Étude des paramètres des codes topologiques quantiques

Nicolas Delfosse

LIX-Qualcomm, École Polytechnique
INRIA Saclay, Équipe GRACE

Groupe de travail BAC - Telecom Paristech
23 Novembre 2012

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 $d = \min\{w(x) \mid x \in C\}$.
- Les paramètres de C : $[n, k, d]$.

Proposition

Il existe une famille de codes avec $k = \Theta(n)$ et $d = \Theta(n)$.

Codes LDPC

LDPC : Low Density Parity–Check

- matrice de parité de C : $H \in \mathcal{M}_{r,n}(\mathbb{F}_2)$ telle que :

$$C = \{x \in \mathbb{F}_2^n \mid Hx^t = 0\}.$$

- code LDPC : C admet une matrice de parité creure.

Pourquoi des codes LDPC ?

- algorithme de décodage efficace et performant
- atteingent la capacité du canal

Codes LDPC réguliers

$C = \mathrm{Ker}\, H$ est un code LDPC de type (ℓ, m) si :

- les colonnes de H sont de poids ℓ,
- les lignes de H sont de poids m.

Proposition

Il existe une famille de codes de type (ℓ, m) *avec* $k = \Theta(n)$ *et* $d = \Theta(n)$ *si* $\ell \geq 3$.
MAIS si $\ell = 2$, *on a* $d = O(\log(n))$.

Codes des cycles

$C = \ker H$ de type (ℓ, m).
Si $\ell = 2$, H est la matrice d'incidence d'un graphe G :

- sommets de G = lignes de H
- aretes de G = colonnes de H
- le sommet i est incident à l'arête j ssi $H_{i,j} = 1$.

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

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

Le graphe G est régulier de degré m.

Le graphe de Petersen

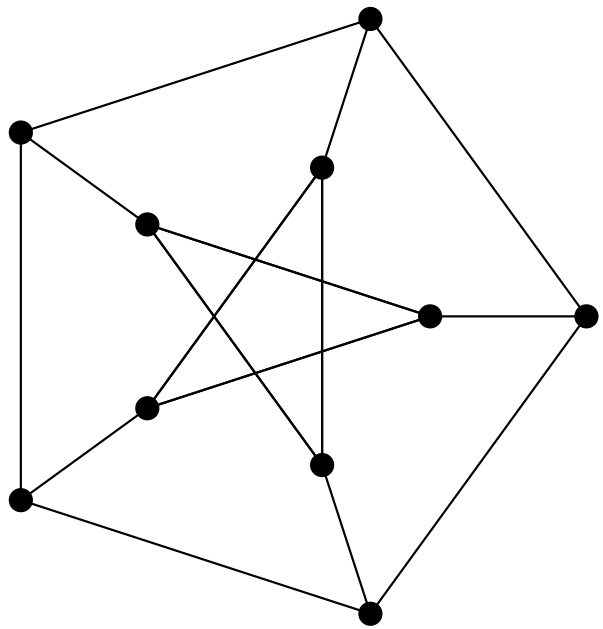
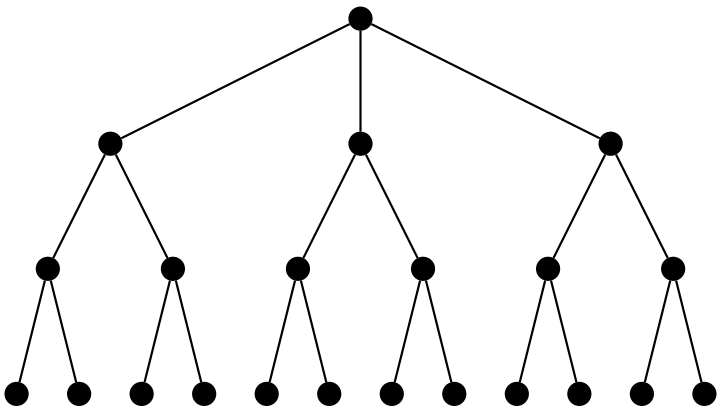


FIGURE : Le code des cycles du graphe de Petersen est un code $[15, 6, 5]$

Maille maximale d'un graphe régulier

Si G est un graphe m-régulier de maille d alors

$$|V| \geq 1 + m + m(m-1) + \dots m(m-1)^{\lfloor (d-1)/2 \rfloor}.$$



- Assymptotiquement, on a $d \leq C \log_{m-1} |V|$.
- Déterminer C ?
  - Erdos, Sachs 1963 : $C \geq 1$ (méthode probabiliste)
  - Margulis 1982 : mois bien mais explicite
  - Lubotzky, Philips, Sarnak & Margulis 1987 : $C \geq 4/3$

La construction de Margulis

$S = \{A, A^{-1}, B, B^{-1}\} \subset SL_2(\mathbb{Z})$ engendre un groupe libre avec :

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

Son graphe de Cayley est un arbre 4-régulier :

- Sommets = éléments du groupe
- Arêtes = $\{x, sx\}$ pour $s \in S$

Réduire ce groupe modulo un grand nombre premier p :

- groupe fini $\rightarrow$ graphe fini
- pas de relation courte $\rightarrow$ grande maille

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 : $d = \inf\{w(x) \mid x \in C_X \setminus C_Z^\perp \cup C_Z \setminus C_X^\perp\}$

Proposition

Il existe une famille de codes CSS avec $k = \Theta(n)$ et $d = \Theta(n)$.

Constructions des codes LDPC quantiques

Code LDPC quantique = code quantique avec $\mathbf{H}_X$ et $\mathbf{H}_Z$ creuses

Deux grandes familles de LDPC quantiques :

- basés sur des LDPC classiques : Rendement $R = k/n$ élevé mais d trop faible
- codes topologiques basés sur des pavages : meilleure distance, applications au calcul quantique tolerant aux fautes, hautement dégénérés

Le code Torique de Kitaev

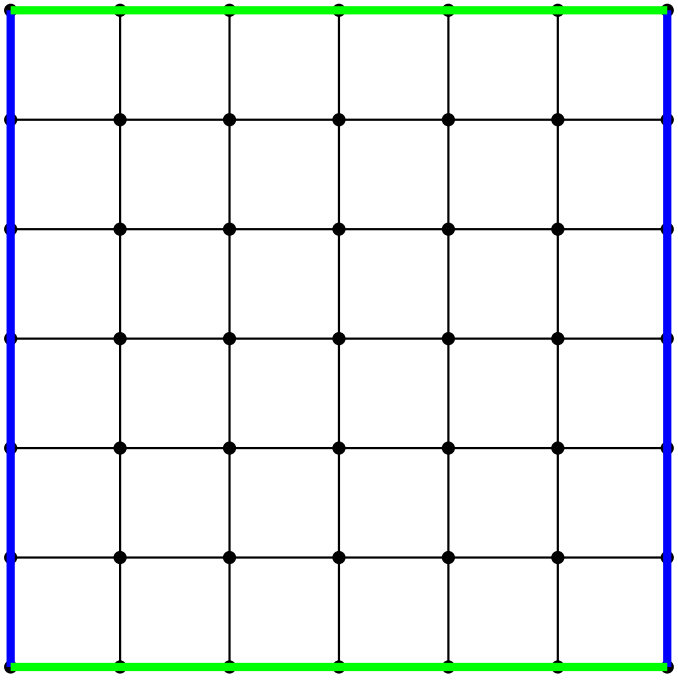
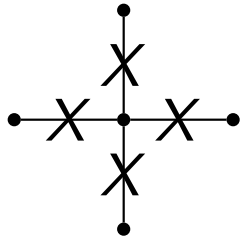


