



Comprendre l'informatique quantique - qubits

On peut comprendre le fonctionnement d'un ordinateur quantique sans trop se plonger dans la mécanique quantique au-delà de la compréhension de ses mécanismes de base, vus dans dans l'**épisode précédent de cette série d'articles**, et surtout celui de l'intrication. Par contre, il faut se plonger un peu dans quelques éléments de mathématiques, d'algèbre linéaire et de trigonométrie, ce que nous allons commencer à faire ici.

Le premier élément de base d'un ordinateur quantique est l'inévitable qubit. Vous avez certainement déjà entendu parler de cet objet mystérieux capable d'être simultanément dans la valeur 0 et 1. Les explications courantes s'arrêtent le plus souvent là et vous tombez immédiatement dans l'expectative, vous demandant comment cela peut ensuite bien fonctionner.

Nous allons donc commencer ici par expliquer le fonctionnement logique, mathématique et matériel de ces qubits. Dans la partie suivante de cette série d'articles, nous irons plus loin en décrivant tour à tour les registres, les portes, l'organisation et l'architecture complète d'un ordinateur quantique. A chaque fois, lorsque nécessaire, nous ferons le parallèle avec les ordinateurs traditionnels.

Pour pouvoir suivre cette partie, il faut connaître quelques basiques mathématiques : la trigonométrie, les vecteurs et matrices et avoir déjà entendu parler des nombres complexes.



(ci-dessus, illustration de la conférence "Le quantique, c'est fantastique" du 14 juin 2018 à

Nantes au Web2day par H el ene Pouille, c.f. **son site** et la **vid e de la conf rence**)

Le principe des qubits

Les qubits sont les  l ments de manipulation de base de l'information dans les ordinateurs quantiques. Ils s'opposent aux bits de l'informatique traditionnelle. Avec eux, on passe d'un monde d terministe   un monde probabiliste.

Dans l'informatique traditionnelle, les bits correspondent   des charges  lectriques circulantes qui traduisent le passage d'un courant  lectrique ou son absence. Un bit est de valeur 1 si le courant passe soit de 0 si le courant ne passe pas. La lecture d'un bit donne 1 ou 0. Elle est d terministe,   savoir que si l'on r p te l'op ration de lecture plusieurs fois, ou l'op ration de lecture apr s une r dition du calcul, on obtiendra normalement le m me r sultat.

C'est vrai aussi bien pour le stockage de l'information que pour son transport et pour les traitements dans des processeurs. Ceci est valable modulo les erreurs qui peuvent intervenir dans le parcours. Celles-ci interviennent le plus souvent au niveau de la m moire et sont corrig es via des syst mes... de correction d'erreurs utilisant de la redondance.

	bits : 0 ou 1	qubits : 0 et 1
�tats	deux �tats possibles exclusifs	deux �tats possibles simultan�s
initialisation	0 ou 1	0
repr�sentation interne	0 ou 1	vecteur � deux dimensions
dimensionnalit� interne	1 binary digit	deux nombres flottants
modifications	portes logiques	portes quantiques
lecture	0 ou 1, d�terministe	0 ou 1, probabiliste

Dans un qubits, rien   voir ! Si les qubits sont g n ralement initialis s   0, les op rations portant dessus vont g n ralement les amener   avoir un  tat de superposition entre 0 et 1. Ces  tats correspondent   l' tat de base ("ground state") et   l' tat excit  ("excited state") d'un syst me quantique   deux  tats possibles. Ces qubits peuvent donc  tre   la fois   la valeur 0 et 1, et dans une proportion qui est variable et qui correspond   la notion de superposition d' tats  voqu e dans la partie pr c dente sur les fondements de la m canique quantique. A la fin des calculs, lorsque l'on lit la valeur d'un qubit, on retrouve 0 ou 1. La richesse des valeurs du qubits se manifeste donc uniquement pendant les calculs et non pas   leur initialisation o  lors de leur lecture   la fin des calculs. C'est un concept que vous ne comprendrez compl tement que lorsque nous aurons d crit quelques algorithmes quantiques lors d'une partie suivante de cette s rie.

Ici, nous allons d'abord creuser le mod le math matique de repr sentation des qubits et comprendre comment on peut se le repr senter physiquement et mentalement.

Nous ferons alors un tour des diff rents types de qubits physiques. Les mod les math matiques de repr sentation des qubits ne d pendent pas de leur type physique. Seules les caract ristiques de l'ordinateur sont affect es comme le taux d'erreur et la nature des portes quantiques physiques de base dites "universelles" agissant sur les qubits sachant que toutes les portes quantiques sont ex cutables sur les ordinateurs quantiques.

La sph re de Bloch de repr sentation de l' tat des qubits

Dans un modèle probabiliste classique, un pbit ou bit probabiliste aurait une probabilité p d'avoir la valeur 0 et $1-p$ d'avoir la valeur 1. Ce serait un modèle probabiliste linéaire.

