# LA THÈSE DE TURING PHYSIQUE ET L'INFORMATIQUE QUANTIQUE

Florent FRANCHETTE
(M2 Paris I)

## RÉSUMÉ

Selon la thèse de Turing, tout ce qui est calculable par une procédure effective (notion intuitive) est calculable par une Machine de Turing (notion formelle). La thèse de Turing physique affirme quant à elle que tout ce qui peut être calculé par un système matériel est calculable par une Machine de Turing. Etant donnée sa nature d'énoncé universel, il ne suffit pas pour prouver cette thèse, de montrer que tout ce qui est calculable par nos systèmes matériels actuels est aussi calculable par une Machine de Turing. En revanche, la thèse de Turing physique serait falsifiée si l'on proposait un mécanisme de calcul qui résoudrait un problème qui ne serait pas décidable par une Machine de Turing. Nous essaierons de répondre dans cet article à la question suivante : pourquoi les récents résultats en informatique quantique apportent de nouvelles perspectives quant à la validité de la thèse de Turing physique?

## 1. LA THÈSE DE TURING PHYSIQUE

Une première tentative afin de caractériser ce qu'est une procédure effective est la suivante. Une procédure M, exécutée dans le but d'obtenir un résultat, est dite « effective » lorsque :

1. M est définie à partir d'un nombre fini d'instructions;

2. M produit le résultat désiré en un nombre fini d'étapes;

3. M peut (en pratique ou en principe) être exécutée par un être humain sans l'aide d'aucune machine;

4. M ne demande aucune perspicacité ni ingéniosité de la part de l'être humain qui l'exécute.

Toutefois, notre définition n'est pas suffisante pour caractériser le fait qu'une fonction est calculable par une procédure effective. Un essai afin de formaliser un prédicat dont la signification informelle est celle de « peut être calculé au moyen d'une procédure effective » a été présenté par Alan Turing, qui proposa en 1936, le prédicat formel de « calculé par Machine de Turing » . Dans le but de comprendre en quoi une Machine de Turing est un modèle mathématique représentant une procédure effective exécutée par un être humain, donnons en une définition en citant Turing :

« Un homme en train de calculer la valeur d'un nombre peut être comparé à *une machine* susceptible de se trouver dans un nombre fini d'états. La machine est alimentée avec une *bande* (analogue au papier qu'utilise l'homme) et divisée en cases dans chacune desquelles peut être inscrit un *symbole*. À chaque instant, la liste des comportements possibles de la machine est entièrement déterminée par sa configuration, caractérisée par l'ensemble de ses états et le symbole inspecté. C'est cette configuration qui détermine l'évolution possible de la machine (...) Ce que j'affirme, c'est que ces opérations englobent toutes celles qui peuvent être utilisées pour calculer la valeur d'un nombre (...) Une séquence est dite *calculable* s'il existe une Machine de Turing qui la calcule » (Turing, 1936)

À partir de l'examen de la Machine de Turing, la théorie de la calculabilité, qui est une partie de la logique mathématique, a pu produire une série de résultats définissant les limites de ce qui est calculable par une procédure effective.

En particulier, Turing défendait l'affirmation suivante, nommée thèse de Turing ou thèse **M** : **Une fonction est calculable par une procédure effective si et seulement si elle peut être calculée par une Machine de Turing**. Remarquons le fait que cette thèse n'est pas un théorème car elle lie une notion informelle (celle de procédure effective) à une notion mathématique (celle de calculable par une Machine de Turing). Il est par conséquent impossible de démontrer que toute procédure effective est calculable par une Machine de Turing. En revanche, si la thèse de Turing est correcte, certaines fonctions ne sont pas calculables par une procédure effective car il peut être démontré qu'il n'existe pas de Machine de Turing pouvant les calculer[1].

Cependant, la thèse **M**, à partir de la définition mathématique de la Machine de Turing, détermine uniquement les fonctions pouvant être calculées par des moyens purement mathématiques. Par conséquent, cette dernière n'affirme rien concernant ce qui est calculable à l'aide de moyens extrinsèques aux mathématiques. Ainsi, que se passerait-il si l'on étendait la notion de procédure effective à la physique? Autrement dit, la thèse **M** définie-t-elle les limites de ce qui est calculable par une procédure effective indépendamment du domaine ou l'on se place? Une première étape afin de répondre à ces questions est d'étudier une version « plus physique » de la thèse de Turing qui concerne la notion de tâche réalisable en temps fini par un système matériel.