FIGURE : Un pavage carré du tore

Lignes de $\mathbf{H}_X =$ 

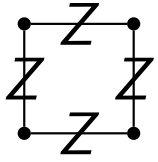
Lignes de $\mathbf{H}_Z =$ 

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

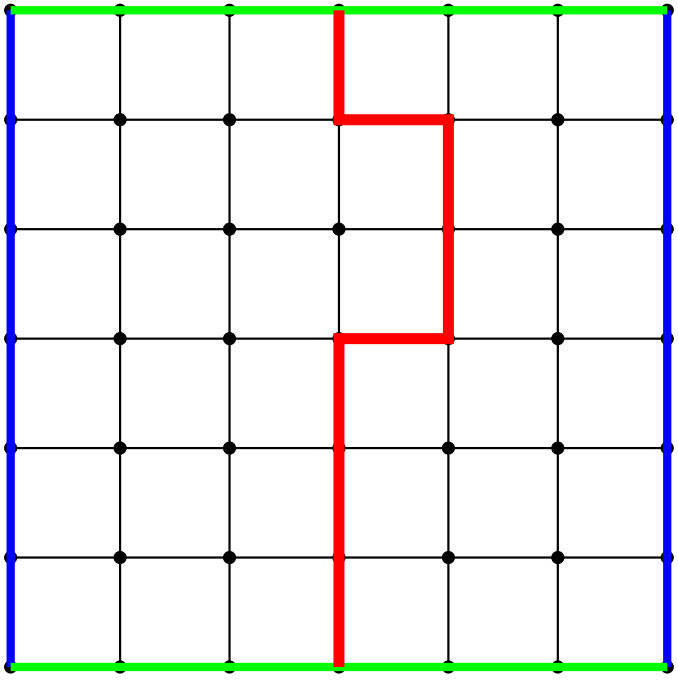


FIGURE : Un pavage carré du tore

- 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 $\mathbf{H}_Z =$

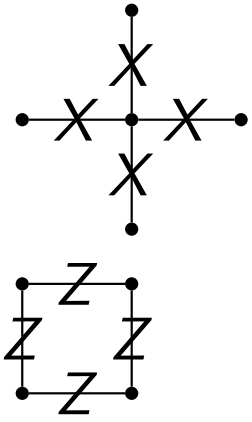


FIGURE : Générateurs du code de Kitaev

Le code Torique de Kitaev

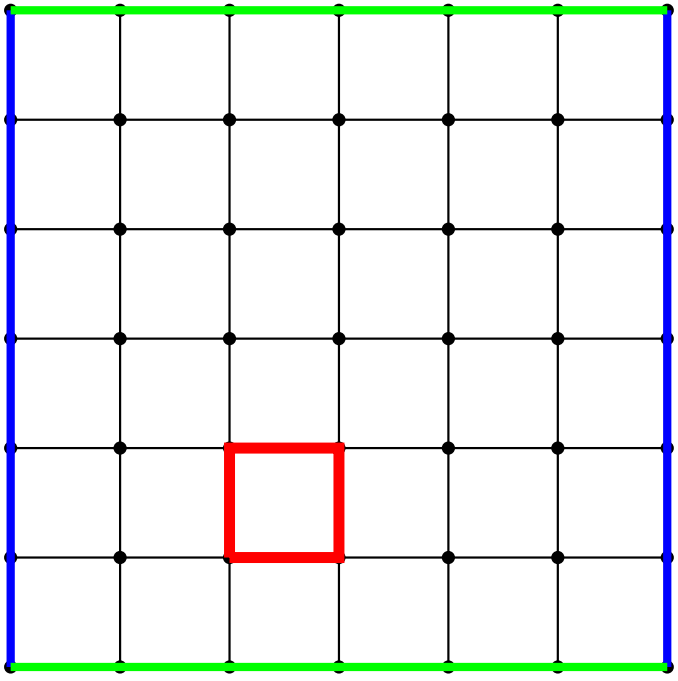


FIGURE : Un pavage carré du tore

- 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 $\mathbf{H}_Z =$

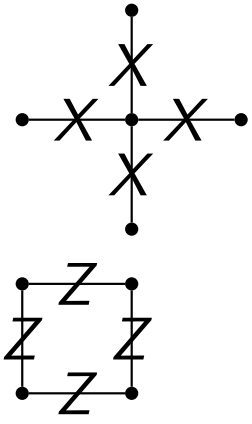


FIGURE : Générateurs du code de Kitaev

Le code Torique de Kitaev

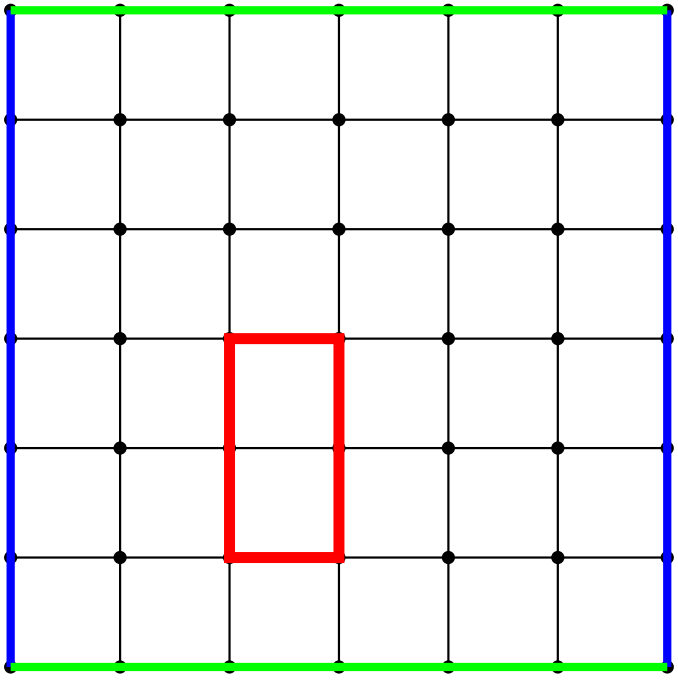
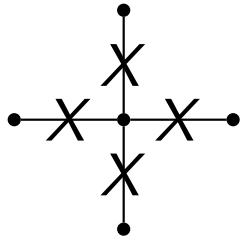


FIGURE : Un pavage carré du tore

Lignes de $\mathbf{H}_X =$ 

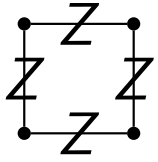
Lignes de $\mathbf{H}_Z =$ 

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

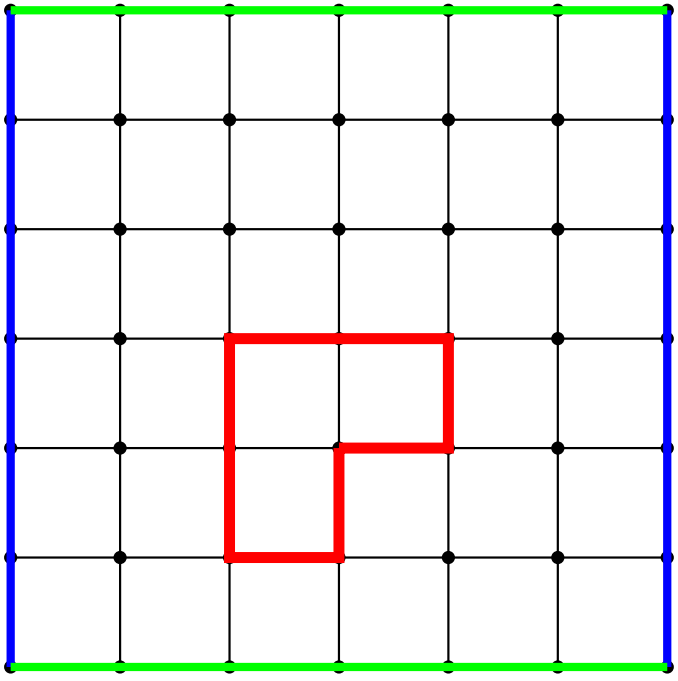
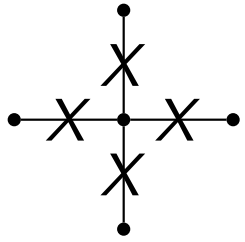


FIGURE : Un pavage carré du tore

Lignes de $\mathbf{H}_X =$ 

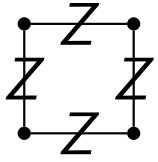
Lignes de $\mathbf{H}_Z =$ 

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

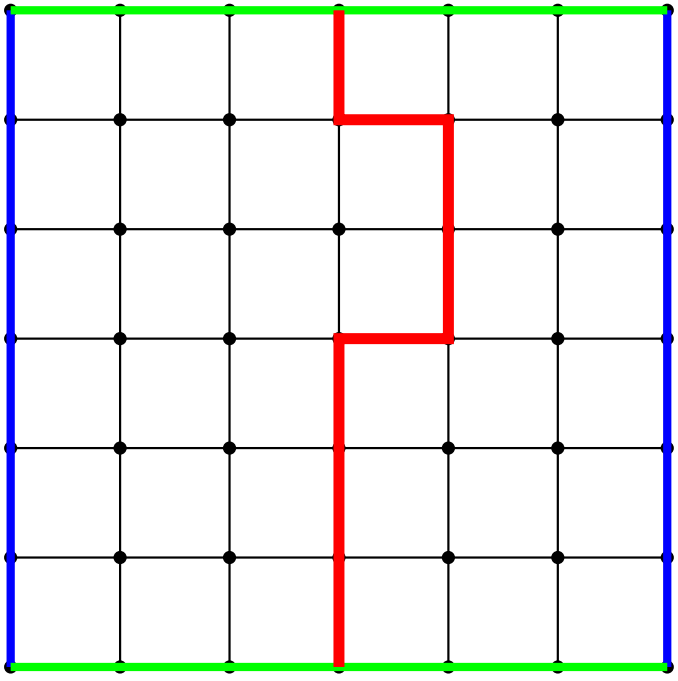


FIGURE : Un pavage carré du tore

- 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 $\mathbf{H}_Z =$

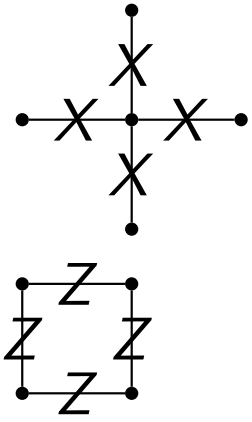


FIGURE : Générateurs du code de Kitaev

Le code Torique de Kitaev

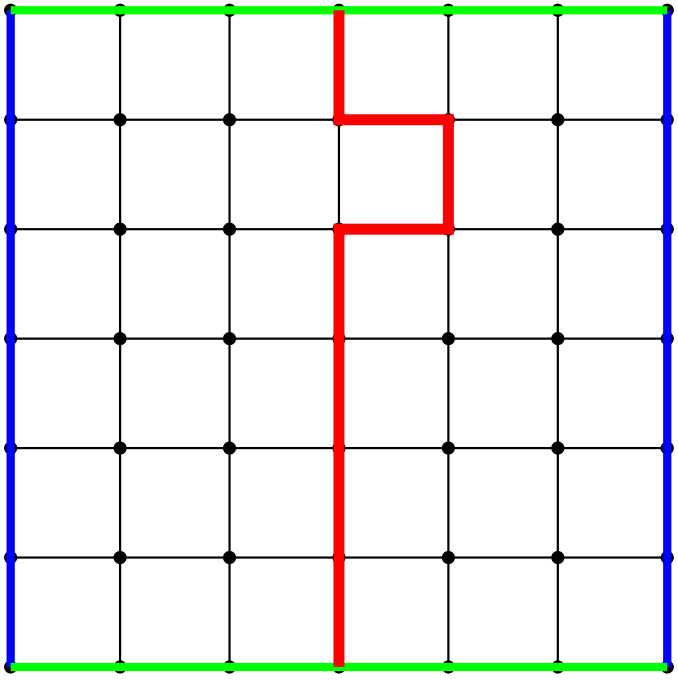
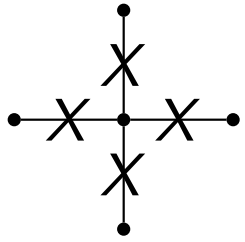


