CANA seminar
September 16th, 2025

Optimal exploration of locally-generated permutations and application to combinatorial optimization

Dylan Laplace Mermoud, Sourour Elloumi, Andrea Simonetto

arXiv:2505.05981

With the support of

FMJH PGMO: P-2023-0009

ANR: HQI-ANR-22-PNCQ-0002

Outline of the presentation

Goal of this work:

- We are given a set of *primitive permutations* $\{\mathtt{x}, \mathtt{cx}\}$ that can be 'on' or 'off'.

Outline of the presentation

Goal of this work:

- We are given a set of *primitive permutations* $\{\mathtt{x}, \mathtt{cx}\}$ that can be 'on' or 'off'.
- Using *only* these gates, how can we design a circuit that can reach *all possible permutations*, while keeping its *depth* and *size* as small as possible?

Outline of the presentation

Goal of this work:

- We are given a set of *primitive permutations* $\{\mathtt{x}, \mathtt{cx}\}$ that can be 'on' or 'off'.
- Using *only* these gates, how can we design a circuit that can reach *all possible permutations*, while keeping its *depth* and *size* as small as possible?

How we did it:

- First, we need to understand the *group* generated by these primitives gates;
- Then, to decompose it into groups that we can *translate* into circuits.

Outline of the presentation

Goal of this work:

- We are given a set of *primitive permutations* $\{\mathtt{x}, \mathtt{cx}\}$ that can be 'on' or 'off'.
- Using *only* these gates, how can we design a circuit that can reach *all possible permutations*, while keeping its *depth* and *size* as small as possible?

How we did it:

- First, we need to understand the *group* generated by these primitives gates;
- Then, to decompose it into groups that we can *translate* into circuits.

Then:

- We use these to solve combinatorial optimization problems on permutations.

Optimizing over the permutations: quadratic assignment problems

- We are interested in the approximate resolution of *quadratic assignment problems*:

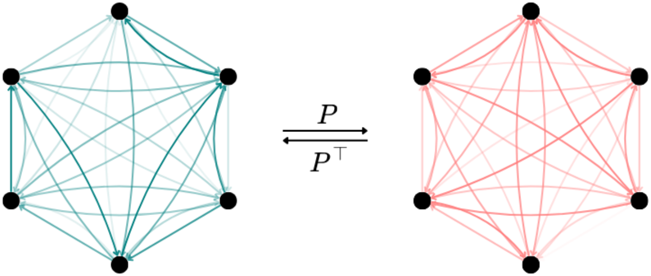


Figure: A 6-vertex instance of QAP.

Optimizing over the permutations: quadratic assignment problems

▷ We are interested in the approximate resolution of *travelling salesperson problems*:

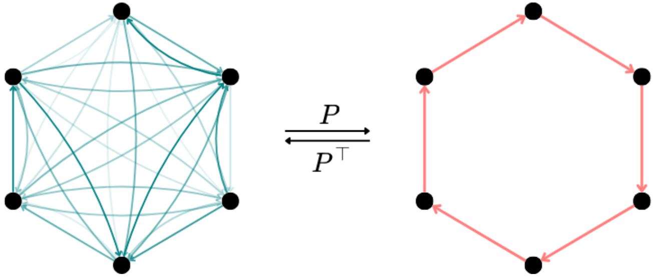


Figure: A 6-vertex instance of TSP.

Optimizing over the permutations: quadratic assignment problems

▷ We are interested in the approximate resolution of *heaviest k-subgraph problems*:

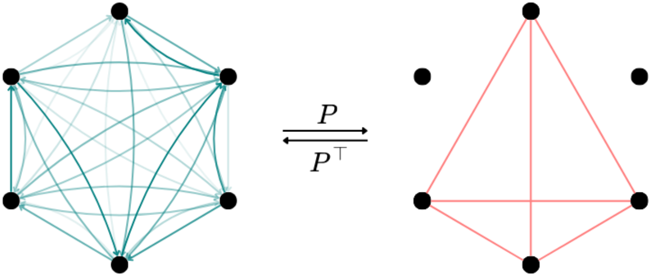


Figure: A 6-vertex instance of heaviest 4-subgraph problem.

Optimizing over the permutations: quadratic assignment problems

- We are interested in the approximate resolution of *graph isomorphism problems*:

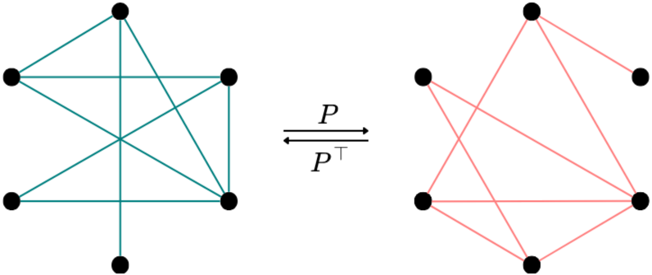


Figure: A 6-vertex instance of GIP.

