Classification of Sub-Universal Quantum Gatesets

Rachel Castro, Alexey Slizkov

Tufts University

December 26, 2025

Outline

Question

When do sub-universal quantum gatesets admit efficient classical simulation? How can we classify them?

Gottesman-Knill

Theorem 1 (Gottesman-Knill '98)

A quantum circuit comprised of the following:

- *Preparation of qubits in the computational basis*
- *Clifford gates*
- *Measurement in the computational basis*

can be simulated efficiently on a classical computer. *[Gottesman, 1998]*

Gottesman-Knill

Theorem 1 (Gottesman-Knill '98)

A quantum circuit comprised of the following:

- *Preparation of qubits in the computational basis*
- *Clifford gates*
- *Measurement in the computational basis*

can be simulated efficiently on a classical computer. *[Gottesman, 1998]*

Matchgates are also easy to compute on classical computers.
[Valiant, 2001]

Gottesman-Knill

Theorem 1 (Gottesman-Knill '98)

A quantum circuit comprised of the following:

- *Preparation of qubits in the computational basis*
- *Clifford gates*
- *Measurement in the computational basis*

can be simulated efficiently on a classical computer. *[Gottesman, 1998]*

Matchgates are also easy to compute on classical computers.
[Valiant, 2001]
So what else is easy, and how can we find it?

Quantum Gateset Universality

Definition 2 (Universal Gateset)

A set G of quantum gates is **universal** in one qubit if it generates a dense subgroup of $SU(2)$.

Quantum Gateset Universality

Definition 2 (Universal Gateset)

A set G of quantum gates is **universal** in one qubit if it generates a dense subgroup of $SU(2)$.

- What is $SU(2)$?

Quantum Gateset Universality

Definition 2 (Universal Gateset)

A set G of quantum gates is **universal** in one qubit if it generates a dense subgroup of $SU(2)$.

- What is $SU(2)$?
  - Special unitary group: $SU(2) \subset U(2) \subset GL_2(\mathbb{C})$.
  - (Note, we usually consider $SU(2)\ /\mathbb{Z}_2$, which happens to be isomorphic to $SO(3)$ via the so-called "double-cover isomorphism".)
- What is a dense subgroup?

Quantum Gateset Universality

Definition 2 (Universal Gateset)

A set G of quantum gates is **universal** in one qubit if it generates a dense subgroup of $SU(2)$.

- What is $SU(2)$?
  - Special unitary group: $SU(2) \subset U(2) \subset GL_2(\mathbb{C})$.
  - (Note, we usually consider $SU(2)\ /\mathbb{Z}_2$, which happens to be isomorphic to $SO(3)$ via the so-called "double-cover isomorphism".)
- What is a dense subgroup?
  - If H is a subgroup of G, then $\overline{H} = G$ implies H is dense in G.
  - ie, for any sequence of matrices in H, its limit is in G, and there are no points in G that are not either in H or a limit point of H.
  - $\overline{(\mathbb{Q}, +)} = (\mathbb{R}, +)$