FIGURE : Un pavage carré du tore

Lignes de $\mathbf{H}_X =$ 

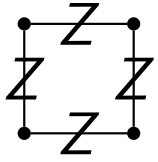
Lignes de $\mathbf{H}_Z =$ 

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

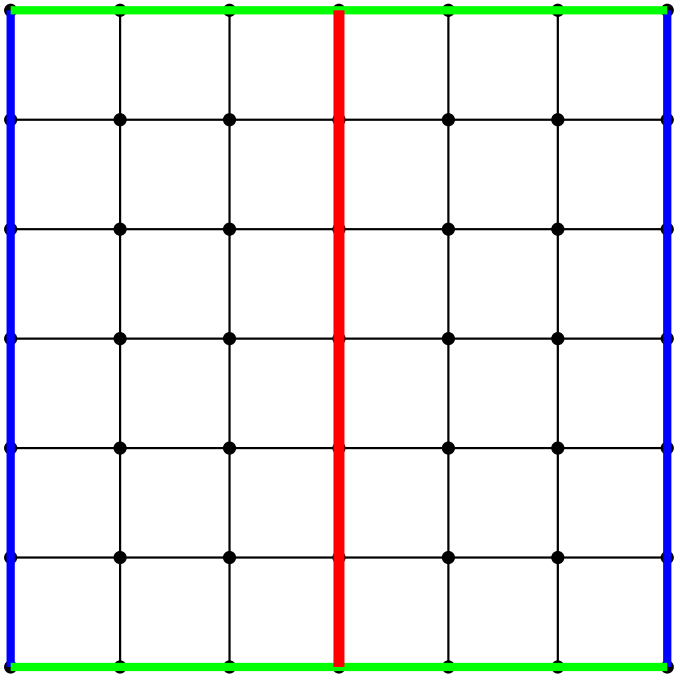
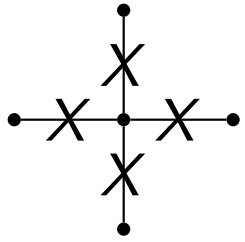


FIGURE : Un pavage carré du tore

Lignes de $\mathbf{H}_X =$ 

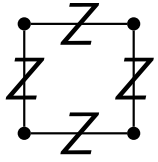
Lignes de $\mathbf{H}_Z =$ 

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

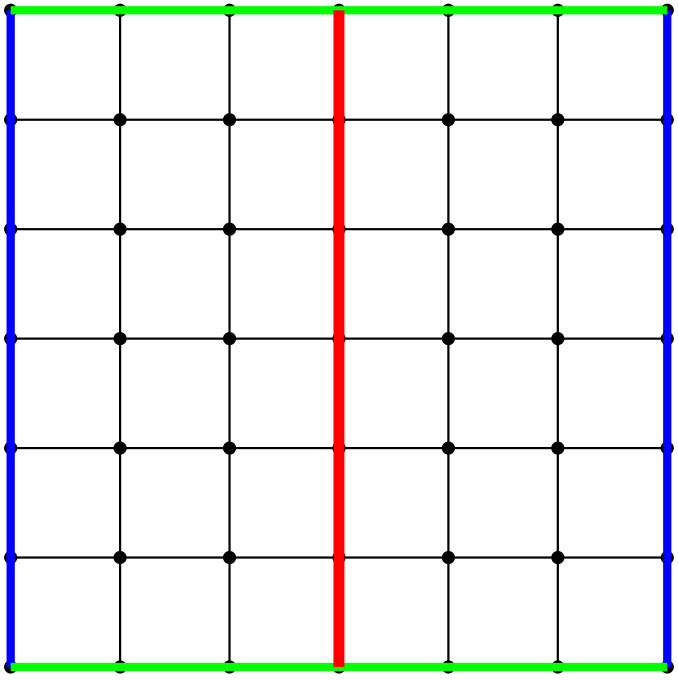


FIGURE : Un pavage carré du tore

- 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 $\mathbf{H}_Z =$

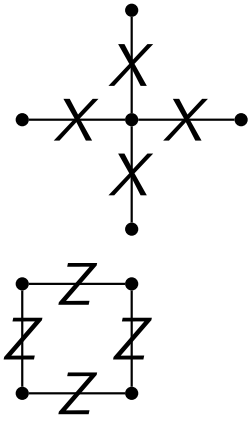


FIGURE : Générateurs du code de Kitaev

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 $d = O(n^{1/2})$?

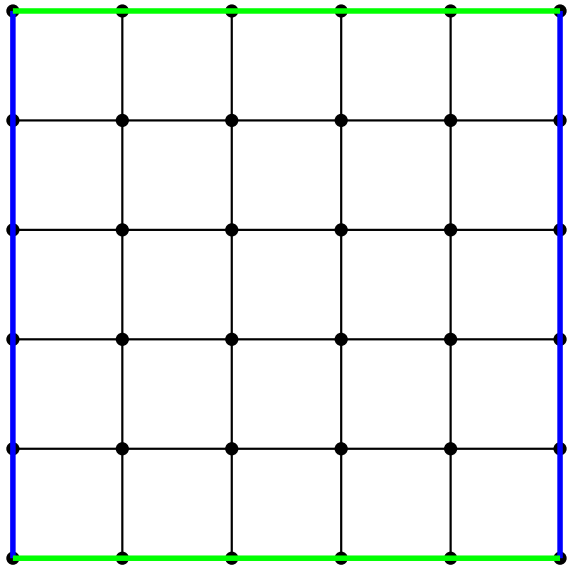


FIGURE : Une boule du pavage carré du tore

Distance minimale des codes topologiques

D'où vient ce $d = O(n^{1/2})$?

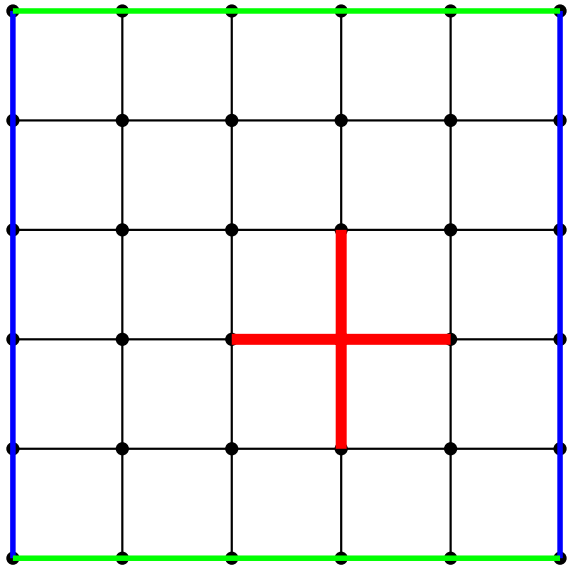


FIGURE : Une boule du pavage carré du tore

Distance minimale des codes topologiques

D'où vient ce $d = O(n^{1/2})$?

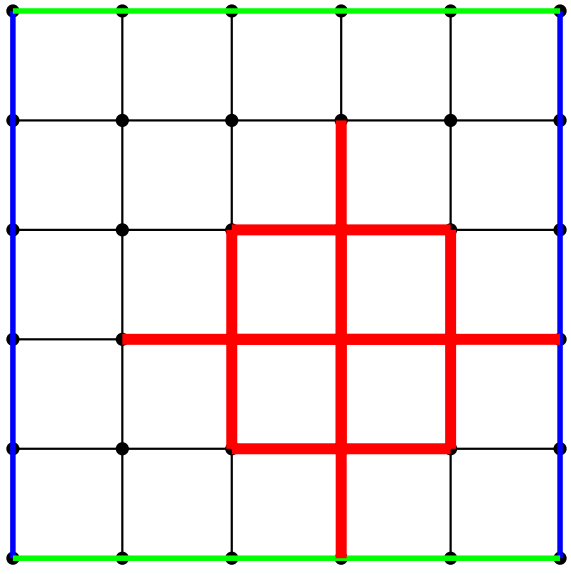


FIGURE : Une boule du pavage carré du tore

Distance minimale des codes topologiques

D'où vient ce $d = O(n^{1/2})$?

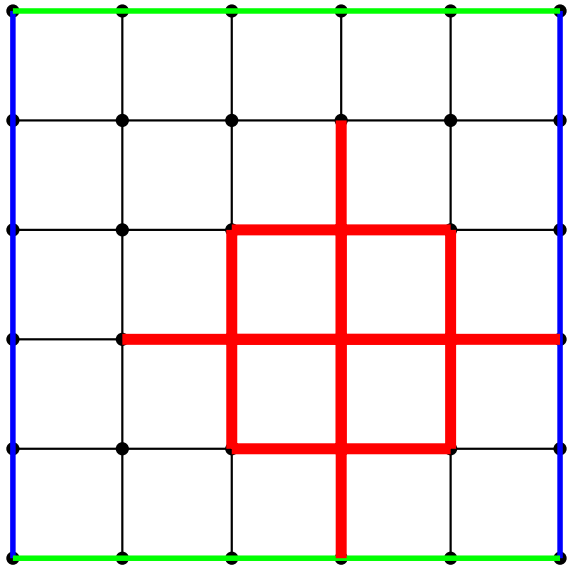


FIGURE : Une boule du pavage carré du tore

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

Distance minimale des codes topologiques

D'où vient ce $d = O(n^{1/2})$?

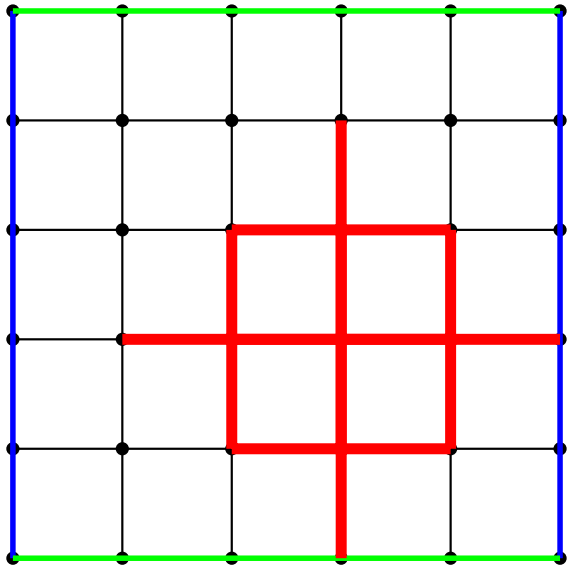


FIGURE : Une boule du pavage carré du tore

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.

