Un chemin pour Hamilton

Présentation du LSV

Aliaume Lopez

11 Juin 2019

En thèse sous la direction de
Sylvain Schmitz
Jean Goubault-Larrecq

école
normale
supérieure
paris–saclay

La recherche en informatique

Des domaines variés

Survolez la minicarte

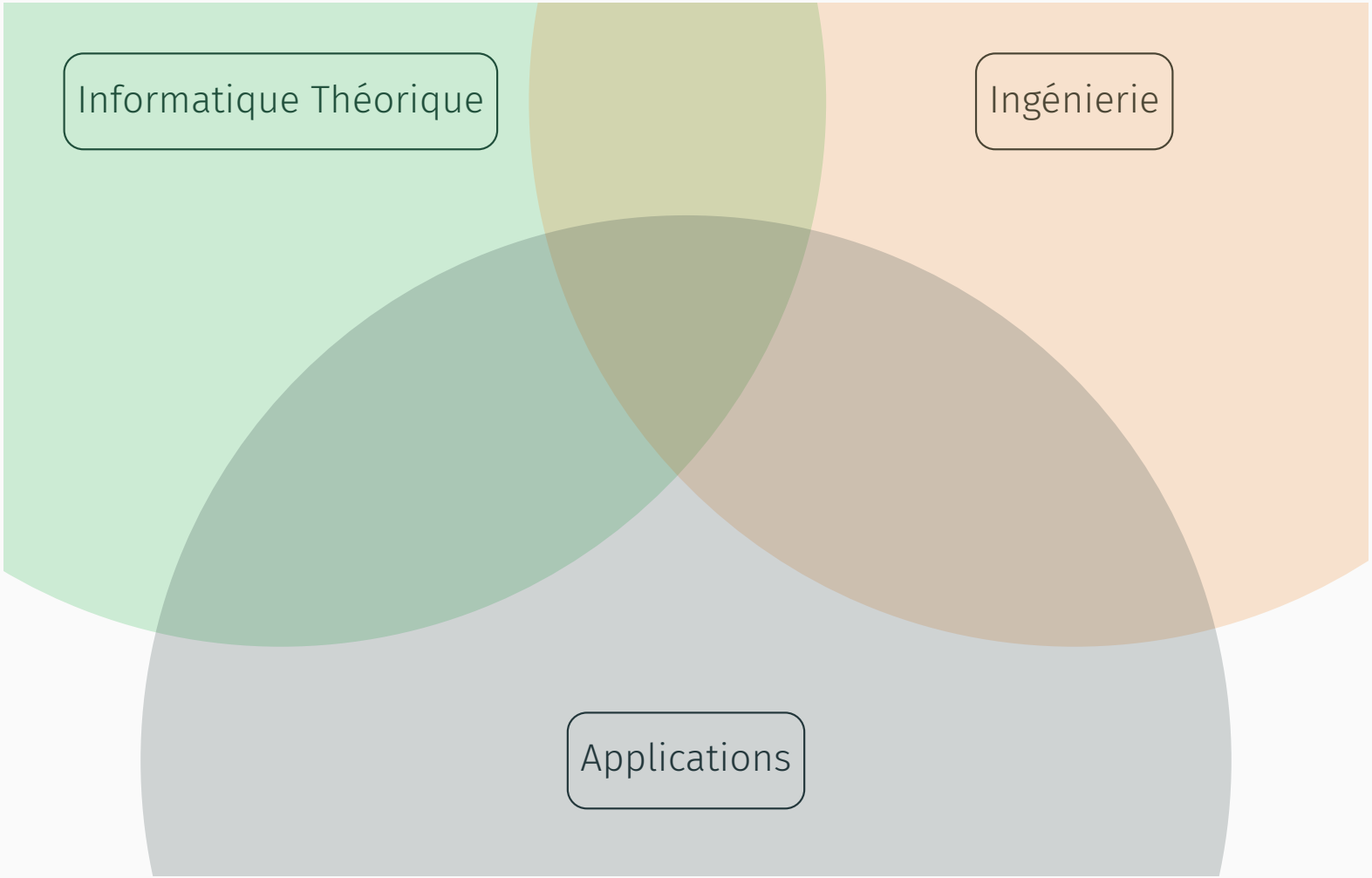


Figure 1 – « Je ne cherche pas à connaitre les réponses, je cherche à comprendre les questions » — Confucius