Bits, Pbits, Qubits

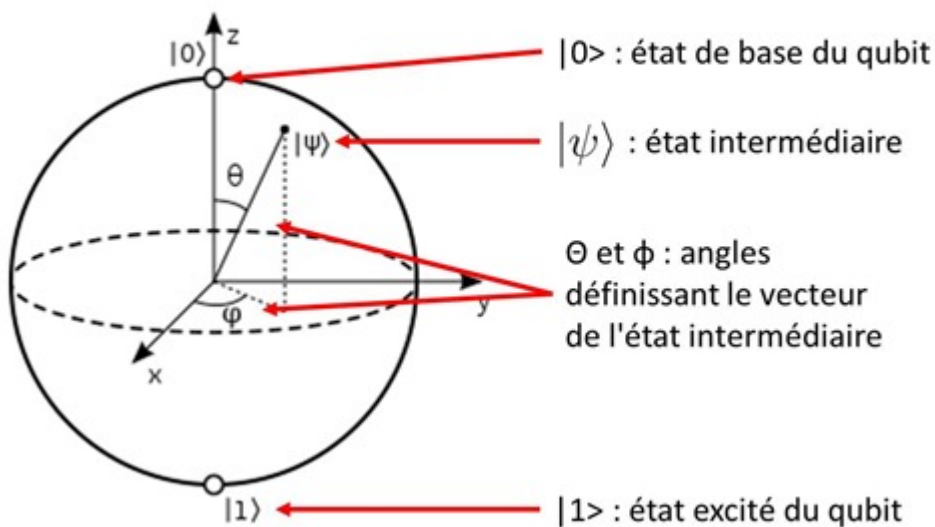
	bit	probabilistic bit	quantum bit
Configurations:	$\boxed{0} \ \boxed{1}$	$\boxed{0} \ \boxed{1}$	$\boxed{0} \ \boxed{1}$
Description:	$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$\begin{bmatrix} p \\ 1-p \end{bmatrix}$ $p \in \mathbb{R}$	$\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ $\alpha, \beta \in \mathbb{C}$
Observation:	$\boxed{0}$ certainty	$\boxed{0}$ p percent $\boxed{1}$ $1-p$ percent	$\boxed{0}$ $ \alpha ^2$ percent $\boxed{1}$ $ \beta ^2$ percent
Evolution:	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1-q & r \\ q & 1-r \end{bmatrix}$	$\begin{bmatrix} u & v \\ w & x \end{bmatrix}$
	deterministic	stochastic	unitary

Dans un qubit, c'est bien différent ! Le modèle de représentation mathématique de l'état d'un qubit s'appuie sur la fameuse **sphère de Bloch**, qui m'a donné bien du fil à retordre en termes de compréhension. Je vais partager avec vous ce que j'ai pu en comprendre après des mois de recherche dans des dizaines de cours, articles scientifiques et livres sur le calcul quantique.

Ce modèle est lié à la représentation de l'état d'un qubit ou de tout quantum à deux états par un vecteur à deux dimensions dont la longueur dite "norme" est toujours de 1. Ce vecteur a la particularité de comporter deux éléments : un nombre réel (alpha) et un nombre complexe (beta).

Dans la sphère de Bloch, l'état $|0\rangle$ d'un quantum à deux états est figuré par la position d'un vecteur de longueur 1 allant du centre de la sphère vers le pôle Nord de la sphère et l'état $|1\rangle$ est un vecteur allant du centre de la sphère à son pôle Sud.

sphère de Bloch



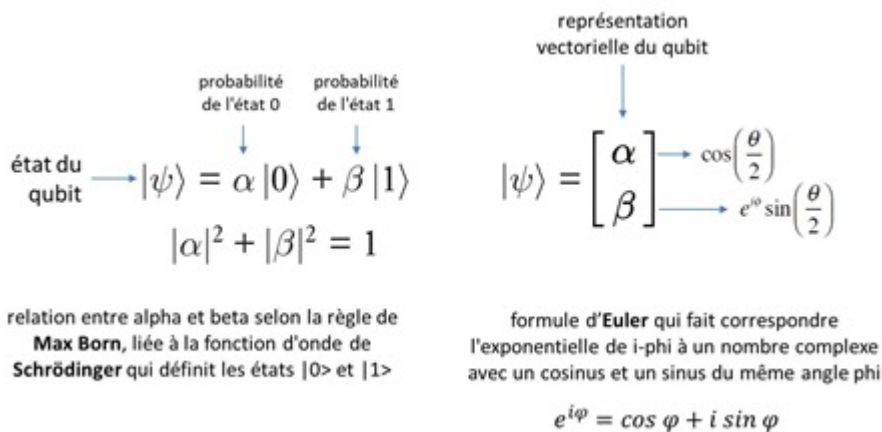
Les états intermédiaires sont représentés par des vecteurs partant du centre de la sphère qui sont toujours de longueur 1 avec un angle θ par rapport à la verticale z et un angle ψ par rapport à l'axe x situé allant du centre de la sphère à son équateur et autour de l'axe z . Histoire de simplifier les choses, les états $|0\rangle$ et $|1\rangle$ qui sont opposés dans la sphère de Bloch sont dits "orthogonaux" alors qu'ils sont opposés dans la sphère. Nous allons rapidement comprendre pourquoi.

