Computation of the Hilbert Series for the Support-Minors modeling of the MinRank pb

arxiv.org/abs/2502.12721

Magali Bardet Alban Gilard

magali.bardet@univ-rouen.fr
alban.gilard@univ-rouen.fr

JNCF 2025, March 13, 2025

Laboratoire d'Informatique, du Traitement de l'Information et des Systèmes

Université de Rouen Normandie

NIST Post-Quantum Cryptography Standardization Process, 2016–2025–?

- mathematical problems resistant to quantum computer.
- 4 Rounds since 2017.
- first selection for standardization in 07/2022, FIPS standards:
  - 1 lattice-based KEM: ML-KEM[1];
  - 2 lattice-based signatures: ML-DSA, FN-DSA[2];
  - 1 Hash-based signature: SLH-DSA[3].
- 1 code-based KEM selected *two days ago*: HQC-KEM[4] (*my guess for the name*).

[1] FIPS 203 and FIPS 204 Module-Lattice-Based KEM and DSA Standard, 08/2024.
[2] FIPS 206 Fast Fourier Transform over NTRU Lattices DSA, under development
[3] FIPS 205 Stateless Hash-Based DSA Standard, 08/2024
[4] Hamming Quasi-Cyclic, selected on 11/03/2025

NIST Post-Quantum Cryptography Standardization Process, 2016–2025–?

- mathematical problems resistant to quantum computer.
- 4 Rounds since 2017.
- first selection for standardization in 07/2022, FIPS standards:
  - 1 lattice-based KEM: ML-KEM[1];
  - 2 lattice-based signatures: ML-DSA, FN-DSA[2];
  - 1 Hash-based signature: SLH-DSA[3].
- 1 code-based KEM selected *two days ago*: HQC-KEM[4] (*my guess for the name*).

Most important parameter for the choice: **confidence in the security** of the scheme.

[1] FIPS 203 and FIPS 204 Module-Lattice-Based KEM and DSA Standard, 08/2024.
[2] FIPS 206 Fast Fourier Transform over NTRU Lattices DSA, under development
[3] FIPS 205 Stateless Hash-Based DSA Standard, 08/2024
[4] Hamming Quasi-Cyclic, selected on 11/03/2025

NIST call for Digital Signatures

Additional Digital Signature Schemes, 06/2023–

- 10/2024–. Round 2 ongoing.
- 14 submissions, with:
  - multivariate Signatures: **MAYO, QR-UOV, UOV, SNOVA**;
  - code-based Signatures: **CROSS, LESS**;
  - Symmetric-based Signatures: **FAEST**;
  - Lattice-based Signatures: **HAWK**;
  - Isogeny Signatures: **SQIsign**.
  - MPC-in-the-Head Signatures: **Mirath, MQOM, PERK, RYDE, SDitH**.

NIST call for Digital Signatures

Additional Digital Signature Schemes, 06/2023–

- 10/2024–. Round 2 ongoing.
- 14 submissions, with:
  - multivariate Signatures: **MAYO, QR-UOV, UOV, SNOVA**;
  - code-based Signatures: **CROSS, LESS**;
  - Symmetric-based Signatures: **FAEST**;
  - Lattice-based Signatures: **HAWK**;
  - Isogeny Signatures: **SQIsign**.
  - MPC-in-the-Head Signatures: **Mirath,** **MQOM, PERK, RYDE, SDitH**.

based on random MinRank instances

The MinRank Problem

- `Input`: integers $r, m, n \in \mathbb{N}$, and K matrices $M_1, \ldots, M_K \in \mathbb{F}_q^{m \times n}$
- `Output`: $(x_1, \ldots, x_K) \in \mathbb{F}_q$, not all zero, such that

$$\mathrm{Rank}\left(M_{\boldsymbol{x}} \stackrel{\text{def}}{=} \sum_{i=1}^{K} x_i M_i \right) \leq r.$$

The MinRank Problem

- `Input`: integers $r, m, n \in \mathbb{N}$, and K matrices $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{m \times n}$
- `Output`: $(x_1, \ldots, x_K) \in \mathbb{F}_q$, not all zero, such that

$$\mathrm{Rank}\left(\boldsymbol{M}_{\boldsymbol{x}} \stackrel{\text{def}}{=} \sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leq r.$$

