

MATHÉMATIQUES

Gammes naturelles I

Yves HELLEGOUARCH (Université de Caen)

Si votre idée des gammes et de la justesse est basée sur l'accord du piano vous trafiquez dans la supercherie, pour dire les choses crûment ! Cette supercherie fut partiellement approuvée par J.-S. Bach et reçut l'appui total de son fils C.P.E. Bach, mais je ne pense pas que la seule vertu de ce nom illustre la préserve de toute critique !

Christopher Bunting [2]

Préambule

A lors que la théorie officielle de la musique est basée sur la notion d'échelle tempérée et est incapable de donner un fondement à l'attraction en musique ni même de justifier une distinction entre un la^b et un $sol^\#$, les praticiens du même art enseignent que le la^b est plus bas que le $sol^\#$ et que le premier est attiré vers le « sol » alors que le second est attiré vers le « la ».

Le texte qui suit est une version révisée d'une tentative déjà assez ancienne [15] de construction d'un modèle destiné à rapprocher la « musique théorique » de la « musique pratique » (comme aurait dit Euler [12]) tout en préservant la structure de groupe qui fait le succès populaire des échelles tempérées (\mathbb{Z} doit agir sur les gammes abstraites).

Nous allons maintenant rappeler quelques faits bien connus de la pratique des instruments à cordes qui nous serviront de guide.

Quand on déplace l'index de la main gauche sur une corde de violoncelle, en *appuyant*, et que l'on met la corde en vibration (entre le doigt et le chevalet) on obtient un son dont la fréquence mesurée dans une unité convenable est

$\frac{1}{x}$, x étant l'abscisse de l'index comptée de 0 pour le chevalet à 1 pour le sillet ($x \in]0, 1]$).

En revanche lorsque l'on déplace l'index de la main gauche sans appuyer et que l'on essaie de mettre la corde en vibration on peut :

- 1: soit échouer,
- 2: soit obtenir une harmonique naturelle du son de la « corde à vide » ($x = 1$) qui est déterminée de manière univoque lorsque $x = \frac{p}{q} \in]0, 1] \cap \mathbb{Q}$, fraction irréductible « simple » et $q > 0$. Mesurée dans la même unité, la fréquence de cette harmonique est égale à q .

Lorsque x n'est pas rationnel mais simplement « proche » d'une fraction $\frac{p}{q}$ assez « simple » (q est un entier positif pas trop « grand ») l'harmonique naturelle sort quand même comme si $x = \frac{p}{q}$, mais plus ou moins « difficilement ».

Il serait épineux de préciser les notions topologiques qui sont en cause ici : « proximité de x et de $\frac{p}{q}$ », « simplicité de $\frac{p}{q}$ », « facilité de la production de l'harmonique », car elles dépendent de données « physiques » dont nous voulons justement faire abstraction (hauteur de l'index au-dessus de la corde, forme de l'index, nature de la corde, position de l'archet, vitesse de l'archet, pression de l'archet, etc.).

Nous modéliserons la situation en disant que la fonction qui donne la hauteur $h(x)$ de l'harmonique naturelle associée à $x \in]0, 1] \cap \mathbb{Q}$ est définie par :

$$\begin{array}{ccc}]0, 1] \cap \mathbb{Q} & \xrightarrow{h} & \mathbb{R}_+^* \\ \frac{p}{q} & \longmapsto & q \end{array}$$

étant entendu que $\frac{p}{q}$ est irréductible et $q \geq 1$.

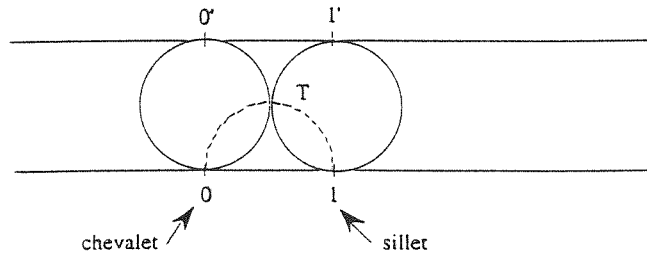
Remarque:

- 1: Si les conditions « physiques » étaient parfaites, on pourrait remplacer \mathbb{Q} par sa complétion non-standard ${}^*\mathbb{Q}$ et estimer que si x est la partie standard de $\frac{p}{q}$, alors $h(x) = q$ si q est limité et $h(x) = \infty$ si q est infiniment grand (donc une harmonique « qui ne sort pas » serait celle d'un $x \in]0, 1]$ qui serait irrationnel). Si l'on considère maintenant un instrument réel et une corde réelle, on constate que les « infiniment grands » ne sont pas très grands et que les harmoniques ne « sortent » plus en dehors d'une certaine suite de Farey \mathcal{F}_n (voir [13 p. 23]. Pour mon instrument $n = 13$.

Remarquons en passant que c'est l'étude des tempéraments musicaux qui a conduit Farey à la définition de ses suites et non ses activités de géologue [13] et [21]!

- 2: Il existe une interprétation géométrique de la fonction h qui rend compte des difficultés pratiques (qui semblent les mêmes en dessin et en musique) de la production des harmoniques naturelles et qui peut donner une intuition de la situation aux non-musiciens.

Dans un plan euclidien muni d'un repère traçons deux cercles de diamètre 1 situés au-dessus de l'axe des abscisses et touchant celui-ci en 0 et 1 :



Ces deux cercles se touchent en T et déterminent avec l'axe des abscisses un triangle curviligne $OT1$ dont le cercle inscrit touche l'axe des abscisses en $1/2$ et a pour diamètre $\frac{1}{2^2}$; ce cercle inscrit est l'inverse de la droite $O'I'$ par rapport au cercle de diamètre 01 qui est orthogonal à l'axe des abscisses, et aux deux cercles précédents.

En itérant cette construction on obtient les *cercles de Ford* des points de $[0, 1] \cap \mathbb{Q}$: ils sont tangents à l'axe des abscisses en $\frac{p}{q}$ (fraction irréductible, $q > 0$), de diamètre $\frac{1}{q^2}$ et situés dans le demi-plan supérieur (voir [18]).

La difficulté de dessiner ces cercles croît très vite et semble analogue à la difficulté de produire les harmoniques correspondantes.

1. Introduction musicale

Comme les motivations des définitions et constructions de ce travail peuvent paraître mystérieuses aux non-musiciens, je vais présenter un certain nombre de remarques préliminaires qui conduiront au point de vue que les paragraphes suivants vont développer de manière abstraite.

1.1. Nous allons commencer par modéliser la notion d'intervalle entre deux notes de fréquences x et y . Ces fréquences dépendent du choix de l'unité de fréquence, mais leur quotient $\frac{y}{x} \in \mathbb{R}_+^*$ est un *invariant* : c'est l'*intervalle* entre x et y (souvent les traités officiels préfèrent prendre le logarithme de ce nombre).

Exemples : Dire que l'intervalle entre x et y est une *octave* signifie que $\frac{y}{x} = 2$, dire que c'est une *quinte pure* signifie que $\frac{y}{x} = \frac{3}{2}$, dire que c'est une *quinte tempérée* signifie que $\frac{y}{x} = 2^{7/12}$.

Remarquons toutefois que l'*octave de S. Cordier* est $\left(\frac{3}{2}\right)^{12/7}$, voir [4].

Il est clair que la théorie de la musique est beaucoup plus concernée par l'étude des intervalles (qui est en lien direct avec l'*oreille relative*) que par celle des fréquences absolues (qui est en lien direct avec l'*oreille absolue*) qui dépend des conventions sociales, des lieux et des époques (voir [7]).

1.2. On s'efforce depuis plusieurs millénaires (voir [8] et [11]) de réduire l'ensemble des intervalles de la théorie de la musique à un sous-groupe propre de \mathbb{R}_+^* : c'est ce que l'on appelle une *échelle musicale*.