Règle de Max Born et probabilités

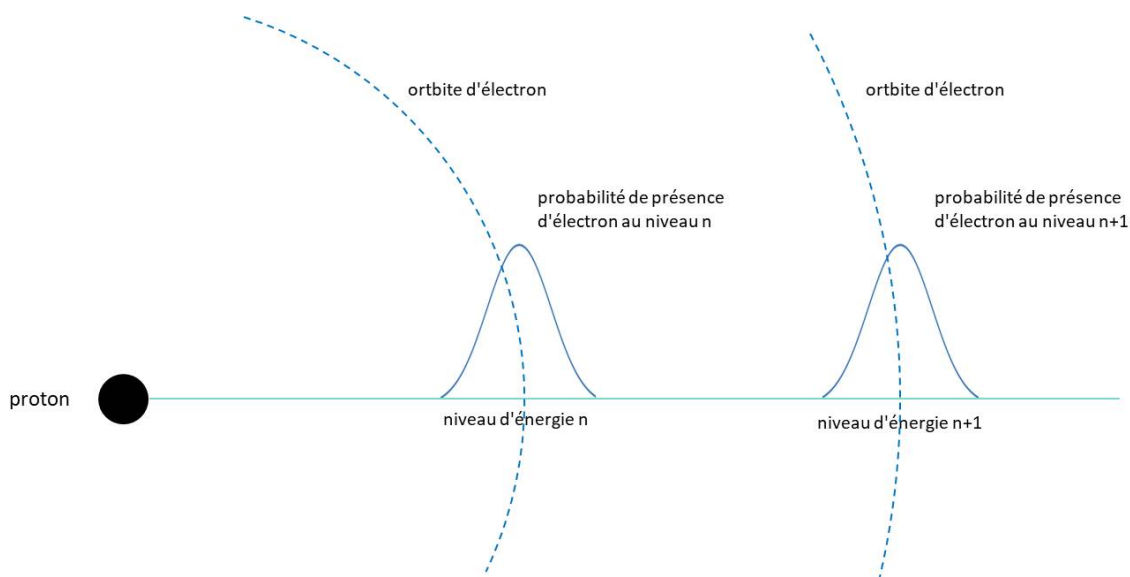
Les équations décrivant l'état d'un qubit indiquent que celui-ci est la superposition de l'état $|0\rangle$ et de l'état $|1\rangle$. Dans les équations, α est un nombre réel qui décrit la probabilité d'obtenir l'état $|0\rangle$ et β est un nombre complexe qui décrit celle d'avoir l'état $|1\rangle$. La somme des probabilités des deux états doit donner 1. Mais ce n'est pas $\alpha + \beta$. C'est α au carré plus β au carré qui donnent 1. Pourquoi donc ? C'est une question qui m'a taraudé des mois pendant la préparation de ce texte.

Ce modèle probabiliste a été élaboré par **Max Born** en 1926. Il donne au carré du module de la fonction d'onde d'un quantum la signification d'une densité de probabilité de présence d'une particule élémentaire. C'est lié au fait que l'état $|0\rangle$ et l'état $|1\rangle$ correspondent non pas à une position précise d'une particule mais sont représentés par la fonction d'onde de **Schrödinger** qui décrit la distribution probabiliste de l'état du quantum dans le temps et dans l'espace. Elle est ici appliquée dans l'espace.

L'état d'un qubit est représenté par un vecteur à deux dimensions, ce qui est une information bien plus riche qu'un 0 ou un 1 d'un simple bit ou même qu'une probabilité linéaire entre 0 et 1. Ce vecteur à deux dimensions comprend les deux composantes α et β que nous venons de définir.



Le passage de la fonction d'onde de Schrödinger à la représentation alpha/beta du qubit avec un nombre réel et un nombre complexe m'échappe encore. Je tente une explication qui fera peut-être s'étrangler les physiciens. Si on prend par exemple deux orbites possibles d'un électron autour du noyau d'un atome dans un modèle d'hydrogène simple (**il en existe plein...**), la fonction d'onde de l'orbite basse dans l'espace sera une sorte de courbe de Gauss décalée de celle de l'orbite haute. Intuitivement, je me dis que la probabilité d'avoir l'électron dans l'orbite haute ou basse est proportionnelle à l'intégrale des fonctions d'onde correspondantes à ces orbites. D'où le carré qui serait une approximation de la valeur du pic de la gaussienne, à supposer que ce pic corresponde à la taille des vecteurs alpha et beta de représentation des états des qubits. M'enfin, je ne suis pas sûr !



