

Calculabilité Distribuée et Topologie Discrète

E. Godard & D. Imbs

LIF – Université Aix-Marseille

Visite ENS Paris-Saclay



Plan de la Séance

- 1 Calculabilité Distribuée
- 2 Prix Gödel 2004
- 3 Topologie Discrète

Problème des Deux Généraux

(J. Gray, 1978)

Deux généraux avec leurs armées sur deux côtés de la vallée, l'ennemi est au milieu.

Les deux généraux doivent décider s'ils attaquent, chacun ayant son propre avis sur la question.

- Ils doivent attaquer simultanément pour vaincre
- Ils communiquent en envoyant des messagers toutes les heures
- Les messagers peuvent être capturés

Comment peuvent-ils se mettre d'accord ?

En termes modernes

Il s'agit du problème du **Consensus** pour **deux** processus communiquant en rondes **synchrones** par **messages**, avec **pertes**.

Application fondamentale pour les bases de bases de données répliquées

Problème du Consensus

Chaque processus *propose* une valeur (dite initiale).
Décider : On dit qu'un processus *décide* lorsqu'une valeur **finale** pour le calcul est donnée par celui-ci.

Consensus

Étant donnés des processus avec chacun une valeur initiale.

Accord Tous les processus décident la même valeur.

Validité La valeur décidée est une des valeurs initiales.

Terminaison Tous les processus décident.

Algorithme Naïf

Algorithme Naïf

- 1 Le général le plus âgé envoie sa décision
mais si le messenger est capturé ?

Algorithme Naïf

- 1 Le général le plus âgé envoie sa décision
mais si le messenger est capturé ?
- 2 Le général le plus âgé envoie un autre messenger
Le général le moins âgé envoie un accusé de réception
mais si ce messenger est capturé ?

Algorithme Naïf

- 1 Le général le plus âgé envoie sa décision
mais si le messenger est capturé ?
- 2 Le général le plus âgé envoie un autre messenger
Le général le moins âgé envoie un accusé de réception
mais si ce messenger est capturé ?
- 3 On envoie un accusé de réception de l'accusé de réception
mais ...

Scénarios

Scénarios

- 1 Tous les messages sont perdus

Scénarios

- 1 Tous les messages sont perdus
- 2 Tous les messages sont perdus sauf un

Scénarios

- 1 Tous les messages sont perdus
- 2 Tous les messages sont perdus sauf un
- 3 Une des deux armées perd tous ses messages à partir d'un certain moment

Scénarios

- 1 Tous les messages sont perdus
- 2 Tous les messages sont perdus sauf un
- 3 Une des deux armées perd tous ses messages à partir d'un certain moment
- 4 ...

Scénarios

- 1 Tous les messages sont perdus
- 2 Tous les messages sont perdus sauf un
- 3 Une des deux armées perd tous ses messages à partir d'un certain moment
- 4 ...
- 5 Au moins un message, par heure, parvient à destination

Scénarios

- 1 Tous les messages sont perdus
- 2 Tous les messages sont perdus sauf un
- 3 Une des deux armées perd tous ses messages à partir d'un certain moment
- 4 ...
- 5 Au moins un message, par heure, parvient à destination
- 6 ...

Scénarios

- 1 Tous les messages sont perdus
- 2 Tous les messages sont perdus sauf un
- 3 Une des deux armées perd tous ses messages à partir d'un certain moment
- 4 ...
- 5 Au moins un message, par heure, parvient à destination
- 6 ...
- 7 Tous les messages d'une des armées parviennent à destination

Scénarios

- 1 Tous les messages sont perdus
- 2 Tous les messages sont perdus sauf un
- 3 Une des deux armées perd tous ses messages à partir d'un certain moment
- 4 ...
- 5 Au moins un message, par heure, parvient à destination
- 6 ...
- 7 Tous les messages d'une des armées parviennent à destination
- 8 Au plus un message est perdu

Scénarios

- 1 Tous les messages sont perdus
- 2 Tous les messages sont perdus sauf un
- 3 Une des deux armées perd tous ses messages à partir d'un certain moment
- 4 ...
- 5 Au moins un message, par heure, parvient à destination
- 6 ...
- 7 Tous les messages d'une des armées parviennent à destination
- 8 Au plus un message est perdu
- 9 Tous les messages parviennent à destination

Une Question Simple

Pour quels scénarios parvient-on toujours à résoudre le problème ?

Une Réponse Simple ?



