Title: A toy theory of quantum speed-ups based on the stabilizer formalism

Date: Nov 09, 2016 04:00 PM

URL: http://pirsa.org/16110067

Abstract: A central question in quantum computation is to identify which problems can be solved faster on a quantum computer. A Holy Grail of the field would be to have a theory of quantum speed-ups that delineates the physical mechanisms sustaining quantum speed-ups and helps in the design of new quantum algorithms. In this talk, we present such a toy theory for the study of a class of quantum algorithms for algebraic problems, including Shorâ€™s celebrated factoring algorithm. Our theory is an extension of Gottesmanâ€™s stabilizer formalism based on elements of group and hypergroup theory. Using our methods, we develop classical simulation algorithms for Clifford-like circuits containing quantum Fourier transforms as well as new quantum algorithms for hidden symmetries and hyper-symmertry problems. During the talk, we will discuss the role of resources such as entanglement, interference and contextuality within our formalism and connect quantum speed-ups therein to the presence of precise algebraic structures.

Based on the following works:

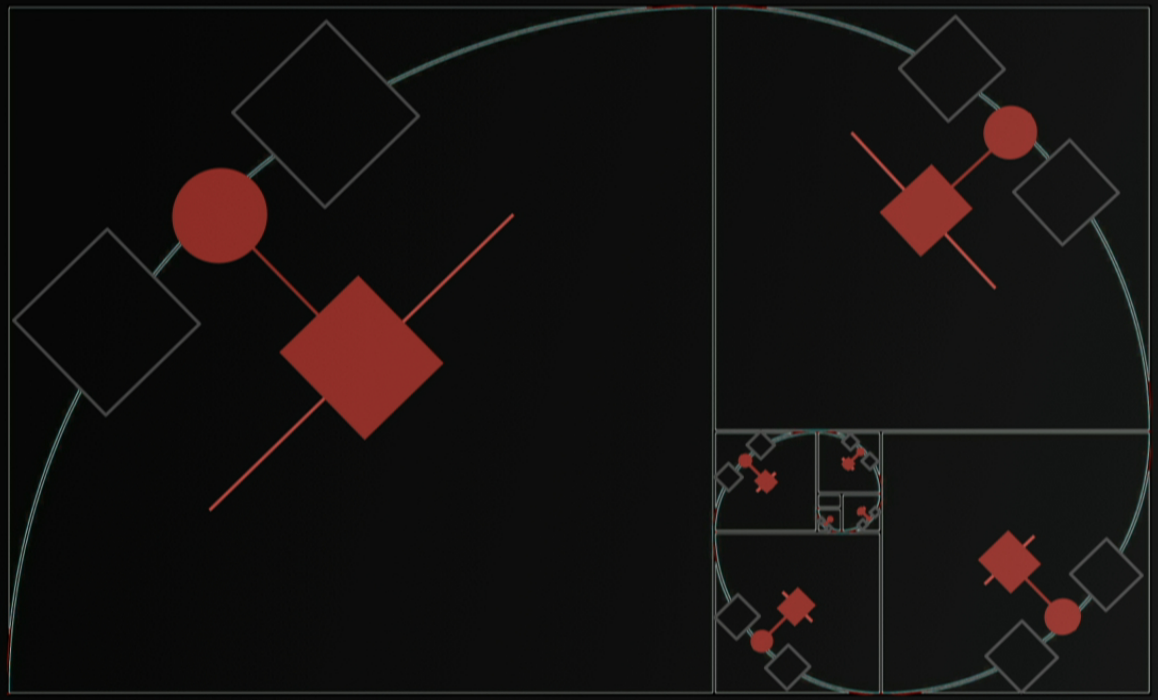
[1] https://arxiv.org/abs/1210.3637
[2] https://arxiv.org/abs/1409.3208
[3] https://arxiv.org/abs/1409.4800
[4] https://arxiv.org/abs/1509.05806

A toy theory of quantum speed-up based on the stabilizer formalism

Juan Bermejo-Vega

FU Berlin (formerly MPI of Quantum Optics)

Perimeter Institute, PiQuDos Seminar (Nov 9, 2016)



This talk

Algebraic formalism of extended Clifford circuits

Key Idea

Pauli operators are elements of algebraic sets (particle theories)

Commutative group

$a + b = c$

Hypergroups (Fusion categories)

$A \times B = \sum_{C \in T} N_{AB}^{C} C$

This talk

Algebraic formalism of extended Clifford circuits

Key Idea

Pauli operators are elements of algebraic sets (particle theories)

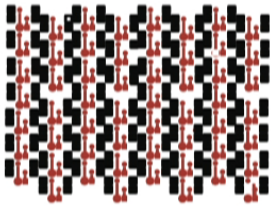
Commutative group

$a + b = c$

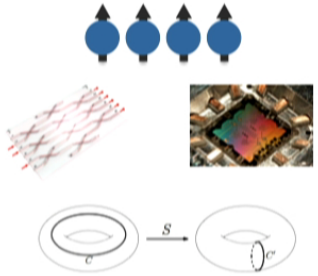
Hypergroups (Fusion categories)

$A \times B = \Sigma_{C \in T} N_{AB}^{C} C$

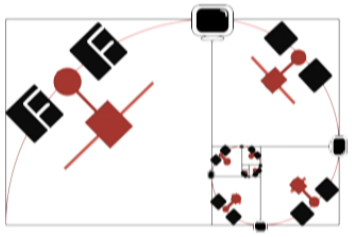
Classical simulations



Describing quantum many-body states

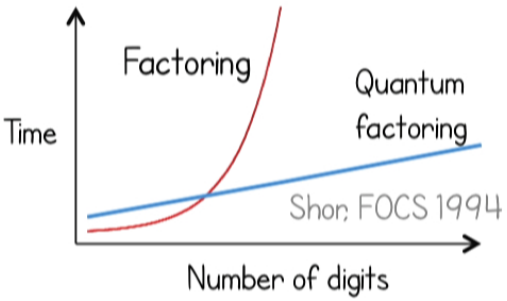


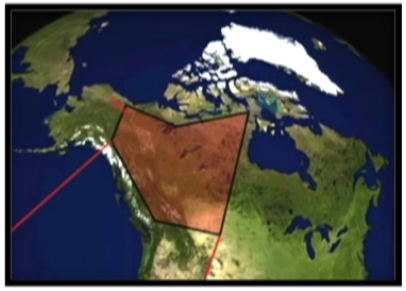
Quantum algorithms



Motivation

What powers quantum computation?

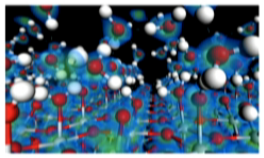




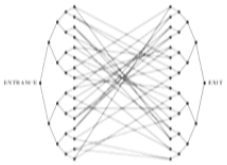
How practical is quantum computation?

Algebraic Problems

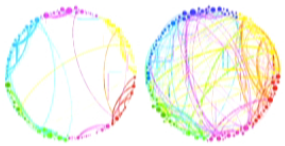
Quantum Simulation



Graph Problems

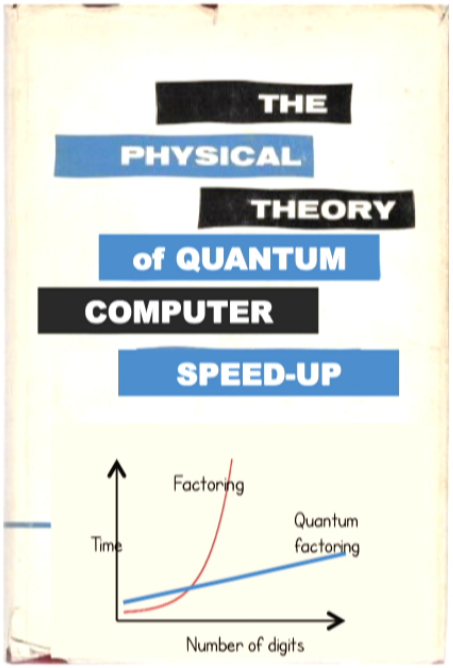


Machine learning



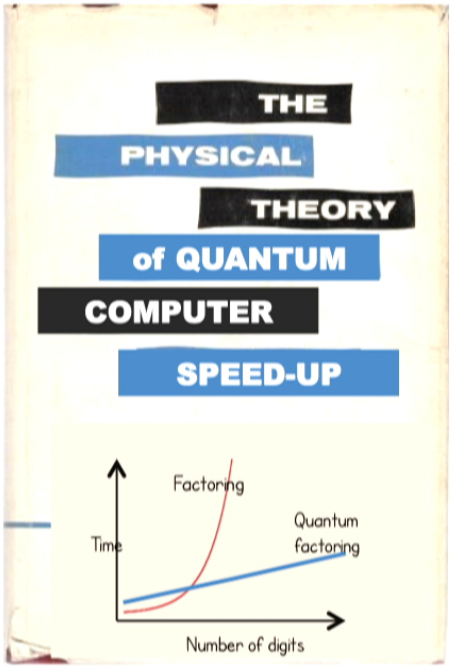
Motivation

Can we have a theory of quantum speed-ups?



Motivation

Can we have a theory of quantum speed-ups?

