Finding Optimal Formulae for Bilinear Maps<br>Razvan Barbulescu, Jérémie Detrey, Nicolas Estibals, Paul Zimmermann

## To cite this version:

Razvan Barbulescu, Jérémie Detrey, Nicolas Estibals, Paul Zimmermann. Finding Optimal Formulae for Bilinear Maps. AriC Seminar, Mar 2012, Lyon, France. hal-01413162

HAL Id: hal-01413162
https://inria.hal.science/hal-01413162
Submitted on 9 Dec 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Finding Optimal Formulae for Bilinear Maps 

(slides courtesy of Nicolas Estibals)

Jérémie Detrey<br>CARAMEL project-team, LORIA<br>INRIA Nancy - Grand Est<br>Jeremie.Detrey@loria.fr

Joint work with:
Răzvan Bărbulescu
Nicolas Estibals
Paul Zimmermann


UNIVERSITÉ DE LORRAINE

## A bit of history

- Multiplication is an expensive arithmetic operation
- Well-studied problem
- Karatsuba (1962)
- Toom-Cook (1963), evaluation-interpolation schemes
- CRT-based algorithms
- Schönhage-Strassen algorithm (1971)
- ...
- Five-, six-, and seven-term Karatsuba-like formulae, P. Montgomery (2005)
- ad-hoc formulae
- exhaustive search for five-term multiplication
- non-exhaustive search for six- and seven-term multiplications
- (January 2011) start a task group to reproduce this work


## Outline of the talk

- Formulae for polynomial multiplication
- Enumerating formulae
- Further improvements and heuristics
- Some results


## Outline of the talk

- Formulae for polynomial multiplication
- Enumerating formulae
- Further improvements and heuristics
- Some results


## Example: a 2-term polynomial times a 3-term one

- We want to compute

$$
\begin{aligned}
C(X) & =\left(a_{1} \cdot X+a_{0}\right) \times\left(b_{2} \cdot X^{2}+b_{1} \cdot X+b_{0}\right) \\
& =a_{1} b_{2} \cdot X^{3}+\left(a_{1} b_{1}+a_{0} b_{2}\right) \cdot X^{2}+\left(a_{0} b_{1}+a_{1} b_{0}\right) \cdot X+a_{0} b_{0}
\end{aligned}
$$

## Example: a 2-term polynomial times a 3-term one

- We want to compute

$$
\begin{aligned}
C(X) & =\left(a_{1} \cdot X+a_{0}\right) \times\left(b_{2} \cdot X^{2}+b_{1} \cdot X+b_{0}\right) \\
& =a_{1} b_{2} \cdot X^{3}+\left(a_{1} b_{1}+a_{0} b_{2}\right) \cdot X^{2}+\left(a_{0} b_{1}+a_{1} b_{0}\right) \cdot X+a_{0} b_{0}
\end{aligned}
$$

- Only 5 products required instead of 6
- use Karatsuba's trick

$$
C(X)=a_{1} b_{2} \cdot X^{3}+\left(a_{1} b_{1}+a_{0} b_{2}\right) \cdot X^{2}+\left(\left(a_{0}+a_{1}\right)\left(b_{0}+b_{1}\right)-a_{1} b_{1}-a_{0} b_{0}\right) \cdot X+a_{0} b_{0}
$$

## Example: a 2-term polynomial times a 3-term one

- We want to compute

$$
\begin{aligned}
C(X) & =\left(a_{1} \cdot X+a_{0}\right) \times\left(b_{2} \cdot X^{2}+b_{1} \cdot X+b_{0}\right) \\
& =a_{1} b_{2} \cdot X^{3}+\left(a_{1} b_{1}+a_{0} b_{2}\right) \cdot X^{2}+\left(a_{0} b_{1}+a_{1} b_{0}\right) \cdot X+a_{0} b_{0}
\end{aligned}
$$

- Only 5 products required instead of 6
- use Karatsuba's trick

$$
C(X)=a_{1} b_{2} \cdot X^{3}+\left(a_{1} b_{1}+a_{0} b_{2}\right) \cdot X^{2}+\left(\left(a_{0}+a_{1}\right)\left(b_{0}+b_{1}\right)-a_{1} b_{1}-a_{0} b_{0}\right) \cdot X+a_{0} b_{0}
$$

- compute the products

$$
\begin{array}{lc}
g_{0}= & a_{0} \cdot b_{0}, \\
g_{1}= & a_{0} \cdot b_{2}, \\
g_{2}= & a_{1} \cdot b_{1}, \\
g_{3}= & a_{1} \cdot b_{2}, \text { and } \\
g_{4}= & \left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{1}\right) .
\end{array}
$$

- reconstruct the result

$$
C(X)=g_{3} \cdot X^{3}+\left(g_{1}+g_{2}\right) \cdot X^{2}+\left(g_{4}-g_{2}-g_{0}\right) \cdot X+g_{0}
$$

## General form of a multiplication formula

- We want to compute, over a given field $K$ (or any $K$-algebra K ),

$$
\left(a_{n-1} \cdot X^{n-1}+\cdots+a_{0}\right) \times\left(b_{m-1} \cdot X^{m-1}+\cdots+b_{0}\right)=c_{n+m-2} \cdot X^{n+m-2}+\cdots+c_{0}
$$

## General form of a multiplication formula

- We want to compute, over a given field $K$ (or any $K$-algebra K ), $\left(a_{n-1} \cdot X^{n-1}+\cdots+a_{0}\right) \times\left(b_{m-1} \cdot X^{m-1}+\cdots+b_{0}\right)=c_{n+m-2} \cdot X^{n+m-2}+\cdots+c_{0}$
- All formulae for multiplication can be expressed as:


## General form of a multiplication formula

- We want to compute, over a given field $K$ (or any $K$-algebra $K$ ), $\left(a_{n-1} \cdot X^{n-1}+\cdots+a_{0}\right) \times\left(b_{m-1} \cdot X^{m-1}+\cdots+b_{0}\right)=c_{n+m-2} \cdot X^{n+m-2}+\cdots+c_{0}$
- All formulae for multiplication can be expressed as:
- compute some linear combinations of the $a_{i}$ 's

$$
a_{j}^{\prime}=\sum \alpha_{i, j} \cdot a_{i}
$$

- compute some linear combinations of the $b_{i}$ 's

$$
b_{j}^{\prime}=\sum \beta_{i, j} \cdot b_{i}
$$

## General form of a multiplication formula

- We want to compute, over a given field $K$ (or any $K$-algebra $K$ ), $\left(a_{n-1} \cdot X^{n-1}+\cdots+a_{0}\right) \times\left(b_{m-1} \cdot X^{m-1}+\cdots+b_{0}\right)=c_{n+m-2} \cdot X^{n+m-2}+\cdots+c_{0}$
- All formulae for multiplication can be expressed as:
- compute some linear combinations of the $a_{i}$ 's

$$
a_{j}^{\prime}=\sum \alpha_{i, j} \cdot a_{i}
$$

- compute some linear combinations of the $b_{i}$ 's

$$
b_{j}^{\prime}=\sum \beta_{i, j} \cdot b_{i}
$$

- perform some products

$$
g_{j}=a_{j}^{\prime} \cdot b_{j}^{\prime}
$$

## General form of a multiplication formula

- We want to compute, over a given field $K$ (or any $K$-algebra $K$ ), $\left(a_{n-1} \cdot X^{n-1}+\cdots+a_{0}\right) \times\left(b_{m-1} \cdot X^{m-1}+\cdots+b_{0}\right)=c_{n+m-2} \cdot X^{n+m-2}+\cdots+c_{0}$
- All formulae for multiplication can be expressed as:
- compute some linear combinations of the $a_{i}$ 's

$$
a_{j}^{\prime}=\sum \alpha_{i, j} \cdot a_{i}
$$

- compute some linear combinations of the $b_{i}$ 's

$$
b_{j}^{\prime}=\sum \beta_{i, j} \cdot b_{i}
$$

- perform some products

$$
g_{j}=a_{j}^{\prime} \cdot b_{j}^{\prime}
$$

- reconstruct the result by linear combinations of the products

$$
c_{k}=\sum \gamma_{j, k} \cdot g_{j}
$$

## General form of a multiplication formula

- We want to compute, over a given field $K$ (or any $K$-algebra $K$ ),

$$
\left(a_{n-1} \cdot X^{n-1}+\cdots+a_{0}\right) \times\left(b_{m-1} \cdot X^{m-1}+\cdots+b_{0}\right)=c_{n+m-2} \cdot X^{n+m-2}+\cdots+c_{0}
$$

- All formulae for multiplication can be expressed as:
- compute some linear combinations of the $a_{i}$ 's

$$
a_{j}^{\prime}=\sum \alpha_{i, j} \cdot a_{i}, \quad \text { with } \alpha_{i, j} \in K
$$

- compute some linear combinations of the $b_{i}$ 's

$$
b_{j}^{\prime}=\sum \beta_{i, j} \cdot b_{i}, \quad \text { with } \beta_{i, j} \in K
$$

- perform some products

$$
g_{j}=a_{j}^{\prime} \cdot b_{j}^{\prime}
$$

- reconstruct the result by linear combinations of the products

$$
c_{k}=\sum \gamma_{j, k} \cdot g_{j}, \quad \text { with } \gamma_{j, k} \in K
$$

## General form of a multiplication formula

- We want to compute, over a given field $K$ (or any $K$-algebra $K$ ),

$$
\left(a_{n-1} \cdot X^{n-1}+\cdots+a_{0}\right) \times\left(b_{m-1} \cdot X^{m-1}+\cdots+b_{0}\right)=c_{n+m-2} \cdot X^{n+m-2}+\cdots+c_{0}
$$

- All formulae for multiplication can be expressed as:
- compute some linear combinations of the $a_{i}$ 's

$$
a_{j}^{\prime}=\sum \alpha_{i, j} \cdot a_{i}, \quad \text { with } \alpha_{i, j} \in K
$$

- compute some linear combinations of the $b_{i}$ 's

$$
b_{j}^{\prime}=\sum \beta_{i, j} \cdot b_{i}, \quad \text { with } \beta_{i, j} \in K
$$

- perform some products

$$
g_{j}=a_{j}^{\prime} \cdot b_{j}^{\prime}, \quad \text { with } a_{j}^{\prime}, b_{j}^{\prime} \in \mathbf{K}
$$

- reconstruct the result by linear combinations of the products

$$
c_{k}=\sum \gamma_{j, k} \cdot g_{j}, \quad \text { with } \gamma_{j, k} \in K
$$

## General form of a multiplication formula

- We want to compute, over a given field $K$ (or any $K$-algebra $K$ ),

$$
\left(a_{n-1} \cdot X^{n-1}+\cdots+a_{0}\right) \times\left(b_{m-1} \cdot X^{m-1}+\cdots+b_{0}\right)=c_{n+m-2} \cdot X^{n+m-2}+\cdots+c_{0}
$$

- All formulae for multiplication can be expressed as:
- compute some linear combinations of the $a_{i}$ 's

$$
a_{j}^{\prime}=\sum \alpha_{i, j} \cdot a_{i}, \quad \text { with } \alpha_{i, j} \in K
$$

- compute some linear combinations of the $b_{i}$ 's

$$
b_{j}^{\prime}=\sum \beta_{i, j} \cdot b_{i}, \quad \text { with } \beta_{i, j} \in K
$$

- perform some products

$$
g_{j}=a_{j}^{\prime} \cdot b_{j}^{\prime}, \quad \text { with } a_{j}^{\prime}, b_{j}^{\prime} \in \mathbf{K}
$$

- reconstruct the result by linear combinations of the products

$$
c_{k}=\sum \gamma_{j, k} \cdot g_{j}, \quad \text { with } \gamma_{j, k} \in K
$$

- This is also valid for any bilinear map

$$
\begin{aligned}
F: \begin{array}{ccc}
K^{n} & \times \quad K^{m} & \longrightarrow \\
\left(\left(a_{0}, \ldots, a_{n-1}\right)\right. & K^{\ell} \\
& \left.\left(b_{0}, \ldots, b_{m-1}\right)\right) & \longmapsto\left(c_{0}, \ldots, c_{\ell-1}\right)
\end{array}
\end{aligned}
$$

# Outline of the talk 

## - Formulae for polynomial multiplication

- Enumerating formulae
- Further improvements and heuristics
- Some results


## Formal framework

$$
F: K^{n} \times K^{m} \rightarrow K^{\ell}
$$

## Formal framework

$$
F: K^{n} \times K^{m} \rightarrow K^{\ell}
$$

- Represent the products and the coefficients of the result as elements of the nm-dimensional $K$-vector space

$$
V=\operatorname{Span} \mathcal{V}, \quad \text { with basis } \mathcal{V}=\left\{a_{i} b_{j}\right\}_{0 \leq i<n, 0 \leq j<m}
$$

where the $a_{i} b_{j}$ 's are seen as formal elements

## Formal framework

$$
F: K^{n} \times K^{m} \rightarrow K^{\ell}
$$

- Represent the products and the coefficients of the result as elements of the $n m$-dimensional $K$-vector space

$$
V=\operatorname{Span} \mathcal{V}, \quad \text { with basis } \mathcal{V}=\left\{a_{i} b_{j}\right\}_{0 \leq i<n, 0 \leq j<m},
$$

where the $a_{i} b_{j}$ 's are seen as formal elements

- Targets: the coefficients of the result form a set

$$
\mathcal{T}=\left\{c_{i}\right\}_{0 \leq i<\ell} \subset V
$$

## Formal framework

$$
F: K^{n} \times K^{m} \rightarrow K^{\ell}
$$

- Represent the products and the coefficients of the result as elements of the $n m$-dimensional $K$-vector space

$$
V=\operatorname{Span} \mathcal{V}, \quad \text { with basis } \mathcal{V}=\left\{a_{i} b_{j}\right\}_{0 \leq i<n, 0 \leq j<m},
$$

where the $a_{i} b_{j}$ 's are seen as formal elements

- Targets: the coefficients of the result form a set

$$
\mathcal{T}=\left\{c_{i}\right\}_{0 \leq i<\ell} \subset V
$$

- Generators: the set $\mathcal{G} \subset V$ of the potential products to use in a formula

$$
\mathcal{G}=\left\{\left(\sum \alpha_{i} a_{i}\right) \cdot\left(\sum \beta_{j} b_{j}\right) \mid \forall i, \alpha_{i} \in K \text { and } \forall j, \beta_{j} \in K\right\} \backslash\{0\}
$$

