Efficient Computation of Order Bases

Wei Zhou, George Labahn

Symbolic Computation Group
University of Waterloo

ISSAC 2009

The Problem

$\mathbb{K}$ a field. Given $\mathbf{F} \in \mathbb{K}[[x]]^{m \times n}$, $m \leq n$. $\sigma \in \mathbb{Z}_{\geq 0}$.

- Consider polynomial vectors $\mathbf{q}$ satisfying $\mathbf{F}\mathbf{q} \equiv 0 \mod x^{\sigma}$
- Infinite such vectors, generated by a basis formed by the columns of a square nonsingular matrix $\mathbf{P}$.
- Want to find a *minimal* such basis. Denote it $(\mathbf{F}, \sigma)$-basis.

Example:

$\mathbb{K} = \mathbb{Z}_2$.

$\mathbf{F} = [1 + x + x^3 + x^7 + \cdots, 1 + x + x^2 + x^3 + x^4 + x^5 + x^7 + \cdots]$.

$\sigma = 7$.

$$\mathbf{P} = [\mathbf{p}_1, \mathbf{p}_2] = \begin{bmatrix} x + x^3 + x^4 & 1 + x + x^3 \\ x & 1 + x + x^2 + x^3 \end{bmatrix}.$$

The Problem

$\mathbb{K}$ a field. Given $\mathbf{F} \in \mathbb{K}[[x]]^{m \times n}$, $m \leq n$. $\sigma \in \mathbb{Z}_{\geq 0}$.

- Consider polynomial vectors $\mathbf{q}$ satisfying $\mathbf{F}\mathbf{q} \equiv 0 \mod x^{\sigma}$.
- Infinite such vectors, generated by a basis formed by the columns of a square nonsingular matrix $\mathbf{P}$.
- Want to find a *minimal* such basis. Denote it $(\mathbf{F}, \sigma)$-basis.

Example:

$\mathbb{K} = \mathbb{Z}_2$.

$\mathbf{F} = [1 + x + x^3 + x^7 + \cdots, 1 + x + x^2 + x^3 + x^4 + x^5 + x^7 + \cdots]$.

$\sigma = 7$.

$$\mathbf{P} = [\mathbf{p}_1, \mathbf{p}_2] = \begin{bmatrix} x + x^3 + x^4 & 1 + x + x^3 \\ x & 1 + x + x^2 + x^3 \end{bmatrix}.$$

The Problem

$\mathbb{K}$ a field. Given $\mathbf{F} \in \mathbb{K}[[x]]^{m \times n}$, $m \leq n$. $\sigma \in \mathbb{Z}_{\geq 0}$.

- Consider polynomial vectors $\mathbf{q}$ satisfying $\mathbf{F}\mathbf{q} \equiv 0 \mod x^{\sigma}$.
- Infinite such vectors, generated by a basis formed by the columns of a square nonsingular matrix $\mathbf{P}$.
- Want to find a minimal such basis. Denote it $(\mathbf{F}, \sigma)$-basis.

Example:
$\mathbb{K} = \mathbb{Z}_2$.
$\mathbf{F} = [1 + x + x^3 + x^7 + \cdots, 1 + x + x^2 + x^3 + x^4 + x^5 + x^7 + \cdots]$.
$\sigma = 7$.

$$\mathbf{P} = [\mathbf{p}_1, \mathbf{p}_2] = \begin{bmatrix} x + x^3 + x^4 & 1 + x + x^3 \\ x & 1 + x + x^2 + x^3 \end{bmatrix}.$$

The Problem

$\mathbb{K}$ a field. Given $\mathbf{F} \in \mathbb{K}[[x]]^{m \times n}$, $m \leq n$. $\sigma \in \mathbb{Z}_{\geq 0}$.

- Consider polynomial vectors $\mathbf{q}$ satisfying $\mathbf{Fq} \equiv 0 \mod x^{\sigma}$.
- Infinite such vectors, generated by a basis formed by the columns of a square nonsingular matrix $\mathbf{P}$.
- Want to find a minimal such basis. Denote it $(\mathbf{F}, \sigma)$-basis.

Example:
$\mathbb{K} = \mathbb{Z}_2$.
$\mathbf{F} = [1 + x + x^3 + x^7 + \cdots, 1 + x + x^2 + x^3 + x^4 + x^5 + x^7 + \cdots]$.
$\sigma = 7$.

$$\mathbf{F} \begin{bmatrix} 1 + x + x^6 \\ 1 + x + x^2 + x^5 \end{bmatrix} = \begin{bmatrix} x^7 + x^{10} + x^{11} + x^{13} + \cdots \end{bmatrix}.$$

$$\mathbf{P} = [\mathbf{p}_1, \mathbf{p}_2] = \begin{bmatrix} x + x^3 + x^4 & 1 + x + x^3 \\ x & 1 + x + x^2 + x^3 \end{bmatrix}.$$

The Problem

$\mathbb{K}$ a field. Given $\mathbf{F} \in \mathbb{K}[[x]]^{m \times n}$, $m \leq n$. $\sigma \in \mathbb{Z}_{\geq 0}$.

- Consider polynomial vectors $\mathbf{q}$ satisfying $\mathbf{Fq} \equiv 0 \mod x^{\sigma}$.
- Infinite such vectors, generated by a basis formed by the columns of a square nonsingular matrix $\mathbf{P}$.
- Want to find a minimal such basis. Denote it $(\mathbf{F}, \sigma)$-basis.

Example:
$\mathbb{K} = \mathbb{Z}_2$.
$\mathbf{F} = [1 + x + x^3 + x^7 + \cdots, 1 + x + x^2 + x^3 + x^4 + x^5 + x^7 + \cdots]$.
$\sigma = 7$.

$$\mathbf{F} \begin{bmatrix} x^2 + x^3 \\ x^2 + x^3 + x^4 \end{bmatrix} = \begin{bmatrix} x^7 + x^9 + x^{10} + x^{13} + \cdots \end{bmatrix}.$$

$$\mathbf{P} = [\mathbf{p}_1, \mathbf{p}_2] = \begin{bmatrix} x + x^3 + x^4 & 1 + x + x^3 \\ x & 1 + x + x^2 + x^3 \end{bmatrix}.$$

The Problem

$\mathbb{K}$ a field. Given $\mathbf{F} \in \mathbb{K}[[x]]^{m \times n}$, $m \leq n$. $\sigma \in \mathbb{Z}_{\geq 0}$.

- Consider polynomial vectors $\mathbf{q}$ satisfying $\mathbf{F}\mathbf{q} \equiv 0 \mod x^{\sigma}$.
- Infinite such vectors, generated by a basis formed by the columns of a square nonsingular matrix $\mathbf{P}$.
- Want to find a minimal such basis. Denote it $(\mathbf{F}, \sigma)$-basis.

Example:

$\mathbb{K} = \mathbb{Z}_2$.

$\mathbf{F} = [1 + x + x^3 + x^7 + \cdots, 1 + x + x^2 + x^3 + x^4 + x^5 + x^7 + \cdots]$.

$\sigma = 7$.

$$\mathbf{F} \begin{bmatrix} x^2 + x^3 \\ x^2 + x^3 + x^4 \end{bmatrix} = \begin{bmatrix} x^7 + x^9 + x^{10} + x^{13} & + \cdots \end{bmatrix}.$$

$$\mathbf{P} = [\mathbf{p}_1, \mathbf{p}_2] = \begin{bmatrix} x + x^3 + x^4 & 1 + x + x^3 \\ x & 1 + x + x^2 + x^3 \end{bmatrix}.$$

The Problem

$\mathbb{K}$ a field. Given $\mathbf{F} \in \mathbb{K}[[x]]^{m \times n}$, $m \leq n$. $\sigma \in \mathbb{Z}_{\geq 0}$.

- Consider polynomial vectors $\mathbf{q}$ satisfying $\mathbf{F}\mathbf{q} \equiv 0 \mod x^{\sigma}$.
- Infinite such vectors, generated by a basis formed by the columns of a square nonsingular matrix $\mathbf{P}$.
- Want to find a minimal such basis. Denote it $(\mathbf{F}, \sigma)$-basis.

