Finite Gröbner bases for quantum symmetric groups

Leonard Schmitz (TU Berlin)
joint w/ **Marcel Wack** (TU Berlin)

https://arxiv.org/abs/2503.15104

ICMS Edinburgh
2025-05-23

Free (associative) algebras

Let $X = \{x, y, \dots\}$ be a set of *variables* equipped with a *lexicographical* order $x > y > \dots$

The *degree-lexicographic order* on all *monomials* $u, v \in X^* := \{w_1 \dots w_\ell \mid w_i \in X\}$ is defined as

$$u > v \;:\Longleftrightarrow\; \begin{cases} \deg(u) > \deg(v) \text{ or} \\ \deg(u) = \deg(v) \text{ and } u >_{\text{lex}} v \end{cases}$$

Example. $xyx > yxx > xy > yx > x$

Let $R := \mathbb{C}\langle X \rangle$ denote the *free algebra*, i.e., all *non-commutative polynomials* f in X with *coefficients* in $\mathbb{C}$. The largest monomial $\text{lm}(f)$ with non-zero coefficient $\text{lc}(f)$ is called *leading monomial*.

Example. $\text{lm}(\frac{1}{2}xyx + yxx) = xyx$
$\text{lc}(3xy + 2yx) = 3$

Two-sided ideals

Definition. $J \subseteq R$ is a *two-sided ideal*, if

i) $f + g \in J \qquad \forall f, g \in J$

ii) $rft \in J \qquad \forall r, t \in R \;\; \forall f \in J$

Fact. Every (fin. gen.) algebra $\mathcal{A}$ is isomorphic to a free algebra R modulo a two-sided ideal $J \subseteq R$, i.e.

$$\mathcal{A} \cong {}^{R}\!/_{J}$$

Word problem. Decide whether $f, g \in R$ are equivalent modulo a given two-sided ideal $J \subset R$, i.e.

$$f = g \mod J \quad \Longleftrightarrow \quad f - g \in J$$

Remark. The word problem is generally *not decidable* in R.

Gröbner bases

procedure NF($h \in R$, $G \subseteq R$) *// normal form*

  if $h = 0$ **return** 0

  while $\exists a, b \in X^* \, \exists f \in G : a \operatorname{lm}(f) b = \operatorname{lm}(h)$

    do $h \leftarrow h - \frac{\operatorname{lc}(h)}{\operatorname{lc}(f)} afb$

  return $\operatorname{lc}(h)\operatorname{lm}(h) + \operatorname{NF}(h - \operatorname{lc}(h)\operatorname{lm}(h), G)$

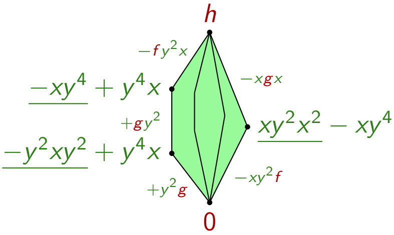
Example. $f := \underline{x^2} - y^2$

$h := \underline{x^2y^2x} - xy^4$

$\operatorname{NF}(h, \{f\}) \neq 0$

$g := fx - xf = \underline{xy^2} - y^2x$

$\operatorname{NF}(h, \{f, g\}) = 0 \implies h \in \langle f \rangle$



Definition. $G \subseteq R$ is a *Gröbner basis (GB)* if

$$h \in \langle G \rangle \iff \operatorname{NF}(h, G) = 0$$

Bergman's diamond lemma

Theorem [2]**.** For any subset $G \subseteq R$, the following statements are equivalent.

i) G is GB.

ii) The output of the reduction algorithm $\mathrm{NF}(f, G)$ is unique for every $f \in R$.

iii) The set of reduced monomials

$$\{\mathrm{NF}(w, G) \mid w \text{ monomial } \}$$

is a $\mathbb{C}$-basis of the factor algebra $R/\langle G\rangle$ when considered as a vector space.

[1] **Bergman** *"The diamond lemma in ring theory"*. **1978**

Buchberger's algorithm

Theorem. Let $F \subseteq R$ be finite such that $\langle F \rangle$ has a finite GB. Then Buchberger's algorithm [2] terminates and provides a finite GB G of $\langle F \rangle = \langle G \rangle$.

Corollary. If we have a finite GB G, then the work problem in $\langle G \rangle$ becomes decidable.

