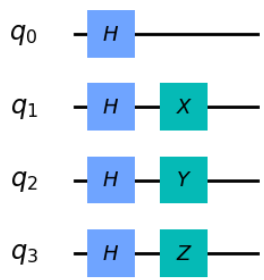
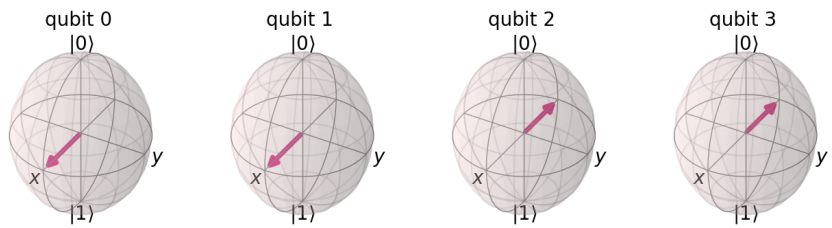
Sur les circuits classiques, reversibles et quantiques

Yvan Le Borgne,
GT Informatique Quantique

8 avril 2020





Références maltraitées (en plus des précédentes)

- https://qiskit.org/textbook: Chapitres 1 (Quantum States and Qubits) et 2 (Multiple Qbits and Entanglement).
- *Elementary gates for quantum computation* de Barenco, Bennett, Cleve, DiVicenzo, Margolus, Shor, Sleator, Smolin, Weinfurter en 1995.
- *The classification of reversible bit operations* de Aaronson, Grier et Schaeffer, 2015.
- *The classification of stabilizer operations over Qubits* de Grier et Schaeffer, 2016.
- *An introduction to quantum error correction and fault-tolerant quantum computation* de Gottesman 2009.

Plan

•1• **Circuits classiques:** Notation matricielle, composition des portes en séquence (produit matriciel) ou en parallèle (produit tensoriel), deux jeux de portes universelles (Treillis de Post) $\{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}\} \cup \{\mathrm{SWAP}, \mathrm{COPY}\}$ et $\{\mathrm{NAND}\} \cup \{\mathrm{SWAP}, \mathrm{COPY}\}$.

•2• **Circuits reversibles:** Portes inversibles (CNOT, Toffoli, Fredkin, . . .), Portes controlées, Classification des jeux de portes.

•3• **Circuits quantiques:** Qubits, Portes unitaires (dont Pauli X, Y, Z, Hadamard H, $\pi/8$), Interférences de Mach-Zender comme une réalisation de circuit quantique, Mesures (dans différentes bases: BB84), Universalité (+Théorème de Solovay Kitaev).

•4• **Des circuits quantiques simulables malgré la superposition:** Stabiliseurs ou quand la sphère de Bloch est remplacée par un cube (Théorème de Gottesman,Knill)

•5• **Un peu de correction d'erreur classique et quantique:** Correction classique par répétition et majorité. Code de Shor à 9 qubits pour la correction quantique.

•1• Circuits classiques

Notation "ket" pour les registres

Un bit $|b>\in\{|0>,|1>\}$,

Deux bits $|b_0 b_1>=|b_0>\otimes|b_1>\in\{|00>,|01>,|10>,|11>\}$

$\ldots n$ bits $|b_0\ldots b_{n-1}>$ dans $(|0>+|1>)^{\otimes n}$.

Ce produit cartésien se généralise en produit tensoriel par exemple si $|b>=p|0>+(1-p)|1>$ et $|b'>=p'|0>+(1-p')|1>$ sont deux bits probabilistes *indépendants* alors

$$|bb'>=|b>\otimes|b'>$$

$$:=pp'|00>+p(1-p')|01>+(1-p)p'|10>+(1-p)(1-p')|11>.$$

Dans le cas quantique, le produit tensoriel travaillera avec des nombres complexes au lieu des booléens ou des réels de $[0,1]$ et traduira la non-intrication (l'indépendance) des sous-systèmes.

Matrices booléennes pour les portes logiques classiques

Pour $n = 2$, l'état d'un registre est une combinaison linéaire des $2^n = 4$ états possibles:

$$|r>= b_{00}|00> +b_{01}|01> +b_{10}|10> +b_{11}|11>= \begin{pmatrix} b_{00} \\ b_{01} \\ b_{10} \\ b_{11} \end{pmatrix}$$

avec exactement un seul coefficient booléen b_{ij} non-nul.

