Symmetric Determinantal Representations of Polynomials in Characteristic 2

Bruno Grenet — ÉNS Lyon
Thierry Monteil — U. Montpellier
Stéphan Thomassé — ÉNS Lyon

Journées Nationales du Calcul Formel
CIRM, Marseille — 15 novembre 2011

Introduction

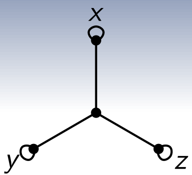
$$xy + yz + xz$$

Introduction

$$xy + yz + xz = \det \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & x & 0 & 0 \\ 1 & 0 & y & 0 \\ 1 & 0 & 0 & z \end{bmatrix}$$

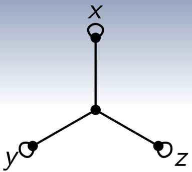
Introduction

$$xy + yz + xz = \det \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & x & 0 & 0 \\ 1 & 0 & y & 0 \\ 1 & 0 & 0 & z \end{bmatrix}$$



Introduction

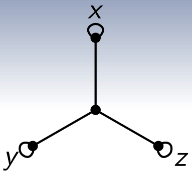
$$xy + yz + xz = \det \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & x & 0 & 0 \\ 1 & 0 & y & 0 \\ 1 & 0 & 0 & z \end{bmatrix}$$



$$xz^2 + y^3 + y^2 + z^2$$

Introduction

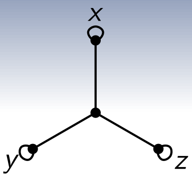
$$xy + yz + xz = \det \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & x & 0 & 0 \\ 1 & 0 & y & 0 \\ 1 & 0 & 0 & z \end{bmatrix}$$



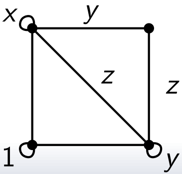
$$xz^2 + y^3 + y^2 + z^2 = \det \begin{bmatrix} x & y & z & 1 \\ y & 0 & z & 0 \\ z & z & y & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

Introduction

$$xy + yz + xz = \det \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & x & 0 & 0 \\ 1 & 0 & y & 0 \\ 1 & 0 & 0 & z \end{bmatrix}$$

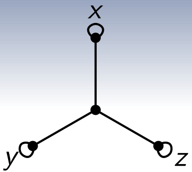


$$xz^2 + y^3 + y^2 + z^2 = \det \begin{bmatrix} x & y & z & 1 \\ y & 0 & z & 0 \\ z & z & y & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

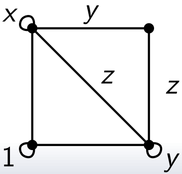


Introduction

$$xy + yz + xz = \det \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & x & 0 & 0 \\ 1 & 0 & y & 0 \\ 1 & 0 & 0 & z \end{bmatrix}$$



$$xz^2 + y^3 + y^2 + z^2 = \det \begin{bmatrix} x & y & z & 1 \\ y & 0 & z & 0 \\ z & z & y & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$



What about $xy + z$?

Formalization

Symmetric Determinantal Representation

SDR of $p \in \mathbb{F}[x_1, \ldots, x_m]$:

- **Symmetric** matrix M;
- Entries: elements of $\mathbb{F} \cup \{x_1, \ldots, x_m\}$;
- $p = \det M$ (as polynomials)

Formalization

Symmetric Determinantal Representation

SDR of $p \in \mathbb{F}[x_1, \ldots, x_m]$:

- **Symmetric** matrix M;
- Entries: elements of $\mathbb{F} \cup \{x_1, \ldots, x_m\}$;
- $p = \det M$ (as polynomials)

A polynomial is said **representable** if it has a SDR.

Problems

Are **all** polynomials representable in characteristic 2?

Problems

Are all polynomials representable in characteristic 2?

1. Characterization of the representable polynomials.

Problems

Are all polynomials representable in characteristic 2?

1. Characterization of the representable polynomials.
2. Polytime algorithm for deciding representability.

Problems

Are all polynomials representable in characteristic 2?

1. Characterization of the representable polynomials.
2. Polytime algorithm for deciding representability.
3. Polytime algorithm for finding SDRs.