Example:
$\mathbb{K} = \mathbb{Z}_2$.
$\mathbf{F} = [1 + x + x^3 + x^7 + \cdots, 1 + x + x^2 + x^3 + x^4 + x^5 + x^7 + \cdots]$.
$\sigma = 7$.

$$\mathbf{F} \begin{bmatrix} x^2 + x^3 \\ x^2 + x^3 + x^4 \end{bmatrix} = \mathbf{F}\mathbf{P} \begin{bmatrix} 1 \\ x \end{bmatrix} = \mathbf{F}(\mathbf{p}_1 + \mathbf{p}_2 x) \equiv 0 \mod x^7.$$

$$\mathbf{P} = [\mathbf{p}_1, \mathbf{p}_2] = \begin{bmatrix} x + x^3 + x^4 & 1 + x + x^3 \\ x & 1 + x + x^2 + x^3 \end{bmatrix}.$$

The Problem

$\mathbb{K}$ a field. Given $\mathbf{F} \in \mathbb{K}[[x]]^{m \times n}$, $m \leq n$. $\sigma \in \mathbb{Z}_{\geq 0}$.

- Consider polynomial vectors $\mathbf{q}$ satisfying $\mathbf{F}\mathbf{q} \equiv 0 \mod x^{\sigma}$.
- Infinite such vectors, generated by a basis formed by the columns of a square nonsingular matrix $\mathbf{P}$.
- Want to find a minimal such basis. Denote it $(\mathbf{F}, \sigma)$-basis.

Example:
$\mathbb{K} = \mathbb{Z}_2$.
$\mathbf{F} = [1 + x + x^3 + x^7 + \cdots, 1 + x + x^2 + x^3 + x^4 + x^5 + x^7 + \cdots]$.
$\sigma = 7$.

$$\mathbf{F} \begin{bmatrix} x^2 + x^3 \\ x^2 + x^3 + x^4 \end{bmatrix} = \mathbf{F}\mathbf{P} \begin{bmatrix} 1 \\ x \end{bmatrix} = \mathbf{F}(\mathbf{p}_1 + \mathbf{p}_2 x) \equiv 0 \mod x^7.$$

$$\mathbf{P} = [\mathbf{p}_1, \mathbf{p}_2] = \begin{bmatrix} x + x^3 + x^4 & 1 + x + x^3 \\ x & 1 + x + x^2 + x^3 \end{bmatrix}.$$

Applications of Order Basis

- Padé, Hermite Padé approximations, and their generalizations (Beckermann and Labahn 1994, 1997, 2000)
- Shifted normal forms (Popov form, Hermite form...) (Beckermann, Labahn and Villard 1999, 2006)
- Column reduction, determinant (Giorgi, Jeannerod and Villard 2003)
- Matrix Inverse (Jeannerod and Villard 2004)
- Nullspace basis (Storjohann and Villard 2005)

Existing Work on Order Basis Computation

- Beckermann and Labahn 1994:
  - Convert problem with input $\mathbf{F} \in \mathbb{K}[x]^{m \times n}$ and order σ to vector input $\mathbf{f} \in \mathbb{K}[x]^{1 \times n}$ and order $m\sigma$
  - Cost $O^{\sim}\left(n^2 m\sigma + nm^2\sigma\right)$ field operations.
- Giorgi, Jeannerod, Villard 2003: More direct approach cost $O^{\sim}(n^{\omega}\sigma)$.
  - Efficient if $m \in \Theta(n)$. Can be improved if m is small as in Hermite Padé approximation.
- Storjohann 2006: Computes basis elements with degrees bounded by δ, with cost $O^{\sim}(n^{\omega}\delta)$ for $\delta \geq \lceil m\sigma/n \rceil$.
  - Cost $O^{\sim}(n^{\omega}\lceil m\sigma/n \rceil)$ when $\delta \in O(m\sigma/n)$.
- We want to compute a complete basis with a cost of $O^{\sim}(n^{\omega}\lceil m\sigma/n \rceil)$.

Existing Work on Order Basis Computation

- Beckermann and Labahn 1994:
  - Convert problem with input $\mathbf{F} \in \mathbb{K}[x]^{m \times n}$ and order σ to vector input $\mathbf{f} \in \mathbb{K}[x]^{1 \times n}$ and order $m\sigma$
  - Cost $O^{\sim}\left(n^2 m\sigma + nm^2\sigma\right)$ field operations.
- Giorgi, Jeannerod, Villard 2003: More direct approach cost $O^{\sim}(n^{\omega}\sigma)$.
  - Efficient if $m \in \Theta(n)$. Can be improved if m is small as in Hermite Padé approximation.
- Storjohann 2006: Computes basis elements with degrees bounded by δ, with cost $O^{\sim}(n^{\omega}\delta)$ for $\delta \geq \lceil m\sigma/n \rceil$.
  - Cost $O^{\sim}(n^{\omega}\lceil m\sigma/n \rceil)$ when $\delta \in O(m\sigma/n)$.
- We want to compute a complete basis with a cost of $O^{\sim}(n^{\omega}\lceil m\sigma/n \rceil)$.

Existing Work on Order Basis Computation

- Beckermann and Labahn 1994:
  - Convert problem with input $\mathbf{F} \in \mathbb{K}[x]^{m \times n}$ and order σ to vector input $\mathbf{f} \in \mathbb{K}[x]^{1 \times n}$ and order $m\sigma$
  - Cost $O^{\sim}\left(n^2 m\sigma + nm^2\sigma\right)$ field operations.
- Giorgi, Jeannerod, Villard 2003: More direct approach cost $O^{\sim}(n^{\omega}\sigma)$.
  - Efficient if $m \in \Theta(n)$. Can be improved if m is small as in Hermite Padé approximation.
- Storjohann 2006: Computes basis elements with degrees bounded by δ, with cost $O^{\sim}(n^{\omega}\delta)$ for $\delta \geq \lceil m\sigma/n \rceil$.
  - Cost $O^{\sim}(n^{\omega}\lceil m\sigma/n \rceil)$ when $\delta \in O(m\sigma/n)$.
- We want to compute a complete basis with a cost of $O^{\sim}(n^{\omega}\lceil m\sigma/n \rceil)$.

Existing Work on Order Basis Computation

- Beckermann and Labahn 1994:
  - Convert problem with input $\mathbf{F} \in \mathbb{K}[x]^{m \times n}$ and order σ to vector input $\mathbf{f} \in \mathbb{K}[x]^{1 \times n}$ and order $m\sigma$
  - Cost $O^{\sim}\left(n^2 m\sigma + nm^2\sigma\right)$ field operations.
- Giorgi, Jeannerod, Villard 2003: More direct approach cost $O^{\sim}(n^{\omega}\sigma)$.
  - Efficient if $m \in \Theta(n)$. Can be improved if m is small as in Hermite Padé approximation.
- Storjohann 2006: Computes basis elements with degrees bounded by δ, with cost $O^{\sim}(n^{\omega}\delta)$ for $\delta \geq \lceil m\sigma/n \rceil$.
  - Cost $O^{\sim}(n^{\omega}\lceil m\sigma/n \rceil)$ when $\delta \in O(m\sigma/n)$.
- We want to compute a complete basis with a cost of $O^{\sim}(n^{\omega}\lceil m\sigma/n \rceil)$.

Assumptions

- Focus on $m = 1$ in this talk for simplicity.
- Assume σ, n are powers of two.

Assumptions

- Focus on $m = 1$ in this talk for simplicity.
- Assume σ, n are powers of two.

Size of Input and Output

- For computing a $(\mathbf{F}, \sigma)$-basis, can always treat input $\mathbf{F}$ as a polynomial matrix of degree $\sigma - 1$
  - Then total size is $n\sigma$ coefficients (assumed $m = 1$).
- Output can have degree σ
  - e.g. $\mathrm{diag}([x^\sigma, 1, \ldots, 1])$ is a $([1, 0, \ldots, 0], \sigma)$-basis
  - But sum of all column degrees is bounded by σ, so total size is also bounded by $n\sigma$.
- Hence $d = \sigma/n$ is the bound on the average degree of the input and output.
- Goal is to compute a $(\mathbf{F}, \sigma)$-basis with a cost $O^\sim(n^\omega d)$.
- Obstacles: high input and output degrees.

Size of Input and Output

- For computing a $(\mathbf{F}, \sigma)$-basis, can always treat input $\mathbf{F}$ as a polynomial matrix of degree $\sigma - 1$
  - Then total size is $n\sigma$ coefficients (assumed $m = 1$).
- Output can have degree σ
  - e.g. $\mathrm{diag}([x^\sigma, 1, \ldots, 1])$ is a $([1, 0, \ldots, 0], \sigma)$-basis
  - But sum of all column degrees is bounded by σ, so total size is also bounded by $n\sigma$.
- Hence $d = \sigma/n$ is the bound on the average degree of the input and output.
- Goal is to compute a $(\mathbf{F}, \sigma)$-basis with a cost $O^\sim(n^\omega d)$.
- Obstacles: high input and output degrees.

