Réécriture et Calcul quantique

Pablo Arrighi*, Gilles Dowek†

13.03.04, Nancy

*arrighi@univ-mlv.fr, IGM, Université de Marne-la-Vallée
†gilles.dowek@polytechnique.fr, LIX, Ecole Polytechnique

La théorie quantique
- Le principe de superposition
- Les états
- Les évolutions
- Les mesures
- Les systèmes composés

Un premier algorithme
- Le problème
- La solution

Fiction ou réalité?

Modèles de calcul quantiques

Le principe de superposition

Si ψ et ϕ sont deux états possibles d'un sytème, alors $\alpha\psi + \beta\phi$ l'est aussi (avec $|\alpha|^2 + |\beta|^2 = 1$).

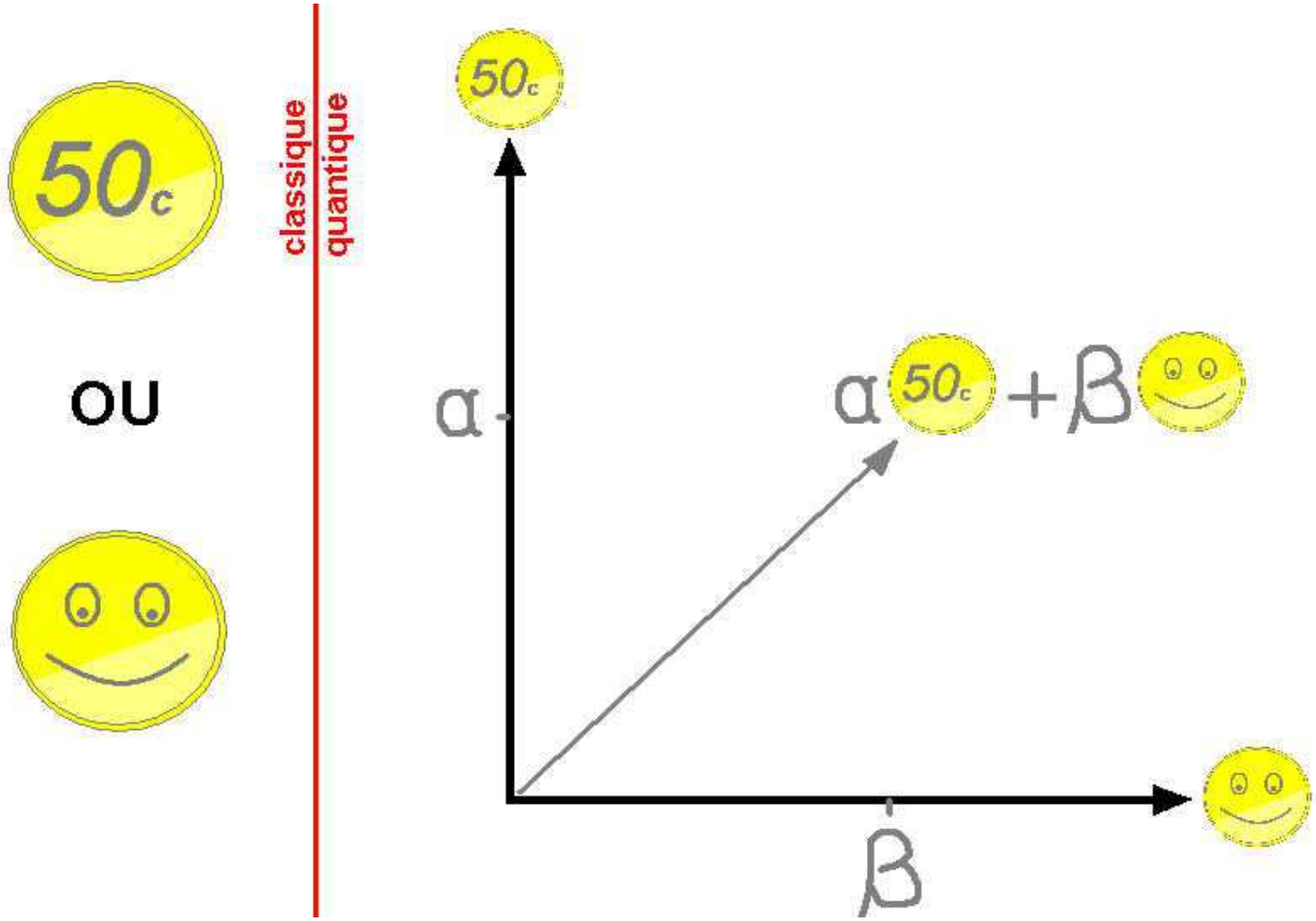
Analogie avec le parallèlisme.