## Formal framework

$$
F: K^{n} \times K^{m} \rightarrow K^{\ell}
$$

- Represent the products and the coefficients of the result as elements of the $n m$-dimensional $K$-vector space

$$
V=\operatorname{Span} \mathcal{V}, \quad \text { with basis } \mathcal{V}=\left\{a_{i} b_{j}\right\}_{0 \leq i<n, 0 \leq j<m}
$$

where the $a_{i} b_{j}$ 's are seen as formal elements

- Targets: the coefficients of the result form a set

$$
\mathcal{T}=\left\{c_{i}\right\}_{0 \leq i<\ell} \subset V
$$

- Generators: the set $\mathcal{G} \subset V$ of the potential products to use in a formula We only consider products modulo a nonzero scalar factor

$$
\mathcal{G}=\left\{\left(\sum \alpha_{i} a_{i}\right) \cdot\left(\sum \beta_{j} b_{j}\right) \mid \forall i, \alpha_{i} \in K \text { and } \forall j, \beta_{j} \in K\right\} \backslash\{0\} / \sim
$$

where $g \sim g^{\prime}$ when $\exists \lambda \in K, \lambda \neq 0$ such that $g=\lambda g^{\prime}$

## Example (cont'd)

Consider the previous example: $2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

Example (cont'd)
Consider the previous example: $2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- $V$ is a 6 -dimensional vector space with basis

$$
\mathcal{V}=\left\{a_{0} b_{0}, a_{0} b_{1}, a_{0} b_{2}, a_{1} b_{0}, a_{1} b_{1}, a_{1} b_{2}\right\}
$$

## Example (cont'd)

Consider the previous example: $2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- $V$ is a 6 -dimensional vector space with basis

$$
\mathcal{V}=\left\{a_{0} b_{0}, a_{0} b_{1}, a_{0} b_{2}, a_{1} b_{0}, a_{1} b_{1}, a_{1} b_{2}\right\}
$$

- The set of targets is

$$
\mathcal{T}=\left\{a_{1} b_{2}, a_{1} b_{1}+a_{0} b_{2}, a_{0} b_{1}+a_{1} b_{0}, a_{0} b_{0}\right\}
$$

## Example (cont'd)

Consider the previous example: $2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- $V$ is a 6 -dimensional vector space with basis

$$
\mathcal{V}=\left\{a_{0} b_{0}, a_{0} b_{1}, a_{0} b_{2}, a_{1} b_{0}, a_{1} b_{1}, a_{1} b_{2}\right\}
$$

- The set of targets is

$$
\mathcal{T}=\left\{a_{1} b_{2}, a_{1} b_{1}+a_{0} b_{2}, a_{0} b_{1}+a_{1} b_{0}, a_{0} b_{0}\right\}
$$

- The set of generators contains 21 products:

$$
\begin{array}{rlrl}
\mathcal{G}=\{ & a_{0} \cdot b_{0}, & a_{1} \cdot b_{0}, & \left(a_{0}+a_{1}\right) \cdot b_{0}, \\
a_{0} \cdot b_{1}, & a_{1} \cdot b_{1}, & \left(a_{0}+a_{1}\right) \cdot b_{1}, \\
a_{0} \cdot\left(b_{0}+b_{1}\right), & a_{1} \cdot\left(b_{0}+b_{1}\right), & \left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{1}\right), \\
& a_{0} \cdot b_{2}, & a_{1} \cdot b_{2}, & \left(a_{0}+a_{1}\right) \cdot b_{2}, \\
a_{0} \cdot\left(b_{0}+b_{2}\right), & a_{1} \cdot\left(b_{0}+b_{2}\right), & \left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{2}\right), \\
a_{0} \cdot\left(b_{1}+b_{2}\right), & a_{1} \cdot\left(b_{1}+b_{2}\right), & \left(a_{0}+a_{1}\right) \cdot\left(b_{1}+b_{2}\right), \\
& a_{0} \cdot\left(b_{0}+b_{1}+b_{2}\right), & a_{1} \cdot\left(b_{0}+b_{1}+b_{2}\right), & \left.\left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{1}+b_{2}\right)\right\}
\end{array}
$$

## Naive algorithm

- Goal: find the optimal formulae (i.e., with a minimum number of products)
- enumerate the subsets $\mathcal{W} \subset \mathcal{G}$ of exactly $k$ products which yield a valid formula
- starting with $k=\operatorname{rk}(\mathcal{T})$, increase $k$ until a solution is found


## Naive algorithm

- Goal: find the optimal formulae (i.e., with a minimum number of products)
- enumerate the subsets $\mathcal{W} \subset \mathcal{G}$ of exactly $k$ products which yield a valid formula
- starting with $k=\operatorname{rk}(\mathcal{T})$, increase $k$ until a solution is found
- Look for $\mathcal{W}$ such that
- $\mathcal{W}$ is a set of $k$ generators:

$$
\mathcal{W} \subset \mathcal{G} \quad \text { and } \quad \# \mathcal{W}=k
$$

- $\mathcal{W}$ linearly generates the coefficients of the results:

$$
\mathcal{T} \subset \operatorname{Span} \mathcal{W}
$$

## Naive algorithm

- Goal: find the optimal formulae (i.e., with a minimum number of products)
- enumerate the subsets $\mathcal{W} \subset \mathcal{G}$ of exactly $k$ products which yield a valid formula
- starting with $k=\operatorname{rk}(\mathcal{T})$, increase $k$ until a solution is found
- Look for $\mathcal{W}$ such that
- $\mathcal{W}$ is a set of $k$ generators:

$$
\mathcal{W} \subset \mathcal{G} \quad \text { and } \quad \# \mathcal{W}=k
$$

- $\mathcal{W}$ linearly generates the coefficients of the results:

$$
\mathcal{T} \subset \operatorname{Span} \mathcal{W}
$$

- Naive approach:
- enumerate the $\binom{\# \mathcal{G}}{k}$ subsets $\mathcal{W}$ of size $k$
- for each subset, test whether it generates $\mathcal{T}$ or not


## Naive algorithm

- Goal: find the optimal formulae (i.e., with a minimum number of products)
- enumerate the subsets $\mathcal{W} \subset \mathcal{G}$ of exactly $k$ products which yield a valid formula
- starting with $k=\operatorname{rk}(\mathcal{T})$, increase $k$ until a solution is found
- Look for $\mathcal{W}$ such that
- $\mathcal{W}$ is a set of $k$ generators:

$$
\mathcal{W} \subset \mathcal{G} \quad \text { and } \quad \# \mathcal{W}=k
$$

- $\mathcal{W}$ linearly generates the coefficients of the results:

$$
\mathcal{T} \subset \operatorname{Span} \mathcal{W}
$$

- Naive approach:
- enumerate the $\binom{\# \mathcal{G}}{k}$ subsets $\mathcal{W}$ of size $k$
- for each subset, test whether it generates $\mathcal{T}$ or not
- $\mathcal{G}$ has to be finite:
- look for formulae over finite fields: $K=\mathbb{F}_{q}$ (typically, $q=2,3,4$ )
- restrict to a finite subset of the generators $\mathcal{G}$ (but search not exhaustive)


## Naive algorithm

- Goal: find the optimal formulae (i.e., with a minimum number of products)
- enumerate the subsets $\mathcal{W} \subset \mathcal{G}$ of exactly $k$ products which yield a valid formula
- starting with $k=\operatorname{rk}(\mathcal{T})$, increase $k$ until a solution is found
- Look for $\mathcal{W}$ such that
- $\mathcal{W}$ is a set of $k$ generators:

$$
\mathcal{W} \subset \mathcal{G} \quad \text { and } \quad \# \mathcal{W}=k
$$

- $\mathcal{W}$ linearly generates the coefficients of the results:

$$
\mathcal{T} \subset \operatorname{Span} \mathcal{W}
$$

- Naive approach:
- enumerate the $\binom{\# \mathcal{G}}{k}$ subsets $\mathcal{W}$ of size $k$
- for each subset, test whether it generates $\mathcal{T}$ or not
- $\mathcal{G}$ has to be finite:
- look for formulae over finite fields: $K=\mathbb{F}_{q}$ (typically, $q=2,3,4$ )
- restrict to a finite subset of the generators $\mathcal{G}$ (but search not exhaustive)
- Drawback: Distinct subsets may span the same subspace


## Improved algorithm: subspaces instead of subsets

- Look instead for subspaces $W$ of $V$ such that
- $W$ can be generated by products only: $\operatorname{Span}(W \cap \mathcal{G})=W$
- only $k$ products are required: $\operatorname{dim} W=k$
- $W$ contains the target space spanned by the target vectors: $T=\operatorname{Span} \mathcal{T} \subset W$


## Improved algorithm: subspaces instead of subsets

- Look instead for subspaces $W$ of $V$ such that
- $W$ can be generated by products only: $\operatorname{Span}(W \cap \mathcal{G})=W$
- only $k$ products are required: $\operatorname{dim} W=k$
- $W$ contains the target space spanned by the target vectors: $T=\operatorname{Span} \mathcal{T} \subset W$
- Algorithm:

1: procedure expand_subspace $(W)$
2: $\quad$ if $\operatorname{dim} W=k$ and $T \subset W$ then
3: $\quad W$ is a solution
4: else if $\operatorname{dim} W<k$ then
5: $\quad$ for each $g \in \mathcal{G} \backslash W$ do
6: $\quad$ expand_subspace $(W \oplus \operatorname{Span}(g))$
7: end procedure
8: expand_subspace(\{0\})

## Improved algorithm: subspaces instead of subsets

- Look instead for subspaces $W$ of $V$ such that
- $W$ can be generated by products only: $\operatorname{Span}(W \cap \mathcal{G})=W$
- only $k$ products are required: $\operatorname{dim} W=k$
- $W$ contains the target space spanned by the target vectors: $T=\operatorname{Span} \mathcal{T} \subset W$
- Algorithm:

1: procedure expand_subspace $(W)$
if $\operatorname{dim} W=k$ and $T \subset W$ then
$W$ is a solution
else if $\operatorname{dim} W<k$ then
for each $g \in \mathcal{G} \backslash W$ do
expand_subspace $(W \oplus \operatorname{Span}(g))$
end procedure
8: expand_subspace(\{0\})

- Several formulae can correspond to a single solution subspace $W$
- each basis of $W$ comprising only elements of $\mathcal{G}$ gives a $k$-product formula


## Improved algorithm: incomplete basis

- We already know part of $W$ !
- target space $T$ is a subspace of every solution space $W$
- find each $W$ by constructing $\mathcal{W}^{\prime} \subset \mathcal{G}$ such that $W=T \oplus \operatorname{Span} \mathcal{W}^{\prime}$


## Improved algorithm: incomplete basis

- We already know part of $W$ !
- target space $T$ is a subspace of every solution space $W$
- find each $W$ by constructing $\mathcal{W}^{\prime} \subset \mathcal{G}$ such that $W=T \oplus \operatorname{Span} \mathcal{W}^{\prime}$
- Modified algorithm:

1: procedure expand_subspace $(W)$
2: $\quad$ if $\operatorname{dim} W=k$ and $T \subset W$ then
$W$ is a solution
else if $\operatorname{dim} W<k$ then
for each $g \in \mathcal{G} \backslash W$ do
expand_subspace $(W \oplus \operatorname{Span}(g))$
7: end procedure
8: expand_subspace( $\{\mathbf{0}\}$ )

## Improved algorithm: incomplete basis

- We already know part of $W$ !
- target space $T$ is a subspace of every solution space $W$
- find each $W$ by constructing $\mathcal{W}^{\prime} \subset \mathcal{G}$ such that $W=T \oplus \operatorname{Span} \mathcal{W}^{\prime}$
- Modified algorithm:

1: procedure expand_subspace $(W)$
if $\operatorname{dim} W=k$ and $T \subset W$ then
$W$ is a solution
else if $\operatorname{dim} W<k$ then
for each $g \in \mathcal{G} \backslash W$ do
expand_subspace $(W \oplus \operatorname{Span}(g))$
7: end procedure
8: expand_subspace $(T)$

## Improved algorithm: incomplete basis

- We already know part of $W$ !
- target space $T$ is a subspace of every solution space $W$
- find each $W$ by constructing $\mathcal{W}^{\prime} \subset \mathcal{G}$ such that $W=T \oplus \operatorname{Span} \mathcal{W}^{\prime}$
- Modified algorithm:

1: procedure expand_subspace $(W)$
2: $\quad$ if $\operatorname{dim} W=k$ and $T \subset W$ then
$W$ is a solution
else if $\operatorname{dim} W<k$ then
for each $g \in \mathcal{G} \backslash W$ do
expand_subspace $(W \oplus \operatorname{Span}(g))$
7: end procedure
8: expand_subspace( $T$ )

## Improved algorithm: incomplete basis

- We already know part of $W$ !
- target space $T$ is a subspace of every solution space $W$
- find each $W$ by constructing $\mathcal{W}^{\prime} \subset \mathcal{G}$ such that $W=T \oplus \operatorname{Span} \mathcal{W}^{\prime}$
- Modified algorithm:

1: procedure expand_subspace $(W)$
if $\operatorname{dim} W=k$ and $\operatorname{rk}(W \cap \mathcal{G})=k$ then
$W$ is a solution
else if $\operatorname{dim} W<k$ then
for each $g \in \mathcal{G} \backslash W$ do
expand_subspace $(W \oplus \operatorname{Span}(g))$
7: end procedure
8: expand_subspace( $T$ )

## Improved algorithm: incomplete basis

- We already know part of $W$ !
- target space $T$ is a subspace of every solution space $W$
- find each $W$ by constructing $\mathcal{W}^{\prime} \subset \mathcal{G}$ such that $W=T \oplus \operatorname{Span} \mathcal{W}^{\prime}$
- Modified algorithm:

1: procedure expand_subspace $(W)$
2: $\quad$ if $\operatorname{dim} W=k$ and $\operatorname{rk}(W \cap \mathcal{G})=k$ then $W$ is a solution
4: else if $\operatorname{dim} W<k$ then
5: $\quad$ for each $g \in \mathcal{G} \backslash W$ do
6: $\quad$ expand_subspace $(W \oplus \operatorname{Span}(g))$
7: end procedure
8: expand_subspace( $T$ )

- Complexity now depends on

$$
\binom{\# \mathcal{G}}{k-\mathrm{rk} \mathcal{T}}
$$

## Example (cont'd)

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

## Example (cont'd)

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- Targets: $\mathcal{T}=\left\{a_{1} b_{2}, a_{1} b_{1}+a_{0} b_{2}, a_{0} b_{1}+a_{1} b_{0}, a_{0} b_{0}\right\}$
- at least $\operatorname{rk}(\mathcal{T})=4$ products required


## Example (cont'd)

## $2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- Targets: $\mathcal{T}=\left\{a_{1} b_{2}, a_{1} b_{1}+a_{0} b_{2}, a_{0} b_{1}+a_{1} b_{0}, a_{0} b_{0}\right\}$
- at least $\operatorname{rk}(\mathcal{T})=4$ products required
- Attempt with $k=4$ :
- $W=T$
- $T \cap \mathcal{G}=\left\{a_{0} \cdot b_{0}, a_{1} \cdot b_{2}, \quad\left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{1}+b_{2}\right)\right\}$


