrée $x \in \Sigma^*$ est acceptée s'il existe une exécution de calcul acceptant sur l'entrée x.

Definition 1.13 (Classe NTIME)
NTIME$(T(n))$ est l'ensemble des langages acceptés par une machine de Turing non déterministe fonctionnant en temps $O(T(n))$ sur toute entrée de taille n et tout chemin de calcul.

Definition 1.14 (Classe NP)
Un langage L est dans **NP** s'il existe une machine non déterministe M fonctionnant en temps polynomial tel que L est l'ensemble des entrées acceptées par M.

$$\mathbf{NP} = \bigcup_{\alpha \geqslant 1} \text{NTIME}(n^\alpha)$$

Theorem 1.15
$L \in \mathbf{NP}$ s'il existe un polynôme p et $A \in \mathbf{P}$ tel que pour tout $x \in \{0,1\}^*$,

$$x \in L \Leftrightarrow \exists y \in \{0,1\}^*, \langle x, y\rangle^{1} \in A$$

[1] $\langle x, y\rangle = 1^{|x|}0xy$

1.3 NP-complétude

Definition 1.16 (Réduction en temps polynomial)
Un problème A se réduit à B en temps polynomial s'il existe une fonction $f : \Sigma^* \to \Sigma^*$ calculable en temps polynomial telle que $x \in \Leftrightarrow f(x) \in B$.

Notation
$A \leqslant_p B$ ou $A \leqslant_m B$

Remark : Si $A \leqslant_m B$ et $B \leqslant_m C$, alors $A \leqslant_m C$ (on compose les réductions).

Definition 1.17 (NP-complétude)
A est **NP**−complet si

1. $A \in \mathbf{NP}$
2. $B \leqslant_m A$ pour tout $B \in \mathbf{NP}$

Supposons A **NP**−complet.
Pour que $A' \in \mathbf{NP}$ soit **NP**−complet, on doit montrer que $A \leqslant_m A'$. Dans ce cas pour tout $B \in \mathbf{NP}$, $B \leqslant_m A \leqslant_m A'$ donc $B \leqslant_m A'$.

Le problème de départ classique : SAT (ou 3-SAT)

Dans ce cours : on part de CircuitSAT (satisfiabilité des circuits booléens).

Chapter 2

Circuits booléens

2.1 Définitions

Definition 2.1 (Circuit booléen)

Un circuit booléen est un DAG (graphe orienté acyclique) dont les sommets sont de degré entrant 0, 1 ou 2.

- Les sommets de degré entrant 2 sont étiquetés par $\wedge$ ou $\vee$.
- Les sommets de degré entrant 1 sont étiquetés par $\neg$.
- Les sommets de degré entrant 0 sont étiquetés par 0, 1 ou des variables booléennes $x_1, \ldots, x_n$

Definition 2.2 (Valuation d'un circuit booléen)

Soit C un circuit booléen avec des variables d'entrée $x_1, \ldots, x_n$. Etant donné $a \in \{0,1\}^n$, on définit pour chaque porte α de C la valeur prise par α sur l'entrée a.

- pour les portes d'entrée, $val(x_i) = a_i$, $val(0) = 0$, $val(1) = 1$.
- pour une porte
  - $\alpha = \beta \vee \gamma$, $val(\alpha) = val(\beta) \vee val(\gamma)$
  - $\alpha = \beta \wedge \gamma$, $val(\alpha) = val(\beta) \wedge val(\gamma)$
  - $\alpha = \neg\beta$, $val(\alpha) = \neg val(\beta)$

Definition 2.3

En supposant que C a une seule porte α de degré sortant 0 : α est la *porte de sortie* de C, et $val(C) = val(\alpha)$.
C calcule une fonction booléenne $f : \{0,1\}^n \to \{0,1\}$.
Si C a s portes de sortie, C calcule $f : \{0,1\}^n \to \{0,1\}^s$.

Remark : toute fonction booléenne peut être calculée par un circuit.

Problème : donner une famille de fonctions booléennes "explicite" $(f_n)_{n\geqslant 1}$ qui n'est pas calculable par des circuits de taille polynomiale

Problème de la valeur de circuit (PVC/CVP)

- Donnée : son circuit C avec n variables d'entrée, et $\alpha \in \{0,1\}^n$
- Question : sortie de C sur l'entrée $a \in \{0,1\}^n$

Lemma 2.4

$$PVC \in \mathbf{P}$$

Algorithme : tant qu'il existe une porte α de C qui n'est pas évaluée, mais dont toutes les entrées le sont, choisir une telle porte et l'évaluer.
Retourner la valeur prise par la porte de sortie.

