Informatique Quantique et Théorie des Graphes

Simon Perdrix

CNRS, LORIA, équipe CARTE
simon.perdrix@loria.fr

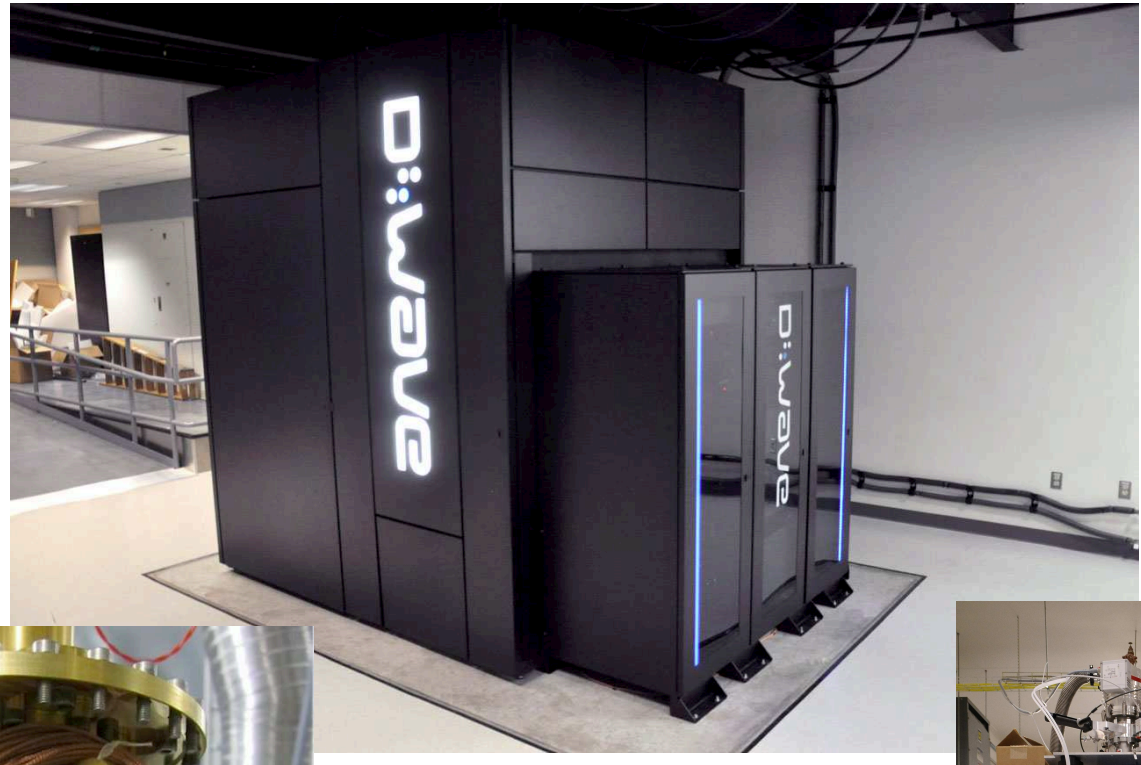
JGA – Orléans 2015

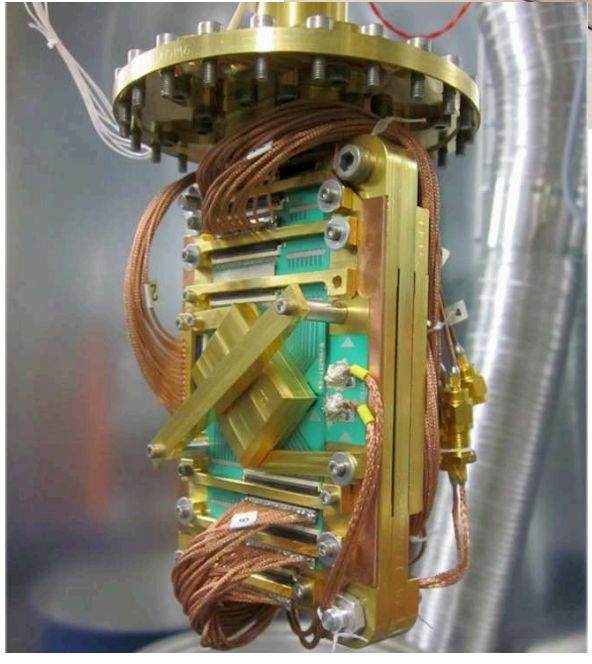
Plan

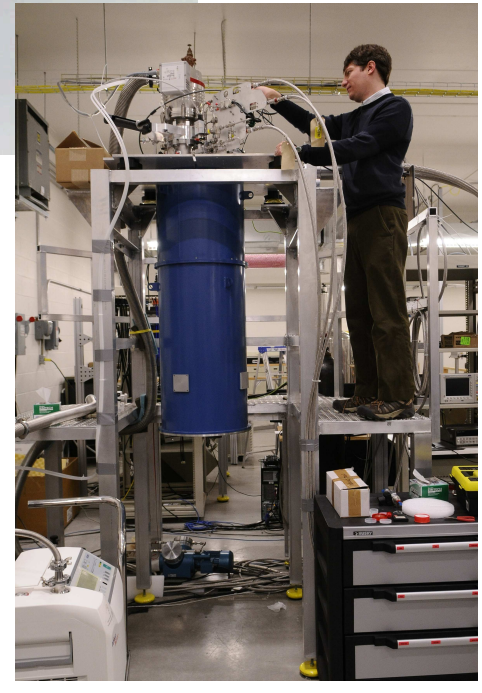
1. Informatique quantique
   - Motivations
   - Formalisme
   - Intrication
2. Représentation de l'intrication
   - Etat graphe
   - Complémentation Locale
   - Rang de coupe
3. Degré minimum par complementation locale
   - Bornes
   - Complexité
   - Algorithmes Exacts

Pourquoi un traitement quantique de l'information ?

