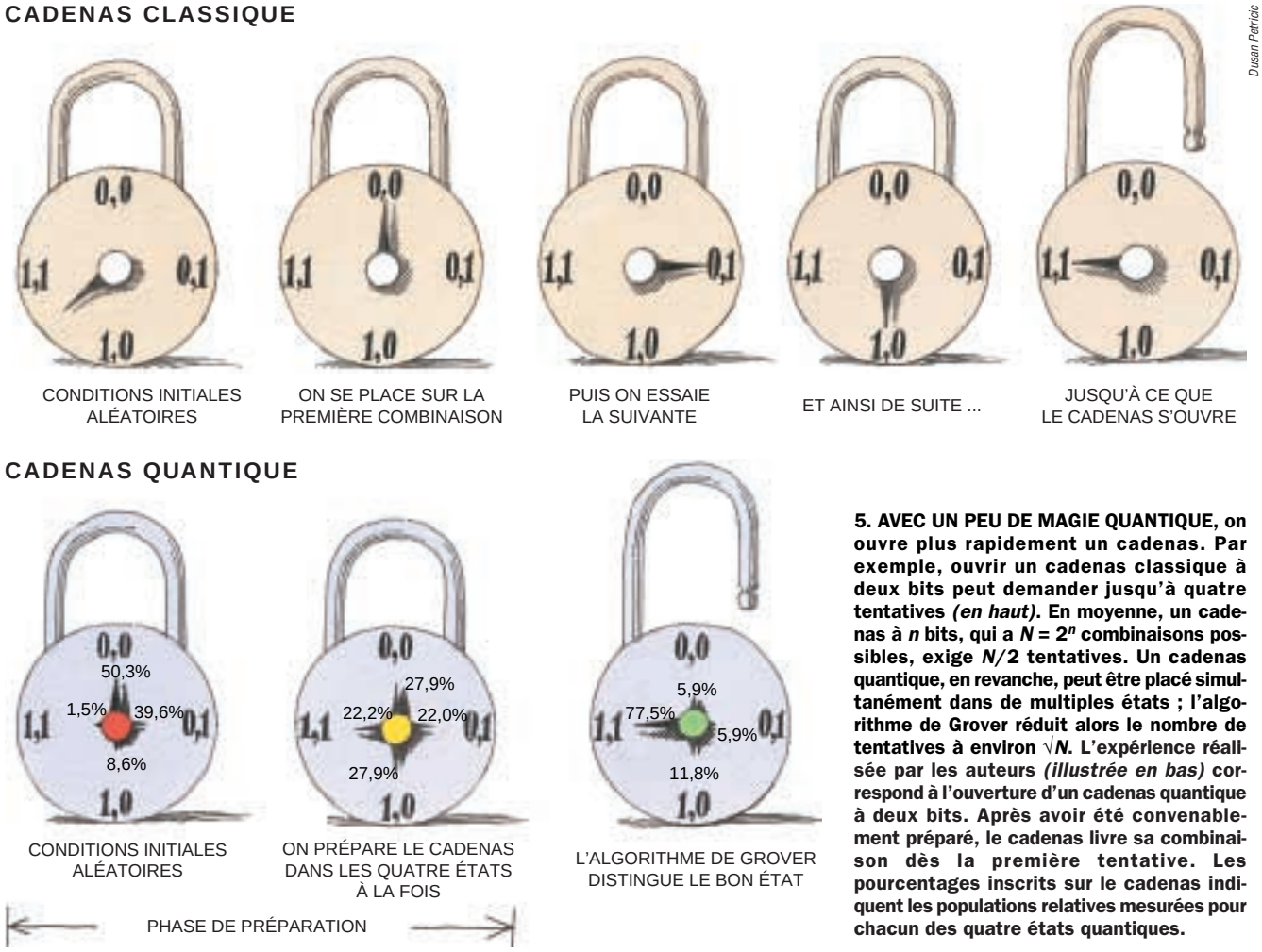


5. AVEC UN PEU DE MAGIE QUANTIQUE, on ouvre plus rapidement un cadenas. Par exemple, ouvrir un cadenas classique à deux bits peut demander jusqu'à quatre tentatives *(en haut)*. En moyenne, un cadenas à n bits, qui a $N = 2^n$ combinaisons possibles, exige $N/2$ tentatives. Un cadenas quantique, en revanche, peut être placé simultanément dans de multiples états ; l'algorithme de Grover réduit alors le nombre de tentatives à environ $\sqrt{N}$. L'expérience réalisée par les auteurs *(illustrée en bas)* correspond à l'ouverture d'un cadenas quantique à deux bits. Après avoir été convenablement préparé, le cadenas livre sa combinaison dès la première tentative. Les pourcentages inscrits sur le cadenas indiquent les populations relatives mesurées pour chacun des quatre états quantiques.

qubits qui corrigeraient les erreurs quantiques.