Bloch Sphere

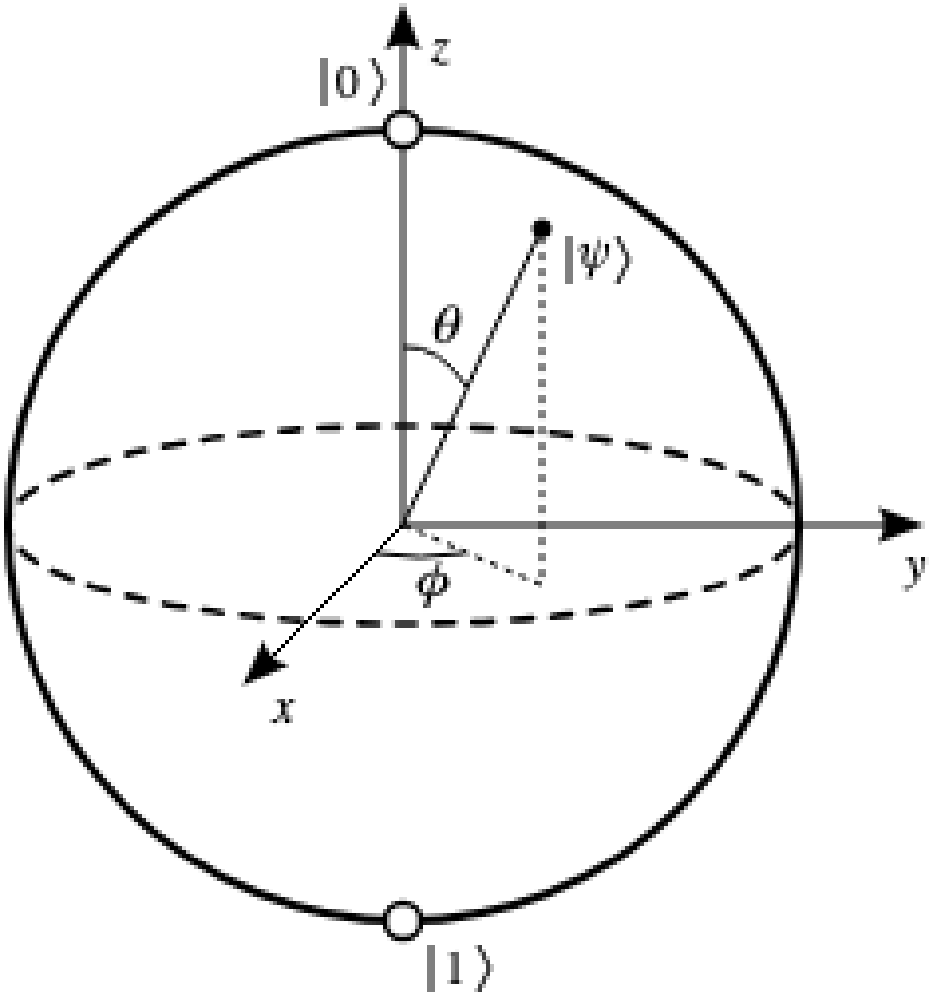
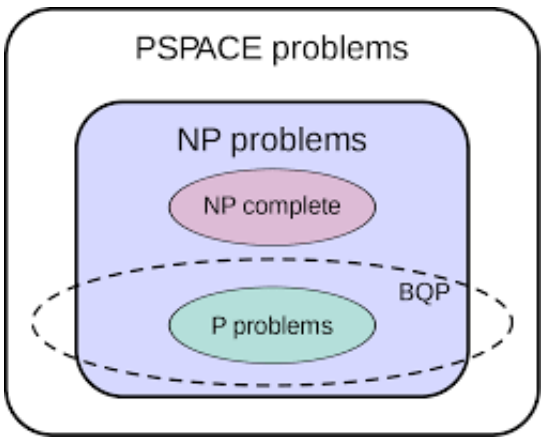


Figure 1: Bloch Sphere

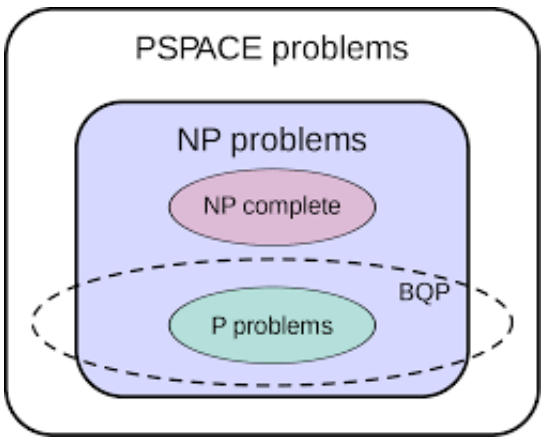
BQP and P

- Rachel believes and Alexey would like it to be known he does not see evidence either way regarding $BQP \nsubseteq P$, so generic quantum circuits likely cannot be easily simulated on classical computers.



BQP and P

- Rachel believes and Alexey would like it to be known he does not see evidence either way regarding $BQP \nsubseteq P$, so generic quantum circuits likely cannot be easily simulated on classical computers.



- Any subgroup that is not dense is not universal, and might be easier to simulate classically.
- How might we classify these sub-universal gatesets?

Boolean Classification

As it turns out, researchers have been trying to classify sub-universal computation for a long time...

