Algèbre linéaire

Réduction de bases de réseaux

Gilles Villard

C2, Dinard, 12 octobre 2012

Codage, cryptographie, algèbre linéaire

- Systèmes algébriques

- Matrices creuses

- Corps, courbes

- Réseaux

Introduction

Algebraic complexity over an abstract field K

$n \times n$ matrix product: $\mathrm{MM}(\mathrm{n})$ operations in K

$$O(n^3), O(n^\omega) \ \ \omega < 2.373$$

$$\mathrm{MM} \preceq \mathrm{Det} \preceq \mathrm{MM}$$

$$\mathrm{LinSys} \preceq \mathrm{MM} \approx \mathrm{Det}$$

Ex: systèmes polynomiaux structurés

[Strassen 69, 73]
[Bunch & Hopcroft 74, Baur & Strassen 83]

Matrix determinant and integer bit size

$$A \approx \begin{bmatrix} 18 & 71 & \dots \\ -63 & -76 & \dots \\ \vdots & \vdots & \ddots \end{bmatrix} \in \mathbb{Z}^{1000\times 1000} \qquad \det A \approx 3000 \text{ bits}$$

$$\det A = \begin{array}{r}
\text{-191673336650569024448403741324108775687962222505302592385948862411235605506198460909814341483} \\
\text{68211177690633788985534403648566772492805606720643383747614926245299288150875038521778163987386911} \\
\text{11070174019492534464779316261920140240884801908792981968357236666629852660365910937047947334336156} \\
\text{56006804299260418928149700385782047181533684979337303560807823459435005127095611394686376494488383} \\
\text{83846481538475645906564896140544084975065210651494199778472629979974904444114511663442032085615475} \\
\text{75570410787516218737785142181056285757365448210711177910151692827795199135101104323021972307255684} \\
\text{84372748940678783930802557098762086453710733826650915878328871392899215031503347362572958019239176} \\
\text{76707975138106944558733377649024369725670332963804704213470418454450694026460617309610621155363366} \\
\text{66536188690851296620964223267943721240715040640855372872360897709499213075139446296026167927278692} \\
\text{49307633609576134998311099022483026074506643763858072678423555416996730474783896174810398366245185} \\
\text{26363154700005631393607356941192361310279508796103069618004364042676569631325666271159580152587251} \\
\text{36857876125814369642129068285088971204187763356831263141296701363080505773868290400611407584225937} \\
\text{58521429841575182982613911779495994453750603246639876663714396548869300718451265639192797842853341} \\
\text{80310410122586347736475777543695026837100702946341634604800475492807140095880789209348607060948598} \\
\text{46744606477514259944274245467583424189700916937428583354605014668335986515393392388599689615145934} \\
\text{13133843846486050073904072779172516735660047769350858076806626049999126518342588327289900883704960} \\
\text{34658245329787532682622229503900785006116012720345332211887986185219725547638682129125507660061734} \\
\text{18079972279367595646052543561457931791704142410767019774611097099912006755160090739042280440523170} \\
\text{06280257946894051274995513638419139342233330977684981908505063334568041303835128069440207218595593} \\
\text{27937268460302412538918531397745625461948843150530124367699051349059409084970915291042905989600060} \\
\text{57727882421491631601125546443613700167414473405771822447587814344243950607025621988939194005030066} \\
\text{71052677317131667253067912856807858148426879934961963056896028233629933917639280800824415383906303} \\
\text{56666836546675943041512643055398825199729505979909856290774527043540260042383292765535813290742352} \\
\text{63203635914378734172434784126639113249706333154694215873009937095252622318490817358980927917483874} \\
\text{34726373553825401994977210700883624573917036186724547199692257213248911521014150957260135956848743} \\
\text{40048491218435584532737461241425241952415316496215040926315616225194607041004800979689132649153198} \\
\text{84189578683427661351075718295708278282730452505800362040608543128508851988739963376431147994345350} \\
\text{53503400883097180301409783967417311295 62}
\end{array}$$

Bit complexity over the integers

Univariate polynomials

$$\text{bit cost} \preceq \text{algebraic cost} \times \text{output size}$$

Ex: determinant bit size $\leq O^{\sim}(n \log \|A\|)$

Computing the determinant: $\leq O^{\sim}(\mathsf{MM}(n) \times n \log \|A\|)$

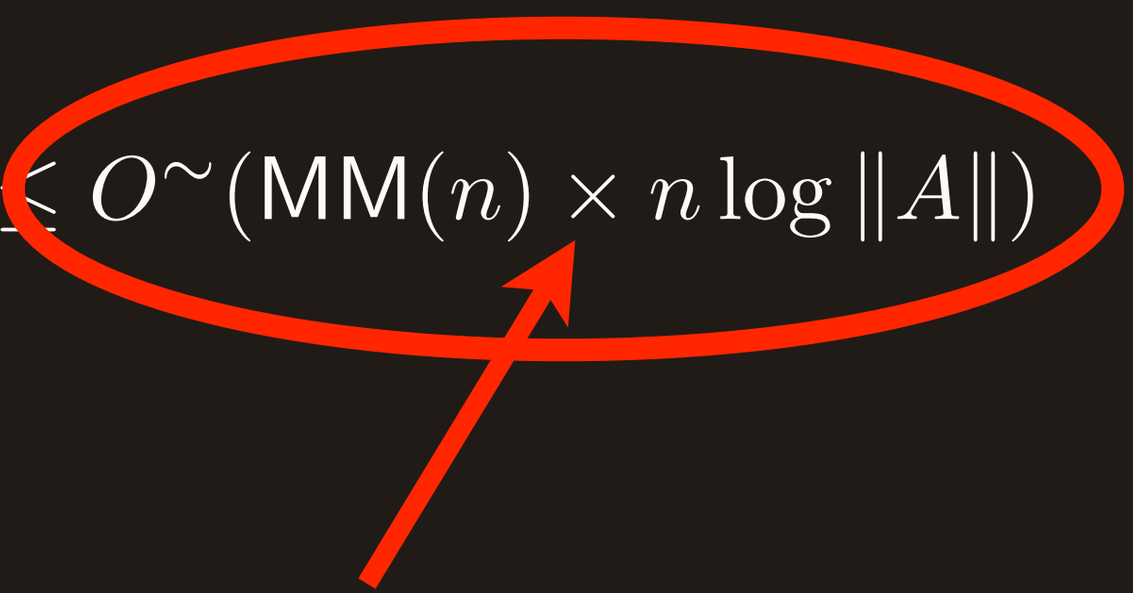
Bit complexity over the integers

Univariate polynomials

$$\text{bit cost} \preceq \text{algebraic cost} \times \text{output size}$$

Ex: determinant bit size $\leq O^{\sim}(n \log \|A\|)$

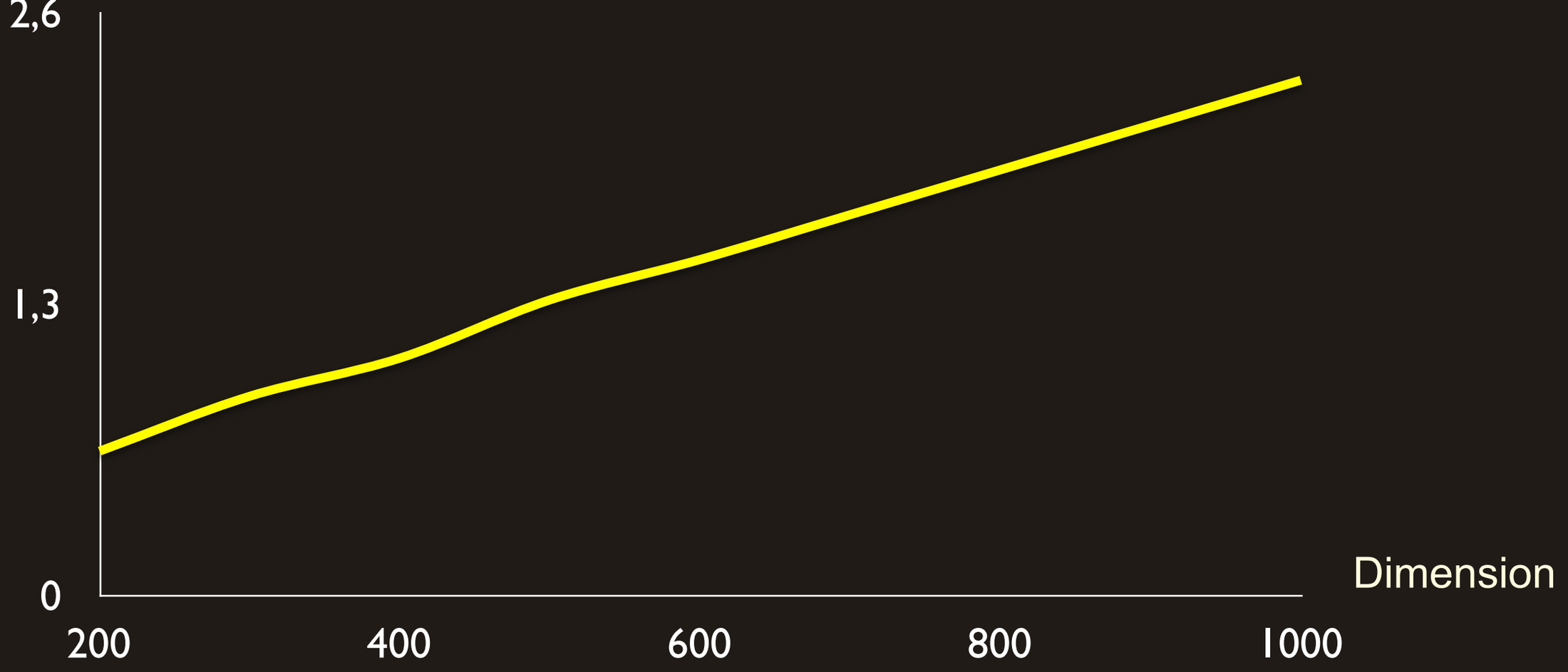
Computing the determinant: $\leq O^{\sim}(\mathsf{MM}(n) \times n \log \|A\|)$



Matrix determinant and integer bit size

$$A \approx \begin{bmatrix} 18 & 71 & \dots \\ -63 & -76 & \dots \\ \vdots & \vdots & \ddots \end{bmatrix} \in \mathbb{Z}^{1000 \times 1000} \qquad \det A \approx 3000 \text{ bits}$$

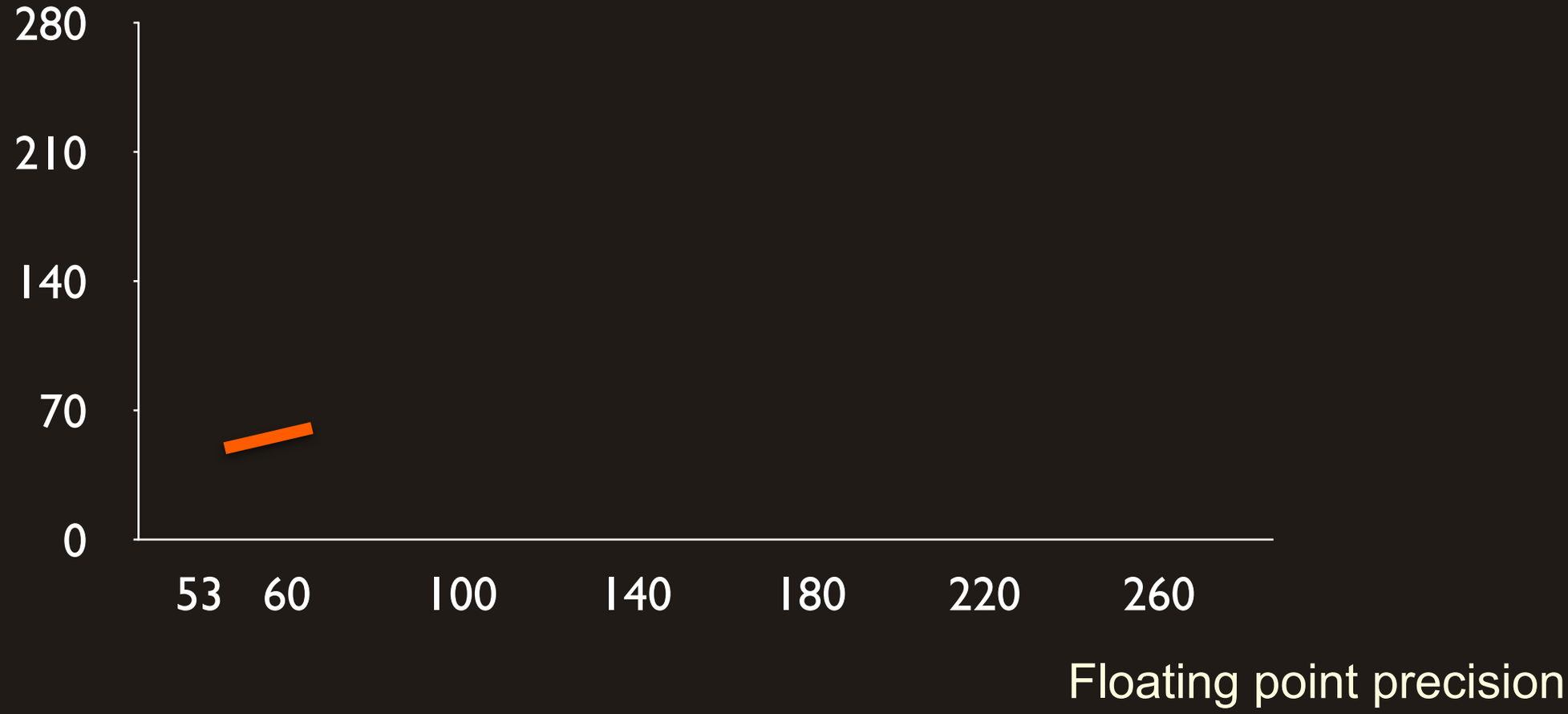
Time ratio
determinant / matrix product



Floating point precision

$$A \approx \begin{bmatrix} 200313259594319107813359471665 8 & 378347629341664670700993561848 4 & \dots \\ -23894451835815687560241235389 & -27572977560418555480185548397 & \dots \\ \vdots & \vdots & \ddots \end{bmatrix} \in \mathbb{Z}^{8\times 8}$$

