Linear algebra over integers and polynomials
Similarities and differences

Arne Storjohann
David R. Cheriton School of Computer Science
University of Waterloo

Example: Linear solving over K: $\mathsf{K} = \mathbb{Z}/(7)$, $n = 5$

$$A = \begin{bmatrix} 5 & 1 & 0 & 4 & 5 \\ 5 & 2 & 3 & 1 & 0 \\ 4 & 6 & 0 & 4 & 0 \\ 5 & 2 & 0 & 2 & 4 \\ 5 & 1 & 1 & 0 & 2 \end{bmatrix} \qquad b = \begin{bmatrix} 1 \\ 6 \\ 2 \\ 4 \\ 3 \end{bmatrix}$$

$\det A = 3$

$$A^{-1}b = \begin{bmatrix} 0 \\ 5 \\ 1 \\ 0 \\ 2 \end{bmatrix}$$

> Classical result: Both $\det A$ and $A^{-1}b$ over K can be computed in $O(n^\theta)$ field operations, where θ is the exponent for matrix multiplication: $2 < \theta \leq 3$.

Note: no expression swell over $\mathbb{Z}/(7)$

Example input over $\mathsf{K}[x]$: $n=5$, $d=2$ $\implies$ expression swell

$$A=\begin{bmatrix} 6x^2+x+5 & 6x+1 & 2x^2 & x+4 & 3x^2+6x+5 \\ 3x+5 & 2x^2+x+2 & 6x^2+2x+3 & 3x^2+2x+1 & x^2+2x \\ 5x^2+x+4 & 6x^2+3x+6 & 5x^2+2x & 5x^2+6x+4 & 3x^2+x \\ 6x^2+6x+5 & 2x^2+3x+2 & 3x^2+6x & 3x^2+2x+2 & 5x^2+5x+4 \\ 3x^2+2x+5 & 5x^2+3x+1 & 4x+1 & 5x^2+4x & 2x^2+3x+2 \end{bmatrix} \qquad b=\begin{bmatrix} x^2+x+1 \\ 2x^2+2x+6 \\ x^2+3x+2 \\ 2x^2+x+4 \\ x^2+4x+3 \end{bmatrix}$$

$$\det A = 6x^{10}+6x^9+x^8+3x^6+x^5+x^4+4x^2+2x+3$$

Degree is $n \times d$ where d is degrees in input matrix.

$$A^{-1}b=\begin{bmatrix} x^{10}+2x^9+2x^8+x^7+3x^6+x^4+6x^3+3x \\ 5x^9+x^8+6x^7+x^5+4x^4+5x^3+x^2+3x+1 \\ 6x^{10}+x^9+3x^8+6x^7+3x^6+2x^5+2x^3+5x^2+3 \\ 5x^{10}+3x^9+4x^8+3x^7+2x^6+3x^5+5x^4+6x \\ 3x^{10}+3x^9+4x^7+5x^6+2x^5+x+6 \end{bmatrix}(1/\det A)$$

Example input over $\mathbb{Z}$: $n = 5$, $d = 3$ $\Longrightarrow$ expression swell

$$A = \begin{bmatrix} 594 & 24 & 601 & 604 & 827 \\ 476 & 397 & 49 & 378 & 174 \\ 7 & 361 & 173 & 939 & 392 \\ 844 & 186 & 655 & 896 & 453 \\ 76 & 621 & 38 & 603 & 582 \end{bmatrix} \qquad b = \begin{bmatrix} 450 \\ 717 \\ 508 \\ 238 \\ 366 \end{bmatrix}$$

$\det A = -26592243059232$

Integer size is about $n \times d$ where d is integer size in input.

$$A^{-1}b = \begin{bmatrix} -58686180258858 \\ 70644871354626 \\ 143314986631278 \\ -49969380574326 \\ -42023211987798 \end{bmatrix} (1/\det A)$$

