Computational studies of entanglement and quantum contextuality properties towards their formal verification

Henri de Boutray

Femto-ST laboratory
DISC department
VESONTIO team
ANR project: I-QUINS

henri.de_boutray@univ-fcomte.fr

PhD thesis defense - December 16, 2021

Studies of quantum entanglement and contextuality

Problematic:

- Lack of specification and verification in current quantum computing

Intermediary objective:

- Understanding key properties to be specified

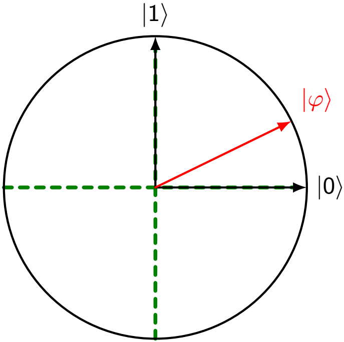
PhD Objectives:

- Entanglement detection
- Algorithm specification with entanglement
- Contextuality detection
  - Contextual experiment generation

Overview

1. Background
   - Quantum computing
   - Classical verification
2. Entanglement
   - Basics
   - Entanglement evaluation
   - Grover's algorithm
   - Results
3. Contextuality
   - Basics
   - Symplectic space
   - A linear problem
   - Results
4. Conclusion

The qubit, superposition



$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\begin{cases} |\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \\ (\alpha, \beta) \in \mathbb{C}^2, |\alpha|^2 + |\beta|^2 = 1 \end{cases}$$

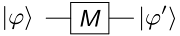
Qubit transformation: the unitary

$$|\varphi\rangle \;\text{—}\boxed{M}\text{—}\; |\varphi'\rangle$$

$$|\varphi'\rangle = [\![M]\!]\,|\varphi\rangle$$

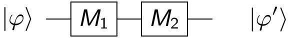
M unitary: $M\overline{M}^{\top} = I$

Qubit transformation: the unitary



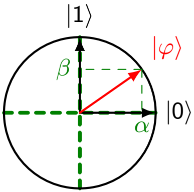
M unitary: $M\overline{M}^{\top} = I$

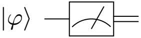
$$\left|\varphi'\right\rangle = [\![M]\!] \left|\varphi\right\rangle$$

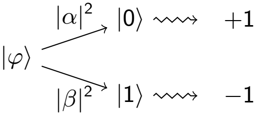


$$\left|\varphi'\right\rangle = M_2 M_1 \left|\varphi\right\rangle$$

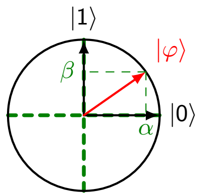
Qubit transformation: the measure

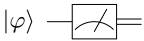


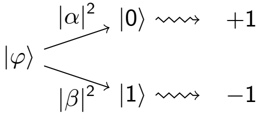




Qubit transformation: the measure







Pauli matrices:

X		Y		Z	
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$		$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$		$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	
$\|-\rangle$	$\|+\rangle$	$\|y_-\rangle$	$\|y_+\rangle$	$\|1\rangle$	$\|0\rangle$
-1	1	-1	1	-1	1

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}, \qquad |y_\pm\rangle = \frac{|0\rangle \pm i\,|1\rangle}{\sqrt{2}}$$

$$E(M_O(|\varphi\rangle)) = \langle\varphi|O|\varphi\rangle$$

Combining qubits

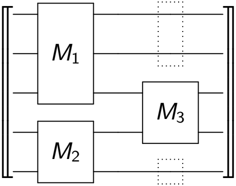
$$|\varphi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle, \qquad |\varphi_2\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle$$

$$\left.\begin{array}{l} |\varphi_1\rangle \; \text{———} \\ |\varphi_2\rangle \; \text{———} \end{array}\right\} |\varphi_1\rangle \otimes |\varphi_2\rangle$$

$$\begin{aligned} |\varphi_1\rangle \otimes |\varphi_2\rangle &= (\alpha_1 |0\rangle + \beta_1 |1\rangle) \otimes (\alpha_2 |0\rangle + \beta_2 |1\rangle) \\ &= \alpha_1\alpha_2 |00\rangle + \alpha_1\beta_2 |01\rangle + \beta_1\alpha_2 |10\rangle + \beta_1\beta_2 |11\rangle \end{aligned}$$

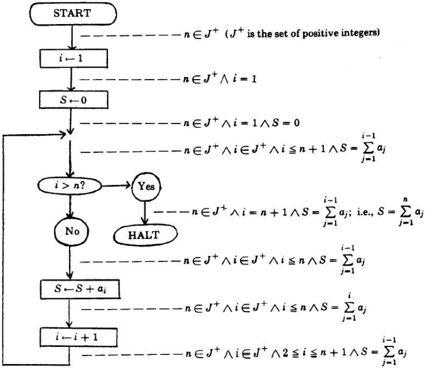
A state on n qubits is a vector of 2^n entries!