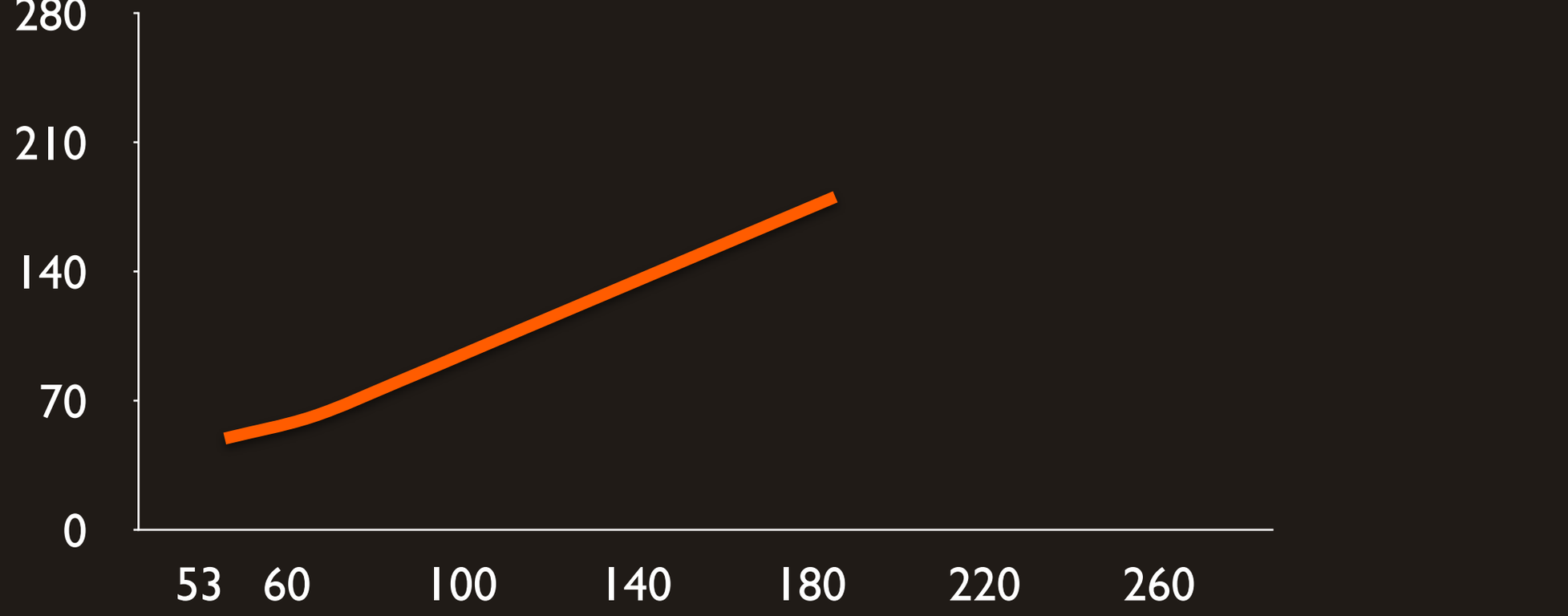
$\log_{10} \mathrm{cond}(A)$



Floating point precision

$$A \approx \begin{bmatrix} 200313259594319107813359471665 8 & 378347629341664670700993561848 4 & \dots \\ -23894451835815687560241235389 & -27572977560418555480185548397 & \dots \\ \vdots & \vdots & \ddots \end{bmatrix} \in \mathbb{Z}^{8\times 8}$$

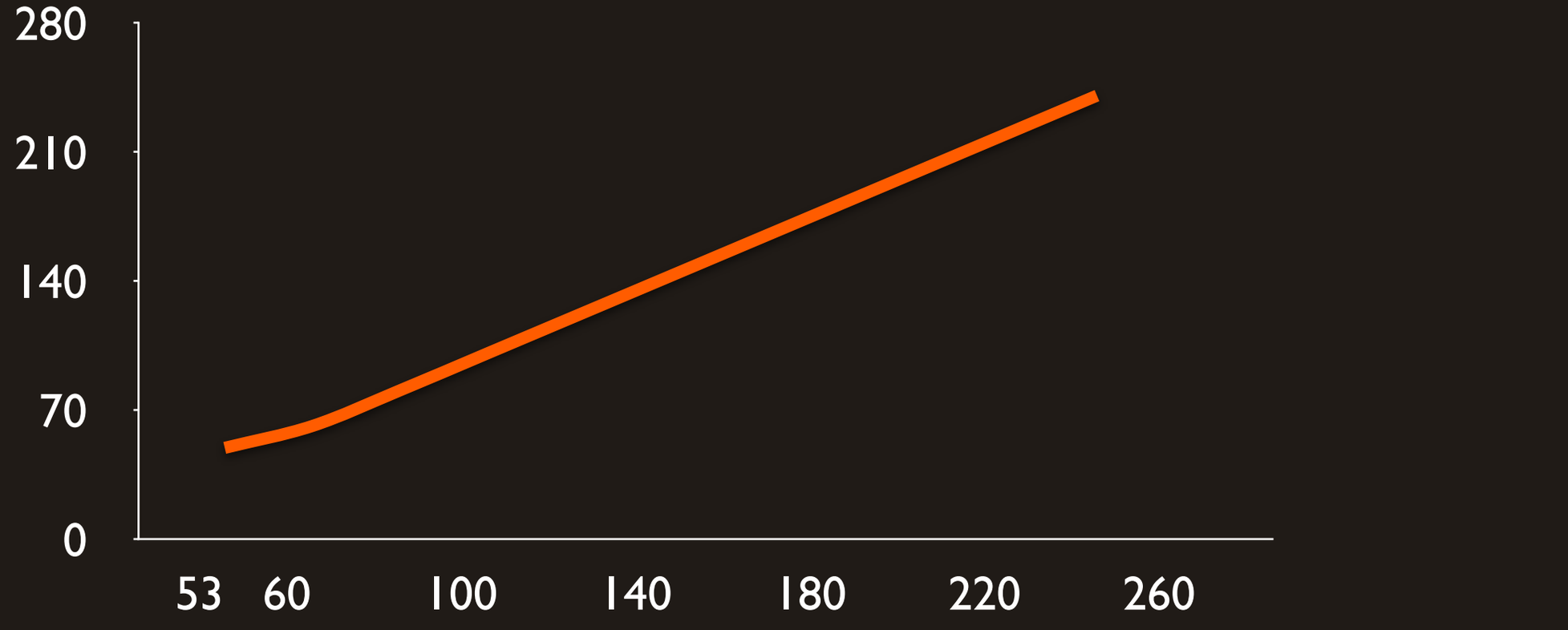
$\log_{10} \mathrm{cond}(A)$



Floating point precision

$$A \approx \begin{bmatrix} 200313259594319107813359471665 8 & 378347629341664670700993561848 4 & \dots \\ -23894451835815687560241235389 & -27572977560418555480185548397 & \dots \\ \vdots & \vdots & \ddots \end{bmatrix} \in \mathbb{Z}^{8\times 8}$$

$\log_{10} \mathrm{cond}(A)$

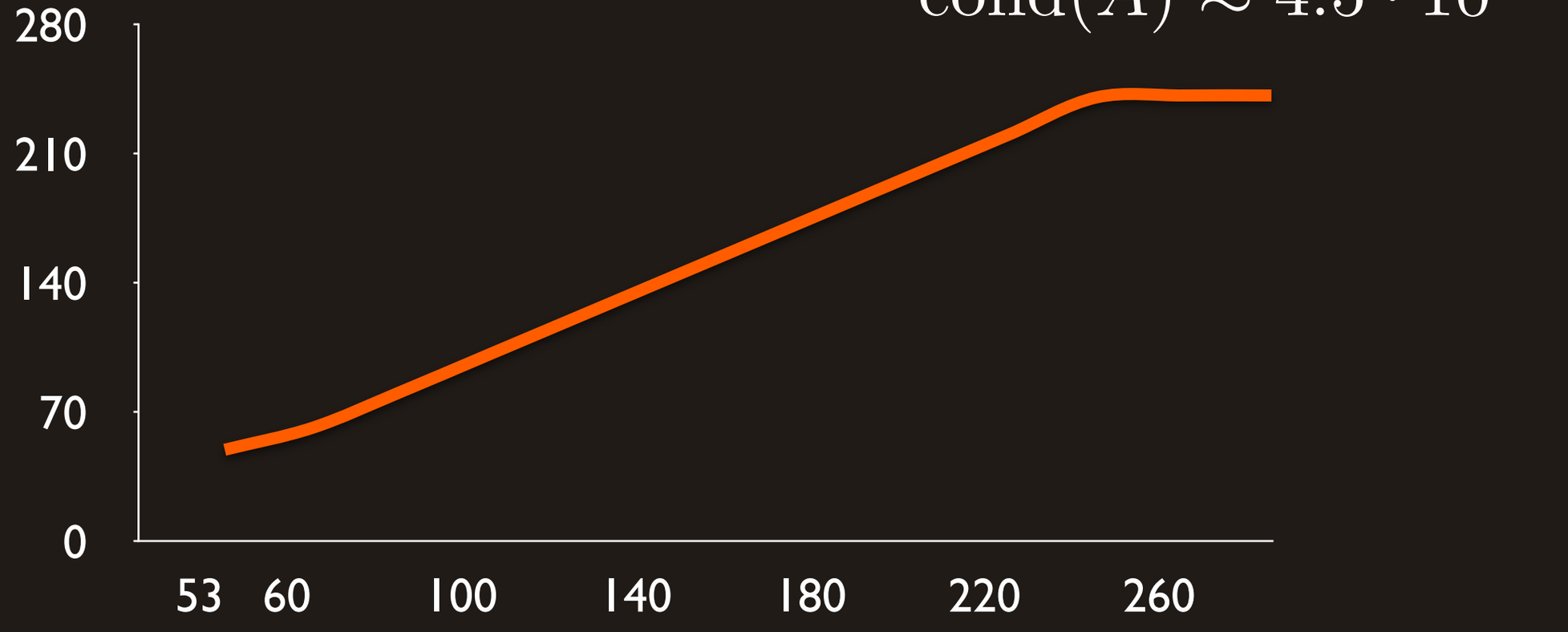


Floating point precision

$$A \approx \begin{bmatrix} 200313259594319107813359471665 8 & 378347629341664670700993561848 4 & \dots \\ -23894451835815687560241235389 & -27572977560418555480185548397 & \dots \\ \vdots & \vdots & \ddots \end{bmatrix} \in \mathbb{Z}^{8\times 8}$$

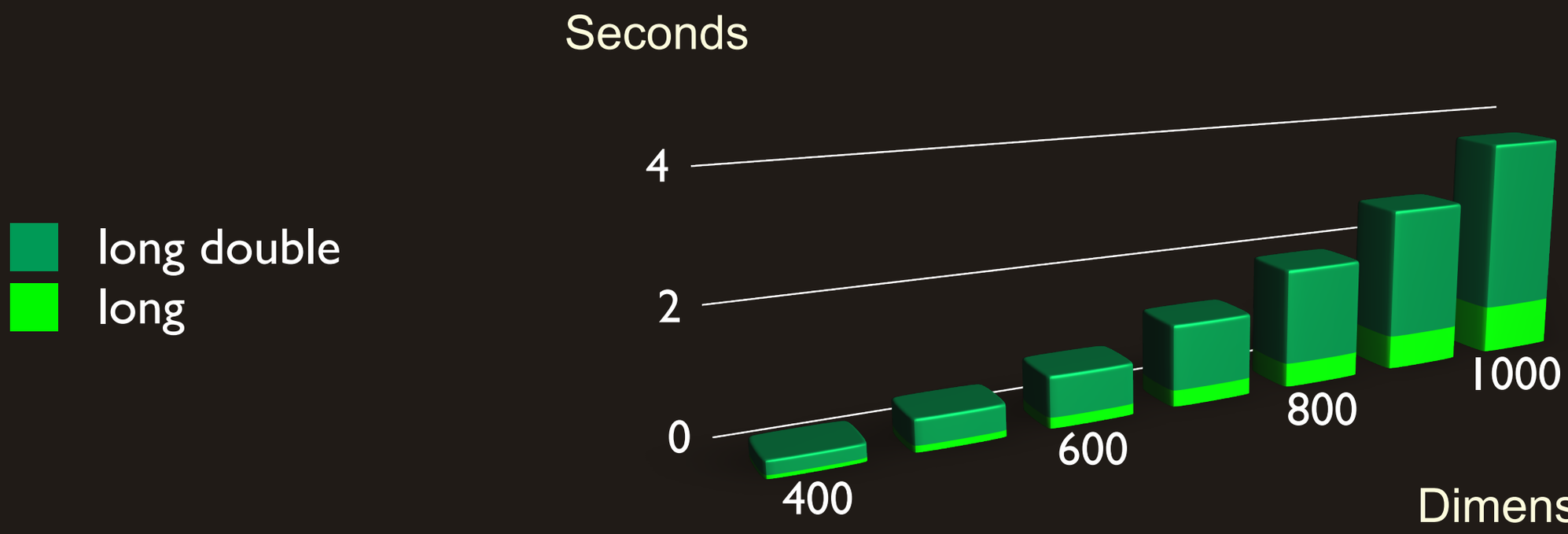
$\log_{10} \mathrm{cond}(A)$

$\mathrm{cond}(A) \approx 4.5 \cdot 10^{242}$



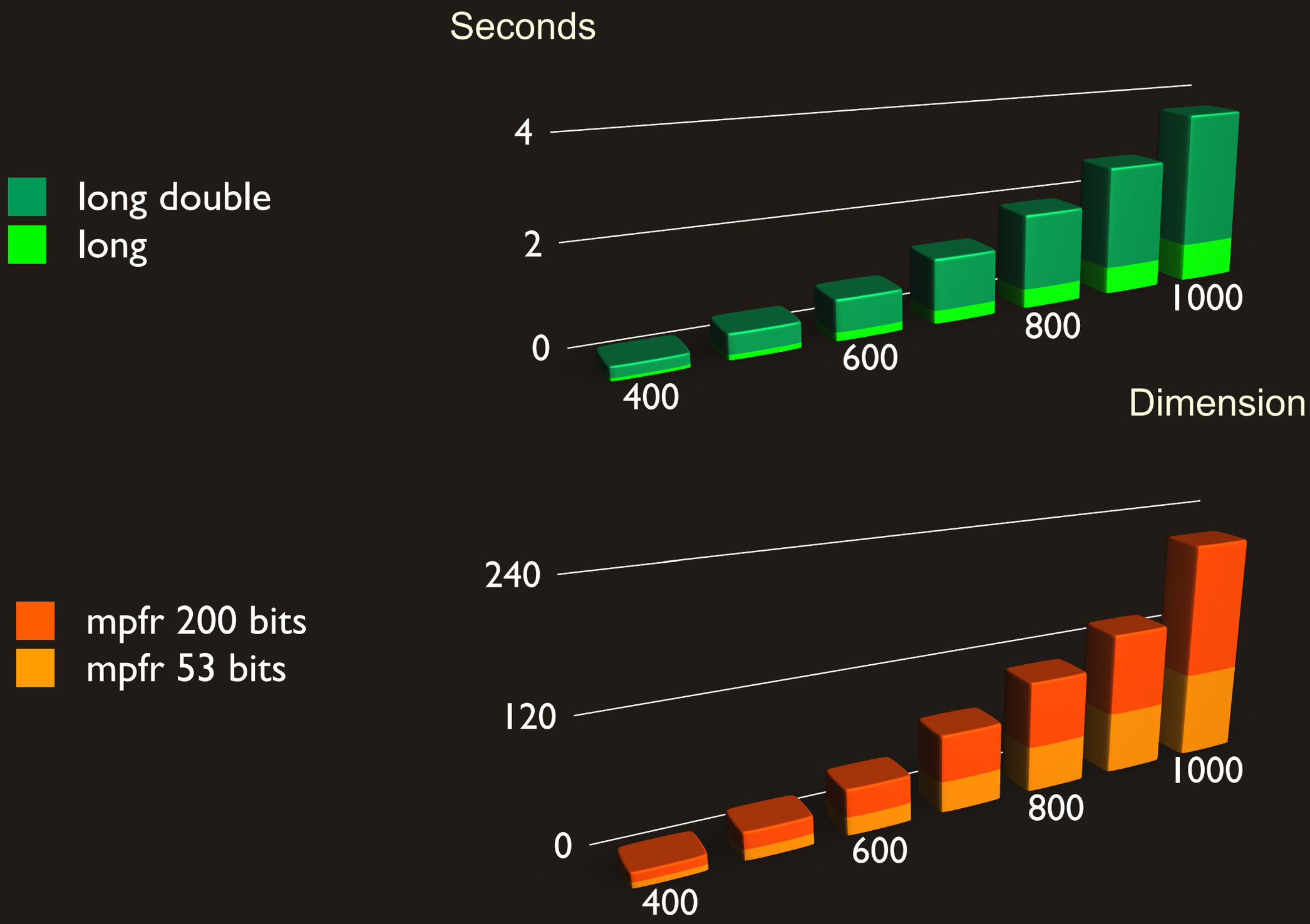
Floating point QR factorization (Householder)