Une porte logique $G = (?_{i,j})_{0\leq i,j\leq 4}$ avec deux bits en entrée et deux bits en sortie comme SWAP ou CNOT est réprésentée par une matrice $2^2 \times 2^2$.

$$\begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{pmatrix} ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{pmatrix} \end{array} \begin{pmatrix} b_{00} \\ b_{01} \\ b_{10} \\ b_{11} \end{pmatrix} = \begin{pmatrix} b'_{00} \\ b'_{01} \\ b'_{10} \\ b'_{11} \end{pmatrix}$$

Exemples de portes

$$\text{Id} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{NOT} := \text{X} := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\text{AND} := \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{OR} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

$$\text{NAND} := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \quad \text{SWAP} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\text{COPY} := \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{CNOT} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

CNOT applique NOT sur le second bit si le premier bit est $|1>$.
(ReLU's style)

Exemples de portes controlées

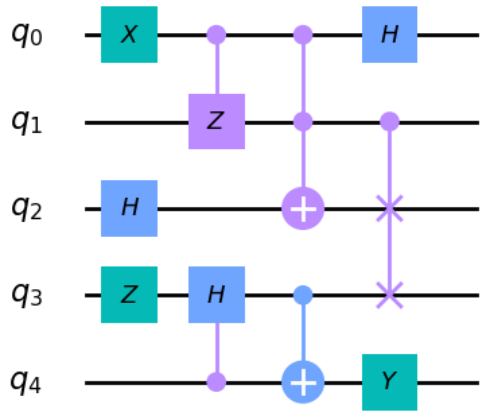
$$(\textit{Fredink})\text{FRE} := \text{CSWAP} :=?$$

$$(\textit{Toffoli})\text{TOF} := \text{CCNOT} :=?$$

Pour une porte G, sa version controlée CG utilise un bit de plus en entrée et sortie qui n'est que lu: la porte G n'est appliquée sur les bits ciblés que si le bit de contrôle est $|1>$.

Remarque: si k bits de contrôle, égaux à $|1^k>$ pour déclencher la porte G sur les bits ciblés, on a aussi la notation $\Lambda^k(G)$ (par exemple $\text{TOF} := \Lambda^2(\text{NOT})$).

Circuits par composition de portes en série et en parallèle



$$H \otimes CSWAP \otimes Y$$

$$\circ$$

$$CCX \otimes CX$$

$$\circ$$

$$CZ \otimes Id \otimes (SWAP \circ CH)$$

$$\circ$$

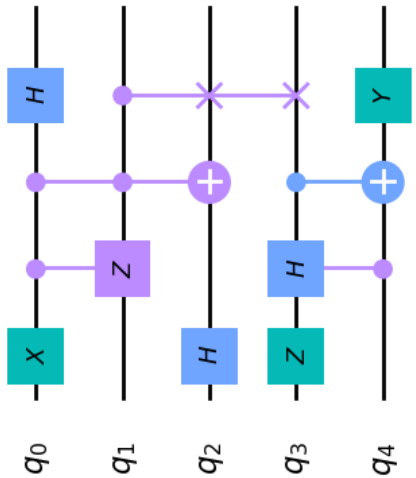
$$X \otimes Id \otimes H \otimes Z \otimes Id$$

$$|q_0 q_1 q_2 q_3 q_4 >$$

Composition en série = Produit de matrice (ici $\circ$).

Composition en parallèle = Produit tensoriel de matrices.

Circuits par composition de portes en série et en parallèle



$$H \otimes CSWAP \otimes Y$$

$$\circ$$

$$CCX \otimes CX$$

$$\circ$$

$$CZ \otimes Id \otimes (SWAP \circ CH)$$

$$\circ$$

$$X \otimes Id \otimes H \otimes Z \otimes Id$$

$$|q_0 q_1 q_2 q_3 q_4 >$$

Composition en série = Produit de matrice (ici $\circ$).

Composition en parallèle = Produit tensoriel de matrices.

Un jeu de portes universelles pour les fonctions booléennes

$\mathbb{B} := \{|0>, |1>\}$.

Une fonction booléenne est une fonction $f : \mathbb{B}^n \to \mathbb{B}$.

Un jeu de porte $\{G_i\}_i$ est universel si toute fonction booléenne s'exprime à l'aide d'un circuit composé de ces portes (avec éventuellement quelques bits auxiliaires initialisés à $|0>$ en plus).

Proposition: $\{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}\} \cup \{\mathrm{SWAP}, \mathrm{COPY}\}$ est universel.