## Example (cont'd)

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- Targets: $\mathcal{T}=\left\{a_{1} b_{2}, a_{1} b_{1}+a_{0} b_{2}, a_{0} b_{1}+a_{1} b_{0}, a_{0} b_{0}\right\}$
- at least $\operatorname{rk}(\mathcal{T})=4$ products required
- Attempt with $k=4$ :
- $W=T$
- $T \cap \mathcal{G}=\left\{a_{0} \cdot b_{0}, \quad a_{1} \cdot b_{2}, \quad\left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{1}+b_{2}\right)\right\}$
- $\operatorname{rk}(T \cap \mathcal{G})=3<k$
- no solutions with $k=4$ products only


## Example (cont'd)

## $2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- Targets: $\mathcal{T}=\left\{a_{1} b_{2}, a_{1} b_{1}+a_{0} b_{2}, a_{0} b_{1}+a_{1} b_{0}, a_{0} b_{0}\right\}$
- at least $\operatorname{rk}(\mathcal{T})=4$ products required
- Attempt with $k=4$ :
- $W=T$
- $T \cap \mathcal{G}=\left\{a_{0} \cdot b_{0}, \quad a_{1} \cdot b_{2}, \quad\left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{1}+b_{2}\right)\right\}$
- $\operatorname{rk}(T \cap \mathcal{G})=3<k$
- no solutions with $k=4$ products only
- Attempt with $k=5$ :
- Try with $W=T \oplus \operatorname{Span}\left\{a_{0} b_{1}\right\}$
- $W \cap \mathcal{G}=\left\{a_{0} \cdot b_{0}\right.$
$a_{1} \cdot b_{0}$
$\left(a_{0}+a_{1}\right) \cdot b_{0}$,
$a_{0} \cdot b_{1}, \quad a_{1} \cdot b_{2}, \quad\left(a_{0}+a_{1}\right) \cdot\left(b_{1}+b_{2}\right)$,
$\left.a_{0} \cdot\left(b_{0}+b_{1}\right), \quad a_{1} \cdot\left(b_{0}+b_{2}\right), \quad\left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{1}+b_{2}\right)\right\}$


## Example (cont'd)

## $2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- Targets: $\mathcal{T}=\left\{a_{1} b_{2}, a_{1} b_{1}+a_{0} b_{2}, a_{0} b_{1}+a_{1} b_{0}, a_{0} b_{0}\right\}$
- at least $\operatorname{rk}(\mathcal{T})=4$ products required
- Attempt with $k=4$ :
- $W=T$
- $T \cap \mathcal{G}=\left\{a_{0} \cdot b_{0}, a_{1} \cdot b_{2}, \quad\left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{1}+b_{2}\right)\right\}$
- $\operatorname{rk}(T \cap \mathcal{G})=3<k$
- no solutions with $k=4$ products only
- Attempt with $k=5$ :
- Try with $W=T \oplus \operatorname{Span}\left\{a_{0} b_{1}\right\}$
- W $\cap \mathcal{G}= \begin{cases}a_{0} \cdot b_{0}, & a_{1} \cdot b_{0}\end{cases}$

$$
\begin{array}{lll}
a_{0} \cdot b_{1}, & a_{1} \cdot b_{2}, & \left(a_{0}+a_{1}\right) \cdot\left(b_{1}+b_{2}\right) \\
a_{0} \cdot\left(b_{0}+b_{1}\right), & a_{1} \cdot\left(b_{0}+b_{2}\right), & \left.\left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{1}+b_{2}\right)\right\}
\end{array}
$$

- $\operatorname{rk}(W \cap \mathcal{G})=5=k, W$ is a solution!


## Example (cont'd)

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- Targets: $\mathcal{T}=\left\{a_{1} b_{2}, a_{1} b_{1}+a_{0} b_{2}, a_{0} b_{1}+a_{1} b_{0}, a_{0} b_{0}\right\}$
- at least $\operatorname{rk}(\mathcal{T})=4$ products required
- Attempt with $k=4$ :
- $W=T$
- $T \cap \mathcal{G}=\left\{a_{0} \cdot b_{0}, \quad a_{1} \cdot b_{2}, \quad\left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{1}+b_{2}\right)\right\}$
- $\operatorname{rk}(T \cap \mathcal{G})=3<k$
- no solutions with $k=4$ products only
- Attempt with $k=5$ :
- Try with $W=T \oplus \operatorname{Span}\left\{a_{0} b_{1}\right\}$
- W $\cap \mathcal{G}= \begin{cases}a_{0} \cdot b_{0}, & a_{1} \cdot b_{0},\end{cases}$ $\left(a_{0}+a_{1}\right) \cdot b_{0}$,
$a_{0} \cdot b_{1}, \quad a_{1} \cdot b_{2}, \quad\left(a_{0}+a_{1}\right) \cdot\left(b_{1}+b_{2}\right)$,
$\left.a_{0} \cdot\left(b_{0}+b_{1}\right), \quad a_{1} \cdot\left(b_{0}+b_{2}\right), \quad\left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{1}+b_{2}\right)\right\}$
- $\operatorname{rk}(W \cap \mathcal{G})=5=k, W$ is a solution!
- $\left\{a_{0} b_{0}, a_{1} b_{0}, a_{0} b_{1}, a_{1} b_{2},\left(a_{0}+a_{1}\right)\left(b_{1}+b_{2}\right)\right\}$ is a basis of $W$, and gives a formula


## Example (cont'd)

## $2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- Targets: $\mathcal{T}=\left\{a_{1} b_{2}, a_{1} b_{1}+a_{0} b_{2}, a_{0} b_{1}+a_{1} b_{0}, a_{0} b_{0}\right\}$
- at least $\operatorname{rk}(\mathcal{T})=4$ products required
- Attempt with $k=4$ :
- $W=T$
- $T \cap \mathcal{G}=\left\{a_{0} \cdot b_{0}, a_{1} \cdot b_{2}, \quad\left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{1}+b_{2}\right)\right\}$
- $\operatorname{rk}(T \cap \mathcal{G})=3<k$
- no solutions with $k=4$ products only
- Attempt with $k=5$ :
- Try with $W=T \oplus \operatorname{Span}\left\{a_{0} b_{1}\right\}$
- W $\cap \mathcal{G}=\left\{a_{0} \cdot b_{0}, \quad a_{1} \cdot b_{0}\right.$, $\left(a_{0}+a_{1}\right) \cdot b_{0}$,
$a_{0} \cdot b_{1}, \quad a_{1} \cdot b_{2}, \quad\left(a_{0}+a_{1}\right) \cdot\left(b_{1}+b_{2}\right)$,

$$
\left.a_{0} \cdot\left(b_{0}+b_{1}\right), \quad a_{1} \cdot\left(b_{0}+b_{2}\right), \quad\left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{1}+b_{2}\right)\right\}
$$

- $\operatorname{rk}(W \cap \mathcal{G})=5=k, W$ is a solution!
- $\left\{a_{0} b_{0}, a_{1} b_{0}, a_{0} b_{1}, a_{1} b_{2},\left(a_{0}+a_{1}\right)\left(b_{1}+b_{2}\right)\right\}$ is a basis of $W$, and gives a formula
- there are 3 such solution spaces which yield a total of 162 formulae


## A generic algorithm

- This algorithm will find all formulae with a prescribed number of products $k$
- as long as we consider all the potential products in $\mathcal{G}$
- can be used to prove lower bounds on the number of required products


## A generic algorithm

- This algorithm will find all formulae with a prescribed number of products $k$
- as long as we consider all the potential products in $\mathcal{G}$
- can be used to prove lower bounds on the number of required products
- This algorithm works for every bilinear maps:
- short products, middle products, cross products
- multiplication in complexes, quaternions, field extensions, matrices
- multiplication of sparse polynomials and matrices
- etc.


## A generic algorithm

- This algorithm will find all formulae with a prescribed number of products $k$
- as long as we consider all the potential products in $\mathcal{G}$
- can be used to prove lower bounds on the number of required products
- This algorithm works for every bilinear maps:
- short products, middle products, cross products
- multiplication in complexes, quaternions, field extensions, matrices
- multiplication of sparse polynomials and matrices
- etc.
- Also works for maps where the coefficients are quadratic forms
- simply requires extending the definition of $\mathcal{G}$ :

$$
\mathcal{G}=\left\{\left(\sum \alpha_{i} a_{i}\right) \cdot\left(\sum \alpha_{i}^{\prime} a_{i}\right) \mid\left(\alpha_{0}, \ldots, \alpha_{n-1}\right) \preccurlyeq \operatorname{lex}\left(\alpha_{0}^{\prime}, \ldots, \alpha_{n-1}^{\prime}\right)\right\} \backslash\{0\} / \sim
$$

## A generic algorithm

- This algorithm will find all formulae with a prescribed number of products $k$
- as long as we consider all the potential products in $\mathcal{G}$
- can be used to prove lower bounds on the number of required products
- This algorithm works for every bilinear maps:
- short products, middle products, cross products
- multiplication in complexes, quaternions, field extensions, matrices
- multiplication of sparse polynomials and matrices
- etc.
- Also works for maps where the coefficients are quadratic forms
- simply requires extending the definition of $\mathcal{G}$ :

$$
\mathcal{G}=\left\{\left(\sum \alpha_{i} a_{i}\right) \cdot\left(\sum \alpha_{i}^{\prime} a_{i}\right) \mid\left(\alpha_{0}, \ldots, \alpha_{n-1}\right) \preccurlyeq \operatorname{lex}\left(\alpha_{0}^{\prime}, \ldots, \alpha_{n-1}^{\prime}\right)\right\} \backslash\{0\} / \sim
$$

- example: squaring of a 2-term polynomial in $\mathbb{F}_{3}[X]$
$\mathcal{G}=\left\{a_{0} \cdot a_{0}\right.$,

$$
\begin{array}{ll}
a_{0} \cdot a_{1}, & a_{1} \cdot\left(a_{0}+a_{1}\right), \\
a_{0} \cdot\left(a_{0}+a_{1}\right), & a_{1} \cdot\left(a_{0}+a_{1}\right), \\
\left(a_{0}+a_{1}\right) \cdot\left(a_{0}+a_{1}\right), \\
a_{0} \cdot\left(a_{0}-a_{1}\right), & a_{1} \cdot\left(a_{0}-a_{1}\right), \\
\left(a_{0}+a_{1}\right) \cdot\left(a_{0}-a_{1}\right) & \left.\left(a_{0}-a_{1}\right) \cdot\left(a_{0}-a_{1}\right)\right\}
\end{array}
$$

# Outline of the talk 

- Formulae for polynomial multiplication
- Enumerating formulae
- Further improvements and heuristics
- Some results


## Symmetric bilinear maps

- We consider only symmetric bilinear maps
- same number of $a_{i}$ 's and $b_{j}$ 's: $F: K^{n} \times K^{n} \rightarrow K^{\ell}$
- symmetry: $F(\mathbf{a}, \mathbf{b})=F(\mathbf{b}, \mathbf{a})$
- for instance, multiplication of two $n$-term polynomials


## Symmetric bilinear maps

- We consider only symmetric bilinear maps
- same number of $a_{i}$ 's and $b_{j}$ 's: $F: K^{n} \times K^{n} \rightarrow K^{\ell}$
- symmetry: $F(\mathbf{a}, \mathbf{b})=F(\mathbf{b}, \mathbf{a})$
- for instance, multiplication of two $n$-term polynomials
- Heuristic: consider only products with same linear combination for the $a_{i}$ 's and $b_{i}$ 's

$$
\mathcal{G}_{\text {sym }}=\left\{\left(\sum \alpha_{i} a_{i}\right) \cdot\left(\sum \alpha_{i} b_{i}\right) \mid \forall i, \alpha_{i} \in K\right\} \backslash\{0\} / \sim
$$

## Symmetric bilinear maps

- We consider only symmetric bilinear maps
- same number of $a_{i}$ 's and $b_{j}$ 's: $F: K^{n} \times K^{n} \rightarrow K^{\ell}$
- symmetry: $F(\mathbf{a}, \mathbf{b})=F(\mathbf{b}, \mathbf{a})$
- for instance, multiplication of two $n$-term polynomials
- Heuristic: consider only products with same linear combination for the $a_{i}$ 's and $b_{i}$ 's

$$
\mathcal{G}_{\text {sym }}=\left\{\left(\sum \alpha_{i} a_{i}\right) \cdot\left(\sum \alpha_{i} b_{i}\right) \mid \forall i, \alpha_{i} \in K\right\} \backslash\{0\} / \sim
$$

(-) reduce the number of generators: $\# \mathcal{G}_{\text {sym }}=\sqrt{\# \mathcal{G}}$
(2) formulae involving asymmetric products will not be found

## Symmetric bilinear maps

- We consider only symmetric bilinear maps
- same number of $a_{i}$ 's and $b_{j}$ 's: $F: K^{n} \times K^{n} \rightarrow K^{\ell}$
- symmetry: $F(\mathbf{a}, \mathbf{b})=F(\mathbf{b}, \mathbf{a})$
- for instance, multiplication of two $n$-term polynomials
- Heuristic: consider only products with same linear combination for the $a_{i}$ 's and $b_{i}$ 's

$$
\mathcal{G}_{\text {sym }}=\left\{\left(\sum \alpha_{i} a_{i}\right) \cdot\left(\sum \alpha_{i} b_{i}\right) \mid \forall i, \alpha_{i} \in K\right\} \backslash\{0\} / \sim
$$

(;) reduce the number of generators: $\# \mathcal{G}_{\text {sym }}=\sqrt{\# \mathcal{G}}$
(:) formulae involving asymmetric products will not be found

- Example: $2 \times 2$-term polynomial product in $\mathbb{F}_{3}[X]$

$$
\begin{aligned}
& \mathcal{G}=\left\{a_{0} \cdot b_{0}, \quad a_{1} \cdot b_{0}, \quad\left(a_{0}+a_{1}\right) \cdot b_{0}, \quad\left(a_{0}-a_{1}\right) \cdot b_{0},\right. \\
& a_{0} \cdot b_{1}, \quad a_{1} \cdot b_{1}, \quad\left(a_{0}+a_{1}\right) \cdot b_{1}, \quad\left(a_{0}-a_{1}\right) \cdot b_{1}, \\
& a_{0} \cdot\left(b_{0}+b_{1}\right), a_{1} \cdot\left(b_{0}+b_{1}\right), \quad\left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{1}\right),\left(a_{0}-a_{1}\right) \cdot\left(b_{0}+b_{1}\right), \\
& \left.a_{0} \cdot\left(b_{0}-b_{1}\right), a_{1} \cdot\left(b_{0}-b_{1}\right),\left(a_{0}+a_{1}\right) \cdot\left(b_{0}-b_{1}\right),\left(a_{0}-a_{1}\right) \cdot\left(b_{0}-b_{1}\right)\right\}
\end{aligned}
$$