Exemples: 1) L'*échelle officielle*, dite « échelle tempérée » ou « échelle de Werckmeister » ou « échelle de Bach » est $\langle 2^{1/12} \rangle$, c'est-à-dire le sous-groupe multiplicatif de \mathbb{R}_+^* engendré par $2^{1/12}$: c'est un sous-groupe discret de \mathbb{R}_+^* .

2) L'*échelle de Serge Cordier* est $\langle \left(\frac{3}{2}\right)^{1/7} \rangle$, c'est aussi une « échelle tempérée » mais il ne faut pas la confondre avec la précédente bien qu'il s'agisse encore d'un sous-groupe discret de \mathbb{R}_+^* .

3) L'*échelle de Pythagore* est $\langle 2, 3 \rangle$, c'est-à-dire le sous-groupe de \mathbb{R}_+^* engendré par 2 et 3 : ce n'est pas un sous-groupe discret de \mathbb{R}_+^* .

4) L'*échelle de Zarlino* est $\langle 2, 3, 5 \rangle$, c'est-à-dire le sous-groupe de \mathbb{R}_+^* engendré par 2, 3 et 5 : ce n'est pas un sous-groupe discret de \mathbb{R}_+^* .

5) L'*échelle mésotonique* est $\langle 2, 5^{1/4} \rangle$ sous-groupe de \mathbb{R}_+^* engendré par 2 et $5^{1/4}$: il n'est pas discret.

6) Dans un travail célèbre [12] L. Euler a estimé que l'échelle $\langle 2, 3, 5, 7 \rangle$ n'était pas intéressante pour les musiciens.

Nous dirons qu'une échelle musicale E est *naturelle* lorsque $E \subset \mathbb{Q}_+^*$ et $2 \in E$.

Exemples: Les échelles de Pythagore et Zarlino sont naturelles, les échelles tempérées et l'échelle mésotonique ne le sont pas.

1.3. Il n'est pas question de répéter ici tout le mal qui a été dit de l'échelle tempérée officielle [21]. Bornons-nous à signaler qu'un piano accordé selon cette échelle sonne tout à fait faux ([24] p. 134) et que cette échelle paraît inadéquate pour modéliser les théories de l'harmonie pour la raison qu'elle ne contient pas les intervalles correspondants aux harmoniques les plus simples (quinte pure redoublée par exemple).

Les difficultés ont été très bien formulées par L. Euler en 1766 lorsqu'il affirmait que « l'organe de l'ouïe est accoutumé de prendre pour proportion simple toutes les proportions qui n'en diffèrent que fort peu, de sorte que la différence soit quasi imperceptible ». On pourrait ajouter que les instruments, eux aussi, « aiment » les fractions simples. Nous appellerons « *principe d'Euler* » cette affirmation.

1.4. Les fractions (supérieures ou égales à 1) les plus simples sont $\frac{1}{1}$ (unisson), $\frac{2}{1}$ (octave), $\frac{3}{2}$ (quinte), $\frac{4}{3}$ (quarte juste), etc.

Selon une étude du psychologue C. Stumpf (1848-1936) 75 % des auditeurs sans formation perçoivent comme un son unique deux sons simultanés à l'octave,

50 % réagissent de même à la quinte, 33 % à la quarte, 25 % à la tierce, 20 % au triton, 10 % à la seconde ([6] p. 187).

Si l'on appelle « hauteur » de la fraction irréductible de dénominateur positif $\frac{p}{q}$, le nombre $h\left(\frac{p}{q}\right) := \sup(p, q)$ et si l'on applique le *principe d'Euler* on obtient ainsi :

nom	fraction	hauteur	pourcentage de C. Stumpf
octave	$\frac{2}{1}$	2	75%
quinte	$\frac{3}{2}$	3	50%
quarte	$\frac{4}{3}$	4	33%
tierce	$\frac{5}{4}$	5	25%
triton	$\frac{7}{5}$	7	20%
seconde	$\frac{9}{8}$	9	10%

Il est difficile de ne pas remarquer que si l'on désigne par $\pi(x)$ le nombre de la dernière colonne situé sur la ligne x , le produit $(h(x) - 1)\pi(x)$ reste à peu près constant ! On est donc conduit à définir une *distance harmonique* sur \mathbb{Q}_+^* en posant :

$$d(x, y) := \text{Log } h\left(\frac{y}{x}\right)$$

On constate aisément en vérifiant les axiomes de la distance (c'est un cas particulier d'un résultat plus général [14]) que :

Théorème 1. — *La fonction $(x, y) \mapsto \text{Log } h\left(\frac{y}{x}\right)$ est une distance invariante sur \mathbb{Q}_+^* .*

Il en résulte que sa restriction à une échelle naturelle E est encore une distance invariante sur E (voir l'annexe pour les autres échelles).

1.5. Etant donnée une échelle naturelle E nous allons chercher un moyen de donner des *noms* aux éléments de E et pour cela il faut construire un morphisme de groupes :

$$\varphi : E \rightarrow \mathbb{Z}, \quad \text{tel que } \varphi(2) > 0.$$

Si x est un élément de E , le *degré* de x sera $\varphi(x)$. Une « *gamme naturelle* » associée à E sera une partie Γ de E telle que l'on ait une bijection $j : \mathbb{Z} \rightarrow \Gamma$ vérifiant la condition suivante :

$$j(n) \text{ est un élément de hauteur minimale de } \varphi^{-1}(n).$$

Alors se pose la question du choix des morphismes φ qui conduisent à des gammes utiles à la théorie de la musique. . .

1.6. La méthode d'accord des pianos par quintes et octaves [24] fournit l'idée de base, nous allons la préciser. Supposons que l'on veuille accorder un piano dont le « la₃ » est juste. Un procédé consiste à parcourir le « cycle » des quintes (intervalles de $\langle \frac{3}{2} \rangle$) :

$$\begin{array}{cccccccc} \text{la,} & \text{ré,} & \text{sol,} & \text{do,} & \text{fa,} & \text{si}^b & \text{mi}^b & \\ \text{la}^b, & \text{ré}^b, & \text{sol}^b, & \text{do}^b, & \text{fa}^b, & \text{si}^{bb} & = ? & \end{array}$$

En fait, si les quintes sont « justes » (égales à $\frac{3}{2}$) et non « tempérées » (égales à $2^{7/12}$) on ne peut pas retomber sur un « la », car l'équation :

$$\left(\frac{3}{2}\right)^{12} = 2^x$$

n'admet pas de solution $x \in \mathbb{N}$.

Deryck Cooke ([3] p. 44) exprime ce fait de manière frappante en disant : « alors que l'équation désirée musicalement est $\frac{3^{12}}{2^{19}} = 1$, l'équation mathématique correcte est $\frac{3^{12}}{2^{19}} = 1,013642\dots$ »

Traduit en termes mathématiques, ce que le musicien souhaite c'est imposer la relation :

$$r = \frac{3^{12}}{2^{19}} \equiv 1$$

dans le groupe abélien libre $\langle 2, 3 \rangle \subset \mathbb{Q}_+^*$; le groupe quotient n'étant alors rien d'autre que \mathbb{Z} . Si, finalement, on applique le principe d'Euler pour trouver un système de représentants des classes de $\langle 2, 3 \rangle$ modulo $\langle r \rangle$ on trouve (miraculeusement !) la « gamme chromatique de Pythagore » telle qu'elle est décrite dans les livres d'Histoire de la musique [7].