La version physique de la thèse de Turing ou thèse **P** s'énonce alors comme ceci : **une fonction est calculable par un système matériel si et seulement si elle peut être calculée par une Machine de Turing**. Cependant, contrairement à la thèse de Turing **M** qui

[1] Par exemple, puisque le problème de déterminer si une formule de la logique du premier ordre est démontrable ou non ne peut être résolu par une Machine de Turing, ce problème ne peut pas être résolu par une procédure effective.

semble être accéptée par la majorité des scientifiques, sa version physique est sujette à des divergences d'opinions quant à son exactitude. En effet, plusieurs scientifiques ont proposé différents mécanismes de calcul qui pourraient remettre en cause la thèse **P** s'ils venaient un jour à exister. Toutefois, cette version physique admet deux interprétations suivant que la phrase « pouvant être calculée par un système matériel » est prise au sens étroit ou au sens large. Au sens étroit, cette phrase doit être interprétée comme « pouvant être calculée par une machine conforme aux lois physiques du monde actuel » tandis qu'au sens large, l'interprétation fait abstraction de la contrainte physique. En interprétant cette thèse dans son sens étroit, la remettre en cause consisterait à proposer un mécanisme de calcul conforme aux lois physiques et pouvant calculer au moins une fonction non calculable par une Machine de Turing. Par conséquent, le calcul ne doit plus être considéré comme un sujet purement mathématique car ce doit être en dernier lieu à la physique de dire si la thèse **P** est juste ou fausse.

Dans ce but, une des propositions les plus prometteuses concernant la création d'une « hypermachine » , c'est-à-dire d'un mécanisme pouvant falsifier la thèse **P** et dont la possible création n'est pas contradictoire avec les lois de la physique, provient des modèles de calcul conçus en mécanique quantique à partir des années 1980.

## 2. LES NOUVELLES PERSPECTIVES DE L'INFORMATIQUE QUANTIQUE

La possibilité d'appliquer la mécanique quantique à l'informatique découle tout d'abord de la confiance que nous accordons à cette théorie. En effet, si nous croyons que la mécanique quantique est la théorie fondamentale d'où dérive toutes les propriétés des objets physiques, alors cette dernière devrait être la base de la description de n'importe quel ordinateur. De plus, la miniaturisation des composants micro-éléctriques devrait bientôt atteindre l'ordre de 10 nanomètres ($10^{-9}$m) faisant de la mécanique quantique la théorie la plus pertinente pour créer certains composants informatiques.

Au cours des années 1980, la notion de procédure effective telle qu'elle est définie à travers la thèse de Turing physique, fut soumise à la question de savoir si elle pouvait être étendue aux principes quantiques. D'une part, les efforts initiaux menés par David Deutsch semblent considérer que les notions de calculabilité quantique et de calculabilité mathématique sont identiques. Cependant, des indications récentes établis par Tien Kieu portent à croire le contraire. Dans un premier temps, le modèle « standard » de la computation défendu par Deutsch sera présenté. Puis dans un second temps, la position controversée de Kieu soutenant que les

ordinateurs quantiques peuvent falsifier la thèse de Turing physique sera exposée.

D'après le modèle standard de la computation quantique, qui est une généralisation de la computation classique, l'unité fondamentale d'un ordinateur quantique est le *bit* quantique ou *qubit*, qui est la généralisation d'un *bit* classique. Mais alors qu'un *bit* classique peut prendre l'une ou l'autre des valeurs possibles servant à coder l'information (0 ou 1 par exemple), un *qubit* a la possibilité d'être dans un état superposé de ces deux valeurs. Toutefois, lorsqu'une mesure est effectuée, cette superposition est détruite, ce qui a pour conséquence de révéler une des deux valeurs classiques prises par le *qubit*.

Nous pouvons distinguer trois étapes principales dans la computation d'un ordinateur quantique : la préparation de l'*input*, le calcul et la mesure de l'*output*. Premièrement, la préparation de l'*input* et la mesure de l'*output* doivent être exécutées de telle façon à ne pas pertuber les autres qubits qui ne seront pas directement mesurés. La seconde étape, correspondant au calcul proprement dit, est l'étape la plus difficile à réaliser physiquement. En principe, le calcul est causée par l'évolution d'opérations réversibles sur les *qubit*s, mais ces derniers doivent être correctement isolés de toute perturbation afin d'éviter le plus possible les effets de décohérence dus à l'environnement.

D'autre part, la supériorité des ordinateurs quantiques sur leurs homologues classiques est due à deux avantages cruciaux. Le premier avantage réside dans un parallélisme massif résultant directement de la superposition des états quantiques. En effet, si chaque *qubit* peut être dans une superposition de deux états, un sytème constitué de *N-qubits* pourrait avoir accès à $2^N$ états simultanément. Le second avantage des ordinateurs quantiques prend racine dans « l'intrication quantique » qui n'a pas de contrepartie classique. Cette propriété quantique veut dire que si deux systèmes A et B sont intriqués, leurs propriétés peuvent être reliées même si les deux systèmes sont séparés spatialement.