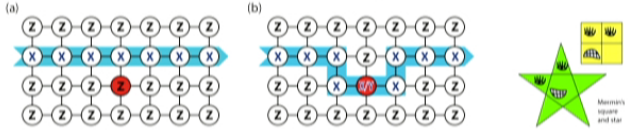


Obstacles:

1. No classical analogue
2. Emergence
3. Existence

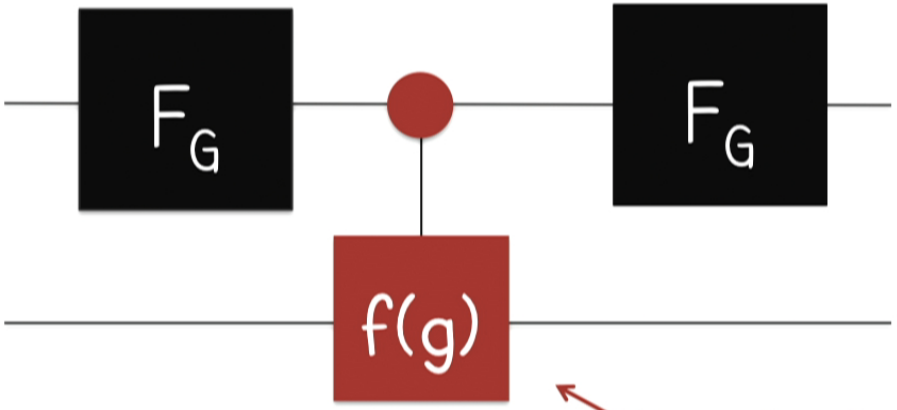
Common approach: resource theories

(Talk tomorrow to 11am, QNC, room 1501)

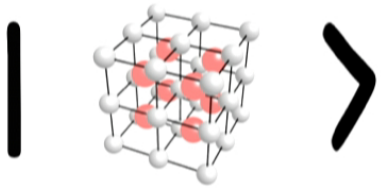


Howard, Wallman, Veitch, Emerson, Nature 2014, arXiv:1401.4174
Delfosse, Allard Guerin, Bian, Raussendorf, PRX 2015, arXiv:1409.5170
Raussendorf, Browne, Delfosse, Okay, **JBV**, arXiv:1511.08506
JBV, Delfosse, Browne, Okay, Raussendorf, arXiv:1610.08529
Delfosse, Okay, **JBV**, Browne, Raussendorf, arXiv:1610.07093

Quantum algorithms for hidden subgroups



Hidden subgroup: $f(g+h)=f(g)$



Group function

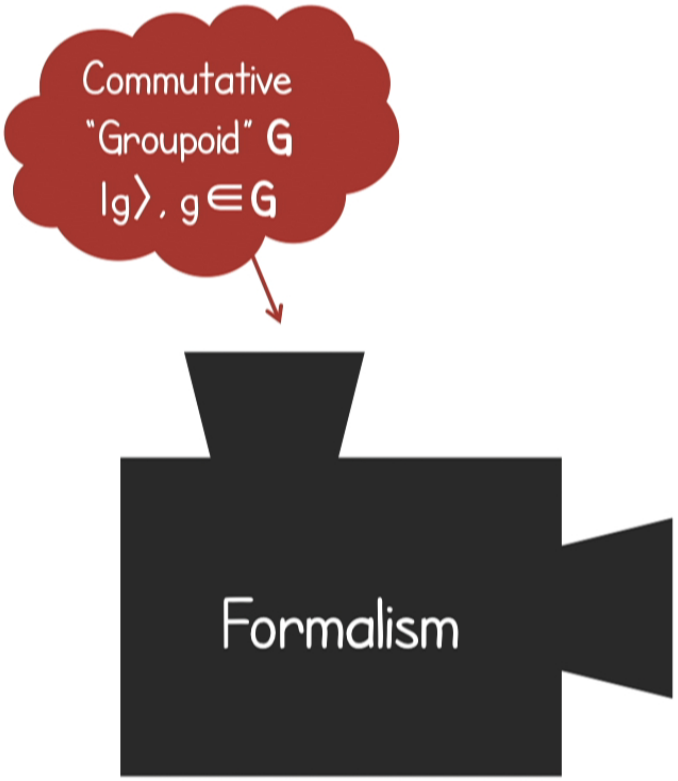
Commutative group!

$G=Z^m \times Z_{d_1} \times \ldots \times Z_{d_n}$

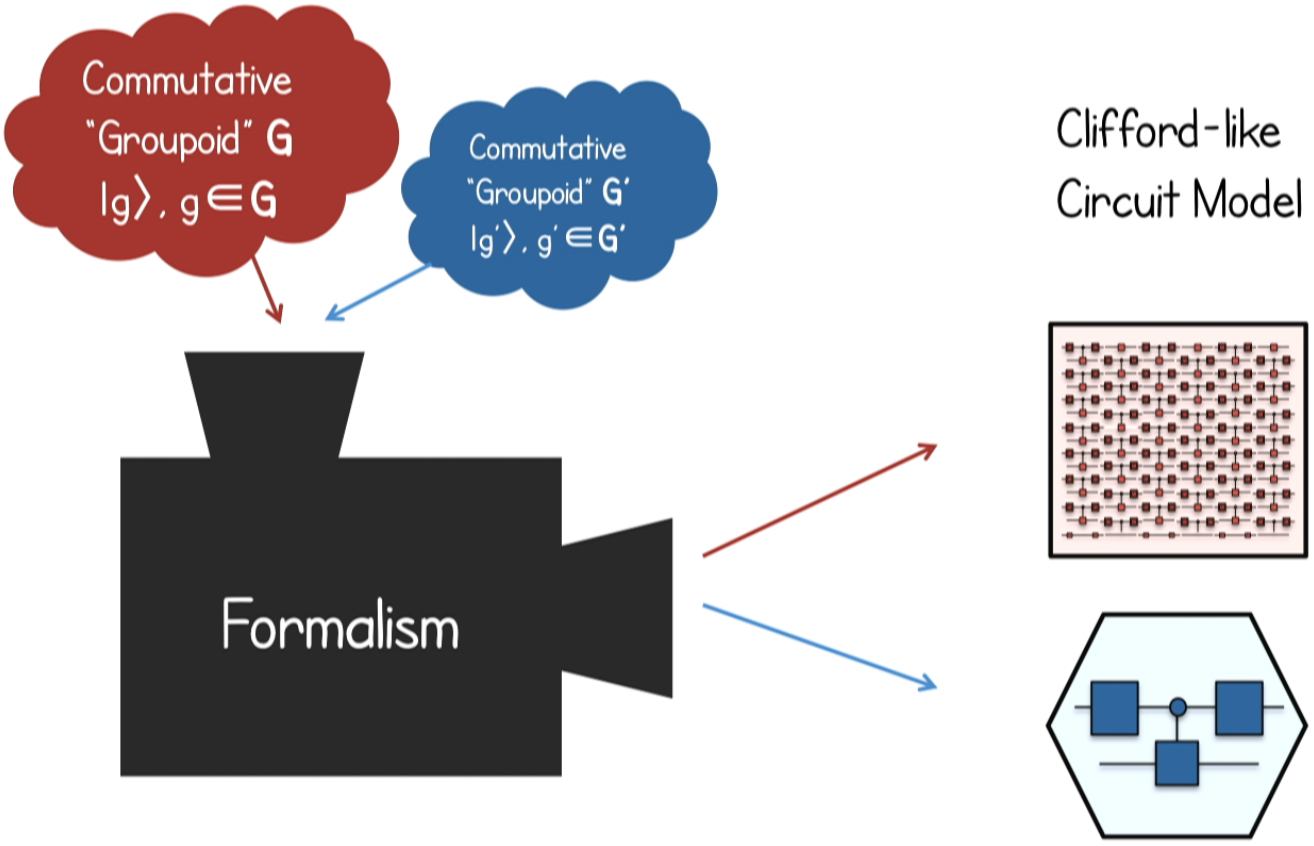
RSA, Diffie-Hellman
Elliptic Curve Cryptography