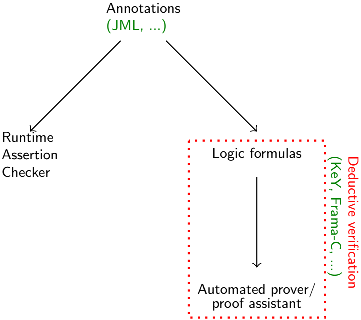
Combining gates



$$= (I_4 \otimes M_3 \otimes I_2) \times (M_1 \otimes M_2)$$

State properties

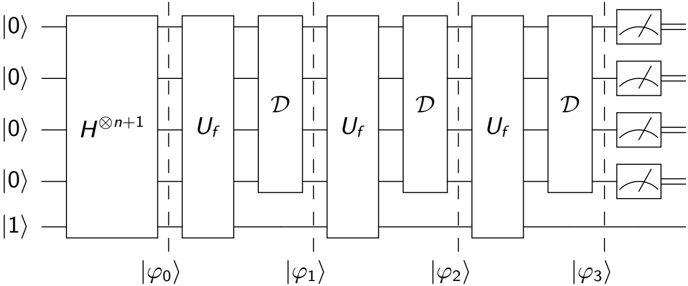




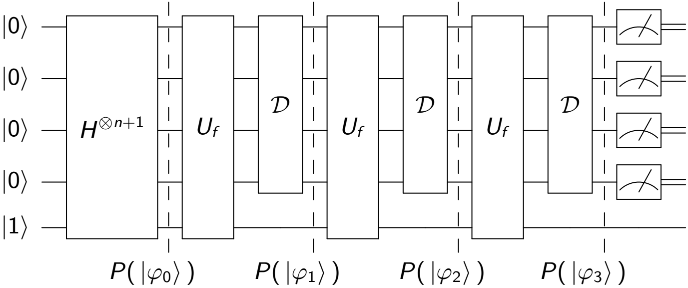
[Flo67] R. Floyd.
Assigning Meanings to Programs.
Proceedings of Symposium on Applied Mathematics, 19: 19–32, 1967.

Entanglement

Quantum annotations



Quantum annotations



Bell inequalities (CHSH actually)

Classical :

A	B	A'	B'	$AB + AB' + A'B - A'B'$
-1	-1	-1	-1	2
-1	-1	-1	1	2
-1	-1	1	-1	2
-1	-1	1	1	-2
-1	1	-1	-1	-2
-1	1	-1	1	-2
-1	1	1	-1	2
-1	1	1	1	-2
1	-1	-1	-1	-2
1	-1	-1	1	2
1	-1	1	-1	-2
1	-1	1	1	-2
1	1	-1	-1	-2
1	1	-1	1	2
1	1	1	-1	2
1	1	1	1	2

$$\langle AB\rangle + \langle AB'\rangle + \langle A'B\rangle - \langle A'B'\rangle \leq 2$$

Quantum :

$$|\Phi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

$$A = X, \qquad A' = Z, \qquad B = -\frac{Z+X}{\sqrt{2}}, \qquad B' = \frac{Z-X}{\sqrt{2}}$$

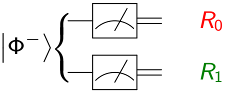
$$\begin{aligned}\langle AB\rangle_{\Phi^-} &= \langle \Phi^- | -X \otimes \tfrac{Z+X}{\sqrt{2}} |\Phi^-\rangle \\ &= -\tfrac{1}{2}\langle \Phi^- | \big(|1\rangle \otimes (|0\rangle - |1\rangle) - \\ &\qquad |0\rangle \otimes (|0\rangle + |1\rangle)\big) \\ &= \tfrac{1}{\sqrt{2}}\end{aligned}$$

similarly $\langle AB'\rangle_{\Phi^-} = \langle A'B\rangle_{\Phi^-} = \frac{1}{\sqrt{2}}$ and $\langle A'B'\rangle_{\Phi^-} = -\frac{1}{\sqrt{2}}$

$$\langle AB\rangle_{\Phi^-} + \langle AB'\rangle_{\Phi^-} + \langle A'B\rangle_{\Phi^-} - \langle A'B'\rangle_{\Phi^-} = 2\sqrt{2} > 2$$

Correlation

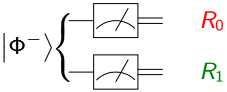
$$|\Phi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$



$R_0 = 1 \implies R_1 = -1$ $\qquad$ $R_0 = -1 \implies R_1 = 1$

Correlation

$$|\Phi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$



$R_0 = 1 \implies R_1 = -1$ $R_0 = -1 \implies R_1 = 1$

$|\Phi^-\rangle$ is not separable: $\nexists\, |\varphi_1\rangle, |\varphi_2\rangle \,/\, |\Phi^-\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$
entangled = not separable

Entanglement evaluations

- entanglement quantification: Geometric Measure of entanglement [WG03], Bell-Mermin inequalities [Mer90, ACG+16], Cayley hyperdeterminant [LT03]
- entanglement classification: Secant varieties [HJN16]

[WG03] Tzu-Chieh Wei and Paul 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.