2.66 GHz Intel core i7



Floating point QR factorization (Householder)

2.66 GHz Intel core i7



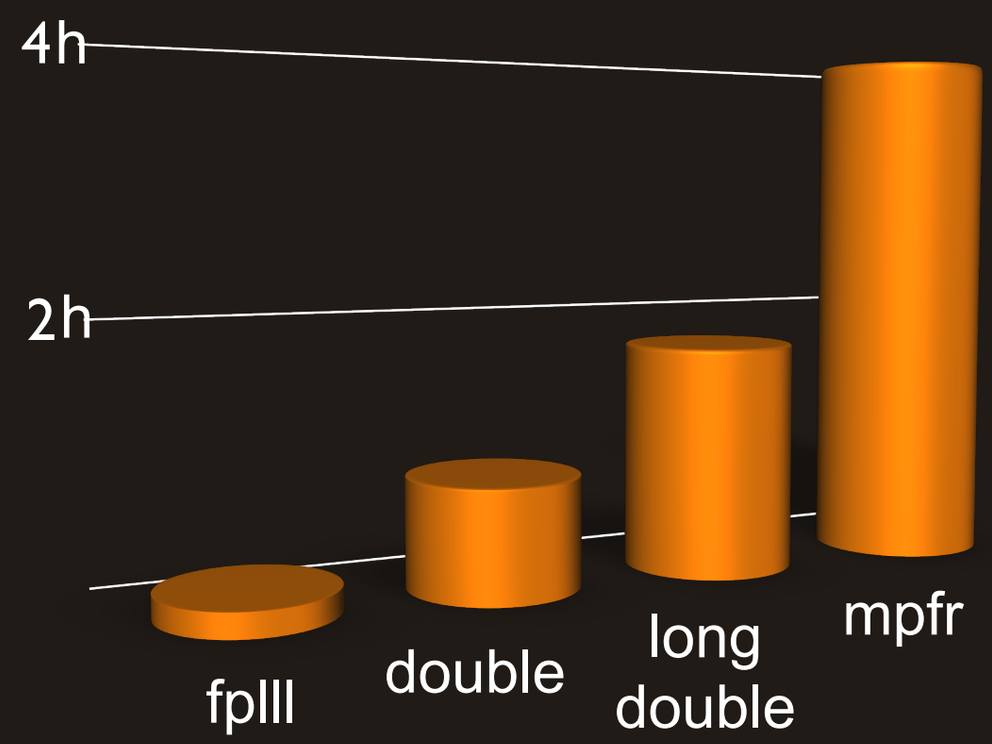
Integer lattice basis reduction

$n = 500$, 10000 bits knapsack

Integer lattice basis reduction

$n = 500$, 10000 bits knapsack

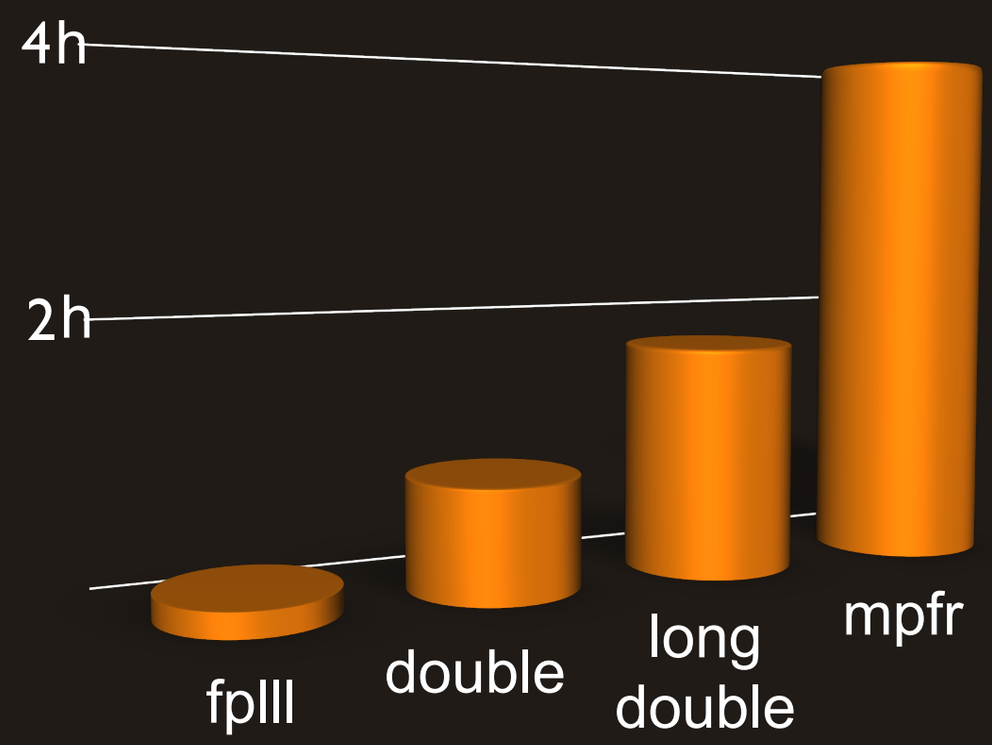
Time spent with the different algorithms or precisions



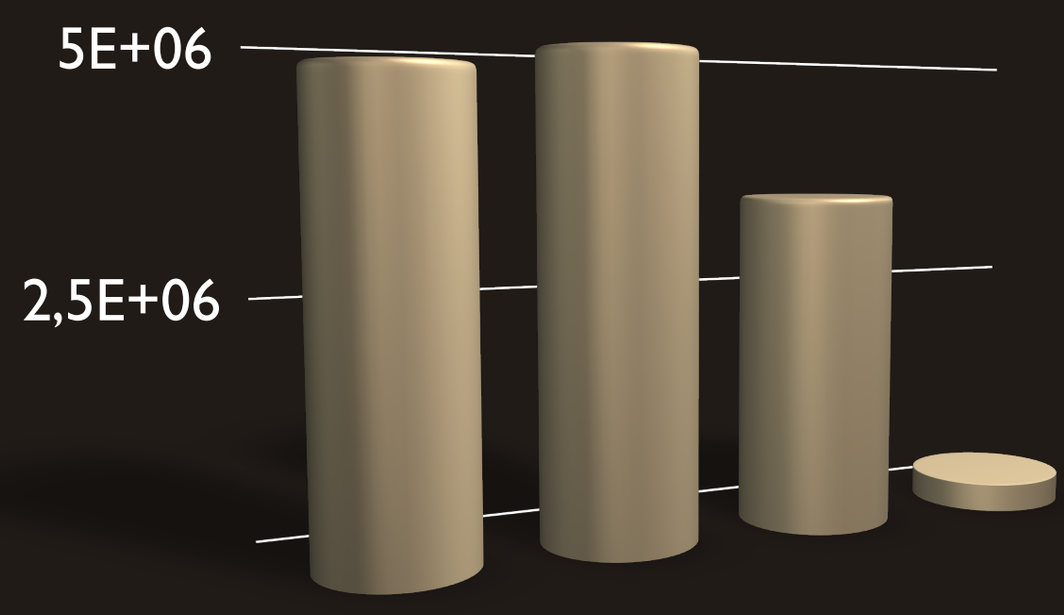
Integer lattice basis reduction

$n = 500$, 10000 bits knapsack

Time spent with the different algorithms or precisions



Contribution to the reduction
Lovász tests

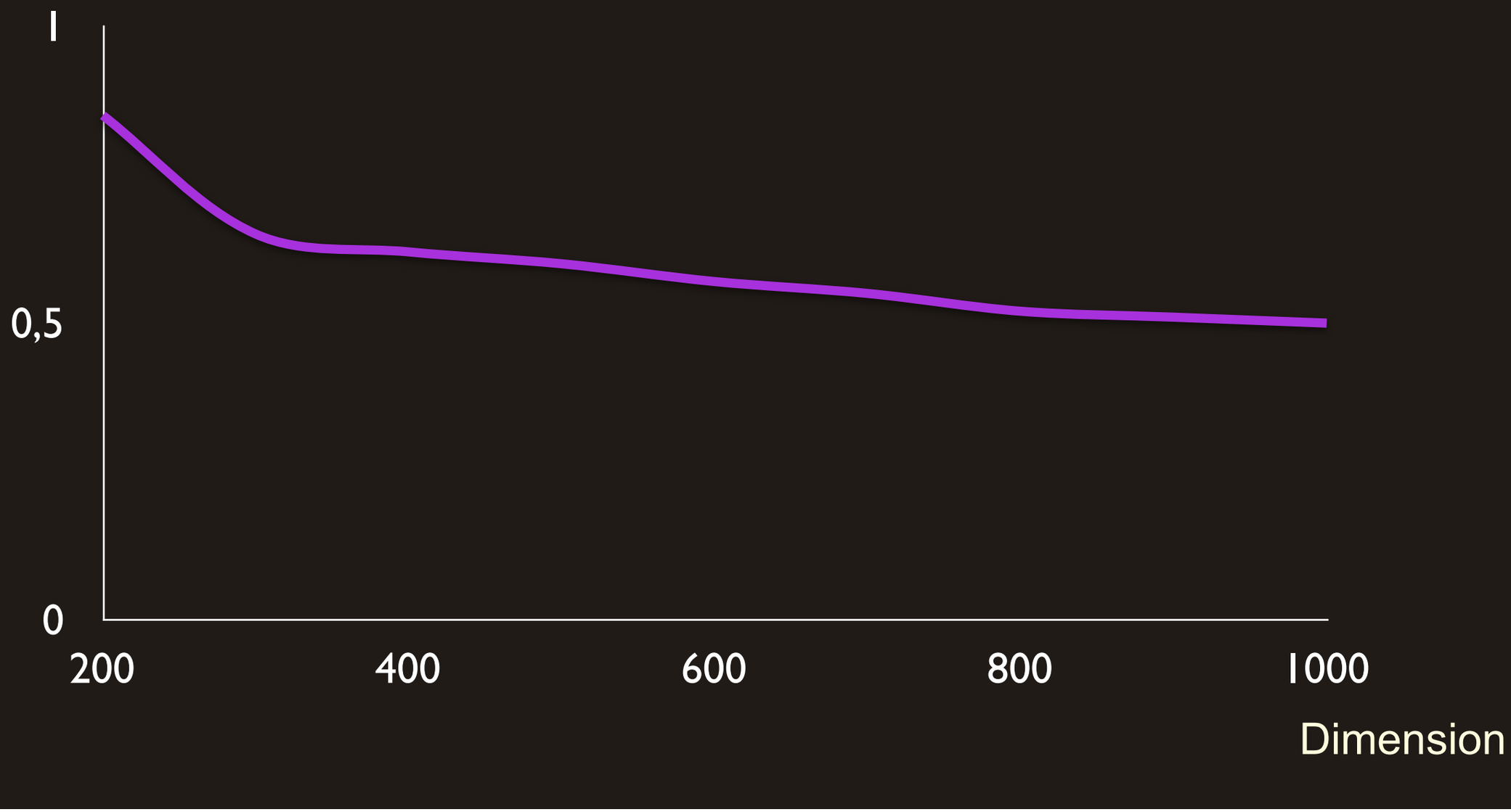


Last 10 years progress

System solution and integer bit size

$$A \approx \begin{bmatrix} 18 & 71 & \dots \\ -63 & -76 & \dots \\ \vdots & \vdots & \ddots \end{bmatrix} \in \mathbb{Z}^{1000\times 1000} \qquad \text{output sizes} \approx 3000 \text{ bits}$$

Time ratio
Ax=b solution / matrix product



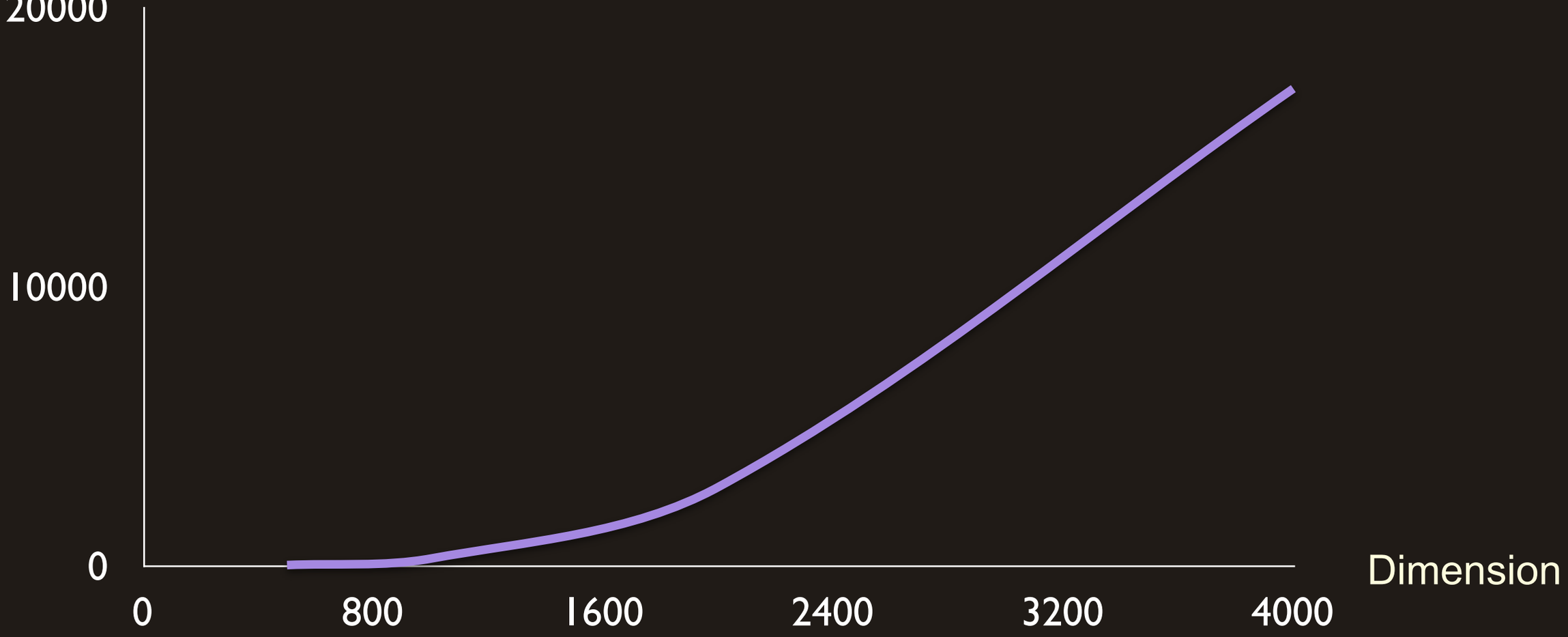
Integer Hermite normal form

(random matrices)