- NP-complete problem Buss, Frandsen, and Shallit (1999),

The MinRank Problem

- `Input`: integers $r, m, n \in \mathbb{N}$, and K matrices $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{m \times n}$
- `Output`: $(x_1, \ldots, x_K) \in \mathbb{F}_q$, not all zero, such that

$$\mathrm{Rank}\left(\boldsymbol{M}_{\boldsymbol{x}} \stackrel{\text{def}}{=} \sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leq r.$$

- NP-complete problem Buss, Frandsen, and Shallit (1999),
- used to cryptanalyse various multivariate and code-based cryptosystems,

The MinRank Problem

- `Input`: integers $r, m, n \in \mathbb{N}$, and K matrices $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{m \times n}$
- `Output`: $(x_1, \ldots, x_K) \in \mathbb{F}_q$, not all zero, such that

$$\mathrm{Rank}\left(\boldsymbol{M}_{\boldsymbol{x}} \stackrel{\text{def}}{=} \sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leq r.$$

- NP-complete problem Buss, Frandsen, and Shallit (1999),
- used to cryptanalyse various multivariate and code-based cryptosystems,
- This is exactly the decoding problem for matrix codes,

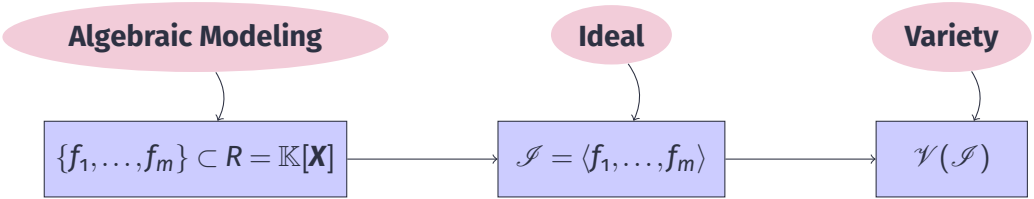
The MinRank Problem

- `Input`: integers $r, m, n \in \mathbb{N}$, and K matrices $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_K \in \mathbb{F}_q^{m \times n}$
- `Output`: $(x_1, \ldots, x_K) \in \mathbb{F}_q$, not all zero, such that

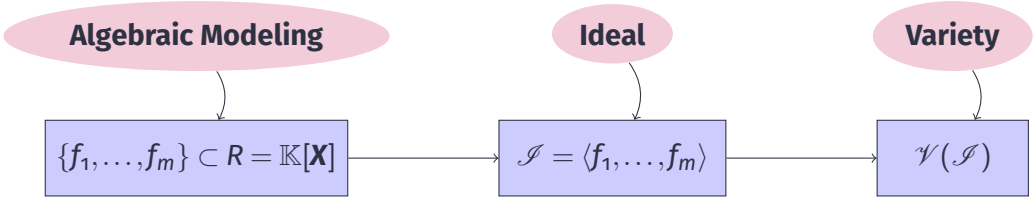
$$\mathrm{Rank}\left(\boldsymbol{M}_{\boldsymbol{x}} \stackrel{\text{def}}{=} \sum_{i=1}^{K} x_i \boldsymbol{M}_i\right) \leq r.$$

- NP-complete problem Buss, Frandsen, and Shallit (1999),
- used to cryptanalyse various multivariate and code-based cryptosystems,
- This is exactly the decoding problem for matrix codes,
- Generalized MinRank Problem: the entries of $\boldsymbol{M}_{\boldsymbol{x}}$ are polynomials of degree D in the $\boldsymbol{x}$ variables.

Estimate the cost of solving the MinRank problem?

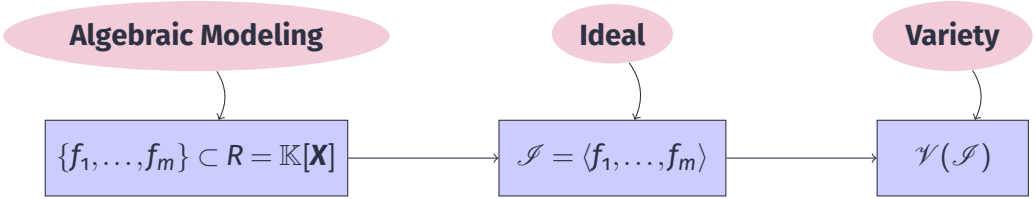


Estimate the cost of solving the MinRank problem?