2. Commas

Soient des nombres de \mathbb{Q}_+^* que l'on note p, q, r , etc. Nous dirons que p, q, r , etc. sont des nombres multiplicativement indépendants dans \mathbb{Q}_+^* si $\text{Log } p, \text{Log } q, \text{Log } r$, etc. sont linéairement indépendants sur \mathbb{Q} et nous noterons par $\langle p, q \rangle, \langle p, q, r \rangle$, etc. les sous-groupes de \mathbb{Q}_+^* engendrés par $\{p, q\}, \{p, q, r\}$, etc. En fait nous penserons plus particulièrement à la suite :

$$\mathcal{S} \quad \langle 2, 3 \rangle, \quad \langle 2, 3, 5 \rangle, \dots$$

dont nous désignerons l'élément général par G .

Il est bien connu que tous ces sous-groupes sont denses dans \mathbb{Q}_+^* (voir [13]). Nous avons montré dans l'introduction l'intérêt des approximations de 1 dans le groupes $G \in \mathcal{S}$: nous appelons « commas » de G les meilleures de ces approximations et nous en donnons la définition suivante.

Définition.- Soit $G \in \mathcal{S}$ et $a \in G$. Nous dirons que a est un comma de G (ou meilleure approximation de 1 dans G) si et seulement si :

- i) $a \neq 1$
- ii) $b \in G \setminus \{1\}$ et $|\text{Log } b| < |\text{Log } a|$ entraînent $h(b) > h(a)$

Remarques :

- 1) Si $a = p_1^{n_1} \dots p_h^{n_h}$ est un comma de G , alors p.g.c.d. $(n_1, \dots, n_h) = 1$.
- 2) Un comma de G ne reste pas toujours un comma dans un groupe $G' \supset G$.
Par exemple $a = \frac{2^8}{3^5}$ est un comma de $\langle 2, 3 \rangle$, mais ce n'est pas un comma de $\langle 2, 3, 5 \rangle$.
- 3) Le critère suivant permet de construire un nombre fini de commas de G .

Critère : Si $G \in \mathcal{S}$ et si $a = \frac{b+1}{b} \in G$ avec $b \in \mathbb{Q}^*$, alors a est un comma de G .

Preuve – Soit $\frac{m}{n} \in \mathbb{Q}_+^*$ telle que $\frac{m}{n} > 1$ et $\text{Log } \frac{m}{n} < \text{Log } \frac{b+1}{b}$, nous voulons montrer que $m > b+1$.

Comme la fonction $x \mapsto \frac{x+1}{x}$ est décroissante sur $]0, +\infty[$ et que $\frac{n+1}{n} \leq \frac{m}{n} < \frac{b+1}{b}$, on voit que $n > b$ et comme $m \geq n+1 > b+1$, on a le résultat. ■

Le fait qu'il n'existe qu'un nombre fini de « commas absolus » de ce type dans un groupe de type fini, résulte du théorème des S -unités de Siegel ([20] ou [26]) qui est infiniment plus profond.

3. Commas des groupes de rang 2

Nous revenons à la situation du paragraphe 2 en prenant un sous-groupe *quelconque* de rang 2 de \mathbb{Q}_+^* que l'on notera encore G . Si $\{p, q\}$ est une base de G , p et q sont multiplicativement indépendants et la recherche des commas de G équivaut à la recherche des couples $(x, y) \in \mathbb{Z}^2$, tels que $(x, y) \neq (0, 0)$ et tels que $x \text{Log } p + y \text{Log } q$ soit voisin de 0. Ainsi $-\frac{x}{y}$ doit être une « bonne

approximation » de l'irrationnel $\alpha = \frac{\text{Log } q}{\text{Log } p} = \text{Log}_p(q)$ que l'on suppose > 1 .

La recherche des bonnes approximations de α se fait habituellement par l'algorithme des fractions continues [27] : on construit ainsi une suite de fractions $\frac{p_n}{q_n}$, les « convergentes » de α , convergeant vers α selon le schéma :

$$\frac{q_0}{p_0} < \frac{q_2}{p_2} \dots < \alpha < \dots < \frac{q_3}{p_3} < \frac{q_1}{p_1}.$$

En posant (un peu arbitrairement) :

$$(x_n, y_n) = ((-1)^{n-1} p_n, (-1)^n q_n)$$

on obtient le résultat suivant.

Théorème 2. — *La suite des rationnels $r_n = p^{x_n} q^{y_n}$ est monotone décroissante et tend vers 1. De plus, on a :*

$$p^{\frac{1}{2|y_{n+1}|}} < r_n < p^{\frac{1}{|y_{n+1}|}}$$

Preuve —

1) On sait que $p_n - q_n \alpha$ a le signe de $(-1)^{n-1}$, [27], donc :

$$x_n + y_n \alpha = (-1)^{n-1} [p_n - \alpha q_n] > 0$$

soit $r_n > 1$.

2) Maintenant :

$$\frac{\text{Log } r_{n+1}}{\text{Log } r_n} = \frac{x_{n+1} + \alpha y_{n+1}}{x_n + \alpha y_n} = -\frac{p_{n+1} - \alpha q_{n+1}}{p_n - \alpha q_n}.$$

Or on sait [27] que :

$$\left| \frac{p_{n+1} - \alpha q_{n+1}}{p_n - \alpha q_n} \right| < 1$$

d'où :

$$\frac{\text{Log } r_{n+1}}{\text{Log } r_n} < 1.$$

3) Les deux inégalités de l'énoncé équivalent à :

$$\frac{1}{2q_{n+1}} < x_n + \alpha y_n < \frac{1}{q_{n+1}}$$

soit encore à :

$$\frac{1}{2q_{n+1}} < |p_n - \alpha q_n| < \frac{1}{q_{n+1}}$$

ce qui est bien connu [27]. ■

Exemple: Le calcul des convergentes de $\alpha = \frac{\text{Log } 3}{\text{Log } 2} = \text{Log}_2(3)$ donne la suite de rationnels :

$$\frac{2}{1} > \frac{3}{2} > \frac{2^2}{3} > \frac{3^2}{2^3} > \frac{2^8}{3^5} > \frac{3^{12}}{2^{19}} > \frac{2^{65}}{3^{41}} > \frac{3^{53}}{2^{84}} > \dots > 1.$$

Si nous posons : $r_{-1} = \frac{2}{1}$, $r_0 = \frac{3}{2}$, $r_1 = \frac{2^2}{3}$, etc. nous constatons que nous avons ainsi construit la suite des commas du groupe $G = \langle 2, 3 \rangle$.

Ce fait est général en un certain sens.

Théorème 3. — *On suppose que p et q sont des entiers positifs premiers entre eux et tels que $1 < p < q$. Alors les commas supérieurs à 1 du groupe $G = \langle p, q \rangle$ sont obtenus par le procédé décrit ci-dessus à partir des convergentes du nombre irrationnel $\alpha = \text{Log}_p q$.*

Preuve —

1) Nous allons décrire un algorithme extrêmement élémentaire (il ne nécessite pas la connaissance de α !) pour construire les commas de $\langle p, q \rangle$.

La première étape consiste à déterminer un entier $a_0 \geq 1$ tel que $p^{a_0} < q < p^{a_0+1}$; un tel entier existe parce que $p < q$.

Si on pose $r_0 = \frac{q}{p^{a_0}}$ et si nous comparons à l'algorithme classique ([27]

p. 187) nous voyons que r_0 est associé à la première convergente $\frac{a_0}{1}$ de α . Supposons maintenant que nous ayons construit r_{n-2} et r_{n-1} (c'est le cas si $n = 1$ en prenant $r_{-1} = \frac{p}{1}$) alors on cherche $a_n \geq 1$ vérifiant la condition :

$$(r_{n-1})^{a_n} < r_{n-2} < (r_{n-1})^{a_n+1}$$

ceci est encore possible parce que $r_{n-1} < r_{n-2}$ et que r_{n-1} et r_{n-2} sont multiplicativement indépendants.