Combinatorial view of groups

A group is fully characterized by

- a set of *generators* $S = \{s_1, \ldots, s_n\}$, from which groups elements are written, as *words of generators*;

Combinatorial view of groups

A group is fully characterized by

- a set of *generators* $S = \{s_1, \ldots, s_n\}$, from which groups elements are written, as *words of generators*;
- a set of *relators* R, which are words of generators that are equal to the identity (the empty word).

Combinatorial view of groups

A group is fully characterized by

- a set of *generators* $S = \{s_1, \ldots, s_n\}$, from which groups elements are written, as *words of generators*;
- a set of *relators* R, which are words of generators that are equal to the identity (the empty word).

A group G defined by a set of generators S and relators R is denoted by $G = \langle S \mid R \rangle$, and this is called a *presentation* of G.

Combinatorial view of groups

Example: The *dihedral group D_N*: group of symmetries of regular N-gons.

- A set of generators is

$$S = \{r, f\}.$$

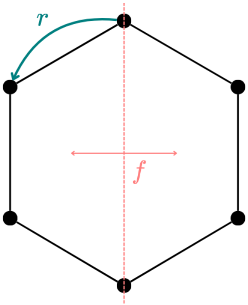


Figure: A regular hexagon and some of its symmetries.

Combinatorial view of groups

Example: The *dihedral group D_N*: group of symmetries of regular N-gons.

- A set of generators is

$$S = \{r, f\}.$$

- A corresponding set of relators is

$$R = \left\{ r^N, f^2, (rf)^2 \right\}.$$

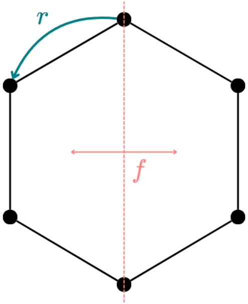


Figure: A regular hexagon and some of its symmetries.

Combinatorial view of groups

Example: The *dihedral group D_N*: group of symmetries of regular N-gons.

- A set of generators is

$$S = \{r, f\}.$$

- A corresponding set of relators is

$$R = \left\{r^N, f^2, (rf)^2\right\}.$$

- So, we have

$$D_N = \left\langle r, f \mid r^N, f^2, (rf)^2 \right\rangle = \mathbb{Z}_N \rtimes \mathbb{Z}_2.$$

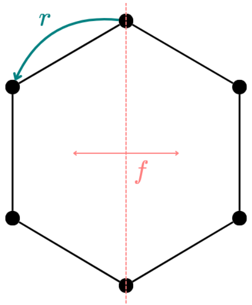


Figure: A regular hexagon and some of its symmetries.

Combinatorial view of quantum circuits

In our case, we have the following set of generators

$$S_q = \{\mathtt{x}_j, \mathtt{cx}_{kl} \mid 1 \leq j, k, l \leq q, k \neq l\}.$$

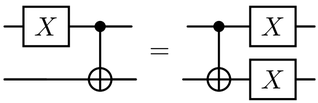
Denote by LX_q the group generated by S_q. What is R_q such that $LX_q = \langle S_q \mid R_q \rangle$?

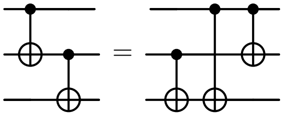
Combinatorial view of quantum circuits

In our case, we have the following set of generators

$$S_q = \{\mathtt{x}_j, \mathtt{cx}_{kl} \mid 1 \leq j, k, l \leq q, k \neq l\}.$$

Denote by LX_q the group generated by S_q. What is R_q such that $LX_q = \langle S_q \mid R_q \rangle$?





How to decompose LX_q?

- We want to study the two following groups individually:
  - X_q, generated by the gates $\{\mathtt{x}_j \mid 1 \leq j \leq q\}$;
  - CX_q, generated by the gates $\{\mathtt{cx}_{kl} \mid 1 \leq k, l \leq q, k \neq l\}$.

How to decompose LX_q?

- We want to study the two following groups individually:
  - X_q, generated by the gates $\{\mathtt{x}_j \mid 1 \leq j \leq q\}$;
  - CX_q, generated by the gates $\{\mathtt{cx}_{kl} \mid 1 \leq k, l \leq q, k \neq l\}$.

- Fortunately, they fit together nicely as in the dihedral group.

How to decompose LX_q?

- We want to study the two following groups individually:
  - X_q, generated by the gates $\{\mathtt{x}_j \mid 1 \leq j \leq q\}$;
  - CX_q, generated by the gates $\{\mathtt{cx}_{kl} \mid 1 \leq k, l \leq q, k \neq l\}$.
- Fortunately, they fit together nicely as in the dihedral group.

Proposition

The group LX_q decomposes as $X_q \rtimes CX_q$.

