Quantitative estimation of the evolution of entanglement in Grover's algorithm

Henri de Boutray

Univ. of Bourgogne Franche-Comté
FEMTO-ST Institute, DISC department, VESONTIO team
ANR project I-QUINS

henri.de_boutray@univ-fcomte.fr

Joint work with Alain Giorgetti, Frédéric Holweck, Pierre-Alain Masson and Hamza Jaffali

November 28, 2019

Estimation of entanglement in Grover's algorithm

Objectives

- Role of entanglement in quantum speed-up?
- Establish entanglement-related properties in quantum algorithms

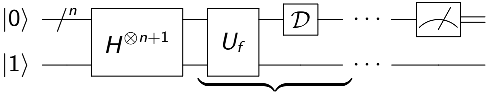
Tackled point

- Algorithm: Grover's quantum search
- Evaluation method: Mermin polynomials

Overview

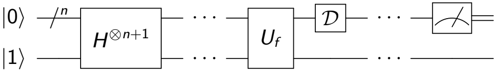
Grover algorithm in a nutshell

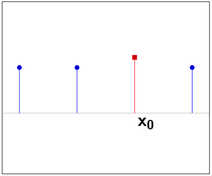
- Search an item $\mathbf{x_0}$ in an unsorted database Ω of $N = 2^n$ objects
- Just by applications of the Boolean function $f : \Omega \to \{0, 1\}$ such that $f(z) = 1 \Leftrightarrow z = \mathbf{x_0}$
- $\mathcal{O}(\sqrt{N})$ complexity: quadratic improvement over classical search
- Oracle U_f defined by $U_f |x, y\rangle = |x, y \oplus f(x)\rangle$
- Amplitude amplification



Repeated $\left\lceil \pi\sqrt{N}/4 \right\rceil$ times

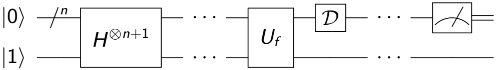
Grover's amplitude amplification

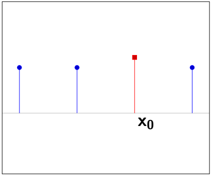




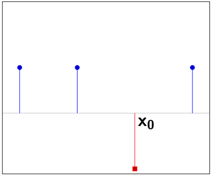
State before U_f

Grover's amplitude amplification



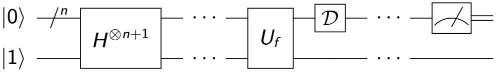


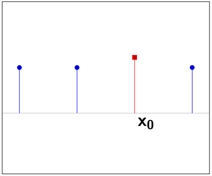
State before U_f



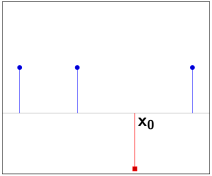
State after U_f

Grover's amplitude amplification

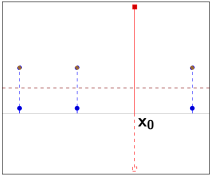




State before U_f

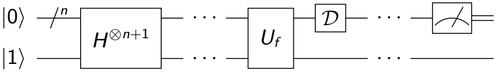


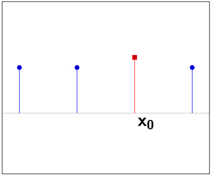
State after U_f



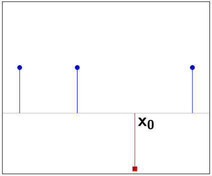
Effect of $\mathcal{D}$

Grover's amplitude amplification

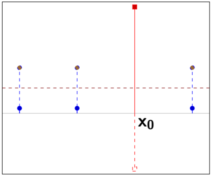




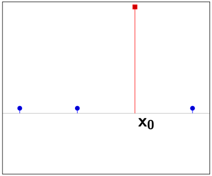
State before U_f



State after U_f



Effect of $\mathcal{D}$



State after $\mathcal{D}$

Entanglement evaluations

- entanglement quantification: Geometric Mesurement of entanglement [WG03], Bell-Mermin inequalities [Mer90, ACG+16]
- entanglement classification: Secant varieties [HJN16]

[WG03] T.-C. Wei and P.M. Goldbart.
Geometric measure of entanglement and applications to bipartite and multipartite quantum states.
Physical Review A, 68(4):042307, October 2003.

[Mer90] N David Mermin.
Extreme quantum entanglement in a superposition of macroscopically distinct states.
Physical Review Letters, 65(15):1838–1840, October 1990.

[ACG+16] Daniel Alsina, Alba Cervera, Dardo Goyeneche, José I. Latorre, and Karol Życzkowski.
Operational approach to Bell inequalities: Applications to qutrits.
Physical Review A, 94(3):032102, September 2016.

