Probabiliste ou quantique ? (Denise Vella-Chemla, 17.2.2019)

On revient sur les règles de combinaisons de lettres qu'on avait mis au jour en février 2014 pour les étudier en termes probabilistes ou quantiques.

On avait pris l'habitude de coder les passages du mot associé à n au mot associé à $n+2$ avec des lettres a, b, c, d mais elles n'étaient pas très parlantes, on va plutôt utiliser ici la lettre p pour premier et la lettre c pour composé.

On a 16 règles qui lient les décompositions $n = x + y$, $n = (x + 2) + (y - 2)$ et $n + 2 = (x + 2) + y$ selon le caractère premier (p) ou composé (c) des quatre nombres $x, y, x + 2$ et $y - 2$. On note ces 16 règles par des transitions d'états codées ainsi : $état_x, état_y, état_{x+2}, état_{y-2} \longrightarrow$état$_{x+2}, état_y$.

$r_1)\ \ p,p,p,p \longrightarrow p,p$	$r_5)\ \ c,p,p,p \longrightarrow p,p$	$r_9)\ \ p,c,p,p \longrightarrow p,c$	$r_{13})\ \ c,c,p,p \longrightarrow p,c$
$r_2)\ \ p,p,c,p \longrightarrow c,p$	$r_6)\ \ c,p,c,p \longrightarrow c,p$	$r_{10})\ \ p,c,c,p \longrightarrow c,c$	$r_{14})\ \ c,c,c,p \longrightarrow c,c$
$r_3)\ \ p,p,p,c \longrightarrow p,p$	$r_7)\ \ c,p,p,c \longrightarrow p,p$	$r_{11})\ \ p,c,p,c \longrightarrow p,c$	$r_{15})\ \ c,c,p,c \longrightarrow p,c$
$r_4)\ \ p,p,c,c \longrightarrow c,p$	$r_8)\ \ c,p,c,c \longrightarrow c,p$	$r_{12})\ \ p,c,c,c \longrightarrow c,c$	$r_{16})\ \ c,c,c,c \longrightarrow c,c$

Prenons un exemple pour fixer les idées : la règle r_{10}, appliquée aux nombres $13, 25, 15, 23$, qui décomposent $n = 38$ qui sont bien (dans l'ordre) p, c, c, p (premier, composé, composé, premier) permettront d'obtenir la décomposition c, c de $n + 2 = 40 = 15 + 25$.

Considérons que les probabilités de $x, y, x+2, y-2$ sont complètement indépendantes les unes des autres ; on aura alors les probabilités suivantes, associées aux règles :

r_1	p,p,p,p	$\left(\frac{1}{ln\ x}\right)^4$	X^4	r_5	c,p,p,p	$\left(\frac{1}{ln\ x}\right)^3\left(1-\frac{1}{ln\ x}\right)$	$X^3(1-X)$
r_2	p,p,c,p	$\left(\frac{1}{ln\ x}\right)^3\left(1-\frac{1}{ln\ x}\right)$	$X^3(1-X)$	r_6	c,p,c,p	$\left(\frac{1}{ln\ x}\right)^2\left(1-\frac{1}{ln\ x}\right)^2$	$X^2(1-X)^2$
r_3	p,p,p,c	$\left(\frac{1}{ln\ x}\right)^3\left(1-\frac{1}{ln\ x}\right)$	$X^3(1-X)$	r_7	c,p,p,c	$\left(\frac{1}{ln\ x}\right)^2\left(1-\frac{1}{ln\ x}\right)^2$	$X^2(1-X)^2$
r_4	p,p,c,c	$\left(\frac{1}{ln\ x}\right)^2\left(1-\frac{1}{ln\ x}\right)^2$	$X^2(1-X)^2$	r_8	c,p,c,c	$\left(\frac{1}{ln\ x}\right)\left(1-\frac{1}{ln\ x}\right)^3$	$X(1-X)^3$
r_9	p,c,p,p	$\left(\frac{1}{ln\ x}\right)^3\left(1-\frac{1}{ln\ x}\right)$	$X^3(1-X)$	r_{13}	c,c,p,p	$\left(\frac{1}{ln\ x}\right)^2\left(1-\frac{1}{ln\ x}\right)^2$	$X^2(1-X)^2$
r_{10}	p,c,c,p	$\left(\frac{1}{ln\ x}\right)^2\left(1-\frac{1}{ln\ x}\right)^2$	$X^2(1-X)^2$	r_{14}	c,c,c,p	$\left(\frac{1}{ln\ x}\right)\left(1-\frac{1}{ln\ x}\right)^3$	$X(1-X)^3$
r_{11}	p,c,p,c	$\left(\frac{1}{ln\ x}\right)^2\left(1-\frac{1}{ln\ x}\right)^2$	$X^2(1-X)^2$	r_{15}	c,c,p,c	$\left(\frac{1}{ln\ x}\right)\left(1-\frac{1}{ln\ x}\right)^3$	$X(1-X)^3$
r_{12}	p,c,c,c	$\left(\frac{1}{ln\ x}\right)\left(1-\frac{1}{ln\ x}\right)^3$	$X(1-X)^3$	r_{16}	c,c,c,c	$\left(1-\frac{1}{ln\ x}\right)^4$	$(1-X)^4$

On obtient comme somme totale des probabilités le polynôme $X^4 + 4X^3(1-X) + 6X^2(1-X)^2 + 4X(1-X)^3 + (1-X)^4$ qui développé vaut bien 1.

