Percolation et codes correcteurs quantiques

Nicolas Delfosse (travail commun avec Gilles Zémor)

LIX-Qualcomm, École Polytechnique
INRIA Saclay, Équipe GRACE

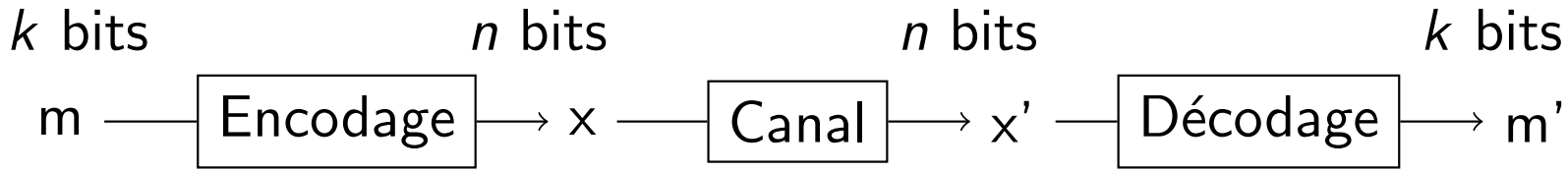
Groupe de travail Combinatoire - LIX - École Polytechnique
26 Novembre 2012

Capacité d'un canal classique

- Le canal introduit des erreurs

1. C. Shannon - A mathematical theory of communication. The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948.

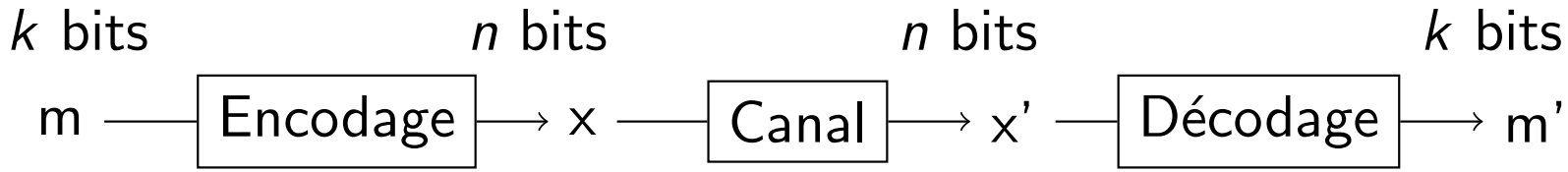
Capacité d'un canal classique



- Le canal introduit des erreurs
  $\longrightarrow$ On ajoute de la redondance

1. C. Shannon - A mathematical theory of communication. The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948.

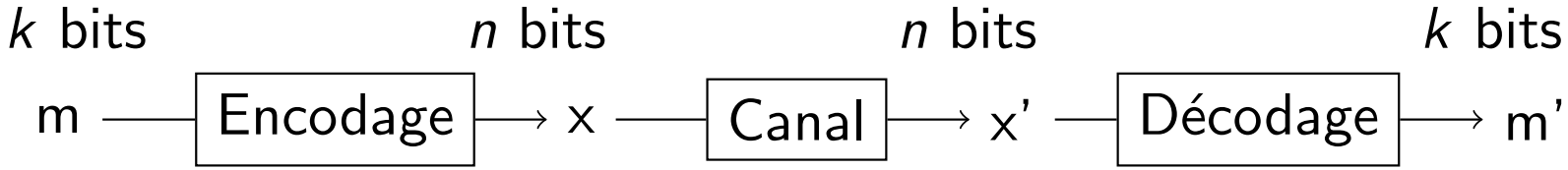
Capacité d'un canal classique



- Le canal introduit des erreurs
  $\longrightarrow$ On ajoute de la redondance
- Quel est le plus grand rendement $R = k/n$ avec $P_{err} \to 0$?
  $\longrightarrow$ C'est la capacité du canal. [1]

1. C. Shannon - A mathematical theory of communication. The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948.

Capacité d'un canal classique



- Le canal introduit des erreurs
  $\longrightarrow$ On ajoute de la redondance
- Quel est le plus grand rendement $R = k/n$ avec $P_{err} \to 0$?
  $\longrightarrow$ C'est la capacité du canal. [1]
- On veut un encodage et décodage rapide et efficace
  $\longrightarrow$ codes LDPC : $C = \mathrm{Ker}\, H$ avec H une matrice creuse
  $\longrightarrow$ En compensation : légèrement sous la capacité.

1. C. Shannon - A mathematical theory of communication. The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948.

Codes correcteurs

Un code (linéaire binaire) est un sous-espace vectoriel C de $\mathbb{F}_2^n$.

- La dimension de C est noté k.
- La distance minimale de C est $d = \min\{w(x) \mid x \in C \backslash \{0\}\}$.
- Les paramètres de C : $[n, k, d]$.

Codes des cycles

$C = \ker H$ avec H la matrice d'incidence d'un graphe G :

C est le code des cycles de ce graphe $G = (V, E)$.

- les vecteurs de C sont les cycles (homologiques) du graphe.
- $k = |E| - |V| + 1$ si le graphe est connexe.
- $d =$ maille $=$ longueur du pus court cycle non nul.

Le graphe de Petersen

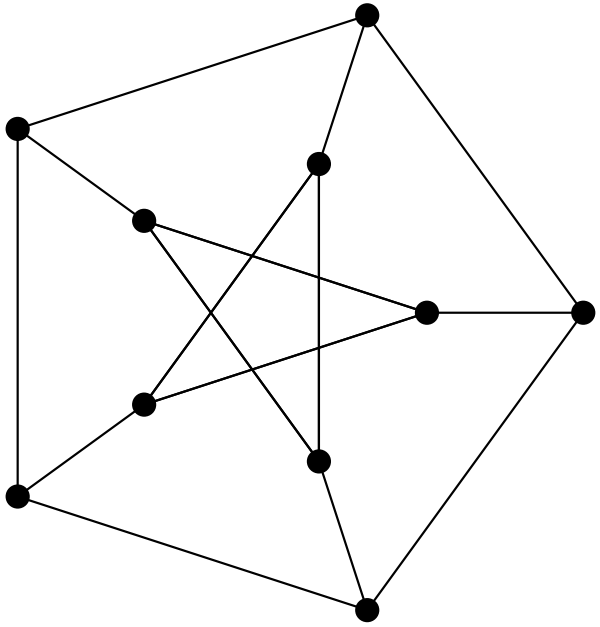


FIGURE : Le code des cycles du graphe de Petersen est un code $[15, 6, 5]$

Le graphe de Petersen

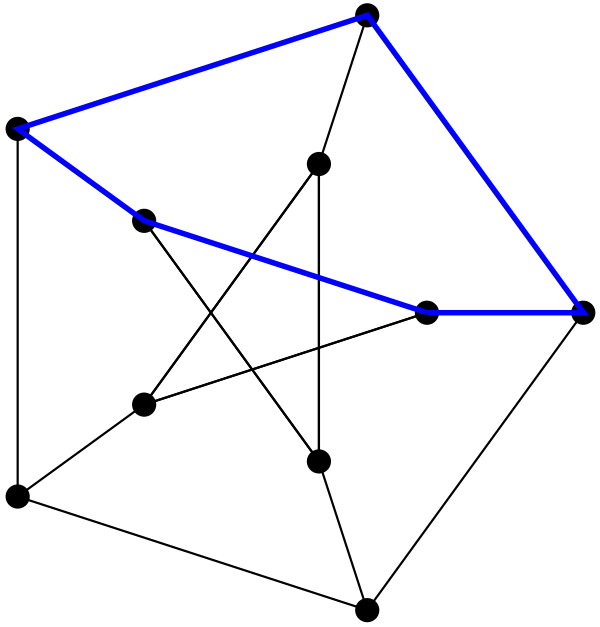


FIGURE : Le code des cycles du graphe de Petersen est un code $[15, 6, 5]$

- En bleu : un cycle

Le graphe de Petersen

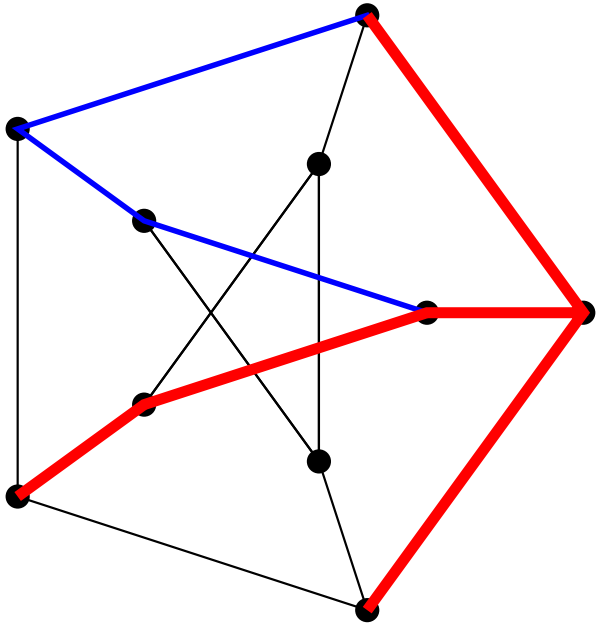


FIGURE : Le code des cycles du graphe de Petersen est un code $[15, 6, 5]$

- En bleu : un cycle
- En rouge : un effacement corrible

Le graphe de Petersen

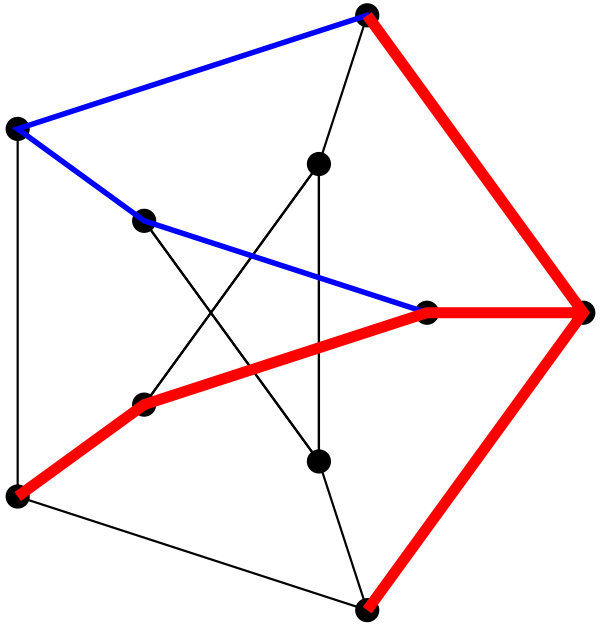


FIGURE : Le code des cycles du graphe de Petersen est un code $[15, 6, 5]$

- En bleu : un cycle
- En rouge : un effacement corrible

Proposition

Un effacement est corrigible ssi il ne couvre pas de cycle non nul.

Percolation dans $\mathbb{Z}^2$

Chaque arête est rouge avec proba p et noire avec proba $1-p$.

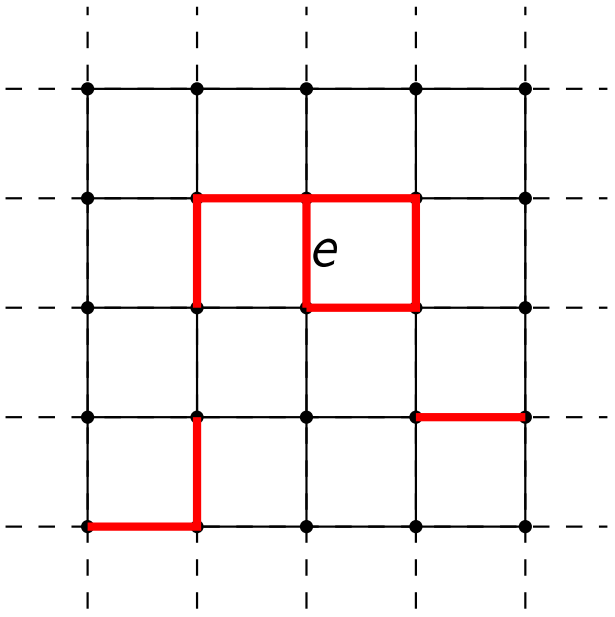


FIGURE : Un évènement avec une composante rouge finie $\mathcal{E}(e)$

Percolation dans $\mathbb{Z}^2$

Question : Quel est la probabilité P_p telle que $\mathcal{E}(e)$ est infini ?

Définition

La probabilité critique est a valeur p_c telle que :

- $P_p = 0$ *lorsque* $p < p_c$,
- $P_p > 0$ *lorsque* $p > p_c$.

Théorème (H. Kesten, 1980 - conjecturé 20 ans avant)

Dans le pavage carré, on a : $p_c = 1/2$.

Nous allons utiliser la théorie de l'information quantique pour borner p_c pour des graphes hyperboliques.