1. Algorithmes plus efficaces :
   Certains problèmes peuvent être résolus (beaucoup) plus rapidement avec un ordinateur quantique.
   - Algorithme polynomial de factorisation [Shor'94]

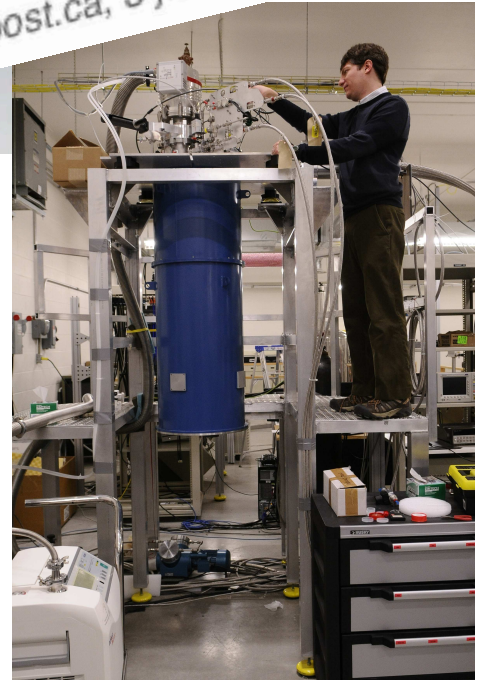

D-Wave
D-Wave





L'Agence nationale de sécurité américaine (NSA) cherche à créer un "ordinateur quantique" à même de décrypter presque n'importe quel code de sécurité, selon le Washington Post qui cite jeudi des documents divulgués par l'ancien consultant Edward Snowden.

huffingtonpost.ca, 3 janvier 2014



Pourquoi un traitement quantique de l'information ?

1. Algorithmes plus efficaces :
   Certains problèmes peuvent être résolus (beaucoup) plus rapidement avec un ordinateur quantique.
   - Algorithme polynomial de factorisation [Shor'94]

2. Communications plus sûres :
   Cryptographie quantique, BB84 [Bennett & Brassard'84].

id Quantique

SEQURENET
A QUANTUM KEY TO NETWORK SECURITY

MagiQ™

Informatique Quantique et Théorie des Graphes

Algorithmes quantiques pour des problèmes de graphes :

- Connexité $\Theta(n^{3/2})$ ($\Theta(n^2)$ en classique) [Dürr, Heiligman, Hoyer, Mhalla'04]
- Recherche de Triangle $O(n^{1.25})$ ($O(n^{2.37})$ en classique) [LeGall'14, Magniez'13]

Informatique Quantique et Théorie des Graphes

Algorithmes quantiques pour des problèmes de graphes :

- Connexité $\Theta(n^{3/2})$ ($\Theta(n^2)$ en classique) [Dürr, Heiligman, Hoyer, Mhalla'04]
- Recherche de Triangle $O(n^{1.25})$ ($O(n^{2.37})$ en classique) [LeGall'14, Magniez'13]

La théorie des graphes comme un outil pour le quantique :

- Modèle de calcul quantique (eg. MBQC : Flot, déterminisme, profondeur...)
- Protocoles de cryptograhie quantique (eg. Partage de secret quantique)
- Fondement : causalité, non localité, intrication.

Une Information Quantique

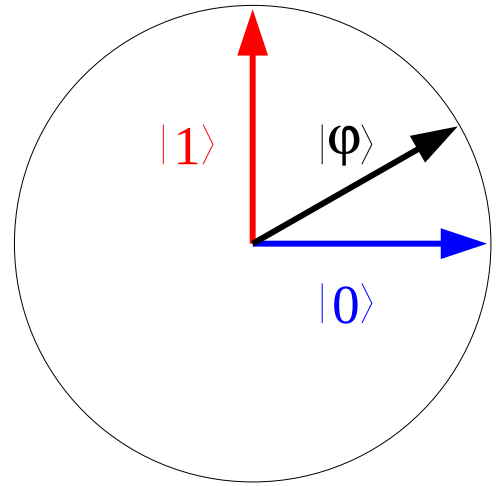
- Brique de base de l'information :

$$\mathbf{0}, \mathbf{1}$$

- Nous vivons dans un monde quantique :

$$\alpha\,|\mathbf{0}\rangle + \beta\,|\mathbf{1}\rangle$$

avec $\alpha, \beta \in \mathbb{C}$ et $|\alpha|^2 + |\beta|^2 = 1$



L'état d'un registre quantique de taille n est un vecteur unité de $\mathbb{C}^{\{0,1\}^n}$:

$$|\varphi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x\,|x\rangle \quad \text{avec} \quad ||\,|\varphi\rangle\,||^2 = \sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1$$

Une Information Quantique

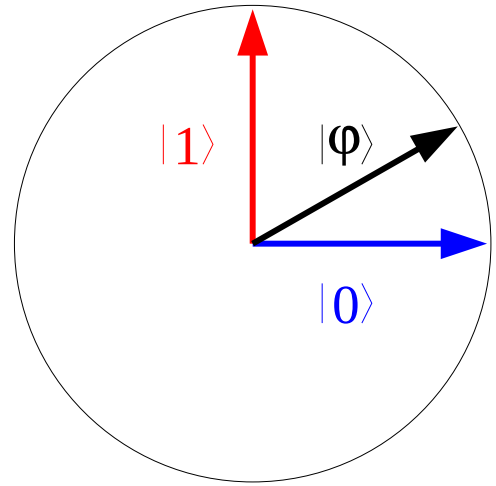
- Brique de base de l'information :

$$\mathbf{0}, \mathbf{1}$$

- Nous vivons dans un monde quantique :

$$\alpha \left|\mathbf{0}\right\rangle + \beta \left|\mathbf{1}\right\rangle$$

avec $\alpha, \beta \in \mathbb{C}$ et $|\alpha|^2 + |\beta|^2 = 1$



L'état d'un registre quantique de taille n est un vecteur unité de $\mathbb{C}^{\{0,1\}^n}$:

$$|\varphi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x \left|x\right\rangle \quad \text{avec} \quad ||\,|\varphi\rangle\,||^2 = \sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1$$