[LT03] Jean-Gabriel Luque, and Jean-Yves Thibon.
The Polynomial Invariants of Four Qubits.
Physical Review A, 67, no. 4: 042303, April 2003.

[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 $a = (a_n)_{n \geq 1}$ and $a' = (a'_n)_{n \geq 1}$ be two families of observables. The *Mermin polynomial* $M_n(a, a')$ is defined by:

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

Mermin polynomials

Definition (Mermin polynomials)

Let $a = (a_n)_{n\geq 1}$ and $a' = (a'_n)_{n\geq 1}$ be two families of observables. The *Mermin polynomial* $M_n(a, a')$ is defined by:

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

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 $a = (a_n)_{n\geq 1}$ and $a' = (a'_n)_{n\geq 1}$ be two families of observables. The *Mermin polynomial* $M_n(a, a')$ is defined by:

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

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 for Grover's algorithm

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

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

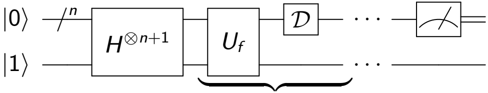
- M_n is a function of $(a_i)_{1\leq i\leq n}$ and $(a'_i)_{1\leq i\leq n}$

$$\forall i, a_i = \alpha X + \beta Y + \delta Z, \quad a'_i = \alpha' X + \beta' Y + \delta' Z$$

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

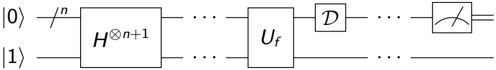
Grover algorithm in a nutshell

- Search an item $\mathbf{x_0}$ in an unsorted database Ω of $N = 2^n$ objects
- Just by applications of the Boolean function $f : \Omega \rightarrow \{0, 1\}$ 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 $U_f \left|x, y\right\rangle = \left|x, y \oplus f(x)\right\rangle$
- Amplitude amplification

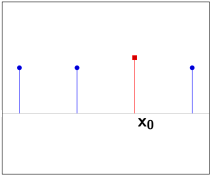


Repeated $\lfloor \pi\sqrt{N}/4 \rceil$ times

Grover's amplitude amplification

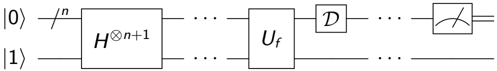


. . .

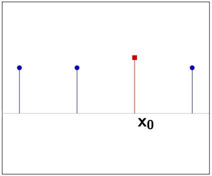


State before U_f

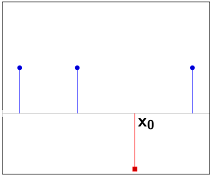
Grover's amplitude amplification



. . .

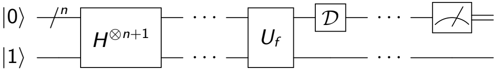


State before U_f

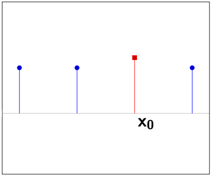


State after U_f

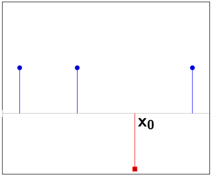
Grover's amplitude amplification



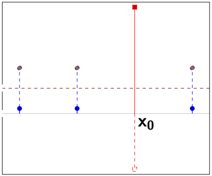
. . .



State before U_f

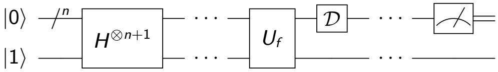


State after U_f

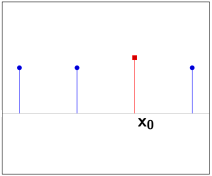


Effect of $\mathcal{D}$

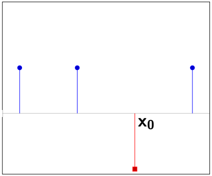
Grover's amplitude amplification



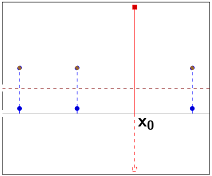
. . .