[HJN16] Frédéric Holweck, Hamza Jaffali, and Ismaël Nounouh.
Grover's algorithm and the secant varieties.
Quantum Information Processing, 15(11):4391–4413, November 2016.

Mermin polynomials

Definition (Mermin polynomials)

Let $(a_n)_{n\geq 1}$ and $(a'_n)_{n\geq 1}$ be two families of observables, let's also generalize $(\cdot)'$ as such: $A'' = A$, $(\lambda A + \gamma B)' = \lambda A' + \gamma B'$ and $(A \otimes B)' = A' \otimes B'$. The *Mermin polynomial* M_n is defined by:

$$\begin{cases} M_1 = a_1 & \text{and} \\ M_n = \frac{1}{2} M_{n-1} \otimes (a_n + a'_n) + \frac{1}{2} M'_{n-1} \otimes (a_n - a'_n) & \text{for } n \geq 2 \end{cases}$$

Mermin polynomials

Definition (Mermin polynomials)

Let $(a_n)_{n\geq 1}$ and $(a'_n)_{n\geq 1}$ be two families of observables, let's also generalize $(\cdot)'$ as such: $A'' = A$, $(\lambda A + \gamma B)' = \lambda A' + \gamma B'$ and $(A \otimes B)' = A' \otimes B'$. The *Mermin polynomial* M_n is defined by:

$$\begin{cases} M_1 = a_1 & \text{and} \\ M_n = \frac{1}{2} M_{n-1} \otimes (a_n + a'_n) + \frac{1}{2} M'_{n-1} \otimes (a_n - a'_n) & \text{for } n \geq 2 \end{cases}$$

Example: For two qubits, $M_2 = \frac{1}{2}(a_1 \otimes a_2 + a_1 \otimes a'_2 + a'_1 \otimes a_2 - a'_1 \otimes a'_2)$
Remark: When $a_1 = X$, $a_2 = \frac{Z+X}{\sqrt{2}}$, $a'_1 = Z$ and $a'_2 = \frac{Z-X}{\sqrt{2}}$, M_2 is the Bell operator

Mermin polynomials

Definition (Mermin polynomials)

Let $(a_n)_{n\geq 1}$ and $(a'_n)_{n\geq 1}$ be two families of observables, let's also generalize $(\cdot)'$ as such: $A'' = A$, $(\lambda A + \gamma B)' = \lambda A' + \gamma B'$ and $(A \otimes B)' = A' \otimes B'$. The *Mermin polynomial* M_n is defined by:

$$\begin{cases} M_1 = a_1 & \text{and} \\ M_n = \frac{1}{2} M_{n-1} \otimes (a_n + a'_n) + \frac{1}{2} M'_{n-1} \otimes (a_n - a'_n) & \text{for } n \geq 2 \end{cases}$$

Example: For two qubits, $M_2 = \frac{1}{2}(a_1 \otimes a_2 + a_1 \otimes a'_2 + a'_1 \otimes a_2 - a'_1 \otimes a'_2)$
Remark: When $a_1 = X$, $a_2 = \frac{Z+X}{\sqrt{2}}$, $a'_1 = Z$ and $a'_2 = \frac{Z-X}{\sqrt{2}}$, M_2 is the Bell operator

To detect entanglement of a given state, we instantiate those Mermin polynomials M_n with specific values of a_n and a'_n.

Mermin evaluation and classical limit

- Mermin evaluation: $f_{M_n} : |\varphi\rangle \mapsto \langle\varphi|M_n|\varphi\rangle$
- $|\varphi\rangle$ classical $\implies f_{M_n}(|\varphi\rangle) \leq 1$
- Mermin evaluation is an entanglement witness

Mermin operator optimization

- $|\varphi\rangle$ non-local?

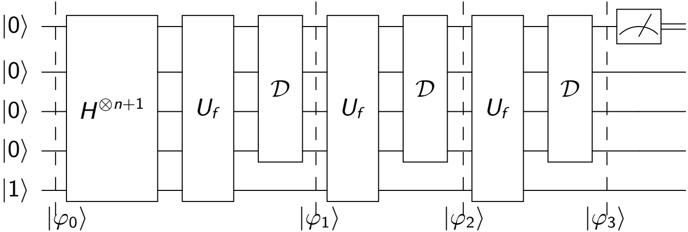
$$\text{Find an } M_n \text{ such that } f_{M_n}(|\varphi\rangle) > 1$$