The Analogy between $\mathsf{K}[x]$ and $\mathbb{Z}$

Polynomial Matrices

$$\begin{bmatrix} 2x^2+6x+4 & 3x^2+5x+3 & 5x^2+4x+5 & 4x^2+6 \\ 2x^2+x+2 & 4x^2+2x+6 & 4x^2+2x+1 & x^2+1 \\ 5x^2+5 & 6x^2 & x^2+5x & 3x^2+2x+5 \\ x^2+2x+2 & x^2+6x+1 & 2x^2+4x & 3x^2+x+3 \end{bmatrix}$$

$$\det = 4x^8+x^7+5x^6+6x^5+4x^3+4x^2+4x+5$$

Integer Matrices

$$\begin{bmatrix} 19664807 & 10690059 & 33070261 & 56138821 & 58713392 \\ 53823071 & 62221765 & 74114539 & 5607878 & 80029954 \\ 11950057 & 75484063 & 79482486 & 69593769 & 30570790 \\ 98824481 & 20449787 & 47014924 & 31388867 & 24938143 \\ 53520576 & 86305734 & 90761911 & 92669416 & 28505719 \end{bmatrix}$$

$$\det = 362395834598355450125706557125187378860$$

Polynomial Matrices	Integer Matrices
principal ideal domain	principal ideal domain
linear growth in degrees	linear growth in word–lengths
count field operations	count machine word operations

<u>Problems:</u> Linear solving, Determinant, Canonical forms

<u>Algorithms:</u> Fraction-free elimination, Modulo determinant canonical form

Analogous fast algorithms for polynomials and integers

[*Modern Computer Algebra*, von zur Gathen & Gerhard]

Polynomials

1. FFT based multiplication: $O(d(\log d)(\log\log d))$
2. Half-gcd algorithm: $O(d(\log d)^2(\log\log d))$
3. Rational function reconstruction
4. Evaluation and interpolation
5. Fast power series expansion

Integers

1. Schönhage Strassen FFT based multiplication
2. Fast continued fraction expansion
3. Rational number reconstruction
4. Homomorphic imaging and chinese remaindering
5. Fast radix conversion

Rational number/function reconstruction

$$\frac{10046631244}{15607862791} \equiv 274965145290403648884 \pmod{10^{21}}$$

$$\frac{5x^2+6x+3}{x^2+4x+3} \equiv 1+3x+2x^2+x^3+5x^4 \pmod{x^5}$$

Radix conversion and series expansion

$$\frac{10046631244}{15607862791} = 884+364(1000)+40(1000^2)+529(1000^3)+\cdots$$

$$\frac{5x^2+6x+3}{x^2+4x+3} = (1+3x)+(2+x)x^2+(1+5x)x^4+\cdots$$

Matrix multiplication

Input: $n \times n$ matrices A and B filled with entries of size d

Output: $C := AB$

Cost: About $O(n^\omega d)$

Note: Entries in C will have size about $2d$

$$\begin{array}{ccc} A & B & C \\ \begin{bmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{bmatrix} & \begin{bmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{bmatrix} = & \begin{bmatrix} ** & ** & ** & ** \\ ** & ** & ** & ** \\ ** & ** & ** & ** \\ ** & ** & ** & ** \end{bmatrix} \end{array}$$

Matrix multiplication

<u>Input:</u> $n \times n$ matrices A and B filled with entries of size d
<u>Output:</u> $C := AB$
<u>Cost:</u> About $O(n^{\omega} d)$
<u>Note:</u> Entries in C will have size about $2d$

$$\overset{A}{\begin{bmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{bmatrix}} \overset{B}{\begin{bmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{bmatrix}} = \overset{C}{\begin{bmatrix} ** & ** & ** & ** \\ ** & ** & ** & ** \\ ** & ** & ** & ** \\ ** & ** & ** & ** \end{bmatrix}}$$

	Over K	Over K$[x]$
Input size	$O(n^2)$	$O(n^2 d)$
Output size	$O(n^2)$	$O(n^2 d)$
Cost	$O(n^{\omega})$	$O(n^{\omega} d)$

Matrix multiplication

<u>Input:</u> $n \times n$ matrices A and B filled with entries of size d
<u>Output:</u> $C := AB$
<u>Cost:</u> About $O(n^{\omega} d)$
<u>Note:</u> Entries in C will have size about $2d$

$$\overset{A}{\begin{bmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{bmatrix}} \overset{B}{\begin{bmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{bmatrix}} = \overset{C}{\begin{bmatrix} ** & ** & ** & ** \\ ** & ** & ** & ** \\ ** & ** & ** & ** \\ ** & ** & ** & ** \end{bmatrix}}$$

Major effort in past decade

Reduce cost of linalg over $\mathbb{Z}/\mathsf{K}[x]$ to matrix multiplication

<u>Classical</u>		<u>Goal</u>
$O(n^{\omega+1} d)$	$\longrightarrow$	$O(n^{\omega} d)$