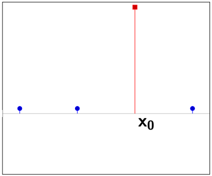
State before U_f



State after U_f

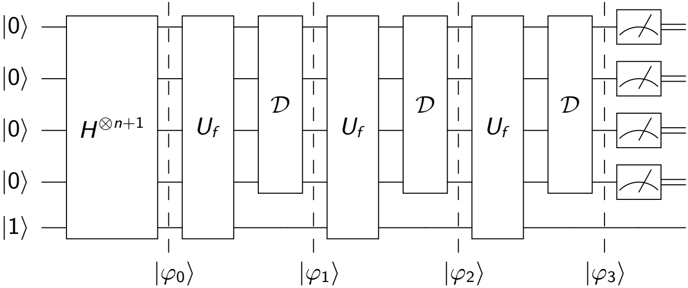


Effect of $\mathcal{D}$



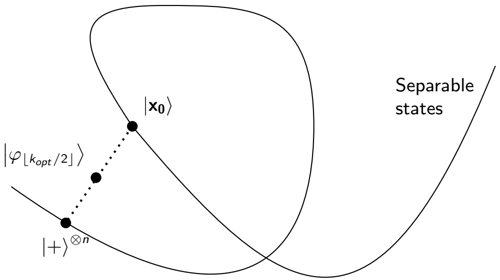
State after $\mathcal{D}$

States naming



Preamble

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



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

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

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

Expected entanglement properties

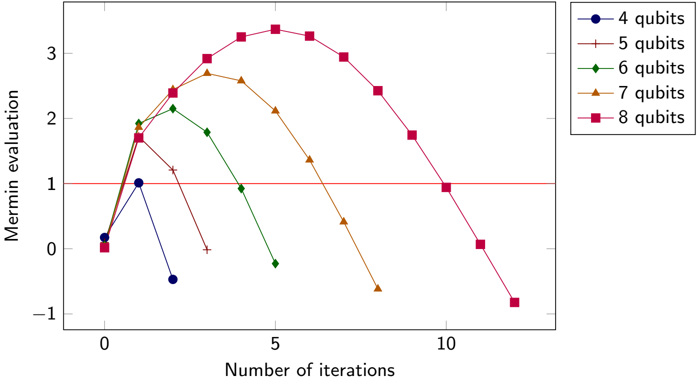
If M_n is chosen to optimize $f_{M_n}(|\varphi_{ent}\rangle)$, then we expect f_{M_n} to behave like a distance measure from $|\varphi_{ent}\rangle$.

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 $[\lfloor k_{opt}/2 \rfloor + 1, k_{opt}]$

Results, 4 to 8

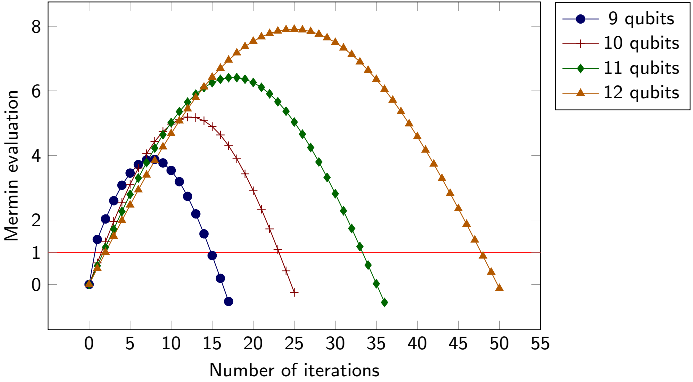
For 8 qubits, 1 week of computation on personal computer with naive implementation.



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

Results, 9 to 12

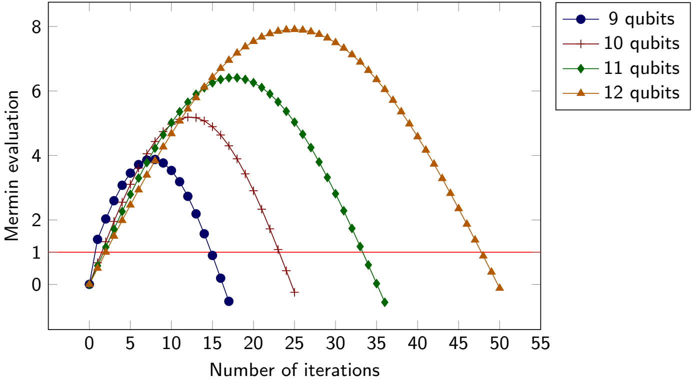
On a supercomputer (Mésocentre UFC):



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

Results, 9 to 12

On a supercomputer (Mésocentre UFC):

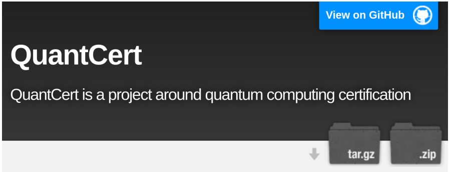


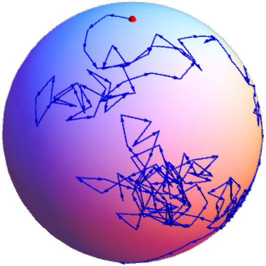
n	9	10	11	12
k_{opt}	17	25	36	50

This was in fact a form of RAC!