La borne de Bravyi-Poulin-Terhal

De nombreuses généralisations du code torique de Kitaev :
Codes torique à bords, codes torique à trous, sur un pavage hexagonal du tore ou sur un pavage carré-octogonal du tore, ...

Tous ces codes sont limités par la borne :

Théorème (Bravyi, Poulin, Tehral - 2009)

Les paramètres $[[n, k, d]]$ *d'un code CSS local défini sur un pavage carré du tore vérifient :*

$$kd^2 \leq cn.$$

Conséquence :

- $R = k/n$ constant + d croissante est impossible
- $d = O(\sqrt{n})$

Dimension des codes de surface

Dimension du code torique ?

mots quantiques = les cycles modulo les faces.
$\rightarrow$ Dans le tore ce quotient est de dimension 2.
$\rightarrow k = 2$.

Dimension d'un code topologique ?

surface (orientable) = recollement de g tores
= surface avec g trous
$\rightarrow k = 2g$

$\rightarrow$ on veut un genre g élevé.

Codes de surface de rendement constant

Code de surfaces : (Bombin, Martin-Delgado, '06)
G un pavage de surface

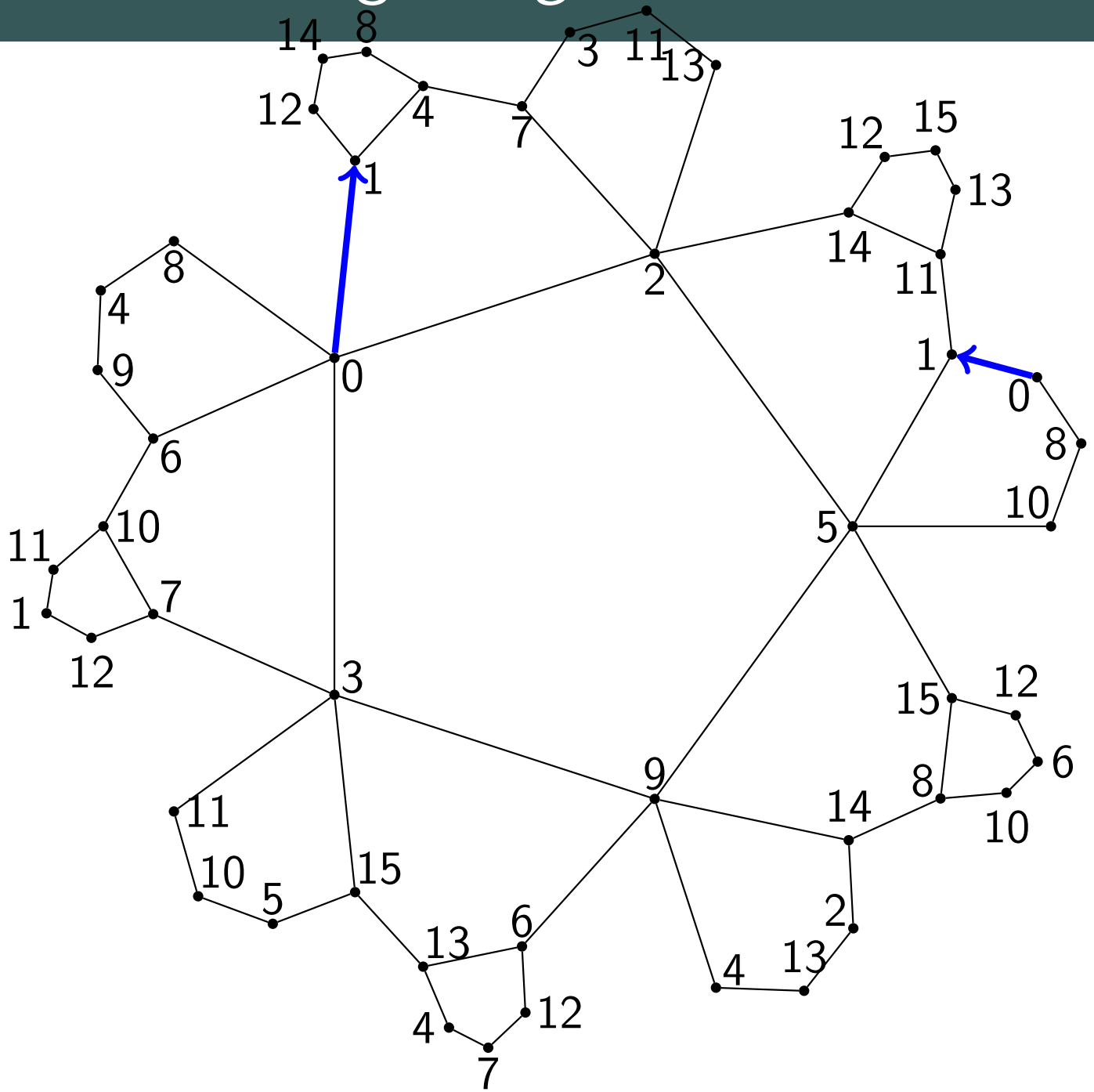
- $\mathbf{H}_X$ = matrice d'incidence de G
- $\mathbf{H}_Z$ = matrice des faces de G

$\Rightarrow$ mots quantiques = les cycles modulo les faces

genre g elevé + les petites boules sont planaires
$\rightarrow R = k/n$ constant et $d = O(\log(n))$

- avec des surfaces hyperboliques (Freedman, Luo, Meyer, '01)
- avec des graphes de Cayley (Zémor, '09)

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

Code de surfaces : (Bombin, Martin-Delgado '06)
G un pavage de surface

- $\mathbf{H}_X$ = matrice d'incidence de G
- $\mathbf{H}_Z$ = matrice des faces de G

$\Rightarrow$ mots quantiques = les cycles modulo les faces

$T =< a, b >$ un groupe fini avec $a^2 = b^m = (ab)^l = 1$ et pas d'autre relation de longueur $\leq r$

surface = graphe de Cayley de T et $S = \{a, b, b^{-1}\}$
$\Rightarrow$ Codes hyperboliques (Zémor '09)

Codes hyperboliques

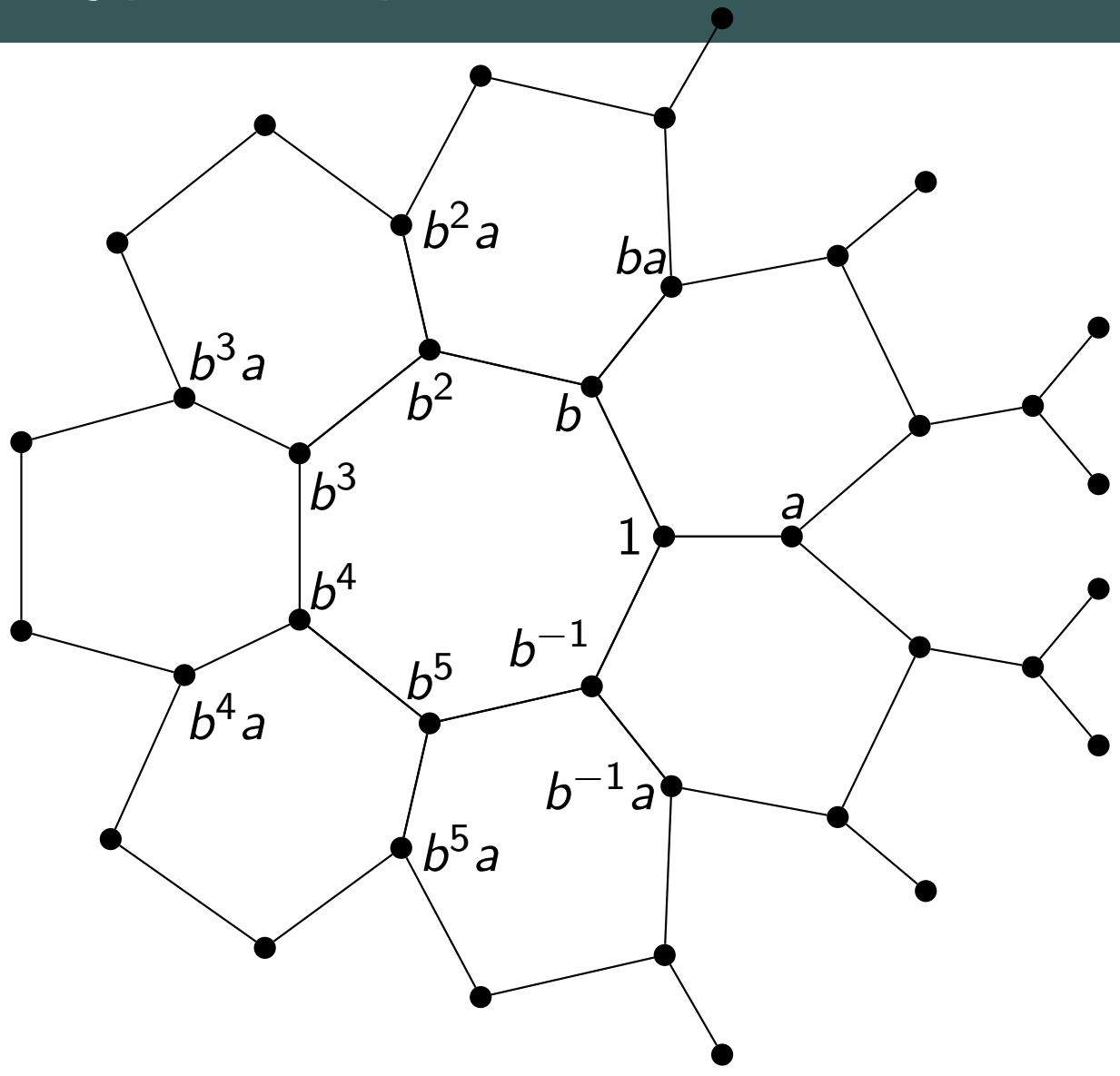


FIGURE : Le graphe de Cayley avec $a^2 = b^7 = (ab)^3 = 1$

Codes hyperboliques

avec les groupes de siran $\Rightarrow$ R constant et d croissante au moins en $\log(n)$:

- pour avoir k grand on choisit de grandes faces
  c'est à dire l et m grand
  $\Rightarrow R = k/n \to \frac{2}{3}\left(\frac{1}{2} - \frac{1}{l} - \frac{1}{m}\right)$
- pas de relation autre que les faces de longueur $\leq r$
  localement planaire dans les boule de rayon $(r-1)/2$
  $\Rightarrow d \geq (r-1)/2$

Systole d'une variété Riemannienne

$\mathcal{V}$ une surface fermée, connexe, de genre $g \geq 2$, équipée d'une métrique riemannienne.