Main results from 2002–2005

2002	Storjohann	LinSys/Det	K$[x]$	$O(n^{\omega}d)$
	$\Rightarrow$ high-order lifting			
2003	Giorgi *et al*	PopovForm	K$[x]$	$O(n^{\omega}d)$
	$\Rightarrow$ optimal lattice basis reduction			
2004	Kaltofen & Villard	CharPoly	K$[x]$ / $\mathbb{Z}$	$O(n^{2.697263}d)$
	$\Rightarrow$ baby steps giant steps block Krylov			
2005	Storjohann	LinSys/Det	$\mathbb{Z}$	$O(n^{\omega}d)$
	$\Rightarrow$ extension of high-order lifting			

Difference between $K[x]$ and $\mathbb{Z}$: Linearization

Multiplication:

$$\left(f_0 + f_1 x + f_2 x^2\right)\left(g_0 + g_1 x + g_2 x^2\right) \quad \longrightarrow \quad \begin{bmatrix} f_0 & & \\ f_1 & f_0 & \\ f_2 & f_1 & f_0 \\ & f_2 & f_1 \\ & & f_2 \end{bmatrix} \begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ 0 \\ 0 \end{bmatrix}$$

Gcd computation:

$$\gcd\left(f_0 + f_1 x + f_2 x^2,\ g_0 + g_1 x + g_2 x^2\right) \quad \longrightarrow \quad \begin{bmatrix} f_2 & f_1 & f_0 & \\ & f_2 & f_1 & f_0 \\ g_2 & g_1 & g_0 & \\ & g_2 & g_1 & g_0 \end{bmatrix}$$

Difference between $\mathsf{K}[x]$ and $\mathbb{Z}$: Non-Archimedean norm

Degree norm is non-Archimedean

$$\deg(f+g) \leq \max(\deg f, \deg g)$$

Magnitude norm is Archimedean

$$|5+7| \leq |5| + |7| = 13$$

Short products over $\mathsf{K}[x]$ and $\mathbb{Z}$

<u>Compute $a \times b \bmod x^2$</u>

$$\overbrace{(5x^3+3x^2+\underline{2x+1})}^{a}\overbrace{(3x^3+2x^2+\underline{6x+3})}^{b} \equiv (2x+1)(6x+3)$$
$$\equiv 5x^2+5x+3$$
$$\equiv 5x+3$$

<u>Compute $a \times b \bmod 10^2$</u>

$$\overbrace{(207989\underline{83})}^{a}\overbrace{(481302\underline{93})}^{b} \equiv (83)(93)$$
$$\equiv 8277$$
$$\equiv 77$$

Short products over $\mathsf{K}[x]$ and $\mathbb{Z}$

Compute $a \times b \bmod x^2$

$$\overset{a}{(5x^3+3x^2+\underline{2x+1})}\overset{b}{(3x^3+2x^2+\underline{6x+3})} \equiv (2x+1)(6x+3)$$
$$\equiv 5x^2+5x+3$$
$$\equiv 5x+3$$

Compute $a \times b \bmod 10^2$

$$\overset{a}{(207989\underline{83})}\overset{b}{(481302\underline{93})} \equiv (83)(93)$$
$$\equiv 8277$$
$$\equiv 77$$

[2000, Mulders, *On computing short products*]

[2003, Hanrot & Zimmerman, *A long note of Mulder's short product*]

Reverse short products over $K[x]$ and $\mathbb{Z}$

Compute leading two coefficients of $a \times b$

$$\overset{a}{(\underline{5x^3+3x^2}+2x+1)}\overset{b}{(\underline{3x^3+2x^2}+6x+3)} = \underline{x^6+5x^5}+5x^3+\cdots+3$$

$$\Rightarrow (\underline{5x^3+3x^2})(\underline{3x^3+2x^2}) = \underline{x^6+5x^5}+6x^4$$

Reverse short products over $\mathsf{K}[x]$ and $\mathbb{Z}$

Compute leading two coefficients of $a \times b$

$$(\overbrace{\underline{5x^3+3x^2}}^{a}+2x+1)(\overbrace{\underline{3x^3+2x^2}}^{b}+6x+3) = \underline{x^6+5x^5}+5x^3+\cdots+3$$

$$\Rightarrow (5x^3+3x^2)(3x^3+2x^2) = \underline{x^6+5x^5}+6x^4$$

Compute leading two digits of $a \times b$

$$(\overbrace{\underline{6453}}^{a}9839)(\overbrace{\underline{4649}}^{b}9832) = \underline{30}0109167080 7048$$

