Audition LIRMM
Sujet : Etude des graphes sans entrelacs

Boris Albar

6 Juin 2011

Stage (Recherche) :

Secrets répartis et matroïdes

Secret Répartis

Problème : Comment partager un secret $\mathcal{S}$ entre un ensemble $\mathcal{P}$ de participants de manière à ce que seul certains sous-ensembles de participants soient autorisés de reconstruire le secret et ce de manière sécurisé, c'est-à-dire que tout sous-ensemble non-autorisé n'obtient aucune information sur le secret.

- L'ensemble des sous-ensembles de participants ayant le droit de reconstuire le secret est appelé la **structure d'accès**.
- On se donne un participant spécial, le "dealer" possédant le secret et chargé de distribuer les clés aux participants.

Secret Répartis

Problème : Comment partager un secret $\mathcal{S}$ entre un ensemble $\mathcal{P}$ de participants de manière à ce que seul certains sous-ensembles de participants soient autorisés de reconstruire le secret et ce de manière sécurisé, c'est-à-dire que tout sous-ensemble non-autorisé n'obtient aucune information sur le secret.

- L'ensemble des sous-ensembles de participants ayant le droit de reconstuire le secret est appelé la **structure d'accès**.
- On se donne un participant spécial, le "dealer" possédant le secret et chargé de distribuer les clés aux participants.

Secret Répartis

Problème : Comment partager un secret $\mathcal{S}$ entre un ensemble $\mathcal{P}$ de participants de manière à ce que seul certains sous-ensembles de participants soient autorisés de reconstruire le secret et ce de manière sécurisé, c'est-à-dire que tout sous-ensemble non-autorisé n'obtient aucune information sur le secret.

- L'ensemble des sous-ensembles de participants ayant le droit de reconstuire le secret est appelé la **structure d'accès**.
- On se donne un participant spécial, le "dealer" possédant le secret et chargé de distribuer les clés aux participants.

Comment mesurer l'efficacité d'un secret répartis ?

Rapport entre la taille de la plus grande clé et la taille du secret :

Théorème (Csirmaz)

La taille des clés est au moins égale à la taille du secret.

Définition

Étant donné une structure d'accès, si il existe un schémas de partage tel que la taille de la plus grande clé soit égale à la taille du secret alors la structure d'accès est dite **idéale**.

Comment mesurer l'efficacité d'un secret répartis ?

Rapport entre la taille de la plus grande clé et la taille du secret :

Théorème (Csirmaz)

La taille des clés est au moins égale à la taille du secret.

Définition

Étant donné une structure d'accès, si il existe un schémas de partage tel que la taille de la plus grande clé soit égale à la taille du secret alors la structure d'accès est dite **idéale**.

Comment mesurer l'efficacité d'un secret répartis ?

Rapport entre la taille de la plus grande clé et la taille du secret :

Théorème (Csirmaz)

La taille des clés est au moins égale à la taille du secret.

Définition

Étant donné une structure d'accès, si il existe un schémas de partage tel que la taille de la plus grande clé soit égale à la taille du secret alors la structure d'accès est dite **idéale**.

Point de vue de la théorie de l'information

On associe une variable aléatoire au secret et une variable aléatoire pour chacune des clés des participant. On considère ensuite l'entropie de Shannon $H(i)$ associé à ces variables aléatoires.

Mesures d'efficacité :

- Taux d'information : $\rho = \frac{H(S)}{\max\limits_{i \in \mathcal{P}} H(i)}$.
- Taux d'information moyen : $\rho^* = \frac{|\mathcal{P}| H(S)}{\sum\limits_{i \in \mathcal{P}} H(i)}$.

Théorème

Si une structure d'accès Γ est idéale alors $\rho(\Gamma) = 1$.

Point de vue de la théorie de l'information

On associe une variable aléatoire au secret et une variable aléatoire pour chacune des clés des participant. On considère ensuite l'entropie de Shannon $H(i)$ associé à ces variables aléatoires.

Mesures d'efficacité :

- Taux d'information : $\rho = \frac{H(S)}{\max\limits_{i \in \mathcal{P}} H(i)}$.
- Taux d'information moyen : $\rho^* = \frac{|\mathcal{P}| H(S)}{\sum\limits_{i \in \mathcal{P}} H(i)}$.