Shor, FOCS 1994
Proos-Zalka, QIC 2003

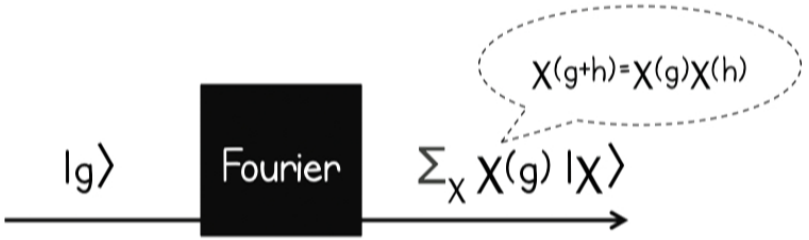
Normalizer Circuit Formalism



Normalizer Circuit Formalism



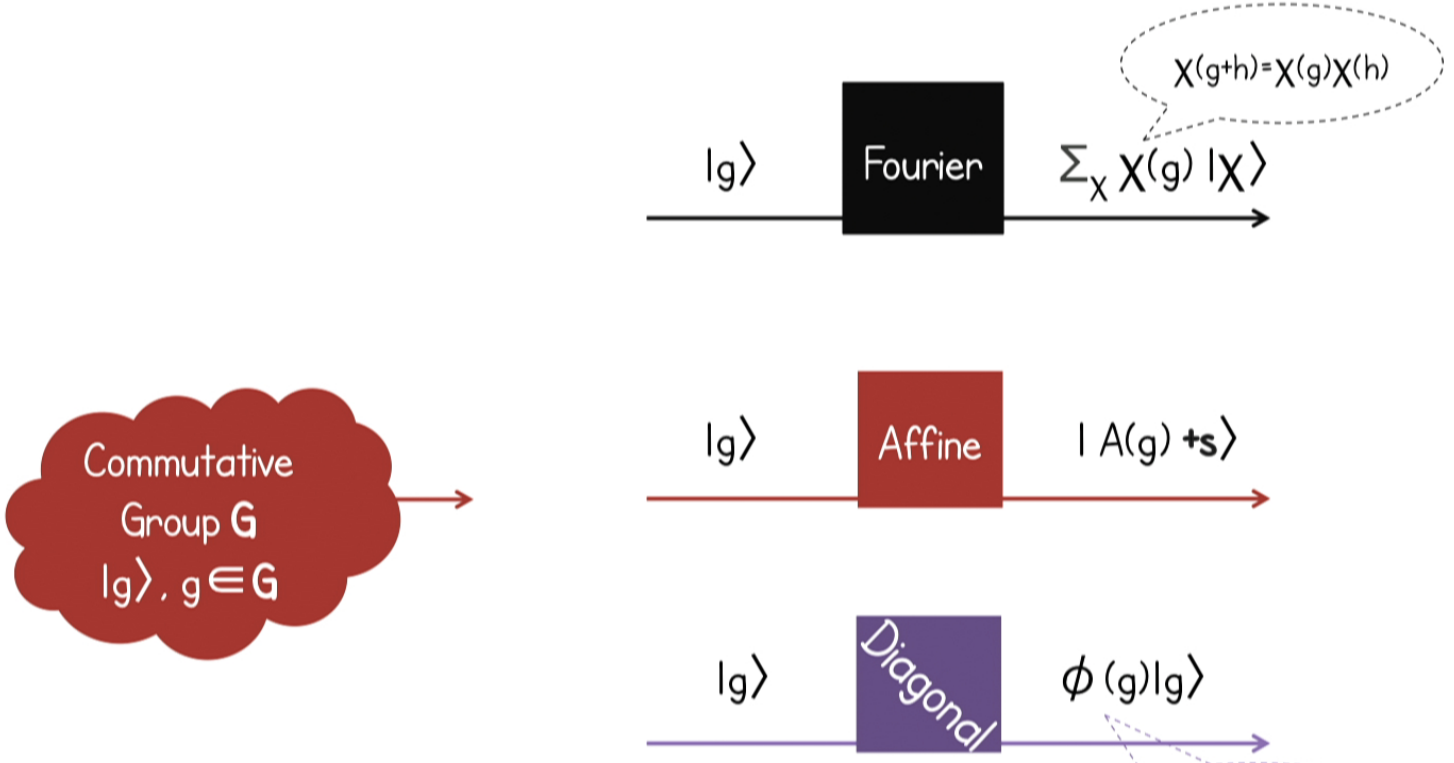
Normalizer Gates over G



Commutative Group **G**
$|g\rangle$, $g \in G$

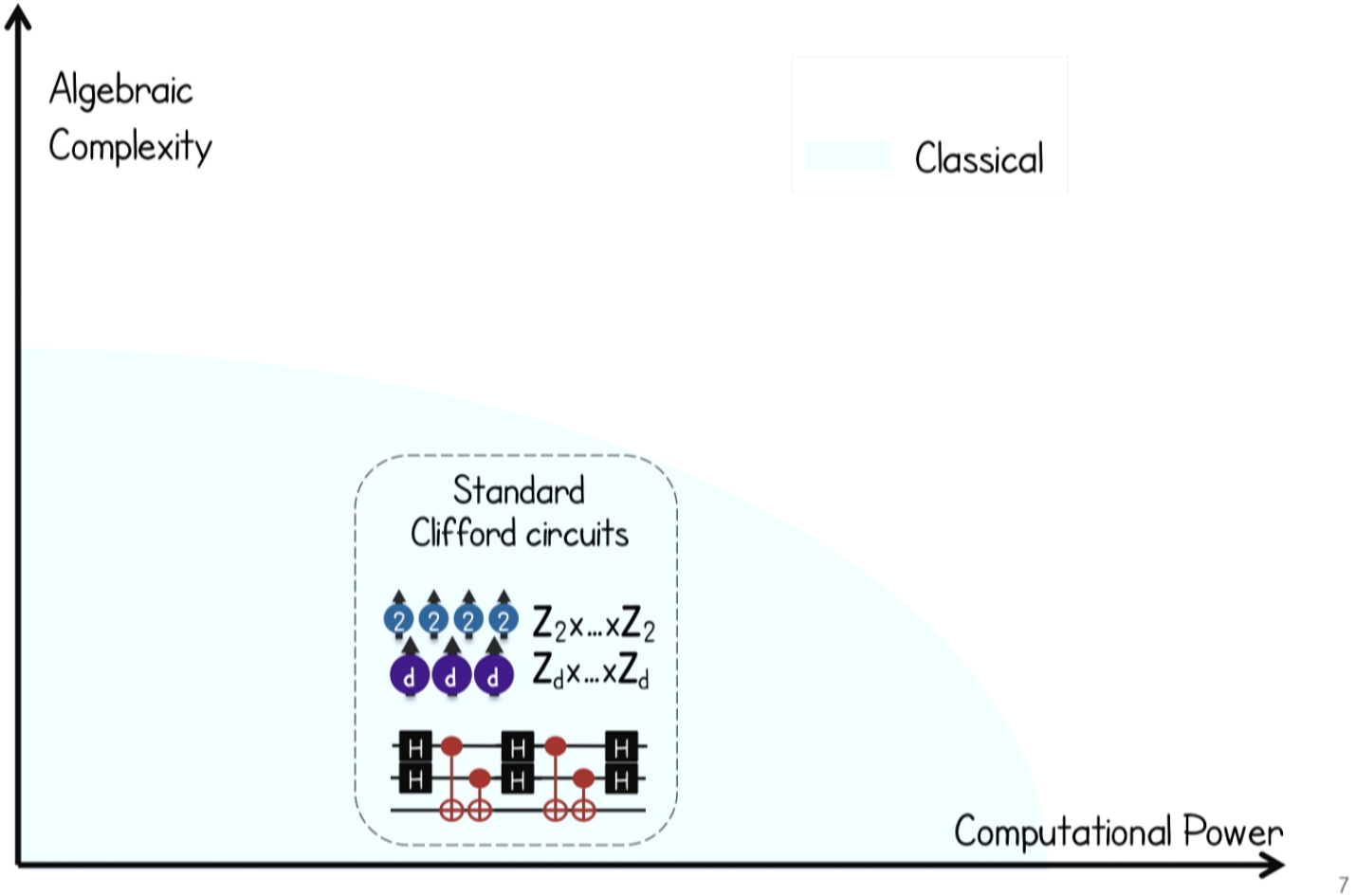
Bermejo-Vega, Van den Nest, QIC 2014, arXiv:1210.3637
Bermejo-Vega, Lin, Van den Nest, QIC 2016, arXiv:1409.3208
Bermejo-Vega, Lin, Van den Nest, arXiv:1409.4800