La recherche en informatique

La position du LSV

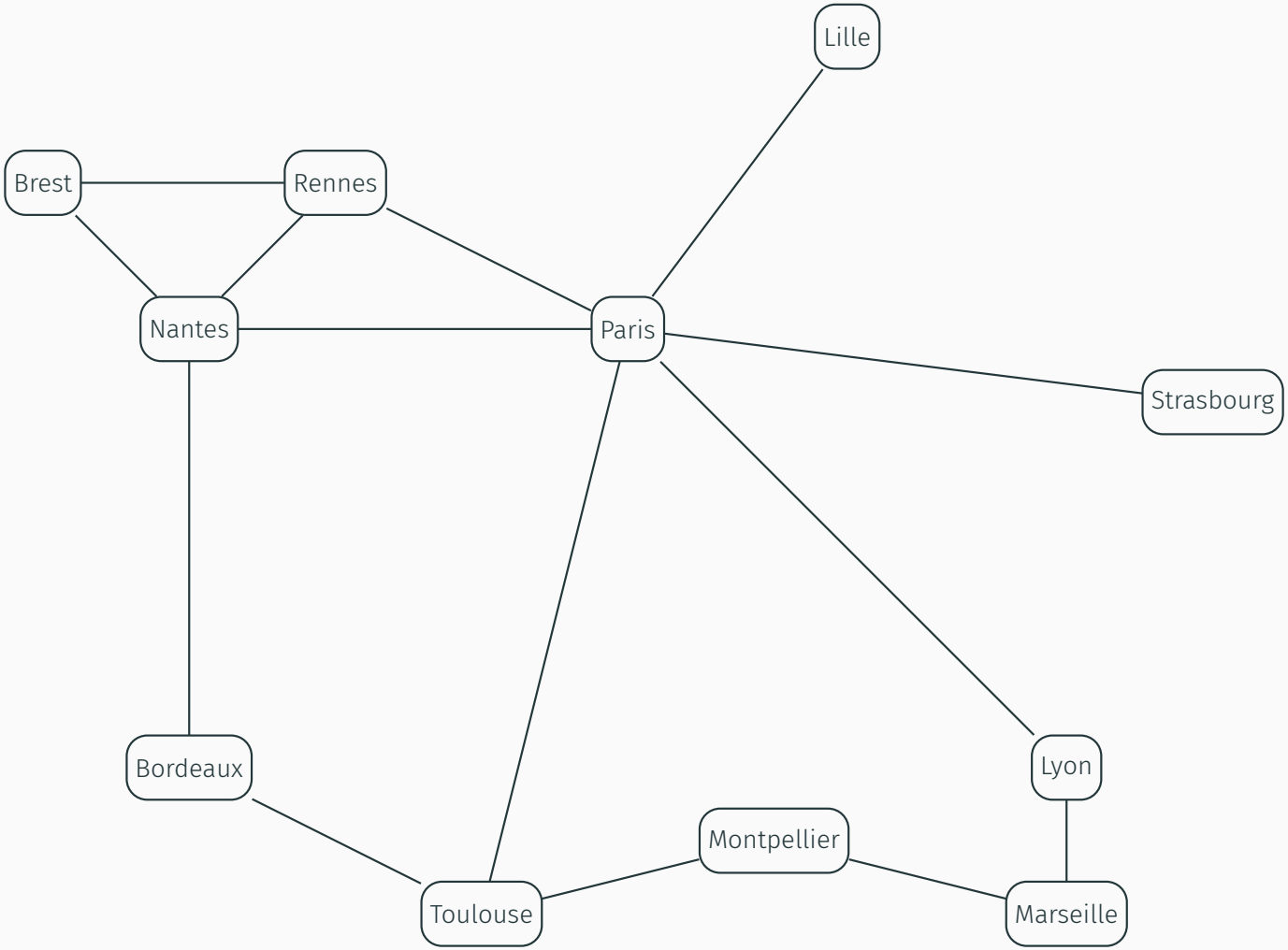
Les intérêts du LSV

1. Vérification
2. Logique
3. Cryptosystèmes
4. Algorithmique

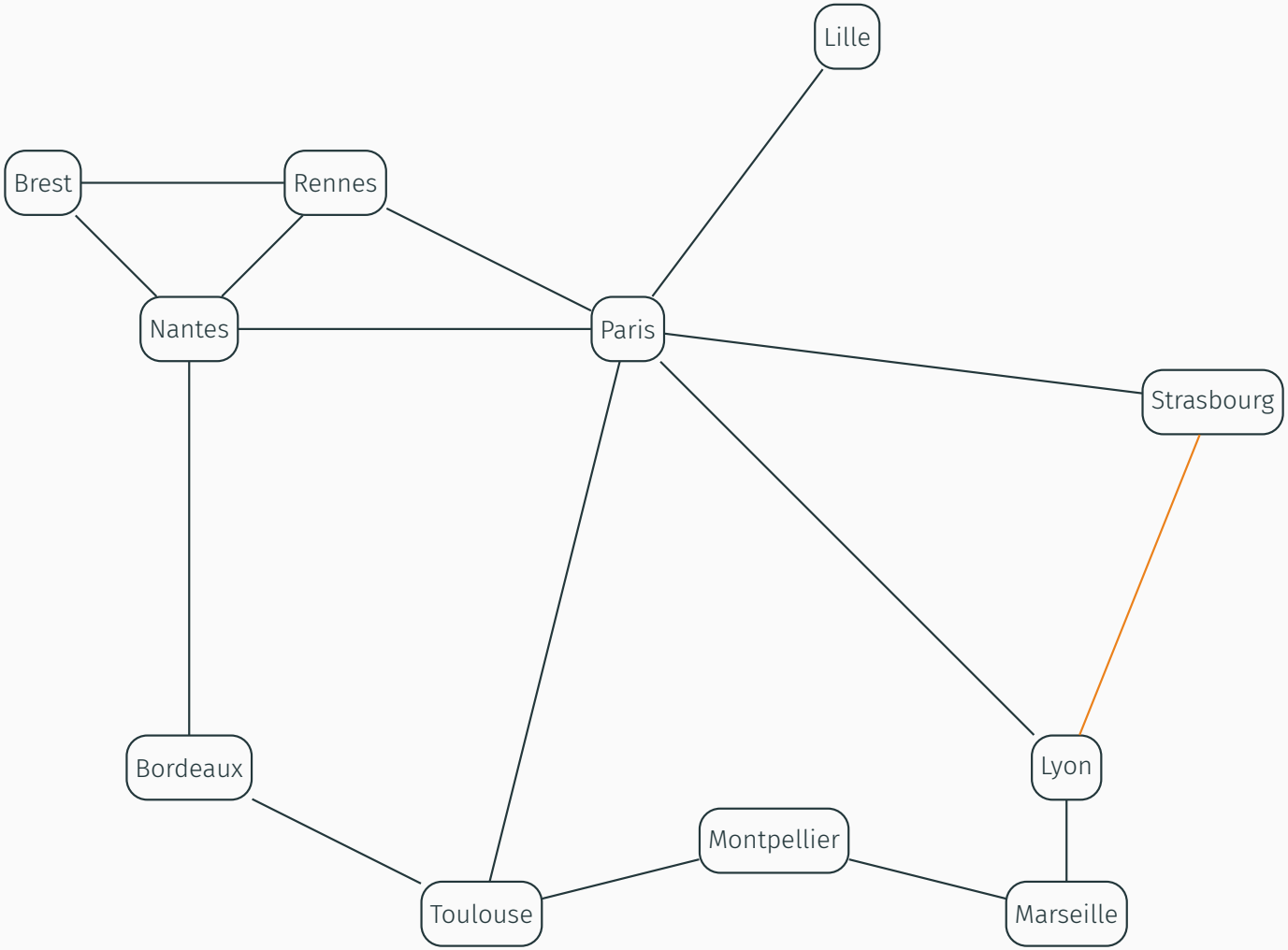
Le chemin hamiltonien

Formalisation du problème

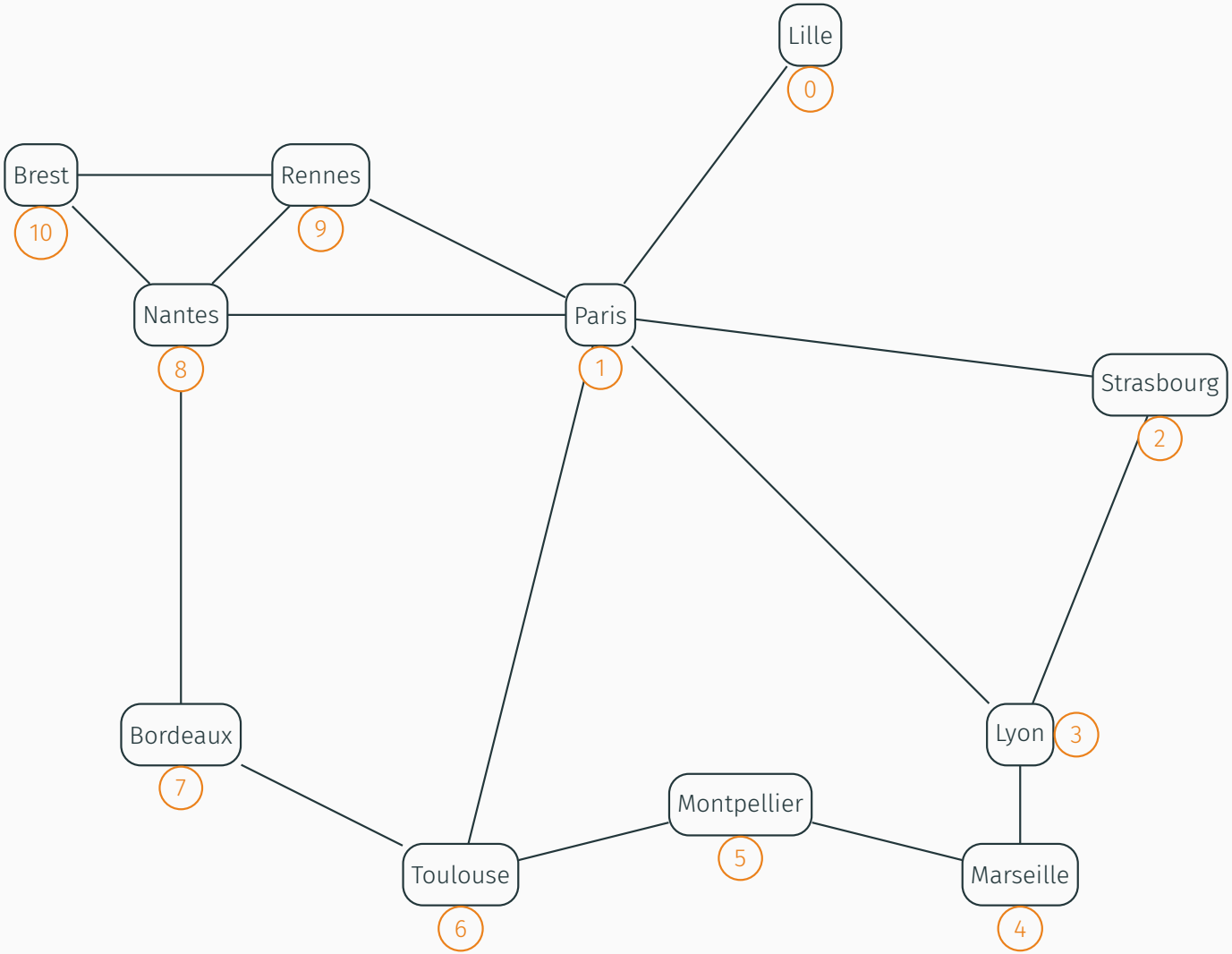
Un chemin passant une unique fois par chaque ville ?



Un chemin passant une unique fois par chaque ville ?



Un chemin passant une unique fois par chaque ville ?