Etats Graphes

Definition. Etant donné un graphe G d'order n,

$$|G\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{|G[x]|} |x\rangle$$

où $G[x]$ est le sous-graphe induit par $supp(x)$.

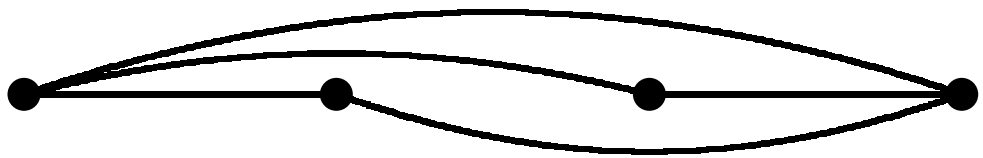
Etats Graphes

Definition. Etant donné un graphe G d'order n,

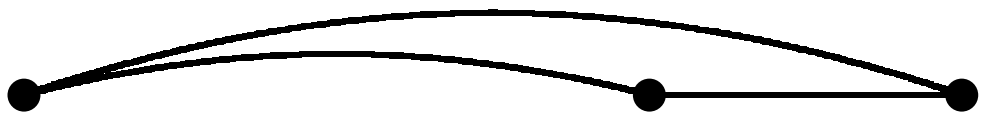
$$|G\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{|G[x]|} |x\rangle$$

où $G[x]$ est le sous-graphe induit par $supp(x)$.

G :



$G[1011]$:



$$\begin{aligned} |G\rangle \quad = \quad & \tfrac{1}{4}(|0000\rangle + |0001\rangle + |0010\rangle - |0011\rangle + |0100\rangle - |0101\rangle + |0110\rangle + |0111\rangle \\ & + |1000\rangle - |1001\rangle - |1010\rangle - |1011\rangle - |1100\rangle - |1101\rangle + |1110\rangle - |1111\rangle) \end{aligned}$$

Système composé

Soit $|\varphi_1\rangle$ l'état d'un registre de n qubits et $|\varphi_2\rangle$ celui d'un registre de m qubits, l'état du registre composé de $(n+m)$ qubits est

$$|\psi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$$

avec $\cdot \otimes \cdot$ bilinéaire et $\forall x \in \{0,1\}^n, \forall y \in \{0,1\}^m, |x\rangle \otimes |y\rangle = |xy\rangle$

- $|0\rangle \otimes (\frac{|0\rangle - |1\rangle}{\sqrt{2}}) = \frac{|00\rangle - |01\rangle}{\sqrt{2}}$
- $\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \quad ? \quad \otimes \quad ?$

Système composé

Soit $|\varphi_1\rangle$ l'état d'un registre de n qubits et $|\varphi_2\rangle$ celui d'un registre de m qubits, l'état du registre composé de $(n+m)$ qubits est

$$|\psi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$$

avec $\cdot \otimes \cdot$ bilinéaire et $\forall x \in \{0,1\}^n, \forall y \in \{0,1\}^m, |x\rangle \otimes |y\rangle = |xy\rangle$

- $|0\rangle \otimes (\frac{|0\rangle - |1\rangle}{\sqrt{2}}) = \frac{|00\rangle - |01\rangle}{\sqrt{2}}$

- $$\begin{aligned} \frac{|00\rangle + |11\rangle}{\sqrt{2}} &= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \\ &= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle \\ &\implies ad = 0 \implies ac = 0 \text{ ou } bd = 0 \quad \text{impossible} \end{aligned}$$

Intrication

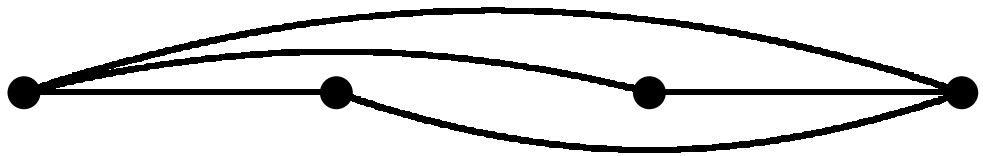
Equivalence d'intrication

Définition Deux états quantiques $|\varphi\rangle$, $|\psi\rangle$ ont la même intrication ($|\varphi\rangle \equiv_{LU} |\psi\rangle$) s'il existe des opérations quantiques sur un qubit U_i, V_i telles que $(U_1 \otimes \ldots \otimes U_n)\,|\varphi\rangle = |\psi\rangle$ et $(V_1 \otimes \ldots \otimes V_n)\,|\psi\rangle = |\varphi\rangle$.

Equivalence d'intrication

Définition Deux états quantiques $|\varphi\rangle$, $|\psi\rangle$ ont la même intrication ($|\varphi\rangle \equiv_{LU} |\psi\rangle$) s'il existe des opérations quantiques sur un qubit U_i, V_i telles que $(U_1 \otimes \ldots \otimes U_n)\,|\varphi\rangle = |\psi\rangle$ et $(V_1 \otimes \ldots \otimes V_n)\,|\psi\rangle = |\varphi\rangle$.