Motivation

- Algebraic Complexity

Motivation

- Algebraic Complexity
  - Universality of the determinant

[Valiant'79, Toda'92, Malod & Portier'06]

Motivation

- Algebraic Complexity
  - Universality of the determinant [Valiant'79, Toda'92, Malod & Portier'06]
  - SDRs in characteristic $\neq 2$ always exist [G., Kaltofen, Koiran, Portier'11]

Motivation

- Algebraic Complexity
  - Universality of the determinant
    [Valiant'79, Toda'92, Malod & Portier'06]
  - SDRs in characteristic $\neq 2$ always exist
    [G., Kaltofen, Koiran, Portier'11]
- Convex Optimization

Determinant and cycle covers

Determinant

$\mathfrak{S}_n$ = Permutation group of $\{1, \dots, n\}$

$$\det A = \sum_{\sigma \in \mathfrak{S}_n} (-1)^{\mathrm{sgn}(\sigma)} \prod_{i=1}^{n} A_{i,\sigma(i)}$$

Determinant and cycle covers

Determinant in characteristic 2

$\mathfrak{S}_n$ = Permutation group of $\{1, \dots, n\}$

$$\det A = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^{n} A_{i,\sigma(i)}$$

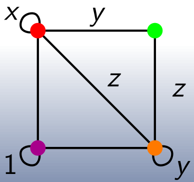
Determinant and cycle covers

Determinant in characteristic 2

$\mathfrak{S}_n$ = Permutation group of $\{1, \ldots, n\}$

$$\det A = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^{n} A_{i,\sigma(i)}$$

$$\begin{bmatrix} x & y & 1 & z \\ y & 0 & 0 & z \\ 1 & 0 & 1 & 1 \\ z & z & 1 & y \end{bmatrix}$$



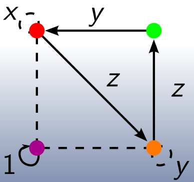
Determinant and cycle covers

Determinant in characteristic 2

$\mathfrak{S}_n =$ Permutation group of $\{1, \ldots, n\}$

$$\det A = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^{n} A_{i,\sigma(i)}$$

$$\begin{bmatrix} x & y & 1 & z \\ y & 0 & 0 & z \\ 1 & 0 & 1 & 1 \\ z & z & 1 & y \end{bmatrix}$$



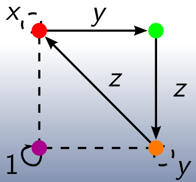
Determinant and cycle covers

Determinant in characteristic 2

$\mathfrak{S}_n$ = Permutation group of $\{1, \ldots, n\}$

$$\det A = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^{n} A_{i,\sigma(i)}$$

$$\begin{bmatrix} x & y & 1 & z \\ y & 0 & 0 & z \\ 1 & 0 & 1 & 1 \\ z & z & 1 & y \end{bmatrix}$$



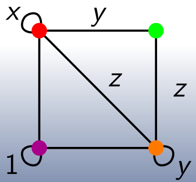
Determinant and partial matchings

Determinant in characteristic 2 of symmetric matrices

$\mathfrak{I}_n$ = Involutions of $\{1, \ldots, n\}$

$$\det A = \sum_{\sigma \in \mathfrak{I}_n} \prod_{i=1}^{n} A_{i,\sigma(i)}$$

$$\begin{bmatrix} x & y & 1 & z \\ y & 0 & 0 & z \\ 1 & 0 & 1 & 1 \\ z & z & 1 & y \end{bmatrix}$$



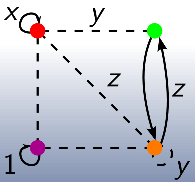
Determinant and partial matchings

Determinant in characteristic 2 of symmetric matrices

$\mathfrak{I}_n$ = Involutions of $\{1, \dots, n\}$

$$\det A = \sum_{\sigma \in \mathfrak{I}_n} \prod_{i=1}^{n} A_{i,\sigma(i)}$$

$$\begin{bmatrix} x & y & 1 & z \\ y & 0 & 0 & z \\ 1 & 0 & 1 & 1 \\ z & z & 1 & y \end{bmatrix}$$



Representable polynomials

Representable polynomials

Lemma

P and Q are representable $\implies$ $P \times Q$ *is representable.*

Representable polynomials

Lemma

P and Q are representable $\implies$ $P \times Q$ is representable.

Lemma

For all P, P^2 is representable.