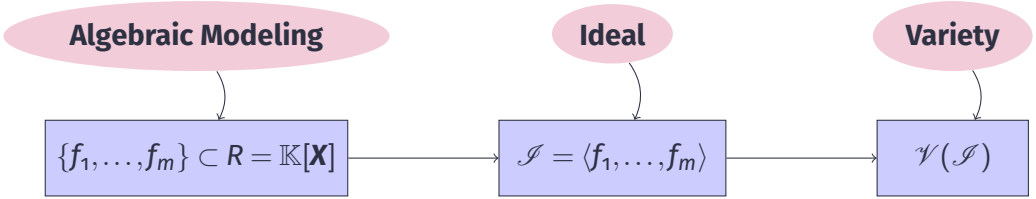
- $\mathbb{K}$-Vector spaces $\mathscr{I}_d \stackrel{\text{def}}{=} \langle \mathfrak{m} f_i : \mathfrak{m} \text{ monomial}, \deg(\mathfrak{m} f_i) = d \rangle_{\mathbb{K}}$, $d \geq 0$.

Estimate the cost of solving the MinRank problem?



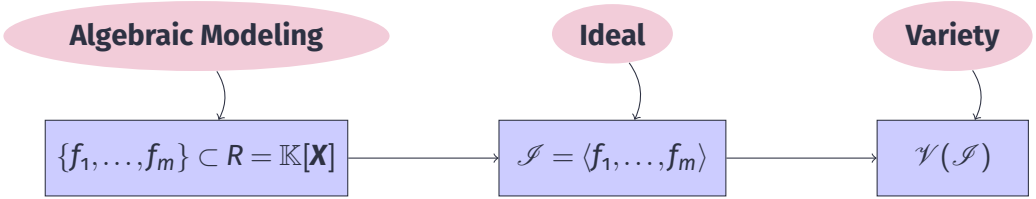
- $\mathbb{K}$-Vector spaces $\mathscr{I}_d \stackrel{\text{def}}{=} \langle \mathfrak{m} f_i : \mathfrak{m} \text{ monomial}, \deg(\mathfrak{m} f_i) = d \rangle_{\mathbb{K}}$, $d \geq 0$.
- $\mathscr{I} = \langle f_1,\ldots,f_m\rangle = \oplus_d \mathscr{I}_d$,

Estimate the cost of solving the MinRank problem?



- $\mathbb{K}$-Vector spaces $\mathscr{I}_d \stackrel{\text{def}}{=} \langle \mathfrak{m} f_i : \mathfrak{m} \text{ monomial}, \deg(\mathfrak{m} f_i) = d \rangle_{\mathbb{K}}$, $d \geq 0$.
- $\mathscr{I} = \langle f_1,\ldots,f_m\rangle = \oplus_d \mathscr{I}_d$,
- Lazard (1983) and Giusti (1984): *linear algebra* $\rightarrow$ basis of all $\mathscr{I}_d$ up to degree $D_s \rightarrow$ Gröbner basis of $\mathscr{I} \rightarrow$ solutions of the system.

Estimate the cost of solving the MinRank problem?



- $\mathbb{K}$-Vector spaces $\mathscr{I}_d \stackrel{\text{def}}{=} \langle \mathfrak{m} f_i : \mathfrak{m} \text{ monomial}, \deg(\mathfrak{m} f_i) = d \rangle_{\mathbb{K}}$, $d \geq 0$.
- $\mathscr{I} = \langle f_1,\ldots,f_m\rangle = \oplus_d \mathscr{I}_d$,
- Lazard (1983) and Giusti (1984): *linear algebra* $\rightarrow$ basis of all $\mathscr{I}_d$ up to degree $D_s \rightarrow$ Gröbner basis of $\mathscr{I} \rightarrow$ solutions of the system.
- Hilbert Series for a system with generic coefficients

$$HS_{R/\mathscr{I}}(t) = \sum_{d \in \mathbb{N}} \dim_{\mathbb{K}}(R/\mathscr{I})_d t^d$$

provides an upper-bound on D_s for generic systems.