Codes CSS

$$\text{Code quantique } = \begin{cases} \mathbf{H}_X \in M_{r_X,n}(\mathbb{F}_2) \\ \mathbf{H}_Z \in M_{r_Z,n}(\mathbb{F}_2) \\ \text{orthogonalité entre les lignes de } \mathbf{H}_X \text{ et } \mathbf{H}_Z \end{cases}$$

$C_X = \operatorname{Ker} \mathbf{H}_X$ et $C_Z = \operatorname{Ker} \mathbf{H}_Z$

- Les mots quantiques : C_Z modulo $C_X^\perp$ et C_X modulo $C_Z^\perp$
- La dimension : $k = n - \operatorname{rg} \mathbf{H}_X - \operatorname{rg} \mathbf{H}_Z$
- La distance : $d = \inf\{w(x) \mid x \in C_X \backslash C_Z^\perp \cup C_Z \backslash C_X^\perp\}$
- Une erreur quantique $= (E_X, E_Z) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$.
  Particularité quantique : Les erreurs de $C_Z^\perp$ et $C_X^\perp$ n'ont aucun effet

Le code Torique de Kitaev

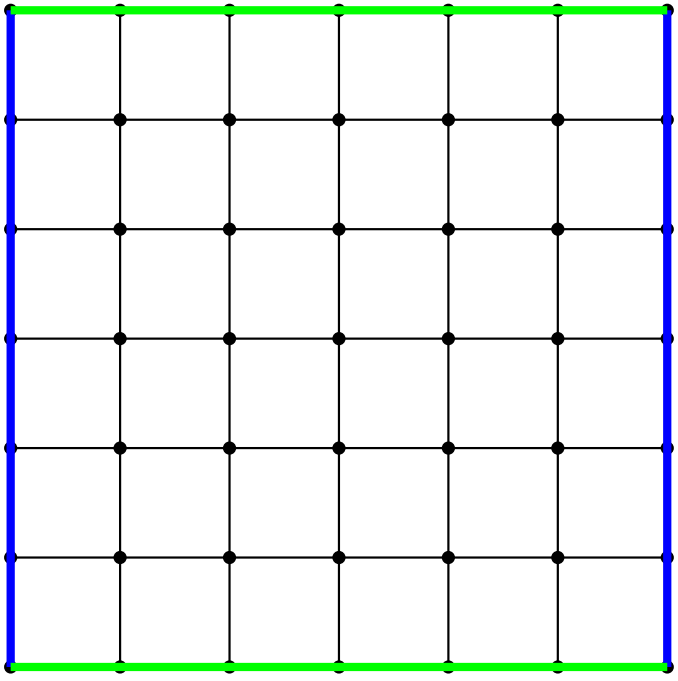
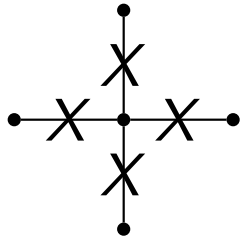


FIGURE : Un pavage carré du tore

Lignes de $\mathbf{H}_X =$ 

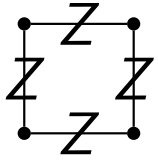
Lignes de $\mathbf{H}_Z =$ 

FIGURE : Générateurs du code de Kitaev

- C_X = les cycles
- $C_Z^{\perp}$ = sommes de faces
- mots quantiques = les cycles modulo les faces (= classes d'homologie)

Le code Torique de Kitaev

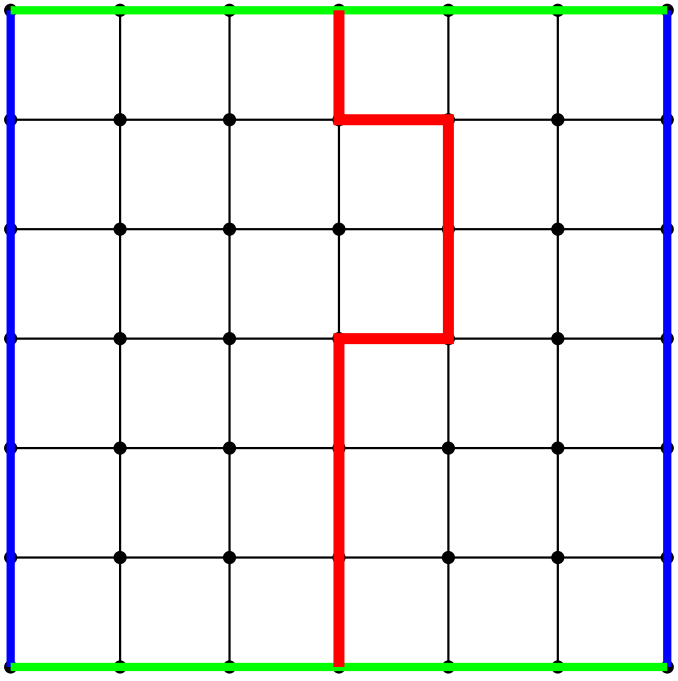


FIGURE : Un pavage carré du tore

- C_X = les cycles
- $C_Z^{\perp}$ = sommes de faces
- mots quantiques = les cycles modulo les faces (= classes d'homologie)

Lignes de $\mathbf{H}_X =$

Lignes de $\mathbf{H}_Z =$

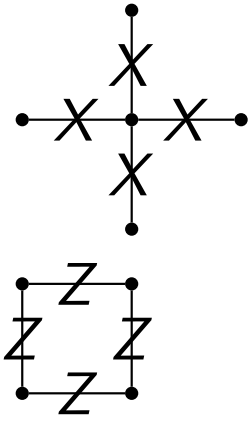


FIGURE : Générateurs du code de Kitaev

Le code Torique de Kitaev

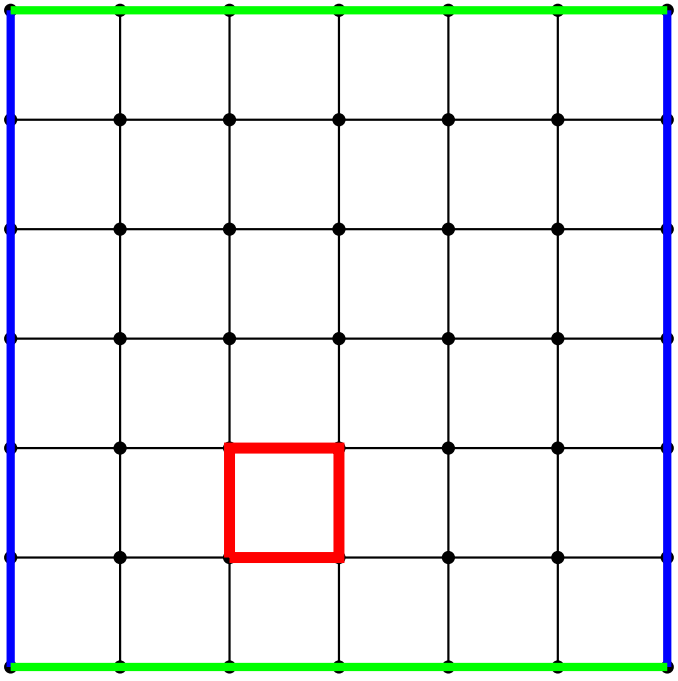


FIGURE : Un pavage carré du tore

- C_X = les cycles
- $C_Z^{\perp}$ = sommes de faces
- mots quantiques = les cycles modulo les faces (= classes d'homologie)

Lignes de $\mathbf{H}_X =$

Lignes de $\mathbf{H}_Z =$

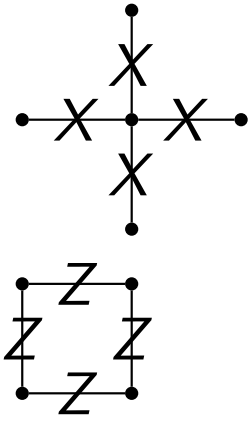


FIGURE : Générateurs du code de Kitaev

Le code Torique de Kitaev

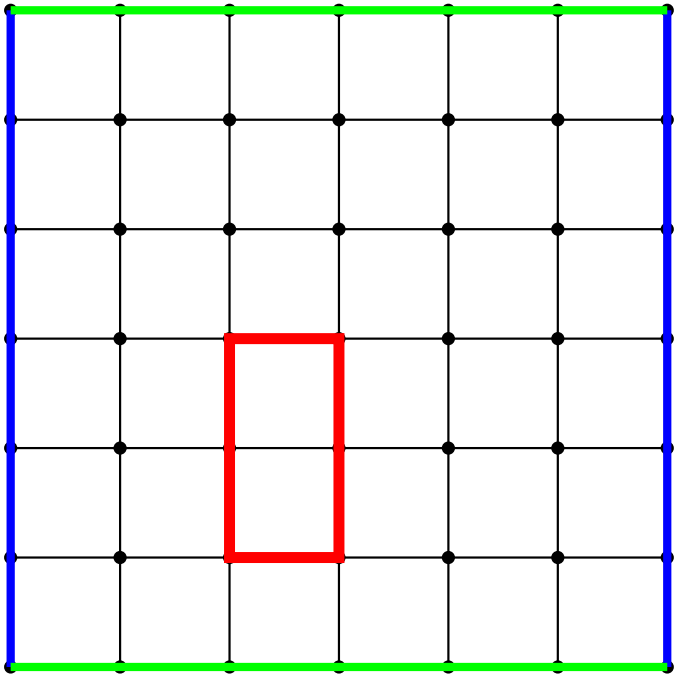
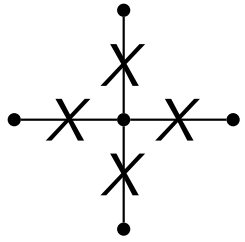


FIGURE : Un pavage carré du tore

Lignes de $\mathbf{H}_X =$ 

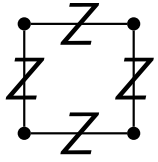
Lignes de $\mathbf{H}_Z =$ 

FIGURE : Générateurs du code de Kitaev

- C_X = les cycles
- $C_Z^{\perp}$ = sommes de faces
- mots quantiques = les cycles modulo les faces (= classes d'homologie)

Le code Torique de Kitaev

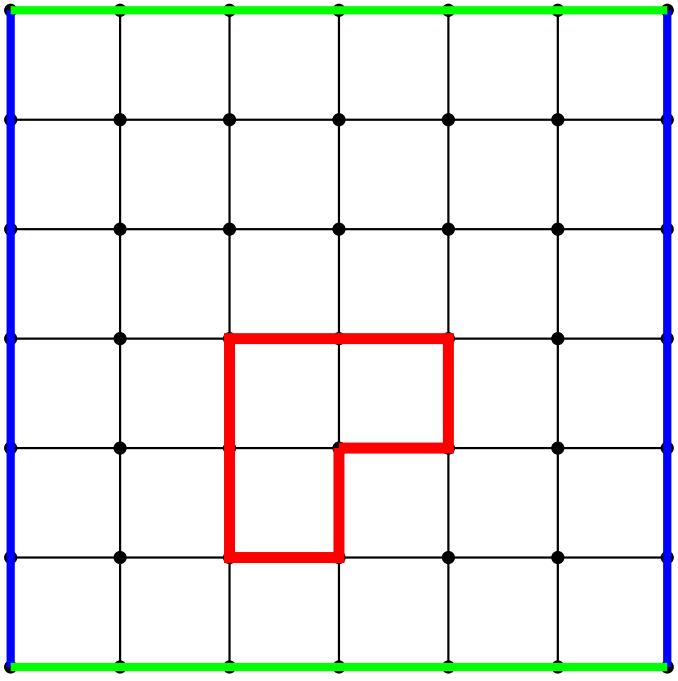
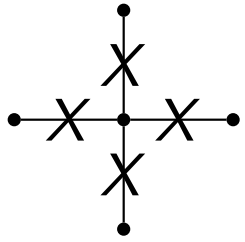


FIGURE : Un pavage carré du tore

Lignes de $\mathbf{H}_X =$ 

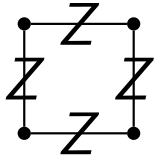
Lignes de $\mathbf{H}_Z =$ 

FIGURE : Générateurs du code de Kitaev

- C_X = les cycles
- $C_Z^{\perp}$ = sommes de faces
- mots quantiques = les cycles modulo les faces (= classes d'homologie)