Technical elements

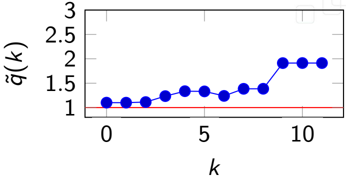
($\sim$ 2000 LoC)



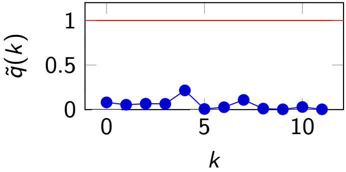


Additional works!

- Work on the Quantum Fourier Transform



- Works on IBM's quantum experience (work with Grâce Amouzou, Lomé university, Togo)



- Formalization of some notions

Coq QWIRE

Contextuality

The Mermin-Peres square

$$
\begin{array}{ccccc}
X \otimes I & — & I \otimes X & — & X \otimes X \\
| & & | & & \| \\
I \otimes Y & — & Y \otimes I & — & Y \otimes Y \\
| & & | & & \| \\
X \otimes Y & — & Y \otimes X & — & Z \otimes Z
\end{array}
$$

The Mermin-Peres square

$$
\begin{array}{ccccccc}
X \otimes I & — & I \otimes X & — & X \otimes X & & \color{green}{I} \\
| & & | & & \| & & \\
I \otimes Y & — & Y \otimes I & — & Y \otimes Y & & \color{green}{I} \\
| & & | & & \| & & \\
X \otimes Y & — & Y \otimes X & — & Z \otimes Z & & \color{green}{I} \\
\color{green}{I} & & \color{green}{I} & & \color{green}{-I} & &
\end{array}
$$

The Mermin-Peres square

$$
\begin{array}{cccccccc}
-1 & & & & & & & \\
X \otimes I & — & I \otimes X & — & X \otimes X & & I \\
| & & | & & \| & & \\
I \otimes Y & — & Y \otimes I & — & Y \otimes Y & & I \\
| & & | & & \| & & \\
X \otimes Y & — & Y \otimes X & — & Z \otimes Z & & I \\
I & & I & & -I & &
\end{array}
$$

The Mermin-Peres square

$$
\begin{array}{ccccccc}
-1 & & -1 & & & & \\
X \otimes I & — & I \otimes X & — & X \otimes X & & I \\
| & & | & & \| & & \\
I \otimes Y & — & Y \otimes I & — & Y \otimes Y & & I \\
| & & | & & \| & & \\
X \otimes Y & — & Y \otimes X & — & Z \otimes Z & & I \\
I & & I & & -I & &
\end{array}
$$

The Mermin-Peres square

$$
\begin{array}{ccccccc}
-1 & & -1 & & 1 & & \\
X \otimes I & — & I \otimes X & — & X \otimes X & & I \\
| & & | & & \| & & \\
I \otimes Y & — & Y \otimes I & — & Y \otimes Y & & I \\
| & & | & & \| & & \\
X \otimes Y & — & Y \otimes X & — & Z \otimes Z & & I \\
I & & I & & -I & &
\end{array}
$$

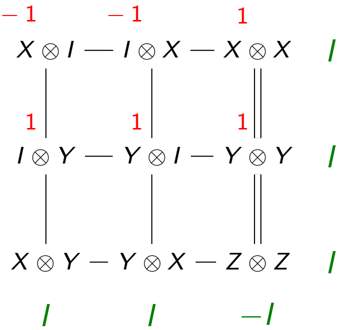
The Mermin-Peres square

$$
\begin{array}{cccccc}
-1 & & -1 & & 1 & \\
X \otimes I & — & I \otimes X & — & X \otimes X & I \\
1 \; | & & | & & \| & \\
I \otimes Y & — & Y \otimes I & — & Y \otimes Y & I \\
| & & | & & \| & \\
X \otimes Y & — & Y \otimes X & — & Z \otimes Z & I \\
I & & I & & -I &
\end{array}
$$

The Mermin-Peres square

-1	-1	1	
$X \otimes I$ —	$I \otimes X$ —	$X \otimes X$	I
1	1		
$I \otimes Y$ —	$Y \otimes I$ —	$Y \otimes Y$	I
$X \otimes Y$ —	$Y \otimes X$ —	$Z \otimes Z$	I
I	I	$-I$	