Remark. A GB is unique after *inter-reduction* and *normalizing*.

Example. i) A GB of $\langle x^2 - y^2 \rangle$ is

$$\{x^2 - y^2, xy^2 - y^2x\}$$

ii) The inter-reduced and normalized GB of $\langle x^2 + yx \rangle$ is

$$\{xy^i x + y^{i+1} x \mid i \in \mathbb{N}_0\}$$

[2] **Mora** *"Gröbner bases in non-commutative algebras"*. **1988**

Application: matrix identities

Lemma. $\begin{cases} A \in \mathrm{GL}_m(\mathbb{C}) \\ C,\ C^{-1} + VA^{-1}U \in \mathrm{GL}_\ell(\mathbb{C}) \end{cases} \implies A + UCV \in \mathrm{GL}_m(\mathbb{C}).$

Proof. The MP-inverse $(A+UCV)^p$ exists, thus the ideal with GB

$$
\begin{aligned}
&\{\ (a+ucv)(a+ucv)^p(a+ucv) - (a+ucv),\ i_\ell c - c,\ (a+ucv)^p(a+ucv)(a+ucv)^p - (a+ucv)^p,\\
&(a+ucv)^*(a+ucv)^{p*}(a+ucv)^* - (a+ucv)^*,\ (a+ucv)^{p*}(a+ucv)^*(a+ucv)^{p*} - (a+ucv)^{p*},\ i_\ell c - c,\\
&(a+ucv)^*(a+ucv)^{p*} - (a+ucv)^p(a+ucv),\ (a+ucv)^{p*}(a+ucv)^* - (a+ucv)(a+ucv)^p,\ i_m a^{-1} - a^{-1},\\
&a(a+ucv)^p a + u(c^{-1}+va^{-1}u)^{-1}v - a,\ \underline{(a+ucv)^{p*}v^*c^*u^* + (a+ucv)^{p*}a^* - i_m},\ a^{-1}i_m - a^{-1},\\
&a^{-1}a - i_m,\ \underline{(a+ucv)^p ucv + (a+ucv)^p a - i_m},\ a^*i_m - a^*,\ a i_m - a,\ (a+ucv)^p i_m - (a+ucv)^p,\ i_\ell i_\ell - i_\ell,\\
&v^*c^*u^*(a+ucv)^{p*} + a^*(a+ucv)^{p*} - i_m,\ i_m a - a,\ aa^{-1} - i_m,\ (c^{-1}+va^{-1}u)^{-1}i_\ell - (c^{-1}+va^{-1}u)^{-1},\\
&(a+ucv)^{p*}i_m - (a+ucv)^{p*},\ i_m a^{-1} - a^{-1},\ i_m(a+ucv)^p - (a+ucv)^p,\ i_m(a+ucv)^{p*} - (a+ucv)^{p*},\\
&i_m i_m - i_m,\ \underline{u(c^{-1}+va^{-1}u)^{-1}va^{-1} + a(a+ucv)^p - i_m},\ i_\ell(c^{-1}+va^{-1}u)^{-1} - (c^{-1}+va^{-1}u)^{-1},\\
&v^*i_\ell - v^*,\ ui_\ell - u,\ a^{-1}u(c^{-1}+va^{-1}u)^{-1} - (a+ucv)^p uc,\ a(a+ucv)^p u - u(c^{-1}+va^{-1}u)^{-1}c^{-1},\\
&i_m u - u,\ i_m v^* - v^*,\ vi_m - v,\ u^*i_m - u^*,\ c^{-1}(c^{-1}+va^{-1}u)^{-1}v - v(a+ucv)^p a,\ i_m a^* - a^*,\ i_\ell c^* - c^*,\\
&i_\ell c^{-1} - c^{-1}\ cv(a+ucv)^p - (c^{-1}+va^{-1}u)^{-1}va^{-1},\ v(a+ucv)^p uc + c^{-1}(c^{-1}+va^{-1}u)^{-1} - i_k,\\
&c^*i_k - c^*,\ ci_k - c,\ cc^{-1} - i_k,\ c^{-1}(c^{-1}+va^{-1}u)^{-1}c^{-1} + v(a+ucv)^p u - c^{-1},\ c^{-1}c - i_k,\ i_\ell u^* - u^*,\\
&(c^{-1}+va^{-1}u)^{-1}(va^{-1}u + c^{-1}) - i_k,\ (va^{-1}u + c^{-1})(c^{-1}+va^{-1}u)^{-1} - i_k,\ i_\ell v - v,\ c^{-1}i_k - c^{-1}\ \}
\end{aligned}
$$