Figure 2: Emil Post circa 1940s

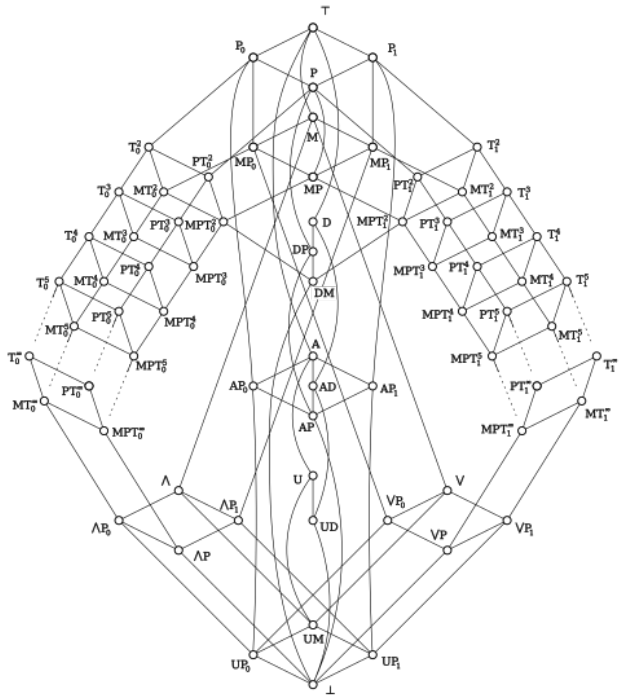


Figure 3: ...and his lattice ('41)