Théorème

Si une structure d'accès Γ est idéale alors $\rho(\Gamma) = 1$.

Point de vue de la théorie de l'information

On associe une variable aléatoire au secret et une variable aléatoire pour chacune des clés des participant. On considère ensuite l'entropie de Shannon $H(i)$ associé à ces variables aléatoires.

Mesures d'efficacité :

- Taux d'information : $\rho = \frac{H(S)}{\max\limits_{i \in \mathcal{P}} H(i)}$.
- Taux d'information moyen : $\rho^* = \frac{|\mathcal{P}| H(S)}{\sum\limits_{i \in \mathcal{P}} H(i)}$.

Théorème

Si une structure d'accès Γ *est idéale alors* $\rho(\Gamma) = 1$.

Matroïdes

Définition

Un matroïde est un couple $(E, \mathcal{I})$ où E est un ensemble fini et $\mathcal{I}$ un ensemble de parties de E vérifiant :

- $\emptyset \in \mathcal{I}$
- *Si* $I_1 \in \mathcal{I}$ *et* $I_2 \subset I_1$ *alors* $I_2 \in \mathcal{I}$.
- *Si* $I_1, I_2 \in \mathcal{I}$ *et* $|I_1| < |I_2|$ *alors* $\exists e \in I_2 \backslash I_1$ *tel que* $I_1 \cup e \in \mathcal{I}$

Circuits = dépendants minimaux

Matroïdes

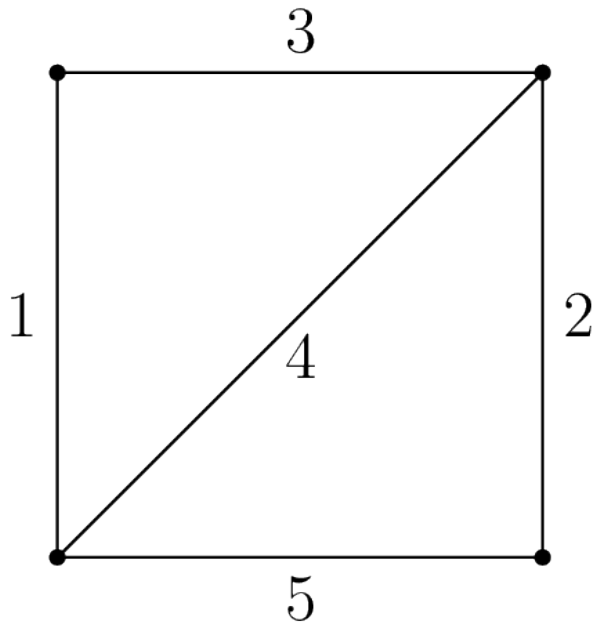
Définition

Un matroïde est un couple $(E, \mathcal{I})$ où E est un ensemble fini et $\mathcal{I}$ un ensemble de parties de E vérifiant :

- $\emptyset \in \mathcal{I}$
- *Si* $I_1 \in \mathcal{I}$ *et* $I_2 \subset I_1$ *alors* $I_2 \in \mathcal{I}$.
- *Si* $I_1, I_2 \in \mathcal{I}$ *et* $|I_1| < |I_2|$ *alors* $\exists e \in I_2 \backslash I_1$ *tel que* $I_1 \cup e \in \mathcal{I}$

Circuits = dépendants minimaux

Matroïdes



Circuits $= \{1, 3, 4\}, \{1, 3, 2, 5\}, \{2, 4, 5\}.$

Matroïdes

A un matroïde $\mathcal{M} = (\mathcal{P} \cup \{d\}, C)$ où C est l'ensemble des circuits du matroîde, on peut associer une structure d'accès où d est le dealer. On considère pour cela :

$$\Gamma = \{\mathcal{A} \,|\exists C_0 \in C \text{ tel que } C_0 \cup \{d\} \subseteq \mathcal{A}\}\,.$$

Théorème (Brickell et Davenport (1990))

Si Γ est une structure d'accès idéale alors elle est induite par un matroïde.