Définition

syst $H_1(\mathcal{V})$:= *plus court cycle qui n'est pas un bord.*

Théorème (Gromov - 1992)

$$(\text{syst } H_1(\mathcal{V}))^2 \leq C \frac{(\log g)^2}{g} \text{ Aire}(\mathcal{V}).$$

Pour l'appliquer aux codes de surface, on construit une métrique riemannienne telle que :

- Aire proportionnelle au nombre de faces
- syst correspond à la distance d
- g proportionnel à la dimension k

Systole d'une variété Riemannienne

Avec des pavages G dont les faces sont de longueur inférieure à m et dont les sommets sont de degré inférieur à m :

Théorème (D. - 2012)

$$kd^2 \leq C(\log k)^2 n,$$

Cor : si $R = k/n$ constant alors $d \leq C' \log(n)$.

Systole d'une variété Riemannienne

Comment dépasser ces bornes avec des LDPC quantiques ?

- Freedman, Luo, Meyer (2001), $k = 1$ et $d = O(n^{1/2}\log(n)^{1/2})$
- Tillich, Zémor (2009) R constant, $d = n^{1/2}$
- Couvreur, Delfosse, Zémor (2011), $k = O\sqrt{n}$, $d = O(\sqrt{n})$
  (avec des lignes de poids $O(\log(n))$)

Ouvert : Peut-on obtenir $d = O(n^{\alpha})$ où $\alpha > 1/2$ avec des LDPC ?

Le code couleur hexagonal

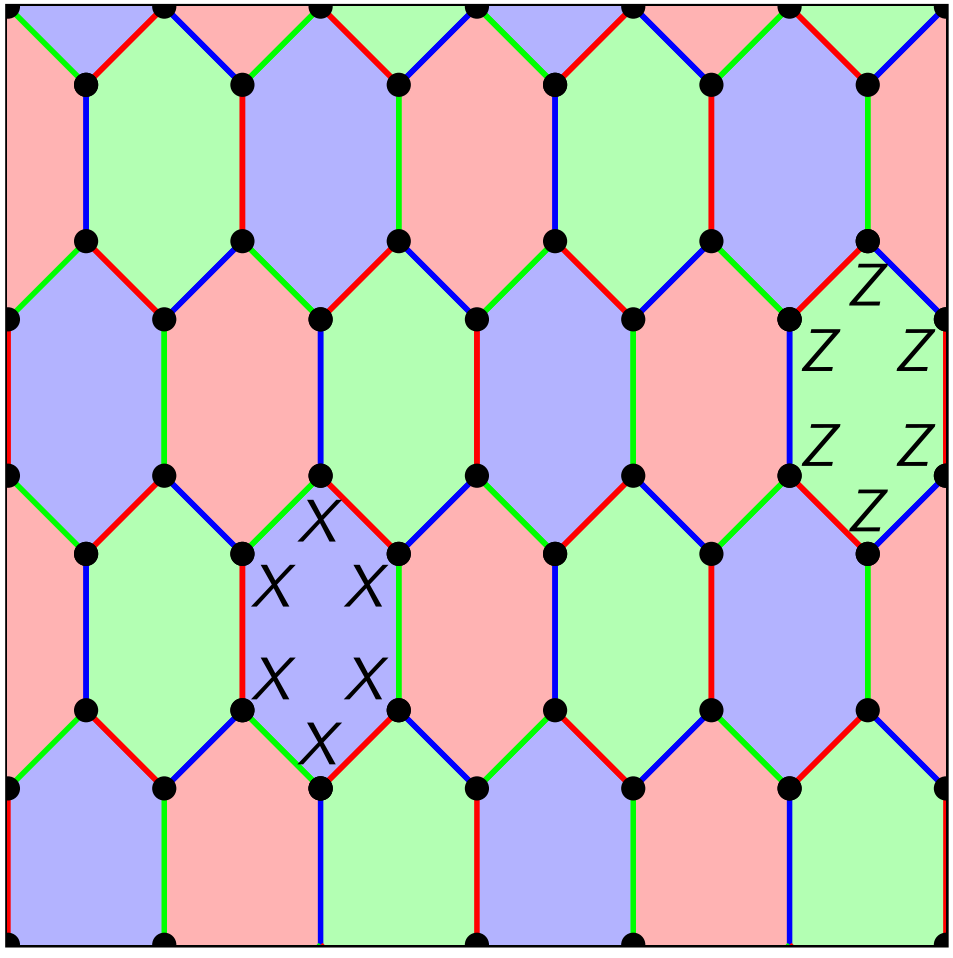


FIGURE : Un code couleur torique

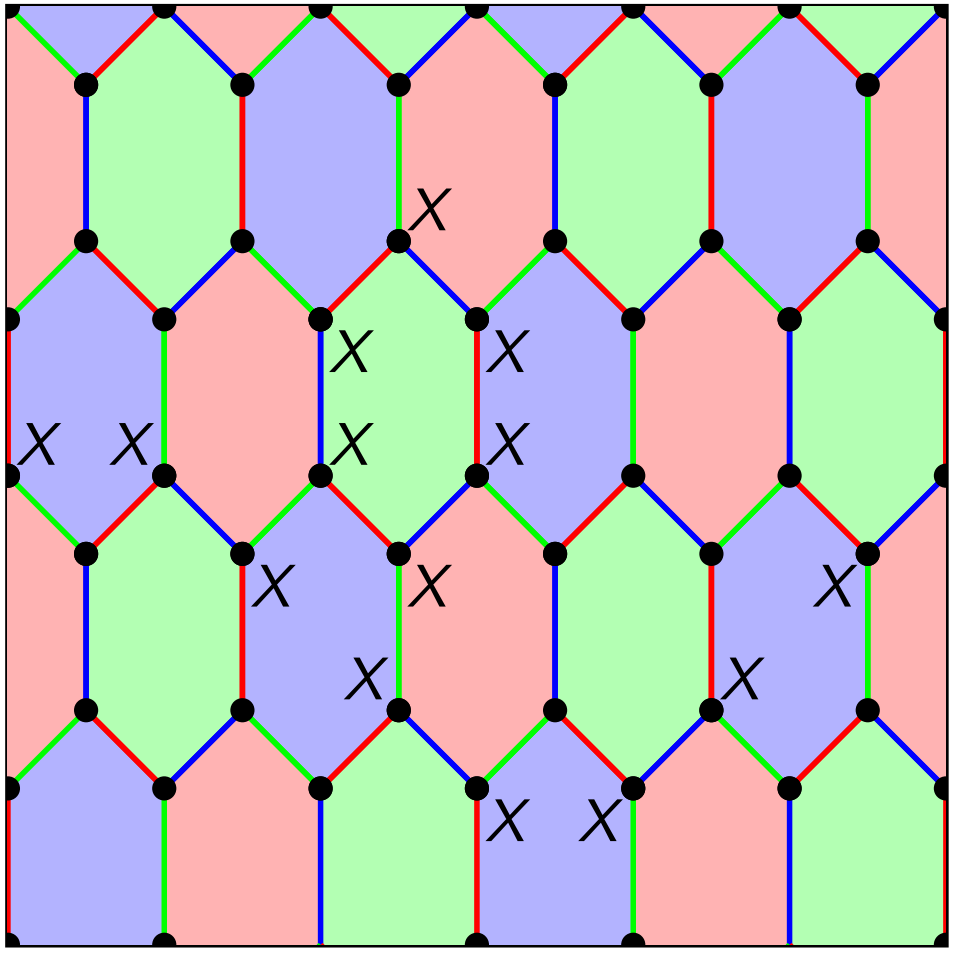
!!! on travaille sur les sommets !!!