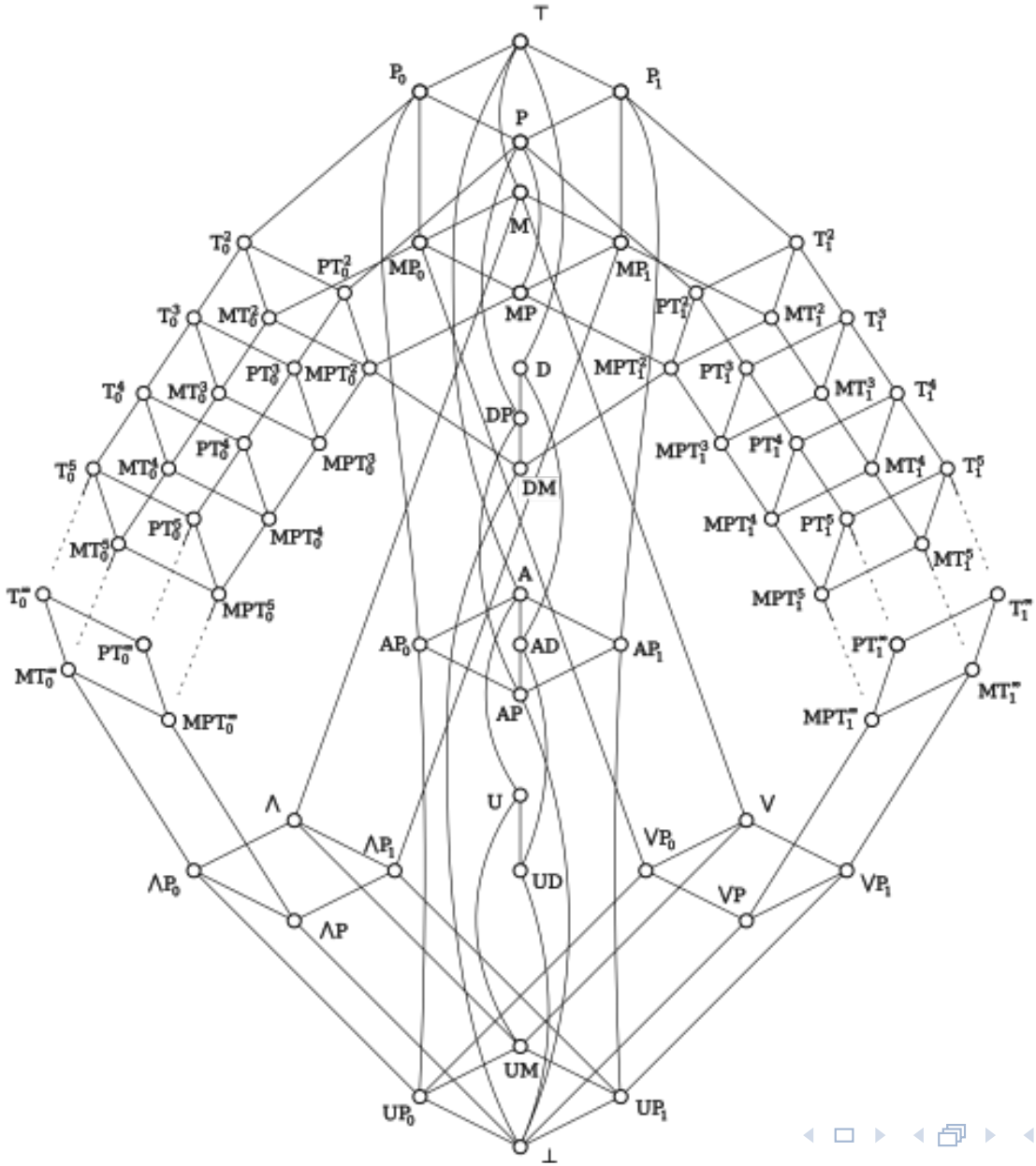
Post's Lattice Continued

- A **clone** is a set of Boolean functions closed under generalized composition, where you can substitute any variable into any argument, including repetitions

Post's Lattice Continued

- A **clone** is a set of Boolean functions closed under generalized composition, where you can substitute any variable into any argument, including repetitions
- The 5 *maximal (proper) clones* famously are:
  - Affine functions (over $\mathbb{F}_2$). Interestingly, this class exists in the generalization of Post's lattice to arbitrary finite domains if and only if the domain size is a prime power, due to the existence of a field of that size
  - 0-preserving ($f(0, 0, \ldots, 0) = 0$) and 1-preserving functions
  - Self-dual ($f(x_1, \ldots, x_n) = \neg f(\neg x_1, \ldots, \neg x_n)$)
  - Monotone functions $x \leq y \implies f(x) \leq f(y)$
- Surprisingly, there exists a complete classification of all clones (not just the maximal ones) of Boolean functions: two countable families and a few dozen exceptions:

An easier picture



More Recently...

- This is a classical direction, there's a lot more known in this direction, but also some questions are still open
- Since the 90s, researchers have been trying to extend this result to quantum computing.

More Recently...

- This is a classical direction, there's a lot more known in this direction, but also some questions are still open
- Since the 90s, researchers have been trying to extend this result to quantum computing.
- Aaronson, Grier, and Schaeffer [Aaronson et al., 2015] classified all classical reversible bit operations.

More Recently...

- This is a classical direction, there's a lot more known in this direction, but also some questions are still open
- Since the 90s, researchers have been trying to extend this result to quantum computing.
- Aaronson, Grier, and Schaeffer [Aaronson et al., 2015] classified all classical reversible bit operations.
- Grier and Schaeffer [Grier and Schaeffer, 2022] continued their work to partition all Clifford gates on n qubits into 57 classes.



Classification of Clifford Gates over Qubits

Definition 3 (Clifford Gateset)

The Clifford group on n qubits normalizes the Pauli group of n-length Pauli strings in $SU(2^n)$.
That is, $C \in \mathcal{C}$ iff $\exists P \in \mathcal{P}^n$ such that:

$$CPC^\dagger \in \mathcal{P}$$

Where $\mathcal{P}^n = \pm\{I, X, Y, Z\}^{\otimes n}$
Generators of this group include $\{S, H, CNOT\}$, $\{R_X, R_Z\}$, $\{H, CZ, X, Z\}$

Classification of Clifford Gates over Qubits

Definition 3 (Clifford Gateset)

The Clifford group on n qubits normalizes the Pauli group of n-length Pauli strings in $SU(2^n)$.
That is, $C \in \mathcal{C}$ iff $\exists P \in \mathcal{P}^n$ such that:

$$CPC^\dagger \in \mathcal{P}$$

Where $\mathcal{P}^n = \pm\{I, X, Y, Z\}^{\otimes n}$
Generators of this group include $\{S, H, CNOT\}$, $\{R_X, R_Z\}$, $\{H, CZ, X, Z\}$

Classification of Clifford Gates over Qubits

Definition 3 (Clifford Gateset)

The Clifford group on n qubits normalizes the Pauli group of n-length Pauli strings in $SU(2^n)$.
That is, $C \in \mathcal{C}$ iff $\exists P \in \mathcal{P}^n$ such that:

$$CPC^\dagger \in \mathcal{P}$$

Where $\mathcal{P}^n = \pm\{I, X, Y, Z\}^{\otimes n}$
Generators of this group include $\{S, H, CNOT\}$, $\{R_X, R_Z\}$, $\{H, CZ, X, Z\}$

There are 57 total classes, 30 "degenerate". The remaining 27 are more interesting.