Exemple : La structure d'accès (minimale) $\Gamma = \{\{3,4\},\{3,2,5\}$ est idéale et le matroïde associé correspond au matroïde donné par le graphe précédent (et où le dealer est l'élément 1).

Matroïdes

A un matroïde $\mathcal{M} = (\mathcal{P} \cup \{d\}, C)$ où C est l'ensemble des circuits du matroîde, on peut associer une structure d'accès où d est le dealer. On considère pour cela :

$$\Gamma = \{\mathcal{A} \,|\exists C_0 \in C \text{ tel que } C_0 \cup \{d\} \subseteq \mathcal{A}\}\,.$$

Théorème (Brickell et Davenport (1990))

Si Γ est une structure d'accès idéale alors elle est induite par un matroïde.

Exemple : La structure d'accès (minimale) $\Gamma = \{\{3,4\},\{3,2,5\}$ est idéale et le matroïde associé correspond au matroïde donné par le graphe précédent (et où le dealer est l'élément 1).

Matroïdes

A un matroïde $\mathcal{M} = (\mathcal{P} \cup \{d\}, C)$ où C est l'ensemble des circuits du matroîde, on peut associer une structure d'accès où d est le dealer. On considère pour cela :

$$\Gamma = \{\mathcal{A} \,|\exists C_0 \in C \text{ tel que } C_0 \cup \{d\} \subseteq \mathcal{A}\}\,.$$

Théorème (Brickell et Davenport (1990))

Si Γ est une structure d'accès idéale alors elle est induite par un matroïde.

Exemple : La structure d'accès (minimale) $\Gamma = \{\{3,4\},\{3,2,5\}$ est idéale et le matroïde associé correspond au matroïde donné par le graphe précédent (et où le dealer est l'élément 1).

Matroïdes

Problème de la réciprocité : Tous les matroïdes induisent-ils des structures d'accès idéales ?

Réponse : Non !

Théorème (Seymour (1990))

Les structures d'accès induites par le matroïde de Vámos ne sont pas idéales.

Théorème (Beimel, Livne, Padro (2008))

Les structures d'accès induites par le matroïde de Vámos ne sont pas presque idéale.

Matroïdes

Problème de la réciprocité : Tous les matroïdes induisent-ils des structures d'accès idéales ?
Réponse : Non !

Théorème (Seymour (1990))

Les structures d'accès induites par le matroïde de Vámos ne sont pas idéales.

Théorème (Beimel, Livne, Padro (2008))

Les structures d'accès induites par le matroïde de Vámos ne sont pas presque idéale.

Matroïdes

Problème de la réciprocité : Tous les matroïdes induisent-ils des structures d'accès idéales ?
Réponse : Non !

Théorème (Seymour (1990))

Les structures d'accès induites par le matroïde de Vámos ne sont pas idéales.

Théorème (Beimel, Livne, Padro (2008))

Les structures d'accès induites par le matroïde de Vámos ne sont pas presque idéale.

Matroïdes

Problème de la réciprocité : Tous les matroïdes induisent-ils des structures d'accès idéales ?
Réponse : Non !

Théorème (Seymour (1990))

Les structures d'accès induites par le matroïde de Vámos ne sont pas idéales.

Théorème (Beimel, Livne, Padro (2008))

Les structures d'accès induites par le matroïde de Vámos ne sont pas presque idéale.

Matroïdes (2)

Néanmoins la réciproque est vraie pour certaines classes de matroïdes :

Théorème (Brickell et Davenport, 1990)

Tous les matroïdes représentables sur un corps fini induisent des structures d'accès idéales.

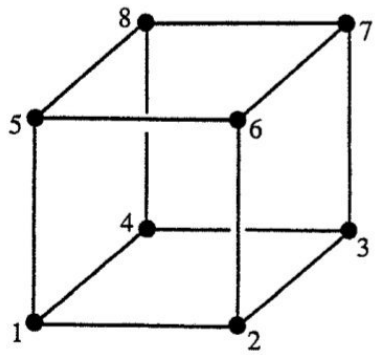
Résultats

Question : Comment construire des matroïdes non iss-représentable et non presque iss-représentable ?

Une première réponse : Considérer des relaxation de certains circuits-hyperplans d'un matroïde représentable.