Etat graphe = représentation graphique de l'intrication ?



A quelle condition sur G et G', $|G\rangle$ et $|G'\rangle$ ont la même intrication ?

Complementation Locale

Théorème [Van den Nest'04] L'intrication d'un état graphe est invariante par complémentation locale :
Pour tout $G = (V, E)$ et tout $u \in V$, $|G\rangle \equiv_{LU} |G * u\rangle$

Complémentation locale [Kotzig'66] : $G = (V, E)$ et $u \in V$,

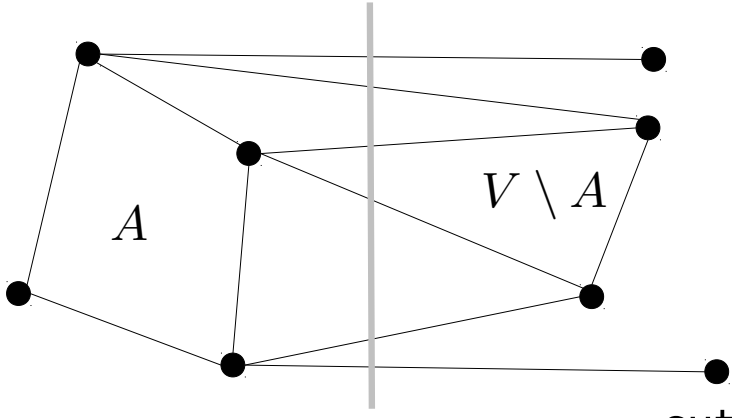
$$G * u = G \Delta K_{N(u)}$$

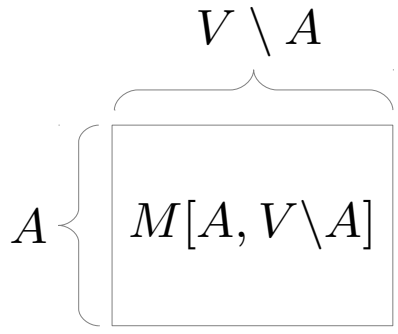
$$G \equiv_{LC} G' \text{ si } \exists u_1, \ldots, u_k, G' = G * u_1 \ldots * u_k$$

Rang de coupe

Théorème [Hein et al.'06] Si $|G\rangle \equiv_{LU} |G'\rangle$ alors G et G' ont le même cutrank : $\text{cutrk}_G(.) = \text{cutrk}_{G'}(.)$

Rang de coupe [Bouchet'87,Oum'06] :



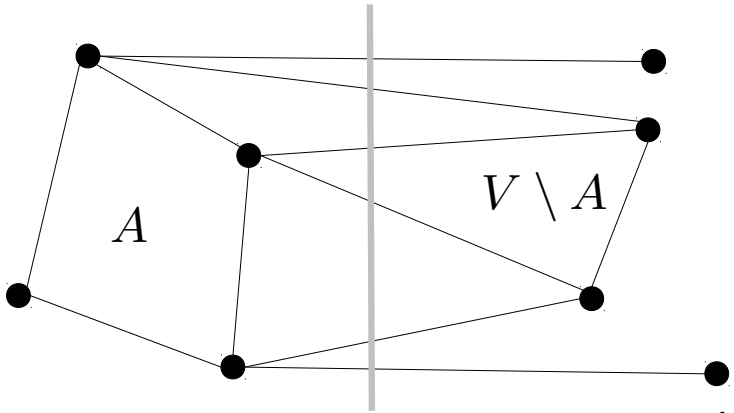


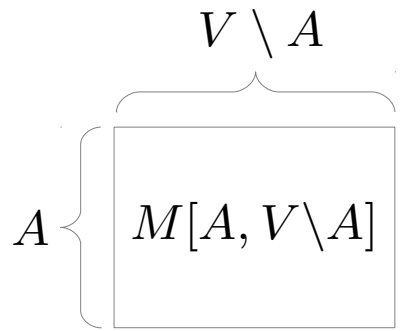
$\text{cutrk}_G(A) := rang(M[A, V \setminus A])$

Rang de coupe

Théorème [Hein et al.'06] Si $|G\rangle \equiv_{LU} |G'\rangle$ alors G et G' ont le même cutrank : $\text{cutrk}_G(.) = \text{cutrk}_{G'}(.)$

Rang de coupe [Bouchet'87,Oum'06] :





$\text{cutrk}_G(A) := rang(M[A, V \setminus A])$

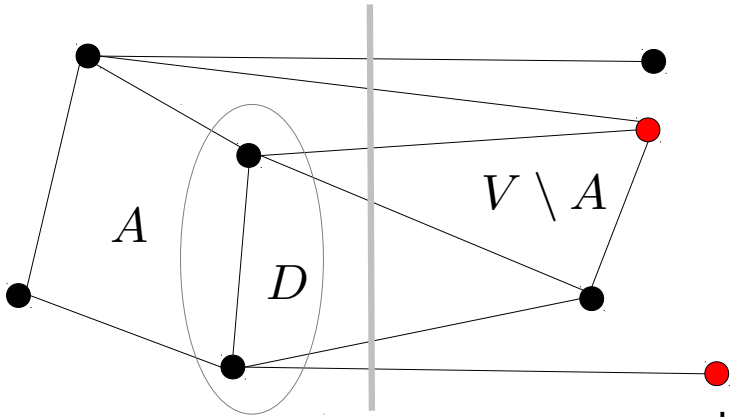
$\text{cutrk}_G(A)$ est le rang de $L_A : 2^A \to 2^{V\setminus A} = D \mapsto Odd_G(D) \cap (V \setminus A)$ où $Odd_G(D) = \Delta_{u\in D} N_G(u)$.