Algebraic Modelings for MinRank: $\mathrm{Rank}(\boldsymbol{M_X}) \leq r$

- Kipnis-Shamir modeling (Kipnis and Shamir (1999))

$$\boldsymbol{M_X}\begin{pmatrix} \boldsymbol{I}_{n-r} \\ -\boldsymbol{C} \end{pmatrix} = \mathrm{O}_{m\times(n-r)}, \quad \boldsymbol{C} \in \mathbb{K}^{r\times(n-r)}, \boldsymbol{x}_i \in \mathbb{K} \tag{KS}$$

Algebraic Modelings for MinRank: $\mathrm{Rank}(M_X) \leq r$

- Minors modeling (Faugère, Safey El Din, and Spaenlehauer (2010))

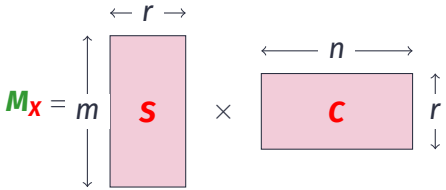
$$\mathrm{Minors}_{r+1}(M_X) = 0 \qquad \text{(Minors)}$$

$$\mathrm{HS}_{\mathrm{Minors}}(t) = \left[\frac{\det(B(t^D))(1-t^D)^{(m-r)(n-r)}}{(1-t)^K} \right]_+$$

$$\text{where } B(t) = \left(\sum_{\ell \geq 0} \binom{n-i}{\ell+j-i} \binom{m-j}{\ell} t^\ell \right)_{1 \leq i,j \leq r}.$$

- The complete Hilbert Series is known, genericity is proven for $K \geq (m-r)(n-r)$.

Support Minors modeling

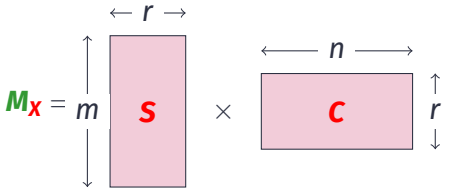


- Support Minors modeling (Bardet, Bros, et al. (2020))

$$\text{Minors}_{r+1}\begin{pmatrix}(M_X)_{j,*}\\ C\end{pmatrix} = 0 \qquad \forall j \in \{1..m\}. \qquad \text{(SM)}$$

with a change of variables for the *minors variables* $c_T = \det\left(C_{*,T}\right)$, $T \subset \{1..n\}, \#T = r$.

Support Minors modeling



- Support Minors modeling (Bardet, Bros, et al. (2020))

$$\text{Minors}_{r+1}\begin{pmatrix}(M_X)_{j,*}\\ C\end{pmatrix} = 0 \qquad \forall j \in \{1..m\}. \qquad \text{(SM)}$$

with a change of variables for the *minors variables* $c_T = \det\left(C_{*,T}\right)$, $T \subset \{1..n\}, \#T = r$.

- the equations are bilinear in the X and c_T's $\rightarrow$ bi-grading in (d_x, d_c).
- The first terms of the bi-Hilbert Series are *conjectured* for $d_c = 1, d_x \leq r+1$.

This work: Hilbert Series for Support Minors

- $R = \mathbb{K}[\boldsymbol{X}, \boldsymbol{C}_T]$ the algebra generated by the $\boldsymbol{X}$ variables and the minors $\boldsymbol{C}_T$ of $\boldsymbol{C}$,

This work: Hilbert Series for Support Minors

- $R = \mathbb{K}[\boldsymbol{X}, \boldsymbol{C}_T]$ the algebra generated by the $\boldsymbol{X}$ variables and the minors $\boldsymbol{C}_T$ of $\boldsymbol{C}$,
- $\mathscr{I} = \langle \mathrm{SM} \rangle_R = \oplus_{d_x,d_c} \mathscr{I}_{d_x,d_c}$, $\mathscr{I}_{d_c} = \oplus_{d_x} \mathscr{I}_{d_x,d_c}$,

This work: Hilbert Series for Support Minors

- $R = \mathbb{K}[\boldsymbol{X}, \boldsymbol{C}_T]$ the algebra generated by the $\boldsymbol{X}$ variables and the minors $\boldsymbol{C}_T$ of $\boldsymbol{C}$,
- $\mathscr{I} = \langle \mathrm{SM} \rangle_R = \oplus_{d_x,d_c} \mathscr{I}_{d_x,d_c}$, $\mathscr{I}_{d_c} = \oplus_{d_x} \mathscr{I}_{d_x,d_c}$,