2) Une comparaison avec [27] p. 187-188, montre que l'on obtient un algorithme identique à l'algorithme classique, ce qui justifie a priori l'indépendance multiplicative de r_{n-1} et r_{n-2} et montre que $G = \langle r_{n-2}, r_{n-1} \rangle$.

3) Montrons que $r_n := r_{n-2} r_{n-1}^{-a_{n-1}}$ est un comma.

Soit $b = p^x q^y \in G \setminus \{1\}$ tel que :

$$|\text{Log}_p(b)| = |x + y \text{Log}_p q| < \text{Log}_p(r_n) = x_n + y_n \text{Log}_p q$$

avec $(x_n, y_n) = ((-1)^{n-1} p_n, (-1)^n q_n)$.

Puisque l'on sait que $\frac{p_n}{q_n}$ est une meilleure approximation de $\text{Log}_p q$ on a : $|y| > q_n$ et $|x| > p_n$ (la seconde inégalité résulte de la première et de $|\text{Log}_p b| < \text{Log}_p r_n$). On voit aussi que x et y ont des signes opposés et on en déduit que $h(b) > h(r_n)$ puisque p et q sont premiers entre eux.

4) Montrons que tout comma est un r_n .

Il suffit de reprendre le point de vue ci-dessus : si $a = p^x q^y$ est un comma, x et y doivent avoir des signes opposés et $\left| \frac{x}{y} \right|$ doit être une meilleure approximation de $\text{Log}_p(q)$. D'après la théorie classique des fractions continues, $\left| \frac{x}{y} \right|$ est une convergente de $\text{Log}_p(q)$. ■

4. Groupes quotients et gammes pour le rang 2

Nous considérons un groupe $G = \langle p, q \rangle$ où p et q sont des entiers multiplicativement indépendants et premiers entre eux et nous nous donnons un commma r_n de G . Nous nous proposons en premier lieu d'étudier le groupe quotient $G / \langle r_n \rangle$ et en second lieu d'étudier sa gamme.

4.1. Comme dans le paragraphe 3) on écrit $r_n = p^{x_n} q^{y_n}$ et on introduit aussi $r_{n-1} = p^{x_{n-1}} q^{y_{n-1}}$. On utilisera la relation classique :

$$(*) \quad x_n y_{n-1} - x_{n-1} y_n = (-1)^{n-1}$$

Théorème 4. — *Désignons par N le groupe $\langle r_n \rangle$. Alors G/N est un groupe isomorphe à \mathbb{Z} qui est engendré par la classe de r_{n-1} .*

Preuve — Il est équivalent de démontrer, en notation additive, que $\mathbb{Z}^2 / \mathbb{Z}(x_n, y_n)$ est un groupe sans torsion qui est engendré par la classe de (x_{n-1}, y_{n-1}) .

1) Groupe sans torsion.

Montrons que si $h > 0$ la relation :

$$h(x, y) \in \mathbb{Z}(x_n, y_n)$$

entraîne que $(x, y) = k(x_n, y_n)$ avec $k \in \mathbb{Z}$.

Notre hypothèse équivaut à :

$$\begin{cases} hx = \ell x_n \\ hy = \ell y_n \end{cases}$$

pour un certain $\ell \in \mathbb{Z}$ et comme x_n et y_n sont premiers entre eux d'après la relation rappelée ci-dessus, on voit que h divise ℓ . Si l'on pose $\ell = hk$ et si l'on simplifie par h , on a le résultat.

2) Générateur.

Dire que (a, b) est un générateur de $\mathbb{Z}^2 / \mathbb{Z}(x_n, y_n)$ revient à dire que tout $(x, y) \in \mathbb{Z}^2$ s'écrit :

$$(x, y) = h(a, b) + k(x_n, y_n)$$

donc que (a, b) et (x_n, y_n) constituent une base de \mathbb{Z}^2 , ce qui est bien le cas si $(a, b) = (x_{n-1}, y_{n-1})$. ■

Théorème 5. — *Dans G/N la classe de p (resp. q) est égale à $|y_n|$ fois (resp. $|x_n|$ fois) la classe du générateur r_{n-1} .*

Preuve — Il suffit de démontrer cette propriété pour la classe de p , ce qui équivaut à :

$$p \equiv r_{n-1}^{|y_n|} \pmod{N}$$

ou bien (en notation additive) :

$$(1, 0) \equiv |y_n| (x_{n-1}, y_{n-1}) \pmod{\mathbb{Z}(x_n, y_n)}.$$

Il résulte de (*) que $|y_n| x_{n-1} + (-1)^{n+1} x_n y_{n-1} = 1$ ce qui prouve le résultat. ■

Dorénavant nous supposons que $p < q$. Puisque r_{n-1} est déterminé de manière canonique nous avons déterminé un *générateur canonique* g_n (la classe de r_{n-1}) dans le quotient $G / \langle r_n \rangle \cong \mathbb{Z}$ (« gamme abstraite »).

Définition.- Soit φ_n l'application canonique :

$$G \rightarrow H_n := G / \langle r_n \rangle$$

Le degré d'un intervalle x de l'échelle G est le nombre $h \in \mathbb{Z}$ tel que $\varphi_n(x) = g_n^h$.

Définition.- La gamme chromatique Γ_n associée à la gamme abstraite $H_n := G / \langle r_n \rangle$ est une famille doublement infinie de représentants de plus petite hauteur des éléments de G modulo $\langle r_n \rangle$.

La première octave de cette gamme est formée par les représentants des classes de $g_n^0, g_n^1, \dots, g_n^{|y_n|}$.

Remarques :

1) On voit de même que la classe de r_{n+1} engendre H_n et que l'on a en fait $r_{n-1} \equiv r_{n+1} \pmod{\langle r_n \rangle}$. Mais ceci ne nous intéresse pas puisque $h(r_{n+1}) > h(r_{n-1})$.

2) Les musiciens s'intéressent surtout aux fréquences des intervalles de la première octave. Pour les octaves supérieures (ou inférieures) ils multiplient ces fréquences par une puissance adéquate de p , ce que nous ne ferons pas.

3) On montre facilement que si r_n est un comma ces représentants sont uniques.

Exemples: Gammes de Pythagore.

On considère l'échelle $G = \langle 2, 3 \rangle$ et on rappelle que ses commas sont :

$$\frac{2}{1} > \frac{3}{2} > \frac{2^2}{3} > \frac{3^2}{2^3} > \frac{2^8}{3^5} > \frac{3^{12}}{2^{19}} > \frac{2^{65}}{3^{41}} > \frac{3^{53}}{2^{84}} > \dots > 1$$

1) $r_{-1} = \frac{2}{1}$, $H_{-1} = G / \langle r_{-1} \rangle \cong \langle 3 \rangle$, $\Gamma_{-1} = \{3^n; n \in \mathbb{Z}\}$

2) $r_0 = \frac{3}{2}$, $H_0 = G / \langle r_0 \rangle$, $\Gamma_0 = \{2^n; n \in \mathbb{Z}\}$

3) $r_1 = \frac{2^2}{3}$, $H_1 = G / \langle r_1 \rangle$, $\Gamma_1 = \dots 3^{-1}, 2^{-1}, 1, 2, 3, 6, 9, 18, \dots$

4) $r_2 = \frac{3^2}{2^3}$, $H_2 = G / \langle r_2 \rangle$, la première octave de Γ_2 est $(1, \frac{3}{2}, 2)$. On voit que dans ce cas r_1 n'est pas l'élément de plus petite hauteur de la classe de g_2 .

5) $r_3 = \frac{2^8}{3^5}$, $H_3 = G / \langle r_3 \rangle$ est la *gamme pentatonique*, la première octave de Γ_3 est $(1, \frac{3^2}{2^3}, \frac{2^2}{3}, \frac{3}{2}, \frac{2^4}{3^2}, 2)$.