Normalizer Gates over G

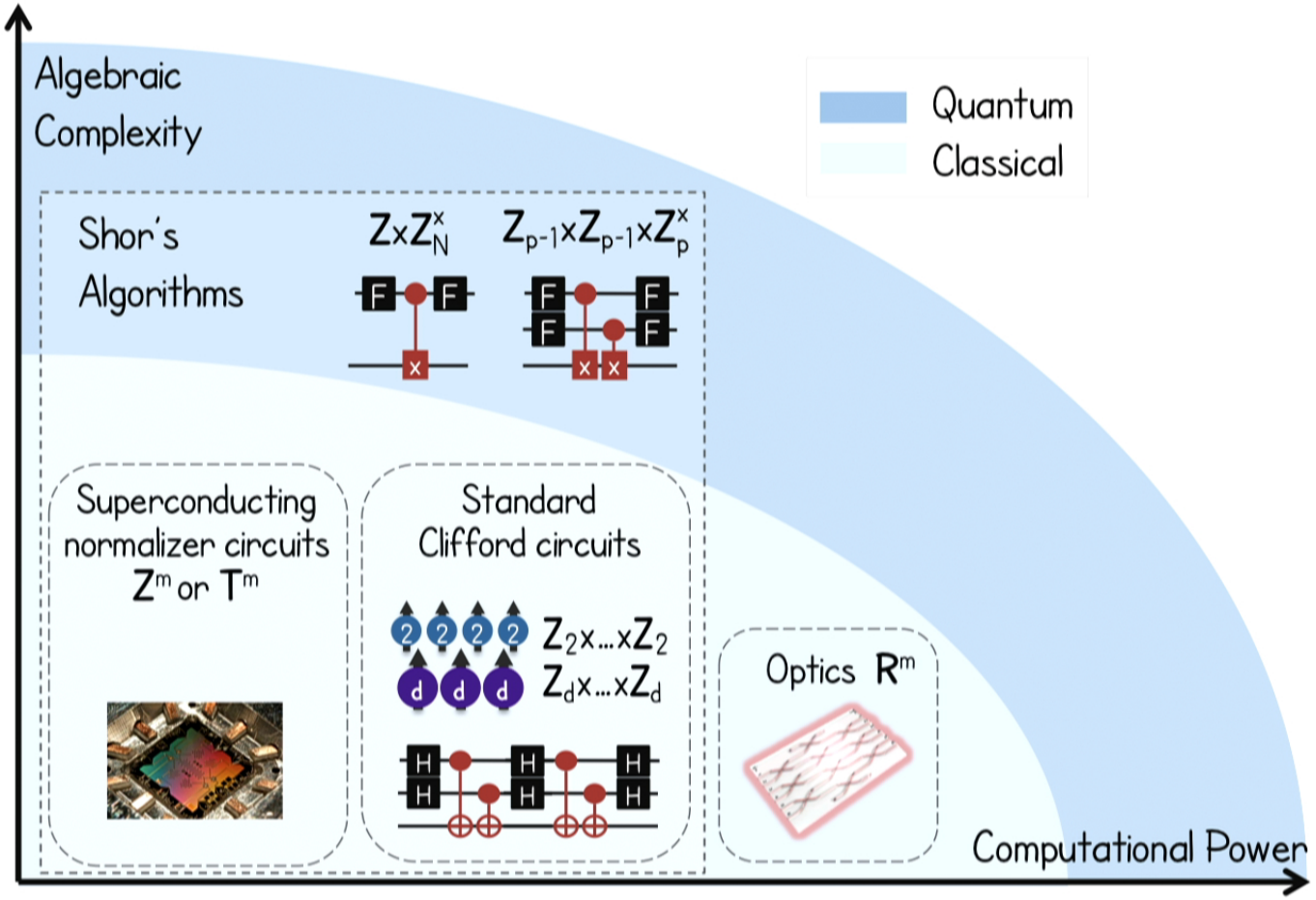


Bermejo-Vega, Van den Nest, QIC 2014, arXiv:1210.3637
Bermejo-Vega, Lin, Van den Nest, QIC 2016, arXiv:1409.3208
Bermejo-Vega, Lin, Van den Nest, arXiv:1409.4800