Où est Al-Khwârizmî ?

Description du problème

Entrée Un graphe G de taille n

Sortie Un chemin hamiltonien $x_1, \ldots, x_n$

Où est Al-Khwârizmî ?

Description du problème

Entrée Un graphe G de taille n

Sortie Un chemin hamiltonien $x_1, \ldots, x_n$

Une variante de décision

Entrée Un graphe G de taille n

Sortie Est-ce qu'il existe un chemin hamiltonien ?

Où est Al-Khwârizmî ?

Description du problème

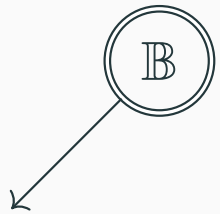
Entrée Un graphe G de taille n

Sortie Un chemin hamiltonien $x_1, \ldots, x_n$

Une variante de décision

Entrée Un graphe G de taille n

Sortie Est-ce qu'il existe un chemin hamiltonien ?



Où est Al-Khwârizmî ?

Un problème plus facile

Entrée Un graphe G de taille n, un chemin $x_1, \ldots, x_n$

Sortie Est-ce que le chemin est hamiltonien ?

Où est Al-Khwârizmî ?

Un problème plus facile

Entrée Un gra emin $x_1, \ldots, x_n$

Sortie Est-ce c iltonien ?