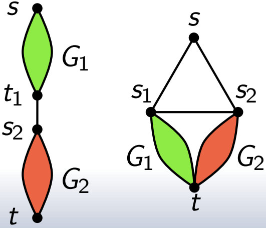
Representable polynomials

Lemma

P and Q are representable $\implies$ *$P \times Q$ is representable.*

Lemma

For all P, P^2 is representable.



Representable polynomials

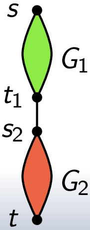
Lemma

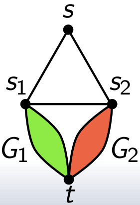
P and Q are representable $\implies$ $P \times Q$ is representable.

Lemma

For all P, P^2 is representable.

- $\det(G \setminus \{s,t\}) = 1$
- $\det(G \setminus \{s\}) = \det(G \setminus \{t\}) = 0$





A class of representable polynomials

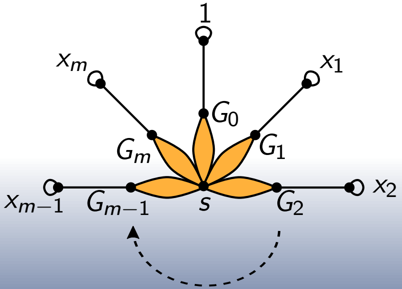
Theorem

$L(x_1, \ldots, x_m) = P_0^2 + x_1 P_1^2 + \cdots + x_m P_m^2$ *is representable.*

A class of representable polynomials

Theorem

$L(x_1,\ldots,x_m) = P_0^2 + x_1P_1^2 + \cdots + x_mP_m^2$ is representable.



Obstructions to representability

Theorem

If P is representable, then

$$P \equiv L_1 \times \cdots \times L_k \bmod \langle x_1^2 + 1, \ldots, x_m^2 + 1 \rangle$$

where the L_i's are linear. *(linear = degree-1)*

Obstructions to representability

Theorem

If P is representable, then

$$P \equiv L_1 \times \cdots \times L_k \bmod \langle x_1^2 + \ell_1, \ldots, x_m^2 + \ell_m \rangle$$

where the L_i's are linear, and the ℓ_i's are squares.

Obstructions to representability

Theorem

If P is representable, then

$$P \equiv L_1 \times \cdots \times L_k \bmod \langle x_1^2 + \ell_1, \ldots, x_m^2 + \ell_m \rangle$$

where the L_i's are linear, and the ℓ_i's are squares.

P is said **factorizable** *modulo* $\langle x_1^2 + \ell_1, \ldots, x_m^2 + \ell_m \rangle$.

Proof idea

- *Modulo* $\langle x_1^2+\ell_1,\dots,x_m^2+\ell_m\rangle$: no variable **outside the diagonal**

$$xz+y^2=\det\begin{pmatrix}x & y\\ y & z\end{pmatrix}$$

Proof idea

- *Modulo* $\langle x_1^2 + \ell_1, \dots, x_m^2 + \ell_m \rangle$: no variable **outside the diagonal**

$$xz + y^2 = \det \begin{pmatrix} x & y \\ y & z \end{pmatrix} \equiv \det \begin{pmatrix} x & 1 \\ 1 & z \end{pmatrix}$$

$$\mod \langle x^2 + 1, y^2 + 1, z^2 + 1 \rangle$$

Proof idea

- *Modulo* $\langle x_1^2 + \ell_1, \dots, x_m^2 + \ell_m \rangle$: no variable **outside the diagonal**
- Row/Column operations :
  - diagonal matrix
  - linear entries

$$xz + y^2 = \det \begin{pmatrix} x & y \\ y & z \end{pmatrix} \equiv \det \begin{pmatrix} x & 1 \\ 1 & z \end{pmatrix}$$

$$\bmod \langle x^2 + 1, y^2 + 1, z^2 + 1 \rangle$$

Proof idea

- *Modulo* $\langle x_1^2 + \ell_1, \ldots, x_m^2 + \ell_m \rangle$: no variable **outside the diagonal**
- Row/Column operations :
  - diagonal matrix
  - linear entries

$$xz + y^2 = \det \begin{pmatrix} x & y \\ y & z \end{pmatrix} \equiv \det \begin{pmatrix} x & 1 \\ 1 & z \end{pmatrix} \equiv \det \begin{pmatrix} x & 1+x \\ 1+x & x+z \end{pmatrix}$$