$\implies (A+UCV)^p(A+UCV) = I_m$ and $((A+UCV)(A+UCV)^p)^* = I_m$

[3] **Hofstadler**, **Raab**, **Regensburger** *"Certifying operator identities via noncommutative Gröbner bases"*. **2019**

[4] **Schmitz**, **Levandovskyy** *"Formally Verifying Proofs for Algebraic Identities of Matrices"*. **2020**

Wang's quantum group

Let $R_n := \mathbb{C}\langle u_{ij} \mid 1 \leq i, j \leq n \rangle$. For any $1 \leq i, k \neq j \leq n$ let

$$\mathrm{rs}_i := \sum_{1 \leq \alpha \leq n} u_{i\alpha} - 1 \qquad \mathrm{cs}_i := \sum_{1 \leq \alpha \leq n} u_{\alpha i} - 1$$

$$\mathrm{inj}_{jik} := u_{ji} u_{ki} \qquad \mathrm{wel}_{ijk} := u_{ik} u_{ij}$$

$$\mathrm{ip}_{ij} := u_{ij}^2 - u_{ij}$$

denote row, column, orthogonal, and idempotent relations. The *quantum symmetric group*

$$\mathfrak{S}_n := {R_n}/{I_n}$$

is the free algebra R_n modulo the two-sided ideal

$$J_n := \left\langle \mathrm{rs}_i, \mathrm{cs}_i, \mathrm{ip}_{ij}, \mathrm{inj}_{jik}, \mathrm{wel}_{ijk} \;\middle|\; \begin{array}{l} 1 \leq i, j, k \leq n \\ \text{with } j \neq k \end{array} \right\rangle$$

[5] **Wang** *"Quantum symmetry groups of finite spaces"*. **1998**

[6] **Timmermann** *"An invitation to quantum groups and duality"*. **2008**

Facts

Theorem i) If $n < 4$, the quantum symmetric group $\mathfrak{S}_n$ is commutative, that is $u_{ij}u_{kl} = u_{kl}u_{ij}$ for all $1 \leq i, j, k, l \leq n$.
ii) If $n \geq 4$, then $\mathfrak{S}_n$ is non-commutative. (e.g. [1])

Definition. *Transposition* is an homomorphism of algebras,

$$(\cdot)^{\times} : R_n \to R_n, \ u_{ij} \mapsto u_{ji}$$

Example. $(u_{23}u_{13})^{\times} = u_{32}u_{31}$
$(u_{21} + u_{22} + u_{23} - 1)^{\times} = u_{12} + u_{22} + u_{32} - 1$

Lemma.

i) $\mathrm{rs}_j{}^{\times} = \mathrm{cs}_j$ **ii)** $\mathrm{ip}_{ij}{}^{\times} = \mathrm{ip}_{ji}$

iii) $\mathrm{wel}_{ijk}{}^{\times} = \mathrm{inj}_{jik}$ **iv)** $\mathrm{rinj}_{kj}{}^{\times} = \mathrm{rwel}_{kj}$

[7] **Lupini, Mancinska, Roberson** *"Nonlocal games and quantum permutation groups"*. **2020**

Reduced orthogonal relations

Lemma. The ideal J_n contains the *reduced orthogonal relations* for $2 \leq j, k \leq n$ with $j \neq k$,

$$\mathrm{rinj}_{jk} := \sum_{3\leq\alpha\leq n} u_{j2}u_{k\alpha} - \sum_{3\leq\alpha\leq n} u_{j\alpha}u_{k1} + u_{k1} - u_{j2}$$

$$\mathrm{rwel}_{jk} := \sum_{3\leq\alpha\leq n} u_{2j}u_{\alpha k} - \sum_{3\leq\alpha\leq n} u_{\alpha j}u_{1k} + u_{1k} - u_{2j}$$

Proof.

