Varieties over module homomorphisms and their correspondence to free algebras

Leonard Schmitz
U Greifswald

Tagung der Fachgruppe Computeralgebra
March 2022

based on same-titled master thesis (RWTH AC 2021)
advised by **Eva Zerz** and **Georg Regensburger**

Identities of $\mathbf{k}$-module homomorphisms

Example. $AUV - A^3 = 0 \implies A(UV)^2 - A^2UVA = 0$

$$\forall A \in \mathrm{Hom}(\mathbf{k}^m, \mathbf{k}^m)$$
$$\forall U \in \mathrm{Hom}(\mathbf{k}^\ell, \mathbf{k}^m)$$
$$\forall V \in \mathrm{Hom}(\mathbf{k}^m, \mathbf{k}^\ell)$$

Proof.

$f := auv - a^3\,, \quad q := a(uv)^2 - a^2uva \quad \in \mathbf{k}\langle a, u, v\rangle$

show membership

$$q = fuv - afa + a^2f \in \langle f \rangle$$

evaluate in $\sigma = (A, U, V)$

$$q(\sigma) = f(\sigma)\,UV - A\,f(\sigma)\,A + A^2\,f(\sigma) = 0$$

New viewpoint: Varieties

$$\sigma \in \mathcal{V}(f) = \mathcal{V}(q, f) \subseteq \mathrm{Hom}(\mathbf{k}^m, \mathbf{k}^m) \times \mathrm{Hom}(\mathbf{k}^\ell, \mathbf{k}^m) \times \mathrm{Hom}(\mathbf{k}^m, \mathbf{k}^\ell)$$

[1] **J. Helton**, **M. Stankus**, and **J. Wavrik**. *"Computer simplification of formulas in linear systems theory"*. IEEE Transactions on Automatic Control. **1998**

Valid polynomials

Definition. $\mathbf{A} = \bigtimes_{1 \leqslant j \leqslant n} \mathrm{Hom}(\mathcal{M}_j, \mathcal{N}_j)$

$\mathtt{I} := \{(\mathcal{M}_k, \mathcal{N}_j) \mid k, j\}$

Free algebra $\mathbf{k}\langle x_1, \ldots, x_n \rangle$

$$\mathcal{U}_{\mathtt{i}} := \left\{ x_{j_1} \ldots x_{j_\ell} \;\middle|\; \begin{matrix} \mathtt{i}_1 = \mathcal{M}_{j_\ell} \quad \mathcal{N}_{j_1} = \mathtt{i}_2 \\ \mathcal{N}_{j_t} = \mathcal{M}_{j_{t-1}} \end{matrix} \right\}$$

$$\mathrm{val}_{\mathbf{A}} := \bigcup_{\mathtt{i} \in \mathtt{I}} \mathrm{span}(\mathcal{U}_{\mathtt{i}})$$

$f \in \mathrm{span}(\mathcal{U}_{\mathtt{i}})$ evaluated in $\sigma \in \mathbf{A}$

$$f(\sigma) \in \mathrm{Hom}(\mathtt{i}_1, \mathtt{i}_2)$$

with $x_j(\sigma) := \sigma_j$ and $g(\sigma) \circ f(\sigma) = (gf)(\sigma)$

[2] **C. G. Raab**, **G. Regensburger**, and **J. H. Poor**. *"Formal proofs of operator identities by a single formal computation"*. Journal of Pure and Applied Algebra. **2020**

[3] **L. Schmitz** and **V. Levandovskyy**. *"Formally verifying proofs for algebraic identities of matrices"*. Intelligent Computer Mathematics CICM, Springer LNCS. **2020**

Varieties

Definition.

$$\mathcal{V} : \mathfrak{P}(\mathrm{val}_{\mathbf{A}}) \longrightarrow \mathfrak{P}(\mathbf{A})$$
$$\mathcal{F} \longmapsto \{\sigma \in \mathbf{A} \mid f(\sigma) = 0 \ \forall f \in \mathcal{F}\}$$