6) $r_4 = \frac{3^{12}}{2^{19}}$, $H_4 = G / \langle r_4 \rangle$ est la *gamme de Pythagore* proprement dite, la première octave de Γ_4 est :

$$\left(1, \frac{2^8}{3^5}, \frac{3^2}{2^3}, \frac{2^5}{3^3}, \frac{3^4}{2^6}, \frac{2^2}{3}, \frac{3^6}{2^9}, \frac{3}{2}, \frac{2^7}{3^4}, \frac{3^3}{2^4}, \frac{2^4}{3^2}, \frac{3^5}{2^7}, 2\right)$$

7) $r_5 = \frac{2^{65}}{3^{41}}$, $H_5 = G / \langle r_5 \rangle$ est la *gamme de Janko* (à 41 degrés dans une octave).

8) $r_6 = \frac{3^{53}}{2^{84}}$, $H_6 = G / \langle r_6 \rangle$ est la *gamme de Mercator* (à 53 degrés dans une octave).

GAMME DE PYTHAGORE A 41 DEGRES :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	$\frac{3^{12}}{2^{19}}$	$\frac{2^{27}}{3^{17}}$	$\frac{2^8}{3^5}$	$\frac{3^7}{2^{11}}$	$\frac{3^{19}}{2^{30}}$	$\frac{2^{16}}{3^{10}}$	$\frac{3^2}{2^3}$	$\frac{3^{14}}{2^{22}}$	$\frac{2^{24}}{3^{15}}$	$\frac{2^5}{3^3}$	$\frac{3^9}{2^{14}}$	$\frac{2^{32}}{3^{20}}$	$\frac{2^{13}}{3^8}$	$\frac{3^4}{2^6}$	$\frac{3^{16}}{2^{25}}$	$\frac{2^{21}}{3^{13}}$	$\frac{2^2}{3}$	$\frac{3^{11}}{2^{17}}$	$\frac{2^{29}}{3^{18}}$	$\frac{2^{10}}{3^6}$
	C do		D ^b ré ^b				D ré			E ^b mi ^b				E mi			F fa			

21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
$\frac{3^6}{2^9}$	$\frac{3^{18}}{2^{28}}$	$\frac{2^{18}}{3^{11}}$	$\frac{3}{2}$	$\frac{3^{13}}{2^{20}}$	$\frac{2^{26}}{3^{16}}$	$\frac{2^7}{3^4}$	$\frac{3^8}{2^{12}}$	$\frac{3^{20}}{2^{31}}$	$\frac{2^{15}}{3^9}$	$\frac{3^3}{2^4}$	$\frac{3^{15}}{2^{23}}$	$\frac{2^{23}}{3^{14}}$	$\frac{2^4}{3^2}$	$\frac{3^{10}}{2^{15}}$	$\frac{2^{31}}{3^{19}}$	$\frac{2^{12}}{3^7}$	$\frac{3^5}{2^7}$	$\frac{3^{17}}{2^{26}}$	$\frac{2^{20}}{3^{12}}$	$\frac{2}{3}$
F [#] fa [#]			G sol			A ^b la ^b				A la			B ^b si ^b			B si				C do

GAMME DE PYTHAGORE A 53 DEGRES :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	$\frac{3^{12}}{2^{19}}$	$\frac{3^{24}}{2^{38}}$	$\frac{2^{27}}{3^{17}}$	$\frac{2^8}{3^5}$	$\frac{3^7}{2^{11}}$	$\frac{3^{19}}{2^{30}}$	$\frac{2^{35}}{3^{22}}$	$\frac{2^{16}}{3^{10}}$	$\frac{3^2}{2^3}$	$\frac{3^{14}}{2^{22}}$	$\frac{3^{26}}{2^{41}}$	$\frac{2^{24}}{3^{15}}$	$\frac{2^5}{3^3}$	$\frac{3^9}{2^{14}}$	$\frac{3^{21}}{2^{33}}$	$\frac{2^{32}}{3^{20}}$	$\frac{2^{13}}{3^8}$
	$\frac{1}{C}$			$\frac{D^b}{re^b}$					$\frac{D}{re}$				$\frac{E^b}{mi^b}$				
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
$\frac{3^4}{2^6}$	$\frac{3^{16}}{2^{25}}$	$\frac{2^{40}}{3^{25}}$	$\frac{2^{21}}{3^{13}}$	$\frac{2^2}{3}$	$\frac{3^{11}}{2^{17}}$	$\frac{3^{23}}{2^{36}}$	$\frac{2^{29}}{3^{18}}$	$\frac{2^{10}}{3^6}$	$\frac{3^6}{2^9}$	$\frac{3^{18}}{2^{28}}$	$\frac{2^{37}}{3^{23}}$	$\frac{2^{18}}{3^{11}}$	$\frac{3}{2}$	$\frac{3^{13}}{2^{20}}$	$\frac{3^{25}}{2^{39}}$	$\frac{2^{26}}{3^{16}}$	$\frac{2^7}{3^4}$
$\frac{E}{mi}$				$\frac{F}{fa}$					$\frac{F\#}{fa\#}$				$\frac{G}{sol}$				$\frac{A^b}{la^b}$
36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53
$\frac{3^8}{2^{12}}$	$\frac{3^{20}}{2^{31}}$	$\frac{2^{34}}{3^{21}}$	$\frac{2^{15}}{3^9}$	$\frac{3^3}{2^4}$	$\frac{3^{15}}{2^{23}}$	$\frac{2^{42}}{3^{26}}$	$\frac{2^{23}}{3^{14}}$	$\frac{2^4}{3^2}$	$\frac{3^{10}}{2^{15}}$	$\frac{3^{22}}{2^{34}}$	$\frac{2^{31}}{3^{19}}$	$\frac{2^{31}}{3^7}$	$\frac{3^5}{2^7}$	$\frac{3^{17}}{2^{26}}$	$\frac{2^{39}}{3^{24}}$	$\frac{2^{20}}{3^{12}}$	$\frac{2}{C}$
				$\frac{A}{la}$				$\frac{B^b}{si^b}$					$\frac{B}{si}$				$\frac{C}{do}$

Les exemples précédents conduisent à conjecturer que Γ_n est une *suite croissante* (au moins pour les gammes de Pythagore et la première octave!). Nous allons prouver cette conjecture dans le cas où $G = \langle p, q \rangle$ avec $1 < p < q$, p et q entiers premiers entre eux. On utilise la relation $r_n = r_{n-2} r_{n-1}^{-a_n}$ du paragraphe 3.

Théorème 6. — *Les commas r_m pour $m < n - 1$ sont les représentants de plus petite hauteur de leurs classes modulo $\langle r_n \rangle$. Ces commas sont dans la première octave de Γ_n et apparaissent par ordre décroissant.*

Si $a_n \geq 2$, r_{n-1} apparaît également au premier degré avant r_{n-2} .

Les degrés des commas $r_{n-1}, r_{n-2}, \dots, r_{-1}$ dans $H_n = G / \langle r_n \rangle$ sont les dénominateurs des convergentes successives de $[1, a_n, a_{n-1}, \dots, a_1]$.

De plus, la gamme Γ_n est croissante.

Preuve — Les premières assertions résultent facilement de la relation rappelée ci-dessus.

Montrons que si ν_i est l'élément général de Γ_n on a $\nu_i < \nu_{i+1}$.

On se borne au cas où $i > 0$, car $\nu_{-i} = \nu_i^{-1}$ si $i > 0$, et on procède par récurrence sur i .

Si $i = 1$, cela résulte des premières assertions.