Les états

L' *état* d'un *système physique clos* est entièrement décrit par un vecteur de nombres complexes de norme un. Autrement dit c'est un vecteur $v \in \mathbb{C}^n$ vérifiant:

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \quad \text{et} \quad v^\dagger v = v_1^* v_1 + \ldots + v_n^* v_n = 1.$$

$\rightarrow$ OK pour l'informatique quantique de ne considérer que les nombres réels.


50c
classique
quantique
ou
50c
α
α 50c + β
β

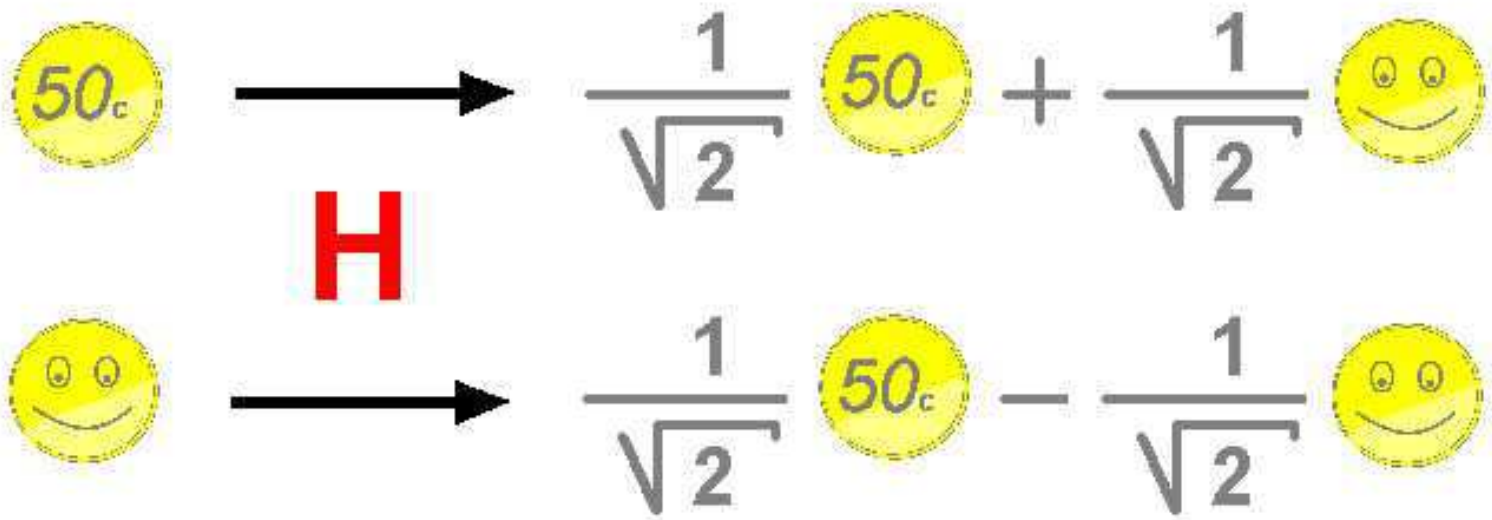
Les évolutions

Un système physique clos dans un état v, évolue, après une certaine période de temps, en un état w selon l'équation

$$w = Uv$$

où U est une matrice unitaire $n \times n$, i.e. $U^\dagger U = Id$.

Notons que les transformations unitaires préservent le produit scalaire et donc la norme. (Rotations complexes). Electronique réversible plus quelques portes telles...


50c
H
1/√2 50c + 1/√2
1/√2 50c − 1/√2

Les mesures

Lorsqu'un système physique ayant pour état

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

est *mesuré*, on obtient le résultat i avec probabilité $p_i = |v_i|^2$.

(...)

Si le résultat i advient, alors le système se trouve désormais dans l'état:

$$w = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i^{th} \text{ position}$$

Notons que la condition de normalization équivaut à $\sum_i p_i = 1$.