Size of Input and Output

- For computing a $(\mathbf{F}, \sigma)$-basis, can always treat input $\mathbf{F}$ as a polynomial matrix of degree $\sigma - 1$
  - Then total size is $n\sigma$ coefficients (assumed $m = 1$).
- Output can have degree σ
  - e.g. $\mathrm{diag}([x^\sigma, 1, \ldots, 1])$ is a $([1, 0, \ldots, 0], \sigma)$-basis
  - But sum of all column degrees is bounded by σ, so total size is also bounded by $n\sigma$.
- Hence $d = \sigma/n$ is the bound on the average degree of the input and output.
- Goal is to compute a $(\mathbf{F}, \sigma)$-basis with a cost $O^\sim(n^\omega d)$.
- Obstacles: high input and output degrees.

Size of Input and Output

- For computing a $(\mathbf{F}, \sigma)$-basis, can always treat input $\mathbf{F}$ as a polynomial matrix of degree $\sigma - 1$
  - Then total size is $n\sigma$ coefficients (assumed $m = 1$).
- Output can have degree σ
  - e.g. $\mathrm{diag}([x^\sigma, 1, \ldots, 1])$ is a $([1, 0, \ldots, 0], \sigma)$-basis
  - But sum of all column degrees is bounded by σ, so total size is also bounded by $n\sigma$.
- Hence $d = \sigma/n$ is the bound on the average degree of the input and output.
- Goal is to compute a $(\mathbf{F}, \sigma)$-basis with a cost $O^\sim(n^\omega d)$.
- Obstacles: high input and output degrees.

Size of Input and Output

- For computing a $(\mathbf{F}, \sigma)$-basis, can always treat input $\mathbf{F}$ as a polynomial matrix of degree $\sigma - 1$
  - Then total size is $n\sigma$ coefficients (assumed $m = 1$).
- Output can have degree σ
  - e.g. $\mathrm{diag}([x^\sigma, 1, \ldots, 1])$ is a $([1, 0, \ldots, 0], \sigma)$-basis
  - But sum of all column degrees is bounded by σ, so total size is also bounded by $n\sigma$.
- Hence $d = \sigma/n$ is the bound on the average degree of the input and output.
- Goal is to compute a $(\mathbf{F}, \sigma)$-basis with a cost $O^\sim(n^\omega d)$.
- Obstacles: high input and output degrees.

Partial Linearization (Storjohann 2006)

- Increase the row dimension to make the input matrix more square while decrease the order/degree.
- $\mathbf{F} = \mathbf{F}_0 + \mathbf{F}_1 x^{\delta} + \mathbf{F}_2 x^{2\delta} + \cdots + \mathbf{F}_l x^{l\delta}$, $\deg \mathbf{F}_i \leq \delta - 1$.
- Computing a $(\mathbf{F}, \sigma)$-basis $\rightarrow$ computing a $(\bar{\mathbf{F}}, 2\delta)$-basis,

$$\bar{\mathbf{F}} = \left[\begin{array}{c|c} \mathbf{F}_0 + \mathbf{F}_1 x^{\delta} & \mathbf{0} \\ \hline \mathbf{F}_1 + \mathbf{F}_2 x^{\delta} & \\ \mathbf{F}_2 + \mathbf{F}_3 x^{\delta} & \mathbf{I} \\ \vdots & \\ \mathbf{F}_{l-1} + \mathbf{F}_l x^{\delta} & \end{array}\right].$$

Partial Linearization (Storjohann 2006)

- Increase the row dimension to make the input matrix more square while decrease the order/degree.
- $\mathbf{F} = \mathbf{F}_0 + \mathbf{F}_1 x^{\delta} + \mathbf{F}_2 x^{2\delta} + \cdots + \mathbf{F}_l x^{l\delta}$, $\deg \mathbf{F}_i \leq \delta - 1$.
- Computing a $(\mathbf{F}, \sigma)$-basis $\rightarrow$ computing a $(\bar{\mathbf{F}}, 2\delta)$-basis,

$$\bar{\mathbf{F}} = \left[\begin{array}{c|c} \mathbf{F}_0 + \mathbf{F}_1 x^{\delta} & \mathbf{0} \\ \hline \mathbf{F}_1 + \mathbf{F}_2 x^{\delta} & \\ \mathbf{F}_2 + \mathbf{F}_3 x^{\delta} & \mathbf{I} \\ \vdots & \\ \mathbf{F}_{l-1} + \mathbf{F}_l x^{\delta} & \end{array}\right].$$

Partial Linearization (Storjohann 2006)

- Increase the row dimension to make the input matrix more square while decrease the order/degree.
- $\mathbf{F} = \mathbf{F}_0 + \mathbf{F}_1 x^{\delta} + \mathbf{F}_2 x^{2\delta} + \cdots + \mathbf{F}_l x^{l\delta}$, $\deg \mathbf{F}_i \leq \delta - 1$.
- Computing a $(\mathbf{F}, \sigma)$-basis $\rightarrow$ computing a $(\bar{\mathbf{F}}, 2\delta)$-basis,

$$\bar{\mathbf{F}} = \left[\begin{array}{c|c} \mathbf{F}_0 + \mathbf{F}_1 x^{\delta} & \mathbf{0} \\ \hline \mathbf{F}_1 + \mathbf{F}_2 x^{\delta} & \\ \mathbf{F}_2 + \mathbf{F}_3 x^{\delta} & \mathbf{I} \\ \vdots & \\ \mathbf{F}_{l-1} + \mathbf{F}_l x^{\delta} & \end{array}\right].$$

Partial Linearization (Storjohann 2006)

- Increase the row dimension to make the input matrix more square while decrease the order/degree.
- $\mathbf{F} = \mathbf{F}_0 + \mathbf{F}_1 x^{\delta} + \mathbf{F}_2 x^{2\delta} + \cdots + \mathbf{F}_l x^{l\delta}$, $\deg \mathbf{F}_i \leq \delta - 1$.
- Computing a $(\mathbf{F}, \sigma)$-basis $\rightarrow$ computing a $(\bar{\mathbf{F}}, 2\delta)$-basis,

$$\bar{\mathbf{F}} = \left[\begin{array}{c|c} \mathbf{F}_0 + \mathbf{F}_1 x^{\delta} & \mathbf{0} \\ \hline \mathbf{F}_1 + \mathbf{F}_2 x^{\delta} & \\ \mathbf{F}_2 + \mathbf{F}_3 x^{\delta} & \mathbf{I} \\ \vdots & \\ \mathbf{F}_{l-1} + \mathbf{F}_l x^{\delta} & \end{array}\right].$$

Example: $\sigma = 8$, $\delta = 4$, $\mathbf{F} =$
$[x + x^2 + x^3 + x^4 + x^5 + x^6, 1 + x + x^5 + x^6 + x^7, 1 + x^2 + x^4 + x^5 + x^6 + x^7, 1 + x + x^3 + x^7]$.
$\bar{\mathbf{F}} = \mathbf{F}$.

Partial Linearization (Storjohann 2006)

- Increase the row dimension to make the input matrix more square while decrease the order/degree.
- $\mathbf{F} = \mathbf{F}_0 + \mathbf{F}_1 x^\delta + \mathbf{F}_2 x^{2\delta} + \cdots + \mathbf{F}_l x^{l\delta}$, $\deg \mathbf{F}_i \leq \delta - 1$.
- Computing a $(\mathbf{F}, \sigma)$-basis $\rightarrow$ computing a $(\bar{\mathbf{F}}, 2\delta)$-basis,

$$\bar{\mathbf{F}} = \left[\begin{array}{c|c} \mathbf{F}_0 + \mathbf{F}_1 x^\delta & \mathbf{0} \\ \hline \mathbf{F}_1 + \mathbf{F}_2 x^\delta & \\ \mathbf{F}_2 + \mathbf{F}_3 x^\delta & \mathbf{I} \\ \vdots & \\ \mathbf{F}_{l-1} + \mathbf{F}_l x^\delta & \end{array}\right].$$

Example: $\sigma = 8$, $\delta = 2$, $\mathbf{F} =$
$[x + x^2 + x^3 + x^4 + x^5 + x^6, 1 + x + x^5 + x^6 + x^7, 1 + x^2 + x^4 + x^5 + x^6 + x^7, 1 + x + x^3 + x^7]$.

$$\bar{\mathbf{F}} = \begin{bmatrix} x + x^2 + x^3 & 1 + x & 1 + x^2 & 1 + x + x^2 & 0 & 0 \\ 1 + x + x^2 + x^3 & x^3 & 1 + x^2 + x^3 & x & 1 & 0 \\ 1 + x + x^2 & x + x^2 + x^3 & 1 + x + x^2 + x^3 & x^3 & 0 & 1 \end{bmatrix}$$