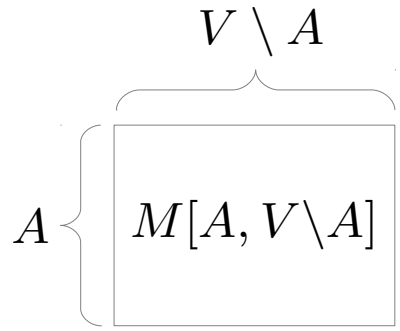
– $L_A(D)$: sommets de $V\setminus A$ ayant un nombre impair de voisins dans D
– $L_A(D_1 \Delta D_2) = L_A(D_1)\Delta L_A(D_2)$
– $D \in ker(L_A)$ ssi $D \cup Odd_G(D) \subseteq A$.

Rang de coupe

Théorème [Hein et al.'06] Si $|G\rangle \equiv_{LU} |G'\rangle$ alors G et G' ont le même cutrank : $\text{cutrk}_G(.) = \text{cutrk}_{G'}(.)$

Rang de coupe [Bouchet'87,Oum'06] :



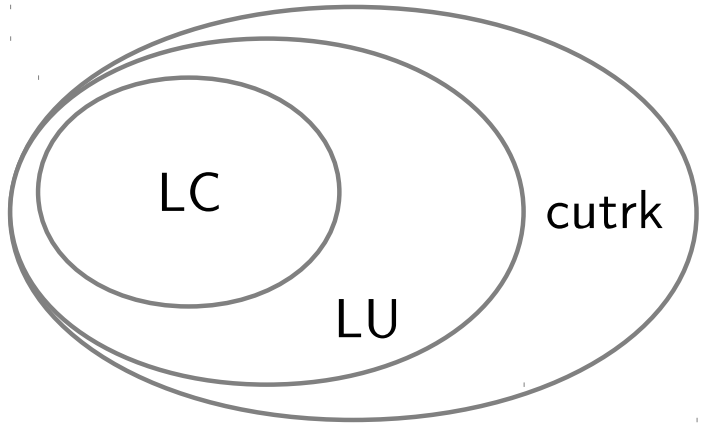


$\text{cutrk}_G(A) := rang(M[A, V \setminus A])$

$\text{cutrk}_G(A)$ est le rang de $L_A : 2^A \to 2^{V\setminus A} = D \mapsto Odd_G(D) \cap (V \setminus A)$ où $Odd_G(D) = \Delta_{u\in D} N_G(u)$.

– $L_A(D)$: sommets de $V\setminus A$ ayant un nombre impair de voisins dans D
– $L_A(D_1 \Delta D_2) = L_A(D_1)\Delta L_A(D_2)$
– $D \in ker(L_A)$ ssi $D \cup Odd_G(D) \subseteq A$.

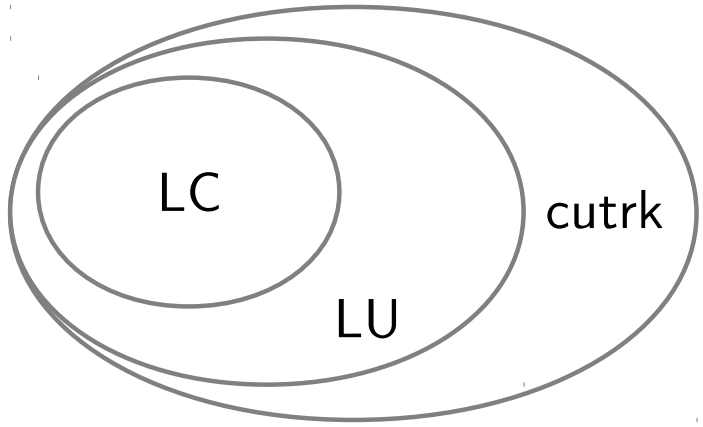
Sandwich



$\rightarrow$ G et $G * u$ ont le même rang de coupe (déjà connu [Bouchet85])

$\rightarrow$ La réciproque a été conjecturée par [Bouchet'85]

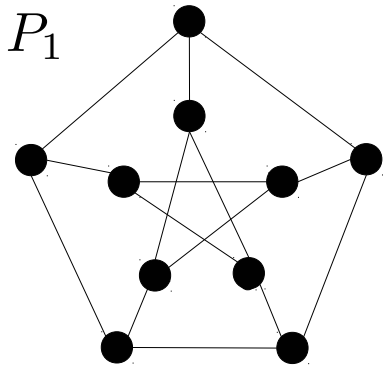
Sandwich

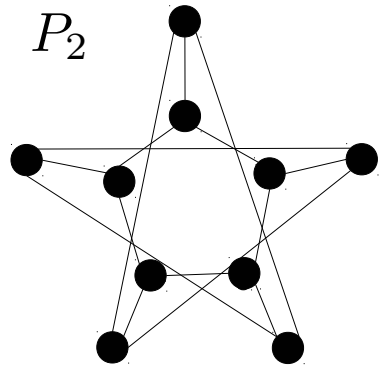


$\rightarrow$ G et $G * u$ ont le même rang de coupe (déjà connu [Bouchet85])

$\rightarrow$ La réciproque a été conjecturée par [Bouchet'85]

$\rightarrow$ Infirmée par [Fon der Flass'96]