Soit $r = \nu_1$: on passe de ν_i à ν_{i+1} en multipliant ν_i par r et en effectuant éventuellement une correction soit par r_n soit par r_n^{-1} (en fonction de a_n) : désignons par r' cette correction.

Puisque ν_i est de plus petite hauteur dans sa classe $h(r'\nu_i) > h(\nu_i)$.

Maintenant on voit que soit $r\nu_i$ est de plus petite hauteur dans sa classe, soit $r'\nu_i$ est l'élément de plus petite hauteur car $r'\nu_i$ et $rr'^{2r}\nu_i$ sont de même type c'est-à-dire qu'ils ont tous les deux une puissance de p en numérateur ou tous les deux une puissance de q en numérateur. Il en résulte que $h(r'^{2r}\nu_i) > h(r'\nu_i)$. ■

Remarque. Le nombre de corrections dans la première octave est égal à $|x_{n-1}|$ si $a_n > 1$ et à $|x_{n-2}|$ si $a_n = 1$.

La seconde partie de l'article Gammes naturelles paraîtra dans le prochain numéro de la Gazette.

Peter W. Shor, Prix Nevanlinna 1998

Franck LEPRÉVOST (*Institut de Mathématiques de Jussieu*)

Introduction

Le prix Nevanlinna 1998 a été remis à Peter W. Shor au cours du congrès international des mathématiciens qui s'est tenu à Berlin. Les travaux de Shor concernent l'informatique quantique (13 publications), la géométrie discrète et combinatoire (15 publications), la compression (11 publications), les probabilités appliquées (3 publications), la combinatoire (9 publications), la théorie de la complexité (3 publications). A ces travaux s'ajoutent 11 autres publications qui ne se rangent dans aucun des domaines précédents. Le lecteur aura compris que Peter Shor a un prisme scientifique particulièrement impressionnant. Et encore, les informations ci-dessus ne reflètent-elles que la version de janvier 1998 de sa liste de publications. Avant d'aller plus loin, nous suggérons au lecteur intéressé de « surfer » à partir de [11]. Nous avons pris dans ce rapport un point de vue particulièrement réducteur : comment faire autrement en quelques pages ? Nous décrivons ici une partie des travaux de Shor relatifs à l'informatique quantique (voir [1], [13]), à la cryptanalyse quantique (voir [14]) et aux codes correcteurs d'erreurs quantiques (voir [2], [3]). Cet article fait en quelque sorte suite à [9].

Peter Shor

Informatique quantique

Circuits quantiques

En termes très informels, l'unité d'information « atomique » de base est appelée bit en informatique classique et qubit en informatique quantique. Par analogie avec un bit classique, dont la valeur est 0 ou 1, un bit quantique ou qubit est un système quantique à deux états et se voit comme élément de \mathbf{C}^2 (en fait, les états quantiques sont invariants par multiplication par des scalaires et vivent donc dans $\mathbf{P}^2(\mathbf{C})$). Soient V_0 et V_1 une base orthogonale de \mathbf{C}^2 . Un des principes de la mécanique quantique implique que l'espace des états quantiques de n qubits est \mathbf{C}^{2^n} . C'est en quelque sorte cette dimension exponentielle qui fournit la « surpuissance » de calcul. Les vecteurs de base sont paramétrés par les suites binaires de longueur n et on note

$$V_{b_1 \dots b_n} = V_{b_1} \otimes \dots \otimes V_{b_n}.$$

Les vecteurs de base peuvent naturellement être normalisés et seront dans la suite supposés unitaires.

Un ordinateur prend une donnée en entrée, agit dessus par des calculs et renvoie un résultat en sortie. Qu'est-ce que cela signifie pour un ordinateur quantique ? Pour un ordinateur quantique, l'entrée est une suite binaire S de longueur k . Elle est codée pour donner l'état initial de l'ordinateur sous la forme d'un vecteur de \mathbf{C}^{2^n} . Pour cela, on concatène S avec $n - k$ 0 : $S0 \cdots 0$, et l'ordinateur quantique est initialisé à $V_{S0 \cdots 0}$.

À la fin du calcul, l'ordinateur quantique est dans un état égal à un vecteur unitaire de \mathbf{C}^{2^n} :

$$W = \sum_s \alpha_s V_s,$$

où $|s| = n$, $\alpha_s \in \mathbf{C}$ et $\sum_s |\alpha_s|^2 = 1$. On dit alors que W est la superposition des vecteurs de base V_s , et que α_s est leur amplitude probabiliste. En mécanique quantique, le principe d'incertitude de Heisenberg dit que nous ne pouvons pas mesurer l'état quantique complet du système. Il y a cependant un grand nombre de mesures possibles : par exemple, toute base orthogonale de \mathbf{C}^{2^n} définit une mesure, dont les résultats possibles sont les éléments de cette base. Nous supposons cependant que le résultat est obtenu par projection de chaque qubit sur la base $\{V_0, V_1\}$. Si on applique cette projection à l'état W , elle produit la suite s avec probabilité $|\alpha_s|^2$. Comme les mesures quantiques sont probabilistes, on n'exige pas que le calcul donne toujours la bonne réponse, mais seulement les 2/3 du temps. En fait, on peut choisir d'avoir un résultat valide pour une proportion x du temps, où $\frac{1}{2} < x < 1$, sans changer ce qui peut être calculé en temps polynômial sur un ordinateur quantique. On peut augmenter la confiance que l'on a en un résultat en répétant plusieurs fois les calculs et en prenant le résultat qui revient le plus souvent.

Qu'en est-il du calcul proprement dit ? En d'autres termes, quelles sont les règles de manipulation d'un état dans un circuit quantique ? Dans un circuit classique, on dispose de trois portes logiques : AND, OR et NOT. Ils forment un ensemble universel de portes logiques dans le sens où ils suffisent pour décrire tout circuit classique. La situation est similaire pour un circuit quantique : les transformations physiques possibles d'un système quantique sont les transformations unitaires et chaque porte logique quantique est une matrice unitaire. Ainsi, une porte logique quantique sur un qubit est une matrice 2×2 , et sur deux qubits, une matrice 4×4 . Comme les matrices unitaires sont inversibles, le calcul est réversible. De plus, la dimension de l'espace de sortie est égale à celle de l'espace d'entrée. Les portes logiques quantiques qui agissent sur un ou deux qubits (\mathbf{C}^2 ou \mathbf{C}^4) induisent naturellement une transformation de l'espace des états de l'ordinateur quantique (\mathbf{C}^{2^n}). Par exemple, si A est une matrice 4×4 agissant sur les qubits i et j , l'action induite sur un vecteur de base de \mathbf{C}^{2^n} est

$$A^{[i,j]} V_{b_1 \cdots b_n} = \sum_{s=0}^1 \sum_{t=0}^1 A_{b_i b_j s t} V_{b_1 \cdots b_{i-1} s b_{i+1} \cdots b_{j-1} t b_{j+1} \cdots b_n}.$$

Cette action est en fait donnée par $A \otimes I$, où A agit sur les qubits i et j et I sur les autres qubits.

Là encore, on dispose d'un ensemble universel de portes logiques pour les circuits quantiques, c'est-à-dire suffisants pour construire les circuits pour tout calcul quantique. Un tel ensemble utile est fourni par exemple par toutes les portes logiques à 1 bit auxquelles on adjoint CNOT (Controlled NOT), qui est une porte logique à 2 bits. cnot envoie V_{XY} sur V_{XZ} où $Z = X + Y \pmod 2$. Ces portes peuvent simuler tous les circuits quantiques dont les portes agissent seulement sur un nombre constant de qubits (voir [1]).