Le code Torique de Kitaev

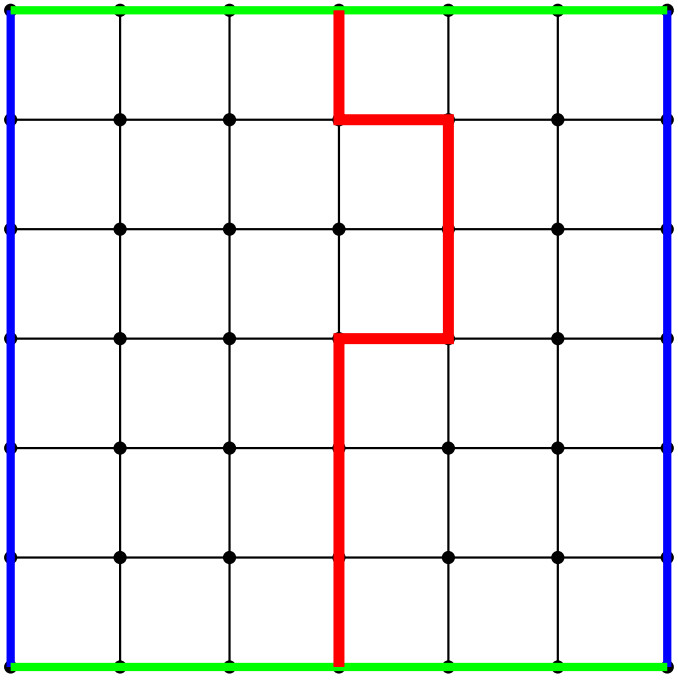


FIGURE : Un pavage carré du tore

- C_X = les cycles
- $C_Z^{\perp}$ = sommes de faces
- mots quantiques = les cycles modulo les faces (= classes d'homologie)

Lignes de $\mathbf{H}_X =$

Lignes de $\mathbf{H}_Z =$

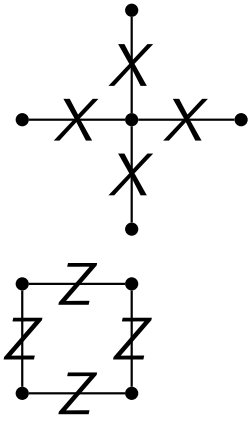


FIGURE : Générateurs du code de Kitaev

Le code Torique de Kitaev

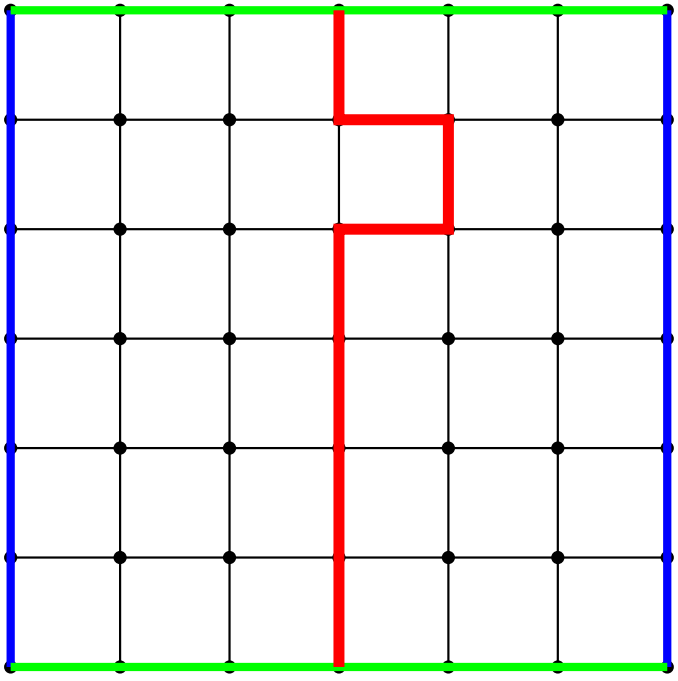
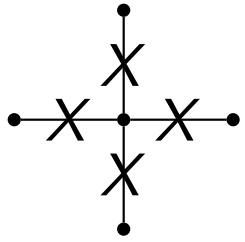


FIGURE : Un pavage carré du tore

Lignes de $\mathbf{H}_X =$ 

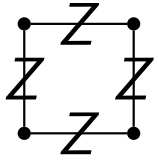
Lignes de $\mathbf{H}_Z =$ 

FIGURE : Générateurs du code de Kitaev

- C_X = les cycles
- $C_Z^{\perp}$ = sommes de faces
- mots quantiques = les cycles modulo les faces (= classes d'homologie)

Le code Torique de Kitaev

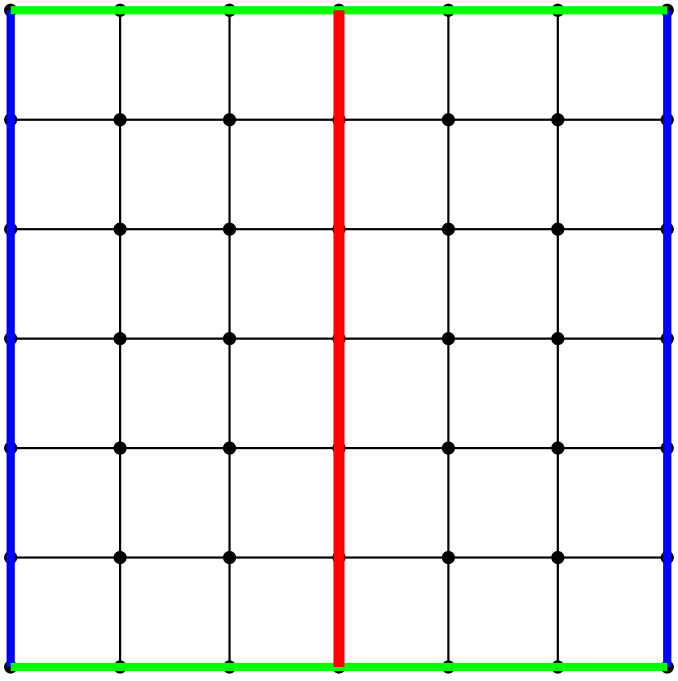
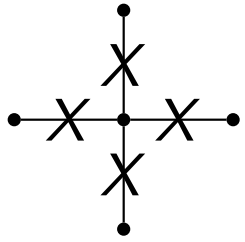


FIGURE : Un pavage carré du tore

Lignes de $\mathbf{H}_X =$ 

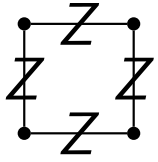
Lignes de $\mathbf{H}_Z =$ 

FIGURE : Générateurs du code de Kitaev

- C_X = les cycles
- $C_Z^{\perp}$ = sommes de faces
- mots quantiques = les cycles modulo les faces (= classes d'homologie)

Le code Torique de Kitaev

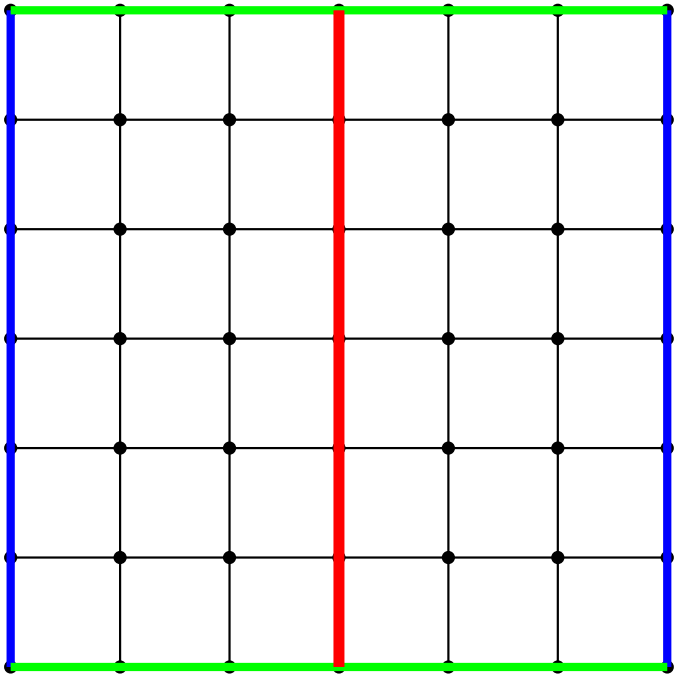


FIGURE : Un pavage carré du tore

- C_X = les cycles
- $C_Z^{\perp}$ = sommes de faces
- mots quantiques = les cycles modulo les faces (= classes d'homologie)

Lignes de $\mathbf{H}_X =$

Lignes de $\mathbf{H}_Z =$

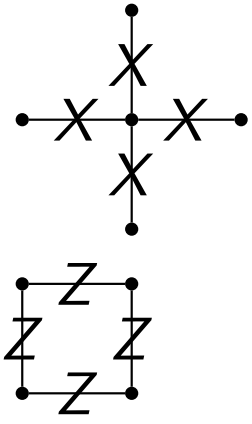


FIGURE : Générateurs du code de Kitaev

Dans le pavage $m \times m$:

- n = nb d'arêtes $= 2m^2$
- d = longueur min d'un cycle non somme de faces de G ou $G^* = m$
- matrices de type $(2, 4)$

Distance minimale des codes topologiques

D'où vient ce $d = O(n^{1/2})$?

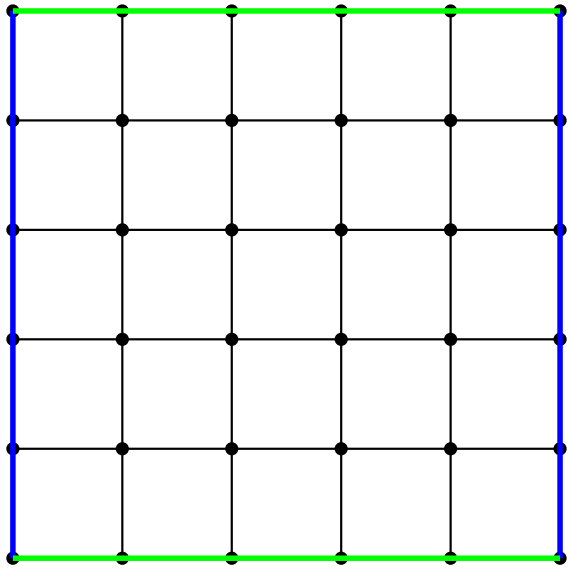


FIGURE : Une boule du pavage carré du tore

Distance minimale des codes topologiques

D'où vient ce $d = O(n^{1/2})$?

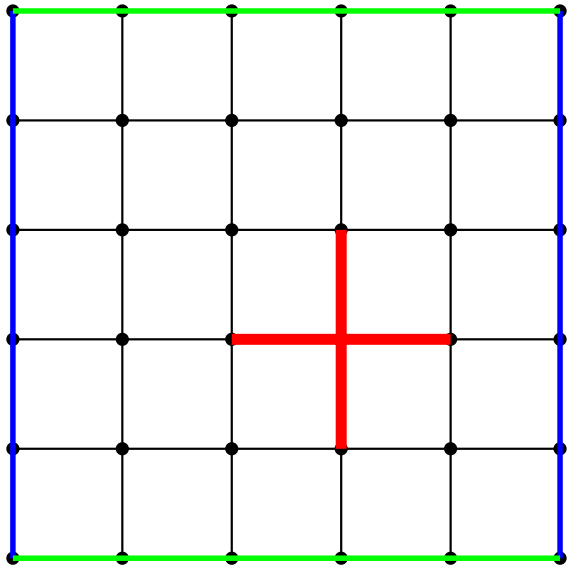


FIGURE : Une boule du pavage carré du tore

Distance minimale des codes topologiques

D'où vient ce $d = O(n^{1/2})$?

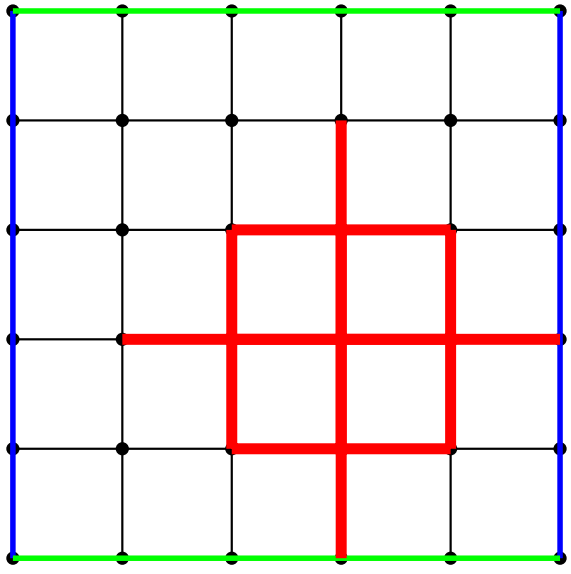


FIGURE : Une boule du pavage carré du tore

Distance minimale des codes topologiques

D'où vient ce $d = O(n^{1/2})$?

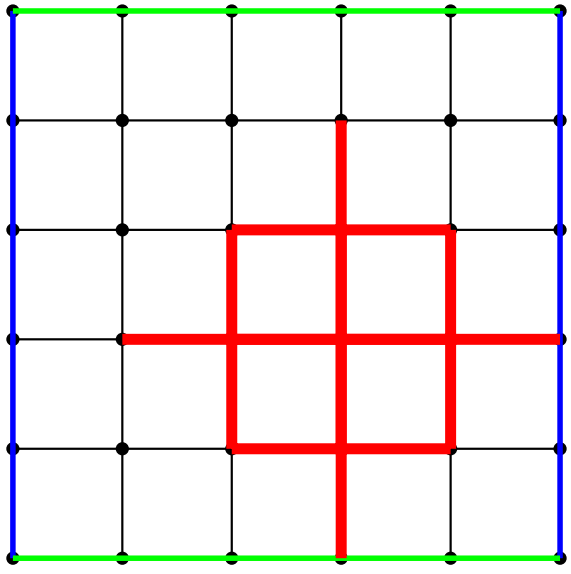


FIGURE : Une boule du pavage carré du tore

pas d'identification jusqu'au rayon $(m-1)/2$ dans le pavage $m \times m$

Distance minimale des codes topologiques

D'où vient ce $d = O(n^{1/2})$?