Preuve où les COPY et SWAP sont implicites:

$$f(w) = \bigvee_{v|f(v)=|1>} (w = v) = \bigvee_{v|f(v)=|1>} \left(\bigwedge_{i=0}^{n-1} \mathrm{NOT}^{1-v_i}(w_i) \right)$$

□

Un jeu universel avec moins de portes

Proposition: $\{\text{NAND}\} \cup \{\text{SWAP}, \text{COPY}\}$ est universel.
Preuve:

$$\text{NOT} := \text{NAND} \circ \text{COPY}.$$

$$\text{AND} := \text{NOT} \circ \text{NAND}.$$

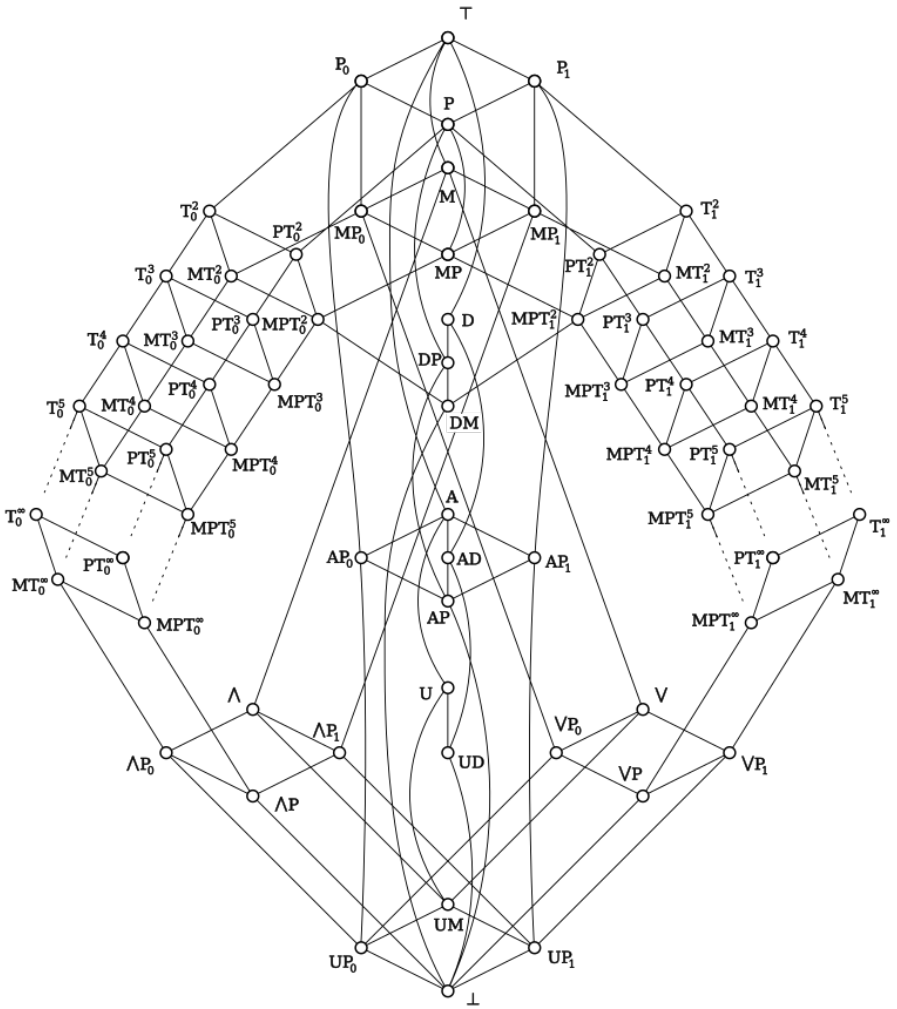
$$\text{OR} := \text{NAND} \circ (\text{NOT} \otimes \text{NOT}).$$

□

Deux type de portes de moins à concevoir mais peut-être des circuits plus gros.

Treillis de Post

Comment ne pas être universel ?



