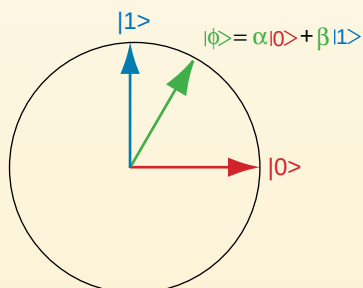


a)



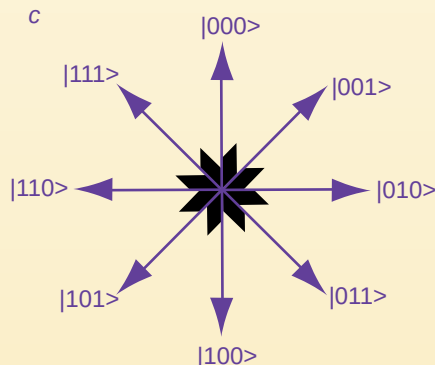
a) L'information unitaire classique est le bit : un objet qui vaut 0 ou 1.

b)



b) L'information unitaire quantique est le qubit (quantum bit). C'est un vecteur dans un espace complexe de dimension 2 muni d'un produit scalaire (deux vecteurs dont le produit est nul sont orthogonaux). Les éléments d'une base orthogonale sont fixés et notés $|0\rangle$ et $|1\rangle$. Un qubit $|\phi\rangle$ se représente sous la forme $\alpha|0\rangle + \beta|1\rangle$ avec $|\alpha|^2 + |\beta|^2 = 1$, où α et β sont des nombres complexes (ainsi le qubit est déterminé par quatre nombres réels). Une mesure amène le qubit $|\phi\rangle$ sur l'un des vecteurs de la base $|0\rangle$, $|1\rangle$. Les règles de la mécanique quantique indiquent qu'on obtient, lors d'une mesure physique, $|0\rangle$ avec la probabilité $|\alpha|^2$ et $|1\rangle$ avec la probabilité $|\beta|^2$.

c)



c) L'état quantique d'un N-qubit est un vecteur dans un espace analogue à celui du qubit, mais de dimension 2^N . On choisit une base orthogonale de cet espace. Pour un 3-qubit on choisit une base orthogonale dont les vecteurs sont : $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$, $|111\rangle$.

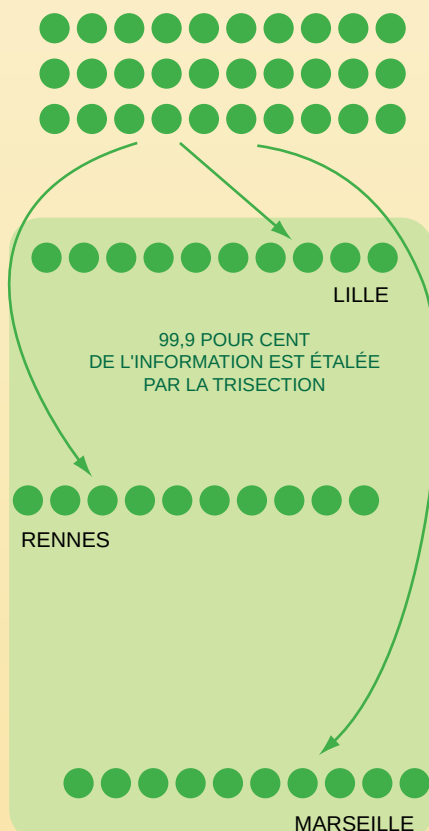
Un état général du 3-qubit est de la forme :

$$a_{000}|000\rangle + a_{001}|001\rangle + a_{010}|010\rangle + a_{011}|011\rangle + a_{100}|100\rangle + a_{101}|101\rangle + a_{110}|110\rangle + a_{111}|111\rangle,$$

où la somme des carrés des $|a_{ijk}|$ est égale à 1.

La lecture du 3-qubit donne un vecteur de la base, chaque vecteur de la base étant obtenu avec une probabilité proportionnelle à $|a_{ijk}|$.

e)



d) Réaliser un calcul quantique consiste à préparer un N-qubit dans un état initial standard, par exemple $|00\dots 0\rangle$ puis à appliquer à cet état une série de transformations unitaires (ce sont des opérations analogues en dimension quelconque aux rotations d'un vecteur). À la fin de cette suite de transformations, on mesure le N-qubit par une expérience qui l'amène dans un état correspondant à un vecteur de la base orthogonale, ce qui donne par exemple $|001\rangle$. Le résultat de cette mesure est probabiliste : on ne sait jamais ce que l'on va trouver. Tout l'art de la programmation quantique réside dans le choix des opérateurs qu'on applique de façon à ce qu'il se produise quelque chose d'intéressant (par exemple, la factorisation d'un entier). Le plus souvent, un calcul quantique commence par la création d'une superposition homogène de tous les états de la base. Pour un 3-qubit, par exemple, on commence par créer : $[|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle] / \sqrt{8}$. Un N-qubit est un objet difficile à décrire : il faut, pour le spécifier complètement, indiquer 2^N nombres complexes.

Il n'était pas évident que les règles délicates du calcul quantique par transformations unitaires produisent des résultats intéressants. C'est pourtant ce qu'ont montré Peter Shor, Lov Grover et les algorithmiciens quantiques.

e) La non-localité : un résultat de Don Page

La possibilité de coder des informations globalement dans un N-qubit est mise en évidence par l'exemple suivant : un de vos amis choisit un 30-qubit et en prépare un très grand nombre d'exemplaires (comme il l'a choisi lui-même, cela ne contredit pas le principe de non-duplication). En faisant une série assez longue de mesures sur les divers exemplaires du 30-qubit on peut en reconstituer l'état avec exactitude. Mais, au lieu de cela, on divise chaque 30-qubit en trois sous-ensembles de 10-qubit qu'on envoie à Rennes, Lille et Marseille. En faisant des mesures localement et indépendamment dans ces trois villes (c'est-à-dire sans coordonner ni corrélérer les mesures), on ne peut, d'après un résultat de Don Page, tirer en moyenne que moins d'un millième de l'information contenue dans le 30-qubit, et cela quel que soit le nombre de copies dont on dispose. L'information contenue dans le 30-qubit est intrinsèquement non locale, les composantes sont corrélées, et seules des mesures collectives peuvent la révéler.