. . . S'agit-il donc de simples probabilités? Le détour par les amplitudes était-il bien utile? cf. Deutsch Josza et cryptographie quantique, pour laquelle il faut les complexes.

On mesure $\frac{1}{\sqrt{2}}$  $+ \frac{1}{\sqrt{2}}$ 

On obtient

Avec probabilité 1/2 → Résultat "Pile", Nouvel état: 

Avec probabilité 1/2 → Résultat "Face", Nouvel état: 

Les systèmes composés

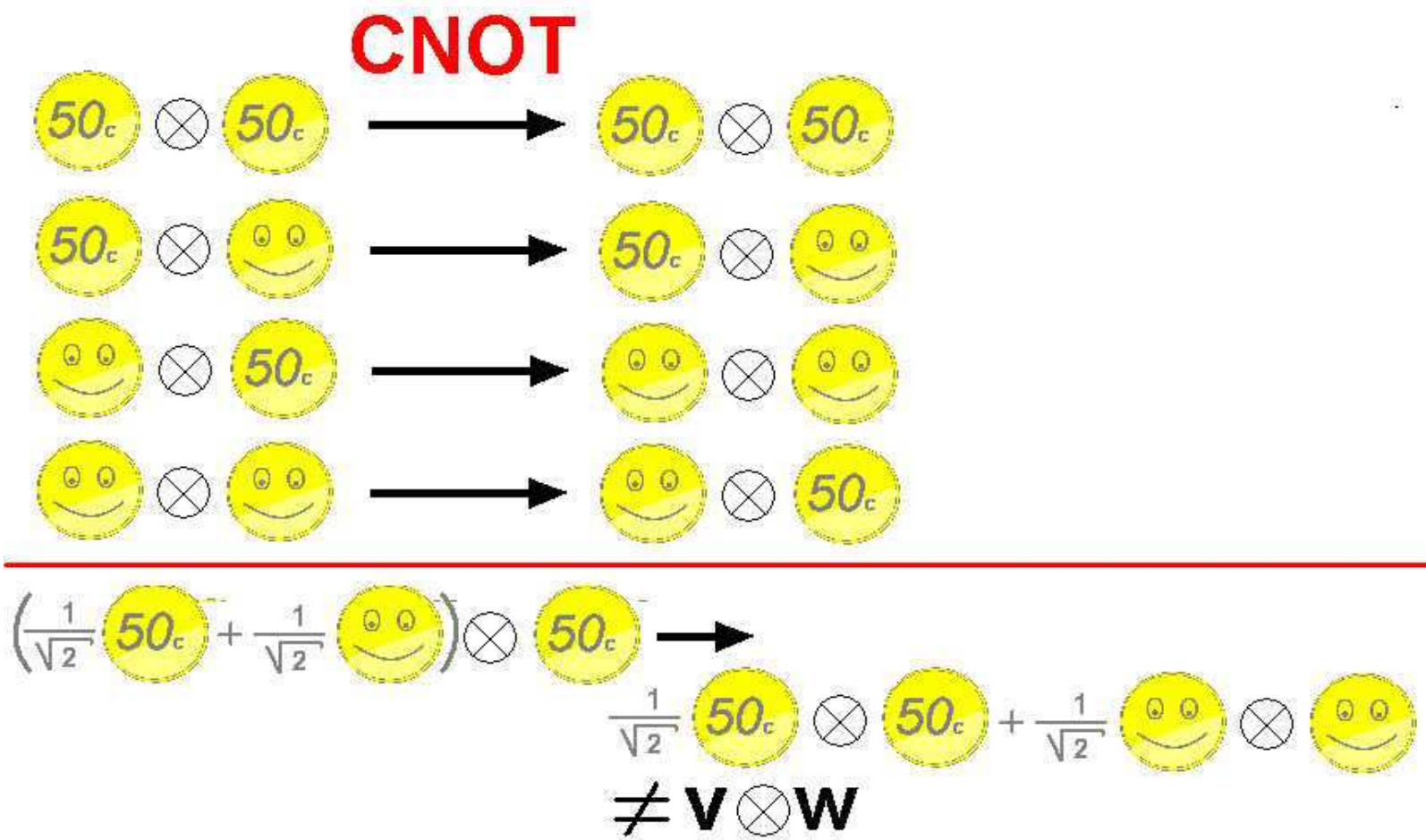
Soit un système physique A d'état $v \in \mathbb{C}^n$.
Soit un système physique B d'état $w \in \mathbb{C}^m$.
L'état du sytème composé AB est un élément de $\mathbb{C}^n \otimes \mathbb{C}^m$.

