Quantum Automorphisms of Matroids

Michael Joswig

TU Berlin & MPI MiS, Leipzig

23 February 2024

joint w/ D. Corey, J. Schanz, M. Wack & M. Weber

Matroids

Definition (matroids via bases axioms)

(r, n)-matroid = subset of $\binom{[n]}{r}$ subject to an *exchange condition*

- generalizes bases of column space of rank-r-matrix with n cols

Example (uniform matroid)

$U_{r,n} = \binom{[n]}{r}$

Example ($r = 2, n = 4$)

$M_5 = \{12, 13, 14, 23, 24\}$

Matroids (continued)

Let M be an (r,n)-matroid.

Definition

independent set = subset of some basis
circuit = minimally dependent set

- generalizes (minimal) support of elements in the right kernel of a rank-r-matrix with n cols

Example (uniform matroid)

$U_{r,n} = \binom{[n]}{r}$
circuits = $\binom{[n]}{r+1}$

Example ($r = 2, n = 4$)

$M_5 = \{12, 13, 14, 23, 24\}$
circuits = $\{34, 123, 124\}$

Automorphisms of Matroids

Let M be a matroid on n elements.

Definition

automorphism = permutation of $[n]$ which maps bases to bases

Example (uniform matroid)

$\mathrm{Aut}(U_{r,n}) = \mathrm{Sym}(n)$

Example ($r = 2, n = 4$)

$\mathrm{Aut}(M_5) = \langle (12), (34) \rangle$

Proposition

A permutation $\pi \in \mathrm{Sym}(n)$ *is an automorphism of* M
$\iff$ π *maps circuits to circuits*
$\iff$ π *maps flats to flats*
$\iff$ $\ldots$

Why Do We Care About Matroids?

- Whitney (1935): abstraction of *independence* common to both graphs and matrices
- van der Waerden (1937): algebraic independence
- Tutte (1954): *Tutte polynomial* (generalizes chromatic polynomial)
- Edmonds (1970): greedy algorithm; optimization of submodular functions
- ...
- Adiprasito, Huh & Katz (2018): Hodge theory for combinatorial geometries
- ...

Main Result

Theorem (Corey, J., Schanz, Wack & Weber 2023+)

For every matroid M we have

$$C(\mathrm{Aut}(M)) = \mathfrak{Aut}_{\mathcal{F}}(M) \leq \mathfrak{Aut}_{\mathcal{B}}(M) = \mathfrak{Aut}_{\mathcal{I}}(M) \ .$$

If M is a simple rank 3 matroid and the ground set $E(M)$ is not equal to $F_1 \cup F_2 \cup F_3$ for triangles $\{F_1, F_2, F_3\}$, then

$$C(\mathrm{Aut}(M)) = \mathfrak{Aut}_{\mathcal{F}}(M) \leq \mathfrak{Aut}_{\mathcal{C}}(M) \leq \mathfrak{Aut}_{\mathcal{B}}(M) = \mathfrak{Aut}_{\mathcal{I}}(M) \ .$$

Quantum Symmetric Groups

Wang (1998)

Let E be a finite set. Noncommutative polynomial ring in $|E|^2$ variables:

$$\mathbb{C}\langle E^2\rangle = \mathbb{C}\langle u_{ij} \ : \ i,j \in E\rangle$$

- involution: $(u_{ij})^* = u_{ij}$, $(uv)^* = v^* u^*$
- (two-sided) ideal:

$$I_E = \left\langle \ u_{ij}^2 - u_{ij}; u_{ik}u_{i\ell}, u_{kj}u_{\ell j} \ (k \neq \ell); \ \sum_{k\in E} u_{kj} - 1, \ \sum_{k\in E} u_{ik} - 1 \ \right\rangle$$

The *quantum symmetric group* on E is

$$\mathfrak{S}_E = \mathbb{C}\langle E^2\rangle / I_E$$

equipped with coproduct

$$\Delta : \mathfrak{S}_E \to \mathfrak{S}_E \otimes \mathfrak{S}_E \qquad \Delta(u_{ij}) = \sum_{k\in E} u_{ik} \otimes u_{kj} \ .$$

Quantum Permutation Groups

Wang (1998)

A *quantum permutation group* $\mathfrak{G}$ on E is an involutive algebra

$$\mathfrak{G} = \mathbb{C}\langle E^2 \rangle / I$$

where $I = I(\mathfrak{G}) \supseteq I_E$ self-adjoint ideal and coproduct Δ restricts to coproduct on $\mathfrak{G}$.