1

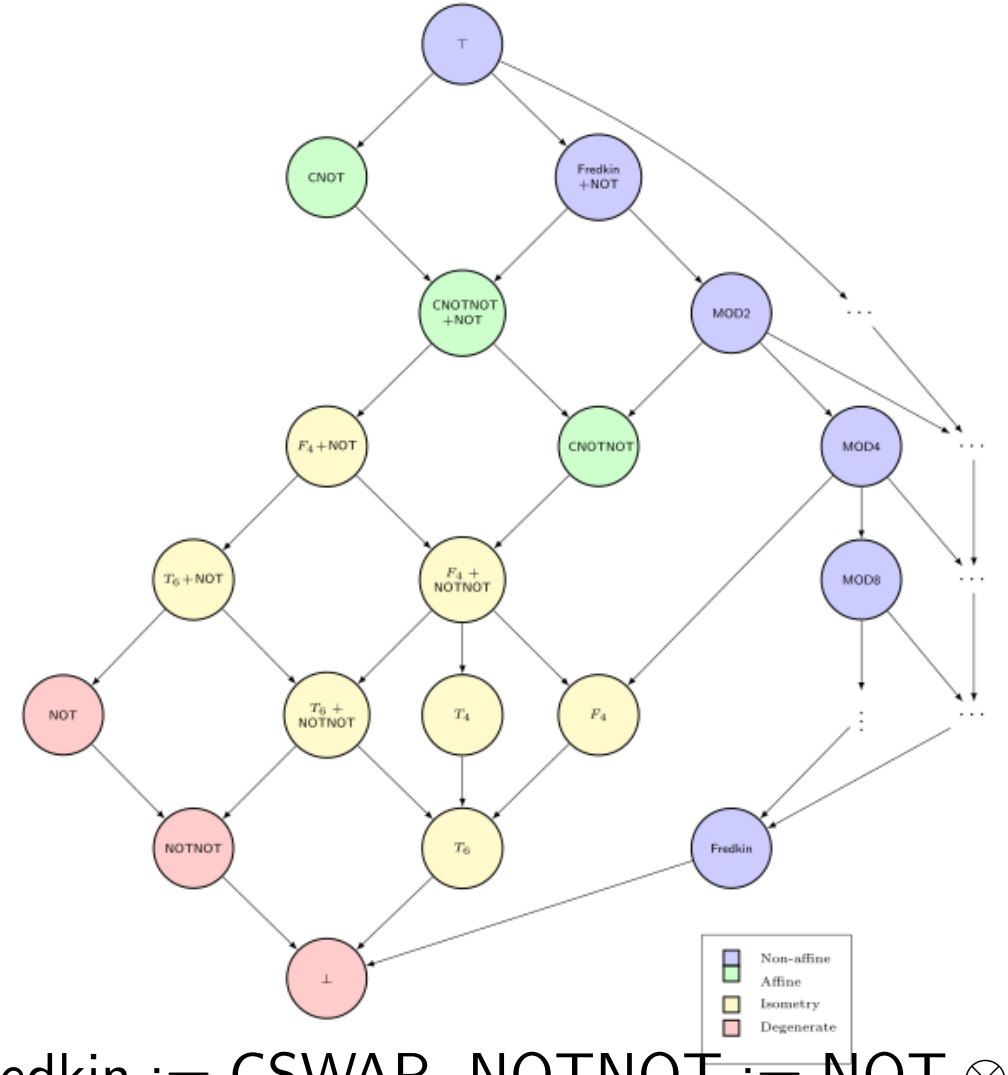
Obstructions:

- Portes monotones comme AND et OR: si $x \leq y$, alors $G(x) \leq G(y)$.
- Portes affines sur $\mathbb{F}_2$ comme NOT et XOR: $f(x_1, x_n) = a_0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n$.
- ...

[1] Diagramme de Hasse du treillis extrait de Wikipedia

•2• Circuits reversibles

Classification des jeux de portes reversibles [AGS15]



