L'ALGORITHME DE GROVER.

Dans ce chapitre nous étudions un algorithme entièrement différent des précédents, qui s'applique à des objets sans structure ou sans symmétrie (il n'y a pas de sous groupe caché, pas de période ect...). Il s'agit d'un algorithme avec oracle qui effectue la recherche d'un "élément marqué" dans un "ensemble sans structure", ou d'une "base de donnée sans structure". Donnons un exemple concret.

Prenons un annuaire (la base de donnée) et supposons que les numéros de téléphone jouent le rôle des entrées, les personnes correspondantes jouent le rôle des sorties. Etant donné une entrée (le numéro de téléphone) il est difficile de retrouver la sortie (le nom de la personne correspondante). La seule façon de procéder est de faire une recherche exhaustive ou bien de procéder à une recherche aléatoire. On montre facilement que ces deux méthodes requièrent de soumettre $O(N)$ questions à l'annuaire où N est le nombre d'entrées.

Donc si $N = 2^m$, c.-à-d que l'on peut décrire tout l'annuaire avec $O(m)$ bits le temps de recherche est exponentiel $O(2^m)$. La raison fondamentale étant que la liste des numéros de téléphone n'est pas ordonnée et ne possède aucunne structure. Bien sur le problème consistant à rechercher le téléphone d'une personne connaissant son nom est facile car la liste des personne est ordonnée par ordre alphabétique.

Nous venons que l'algorithme de Grover permet de résoudre le problème en un temps $O(\sqrt{N})$. Le temps est toujours exponentiel mais (pour N assez grand) au moins nous obtenons, grâce au calcul quantique, une accélération quadratique. Il est possible de montrer que si le problème n'a pas une structure spéciale sous-jacente, il n'est pas possible de faire mieux que $O(\sqrt{N})$ dans le cadre du modèle de Deutsch (circuits quantiques).

Pour illustrer ce dernier point reconsidérons le

problème de la factorisation d'un entier $N = p \cdot q$ avec deux facteurs premiers. Il n'est pas possible d'avoir p et q supérieurs à $\sqrt{N}$, donc l'un des deux est $\leq \sqrt{N}$. En cherchant à travers la liste $\{1, 2, \ldots, \sqrt{N}\}$ nous trouverons surement un des deux facteurs premiers. Avec une recherche exhaustive il faut un temps $\sqrt{N}$, mais avec l'algorithme de Grover (ici l'oracle serait une boîte noire testant la division de N par $x \in \{1, 2 \ldots, \sqrt{N}\}$) il faut un temps $O(N^{1/4})$ ce qui est déjà intéressant. Nous savons qu'il est possible de faire mieux (même classiquement) et d'obtenir une accélération exponentielle grâce à l'algorithme de Shor, mais cela est possible en exploitant la symmétrie (la périodicité) d'une fonction arithmétique reliée au problème de la factorisation.

1. Formulation Mathématique du Problème.

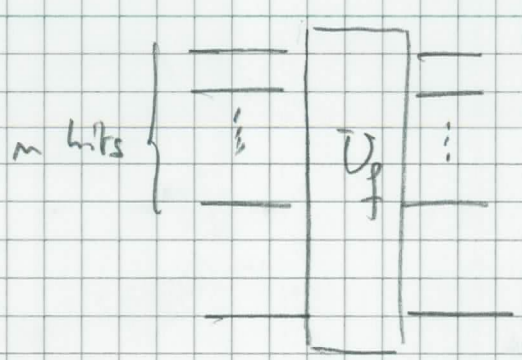
Soit $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2 = \{0, 1\}$ et soit l'équation

$$f(x_1, \ldots, x_n) = 1$$

Nous voulons déterminer parmi les 2^n entrées possibles pour $f(\cdot)$, au moins une solution $\bar{x}_1 \ldots \bar{x}_n$. Nous ne voulons pas déterminer toutes les solutions possibles mais simplement au moins une. L'application typique qui nous interesse est celle où il y a une solution unique.

Comme nous le verrons dans l'algorithme de base il faut connaître à priori le nombre total de solutions, mais cette restriction peut ensuite être supprimée grâce à une extension facile.

Nous supposons avoir à disposition un oracle quantique



$$U_f |x\rangle \otimes |b\rangle = |x\rangle \otimes |b \oplus f(x)\rangle$$

$x \in \mathbb{F}_2^n$ et $b = 0$ ou 1.