This work: Hilbert Series for Support Minors

- $R = \mathbb{K}[\boldsymbol{X}, \boldsymbol{C}_T]$ the algebra generated by the $\boldsymbol{X}$ variables and the minors $\boldsymbol{C}_T$ of $\boldsymbol{C}$,
- $\mathscr{I} = \langle \mathrm{SM} \rangle_R = \oplus_{d_x,d_c} \mathscr{I}_{d_x,d_c}$, $\mathscr{I}_{d_c} = \oplus_{d_x} \mathscr{I}_{d_x,d_c}$,

$$\mathrm{HS}_{\mathbb{K}[\boldsymbol{X}][\boldsymbol{C}_I]_{d_c}/\mathscr{I}_{d_c}}(t) = \left[\frac{\det(B_{d_c}(t^D))(1-t^D)^{(m-r)(n-r)}}{(1-t)^K} \right]_+$$

$$\text{where } B_{d_c}(t) = \left(\sum_{\ell \geq 0} \binom{n+d_c-i}{\ell+d_c+j-i} \binom{m-d_c-j}{\ell} t^\ell \right)_{1 \leq i,j \leq r}.$$

- genericity proven for $K \geq m(n-r)$, conjectured otherwise.

Transfering determinantal properties, d_c fixed

$$\boldsymbol{C} = \begin{pmatrix} c_{1,1} & \cdots & c_{1,n} \\ \vdots & & \vdots \\ c_{r,1} & \cdots & c_{r,n} \end{pmatrix}, \boldsymbol{U} = \begin{pmatrix} u_{1,1} & \cdots & u_{1,n} \\ \vdots & & \vdots \\ u_{m,1} & \cdots & u_{m,n} \end{pmatrix} \longrightarrow \begin{pmatrix} \boldsymbol{C} \\ \boldsymbol{U} \end{pmatrix}$$

- We compute the Hilbert Series of the Determinantal Support Minors ideal in $\mathbb{K}[\boldsymbol{U}][\boldsymbol{C}_T]_{d_c}$ $\rightarrow$ $\mathrm{HS}(t)$
- weight D on $u_{i,j}$ + add the K variables $\boldsymbol{X}$ $\rightarrow$ $\mathrm{HS}(t^D)\frac{1}{(1-t)^K}$
- We add mn generic forms[5] in the $\boldsymbol{X}$ and $\boldsymbol{U}$ variables, they are non-zero divisor at least[6] for $K \geq (m+r-r)(n-r)$ $\rightarrow$ $\mathrm{HS}(t^D)\frac{(1-t^D)^{mn}}{(1-t^K)}$

Over $\overline{\mathbb{K}}$, the set of systems with $u_{i,j}$ polynomials in $\boldsymbol{X}$ having the same Hilbert Series is a non-empty open Zarisky set.

[5] The coefficients are new variables $\mathfrak{b}, \mathfrak{c}$, we compute in $\mathbb{K}(\mathfrak{b}, \mathfrak{c})$

[6] it is true in $\mathbb{K}(\mathfrak{b}, \mathfrak{c})[\boldsymbol{U}, \boldsymbol{C}]$

Minors and bivectors

$$\boldsymbol{U} = \begin{pmatrix} u_{1,1} & \cdots & u_{1,n} \\ \vdots & & \vdots \\ u_{m,1} & \cdots & u_{m,n} \end{pmatrix}.$$

- $(a|b) = (a_p, ..., a_1|b_1, ..., b_p) =$ minors of $\boldsymbol{U}$ with rows indexed by a and columns indexed by b.
  $1 \leq a_1 < a_2 < \cdots < a_p \leq m$ and $1 \leq b_1 < b_2 < \cdots < b_p \leq n$.

$(4,2,1|1,2,3)$ represents the minor $\begin{vmatrix} u_{1,1} & u_{1,2} & u_{1,3} \\ u_{2,1} & u_{2,2} & u_{2,3} \\ u_{4,1} & u_{4,2} & u_{4,3} \end{vmatrix}$.

Partial Order

Partial order on the sets of all minors of $\boldsymbol{U}$

$(a_p, \ldots, a_1 | b_1, \ldots, b_p) \leq (\alpha_s, \cdots, \alpha_1 | \beta_1, \cdots, \beta_s)$ if and only if:

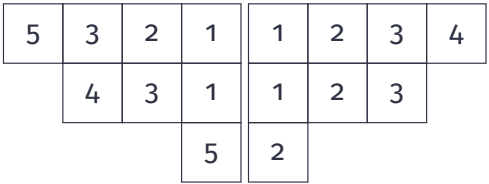
- $p \geq s$, and
- $a_i \leq \alpha_i$ and $b_i \leq \beta_i$ for all $1 \leq i \leq s$.