Example. $\mathbf{A} = \mathrm{End}(\mathbf{k}^m) \times \mathrm{Hom}(\mathbf{k}^m, \mathbf{k}^\ell) \times \mathrm{End}(\mathbf{k}^\ell)^2 \times \mathrm{Hom}(\mathbf{k}^\ell, \mathbf{k}^m)$

$$\mathcal{F} = \{ x_1^2 - x_1,\ x_3^2 - x_3,\ x_5x_3 - x_5,\ x_1x_5 - x_5,\ x_2x_1 - x_2,\ x_3x_2 - x_2,\ x_4(x_2x_5 + x_3) - x_3,\ (x_2x_5 + x_3)x_4 - x_3,\ x_4x_3 - x_4,\ x_3x_4 - x_4 \}$$

evaluated in $\sigma = (\mathrm{I}_m, B, \mathrm{I}_\ell, (BA + \mathrm{I}_\ell)^{-1}, A)$

$$\{ \mathrm{I}_m^2 - \mathrm{I}_m,\ \mathrm{I}_\ell^2 - \mathrm{I}_\ell,\ A\mathrm{I}_\ell - A,\ \mathrm{I}_m A - A,\ B\mathrm{I}_m - B,\ \mathrm{I}_\ell B - B,\ (BA + \mathrm{I}_\ell)^{-1}(BA + \mathrm{I}_\ell) - \mathrm{I}_\ell,\ (BA + \mathrm{I}_\ell)(BA + \mathrm{I}_\ell)^{-1} - \mathrm{I}_\ell,\ (BA + \mathrm{I}_\ell)^{-1}\mathrm{I}_\ell - (BA + \mathrm{I}_\ell)^{-1},\ \mathrm{I}_\ell(BA + \mathrm{I}_\ell)^{-1} - (BA + \mathrm{I}_\ell)^{-1} \}$$

$$\implies \sigma \in \mathcal{V}(\mathcal{F})$$

Vanishing sets

Definition.

$$\mathcal{J} : \mathfrak{P}(\mathbf{A}) \longrightarrow \mathfrak{P}(\mathsf{val}_{\mathbf{A}})$$
$$\mathcal{W} \longmapsto \bigcup_{\mathtt{i} \in \mathtt{I}} \ker(\phi_{\mathcal{W}\,\mathtt{i}})$$

Regular functions

$$\phi_{\mathcal{W}\,\mathtt{i}} : \mathsf{span}(\mathcal{U}_{\mathtt{i}}) \longrightarrow \mathsf{Hom}(\mathtt{i}_1, \mathtt{i}_2)^{\mathcal{W}}$$
$$f \longmapsto \begin{cases} \mathcal{W} \to \mathsf{Hom}(\mathtt{i}_1, \mathtt{i}_2) \\ \sigma \mapsto f(\sigma) \end{cases}$$

Coordinate module

$$\mathcal{O}_{\mathtt{i}}\mathcal{W} := \mathsf{im}(\phi_{\mathcal{W}\,\mathtt{i}})$$

Theorem. $\mathcal{V}$ and $\mathcal{J}$ are Galois connection

Corollary. $\forall\, \mathcal{W}\ \exists!\ \overline{\mathcal{W}} := \mathcal{V} \circ \mathcal{J}(\mathcal{W})$ smallest variety containing $\mathcal{W}$

Lemma. If $\mathbf{k}$ field then $\left\langle \mathcal{J}(\mathcal{W}) \right\rangle \cap \mathsf{val}_{\mathbf{A}} = \mathcal{J}(\mathcal{W})$

Morphisms of varieties

Definition.

$$\bigtimes_{1 \leqslant j \leqslant n} \mathrm{Hom}(\mathcal{M}_j, \mathcal{N}_j) = \mathbf{A} \qquad\qquad \mathbf{A}' = \bigtimes_{1 \leqslant j \leqslant n'} \mathrm{Hom}(\mathcal{M}'_j, \mathcal{N}'_j)$$

$$\mathrm{val}_{\mathbf{A}} \supseteq \mathcal{F} \qquad\qquad \mathcal{F}' \subseteq \mathrm{val}_{\mathbf{A}'}$$

$$\mathcal{V}(\mathcal{F}) =: \mathcal{V} \qquad\qquad \mathcal{V}' := \mathcal{V}(\mathcal{F}')$$

$$\alpha_j \in \mathcal{O}_{\mathtt{i}} \mathcal{V} \cap \mathrm{Hom}(\mathcal{M}'_j, \mathcal{N}'_j)^{\mathcal{V}}$$

$$\alpha : \mathcal{V} \longrightarrow \mathcal{V}'$$
$$\sigma \longmapsto (\alpha_1(\sigma), \ldots, \alpha_{n'}(\sigma))$$