Un Scénario Spécial

Initialement:

- Général ○: ok
- Général ●: ko

Au moins un message, par heure, parvient à destination.

ok, non reçu

ko, reçu



ko, reçu

ok, reçu



ok, reçu

ko, non reçu

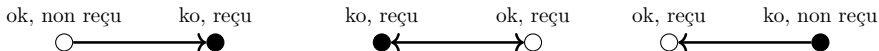


Un Scénario Spécial

Initialement:

- Général ○: ok
- Général ●: ko

Au moins un message, par heure, parvient à destination.



On peut fusionner



Un Scénario Spécial

Au moins un message, par heure, parvient à destination.

Un Scénario Spécial

Au moins un message, par heure, parvient à destination.

① Première heure:



Celui qui n'a rien reçu **doit** choisir sa propre entrée ou **attendre!**

Un Scénario Spécial

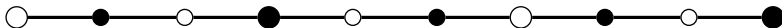
Au moins un message, par heure, parvient à destination.

1 Première heure:



Celui qui n'a rien reçu **doit** choisir sa propre entrée
ou **attendre!**

2 Deuxième heure:



Un Scénario Spécial

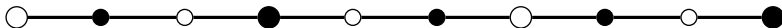
Au moins un message, par heure, parvient à destination.

1 Première heure:



Celui qui n'a rien reçu **doit** choisir sa propre entrée
ou **attendre!**

2 Deuxième heure:



3 ...

Zoo des Modèles Distribués

Il existe de très nombreux systèmes distribués réels:

Internet messages

CPU multicoeur mémoire partagée

De plus, ces modèles de calcul ont des **défaillances**

- crashes
- pertes de messages

Vers une *modélisation universelle* ?

Consensus Généralisé

Accord Ensembliste

Étant donné $n + 1$ processus avec chacun une valeur initiale

Accord Tous les processus décident au plus n valeurs différentes.

Validité Toutes les valeurs décidées sont des valeurs initiales

Terminaison Tous les processus décident.

Calculabilité Distribuée et Prix Gödel

Théorème d'Impossibilité [HS99,SZ00]

Le problème de l'accord ensembliste n'admet pas de solution dans certains modèles fondamentaux (mémoire partagée, passage de messages avec défaillances)

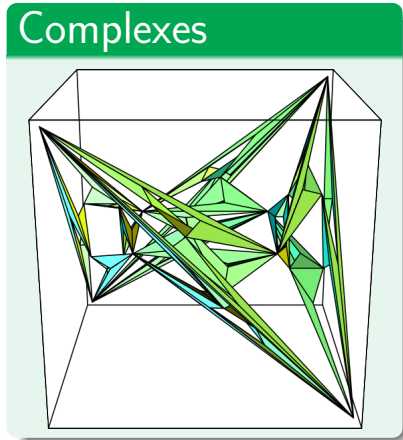
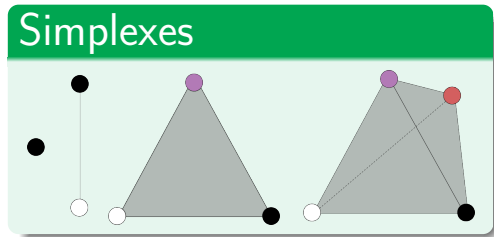
Le prix Gödel 2004 récompense pour ce résultat

- Herlihy et Shavit
- Saks et Zaharoglou

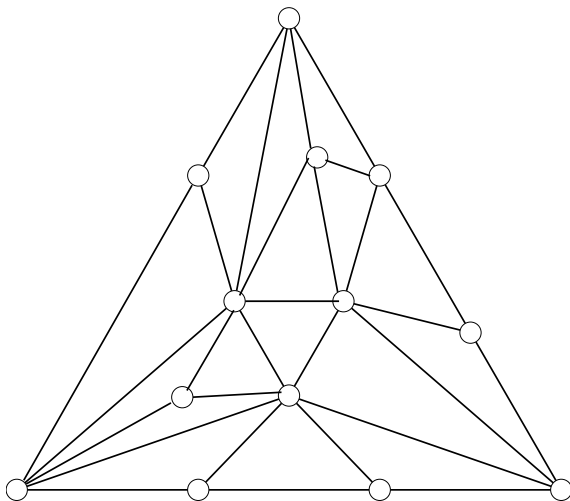
Application de Techniques Topologiques

- HS 1999 Théorème général de calculabilité distribuée
- SZ 2000 Limité à l'accord ensembliste par *simple* application du Lemme de Sperner (1930)