[Micciancio, Warinschi 2001]
[Pernet, Stein 2009]

Sage

n	8 bits	32 bits	128 bits	256 bits	512 bits
50	0.1–0.1	0.2–0.2	0.7–0.8	2.7–2.9	12.45
250	4.1–5.4	6.6–7.1	33.6–37.0	102.8–110.7	470.22
500	24.8–26.6	38.8–43.5	179.4–187.2	534.7–566.1	2169.41
1000	164.9–191.1	266.3–282.8	1081.4–1143.0	2804.9–3149.9	10506
2000	1500.4	2837.5			
4000	11537.3	17105.9			



Integer Hermite normal form

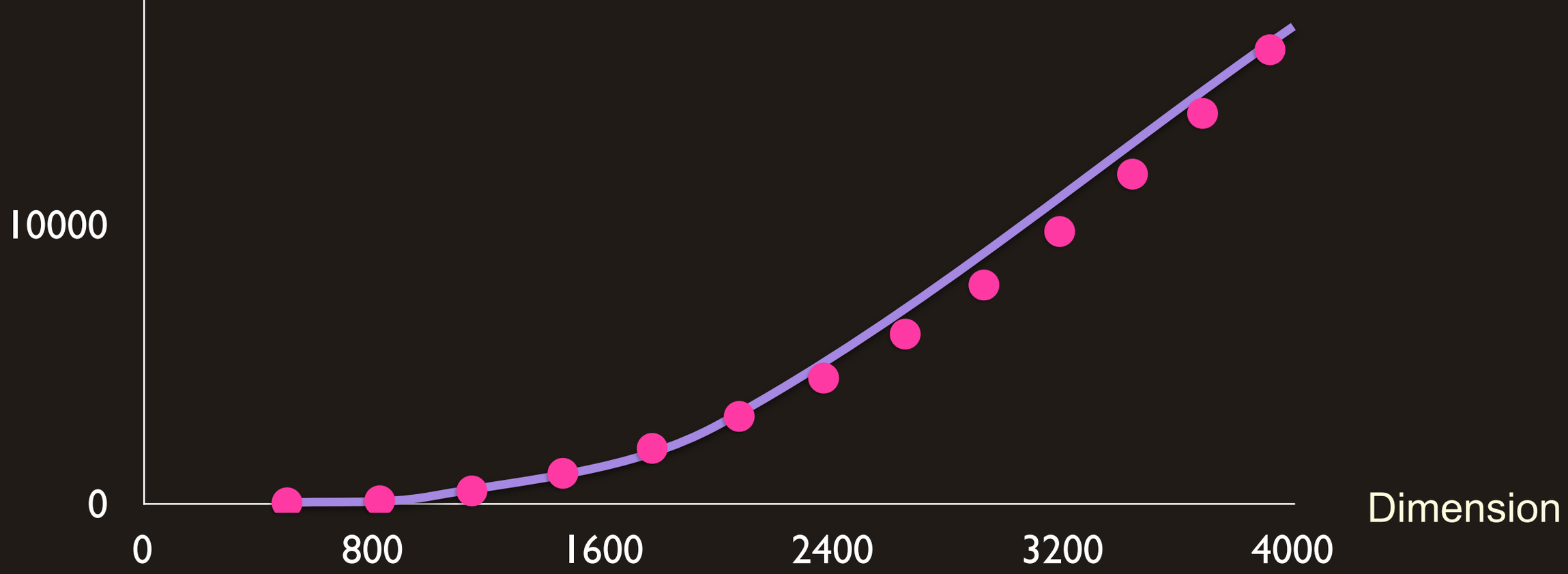
(random matrices)

[Micciancio, Warinschi 2001]
[Pernet, Stein 2009]

Sage

n	8 bits	32 bits	128 bits	256 bits	512 bits
50	0.1–0.1	0.2–0.2	0.7–0.8	2.7–2.9	12.45
250	4.1–5.4	6.6–7.1	33.6–37.0	102.8–110.7	470.22
500	24.8–26.6	38.8–43.5	179.4–187.2	534.7–566.1	2169.41
1000	164.9–191.1	266.3–282.8	1081.4–1143.0	2804.9–3149.9	10506
2000	1500.4	2837.5			
4000	11537.3	17105.9			

“A few linear system solutions”



Talk

Basic complexity bounds

Knuth-Schönhage approach

Essentially optimal matrix inversion

Polynomial lattice reduction

Integer lattice reduction

Ratio w.r.t $O^{\sim}(\mathsf{MM}(n)\log\|A\|)$ + output size	1	$n^{0.323}$	$\mathrm{cond}(A)$	n	$> n$
Ax=b					
Determinant Smith form					
Inversion					
Characteristic polynomial					
Hermite form					
Lattice reduction					

Ratio w.r.t $O^{\sim}(\mathsf{MM}(n)\log\|A\|)$ + output size	1	$n^{0.323}$	$\mathrm{cond}(A)$	n	$> n$
Ax=b	K$[x]$ $\mathbb{Z}$ 2003, 2005				
Determinant Smith form	K$[x]$ $\mathbb{Z}$ 2003, 2005				
Inversion					
Characteristic polynomial					
Hermite form					
Lattice reduction					

Ratio w.r.t $O^{\sim}(\mathsf{MM}(n)\log\|A\|)$ + output size	1	$n^{0.323}$	$\mathrm{cond}(A)$	n	$> n$
Ax=b	$\mathsf{K}[x]$ $\mathbb{Z}$ 2003, 2005				
Determinant **Smith form**	$\mathsf{K}[x]$ $\mathbb{Z}$ 2003, 2005				
Inversion	$\mathsf{K}[x]$ (2005) 2008		$\mathbb{Z}$ 2008		
Characteristic polynomial		$\mathsf{K}[x]$ $\mathbb{Z}$ 2005			
Hermite form					
Lattice reduction					

Ratio w.r.t $O^{\sim}(\mathsf{MM}(n)\log\|A\|)$ + output size	1	$n^{0.323}$	$\mathrm{cond}(A)$	n	$> n$
Ax=b	$\mathsf{K}[x]$ $\mathbb{Z}$ 2003, 2005				
Determinant Smith form	$\mathsf{K}[x]$ $\mathbb{Z}$ 2003, 2005				
Inversion	$\mathsf{K}[x]$ (2005) 2008		$\mathbb{Z}$ 2008		
Characteristic polynomial		$\mathsf{K}[x]$ $\mathbb{Z}$ 2005			
Hermite form	$\mathsf{K}[x]$ 2011			$\mathbb{Z}$ 1991, 1996	
Lattice reduction	$\mathsf{K}[x]$ 2003				$\mathbb{Z}$

Linear system solution

$A \in \mathbb{Z}^{n \times n}$

[Storjohann 2003-2005]

[Moenck, Carter 1979]

$$\mathbb{Z}: \quad O^{\sim}(\mathsf{MM}(n) \log \|A\|)$$

$$\mathsf{K}[x]: \quad O^{\sim}(\mathsf{MM}(n)d)$$

Hint: iterative refinement, high order lifting, doubling argument

→ Diophantine linear systems

[Giesbrecht 1997] [Mulders & Storjohann 1999]

→ Hermite normal form of a random matrix

[Storjohann 1996] [Micciancio, Warinschi 2001] [Pernet, Stein 2009]

Matrix determinant

$A \in \mathbb{Z}^{n \times n}$

[Eberly, Giesbrecht, V. 2000]

[Storjohann 2003, 2005]

$$\mathbb{Z}: \quad O^{\sim}(\mathsf{MM}(n) \log \|A\|)$$

$$\mathsf{K}[x]: \quad O^{\sim}(\mathsf{MM}(n)d)$$

Hint: via the Smith form
Cramer's rule
successive deflations
high order lifting

Matrix determinant

$A \in \mathbb{Z}^{n \times n}$

$$Ax = b$$

$$x_i = \frac{p_i}{q_i} \qquad q_i \approx s_n$$ the largest invariant factor of *A*

$$U \begin{bmatrix} 1570 & 1744 & -1450 & -306 & -4216 & 2220 \\ -884 & 16502 & 18222 & 9044 & -6318 & -1112 \\ 424 & 574 & -410 & 0 & -1198 & 724 \\ 640 & -25452 & -26672 & -13644 & 11160 & 612 \\ -134 & 8572 & 8810 & 4714 & -3844 & 4 \\ -348 & -408 & 328 & 116 & 980 & -488 \end{bmatrix} \quad V = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 124 & 0 & 0 \\ 0 & 0 & 0 & 0 & 124 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4340 \end{bmatrix}$$

Matrix determinant

$A \in \mathbb{Z}^{n \times n}$

$$Ax = b$$

$$x_i = \frac{p_i}{q_i} \qquad q_i \approx s_n$$ the largest invariant factor of *A*

$$U \begin{bmatrix} 1570 & 1744 & -1450 & -306 & -4216 & 2220 \\ -884 & 16502 & 18222 & 9044 & -6318 & -1112 \\ 424 & 574 & -410 & 0 & -1198 & 724 \\ 640 & -25452 & -26672 & -13644 & 11160 & 612 \\ -134 & 8572 & 8810 & 4714 & -3844 & 4 \\ -348 & -408 & 328 & 116 & 980 & -488 \end{bmatrix} \quad V = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 124 & 0 & 0 \\ 0 & 0 & 0 & 0 & 124 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4340 \end{bmatrix}$$

Matrix determinant

$A \in \mathbb{Z}^{n \times n}$

$$Ax = b$$

$$x_i = \frac{p_i}{q_i} \qquad q_i \approx s_n$$ the largest invariant factor of *A*

$$U \begin{bmatrix} 1570 & 1744 & -1450 & -306 & -4216 & 2220 \\ -884 & 16502 & 18222 & 9044 & -6318 & -1112 \\ 424 & 574 & -410 & 0 & -1198 & 724 \\ 640 & -25452 & -26672 & -13644 & 11160 & 612 \\ -134 & 8572 & 8810 & 4714 & -3844 & 4 \\ -348 & -408 & 328 & 116 & 980 & -488 \end{bmatrix} \quad V = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 124 & 0 & 0 \\ 0 & 0 & 0 & 0 & 124 & 0 \\ 0 & 0 & 0 & 0 & 0 & \end{bmatrix}$$

Matrix determinant

$A \in \mathbb{Z}^{n \times n}$

$$Ax = b$$

$$x_i = \frac{p_i}{q_i} \qquad q_i \approx s_n$$ the largest invariant factor of *A*

$$U \begin{bmatrix} 1570 & 1744 & -1450 & -306 & -4216 & 2220 \\ -884 & 16502 & 18222 & 9044 & -6318 & -1112 \\ 424 & 574 & -410 & 0 & -1198 & 724 \\ 640 & -25452 & -26672 & -13644 & 11160 & 612 \\ -134 & 8572 & 8810 & 4714 & -3844 & 4 \\ -348 & -408 & 328 & 116 & 980 & -488 \end{bmatrix} \quad V = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Talk

Basic complexity bounds

Knuth-Schönhage approach

Essentially optimal matrix inversion

Polynomial lattice reduction

Integer lattice reduction

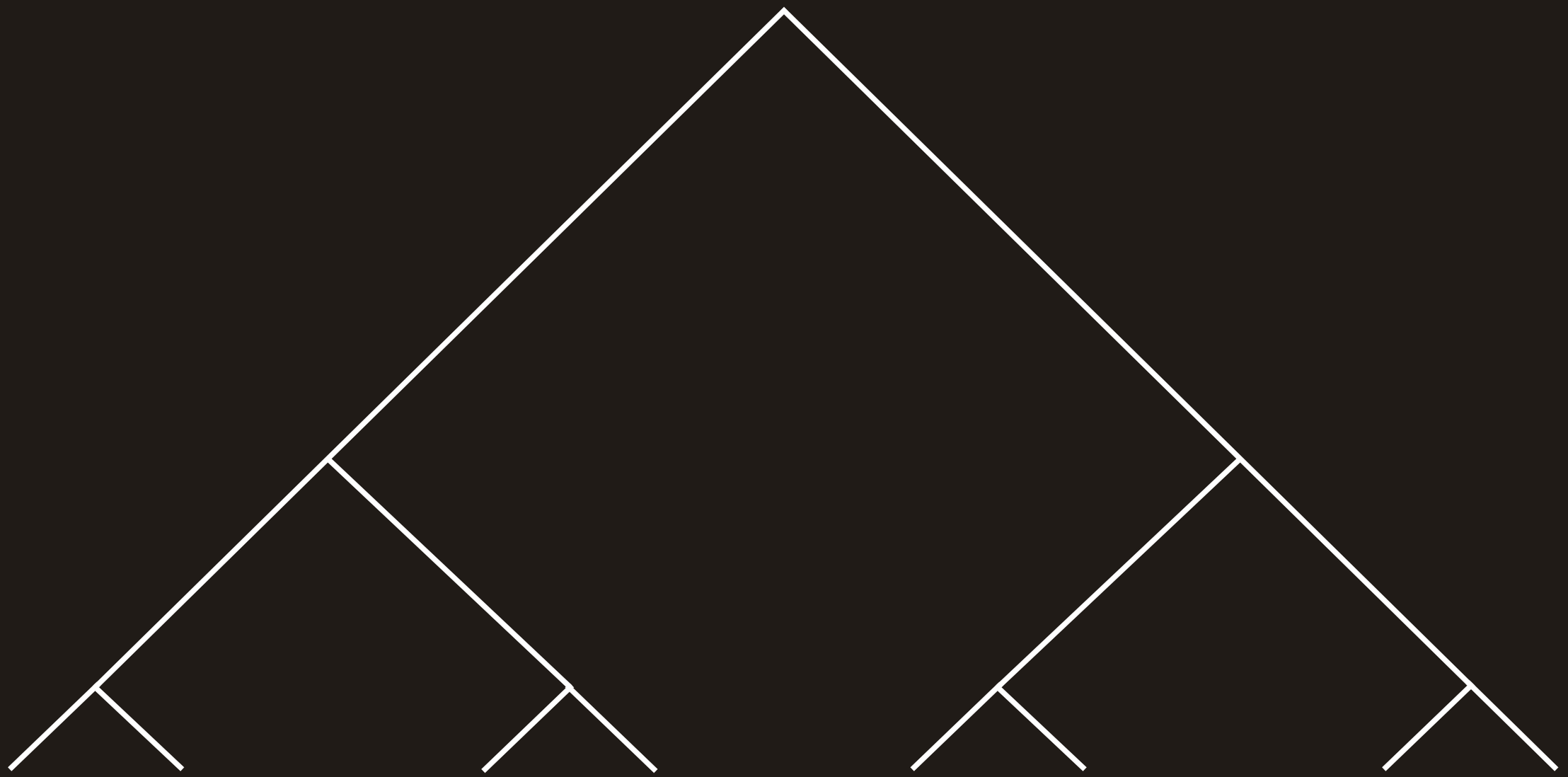
Knuth-Schönhage

[Knuth 1970] [Schönhage 1971] [Moenck 1973]