Notons que $\mathbb{C}^n \otimes \mathbb{C}^m$ est un espace vectoriel de dimension mn. Il faut faire des calculs sur 2^N nombres pour simuler un système quantique de N qubits. Pour simuler un système quantique, il faut un sytème quantique (Feynman).

La seule chose à savoir sur $\otimes$ c'est qu'il est bilinéaire:

$$\lambda.v \otimes w = v \otimes \lambda.w = \lambda.(v \otimes w)$$
$$(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$$
$$v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2$$

.


CNOT
$\left(\frac{1}{\sqrt{2}}50_c + \frac{1}{\sqrt{2}}\right) \otimes 50_c \rightarrow$
$\frac{1}{\sqrt{2}}50_c \otimes 50_c + \frac{1}{\sqrt{2}} \otimes$
$\neq v \otimes w$

Le problème

- Nous est donné une boîte noire **F** : $\mathrm{Bool} \longrightarrow \mathrm{Bool}$.
- On souhaite calculer le 'ou exclusif' (dénoté $\oplus$) de **F**(Vrai) et **F**(False).
- Au bout de sa première utilisation la boîte noire s'autodétruira! (ou disons juste que son utilisation est coûteuse en temps, argent...)

... Clairement, c'est mission impossible?

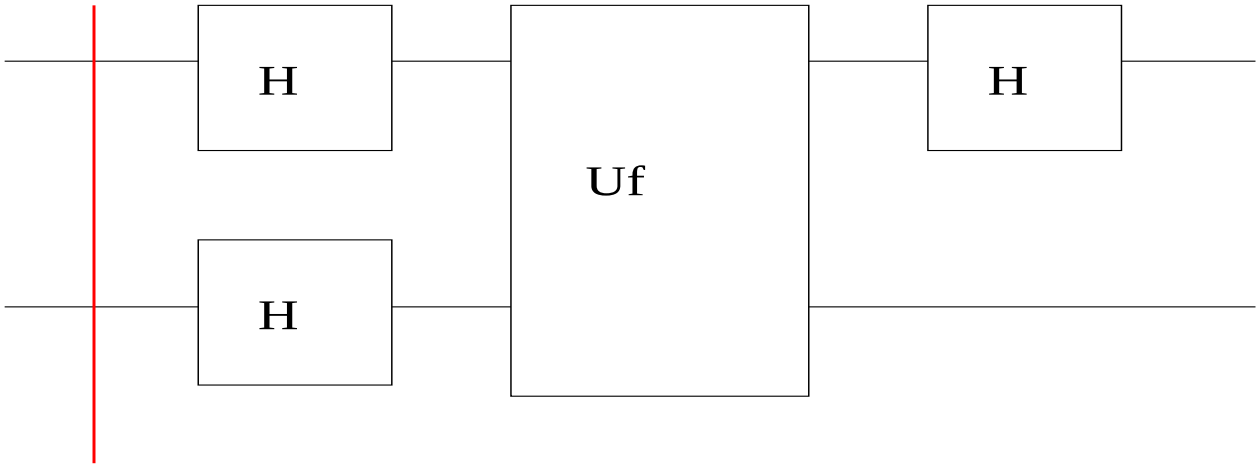
La solution

On suppose **F** implémentée par une boîte quantique:

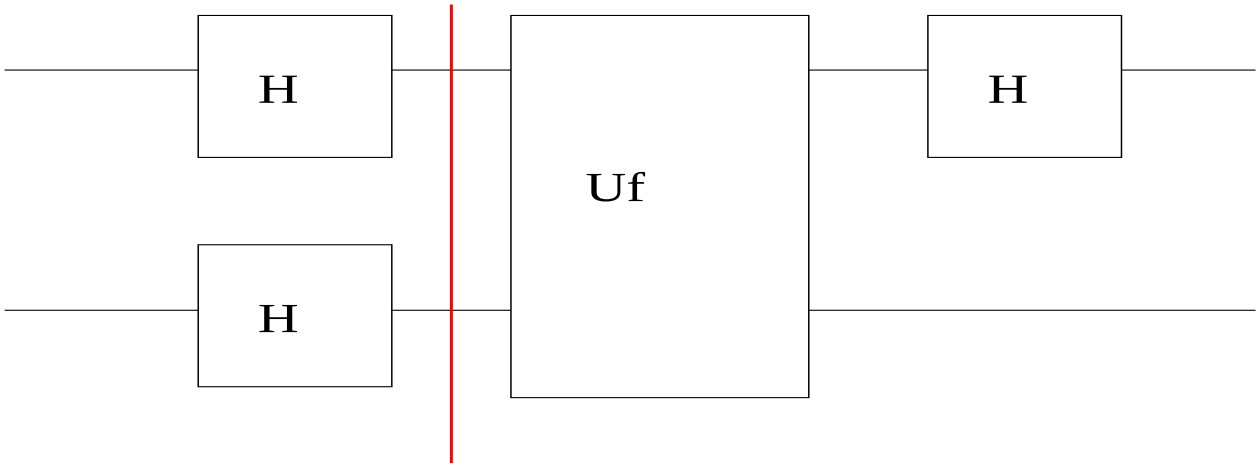
$$a \otimes b \xrightarrow{U_f} a \otimes (\mathbf{F}(a) \oplus b)$$

où a et b sont des valeurs booléennes.

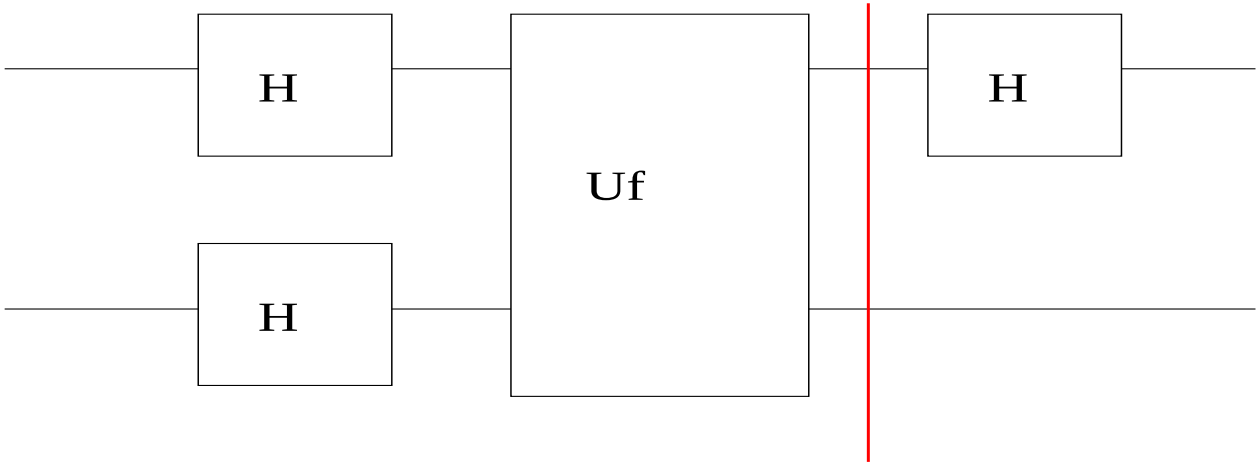
Autrement dit **F** est appliquée à la première valeur booléenne, mais le résultat est enregistré dans la seconde via un $\oplus$. Nécessaire pour avoir l'unitarité.