La classe BQP

Depuis l'avènement des ordinateurs, la distinction entre fonction calculable et pas calculable est devenue trop grossière (bien que nous ne définissions pas ces termes ici). La « bonne » notion est celle de fonction calculable en temps polynômial. Il s'agit des fonctions dont la valeur est calculable en un nombre d'étapes polynômial en la taille des données d'entrée. L'ensemble des langages correspondants (fonctions à valeur dans $\{0, 1\}$) est noté **P** (ou **P**TIME). Dans le cadre des ordinateurs quantiques, on a besoin de définir des notions analogues. C'est pourquoi on introduit la classe de complexité **BQP** (ces initiales signifient *bounded-error quantum polynomial time*). C'est la classe des langages (les fonctions à valeur dans $\{0, 1\}$) qui peuvent être calculés en temps polynômial sur un ordinateur quantique, où la réponse donnée par l'ordinateur est correcte au moins les 2/3 du temps. Plus précisément : tout circuit quantique spécifique peut seulement calculer une fonction qui prend en entrée une suite binaire de taille spécifique. Pour utiliser le modèle des circuits quantiques en vue d'implémenter des fonctions dont l'entrée est de taille arbitraire, on prend une famille de circuits quantiques, avec un circuit par taille. Sans conditions supplémentaires sur cette famille de circuits, il serait possible de cacher une fonction non calculable dans le protocole ! Pour éviter que des fonctions non calculables appartiennent à **BQP**, on ajoute des conditions d'*uniformité* sur la famille de circuits. Nous n'entrons pas davantage dans les détails ici et nous contentons de définir les fonctions calculables en temps polynômial sur un ordinateur quantique comme les fonctions calculables par une famille *uniforme* de circuits dont la taille (égale au nombre de portes logiques) est polynômiale en la longueur de l'entrée et donne la bonne réponse au moins les 2/3 du temps. L'ensemble des langages (les fonctions à valeur dans $\{0, 1\}$) correspondants est noté **BQP**.

Propositions expérimentales

Les ordinateurs quantiques sont des machines dont l'existence est encore hypothétique. Ils utilisent les principes de la mécanique quantique pour leurs opérations de base. Même si aucune loi physique ne semble obstruer la possibilité de les construire, ils ne sont pas du tout aisés à mettre en œuvre. Il s'agit d'utiliser des systèmes quantiques relativement stables qui ont les deux propriétés suivantes :

- Ils interagissent fortement entre eux, ceci afin de transporter rapidement les portes logiques quantiques.

– Ils interagissent faiblement avec tout le reste, afin d'éviter les erreurs causées par l'interaction avec l'environnement.

Quelles sont les propositions actuelles pour l'implémentation expérimentale des ordinateurs quantiques ? Il y en a trois à l'heure où nous écrivons ces lignes :

– utiliser comme qubits les états électroniques des ions dans un piège électromagnétique à ions et les manipuler avec des lasers (voir [4]).

– utiliser comme qubits les spins nucléaires d'atomes dans une molécule complexe et les manipuler à l'aide de résonance magnétique nucléaire (voir [5] et [6]).

– utiliser comme qubits les spins nucléaires des impuretés d'une puce à silicium et les manipuler à l'aide de l'électronique de cette puce (voir [8]).

Aucune de ces propositions n'a été réalisée expérimentalement pour plus que quelques qubits.

Algorithme polynômial de factorisation

Idée générale

Soit N un nombre de taille L bits. Le meilleur algorithme classique de factorisation est NSF (Number Field Sieve), dont la complexité est en $O(\exp(cL^{1/3} \text{Log}^{2/3} L))$. La complexité de l'algorithme quantique de factorisation de Shor est, lui, en $O(L^2 \text{Log} L \text{Log} \text{Log} L)$.

L'idée utilisée ici pour factoriser N consiste à trouver $s \not\equiv \pm t \pmod{N}$ tels que $s^2 \equiv t^2 \pmod{N}$. En ce cas,

$$(s+t)(s-t) \equiv 0 \pmod{N}$$

et $s+t$ (resp. $s-t$) contient un facteur de N . Par l'algorithme d'Euclide, on calcule (sur un ordinateur classique) en temps polynômial le $\text{pgcd}(s \pm t, N)$ qui est l'un des facteurs de N .

Algorithme de factorisation quantique

L'algorithme de factorisation quantique permet de trouver (si elle existe) la période multiplicative d'un résidu $x \pmod{N}$, qui est le plus petit entier $r \geq 1$ tel que :

$$x^r \equiv 1 \pmod{N}.$$

Avec de la chance, r est pair et $x^{r/2} \not\equiv \pm 1 \pmod{N}$. En ce cas, l'équation

$$(x^{r/2} - 1)(x^{r/2} + 1) \equiv 0 \pmod{N}$$

permet de conclure que $\text{pgcd}(x^{r/2} \mp 1, N)$ est un facteur de N . En général, au bout de quelques essais, on obtient un tel x .

L'avantage d'un ordinateur quantique est que l'on peut trouver cette période en temps polynômial en exploitant la dimension égale à 2^{2L} des espaces d'états de $2L$ qubits, et en prenant la transformée de Fourier sur cet espace. Comme la dimension de l'espace est exponentielle, on peut prendre la transformée de Fourier d'une suite de longueur exponentielle.

Qu'est-ce que la transformée de Fourier quantique ? Elle agit sur les qubits en transformant l'état V_a (où a est un entier $0 \leq a \leq 2^k - 1$) en la superposition des états V_b :

$$V_a \longrightarrow \frac{1}{2^{k/2}} \sum_{b=0}^{2^k-1} \exp(2i\pi ab/2^k) V_b.$$

Cette transformation définit une matrice unitaire et s'implémente comme une suite de portes logiques quantiques à 1 ou 2 bits.

Quelles sont les étapes de l'algorithme ? Il faut commencer par faire le schéma d'un circuit de taille polynômiale placé au départ dans l'état quantique $V_{0\dots 0}$ et dont le résultat r renvoyé en sortie permet, pour une probabilité raisonnable, de factoriser N de longueur L -bits en temps polynômial sur un ordinateur classique. Le circuit en question possède deux registres principaux. Le premier (resp. le second) est composé de $2L$ (resp. L) qubits, auxquels s'ajoutent quelques qubits qui fournissent l'espace de travail nécessaire à l'étape 2 ci-dessous.

(1) On commence par mettre l'ordinateur dans l'état représentant la superposition de toutes les valeurs possibles du premier registre :

$$\frac{1}{2^L} \sum_{a=0}^{2^{2L}-1} V_a \otimes V_0.$$

(2) On utilise ensuite la valeur de a dans le premier registre pour calculer la valeur $x^a \pmod{N}$ dans le second registre. Pour cela, on peut se servir d'un circuit réversible classique. L'ordinateur est alors dans l'état :

$$\frac{1}{2^L} \sum_{a=0}^{2^{2L}-1} V_a \otimes V_{x^a \pmod{N}}.$$

(3) On prend la transformée de Fourier du premier registre. L'ordinateur est alors dans l'état :

$$\frac{1}{2^{2L}} \sum_{a=0}^{2^{2L}-1} \sum_{b=0}^{2^{2L}-1} \exp(2i\pi ab/2^{2L}) V_b \otimes V_{x^a \pmod{N}}.$$

(4) Enfin, on mesure l'état. Cela donne en sortie $V_b \otimes V_{x^j \pmod{N}}$, pour une probabilité égale au carré du coefficient de ce vecteur dans l'équation précédente. Comme beaucoup de valeurs de $x^a \pmod{N}$ sont égales, de nombreux termes dans cette somme contribuent à chaque coefficient. Explicitement, cette probabilité est égale à :

$$\frac{1}{2^{4L}} \left| \sum_{\substack{a \equiv j \pmod{r} \\ 1 < a < 2^{2L}}} \sum_{b=0}^{2^{2L}-1} \exp(2i\pi ab/2^{2L}) \right|^2.$$

Cette somme géométrique est très petite sauf quand il existe un entier d tel que $rb \sim d2^{2L}$. Par conséquent, on a des grandes chances d'observer seulement les valeurs de b telles que

$$\frac{b}{2^{2L}} \sim \frac{d}{r}.$$

Connaissant b et 2^{2L} , on veut trouver r . Comme $2L$ est la taille du premier registre, $\frac{d}{r}$ est vraisemblablement la fraction la plus proche de $\frac{b}{2^{2L}}$ avec dénominateur $\leq N$. Par conséquent, pour trouver r , il faut approcher $\frac{b}{2^{2L}}$ par une fraction à dénominateur $\leq N$, ce qui est réalisable en temps polynômial avec l'algorithme des fractions continues.