Bien que les ordinateurs classiques utilisent des bits supplémentaires pour détecter et corriger les erreurs, nombre de spécialistes ont été surpris lorsque P. Shor et d'autres chercheurs montrèrent que l'on pouvait faire de même avec les ordinateurs quantiques. Ils pensaient que la correction d'erreurs quantiques imposerait de mesurer l'état du système et donc de détruire sa cohérence quantique. Il apparaît que l'on peut corriger les erreurs quantiques à l'intérieur de l'ordinateur sans que l'opérateur ait à lire les états responsables *(voir l'article de Jean-Paul Delahaye, page 66, pour plus de détails)*.

La construction d'ordinateurs quantiques suffisamment gros pour rivaliser avec les plus rapides des ordinateurs classiques sera particulièrement difficile, mais les enjeux sont considérables : même les plus modestes ordinateurs quantiques constitueront de superbes laboratoires d'analyse des principes de la théorie quantique.

Paradoxalement, ces ordinateurs quantiques pourraient résoudre les problèmes inhérents aux puces électroniques, dont les minuscules transistors se comportent de manière quantique lorsqu'on réduit leur taille jusqu'aux échelles atomiques.

Les ordinateurs classiques ne résolvent que très péniblement ces problèmes, qui seraient probablement très simples pour les ordinateurs quantiques, comme l'envisageait Richard Feynman dès 1982.

Un point très encourageant est que ces ordinateurs n'exigeront pas de minuscules circuits à l'échelle atomique : la nature a déjà fait le plus gros du travail en assemblant les composants de base. Les molécules effectuent elles-mêmes des calculs remarquables. Seulement, on ne leur avait jamais posé les bonnes questions.

Neil GERSHENFELD est professeur à l'Institut de technologie du Massachusetts. Isaac CHUANG travaille au Centre de recherche d'IBM à San Jose (Californie).

Charles SLICHTER, *Principles of Magnetic Resonance*, troisième édition, Springer-Verlag, 1992.

Charles BENNETT, *Quantum Information and Computation*, in *Physics Today*, vol. 48, n° 10, pp. 24-30, octobre 1995.

Seth LLOYD, *Les ordinateurs quantiques, Pour la Science*, n° 218, pp. 44-50, déc. 1995.

Neil GERSHENFELD et Isaac CHUANG, *Bulk Spin-Resonance Quantum Computation*, in *Science*, vol. 275, pp. 350-356, 17 janvier 1997.

Lov GROVER, *Quantum Mechanics Helps in Searching for a Needle in a Haystack*, in *Physical Review Letters*, vol. 79, n° 2, pp. 325-328, 14 juillet 1997.

Jean-Paul DELAHAYE, *Les ordinateurs quantiques, Pour la Science*, vol. 209, pp. 100-104, mars 1995.

Les lois nouvelles de l'information quantique

JEAN-PAUL DELAHAYE

Principe de non-duplication, téléportation, cryptographie inviolable, codes correcteurs, parallélisme illimité : l'informatique quantique est née.

Quand, en 1937, George Stibitz fabrique dans sa cuisine un additionneur binaire à relais qui fonctionne avec deux chiffres (et qui ne fait donc que 4 additions différentes, 0+0, 0+1, 1+0 et 1+1), il ne suscite aucun enthousiasme. Quelques années plus tard, les descendants de sa machine, les ordinateurs, ont envahi le monde.