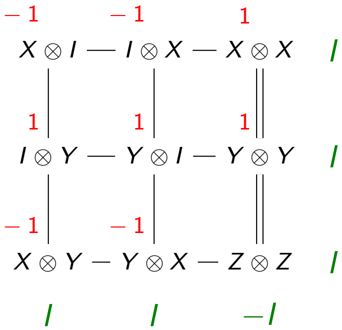
The Mermin-Peres square



The Mermin-Peres square

$$
\begin{array}{ccccccc}
-1 & & -1 & & 1 & & \\
X \otimes I & — & I \otimes X & — & X \otimes X & & I \\
| & & | & & \| & & \\
1 & & 1 & & 1 & & \\
I \otimes Y & — & Y \otimes I & — & Y \otimes Y & & I \\
| & & | & & \| & & \\
-1 & & & & & & \\
X \otimes Y & — & Y \otimes X & — & Z \otimes Z & & I \\
 & & & & & & \\
I & & I & & -I & &
\end{array}
$$

The Mermin-Peres square



The Mermin-Peres square

-1	-1	1	
$X \otimes I$ —	$I \otimes X$ —	$X \otimes X$	I
1	1	1	
$I \otimes Y$ —	$Y \otimes I$ —	$Y \otimes Y$	I
-1	-1	?	
$X \otimes Y$ —	$Y \otimes X$ —	$Z \otimes Z$	I
I	I	$-I$	

Unsatisfiable!

Contextuality

An experiment is contextual if no non-contextual classical theory can predict its results.

In quantum physics, a context $c \in C$ is a sequence of compatible (commuting) observables. The measures e_O are eigenvalues of observables $O \in \mathcal{O}$ and the product of measures is the eigenvalue of the product of observables: $\prod_{O \in c} e_O = e_{\prod_{O \in c} O}$.

The experiment $(\mathcal{O}, C)$ is contextual if

$$\nexists f : \mathcal{O} \to \{-1, 1\} \ / \ \forall c \in C, \prod_{O \in c} f(O) = e_{\prod_{O \in c} O}.$$

Binary polar symplectic space

We are interested by geometries such as the Mermin-Peres square, we explore a space containing them, the binary polar symplectic space.

$O = s \bigotimes_k O_k \in \mathcal{P}_n$ with $O_k \in \{I, X, Y, Z\}$ and $s \in \{\pm 1, \pm i\}$

We build the bijection $\pi_n : \mathcal{P}_n / \{\pm I, \pm iI\} \to (\mathbb{Z}/2\mathbb{Z})^{2n}$

$$\pi_1(I) = (0,0)$$
$$\pi_1(X) = (0,1)$$
$$\pi_1(Y) = (1,1)$$
$$\pi_1(Z) = (1,0)$$

$$\pi_n(O_1 \otimes O_2) = \text{cat}(\pi_{n_1}(O_1), \pi_{n_2}(O_2)), \quad n_1 + n_2 = n$$

Example: $\pi_3(X \otimes Y \otimes I) = (0,1,1,1,0,0)$

Symplectic product

We have a representation of the *operators* (without their phase), of their *product* (the sum of points), but we lost the *commutation relation*. To recover it, let us check the condition on the coefficients.

$\pi_1(O) = (z, x), \quad O = sZ^zX^x, s \in \{\pm 1, \pm i\}$

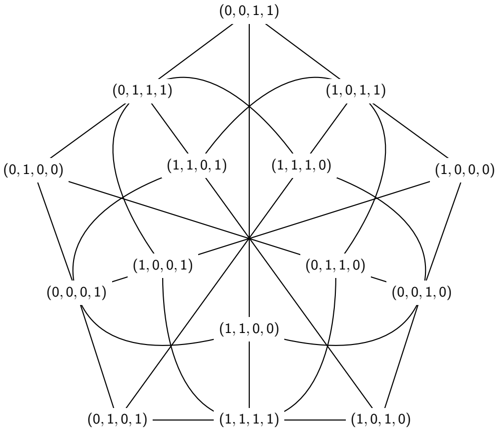
$$\begin{aligned} OO' &= O'O \\ ss'(Z^zX^x)(Z^{z'}X^{x'}) &= s's(Z^{z'}X^{x'})(Z^zX^x) \\ (Z^zX^x)(Z^{z'}X^{x'}) - (Z^{z'}X^{x'})(Z^zX^x) &= 0 \\ (-1)^{xz'}Z^zZ^{z'}X^xX^{x'} - (-1)^{x'z}Z^{z'}Z^zX^{x'}X^x &= 0 \\ ((-1)^{xz'} - (-1)^{x'z})Z^{z+z'}X^{x+x'} &= 0 \\ ((-1)^{xz'} - (-1)^{x'z}) &= 0 \\ xz' &= x'z \end{aligned}$$

For $\pi_n(O) = (o_1, \ldots, o_{2n})$,

$$\langle O | O' \rangle = \sum_{i=1}^{n} o_{2i-1}o'_{2i} + o_{2i}o'_{2i-1}$$

Building geometries

The space with all possible points and the isotropic subspaces: $W(2n-1,2)$ (shorthanded W_n). Example for $n=2$, the Doily:



Hyperplanes

Isotropic subspace of W_n: maximal set of points P such that $\forall p_1, p_2 \in P, \langle p_1 | p_2 \rangle = 0$.