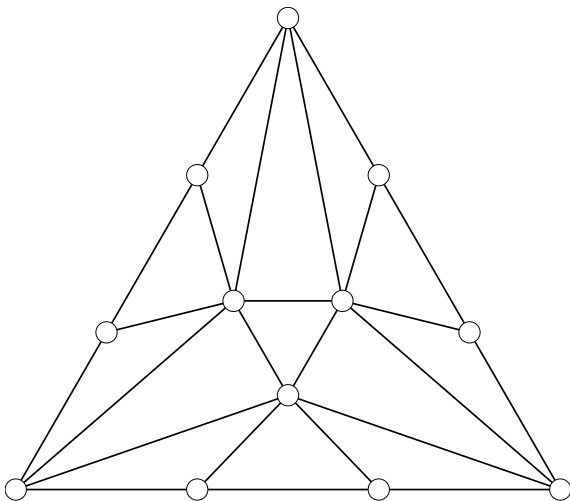
Préliminaires



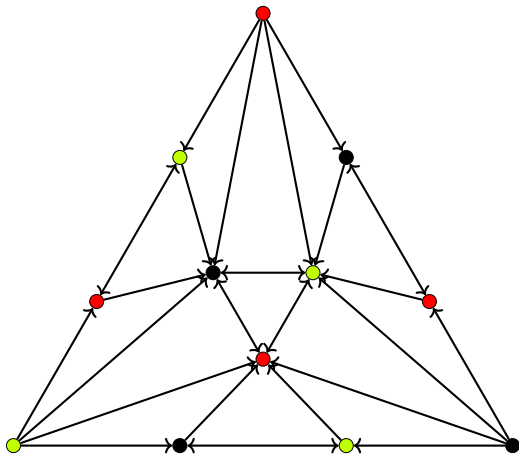
Subdivision (Triangulation)



Non-Déterminisme et Subdivision

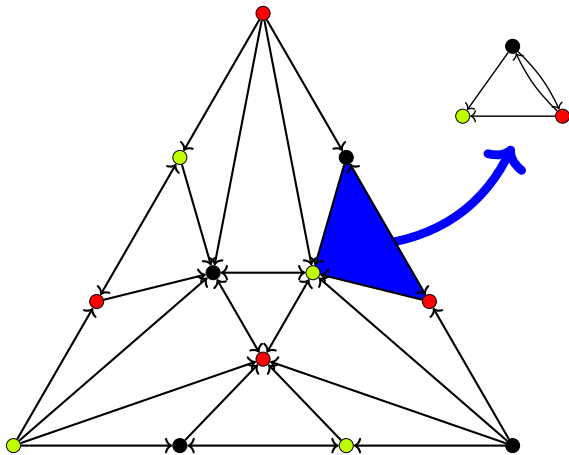


Non-Déterminisme et Subdivision



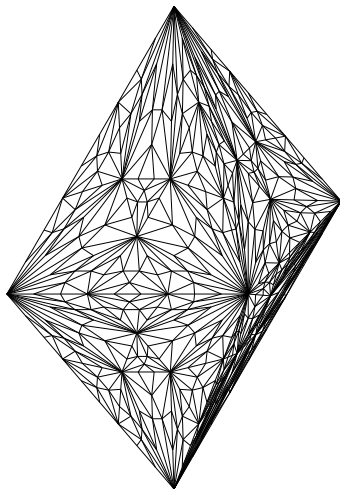
- chaque sommet correspond à l'état local d'un processus obtenu pour certaines exécutions

Non-Déterminisme et Subdivision



- chaque sommet correspond à l'état local d'un processus obtenu pour certaines exécutions

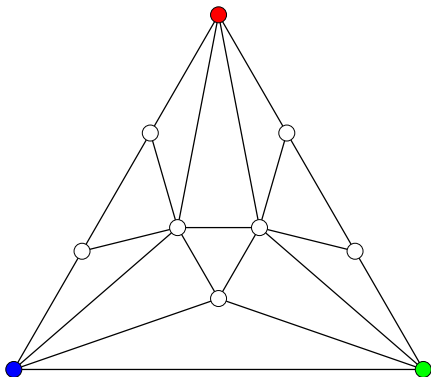
Non-Déterminisme et Subdivision



Un Jeu de Coloriage

Colorier la triangulation

- en utilisant les mêmes couleurs qu'aux coins sur chaque face
- sans créer de triangle avec **3 couleurs**.