Le lecteur considérera la généralité du problème formulé ci-dessus.

2. Dérivation de l'algorithme.

Dans les chapitres précédents nous avons toujours commencé par donner le circuit de l'algorithme. Cette fois nous procédons de façon plus inductive et verrons que l'algorithme de Grover peut être construit de façon assez naturelle.

L'état initial entrant dans le circuit est :

$$\underbrace{|0 \ldots 0\rangle}_{n \text{ fois}} \otimes |1\rangle$$

où les n premiers qubits stockent les entrées et le dernier bit est un bit auxiliaire. Pour exploiter le parallélisme quantique nous formons une superposition cohérente sur toutes les entrées possibles grâce aux portes de Hadamard agissant sur tous les qubits du premier registre :

$$(H \otimes \dots \otimes H) \otimes \mathbb{1} \; |0 \dots 0\rangle \otimes |1\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} |x\rangle \otimes |1\rangle$$

L'opération de Hadamard sur le second registre se réécrit sous la forme ci-dessous (pour obtenir le phénomène "kick-back phase")

L'état devient alors :

$$\frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) .$$

Appliquons maintenant U_f. L'état devient

$$\frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} |x\rangle \otimes \frac{1}{\sqrt{2}}(|f(x)\rangle - |\overline{f(x)}\rangle) .$$

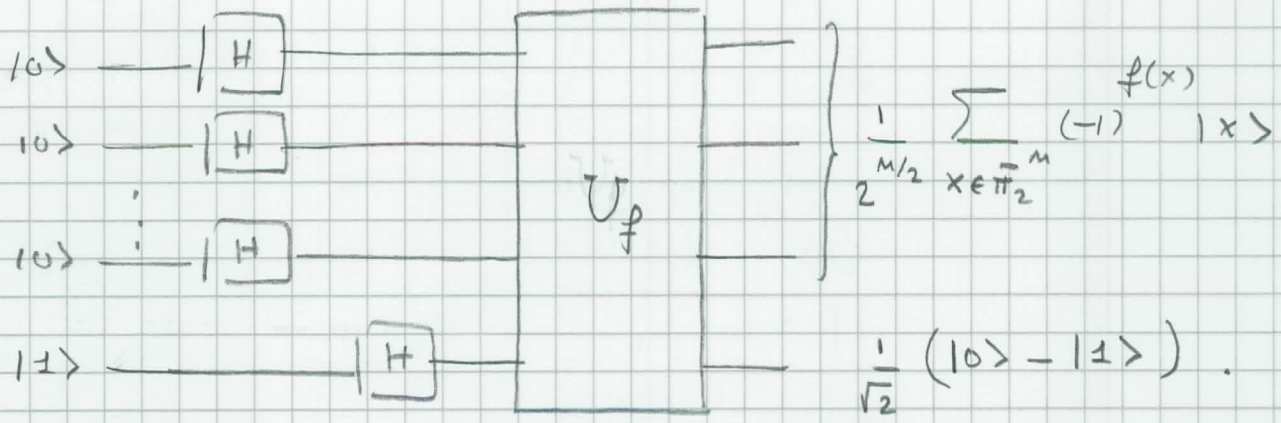
On note que

$$|f(x)\rangle - |\overline{f(x)}\rangle = (-1)^{f(x)} (|0\rangle - |1\rangle) .$$

ce qui donne l'état

$$\frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) .$$

Les opérations ci-dessus sont résumées dans la figure



Dans l'état résultant nous voyons que la solution de l'équation $f(x) = 1$ a été "marquée" d'une phase égale à -1 (ou π).