Reverse short products over $\mathsf{K}[x]$ and $\mathbb{Z}$

Compute leading two coefficients of $a \times b$

$$(\underbrace{5x^3+3x^2}_{}\overset{a}{}+2x+1)(\underbrace{3x^3+2x^2}_{}\overset{b}{}+6x+3) = \underline{x^6+5x^5}+5x^3+\cdots+3$$

$$\Rightarrow (5x^3+3x^2)(3x^3+2x^2) = \underline{x^6+5x^5}+6x^4$$

Compute leading two digits of $a \times b$

$$(\overset{a}{\underline{6453}}9839)(\overset{b}{\underline{4649}}9832) = \underline{30}0109167080704\,8$$

$$\Rightarrow (\underline{6453})(\underline{4649}) = \underline{29}999997$$

Reverse short products over $\mathsf{K}[x]$ and $\mathbb{Z}$

Compute leading two coefficients of $a \times b$

$$(\underbrace{5x^3+3x^2}_{a}+2x+1)(\underbrace{3x^3+2x^2}_{b}+6x+3) = \underline{x^6+5x^5}+5x^3+\cdots+3$$

$$\Rightarrow (5x^3+3x^2)(3x^3+2x^2) = \underline{x^6+5x^5}+6x^4$$

Compute leading two digits of $a \times b$

$$(\underbrace{6453}_{a}9839)(\underbrace{4649}_{b}9832) = \underline{30}01091670807048$$

$$\Rightarrow (\underline{6453})(\underline{4649}) = \underline{29}999997$$

[1993, Krandick & Johnson, *Efficient multiprecision floating point multiplication with optimal directional rounding*]

Part II

High-order lifting and the sparse inverse formula

Alternative representations for the inverse of $A = \begin{bmatrix} 3 & 2 \\ x & 5 \end{bmatrix}$

$$A^{-1} = \begin{bmatrix} \frac{2}{6+2x} & \frac{2}{6+2x} \\ \frac{x}{6+2x} & \frac{4}{6+2x} \end{bmatrix}$$

$$= \left[\begin{array}{c|c} 1+x+x^2+x^3+\cdots & -1-x-x^2-x^3+\cdots \\ \hline -x-x^2-x^3+\cdots & 1+x+x^2+x^3+\cdots \end{array}\right]$$

$$= \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} x + \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} x^2 + \cdots.$$

The sparse inverse formula for $A = \left[\, 1 - cx \,\right]$

Explicit inverse modulo x^{32}

$$(1-cx)^{-1} \bmod x^{32} \;\equiv\; 1 + cx + c^2x^2 + c^3x^3 + c^4x^4 + c^5x^5 + \cdots + c^{31}x^{31}$$

The sparse inverse formula for $A = \left[\, 1 - cx \,\right]$

Explicit inverse modulo x^{32}

$$(1-cx)^{-1} \bmod x^{32} \;\equiv\; 1 + cx + c^2x^2 + c^3x^3 + c^4x^4 + c^5x^5 + \cdots + c^{31}x^{31}$$

$$\equiv\; (1+cx)(1+c^2x^2)(1+c^4x^4)(1+c^8x^8)(1+c^{16}x^{16})$$

The sparse inverse formula for $A = \left[\, 1 - cx \,\right]$

Explicit inverse modulo x^{32}

$$(1-cx)^{-1} \bmod x^{32} = \overbrace{1 + cx + c^2x^2 + c^3x^3 + c^4x^4 + c^5x^5 + \cdots + c^{31}x^{31}}^{\text{32 coefficients}}$$

$$= \underbrace{(1+cx)(1+c^2x^2)(1+c^4x^4)(1+c^8x^8)(1+c^{16}x^{16})}_{\text{5 coefficients}}$$

$$\underbrace{(1+\overbrace{c}^{R_1}x)(1+\overbrace{c^2}^{R_2}x^2)(1+\overbrace{c^4}^{R_4}x^4)}_{(1-cx)^{-1} \bmod x^8}(1+\overbrace{c^8}^{R_8}x^8)(1+\overbrace{c^{16}}^{R_{16}}x^{16})$$