Lemme de Sperner (1930)

Coloration de Sperner

On doit choisir une couleur pour chaque sommet

- tous les coins ont une couleur différente
- les sommets d'une face externe doivent avoir la même couleur qu'un des coins de la face

Lemme de Sperner (1930)

Coloration de Sperner

On doit choisir une couleur pour chaque sommet

- tous les coins ont une couleur différente
- les sommets d'une face externe doivent avoir la même couleur qu'un des coins de la face

Lemme de Sperner

Toute coloration de Sperner d'une subdivision simpliciale de dimension n contient au moins un simplexe à $n + 1$ couleurs.

Preuve

Propriété : Le nombre de simplexe panchromatique est **impair**.

La preuve est *par récurrence* sur la dimension.

Preuve

Propriété : Le nombre de simplexe panchromatique est **impair**.

La preuve est *par récurrence* sur la dimension.

Cas de base dimension 1, avec 2 couleurs

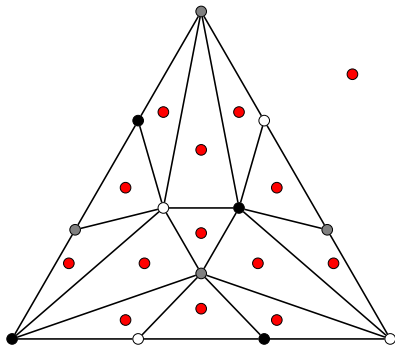


Nombre *impair* de passages de blanc à noir

Induction: $n + 1$ couleurs

On construit un graphe G :

- Un sommet par région (intérieures + extérieure)

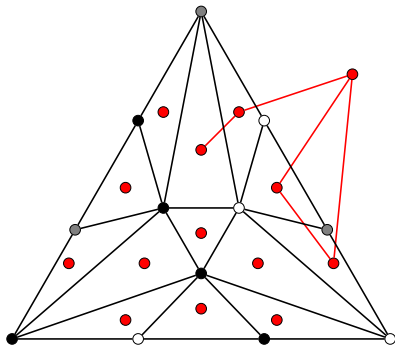


Induction: $n + 1$ couleurs

On construit un graphe G :

- Un sommet par région (intérieures + extérieure)
- Une arête si deux régions partagent une face

$\{1, \dots, n\}$

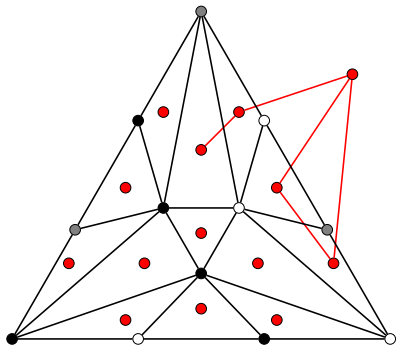


Induction ...

On construit un graphe G :

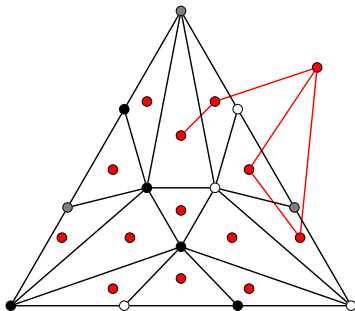
- Un sommet par région (intérieures + extérieure)
- Une arête si deux régions partagent une face

$\{1, \dots, n\}$



- Degré de la région extérieure: impair
- Degré d'une région intérieure: 0, 1 ou 2

Induction ...



- Degré de la région extérieure: impair
- Degré d'une région intérieure: 0, 1 ou 2
- Degré 1 \Rightarrow simplexe panchromatique
- Nb pair de sommets de degré impair \Rightarrow nb impair de simplexes panchromatiques

Conclusion

- **Algorithmique Distribuée** : informatique fondamentale influencée par la pratique
- Des questions de **calculabilité distribuée**
- Une modélisation correspondant exactement à un théorème de topologie discrète de 1930
- Encore de nombreuses questions ouvertes ...

Dans l'équipe DALGO

De nombreux résultats de calculabilité distribuée

- Réseaux dynamiques
- Consensus pour les Réseaux Homogènes : OK
 - Accord ensembliste pour les Réseaux Homogènes à défaillances : OK
 - Accord ensembliste pour les Réseaux Homogènes : *ouvert*

Equivalence de modèles mémoire partagée, adversaires à message, diffusion, réseaux dynamiques

Réseaux Anonymes / Agents Mobiles

- techniques à base de revêtements topologiques