Examples

- $(4,2,1|1,2,3) \leq (5,2|2,3) \leq (5,4|3,4)$
- $(4,3,1|1,2,3) \not\leq (2,1|2,3)$
- $(5,2|2,3) \not\leq (5,1|2,3)$

Standard Monomials

$Y = \gamma_1 \cdots \gamma_t$ is a Standard monomial if $\gamma_1 \leq \cdots \leq \gamma_t$ with γ_i minors of $\boldsymbol{U}$.

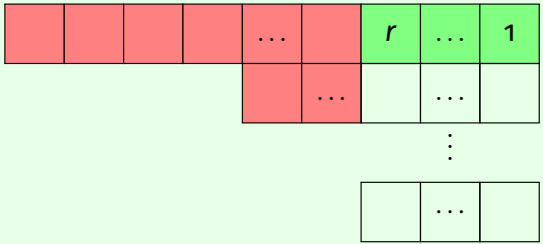


- shape $(3,2,2,1)$,
- length 4,
- degree 8.

- Standard monomials form a basis of $\mathbb{K}[\boldsymbol{U}]$ as a $\mathbb{K}$-vector space.
- Straightening law to rewrite non-standard monomials.
- The number of standard monomials of a given shape is known.

Generating set for the Support-Minors ideal

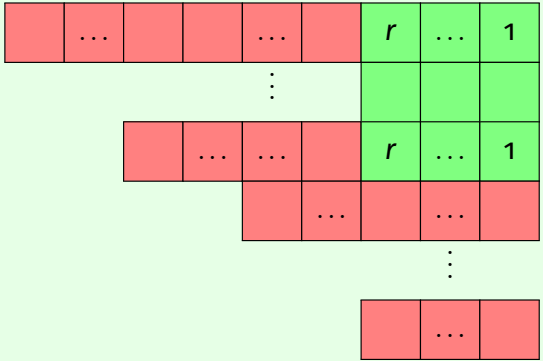
Lemma: the standard monomials with left tableau



form a $\mathbb{K}$-basis of the ideal $\langle \mathrm{SM} \rangle_{\mathbb{K}[\boldsymbol{U},\boldsymbol{C}]}$.

$> r$ $\leq r$

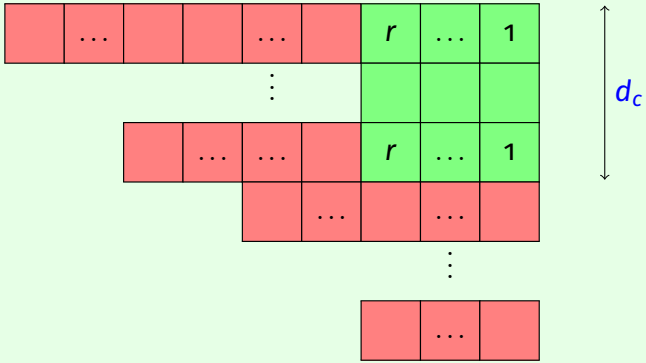
Lemma: the standard monomials with left tableau



form a $\mathbb{K}$-basis of the ideal $\langle \mathrm{SM} \rangle_{\mathbb{K}[\boldsymbol{u},\boldsymbol{c}_T]}$.

$> r$ $\leq r$

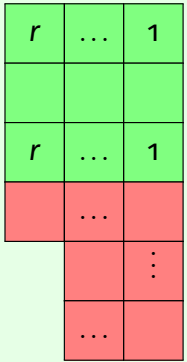
Lemma: the standard monomials with left tableau

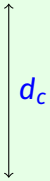


form a $\mathbb{K}$-basis of the ideal $\langle \mathrm{SM} \rangle_{\mathbb{K}[\boldsymbol{U},\boldsymbol{C}_T]_{d_c}}$.

$> r$ $\leq r$

Lemma: the standard monomials with left tableau





form a $\mathbb{K}$-basis of $R/\langle \mathrm{SM} \rangle_{\mathbb{K}[\boldsymbol{u},\boldsymbol{c}_T]_{d_c}}$.