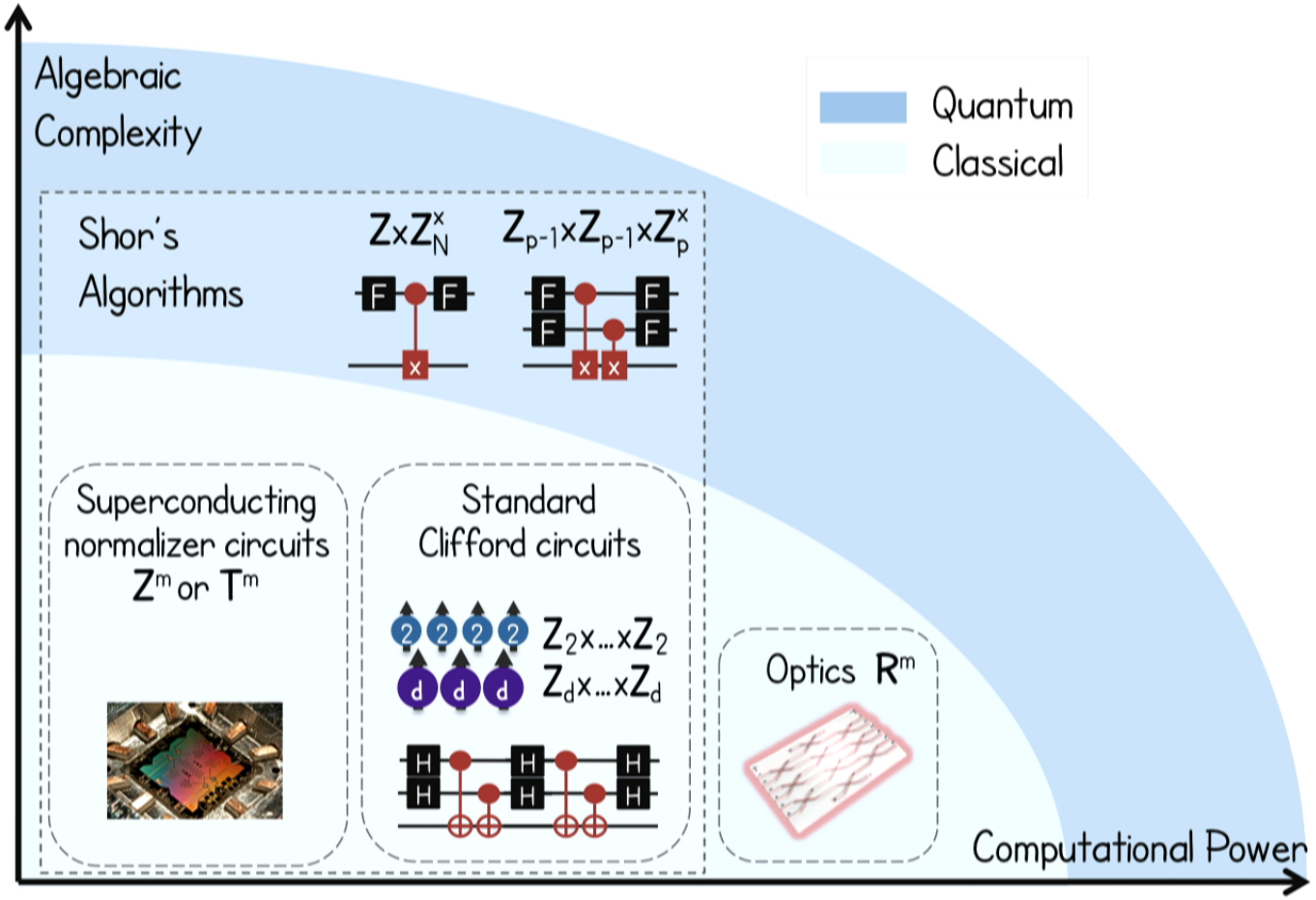
Emergence of Quantum Speed-Up



Emergence of Quantum Speed-Up

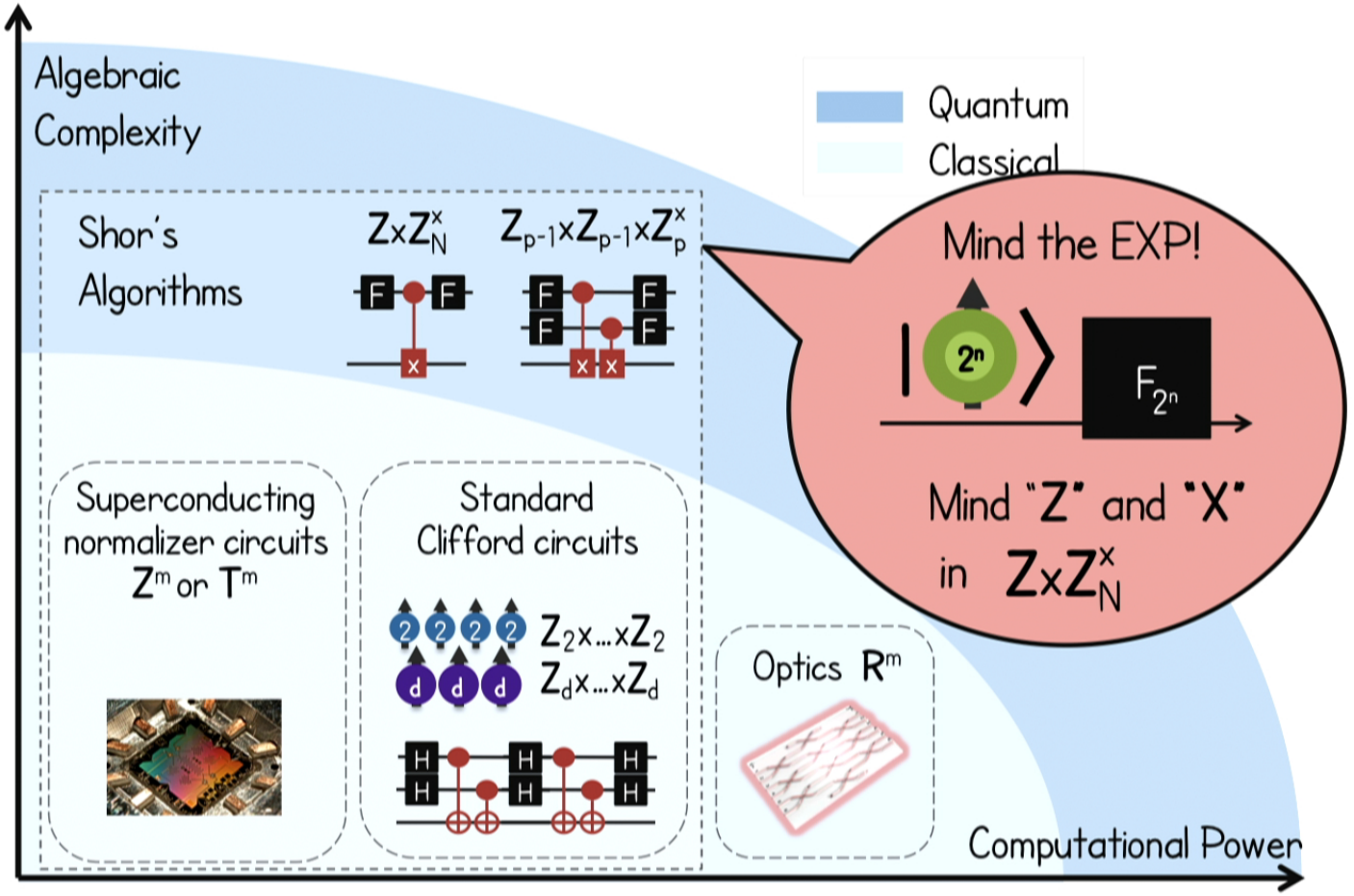


Emergence of Quantum Speed-Up



7

Emergence of Quantum Speed-Up



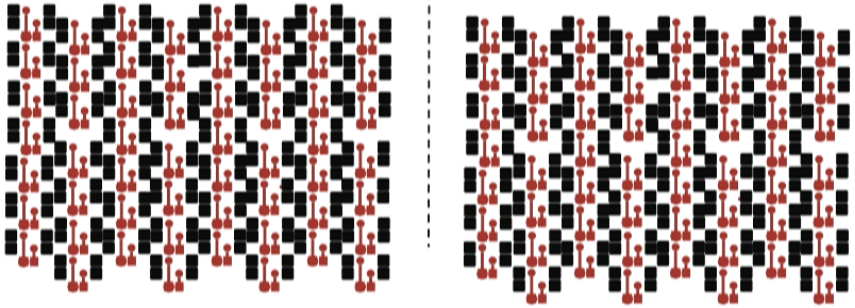
7

Classical Simulation Techniques

Analytical tools + efficient algorithms for

$G = R^a \times Z^b \times T^c \times Z_{D_1} \times \ldots \times Z_{D_d}$

$\psi = \int_H dx\, \psi(h) |h+s\rangle$ $\qquad$ $\psi(h) = e^{i\pi (h^T A h + b.h)}$



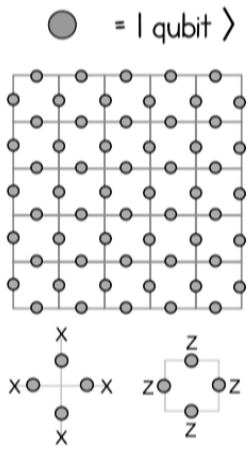
Finite groups -> **JBV**, Van den Nest, QIC 2014, arXiv:1210.3637

Discrete-compact groups -> **JBV**, Lin, Van den Nest, QIC 2016, arXiv:1409.3208

Real groups R^a ->**JBV**, Giedke (unpublished, cf. JBV's PhD Thesis)

Classical Simulation Techniques

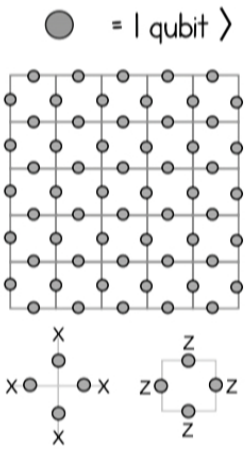
Stabilizer Code Formalism



Gottesman, PhD Thesis 1998
Aaronson, Gottesman, PRA, 2004

Classical Simulation Techniques

Stabilizer Code Formalism



+

Pauli Tracking

+

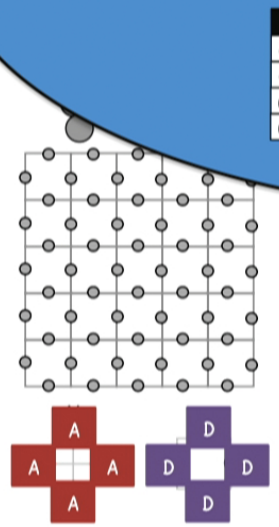
Gaussian Elimination

Gottesman, PhD Thesis 1998
Aaronson, Gottesman, PRA, 2004

SUBTLE

We exploit that Pauli operators are MONOMIAL

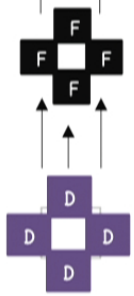
Van den Nest, NJP 2011, arXiv:1108.0531



Group Paulis

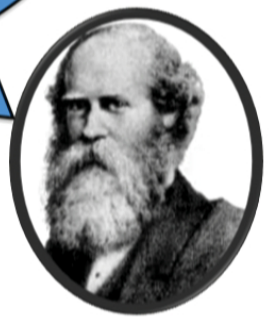
$X(g)|h\rangle = |g+h\rangle$

$Z(\chi)|h\rangle = \chi(h)|h\rangle$



Linear Encodings

$(g,\chi) = A_m \ldots A_2 A_1 G$



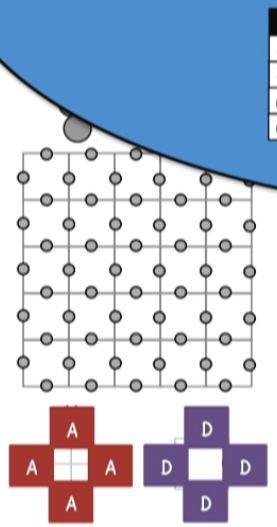
Storjohann, PhD Thesis 2000

* Smith Normal Forms
* Linear equations
  Ax=b over groups

SUBTLE

We exploit that Pauli operators are MONOMIAL

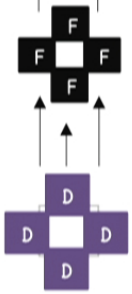
Van den Nest, NJP 2011, arXiv:1108.0531



Group Paulis

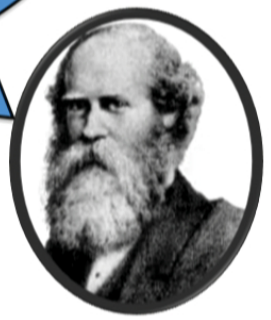
$X(g)|h\rangle = |g+h\rangle$

$Z(\chi)|h\rangle = \chi(h)|h\rangle$



Linear Encodings

$(g,\chi) = A_m \ldots A_2 A_1 G$



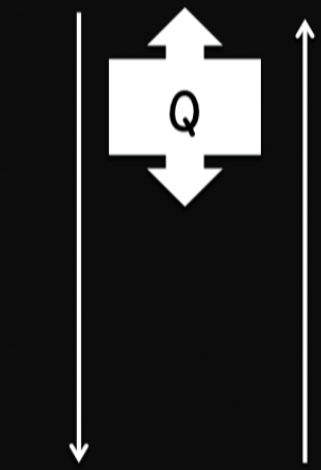
Storjohann, PhD Thesis 2000

* Smith Normal Forms
* Linear equations
  Ax=b over groups

Applications

New quantum algorithm

$G = \langle \alpha_1, \cdots, \alpha_m \rangle$

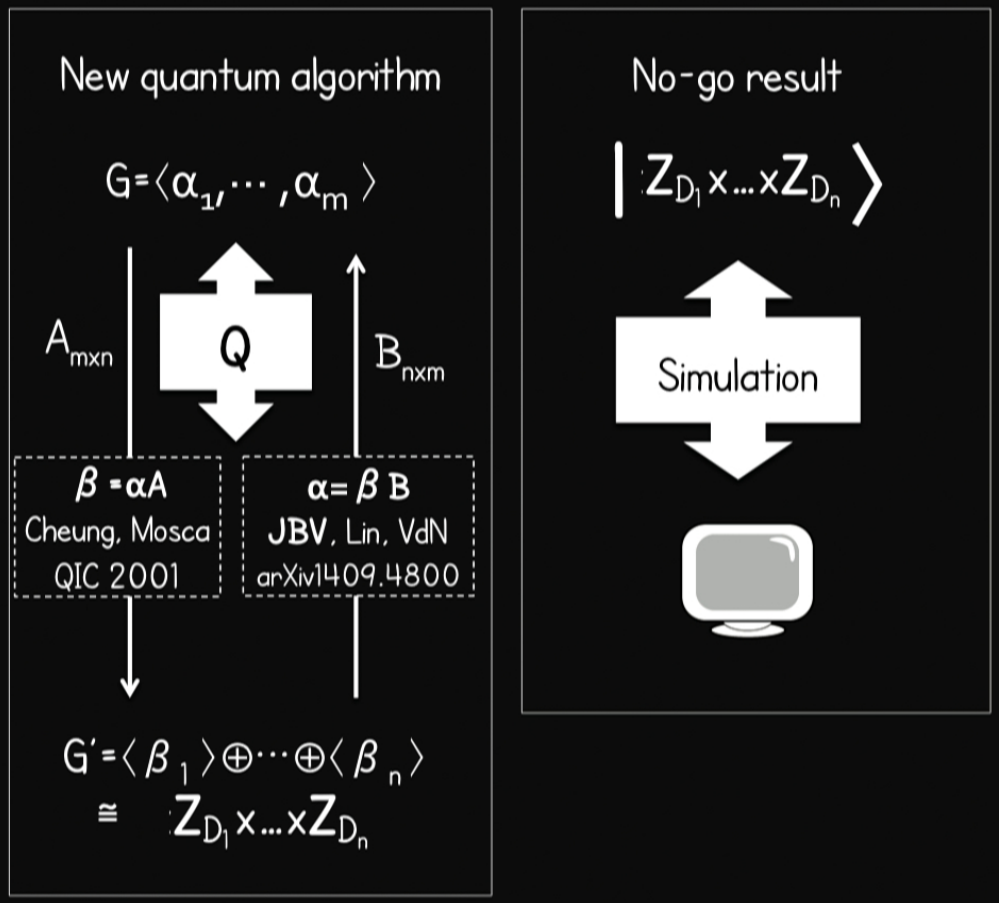


$G' = \langle \beta_1 \rangle \oplus \cdots \oplus \langle \beta_n \rangle$

$\cong Z_{D_1} \times \ldots \times Z_{D_n}$

Trade-offs

Applications



Trade-offs

Applications

New quantum algorithm

$G = \langle \alpha_1, \cdots, \alpha_m \rangle$

A_{mxn} — Q — B_{nxm}

$\beta = \alpha A$
Cheung, Mosca
QIC 2001

$\alpha = \beta B$
JBV, Lin, VdN
arXiv1409.4800

$G' = \langle \beta_1 \rangle \oplus \cdots \oplus \langle \beta_n \rangle \cong |Z_{D_1} x \ldots x Z_{D_n}\rangle$