## Symmetric bilinear maps

- We consider only symmetric bilinear maps
- same number of $a_{i}$ 's and $b_{j}$ 's: $F: K^{n} \times K^{n} \rightarrow K^{\ell}$
- symmetry: $F(\mathbf{a}, \mathbf{b})=F(\mathbf{b}, \mathbf{a})$
- for instance, multiplication of two $n$-term polynomials
- Heuristic: consider only products with same linear combination for the $a_{i}$ 's and $b_{i}$ 's

$$
\mathcal{G}_{\text {sym }}=\left\{\left(\sum \alpha_{i} a_{i}\right) \cdot\left(\sum \alpha_{i} b_{i}\right) \mid \forall i, \alpha_{i} \in K\right\} \backslash\{0\} / \sim
$$

(;) reduce the number of generators: $\# \mathcal{G}_{\text {sym }}=\sqrt{\# \mathcal{G}}$
(:) formulae involving asymmetric products will not be found

- Example: $2 \times 2$-term polynomial product in $\mathbb{F}_{3}[X]$

$$
\begin{array}{rlll}
\mathcal{G}_{\text {sym }}=\left\{\begin{array}{lll}
a_{0} \cdot b_{0}, & a_{1} \cdot b_{0}, & \left(a_{0}+a_{1}\right) \cdot b_{0},
\end{array}\right. & \left(a_{0}-a_{1}\right) \cdot b_{0}, \\
a_{0} \cdot b_{1}, & a_{1} \cdot b_{1}, & \left(a_{0}+a_{1}\right) \cdot b_{1}, & \left(a_{0}-a_{1}\right) \cdot b_{1}, \\
a_{0} \cdot\left(b_{0}+b_{1}\right), & a_{1} \cdot\left(b_{0}+b_{1}\right), & \left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{1}\right), & \left(a_{0}-a_{1}\right) \cdot\left(b_{0}+b_{1}\right), \\
a_{0} \cdot\left(b_{0}-b_{1}\right), & a_{1} \cdot\left(b_{0}-b_{1}\right), & \left(a_{0}+a_{1}\right) \cdot\left(b_{0}-b_{1}\right), & \left.\left(a_{0}-a_{1}\right) \cdot\left(b_{0}-b_{1}\right)\right\}
\end{array}
$$

## Orbits of a group action

Back to bilinear maps $F: K^{n} \times K^{m} \rightarrow K^{\ell}$

## Orbits of a group action

Back to bilinear maps $F: K^{n} \times K^{m} \rightarrow K^{\ell}$

- Consider the vector space $V=\operatorname{Span} \mathcal{V}$, with basis $\mathcal{V}=\left\{a_{i} b_{j}\right\}_{0 \leq i<n, 0 \leq j<m}$


## Orbits of a group action

Back to bilinear maps $F: K^{n} \times K^{m} \rightarrow K^{\ell}$

- Consider the vector space $V=$ Span $\mathcal{V}$, with basis $\mathcal{V}=\left\{a_{i} b_{j}\right\}_{0 \leq i<n, 0 \leq j<m}$
- Suppose there exists $\sigma \in \operatorname{Aut}(V)$ such that
- the set of generators $\mathcal{G} \subset V$ is fixed by $\sigma: \mathcal{G}^{\sigma}=\mathcal{G}$
- the target space $T \subset V$ is also fixed by $\sigma: T^{\sigma}=T$


## Orbits of a group action

Back to bilinear maps $F: K^{n} \times K^{m} \rightarrow K^{\ell}$

- Consider the vector space $V=$ Span $\mathcal{V}$, with basis $\mathcal{V}=\left\{a_{i} b_{j}\right\}_{0 \leq i<n, 0 \leq j<m}$
- Suppose there exists $\sigma \in \operatorname{Aut}(V)$ such that
- the set of generators $\mathcal{G} \subset V$ is fixed by $\sigma: \mathcal{G}^{\sigma}=\mathcal{G}$
- the target space $T \subset V$ is also fixed by $\sigma: T^{\sigma}=T$
- for instance, for the $n \times m$-term polynomial product over $K$ :
$\sigma:$
$a_{i} b_{j}$
$\longmapsto$

$$
a_{n-1-i} b_{m-1-j}
$$

## Orbits of a group action

Back to bilinear maps $F: K^{n} \times K^{m} \rightarrow K^{\ell}$

- Consider the vector space $V=\operatorname{Span} \mathcal{V}$, with basis $\mathcal{V}=\left\{a_{i} b_{j}\right\}_{0 \leq i<n, 0 \leq j<m}$
- Suppose there exists $\sigma \in \operatorname{Aut}(V)$ such that
- the set of generators $\mathcal{G} \subset V$ is fixed by $\sigma: \mathcal{G}^{\sigma}=\mathcal{G}$
- the target space $T \subset V$ is also fixed by $\sigma: T^{\sigma}=T$
- for instance, for the $n \times m$-term polynomial product over $K$ :

$$
\begin{aligned}
& \sigma: \quad a_{i} b_{j} \quad \longmapsto \quad a_{n-1-i} b_{m-1-j} \\
& \left(\sum \alpha_{i} a_{i}\right) \cdot\left(\sum \beta_{j} b_{j}\right) \longmapsto\left(\sum \alpha_{n-1-i} a_{i}\right) \cdot\left(\sum \beta_{m-1-j} b_{j}\right)
\end{aligned}
$$

## Orbits of a group action

Back to bilinear maps $F: K^{n} \times K^{m} \rightarrow K^{\ell}$

- Consider the vector space $V=\operatorname{Span} \mathcal{V}$, with basis $\mathcal{V}=\left\{a_{i} b_{j}\right\}_{0 \leq i<n, 0 \leq j<m}$
- Suppose there exists $\sigma \in \operatorname{Aut}(V)$ such that
- the set of generators $\mathcal{G} \subset V$ is fixed by $\sigma: \mathcal{G}^{\sigma}=\mathcal{G}$
- the target space $T \subset V$ is also fixed by $\sigma: T^{\sigma}=T$
- for instance, for the $n \times m$-term polynomial product over $K$ :

$$
\begin{aligned}
\sigma: \quad a_{i} b_{j} & \longmapsto
\end{aligned} \stackrel{a_{n-1-i} b_{m-1-j}}{\left(\sum \alpha_{i} a_{i}\right) \cdot\left(\sum \beta_{j} b_{j}\right)} \stackrel{\longmapsto}{\left(\sum \alpha_{n-1-i} a_{i}\right) \cdot\left(\sum \beta_{m-1-j} b_{j}\right)}
$$

(corresponds to replacing $X$ by $1 / X$ )

## Orbits of a group action

Back to bilinear maps $F: K^{n} \times K^{m} \rightarrow K^{\ell}$

- Consider the vector space $V=$ Span $\mathcal{V}$, with basis $\mathcal{V}=\left\{a_{i} b_{j}\right\}_{0 \leq i<n, 0 \leq j<m}$
- Suppose there exists $\sigma \in \operatorname{Aut}(V)$ such that
- the set of generators $\mathcal{G} \subset V$ is fixed by $\sigma: \mathcal{G}^{\sigma}=\mathcal{G}$
- the target space $T \subset V$ is also fixed by $\sigma: T^{\sigma}=T$
- for instance, for the $n \times m$-term polynomial product over $K$ :

$$
\begin{aligned}
& \sigma: \quad a_{i} b_{j} \quad \longmapsto \quad a_{n-1-i} b_{m-1-j} \\
& \left(\sum \alpha_{i} a_{i}\right) \cdot\left(\sum \beta_{j} b_{j}\right) \longmapsto\left(\sum \alpha_{n-1-i} a_{i}\right) \cdot\left(\sum \beta_{m-1-j} b_{j}\right)
\end{aligned}
$$

(corresponds to replacing $X$ by $1 / X$ )

- Fact: if $W$ is a solution space, then so is $W^{\sigma}$


## Orbits of a group action

Back to bilinear maps $F: K^{n} \times K^{m} \rightarrow K^{\ell}$

- Consider the vector space $V=\operatorname{Span} \mathcal{V}$, with basis $\mathcal{V}=\left\{a_{i} b_{j}\right\}_{0 \leq i<n, 0 \leq j<m}$
- Suppose there exists $\sigma \in \operatorname{Aut}(V)$ such that
- the set of generators $\mathcal{G} \subset V$ is fixed by $\sigma: \mathcal{G}^{\sigma}=\mathcal{G}$
- the target space $T \subset V$ is also fixed by $\sigma: T^{\sigma}=T$
- for instance, for the $n \times m$-term polynomial product over $K$ :

$$
\begin{aligned}
\sigma: \quad a_{i} b_{j} & \longmapsto
\end{aligned} \stackrel{a_{n-1-i} b_{m-1-j}}{\left(\sum \alpha_{i} a_{i}\right) \cdot\left(\sum \beta_{j} b_{j}\right)} \stackrel{\longmapsto}{\left(\sum \alpha_{n-1-i} a_{i}\right) \cdot\left(\sum \beta_{m-1-j} b_{j}\right)}
$$

(corresponds to replacing $X$ by $1 / X$ )

- Fact: if $W$ is a solution space, then so is $W^{\sigma}$
- Idea: group generators $g \in \mathcal{G}$ according to their $\sigma$-orbit

$$
\overline{\mathcal{G}}=\{\bar{g} \mid g \in \mathcal{G}\}, \quad \text { where } \bar{g}=\left\{g^{\prime} \in \mathcal{G} \mid g^{\prime}=\sigma^{i}(g)\right\}
$$

## Orbits of a group action

Back to bilinear maps $F: K^{n} \times K^{m} \rightarrow K^{\ell}$

- Consider the vector space $V=\operatorname{Span} \mathcal{V}$, with basis $\mathcal{V}=\left\{a_{i} b_{j}\right\}_{0 \leq i<n, 0 \leq j<m}$
- Suppose there exists $\sigma \in \operatorname{Aut}(V)$ such that
- the set of generators $\mathcal{G} \subset V$ is fixed by $\sigma: \mathcal{G}^{\sigma}=\mathcal{G}$
- the target space $T \subset V$ is also fixed by $\sigma: T^{\sigma}=T$
- for instance, for the $n \times m$-term polynomial product over $K$ :

$$
\left.\begin{array}{rl}
\sigma: \quad a_{i} b_{j} & \longmapsto
\end{array} \stackrel{a_{n-1-i} b_{m-1-j}}{ } \quad \begin{array}{l}
\left(\sum \alpha_{i} a_{i}\right) \cdot\left(\sum \beta_{j} b_{j}\right)
\end{array}\right)\left(\sum \alpha_{n-1-i} a_{i}\right) \cdot\left(\sum \beta_{m-1-j} b_{j}\right)
$$

(corresponds to replacing $X$ by $1 / X$ )

- Fact: if $W$ is a solution space, then so is $W^{\sigma}$
- Idea: group generators $g \in \mathcal{G}$ according to their $\sigma$-orbit

$$
\overline{\mathcal{G}}=\{\bar{g} \mid g \in \mathcal{G}\}, \quad \text { where } \bar{g}=\left\{g^{\prime} \in \mathcal{G} \mid g^{\prime}=\sigma^{i}(g)\right\}
$$

- As long as $W$ is fixed by $\sigma$, try only one generator per equivalence class


## Orbits of a group action

Back to bilinear maps $F: K^{n} \times K^{m} \rightarrow K^{\ell}$

- Consider the vector space $V=\operatorname{Span} \mathcal{V}$, with basis $\mathcal{V}=\left\{a_{i} b_{j}\right\}_{0 \leq i<n, 0 \leq j<m}$
- Suppose there exists $\sigma \in \operatorname{Aut}(V)$ such that
- the set of generators $\mathcal{G} \subset V$ is fixed by $\sigma: \mathcal{G}^{\sigma}=\mathcal{G}$
- the target space $T \subset V$ is also fixed by $\sigma: T^{\sigma}=T$
- for instance, for the $n \times m$-term polynomial product over $K$ :

$$
\begin{aligned}
& \sigma: \quad a_{i} b_{j} \longmapsto \\
&\left(\sum \alpha_{i} a_{i}\right) \cdot\left(\sum \beta_{j} b_{j}\right) a_{n-1-i} b_{m-1-j} \\
&\left(\sum \alpha_{n-1-i} a_{i}\right) \cdot\left(\sum \beta_{m-1-j} b_{j}\right)
\end{aligned}
$$

(corresponds to replacing $X$ by $1 / X$ )

- Fact: if $W$ is a solution space, then so is $W^{\sigma}$
- Idea: group generators $g \in \mathcal{G}$ according to their $\sigma$-orbit

$$
\overline{\mathcal{G}}=\{\bar{g} \mid g \in \mathcal{G}\}, \quad \text { where } \bar{g}=\left\{g^{\prime} \in \mathcal{G} \mid g^{\prime}=\sigma^{i}(g)\right\}
$$

- As long as $W$ is fixed by $\sigma$, try only one generator per equivalence class
- Heuristic: add whole equivalence classes $\bar{g}$ to $W$, instead of single generators


## Orbits of a group action

Back to bilinear maps $F: K^{n} \times K^{m} \rightarrow K^{\ell}$

- Consider the vector space $V=\operatorname{Span} \mathcal{V}$, with basis $\mathcal{V}=\left\{a_{i} b_{j}\right\}_{0 \leq i<n, 0 \leq j<m}$
- Suppose there exists $\sigma \in \operatorname{Aut}(V)$ such that
- the set of generators $\mathcal{G} \subset V$ is fixed by $\sigma: \mathcal{G}^{\sigma}=\mathcal{G}$
- the target space $T \subset V$ is also fixed by $\sigma: T^{\sigma}=T$
- for instance, for the $n \times m$-term polynomial product over $K$ :

$$
\begin{aligned}
\sigma: & a_{i} b_{j} \\
\left(\sum \alpha_{i} a_{i}\right) \cdot\left(\sum \beta_{j} b_{j}\right) & \longmapsto
\end{aligned} \stackrel{a_{n-1-i} b_{m-1-j}}{ }\left(\sum \alpha_{n-1-i} a_{i}\right) \cdot\left(\sum \beta_{m-1-j} b_{j}\right)
$$

(corresponds to replacing $X$ by $1 / X$ )

- Fact: if $W$ is a solution space, then so is $W^{\sigma}$
- Idea: group generators $g \in \mathcal{G}$ according to their $\sigma$-orbit

$$
\overline{\mathcal{G}}=\{\bar{g} \mid g \in \mathcal{G}\}, \quad \text { where } \bar{g}=\left\{g^{\prime} \in \mathcal{G} \mid g^{\prime}=\sigma^{i}(g)\right\}
$$

- As long as $W$ is fixed by $\sigma$, try only one generator per equivalence class
- Heuristic: add whole equivalence classes $\bar{g}$ to $W$, instead of single generators
- Going further: instead of a single $\sigma \in \operatorname{Aut}(V)$, take a whole subgroup $S \subset \operatorname{Aut}(V)$


# Orbits of a group action: Example 

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- $\mathcal{G}$ and $T$ are fixed by $S=\left\langle\sigma_{0}, \sigma_{1}\right\rangle \subset \operatorname{Aut}(V)$ with
- $\sigma_{0}: a_{i} b_{j} \mapsto a_{1-i} b_{2-j}$ (i.e., replace $X$ by $1 / X$ )
- $\sigma_{1}: a_{i} b_{j} \mapsto\left(\sum_{k=i}^{1}\binom{k}{i} a_{k}\right) \cdot\left(\sum_{k=j}^{2}\binom{k}{j} b_{k}\right)$ (i.e., replace $X$ by $\left.1-X\right)$


## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- $\mathcal{G}$ and $T$ are fixed by $S=\left\langle\sigma_{0}, \sigma_{1}\right\rangle \subset \operatorname{Aut}(V)$ with
- $\sigma_{0}: a_{i} b_{j} \mapsto a_{1-i} b_{2-j}$ (i.e., replace $X$ by $1 / X$ )
- $\sigma_{1}: a_{i} b_{j} \mapsto\left(\sum_{k=i}^{1}\binom{k}{i} a_{k}\right) \cdot\left(\sum_{k=j}^{2}\binom{k}{j} b_{k}\right)$ (i.e., replace $X$ by $\left.1-X\right)$
- Remark that $\# S=6$ (hurray for non-commutativity!)


## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- $\mathcal{G}$ and $T$ are fixed by $S=\left\langle\sigma_{0}, \sigma_{1}\right\rangle \subset \operatorname{Aut}(V)$ with
- $\sigma_{0}: a_{i} b_{j} \mapsto a_{1-i} b_{2-j}$ (i.e., replace $X$ by $1 / X$ )
- $\sigma_{1}: a_{i} b_{j} \mapsto\left(\sum_{k=i}^{1}\binom{k}{i} a_{k}\right) \cdot\left(\sum_{k=j}^{2}\binom{k}{j} b_{k}\right)$ (i.e., replace $X$ by $\left.1-X\right)$
- Remark that $\# S=6$ (hurray for non-commutativity!)
- $\mathcal{G}$ can be partitioned into


## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- $\mathcal{G}$ and $T$ are fixed by $S=\left\langle\sigma_{0}, \sigma_{1}\right\rangle \subset \operatorname{Aut}(V)$ with
- $\sigma_{0}: a_{i} b_{j} \mapsto a_{1-i} b_{2-j}$ (i.e., replace $X$ by $1 / X$ )
- $\sigma_{1}: a_{i} b_{j} \mapsto\left(\sum_{k=i}^{1}\binom{k}{i} a_{k}\right) \cdot\left(\sum_{k=j}^{2}\binom{k}{j} b_{k}\right)$ (i.e., replace $X$ by $\left.1-X\right)$
- Remark that $\# S=6$ (hurray for non-commutativity!)
- $\mathcal{G}$ can be partitioned into
- 3 orbits of size 3:

$$
\begin{array}{lll}
\overline{g_{0}}=\left\{a_{0} \cdot b_{0},\right. & a_{1} \cdot b_{2}, & \left.\left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{1}+b_{2}\right)\right\}, \\
\overline{g_{1}}=\left\{a_{0} \cdot b_{1},\right. & a_{1} \cdot b_{1}, & \left.\left(a_{0}+a_{1}\right) \cdot b_{1}\right\}, \\
\overline{g_{2}}=\left\{a_{0} \cdot\left(b_{0}+b_{1}\right),\right. & a_{1} \cdot\left(b_{1}+b_{2}\right), & \left.\left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{2}\right)\right\}, \text { and }
\end{array}
$$

## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- $\mathcal{G}$ and $T$ are fixed by $S=\left\langle\sigma_{0}, \sigma_{1}\right\rangle \subset \operatorname{Aut}(V)$ with
- $\sigma_{0}: a_{i} b_{j} \mapsto a_{1-i} b_{2-j}$ (i.e., replace $X$ by $1 / X$ )
- $\sigma_{1}: a_{i} b_{j} \mapsto\left(\sum_{k=i}^{1}\binom{k}{i} a_{k}\right) \cdot\left(\sum_{k=j}^{2}\binom{k}{j} b_{k}\right)$ (i.e., replace $X$ by $\left.1-X\right)$
- Remark that $\# S=6$ (hurray for non-commutativity!)
- $\mathcal{G}$ can be partitioned into
- 3 orbits of size 3:

$$
\begin{array}{lll}
\overline{g_{0}}=\left\{a_{0} \cdot b_{0},\right. & a_{1} \cdot b_{2}, & \left.\left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{1}+b_{2}\right)\right\}, \\
\overline{g_{1}}=\left\{a_{0} \cdot b_{1},\right. & a_{1} \cdot b_{1}, & \left.\left(a_{0}+a_{1}\right) \cdot b_{1}\right\}, \\
\overline{g_{2}}=\left\{a_{0} \cdot\left(b_{0}+b_{1}\right),\right. & a_{1} \cdot\left(b_{1}+b_{2}\right), & \left.\left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{2}\right)\right\}, \text { and }
\end{array}
$$

- 2 orbits of size 6 :

$$
\begin{aligned}
& \overline{g_{3}}=\left\{a_{0} \cdot b_{2}, \quad a_{0} \cdot\left(b_{0}+b_{1}+b_{2}\right),\left(a_{0}+a_{1}\right) \cdot b_{0},\right. \\
& \left.a_{1} \cdot b_{0}, \quad a_{1} \cdot\left(b_{0}+b_{1}+b_{2}\right),\left(a_{0}+a_{1}\right) \cdot b_{2}\right\}, \\
& \overline{g_{4}}=\left\{a_{0} \cdot\left(b_{0}+b_{2}\right), a_{0} \cdot\left(b_{1}+b_{2}\right), \quad\left(a_{0}+a_{1}\right) \cdot\left(b_{0}+b_{1}\right),\right. \\
& \left.a_{1} \cdot\left(b_{0}+b_{2}\right), a_{1} \cdot\left(b_{0}+b_{1}\right), \quad\left(a_{0}+a_{1}\right) \cdot\left(b_{1}+b_{2}\right)\right\}
\end{aligned}
$$

## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- First, consider adding to $T$ a generator from orbit $\overline{g_{1}}$ :

$$
\sigma_{0} G\left(a_{0}+a_{1}\right) \cdot b_{1} \stackrel{\sigma_{1}}{\leftrightarrows} a_{0} \cdot b_{1} \stackrel{\sigma_{0}}{\leftrightarrows} a_{1} \cdot b_{1} \bigcirc \sigma_{1}
$$

## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- First, consider adding to $T$ a generator from orbit $\overline{g_{1}}$ :

$$
\sigma_{0} G\left(a_{0}+a_{1}\right) \cdot b_{1} \stackrel{\sigma_{1}}{\leftrightarrows} a_{0} \cdot b_{1} \stackrel{\sigma_{0}}{\leftrightarrows} a_{1} \cdot b_{1} \bigcirc \sigma_{1}
$$

## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- First, consider adding to $T$ a generator from orbit $\overline{g_{1}}$ :

$$
\sigma_{0} G\left(a_{0}+a_{1}\right) \cdot b_{1} \stackrel{\sigma_{1}}{\leftrightarrows} a_{0} \cdot b_{1} \stackrel{\sigma_{0}}{\leftrightarrows} a_{1} \cdot b_{1} \bigcirc \sigma_{1}
$$



## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- First, consider adding to $T$ a generator from orbit $\overline{g_{1}}$ :

$$
\sigma_{0} G\left(a_{0}+a_{1}\right) \cdot b_{1} \stackrel{\sigma_{1}}{\leftrightarrows} a_{0} \cdot b_{1} \stackrel{\sigma_{0}}{\leftrightarrows} a_{1} \cdot b_{1} \bigcirc \sigma_{1}
$$



## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- First, consider adding to $T$ a generator from orbit $\overline{g_{1}}$ :

$$
\sigma_{0} G\left(a_{0}+a_{1}\right) \cdot b_{1} \stackrel{\sigma_{1}}{\leftrightarrows} a_{0} \cdot b_{1} \stackrel{\sigma_{0}}{\leftrightarrows} a_{1} \cdot b_{1} \bigcirc \sigma_{1}
$$

- For any solution of the form $W=T \oplus \operatorname{Span}\left(a_{0} \cdot b_{1}\right) \oplus \operatorname{Span} \mathcal{W}^{\prime}$, with $\mathcal{W}^{\prime} \subset \mathcal{G}$ :



## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- First, consider adding to $T$ a generator from orbit $\overline{g_{1}}$ :

$$
\sigma_{0} G\left(a_{0}+a_{1}\right) \cdot b_{1} \stackrel{\sigma_{1}}{\leftrightarrows} a_{0} \cdot b_{1} \stackrel{\sigma_{0}}{\leftrightarrows} a_{1} \cdot b_{1} \bigcirc \sigma_{1}
$$

- For any solution of the form $W=T \oplus \operatorname{Span}\left(a_{0} \cdot b_{1}\right) \oplus \operatorname{Span} \mathcal{W}^{\prime}$, with $\mathcal{W}^{\prime} \subset \mathcal{G}$ :
- $W^{\sigma_{1}}=T \oplus \operatorname{Span}\left(\left(a_{0}+a_{1}\right) \cdot b_{1}\right) \oplus \mathcal{W}^{\prime \sigma_{1}}$, with $\mathcal{W}^{\prime \sigma_{1}} \subset \mathcal{G}$, is also a solution

$$
T \xlongequal{\ldots \ldots \ldots \ldots}\left(\begin{array}{l}
\left.a_{0}+a_{1}\right) \cdot b_{1} \\
a_{0} \cdot b_{1} \\
a_{1} \cdot b_{1} \\
\ldots
\end{array} \quad \equiv \begin{array}{c} 
\\
\ldots \ldots \ldots
\end{array}\right.
$$

## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- First, consider adding to $T$ a generator from orbit $\overline{g_{1}}$ :

$$
\sigma_{0} G\left(a_{0}+a_{1}\right) \cdot b_{1} \stackrel{\sigma_{1}}{\leftrightarrows} a_{0} \cdot b_{1} \stackrel{\sigma_{0}}{\leftrightarrows} a_{1} \cdot b_{1} \bigcirc \sigma_{1}
$$

- For any solution of the form $W=T \oplus \operatorname{Span}\left(a_{0} \cdot b_{1}\right) \oplus \operatorname{Span} \mathcal{W}^{\prime}$, with $\mathcal{W}^{\prime} \subset \mathcal{G}$ :
- $W^{\sigma_{1}}=T \oplus \operatorname{Span}\left(\left(a_{0}+a_{1}\right) \cdot b_{1}\right) \oplus \mathcal{W}^{\prime \sigma_{1}}$, with $\mathcal{W}^{\prime \sigma_{1}} \subset \mathcal{G}$, is also a solution
- thus, no need to enumerate both $\left(a_{0}+a_{1}\right) \cdot b_{1}$ and $a_{0} \cdot b_{1}$



## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- First, consider adding to $T$ a generator from orbit $\overline{g_{1}}$ :

$$
\sigma_{0} G\left(a_{0}+a_{1}\right) \cdot b_{1} \stackrel{\sigma_{1}}{\leftrightarrows} a_{0} \cdot b_{1} \stackrel{\sigma_{0}}{\leftrightarrows} a_{1} \cdot b_{1} \bigcirc \sigma_{1}
$$

- For any solution of the form $W=T \oplus \operatorname{Span}\left(a_{0} \cdot b_{1}\right) \oplus \operatorname{Span} \mathcal{W}^{\prime}$, with $\mathcal{W}^{\prime} \subset \mathcal{G}$ :
- $W^{\sigma_{1}}=T \oplus \operatorname{Span}\left(\left(a_{0}+a_{1}\right) \cdot b_{1}\right) \oplus \mathcal{W}^{\prime \sigma_{1}}$, with $\mathcal{W}^{\prime \sigma_{1}} \subset \mathcal{G}$, is also a solution
- thus, no need to enumerate both $\left(a_{0}+a_{1}\right) \cdot b_{1}$ and $a_{0} \cdot b_{1}$



## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- First, consider adding to $T$ a generator from orbit $\overline{g_{1}}$ :

$$
\sigma_{0} G\left(a_{0}+a_{1}\right) \cdot b_{1} \stackrel{\sigma_{1}}{\leftrightarrows} a_{0} \cdot b_{1} \stackrel{\sigma_{0}}{\leftrightarrows} a_{1} \cdot b_{1} \bigcirc \sigma_{1}
$$

- For any solution of the form $\mathcal{W}=T \oplus \operatorname{Span}\left(a_{0} \cdot b_{1}\right) \oplus \operatorname{Span} \mathcal{W}^{\prime}$, with $\mathcal{W}^{\prime} \subset \mathcal{G}$ :
- $W^{\sigma_{1}}=T \oplus \operatorname{Span}\left(\left(a_{0}+a_{1}\right) \cdot b_{1}\right) \oplus \mathcal{W}^{\prime \sigma_{1}}$, with $\mathcal{W}^{\prime \sigma_{1}} \subset \mathcal{G}$, is also a solution
- thus, no need to enumerate both $\left(a_{0}+a_{1}\right) \cdot b_{1}$ and $a_{0} \cdot b_{1}$
- Similarly, for any solution $W=T \oplus \operatorname{Span}\left(a_{1} \cdot b_{1}\right) \oplus \operatorname{Span} \mathcal{W}^{\prime}$, with $\mathcal{W}^{\prime} \subset \mathcal{G}$ :
- $W^{\sigma_{0} \sigma_{1}}=T \oplus \operatorname{Span}\left(\left(a_{0}+a_{1}\right) \cdot b_{1}\right) \oplus \mathcal{W}^{\prime \sigma_{0} \sigma_{1}}$, with $\mathcal{W}^{\prime \sigma_{0} \sigma_{1}} \subset \mathcal{G}$, is also a solution



# Orbits of a group action: Example 

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- So we add generator $\left(a_{0}+a_{1}\right) \cdot b_{1}$, fixed by $\sigma_{0}$



## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- So we add generator $\left(a_{0}+a_{1}\right) \cdot b_{1}$, fixed by $\sigma_{0}$
- Now, consider adding to $T \oplus \operatorname{Span}\left(\left(a_{0}+a_{1}\right) \cdot b_{1}\right)$ a generator from orbit $\overline{g_{3}}$ :

$$
\begin{array}{ccc}
a_{0} \cdot b_{2} & \stackrel{\sigma_{0}}{\leftrightarrows} & a_{1} \cdot b_{0} \quad \stackrel{\sigma_{1}}{\leftrightarrows} a_{1} \cdot\left(b_{0}+b_{1}+b_{2}\right) \\
\begin{array}{c}
\sigma_{1} \uparrow \downarrow \\
\left(a_{0}+a_{1}\right) \cdot b_{2}
\end{array} & \stackrel{\sigma_{0}}{\leftrightarrows}\left(a_{0}+a_{1}\right) \cdot b_{0} & \stackrel{\sigma_{1}}{\leftrightarrows} a_{0} \cdot\left(b_{0}+b_{1}+b_{2}\right)
\end{array}
$$

## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- So we add generator $\left(a_{0}+a_{1}\right) \cdot b_{1}$, fixed by $\sigma_{0}$
- Now, consider adding to $T \oplus \operatorname{Span}\left(\left(a_{0}+a_{1}\right) \cdot b_{1}\right)$ a generator from orbit $\overline{g_{3}}$ :

$$
\begin{array}{ccc}
a_{0} \cdot b_{2} & \stackrel{\sigma_{0}}{\leftrightarrows} & a_{1} \cdot b_{0} \quad \stackrel{\sigma_{1}}{\leftrightarrows} a_{1} \cdot\left(b_{0}+b_{1}+b_{2}\right) \\
\sigma_{1} \uparrow \downarrow \\
\left(a_{0}+a_{1}\right) \cdot b_{2} & \stackrel{\sigma_{0}}{\leftrightarrows}\left(a_{0}+a_{1}\right) \cdot b_{0} \stackrel{\sigma_{0}}{\leftrightarrows} a_{0} \cdot\left(b_{0}+b_{1}+b_{2}\right)
\end{array}
$$

## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- So we add generator $\left(a_{0}+a_{1}\right) \cdot b_{1}$, fixed by $\sigma_{0}$
- Now, consider adding to $T \oplus \operatorname{Span}\left(\left(a_{0}+a_{1}\right) \cdot b_{1}\right)$ a generator from orbit $\overline{g_{3}}$ :

$$
\begin{array}{ccc}
a_{0} \cdot b_{2} & \stackrel{\sigma_{0}}{\leftrightarrows} & a_{1} \cdot b_{0} \quad \stackrel{\sigma_{1}}{\leftrightarrows} a_{1} \cdot\left(b_{0}+b_{1}+b_{2}\right) \\
\sigma_{1} \uparrow \downarrow \\
\left(a_{0}+a_{1}\right) \cdot b_{2} & \stackrel{\sigma_{0}}{\leftrightarrows}\left(a_{0}+a_{1}\right) \cdot b_{0} \stackrel{\sigma_{0}}{\leftrightarrows} a_{0} \cdot\left(b_{0}+b_{1}+b_{2}\right)
\end{array}
$$



## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- So we add generator $\left(a_{0}+a_{1}\right) \cdot b_{1}$, fixed by $\sigma_{0}$
- Now, consider adding to $T \oplus \operatorname{Span}\left(\left(a_{0}+a_{1}\right) \cdot b_{1}\right)$ a generator from orbit $\overline{g_{3}}$ :

$$
\begin{array}{ccc}
a_{0} \cdot b_{2} & \stackrel{\sigma_{0}}{\leftrightarrows} & a_{1} \cdot b_{0} \quad \stackrel{\sigma_{1}}{\leftrightarrows} a_{1} \cdot\left(b_{0}+b_{1}+b_{2}\right) \\
\sigma_{1} \uparrow \downarrow \\
\left(a_{0}+a_{1}\right) \cdot b_{2} & \stackrel{\sigma_{0}}{\leftrightarrows}\left(a_{0}+a_{1}\right) \cdot b_{0} & \stackrel{\sigma_{0}}{\leftrightarrows} a_{0} \cdot\left(b_{0}+b_{1}+b_{2}\right)
\end{array}
$$

- Since $T \oplus \operatorname{Span}\left(\left(a_{0}+a_{1}\right) \cdot b_{1}\right)$ is fixed by $\sigma_{0}$, we can still partition $\overline{g_{3}}$ according to its $\sigma_{0}$-orbits



## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- So we add generator $\left(a_{0}+a_{1}\right) \cdot b_{1}$, fixed by $\sigma_{0}$
- Now, consider adding to $T \oplus \operatorname{Span}\left(\left(a_{0}+a_{1}\right) \cdot b_{1}\right)$ a generator from orbit $\overline{g_{3}}$ :

$$
\begin{array}{ccc}
a_{0} \cdot b_{2} & \stackrel{\sigma_{0}}{\leftrightarrows} & a_{1} \cdot b_{0} \quad \stackrel{\sigma_{1}}{\leftrightarrows} a_{1} \cdot\left(b_{0}+b_{1}+b_{2}\right) \\
\sigma_{1} \uparrow \downarrow \\
\left(a_{0}+a_{1}\right) \cdot b_{2} & \stackrel{\sigma_{0}}{\leftrightarrows}\left(a_{0}+a_{1}\right) \cdot b_{0} \stackrel{\sigma_{0}}{\leftrightarrows} a_{0} \cdot\left(b_{0}+b_{1}+b_{2}\right)
\end{array}
$$

- Since $T \oplus \operatorname{Span}\left(\left(a_{0}+a_{1}\right) \cdot b_{1}\right)$ is fixed by $\sigma_{0}$, we can still partition $\overline{g_{3}}$ according to its $\sigma_{0}$-orbits



## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- So we add generator $\left(a_{0}+a_{1}\right) \cdot b_{1}$, fixed by $\sigma_{0}$
- Now, consider adding to $T \oplus \operatorname{Span}\left(\left(a_{0}+a_{1}\right) \cdot b_{1}\right)$ a generator from orbit $\overline{g_{3}}$ :

$$
\begin{array}{ccc}
a_{0} \cdot b_{2} & \stackrel{\sigma_{0}}{\leftrightarrows} & a_{1} \cdot b_{0} \quad \stackrel{\sigma_{1}}{\leftrightarrows} a_{1} \cdot\left(b_{0}+b_{1}+b_{2}\right) \\
\sigma_{1} \uparrow \downarrow \\
\left(a_{0}+a_{1}\right) \cdot b_{2} & \stackrel{\sigma_{0}}{\leftrightarrows}\left(a_{0}+a_{1}\right) \cdot b_{0} \stackrel{\sigma_{0}}{\leftrightarrows} a_{0} \cdot\left(b_{0}+b_{1}+b_{2}\right)
\end{array}
$$

- Since $T \oplus \operatorname{Span}\left(\left(a_{0}+a_{1}\right) \cdot b_{1}\right)$ is fixed by $\sigma_{0}$, we can still partition $\overline{g_{3}}$ according to its $\sigma_{0}$-orbits



## Orbits of a group action: Example

$2 \times 3$-term polynomial product in $\mathbb{F}_{2}[X]$

- So we add generator $\left(a_{0}+a_{1}\right) \cdot b_{1}$, fixed by $\sigma_{0}$
- Now, consider adding to $T \oplus \operatorname{Span}\left(\left(a_{0}+a_{1}\right) \cdot b_{1}\right)$ a generator from orbit $\overline{g_{3}}$ :

$$
\begin{array}{ccc}
a_{0} \cdot b_{2} & \stackrel{\sigma_{0}}{\leftrightarrows} & a_{1} \cdot b_{0} \quad \stackrel{\sigma_{1}}{\leftrightarrows} a_{1} \cdot\left(b_{0}+b_{1}+b_{2}\right) \\
\uparrow \downarrow \downarrow \sigma_{0} \\
\left(a_{0}+a_{1}\right) \cdot b_{2} \uparrow \downarrow \\
& \stackrel{\sigma_{0}}{\leftrightarrows}\left(a_{0}+a_{1}\right) \cdot b_{0} \stackrel{\sigma_{1}}{\leftrightarrows} a_{0} \cdot\left(b_{0}+b_{1}+b_{2}\right)
\end{array}
$$

- Since $T \oplus \operatorname{Span}\left(\left(a_{0}+a_{1}\right) \cdot b_{1}\right)$ is fixed by $\sigma_{0}$, we can still partition $\overline{g_{3}}$ according to its $\sigma_{0}$-orbits



# Outline of the talk 

- Formulae for polynomial multiplication
- Enumerating formulae
- Further improvements and heuristics
- Some results


## $\mathrm{n} \times$ m-term polynomial multiplication

| Ring | $\mathbf{n} \times \mathbf{m}$ | $\# \mathcal{G}$ | k | \# of tests | \# of solutions | \# of formulae | Calculation time [s] |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $\mathrm{F}_{2}[\mathrm{X}]$ | $2 \times 2$ | 9 | 3 | 1 | 1 | 1 | 0.00 |
|  | $3 \times 3$ | 49 | 6 | 9 | 3 | 9 | 0.00 |
|  | $4 \times 4$ | 225 | 9 | $6.60 \cdot 10^{3}$ | 4 | 4 | 0.03 |
|  | $5 \times 5$ | 961 | 13 | $9.65 \cdot 10^{9}$ | 27 | 27 | $2.28 \cdot 10^{5}$ |
|  | $6 \times 6$ | 3969 | 14 | $4.37 \cdot 10^{9}$ | - | - | $6.03 \cdot 10^{5}$ |
|  |  | (Sym.) 63 | 17 | $8.08 \cdot 10^{6}$ | 6 | 54 | 17.7 |
|  | $7 \times 7$ | (Sym.) 127 | 22 | $3.38 \cdot 10^{12}$ | 2618 | 19550 | $1.59 \cdot 10^{7}$ |
| $\mathrm{F}_{3}[\mathrm{X}]$ | $2 \times 2$ | 16 | 3 | 1 | 1 | 4 | 0.00 |
|  | $3 \times 3$ | 169 | 6 | 24 | 22 | 1493 | 0.00 |
|  | $4 \times 4$ | 1600 | 9 | $4.11 \cdot 10^{5}$ | 726 | 50640 | 14.9 |
|  | $5 \times 5$ | 14641 | 11 | $4.89 \cdot 10^{7}$ | - | - | $4.02 \cdot 10^{4}$ |
|  |  | (Sym.) 121 | 12 | $3.93 \cdot 10^{4}$ | 31 | 6460 | 0.14 |
|  | $6 \times 6$ | (Sym.) 364 | 15 | $2.37 \cdot 10^{8}$ | 4 | 1024 | $3.79 \cdot 10^{3}$ |
|  | $7 \times 7$ | (Sym.) 1093 | 17 | $2.69 \cdot 10^{10}$ | - | - | $1.50 \cdot 10^{6}$ |

## $\mathrm{n} \times$ m-term polynomial multiplication

| Ring | $\mathbf{n} \times \mathbf{m}$ | $\# \mathcal{G}$ | k | \# of tests | \# of solutions | \# of formulae | Calculation time [s] |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $\mathrm{F}_{2}[\mathrm{X}]$ | $2 \times 2$ | 9 | 3 | 1 | 1 | 1 | 0.00 |
|  | $3 \times 3$ | 49 | 6 | 9 | 3 | 9 | 0.00 |
|  | $4 \times 4$ | 225 | 9 | $6.60 \cdot 10^{3}$ | 4 | 4 | 0.03 |
|  | $5 \times 5$ | 961 | 13 | $9.65 \cdot 10^{9}$ | 27 | 27 | $2.28 \cdot 10^{5}$ |
|  | $6 \times 6$ | 3969 | 14 | $4.37 \cdot 10^{9}$ | - | - | $6.03 \cdot 10^{5}$ |
|  |  | (Sym.) 63 | 17 | $8.08 \cdot 10^{6}$ | 6 | 54 | 17.7 |
|  | $7 \times 7$ | (Sym.) 127 | 22 | $3.38 \cdot 10^{12}$ | 2618 | 19550 | $1.59 \cdot 10^{7}$ |
| $\mathrm{F}_{3}[\mathrm{X}]$ | $2 \times 2$ | 16 | 3 | 1 | 1 | 4 | 0.00 |
|  | $3 \times 3$ | 169 | 6 | 24 | 22 | 1493 | 0.00 |
|  | $4 \times 4$ | 1600 | 9 | $4.11 \cdot 10^{5}$ | 726 | 50640 | 14.9 |
|  | $5 \times 5$ | 14641 | 11 | $4.89 \cdot 10^{7}$ | - | - | $4.02 \cdot 10^{4}$ |
|  |  | (Sym.) 121 | 12 | $3.93 \cdot 10^{4}$ | 31 | 6460 | 0.14 |
|  | $6 \times 6$ | (Sym.) 364 | 15 | $2.37 \cdot 10^{8}$ | 4 | 1024 | $3.79 \cdot 10^{3}$ |
|  | $7 \times 7$ | (Sym.) 1093 | 17 | $2.69 \cdot 10^{10}$ | - | - | $1.50 \cdot 10^{6}$ |

## $\mathrm{n} \times$ m-term polynomial multiplication

| Ring | $\mathbf{n} \times \mathbf{m}$ | \#G | k | \# of <br> tests | \# of solutions | \# of formulae | Calculation time [s] |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $\mathrm{F}_{2}[\mathrm{X}]$ | $2 \times 2$ | 9 | 3 | 1 | 1 | 1 | 0.00 |
|  | $3 \times 3$ | 49 | 6 | 9 | 3 | 9 | 0.00 |
|  | $4 \times 4$ | 225 | 9 | $6.60 \cdot 10^{3}$ | 4 | 4 | 0.03 |
|  | $5 \times 5$ | 961 | 13 | $9.65 \cdot 10^{9}$ | 27 | 27 | $2.28 \cdot 10^{5}$ |
|  | $6 \times 6$ | 3969 | 14 | $4.37 \cdot 10^{9}$ | - | - | $6.03 \cdot 10^{5}$ |
|  |  | (Sym.) 63 | 17 | $8.08 \cdot 10^{6}$ | 6 | 54 | 17.7 |
|  | $7 \times 7$ | (Sym.) 127 | 22 | $3.38 \cdot 10^{12}$ | 2618 | 19550 | $1.59 \cdot 10^{7}$ |
| $\mathrm{F}_{3}[\mathrm{X}]$ | $2 \times 2$ | 16 | 3 | 1 | 1 | 4 | 0.00 |
|  | $3 \times 3$ | 169 | 6 | 24 | 22 | 1493 | 0.00 |
|  | $4 \times 4$ | 1600 | 9 | $4.11 \cdot 10^{5}$ | 726 | 50640 | 14.9 |
|  | $5 \times 5$ | 14641 | 11 | $4.89 \cdot 10^{7}$ | - | - | $4.02 \cdot 10^{4}$ |
|  |  | (Sym.) 121 | 12 | $3.93 \cdot 10^{4}$ | 31 | 6460 | 0.14 |
|  | $6 \times 6$ | (Sym.) 364 | 15 | $2.37 \cdot 10^{8}$ | 4 | 1024 | $3.79 \cdot 10^{3}$ |
|  | $7 \times 7$ | (Sym.) 1093 | 17 | $2.69 \cdot 10^{10}$ | - | - | $1.50 \cdot 10^{6}$ |