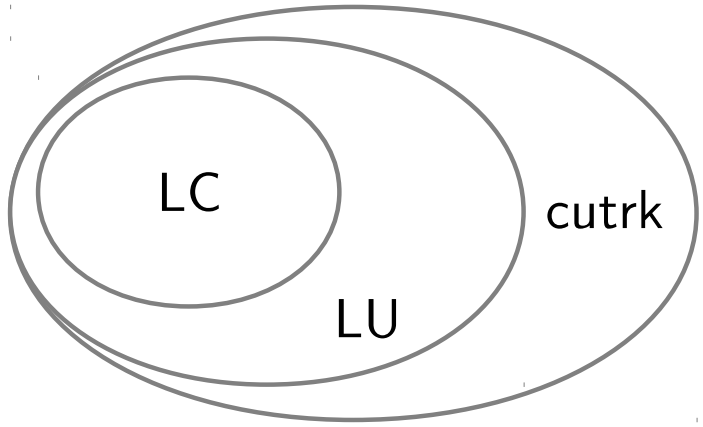




$$\text{cutrk}_{P_1}(.) = \text{cutrk}_{P_2}(.)$$

$$P_1 \not\equiv_{LC} P_2$$

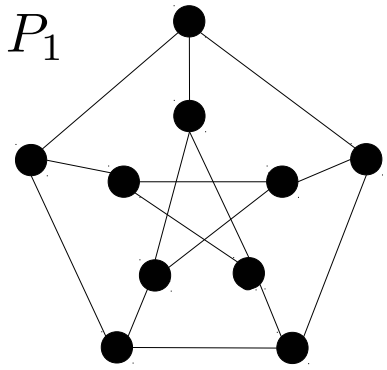
Sandwich

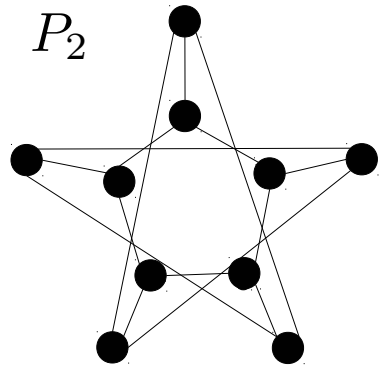


$\rightarrow$ G et $G * u$ ont le même rang de coupe (déjà connu [Bouchet85])

$\rightarrow$ La réciproque a été conjecturée par [Bouchet'85]

$\rightarrow$ Infirmée par [Fon der Flass'96]



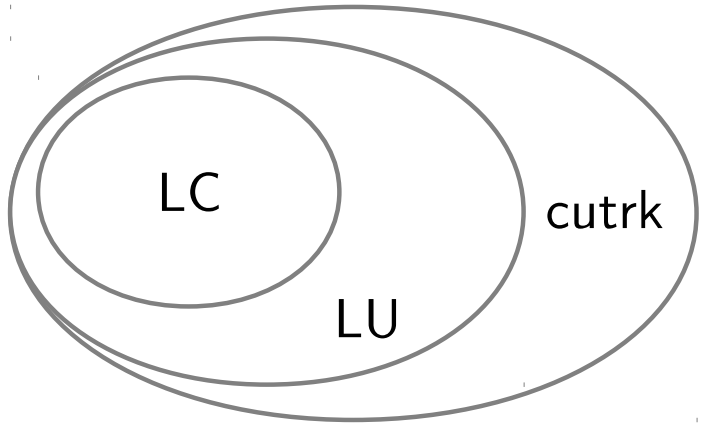


$$\mathsf{cutrk}_{P_1}(.) = \mathsf{cutrk}_{P_2}(.)$$

$$P_1 \not\equiv_{LC} P_2$$

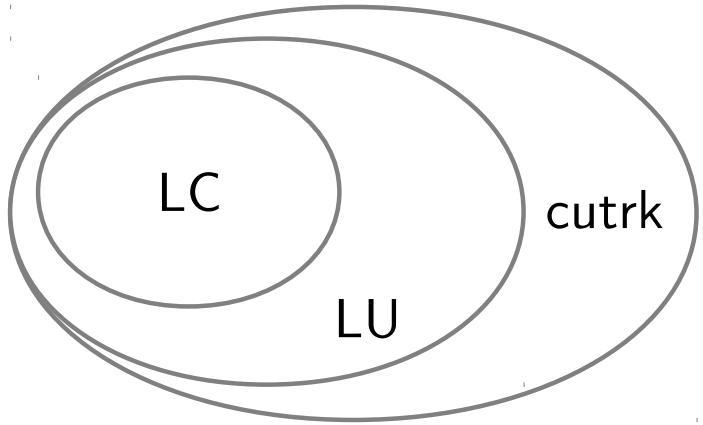
$$|P_1\rangle \not\equiv_{LU} |P_2\rangle$$

$LU = LC?$



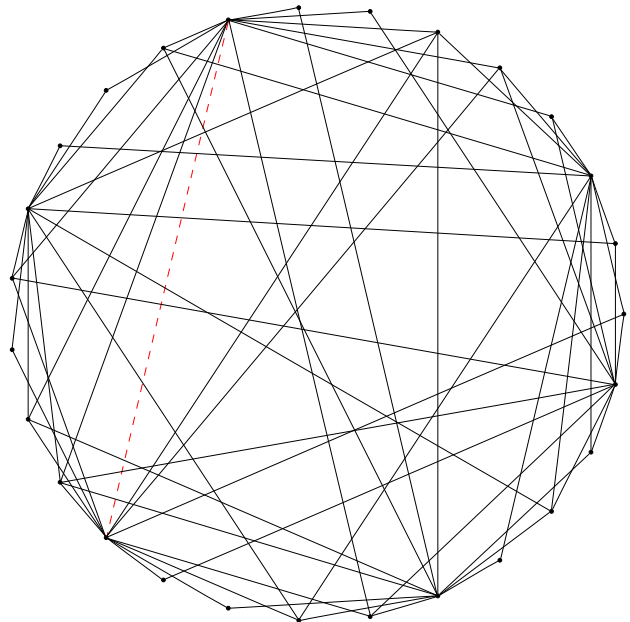
$\rightarrow$ [Van den Nest'04] conjecture $|G\rangle \equiv_{LU} |G'\rangle \iff G \equiv_{LC} G'$