Lemma. $\alpha \in \mathrm{Mor}(\mathcal{V}, \mathcal{V}')$ and $\mathcal{W}$ subvariety $\mathcal{V}' \implies \alpha^{-1}(\mathcal{W})$ variety

Morphisms of varieties

Example. $\mathbf{A} = \mathrm{End}(\mathbf{k}^m) \times \mathrm{Hom}(\mathbf{k}^m, \mathbf{k}^\ell) \times \mathrm{End}(\mathbf{k}^\ell)^2 \times \mathrm{Hom}(\mathbf{k}^\ell, \mathbf{k}^m)$

$\mathbf{A}' = \mathbf{A} \times \mathrm{End}(\mathbf{k}^m)$

$$\mathcal{F} = \{\, x_1^2 - x_1,\; x_3^2 - x_3,\; x_5x_3 - x_5,\; x_1x_5 - x_5,\; x_2x_1 - x_2,\; x_3x_2 - x_2,\; x_4\,(x_2x_5 + x_3) - x_3,\; (x_2x_5 + x_3)\,x_4 - x_3,\; x_4x_3 - x_4,\; x_3x_4 - x_4 \,\}$$

$$\mathcal{F}' = \mathcal{F} \cup \{x_6x_1 - x_6,\; x_1x_6 - x_6, x_6\,(x_5x_2 + x_1) - x_1, \quad (x_5x_2 + x_1)\,x_6 - x_1\}$$

$$\mathcal{V}(\mathcal{F}) \overset{\sim}{\longleftrightarrow} \mathcal{V}(\mathcal{F}')$$

$$\sigma \longmapsto (\sigma_1, \dots, \sigma_5, -\sigma_5\sigma_4\sigma_2 + \sigma_1)$$

$$(\sigma_1, \dots, \sigma_5) \longleftarrow (\sigma_1, \dots, \sigma_5, \sigma_6)$$

$$BA + \mathrm{I}_\ell \in \mathrm{GL}_\ell(\mathbf{k}) \implies (\mathrm{I}_m, B, \mathrm{I}_\ell, (BA + \mathrm{I}_\ell)^{-1}, A) \in \mathcal{V}(\mathcal{F})$$

$$\implies AB + \mathrm{I}_m \in \mathrm{GL}_m(\mathbf{k})$$

Coordinate morphisms

For all $(\mathtt{i}_1, \mathtt{i}_2), (\mathtt{i}_2, \mathtt{i}_3) \in \mathtt{I}$ bilinear

$$b_{\mathtt{i}_1 \mathtt{i}_2 \mathtt{i}_3} : \mathrm{Hom}(\mathtt{i}_2, \mathtt{i}_3)^{\mathcal{V}} \times \mathrm{Hom}(\mathtt{i}_1, \mathtt{i}_2)^{\mathcal{V}} \to \mathrm{Hom}(\mathtt{i}_1, \mathtt{i}_3)^{\mathcal{V}}$$

$$(\beta_2, \beta_1) \mapsto \begin{cases} \mathcal{V} \to \mathrm{Hom}(\mathtt{i}_1, \mathtt{i}_3) \\ \sigma \;\; \mapsto \beta_2(\sigma) \circ \beta_1(\sigma) \end{cases}$$

Definition. $\gamma : \bigcup_{\mathtt{i} \in \mathtt{I}'} \mathcal{O}_{\mathtt{i}} \mathcal{V}' \to \bigcup_{\mathtt{i} \in \mathtt{I}} \mathcal{O}_{\mathtt{i}} \mathcal{V}$ morphism if

(i) $\mathtt{I}' \subseteq \mathtt{I}$

(ii) $\gamma_{\mathtt{i}} : \mathcal{O}_{\mathtt{i}} \mathcal{V}' \to \mathcal{O}_{\mathtt{i}} \mathcal{V}, \beta \mapsto \gamma(\beta)$ module homomorphism $\forall \mathtt{i}$