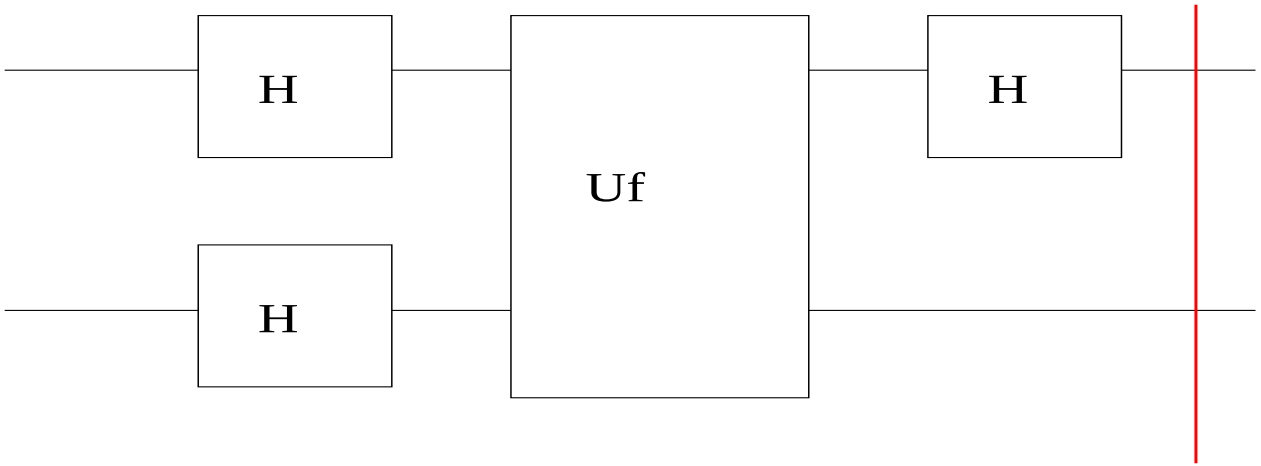
$$\text{Faux} \otimes \text{Vrai}$$



$$\frac{1}{\sqrt{2}}(\text{Faux} + \text{Vrai}) \otimes \frac{1}{\sqrt{2}}(\text{Faux} - \text{Vrai})$$
$$= \frac{1}{2}\left(\text{Faux} \otimes (\text{Faux} - \text{Vrai}) + \text{Vrai} \otimes (\text{Faux} - \text{Vrai})\right)$$



$$\frac{1}{2}\left((-1)^{\mathbf{F}(\mathit{Faux})}\mathrm{Faux}\otimes(\mathrm{Faux}-\mathrm{Vrai})+(-1)^{\mathbf{F}(\mathit{Vrai})}\mathrm{Vrai}\otimes(\mathrm{Faux}-\mathrm{Vrai})\right)$$
$$=\frac{1}{\sqrt{2}}((-1)^{\mathbf{F}(\mathit{Faux})}\mathrm{Faux}+(-1)^{\mathbf{F}(\mathit{Vrai})}\mathrm{Vrai})\otimes\frac{1}{\sqrt{2}}(\mathrm{Faux}-\mathrm{Vrai})$$
$$=\pm\frac{1}{\sqrt{2}}(\mathrm{Faux}+(-1)^{\mathbf{F}(\mathit{Faux})\oplus\mathbf{F}(\mathit{Vrai})}\mathrm{Vrai})\otimes\ldots$$



$$\pm(\mathbf{F}(\mathit{Faux}) \oplus \mathbf{F}(\mathit{Vrai})) \otimes \ldots$$

Fiction ou réalité?

- Des algorithmes plus utiles: Shor, Grover.
- Une théorie centenaire et vérifiée expérimentalement.
- Diverses pistes de réalisations physiques: ions, photons, quantum dots...

- Les critères de DiVicenzo sont en concurrence: isolation du sytème, possibilité de le préparer dans un état initial, de le faire évoluer arbitrairement, de le mesurer.
- Plus le système est grand, plus c'est difficile, mais passé un certain seuil les codes de correction quantique d'erreur prennent le relais.
- Deutsch-Josza a été implémenté, on a factorisé 15, des systèmes de cryptographie quantique sont commercialisés.

Modèles de calcul quantiques

- *Le modèle des circuits quantiques.* Universalité au sens des circuits: pas de structures de contrôle. Opaque.
- *La machine de Turing quantique.* Véritable universalité. Très opaque:

$$\delta : Q \times \Sigma \longrightarrow (Q \times \Sigma \times \{Left, Right\} \to \tilde{\mathbb{C}}).$$

...plus une contrainte d'unitarité.

Il manque l'informatique quantique un modèle de calcul qui soit:

- Universel au sens de la machine de Turing
- Utilisable pour la programmation, proche de ses spécifications
- Pas une simple juxtaposition de controle classique et de circuits quantiques

Les boucles WHILE, branches IF etc. semblent fondamentalement classiques. L'approche fonctionnelle semble prometteuse:

- Structure de contrôle plus compatible avec la quantique
- Proximité avec la spécification et la logique
- Possibilité d'une sémantique opérationnelle en système de réécriture

Nous aurions donc:

$$(H \otimes Id)U_f(H\ \mathrm{Faux} \otimes H\ \mathrm{Vrai})$$

...la suite cet après-midi.