Supposons que le nombre de solutions est M et définissons deux états quantiques

$|S\rangle =$

$$|S\rangle = \frac{1}{\sqrt{M}} \sum_{x\text{-sol}} |x\rangle$$

$$|I\rangle = \frac{1}{\sqrt{N-M}} \sum_{x\text{-pas sol}} |x\rangle .$$

On peut alors voir que :

$$\frac{1}{\sqrt{N}} \sum_{x} |x\rangle = \sqrt{\frac{M}{N}}\, |S\rangle + \sqrt{\frac{N-M}{N}}\, |I\rangle$$

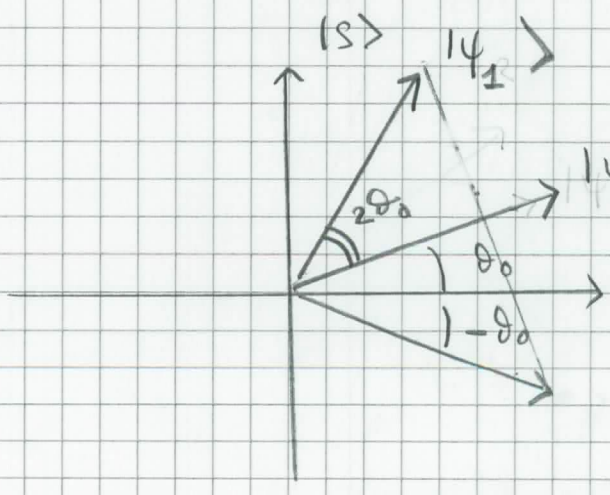
$$\frac{1}{\sqrt{N}} \sum_x (-1)^{f(x)} |x\rangle = -\sqrt{\frac{M}{N}}\,|S\rangle + \sqrt{\frac{N-M}{N}}\,|\Gamma\rangle$$

Puisque $\sqrt{\frac{M}{N}}$ et $\sqrt{\frac{N-M}{N}}$ sont ≤ 1 et $\left(\sqrt{\frac{M}{N}}\right)^2 + \left(\sqrt{\frac{N-M}{N}}\right)^2 = 1$

on peut définir un angle ϑ_0 tel que

$$\sin\vartheta_0 = \sqrt{\frac{M}{N}} \quad \text{et} \quad \cos\vartheta_0 = \sqrt{\frac{N-M}{N}}\,.$$

Nous avons maintenant une interprétation géométrique du circuit ci-dessus. L'entrée du premier registre est un vecteur dans le plan $\{|\Gamma\rangle, |S\rangle\}$ formant un angle ϑ_0 avec l'axe $|\Gamma\rangle$. La sortie est le vecteur obtenu par réflexion par rapport à $|\Gamma\rangle$ et formant l'angle $-\vartheta_0$ avec ce dernier. (Voir figure).



L'état réfléchi contient les solutions marquées par une phase -1. Nous devons maintenant analyser cet état de façon à déterminer l'axe $|S\rangle$ ou en d'autre terme le sous-espace des solutions. Une idée naturelle est de faire une réflection par le rapport à $|\psi\rangle$, ce qui nous amène sur $|\psi_1\rangle$ (voir figure). On notera deux points importants :

- En obtenant $|\psi_1\rangle$ on s'est rapproché de $|S\rangle$ (au moins si ϑ_0 était faible au départ, donc $M \ll N$).
- La réflection est faite par rapport à $|\psi_0\rangle$ et n'utilise aucune information sur les solutions (inconnues).

Nous avons

$$|\psi_1\rangle = \cos 3\vartheta_0 \, |P\rangle + \sin 3\vartheta_0 \, |S\rangle.$$

Le troisième point crucial qu'il faut remarque est que

- $|\psi_1\rangle$ est une rotation d'angle $2\vartheta_0$ de $|\psi_0\rangle$ dans le plan $\{|P\rangle, |S\rangle\}$.

En itérant ce procédé — réflection autour de $|\Pi\rangle$, puis réflection autour de $|\psi_0\rangle$ — on obtient la suite d'états obtenus par rotations successives d'angle $2\theta_0$:

$$|\psi_K\rangle = \cos((2K+1)\theta_0)\,|\Pi\rangle + \sin((2K+1)\theta_0)\,|S\rangle.$$

Si θ_0 est assez petit (ce qui sera le cas en pratique car $M \ll N$) et si M est connu on peut choisir le nombre d'itérations K t.q : $(2K+1)\theta_0 \approx \frac{\pi}{2}$ pour amener l'état presque parallèle à $|S\rangle$. Une mesure donnera alors une solution avec probabilité proche de 1. Cette analyse est présentée dans le prochain paragraphe.