Recursive tree

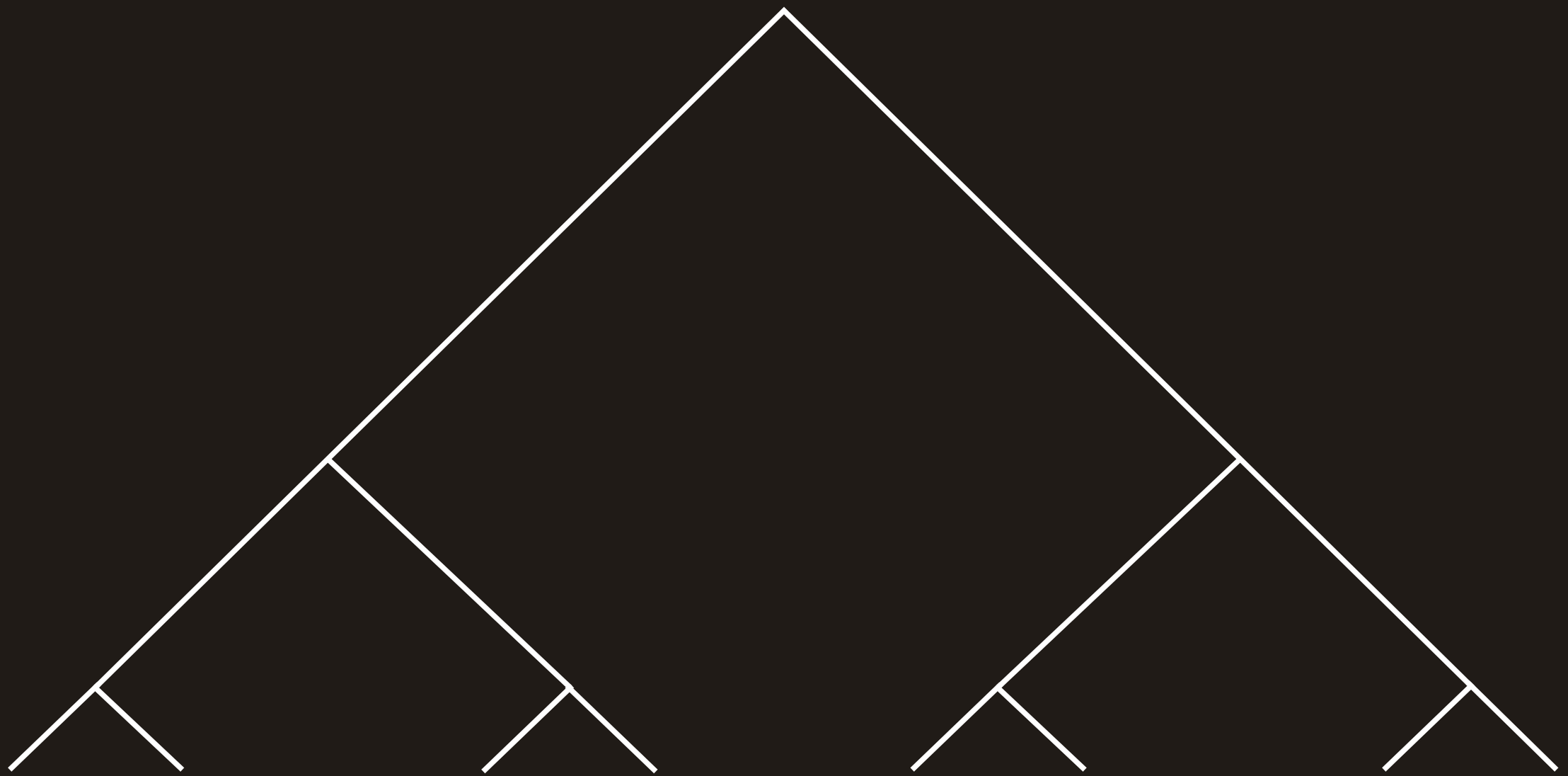
Knuth-Schönhage

$$\mathrm{EEA}(432332445675543199864 53, 7644354322788765567 77)$$

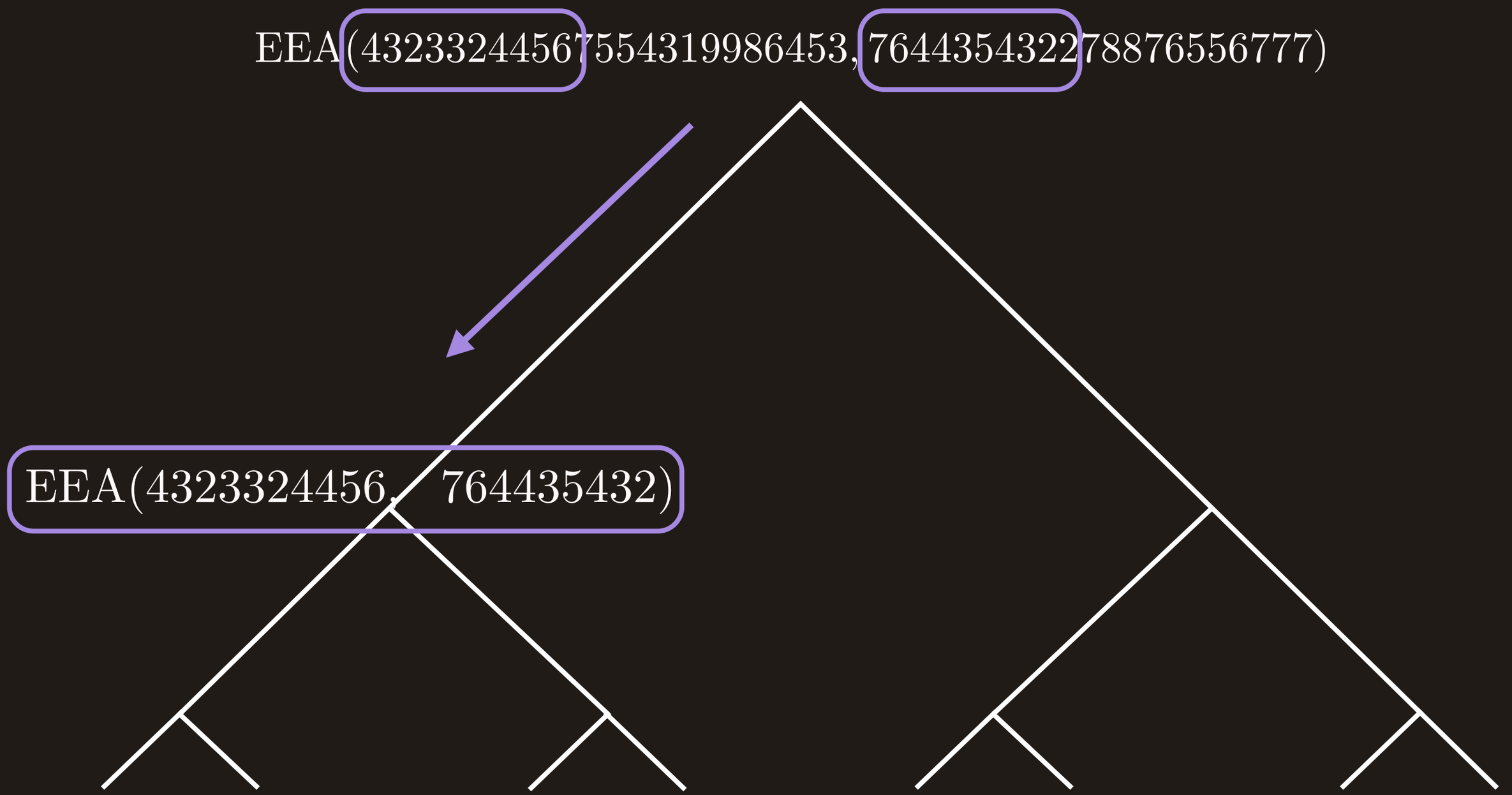


Knuth-Schönhage

$$\mathrm{EEA}(432332445675543199864 53, 7644354322788765567 77)$$



Knuth-Schönhage



Knuth-Schönhage

Gcd operations on β bits integers: $\boxed{\mathrm{M}(\beta)\log\beta}$

Minimal approximant bases

[Beckermann, Labahn 1994]

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

Minimal approximant bases

[Beckermann, Labahn 1994]

$$\begin{bmatrix} . & . & . \\ . & . & . \\ . & . & . \end{bmatrix} \begin{bmatrix} -x+x^2+x^3+x^4 & x^3 \\ 1+x-x^2+x^3 & -1-x-x^4 \\ 1-x+x^4 & 1-x+x^2+x^4-x^3 \end{bmatrix} \equiv 0 \bmod x^4$$

$$N(x)A(x) \equiv 0 \bmod x^d \ ?$$

$$\begin{bmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{bmatrix} \begin{bmatrix} -x+x^2+x^3+x^4 & x^3 \\ 1+x-x^2+x^3 & -1-x-x^4 \\ 1-x+x^4 & 1-x+x^2+x^4-x^3 \end{bmatrix} \equiv 0 \bmod x^4$$

?

$A(x)$

$N(x)A(x) \equiv 0 \bmod x^d$

First consider the lowest order terms

$$\begin{bmatrix} . & . & . \\ . & . & . \\ . & . & . \end{bmatrix} \begin{bmatrix} -x + x^2 + x^3 + x^4 & x^3 \\ 1 + x - x^2 + x^3 & -1 - x - x^4 \\ 1 - x + x^4 & 1 - x + x^2 + x^4 - x^3 \end{bmatrix} \equiv 0 \bmod x^4$$

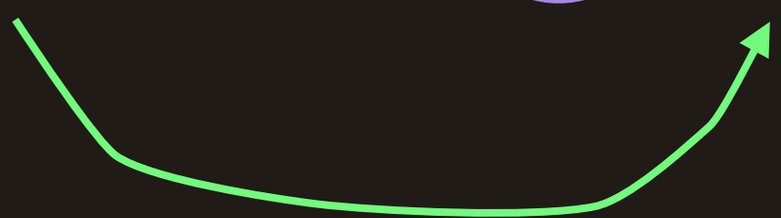
?

$A(x)$

$N(x)A(x) \equiv 0 \bmod x^d$

$$\begin{bmatrix} -x & 0 & 0 \\ 0 & -x^2 & 0 \\ 1 & -x & -x \end{bmatrix} \begin{bmatrix} x^2 - x & 0 \\ 1 - x^2 + x & -1 - x \\ 1 - x & 1 + x^2 - x \end{bmatrix} \equiv 0 \bmod x^2$$

$A(x)$ $\qquad$ $N_1(x)\tilde{A}(x) \equiv x^{d/2} R(x)$



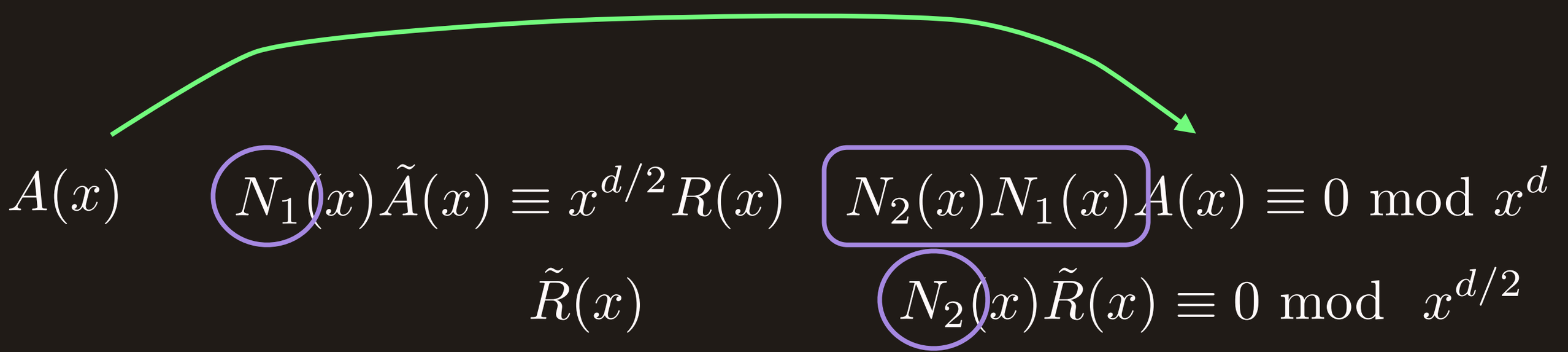
Restart from the truncated residue

$$N_2 = \begin{bmatrix} -x^2 & 0 & 0 \\ x & 1-x & 1 \\ -x & -1 & -1-x \end{bmatrix}$$

$A(x)$ $\quad N_1(x)\tilde{A}(x) \equiv x^{d/2} R(x)$

$\tilde{R}(x)$ $\quad N_2(x)\tilde{R}(x) \equiv 0 \mod x^{d/2}$

$$\begin{bmatrix} x^3 & 0 & 0 \\ 1-x^2 & x^3-x^2-x & -x \\ -1+x^2-x & -x^2+x & x^2+x \end{bmatrix} \quad A(x) \quad \equiv 0 \bmod x^4$$



Minimal approximant bases $\approx$ matrix product

$$N(x)A(x) \equiv 0 \bmod x^d$$

$\log d$ steps

One matrix product of degree d

Two matrix products of degree $d/2$

...

d constant matrix products

$$O^{\sim}(\mathsf{MM}(n,d))$$

[Beckermann, Labahn 1994]

[Giorgi, Jeannerod, V. 2003]