$LU = LC?$



$\rightarrow$ [Van den Nest'04] conjecture $|G\rangle \equiv_{LU} |G'\rangle \iff G \equiv_{LC} G'$

$\rightarrow$ Infirmée par [Ji, Chen, Wei, Ying'08]



Degré Minimum par Comp. Locale

Définition. Etant donné un graphe $G = (V, E)$,

$$\delta_{loc}(G) = \min_{H \equiv_{LC} G} \delta(H)$$

Théorème [Hoyer, Mhalla, P.'06] Pour tout graphe $G = (V, E)$,

$$\delta_{loc}(G)+1 = \min_{\emptyset \subset D \subseteq V} |D \cup Odd_G(D)| = \min\{|A| : A \subseteq V \wedge \mathsf{cutrk}_G(A) < |A|\}$$

Degré Minimum par Comp. Locale

Définition. Etant donné un graphe $G = (V, E)$,

$$\delta_{loc}(G) = \min_{H \equiv_{LC} G} \delta(H)$$

Théorème [Hoyer, Mhalla, P.'06] Pour tout graphe $G = (V, E)$,

$$\delta_{loc}(G)+1 = \min_{\emptyset \subset D \subseteq V} |D \cup Odd_G(D)| = \min\{|A| : A \subseteq V \wedge \mathsf{cutrk}_G(A) < |A|\}$$

Corollaires

– si $\mathsf{cutrk}_G(.) = \mathsf{cutrk}_{G'}(.)$ alors $\delta_{loc}(G) = \delta_{loc}(G')$

– si $|G\rangle = |G'\rangle$ alors $\delta_{loc}(G) = \delta_{loc}(G')$

$$\delta_{loc}(G) = \min_{H \equiv_{LC} G} \delta(H) = \min_{H \equiv_{LU} G} \delta(H) = \min_{\mathsf{cutrk}_H = \mathsf{cutrk}_G} \delta(H)$$

Degré Minimum par Comp. Locale

Définition. Etant donné un graphe $G = (V, E)$,

$$\delta_{loc}(G) = \min_{H \equiv_{LC} G} \delta(H)$$

Théorème [Hoyer, Mhalla, P.'06] Pour tout graphe $G = (V, E)$,

$$\delta_{loc}(G)+1 = \min_{\emptyset \subset D \subseteq V} |D \cup Odd_G(D)| = \min\{|A| : A \subseteq V \wedge \mathsf{cutrk}_G(A) < |A|\}$$

Corollaires

– si $\mathsf{cutrk}_G(.) = \mathsf{cutrk}_{G'}(.)$ alors $\delta_{loc}(G) = \delta_{loc}(G')$

– si $|G\rangle = |G'\rangle$ alors $\delta_{loc}(G) = \delta_{loc}(G')$

$$\delta_{loc}(G) = \min_{H \equiv_{LC} G} \delta(H) = \min_{H \equiv_{LU} G} \delta(H) = \min_{\mathsf{cutrk}_H = \mathsf{cutrk}_G} \delta(H)$$

Propriétés quantiques de δ_{loc} :

– robustesse de l'état quantique ;

– distance minimale de code quantique ;

– complexité de préparation des état graphes.

Bornes sur δ_{loc}

- Hypercube H_n d'ordre n,

$$\delta_{loc}(H_n) = \Theta(\log_2(n))$$

- Graphes de Paley $\mathcal{P}_n$, $n = 1 \bmod 4$ premier, $V(\mathcal{P}_n) = \{0, ..., n-1\}$, $(i,j) \in E(\mathcal{P}_n) \Leftrightarrow \exists x, x^2 = i - j \bmod n$

$$\delta_{loc}(P_n) > \sqrt{n} - \frac{3}{2}$$

- Graphes Aléatoires $G(n, 1/2)$

$$Pr(\delta_{loc}(G(n, 1/2)) > 0.189n) > 1 - 2^{-\Omega(n)}$$

Bornes sur δ_{loc}

- Hypercube H_n d'ordre n,

$$\delta_{loc}(H_n) = \Theta(\log_2(n))$$

- Graphes de Paley $\mathcal{P}_n$, $n = 1 \bmod 4$ premier, $V(\mathcal{P}_n) = \{0, ..., n-1\}$, $(i,j) \in E(\mathcal{P}_n) \Leftrightarrow \exists x, x^2 = i - j \bmod n$

$$\delta_{loc}(P_n) > \sqrt{n} - \frac{3}{2}$$

- Graphes Aléatoires $G(n, 1/2)$

$$Pr(\delta_{loc}(G(n, 1/2)) > 0.189n) > 1 - 2^{-\Omega(n)}$$

Théorème (Bipartite) Local Minimum Degree est NPC.

Bornes sur δ_{loc}

- Hypercube H_n d'ordre n,

$$\delta_{loc}(H_n) = \Theta(\log_2(n))$$

- Graphes de Paley $\mathcal{P}_n$, $n = 1 \bmod 4$ premier, $V(\mathcal{P}_n) = \{0, ..., n-1\}$, $(i,j) \in E(\mathcal{P}_n) \Leftrightarrow \exists x, x^2 = i - j \bmod n$

$$\delta_{loc}(P_n) > \sqrt{n} - \frac{3}{2}$$

- Graphes Aléatoires $G(n, 1/2)$

$$Pr(\delta_{loc}(G(n, 1/2)) > 0.189n) > 1 - 2^{-\Omega(n)}$$

Théorème (Bipartite) Local Minimum Degree est NPC.