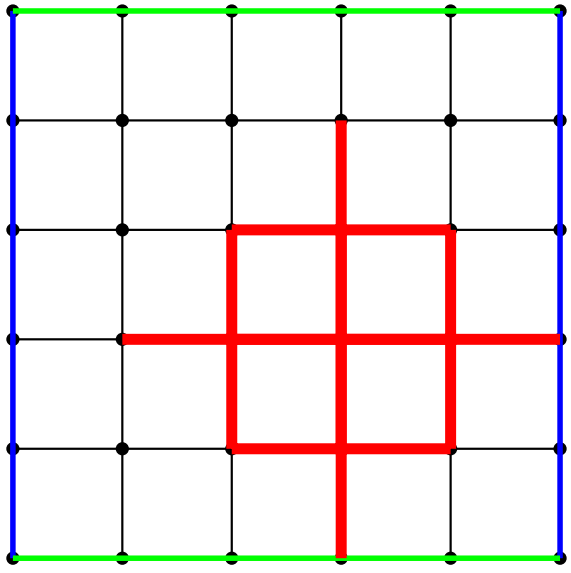


FIGURE : Une boule du pavage carré du tore

pas d'identification jusqu'au rayon $(m-1)/2$ dans le pavage $m \times m$
$\Rightarrow$ cette boule est planaire
$\Rightarrow$ tt cycle inclus dans une telle boule est somme de faces
$\Rightarrow$ ne compte pas dans d.

Correction des effacements quantiques

Les qubits correspondent aux arêtes

$$\text{qubit effacé} \longleftrightarrow \begin{cases} \text{erreur aléatoire } I, X, Y, Z \\ \text{position connue} \end{cases}$$

Par le canal à effacement quantique chaque qubit est effacé, indépendamment, avec probabilité p.

Proposition

La capacité du canal à effacement quantique est $1 - 2p$.

Proposition

Si $p < p_c = 1/2$ *alors la probabilité d'erreur après décodage avec le code torique tend vers 0.*

Correction des effacements quantiques

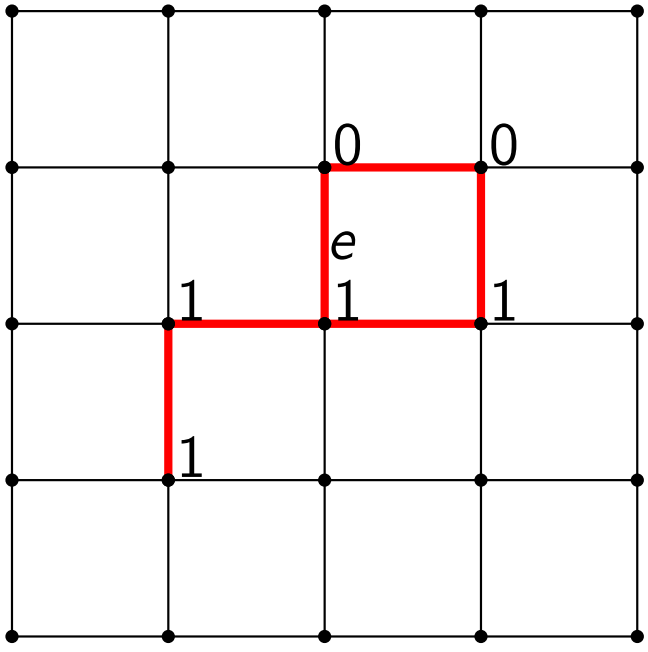


FIGURE : La composante effacée $\mathcal{E}(e)$ et son syndrome dans G

- En rouge : les arêtes effacées
- Le syndrome est le bord des arêtes portant un Z.
- Nous cherchons à identifier les Z à partir du syndrome.

On corrige les erreurs en X de la même manière dans le graphe dual.

Lorsque $\mathcal{E}(e)$ est petite, on peut corriger cet effacement.

Correction des effacements quantiques

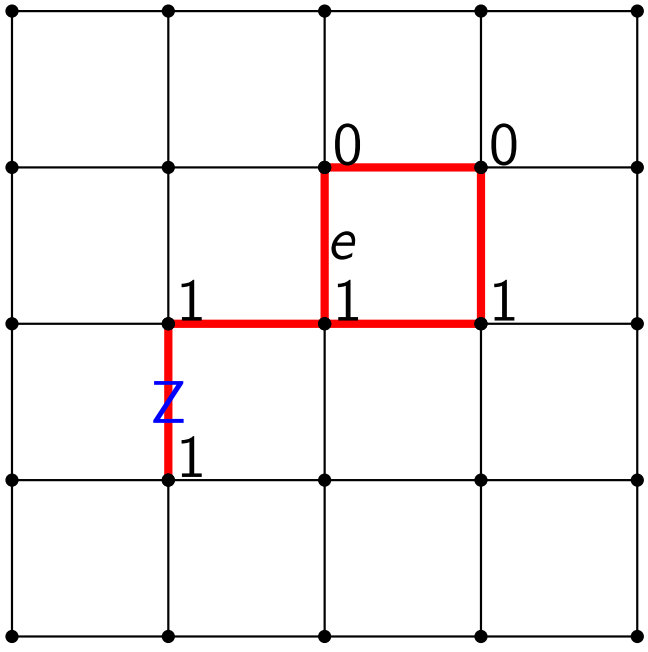


FIGURE : La composante effacée $\mathcal{E}(e)$ et son syndrome dans G

- En rouge : les arêtes effacées
- Le syndrome est le bord des arêtes portant un Z.
- Nous cherchons à identifier les Z à partir du syndrome.

On corrige les erreurs en X de la même manière dans le graphe dual.

Lorsque $\mathcal{E}(e)$ est petite, on peut corriger cet effacement.

Correction des effacements quantiques

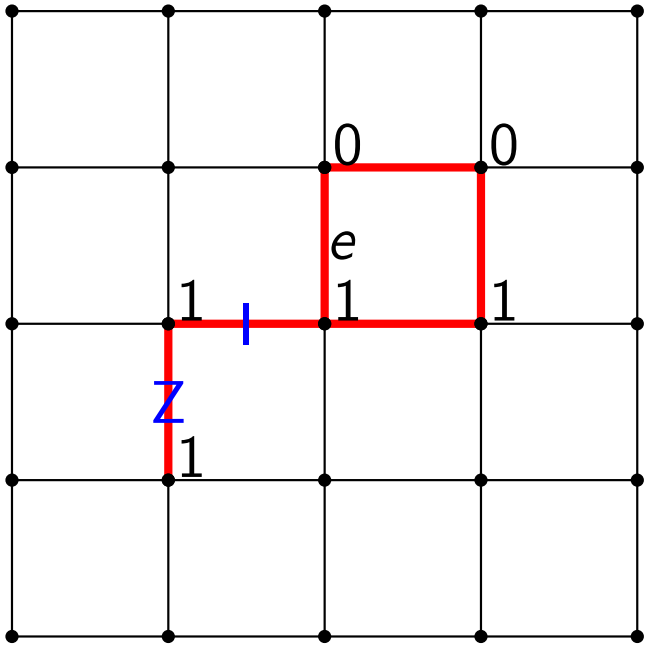


FIGURE : La composante effacée $\mathcal{E}(e)$ et son syndrome dans G

Lorsque $\mathcal{E}(e)$ est petite, on peut corriger cet effacement.

- En rouge : les arêtes effacées
- Le syndrome est le bord des arêtes portant un Z.
- Nous cherchons à identifier les Z à partir du syndrome.

On corrige les erreurs en X de la même manière dans le graphe dual.

Correction des effacements quantiques

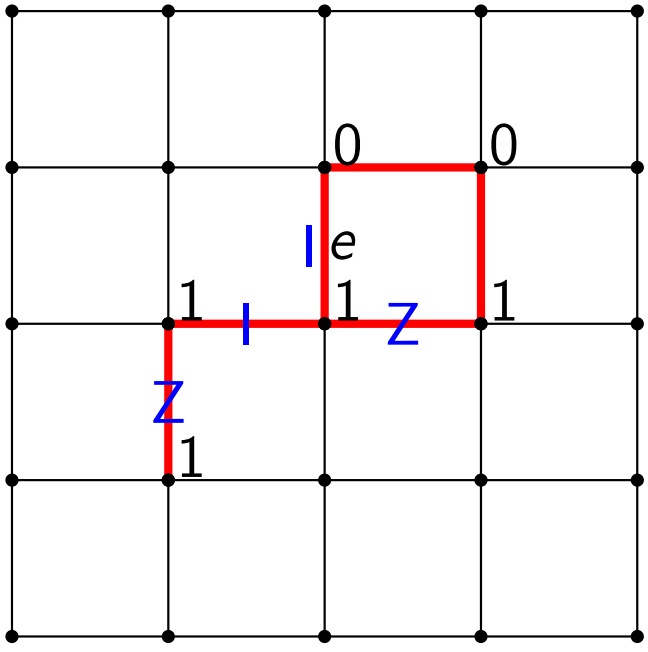


FIGURE : La composante effacée $\mathcal{E}(e)$ et son syndrome dans G

Lorsque $\mathcal{E}(e)$ est petite, on peut corriger cet effacement.

- En rouge : les arêtes effacées
- Le syndrome est le bord des arêtes portant un Z.
- Nous cherchons à identifier les Z à partir du syndrome.

On corrige les erreurs en X de la même manière dans le graphe dual.

Correction des effacements quantiques

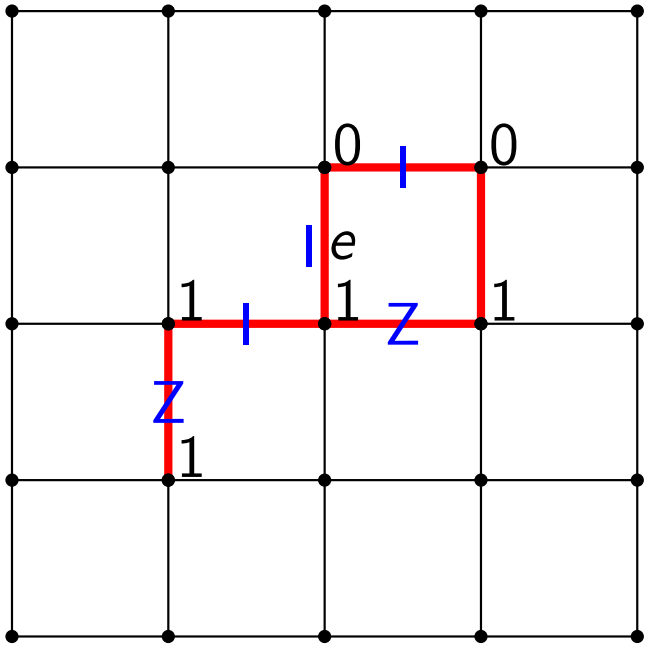


FIGURE : La composante effacée $\mathcal{E}(e)$ et son syndrome dans G

Lorsque $\mathcal{E}(e)$ est petite, on peut corriger cet effacement.

- En rouge : les arêtes effacées
- Le syndrome est le bord des arêtes portant un Z.
- Nous cherchons à identifier les Z à partir du syndrome.

On corrige les erreurs en X de la même manière dans le graphe dual.

Correction des effacements quantiques

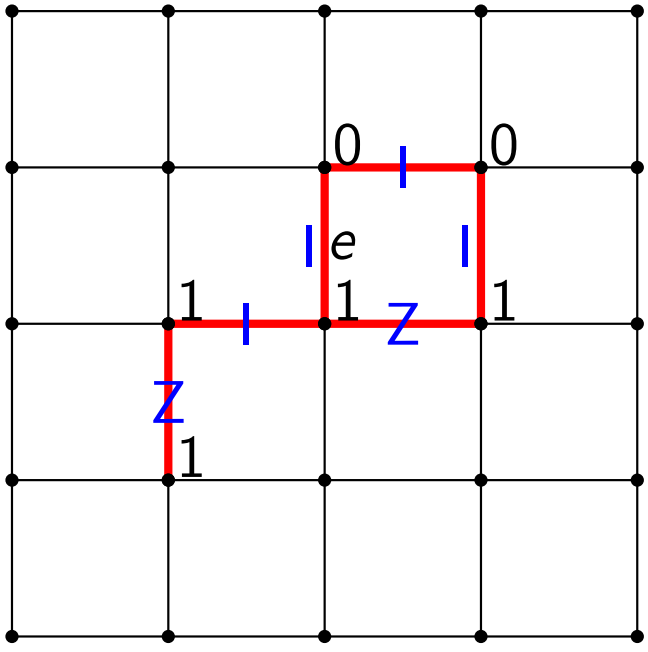


FIGURE : La composante effacée $\mathcal{E}(e)$ et son syndrome dans G

Lorsque $\mathcal{E}(e)$ est petite, on peut corriger cet effacement.