No-go result

$|Z_{D_1} x \ldots x Z_{D_n}\rangle$

Simulation

Trade-offs

Bermejo-Vega, Van den Nest, QIC 2014, arXiv:1210.3637
Bermejo-Vega, Lin, Van den Nest, QIC 2016, arXiv:1409.3208

Applications

New quantum algorithm

$G=\langle \alpha_1, \cdots, \alpha_m \rangle$

A_{mxn} — Q — B_{nxm}

$\beta = \alpha A$
Cheung, Mosca
QIC 2001

$\alpha = \beta B$
JBV, Lin, VdN
arXiv1409.4800

$G' = \langle \beta_1 \rangle \oplus \cdots \oplus \langle \beta_n \rangle \cong |Z_{D_1} x \ldots x Z_{D_n}\rangle$

No-go result

$|Z_{D_1} x \ldots x Z_{D_n}\rangle$

Simulation

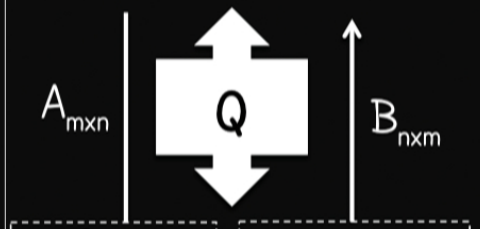
Trade-offs

Bermejo-Vega, Van den Nest, QIC 2014, arXiv:1210.3637
Bermejo-Vega, Lin, Van den Nest, QIC 2016, arXiv:1409.3208

Applications

New quantum algorithm

$G = \langle \alpha_1, \cdots, \alpha_m \rangle$



$\beta = \alpha A$
Cheung, Mosca
QIC 2001

$\alpha = \beta B$
JBV, Lin, VdN
arXiv1409.4800

$G' = \langle \beta_1 \rangle \oplus \cdots \oplus \langle \beta_n \rangle \cong Z_{D_1} \times \ldots \times Z_{D_n}$

Home Message

$|Z_{D_1} \times \ldots \times Z_{D_n}\rangle$

Normalizer circuits exhibit quantum speed-up*

$\Leftrightarrow$

underlying group G is BIG

group decomposition is unknown

=> Our measure of complexity

* (exponential and over known classical algorithsm)

Bermejo-Vega, Van den Nest, QIC 2014, arXiv:1210.3637
Bermejo-Vega, Lin, Van den Nest, QIC 2016, arXiv:1409.3208

Discussion: quantum computational resources

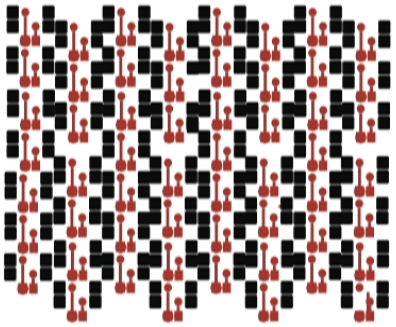
- Entanglement*, interference are quantum resources [Vidal PRL 03, Van den Nest QIC 11]
- In Clifford circuits both fail to provide a quantum speed-up
- How does this translate to normalizer circuits?

For entanglement

efficient simulability depends on knowledge of some classical data

Example:

"Shor's lasagna"



*As measured by the Schmidt rank.

Discussion: quantum computational resources

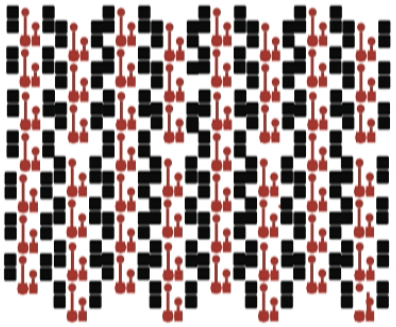
- Entanglement*, interference are quantum resources [Vidal PRL 03, Van den Nest QIC 11]
- In Clifford circuits both fail to provide a quantum speed-up
- How does this translate to normalizer circuits?

For entanglement

efficient simulability depends on knowledge of some classical data

Example:

"Shor's lasagna"



Interference

exploited only in "moderate" degrees in (some) FTF† circuits

Schwarz, Van den Nest, 1310.6749 [quant-ph]

*As measured by the Schmidt rank.

Discussion: quantum computational resources

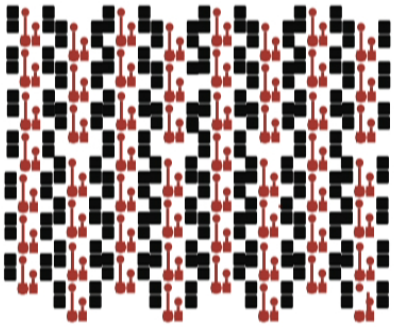
- Entanglement*, interference are quantum resources [Vidal PRL 03, Van den Nest QIC 11]
- In Clifford circuits both fail to provide a quantum speed-up
- How does this translate to normalizer circuits?

For entanglement

efficient simulability depends on knowledge of some classical data

Example:

"Shor's lasagna"

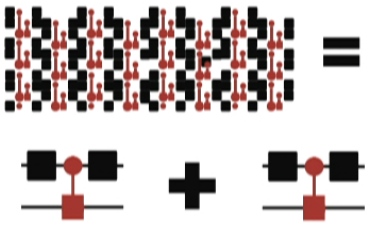


Interference

exploited only in "moderate" degrees in (some) FTF^{t} circuits

Schwarz, Van den Nest, 1310.6749 [quant-ph]

Conjecture: result extends to group normalizer circuits



*As measured by the Schmidt rank.

Discussion: quantum computational resources

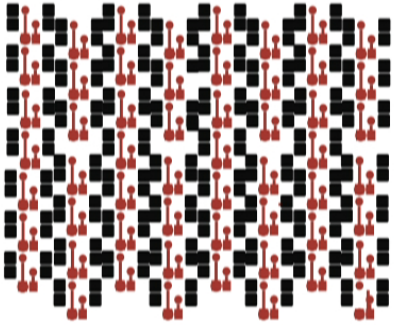
- Entanglement*, interference are quantum resources [Vidal PRL 03, Van den Nest QIC 11]
- In Clifford circuits both fail to provide a quantum speed-up
- How does this translate to normalizer circuits?

For entanglement

efficient simulability depends on knowledge of some classical data

Example:

"Shor's lasagna"

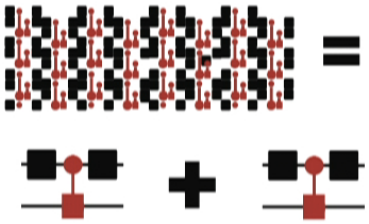


Interference

exploited only in "moderate" degrees in (some) FTF† circuits

Schwarz, Van den Nest, 1310.6749 [quant-ph]

Conjecture: result extends to group normalizer circuits



Contextuality of magic states

resource in odd dimensions, and *any* local dimension if it is not state-independent

[talk tomorrow in CNF]

Conjecture: this extends to group normalizer circuits

*As measured by the Schmidt rank.

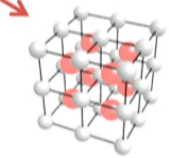
Part II

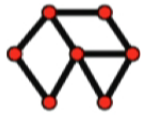
Normalizer circuits over commutative hyper-groups

Can we use similar techniques to find other new algorithms?

Standard approach -> non-commutative hidden symmetry problems

Hidden subgroup: f(gh)=f(g)

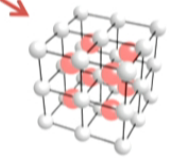




Can we use similar techniques to find other new algorithms?