- $\mathfrak{G}_1 \leq \mathfrak{G}_2$ means $I(\mathfrak{G}_1) \supseteq I(\mathfrak{G}_2)$, read: *(quantum) subgroup*
- $\mathfrak{G} \leq \mathfrak{S}_E$ is *commutative* if $u_{ij} u_{k\ell} = u_{k\ell} u_{ij}$ for all $i, j, k, \ell \in E$
- $C(G)$ = involutive algebra of complex-valued functions on finite group G
- Gelfand & Naimark (1943): $\mathfrak{G}$ is commutative if and only if $\mathfrak{G} = C(G)$ for some finite group G
- $C(\mathrm{Sym}(E)) < \mathfrak{S}_E \iff |E| \geq 4$

Some Identities in the Quantum Symmetric Group $\mathfrak{S}_E$

For $A = (a_1, \ldots, a_k), B = (b_1, \ldots, b_k) \in E^k$ let

$$u_{AB} := u_{a_1,b_1} \cdots u_{a_k,b_k} \quad .$$

Lemma

$$\sum_{C \in E^k} u_{AC} = 1 \quad \textit{and} \quad \sum_{C \in E^k} u_{CB} = 1$$

$$\Delta(u_{AB}) = \sum_{C \in E^k} u_{AC} \otimes u_{CB}$$

A Large Class of Subgroups of $\mathfrak{S}_E$

For nonempty $\mathcal{A} \subseteq E^k$ let

$$I_{\mathcal{A}} = \langle u_{AB} \, : \, (A \in \mathcal{A} \text{ and } B \notin \mathcal{A}) \text{ or } (A \notin \mathcal{A} \text{ and } B \in \mathcal{A}) \rangle$$

$$\mathfrak{G}_{\mathcal{A}} = \mathfrak{S}_E / I_{\mathcal{A}}$$

Proposition

The quotient $\mathfrak{G}_{\mathcal{A}}$ is a subgroup of $\mathfrak{S}_E$.

Proof.

- $I_{\mathcal{A}}$ self-adjoint, thus $\mathfrak{G}_{\mathcal{A}}$ involutive algebra
- Suppose $u_{AB} \in I_{\mathcal{A}}$ with $A \in \mathcal{A}$ and $B \notin \mathcal{A}$. If $C \in \mathcal{A}$, then $u_{CB} \in I_{\mathcal{A}}$. Otherwise, $C \notin \mathcal{A}$, and so $u_{AC} \in I_{\mathcal{A}}$.
- Hence $\Delta(u_{AB}) = \sum_{C \in E^k} u_{AC} \otimes u_{CB}$ lies in $I_{\mathcal{A}} \otimes I_{\mathcal{A}}$, as required.

□

An Entire Zoo of Quantum Automorphism Groups

Let M be a matroid.

Denote by $\overline{\mathcal{I}}(M)$, $\overline{\mathcal{B}}(M)$, $\overline{\mathcal{F}}(M)$, and $\overline{\mathcal{C}}(M)$ the sets of independent, basis, flat, and circuit *tuples* of M, respectively.

Definition

- The *independent sets* quantum automorphism group is $\mathfrak{Aut}_{\mathcal{I}}(M) = \mathfrak{G}_{\overline{\mathcal{I}}(M)}$.
- The *bases* quantum automorphism group is $\mathfrak{Aut}_{\mathcal{B}}(M) = \mathfrak{G}_{\overline{\mathcal{B}}(M)}$.
- The *circuits* quantum automorphism group is $\mathfrak{Aut}_{\mathcal{C}}(M) = \mathfrak{G}_{\overline{\mathcal{C}}(M)}$.
- The *flats* quantum automorphism group is $\mathfrak{Aut}_{\mathcal{F}}(M) = \mathfrak{G}_{\overline{\mathcal{F}}(M)}$.

Quantizations of $\mathrm{Aut}(M)$

Given a quantum permutation group $\mathfrak{G} \leq \mathfrak{S}_E$, denote by $\mathfrak{G}^{\mathrm{com}}$ the commutative quantum permutation group

$$\mathfrak{G}^{\mathrm{com}} = \mathfrak{G} / \langle u_{ab}u_{cd} - u_{cd}u_{ab} \ : \ a, b, c, d \in E \rangle.$$