- Hence, from the presentations of X_q and CX_q we deduce the one of LX_q.

How to decompose LX_q?

Proposition

The group LX_q decomposes as $X_q \rtimes CX_q$.

- Hence, from the presentations of X_q and CX_q we deduce the one of LX_q.

Corollary

Any quantum circuit $\mathcal{C}$ composed solely of `x` and `cx` gates can be decomposed into into two circuits $\mathcal{C}_X$ and $\mathcal{C}_{CX}$, respectively composed only of `x` and `cx` gates, such that

$$\mathcal{C} = \mathcal{C}_X \mathcal{C}_{CX}.$$

The structure of the group X_q

- Any $\mathtt{x}$ gate applies to a *unique* qubit.
- So, all gates *commute*, and X_q is abelian.
- Hence, $X_q \simeq \mathbb{Z}_2^q$ and

$$X_q = \left\langle \mathtt{x}_j, 1 \leq j \leq q \mid \left(\mathtt{x}_j \mathtt{x}_k\right)^2, 1 \leq j, k \leq q \right\rangle.$$

The structure of the group CX_q

Definition

The *general linear group* of degree n over the ring R, denoted by $\mathrm{GL}_n(R)$ is the set of $n \times n$ invertible matrices with entries in R, together with the usual matrix product.

Theorem (Bataille, 2022)

The group CX_q is isomorphic to $\mathrm{GL}_q(\mathbb{Z}_2)$.

The structure of the group CX_q

Corollary (of Steinberg, 1968 and Bataille, 2022)

If $q \geq 3$, a presentation of CX_q is given by the set of generators

$$\{\mathtt{cx}_{kl} \mid 1 \leq k, l \leq q, k \neq l\},$$

and the following set of relations:

$$\begin{aligned} &\mathtt{cx}_{kl}^2, && \\ &(\mathtt{cx}_{kl}\mathtt{cx}_{lm})^2\,\mathtt{cx}_{km}, && \text{for } k, l \text{ and } m \text{ distinct}, \\ &(\mathtt{cx}_{kl}\mathtt{cx}_{mp})^2\,, && \text{for } k \neq p \text{ and } l \neq m. \end{aligned}$$

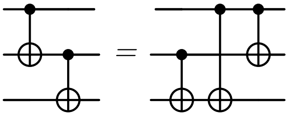
The structure of the group CX_q

Corollary (of Steinberg, 1968 and Bataille, 2022)

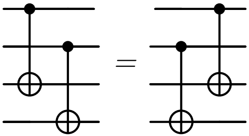
If $q \geq 3$, a presentation of CX_q is given by the set of generators

$$\{\mathtt{cx}_{kl} \mid 1 \leq k, l \leq q, k \neq l\},$$

and the following set of relations: $\mathtt{cx}^2$,

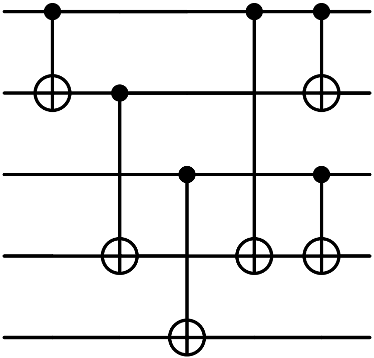


,   *and*

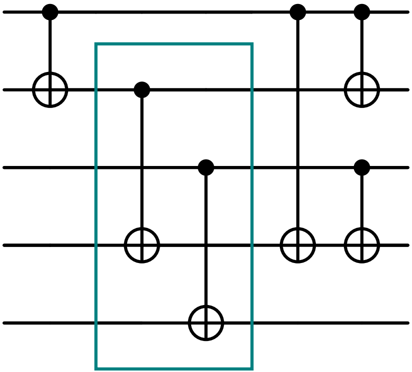


.