$$\bmod \langle x^2+1, y^2+1, z^2+1 \rangle$$

Proof idea

- *Modulo* $\langle x_1^2 + \ell_1, \ldots, x_m^2 + \ell_m \rangle$: no variable **outside the diagonal**
- Row/Column operations :
  - diagonal matrix
  - linear entries

$$xz + y^2 = \det \begin{pmatrix} x & y \\ y & z \end{pmatrix} \equiv \det \begin{pmatrix} x & 1 \\ 1 & z \end{pmatrix} \equiv \det \begin{pmatrix} x & 1+x \\ 1+x & x+z \end{pmatrix}$$

$$\equiv \det \begin{pmatrix} x & 0 \\ 0 & x+z \end{pmatrix} \qquad \mod \langle x^2+1, y^2+1, z^2+1 \rangle$$

Proof idea

- *Modulo* $\langle x_1^2+\ell_1,\dots,x_m^2+\ell_m\rangle$: no variable **outside the diagonal**
- Row/Column operations :
  - diagonal matrix
  - linear entries

$$xz+y^2=\det\begin{pmatrix}x & y\\ y & z\end{pmatrix}\equiv\det\begin{pmatrix}x & 1\\ 1 & z\end{pmatrix}\equiv\det\begin{pmatrix}x & 1+x\\ 1+x & x+z\end{pmatrix}$$

$$\equiv\det\begin{pmatrix}x & 0\\ 0 & x+z\end{pmatrix}\equiv x(x+z)\bmod\langle x^2+1,y^2+1,z^2+1\rangle$$

Multilinear polynomials

Theorem

Let P be a multilinear polynomial. The three following propositions are equivalent:

(i) P *is representable.*

(ii) $\exists \ell$, P *is factorizable modulo* $\langle x_1^2 + \ell_1, \ldots, x_m^2 + \ell_m \rangle$.

(iii) $\forall \ell$, P *is factorizable modulo* $\langle x_1^2 + \ell_1, \ldots, x_m^2 + \ell_m \rangle$.

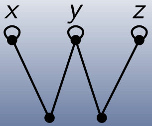
Proof idea

1. $xy + yz + xz \equiv xyz(x + y + z) \mod \langle x^2 + 1, y^2 + 1, z^2 + 1 \rangle$

Proof idea

1. $xy + yz + xz \equiv xyz(x+y+z) \mod \langle x^2+1, y^2+1, z^2+1 \rangle$

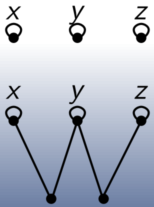
2. $xyz(x+y+z) = \det \begin{bmatrix} x & 0 & 0 & & & & & \\ 0 & y & 0 & & & & & \\ 0 & 0 & z & & & & & \\ & & & x & 1 & 0 & 0 & 0 \\ & & & 1 & 0 & 1 & 0 & 0 \\ & & & 0 & 1 & y & 1 & 0 \\ & & & 0 & 0 & 1 & 0 & 1 \\ & & & 0 & 0 & 0 & 1 & z \end{bmatrix}$



Proof idea

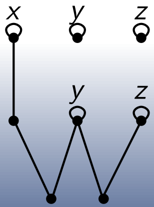
1. $xy + yz + xz \equiv xyz(x+y+z) \mod \langle x^2+1, y^2+1, z^2+1 \rangle$

2. $$xyz(x+y+z) \equiv \det \begin{bmatrix} x & 0 & 0 & & & & & \\ 0 & y & 0 & & & & & \\ 0 & 0 & z & & & & & \\ & & & x & 1 & 0 & 0 & 0 \\ & & & 1 & 0 & 1 & 0 & 0 \\ & & & 0 & 1 & y & 1 & 0 \\ & & & 0 & 0 & 1 & 0 & 1 \\ & & & 0 & 0 & 0 & 1 & z \end{bmatrix}$$