$$\mathrm{inj}_{k1j} = u_{k1}u_{j1} \xrightarrow{\mathrm{rs}_k} -\sum_{\alpha\neq 1} \underline{u_{k\alpha}u_{j1}} + u_{j1}$$

$$\xrightarrow{\mathrm{rs}_j} \sum_{\alpha\neq 1} \underline{u_{k2}u_{j\alpha}} - \sum_{\alpha\neq 1,2} u_{k\alpha}u_{j1} + u_{j1} - u_{k2}$$

$$\xrightarrow{\mathrm{inj}_{k2j}} \sum_{\alpha\neq 1,2} \underline{u_{k2}u_{j\alpha}} - \sum_{\alpha\neq 1,2} u_{k\alpha}u_{j1} + u_{j1} - u_{k2} = \mathrm{rinj}_{kj}$$

Main result

Theorem [S, Wack '25]. For $n \geq 4$ the ideal J_n has a finite GB

$$G_n := \{\mathrm{cs}_1\} \cup \left\{ \begin{array}{l} \mathrm{cs}_i, \mathrm{rs}_i, \mathrm{ip}_{ij}, \mathrm{inj}_{ijk} \\ \mathrm{wel}_{ijk}, \mathrm{rinj}_{kj}, \mathrm{rwel}_{kj} \end{array} \;\middle|\; i,j,k \neq 1 \right\}$$
$$\cup \left\{ u_{k2}\mathrm{inj}_{j3i} - \mathrm{rinj}_{kj} u_{i3} \;\middle|\; \begin{array}{l} i,j,k \neq 1 \text{ and} \\ (k,j) \neq (2,3) \neq (j,i) \end{array} \right\}$$
$$\cup \left\{ u_{2k}\mathrm{wel}_{3ji} - \mathrm{rwel}_{kj} u_{3i} \;\middle|\; \begin{array}{l} i,j,k \neq 1, \\ (k,j) \neq (2,3) \neq (j,i) \\ \text{and } (k,j,i) \neq (2,4,3) \end{array} \right\}$$

with respect to the graded lexicographic order via row-wise ordering in $(u_{ij})_{1 \leq i,j \leq n}$. Its cardinality is

$$\# G_n = 4n^3 - 15n^2 + 16n - 2$$

Corollary. The word problem in $\mathfrak{S}_n$ is decidable.

Overlap polynomials

Definition. For $f, g \in R_n$ we obtain (fin. many) *overlap polynomials*

$$\begin{cases} \frac{1}{\mathrm{lc}(f)} fa - \frac{1}{\mathrm{lc}(g)} bg & \text{if } \mathrm{lm}(f)a = b\,\mathrm{lm}(g) \\ \frac{1}{\mathrm{lc}(f)} af - \frac{1}{\mathrm{lc}(g)} gb & \text{if } a\,\mathrm{lm}(f) = \mathrm{lm}(g)b \end{cases}$$

where a, b are monomials with

$$0 < \mathrm{len}(a) \leq \mathrm{len}(\mathrm{lm}(g)) \text{ and } 0 < \mathrm{len}(b) \leq \mathrm{len}(\mathrm{lm}(f))$$

Example.

$$\begin{array}{rl} \mathrm{lm}(\mathrm{inj}_{i2j} u_{k3}) = & u_{i2} \cdot u_{j2} \mid u_{k3} \\ \hline \mathrm{lm}(u_{i2} \mathrm{rinj}_{jk}) = & u_{i2} \mid u_{j2} \cdot u_{k3} \end{array}$$

$\implies$ $\mathrm{inj}_{i2j} u_{k3} - u_{i2} \mathrm{rinj}_{jk}$ overlap polynomial

Definition. Similarly we obtain (fin. many) *division polynomials*

$$\frac{1}{\mathrm{lc}(f)} afb - \frac{1}{\mathrm{lc}(g)} g \qquad \text{if } a\,\mathrm{lm}(f)b = \mathrm{lm}(g)$$

Buchberger's criterion

Theorem. [1]. A subset $G \subset R_n$ is a GB if and only if each overlap and division relation of any $f, g \in G$ reduces to zero modulo G.

Remark. This is computably accessible and the key observation for Buchberger's algorithm [2] to compute a GB for an input set.