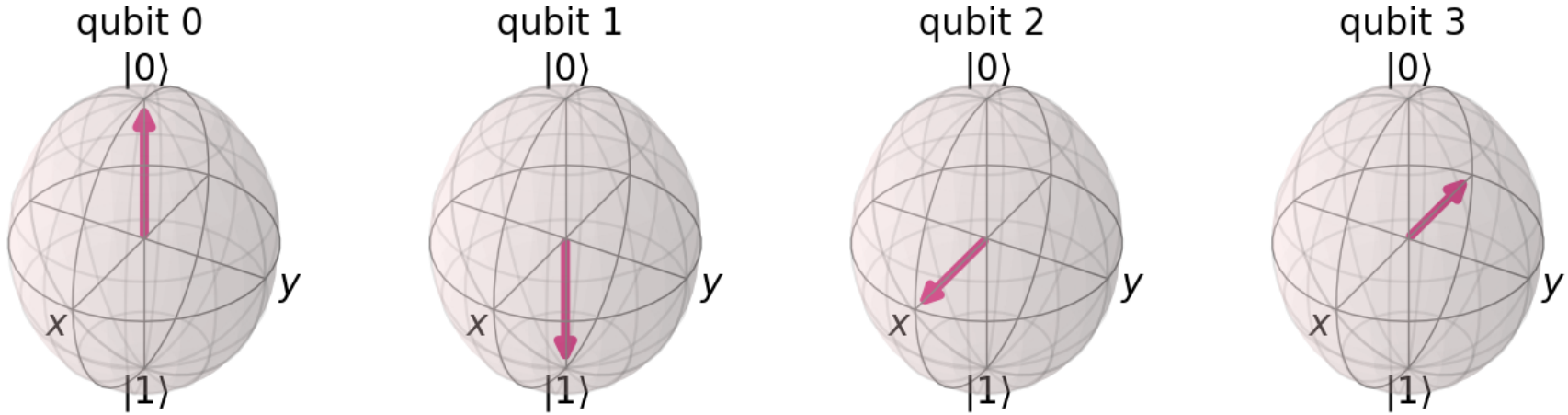
T := TOF, Fredkin := CSWAP, NOTNOT := NOT $\otimes$ NOT,
MOD2^k := CSWAP+ échange 0^k et 1^k laissant le reste invariant.
T$^k(x)$:= NOT$^{\otimes k}(x)$ si $|x| := \bigoplus_{i=0}^{k-1} x_i$ est impair, sinon x.
F^k := NOT$^{\otimes k} \circ$ T^k.

•3• Circuits quantiques

Quantum bit (Qubit) et sphère de Bloch

$$|b>=\alpha|0>+\beta|1>=\cos(\theta/2)|0>+e^{i\phi}\sin(\theta/2)|1>$$

où $\alpha, \beta \in \mathbb{C}$ et $|\alpha|^2+|\beta|^2=1=\alpha\overline{\alpha}+\beta\overline{\beta}$, $\theta \in [0,\pi], \phi \in [0,2\pi)]$.



$\|0>$	$\|1>$	$\frac{1}{\sqrt{2}}(\|0>+\|1>)$	$\frac{1}{\sqrt{2}}(\|0>-\|1>)$
$\theta=0,\phi=0$	$\theta=\pi,\phi=0$	$\theta=\pi/2,\phi=0$	$\theta=\pi/2,\phi=\pi$

.

A partir d'un état $|q>=\sum_i \alpha_i|i>$ décrit dans une base $(|i>)_i$ par les amplitudes $(\alpha_i)_i$, la probabilité de mesurer/projeter l'état $|q>$ en l'état déterministe $|i>$ est $\alpha_i\overline{\alpha_i}=|\alpha_i p|^2$

Portes quantique, transformations unitaires

$$|b>=\sum_i \alpha_i |i>$$

$$\sum_i |\alpha_i|^2 = 1 = \sum_i \alpha_i \overline{\alpha_i} = (\alpha, \overline{\alpha}) =: \|\alpha\|^2$$

où $\alpha := (\alpha_i)_i$ est le vecteur des amplitudes.
Une porte quantique G doit préserver la mesure de probabilité donc la matrice G doit préserver la distance $\|.\|$ car en terme de vecteur d'amplitudes $\|\alpha\|^2 = 1 = \|G\alpha\|^2$.
Cette condition nécessaire méne avec des arguments de la physique au fait que les portes quantiques G correspondent aux transformations unitaires: $GG^* = Id = G^*G$ où l'inverse $G^* := \overline{G}^t$.

Ex: Porte à 1 qubit du "jeu d'instructions" QASM (IBM),

$$U_3(\theta, \phi, \lambda) := \begin{pmatrix} \cos\theta/2 & -e^{i\lambda}\sin(\theta/2) \\ e^{i\phi}\sin(\theta/2) & e^{i\lambda+i\phi}\cos(\theta/2) \end{pmatrix}.$$

Un peu de zoologie sur les portes quantiques

$$\mathrm{U}_3(\theta,\phi,\lambda) := \begin{pmatrix} \cos\theta/2 & -e^{i\lambda}\sin(\theta/2) \\ e^{i\phi}\sin(\theta/2) & e^{i\lambda+i\phi}\cos(\theta/2) \end{pmatrix}, (\theta,\phi,\lambda) \in [0,4\pi)^3;$$

$$\mathrm{Id} := \mathrm{U}_3(0,0,0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; (\textit{Hadamard})\mathrm{H} := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix};$$

$$\mathrm{NOT} := \mathrm{X} := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \mathrm{Y} := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \mathrm{Z} := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix};$$