Classical Hensel/Newton iteration (Quadratic lifting)

Example: Compute inverse of $A = [1 - cx]$ over $\mathsf{K}[[x]]$

<u>Initialize:</u> $A^{-1} \bmod x^2 = 1 + cx$

<u>Lift 1:</u>

$$\begin{aligned} R_2 x^2 &= I - A(1 + cx) \\ &= c^2 x^2 \end{aligned}$$

$$\begin{aligned} A^{-1} \bmod x^4 &= (1 + cx)(1 + R_2 x^2) \\ &= 1 + cx + c^2 x^2 + c^3 x^3 \end{aligned}$$

<u>Lift 2:</u>

$$\begin{aligned} R_4 x^2 &= I - A(1 + cx + c^2 x^2 + c^3 x^3) \\ &= c^4 x^4 \end{aligned}$$

$$\begin{aligned} A^{-1} \bmod x^8 &= (1 + cx + c^2 x^2 + c^3 x^3)(1 + R_4 x^4) \\ &= 1 + cx + c^2 x^2 + c^3 x^3 + c^4 x^5 + c^5 x^5 + c^6 x^6 + c^7 x^7 \end{aligned}$$

Computing the residues for $A = 1 - cx$

$$
\begin{aligned}
R_2 x^2 &= I - A(1 + cx) \\
&= c^2 x^2 \\
R_4 x^2 &= I - A(\overbrace{1 + cx + c^2x^2 + c^3x^3}^{A^{-1} \bmod x^4}) \\
&= c^4 x^4 \\
R_8 x^8 &= I - A(\overbrace{1 + cx + c^2x^2 + c^3x^3 + c^4x^4 + c^5x^5 + c^6x^6 + c^7x^7}^{A^{-1} \bmod x^8}) \\
&= c^8 x^8
\end{aligned}
$$

Computing the residues for $A = 1 - cx$

$$\begin{aligned}
R_2 x^2 &= I - A(1 + cx) \\
&= c^2 x^2 \\
R_4 x^2 &= I - A(\overbrace{1 + cx + c^2x^2 + c^3x^3}^{A^{-1} \bmod x^4}) \\
&= c^4 x^4 \\
R_8 x^8 &= I - A(\overbrace{1 + cx + c^2x^2 + c^3x^3 + c^4x^4 + c^5x^5 + c^6x^6 + c^7x^7}^{A^{-1} \bmod x^8}) \\
&= c^8 x^8
\end{aligned}$$

- If $\det A = d$ then $R_2, R_4, R_8, \cdots$ have degree $\leq d - 1$.
- Can use reverse short product
  $\Rightarrow$ need only top d coefficients of $A^{-1} \bmod x^*$

Computing the residue via reverse short product

- Let $A = 1 + 5x + 6x^2$
- Suppose we have

$$A^{-1} \bmod x^{64} = 1 + 2x + 5x^3 + \cdots + 2x^{61} + 5x^{62} + 5x^{63}$$

<u>Exact formula for R_{64}:</u>

$$\begin{aligned} R_{64}x^{64} &= (1 + 5x + 6x^2)(1 + 2x + 5x^3 + \cdots + 2x^{61} + 5x^{62} + 5x^{63}) - I \\ &= 6x^{64} + 2x^{65} \end{aligned}$$