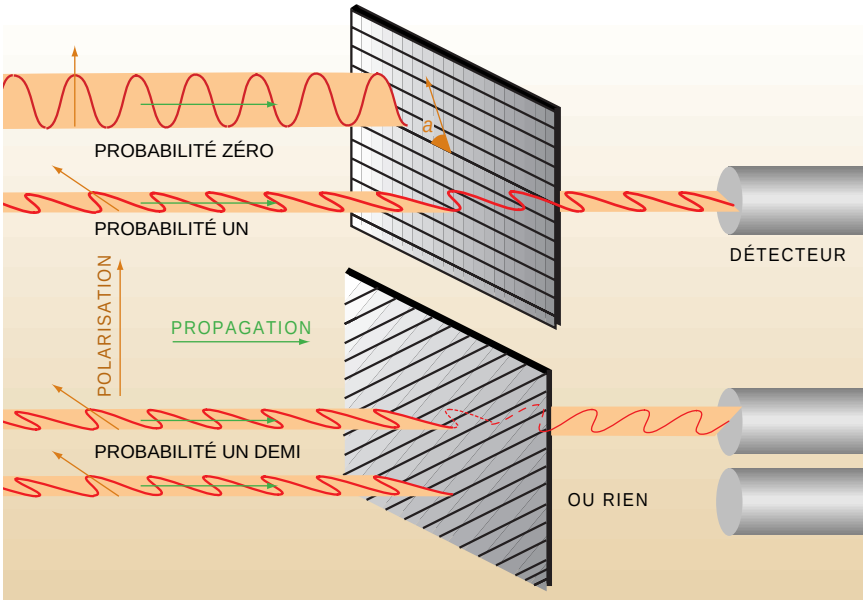
Les physiciens quantiques viennent de fabriquer l'équivalent quantique de l'additionneur de Stibitz et la théorie du calcul quantique prouve que, si l'on progresse normalement, les ordinateurs quantiques seront plus puissants que ne pourrait l'être un ordinateur classique de la taille du système solaire fonctionnant à la vitesse de la lumière avec des unités de mémoire de la taille de l'atome : nous vivons la naissance d'une technologie fondée sur les miracles théoriques du monde quantique, et qui projette ceux-ci dans notre réalité quotidienne.

Parallèlement à nos premiers pas vers ces calculateurs de rêve, une révolution modifie notre conception de l'information. Naïvement, nous avons trop longtemps adopté une vue préquantique de l'information. Pourtant ce qui «va de soi» concernant l'information est erroné si le monde est régi par la mécanique quantique. Le traitement de l'information dans un monde quantique est différent de sa manipulation dans un monde classique : il nous faut découvrir et pratiquer de nouvelles règles pour acquérir de l'information, la copier, la cacher, la mémoriser, la combiner, etc. En conséquence, la définition et la pratique du calcul changent et remettent en cause les fondements de l'informatique théorique.

Nous allons passer en revue dans cet article, en complément du précédent, quelques unes des différences entre information classique et information quantique. Précisons, avant cet examen, que nous adopterons une vue «physicienne» de l'information et que nous ne traitons évidemment pas d'information sémantique (le sens d'un mot, d'un texte, d'une musique, etc.) ou d'autres notions d'information destinées à cerner des contenus non symboliques.

Le lecteur quantique modifie le livre

Dans le monde classique, la consultation de l'information n'en modifie pas la teneur : lire un livre n'en change pas le texte, consulter un site Internet le laisse inchangé. Dans le monde classique, un objet est le même, qu'il soit connu ou pas. En revanche, l'ac-



1. INFORMATION ALÉATOIRE ET DUPLICATION INTERDITE. Un photon se propage selon une direction de polarisation perpendiculaire à son axe de propagation. Cette direction de polarisation est caractérisée par un angle *a*, qu'aucune mesure ne peut déterminer entièrement. Si, pour tenter de connaître cet angle, on place sur le trajet du photon un filtre polarisant d'angle 0, suivi d'un détecteur, alors le photon passera certainement si *a* égale 0, sera intercepté si *a* égale 90°, et passera avec une probabilité $\cos^2 a$ pour les angles intermédiaires. La détection ou non du photon est donc insuffisante pour connaître l'angle *a*. Dans une suite de photons ayant chacun un angle de polarisation égal à 45 degrés, la probabilité que chaque photon soit détecté après passage par le filtre est 1/2. En passant par le filtre polarisant, le photon perd son orientation primitive, ce qui rend l'angle *a* définitivement inconnaissable et le photon impossible à dupliquer.