(iii) $\gamma(b_{\mathtt{i}_1 \mathtt{i}_2 \mathtt{i}_3}(\beta_2, \beta_1)) = b_{\mathtt{i}_1 \mathtt{i}_2 \mathtt{i}_3}(\gamma(\beta_2), \gamma(\beta_1)) \;\; \forall \beta_1, \beta_2$

Theorem. Fully faithful functor

$$F\mathcal{V} := \bigcup_{\mathtt{i} \in \mathtt{I}} \mathcal{O}_{\mathtt{i}} \mathcal{V}$$

and for $\alpha \in \mathrm{Mor}(\mathcal{V}, \mathcal{V}')$

$$F\alpha \in \mathrm{Mor}(F\mathcal{V}', F\mathcal{V})), \; \beta \mapsto \beta \circ \alpha$$

From $\mathbf{k}$-modules to $\mathbf{k}$-algebras

$\gamma := F\alpha \in \mathrm{Mor}(F\mathcal{V}', F\mathcal{V})$

$\forall \mathtt{i} \in \mathtt{I}' \; \exists \zeta_{\mathtt{i}}$: diagram of $\mathbf{k}$-module homomorphisms commutes

$$
\begin{array}{ccc}
\mathcal{O}_{\mathtt{i}}\mathcal{V}' & \xrightarrow{\gamma_{\mathtt{i}}} & \mathcal{O}_{\mathtt{i}}\mathcal{V} \\
\updownarrow \wr & & \updownarrow \wr \\
\mathrm{span}(\mathcal{U}'_{\mathtt{i}}) / \ker(\phi'_{\mathcal{V}'\,\mathtt{i}}) & \overset{\zeta_{\mathtt{i}}}{\dashrightarrow} & \mathrm{span}(\mathcal{U}_{\mathtt{i}}) / \ker(\phi_{\mathcal{V}\,\mathtt{i}})
\end{array}
$$

Lemma. If $\mathbf{k}$ field then

$\forall i \; \exists \tau_i$: diagram of $\mathbf{k}$-module homomorphisms commutes

$$
\begin{array}{ccc}
\mathbf{k}\langle X \rangle & \overset{\pi}{\twoheadrightarrow} & \mathbf{k}\langle X \rangle / \langle \mathcal{J}(\mathcal{V}) \rangle \\
\uparrow \iota_{\mathtt{i}} & & \uparrow \tau_{\mathtt{i}} \\
\mathrm{span}(\mathcal{U}_{\mathtt{i}}) & \overset{\pi_{\mathtt{i}}}{\twoheadrightarrow} & \mathrm{span}(\mathcal{U}_{\mathtt{i}}) / \ker(\phi_{\mathcal{V}\,\mathtt{i}})
\end{array}
$$

Functor from varieties to $\mathbf{k}$-algebras

Theorem. Faithful functor

$$G\mathcal{V} := {}^{\mathbf{k}\langle X\rangle}\big/_{\langle \mathcal{J}(\mathcal{V})\rangle}$$

$\forall \alpha \in \mathrm{Mor}(\mathcal{V},\ \mathcal{V}')\ \exists!\ G\alpha \in \mathrm{Hom}(G\mathcal{V}',\ G\mathcal{V})$: diagram commutes $\forall \mathtt{i} \in \mathtt{I}'$