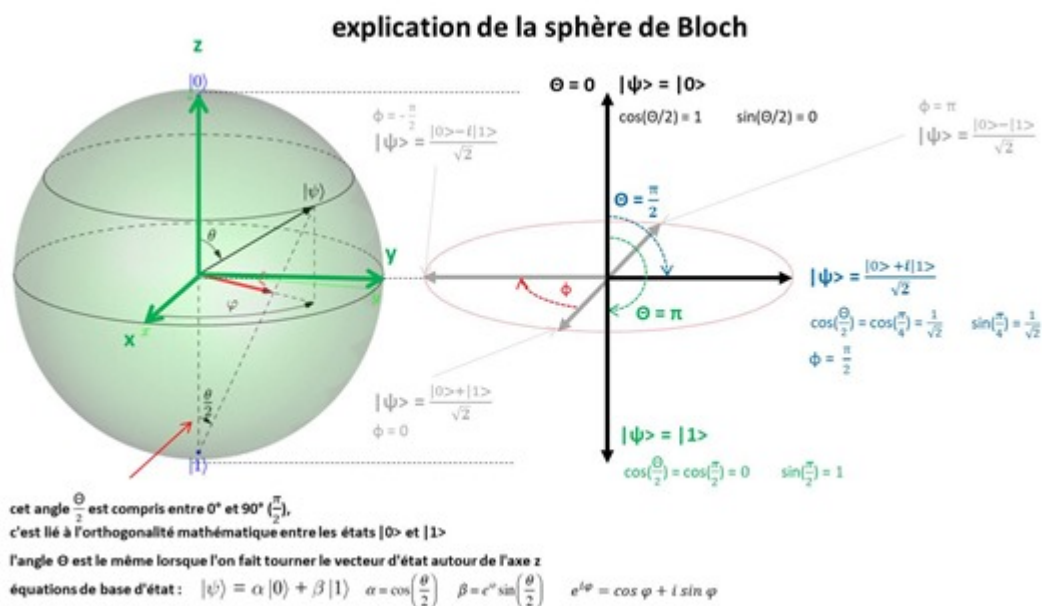
Pour en savoir plus et avec une meilleure exactitude scientifique, vous pouvez consulter la fiche Wikipedia de la **fonction d'onde** ainsi que celle de la **probabilité d'amplitude**. On trouve d'autres explications dans l'exemple des niveaux d'orbites d'électrons dans l'atome d'hydrogène dans **Quantum Mechanics and the hydrogen atom** (19 slides). L'interprétation physique de la règle statistique de Max Born reste en tout cas ouverte si l'on en juge par ce papier de juin 2018 d'Arkady Bolotin, **Quantum probabilities and the Born rule in the intuitionistic interpretation of quantum mechanics** (14 pages).

Trigonométrie dans la sphère de Bloch

Second mystère à résoudre, pourquoi donc l'angle theta est-il divisé par deux dans les équations

décrivant un état quantique dans la sphère de Bloch dans les calculs de sinus et de cosinus des formules donnant alpha et beta ? Cela vient de ce que l'état $|1\rangle$ est placé en bas de la sphère pour que l'espace des états du qubit occupe toute la sphère et pas seulement son hémisphère nord.

C'est décrypté dans **The Bloch Sphere de Ian Glendinning**, 2005 (33 slides) qui explique cela par l'orthogonalité mathématique des deux états $|0\rangle$ et $|1\rangle$ qui sont pourtant opposés dans la sphère de Bloch. C'est encore mieux expliqué dans **Why is theta/2 used for a Bloch sphere instead of theta ?** qui a définitivement éclairci ce mystère pour moi. Je m'en suis inspiré pour créer le schéma ci-dessous. C'est un peu tarabiscoté et vous n'êtes pas obligés d'y passer du temps.



Comme l'état $|1\rangle$ est mathématiquement orthogonal par construction à l'état $|0\rangle$, leur angle "mathématique" calculé doit être de 90° ($\pi/2$). Or, l'angle theta est du double de cet angle dans la sphère car il est de π (pour mémoire $\pi \times 2 =$ circonférence de 360°). Donc, on divise theta par deux pour relier la représentation géométrique dans la sphère avec la représentation mathématique de l'état du qubit. Et surtout, pour permettre un étalement de tous les états d'un qubits sur l'ensemble de la sphère.

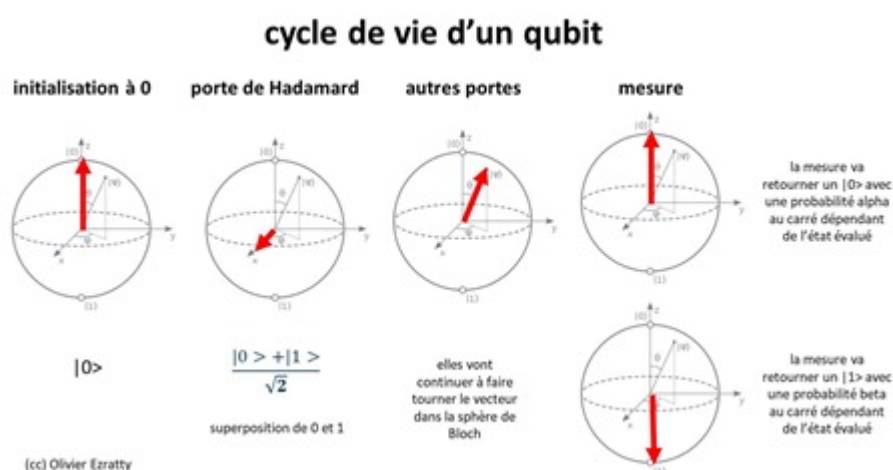
J'illustre ceci dans le schéma composite ci-dessus qui sert à comprendre la chose pour les lecteurs patients et comprenant les bases de la trigonométrie et des nombres complexes. Dans l'histoire, alpha est toujours un nombre réel car c'est un simple cosinus. Seul beta peut-être un nombre complexe. Il l'est dès lors que le qubit n'est pas dans le plan croisant l'axe x (theta = 0) et l'axe z (phi = 0) de la sphère de Bloch. Ce nombre complexe associe une partie réelle pour la direction x et une partie complexe pour la dimension y qui est orthogonale à x.