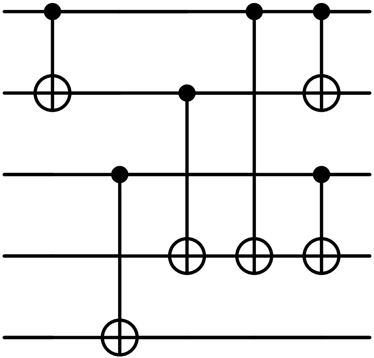
The structure of the group CX_q



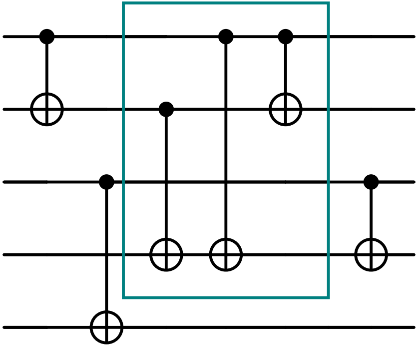
The structure of the group CX_q



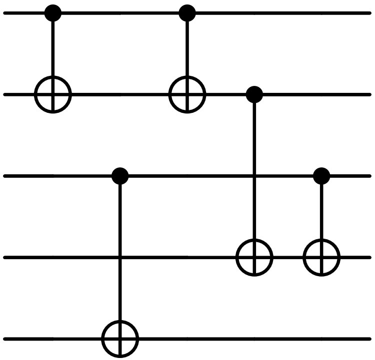
The structure of the group CX_q



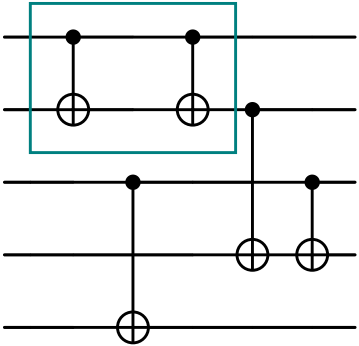
The structure of the group CX_q



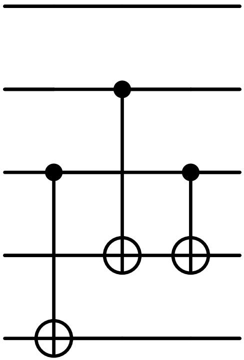
The structure of the group CX_q



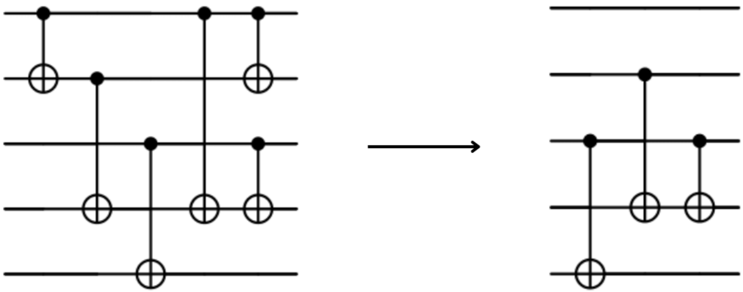
The structure of the group CX_q



The structure of the group CX_q

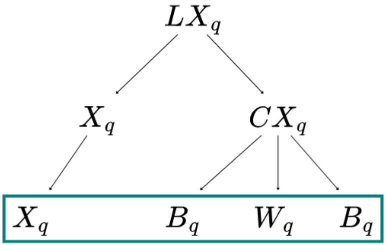


The structure of the group CX_q



How to further decompose LX_q?

- Borel subgroup: $B_q < \mathrm{GL}_q(\mathbb{Z}_2)$ the subgroup of upper-triangular matrices ;
- Weyl subgroup: $W_q < \mathrm{GL}_q(\mathbb{Z}_2)$ the subgroup of permutation matrices.



Theorem (Bruhat and Tits, 1972)

We have $CX_q = B_q W_q B_q$.

This is known as the *Bruhat decomposition*.

A quantum circuit to span X_q

- We showed that $X_q = \mathbb{Z}_2^q$. So, denoting θ for $R_X(\theta)$, we have

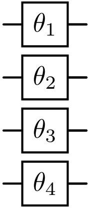


Figure: Circuit spanning X_4 when $\theta \in \{0, \pi\}^4$.

A quantum circuit to span the Borel subgroup B_q

- It is known that upper-triangular matrices over $\mathbb{Z}_2$ are generated by *transvections*:

$$T_{kl} = I + E_{kl} \qquad \text{with} \qquad [E_{kl}]_{mp} = \begin{cases} 1, & \text{if } (k,l) = (m,p), \\ 0, & \text{otherwise.} \end{cases}$$

A quantum circuit to span the Borel subgroup B_q

- It is known that upper-triangular matrices over $\mathbb{Z}_2$ are generated by *transvections*:

$$T_{kl} = I + E_{kl} \qquad \text{with} \qquad [E_{kl}]_{mp} = \begin{cases} 1, & \text{if } (k,l) = (m,p), \\ 0, & \text{otherwise.} \end{cases}$$

- Bataille (2022) proved that $\mathrm{GL}_q(\mathbb{Z}_2) \simeq CX_q$ by showing $\texttt{cx}_{kl} \longleftrightarrow T_{kl}$.

A quantum circuit to span the Borel subgroup B_q

How to fit *all* transvections into one *short* circuit?

A quantum circuit to span the Borel subgroup B_q

How to fit *all* transvections into one *short* circuit?

- Multiplying by the matrix T_{kl} adds the l-th row of a matrix to its k-th row.

A quantum circuit to span the Borel subgroup B_q

How to fit *all* transvections into one *short* circuit?