Code couleur :
$\mathbf{H}_X = \mathbf{H}_Z =$ matrice des faces (en fonction des sommets)

$\rightarrow$ étudier :

- le code auto-orthogonal $C = \mathrm{Ker}\,\mathbf{H}_X = \mathrm{Ker}\,\mathbf{H}_Z$
- les mots quantiques $= C$ modulo $C^{\perp}$

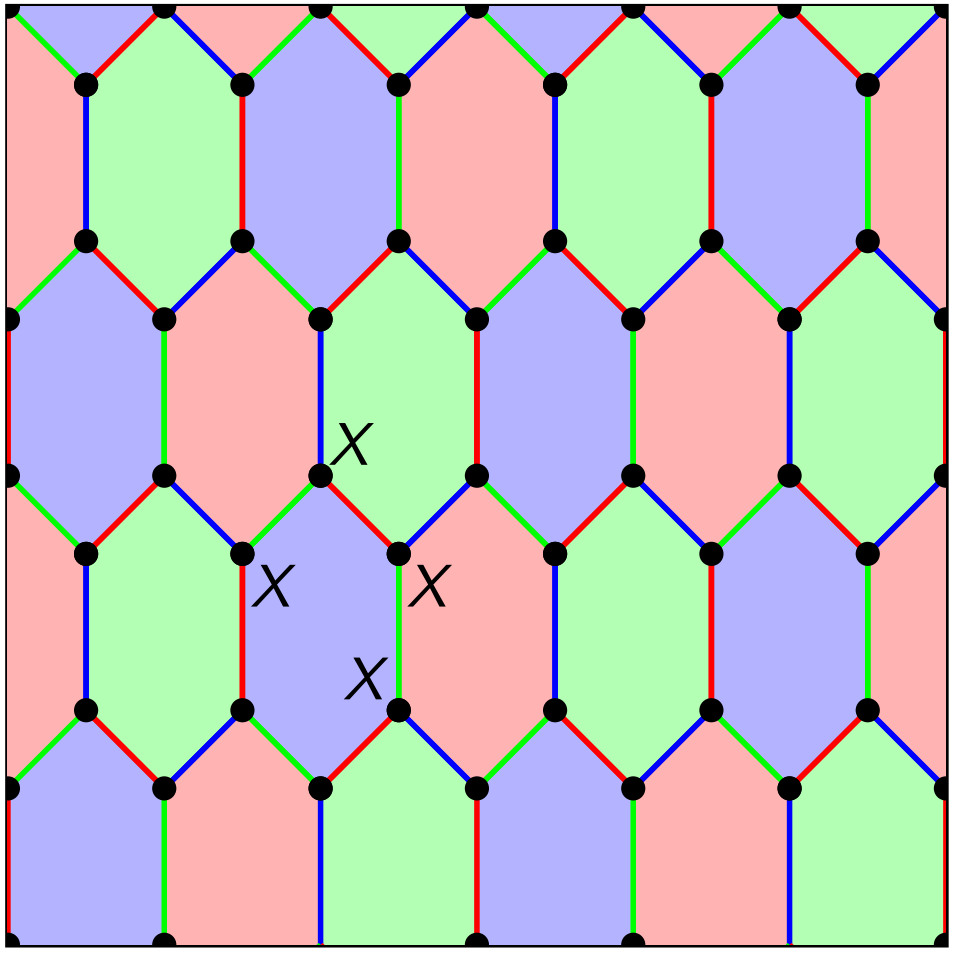
Représentation graphique du code C



1. Soit $x \in C$
2. On se restreint à une face bleue
3. On couple les sommets de x
4. On prolonge ces arêtes
5. On obtient 2 cycles

FIGURE : Représentation cyclique d'un mot de C

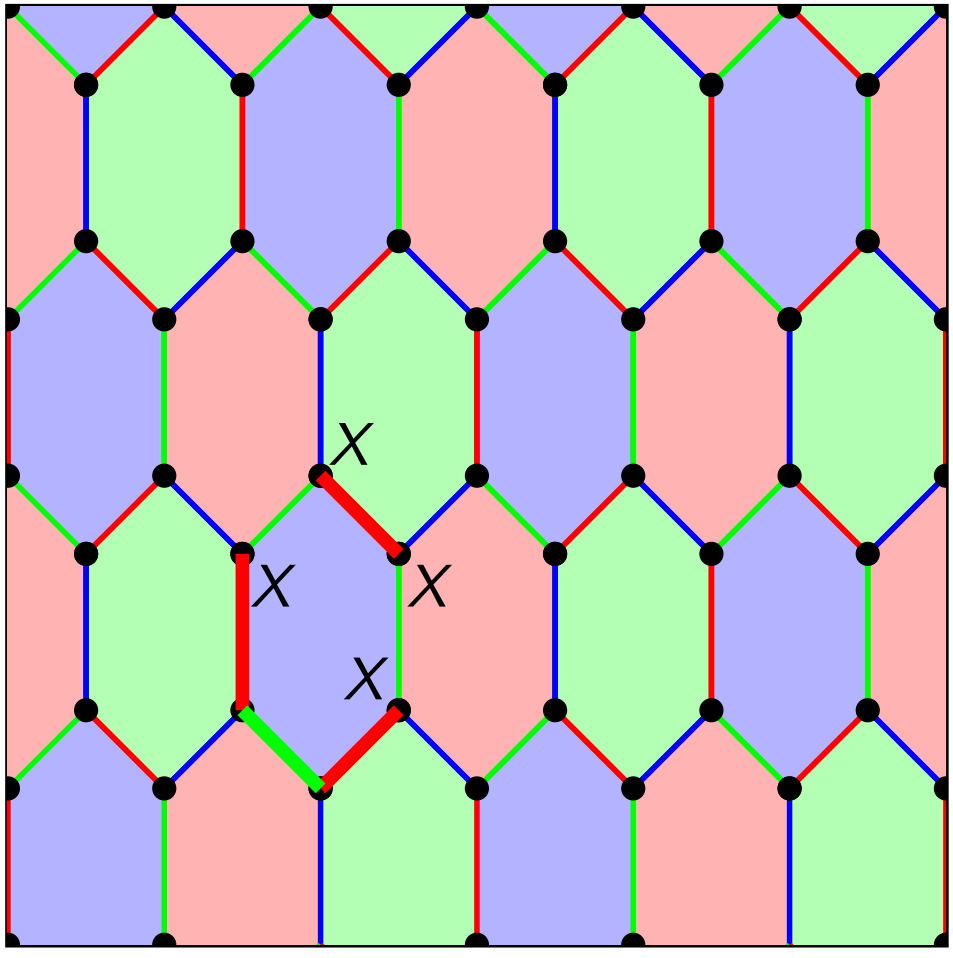
Représentation graphique du code C



1. Soit $x \in C$
2. On se restreint à une face bleue
3. On couple les sommets de x
4. On prolonge ces arêtes
5. On obtient 2 cycles

FIGURE : Représentation cyclique d'un mot de C

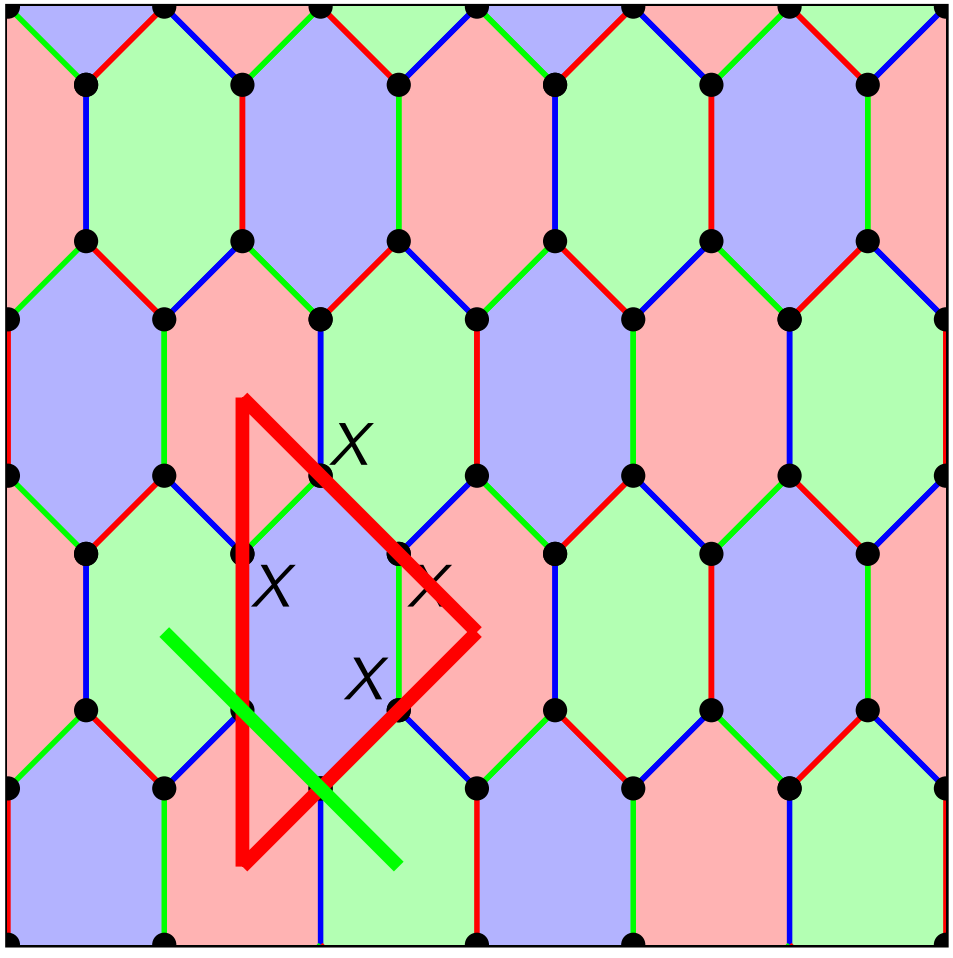
Représentation graphique du code C



1. Soit $x \in C$
2. On se restreint à une face bleue
3. On couple les sommets de x
4. On prolonge ces arêtes
5. On obtient 2 cycles