Un point important à noter est que la représentation sur la sphère de Bloch est un modèle mathématique probabiliste. Elle ne correspond pas à un modèle physique, comme l'angle de polarisation d'un photon ou le spin d'un électron, malgré les similitudes. Sachant néanmoins que ce modèle a été créé à l'origine pour représenter le spin d'électrons.

Lorsque le vecteur d'état du qubit est horizontal dans la sphère, c'est-à-dire qu'il va jusqu'à son équateur (schéma ci-dessous), nous sommes dans un état superposant l'état 0 et l'état 1 à égalité,

- On l'**initialise** toujours à 0, correspondant à l'état de base du qubit.
- On le **modifie** ensuite de manière programmatique avec des portes quantiques pour lui faire prendre des valeurs qui sont des vecteurs dans la sphère de Bloch. La porte de Hadamard est l'une des plus courantes et elle crée un état de superposition entre un 0 et un 1. Les manipulations mathématiques de ce vecteur consistent ensuite à le faire tourner dans la sphère de Bloch avec des portes quantiques unitaires que nous verrons dans la partie suivante consacrée à la description du fonctionnement d'un ordinateur quantique. Ces manipulations reviennent à multiplier le vecteur représentant le qubit $[\alpha, \beta]$ par une matrice de deux lignes et deux colonnes de nombres complexes conservant la norme du vecteur, qui doit rester à 1. Les portes quantiques non unitaires relient les qubits entre eux et en font évaluer les valeurs de manière conditionnelle. Sans ces différentes portes quantiques, on ne pourrait pas faire grand chose avec les qubits.
- L'**information dans les qubits** qui est manipulée lors des calculs est "riche" avec une dimension de deux nombres réels, les angles theta et phi.
- A part le cas où le qubit est initialisé à l'état $|0\rangle$ ou inversé à l'état $|1\rangle$, celui-ci est en **état de superposition**. La représentation mathématique d'un qubit et son incarnation visuelle dans la sphère de Bloch montrent qu'un qubit peut-être dans une infinité d'états superposés différents.
- Lorsque l'on **lit la valeur du qubit**, on retombe sur un 0 ou un 1 avec un retour probabiliste dépendant des paramètres du vecteur de l'état du qubit dans la sphère de Bloch.
- Donc, nous avons un 0 en entrée, un 0 ou un 1 en sortie, et une **infinité d'états** entre les deux pendant les calculs !

Voici cela illustré dans le schéma *ci-dessous* :



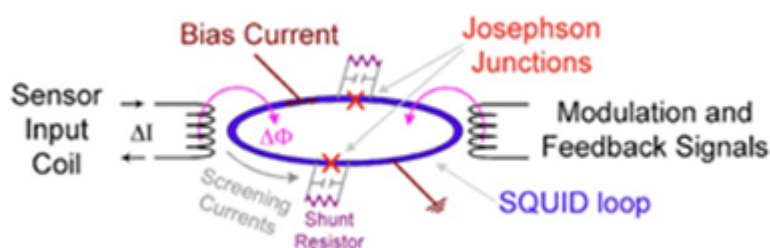
Tout ça pour dire que la richesse mathématique du qubit intervient pendant les traitements et seulement pendant les traitements. Mais pas au départ ni à l'arrivée des traitements. La magie mathématique de l'ordinateur quantique est là !

Types de qubits

D'un point de vue physique, les qubits des calculateurs quantiques sont des dispositifs matériels qui intègrent des particules élémentaires qui ont deux états possibles que l'on peut initialiser, modifier avec des portes quantiques puis dont on peut évaluer l'état. Il s'agit parfois de particules élémentaires unitaires, comme avec les ions piégés ! Une seule à la fois ! Dans le cas des supraconducteurs ou de quantum dots à silicium, l'état quantique s'appuie sur un grand nombre de particules, ici, des électrons.

Voici les principaux types de qubits qui sont étudiés, expérimentés voire utilisés en production actuellement :