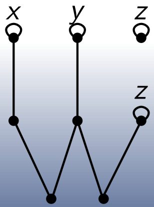
Proof idea

1. $xy + yz + xz \equiv xyz(x+y+z) \mod \langle x^2+1, y^2+1, z^2+1 \rangle$
2. $xyz(x+y+z) \equiv \det \begin{bmatrix} x & 0 & 0 & 1 & & & & \\ 0 & y & 0 & & & & & \\ 0 & 0 & z & & & & & \\ 1 & & & 0 & 1 & 0 & 0 & 0 \\ & & & 1 & 0 & 1 & 0 & 0 \\ & & & 0 & 1 & y & 1 & 0 \\ & & & 0 & 0 & 1 & 0 & 1 \\ & & & 0 & 0 & 0 & 1 & z \end{bmatrix}$



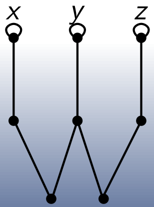
Proof idea

1. $xy + yz + xz \equiv xyz(x+y+z) \mod \langle x^2+1, y^2+1, z^2+1 \rangle$
2. $xyz(x+y+z) \equiv \det \begin{bmatrix} x & 0 & 0 & 1 & & & & \\ 0 & y & 0 & & & 1 & & \\ 0 & 0 & z & & & & & \\ 1 & & & 0 & 1 & 0 & 0 & 0 \\ & & & 1 & 0 & 1 & 0 & 0 \\ & 1 & & 0 & 1 & 0 & 1 & 0 \\ & & & 0 & 0 & 1 & 0 & 1 \\ & & & 0 & 0 & 0 & 1 & z \end{bmatrix}$



Proof idea

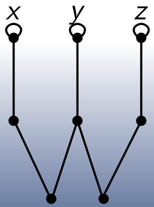
1. $xy + yz + xz \equiv xyz(x+y+z) \mod \langle x^2+1, y^2+1, z^2+1\rangle$
2. $xyz(x+y+z) \equiv \det \begin{bmatrix} x & 0 & 0 & 1 & & & & \\ 0 & y & 0 & & & 1 & & \\ 0 & 0 & z & & & & & 1 \\ 1 & & & 0 & 1 & 0 & 0 & 0 \\ & & & 1 & 0 & 1 & 0 & 0 \\ & 1 & & 0 & 1 & 0 & 1 & 0 \\ & & & 0 & 0 & 1 & 0 & 1 \\ & & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$



Proof idea

1. $xy + yz + xz \equiv xyz(x+y+z) \mod \langle x^2+1, y^2+1, z^2+1 \rangle$

2. $$xyz(x+y+z) \equiv \det \begin{bmatrix} x & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & y & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & z & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} = xy + yz + xz$$



Non-multilinear polynomials

$$xyz^2 + y^3z + x^3y^2z \longrightarrow \xi_z^2 \cdot xy + \xi_y^2 \cdot yz + \xi_x^2\xi_y^2 \cdot xz$$

Non-multilinear polynomials

$$xyz^2 + y^3z + x^3y^2z \longrightarrow \xi_z^2 \cdot xy + \xi_y^2 \cdot yz + \xi_x^2\xi_y^2 \cdot xz$$

- Multilinear again in x, y and z!

Non-multilinear polynomials

$$xyz^2 + y^3z + x^3y^2z \longrightarrow \xi_z^2 \cdot xy + \xi_y^2 \cdot yz + \xi_x^2\xi_y^2 \cdot xz$$

- Multilinear again in x, y and z!
- Representable if and only if factorizable

Non-multilinear polynomials

$$xyz^2 + y^3z + x^3y^2z \longrightarrow \xi_z^2 \cdot xy + \xi_y^2 \cdot yz + \xi_x^2\xi_y^2 \cdot xz$$

- Multilinear again in x, y and z!
- Representable if and only if factorizable
- **But** linears with coefficients in $\mathbb{F}(\xi_x, \xi_y, \xi_z)$ rather than $\mathbb{F}[\xi_1, \xi_y, \xi_z]$

Non-multilinear polynomials

$$xyz^2 + y^3z + x^3y^2z \longrightarrow \xi_z^2 \cdot xy + \xi_y^2 \cdot yz + \xi_x^2\xi_y^2 \cdot xz$$

- Multilinear again in x, y and z!
- Representable if and only if factorizable
- But linears with coefficients in $\mathbb{F}(\xi_x, \xi_y, \xi_z)$ rather than $\mathbb{F}[\xi_1, \xi_y, \xi_z]$

Theorem

- *Factorizable in* $\mathbb{F}[\xi_x, \xi_y, \xi_z][x, y, z] \implies$ *representable*
- *Not factorizable in* $\mathbb{F}(\xi_x, \xi_y, \xi_z)[x, y, z] \implies$ *not representable*

Conclusion

- Not all polynomials are representable

Conclusion

- Not all polynomials are representable
- Characterization for multilinear polynomials

Conclusion

- Not all polynomials are representable
- Characterization for multilinear polynomials
- Sufficient and necessary conditions for other polynomials

Conclusion

- Not all polynomials are representable
- Characterization for multilinear polynomials
- Sufficient and necessary conditions for other polynomials

Wait! Is $xy + z$ representable?