Revenons maintenant à l'implémentation de la réflection autour de $|\psi_0\rangle$ dans le circuit quantique. La réflection d'un vecteur $\vec{v}$ par rapport à $\vec{\psi_0}$ correspond à l'opération suivante (prouvez le avec un dessin!)

$$\vec{v} \longmapsto 2(\vec{\psi_0}^T \cdot \vec{v})\,\vec{\psi_0} - \vec{v}$$

En notation de Dirac :

$$|v\rangle \longmapsto 2|\psi_0\rangle\langle\psi_0|v\rangle - |v\rangle$$

$$= (2|\psi_0\rangle\langle\psi_0| - I)|v\rangle .$$

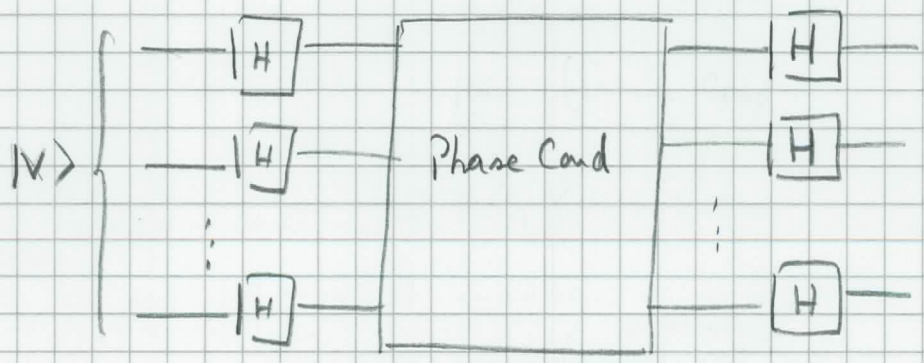
$$= H^{\otimes n}(2|0\dots0\rangle\langle 0\dots0| - I)H^{\otimes n}|v\rangle .$$

L'opérateur dans les parenthèses (une matrice égale à 2 (projecteur sur $|0\dots0\rangle$) − Identité) a pour effet de changer la phase des entrées non nulles :

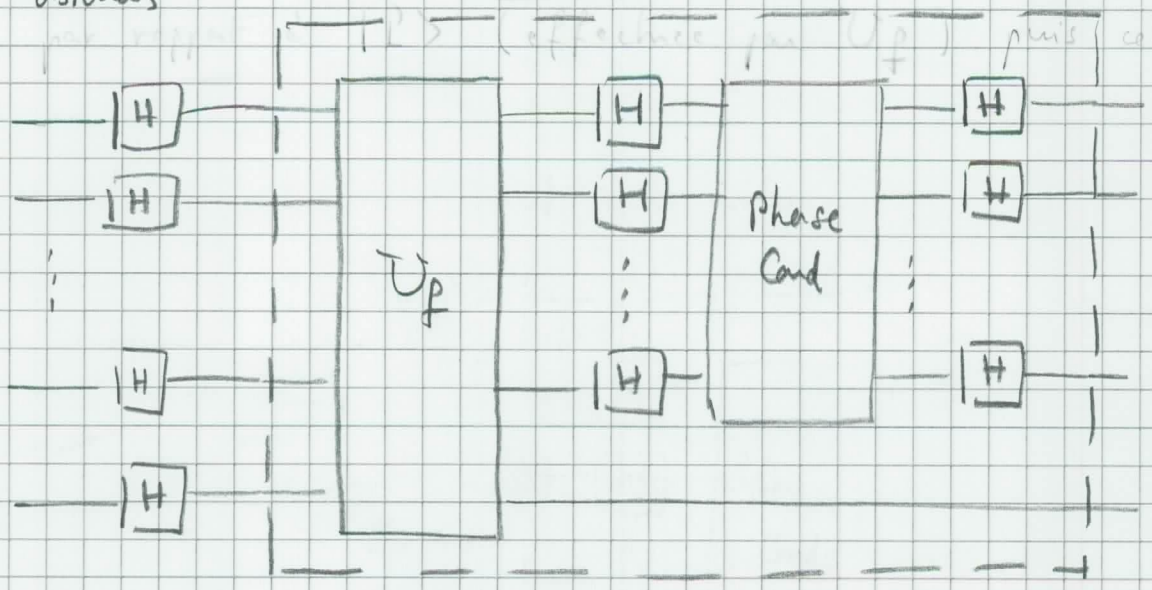
$$(2|0\dots0\rangle\langle 0\dots0| - I)|x\rangle = \begin{cases} |0\dots0\rangle & \text{si } x = (0\dots0) \\ -|x\rangle & \text{sinon} \end{cases}$$

Nous appelons cet opérateur (Phase Cond) pour (phase conditionnelle).