Proposition

The commutative quantum groups

$$\mathfrak{Aut}_{\mathcal{I}}(\mathrm{M})^{\mathrm{com}}, \ \mathfrak{Aut}_{\mathcal{B}}(\mathrm{M})^{\mathrm{com}}, \ \mathfrak{Aut}_{\mathcal{F}}(\mathrm{M})^{\mathrm{com}}, \ \mathfrak{Aut}_{\mathcal{C}}(\mathrm{M})^{\mathrm{com}}$$

are all isomorphic to $C(\mathrm{Aut}(\mathrm{M}))$*.*

Main Result (again)

Theorem (Corey, J., Schanz, Wack & Weber 2023+)

For every matroid M we have

$$C(\mathrm{Aut}(M)) = \mathfrak{Aut}_{\mathcal{F}}(M) \leq \mathfrak{Aut}_{\mathcal{B}}(M) = \mathfrak{Aut}_{\mathcal{I}}(M) \ .$$

If M is a simple rank 3 matroid and the ground set $E(M)$ is not equal to $F_1 \cup F_2 \cup F_3$ for triangles $\{F_1, F_2, F_3\}$, then

$$C(\mathrm{Aut}(M)) = \mathfrak{Aut}_{\mathcal{F}}(M) \leq \mathfrak{Aut}_{\mathcal{C}}(M) \leq \mathfrak{Aut}_{\mathcal{B}}(M) = \mathfrak{Aut}_{\mathcal{I}}(M) \ .$$

Algorithms

Computations take place in the polynomial ring $R = \mathbb{Q}\langle X \rangle$ with a finite set X of noncommuting variables.

- not Noetherian!
- goal: find non-commutative Gröbner bases for ideals $I_{\overline{\mathcal{B}}(M)}, I_{\overline{\mathcal{C}}(M)}$
  - to decide commutativity

La Scala & Levandovsky (2009):

- letterplace ideals
- yields truncated Gröbner basis
- degree bounds in the homogeneous case

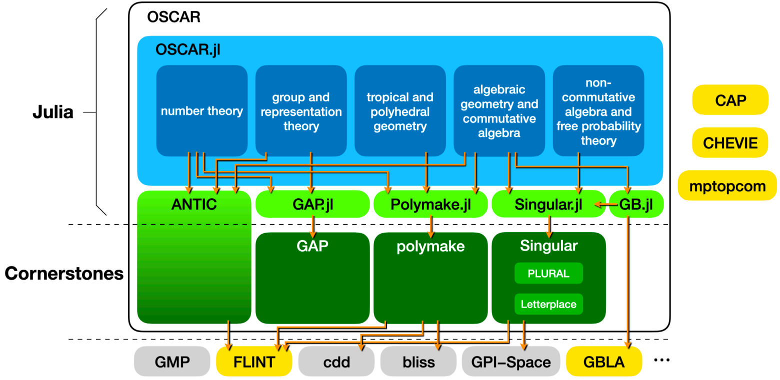
Xiu (2012):

- noncommutative Buchberger algorihm
- yields Gröbner basis, if it terminates

The OSCAR Project

http://oscar-system.org/

- joint software project of the CRC TRR 195, funded by DFG
  - written in Julia
  - planned duration: 2017–2028, three phases (rc1 of v1.0.0 today!)
  - with W. Decker, C. Fieker, M. Horn and many others



Computing $\mathfrak{Aut}_{\mathcal{B}}(M_5)$

https://github.com/dmg-lab/QuantumAutomorphismGroups.jl.git

```
julia> M = matroid_from_nonbases([[3,4]], 4)
Matroid of rank 2 on 4 elements

julia> rels, u, A = getMatroidRelations(M, :bases);

julia> A
Free associative algebra on 16 indeterminates u[1,1], u[1,2
  over rational field

julia> G = AbstractAlgebra.groebner_basis(rels)
249-element Vector{AbstractAlgebra.Generic.FreeAssAlgElem{Q
[...]

julia> isCommutative(G)
(false, Dict{FreeAssAlgElem, Bool}(u[2,4]*u[4,2] - u[4,2]*u
```

Conclusion

- Inspired by: quantum automorphisms of graphs; Bichon (2003), Banica (2005), Levandovsky et al. (2022), ...
- Question: is commutativity of $\mathfrak{Aut}_{\mathcal{B}}(M)$ and $\mathfrak{Aut}_{\mathcal{C}}(M)$ decidable?
- Question: what does it mean for a matroid to have quantum automorphisms?

Daniel Corey, Michael Joswig, Julien Schanz, Marcel Wack, and Moritz Weber, *Quantum automorphisms of matroids*, 2023, Preprint `arXiv:2312.13464`.

Wolfram Decker, Christian Eder, Claus Fieker, Max Horn, and Michael Joswig (eds.), *The OSCAR book*, Springer, 2024.