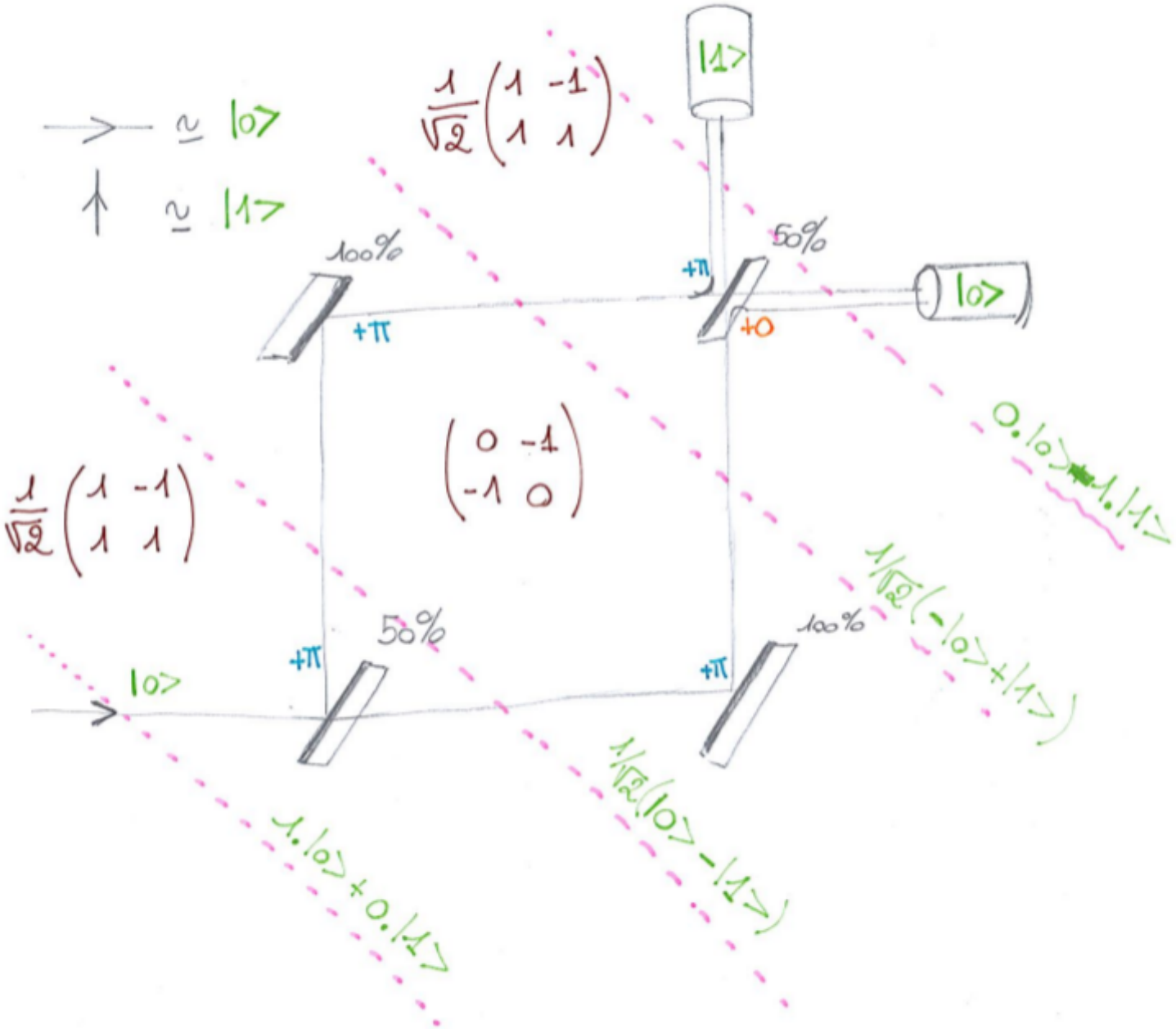
X, Y, Z forment les portes de Pauli.

$$\mathrm{R}_\phi := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}; \mathrm{S} := \sqrt{\mathrm{Z}} := R_{\pi/2}; \mathrm{T} := \sqrt{\sqrt{\mathrm{Z}}} := R_{\pi/4};$$

$$\mathrm{SWAP} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \mathrm{CNOT} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$(\textit{Fredink})\mathrm{FRE} := \mathrm{CSWAP}$ $(\textit{Toffoli})\mathrm{TOF} := \mathrm{CCNOT}$