Talk

Basic complexity bounds

Knuth-Schönhage approach

Essentially optimal matrix inversion

Polynomial lattice reduction

Integer lattice reduction

```
> A:=RandomMatrix(9,9);
```

$$A := \begin{bmatrix} 34 & -53 & -41 & 42 & -23 & -74 & -42 & -10 & 56 \\ 33 & -40 & -33 & 89 & -8 & -81 & -89 & 93 & -99 \\ -64 & -1 & -30 & 55 & -36 & -70 & 80 & -59 & 66 \\ -55 & -14 & 14 & -87 & 9 & 27 & 25 & -84 & 9 \\ -29 & -77 & -10 & 25 & 61 & 34 & 93 & 54 & 62 \\ -76 & -56 & -40 & 94 & -67 & 67 & 29 & -42 & 8 \\ 3 & -37 & -73 & -13 & -58 & 48 & -94 & 82 & 48 \\ 53 & 58 & 26 & -82 & -93 & 43 & 50 & 60 & 46 \\ -33 & -35 & -76 & 72 & 64 & 82 & 77 & -91 & 78 \end{bmatrix}$$

```
> B:=1/A;
```

$$B := \begin{bmatrix} \frac{718867779677771}{9497658035230014 8} & \frac{370831999591585}{9497658035230014 8} & -\frac{309014794005279}{4748829017615007 4} & \frac{110101829987455}{9497658035230014 8} & -\frac{31943361748978}{2374414508807503 7} & -\frac{47987727329019}{9497658035230014 8} & -\frac{134522949617691}{2374414508807503 7} & \frac{674027869533223}{9497658035230014 8} & \frac{504920365344469}{9497658035230014 8} \\ -\frac{51070303483007363}{6363430883604109916} & -\frac{20768241926457653}{6363430883604109916} & \frac{17634479026829359}{3181715441802054958} & -\frac{46555916660652219}{6363430883604109916} & -\frac{7997668680155107}{1590857720901027479} & -\frac{27072059120180677}{6363430883604109916} & \frac{5155810892969874}{1590857720901027479} & -\frac{12202076902782199}{6363430883604109916} & \frac{8545015569886879}{6363430883604109916} \\ \frac{7297027484998171}{1590857720901027479} & -\frac{21755927430190784}{1590857720901027479} & -\frac{8654641928475533}{1590857720901027479} & -\frac{15390411887609778}{1590857720901027479} & \frac{4949823496906637}{1590857720901027479} & \frac{10500794672814898}{1590857720901027479} & -\frac{6697258494484534}{1590857720901027479} & -\frac{10792689242824076}{1590857720901027479} & -\frac{18278379253416379}{1590857720901027479} \\ \frac{1103466647353453}{1590857720901027479} & -\frac{7676207005015613}{1590857720901027479} & -\frac{1105366422013129}{1590857720901027479} & -\frac{15593232730339549}{1590857720901027479} & -\frac{810000743524982}{1590857720901027479} & -\frac{6466422855851044}{1590857720901027479} & -\frac{2542356795219104}{1590857720901027479} & -\frac{6119360796657798}{1590857720901027479} & -\frac{2646576426332056}{1590857720901027479} \\ -\frac{16734410381339997}{6363430883604109916} & -\frac{10797479249553819}{6363430883604109916} & -\frac{959655585334793}{3181715441802054958} & -\frac{13576202591225725}{6363430883604109916} & -\frac{2781878616003364}{1590857720901027479} & -\frac{30859830715258307}{6363430883604109916} & -\frac{1497372714984050}{1590857720901027479} & -\frac{30973807044462049}{6363430883604109916} & -\frac{10401400101999805}{6363430883604109916} \\ -\frac{2437697568135695}{1590857720901027479} & -\frac{4588032906688828}{1590857720901027479} & -\frac{7868542124985355}{1590857720901027479} & -\frac{3564855319079428}{1590857720901027479} & -\frac{458030332293138}{1590857720901027479} & -\frac{5595484148434489}{1590857720901027479} & -\frac{901428018815201}{1590857720901027479} & -\frac{2421583422211146}{1590857720901027479} & -\frac{2088839268507045}{1590857720901027479} \\ -\frac{9365189585916853}{6363430883604109916} & -\frac{46583341843460593}{6363430883604109916} & -\frac{6770319170809549}{3181715441802054958} & -\frac{33035115806165079}{6363430883604109916} & -\frac{3831360618558680}{1590857720901027479} & -\frac{5978328647990119}{6363430883604109916} & -\frac{6610373772075073}{1590857720901027479} & -\frac{46347817219431339}{6363430883604109916} & -\frac{27949290441506885}{6363430883604109916} \\ -\frac{28053732991686229}{6363430883604109916} & -\frac{3963459546062293}{6363430883604109916} & -\frac{7242872810696229}{3181715441802054958} & -\frac{20054906889676997}{6363430883604109916} & -\frac{5950185181054409}{1590857720901027479} & -\frac{11267978124870407}{6363430883604109916} & -\frac{5599359176716554}{1590857720901027479} & -\frac{1721034525794485}{6363430883604109916} & -\frac{15302371539176611}{6363430883604109916} \\ -\frac{22323730289620027}{6363430883604109916} & -\frac{68466183019896695}{6363430883604109916} & -\frac{3426768764295023}{3181715441802054958} & -\frac{50056500744294437}{6363430883604109916} & -\frac{2435023106885114}{1590857720901027479} & -\frac{1910967623821859}{6363430883604109916} & -\frac{5203496122478757}{1590857720901027479} & -\frac{29203833917781669}{6363430883604109916} & -\frac{24499589571635583}{6363430883604109916} \end{bmatrix}$$

Transference theorem and Kronecker indice
Minimal nullspace basis (generic case)

$$\begin{bmatrix}
x & 0 & -x+1 & x-1 \\
2\,x+2 & 0 & x & -x-1 \\
-2\,x & -x+2 & -2\,x+2 & 2\,x \\
-2\,x-2 & -x+2 & 2\,x+2 & -x-2 \\
-2 & 2\,x+2 & -2\,x-2 & -x \\
-x-2 & -x-1 & -x & 0 \\
x-2 & 2\,x-1 & -2 & 2\,x \\
2\,x-2 & -x+1 & x-1 & -2\,x
\end{bmatrix}$$

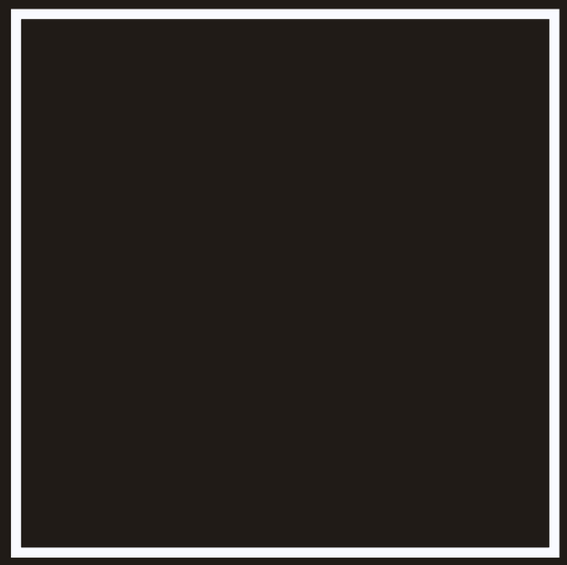
Transference theorem and Kronecker indice
Minimal nullspace basis (generic case)

$$\begin{bmatrix} 2\,x & x & -x+1 & -2\,x & x-2 & -2 & 2 & 2 \\ -1-2\,x & -2\,x-2 & 1-2\,x & x-1 & -1 & x-1 & 0 & 1 \\ -1-2\,x & 2 & -x-2 & -2\,x+2 & 1 & 0 & x-2 & 1 \\ 1 & -2\,x-2 & 1-2\,x & x-2 & -2 & 1 & 2 & x-1 \end{bmatrix} \times \begin{bmatrix} x & 0 & -x+1 & x-1 \\ 2\,x+2 & 0 & x & -x-1 \\ -2\,x & -x+2 & -2\,x+2 & 2\,x \\ -2\,x-2 & -x+2 & 2\,x+2 & -x-2 \\ -2 & 2\,x+2 & -2\,x-2 & -x \\ -x-2 & -x-1 & -x & 0 \\ x-2 & 2\,x-1 & -2 & 2\,x \\ 2\,x-2 & -x+1 & x-1 & -2\,x \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

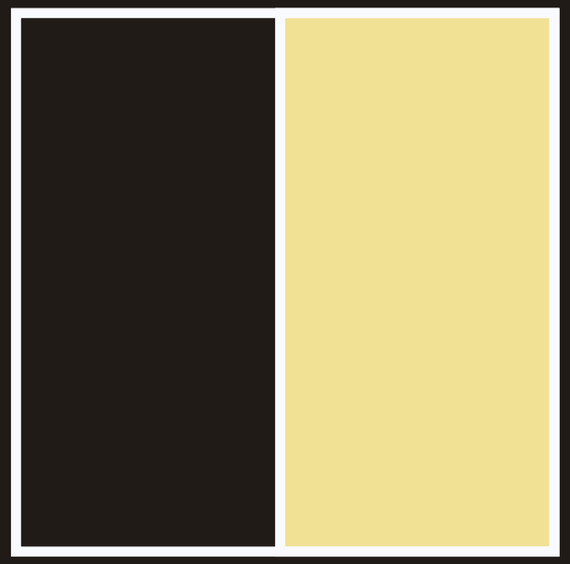
degree $d = 1$

degree $d = 1$

$$A \in \mathsf{K}[x]^{n \times n}$$



$$A \in \mathsf{K}[x]^{n \times n}$$



Minimal approximant bases

→ minimal nullspace basis

$$A \in \mathsf{K}[x]^{n \times n}$$

$$N(x)A_R(x) \equiv 0 \bmod x^{2d+1}$$

$$A \in \mathsf{K}[x]^{n \times n}$$

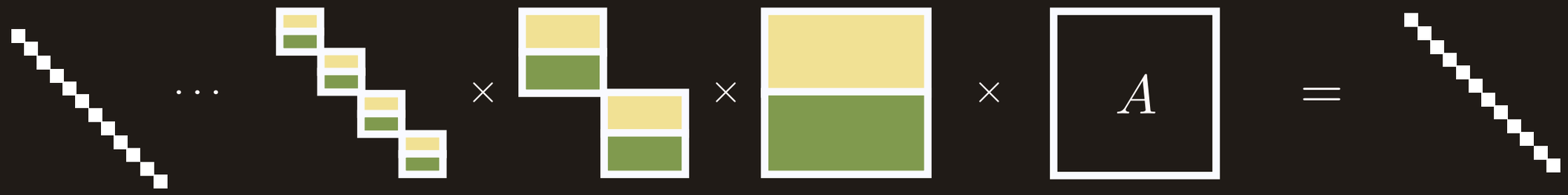
$$A \in \mathsf{K}[x]^{n \times n}$$

Transference theorem

$$A \in \mathsf{K}[x]^{n \times n}$$

degree d degree d degree $2d$

two problems of dimension $n/2$

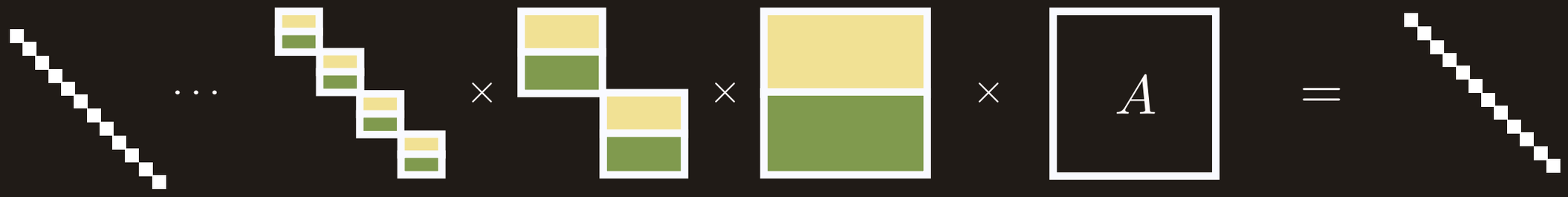


$\log d$ steps

Matrix product $n \times n$ d

Two matrix products $n/2 \times n/2$ $2d$

...



$\log d$ steps

Matrix product $n \times n$ d

Two matrix products $n/2 \times n/2$ $2d$

...

Computing the factorization: $O^{\sim}(\mathsf{MM}(n, d))$

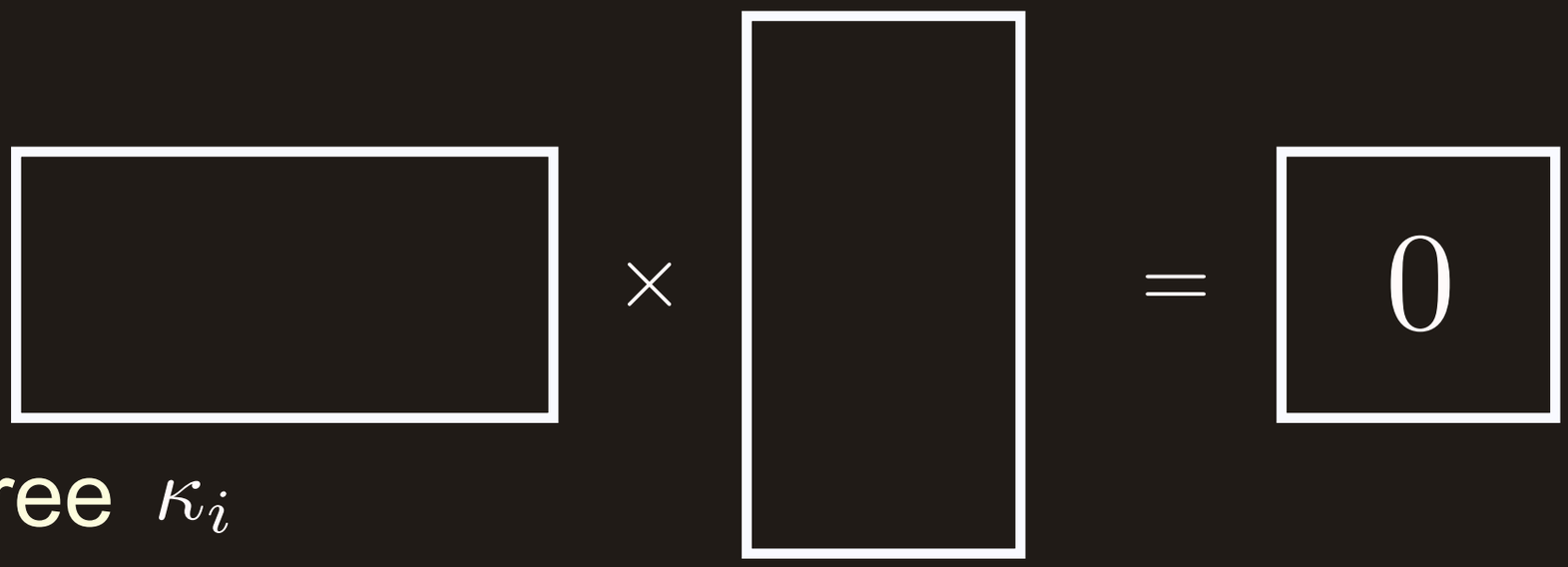
Matrix inversion: $O^{\sim}(n^2 \times nd)$

[Giorgi, Jeannerod, V. 2003]

Non generic minimal nullspace basis

[Zhou, Labahn, Storjohann 2012]

$$A \in \mathsf{K}[x]^{2n \times n}$$



row degree κ_i

$$\sum_{i=1}^{n} \kappa_i = nd$$

degree d

$$O\tilde{}(\mathsf{MM}(n,d))$$

Integer matrix inversion

[Storjohann 2008]

$$A = \begin{bmatrix} -93 & -32 & 8 & 44 \\ -76 & -74 & 69 & 92 \\ -72 & -4 & 99 & -31 \\ -2 & 27 & 29 & 67 \end{bmatrix}$$

$$A^* \equiv \begin{bmatrix} -28408 \\ 861667 \\ 181262 \\ 533666 \end{bmatrix} \begin{bmatrix} -27259506 & 11404741 & -8995165 & 1 \end{bmatrix} \bmod \det(A)$$

$$\equiv \begin{bmatrix} -853217 & 368292 & -179420 & -28408 \\ 409178 & -744548 & 233455 & 861667 \\ -584392 & 295157 & 438250 & 181262 \\ 62584 & 183281 & -289125 & 533666 \end{bmatrix} \bmod 64334045$$

Integer matrix inversion

[Storjohann 2008]

Outer product adjoint formula

$$A^* \equiv \frac{\det A}{s_n} v_n u_n + \frac{\det A}{s_{n-1}} v_{n-1} u_{n-1} + \ldots + \frac{\det A}{s_1} v_1 u_1 \bmod \det A$$

Integer matrix inversion

[Storjohann 2008]