$> r$ $\leq r$

Theorem (B., Gilard). For all $d_c \geq 1$, we have:

$$\mathrm{HS}_{\mathbb{K}[\boldsymbol{u}]_{d_c}/\mathscr{S}_{d_c}}(t) = \sum_{d_u \geq 0} m_{d_u,d_c} t^{d_u}$$

where

$$m_{d_u,d_c} = \sum_{v \overset{r}{\rightsquigarrow} d_u} \det\left(\begin{bmatrix} m-j \\ v(i)+j-i \end{bmatrix}\right)_{1\leq i,j\leq r} \det\left(\begin{bmatrix} n-j \\ v(i)+d_c+j-i \end{bmatrix}\right)_{1\leq i,j\leq r}$$

$$\begin{bmatrix} a \\ b \end{bmatrix} = \binom{a+b}{b}$$

The sum is over all shapes that have degree d_u and indices in $\{r+1..r+m\}$.

Compact formula

Factorization as a determinant with the Cauchy-Binet Formula Galligo (1983) + Saalschütz formula Gessel and Stanton (1985):

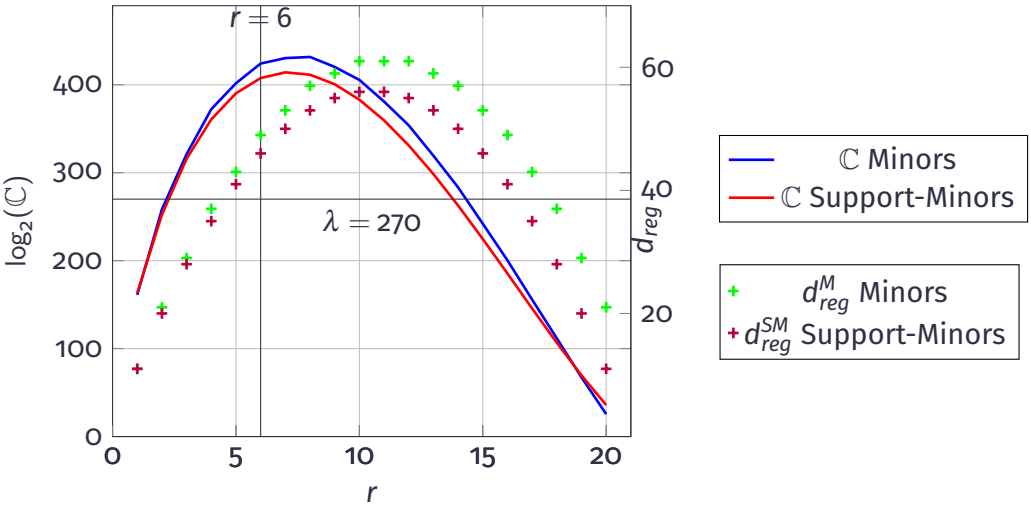
For all $d_c \geq 1$,

$$\mathrm{HS}_{\mathbb{K}[\boldsymbol{u}]_{d_c}/\mathscr{S}_{d_c}}(t) = \det\left(\Delta_{d_c}(t)\right) = \frac{\det(B_{d_c}(t))}{(1-t)^{(m+n-r)r}}$$

where $\Delta_{d_c}(t) = \left(\sum_{\ell \geq 0} \begin{bmatrix} m-i \\ \ell \end{bmatrix} \begin{bmatrix} n-j \\ \ell + d_c + j - i \end{bmatrix} t^\ell\right)_{1 \leq i,j \leq r}$

and $B_{d_c}(t) = \left(\sum_{\ell \geq 0} \binom{n+d_c-i}{\ell+d_c+j-i} \binom{m-d_c-j}{\ell} t^\ell\right)_{1 \leq i,j \leq r}$

MIRATH-V ($m = n = 22$, $r = 6$, $K = (m-r)(n-r)-1$, $\mathbb{F}_{16}$)



Parameters for Mirath with Support Minors

					Before				This work			
Security level	m	n	K	r	$\log_2(\mathbb{C})$	d_c	d_{reg}	a	$\log_2(\mathbb{C})$	d_c	d_{reg}	a
NIST-I	16	16	143	4	166	1	2	8	**164**	1	6	5
NIST-III	19	19	195	5	227	1	6	7	227	1	6	7
NIST-V	22	22	255	6	301	1	1	11	**298**	1	10	7

- $\mathbb{C} = 3K(r+1)\binom{n}{r}^2\binom{K+d_{reg}^{SM}-1}{d_{reg}^{SM}}^2$ with the Wiedemann algorithm.
- $\mathbb{C}(m,n,K,r) = q^{ar}\mathbb{C}(m,n-a,K-am,r)$ (Bardet, Briaud, et al. (2023))