Résultat

La famille de matroïdes $AG(3,2)'$, F_8 et Q_8 obenu en relaxant (resp.) 1, 2 et 3 circuits-hyperplans de la géométrie affine $AG(3,2)$ est non presque idéale.

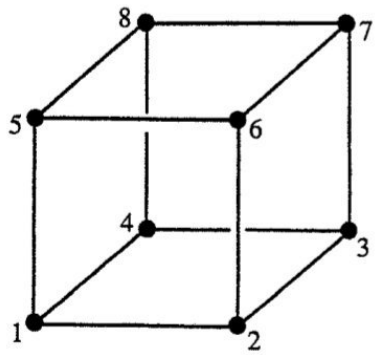


Résultats

Question : Comment construire des matroïdes non iss-représentable et non presque iss-représentable ?
Une première réponse : Considérer des relaxation de certains circuits-hyperplans d'un matroïde représentable.

Résultat

La famille de matroïdes $AG(3,2)'$, F_8 et Q_8 obenu en relaxant (resp.) 1, 2 et 3 circuits-hyperplans de la géométrie affine $AG(3,2)$ est non presque idéale.

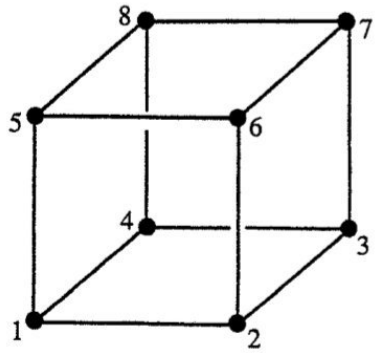


Résultats

Question : Comment construire des matroïdes non iss-représentable et non presque iss-représentable ?
Une première réponse : Considérer des relaxation de certains circuits-hyperplans d'un matroïde représentable.

Résultat

La famille de matroïdes $AG(3,2)'$, F_8 et Q_8 obenu en relaxant (resp.) 1, 2 et 3 circuits-hyperplans de la géométrie affine $AG(3,2)$ est non presque idéale.



Amalgamations de matroïdes

Une deuxième réponse : Combiner des matroïdes ayant certaines "bonnes" propriétés

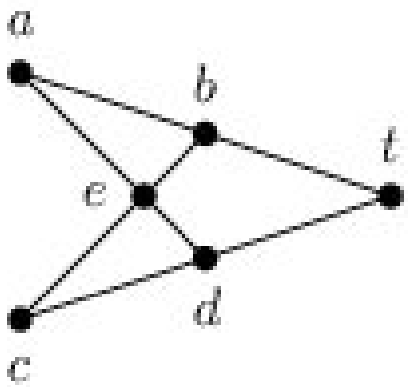
Nous avons étudié les amalgamations de matroïdes, sorte de généralisation des "clique-sum" à la classe des matroïdes. Le principe consiste à recoller deux matroïdes le long d'un fermé modulaire.

Amalgamations de matroïdes

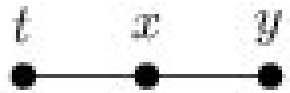
Une deuxième réponse : Combiner des matroïdes ayant certaines "bonnes" propriétés

Nous avons étudié les amalgamations de matroïdes, sorte de généralisation des "clique-sum" à la classe des matroïdes. Le principe consiste à recoller deux matroïdes le long d'un fermé modulaire.