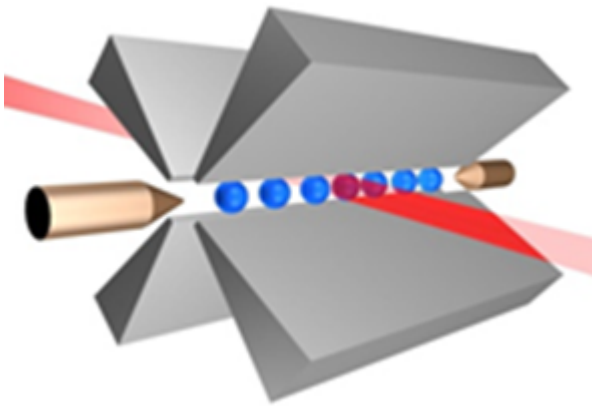
Les supraconducteurs : le qubit prend la forme de l'état d'un courant supraconducteur qui traverse une barrière très fine en s'appuyant sur l'effet Josephson. Il existe plusieurs types de qubits supraconducteurs, de flux, de phase et de charge. Ne rentrons pas dans les détails. Dans tous les cas, il s'agit de créer une superposition de deux états bien distincts d'un courant oscillant à haute fréquence et traversant la jonction Josephson dans une boucle supraconductrice. L'oscillation est rendue possible par le fait que la boucle intègre l'équivalent d'une inductance et d'une résistance. L'oscillation du courant est activée par l'application de micro-ondes de fréquences situées entre 5 et 10 GHz transmises par voie conductrice et physique. Ce ne sont pas des ondes émises par la voie "radio". L'état du qubit est pour sa part mesuré avec un magnétomètre intégré dans le circuit.



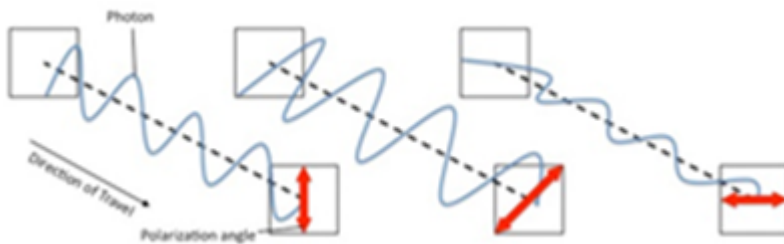
C'est la technique la plus couramment employée aujourd'hui, notamment par IBM, Google et Intel pour des ordinateurs quantiques à circuits universels et avec les ordinateurs quantiques adiabatiques du Canadien D-Wave qui utilisent un autre arrangement de qubits de qualité moins bonne du côté du bruit et du taux d'erreurs. Elle est relativement facile à fabriquer car elle s'appuie sur les techniques de création de circuits CMOS même si certains des matériaux sont différents, comme le niobium qui est utilisé chez D-Wave. Cf **Practical realization of Quantum Computation Supraconducting** (36 slides). Notons, nous le verrons plus tard, que l'équipe de Daniel Estève au CEA de Saclay fait partie des précurseurs de la création de tels qubits supraconducteurs.

Les ions piégés : il s'agit d'ions d'atomes qui peuvent être du calcium et qui sont maintenus sous vide et suspendus par suspension électrostatique. Un pompage optique est réalisé pour leur initialisation. Un laser sert à la mesure et exploite le phénomène de fluorescence des ions excités par le laser. Le magnétisme est utilisé pour l'activation des portes quantiques. La startup IonQ issue de l'Université de Maryland planche là-dessus tout comme l'université d'Innsbruck en Autriche et sa spinoff AQT. Dans un tel système, plusieurs ions sont piégés de manière équidistante les uns des autres. Ils sont alignés en rang d'oignons. Il est difficile de faire "scaler" ce genre d'arrangement au-delà d'une centaine et quelques d'ions. Par contre, ils présentent

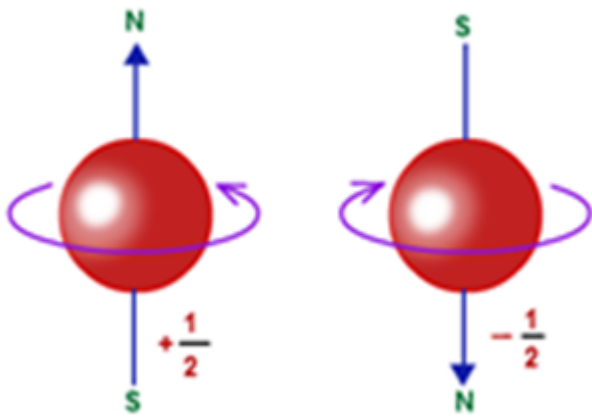
l'avantage de bien pouvoir être intriqués les uns avec les autres, ce qui est moins le cas des qubits à base de supraconducteurs.



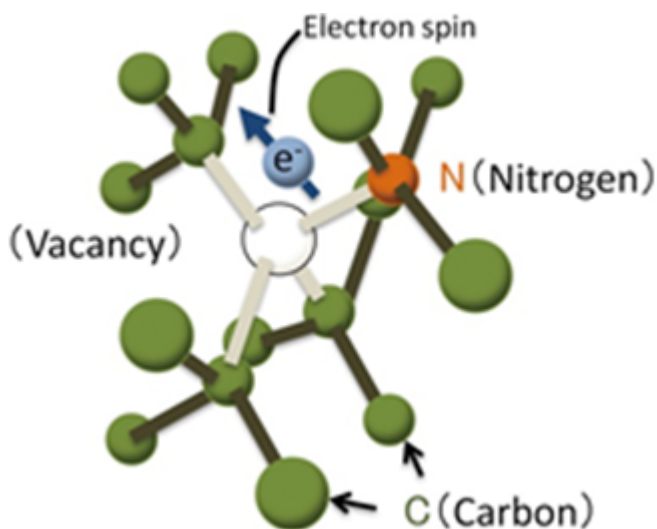
Les photons : leur état quantique est leur polarisation horizontale ou verticale. Cela fait partie du champ de l'optique linéaire. Il manipule des photons individuels. Les portes quantiques sont réalisées à l'aide de dispositifs optiques avec des filtres dichroïques ou polarisants. Il faut un grand nombre de lasers pour piloter l'ensemble. C'est donc pour l'instant assez embarrassant. L'avantage est que ces qubits fonctionnent à température ambiante. Mais ce type de qubit n'est pour l'instant utilisé qu'en laboratoire et à petite échelle et aucune société privée ne semble s'être embarquée dans ce chemin.