Enfin, ces caratéristiques ont été exploitées dans le but de réduire la complexité en temps de certains problèmes. L'algorithme le plus célèbre, celui de Peter Shor permet de résoudre dans un temps raisonnable le problème de la décomposition d'un nombre en un produit de facteurs premiers (Shor, 1994). En revanche, malgré les avantages du modèle standard (parallélisme et intrication), David Deutsch a démontré dans les années 1980 que ce modèle était Turing-équivalent, c'est-à-dire qu'il calculait exactement les mêmes fonctions que la Machine de Turing (Deutch 1985). Toutefois, le modèle standard n'est pas le seul modèle disponible.

En effet, un modèle alternatif de computation quantique employant des processus adiabatiques a été conçu récemment. L'idée de cette méthode est de coder la solution du problème voulant

être résolu dans l'état fondamental $|g\rangle$ d'un opérateur hamiltonien $H_P$ qui est l'énergie totale du système. Cependant, comme il est plus facile d'implémenter l'hamiltonien que de trouver son état fondamental, nous devons commencer la computation avec un autre état fondamental $|g_I\rangle$ d'un autre hamiltonien $H_I$ pouvant lui, être obtenu. Nous devons ensuite transformer l'hamiltonien initial $H_I$ au cours d'un temps $T$ vers l'hamiltonien $H_P$ qui possède l'état fondamental désiré, ceci à travers un processus dépendant du temps. Enfin, le théorème adiabatique de la mécanique quantique affirme que si le temps de la transformation est suffisamment lent, l'état initial évoluera vers l'état fondamental désiré avec une forte probabilité (Messiah, 1964).

À partir de ce modèle et d'après les idées de Kieu (Kieu, 2003) un ordinateur quantique utilisant les processus adiabatiques pourrait résoudre le 10ème problème de Hilbert qui est indécidable par les Machines de Turing[2]. Autrement dit, si l'ordinateur quantique de Kieu nous permettait de résoudre ce problème de manière effective, la thèse de Turing physique se trouverait falsifiée. L'algorithme de Kieu est de manière schématique le suivant :

1.Tout d'abord, étant donnée une équation diophantienne, nous codons l'équation en un nombre fini d'étapes dans un système ayant une infinité de niveaux d'énergie (tous les atomes en ont une infinité).

2. Puis, nous simulons le processus adiabatique.

3. Enfin, si l'état fondamental peut être obtenu avec une forte probabilité, une mesure praticable en un nombre fini d'étapes est mené sur ce système. Cette dernière extrait une information sur l'équation codée, indiquant qu'elle possède des solutions ou qu'elle n'en possède pas. Pour résumé, l'algorithme peut être vu comme une recherche infinie menée en un temps fini à travers les nombres entiers afin de trouver s'il existe ou non des solutions à l'équation.

## 3. CONCLUSION

Le résultat de Peter Shor est le résultat de la computation quantique le plus spectaculaire de tout ceux obtenus jusqu'à présent, ce qui tend à confirmer que les ordinateurs quantiques sont plus puissants en terme de vitesse que les ordinateurs classiques. Peuvent-ils pour autant résoudre des problèmes indécidables par les Machines de Turing? Deutsch dans son modèle quantique soutient

[2] Ce problème est le suivant : est-il possible de concevoir une procédure effective permettant de déterminer si une équation polynomiale à coefficients entiers (une équation diophantienne) a des solutions ou non?

que non : la classe des fonctions qu'un ordinateur quantique calcule est la même que celle d'un ordinateur classique. En revanche, si l'algorithme de Kieu est réalisable et nous n'avons pour l'instant aucune preuve du contraire, la thèse de Turing physique devra être modifiée d'après les ordinateurs quantiques. Toutefois, l'algorithme de Kieu est controversé car il se fonde sur de forts présuposés indispensables au bon déroulement de la procédure (Hagar and Korolev, 2007) :

1. L'exactitude de la mécanique quantique dans la description et la prédiction des processus physiques quelle que soit l'echelle de mesure (du microscopique au macroscopique).

2. Notre capacité à implémenter physiquement certains opérateurs hamiltoniens ayant un nombre infini de niveaux d'énergie.

3. Notre capacité à obtenir de manière physique les états fondamentaux.

Dans tous les cas, ne doutons pas que le débat qui va se poursuivre au sein de la recherche sera riche et passionnant.

## RÉFÉRENCES

DEUTSCH, David (1985). Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer, *Proceedings of the Royal Society of London*, A 400, pp. 97-117.

HAGAR, Amit and KOROLEV, Alex (2007). Quantum Hypercomputation : Hype or Computation?, *Archiv*.

KIEU, Tien (2003). Computing the Non-computable, *Contemporary Physics*, 44.

MESSIAH, Albert (1964). *Mécanique Quantique*, Dunod.

SHOR, Peter (1994). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithm on a Quantum Computer, *35th Annual Symp. on Foundations of Computer Science*, pp. 124-139.

TURING, Alan (1936). On Computable Numbers, with an Application to the Entscheidungs-problem, *Proceedings of the Mathematical Society*, 42.