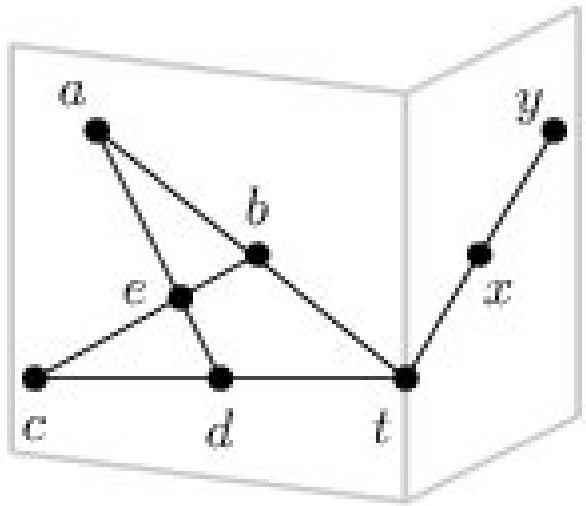
Exemple d'amalgamation



(a) K_4

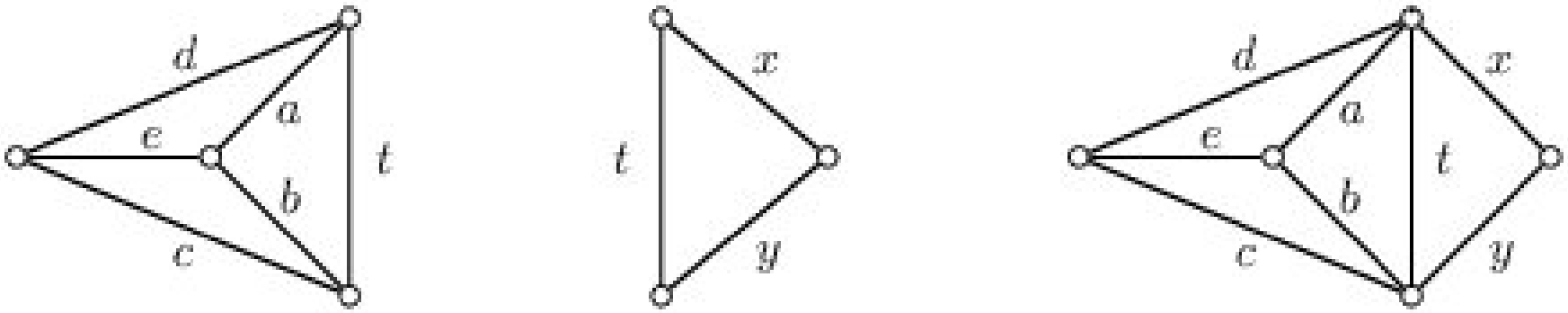


(b) K_3



(c) $P_{\mathcal{U}_{1,1}}(K_4, K_3)$

Exemple d'amalgamation (2)



(a) K_4 (b) K_3 (c) $P_{\mathcal{U}_{1,1}}(K_4, K_3)$

Figure: Connexion parallèle généralisé en terme de graphe

Résultats (2)

Résultat

On obtient une famille infinie de matroïdes non-presque idéaux en recollant deux copies d'un matroïdes non-presque idéal le long du dealer.

Exemple : On considère l'une des deux structures d'accès induite par le matroïde de Vámos, on a alors les bornes suivantes : $\rho_{V_8} \leq \frac{17}{19}$ et $\rho^*_{V_8} \leq \frac{136}{138}$. En recollant deux copies de ce matroïde, on peut obtenir une structure d'accès avec les paramètres suivants :

$$\rho = \rho_{V_8} = \frac{17}{19} \text{ et } \rho^* = \frac{255}{259} < \rho^*_{V_8}.$$

Résultats (2)

Résultat

On obtient une famille infinie de matroïdes non-presque idéaux en recollant deux copies d'un matroïdes non-presque idéal le long du dealer.

Exemple : On considère l'une des deux structures d'accès induite par le matroïde de Vámos, on a alors les bornes suivantes : $\rho_{V_8} \leq \frac{17}{19}$ et $\rho^*_{V_8} \leq \frac{136}{138}$. En recollant deux copies de ce matroïde, on peut obtenir une structure d'accès avec les paramètres suivants :

$$\rho = \rho_{V_8} = \frac{17}{19} \text{ et } \rho^* = \frac{255}{259} < \rho^*_{V_8}.$$

Dualité

Définition

Soit Γ une structure d'accès, on définit la structure d'accès duale par :

$$\Gamma^* = \{\mathcal{A} \subset \mathcal{P} \mid \mathcal{P} - \mathcal{A} \notin \Gamma\}.$$

Remarque : Lorsque la structure d'accès est induite par un matroïde $\mathcal{M}$ alors la structure d'accès duale est induite par le matroïde dual $\mathcal{M}^*$.

Question : Si la structure d'accès est idéale et induite par un matroïde, la structure d'accès duale est-elle aussi idéale ?