Le circuit implémentant la réflection par rapport à $|\psi_0\rangle$ est



En combinant ce circuit avec celui de la figure 1 nous obtenons



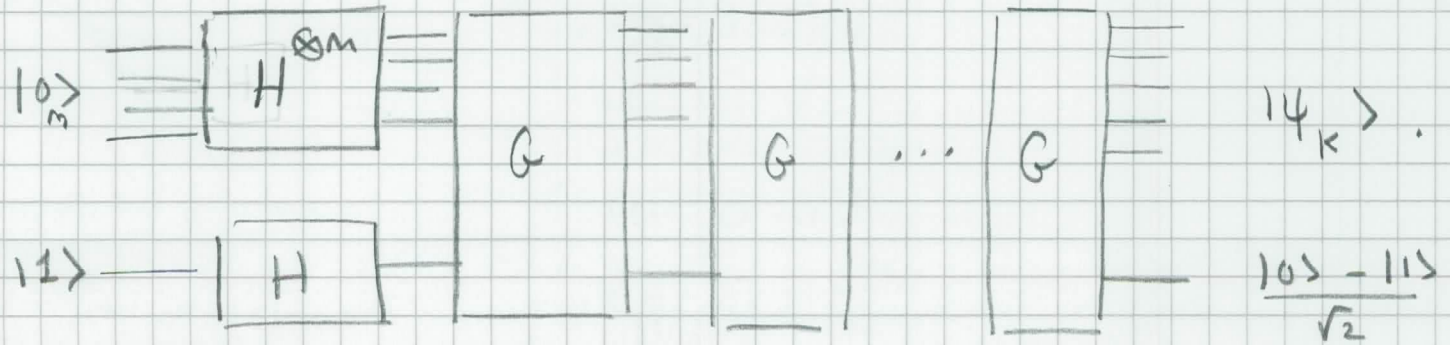
La boite encadrée représente l'"opérateur de Grover" appelé G. Son effet sur

$$\frac{1}{\sqrt{N}} \sum_x |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \left(\cos\vartheta_0 |I\rangle + \sin\vartheta_0 |S\rangle\right) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

est d'effectuer une rotation d'angle $2\vartheta_0$ dans le plan $\{|I\rangle, |S\rangle\}$. Le sorte est

$$\left(\cos 3\vartheta_0 |I\rangle + \sin 3\vartheta_0 |S\rangle\right) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

L'algorithme de Grover consiste à itérer cette opération G un certain nombre de fois. Son circuit peut être symbolisé comme suit :



La profondeur (temps de calcul) du circuit est $O(K)$ et sa largeur $n+1$.

3. Analyse Probabiliste.

Nous faisons une mesure sur les bits du premier registre dans la base computationnelle. La probabilité d'obtenir un état $|x\rangle$ qui est solution est :

$$\left(\sin(2K+1)\theta_0\right)^2 = |\langle s|\psi_k\rangle|^2 .$$

Rappelons que $\sin\theta_0 = \sqrt{\frac{M}{N}}$ et $\cos\theta_0 = \sqrt{1-\frac{M}{N}}$.

Discutons d'abord le cas facile $M = \frac{N}{4}$. Dans ce cas $\sin\theta_0 = \frac{1}{2}$ et $\cos\theta_0 = \frac{\sqrt{3}}{2}$ ce qui signifie $\theta_0 = \frac{\pi}{6}$. Au bout d'une itération ($K=1$) l'état est aligné avec $|S\rangle$ car $3\theta_0 = \frac{\pi}{2}$. Nous trouvons donc 1 solution avec probabilité égale à 1 en une mesure et l'oracle a été consulté 1 fois. Bien sûr ce cas est médiocrement intéressant car

quand il y a $\frac{N}{4}$ solutions on peut en trouver une avec probabilité $\frac{1}{4}$ en posant une question aléatoire à un oracle classique. Ensuite on peut amplifier cette probabilité à $1-\epsilon$ en répétant l'expérience $O(|\ln \epsilon|)$ fois.