$H \circ X \circ H|0> = |1>$ et l'interferomètre de Mach-Zehnder



BB84 pour illustrer les mesures dans différentes bases

Jeux de portes universels ou non

Universels:

$\{\text{CNOT}, (\text{U}_3(\theta, \phi, \lambda))_{(\theta,\phi,\lambda)\in[0,4\pi)^3}\}$ [Barenco et all]

$\{\text{H}, \text{TOF}\}$ [Shi]

$\{\text{NOT}, \text{SWAP}, \text{TOF}\} \cup \{\text{H}, \text{T} = \text{R}_{\pi/4}\}$ [Kitaev,Shen,Vialyi]

Non-universels:

Jeux préservant les bases (comme $\{\text{SWAP}\}$).

Les jeux de portes manipulant un seul qubit.

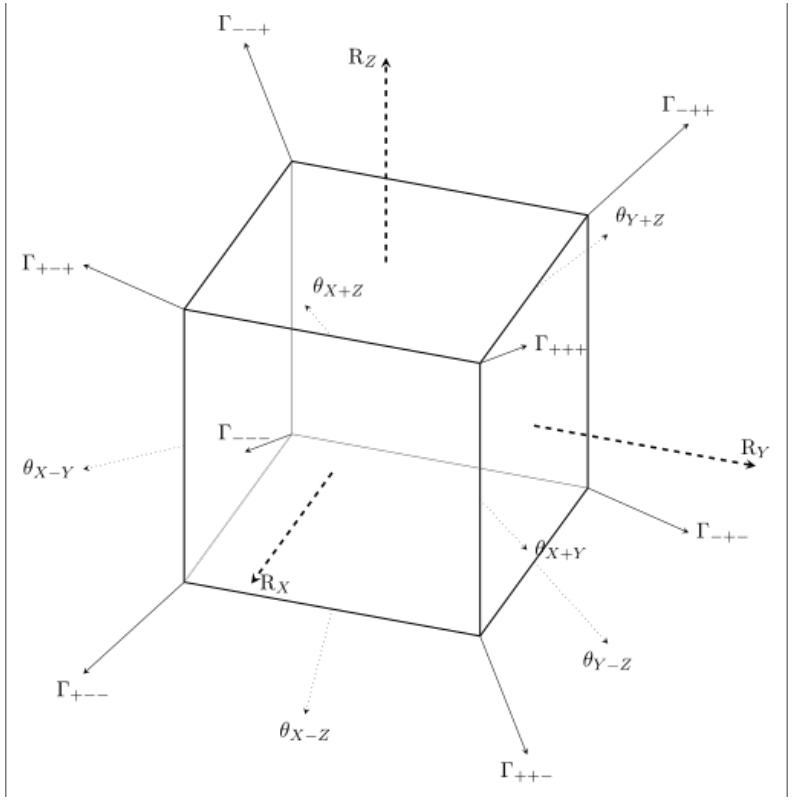
Les stabiliseurs $\{\text{CNOT}, H, S = \text{R}_{\pi/2}\}$.

Théorème (Solovay-Kitaev): Pour tout jeu de porte universel $\mathcal{G} := \{G_i\}_i$, et toute précision $\epsilon > 0$ souhaitée, il existe une constante c telle que pour toute transformation unitaire U, il existe un $\mathcal{G}$-circuit d'au plus $O(\log^c(1/\epsilon))$ portes générant une transformation unitaire S à distance au plus ϵ de U.

•4• Circuits quantiques simulables

Théorème de Gottesman et Knill autour des stabiliseurs

Les $\{\mathrm{H}, \mathrm{S} = \mathrm{R}_{\pi/2}, \mathrm{CNOT}\}$-circuits avec des mesures "sur les bases de Pauli" forment un jeu de portes non-universelle autorisant la superposition d'états.



Théorème Ces circuits quantiques sont simulables parfaitement en temps polynomial par une machine classique probabiliste

Classification des circuits de stabiliseurs [GS16]