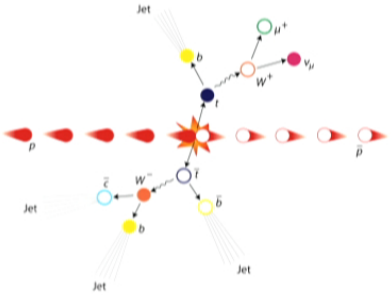
Standard approach -> non-commutative hidden symmetry problems

Hidden subgroup: f(gh)=f(g)



Different approach -> commutative hidden **hyper-symmetry** problems

JBV, Kevin Zatloukal, arXiv:1509.05806



Hypergroup Theory

Commutative Hypergroups:

commutative algebras with
a basis of "particle types"

Hypergroup Theory

Commutative Hypergroups:

commutative algebras with a basis of "particle types"

$a \times b = \sum_{c \in T} n_{ab}^{\ c} c$

c with probability $n_{ab}^{\ c}$

- Basis "T"
- Commutative: $ab = ba$
- Associative: $(ab)c = a(bc)$
- Vacuum (unit): $a \times 1 = a$
- Antiparticles: $n_{aa^*}^{\ 1} \neq 0$
- Weights: $w_a = 1/n_{aa^*}^{\ 1}$

Hypergroup Theory

Commutative Hypergroups:

commutative algebras with a basis of "particle types"

$a \times b = \sum_{c \in T} n_{ab}^{\ c} c$

c with probability $n_{ab}^{\ c}$

- Basis "T"
- Commutative: $ab = ba$
- Associative: $(ab)c = a(bc)$
- Vacuum (unit): $a \times 1 = a$
- Antiparticles: $n_{aa^*}^{\ 1} \neq 0$
- Weights: $w_a = 1/n_{aa^*}^{\ 1}$

Hypergroup Theory

Commutative Hypergroups:

commutative algebras with a basis of "particle types"

$a \times b = \sum_{c \in T} n_{ab}^{\ c} c$

c with probability $n_{ab}^{\ c}$

- Basis "T"
- Commutative: $ab = ba$
- Associative: $(ab)c = a(bc)$
- Vacuum (unit): $a \times 1 = a$
- Antiparticles: $n_{aa^*}^{\ 1} \neq 0$
- Weights: $w_a = 1/n_{aa^*}^{\ 1}$

Hypergroup Theory

Commutative Hypergroups:

commutative algebras with a basis of "particle types"

$a \times b = \sum_{c \in T} n_{ab}^{\ c} c$

c with probability $n_{ab}^{\ c}$

- Basis "T"
- Commutative: $ab = ba$
- Associative: $(ab)c = a(bc)$
- Vacuum (unit): $a \times 1 = a$
- Antiparticles: $n_{aa^*}^{\ 1} \neq 0$
- Weights: $w_a = 1/n_{aa^*}^{\ 1}$

Example 1: Anyons

(Fusion Categories)

$A \times B = \sum_{C \in T} N_{AB}^{\ C} C$

*Normalization

$a = A / d_A$

* Fusion constants

$n_{ab}^{\ c} = N_{AB}^{\ C} d_C / d_A d_B$

* Weights

$w_a = d_A^{\ 2}$

Example 2

Conjugacy classes & characters of finite group G

Class Hypergroup

$C_a = \sum_{g \in G} \frac{gag^{-1}}{|C_a|}$

$C_a C_b = \sum_c n_{ab}^{\ c} C_c$

Character Hypergroup

$X_\mu(C_a) = \psi_\mu(a)/d_\mu$

$X_\mu(C_a) X_\upsilon(C_a) = \sum_{c \in T} m_{\mu\upsilon}^{\ \gamma} X_\gamma(C_a)$

Hypergroup Characters

$X_\mu(C_a C_b) = X_\mu(C_a) X_\mu(C_b) = \sum_{c \in T} n_{ab}^{\ c} X_\mu(C_c)$

13

Hypergroup Theory

Commutative Hypergroups:

commutative algebras with a basis of "particle types"

$a \times b = \sum_{c \in T} n_{ab}^{\ c} c$

c with probability $n_{ab}^{\ c}$

- Basis "T"
- Commutative: $ab = ba$
- Associative: $(ab)c = a(bc)$
- Vacuum (unit): $a \times 1 = a$
- Antiparticles: $n_{aa^*}^{\ 1} \neq 0$
- Weights: $w_a = 1/n_{aa^*}^{\ 1}$

Example 1: Anyons

(Fusion Categories)

$A \times B = \sum_{C \in T} N_{AB}^{\ C} C$

*Normalization

$a = A / d_A$

* Fusion constants

$n_{ab}^{\ c} = N_{AB}^{\ C} d_C / d_A d_B$

* Weights

$w_a = d_A^{\ 2}$

Example 2

Conjugacy classes & characters of finite group G

Class Hypergroup

$C_a = \sum_{g \in G} \frac{gag^{-1}}{|C_a|}$

$C_a C_b = \sum_c n_{ab}^{\ c} C_c$

Character Hypergroup

$X_\mu(C_a) = \psi_\mu(a)/d_\mu$

$X_\mu(C_a) X_\upsilon(C_a) = \sum_{c \in T} m_{\mu\upsilon}^{\ \gamma} X_\gamma(C_a)$

Hypergroup Characters

$X_\mu(C_a C_b) = X_\mu(C_a) X_\mu(C_b) = \sum_{c \in T} n_{ab}^{\ c} X_\mu(C_c)$

13

A Hypergroup Stabilizer Formalism

arXiv:1509.05806

Hypergroup Paulis

$$X(a)|b\rangle = \sum_{b,c} \left(\frac{w_a}{w_b}\right)^{1/2} n_{ab}{}^{c} |c\rangle$$

$$Z(\chi_\alpha)|b\rangle = \chi_\alpha(b)\,|b\rangle$$

Abelian features

commute

$$X(a)X(b) = \sum_c n_{ab}{}^{c} X(c)$$

commute

$$Z(\chi_\alpha)Z(\chi_\beta) = \sum_\gamma m_{\alpha\beta}{}^{\gamma} Z(\chi_\gamma)$$

Hypergroup Stabilizer States

$$|\psi\rangle = \sum_{c \in bN} w_a^{1/2}\, \chi_\alpha(a)\,|a\rangle$$

Dual subhypergroups

N $\quad N^{\perp} = \{\chi_\alpha : \chi_\alpha(a)=1, \forall a \in N\}$

Stabilizer Hypergroups

$$S_X = \{ X(a) : a \in N \}$$

$$S_Z = \{ Z(\chi_\alpha) : \chi_\alpha \in N^{\perp} \}$$

A Hypergroup Stabilizer Formalism

arXiv:1509.05806

Hypergroup Paulis

$$X(a)|b\rangle = \sum_{b,c} \left(\frac{w_a}{w_b}\right)^{1/2} n_{ab}{}^{c} |c\rangle$$

$$Z(\chi_\alpha)|b\rangle = \chi_\alpha(b)\,|b\rangle$$

Abelian features

commute

$$X(a)X(b) = \sum_c n_{ab}{}^{c} X(c)$$

commute

$$Z(\chi_\alpha)Z(\chi_\beta) = \sum_\gamma m_{\alpha\beta}{}^{\gamma} Z(\chi_\gamma)$$

Hypergroup Stabilizer States

$$|\psi\rangle = \sum_{c \in bN} w_a^{1/2}\, \chi_\alpha(a)\,|a\rangle$$

Dual subhypergroups

N $\quad N^{\perp} = \{\chi_\alpha : \chi_\alpha(a) = 1, \forall a \in N\}$

Stabilizer Hypergroups

$$S_X = \{ X(a) : a \in N \}$$

$$S_Z = \{ Z(\chi_\alpha) : \chi_\alpha \in N^{\perp} \}$$

A Hypergroup Stabilizer Formalism

arXiv:1509.05806

Hypergroup Paulis

$$X(a)|b\rangle = \sum_{b,c} \left(\frac{w_a}{w_b}\right)^{1/2} n_{ab}{}^{c} |c\rangle$$

$$Z(\chi_\alpha)|b\rangle = \chi_\alpha(b)\,|b\rangle$$

Abelian features

commute

$$X(a)X(b) = \sum_c n_{ab}{}^{c} X(c)$$

commute

$$Z(\chi_\alpha)Z(\chi_\beta) = \sum_\gamma m_{\alpha\beta}{}^{\gamma} Z(\chi_\gamma)$$

Hypergroup Stabilizer States

$$|\psi\rangle = \sum_{c \in bN} w_a^{1/2}\, \chi_\alpha(a)\,|a\rangle$$

Dual subhypergroups

N $\quad N^{\perp} = \{\chi_\alpha : \chi_\alpha(a) = 1, \forall a \in N\}$

Stabilizer Hypergroups

$$S_X = \{ X(a) : a \in N \}$$

$$S_Z = \{ Z(\chi_\alpha) : \chi_\alpha \in N^{\perp} \}$$

A Hypergroup Stabilizer Formalism arXiv:1509.05806

Hypergroup Paulis

$$X(a)|b\rangle = \sum_{b,c} \left(\frac{w_a}{w_b}\right)^{1/2} n_{ab}{}^{c} |c\rangle$$

$$Z(X_\alpha)|b\rangle = X_\alpha(b)\,|b\rangle$$

Hypergroup Stabilizer States

$$|\psi\rangle = \sum_{c \in bN} w_a^{1/2}\, X_\alpha(a)\,|a\rangle$$

Dual subhypergroups

$N \quad N^{\perp} = \{X_\alpha : X_\alpha(a)=1, \forall a \in N\}$

Abelian features

commute

$$X(a)X(b) = \sum_c n_{ab}{}^{c} X(c)$$

commute

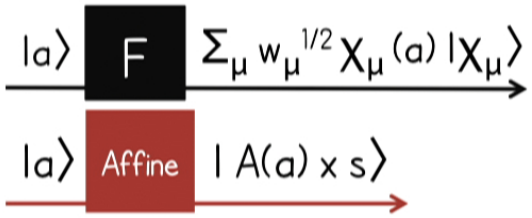
$$Z(X_\alpha)Z(X_\beta) = \sum_\Upsilon m_{\alpha\beta}{}^{\Upsilon} Z(X_\Upsilon)$$