Computing the residue via reverse short product

- Let $A = 1 + 5x + 6x^2$
- Suppose we have

$$A^{-1} \bmod x^{64} = 1 + 2x + 5x^3 + \cdots + 2x^{61} + 5x^{62} + 5x^{63}$$

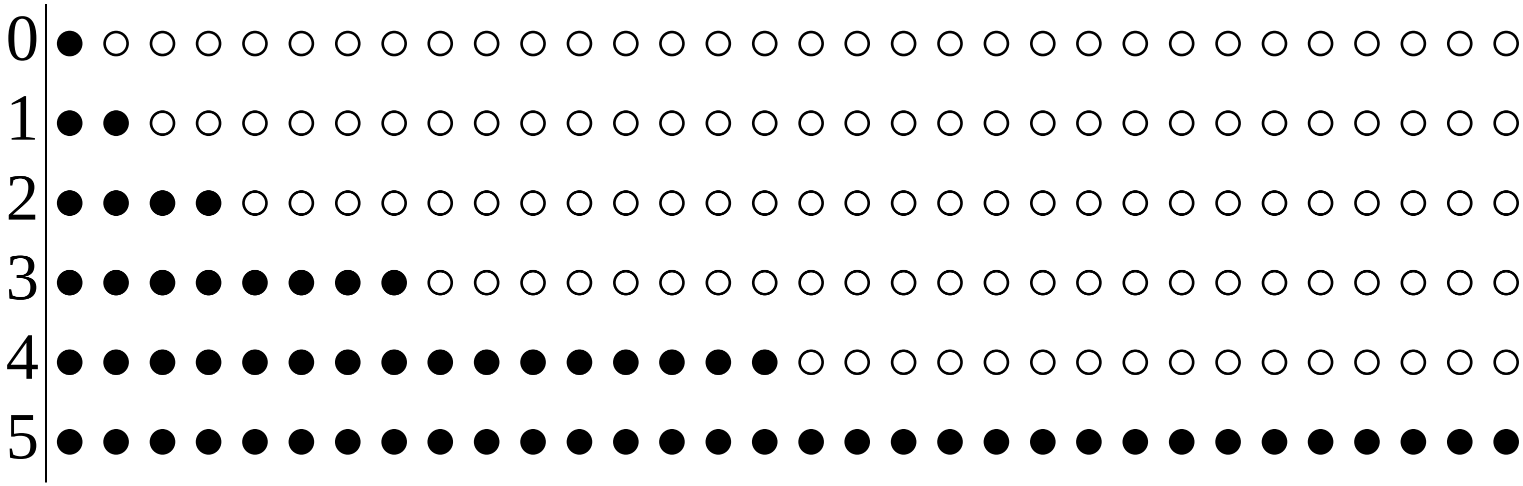
<u>Exact formula for R_{64}:</u>

$$\begin{aligned} R_{64}x^{64} &= (\underline{1 + 5x + 6x^2})(1 + 2x + 5x^3 + \cdots + 2x^{61} + \underline{5x^{62} + 5x^{63}}) - I \\ &= \underline{6x^{64} + 2x^{65}} \end{aligned}$$

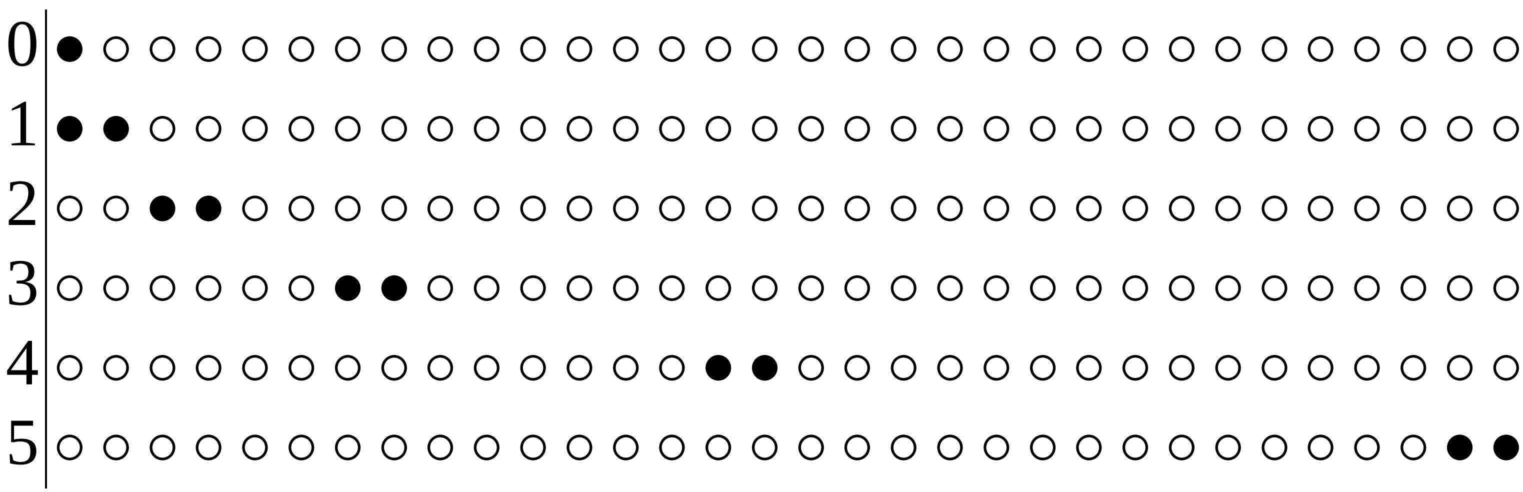
<u>Reverse short product for R_{64}:</u>

$$(\underline{1 + 5x + 6x^2})(\underline{5x^{62} + 5x^{63}}) = 5x^{62} + 2x^{63} + \underline{6x^{64} + 2x^{65}}$$