FIGURE : Représentation cyclique d'un mot de C

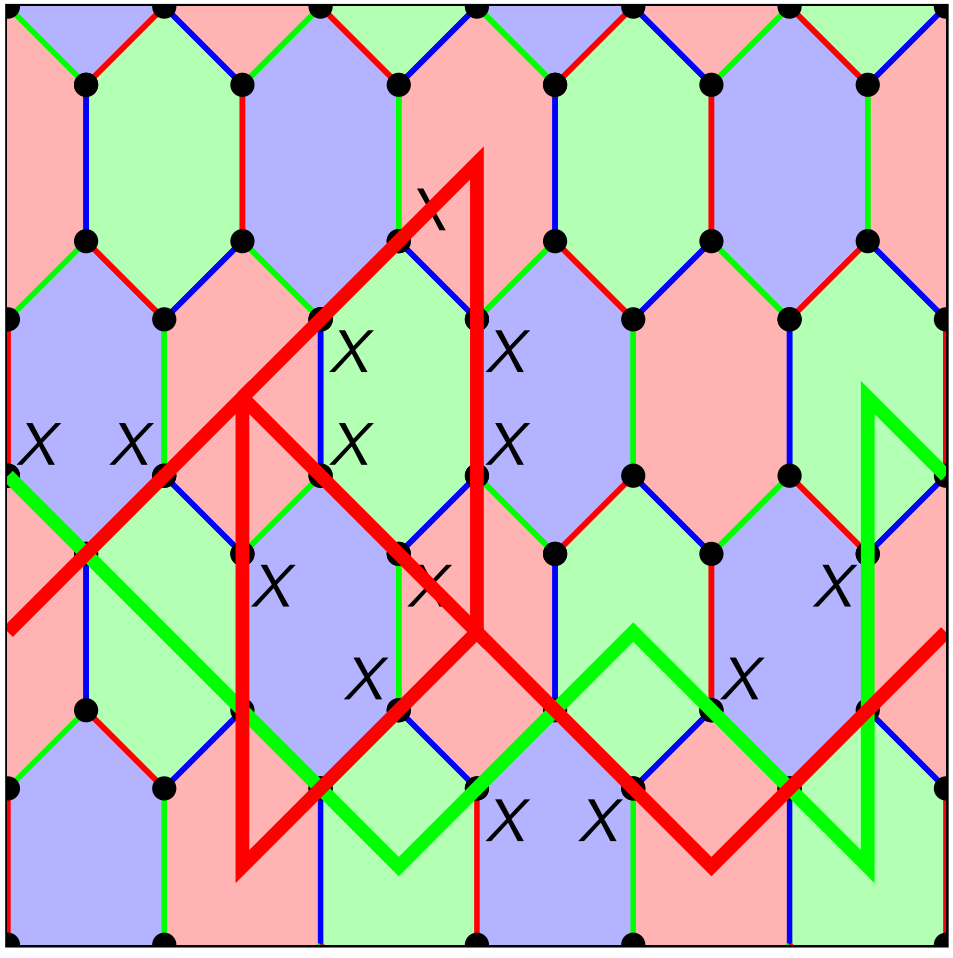
Représentation graphique du code C



1. Soit $x \in C$
2. On se restreint à une face bleue
3. On couple les sommets de x
4. On prolonge ces arêtes
5. On obtient 2 cycles

FIGURE : Représentation cyclique d'un mot de C

Représentation graphique du code C



1. Soit $x \in C$
2. On se restreint à une face bleue
3. On couple les sommets de x
4. On prolonge ces arêtes
5. On obtient 2 cycles

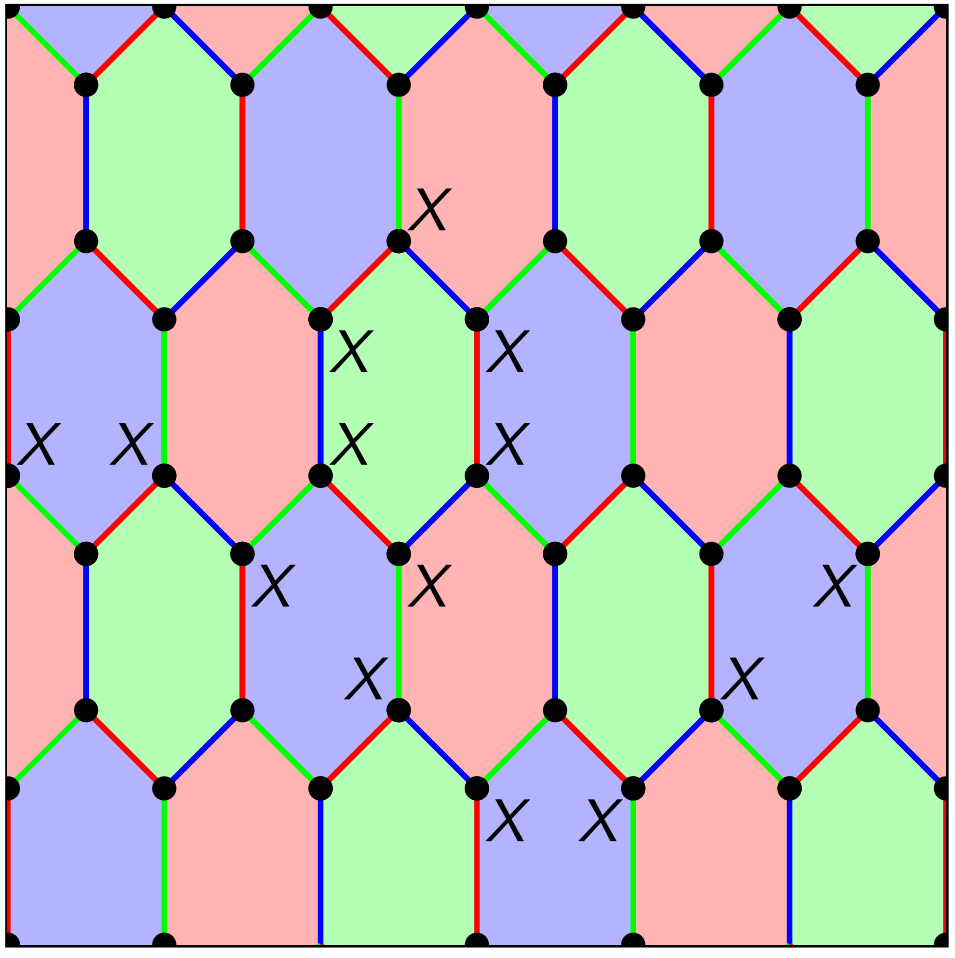
FIGURE : Représentation cyclique d'un mot de C

Représentation graphique du code C

$C = \mathrm{Ker}\,\mathbf{H}_X$ correspond à des paires de cycles.

mots quantiques $= C$ modulo $C^\perp$
Comment décrire $C^\perp$? les mots quantiques ?

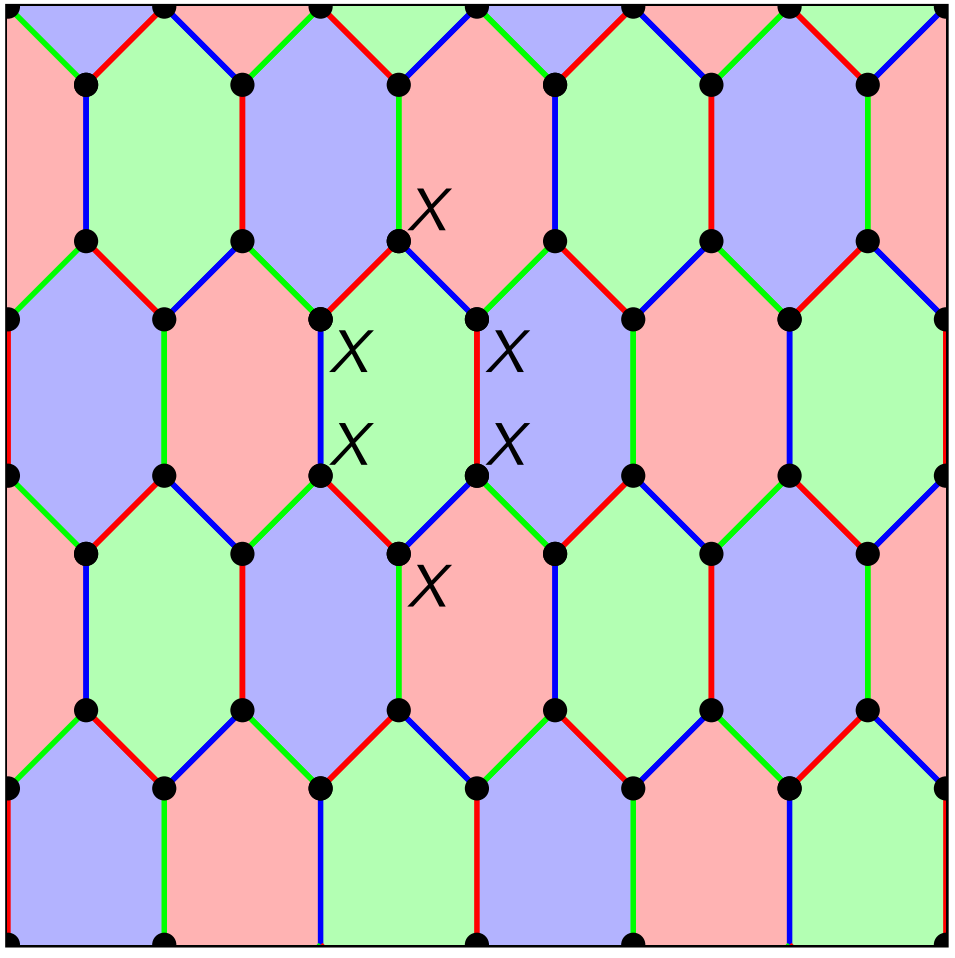
Représentation graphique des mots quantiques