Dualité

Définition

Soit Γ une structure d'accès, on définit la structure d'accès duale par :

$$\Gamma^* = \{\mathcal{A} \subset \mathcal{P} \mid \mathcal{P} - \mathcal{A} \notin \Gamma\}.$$

Remarque : Lorsque la structure d'accès est induite par un matroïde $\mathcal{M}$ alors la structure d'accès duale est induite par le matroïde dual $\mathcal{M}^*$.

Question : Si la structure d'accès est idéale et induite par un matroïde, la structure d'accès duale est-elle aussi idéale ?

Dualité

Définition

Soit Γ *une structure d'accès, on définit la structure d'accès duale par :*

$$\Gamma^* = \{\mathcal{A} \subset \mathcal{P} \mid \mathcal{P} - \mathcal{A} \notin \Gamma\}.$$

Remarque : Lorsque la structure d'accès est induite par un matroïde $\mathcal{M}$ alors la structure d'accès duale est induite par le matroïde dual $\mathcal{M}^*$.

Question : Si la structure d'accès est idéale et induite par un matroïde, la structure d'accès duale est-elle aussi idéale ?

Dualité (2)

Si le matroïde est représentable sur un corps fini, c'est vrai en utilisant le théorème suivant :

Théorème

Le dual d'un matroïde représentable est représentable.

Corollaire

Si la structure d'accès idéale est induite par un matroïde représentable alors la structure d'accès duale est aussi idéale.

Dualité (3)

On a résultat plus général pour les matroïdes multilinéairement représentables :

Théorème (Simonis et Ashikhmin (1996))

Les structures d'accès induites par un matroïde multilinéairement représentable sont idéales.

Résultat

Le dual d'un matroïde multilinéairement représentable est multilinéairement représentable.

Dualité (3)

On a résultat plus général pour les matroïdes multilinéairement représentables :

Théorème (Simonis et Ashikhmin (1996))

Les structures d'accès induites par un matroïde multilinéairement représentable sont idéales.

Résultat

Le dual d'un matroïde multilinéairement représentable est multilinéairement représentable.

Matroïde dit "non-Pappus"

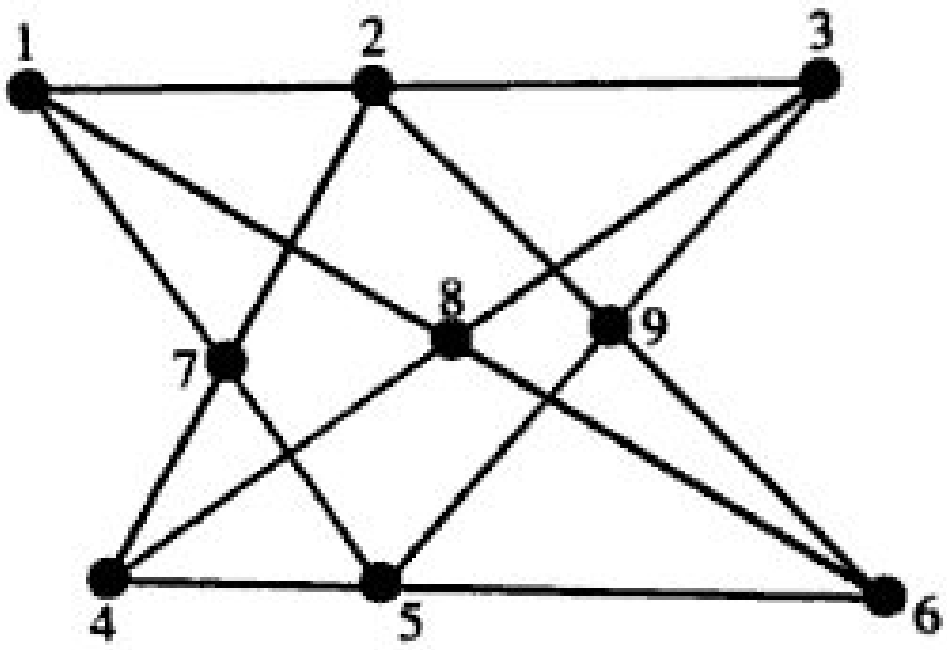


Figure: Ce matroïde n'est pas représentable !