## $\mathrm{n} \times$ m-term polynomial multiplication

| Ring | $\mathbf{n} \times \mathbf{m}$ | $\# \mathcal{G}$ | k | \# of tests | \# of solutions | \# of formulae | Calculation time [s] |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $\mathrm{F}_{2}[\mathrm{X}]$ | $2 \times 2$ | 9 | 3 | 1 | 1 | 1 | 0.00 |
|  | $3 \times 3$ | 49 | 6 | 9 | 3 | 9 | 0.00 |
|  | $4 \times 4$ | 225 | 9 | $6.60 \cdot 10^{3}$ | 4 | 4 | 0.03 |
|  | $5 \times 5$ | 961 | 13 | $9.65 \cdot 10^{9}$ | 27 | 27 | $2.28 \cdot 10^{5}$ |
|  | $6 \times 6$ | 3969 | 14 | $4.37 \cdot 10^{9}$ | - | - | $6.03 \cdot 10^{5}$ |
|  |  | (Sym.) 63 | 17 | $8.08 \cdot 10^{6}$ | 6 | 54 | 17.7 |
|  | $7 \times 7$ | (Sym.) 127 | 22 | $3.38 \cdot 10^{12}$ | 2618 | 19550 | $1.59 \cdot 10^{7}$ |
| $\mathrm{F}_{3}[\mathrm{X}]$ | $2 \times 2$ | 16 | 3 | 1 | 1 | 4 | 0.00 |
|  | $3 \times 3$ | 169 | 6 | 24 | 22 | 1493 | 0.00 |
|  | $4 \times 4$ | 1600 | 9 | $4.11 \cdot 10^{5}$ | 726 | 50640 | 14.9 |
|  | $5 \times 5$ | 14641 | 11 | $4.89 \cdot 10^{7}$ | - | - | $4.02 \cdot 10^{4}$ |
|  |  | (Sym.) 121 | 12 | $3.93 \cdot 10^{4}$ | 31 | 6460 | 0.14 |
|  | $6 \times 6$ | (Sym.) 364 | 15 | $2.37 \cdot 10^{8}$ | 4 | 1024 | $3.79 \cdot 10^{3}$ |
|  | $7 \times 7$ | (Sym.) 1093 | 17 | $2.69 \cdot 10^{10}$ | - | - | $1.50 \cdot 10^{6}$ |

## $\mathrm{n} \times$ m-term polynomial multiplication

| Ring | $\mathbf{n} \times \mathbf{m}$ | $\# \mathcal{G}$ | k | \# of tests | \# of solutions | \# of formulae | Calculation time [s] |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $\mathrm{F}_{2}[\mathrm{X}]$ | $2 \times 2$ | 9 | 3 | 1 | 1 | 1 | 0.00 |
|  | $3 \times 3$ | 49 | 6 | 9 | 3 | 9 | 0.00 |
|  | $4 \times 4$ | 225 | 9 | $6.60 \cdot 10^{3}$ | 4 | 4 | 0.03 |
|  | $5 \times 5$ | 961 | 13 | $9.65 \cdot 10^{9}$ | 27 | 27 | $2.28 \cdot 10^{5}$ |
|  | $6 \times 6$ | 3969 | 14 | $4.37 \cdot 10^{9}$ | - | - | $6.03 \cdot 10^{5}$ |
|  |  | (Sym.) 63 | 17 | $8.08 \cdot 10^{6}$ | 6 | 54 | 17.7 |
|  | $7 \times 7$ | (Sym.) 127 | 22 | $3.38 \cdot 10^{12}$ | 2618 | 19550 | $1.59 \cdot 10^{7}$ |
| $\mathrm{F}_{3}[\mathrm{X}]$ | $2 \times 2$ | 16 | 3 | 1 | 1 | 4 | 0.00 |
|  | $3 \times 3$ | 169 | 6 | 24 | 22 | 1493 | 0.00 |
|  | $4 \times 4$ | 1600 | 9 | $4.11 \cdot 10^{5}$ | 726 | 50640 | 14.9 |
|  | $5 \times 5$ | 14641 | 11 | $4.89 \cdot 10^{7}$ | - | - | $4.02 \cdot 10^{4}$ |
|  |  | (Sym.) 121 | 12 | $3.93 \cdot 10^{4}$ | 31 | 6460 | 0.14 |
|  | $6 \times 6$ | (Sym.) 364 | 15 | $2.37 \cdot 10^{8}$ | 4 | 1024 | $3.79 \cdot 10^{3}$ |
|  | $7 \times 7$ | (Sym.) 1093 | 17 | $2.69 \cdot 10^{10}$ | - | - | $1.50 \cdot 10^{6}$ |

## $\mathrm{n} \times$ m-term polynomial multiplication

| Ring | $\mathbf{n} \times \mathbf{m}$ | $\# \mathcal{G}$ | k | \# of tests | \# of solutions | \# of formulae | Calculation time [s] |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $\mathrm{F}_{2}[\mathrm{X}]$ | $2 \times 2$ | 9 | 3 | 1 | 1 | 1 | 0.00 |
|  | $3 \times 3$ | 49 | 6 | 9 | 3 | 9 | 0.00 |
|  | $4 \times 4$ | 225 | 9 | $6.60 \cdot 10^{3}$ | 4 | 4 | 0.03 |
|  | $5 \times 5$ | 961 | 13 | $9.65 \cdot 10^{9}$ | 27 | 27 | $2.28 \cdot 10^{5}$ |
|  | $6 \times 6$ | 3969 | 14 | $4.37 \cdot 10^{9}$ | - | - | $6.03 \cdot 10^{5}$ |
|  |  | (Sym.) 63 | 17 | $8.08 \cdot 10^{6}$ | 6 | 54 | 17.7 |
|  | $7 \times 7$ | (Sym.) 127 | 22 | $3.38 \cdot 10^{12}$ | 2618 | 19550 | $1.59 \cdot 10^{7}$ |
| $\mathrm{F}_{3}[\mathrm{X}]$ | $2 \times 2$ | 16 | 3 | 1 | 1 | 4 | 0.00 |
|  | $3 \times 3$ | 169 | 6 | 24 | 22 | 1493 | 0.00 |
|  | $4 \times 4$ | 1600 | 9 | $4.11 \cdot 10^{5}$ | 726 | 50640 | 14.9 |
|  | $5 \times 5$ | 14641 | 11 | $4.89 \cdot 10^{7}$ | - | - | $4.02 \cdot 10^{4}$ |
|  |  | (Sym.) 121 | 12 | $3.93 \cdot 10^{4}$ | 31 | 6460 | 0.14 |
|  | $6 \times 6$ | (Sym.) 364 | 15 | $2.37 \cdot 10^{8}$ | 4 | 1024 | $3.79 \cdot 10^{3}$ |
|  | $7 \times 7$ | (Sym.) 1093 | 17 | $2.69 \cdot 10^{10}$ | - | - | $1.50 \cdot 10^{6}$ |

## Multiplication in small finite-field extensions

| Finite field | \#G | k | \# of <br> tests | \# of solutions | \# of formulae | Calculation time [s] |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $\mathrm{F}_{2^{2}}$ | 9 | 3 | 3 | 3 | 3 | 0.00 |
| $F_{2^{3}}$ | 49 | 6 | $7.03 \cdot 10^{3}$ | 105 | 147 | 0.01 |
| $\mathrm{F}_{2^{4}}$ | 225 | 9 | $2.57 \cdot 10^{9}$ | 2025 | 2025 | $1.13 \cdot 10^{4}$ |
| $\mathrm{F}^{5}$ | 961 | 9 | $3.10 \cdot 10^{10}$ | - | - | $8.11 \cdot 10^{5}$ |
|  | (Sym.) 31 | 13 | $3.49 \cdot 10^{6}$ | 2015 | 2015 | 6.24 |
| $\mathrm{F}_{2}{ }^{6}$ | (Sym.) 63 | 15 | $2.21 \cdot 10^{10}$ | 21 | 21 | $6.63 \cdot 10^{4}$ |
| $F_{2^{7}}$ | (Sym.) 127 | 15 | $1.34 \cdot 10^{12}$ | - | - | $6.17 \cdot 10^{6}$ |
| $F^{3}$ | 16 | 3 | 3 | 4 | 16 | 0.00 |
| $F_{3^{3}}$ | 169 | 6 | $2.42 \cdot 10^{5}$ | 11843 | 105963 | 1.08 |
| $\mathrm{F}_{3}{ }^{4}$ | 1600 | 8 | $2.27 \cdot 10^{11}$ | - | - | $1.08 \cdot 10^{7}$ |
|  | (Sym.) 40 | 9 | $1.10 \cdot 10^{5}$ | 234 | 615240 | 0.45 |
| $\mathrm{F}_{3}{ }^{5}$ | (Sym.) 121 | 11 | $2.66 \cdot 10^{9}$ | 121 | 121 | $1.45 \cdot 10^{4}$ |
| $F^{36}$ | (Sym.) 364 | 12 | $3.01 \cdot 10^{12}$ | - | - | $4.50 \cdot 10^{7}$ |

## Multiplication in small finite-field extensions

| Finite field | \#G | k | \# of <br> tests | \# of solutions | \# of formulae | Calculation time [s] |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $\mathrm{F}_{2^{2}}$ | 9 | 3 | 3 | 3 | 3 | 0.00 |
| $F_{2^{3}}$ | 49 | 6 | $7.03 \cdot 10^{3}$ | 105 | 147 | 0.01 |
| $\mathrm{F}_{2^{4}}$ | 225 | 9 | $2.57 \cdot 10^{9}$ | 2025 | 2025 | $1.13 \cdot 10^{4}$ |
| $\mathrm{F}^{5}$ | 961 | 9 | $3.10 \cdot 10^{10}$ | - | - | $8.11 \cdot 10^{5}$ |
|  | (Sym.) 31 | 13 | $3.49 \cdot 10^{6}$ | 2015 | 2015 | 6.24 |
| $\mathrm{F}_{2}{ }^{6}$ | (Sym.) 63 | 15 | $2.21 \cdot 10^{10}$ | 21 | 21 | $6.63 \cdot 10^{4}$ |
| $F_{2^{7}}$ | (Sym.) 127 | 15 | $1.34 \cdot 10^{12}$ | - | - | $6.17 \cdot 10^{6}$ |
| $F^{3}$ | 16 | 3 | 3 | 4 | 16 | 0.00 |
| $F_{3^{3}}$ | 169 | 6 | $2.42 \cdot 10^{5}$ | 11843 | 105963 | 1.08 |
| $F^{3}$ | 1600 | 8 | $2.27 \cdot 10^{11}$ | - | - | $1.08 \cdot 10^{7}$ |
|  | (Sym.) 40 | 9 | $1.10 \cdot 10^{5}$ | 234 | 615240 | 0.45 |
| $\mathrm{F}_{35}$ | (Sym.) 121 | 11 | $2.66 \cdot 10^{9}$ | 121 | 121 | $1.45 \cdot 10^{4}$ |
| $F_{36}$ | (Sym.) 364 | 12 | $3.01 \cdot 10^{12}$ | - | - | $4.50 \cdot 10^{7}$ |

## Conclusion

- General algorithm
- Method that proves lower bounds on the number of subproducts


## Conclusion

- General algorithm
- Method that proves lower bounds on the number of subproducts
- Gives all formulae
- Provides new formulae that cannot be found with previous methods
- We can cherry-pick the one with minimum number of additions and scalar multiplications


## Conclusion

- General algorithm
- Method that proves lower bounds on the number of subproducts
- Gives all formulae
- Provides new formulae that cannot be found with previous methods
- We can cherry-pick the one with minimum number of additions and scalar multiplications
- Work in progress and perspectives
- Lifting formulae for higher-characteristic or characteristic-0 fields
- Find formulae for your bilinear application!


# Thank you for your attention 

## Questions?

## Representing elements

- Finite field $K$ :
- elements represented using $\log _{2} \# K$ bits
- small fields $\Rightarrow$ fits within a word, within a uint8_t (1 byte)


## Representing elements

- Finite field $K$ :
- elements represented using $\log _{2} \# K$ bits
- small fields $\Rightarrow$ fits within a word, within a uint8_t (1 byte)
- $V$ : $N$-dimensional $K$-vector space
- elements represented using $\log _{2} \# K$ vectors of $N$ bits (bitsliced representation)


## Representing elements

- Finite field $K$ :
- elements represented using $\log _{2} \# K$ bits
- small fields $\Rightarrow$ fits within a word, within a uint8_t (1 byte)
- $V$ : $N$-dimensional $K$-vector space
- elements represented using $\log _{2} \# K$ vectors of $N$ bits (bitsliced representation)
- for instance, for the $2 \times 3$-term polynomial multiplication over $\mathbb{F}_{3}[X]$ :

$$
v=a_{0} b_{1}-a_{1} b_{0}+a_{1} b_{2}
$$

## Representing elements

- Finite field $K$ :
- elements represented using $\log _{2} \# K$ bits
- small fields $\Rightarrow$ fits within a word, within a uint8_t (1 byte)
- $V$ : $N$-dimensional $K$-vector space
- elements represented using $\log _{2} \# K$ vectors of $N$ bits (bitsliced representation)
- for instance, for the $2 \times 3$-term polynomial multiplication over $\mathbb{F}_{3}[X]$ :

$$
\begin{aligned}
& v=a_{0} b_{1}-a_{1} b_{0}+a_{1} b_{2} \\
& a_{0} b_{0} a_{0} b_{1} a_{0} b_{2} a_{1} b_{0} a_{1} b_{1} a_{1} b_{2} \\
& =\quad(0,1,0,-1,0,1)
\end{aligned}
$$

## Representing elements

- Finite field $K$ :
- elements represented using $\log _{2} \# K$ bits
- small fields $\Rightarrow$ fits within a word, within a uint8_t (1 byte)
- $V$ : $N$-dimensional $K$-vector space
- elements represented using $\log _{2} \# K$ vectors of $N$ bits (bitsliced representation)
- for instance, for the $2 \times 3$-term polynomial multiplication over $\mathbb{F}_{3}[X]$ :

$$
\begin{aligned}
v & =a_{0} b_{1}-a_{1} b_{0}+a_{1} b_{2} \\
& =\quad\left(\begin{array}{lllllll}
0, & 1, & 0, & 2, & 0, & 1
\end{array}\right)
\end{aligned}
$$

## Representing elements

- Finite field $K$ :
- elements represented using $\log _{2} \# K$ bits
- small fields $\Rightarrow$ fits within a word, within a uint8_t (1 byte)
- $V$ : $N$-dimensional $K$-vector space
- elements represented using $\log _{2} \# K$ vectors of $N$ bits (bitsliced representation)
- for instance, for the $2 \times 3$-term polynomial multiplication over $\mathbb{F}_{3}[X]$ :

$$
\begin{aligned}
& v=a_{0} b_{1}-a_{1} b_{0}+a_{1} b_{2} \\
& a_{0} b_{0} \quad a_{0} b_{1} a_{0} b_{2} a_{1} b_{0} a_{1} b_{1} a_{1} b_{2} \\
& =\quad(0,1,0,2,0,1) \\
& =(0,1,0,0,0,1)+ \\
& 2 \cdot(0,0,0,1,0,0)
\end{aligned}
$$