- Multiplying by the matrix T_{kl} adds the l-th row of a matrix to its k-th row.

$$\begin{pmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&1&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}\begin{pmatrix}1&0&1&1&0\\0&1&1&0&1\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}=\begin{pmatrix}1&0&1&1&0\\0&1&1&0&1\\&&&&\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}.$$

A quantum circuit to span the Borel subgroup B_q

How to fit *all* transvections into one *short* circuit?

- ▷ Multiplying by the matrix T_{kl} adds the l-th row of a matrix to its k-th row.

$$\begin{pmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&1&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}\begin{pmatrix}1&0&1&1&0\\0&1&1&0&1\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}=\begin{pmatrix}1&0&1&1&0\\0&1&1&0&1\\0&0&1&1&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}.$$

A quantum circuit to span the Borel subgroup B_q

How to fit *all* transvections into one *short* circuit?

- ▷ Multiplying by the matrix T_{kl} adds the l-th row of a matrix to its k-th row.

Proposition

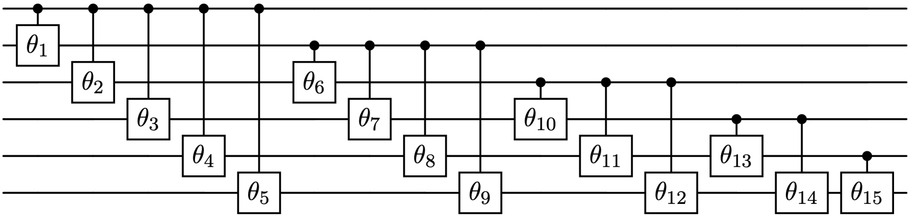
Any element of B_q is uniquely written as a subword of

$$T_{(q-1\ q)} T_{(q-2\ q-1)} T_{(q-2\ q)} \dots T_{(jq)} \dots T_{(j\ j-1)} T_{(j-1\ q)} \dots T_{(23)} T_{(1q)} \dots T_{(13)} T_{(12)}.$$

A quantum circuit to span the Borel subgroup B_q

Theorem

Any element of B_q can *uniquely* be written as



for adequate parameters $\theta_* \in \{0, \pi\}$. The size scales in $O(q^2)$ and the depth in $O(q)$.

A quantum circuit to span the Weyl subgroup $W_q \simeq S_q$

- We leverage the *Bruhat order* on the symmetric group.

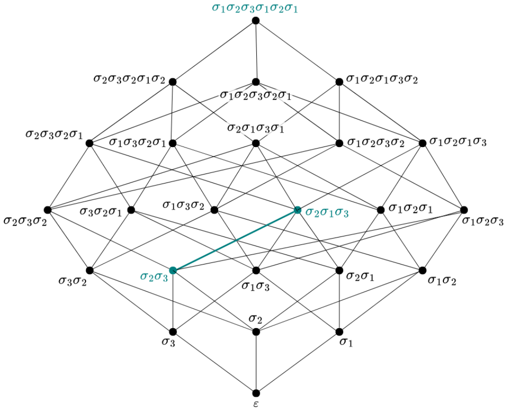
A quantum circuit to span the Weyl subgroup $W_q \simeq S_q$

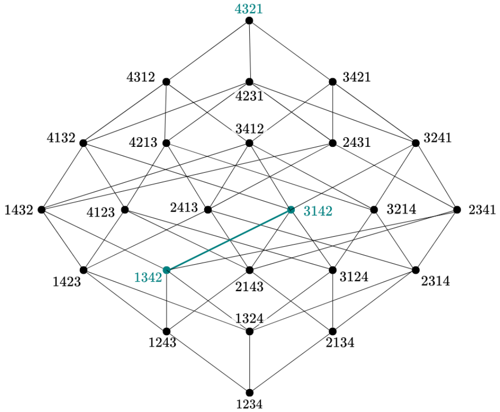
- We leverage the *Bruhat order* on the symmetric group.
- A permutation σ_1 is *lower than or equal to* another permutation σ_2 if there exists a word of σ_1 that is a *subword* of a (or equivalently, any) reduced word of σ_2.

A quantum circuit to span the Weyl subgroup $W_q \simeq S_q$

- We leverage the *Bruhat order* on the symmetric group.
- A permutation σ_1 is *lower than or equal to* another permutation σ_2 if there exists a word of σ_1 that is a *subword* of a (or equivalently, any) reduced word of σ_2.
- There exists a *unique maximal element* for the Bruhat order on S_q.

A quantum circuit to span the Weyl subgroup $W_q \simeq S_q$

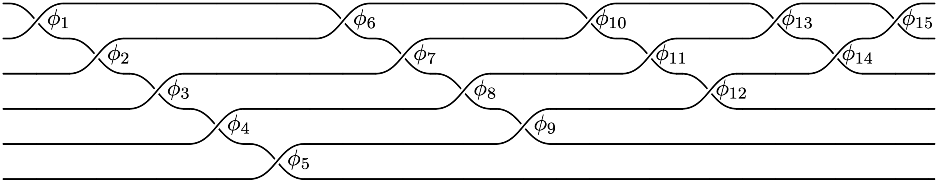




A quantum circuit to span the Weyl subgroup $W_q \simeq S_q$

Theorem

Any element of W_q can be written as



for adequate parameters $\phi_* \in \{0, \pi\}$. The size scales in $O(q^2)$ and the depth in $O(q)$.