Finding a factor

$$(x+y+z+1)\times(x+y+z+1)\times\cdots\times(x+y+z+1)$$
$$\stackrel{?}{\equiv} xy+z \mod \langle x^2, y^2, z^2\rangle$$

Finding a factor

$$(x+y+z+1)\times(x+y+z+1)\times\cdots\times(x+y+z+1)$$
$$\overset{?}{\equiv} xy+z \mod \langle x^2,y^2,z^2\rangle$$

Finding a factor

$$(x + y + z + 1) \times (x + y + z + 1) \times \cdots \times (x + y + z + 1)$$
$$\overset{?}{\equiv} xy + z \mod \langle x^2, y^2, z^2 \rangle$$

Finding a factor

$$(x + y + z + 1) \times (x + y + z + 1) \times \cdots \times (x + y + z + 1)$$
$$\overset{?}{\equiv} xy + z \mod \langle x^2, y^2, z^2 \rangle$$

Finding a factor

$$(x + y + z \qquad) \times (x + y + z + 1) \times \cdots \times (x + y + z + 1)$$

$$\stackrel{?}{\equiv} xy + z \mod \langle x^2, y^2, z^2 \rangle$$

Finding a factor

$$(x+y+z \qquad) \times (x+y+z+1) \times \cdots \times (x+y+z+1)$$

$$\overset{?}{\equiv} xy+z \mod \langle x^2, y^2, z^2 \rangle$$

Finding a factor

$$(\quad z \quad) \times (x+y+z+1) \times \cdots \times (x+y+z+1)$$

$$\stackrel{?}{\equiv} xy + z \mod \langle x^2, y^2, z^2 \rangle$$

Finding a factor

$$(\qquad z \qquad) \times (x+y+z+1) \times \cdots \times (x+y+z+1)$$
$$\stackrel{?}{\equiv} xy + z \mod \langle x^2, y^2, z^2 \rangle$$

- $\mathrm{Lin}(xy + yz + y + z + 1) = y + z + 1$
- $\mathcal{I}_0 = \langle x^2, y^2, z^2 \rangle$

Finding a factor

$$(\qquad z \qquad) \times (x+y+z+1) \times \cdots \times (x+y+z+1)$$
$$\stackrel{?}{\equiv} xy + z \mod \langle x^2, y^2, z^2 \rangle$$

- $\mathrm{Lin}(xy + yz + y + z + 1) = y + z + 1$
- $\mathcal{I}_0 = \langle x^2, y^2, z^2 \rangle$

Lemma

Let P s.t. $P(0) = 0$, $\mathrm{Lin}(P) \neq 0$. Then

$$P \equiv L_1 \cdots L_k \mod \mathcal{I}_0 \implies L_i = \mathrm{Lin}(P) \text{ for some } i.$$

Divisibility

Lemma

- P: *multilinear polynomial,*
- L: *monic linear polynomial s.t.* $L(0) = 0$.

Then

$$\exists Q, P \equiv L \times Q \mod \mathcal{I}_0 \implies P \equiv L \times \frac{\partial P}{\partial x} \mod \mathcal{I}_0.$$

Preparation

Lemma

Let P be a multilinear polynomial. Then there exists Q and a multilinear $P^\star$ such that

- $P^\star \equiv P \times Q \mod \langle x^2+1, y^2+1, z^2+1\rangle$
- $\mathrm{Lin}(P^\star) \neq 0$
- $P^\star(0) = 0$

Preparation

Lemma

Let P be a multilinear polynomial. Then there exists Q and a multilinear $P^\star$ such that

- $P^\star \equiv P \times Q \mod \langle x^2+1, y^2+1, z^2+1\rangle$
- $\mathrm{Lin}(P^\star) \neq 0$
- $P^\star(0) = 0$

$\rightsquigarrow$ $P^\star$ is representable if and only if P is representable.