Dualité (4)

Théorème (Simonis & Ashikhmin (1996))

Le matroïde non-Pappus est multilinéairement représentable sur $(\mathbb{Z}_3)^2$.

Corollaire

Les structures d'accès induites par le dual du matroïde non-Pappus sont idéales.

Dualité (4)

Théorème (Simonis & Ashikhmin (1996))

Le matroïde non-Pappus est multilinéairement représentable sur $(\mathbb{Z}_3)^2$.

Corollaire

Les structures d'accès induites par le dual du matroïde non-Pappus sont idéales.

Sujet de thèse :

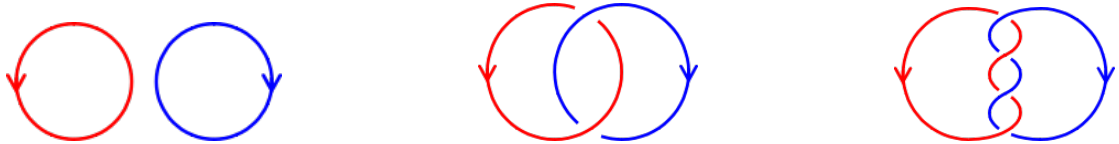
Graphes sans entrelacs

Nombre d'enlacement

Nombre d'enlacement de deux courbes fermées simples C et D :

$$\mathrm{lk}(C,D) = \deg(H_1(S^1) \xrightarrow{(C)_*} H_1(S^3 \backslash D) \simeq < \mu_D >)$$

$$= \text{"} \; \overset{C}{\times} \; \overset{D}{} \; - \; \overset{D}{\times} \; \overset{C}{} \; \text{"}$$



(a) lk = 0 (b) lk = 1 (c) lk = 2

Figure: Nombre d'enlacement

Graphes sans entrelacs

Définition

Un graphe G est dit "sans entrelacs" si il existe un plongement $\Phi : G \hookrightarrow \mathbb{R}^3$ tel que pour toute paire de cycles disjoints (C, D) de G, $lk(\Phi(C), \Phi(D)) = 0$.

Exemple :

- Les graphes planaires ou apex sont sans entrelacs.
- Le graphe K_6 n'est pas sans entrelacs.

Graphes sans entrelacs

Définition

Un graphe G est dit "sans entrelacs" si il existe un plongement $\Phi : G \hookrightarrow \mathbb{R}^3$ tel que pour toute paire de cycles disjoints (C, D) de G, $lk(\Phi(C), \Phi(D)) = 0$.

Exemple :

- Les graphes planaires ou apex sont sans entrelacs.
- Le graphe K_6 n'est pas sans entrelacs.

Plongement plat

Définition (Plongement plat)

G admet un plongement plat dans $\mathbb{R}^3$ si il existe un plongement tel que pour tout cycle C de G, il existe un disque D tel que $\Phi(G) \cap D = \partial D = \Phi(C)$.

Théorème (Robertson et al. (1995))

Un plongement Φ d'un graphe est plat ssi pour tout sous-graphe G', $\pi_1(\mathbb{R}^3 \backslash \Phi(G'))$ est libre.

Plongement plat

Définition (Plongement plat)

G admet un plongement plat dans $\mathbb{R}^3$ si il existe un plongement tel que pour tout cycle C de G, il existe un disque D tel que $\Phi(G) \cap D = \partial D = \Phi(C)$.

Théorème (Robertson et al. (1995))

Un plongement Φ d'un graphe est plat ssi pour tout sous-graphe G', $\pi_1(\mathbb{R}^3 \backslash \Phi(G'))$ est libre.