Finally, a quantum circuit to span the entirety of LX_q

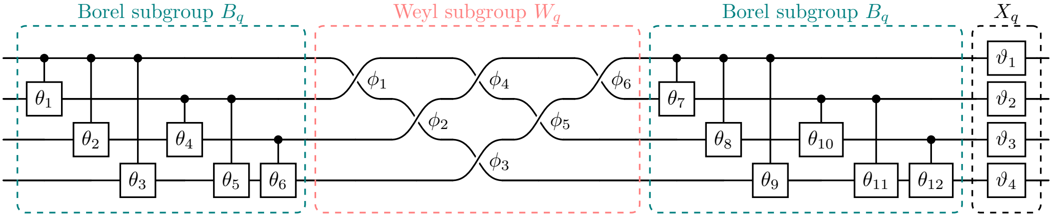


Figure: Circuit spanning LX_4. The size of such circuits scales in $O(q^2)$, and the depth in $O(q)$.

How many permutations have we reached?

Proposition

This algorithm can span up to p distinct permutations, with

$$p = |X_q| \cdot |CX_q| = 2^{\frac{q(q+1)}{2}} \prod_{k=1}^{q} \left(2^k - 1\right).$$

q	1	2	3	4	5	6
p	2	24	1344	322,560	319,979,520	1,290,157,424,640

Figure: Number p of spanned permutations for some numbers of qubits q.

A circuit spanning all permutations for $q = 2$

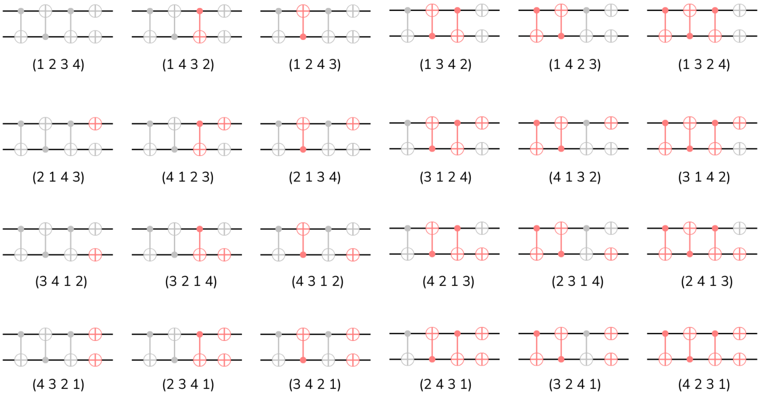


Figure: Permutations of $\{1, 2, 3, 4\}$, each with one of their circuits.

How many permutations do we span?

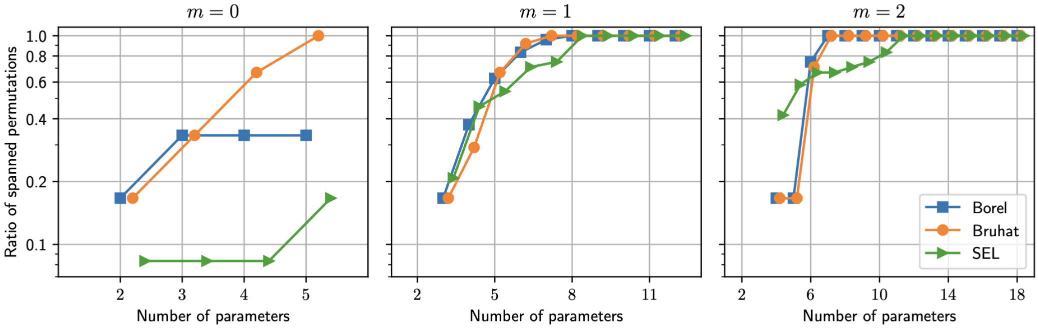


Figure: Ratio of the spanned permutations as a function of the number of parameters for $q = 2$, i.e., $n = 4$. Recall that the Bruhat span of n is 24 and $n! = 24$.

How many permutations do we span?