Preparation

Lemma

Let P be a multilinear polynomial. Then there exists Q and a multilinear $P^\star$ such that

- $P^\star \equiv P \times Q \mod \langle x^2+1, y^2+1, z^2+1 \rangle$
- $\mathrm{Lin}(P^\star) \neq 0$
- $P^\star(0) = 0$

$\rightsquigarrow$ $P^\star$ is representable if and only if P is representable.

Example. Suppose $P = xy + yz + x + 1$. Then $P \times y \equiv x + z + xy + y$ mod $\langle x^2+1, y^2+1, z^2+1 \rangle$.

An algorithm

IsRepresentable(P): P multilinear

1. **If** P is linear **Then** Return **True**

An algorithm

IsRepresentable(P): P multilinear

1. **If** P is linear **Then** Return **True**
2. Compute $P^\star$, multilinear, and Q such that
   - $P^\star \equiv P \times Q \bmod \langle x_i^2 + 1 \rangle$
   - $P^\star(0) = 0$ and $\mathrm{Lin}(P^\star) \neq 0$

An algorithm

IsRepresentable(P): P multilinear

1. **If** P is linear **Then** Return **True**
2. Compute $P^\star$, multilinear, and Q such that
   - $P^\star \equiv P \times Q \bmod \langle x_i^2 + 1 \rangle$
   - $P^\star(0) = 0$ and $\mathrm{Lin}(P^\star) \neq 0$
3. $P_0 \leftarrow \partial P^\star / \partial x_1$

An algorithm

IsRepresentable(P): P multilinear

1. **If** P is linear **Then** Return **True**
2. Compute $P^\star$, multilinear, and Q such that
   - $P^\star \equiv P \times Q \bmod \langle x_i^2 + 1 \rangle$
   - $P^\star(0) = 0$ and $\mathrm{Lin}(P^\star) \neq 0$
3. $P_0 \leftarrow \partial P^\star / \partial x_1$
4. **If** $P^\star \equiv \mathrm{Lin}(P^\star) \times P_0 \bmod \langle x_i^2 \rangle$

An algorithm

IsRepresentable(P): P multilinear

1. **If** P is linear **Then** Return **True**
2. Compute $P^\star$, multilinear, and Q such that
   - $P^\star \equiv P \times Q \bmod \langle x_i^2 + 1 \rangle$
   - $P^\star(0) = 0$ and $\mathrm{Lin}(P^\star) \neq 0$
3. $P_0 \leftarrow \partial P^\star / \partial x_1$
4. **If** $P^\star \equiv \mathrm{Lin}(P^\star) \times P_0 \bmod \langle x_i^2 \rangle$
   - **Then** IsRepresentable(P_0)

An algorithm

IsRepresentable(P): P multilinear

1. **If** P is linear **Then** Return **True**
2. Compute $P^\star$, multilinear, and Q such that
   - $P^\star \equiv P \times Q \bmod \langle x_i^2 + 1\rangle$
   - $P^\star(0) = 0$ and $\mathrm{Lin}(P^\star) \neq 0$
3. $P_0 \leftarrow \partial P^\star / \partial x_1$
4. **If** $P^\star \equiv \mathrm{Lin}(P^\star) \times P_0 \bmod \langle x_i^2 \rangle$
   - **Then** IsRepresentable(P_0)
   - **Else** Return **False**

Construction of SDRs

Lemma

Let P_1, P_2 be multilinear polynomials, with resp. SDRs M_1, M_2.

Construction of SDRs

Lemma

Let P_1, P_2 be multilinear polynomials, with resp. SDRs M_1, M_2. Let Q, multilinear, s.t. $Q \equiv P_1 \times P_2 \mod \langle x_1^2 + \ell_1, \ldots, x_m^2 + \ell_m \rangle$.

Construction of SDRs

Lemma

Let P_1, P_2 be multilinear polynomials, with resp. SDRs M_1, M_2.
Let Q, multilinear, s.t. $Q \equiv P_1 \times P_2 \mod \langle x_1^2 + \ell_1, \ldots, x_m^2 + \ell_m \rangle$.