The *lines* of W_n are isotropic subspaces of three elements.

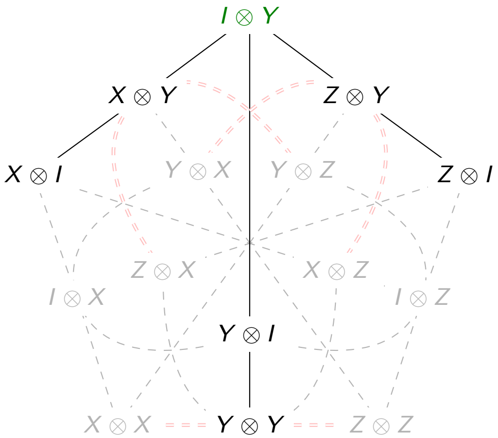
The *hyperplanes* are isotropic subspaces of W_n such that a line of W_n is either entirely in the subspace or intersecting the subspace in a single point.

A hyperplane is either a *perpset* or a *quadric*.

Perpset

A perpset P_r is a set of points that do commute with a single point r:

$$P_r = \{p \in W_n, \langle p|r\rangle = 0\}$$



Quadric

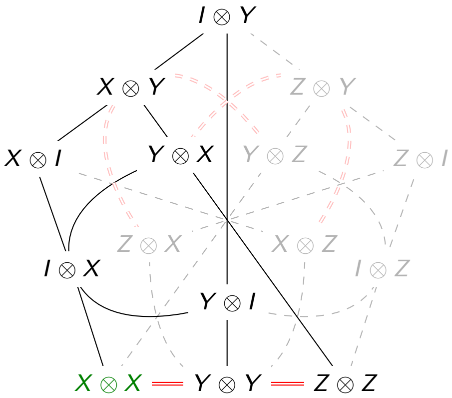
The standard quadratic form $\mathcal{Q}_0(x) = \sum_{i=1}^{n} x_{2i-1}x_{2i}$ let us define a *quadratic form* for each point p of W_n: $\mathcal{Q}_p(x) = \mathcal{Q}_0(x) + \langle x|p\rangle$.

The *quadric* Q_p is the set of points annihilating the quadratic form $\mathcal{Q}_p$.

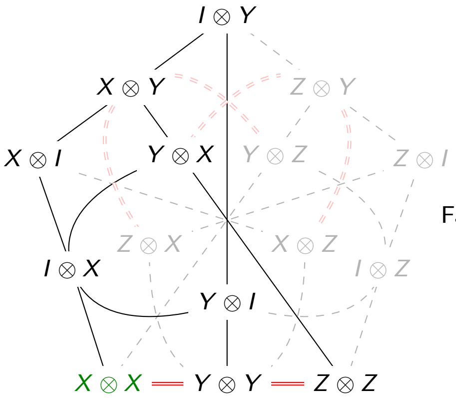
A quadric (resp. quadratic form) Q_p (resp. $\mathcal{Q}_p$) is said to be *hyperbolic* if $\mathcal{Q}_0(p) = 0$, and *elliptic* otherwise.

Note that Q_0 is counted in the hyperbolic quadrics.

Hyperbolic

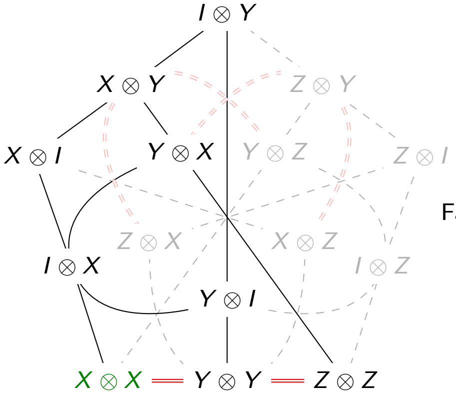


Hyperbolic

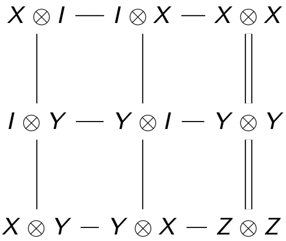


Familiar?