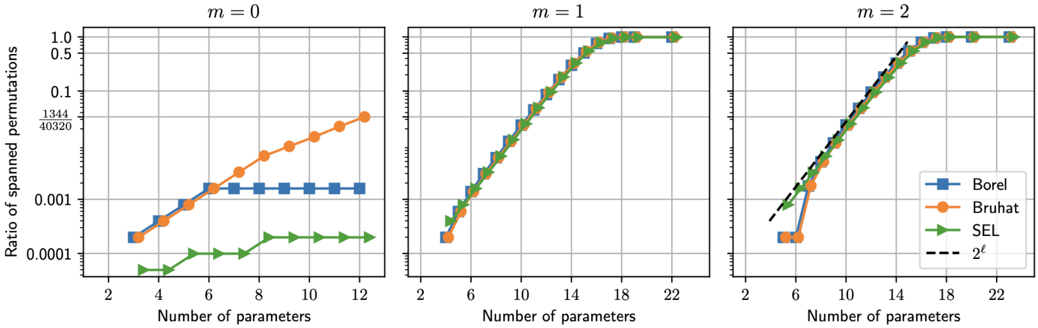


Figure: Ratio of the spanned permutations as a function of the number of parameters for $q = 3$, i.e., $n = 8$. Recall that the Bruhat span of n is $1,344$ and $n! = 40,320$.

The quadratic assignment problems

The cost function we aim to optimize is of the form

$$f\left(\widehat{P}_\theta\right) = \mathrm{tr}\left(W\widehat{P}_\theta D^\top \widehat{P}_\theta^\top\right),$$

where W and D are two adjacency matrices in $\mathbb{R}^{n\times n}$.

The quadratic assignment problems

The cost function we aim to optimize is of the form

$$f\left(\widehat{P}_\theta\right) = \mathrm{tr}\left(W\widehat{P}_\theta D^\top \widehat{P}_\theta^\top\right),$$

where W and D are two adjacency matrices in $\mathbb{R}^{n\times n}$.

- None of the matrices are assumed to be symmetric.

The quadratic assignment problems

The cost function we aim to optimize is of the form

$$f\left(\widehat{P}_\theta\right) = \mathrm{tr}\left(W\widehat{P}_\theta D^\top \widehat{P}_\theta^\top\right),$$

where W and D are two adjacency matrices in $\mathbb{R}^{n\times n}$.

- None of the matrices are assumed to be symmetric.
- The quadratic assignment problem is NP-hard. The existence of a polynomial time ε-approximation algorithm implies P $=$ NP.

Simulations on instances of QAPLib

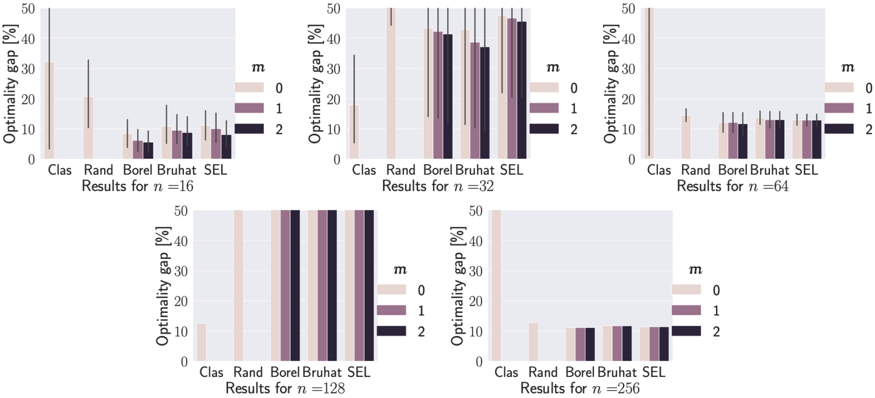


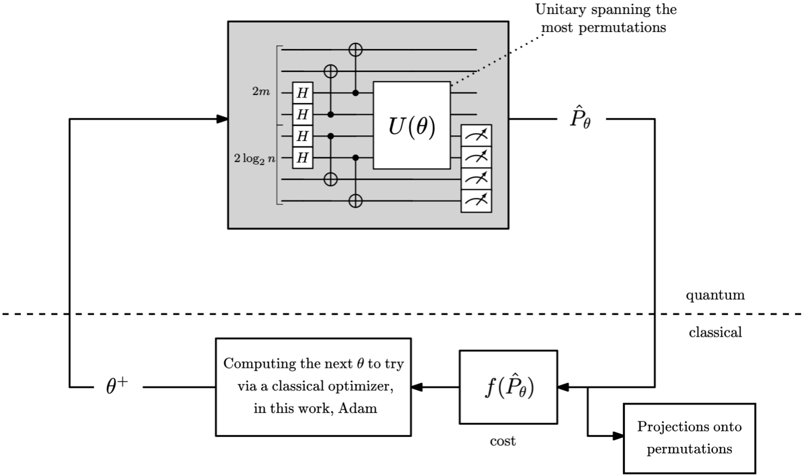
Figure: Numerical comparisons on instances taken from QAPLin. Clas denotes the classical heuristic and Rand the naive random method. We present here the mean over the instances and the standard deviation. We zoom on the range [0, 50%] for readability.