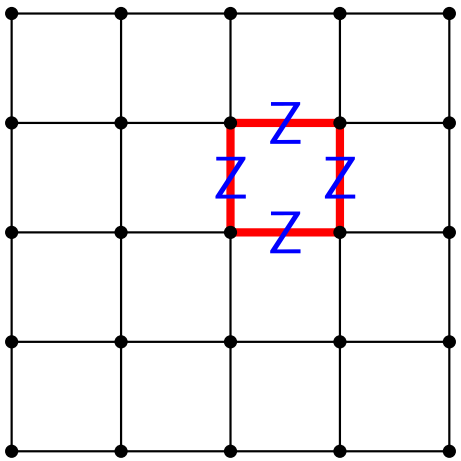
- En rouge : les arêtes effacées
- Le syndrome est le bord des arêtes portant un Z.
- Nous cherchons à identifier les Z à partir du syndrome.

On corrige les erreurs en X de la même manière dans le graphe dual.

Correction des effacements quantiques

Problème : Il y a deux correction possibles.

$\longrightarrow$ Elles diffèrent d'une somme de faces.



$\longrightarrow$ Ces erreurs sont triviales donc on a bien corrigé

Un effacement problématique

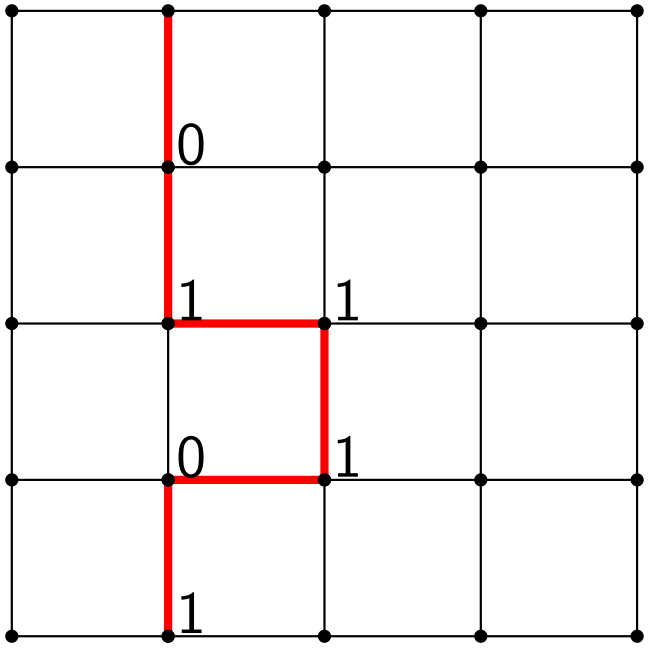


FIGURE : Un effacement problématique

Un effacement problématique

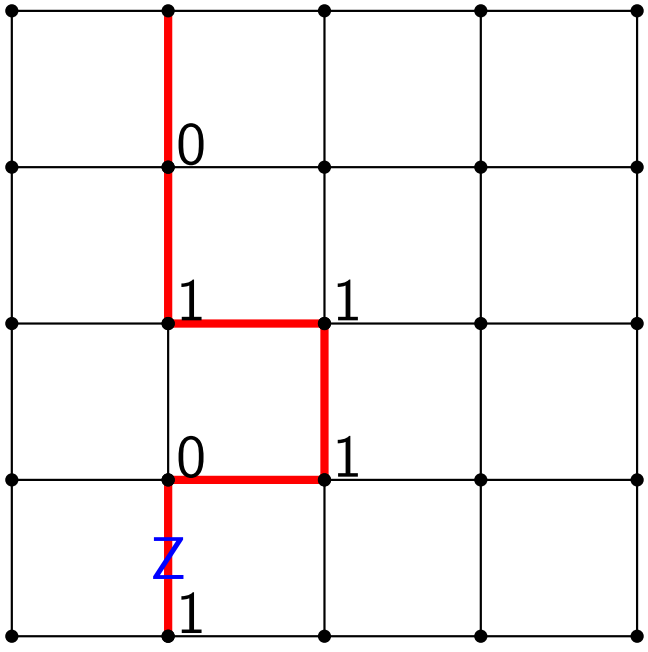


FIGURE : Un effacement problématique

Un effacement problématique

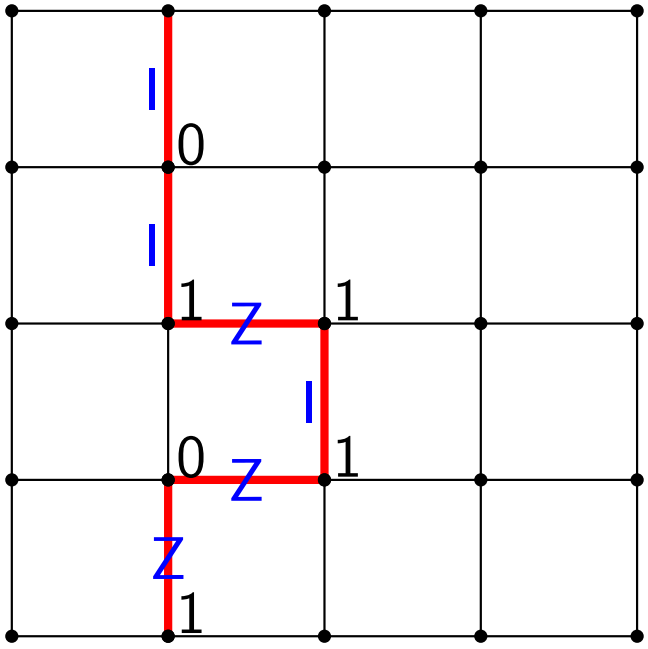


FIGURE : Un effacement problématique

Un effacement problématique

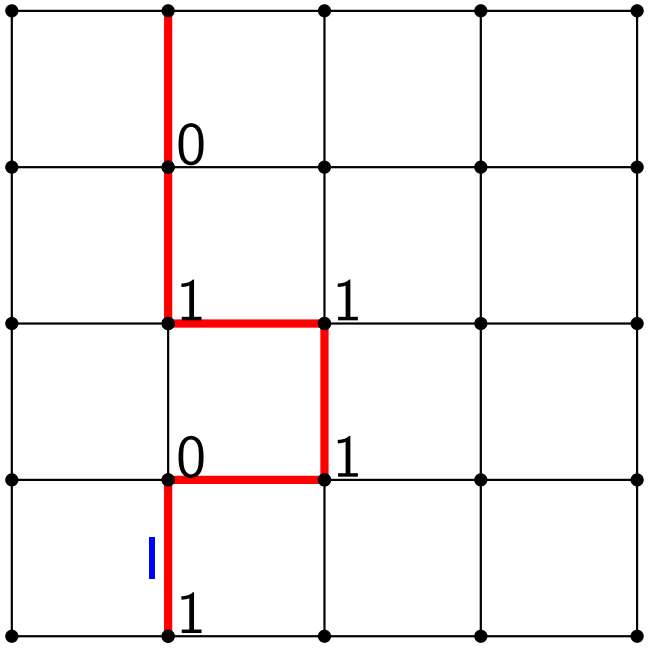


FIGURE : Un effacement problématique

Un effacement problématique

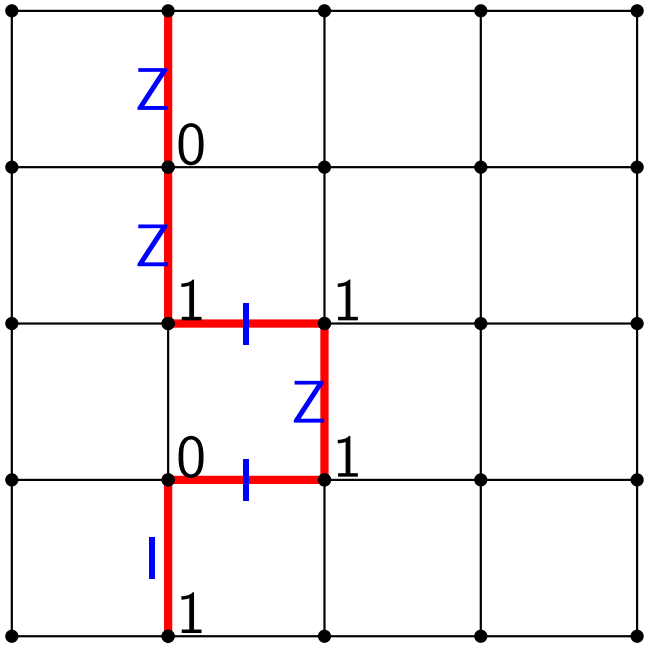


FIGURE : Un effacement problématique

Un effacement problématique

Probléme : Il y a deux corrections possibles

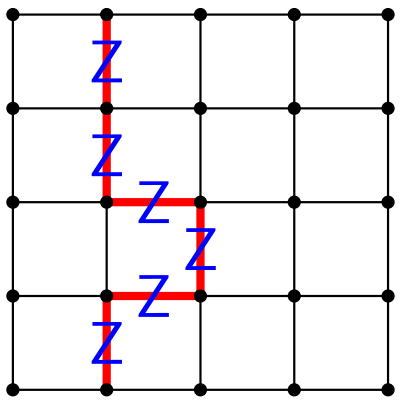


FIGURE : Une erreur quantique non triviale

$\longrightarrow$ Elles n'ont pas le même effet sur le code quantique

$\longrightarrow$ On ne peut pas identifier l'erreur

Un effacement problématique

Pour résumer :

p_c est un seuil pour la percolation dans $\mathbb{Z}^2$.

$\longrightarrow$ seuil pour les effacements

- $p < p_c \Rightarrow$ on peut corriger
- $p > p_c \Rightarrow$ l'information quantique est perdue

Hyperbolic graphs

Objectif : relier percolation et probabilité d'effacement pour d'autres graphes.

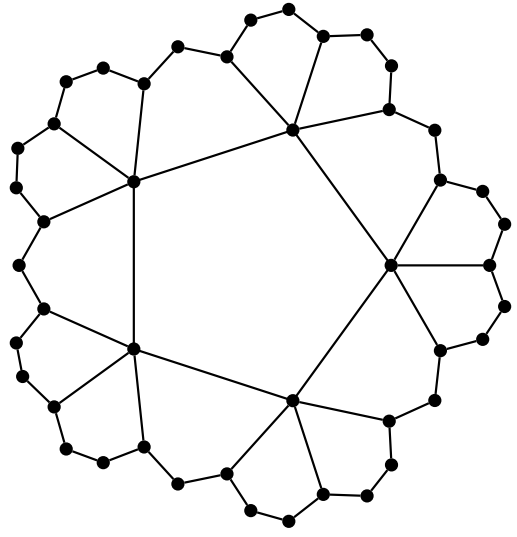


FIGURE : Structure locale du pavage 5-régulier $G(5)$

Définition

Soit $G(m)$ le pavage planaire infini m-régulier.

Hyperbolic graphs

La détermination de p_c est difficile dans $G(m)$.
Étudié par Benjamini, Schramm en 1996,
par Baek, Kim, Minnhagen in 2009.

Borne connue :

Proposition

Dans le graphe $G(m)$, on a :

$$\frac{1}{m-1} \leq p_c \leq 1 - \frac{1}{m-1}.$$

Grâce à la théorie de l'information quantique, nous allons borner p_c.