Le spin d'électron : haut ou bas, une sorte de sens de polarisation magnétique, que l'on retrouve dans les ordinateurs à base de quantum dots, notamment chez Intel ou dans des prototypes de qubits réalisés au CEA à Grenoble. Ces qubits sont intégrés dans des circuits à base de semi-conducteurs CMOS. Ils bénéficient donc de la réutilisation de processus de fabrication de composants CMOS déjà bien maîtrisés. Ces qubits sont cependant pour l'instant plutôt "broyants", même en les exploitant à des températures proches du zéro absolu. Le plan consiste à en aligner des batteries pour créer des qubits logiques, un concept que nous étudierons dans la prochaine partie.



Les centres NV pour Nitrogen Vacancy : ce sont des structures de diamant artificiel dans lesquelles un atome de carbone a été remplacé par un atome d'azote et à proximité duquel se situe une lacune d'atome de carbone. Les électrons des atomes de carbone adjacents à cette lacune occupent l'espace vide et avec un spin variable. Bref, l'état de la lacune est instable et quantique. Cet état est excité par laser et micro-ondes. La lecture de l'état du qubit est réalisée par une mesure de brillance de fluorescence. Seule la startup QDTI planche commercialement sur cette technique. Ce n'est visiblement pas encore au point.



Voici, *ci-dessous*, un schéma d'ensemble du mécanisme de contrôle de ces qubits vu dans **Forefront engineering of nitrogen-vacancy centers in diamond for quantum technologies** 2017 (235 pages).

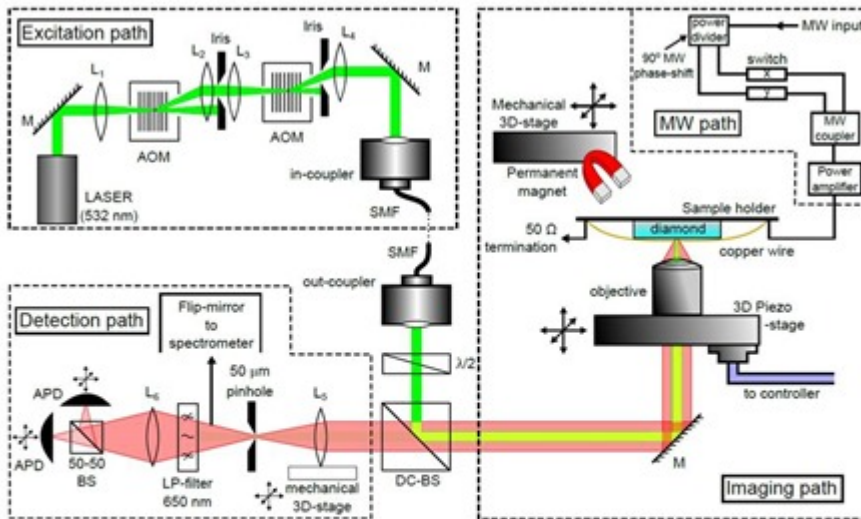
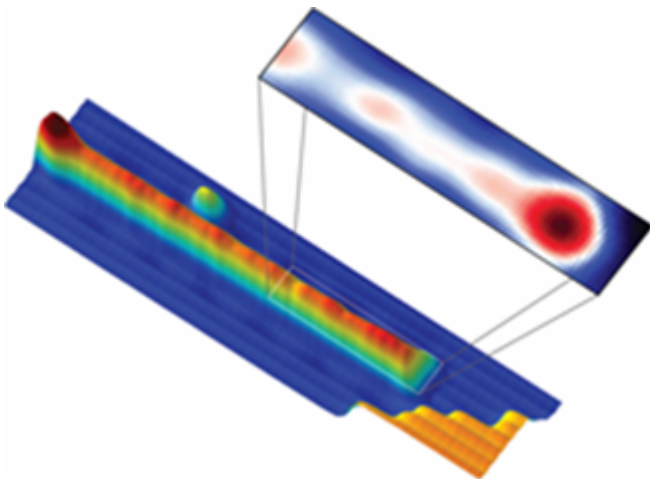


Figure A.1.: Schematic representation of the utilized setup for the characterization of NV centers. Experimental setup utilized for optical characterization and coherent spin manipulation of NV centers, comprising of a home-built confocal microscope, a scanning-stage for the imaging of diamond, and external magnet and microwave apparatus. The excitation wavelength is 532 nm. In the figure, mirrors are represented by M, lenses by L_i , single-mode optical fiber by SMF, beam-splitters by BS, and avalanche photo-diodes by APD.