Example. i) $\{\mathrm{inj}_{ikj}, \mathrm{wel}_{kij} \mid 1 \leq i, j, k \leq n, i \neq j\}$ is a GB

ii) $\{\mathrm{ip}_{ij} \mid 1 \leq i, j \leq n\}$ is a GB since the only overlap is

$$u_{ij}\mathrm{ip}_{ij} - \mathrm{ip}_{ij}u_{ij} = 0$$

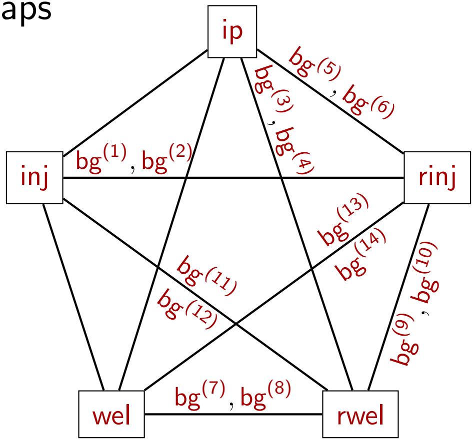
iii) $G := \{\mathrm{rs}_2, \dots, \mathrm{rs}_n, \mathrm{cs}_1, \dots, \mathrm{cs}_n\}$ is a GB of $\langle \mathrm{rs}_1 \cup G\rangle$ since

$$\mathrm{rs}_1 \xrightarrow{\mathrm{cs}_1} \mathrm{rs}_1 - \mathrm{cs}_1 \xrightarrow{\mathrm{cs}_2} \dots \xrightarrow{\mathrm{cs}_n} \mathrm{rs}_1 - \sum_{1 \leq i \leq n} \mathrm{cs}_i \xrightarrow{\mathrm{rs}_2} \dots \xrightarrow{\mathrm{rs}_n} 0.$$

[1] **Bergman** *"The diamond lemma in ring theory"*. **1978**

[2] **Mora** *"Gröbner bases in non-commutative algebras"*. **1988**

Graph of overlaps

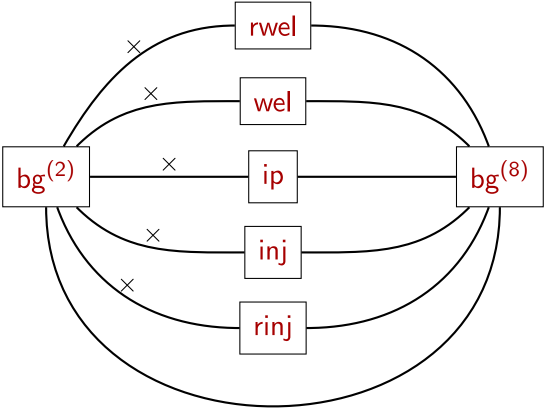


Only very few relations survive reduction

$$B_n := \left\{ \mathrm{bg}^{(2)}_{kji} = u_{k2}\mathrm{inj}_{j3i} - \mathrm{rinj}_{kj}u_{i3} \;\middle|\; \begin{array}{l} i,j,k \neq 1 \text{ and} \\ (k,j) \neq (2,3) \neq (j,i) \end{array} \right\}$$

$$\cup \left\{ \mathrm{bg}^{(8)}_{kji} = u_{2k}\mathrm{wel}_{3ji} - \mathrm{rwel}_{kj}u_{3i} \;\middle|\; \begin{array}{l} i,j,k \neq 1, \\ (k,j) \neq (2,3) \neq (j,i) \\ \text{and } (k,j,i) \neq (2,4,3) \end{array} \right\}$$

2nd round of overlapping



Here, no overlaps survive. Therefore J_n has the finite GB

$$\left\{ \mathsf{rs}_i, \mathsf{cs}_i, \mathsf{ip}_{ij}, \mathsf{inj}_{jik}, \mathsf{wel}_{ijk} \;\middle|\; \begin{array}{l} 1 \leq i, j, k \leq n \\ \text{with } j \neq k \end{array} \right\} \cup B_n$$

Outlook and future work

[8] **Corey**, **Joswig**, **Schanz**, **Wack**, **Weber** *"Quantum automorphisms of matroids"*. **2023**

[9] **Levandovskyy**, **Eder**, **Schanz**, **Schmidt**, **Steenpass**, **Weber** *"Existence of quantum symmetries for graphs on up to seven vertices: a computer based approach"*. **2022**

[10] **Preiß** *"An algebraic geometry of paths via the iterated-integral signature"*. **2023**