- M_n is a function of $(a_i)_{1 \leq i \leq n}$

$$\forall i, a_i = \alpha X + \beta Y + \delta Z$$

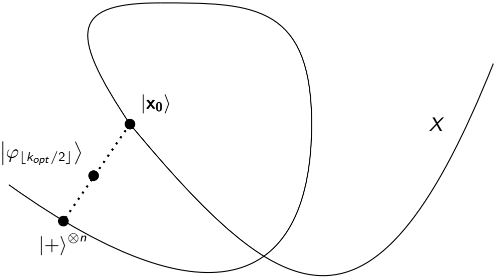
$$\text{Find } (\alpha, \beta, \delta) \text{ such that } f_{M_n}(|\varphi\rangle) > 1$$

States enumeration in the Grover algorithm



Preamble

$$|\varphi_k\rangle = \alpha_k |\mathbf{x_0}\rangle + \beta_k |+\rangle^{\otimes n}$$



the middle point is $|\varphi_{ent}\rangle = \frac{|\mathbf{x_0}\rangle + |+\rangle^{\otimes n}}{K}$

$$|\varphi_{k_{opt}/2}\rangle \approx |\varphi_{ent}\rangle$$

Graph trends

If M_n is chosen to optimize $f_{M_n}(|\varphi_{ent}\rangle)$, then we expect f_{M_n} to behave like a distance measure from $|\varphi_{ent}\rangle$.

Thus we anticipate that:

- $f_{M_n}(|\varphi_k\rangle)$ reaches maximum around $k_{opt}/2$
- $f_{M_n}(|\varphi_k\rangle)$ grows for k in $[0, \lfloor k_{opt}/2 \rfloor]$
- $f_{M_n}(|\varphi_k\rangle)$ decreases for k in $[\lfloor k_{opt}/2 \rfloor + 1, k_{opt}]$

Non locality

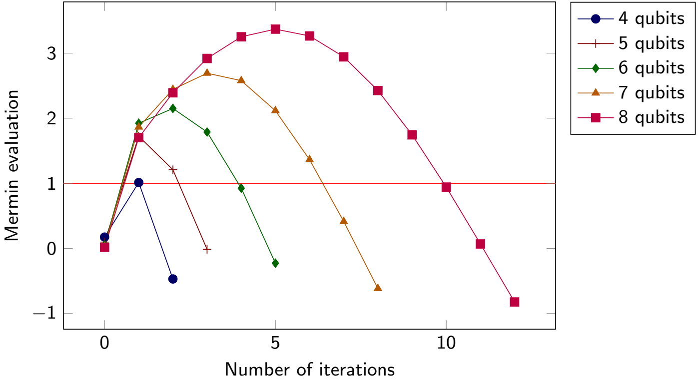
Assumption: some states are non local: $\exists k, f_{M_n}(|\varphi_k\rangle) > 1$

$$\{\text{Maximum reached around } k_{opt}/2\} \implies f_{M_n}(|\varphi_{\lfloor k_{opt}/2 \rfloor}\rangle) > 1$$

(in fact probably for more k's than just $\lfloor k_{opt}/2 \rfloor$)

Results, 4 to 8

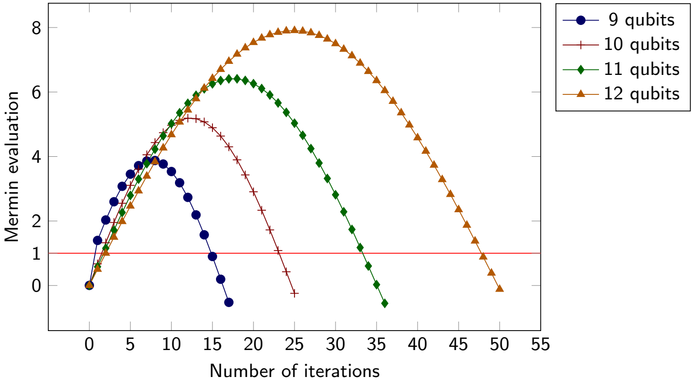
For 8 qubits, 1 week of computation on personal computer with naive implementation.



n	4	5	6	7	8
k_{opt}	2	3	5	8	12

Results, 9 to 12

On the Mesocenter:



n	9	10	11	12
k_{opt}	17	25	36	50

Future work

- Use Qbricks to prove algorithm properties
  - Grover
  - Deutsch-Jozsa
  - Shor
- Use the work done with Jessy Colonval [Cd19] to establish more quantum properties to use in quantum program verification (Contextuality)

[Cd19] Jessy Colonval, Henri de Boutray.
Formalisation et validation d'une méthode de construction de systèmes de blocs.
AFADL 2019.

Thank you for your attention