mots quantiques
$= C \text{ mod } C^{\perp}$

FIGURE : Représentation cyclique d'un mot de C

Représentation graphique des mots quantiques

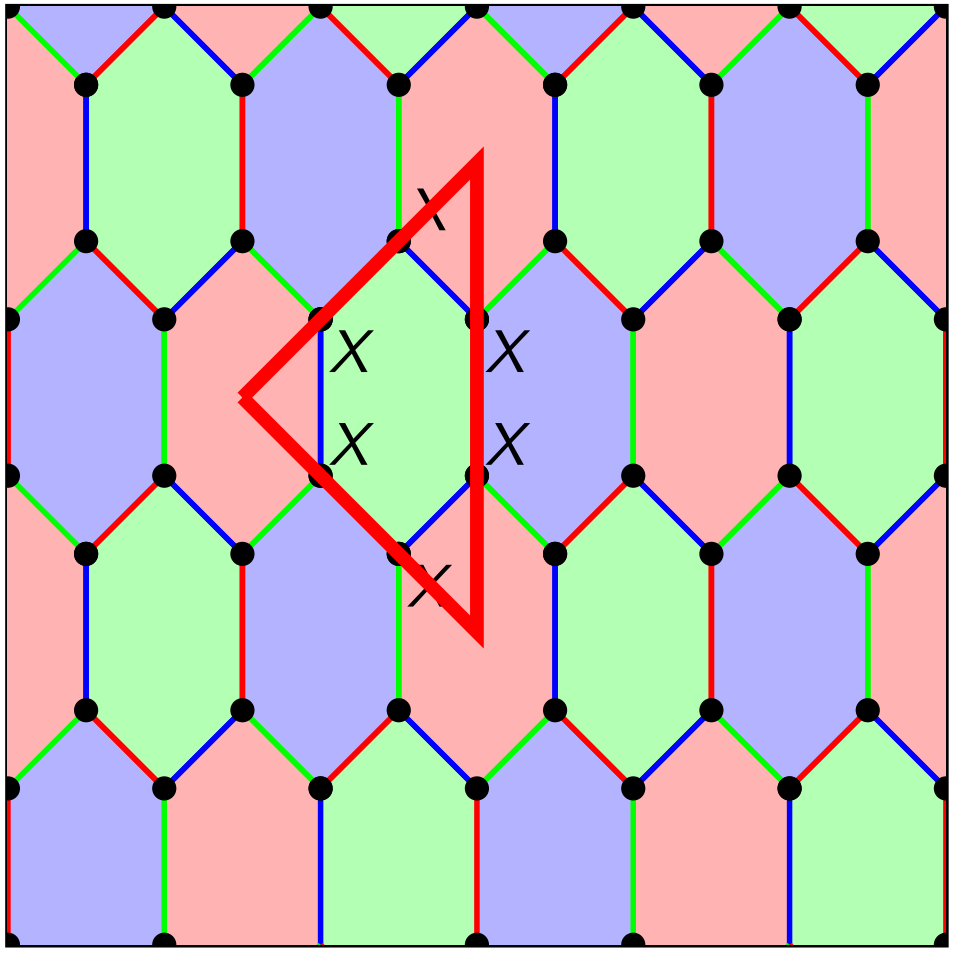


mots quantiques
$= C \text{ mod } C^{\perp}$

On voit une ligne de $\mathbf{H}_X$

FIGURE : Représentation cyclique d'un mot de C

Représentation graphique des mots quantiques



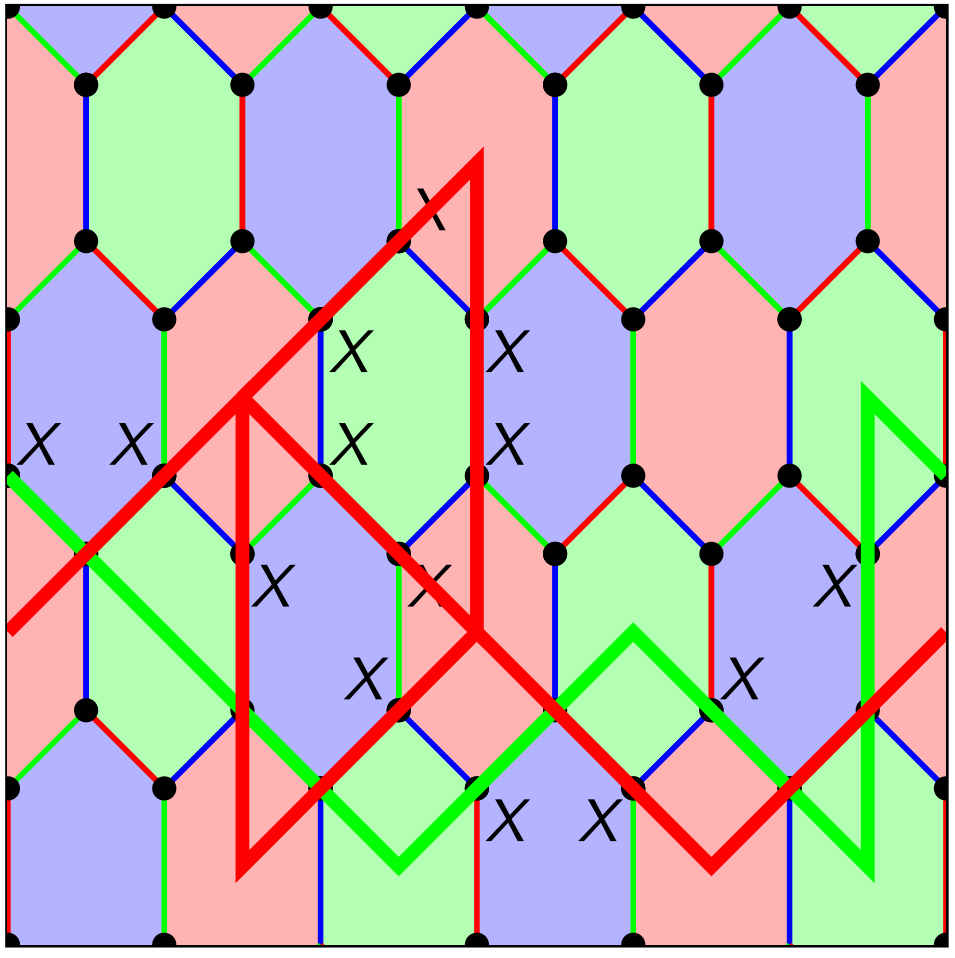
mots quantiques
$= C \text{ mod } C^{\perp}$

On voit une ligne de $\mathbf{H}_X$

C'est une face rouge

FIGURE : Représentation cyclique d'un mot de C

Représentation graphique des mots quantiques



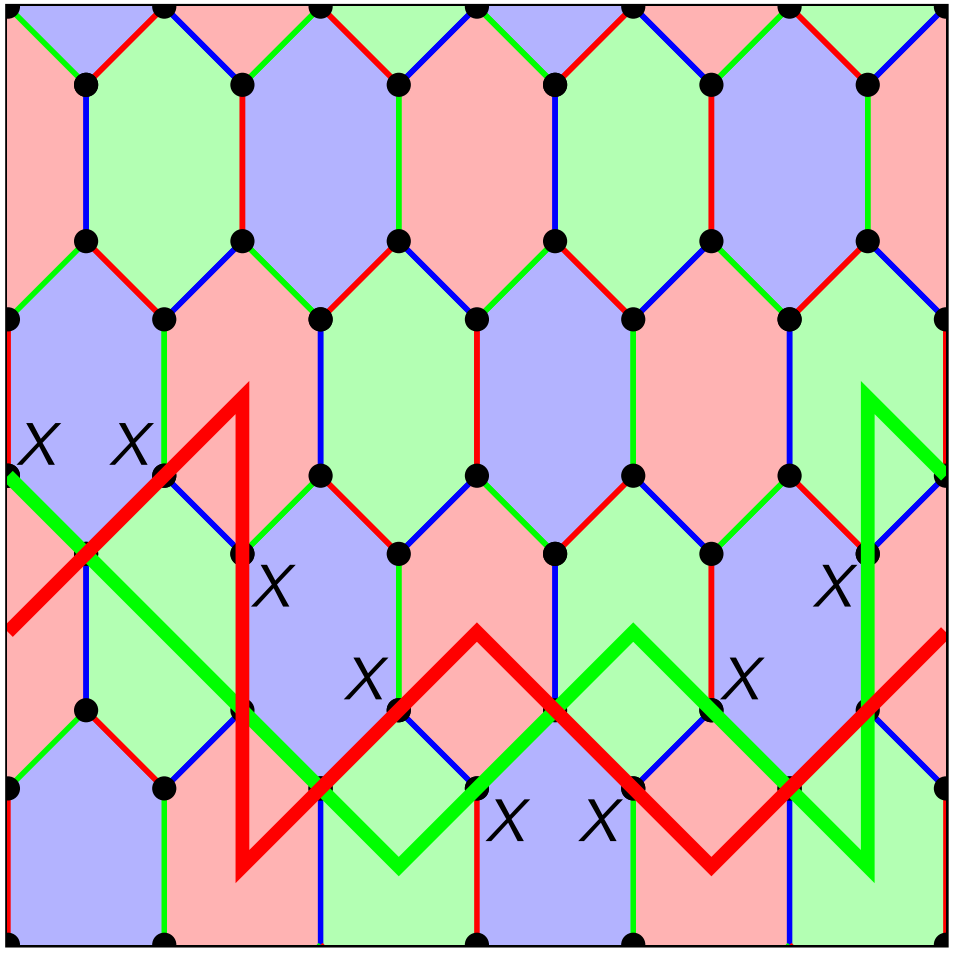
mots quantiques
$= C \text{ mod } C^{\perp}$

On voit une ligne de $\mathbf{H}_X$

C'est une face rouge

FIGURE : Représentation cyclique d'un mot de C

Représentation graphique des mots quantiques



mots quantiques
$= C \bmod C^{\perp}$

On voit une ligne de $\mathbf{H}_X$

C'est une face rouge

FIGURE : Représentation cyclique d'un mot de C

Application des bornes de Gromov

Grâce à cette intrétation graphique :
mot quantique = paire de cycles modulo les faces

- dans une boule planaire pas de mot quantique $\neq 0$
- $k = 4g$ (par la dimension du code des cycles)

Avec des pavages G dont les faces sont de longueur inférieure à m et dont les sommets sont de degré inférieur à m :

Théorème (D. - 2012)

$$kd^2 \leq C(\log k)^2 n,$$

Application des bornes de Gromov

Remarques :

- Avec Gilles Zémor nous avons construits des codes couleur hyperboliques qui atteignent la borne de Gromov pour R constant
- Tout complexe de chaîne permet de définir un code quantique

Questions ouvertes :

- Peut on atteindre $d = O(n^{1/2+\alpha})$ avec des codes LDPC quantiques ?
- seuil des codes de surfaces ?

Application des bornes de Gromov

Merci de votre attention !