Partial Linearization (Storjohann 2006)

- Increase the row dimension to make the input matrix more square while decrease the order/degree.
- $\mathbf{F} = \mathbf{F}_0 + \mathbf{F}_1 x^{\delta} + \mathbf{F}_2 x^{2\delta} + \cdots + \mathbf{F}_l x^{l\delta}$, $\deg \mathbf{F}_i \leq \delta - 1$.
- Computing a $(\mathbf{F}, \sigma)$-basis $\rightarrow$ computing a $(\bar{\mathbf{F}}, 2\delta)$-basis,

$$\bar{\mathbf{F}} = \left[\begin{array}{c|c} \mathbf{F}_0 + \mathbf{F}_1 x^{\delta} & \mathbf{0} \\ \hline \mathbf{F}_1 + \mathbf{F}_2 x^{\delta} & \\ \mathbf{F}_2 + \mathbf{F}_3 x^{\delta} & \mathbf{I} \\ \vdots & \\ \mathbf{F}_{l-1} + \mathbf{F}_l x^{\delta} & \end{array}\right].$$

Example: $\sigma = 8$, $\delta = 1$, $\mathbf{F} =$
$[x+x^2+x^3+x^4+x^5+x^6, 1+x+x^5+x^6+x^7, 1+x^2+x^4+x^5+x^6+x^7, 1+x+x^3+x^7]$.

$$\bar{\mathbf{F}} = \begin{bmatrix} x & 1+x & 1 & 1+x & 0 & 0 & 0 & 0 & 0 & 0 \\ 1+x & 1 & x & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1+x & 0 & 1 & x & 0 & 1 & 0 & 0 & 0 & 0 \\ 1+x & 0 & x & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1+x & x & 1+x & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1+x & 1+x & 1+x & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1+x & 1+x & x & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Partial Linearization (Storjohann 2006)

- A $(\bar{\mathbf{F}}, 2\delta)$-basis of the partial linearization provides a partial $(\mathbf{F}, \sigma)$-basis, containing elements of degree less than δ.

- Example: $\sigma = 8$, $\delta = 2$, $\mathbf{F} =$

$$[x+x^2+x^3+x^4+x^5+x^6,\ 1+x+x^5+x^6+x^7,\ 1+x^2+x^4+x^5+x^6+x^7,\ 1+x+x^3+x^7].$$

$$\bar{\mathbf{F}} = \begin{bmatrix} x+x^2+x^3 & 1+x+x^5 & 1+x^2 & 1+x+x^3 & 0 & 0 \\ 1+x+x^2+x^3 & x^3 & 1+x^2+x^3 & x & 1 & 0 \\ 1+x+x^2 & x+x^2+x^3 & 1+x+x^2+x^3 & x^3 & 0 & 1 \end{bmatrix}$$

- a $(\bar{\mathbf{F}}, 4)$-basis $\begin{bmatrix} 1 & x & 1 & x^2+x^3 & 0 & x+x^2+x^3 \\ 0 & 1 & 0 & x^2 & x^2+x^3 & 0 \\ 1 & 1+x & x+x^2 & x^2 & x^2 & x^2 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & x^2 & x+x^2+x^3 \\ 0 & 1 & 1+x^2 & 0 & x^2 & x+x^2 \end{bmatrix}$

- A $(\mathbf{F}, 8)$-basis is $\begin{bmatrix} 1 & x & 1 & x^2 \\ 0 & 1 & x^2+x^3 & 0 \\ 1 & 1+x & x & x^3+x^4 \\ 1 & 0 & 0 & 0 \end{bmatrix}$

Partial Linearization (Storjohann 2006)

- A $(\bar{\mathbf{F}}, 2\delta)$-basis of the partial linearization provides a partial $(\mathbf{F}, \sigma)$-basis, containing elements of degree less than δ.

- Example: $\sigma = 8$, $\delta = 2$, $\mathbf{F} =$

$$[x+x^2+x^3+x^4+x^5+x^6, 1+x+x^5+x^6+x^7, 1+x^2+x^4+x^5+x^6+x^7, 1+x+x^3+x^7].$$

$$\bar{\mathbf{F}} = \begin{bmatrix} x+x^2+x^3+x^4+x^5+x^6 & 1+x+x^5+x^6+x^7 & 1+x^2+x^6+x^7 & 1+x+x^3+x^7 & 0 & 0 \\ 1+x+x^2+x^3 & x^3 & 1+x^2+x^3 & x & 1 & 0 \\ 1+x+x^2 & x+x^2+x^3 & 1+x+x^2+x^3 & x^3 & 0 & 1 \end{bmatrix}$$

- a $(\bar{\mathbf{F}}, 4)$-basis $\begin{bmatrix} 1 & x & 1 & x^2+x^3 & 0 & x+x^2+x^3 \\ 0 & 1 & 0 & x^2 & x^2+x^3 & 0 \\ 1 & 1+x & x+x^2 & x^2 & x^2 & x^2 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & x^2 & x+x^2+x^3 \\ 0 & 1 & 1+x^2 & 0 & x^2 & x+x^2 \end{bmatrix}$

- A $(\mathbf{F}, 8)$-basis is $\begin{bmatrix} 1 & x & 1 & x^2 \\ 0 & 1 & x^2+x^3 & 0 \\ 1 & 1+x & x & x^3+x^4 \\ 1 & 0 & 0 & 0 \end{bmatrix}$

Key ideas

- The result of a partial linearized problem can be extended to that of another partial linearized problem of a higher degree.
- The extension can be done efficiently by disregarding basis elements computed previously.

Key ideas

- The result of a partial linearized problem can be extended to that of another partial linearized problem of a higher degree.
- The extension can be done efficiently by disregarding basis elements computed previously.

The Big Picture

Example: $\mathbf{F} = \mathtt{ABCDEFHIJKLMNOP}$ represent $\mathbf{F} = \mathtt{A} + \mathtt{B}x^{d} + \mathtt{C}x^{2d} + \cdots + \mathtt{P}x^{15d}$

The Big Picture

Example: $\mathbf{F} = \texttt{ABCDEFHIJKLMNOP}$, $\sigma = 16d$, $\delta = d$,

$$\bar{\mathbf{F}} = \left[\begin{array}{l|l} \texttt{ABCDEFGHIJKLMNOP} & \\ \hline \texttt{BC} & \\ \texttt{CDEF} & \\ \texttt{DE} & \\ \texttt{EFGHIJKL} & \\ \texttt{FG} & \\ \texttt{GHIJ} & \\ \texttt{HI} & \mathbf{I} \\ \texttt{IJKLMNOP} & \\ \texttt{JK} & \\ \texttt{KLMN} & \\ \texttt{LM} & \\ \texttt{MNOP} & \\ \texttt{NO} & \\ \texttt{OP} & \end{array}\right]$$

The Big Picture

Example: $\mathbf{F} = \texttt{ABCDEFHIJKLMNOP}$, $\sigma = 16d$, $\delta = 2d$,

$$\bar{\mathbf{F}} = \left[\begin{array}{l|l} \texttt{ABCDEFGHIJKLMNOP} & \\ \hline \texttt{BC} & \\ \texttt{CDEF} & \\ \texttt{DE} & \\ \texttt{EFGHIJKL} & \\ \texttt{FG} & \\ \texttt{GHIJ} & \\ \texttt{HI} & \mathbf{I} \\ \texttt{IJKLMNOP} & \\ \texttt{JK} & \\ \texttt{KLMN} & \\ \texttt{LM} & \\ \texttt{MNOP} & \\ \texttt{NO} & \\ \texttt{OP} & \end{array}\right]$$

The Big Picture

Example: $\mathbf{F} = \texttt{ABCDEFHIJKLMNOP}$, $\sigma = 16d$, $\delta = 4d$,

$$\bar{\mathbf{F}} = \left[\begin{array}{c|c} \texttt{ABCDEFGHIJKLMNOP} & \\ \hline \texttt{BC} & \\ \texttt{CDEF} & \\ \texttt{DE} & \\ \texttt{EFGHIJKL} & \\ \texttt{FG} & \\ \texttt{GHIJ} & \\ \texttt{HI} & \mathbf{I} \\ \texttt{IJKLMNOP} & \\ \texttt{JK} & \\ \texttt{KLMN} & \\ \texttt{LM} & \\ \texttt{MNOP} & \\ \texttt{NO} & \\ \texttt{OP} & \end{array}\right]$$