Closure

Definition 4 (Closure)

A class $\mathcal{C}$ of Clifford gates is **closed** under the following (for $f, g \in \mathcal{C}$)

1. Composition: $f \circ g \in \mathcal{C}$
2. Tensor Product: $f \otimes g \in \mathcal{C}$
3. SWAP
4. Arbitrary ancilla (no magic states): if $f \in \mathcal{C}, \exists h \in \mathcal{C}, \exists \left|\psi\right\rangle$ such that:

$$f(\left|x\right\rangle \otimes \left|\psi\right\rangle) = g(\left|x\right\rangle) \otimes \left|\psi\right\rangle, \forall x$$

It follows that $\mathcal{C}$ is closed under inverse and that $I \in \mathcal{C}$.

Lattice

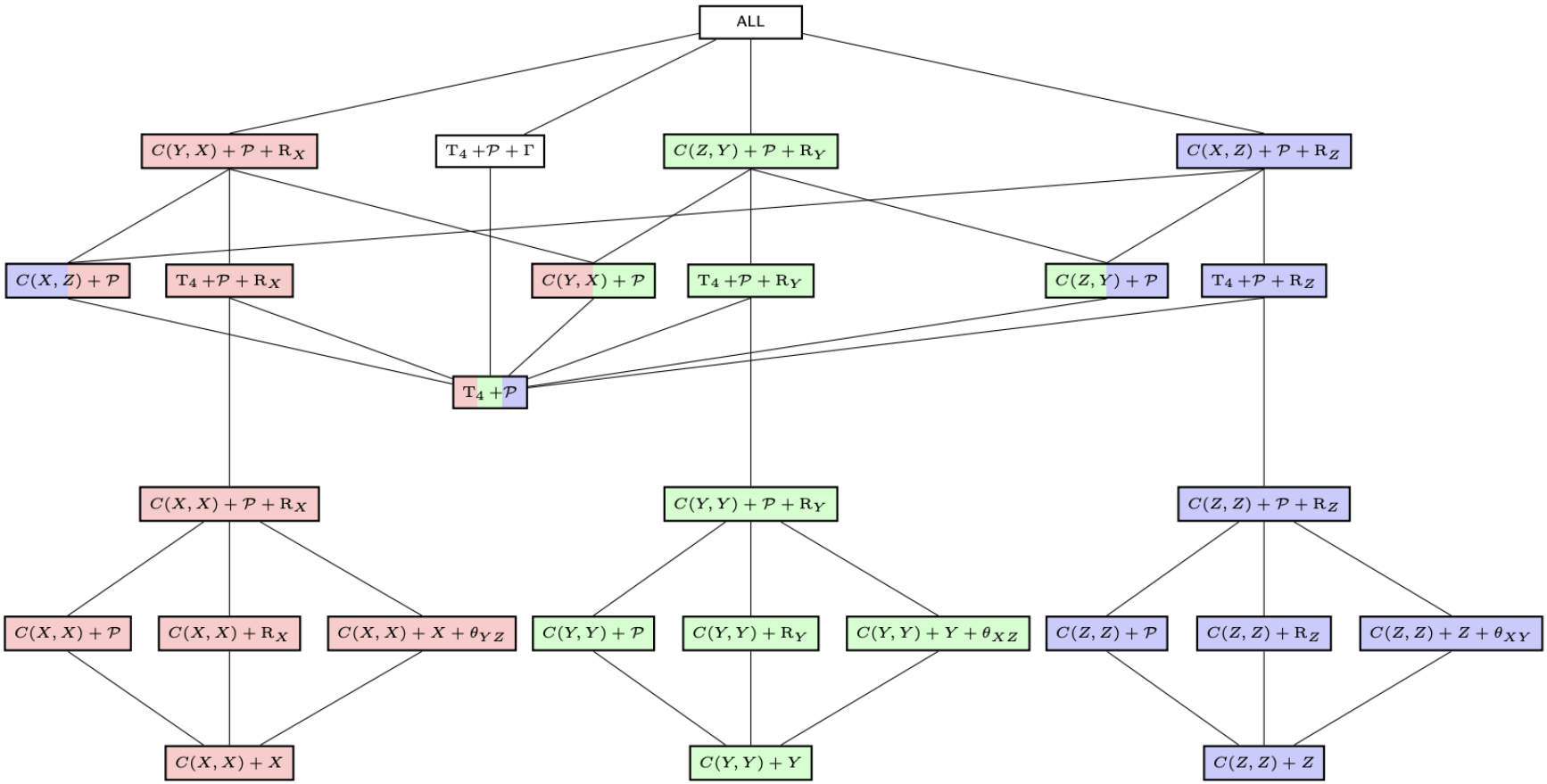


Figure 2: The inclusion lattice of non-degenerate Clifford gate classes. Red, green, blue denote X-, Y-, and Z-preserving, respectively.

More Classification

So how do we actually distinguish these classes?

More Classification

So how do we actually distinguish these classes? Invariants!

- X, Y, Z Preserving - mapping basis states to themselves
  - ex: $X, CNOT, T_4$ are Z-preserving.
- "Degenerate" - each input effects exactly one output
  - All degenerates are generated by single-qubit gates and $SWAP$.
- X, Y, Z "Degenerate" - flipping any bit in the related basis input flips exactly one bit of the output.
  - ex: R_Z, $\mathcal{P}$
- X, Y, Z "Orthogonal" - built from Z-preserving gates and T_4
- "Egalitarian" - symmetric across bases
  - ex: Γ, T_4

Our Work So Far

- We are trying to understand how non-dense subgroups of $SU(2)/\mathbb{Z}_2 \cong SO(3) \cong PU(2)$ and $SU(4)/\text{Phase} \cong PU(4)$ are classified.

SO(3)

- For $SO(3)$, there's a technique based on the counting of pairs (g, p) s.t. $g \in G \backslash \{1\}$ fixes p. It turns out that $SO(3)$ has a complete classification of (maximal) finite subgroups:
  - Dihedral groups D_n of arbitrary order – rotate around an axis and allow flipping,
  - S_4 – because it's the symmetry group of a cube/octahedron,
  - even A_5 – the symmetry group of an isocahedron/dodecahedron.

Figure 4: Octahedron and cube are duals

SU(2)