Prenons maintenant le cas $M = 1$ qui est intuitivement le plus difficile. Dans ce cas $\sin\vartheta_0 = \frac{1}{\sqrt{N}}$ et donc l'angle ϑ_0 est très petit, $\vartheta_0 \simeq \frac{1}{\sqrt{N}}$. Donc

$$\sin^2(2K+1)\vartheta_0 \simeq \sin^2\left(\frac{2K+1}{\sqrt{N}}\right)$$

Pour $\frac{2K+1}{\sqrt{N}} \simeq \frac{\pi}{2}$ cette probabilité est proche de 1. C'est à dire qu'avec $K = \left[\frac{\pi}{4}\sqrt{N}\right]$ (partie entière supérieure ou inférieure, c'est égal) la probabilité de succès est proche 1. On peut voir que cette dernière est $1 - O\left(\frac{1}{N}\right)$.

Cas général avec M général connu.

- Si $M < \frac{3}{4}N$ alors $\sin\vartheta_0 < \frac{\sqrt{3}}{2} \Rightarrow \vartheta_0 < \frac{\pi}{3}$.

Itérons $\left[\frac{\pi}{4\vartheta_0}\right] = K$ fois.

$= 2$

Puisque $\left\lfloor \frac{\pi}{4\vartheta_0} \right\rfloor = \frac{\pi}{4\vartheta_0} - \frac{1}{2} + \delta$ avec $|\delta| < \frac{1}{2}$ on a :

$$(2k+1)\vartheta_0 = \frac{\pi}{2} + 2\delta\vartheta_0$$

avec $2|\delta|\vartheta_0 < 2|\delta|\frac{\pi}{3} < \frac{\pi}{3}$. Donc $(2k+1)\vartheta_0 > \frac{\pi}{2} - \frac{\pi}{3}$ et

$$\sin^2(2k+1)\vartheta_0 > \sin^2\left(\frac{\pi}{2} - \frac{\pi}{3}\right) = \sin^2\frac{\pi}{6} = \left(\frac{1}{2}\right)^2 = \frac{1}{4}.$$

La probabilité de succès est au moins $\frac{1}{4}$ et peut ensuite être amplifiée comme avant.

- Si $M > \frac{3}{4}N$ on a une probabilité de succès de $\frac{3}{4}$ grâce à une recherche classique.

Cas général avec M inconnu.

Si M est inconnu nous ne savons pas combien de fois itérer et le problème serait que nous itérions par essai au trop. L'algorithme suivant a une probabilité de succès de $1/4$ (ce qui nous suffit car celle-ci peut ensuite être amplifiée).

1) Prendre une entrée x aléatoirement uniformément.
Si $f(x) = 1 \rightarrow$ succès.

2) Si on a choisi $R \in \{0, 1, 2, \ldots, \sqrt{N} - 1\}$ uniformément aléatoirement et appliquer Grover avec R itérations. Mesurer la sortie.

Montrons que la probabilité de succès est toujours $\geq \frac{1}{4}$.

Si $M \geq \frac{3}{4} N$ le point 1 à une probabilité de succès $\frac{3}{4}$ qui est plus grand que $\frac{1}{4}$.

Si $M < \frac{3}{4} N$ et on a surement :

$$\text{Prob (succès)} \geq \text{Prob (succès au point 2)}.$$

Mais

$$\text{Prob (succès au point 2)} = \sum_{R=1}^{\sqrt{N}+1} \text{Prob (succès en 2} \mid R) \, \text{Prob}(R).$$

$$= \frac{1}{\sqrt{N}} \sum_{R=0}^{\sqrt{N}-1} \sin^2 (2R+1)\vartheta_0 = \frac{1}{2} - \frac{\sin 4\sqrt{N}\vartheta_0}{4\sqrt{N} \sin 2\vartheta_0}$$

Mais $\sin 4\sqrt{N}\,\vartheta_0 < 1$ et

$$\sin 2\vartheta_0 = 2\sin\vartheta_0 \cos\vartheta_0 = 2\sqrt{\frac{M}{N}}\sqrt{\frac{N-M}{N}} > 2\sqrt{\frac{M}{N}}\sqrt{\frac{N}{4N}} > \frac{1}{\sqrt{N}}$$

$$\Rightarrow \text{Prob (succès au point 2)} \geq \frac{1}{2} - \frac{1}{4} = \frac{1}{4}.$$