The Big Picture

Example: $\mathbf{F} = \texttt{ABCDEFHIJKLMNOP}$, $\sigma = 16d$, $\delta = 8d$,

$$\mathbf{F} = \left[\begin{array}{l|l} \texttt{ABCDEFGHIJKLMNOP} & \\ \hline \texttt{BC} & \\ \texttt{CDEF} & \\ \texttt{DE} & \\ \texttt{EFGHIJKL} & \\ \texttt{FG} & \\ \texttt{GHIJ} & \\ \texttt{HI} & \mathsf{I} \\ \texttt{IJKLMNOP} & \\ \texttt{JK} & \\ \texttt{KLMN} & \\ \texttt{LM} & \\ \texttt{MNOP} & \\ \texttt{NO} & \\ \texttt{OP} & \end{array}\right]$$

Introducing Auxiliary Problem

Example: $\mathbf{F} = \mathtt{ABCDEFHIJKLMNOP}$, $\sigma = 16d$, $\delta = d$,

$$\bar{\mathbf{F}} = \left[\begin{array}{l|l} \mathtt{ABCDEFGHIJKLMNOP} & \\ \hline \mathtt{BC} & \\ \mathtt{CDEF} & \\ \mathtt{DE} & \\ \mathtt{EFGHIJKL} & \\ \mathtt{FG} & \\ \mathtt{GHIJ} & \\ \mathtt{HI} & \mathbf{I} \\ \mathtt{IJKLMNOP} & \\ \mathtt{JK} & \\ \mathtt{KLMN} & \\ \mathtt{LM} & \\ \mathtt{MNOP} & \\ \mathtt{NO} & \\ \mathtt{OP} & \end{array}\right]$$

Introducing Auxiliary Problem

Example: $\mathbf{F} = \mathtt{ABCDEFHIJKLMNOP}$, $\sigma = 16d$, $\delta = 2d$,

$$\check{\mathbf{F}} = \left[\begin{array}{l|l} \mathtt{ABCDEFGHIJKLMNOP} & \\ \hline \mathtt{BC} & \\ \mathtt{CDEF} & \\ \mathtt{DE} & \\ \mathtt{EFGHIJKL} & \\ \mathtt{FG} & \\ \mathtt{GHIJ} & \\ \mathtt{HI} & \mathbf{I} \\ \mathtt{IJKLMNOP} & \\ \mathtt{JK} & \\ \mathtt{KLMN} & \\ \mathtt{LM} & \\ \mathtt{MNOP} & \\ \mathtt{NO} & \\ \mathtt{OP} & \end{array}\right]$$

Introducing Auxiliary Problem

Example: $\mathbf{F} = \mathtt{ABCDEFHIJKLMNOP}$, $\sigma = 16d$, $\delta = 2d$,

$$\bar{\mathbf{F}} = \left[\begin{array}{l|l} \mathtt{ABCDEFGHIJKLMNOP} & \\ \hline \mathtt{BC} & \\ \mathtt{CDEF} & \\ \mathtt{DE} & \\ \mathtt{EFGHIJKL} & \\ \mathtt{FG} & \\ \mathtt{GHIJ} & \\ \mathtt{HI} & \mathbf{I} \\ \mathtt{IJKLMNOP} & \\ \mathtt{JK} & \\ \mathtt{KLMN} & \\ \mathtt{LM} & \\ \mathtt{MNOP} & \\ \mathtt{NO} & \\ \mathtt{OP} & \end{array}\right]$$

Introducing Auxiliary Problem

Example: $\mathbf{F} = \mathtt{ABCDEFHIJKLMNOP}$, $\sigma = 16d$, $\delta = 4d$,

$$\check{\mathbf{F}} = \left[\begin{array}{l|l} \mathtt{ABCDEFGHIJKLMNOP} & \\ \hline \mathtt{BC} & \\ \mathtt{CDEF} & \\ \mathtt{DE} & \\ \mathtt{EFGHIJKL} & \\ \mathtt{FG} & \\ \mathtt{GHIJ} & \\ \mathtt{HI} & \mathbf{I} \\ \mathtt{IJKLMNOP} & \\ \mathtt{JK} & \\ \mathtt{KLMN} & \\ \mathtt{LM} & \\ \mathtt{MNOP} & \\ \mathtt{NO} & \\ \mathtt{OP} & \end{array}\right]$$

Introducing Auxiliary Problem

Example: $\mathbf{F} = \texttt{ABCDEFHIJKLMNOP}$, $\sigma = 16d$, $\delta = 4d$,

$$\bar{\mathbf{F}} = \left[\begin{array}{l|l} \texttt{ABCDEFGHIJKLMNOP} & \\ \hline \texttt{BC} & \\ \texttt{CDEF} & \\ \texttt{DE} & \\ \texttt{EFGHIJKL} & \\ \texttt{FG} & \\ \texttt{GHIJ} & \\ \texttt{HI} & \mathbf{I} \\ \texttt{IJKLMNOP} & \\ \texttt{JK} & \\ \texttt{KLMN} & \\ \texttt{LM} & \\ \texttt{MNOP} & \\ \texttt{NO} & \\ \texttt{OP} & \end{array}\right]$$

Introducing Auxiliary Problem

Example: $\mathbf{F} = \texttt{ABCDEFHIJKLMNOP}$, $\sigma = 16d$, $\delta = 8d$,

$$\check{\mathbf{F}} = \left[\begin{array}{l|l} \texttt{ABCDEFGHIJKLMNOP} & \\ \hline \texttt{BC} & \\ \texttt{CDEF} & \\ \texttt{DE} & \\ \texttt{EFGHIJKL} & \\ \texttt{FG} & \\ \texttt{GHIJ} & \\ \texttt{HI} & \mathbf{I} \\ \texttt{IJKLMNOP} & \\ \texttt{JK} & \\ \texttt{KLMN} & \\ \texttt{LM} & \\ \texttt{MNOP} & \\ \texttt{NO} & \\ \texttt{OP} & \end{array}\right]$$

Introducing Auxiliary Problem

Example: $\mathbf{F} = \texttt{ABCDEFHIJKLMNOP}$, $\sigma = 16d$, $\delta = 8d$,

$$\mathbf{F} = \left[\begin{array}{l|l} \texttt{ABCDEFGHIJKLMNOP} & \\ \hline \texttt{BC} & \\ \texttt{CDEF} & \\ \texttt{DE} & \\ \texttt{EFGHIJKL} & \\ \texttt{FG} & \\ \texttt{GHIJ} & \\ \texttt{HI} & I \\ \texttt{IJKLMNOP} & \\ \texttt{JK} & \\ \texttt{KLMN} & \\ \texttt{LM} & \\ \texttt{MNOP} & \\ \texttt{NO} & \\ \texttt{OP} & \end{array}\right]$$

Example: Extending the Result

$$\mathbf{F} = \begin{bmatrix} x+x^2+x^3+x^4+x^5+x^6 & 1+x+x^5+x^6+x^7 & 1+x^2+x^6+x^7 & 1+x+x^3+x^7 & 0 & 0 \\ 1+x+x^2+x^3 & x^3 & 1+x^2+x^3 & x & 1 & 0 \\ 1+x+x^2 & x+x^2+x^3 & 1+x+x^2+x^3 & x^3 & 0 & 1 \end{bmatrix}$$

A $(\bar{\mathbf{F}},4)$-basis $\bar{\mathbf{P}} = \begin{bmatrix} 1 & x & 1 & x^2+x^3 & 0 & x+x^2+x^3 \\ 0 & 1 & 0 & x^2 & x^2+x^3 & 0 \\ 1 & 1+x & x+x^2 & x^2 & x^2 & x^2 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & x^2 & x+x^2+x^3 \\ 0 & 1 & 1+x^2 & 0 & x^2 & x+x^2 \end{bmatrix}$

The residual $\check{\mathbf{F}}\bar{\mathbf{P}} = \begin{bmatrix} 0 & x^8 & x^6+x^9 & x^4+x^6+x^9 & x^6+x^8+x^9+x^{10} & x^5+x^8 \\ 0 & 0 & x^5 & x^4+x^6 & x^4+x^6 & x^5+x^6 \\ 0 & x^4 & x^5 & x^5 & x^4+x^5+x^6 & x^4 \end{bmatrix}$

A $(\check{\mathbf{F}}\bar{\mathbf{P}},[8,4,4],[0,1,2,3,3,3])$-basis $\bar{\mathbf{Q}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & x^2 & x & 1 \\ 0 & 0 & 0 & 0 & x & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & x \end{bmatrix}$