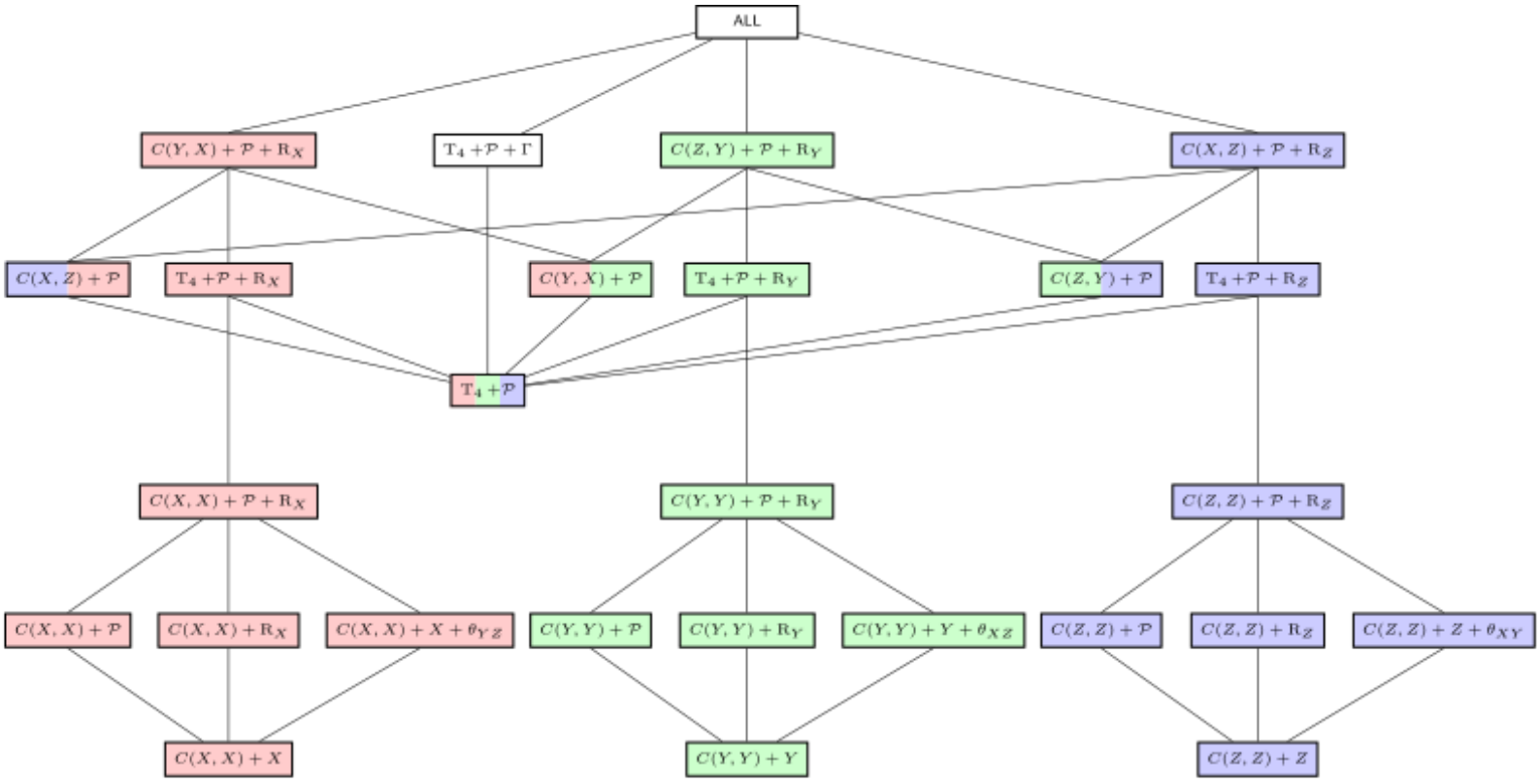


Figure 5: The inclusion lattice of non-degenerate stabilizer gate classes. Red, green, blue denote X-, Y-, and Z-preserving, respectively.

Généralisation de la porte CNOT pour deux portes P et Q:

$$\mathrm{C}(\mathrm{P},\mathrm{Q}) = \frac{1}{2}\left(\mathrm{Id}\otimes\mathrm{Id} + \mathrm{P}\otimes\mathrm{Id} + \mathrm{Id}\otimes\mathrm{Q} - \mathrm{P}\otimes\mathrm{Q}\right)$$

Exemple: CNOT := C(Z, X).

•5• Correction d'erreur, tolérance aux fautes

Correction d'erreur vs Tolérance aux fautes

• Correction d'erreur: Des erreurs peuvent avoir été commises et on dispose de moyens de calcul sans erreur pour les corriger.
• Tolérance aux fautes: Des erreurs peuvent avoir eté commises et on dispose de moyens de calcul susceptible également de faire des erreurs pour les corriger.
$\Longrightarrow$ Introduction à la simple correction d'erreur classique et quantique.
$\Longrightarrow$ La multiplicité des bases universelles est motivée par des aspects de tolérance aux fautes.