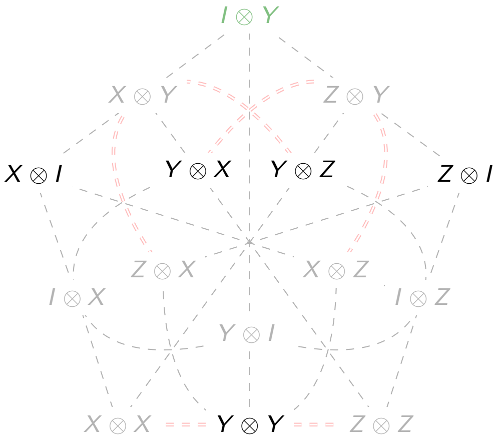
Hyperbolic



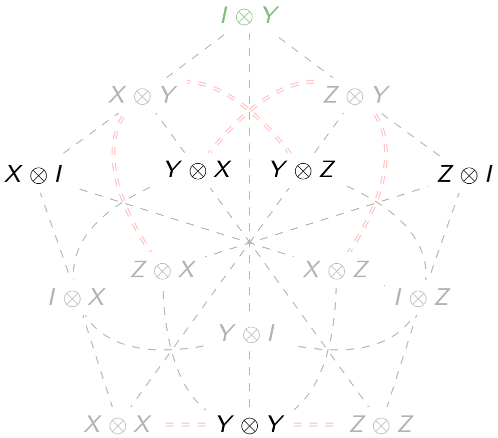
Familiar?



Elliptic



Elliptic



No line! . . . only for W_2

Contextuality as a linear problem

Recall, the experiment $G = (\mathcal{O}, C)$ is contextual when

$$\nexists f : \mathcal{O} \to \{-1, 1\} \;/\; \forall c \in C, \prod_{O \in c} f(O) = e_{\prod_{O\in c} O}.$$

$$(\{-1, 1\}, \times) \to (\mathbb{Z}/2\mathbb{Z}, +)$$

Let $A = Inc(G)$, e the evaluation vector such that its c^{th} entry e_c corresponds to context $c \in C$ and $(-1)^{e_c} I = \Pi_{O \in c} O$:

$$\nexists x \;/\; Ax = e$$

Families contextuality

Geometries	$n=2$	$n=3$	$n=4$	$n=5$
Whole space	C(1)	C(1)	C(1)	C(1)
Hyperbolics	C(10)	**C(36)**	**C(136)**	**C(528)**
Elliptics	N/A (6)	**C(28)**	**C(120)**	**C(496)**
Perpsets	N(15)	**N(63)**	**N(255)**	**N(1023)**

n: Number of qubits of the system

N: Non-contextual

C: Contextual

(k): There are k instances in this family

N/A: Not applicable

bold: New results

Technicalities

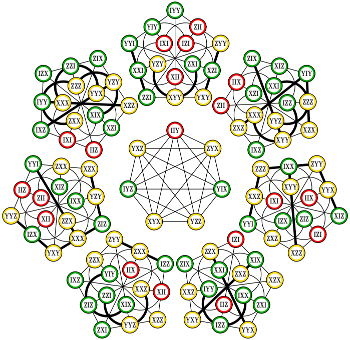
MAGMA
COMPUTER • ALGEBRA

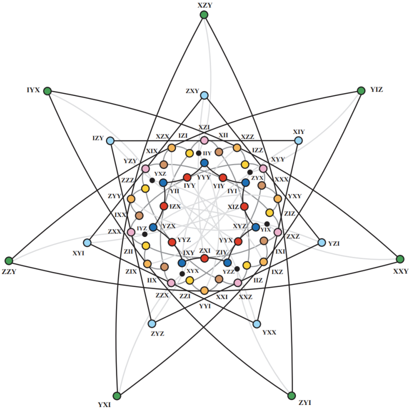
($\sim$ 3000 LoC)

$$4^n - 1 \text{ points in } W_n \implies \begin{cases} \text{Geometric understanding} \\ \\ \text{Intensive computer testing} \end{cases}$$

- Preamble work on incidence structures (work lead by Jessy Colonval, UFC),
- many more geometries explored (with Metod Saniga, Astronomical Institute of the Slovak Academy of Sciences)

Other geometries





Works

- Journal articles
  - QIP'20
  - Mathematics'21
- Conference paper
  - AFADL'19
- Conference posters
  - GDR-IM'20
  - QPL'21
- Presentations
  - JDD'19
  - GT-IQ'19
  - R&Days'21
  - Auburn algebra seminar'21
- Website
  - `quantcert.github.io`
- Draft
  - Contextuality degree study

New horizons

- Using these notions in formalization frameworks
  - Mermin polynomials (started in QWIRE, Coq)
  - Contextuality (started in Why3, Qbricks ?)
- More geometries to explore!
  - Cayley hexagons
  - Quadratic W_4 doilies
  - ...

Thank you for your attention