A $(\check{\mathbf{F}},[8,4,4])$-basis $\bar{\mathbf{P}}\bar{\mathbf{Q}} = \begin{bmatrix} 1 & x & 1 & x^2 & x^2+x^4 & 1+x^2+x^3+x^4 \\ 0 & 1 & x^2+x^3 & 0 & x^3 & 0 \\ 1 & 1+x & x & x^3+x^4 & 0 & x+x^2+x^3 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1+x^2 & x^2 & x^2+x^3 & 1+x^2+x^3+x^4 \\ 0 & 1 & 1 & x^2+x^4 & x^2+x^3 & 1+x^3 \end{bmatrix}$

Example: Extending the Result

$$\bar{F} = \begin{bmatrix} x+x^2+x^3+x^4+x^5+x^6 & 1+x+x^5+x^6+x^7 & 1+x^2+x^6+x^7 & 1+x+x^3+x^7 & 0 & 0 \\ 1+x+x^2+x^3 & x^3 & 1+x^2+x^3 & x & 1 & 0 \\ 1+x+x^2 & x+x^2+x^3 & 1+x+x^2+x^3 & x^3 & 0 & 1 \end{bmatrix}$$

$$\text{A } (\bar{F},4)\text{-basis } \bar{P} = \begin{bmatrix} 1 & x & 1 & x^2+x^3 & 0 & x+x^2+x^3 \\ 0 & 1 & 0 & x^2 & x^2+x^3 & 0 \\ 1 & 1+x & x+x^2 & x^2 & x^2 & x^2 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & x^2 & x+x^2+x^3 \\ 0 & 1 & 1+x^2 & 0 & x^2 & x+x^2 \end{bmatrix}$$

$$\text{The residual } \check{F}\bar{P} = \begin{bmatrix} 0 & x^8 & x^6+x^9 & x^4+x^6+x^9 & x^6+x^8+x^9+x^{10} & x^5+x^8 \\ 0 & 0 & x^5 & x^4+x^6 & x^4+x^6 & x^5+x^6 \\ 0 & x^4 & x^5 & x^5 & x^4+x^5+x^6 & x^4 \end{bmatrix}$$

$$\text{A } (\check{F}\bar{P},[8,4,4],[0,1,2,3,3,3])\text{-basis } \bar{Q} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & x^2 & x & 1 \\ 0 & 0 & 0 & 0 & x & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & x \end{bmatrix}$$

$$\text{A } (\check{F},[8,4,4])\text{-basis } \bar{P}\bar{Q} = \begin{bmatrix} 1 & x & 1 & x^2 & x^2+x^4 & 1+x^2+x^3+x^4 \\ 0 & 1 & x^2+x^3 & 0 & x^3 & 0 \\ 1 & 1+x & x & x^3+x^4 & 0 & x+x^2+x^3 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1+x^2 & x^2 & x^2+x^3 & 1+x^2+x^3+x^4 \\ 0 & 1 & 1 & x^2+x^4 & x^2+x^3 & 1+x^3 \end{bmatrix}$$

Example: Extending the Result

$$\check{F} = \begin{bmatrix} x+x^2+x^3+x^4+x^5+x^6 & 1+x+x^5+x^6+x^7 & 1+x^2+x^6+x^7 & 1+x+x^3+x^7 & 0 & 0 \\ 1+x+x^2+x^3 & x^3 & 1+x^2+x^3 & x & 1 & 0 \\ 1+x+x^2 & x+x^2+x^3 & 1+x+x^2+x^3 & x^3 & 0 & 1 \end{bmatrix}$$

$$\text{A } (\bar{F},4)\text{-basis } \bar{P} = \begin{bmatrix} 1 & x & 1 & x^2+x^3 & 0 & x+x^2+x^3 \\ 0 & 1 & 0 & x^2 & x^2+x^3 & 0 \\ 1 & 1+x & x+x^2 & x^2 & x^2 & x^2 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & x^2 & x+x^2+x^3 \\ 0 & 1 & 1+x^2 & 0 & x^2 & x+x^2 \end{bmatrix}$$

$$\text{The residual } \check{F}\bar{P} = \begin{bmatrix} 0 & x^8 & x^6+x^9 & x^4+x^6+x^9 & x^6+x^8+x^9+x^{10} & x^5+x^8 \\ 0 & 0 & x^5 & x^4+x^6 & x^4+x^6 & x^5+x^6 \\ 0 & x^4 & x^5 & x^5 & x^4+x^5+x^6 & x^4 \end{bmatrix}$$

$$\text{A } (\check{F}\bar{P},[8,4,4],[0,1,2,3,3,3])\text{-basis } \bar{Q} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & x^2 & x & 1 \\ 0 & 0 & 0 & 0 & x & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & x \end{bmatrix}$$

$$\text{A } (\check{F},[8,4,4])\text{-basis } \bar{P}\bar{Q} = \begin{bmatrix} 1 & x & 1 & x^2 & x^2+x^4 & 1+x^2+x^3+x^4 \\ 0 & 1 & x^2+x^3 & 0 & x^3 & 0 \\ 1 & 1+x & x & x^3+x^4 & 0 & x+x^2+x^3 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1+x^2 & x^2 & x^2+x^3 & 1+x^2+x^3+x^4 \\ 0 & 1 & 1 & x^2+x^4 & x^2+x^3 & 1+x^3 \end{bmatrix}$$

Example: Extending the Result

$$\check{\mathbf{F}} = \begin{bmatrix} x+x^2+x^3+x^4+x^5+x^6 & 1+x+x^5+x^6+x^7 & 1+x^2+x^6+x^7 & 1+x+x^3+x^7 & 0 & 0 \\ 1+x+x^2+x^3 & x^3 & 1+x^2+x^3 & x & 1 & 0 \\ 1+x+x^2 & x+x^2+x^3 & 1+x+x^2+x^3 & x^3 & 0 & 1 \end{bmatrix}$$

$$\text{A } (\bar{\mathbf{F}},4)\text{-basis } \bar{\mathbf{P}} = \begin{bmatrix} 1 & x & 1 & x^2+x^3 & 0 & x+x^2+x^3 \\ 0 & 1 & 0 & x^2 & x^2+x^3 & 0 \\ 1 & 1+x & x+x^2 & x^2 & x^2 & x^2 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & x^2 & x+x^2+x^3 \\ 0 & 1 & 1+x^2 & 0 & x^2 & x+x^2 \end{bmatrix}$$

$$\text{The residual } \check{\mathbf{F}}\bar{\mathbf{P}} = \begin{bmatrix} 0 & x^8 & x^6+x^9 & x^4+x^6+x^9 & x^6+x^8+x^9+x^{10} & x^5+x^8 \\ 0 & 0 & x^5 & x^4+x^6 & x^4+x^6 & x^5+x^6 \\ 0 & x^4 & x^5 & x^5 & x^4+x^5+x^6 & x^4 \end{bmatrix}$$

$$\text{A } (\check{\mathbf{F}}\bar{\mathbf{P}},[8,4,4],[0,1,2,3,3,3])\text{-basis } \bar{\mathbf{Q}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & x^2 & x & 1 \\ 0 & 0 & 0 & 0 & x & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & x \end{bmatrix}$$

$$\text{A } (\check{\mathbf{F}},[8,4,4])\text{-basis } \bar{\mathbf{P}}\bar{\mathbf{Q}} = \begin{bmatrix} 1 & x & 1 & x^2 & x^2+x^4 & 1+x^2+x^3+x^4 \\ 0 & 1 & x^2+x^3 & 0 & x^3 & 0 \\ 1 & 1+x & x & x^3+x^4 & 0 & x+x^2+x^3 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1+x^2 & x^2 & x^2+x^3 & 1+x^2+x^3+x^4 \\ 0 & 1 & 1 & x^2+x^4 & x^2+x^3 & 1+x^3 \end{bmatrix}$$

Example: Extending the Result

$$\mathbf{F} = \begin{bmatrix} x+x^2+x^3+x^4+x^5+x^6 & 1+x+x^5+x^6+x^7 & 1+x^2+x^6+x^7 & 1+x+x^3+x^7 & 0 & 0 \\ 1+x+x^2+x^3 & x^3 & 1+x^2+x^3 & x & 1 & 0 \\ 1+x+x^2 & x+x^2+x^3 & 1+x+x^2+x^3 & x^3 & 0 & 1 \end{bmatrix}$$

A $(\bar{\mathbf{F}},4)$-basis $\bar{\mathbf{P}} = \begin{bmatrix} 1 & x & 1 & x^2+x^3 & 0 & x+x^2+x^3 \\ 0 & 1 & 0 & x^2 & x^2+x^3 & 0 \\ 1 & 1+x & x+x^2 & x^2 & x^2 & x^2 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & x^2 & x+x^2+x^3 \\ 0 & 1 & 1+x^2 & 0 & x^2 & x+x^2 \end{bmatrix}$