## Representing elements

- Finite field $K$ :
- elements represented using $\log _{2} \# K$ bits
- small fields $\Rightarrow$ fits within a word, within a uint8_t (1 byte)
- $V$ : $N$-dimensional $K$-vector space
- elements represented using $\log _{2} \# K$ vectors of $N$ bits (bitsliced representation)
- for instance, for the $2 \times 3$-term polynomial multiplication over $\mathbb{F}_{3}[X]$ :

$$
\left.\left.\begin{array}{rl}
v= & a_{0} b_{1}-a_{1} b_{0}+a_{1} b_{2} \\
= & \left.\begin{array}{llllll}
a_{0} b_{0} & a_{0} b_{1} & a_{0} b_{2} & a_{1} b_{0} & a_{1} b_{1} a_{1} b_{2} \\
0, & 1, & 0, & 2, & 0, & 1
\end{array}\right) \\
= & \left(\begin{array}{lllll}
0, & 1, & 0, & 0, & 0,
\end{array} 1\right.
\end{array}\right)+\right\}
$$

## Representing elements

- Finite field $K$ :
- elements represented using $\log _{2} \# K$ bits
- small fields $\Rightarrow$ fits within a word, within a uint8_t (1 byte)
- V: $N$-dimensional $K$-vector space
- elements represented using $\log _{2} \# K$ vectors of $N$ bits (bitsliced representation)
- for instance, for the $2 \times 3$-term polynomial multiplication over $\mathbb{F}_{3}[X]$ :

$$
\begin{aligned}
& v=a_{0} b_{1}-a_{1} b_{0}+a_{1} b_{2} \\
& a_{0} b_{0} \quad a_{0} b_{1} a_{0} b_{2} a_{1} b_{0} a_{1} b_{1} a_{1} b_{2} \\
& =\quad(0,1,0,2,0,1) \\
& =(0,1,0,0,0,1)+ \\
& 2 \cdot(0,0,0,1,0,0) \\
& \text { uint } N_{-} \mathrm{t} v[2]=\{0 \mathrm{x} 22 \mathrm{u}, 0 \mathrm{x} 08 \mathrm{u}\} \text {; }
\end{aligned}
$$

- coefficient-wise add, sub, mul, etc. using bitwise operations on $N$-bit words


## Representing elements

- Finite field $K$ :
- elements represented using $\log _{2} \# K$ bits
- small fields $\Rightarrow$ fits within a word, within a uint8_t (1 byte)
- V: $N$-dimensional $K$-vector space
- elements represented using $\log _{2} \# K$ vectors of $N$ bits (bitsliced representation)
- for instance, for the $2 \times 3$-term polynomial multiplication over $\mathbb{F}_{3}[X]$ :

$$
\operatorname{uint} N_{-} \mathrm{t} \mathrm{v}[2]=\{0 \mathrm{x} 22 \mathrm{u}, 0 \mathrm{x} 08 \mathrm{u}\} ;
$$

- coefficient-wise add, sub, mul, etc. using bitwise operations on $N$-bit words e.g., addition $w \leftarrow u+v$ with $K=\mathbb{F}_{3}$ :

$$
\begin{aligned}
& w[0]=(u[0] \mid v[0]) \sim((u[0] \mid u[1]) \&(v[0] \mid v[1])) ; \\
& w[1]=(u[1] \mid v[1]) \sim((u[0] \mid u[1]) \&(v[0] \mid v[1])) ;
\end{aligned}
$$

$$
\begin{aligned}
& v=a_{0} b_{1}-a_{1} b_{0}+a_{1} b_{2} \\
& a_{0} b_{0} \quad a_{0} b_{1} a_{0} b_{2} a_{1} b_{0} a_{1} b_{1} a_{1} b_{2} \\
& =\quad(0,1,0,2,0,1) \\
& =(0,1,0,0,0,1)+ \\
& 2 \cdot(0,0,0,1,0,0)
\end{aligned}
$$

## Representing elements

- Finite field $K$ :
- elements represented using $\log _{2} \# K$ bits
- small fields $\Rightarrow$ fits within a word, within a uint8_t (1 byte)
- V: $N$-dimensional $K$-vector space
- elements represented using $\log _{2} \# K$ vectors of $N$ bits (bitsliced representation)
- for instance, for the $2 \times 3$-term polynomial multiplication over $\mathbb{F}_{3}[X]$ :

$$
\begin{aligned}
v & =a_{0} b_{1}-a_{1} b_{0}+a_{1} b_{2} \\
& \left.=\quad \begin{array}{llllll}
a_{0} b_{0} & a_{0} b_{1} & a_{0} b_{2} & a_{1} b_{0} & a_{1} b_{1} & a_{1} b_{2} \\
0, & 1, & 0, & 2, & 0, & 1
\end{array}\right) \\
& = \\
& 2 \cdot\left(\begin{array}{llllll}
0, & 1, & 0, & 0, & 0, & 1
\end{array}\right)+
\end{aligned}
$$

$$
\operatorname{uint} N_{-} \mathrm{t} v[2]=\{0 \mathrm{x} 22 \mathrm{u}, 0 \mathrm{x} 08 \mathrm{u}\} ;
$$

- coefficient-wise add, sub, mul, etc. using bitwise operations on $N$-bit words e.g., addition $w \leftarrow u+v$ with $K=\mathbb{F}_{3}$ :

$$
\begin{aligned}
& \mathrm{w}[0]=(u[0] \mid v[0]) \sim((u[0] \mid u[1]) \&(v[0] \mid v[1])) ; \\
& w[1]=(u[1] \mid v[1]) \sim((u[0] \mid u[1]) \&(v[0] \mid v[1])) ;
\end{aligned}
$$

- machine-specific bound on $N: \leq 64, \leq 128$ (SSE2), or $\leq 256$ (AVX)


## Representing subspaces

- Subspaces $W \subset V$ represented using matrices in row echelon form

where each pivot $w_{i, j_{i}} \neq 0$, and with $j_{1}<j_{2}<\cdots<j_{r}$


## Representing subspaces

- Subspaces $W \subset V$ represented using matrices in row echelon form

where each pivot $w_{i, j_{i}} \neq 0$, and with $j_{1}<j_{2}<\cdots<j_{r}$
- Actual representation: since $\operatorname{dim} W \leq \operatorname{dim} V$, force the matrix $W$ to $N$ rows
- rows corresponding to pivot $w_{i, j_{i}}$ placed at row $j_{i}$
- other rows set to zero


## Representing subspaces

- Subspaces $W \subset V$ represented using matrices in row echelon form

where each pivot $w_{i, j_{i}} \neq 0$, and with $j_{1}<j_{2}<\cdots<j_{r}$
- Actual representation: since $\operatorname{dim} W \leq \operatorname{dim} V$, force the matrix $W$ to $N$ rows
- rows corresponding to pivot $w_{i, j_{i}}$ placed at row $j_{i}$
- other rows set to zero


## Representing subspaces

- Subspaces $W \subset V$ represented using matrices in row echelon form

where each pivot $w_{i, j_{i}} \neq 0$, and with $j_{1}<j_{2}<\cdots<j_{r}$
- Actual representation: since $\operatorname{dim} W \leq \operatorname{dim} V$, force the matrix $W$ to $N$ rows
- rows corresponding to pivot $w_{i, j_{i}}$ placed at row $j_{i}$
- other rows set to zero
- all pivots now lie on the diagonal


## Representing subspaces

- Subspaces $W \subset V$ represented using matrices in row echelon form

where each pivot $w_{i, j_{i}} \neq 0$, and with $j_{1}<j_{2}<\cdots<j_{r}$
- Actual representation: since $\operatorname{dim} W \leq \operatorname{dim} V$, force the matrix $W$ to $N$ rows
- rows corresponding to pivot $w_{i, j_{i}}$ placed at row $j_{i}$
- other rows set to zero
- all pivots now lie on the diagonal
(2) waste of memory
() easier to insert extra rows when expanding $W$


## Reduction by a subspace

- Given a vector $v \in V$ and a subspace $W$ :
- sequentially cancel the contribution of pivot rows of $W$ to $v$
- stop when no pivot corresponds to the leading coefficient of $v$


## Reduction by a subspace

- Given a vector $v \in V$ and a subspace $W$ :
- sequentially cancel the contribution of pivot rows of $W$ to $v$
- stop when no pivot corresponds to the leading coefficient of $v$

```
for \(i \leftarrow 1\) to \(N\) do
    if \(v=0\) then return 0
    if \(v_{i} \neq 0\) then
        if \(w_{i, i} \neq 0\) then \(v \leftarrow v-\left(v_{i} / w_{i, i}\right) w_{i}\)
                        else return \(v\)
    end for
```


## Reduction by a subspace

- Given a vector $v \in V$ and a subspace $W$ :
- sequentially cancel the contribution of pivot rows of $W$ to $v$
- stop when no pivot corresponds to the leading coefficient of $v$

```
for \(i \leftarrow 1\) to \(N\) do
    if \(v=0\) then return 0
    if \(v_{i} \neq 0\) then
        if \(w_{i, i} \neq 0\) then \(v \leftarrow v-\left(v_{i} / w_{i, i}\right) w_{i}\)
                        else return \(v\)
    end for
```

- Test if $v \in W$ :
- $v \in W$ if and only if reduce $(v, W)=0$


## Reduction by a subspace

- Given a vector $v \in V$ and a subspace $W$ :
- sequentially cancel the contribution of pivot rows of $W$ to $v$
- stop when no pivot corresponds to the leading coefficient of $v$

```
for }i\leftarrow1\mathrm{ to }N\mathrm{ do
    if v}=0\mathrm{ then return 0
    if }\mp@subsup{v}{i}{}\not=0\mathrm{ then
        if w
                        else return v
    end for
```

- Test if $v \in W$ :
- $v \in W$ if and only if reduce $(v, W)=0$
- Construct $W \oplus \operatorname{Span}(g)$, for $g \in \mathcal{G} \backslash W$ :
- compute $\tilde{g} \leftarrow$ reduce $(g, W)$
- let $i$ be the iteration at which the algorithm returns $\tilde{g}(\neq 0)$
- then $w_{i} \leftarrow \tilde{g}$


## Reduction by a subspace

- Given a vector $v \in V$ and a subspace $W$ :
- sequentially cancel the contribution of pivot rows of $W$ to $v$
- stop when no pivot corresponds to the leading coefficient of $v$

```
for }i\leftarrow1\mathrm{ to }N\mathrm{ do
    if v}=0\mathrm{ then return 0
    if }\mp@subsup{v}{i}{}\not=0\mathrm{ then
        if w
                        else return v
    end for
```

- Test if $v \in W$ :
- $v \in W$ if and only if reduce $(v, W)=0$
- Construct $W \oplus \operatorname{Span}(g)$, for $g \in \mathcal{G} \backslash W$ :
- compute $\tilde{g} \leftarrow$ reduce $(g, W)$
- let $i$ be the iteration at which the algorithm returns $\tilde{g}(\neq 0)$
- then $w_{i} \leftarrow \tilde{g}$
- Improvement: since $W$ is constructed incrementally
- keep the vectors of $\mathcal{G}$ reduced by $W$ at all times
- when expanding $W$ by $\operatorname{Span}(g)$, reduce $\mathcal{G}$ by $g$ only


## Computing $\mathrm{W} \cap \mathcal{G}$

- Find all $g \in \mathcal{G}$ such that $g \in W$


## Computing $\mathbf{W} \cap \mathcal{G}$

- Find all $g \in \mathcal{G}$ such that $g \in W$
- For each $g \in \mathcal{G}$, test if reduce $(g, W)=0$ ?
- slow (only one vector at a time, lots of conditional branches, etc.)
- we don't need to reduce $g$ by $W$


## Computing $\mathrm{W} \cap \mathcal{G}$

- Find all $g \in \mathcal{G}$ such that $g \in W$
- For each $g \in \mathcal{G}$, test if reduce $(g, W)=0$ ?
- slow (only one vector at a time, lots of conditional branches, etc.)
- we don't need to reduce $g$ by $W$
- Idea (courtesy of $E$. Thomé): put matrix $W$ in reduced row echelon form



## Computing $\mathrm{W} \cap \mathcal{G}$

- Find all $g \in \mathcal{G}$ such that $g \in W$
- For each $g \in \mathcal{G}$, test if reduce $(g, W)=0$ ?
- slow (only one vector at a time, lots of conditional branches, etc.)
- we don't need to reduce $g$ by W
- Idea (courtesy of E . Thomé): put matrix $W$ in reduced row echelon form



## Computing $\mathrm{W} \cap \mathcal{G}$

- Find all $g \in \mathcal{G}$ such that $g \in W$
- For each $g \in \mathcal{G}$, test if reduce $(g, W)=0$ ?
- slow (only one vector at a time, lots of conditional branches, etc.)
- we don't need to reduce $g$ by $W$
- Idea (courtesy of $E$. Thomé): put matrix $W$ in reduced row echelon form



## Computing $\mathrm{W} \cap \mathcal{G}$

- Find all $g \in \mathcal{G}$ such that $g \in W$
- For each $g \in \mathcal{G}$, test if reduce $(g, W)=0$ ?
- slow (only one vector at a time, lots of conditional branches, etc.)
- we don't need to reduce $g$ by $W$
- Idea (courtesy of $E$. Thomé): put matrix $W$ in reduced row echelon form

- all pivot columns $j_{i}$ to 0 , except for $w_{j_{i}, j_{i}}=1$


## Computing $\mathrm{W} \cap \mathcal{G}$

- Find all $g \in \mathcal{G}$ such that $g \in W$
- For each $g \in \mathcal{G}$, test if reduce $(g, W)=0$ ?
- slow (only one vector at a time, lots of conditional branches, etc.)
- we don't need to reduce $g$ by $W$
- Idea (courtesy of E . Thomé): put matrix $W$ in reduced row echelon form

- all pivot columns $j_{i}$ to 0 , except for $w_{j_{i}, j_{i}}=1$
- $g \in W$ if and only if $g^{\top} \cdot W^{\prime}=g$


## Computing $\mathrm{W} \cap \mathcal{G}$

- Find all $g \in \mathcal{G}$ such that $g \in W$
- For each $g \in \mathcal{G}$, test if reduce $(g, W)=0$ ?
- slow (only one vector at a time, lots of conditional branches, etc.)
- we don't need to reduce $g$ by $W$
- Idea (courtesy of E . Thomé): put matrix $W$ in reduced row echelon form

- all pivot columns $j_{i}$ to 0 , except for $w_{j_{i}, j_{i}}=1$
- $g \in W$ if and only if $g^{\top} \cdot W^{\prime}=g$
- batch 64,128 , or 256 products $g^{\top} \cdot\left(W^{\prime}-I d\right)$