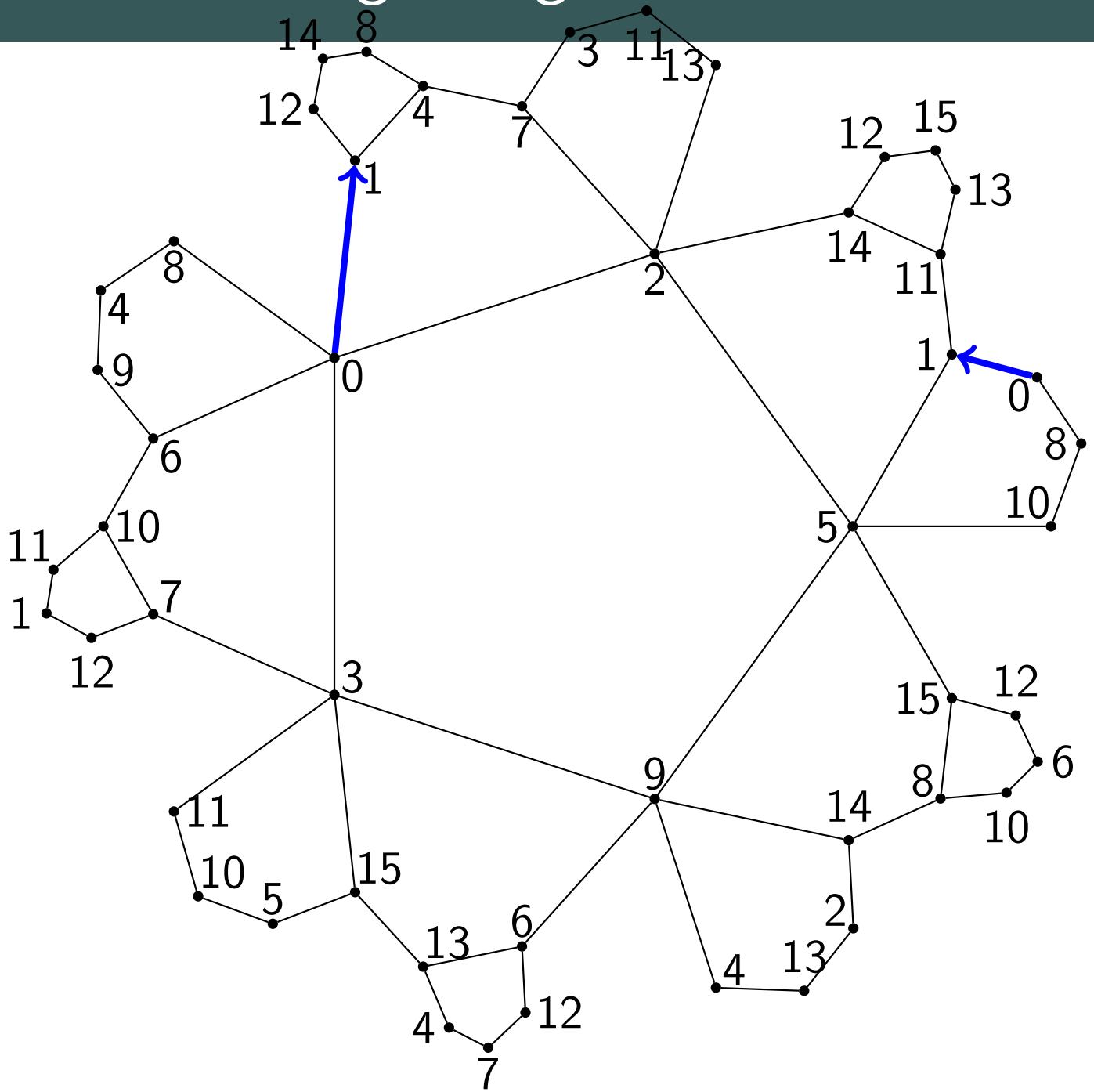
Hyperbolic graphs

Théorème (J. Siran - 2001)

$\forall m \geq 5$ et $\forall r \in \mathbb{N}$, il existe un graphe fini m-régulier $G_r(m)$ tel que toute boule de rayon r est planaire.

$\longrightarrow$ A partir de ces graphes finis, on peut définir des codes quantiques.

Une surface de genre $g = 5$



Un code quantique $[[40, 10, 4]]$

$$\mathbf{H}_X = \begin{pmatrix} 0 & 1 & 2 & 3 & 8 \\ 1 & 4 & 5 & 11 & 20 \\ 2 & 6 & 7 & 14 & 25 \\ 0 & 9 & 10 & 18 & 28 \\ 5 & 12 & 13 & 22 & 32 \\ 4 & 7 & 15 & 21 & 31 \\ 3 & 16 & 17 & 27 & 36 \\ 6 & 10 & 13 & 19 & 23 \\ 8 & 12 & 24 & 33 & 38 \\ 9 & 15 & 17 & 22 & 26 \\ 16 & 19 & 21 & 24 & 29 \\ 11 & 28 & 29 & 30 & 35 \\ 20 & 23 & 27 & 34 & 39 \\ 14 & 32 & 35 & 36 & 37 \\ 25 & 26 & 30 & 33 & 34 \\ 18 & 31 & 37 & 38 & 39 \end{pmatrix}$$

$$\mathbf{H}_Z = \begin{pmatrix} 0 & 2 & 7 & 9 & 15 \\ 1 & 2 & 5 & 6 & 13 \\ 0 & 3 & 10 & 16 & 19 \\ 1 & 4 & 8 & 21 & 24 \\ 3 & 8 & 12 & 17 & 22 \\ 4 & 7 & 11 & 25 & 30 \\ 5 & 12 & 20 & 33 & 34 \\ 6 & 10 & 14 & 28 & 35 \\ 9 & 17 & 18 & 36 & 37 \\ 11 & 19 & 20 & 23 & 29 \\ 13 & 23 & 27 & 32 & 36 \\ 14 & 22 & 25 & 26 & 32 \\ 15 & 26 & 31 & 33 & 38 \\ 16 & 24 & 27 & 38 & 39 \\ 18 & 21 & 28 & 29 & 31 \\ 30 & 34 & 35 & 37 & 39 \end{pmatrix}$$

Codes hyperboliques

Pour construire un code hyperbolique $Q_r(m)$:

- $\mathbf{H}_X$ est la matrice d'incidence du graphe $G_r(m)$,
- $\mathbf{H}_Z$ est la matrice des faces.

Avec cette construction :

Proposition

- $n = |E|$ *est le nombre de qubits,*
- $k = \left(1 - \frac{4}{m}\right) n + 2$,
- d *est logarithmique en* n.

Codes hyperboliques

- $\mathbf{H}_X$ est la matrice d'incidence du graphe $G_r(m)$,
- $\mathbf{H}_Z$ est la matrice des faces.

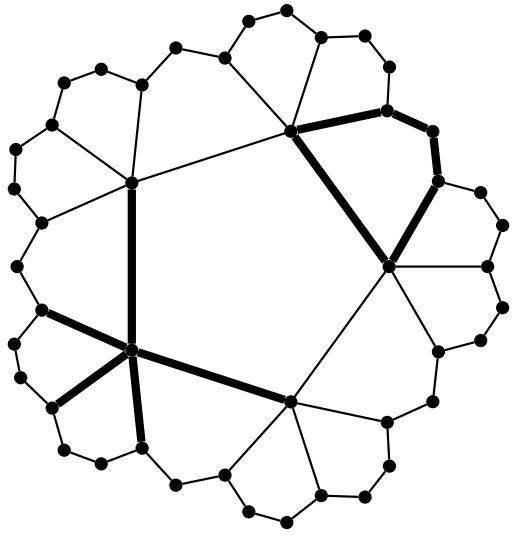


FIGURE : Les relations d'orthogonalité

Ce sont des codes LDPC.

Percolation et capacité

Argument : si $p < p_c$ alors $1 - \frac{4}{m} \leq R \leq 1 - 2p$

Théorème (D., Zémor - 2010)

Le seuil critique du graphe $G(m)$ vérifie :

$$p_c \leq \frac{2}{m}.$$

Percolation et capacité

IDÉE DE LA PREUVE :

Si $p < p_c$ alors $\mathcal{E}(e)$ est petite.
On peut déterminer l'erreur qui touche e.
$\longrightarrow$ La probabilité d'erreur par qubit tend vers 0, lorsque $r \to \infty$.

On veut que la probabilité d'erreur tende vers 0.
On aoute quelques lignes aux matrices $\mathbf{H}_X$ et $\mathbf{H}_Z$.
$\longrightarrow$ Il existe $Q'_r(m) \subset Q_r(m)$ avec $\begin{cases} \frac{k}{n} \text{ goes to } 1 - \frac{4}{m}, \\ d \text{ proportional to } n. \end{cases}$

Percolation et capacité

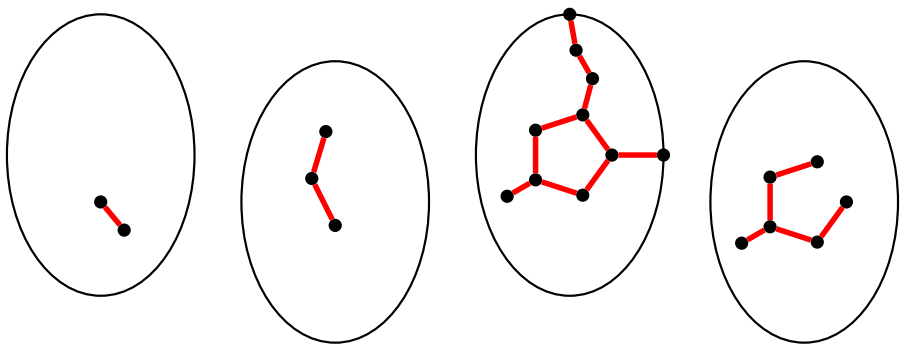


FIGURE : Les composantes connexes d'un effacement pour $p < p_c$

Percolation et capacité

- Avec le syndrome de $Q_r(m)$, on peut corriger les petites composantes de l'effacement.

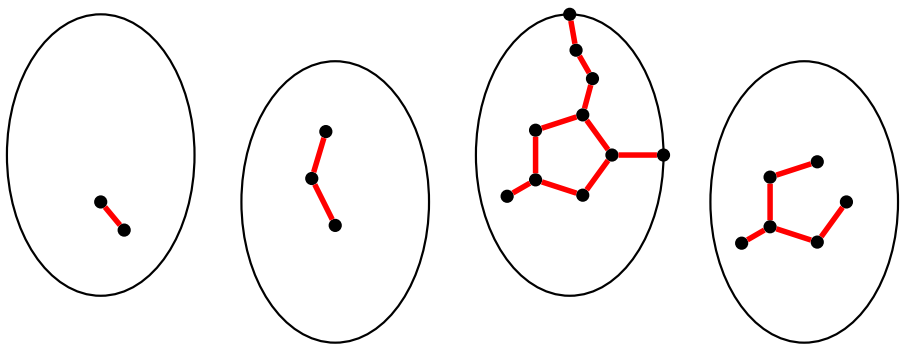


FIGURE : Les composantes connexes d'un effacement pour $p < p_c$

Percolation et capacité

- Avec le syndrome de $Q_r(m)$, on peut corriger les petites composantes de l'effacement.
- Il reste une partie problématique $\mathcal{E}_P$.

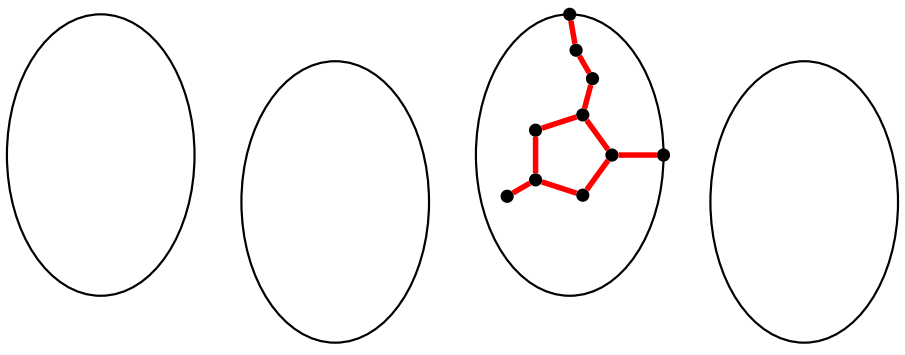


FIGURE : Les composantes connexes d'un effacement pour $p < p_c$

Percolation et capacité

- Avec le syndrome de $Q_r(m)$, on peut corriger les petites composantes de l'effacement.
- Il reste une partie problématique $\mathcal{E}_P$.
- Si $p < p_c$ et r est grand, $|\mathcal{E}_P|$ est une petite fraction de n.

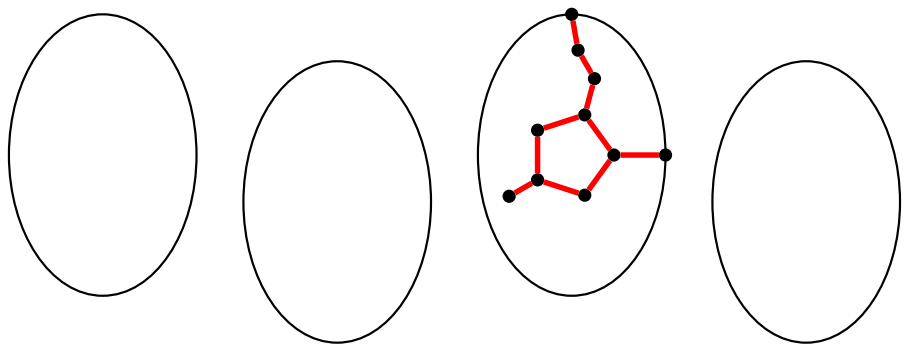


FIGURE : Les composantes connexes d'un effacement pour $p < p_c$

Percolation et capacité

- Avec le syndrome de $Q_r(m)$, on peut corriger les petites composantes de l'effacement.
- Il reste une partie problématique $\mathcal{E}_P$.
- Si $p < p_c$ et r est grand, $|\mathcal{E}_P|$ est une petite fraction de n.
- Avec $Q'_r(m)$ on peut corriger $\mathcal{E}_P$ avec proba élevée.

