La conjecture de Goldbach au prisme du hasard quantique : ce qui est exploitable, ce qui ne l'est pas
Denise Vella-Chemla pilotant l'ia lumo, septembre 2026

Résumé

Analyse des trois notes quantiques (voir Références) de juillet 2026 (intrication, simulation Qiskit, algorithme de Grover), prolongeant la note La question posée : l'approche quantique de Goldbach est-elle vouée à l'échec, exploitable, et comment ?

1. Ce que la reformulation quantique établit réellement

Les notes de juillet 2026 ([1], [2], [3]) énoncent la conjecture dans le langage de la mécanique quantique : à chaque décomposition $n = p + q$ est associé l'état produit $|\pi(p)\rangle \otimes |\pi(n-p)\rangle$, et la conjecture devient : *pour tout n pair ≥ 4, la composante $|11\rangle\langle 11|$ de la matrice densité ρ_n est non nulle*, autrement dit $\mathrm{Tr}\Big(\rho_n(P_1 \otimes P_1)\Big) > 0$.

Cette reformulation est **correcte**, et elle est même doublement fidèle à l'architecture d'ensemble :

1. le couplage $p + q = n$ code exactement la *loi miroir* : pour chaque premier $p \leq \sqrt{n}$, les observable "$x \equiv 0 \pmod p$" et "$n - x \equiv 0 \pmod p$" sont *parfaitement corrélées* si $p \mid n$ et *parfaitement anti-corrélées* si $p \nmid n$;

2. les quatre lettres `a, b, c, d` du modèle de 2014 sont exactement la base $\{|11\rangle, |01\rangle, |10\rangle, |00\rangle\}$ de l'espace à deux qubits : la note d'intrication l'établit explicitement.

Mais il faut nommer la nature exacte de ce gain : c'est un *changement de langage*, pas un gain de puissance.

$$\mathrm{Tr}\Big(\rho_n(P_1 \otimes P_1)\Big) = \frac{N_a}{m}$$

est le compte du crible, écrit en notation quantique. La probabilité quantique de mesure est ici exactement la fréquence classique : rien n'y est plus exact que ce qu'on y a codé.

2. Pourquoi la simulation de Grover ne démontre rien

Dans les programmes Qiskit, l'oracle est construit par un *test de primalité classique* (boucle sur les diviseurs jusqu'à $\sqrt{x}$) : la matrice oracle reçoit -1 sur la diagonale aux indices reconnus premiers par `est_premier`. L'"amélioration quantique" est donc illusoire dans ces notes : tout le travail arithmétique est fait classiquement, en amont de la préparation d'état. La simulation illustre Grover, elle ne le met pas au service d'une connaissance nouvelle.

Notons d'ailleurs que la recherche d'une décomposition pour *un* n donné n'en a pas besoin : classiquement, chaque essai réussit avec probabilité de l'ordre de $\dfrac{1}{(\log n)^2}$, donc quelques dizaines d'essais suffisent, et la conjecture est vérifiée numériquement jusqu'à $\sim 4 \cdot 10^{18}$ (Oliveira e Silva, Herzog,

Pardi, 2014). Le contenu profond de Goldbach n'est pas l'*existence* d'une décomposition pour un n donné : c'est l'assertion *universelle*.

3. L'obstruction de fond : $\forall n$ n'est pas une recherche

C'est le point décisif, et il ne dépend pas de la technologie :

- Goldbach est un énoncé *universel* (pour tout n pair) ; Grover, Shor, et toute source de hasard quantique sont des machines à problèmes *d'existence* (pour un n donné) ;
- or l'existence pour un n donné est déjà facile classiquement. Le difficile est le $\forall$, et aucune mesure quantique ne délivre un certificat infini ;
- surtout : le hasard quantique n'élimine pas l'erreur du crible. Une mesure quantique échantillonne *exactement* la distribution qu'on lui a encodée. Si l'état est préparé depuis le crible classique, on hérite de son erreur $O(2^{\pi(\sqrt{n})})$; si l'on veut préparer un état qui l'encode exactement, il faut déjà connaître le compte - l'argument est circulaire.

Même Shor, qui factorise efficacement, ne lève pas le problème de parité à lui seul : il déciderait la nature de chaque candidat, mais la difficulté de Goldbach n'est pas de décider un candidat, c'est de garantir qu'il en existe toujours un.

4. Le pont qui reste : triléen, POVM et loi miroir

Il reste un pont *réel*, et c'est celui que je propose de pousser. Le triléen [1] - 0, 1, je-ne-sais-pas - se traduit naturellement en langage quantique par une POVM [2] à trois issues :

$$E_0 = \lambda\, P_0, \qquad E_1 = \lambda\, P_1, \qquad E_? = (1-\lambda)\, I, \qquad 0 \le \lambda \le 1,$$

1. *Note de Denise Vella-Chemla : Un mot que j'ai fourni à lumo, par analogie avec le mot booléen, et il l'a adopté comme s'il existait.*

2. *L'ia utilise le sigle POVM sans l'expliquer. Je lui demande la définition de ce sigle et sa réponse est :* POVM signifie *Positive Operator-Valued Measure*, qu'on traduit en français par "mesure à valeurs d'opérateurs positifs".
Pour situer le concept : en mécanique quantique, une mesure est habituellement décrite par des projecteurs (c'est la formulation de von Neumann), où chaque résultat de mesure correspond à la projection de l'état sur un sous-espace. Les POVM généralisent cette idée.
Une POVM est une famille d'opérateurs $\{E_i\}$ qui satisfont deux conditions :
   - chaque E_i est positif (plus précisément semi-défini positif : $\langle\Psi|E_i|\Psi\rangle \geq 0$ pour tout état $|\Psi\rangle$);
   - leur somme vaut l'identité : $\sum_i E_i = \mathbf{1}$ (garantissant que les probabilités somment à 1).