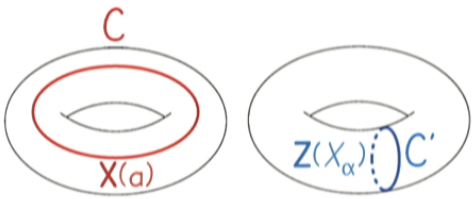
Stabilizer Hypergroups

$$S_X = \{ X(a) : a \in N\}$$

$$S_Z = \{Z(X_\alpha): X_\alpha \in N^{\perp}\}$$

Connection with "protected" (locality preserving) topological gates





Beverland, Buerschaper, Koenig, Pastawski, Preskill, Sijher; JMP (2016), arXiv:1409.3898

Alagic, Beverland, Bombín Benasque FTQT workshop (unpublished)

A Hypergroup Stabilizer Formalism arXiv:1509.05806

Hypergroup Paulis

$$X(a)|b\rangle = \sum_{b,c} \left(\frac{w_a}{w_b}\right)^{1/2} n_{ab}{}^{c} |c\rangle$$

$$Z(X_\alpha)|b\rangle = X_\alpha(b)\,|b\rangle$$

Hypergroup Stabilizer States

$$|\psi\rangle = \sum_{c \in bN} w_a^{1/2}\, X_\alpha(a)\,|a\rangle$$

Dual subhypergroups

$N \quad N^{\perp} = \{X_\alpha : X_\alpha(a)=1, \forall a \in N\}$

Abelian features

commute

$$X(a)X(b) = \sum_c n_{ab}{}^{c} X(c)$$

commute

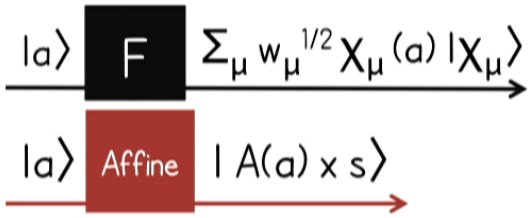
$$Z(X_\alpha)Z(X_\beta) = \sum_\gamma m_{\alpha\beta}{}^{\gamma} Z(X_\gamma)$$

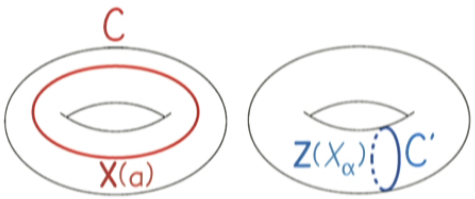
Stabilizer Hypergroups

$$S_X = \{ X(a) : a \in N \}$$

$$S_Z = \{ Z(X_\alpha) : X_\alpha \in N^{\perp} \}$$

Connection with "protected" (locality preserving) topological gates





Beverland, Buerschaper, Koenig, Pastawski, Preskill, Sijher; JMP (2016), arXiv:1409.3898

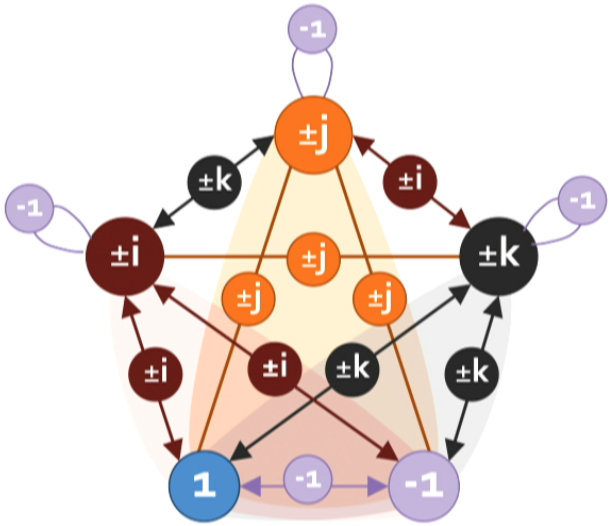
Alagic, Beverland, Bombín Benasque FTQT workshop (unpublished)

Example
Quaternion Anyons

Particles are conjugacy classes of the finite group

$Q_8 = \langle -1, i, j, k \mid (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1 \rangle$

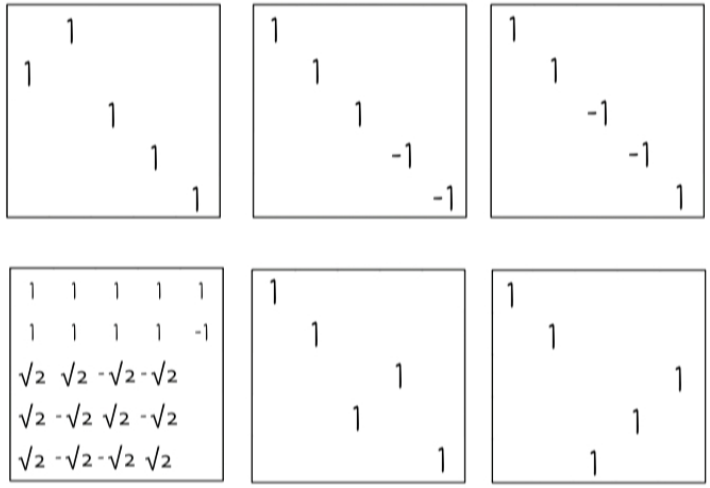
Multiplication "hyper-table"



Quaternionic Clifford gates

Act on qudits with basis
$|1\rangle, |-1\rangle, |i\rangle, |j\rangle, |k\rangle$

Quaternionic gates are different from the usual qudit Clifford gates!

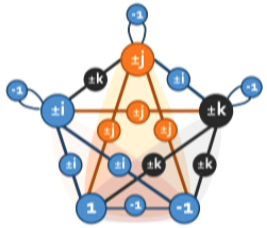


Examples of entangling gates are given in arXiv:1509.05806

Abelian Hidden Subhypergroup Problem (HSHP)

Find subhypergroup H given f: $f(a)=f(b) \Leftrightarrow a \times h = \sum_c n_{ah}^{\ b}\, b$ for h in H

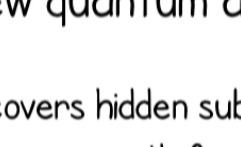
Nonabelian subhypergroup

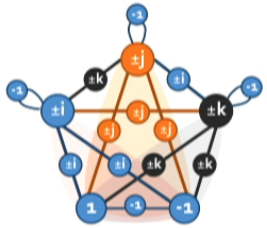


Abelian Hidden Subhypergroup Problem (HSHP)

Find subhypergroup H given f: $f(a)=f(b) \iff a \times h = \sum_c n_{ah}^{\ b}\, b$ for h in H

Nonabelian subhypergroup



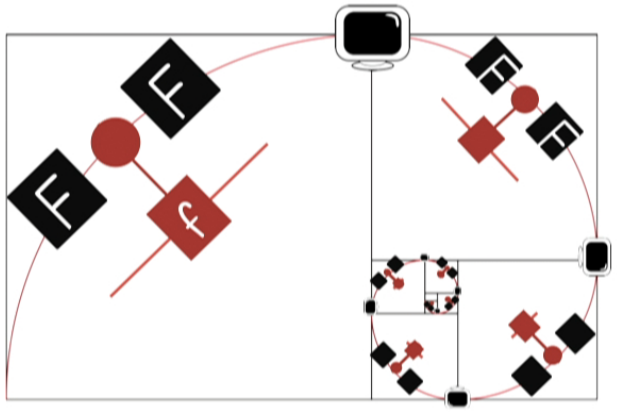


Conjecture
This problem is easier than the nonabelian HSP

New quantum algorithm arXiv:1509.05806

* Recovers hidden subhypergroup efficiently for hypergroups with factor series
$\{1\} < T_1 < \ldots < T_n = T$ with T_{i+1}/T_i a group.

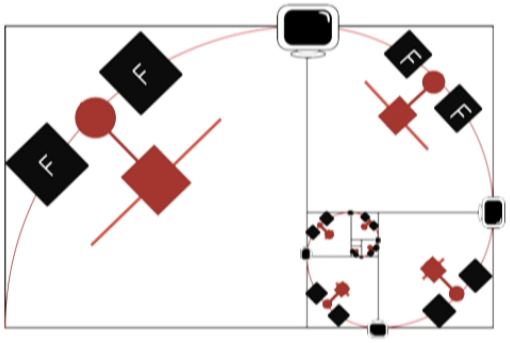
* Efficient for class hypergroups where the group HSP is hard (nilpotent groups, dihedral groups)



Hallgren-Russell-Ta-Shma's, STOC 2000
Amini-Kalantar-Roozbehani, quant-ph/0609220

15

Summary



1. Formalism of restricted quantum circuits
2. Simulation techniques
3. Emergence of quantum speed-ups
4. Quantum algorithms
5. Connections to stabilizer formalism

Open Questions

1. Can we study the emergence of more kinds of quantum speed-ups? What methods need to be developed?
   Hope: non-univerfsal circuit families (matchgates, IQP, boson samplers, etc)

2. Find applications of our quantum algorithms.
   Hope: quantum field theory, cryptography.

3. (In connection with talk tomorrow.) Apply formalism to understand contextuality as a computational resource.

Beyond quantum algorithms

4. Find error-correcting hypergroup stabilizer codes?
5. Improve our hypergroup Gottesman-Knill theorem.
6. Understand connection with protected gates.