Caractérisations

Théorème (Robertson, Seymour & Thomas)

Les conditions suivantes sont équivalentes :

- *G admet un plongement sans entrelacs.*
- *G admet un plongement plat.*
- *G n'a pas de mineur isomorphe à un graphe de la famille de Petersen.*

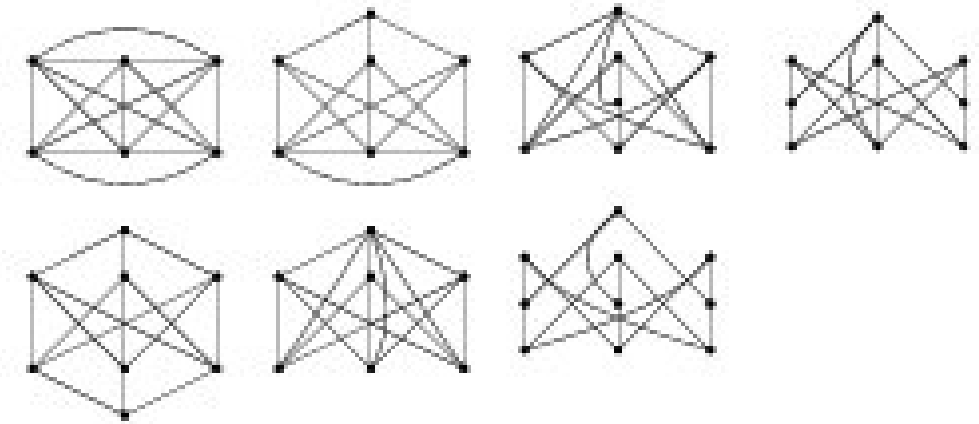


Figure: La famille de Petersen

L'invariant de Colin de Verdière

Colin de Verdière a introduit un invariant calculé à partir la deuxième plus grande valeur de propre d'une famille d'opérateur symétriques (appelés opérateurs de Schrödinger) associé à un graphe G. ($\approx$ multiplicité maximale de la deuxième valeur propre dans cette famille d'opérateurs vérifiant certaines conditions de non-dégénérescence). Cet invariant est noté $\mu(G)$.

Théorème (Lovász & Schrijver)

Les conditions suivantes sont équivalentes :

- *G admet un plongement plat.*
- $\mu(G) \leq 4$

Exemples : $\mu(K_n) = n - 1$, $\mu(K_{3,3}) = 4$

L'invariant de Colin de Verdière

Colin de Verdière a introduit un invariant calculé à partir la deuxième plus grande valeur de propre d'une famille d'opérateur symétriques (appelés opérateurs de Schrödinger) associé à un graphe G. ($\approx$ multiplicité maximale de la deuxième valeur propre dans cette famille d'opérateurs vérifiant certaines conditions de non-dégénérescence). Cet invariant est noté $\mu(G)$.

Théorème (Lovász & Schrijver)

Les conditions suivantes sont équivalentes :

- *G admet un plongement plat.*
- $\mu(G) \leq 4$

Exemples : $\mu(K_n) = n - 1$, $\mu(K_{3,3}) = 4$

L'invariant de Colin de Verdière

Colin de Verdière a introduit un invariant calculé à partir la deuxième plus grande valeur de propre d'une famille d'opérateur symétriques (appelés opérateurs de Schrödinger) associé à un graphe G. ($\approx$ multiplicité maximale de la deuxième valeur propre dans cette famille d'opérateurs vérifiant certaines conditions de non-dégénérescence). Cet invariant est noté $\mu(G)$.

Théorème (Lovász & Schrijver)

Les conditions suivantes sont équivalentes :

- *G admet un plongement plat.*
- $\mu(G) \leq 4$

Exemples : $\mu(K_n) = n - 1$, $\mu(K_{3,3}) = 4$

Hiérarchie

Un graphe G est :

- une forêt de chemin si et seulement si $\mu_G \leq 1$.
- planaire externe si et seulement si $\mu_G \leq 2$.
- planaire si et seulement si $\mu_G \leq 3$.
- sans entrelacs si et seulement si $\mu_G \leq 4$.

Algorithmique

Kawarabayashi, Kreutzer & Mohar (2010) ont trouvés un algorithme en $\mathcal{O}(n^2)$ qui, étant donné un graphe G, retourne un mineur de la famille de Petersen si G n'est pas plongeable sans entrelacs et sinon retourne un plongement.

Sur le sujet ...

Quelles autres propriétés des graphes planaires se généralisent aux graphes sans entrelacs ?

- Caractérisation en terme de poset d'incidence et caractérisation géométriques ?
- Un théorème de Fáry pour les graphes sans entrelacs ?
- Algorithme de reconnaissance linéaire ?
- Algorithme effectifs ?
- ?