Standard quadratic lifting



High-order component lifting



High-order lifting example: $A = 1 + 5x + 6x^2$

$$A^{-1} \bmod x^{128} = \overbrace{1 + \cdots + 2x^{61} + 5x^{62} + 5x^{63}}^{L} + \overbrace{x^{64} + \cdots + x^{125} + \underline{x^{126} + 2x^{127}}}^{Hx^{64}}$$

$$= \big(\overbrace{1 + \cdots + 2x^{61} + 5x^{62} + 5x^{63}}^{L}\big)\big(1 + \overbrace{(1 + 5x)}^{R_{64}} x^{64}\big)$$

High-order lifting example: $A = 1 + 5x + 6x^2$

$$A^{-1} \bmod x^{128} = \overbrace{1 + \cdots + 2x^{61} + 5x^{62} + 5x^{63}}^{L} + \overbrace{x^{64} + \cdots + x^{125} + \underline{x^{126} + 2x^{127}}}^{Hx^{64}}$$

$$= \overbrace{(1 + \cdots + \underline{2x^{61} + 5x^{62} + 5x^{63}})}^{L}(1 + \overbrace{(\underline{1 + 5x})}^{R_{64}} x^{64})$$

<u>Via reverse short product</u>

$$(\underline{2x^{61} + 5x^{62} + 6x^{63}})\overbrace{(\underline{1 + 5x})}^{R_{64}} x^{64} = 2x^{125} + \underline{x^{126} + 2x^{127}} + 4x^{128}$$

- top d coefficient of L suffice to get top $d-1$ coefficients of H

Sparse inverse formula

Special case: $\deg A = 1$

$$A^{-1} \bmod x^{32} = (A^{-1} \bmod x^4)(I + R_4 x^4)(I + R_8 x^8)(I + R_{16} x^{16})$$

General case: $\deg A = 3$

$$A^{-1} \bmod x^8 \;=\; (A^{-1} \bmod x^4)(I + R_4 x^4) - M_4 x^8$$

$$A^{-1} \bmod x^{16} \;=\; (((A^{-1} \bmod x^4)(I + R_4 x^4) - M_4 x^8)(1 + R_8 x^8) - M_8 x^{16}$$

$$A^{-1} \bmod x^{32} \;=\; (A^{-1} \bmod x^{16})(1 + R_{16} x^{16}) - M_{16} x^{32}$$

Sparse inverse formula for integer matrices

Example for $7^{-1} \bmod x^{32}$, $x = 11$

$7^{-1} \bmod x^{32}$

$$= 9048761462293951223766922518042 52$$

$$= (((52(1-3x^2)+2x^4)(1-5x^4)+4x^8)(1-3x^8)+2x^{16})(1-5x^{16})+4x^{32}$$

General case:

- Formula exists for any $A \in \mathbb{Z}^{n\times n}$ provided $x \perp \det A$.
- $A^{-1} \bmod x^n$ has size $O(n^3 d)$.
- Sparse inverse formula for $A^{-1} \bmod x^n$ has size $O(n^2(\log n)d)$.

Sparse inverse formula for integer matrices

Example for $7^{-1} \bmod x^{32}$, $x = 11$

$$7^{-1} \bmod x^{32}$$

$$= 9048761462293951223766922518042 52$$

$$= (((52(1-3x^2)+2x^4)(1-5x^4)+4x^8)(1-3x^8)+2x^{16})(1-5x^{16})+4x^{32}$$

General case:

- Formula exists for any $A \in \mathbb{Z}^{n\times n}$ provided $x \perp \det A$.
- $A^{-1} \bmod x^n$ has size $O(n^3 d)$.
- Sparse inverse formula for $A^{-1} \bmod x^n$ has size $O(n^2 (\log n) d)$.

Q: How to compute reverse short products correctly over $\mathbb{Z}$?
A: [2005, Storjohann, *The shifted number system...*]