Les formules SAT

Formalisation du problème

Menteurs et diseurs de vérité

Description informelle

Amy dit « Bob est un menteur », Bob dit « Cal est un menteur » et Cal dit « Amy et Bob sont des menteurs ». Est-ce possible ?

Description formelle

$$A \iff \neg B$$

$$B \iff \neg C$$

$$C \iff \neg A \wedge \neg B$$

Menteurs et diseurs de vérité

Mise en CNF

$$\{\neg A \vee \neg B; B \vee A; \neg B \vee \neg C; C \vee B; \neg C \vee \neg A; \neg C \vee \neg B; A \vee B \vee C\}$$

Le problème associé

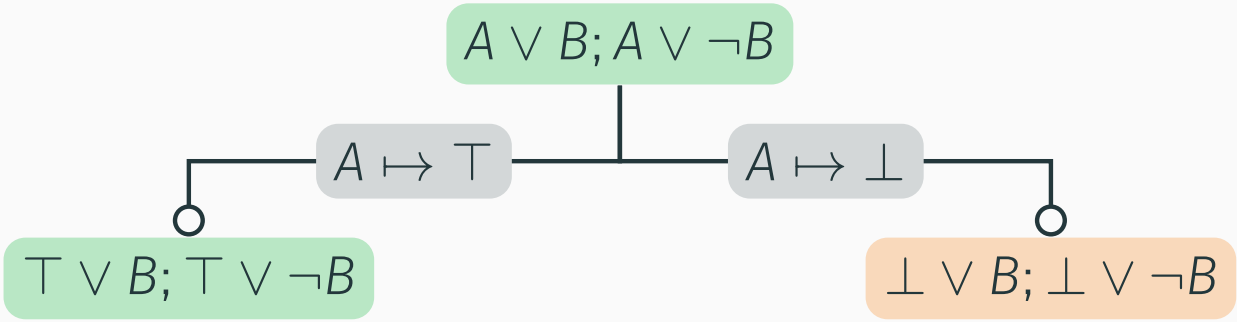
Entrée Une formule ϕ en CNF

Sortie Est-ce que la formule est satisfiable ?