→ "Generic matrix" (small condition number)

$$O^{\sim}(n^3 \log \|A\|)$$ bit operations

→ General case

The determinant should not be too small w.r.t. the adjoint matrix
May be modeled in terms of the condition number $\|A\|\|A^{-1}\|$

$$O^{\sim}(n^3 \log \|A\| + n^3 \log \mathrm{cond}(A))$$ bit operations

Talk

Basic complexity bounds

Knuth-Schönhage approach

Essentially optimal matrix inversion

Polynomial lattice reduction

Integer lattice reduction

$$A \in (\mathbb{Z}/3\mathbb{Z})^{3\times 2}$$

$$\begin{bmatrix} 2\,x^2 & 2\,x^2+1 \\ 2\,x^3+x^2+2\,x+2 & 2\,x^3+x^2+1 \\ 2\,x^2+1 & 2\,x^2+2 \end{bmatrix}$$

$$A \in (\mathbb{Z}/3\mathbb{Z})^{3\times 2}$$

$$\begin{bmatrix} 2\,x^2 & 2\,x^2+1 \\ 2\,x^3+x^2+2\,x+2 & 2\,x^3+x^2+1 \\ 2\,x^2+1 & 2\,x^2+2 \end{bmatrix}$$

Highest column degree dependence

$$A \in (\mathbb{Z}/3\mathbb{Z})^{3\times 2}$$

$$\begin{bmatrix} 2\,x^2 & 2\,x^2+1 \\ 2\,x^3+x^2+2\,x+2 & 2\,x^3+x^2+1 \\ 2\,x^2+1 & 2\,x^2+2 \end{bmatrix}$$

Highest column degree dependence

Unimodular column transformation

$$\begin{bmatrix} 2 & 2\,x^2+1 \\ 2\,x+1 & 2\,x^3+x^2+1 \\ 2 & 2\,x^2+2 \end{bmatrix}$$

$$A \in (\mathbb{Z}/3\mathbb{Z})^{3\times 2}$$

$$\begin{bmatrix} 2\,x^2 & 2\,x^2+1 \\ 2\,x^3+x^2+2\,x+2 & 2\,x^3+x^2+1 \\ 2\,x^2+1 & 2\,x^2+2 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 2\,x^2+1 \\ 2\,x+1 & 2\,x^3+x^2+1 \\ 2 & 2\,x^2+2 \end{bmatrix}$$

$$A \in (\mathbb{Z}/3\mathbb{Z})^{3\times 2}$$

$$\begin{bmatrix} 2\,x^2 & 2\,x^2+1 \\ 2\,x^3+x^2+2\,x+2 & 2\,x^3+x^2+1 \\ 2\,x^2+1 & 2\,x^2+2 \end{bmatrix}$$

↓

$$\begin{bmatrix} 2 & 2\,x^2+1 \\ 2\,x+1 & 2\,x^3+x^2+1 \\ 2 & 2\,x^2+2 \end{bmatrix}$$

↓ Unimodular column transformation

$$\begin{bmatrix} 2 & 1 \\ 2\,x+1 & 1 \\ 2 & 2 \end{bmatrix}$$

Minimal lattice basis

Polynomial basis reduction

Non singular square case

[Giorgi, Jeannerod, V. 2003]

[Gupta, Sarkar, Valeriote, Storjohann 2010]

$A(x)U(x) = R(x)$?

Minimal degrees ?

Polynomial basis reduction

Non singular square case

[Giorgi, Jeannerod, V. 2003]

[Gupta, Sarkar, Valeriote, Storjohann 2010]

$A(x)U(x) = R(x)$? Minimal degrees ?

Phase 1. Translation into a “regular case”: U small

High order lifting

or

Linearization via the Hermite form

Polynomial basis reduction

Non singular square case

[Giorgi, Jeannerod, V. 2003]

[Gupta, Sarkar, Valeriote, Storjohann 2010]

$A(x)U(x) = R(x)$? Minimal degrees ?

Phase 1. Translation into a “regular case”: U small

Phase 2. Solve a minimal approximant problem

Hint: $A(x)U(x) = R(x) \longleftrightarrow [A(x) \ -I] \begin{bmatrix} U(x) \\ R(x) \end{bmatrix} \bmod x^k$

Minimal approximant bases

$$O\tilde{}(\mathrm{MM}(n,d))$$

Polynomial basis reduction

Square case

[Giorgi, Jeannerod, V. 2003]

[Gupta, Sarkar, Valeriote, Storjohann 2010]

Talk

Basic complexity bounds

Knuth-Schönhage approach

Essentially optimal matrix inversion

Polynomial lattice reduction

Integer lattice reduction

$$\begin{bmatrix} 1000000 & 704155 & 495834 & 349144 & 245851 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1000000 & 704155 & 495834 & 349144 & 245851 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Unimodular column operations

$$\begin{bmatrix} 1000000 & 704155 & 495834 & 349144 & 245851 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Unimodular column operations

“Small” norms ?

$$\begin{bmatrix} 1000000 & 704155 & 495834 & 349144 & 245851 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Unimodular column operations

“Small” norms

$$\begin{bmatrix} -2 & 1 & 13 & -16 & 0 \\ 1 & -9 & 4 & 9 & 17 \\ 0 & -10 & 0 & 5 & -24 \\ -12 & 5 & 1 & -5 & 1 \\ 1 & 6 & 5 & 5 & 1 \\ 5 & -1 & -5 & -5 & 3 \end{bmatrix}$$

Towards the integer case

Notion of **elementary step** ? (Order)

Cost in adequation with the actual progress ?
(Degree d for order d, and truncations)

$n \times n$ $\quad \max \log \|A_j\| \leq \beta$

[Lenstra, Lenstra, Lovász 1982]

[Kaltofen 1983]

[Schnorr 1988]

[Schönhage 1984]

[Storjohann 1996] (relaxed)

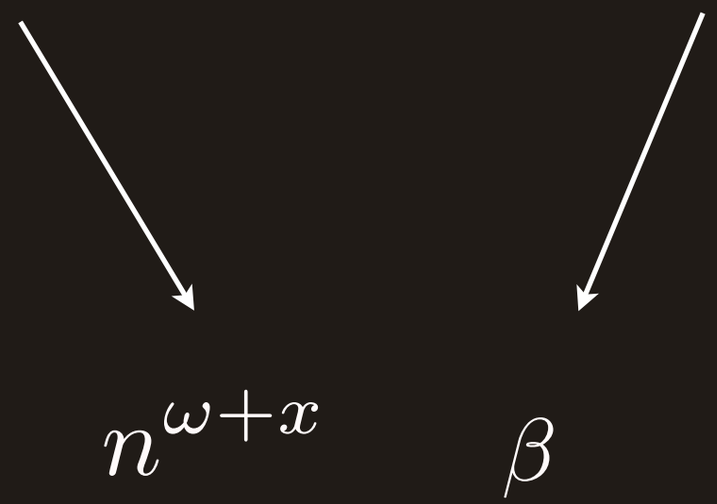
[Schnorr 2006] (relaxed)

[Nguyen, Stehlé 2006]

$$O^{\sim}(n^{3.5}\beta^2)$$

$$O^{\sim}(n^4)\beta(n+\beta)$$

exponent of n exponent of β



$n^{\omega+x}$ $\quad \beta$

[Novocin, Stehlé, V. 2010-2011]

[Hanrot, Pujol, Stehlé, V. 2010-]

$n \times n$ $\quad \max \log \|A_j\| \leq \beta$

[Lenstra, Lenstra, Lovász 1982]

[Kaltofen 1983]

[Schnorr 1988]

[Schönhage 1984]

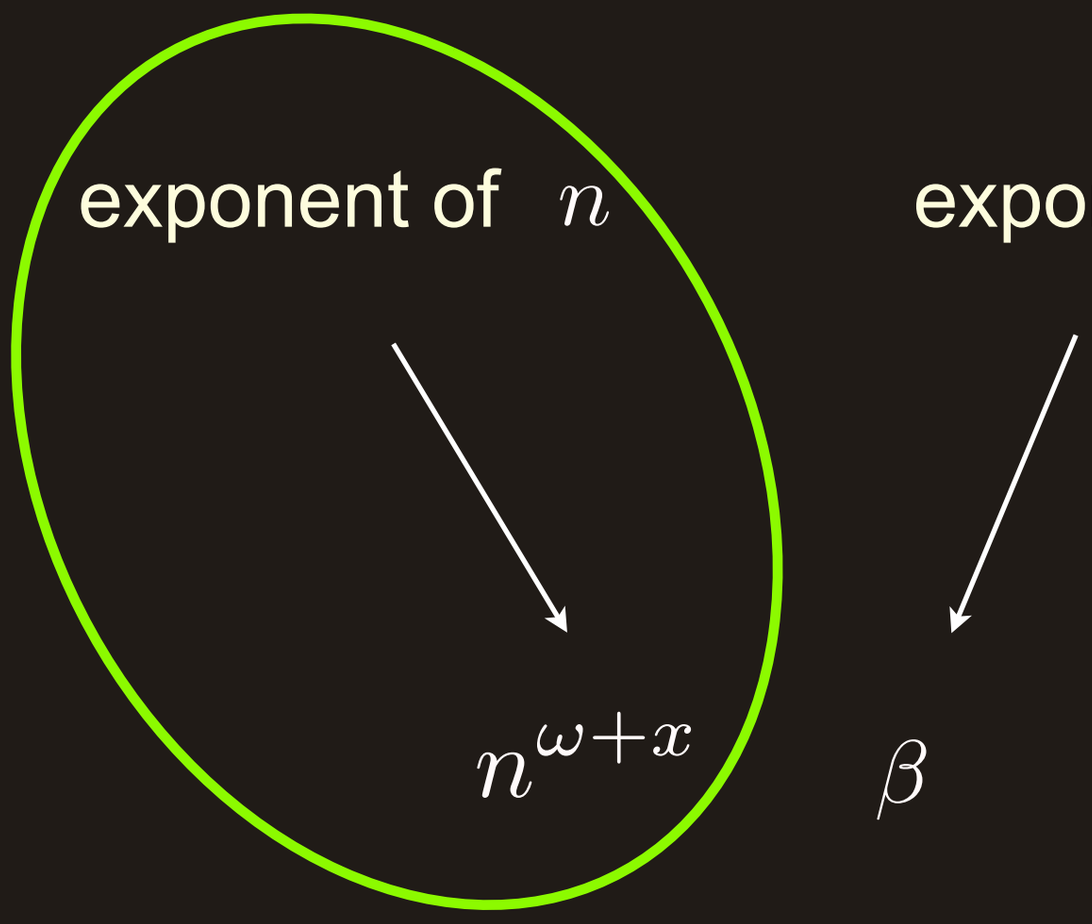
[Storjohann 1996] (relaxed)

[Schnorr 2006] (relaxed)

[Nguyen, Stehlé 2006]

$$O^{\sim}(n^{3.5}\beta^2)$$

$$O^{\sim}(n^4)\beta(n+\beta)$$



[Novocin, Stehlé, V. 2010-2011]

[Hanrot, Pujol, Stehlé, V. 2010-]

LLL basis reduction

Unimodular operations

Orthogonalization

$$
B = \begin{bmatrix}
 & b_i & & \\
829556 & 161099 & 11567 & 521155 \\
769480 & 639201 & 689979 & 53629 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}
$$

Gram-Schmidt orthogonalization

$$b_i^*$$

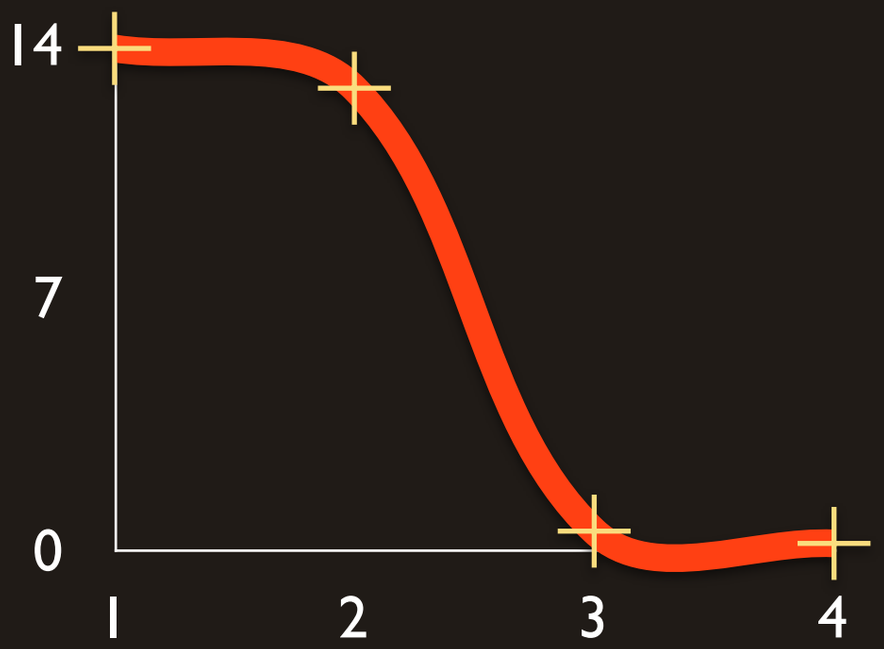
$$R = \begin{bmatrix} -1.13\ 10^6 & -5.52\ 10^5 & -4.77\ 10^5 & -4.18\ 10^5 \\ 0 & -3.59\ 10^5 & -4.97\ 10^5 & 3.15\ 10^5 \\ 0 & 0 & -1.72 & 0.82 \\ 0 & 0 & 0 & 1.31 \end{bmatrix}$$

Gram-Schmidt orthogonalization

b_i^*

$$R = \begin{bmatrix} -1.13\ 10^6 & -5.52\ 10^5 & -4.77\ 10^5 & -4.18\ 10^5 \\ 0 & -3.59\ 10^5 & -4.97\ 10^5 & 3.15\ 10^5 \\ 0 & 0 & -1.72 & 0.82 \\ 0 & 0 & 0 & 1.31 \end{bmatrix}$$

$\log \|b_i^*\|$

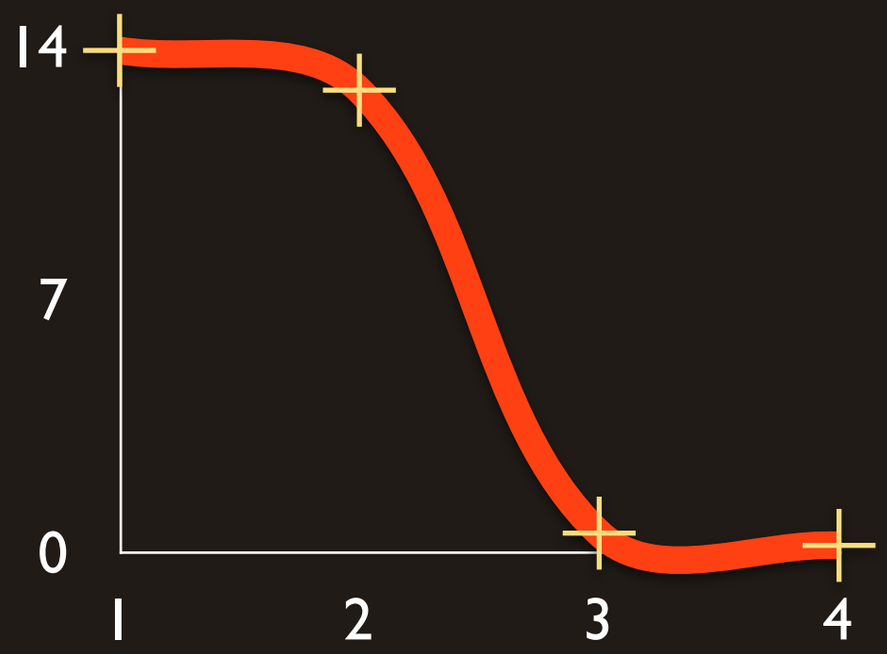


Gram-Schmidt orthogonalization

b_i^*

$$R = \begin{bmatrix} -1.13\ 10^6 & -5.52\ 10^5 & -4.77\ 10^5 & -4.18\ 10^5 \\ 0 & -3.59\ 10^5 & -4.97\ 10^5 & 3.15\ 10^5 \\ 0 & 0 & -1.72 & 0.82 \\ 0 & 0 & 0 & 1.31 \end{bmatrix}$$