$$\begin{array}{ccc}
\pi'_{\mathtt{i}}\left(\mathrm{span}(\mathcal{U}'_{\mathtt{i}})\right) & \xrightarrow{\ \zeta_{\mathtt{i}}\ } & \pi_{\mathtt{i}}\left(\mathrm{span}(\mathcal{U}_{\mathtt{i}})\right) \\
\Big\downarrow{\scriptstyle \tau'_{\mathtt{i}}} & & \Big\downarrow{\scriptstyle \tau_{\mathtt{i}}} \\
G\mathcal{V}' & \overset{G\alpha}{\dashrightarrow} & G\mathcal{V} \\
\Big\uparrow{\scriptstyle \pi'\circ\iota'_{\mathtt{i}}} & & \Big\uparrow{\scriptstyle \pi\circ\iota_{\mathtt{i}}} \\
\mathrm{span}(\mathcal{U}'_{\mathtt{i}}) & & \mathrm{span}(\mathcal{U}_{\mathtt{i}})
\end{array}
\qquad
\pi'_{\mathtt{i}} : \mathrm{span}(\mathcal{U}'_{\mathtt{i}}) \twoheadrightarrow \pi'_{\mathtt{i}}\left(\mathrm{span}(\mathcal{U}'_{\mathtt{i}})\right),\quad
\pi_{\mathtt{i}} : \mathrm{span}(\mathcal{U}_{\mathtt{i}}) \twoheadrightarrow \pi_{\mathtt{i}}\left(\mathrm{span}(\mathcal{U}_{\mathtt{i}})\right)$$

Corollary.

(i) $G\alpha(\pi'(x_j)) = \pi(f_j)$ where $\alpha_j = \phi_{\mathcal{V}\,(\mathcal{M}'_j,\,\mathcal{N}'_j)}(f_j)$

(ii) $\mathcal{V} \cong \mathcal{V}' \implies G\mathcal{V} \cong G\mathcal{V}'$

(iii) $\exists G\alpha,\ G\alpha' :\ G\alpha\circ G\alpha' = \mathrm{id}_{G\mathcal{V}} \wedge G\alpha'\circ G\alpha = \mathrm{id}_{G\mathcal{V}'} \implies \mathcal{V} \cong \mathcal{V}'$

Application: Stabilizing controllers

Theorem. Transcendental extension $\mathbf{k} = \mathbb{R}(\mathrm{z})$

$$X_0 = \left\{ A,\ (\mathrm{z}\,\mathrm{I}_m - A)^{-1},\ \mathrm{I}_m,\ B_2,\ C_2,\ \mathrm{I}_p \right\}$$

$$\mathbf{A_0} = \mathrm{End}(\mathbf{k}^m)^4 \times \mathrm{Hom}(\mathbf{k}^m, \mathbf{k}^p) \times \mathrm{End}(\mathbf{k}^p)$$

$$\begin{aligned}\mathcal{F}_0 = \{ &(\mathrm{z}\,\mathrm{I}_m - A)(\mathrm{z}\,\mathrm{I}_m - A)^{-1} - \mathrm{I}_m, \\ &(\mathrm{z}\,\mathrm{I}_m - A)^{-1}(\mathrm{z}\,\mathrm{I}_m - A) - \mathrm{I}_m, \\ &\mathrm{I}_p^2 - \mathrm{I}_p,\ \mathrm{I}_m^2 - \mathrm{I}_m,\ A\,\mathrm{I}_m - A,\ B_2\mathrm{I}_m - B_2,\ C_2\mathrm{I}_m - C_2, \\ &(\mathrm{z}\,\mathrm{I}_m - A)^{-1}\mathrm{I}_m - (\mathrm{z}\,\mathrm{I}_m - A)^{-1},\ \mathrm{I}_m A - A, \\ &\mathrm{I}_m B_2 - B_2,\ \mathrm{I}_p C_2 - C_2,\ \mathrm{I}_m(\mathrm{z}\,\mathrm{I}_m - A)^{-1} - (\mathrm{z}\,\mathrm{I}_m - A)^{-1} \}\end{aligned}$$

[4] **D. Youla**, **H. Jabr**, and **J. Bongiorno**. *"Modern Wiener-Hopf design of optimal controllers II: The multivariable case"*. IEEE Transactions on Automatic Control. **1976**

[5] **Y. Zheng**, **L. Furieri**, **A. Papachristodoulou**, **N. Li**, and **M. Kamgarpour**. *"On the equivalence of Youla, system-level and input-output parameterizations"*. IEEE Transactions on Automatic Control. **2020**