Conclusion and future work

- We computed the Hilbert Series for generic Support Minors ideals.
- Those results comfort the choice of parameters for Mirath and the security of the scheme.
- By-product: the equations $\text{Minors} \times \boldsymbol{C}_T$ are in SM for any $\boldsymbol{C}_T$ at degree $(r+1, 1)$.
- Experiments for $d_c = 1$ for small values of n up to large d_x.
- Experiments for $d_c > 1$ will need the Plücker relations between minors.
- F_5 criterion to construct full rank matrices?

arxiv.org/abs/2502.12721

This research was funded by the French *Agence Nationale de la Recherche* and *plan France 2030* program under grant ANR-22-PETQ-0008 PQ-TLS.

- Bardet, Magali, Pierre Briaud, et al. (2023). **"Revisiting Algebraic Attacks on MinRank and on the Rank Decoding Problem".** In: *Designs, Codes and Cryptography* 91, pp. 3671–3707.
- Bardet, Magali, Maxime Bros, et al. (2020). **"Improvements of Algebraic Attacks for solving the Rank Decoding and MinRank problems".** In: *Advances in Cryptology - ASIACRYPT 2020, International Conference on the Theory and Application of Cryptology and Information Security, 2020. Proceedings*, pp. 507–536.
- Buss, Jonathan F., Gudmund S. Frandsen, and Jeffrey O. Shallit (June 1999). **"The Computational Complexity of Some Problems of Linear Algebra".** In: *J. Comput. System Sci.* 58.3, pp. 572–596.
- Faugère, Jean-Charles, Mohab Safey El Din, and Pierre-Jean Spaenlehauer (2010). **"Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology".** In: *International Symposium on Symbolic and Algebraic Computation, ISSAC 2010, Munich, Germany, July 25-28, 2010*, pp. 257–264.

- Galligo, André (Oct. 1983). **"Computation of some Hilbert functions related to Schubert Calculus".** In: *Algebraic Geometry, Sitges (Barcelona, Spain), 1983*. Ed. by Gerald Welters Eduardo Casas-Alvero and Sebastian Xambó-Descamps. Vol. 1124. Algebraic Geometry, Sitges (Barcelona, Spain), 1983. Document d'archive. Sebastian Xambó-Descamps. Sitges, Spain: Springer, Berlin, pp. 79–97.
- Gessel, Ira and Dennis Stanton (1985). **"Short Proofs of Saalschütz's and Dixon's theorems".** In: *Journal of Combinatorial Theory, Series A* 38.1, pp. 87–90.
- Giusti, M. (1984). **"Some effectivity problems in polynomial ideal theory".** In: *Eurosam 84*. Ed. by John Fitch. Vol. 174. Lecture Notes in Computer Science. Cambridge, 1984. Berlin: Springer Berlin / Heidelberg, pp. 159–171.
- Kipnis, Aviad and Adi Shamir (Aug. 1999). **"Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization".** In: *Advances in Cryptology - CRYPTO'99*. Vol. 1666. LNCS. Santa Barbara, California, USA: Springer, pp. 19–30.
- Lazard, D. (1983). **"Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations".** In: *Computer algebra*. Vol. 162. LNCS. Proceedings Eurocal'83, London, 1983. Berlin: Springer, pp. 146–156.

Support-Minors Hilbert series

Proposition Bardet, Bros, et al. (2020)

We fix $d_c = 1$. Then $HS(t) = \left[\sum_{d_x} a_{d_x} t^{d_x}\right]_+$, with

$$a_{d_x,1} = \sum_{i=1}^{d_x} (-1)^{i+1} \binom{n}{r+i} \binom{m+i-1}{i} \binom{K+d_x-i-1}{d_x-i}$$

as long as $1 \leq d_x \leq r+1$.

Degree of regularity

Proposition

If $K = (m-r)(n-r)$ and $d_c \leq m-r$, for generic SM instances,

$$\begin{aligned} d_{reg}^{\mathrm{SM}} &\leq rD(\min(m-d_c, n)-r)+(D-1)K+1 \\ d_{reg}^{\mathrm{SM}}(D=2) &\leq r(\min(m-d_c, n)-r)+1 \\ d_{reg}^{\mathrm{Minors}} &\leq rD(\min(m, n)-r)+(D-1)K+1 \end{aligned}$$