The residual $\check{\mathbf{F}}\bar{\mathbf{P}} = \begin{bmatrix} 0 & x^8 & x^6+x^9 & x^4+x^6+x^9 & x^6+x^8+x^9+x^{10} & x^5+x^8 \\ 0 & 0 & x^5 & x^4+x^6 & x^4+x^6 & x^5+x^6 \\ 0 & x^4 & x^5 & x^5 & x^4+x^5+x^6 & x^4 \end{bmatrix}$

A $(\check{\mathbf{F}}\bar{\mathbf{P}},[8,4,4],[0,1,2,3,3,3])$-basis $\bar{\mathbf{Q}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & x^2 & x & 1 \\ 0 & 0 & 0 & 0 & x & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & x \end{bmatrix}$

A $(\check{\mathbf{F}},[8,4,4])$-basis $\bar{\mathbf{P}}\bar{\mathbf{Q}} = \begin{bmatrix} 1 & x & 1 & x^2 & x^2+x^4 & 1+x^2+x^3+x^4 \\ 0 & 1 & x^2+x^3 & 0 & x^3 & 0 \\ 1 & 1+x & x & x^3+x^4 & 0 & x+x^2+x^3 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1+x^2 & x^2 & x^2+x^3 & 1+x^2+x^3+x^4 \\ 0 & 1 & 1 & x^2+x^4 & x^2+x^3 & 1+x^3 \end{bmatrix}$

Example: Simplify the Computation

$$\check{F} = \begin{bmatrix} x+x^2+x^3+x^4+x^5+x^6 & 1+x+x^5+x^6+x^7 & 1+x^2+x^6+x^7 & 1+x+x^3+x^7 & 0 & 0 \\ 1+x+x^2+x^3 & x^3 & 1+x^2+x^3 & x & 1 & 0 \\ 1+x+x^2 & x+x^2+x^3 & 1+x+x^2+x^3 & x^3 & 0 & 1 \end{bmatrix}$$

A $(\bar{F},4)$-basis $\bar{P} = \begin{bmatrix} 1 & x & 1 & x^2+x^3 & 0 & x+x^2+x^3 \\ 0 & 1 & 0 & x^2 & x^2+x^3 & 0 \\ 1 & 1+x & x+x^2 & x^2 & x^2 & x^2 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & x^2 & x+x^2+x^3 \\ 0 & 1 & 1+x^2 & 0 & x^2 & x+x^2 \end{bmatrix}$

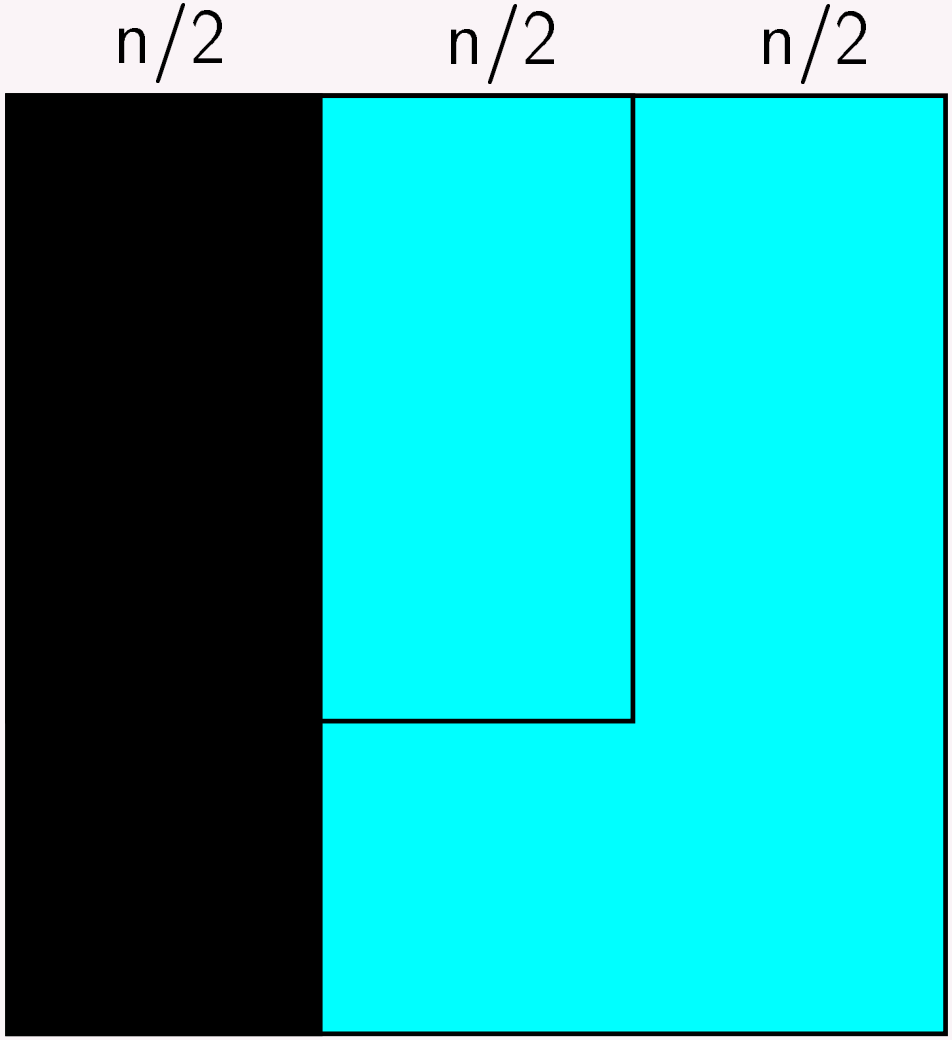
The residual $\check{F}\bar{P} = \begin{bmatrix} 0 & x^8 & x^6+x^9 & x^4+x^6+x^9 & x^6+x^8+x^9+x^{10} & x^5+x^8 \\ 0 & 0 & x^5 & x^4+x^6 & x^4+x^6 & x^5+x^6 \\ 0 & x^4 & x^5 & x^5 & x^4+x^5+x^6 & x^4 \end{bmatrix}$

A $(\check{F}\bar{P},[8,4,4],[0,1,2,3,3,3])$-basis $\bar{Q} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & x^2 & x & 1 \\ 0 & 0 & 0 & 0 & x & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & x \end{bmatrix}$

A $(\check{F},[8,4,4])$-basis $\bar{P}\bar{Q} = \begin{bmatrix} 1 & x & 1 & x^2 & x^2+x^4 & 1+x^2+x^3+x^4 \\ 0 & 1 & x^2+x^3 & 0 & x^3 & 0 \\ 1 & 1+x & x & x^3+x^4 & 0 & x+x^2+x^3 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1+x^2 & x^2 & x^2+x^3 & 1+x^2+x^3+x^4 \\ 0 & 1 & 1 & x^2+x^4 & x^2+x^3 & 1+x^3 \end{bmatrix}$