- Pour tout $n > 1$, il existe G biparti d'ordre n tel que

$$\delta_{loc}(G) > 0.110n$$

Bornes Sup

Pour tout graphe G d'ordre n,

$$\delta_{loc}(G) \leq n/2$$

Théorème. Pour tout graphe G, $|G| > 0$,

$$2\delta_{loc}(G) \leq \tau(G) + \log_2(\tau(G)) + 1$$

où $\tau(G)$ est la taille de la plus petite couverture par sommets.

Corollaire. Si G est biparti d'ordre $n > 0$,

$$\delta_{loc}(G) < n/4 + \log_2(n)$$

Théorème. Pour tout G d'ordre $n > 0$,

$$\delta_{loc}(G) \leq 3n/8 + \log_2(n)$$

Bornes Sup

Pour tout graphe G d'ordre n,

$$\delta_{loc}(G) \leq n/2$$

Théorème. Pour tout graphe G, $|G| > 0$,

$$2\delta_{loc}(G) \leq \tau(G) + \log_2(\tau(G)) + 1$$

où $\tau(G)$ est la taille de la plus petite couverture par sommets.

Corollaire. Si G est biparti d'ordre $n > 0$,

$$\delta_{loc}(G) < n/4 + \log_2(n)$$

Théorème. Pour tout G d'ordre $n > 0$,

$$\delta_{loc}(G) \leq 3n/8 + \log_2(n)$$

Algorithmes Exacts

Corollaire.

$$\delta_{loc}(G) + 1 = \min_{\emptyset \subset D \subseteq V} |D \cup Odd_G(D)|$$

- Pour tout graphe G d'ordre n, $\delta_{loc}(G)$ en temps $\mathcal{O}^*(1.938^n)$.
- Pour tout graphe biparti G d'ordre n, $\delta_{loc}(G)$ en temps $\mathcal{O}^*(1.755^n)$.

Algorithmes Exacts

Corollaire.

$$\delta_{loc}(G) + 1 = \min_{\emptyset \subset D \subseteq V} |D \cup Odd_G(D)|$$

- Pour tout graphe G d'ordre n, $\delta_{loc}(G)$ en temps $\mathcal{O}^*(1.938^n)$.
- Pour tout graphe biparti G d'ordre n, $\delta_{loc}(G)$ en temps $\mathcal{O}^*(1.755^n)$.

Théorème. Pour tout graphe biparti G d'ordre n, $\delta_{loc}(G)$ peut être calculé en temps $\mathcal{O}^*(1.466^n)$.

Complexité paramétrée

Local Minimum Degree :
input : A graph G
parameter : An integer k
question : Is $\delta_{loc}(G) \leq k$?

Bipartite Local Minimum Degree :
input : A bipartite graph G
parameter : An integer k
question : Is $\delta_{loc}(G) \leq k$?

Théorème. (Bipartite) Local Minimum Degree est dans W[2].

Théorème. (Bipartite) Local Minimum Degree est FPT-équivalent à EvenSet.

EvenSet :
input : A bipartite graph $G = (R, B, E)$
parameter : An integer k
question : Is there a non empty $D \subseteq R$, such that $|D| \leq k$ and $Odd_G(D) = \emptyset$

Complexité paramétrée

Local Minimum Degree :
input : A graph G
parameter : An integer k
question : Is $\delta_{loc}(G) \leq k$?

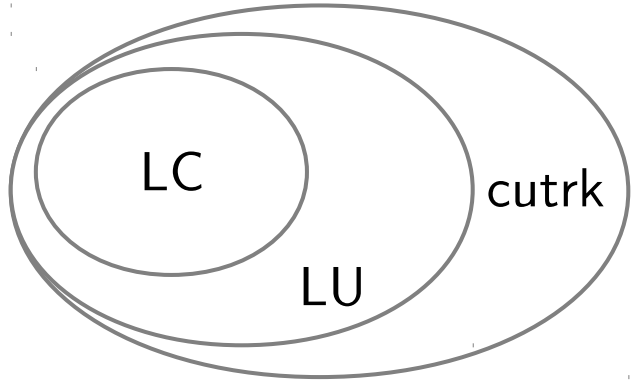
Bipartite Local Minimum Degree :
input : A bipartite graph G
parameter : An integer k
question : Is $\delta_{loc}(G) \leq k$?

Théorème. (Bipartite) Local Minimum Degree est dans W[2].

Théorème. (Bipartite) Local Minimum Degree est FPT-équivalent à EvenSet.

EvenSet :
input : A bipartite graph $G = (R, B, E)$
parameter : An integer k
question : Is there a non empty $D \subseteq R$, such that $|D| \leq k$ and $Odd_G(D) = \emptyset$

Conclusion



$\delta_{loc}(G) = \min_{G \equiv_{LC} H} \delta(H)$

- $\forall n, \exists G$ d'ordre n, $\delta_{loc}(G) \geq 0.189n$ ($0.110n$ pour les bipartis)
- $\forall G$ d'ordre n, $\delta_{loc}(G) \leq 0.375n$ ($0.250n$ pour les bipartis)
- NPC, non-approx., W[2]
- Algorithme en $\mathcal{O}^*(1.938^n)$ ($\mathcal{O}^*(1.466^n)$ pour les bipartis)

Perspectives

- Améliorer bornes et algorithmes.
- Famille de graphes pour laquelle δ_{loc} est "grand" mais "facile" à calculer.
- Pivot ($G \wedge uv := G * u * v * u$) v.s Complémentation Locale