Actuellement (voir [16]), $3L + o(L)$ qubits sont nécessaires pour la mise en œuvre de cet algorithme, qui est d'ailleurs parallélisable.

Autres résultats

Les idées de Shor (voir [12]) permettent également de résoudre le problème du logarithme discret en temps polynômial. Dans sa version la plus courante, ce problème s'exprime de la manière suivante : soit $p > 2$ un nombre premier et g un générateur du groupe multiplicatif cyclique \mathbf{F}_p^* . Le logarithme discret d'un élément $x \in \mathbf{F}_p^*$ est l'entier $0 \leq r < p - 1$ tel que $g^r \equiv x \pmod{p}$. L'algorithme classique de résolution de ce problème est l'adaptation du NSF décrit dans [7], dont la complexité est de $\exp(O((\text{Log}p)^{1/3}(\text{LogLog}p)^{2/3}))$. Dans [12], Shor montre comment résoudre ce problème sur un ordinateur quantique avec deux exponentiations modulaires et deux transformations de Fourier quantiques. Shor est également en mesure de résoudre en temps polynômial le problème du log discret formulé pour les variétés abéliennes sur un corps fini ([14]).

Codes correcteurs d'erreurs quantiques

Les premières réactions à ces algorithmes ont été pessimistes : en effet, ces algorithmes n'ont d'utilité que si on peut réduire la décohérence et les erreurs à des niveaux très faibles. En fait, sans corrections d'erreurs, il serait impossible en pratique de construire des ordinateurs quantiques assez puissants pour, par exemple, factoriser des nombres de 100 chiffres : en gros, une telle tâche nécessite des milliards d'étapes et la précision de chacune devrait donc être juste à des milliards de chiffres après la virgule près. Cependant, il est possible de faire le schéma de circuits quantiques tolérant des erreurs, ce qui, en théorie, permet d'effectuer des calculs de taille arbitraire, mais à l'aide de portes logiques « justes à seulement une constante près » (à l'heure actuelle, cette constante est 10^{-4} , voir [10]). Ceci étant, il y a loin de la coupe aux lèvres ; un argument contre l'existence de codes correcteurs d'erreurs quantiques est basé sur le théorème suivant, lié au principe d'incertitude d'Heisenberg : un état quantique inconnu ne peut pas être dupliqué. Par conséquent, si on ne peut pas dupliquer l'information quantique, on ne peut pas avoir plus qu'une copie d'un qubit à chaque instant et donc il serait impossible de protéger les qubits des erreurs ! En effet, déjà le plus simple des codes correcteurs d'erreurs classiques est le code à trois répétitions, qui utilise trois copies de chaque bit : est-ce la fin de l'aventure ? Eh bien non ! Des codes correcteurs d'erreurs quantiques existent (voir [3] et [15]), dont le plus simple est une variante quantique du

code 7-bit de Hamming. Ces codes, appelés CSS du nom de leurs auteurs ([3], [15]), protègent les informations quantiques des erreurs et de la décohérence, non pas en les dupliquant, mais en les cachant dans des sous-espaces de \mathbf{C}^{2^n} , qui, eux, sont très peu affectés par la décohérence et les erreurs.

Conclusion

Shor a prouvé qu'un ordinateur quantique pouvait factoriser des grands nombres premiers ou résoudre le problème du log discret en temps polynomial. Par rapport aux algorithmes connus jusqu'alors, c'est un progrès quasi-exponentiel! Si les différents problèmes pratiques liés à la décohérence et aux erreurs sont un jour résolus et permettent de construire des ordinateurs quantiques, ces algorithmes auront un impact planétaire révolutionnaire immédiat en ce qui concerne les communications sécurisées. En effet, c'est précisément sur la difficulté à résoudre ces problèmes que sont basés tous les algorithmes de cryptographie à clef publique (voir [9] pour un résumé des activités actuelles de standardisation). Donc, au delà de l'intérêt scientifique, on imagine aisément les conséquences politiques, diplomatiques et financières des travaux de Shor. Peter W. Shor est un mathématicien particulièrement fécond et dont les idées très variées peuvent un jour révolutionner la façon dont nous vivons l'informatique et la cryptographie au quotidien.

Bibliographie

- [1] A. BARENCO, C. H. BENNETT, R. CLEVE, D. P. DI VINCENZO, N. MARGOLUS, P. W. SHOR, T. SLEATOR, J. A. SMOLIN, H. WEINFURTER : Elementary gates for quantum computation, *Phys. Rev. A* **52**, p. 3457-3467 (1995)
- [2] A. R. CALDERBANK, E. M. RAINS, P. W. SHOR, N. J. A. SLOANE : Quantum error correction via codes over GF(4), *IEEE Transactions on Information Theory* **44**, p. 1369-1387 (1998)
- [3] A. R. CALDERBANK, P. W. SHOR : Good quantum error-correcting codes exist, *Phys. Rev. A* **54**, p. 1098-1106 (1995)
- [4] J. I. CIRIAC, P. ZOLLER : Quantum computations with cold trapped ions, *Phys. Rev. Lett.* **74**, p. 4091-4094 (1995)
- [5] D. G. CORY, A. F. FAHMY, T. F. HAVEL : Ensemble quantum computing by nuclear magnetic resonance spectroscopy, *Proc. Nat. Acad. Sci.* **94**, p. 1634-1639 (1997)
- [6] N. A. GERSHENFELD, I. L. CHUANG : Bulk spin resonance quantum computation, *Science* **275**, p. 350-356 (1997)
- [7] D. M. GORDON : Discrete logarithms in GF(p) using the number field sieve, *SIAM J. Discrete Math.*, **6**, p. 124-139 (1993)
- [8] B. E. KANE : A silicon-based nuclear spin quantum computer, *Nature* **393**, p. 133-137 (1998)
- [9] F. LEPRÉVOST : Les standards cryptographiques du XXI-ème siècle : AES et IEEE-P1363, à paraître à la *Gazette des Mathématiciens*
- [10] J. PRESKILL : Fault-tolerant quantum computation, à paraître dans *Introduction to quantum computation*, H.-K. Lo, S. Popescu and T. P. Spiller, eds (1998), LANL e-print quant-ph/9712048 (1997), accessible online via <http://xxx.lanl.gov/>
- [11] P. W. SHOR : <http://www.research.att.com/~shor/>
- [12] P. W. SHOR : Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Journal of Computing* **26**, p. 1484-1509 (1997)
- [13] P. W. SHOR : Quantum Computing, *Proceedings of the International Congress of Mathematicians*, Berlin, Documenta Mathematica, Journal der Deutschen Mathematiker-Vereinigung (1998)

- [14] P. W. SHOR : Communication personnelle (1998)
- [15] A. STEANE : Multiple particle interference and quantum error correction, Proc. Roy. Soc. London Ser. **A 452**, p. 2551-2577 (1996)
- [16] C. ZALKA : Fast versions of Shor's quantum factoring algorithm, LANL e-print quant-ph/9806084 (1998), accessible online via <http://xxx.lanl.gov/>