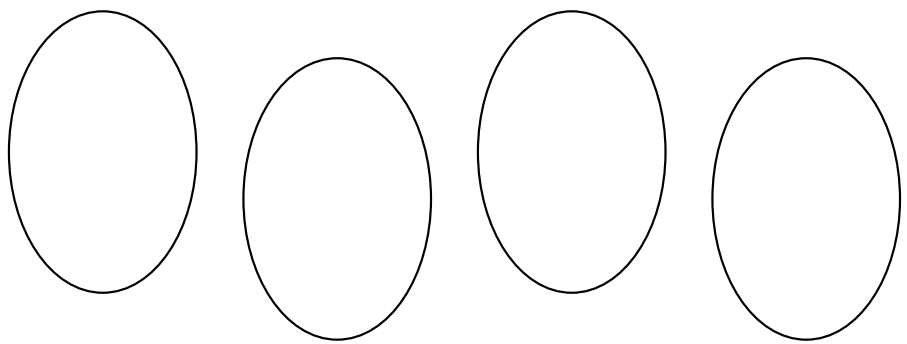


FIGURE : Les composantes connexes d'un effacement pour $p < p_c$

Percolation et capacité

Si $p < p_c$, la probabilité d'erreur tend vers 0.

Proposition (Bennett, DiVincenzo, Smolin - 1997)

La capacité du canal à effacement quantique de probabilité p est $1 - 2p$.

$\longrightarrow$ borne supérieure sur le rendement limite de $Q'_r(m)$.

Théorème (D., Zémor - 2010)

La probabilité critique du graphe $G(m)$ vérifie :

$$p_c \leq \frac{2}{m}.$$

Les effacement problématiques

Un effacement classique : $(01010) \mapsto (0??010)$

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$e = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

Les effacement problématiques

Un effacement classique : $(01010) \mapsto (0??010)$

$$H_e = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$e = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

Les effacement problématiques

Un effacement classique : $(01010) \mapsto (0??010)$

$$H_{\bar{e}} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$e = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

Les effacement problématiques

Un effacement classique : $(01010) \mapsto (0??010)$

$$H_{\bar{e}} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$e = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

e est corrigible $\Leftrightarrow$ e ne couvre pas de mot de code $\neq 0$
$\Leftrightarrow \operatorname{rg} H_e = w(e)$

L'analogue quantique :

Proposition

e corrigible $\Leftrightarrow$ e ne couvre pas de cycle non somme de face $\Leftrightarrow$
$\operatorname{rg} \mathbf{H}_X + \operatorname{rg} \mathbf{H}_Z - (\operatorname{rg} \mathbf{H}_{X,\bar{e}} + \operatorname{rg} \mathbf{H}_{Z,\bar{e}} - \operatorname{rg} \mathbf{H}_{X,e} - \operatorname{rg} \mathbf{H}_{Z,e}) = 2w(e)$

Une borne combinatoire sur la capacité

Soit $(\mathbf{H}_{X,t})$ et $(\mathbf{H}_{Z,t})$ définissant une famille de codes quantiques de rendement R.

Théorème (D., Zémor - '12)

Si $P_{err} \to 0$ alors

$$R \leq 1 - 2p - D(p) \leq 1 - 2p,$$

où

$$D(p) = \limsup E_p \left(\frac{\operatorname{rg} \mathbf{H}_{X,\bar{e}} - \operatorname{rg} \mathbf{H}_{X,e}}{n} + \frac{\operatorname{rg} \mathbf{H}_{Z,\bar{e}} - \operatorname{rg} \mathbf{H}_{Z,e}}{n} \right)$$

Une borne combinatoire sur la capacité

Soit $(\mathbf{H}_{X,t})$ et $(\mathbf{H}_{Z,t})$ définissant une famille de codes quantiques de rendement R.

Théorème (D., Zémor - '12)

Si $P_{err} \to 0$ alors

$$R \leq 1 - 2p - D(p) \leq 1 - 2p,$$

où

$$D(p) = \limsup E_p \left(\frac{\operatorname{rg} \mathbf{H}_{X,\bar{e}} - \operatorname{rg} \mathbf{H}_{X,e}}{n} + \frac{\operatorname{rg} \mathbf{H}_{Z,\bar{e}} - \operatorname{rg} \mathbf{H}_{Z,e}}{n} \right)$$

- Pour des matrices quelconques $D(p)$ peut être petit (≈ 0)
- MAIS pour des matrices creuses, cette borne est sous la capacité

But : estimer $D(p)$ pour des matrices creuses

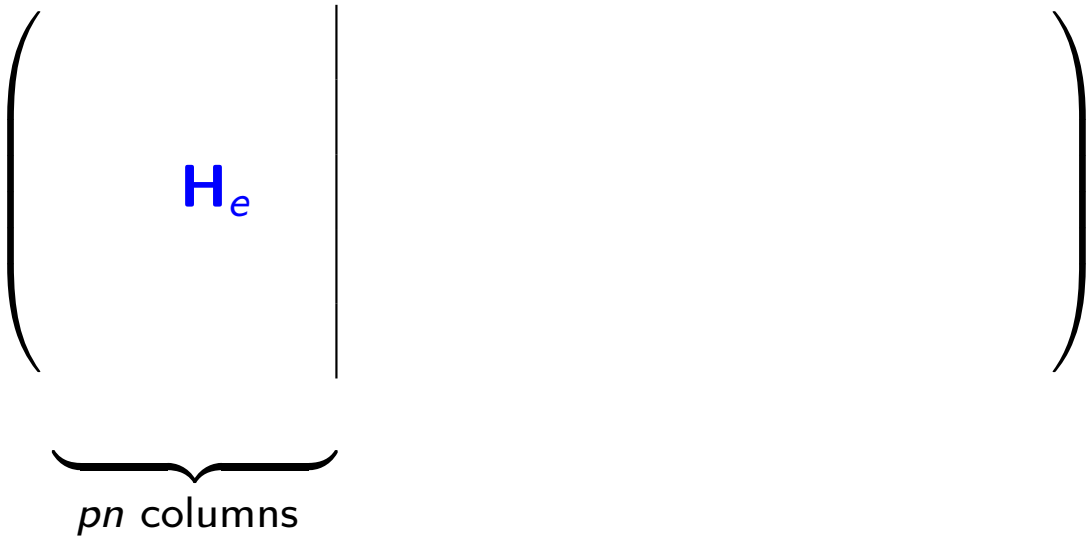
Rang d'une matrice creuse aléatoire

- Typiquement : $\mathbf{H}_e$ est une matrice $r \times np$

Rang d'une matrice creuse aléatoire

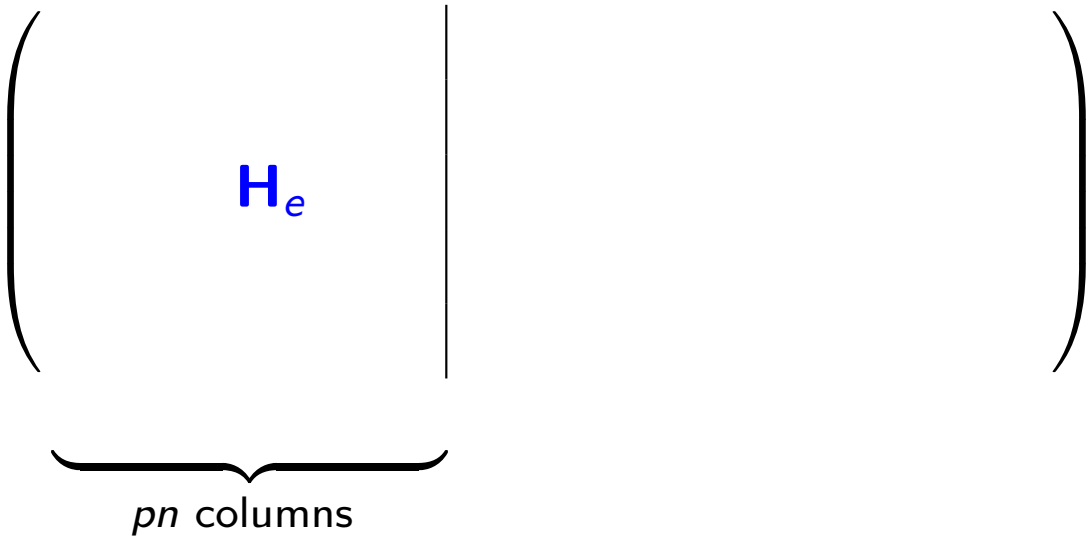
- Typiquement : $\mathbf{H}_e$ est une matrice $r \times np$

Rang d'une matrice creuse aléatoire



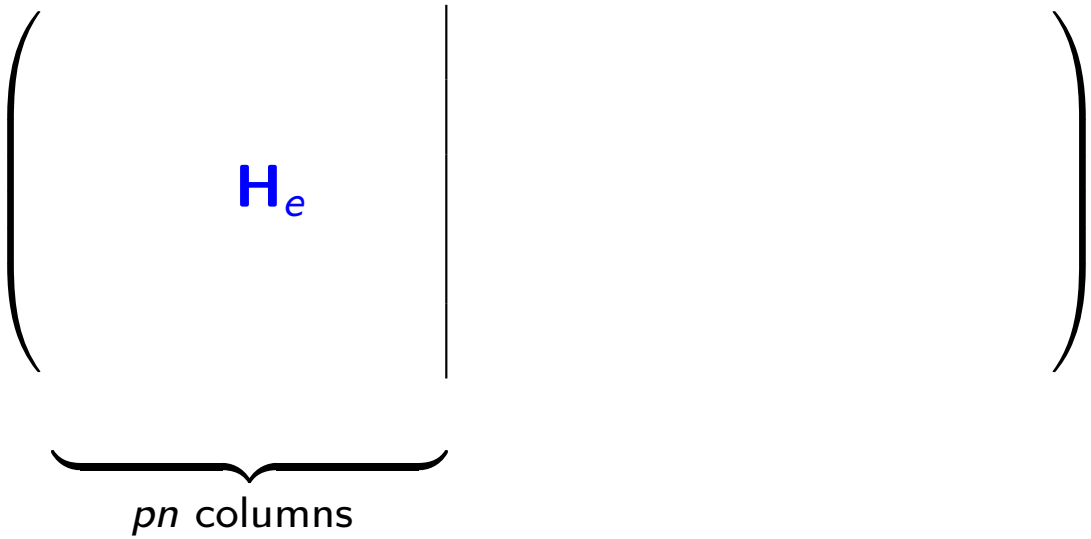
- Typiquement : $\mathbf{H}_e$ est une matrice $r \times np$

Rang d'une matrice creuse aléatoire



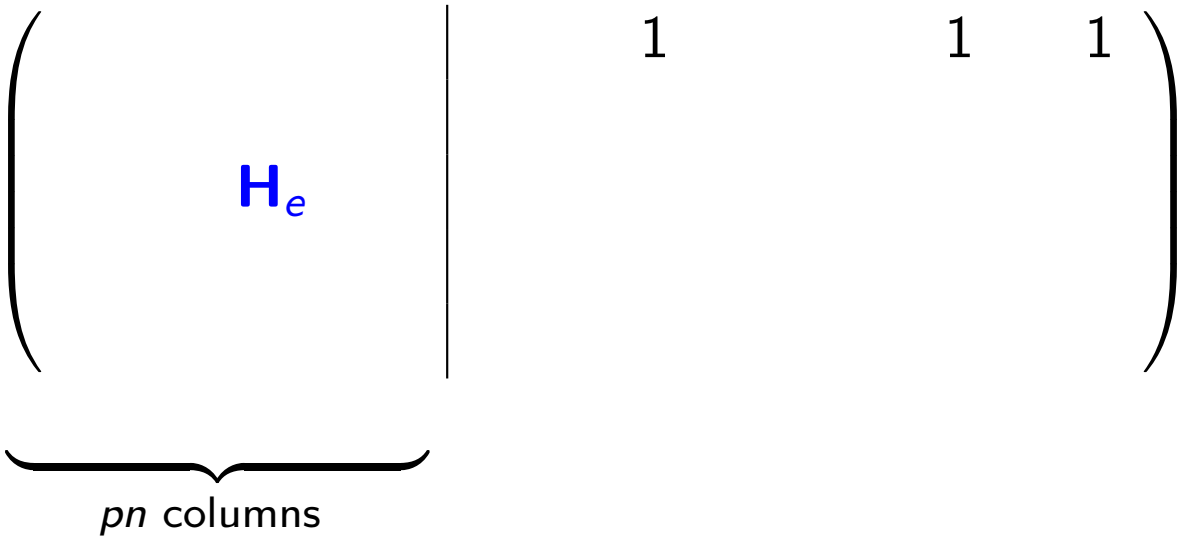
- Typiquement : $\mathbf{H}_e$ est une matrice $r \times np$