Thank you for your attention.

arXiv:2505.05981

dylan.laplace.mermoud@protonmail.com

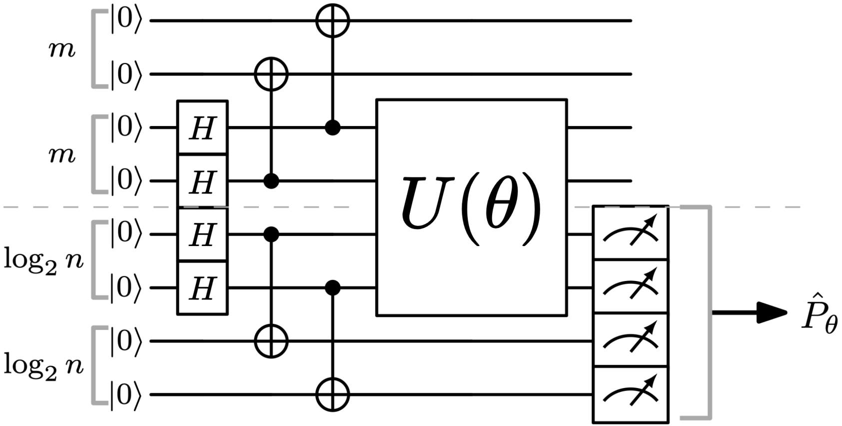
Solving optimization problems



1

[1] Circuit from Mariella et al. (2024) "Quantum theory and application of contextual optimal transport".

Measuring a superposition of permutations



An algorithm to solve quadratic assignment problems

Algorithm QuPer

Require: Ansatz, number of ancilla qubit m^*, number of iterations I

Define $\theta^{(0)}$ uniformly in $\frac{\pi}{2} \pm 0.05$ according to the chosen ansatz
for m in $\{0, \ldots, m^*\}$ **do**
    while convergence not reached **do** ▷ We set $I = 300$ iterations
        $\theta^{(i+1)} \leftarrow \textsc{Adam}(\theta^{(i)})$ ▷ Adam calls the quantum circuit
        if $i \,\%\, 10 = 0$ **then**
            get $\tilde{P}$ by projecting $\widehat{P}_{\theta^{(i+1)}}$
            get $\tilde{v}$ by evaluating the cost classically
            if $\tilde{v} < v$ **then**
                $v \leftarrow \tilde{v}$, $P \leftarrow \tilde{P}$
    return v, P ▷ We returned the results for each m
    pad the final θ with zeros

Simulations on random instances

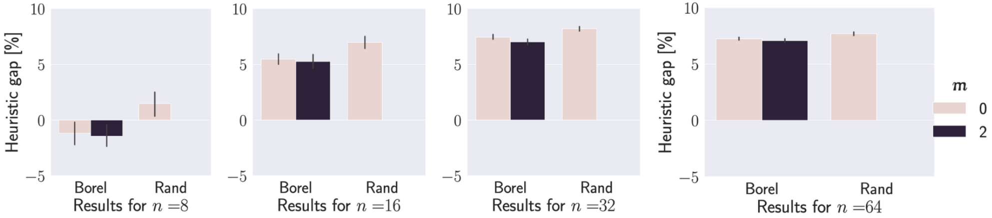


Figure: Numerical comparisons on 25 Gaussian random instances with respect to the classical heuristic. We present here the mean over the instances and the standard deviation.

Simulations on random graph isomorphism problem instances

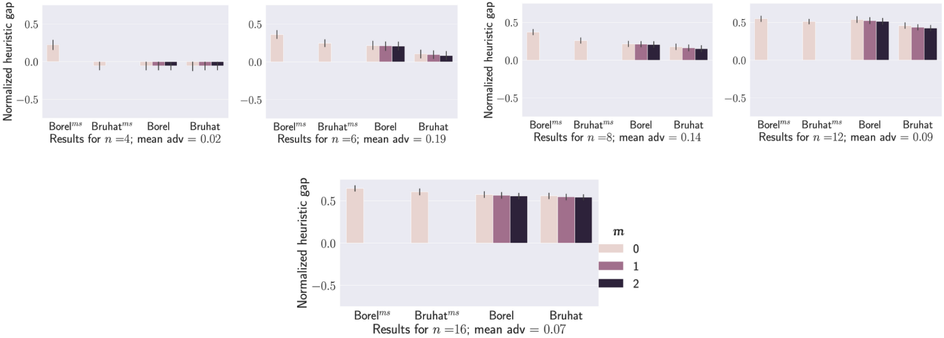


Figure: Numerical comparisons on 100 random instances with respect to the classical heuristic. We present here the mean over the instances and the standard deviation. Borel^{ms} and Bruhat^{ms} represent the approach of Mariella and Simonetto[2].

[2]Nicola Mariella and Andrea Simonetto. (2023) "A quantum algorithm for the sub-graph isomorphism problem".