Application: Stabilizing controllers

System-level parametrization $\mathbf{A} = \mathbf{A_0} \times \mathrm{End}(\mathbf{k}^m)^2 \times \mathrm{Hom}(\mathbf{k}^p, \mathbf{k}^m)^2$

$$X = X_0 \cup \{R, M, N, L\}$$

$$\begin{aligned}\mathcal{F} = \mathcal{F}_0 \cup \{\, & (\mathrm{z}\,\mathrm{I}_m - A)R - B_2 M - \mathrm{I}_m,\ (\mathrm{z}\,\mathrm{I}_m - A)N - B_2 L,\\ & R(\mathrm{z}\,\mathrm{I}_m - A) - NC_2 - \mathrm{I}_m,\ M(\mathrm{z}\,\mathrm{I}_m - A) - LC_2,\\ & R\,\mathrm{I}_m - R,\ N\,\mathrm{I}_p - N,\ M\,\mathrm{I}_m - M,\ L\,\mathrm{I}_p - L,\\ & \mathrm{I}_m R - R,\ \mathrm{I}_m N - N,\ \mathrm{I}_m M - M,\ \mathrm{I}_m L - L\,\}\end{aligned}$$

Input-output parametrization

$$\mathbf{A}' := \mathbf{A_0} \times \mathrm{End}(\mathbf{k}^p) \times \mathrm{Hom}(\mathbf{k}^p, \mathbf{k}^m) \times \mathrm{Hom}(\mathbf{k}^m, \mathbf{k}^p) \times \mathrm{End}(\mathbf{k}^m)$$

$$X' = X_0 \cup \{Y, U, W, Z\}$$

$$\begin{aligned}\mathcal{F}' = \mathcal{F}_0 \cup \{\, & \mathrm{I}_p Y - C_2(z\,\mathrm{I}_m - A)^{-1} B_2 U - \mathrm{I}_p,\ \mathrm{I}_p W - C_2(z\,\mathrm{I}_m - A)^{-1} B_2 Z,\\ & -YC_2(z\,\mathrm{I}_m - A)^{-1} B_2 + W\mathrm{I}_m,\ -UC_2(z\,\mathrm{I}_m - A)^{-1} B_2 + Z\mathrm{I}_m - \mathrm{I}_m,\\ & Y\mathrm{I}_p - Y,\ U\mathrm{I}_p - U,\ W\mathrm{I}_m - W,\ Z\mathrm{I}_m - Z,\\ & \mathrm{I}_p Y - Y,\ \mathrm{I}_m U - U,\ \mathrm{I}_p W - W,\ \mathrm{I}_m Z - Z\,\}\end{aligned}$$

$$\implies \mathcal{V}(\mathcal{F}) \cong \mathcal{V}(\mathcal{F}')$$

Future work

- Applications in **elementary homology**, theory on **generalized inverses** [6,7,8,12] and **control theory** [4,8]
- Interconnection with noncommutative algebraic geometry [10]
- Related **computational issues** with Gröbner bases [11]

[6] **D. Cvetkovic-Ilic**, **C. Hofstadler**, **J. Hossein Poor**, **J. Milosevic**, **C. Raab**, and **G. Regensburger**. *"Algebraic proof methods for identities of matrices and operators: improvements of Hartwig's triple reverse order law"*. **2020**

[7] **T. Damm** and **H. K. Wimmer**. *"A cancellation property of the Moore-Penrose inverse of triple products"*. J. Aust. Math. Soc.. **2009**

[8] **M. P. Drazin**. *"Left and right generalized inverses"*. Linear Algebra and its Applications. **2016**

[9] **L. Furieri**, **Y. Zheng**, **A. Papachristodoulou**, and **M. Kamgarpour**. *"An input–output parametrization of stabilizing controllers: Amidst Youla and system level synthesis"*. IEEE Control Systems Letters. **2019**

[10] **J. W. Helton**, **I. Klep**, and **J. Volčič**. *"Factorization of noncommutative polynomials and Nullstellensätze for the free algebra"*. International Mathematics Research Notices. **2020**

[11] **V. Levandovskyy**, **T. Metzlaff**, and **K. A. Zeid**. *"Computations of free non-commutative Gröbner bases over $\mathbb{Z}$ with Singular:Letterplace"*. ISSAC. **2020**

[12] **D. W. Robinson** and **R. Puystjens**. *"Generalized inverses of morphisms with kernels"*. Linear Algebra and its Applications. **1987**