$\rightsquigarrow$ $\textsc{Merge}_\ell(M_1, M_2)$: *SDR of Q (linear time)*

New algorithm

SDR(P): P multilinear

1. **If** P is linear **Then** RETURN **TRUE**
2. Compute $P^\star$, multilinear, and Q such that
   - $P^\star \equiv P \times Q \bmod \langle x_i^2 + 1 \rangle$
   - $P^\star(0) = 0$ and $\mathrm{Lin}(P^\star) \neq 0$
3. $P_0 \leftarrow \partial P^\star / \partial x_1$
4. **If** $P^\star \equiv \mathrm{Lin}(P^\star) \times P_0 \bmod \langle x_i^2 \rangle$
   - **Then** ISREPRESENTABLE(P_0)
   - **Else** RETURN **FALSE**

New algorithm

SDR(P): P multilinear

1. **If** P is linear **Then** RETURN MAT(P)
2. Compute $P^\star$, multilinear, and Q such that
   - $P^\star \equiv P \times Q \bmod \langle x_i^2 + 1 \rangle$
   - $P^\star(0) = 0$ and $\mathrm{Lin}(P^\star) \neq 0$
3. $P_0 \leftarrow \partial P^\star / \partial x_1$
4. **If** $P^\star \equiv \mathrm{Lin}(P^\star) \times P_0 \bmod \langle x_i^2 \rangle$
   - **Then** ISREPRESENTABLE(P_0)
   - **Else** RETURN **FALSE**

New algorithm

SDR(P): P multilinear

1. **If** P is linear **Then** RETURN MAT(P)
2. Compute $P^\star$, multilinear, and Q such that
   - $P^\star \equiv P \times Q \bmod \langle x_i^2 + 1 \rangle$
   - $P^\star(0) = 0$ and $\mathrm{Lin}(P^\star) \neq 0$
3. $P_0 \leftarrow \partial P^\star / \partial x_1$
4. **If** $P^\star \equiv \mathrm{Lin}(P^\star) \times P_0 \bmod \langle x_i^2 \rangle$
   - **Then**
     - $M_0 \leftarrow \mathrm{SDR}(P_0)$
     - $M_1 \leftarrow \mathrm{MAT}(\mathrm{Lin}(P^\star))$
     - $M_2 \leftarrow \mathrm{MAT}(Q)$
     - RETURN $\mathrm{MERGE}_1(M_2, \mathrm{MERGE}_0(M_1, M_0))$
   - **Else** RETURN **FALSE**

Summary

- Characterization of multilinear representable polynomials

Summary

- Characterization of multilinear representable polynomials
- Polynomial-time algorithm for multilinear polynomials:

Summary

- Characterization of multilinear representable polynomials
- Polynomial-time algorithm for multilinear polynomials:
  - If representable: find a matrix

Summary

- Characterization of multilinear representable polynomials
- Polynomial-time algorithm for multilinear polynomials:
  - If representable: find a matrix
  - Else: Answers **False**

Summary

- Characterization of multilinear representable polynomials
- Polynomial-time algorithm for multilinear polynomials:
  - If representable: find a matrix
  - Else: Answers **False**
- Non-multilinear polynomials:

Summary

- Characterization of multilinear representable polynomials
- Polynomial-time algorithm for multilinear polynomials:
  - If representable: find a matrix
  - Else: Answers **False**
- Non-multilinear polynomials:
  - Necessary and Sufficient Conditions

Summary

- Characterization of multilinear representable polynomials
- Polynomial-time algorithm for multilinear polynomials:
  - If representable: find a matrix
  - Else: Answers **False**
- Non-multilinear polynomials:
  - Necessary and Sufficient Condition<u>s</u>
  - Algorithm: Either answer **False**, or a matrix to check

Summary

- Characterization of multilinear representable polynomials
- Polynomial-time algorithm for multilinear polynomials:
  - If representable: find a matrix
  - Else: Answers **False**
- Non-multilinear polynomials:
  - Necessary and Sufficient Conditions
  - Algorithm: Either answer **False**, or a matrix to check
- Full characterization?

Summary

- Characterization of multilinear representable polynomials
- Polynomial-time algorithm for multilinear polynomials:
  - If representable: find a matrix
  - Else: Answers **False**
- Non-multilinear polynomials:
  - Necessary and Sufficient Condition<u>s</u>
  - Algorithm: Either answer **False**, or a matrix to check
- Full characterization?

Thank you!