- In representation theory, there's a known surjective homomorphism $\Phi\colon SU(2) \to SO(3)$, s.t. $SU(2)/SO(3) \cong \mathbb{Z}_2$. It's called the double cover homomorphism, because $\forall y \in SO(3)\ |\Phi^{-1}(y)| = 2$
- It's very useful for studying SU(2), because you can employ a lot of geometric insights to study SO(3), and then lift your results through this homomorphism
- Note: The homomorphism Φ is actually the action of $SU(2)$ on $\mathrm{Span}_{\mathbb{R}}(i\sigma_x, i\sigma_y, i\sigma_z)$ by conjugations
- Using this techniques, one can classify maximal subgroups of $SU(2)$:
  - binary dihedral groups $\mathcal{BD}_n$ of arbitrary order
  - the binary cube/octahedral group $\mathcal{BO}$
  - the binary dodecahedron/icosahedron group $\mathcal{BI}$

SU(¿2), SO(¿3)

- The double cover homomorphism no longer exists to aide us to understand one group through another
- In 4 dimensions, there are 6 regular polyhedra, including one with 1200 faces!
- Though to be fair, it's also known that for 5d+, there are only two (the symplex and the cube)
- Compared to the 2-dimensional $PU(2)$, $PU(4)$ is 14-dimensional, making the involved geometric structure slightly more involved

Conclusion

We are investigating what connection there is, if any, between group structure of sub-universal quantum gates and easy classical simulation.

- We saw the Gottesman-Knill and Valiant results
- We discussed how gatesets have been classified in classical computing
- We followed the attempts to extend these results into quantum computing
- We saw the areas of future work to continue classifying quantum gatesets

References I


Aaronson, S., Grier, D., and Schaeffer, L. (2015).
The classification of reversible bit operations.


Gottesman, D. (1998).
The heisenberg representation of quantum computers.


Grier, D. and Schaeffer, L. (2022).
The classification of clifford gates over qubits.


Valiant, L. G. (2001).
Quantum circuits that can be simulated classically in polynomial time.
In *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing (STOC'01)*, pages 114–123.