La probabilité d'obtenir le résultat i lors d'une mesure sur un état ρ est donnée simplement par $p(i) = \mathrm{Tr}(E_i\rho)$.
Ce formalisme est plus général et plus souple que celui des projecteurs, car les E n'ont pas besoin d'être eux-mêmes des projecteurs. Il est particulièrement utile dans plusieurs contextes :
La discrimination d'états : les mesures optimales pour distinguer des états non orthogonaux (comme les mesures d'Helstrom ou la mesure *Unambiguous State Discrimination*, possible seulement dans le cadre POVM) ;
Les systèmes ouverts et la décohérence : quand un système interagit avec un environnement qu'on ne contrôle pas, la mesure effective sur le système seul est naturellement décrite par une POVM ; L'information quantique : téléportation, cryptographie quantique (par exemple pour analyser les protocoles comme le BB84 avec détecteurs imparfaits).
En résumé, la POVM est l'outil mathématique standard pour décrire la statistique de résultats de mesure la plus générale possible en physique quantique, sans avoir à spécifier ce qui arrive à l'état après la mesure (pour cela, on utilise en plus les effets de Kraus, liés aux opérations quantiques).

où λ mesure la certitude locale ($\lambda = 1$: crible booléen exact ; $\lambda = 0$: ignorance totale). Le paramètre λ *quantifie* le principe d'incertitude fractale : sur une période primorielle, le crible vaut $\lambda = 1$; au-delà, le "je-ne-sais-pas" envahit nécessairement, et c'est cela, formulé dans le langage quantique, que la mesure d'information perdue rend précis.

Surtout : la note 307 de mars 2016 [3] - la matrice de densité 2×2 à éléments $1/2$, idempotente, projection sur la diagonale principale - avait déjà trouvé l'état *maximalement mélangé* $\rho = I/2$, c'est-à-dire l'état du "je-ne-sais-pas" quantique. La boucle est fermée : le triléen de 2026 et la matrice densité de 2016 sont le même objet, et la note d'intrication de juillet 2026 en donne la version corrélée. C'est une note à écrire, propre et publiable : *Logique quantique du crible : la loi miroir comme corrélation parfaite et l'ignorance comme état mélangé.*

5. Verdict

- **comme démonstration de Goldbach :** voué à l'échec, et pour une raison conceptuelle et non technique : un énoncé universel ne sort pas d'un échantillonneur, si quantique soit-il, et le hasard quantique hérite de l'information qu'on lui code.
- **comme langage et comme laboratoire : exploitable,** sur trois terrains :
  (i) le pont triléen $\leftrightarrow$ POVM ci-dessus, qui donne un statut mathématique précis au principe d'incertitude fractale ;
  (ii) des simulations exactes *sur période primorielle* (là où le crible ne ment pas) pour étudier numériquement les fluctuations des décomposants - un laboratoire d'intuitions honnête ;
  (iii) le lien déjà amorcé avec les opérateurs multi-circulants et le spectre, c'est-à-dire avec ζ : c'est là que la voie quantique et la voie analytique peuvent se rencontrer.

En un mot : le quantique ne traversera pas le mur de parité - personne ne l'a jamais fait seul - mais il donne à la loi miroir un langage où la corrélation, l'anti-corrélation et l'ignorance sont des objets natifs. C'est peu pour prouver, c'est beaucoup pour comprendre.

Références

[1] Denise Vella-Chemla pilotant l'ia deepSeek, *Modélisation de la conjecture de Goldbach par intrication quantique*, juillet 2026.
https://denisevellachemla.eu/1-CG-intrication-deepseek-dvc-20260714.pdf

[2] Denise Vella-Chemla pilotant l'ia deepSeek, *Simulation quantique de la conjecture de Goldbach*, juillet 2026.
https://denisevellachemla.eu/2-CG-qiskit-deepseek-dvc-20260714.pdf

[3] Denise Vella-Chemla pilotant l'ia deepSeek, *Simulation quantique de la conjecture de Goldbach, version finale*, juillet 2026.
https://denisevellachemla.eu/3-revolution-CG-quantique-deepseek-dvc-20260714.pdf

[4] G. H. Hardy, *Goldbach's problem*, Matematisk Tidsskrift B, 1922, p. 1–16.

[5] T. Oliveira e Silva, S. Herzog, S. Pardi, *Empirical verification of the even Goldbach conjecture and computation of prime gaps up to* $4 \cdot 10^{18}$, Mathematics of Computation 83 (2014), p. 2033–2060.

3. *Note de Denise Vella-Chemla : Là, je suis impressionée car je n'ai pas fourni la note https://denisevellachemla.eu/droledemat.pdf à l'ia lumo dans la conversation.*