On peut exécuter cet algorithme à l'aide d'un tri topologique pour l'ordre d'évaluation.

2.2 Simulation des machines de Turing par les circuits

Proposition 2.5

Soit M une machine à un ruban fonctionnant en temps $T(n)$. M peut être simulée sur les entrées de taille n par un circuit de taille $O(T(n)^2)$.

Remark : on peut donner la borne $O(T(n)\log(T(n)))$ au lieu de $O(T(n)^2)$, même pour des machines à plusieurs rubans.

2.2.1 Diagramme espace-temps

[[PLS SI QQN A DES FIGURES]]
On doit considérer un diagramme de taille $(T(n)+1)\times(T(n)+1)$.
Contenu de la cellule (i,t) : dépend uniquement du contenu de 3 cellules[1] (bas gauche, bas, bas droite).

[1] C'est le principe de localité du calcul

- $l_{a,i,t} \Leftrightarrow$ à l'instant t, la case i contient la lettre a
- $q_{r,i,t} \Leftrightarrow$ à l'instant t, la machine est dans l'état r et la tête de lecture est sur la case i.

Les valeurs de ces variables peuvent s'obtenir à partir des valeurs des variables pour les 3 cellules $(i-1,t-1),(i,t-1),(i+1,t-1) \rightsquigarrow$ fonction booléenne $f : \{0,1\}^{3p} \to \{0,1\}^p$.

f dépend uniquement de $M \Rightarrow f$ est calculée par un circuit C.

Le circuit final s'obtient en récoltant $O(T(n)^2)$ copies de C.

L'entrée est acceptée si $\bigvee_{i=0}^{T(n)} q_{q_a,i,T(n)}$.

Definition 2.6 (Famille de circuits uniforme)

Soit $(C_n)_{n\geqslant 1}$ une famille de circuits sur n variables d'entrées $x_1, \ldots, x_n$. Cette famille est *uniforme* s'il existe une machine de Turing en temps polynomial qui sur l'entrée 1^n calcule une description complète de C_n : pour chaque porte α elle calcule

- le type de la porte
- si c'est une porte d'entrée, son étiquette
- si ce n'est pas une porte d'entrée, les numéros des portes en entrée de α

Remark : C_n est de taille polynomiale en n

Theorem 2.7

Un langage $L \subseteq \{0,1\}^*$ est dans **P** si et seulement si L est reconnu par une famille uniforme de circuits booléens de taille polynomiale.

Proof

$\Rightarrow$ Soit $L \in \mathbf{P}$. On a vu que L peut être reconnu par une famille de circuits de taille polynomiale.

Algorithme : boucle sur i et $t \rightsquigarrow$ construction en temps polynomial (espace logarithmique)

$\Leftarrow$ Algorithme de reconnaissance de L :

- sur l'entrée $x \in \{0,1\}^n$, construire C_n en temps polynomial

- évaluer C_n sur l'entrée x en temps polynomiale

□

2.3 Un premier problème NP-complet

Theorem 2.8

CircuitSAT est **NP**−complet.

Données : un circuit booléen C avec n variables d'entrée.
Question : existe-t-il une entrée $a \in \{0,1\}^n$ telle que $C(a) = 1$?

Proof

- CircuitSAT $\in$ **NP** : a est le certificat.
- Soit $L \in$ **NP**. Il existe une machine de Turing non déterministe M fonctionnant en temps polynomial $T(n)$ qui reconnaît L.

  Soit $x \in \{0,1\}^n$. On doit construire en temps polynomial un circuit C_x tel que C_x est satisfiable si et seulement si $x \in L$.

  On peut simuler M sur l'entrée x par un circuit de taille $O(T(n)^2)$, mais ce circuit n'est pas suffisant : il faut modéliser le non déterminisme.

  On ajoute des variables d'entrée supplémentaires $y_1, \ldots, y_{T(n)}$ qui modélisent les choix non déterministes de la machine.

  On construit un circuit C_x qui simule M sur l'entrée x, en utilisant les variables y_i pour les choix non déterministes.

  Alors C_x est satisfiable si et seulement si il existe une suite de choix non déterministes (valeurs des y_i) telle que M accepte l'entrée x, c'est-à-dire si et seulement si $x \in L$.

□

Theorem 2.9 (Cook-Levin)

3-SAT est **NP**−complet.

Proof

- 3-SAT $\in$ **NP** : la valuation satisfaisante est le certificat.
- On fait une réduction de CircuitSAT à 3-SAT.