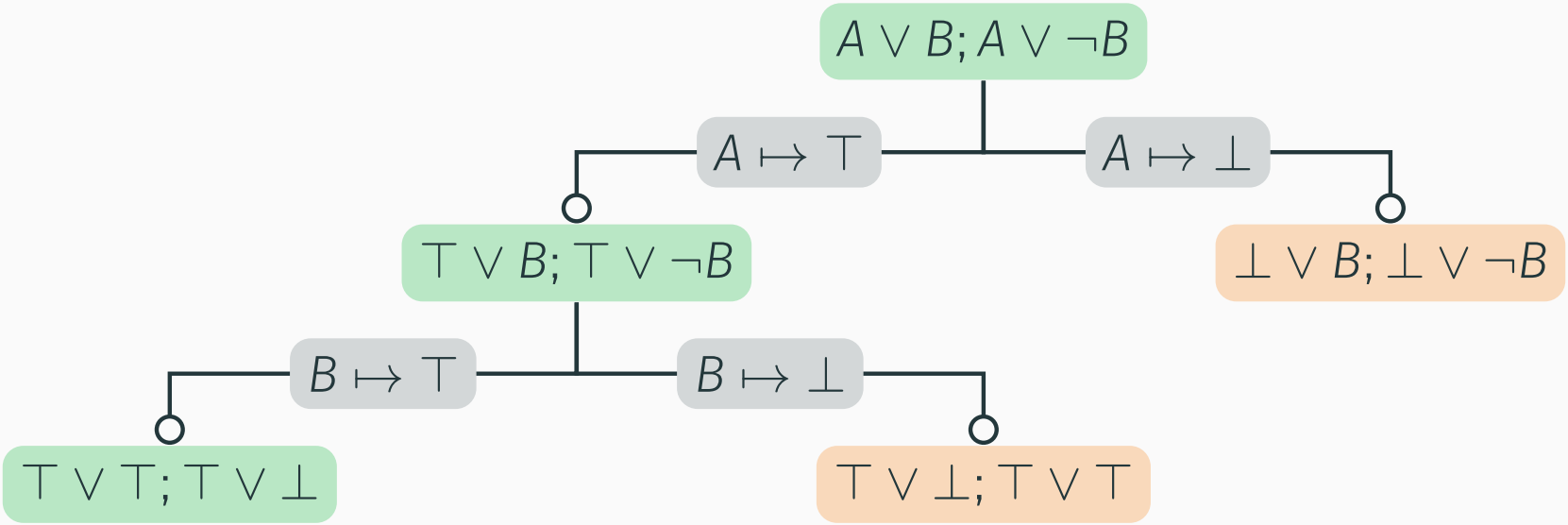
Auto-réduction

$A \vee B; A \vee \neg B$

Auto-réduction



Auto-réduction

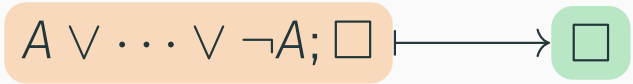


Les formules SAT

L'algorithme DPLL

L'algorithme de Davis–Putnam–Logemann–Loveland

(i) Élimination des tautologies



Un système de réécriture

L'algorithme de Davis–Putnam–Logemann–Loveland

(i) Élimination des tautologies

$$A \vee \cdots \vee \neg A; \square \longmapsto \square$$

(ii) Propagation des littéraux

$$A; \square \longmapsto \square[A/\top]$$

Un système de réécriture

L'algorithme de Davis–Putnam–Logemann–Loveland

(i) Élimination des tautologies

$$A \vee \cdots \vee \neg A; \square \longmapsto \square$$

(ii) Propagation des littéraux

$$A; \square \longmapsto \square[A/\top]$$

(iii) Détection des littéraux purs

$$A \vee \square; A \vee \circ; \cdots \longmapsto \square; \circ; \cdots$$

Un système de réécriture

L'algorithme de Davis–Putnam–Logemann–Loveland

(i) Élimination des tautologies

$$A \vee \cdots \vee \neg A; \square \longmapsto \square$$

(ii) Propagation des littéraux

$$A; \square \longmapsto \square[A/\top]$$

(iii) Détection des littéraux purs

$$A \vee \square; A \vee \circ; \cdots \longmapsto \square; \circ; \cdots$$

(iv) Splitting

$$A \vee \circ; \square \mapsto \square[A/\top] \quad A \vee \circ; \square \mapsto \square[A/\bot]$$

En pratique...

Exercice
Montrer la correction de l'algorithme. Quelle est sa complexité ?

En pratique...

Exercice
Montrer la correction de l'algorithme. Quelle est sa complexité ?

Améliorations
Le fabuleux... MiniSat.

> *MiniSat is a minimalistic, open-source SAT solver, developed to help researchers and developers alike to get started on SAT.*

Les formules SAT

NP-complétude

Une vision haut niveau

Une classe de problèmes

Notons NP la classe des problèmes où la vérification se fait en temps polynomial

Exemples

(i) Le problème de décision SAT

(ii) Le problème de décision HamPath

Un résultat théorique

Théorème (Cook, 1971)
Tout problème dans NP se réduit à SAT

Retour sur le chemin hamiltonien

Encodage dans SAT

Le salaire du solveur

Choix des variables

$$x_{u,t} \triangleq \text{ au temps } t \text{ le chemin passe par le sommet } u \qquad (1)$$

Contraintes

1. Le chemin passe par tous les sommets
2. Chaque sommet apparaît une unique fois
3. Le chemin respecte le graphe

Le salaire du solveur

Le chemin passe par tous les sommets

$$\forall u.\exists t. \quad x_{t,u} \tag{2}$$

Chaque sommet apparaît une unique fois

$$\forall u.\neg\left(\exists t_1 \neq t_2. \quad x_{t_1,u} \wedge x_{t_2,u}\right) \tag{3}$$

Le chemin respecte le graphe

$$\forall u.\forall v.\forall t. \quad x_{u,t} \wedge x_{v,t+1} \implies (u,v) \in G \tag{4}$$

Retour sur le chemin hamiltonien

Démonstration

Sortez les ordinateurs !

Une approche de l'informatique

Théorie et pratique

L'informatique théorique

1. Avoir une vision très mathématique (spécifications)
2. Coder peu, coder juste (réécriture)
3. Ne pas avoir peur de la complexité (algorithmes naïfs)
4. Étudier les relations entre les problèmes (classes de complexité)
5. Entrer dans un monde plus abstrait (auto-réduction)

Cook, S. A. (1971). The complexity of theorem-proving procedures. In *Proceedings of the Third Annual ACM Symposium on Theory of Computing*, STOC '71, pages 151–158, New York, NY, USA. ACM.