Si on raisonne maintenant quantiquement plutôt que probabilistiquement, on aura les probabilités suivantes, présentées selon le tableau utilisé dans la littérature pour faire la différence entre bit, pbit (ou bit probabiliste) et enfin qubit (ou bit quantique).

variable décrivant l'état	*bit*	*bit probabiliste*	*bit quantique*
type	*bit*	*pbit*	*qubit*
représentation	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}p\\1-p\end{pmatrix}$	$\begin{pmatrix}\alpha\\\beta\end{pmatrix}$
caractéristique del'observation	*certitude sur la valeur* à *prendre*	p% *de chances de valoir* 0 $(1-p)$% *de chances de valoir* 1 $p \in \mathbb{R}$	$\lvert\alpha\rvert^2$% *de chances de valoir* 0 $\lvert\beta\rvert^2$% *de chances de valoir* 1 $\alpha, \beta \in \mathbb{C}$
matrice de transition	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$	$\begin{pmatrix}1-q&q\\r&1-r\end{pmatrix}$	$\begin{pmatrix}u&v\\w&x\end{pmatrix}$
type de la matrice	*déterministe*	*stochastique*	*unitaire*

Concernant la matrice stochastique de la modélisation probabiliste par des pbits (colonne au milieu du tableau), il y a 2 états et 2 transitions possibles pour chaque état et la somme des nombres sur chacune des deux lignes de la matrice vaut 1 (cela correspond aux probabilités de transition de l'un des 2 états vers lui-même ou bien vers l'autre). Imaginons quelles peuvent être les valeurs des éléments d'une matrice stochastique (probabiliste) pour la divisibilité par p : on a les 2 états possibles d'un nombre "être divisible par p" et "ne pas être divisible par p". La matrice prend la forme suivante :

$$\begin{pmatrix} 0 & 1 \\ \frac{1}{p-1} & \frac{p-2}{p-1} \end{pmatrix}$$

En effet, prenons la divisibilité par 5 des nombres de 10 à 15 : après un nombre divisible par 5 (comme 10) il y a forcément un nombre non divisible par 5 (comme 11), d'où le 0 et le 1 de la première ligne de la matrice correspondant aux 2 transitions à partir d'un nombre divisible par 5.

Pour la deuxième ligne, on part d'un nombre non-divisible par 5, comme 11, 12, 13 et 14. Parmi eux, au nombre de 4 (soit $p-1$), l'un fournit une transition vers un nombre divisible par 5 (ici 14 qui devient 15) et les 3 autres (soit $p-2$) fournissent une transition vers un nombre non-divisible par 5 ; on a expliqué les nombres de la deuxième ligne de la matrice stochastique, dont la somme vaut bien 1.

Concernant la modélisation quantique par qubits (dernière colonne du tableau) des nombres premiers, il faut alors imaginer les nombres premiers comme "polarisant" les autres nombres, dans le sens où, selon chaque nombre premier, tout autre nombre a une certaine probabilité qui varie de façon continue sur l'intervalle $[0,1]$ d'être "touché", "affecté" [1] par lui en quelque sorte, et non plus d'être divisible par lui : même si la divisibilité est une notion tout ce qu'il y a de plus binaire (un nombre étant soit divisible soit non divisible par un autre), cette notion de polarisation modéliserait le fait qu'un nombre est à une certaine distance d'être divisible ou pas par un autre. C'est la réduction du paquet d'onde qui fixe les valeurs de divisibilité d'un nombre donné par les autres. Cette notion peut permettre d'intriquer les divisibilités de x et $n-x$ par p si on connaît la divisibilité de n par p.

Comme la matrice, dans le cas quantique, doit être unitaire, il semblerait que ses éléments doivent prendre les valeurs $\frac{1}{\sqrt{p-1}}$ et $\sqrt{\frac{p-2}{p-1}}$ pour qu'on ait bien $\left(\frac{1}{\sqrt{p-1}}\right)^2 + \left(\sqrt{\frac{p-2}{p-1}}\right)^2 = \frac{1}{p-1} + \frac{p-2}{p-1} = 1$.

On s'est appuyé pour nos propositions sur l'exemple d'un fichier de Philippe Grangier [2] des personnes "plus ou moins blondes" ; on noterait notre "divisibilité polarisée" par les superpositions linéaires d'états $|0_p\rangle \left(\frac{1}{\sqrt{p-1}}\right) + |1_p\rangle \left(\sqrt{\frac{p-2}{p-1}}\right)$ par la superposition d'état $(|0_p\rangle + |1_p\rangle)/\sqrt{p-1}$.

On n'a cependant pas les moyens de mettre en oeuvre ce dispositif d'une quelconque manière.

1. comme un filtre polarisant affecte la lumière.

2. consultable ici http://www.cmls.polytechnique.fr/perso/paul/SoireesPoincare/transgrangier.pdf, transparents d'une conférence "De la sphère de Poincaré aux bits quantiques : le contrôle de la polarisation de la lumière" de Philippe Grangier (soirée Poincaré du 16 octobre 2012)