Les fermions de Majorana : ce sont des anyons ou quasi-particules qui sont des états particuliers de nuages d'électrons organisées par paires. Pratiquement, ce sont des spins d'électrons aux deux bouts de fils supraconducteurs. On peut d'ailleurs considérer à ce titre là que c'est une variation des qubits supraconducteurs. De ce fait, ces ordinateurs quantiques doivent aussi être refroidis à une température voisine du zéro absolu, aux alentours de 10mK. C'est la voie choisie par Microsoft. Sachant que l'existence des fermions de Majorana est à peine prouvée. Et les quasi-particules sur lesquelles planchent les équipes de Microsoft ne seraient pas des fermions de Majorana. Il y a de quoi y perdre son latin ! Nous reviendrons dessus dans une prochaine partie de cette série.



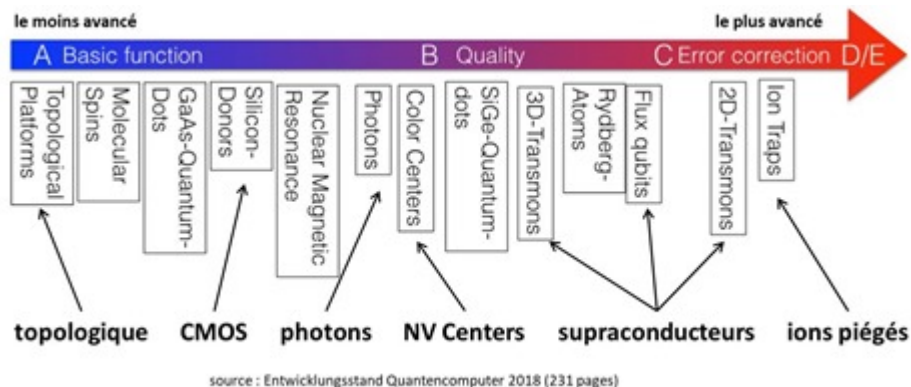
Aucune de ces techniques n'est pour l'instant éprouvée à grande échelle. Elles ont toutes leurs avantages et inconvénients qui se situent dans plusieurs dimensions : la stabilité des qubits, la possibilité de les intriquer, le niveau d'erreurs dans les qubits et dans les portes qui les relie, la durée de cohérence des qubits, la température de fonctionnement, le niveau de miniaturisation, le processus de fabrication (qui est moins cher lorsque c'est du silicium en technologie CMOS). Nous verrons tout cela plus tard quand nous aborderons les différentes offres et projets

d'ordinateurs quantiques.

En résumé, voici les principaux types de qubits et leurs caractéristiques clés avec la nature des qubits, la manière de stocker leur état, la nature des portes quantiques qui les modifient et de la mesure de l'état des qubits.

							
qubit	supraconducteur effet Josephson	supraconducteur effet Josephson	quasi-particules faites de paires d'anyons	photons	spin d'électrons dans semi- conducteur	ions piégés magnétiquement	spin de noyau d'atomes
# qubit	2048 qubits (D-Wave)	50 qubits (IBM) 72 qubits (Google)	N/A	quelques-uns	49 qubits (Intel)	53 qubits (IonQ) 51 qubits (MIT) 20 qubits (IQOQ)	6 qubits (ODTI)
état	sens du courant	phase de résonance ou sens du courant	sens de l'anyon	phase de photon	spins d'électrons	niveau énergétique de l'ion piégé	niveau d'énergie de la cavité
portes	micro-ondes 5 GHz et effet Josephson	micro-ondes 5 GHz et effet Josephson	inversions 2D d'anyons	filtres polarisants et dichroïques	micro-ondes	laser	laser
mesure	magnétomètre	magnétomètre	fusion d'anyons	détecteurs de photons	conversion spins to charge	fluorescence	fluorescence

Leur niveau d'avancement est décrit dans cet excellent document de l'équivalent allemand de l'ANSSI, *Entwicklungsstand Quantencomputer (état des lieux de l'informatique quantique*, 231 pages, en anglais). Il évoque d'autres technologies que celles qui sont citées dans mon inventaire et que je ne cite pas car elles ont pour l'instant peu de chances d'aboutir et n'ont été adoptées par aucun industriel ou aucune startup.



Voilà pour l'histoire des qubits. Mais celle-ci ne fait que commencer. Dans la **partie suivante**, nous allons aller plus loin et découvrir comment sont architecturés les ordinateurs quantiques dans la pratique avec leurs registres, leurs portes, leurs dispositifs de lecture, leurs systèmes de correction d'erreur ainsi que leur système de cryogénie pour ceux que cela concerne comme les ordinateurs à qubits supraconducteurs. Nous pourrions comprendre comment fonctionne un cycle complet de calcul dans un ordinateur quantique. La partie d'après donnera corps à l'ensemble avec un descriptif des principaux algorithmes connus pouvant être exploités sur les ordinateurs quantiques.

Cet article a été publié le 8 juillet 2018 et édité en PDF le 13 juillet 2018.
(cc) Olivier Ezratty - "Opinions Libres" - <http://www.oezratty.net>