  Soit C un circuit booléen avec des variables d'entrée $x_1, \ldots, x_n$. Pour chaque porte α de C, on crée une variable z_α qui représente la valeur prise par la porte α. On utilise l'identité $P \Rightarrow Q \Leftrightarrow \neg P \vee Q$ pour construire des clauses qui contraignent les variables z_α à respecter le fonctionnement des portes. Par exemple :

  - si $\alpha = \beta \wedge \gamma$, on ajoute les clauses $(\neg z_\beta \vee \neg z_\gamma \vee z_\alpha)$, $(z_\beta \vee \neg z_\alpha)$, $(z_\gamma \vee \neg z_\alpha)$
  - si $\alpha = \beta \vee \gamma$, on ajoute les clauses $(z_\beta \vee z_\gamma \vee \neg z_\alpha)$, $(\neg z_\beta \vee z_\alpha)$, $(\neg z_\gamma \vee z_\alpha)$
  - si $\alpha = \neg\beta$, on ajoute les clauses $(\neg z_\beta \vee \neg z_\alpha)$, $(z_\beta \vee z_\alpha)$

  Enfin, on ajoute la clause $(z_{\alpha_{sortie}})$ pour forcer la porte de sortie à être vraie.

□

Chapter 3

Complexité en espace

Definition 3.1

L'*espace utilisé par une machine de Turing déterministe* sur l'entrée x est le nombre de cases distinctes utilisées sur les **rubans de travail** au cours de son calcul sur x.

On dit que M fonctionne en espace $s(n)$ si M s'arrête sur toutes ses entrées, et utilise un espace au plus $s(n)$ sur toute entrée de taille n.

DSPACE($s(n)$) est la classe des langages reconnus par une machine de Turing déterministe fonctionnant en espace $O(s(n))$.

On supposera que sur le ruban d'entrée, la tête de lecture ne dépasse jamais la fin de l'entrée.

Example

- Un algorithme naïf pour SAT utilise un espace $O(n)$: on peut énumérer toutes les affectations possibles des variables en utilisant un compteur binaire de taille n, et vérifier si l'une d'entre elles satisfait la formule.
- L'addition de deux entiers de taille n peut être effectuée en espace $O(\log n)$: il suffit de stocker les positions des bits en cours d'addition et la retenue.

Proposition 3.2

$$\text{NTIME}(f(n)) \subseteq \text{DSPACE}(f(n))$$

Definition 3.3 (Fonction constructible en espace)

Une fonction $t : \mathbb{N} \to \mathbb{N}$ est *constructible en espace* s'il existe une machine de Turing qui sur l'entrée 1^n calcule $1^{t(n)}$ en espace $O(t(n))$.

Proof (de la proposition)

En supposant t constructible en espace

Soit $L \in \text{NTIME}(t(n))$, et M une machine non déterministe qui reconnaît L en temps $\leqslant \alpha t(n)$.
On code un chemin de calcul de M $y \in \{0, 1, \ldots, R-1\}^{\alpha t(n)}$ où R est le nombre de choix possibles à chaque étape (dépendant de M).

Algorithme : sur l'entrée x de taille n

1. Calculer $t(n)$ en espace $O(t(n))$
2. Pour chaque y de taille $\alpha t(n)$, simuler M sur l'entrée x en suivant les choix donnés par y. Si l'une des simulations accepte, accepter.
3. Rejeter si aucune simulation n'accepte.

Sans l'hypothèse de constructabilité en espace, on peut obtenir la même inclusion avec une légère modification de l'argument.
On fait fonctionner le même algorithme pour des chemins de calcul de longueur $t = 1, 2, 3, \ldots$ jusqu'à ce que la simulation de M sur l'entrée x s'arrête (ce qui arrive forcément si $x \in L$). On s'arrête pour $t = \alpha t(n)$ au plus. □

Proposition 3.4

Si $L \in \text{DSPACE}(s(n))$ alors $L \in \text{DTIME}\left(2^{C \cdot s(n)}\right)$ pour une constante C si $s(n) \geqslant \log n$.

Proof

On compte le nombre de configurations distinctes possibles d'une machine M sur l'entrée x de taille n.
Si le calcul prend un temps $> N$, on boucle. On doit montrer que N est $2^{O(s(n))}$.

Une configuration est définie[1] par :

- l'état courant : au plus Q possibilités
- la position de la tête de lecture sur le ruban d'entrée : au plus n possibilités
- le contenu des cases utilisées sur les rubans de travail : au plus $|\Gamma|^{s(n)}$ possibilités
- la position des têtes de lecture sur les rubans de travail : au plus $s(n)^k$ possibilités si k est le nombre de rubans de travail

□

[1] On n'a pas besoin de la position de la tête sur le ruban de sortie car ça n'influt pas le calcul.

Index