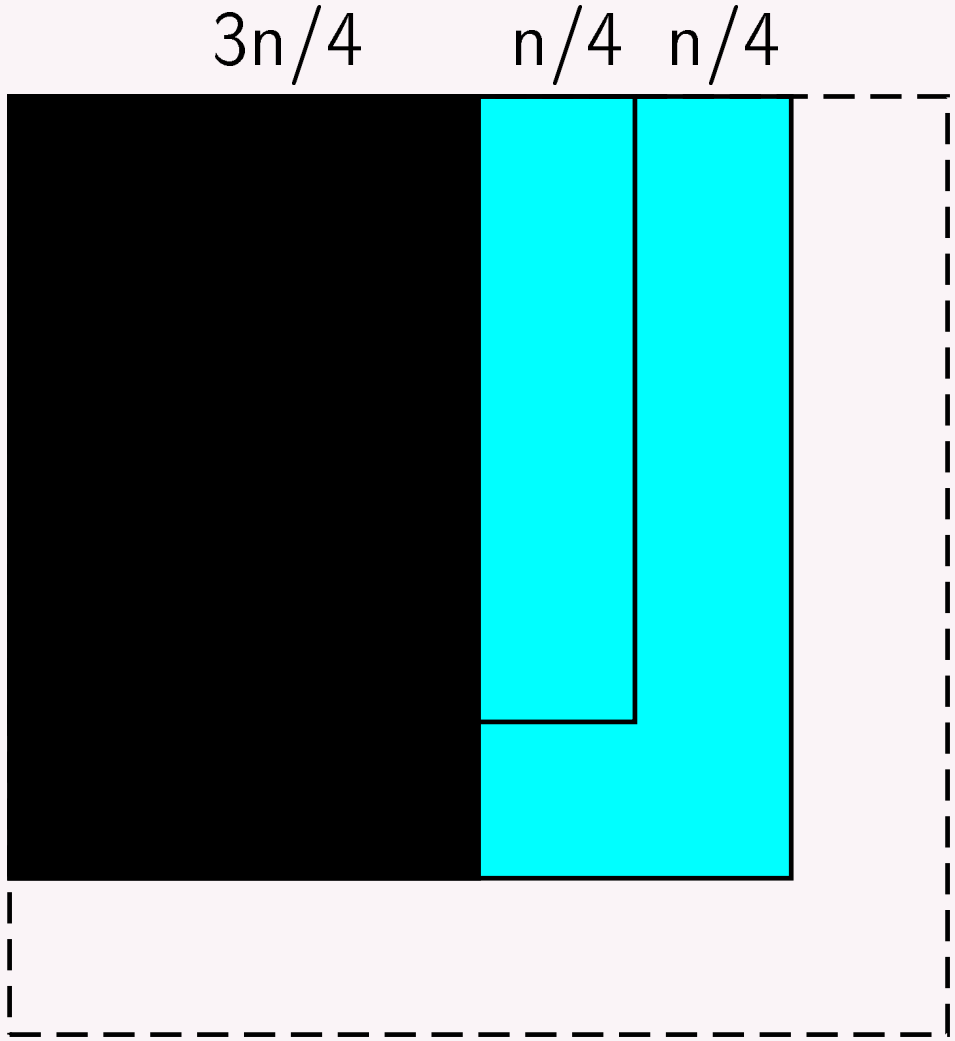
Remaining Columns to Work on

$\delta = 2d$



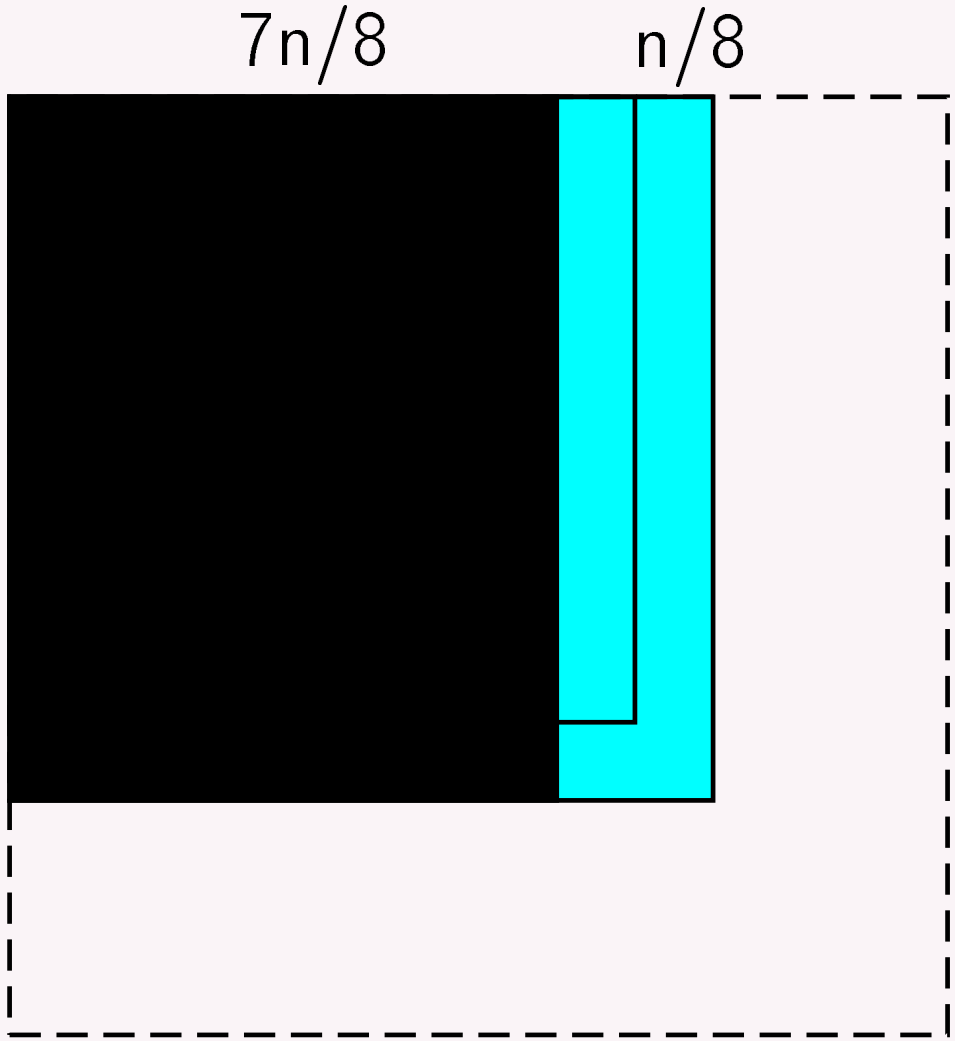
Remaining Columns to Work on

$\delta = 4d$



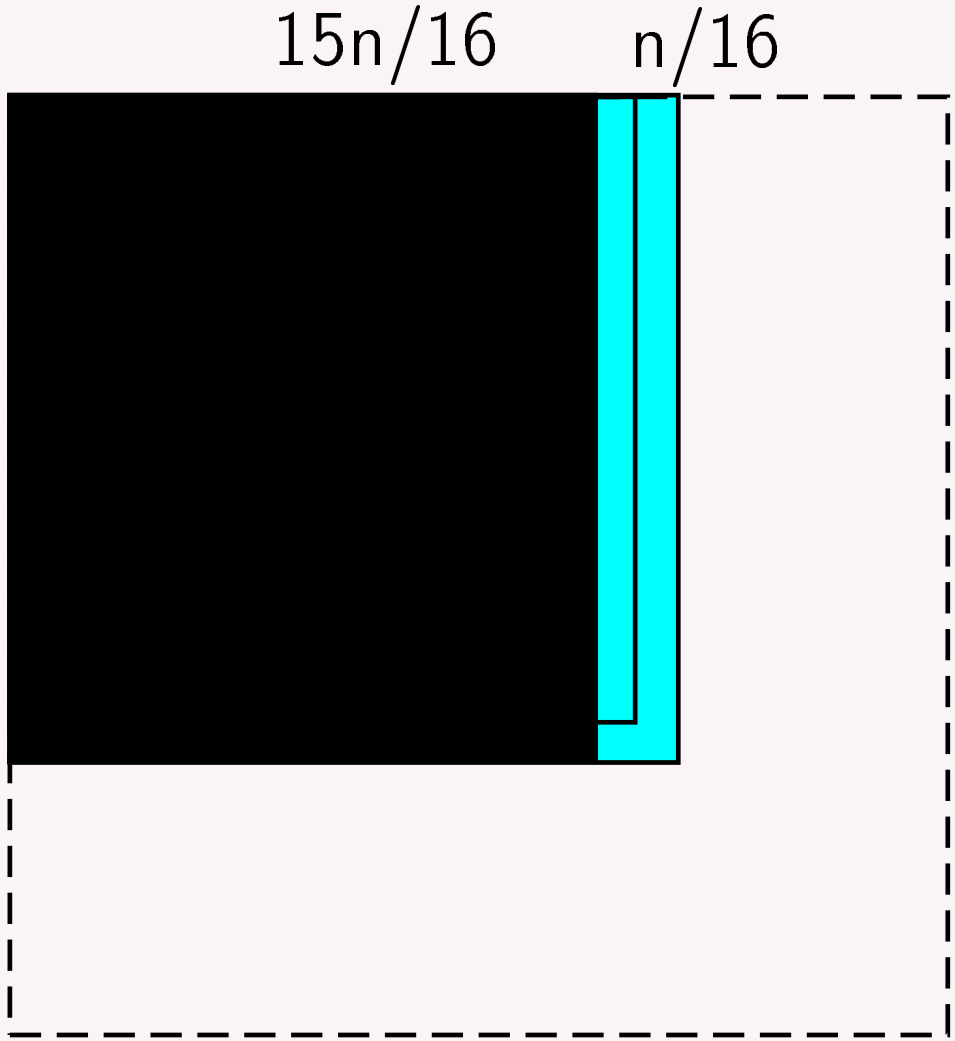
Remaining Columns to Work on

$\delta = 8d$



Remaining Columns to Work on

$\delta = 16d$



Future Work

- Order basis with general unbalanced shift
- Minimal null space basis
- Column reduction, shifted normal forms