Rang d'une matrice creuse aléatoire



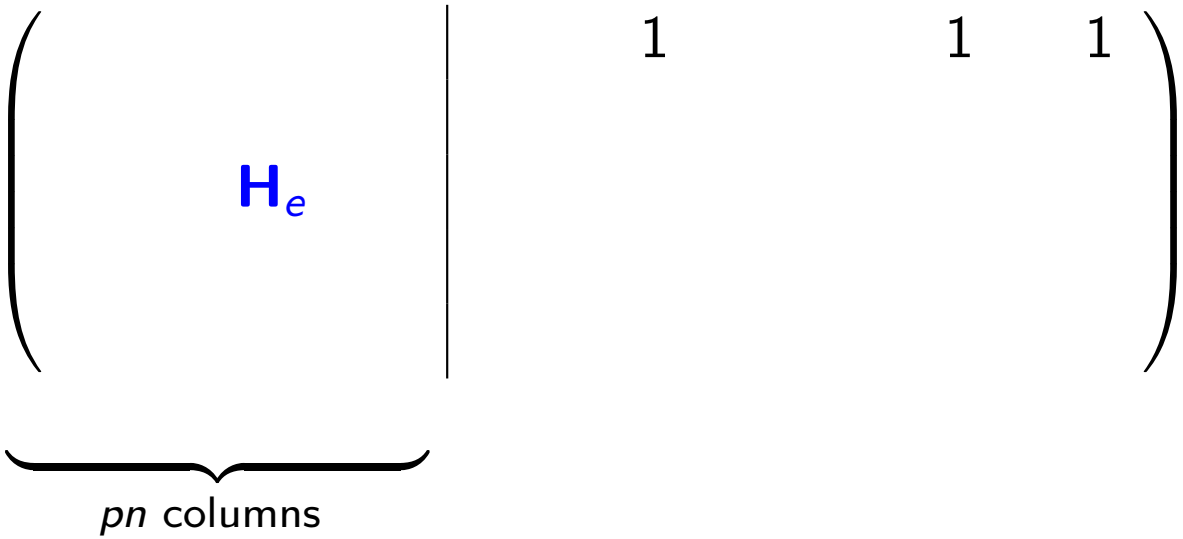
- Typiquement : $\mathbf{H}_e$ est une matrice $r \times np$
- Lorsque $np = r$, la matrice carré $\mathbf{H}_e$ est de rend presque plein $\longrightarrow D(p)$ est proche de 0

Rang d'une matrice creuse aléatoire



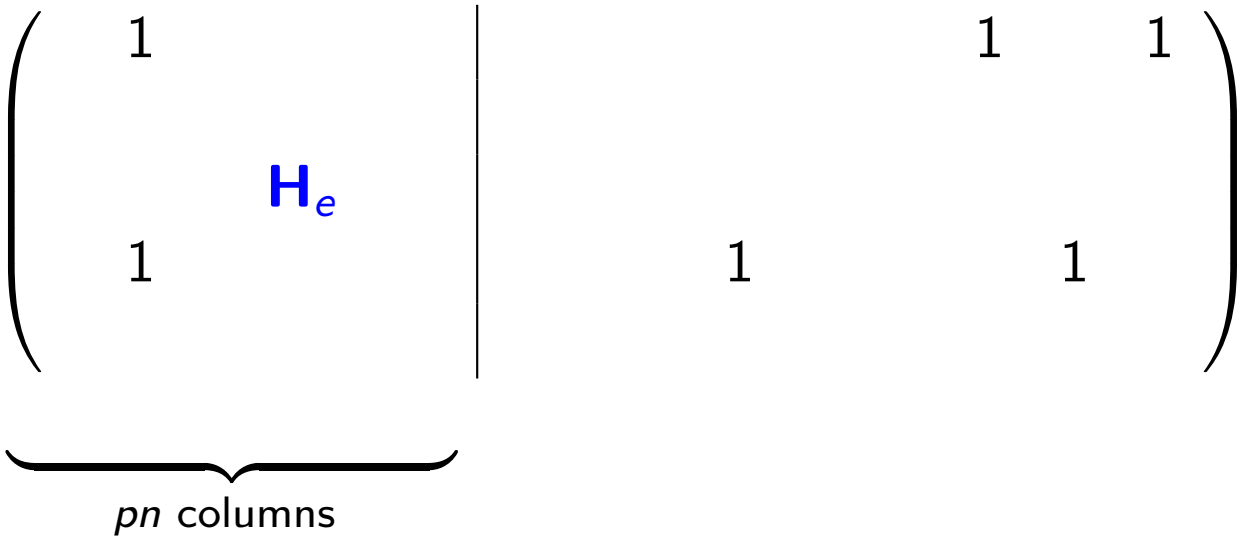
- Typiquement : $\mathbf{H}_e$ est une matrice $r \times np$
- Lorsque $np = r$, la matrice carré $\mathbf{H}_e$ est de rend presque plein $\longrightarrow D(p)$ est proche de 0

Rang d'une matrice creuse aléatoire



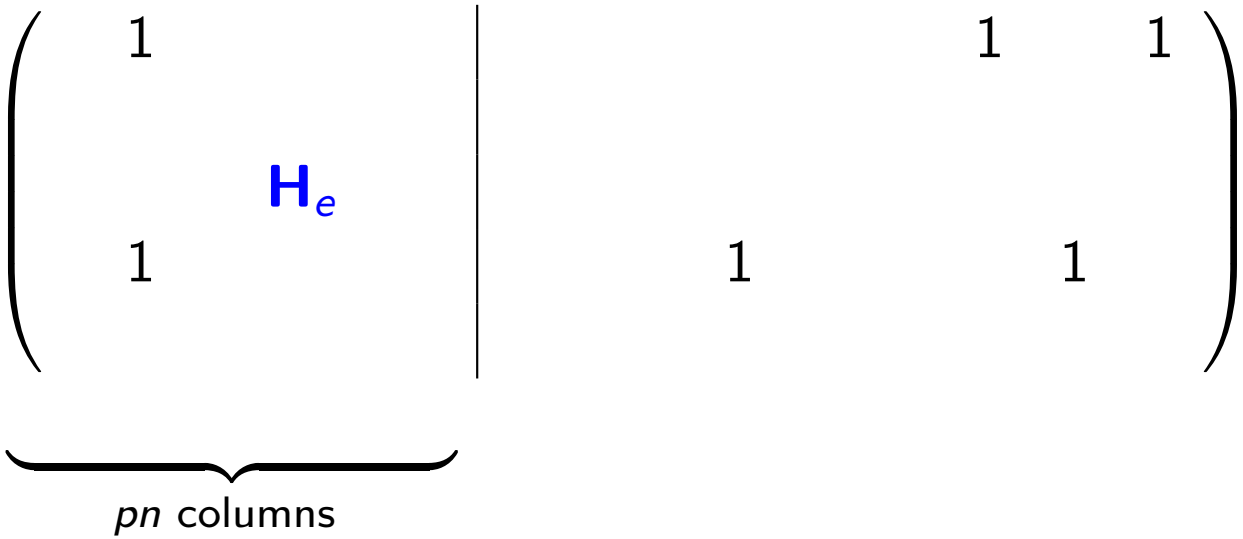
- Typiquement : $\mathbf{H}_e$ est une matrice $r \times np$
- Lorsque $np = r$, la matrice carré $\mathbf{H}_e$ est de rend presque plein
  $\longrightarrow D(p)$ est proche de 0
- MAIS pour une matrice creuse $\mathbf{H}$, il y a αn lignes nulles dans $\mathbf{H}_e$
  $\longrightarrow D(p) > \lambda$
  $\longrightarrow$ Borne sur le rendement des codes LDPC quantique

Rang d'une matrice creuse aléatoire



- Typiquement : $\mathbf{H}_e$ est une matrice $r \times np$
- Lorsque $np = r$, la matrice carré $\mathbf{H}_e$ est de rend presque plein
  $\longrightarrow D(p)$ est proche de 0
- MAIS pour une matrice creuse $\mathbf{H}$, il y a αn lignes nulles dans $\mathbf{H}_e$
  $\longrightarrow D(p) > \lambda$
  $\longrightarrow$ Borne sur le rendement des codes LDPC quantique

Rang d'une matrice creuse aléatoire



- Typiquement : $\mathbf{H}_e$ est une matrice $r \times np$
- Lorsque $np = r$, la matrice carré $\mathbf{H}_e$ est de rend presque plein
  $\longrightarrow D(p)$ est proche de 0
- MAIS pour une matrice creuse $\mathbf{H}$, il y a αn lignes nulles dans $\mathbf{H}_e$
  $\longrightarrow D(p) > \lambda$
  $\longrightarrow$ Borne sur le rendement des codes LDPC quantique
- Ensuite, il y a βn lignes identique de poids 1 ...
  $\longrightarrow$ amélioration de la borne

Rang d'une matrice creuse aléatoire

Théorème (D., Zémor - 2012)

Les rendements atteignables avec $\mathbf{H}_X$ *et* $\mathbf{H}_Z$ *de type* $(2, m)$*, et avec* $d_X, d_Z \geq 2\delta + 1$*, sur le canal à effacement quantique de probabilité* p *:*

$$\begin{aligned} R &\leq 1 - 2p - D(p) \\ &\leq (1-2p)\Big(\frac{4}{mp}\big(1 - (1-p)^m S_\delta(p(1-p)^{m-2})\big) - 1\Big) \end{aligned}$$

S_δ dépend de la série génératrice des sous-arbres enracinés de l'arbre m-régulier.

Rang d'une matrice creuse aléatoire

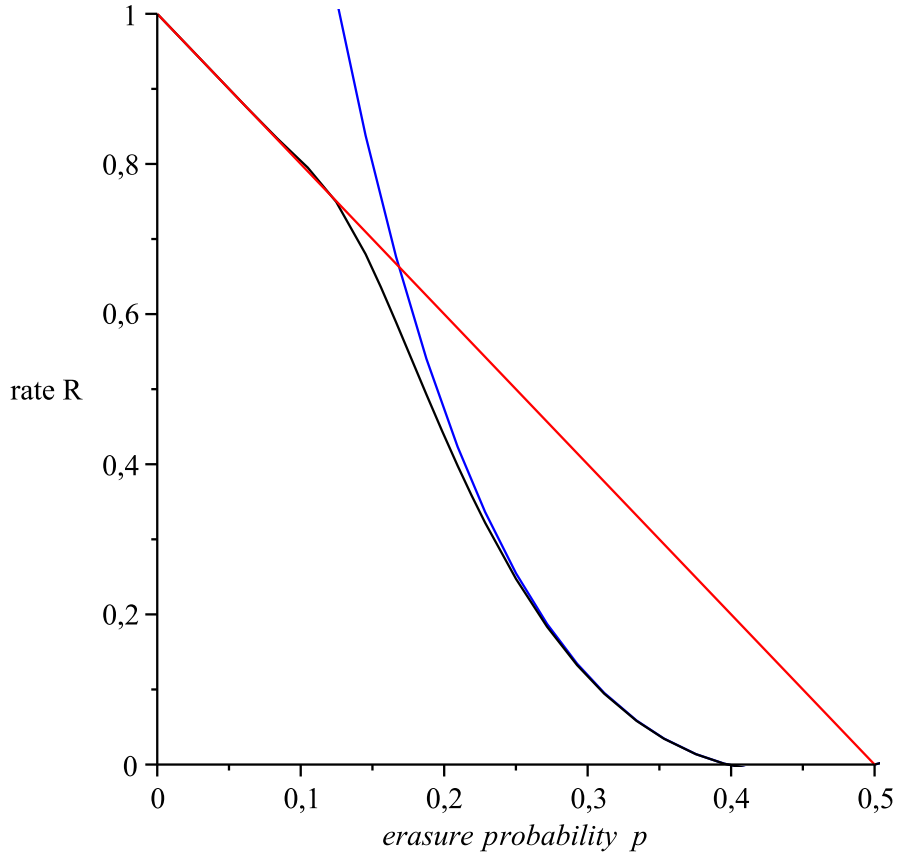


FIGURE : Borne sur le rendement des codes quantiques $(2, 8)$

En bleu : en comptant le nombre moyen de lignes nulles
En noir : en comptant les relations de longueur ≤ 6 entre les lignes de $\mathbf{H}_e$

Résultats numériques

m	$\frac{1}{m-1} \leq p_c$	borne améliorée : $p_c \leq$	avec la capacité : $p_c \leq \frac{2}{m}$
5	0.25	0.38	0.40
10	0.11	0.17	0.20
20	0.053	0.073	0.100
30	0.035	0.046	0.067
40	0.026	0.034	0.050
50	0.020	0.026	0.040

Résultats numériques

Questions :

- Valeur exacte de p_c
- Compter les composantes connexes d'un sous-graphe aléatoire
- Généraliser à d'autres modèles d'erreurs (sans connaitre les positions en erreur)
- Construction de codes de surface atteignant un seuil optimal

Pour en discuter : Bureau 2044 jusqu'en Octobre 2013.

Résultats numériques

Merci de votre attention !