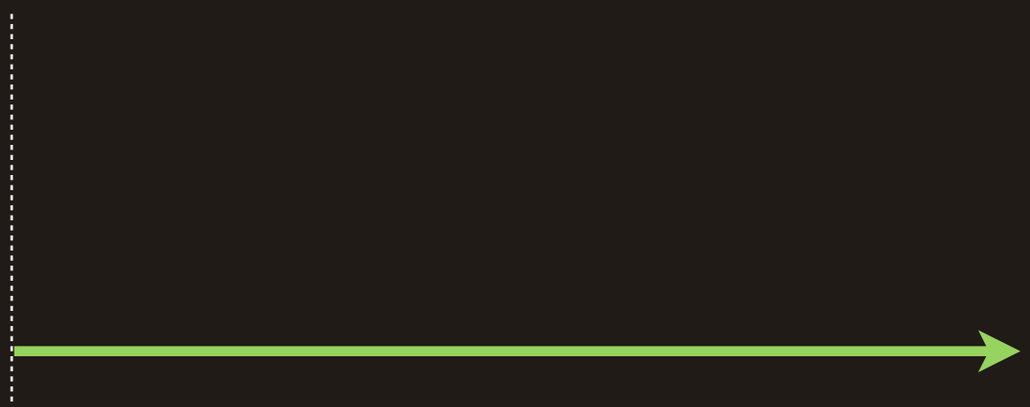
$\log \|b_i^*\|$



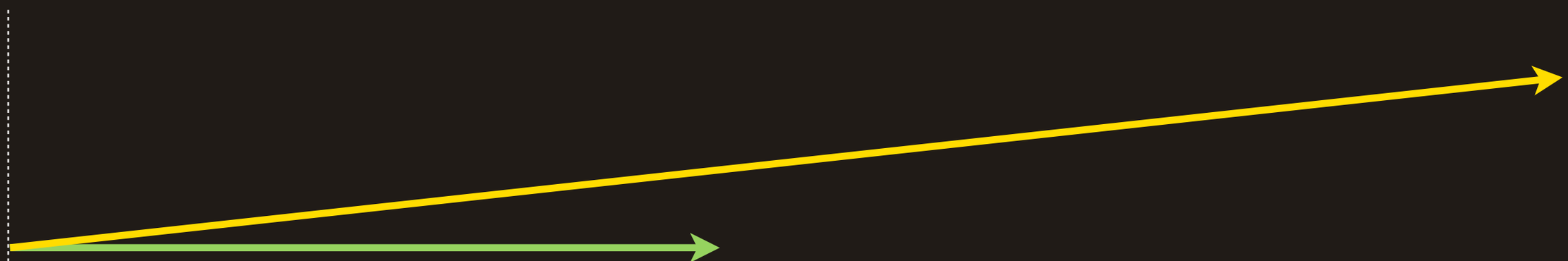
Reduction: application of transformations that one reads on the orthogonalized vectors

$$\begin{bmatrix} 44 & 93 \\ 3 & -4 \\ 1 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 44 & 93 \\ 3 & -4 \\ 1 & 2 \end{bmatrix}$$

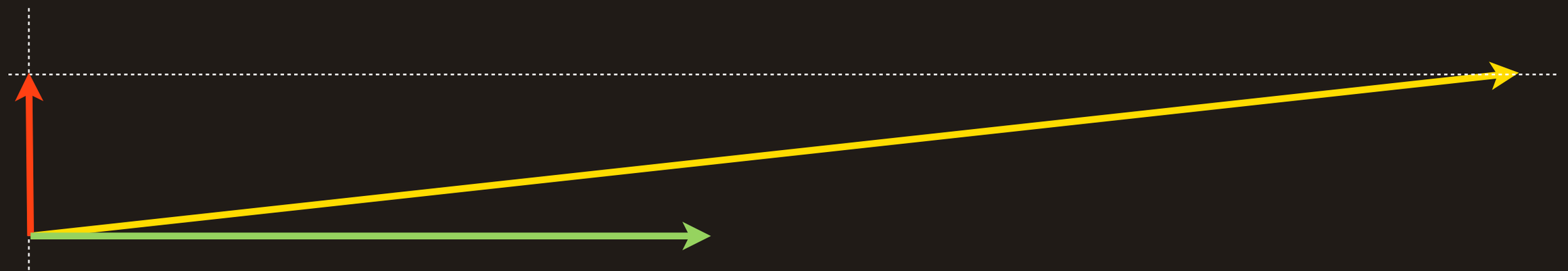


$$\begin{bmatrix} 44 & 93 \\ 3 & -4 \\ 1 & 2 \end{bmatrix}$$



$$\begin{bmatrix} 44 & 93 \\ 3 & -4 \\ 1 & 2 \end{bmatrix}$$

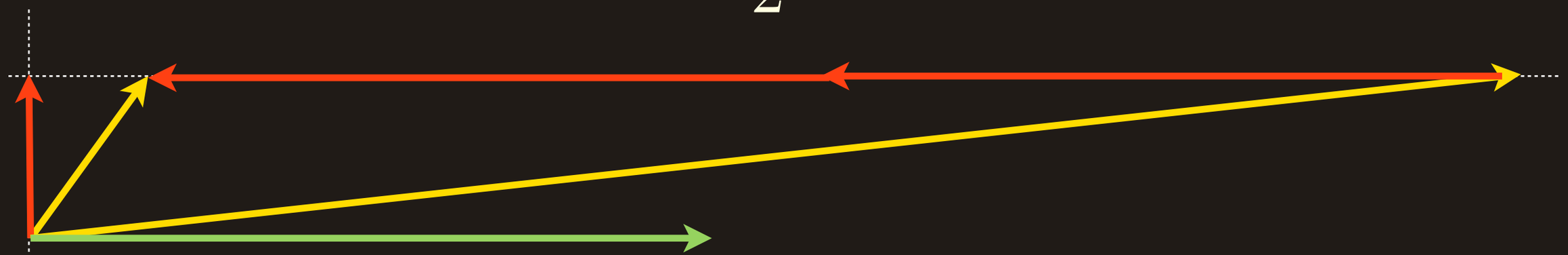
$$\begin{bmatrix} 44.113 & 92.534 \\ 0.0 & 10.317 \end{bmatrix}$$



$$\begin{bmatrix} 44 & 93 \\ 3 & -4 \\ 1 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 44.113 & 92.534 \\ 0.0 & 10.317 \end{bmatrix}$$

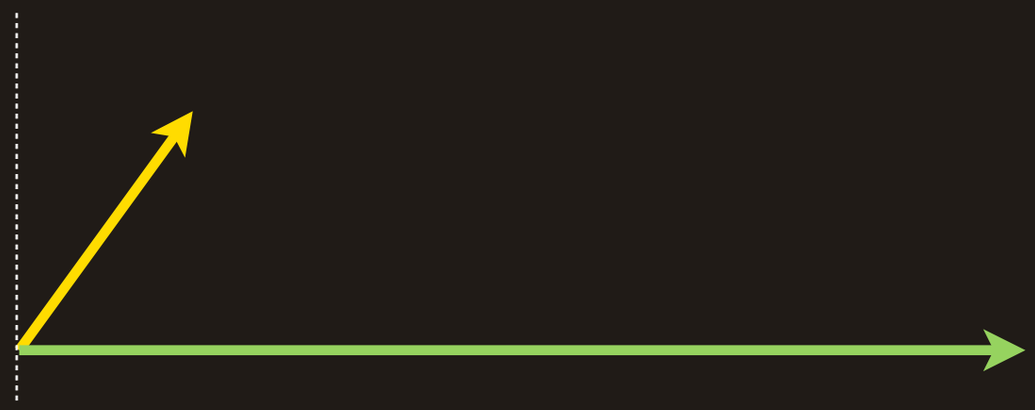
-2



“Quotient” (translation)

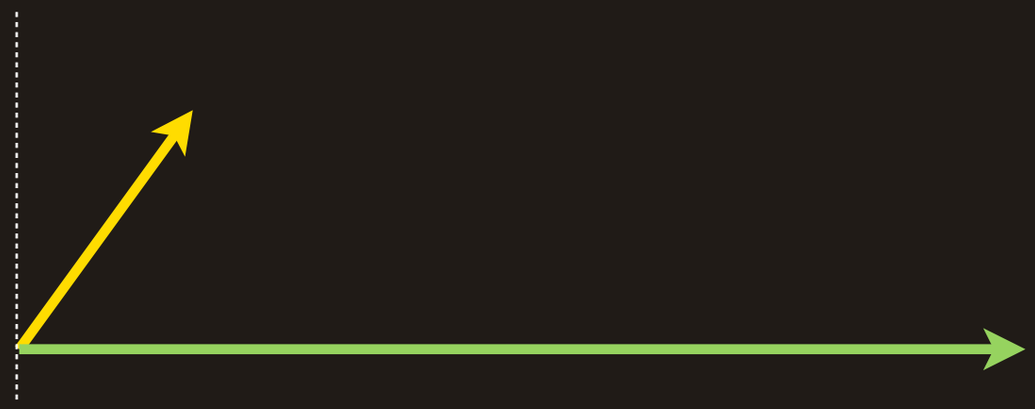
$$\begin{bmatrix} 44 & 5 \\ 3 & -10 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 44.113 & 4.3071 \\ 0.0 & 10.317 \end{bmatrix}$$



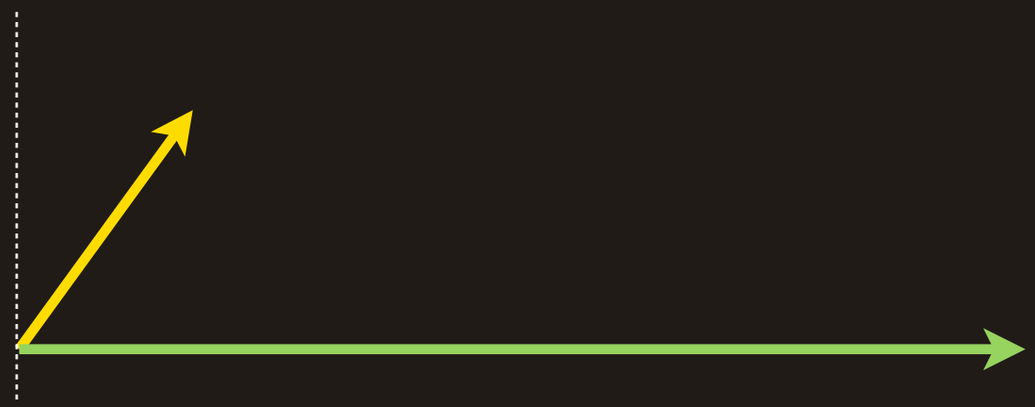
$$\begin{bmatrix} 44 & 5 \\ 3 & -10 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 44.113 & 4.3071 \\ 0.0 & 10.317 \end{bmatrix}$$



$$\begin{bmatrix} 44 & 5 \\ 3 & -10 \\ 1 & 0 \end{bmatrix}$$

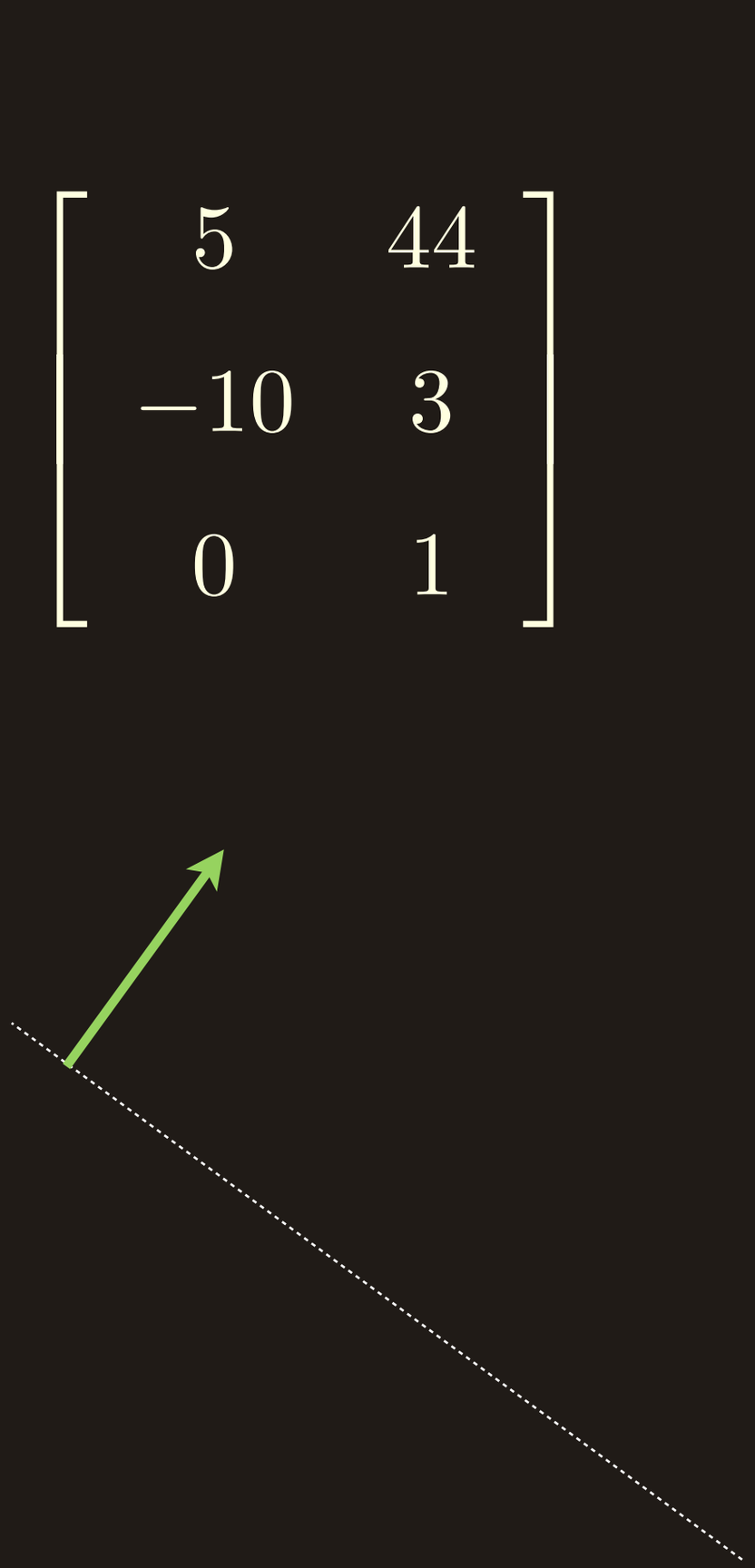
$$\begin{bmatrix} 44.113 & 4.3071 \\ 0.0 & 10.317 \end{bmatrix}$$



Swap

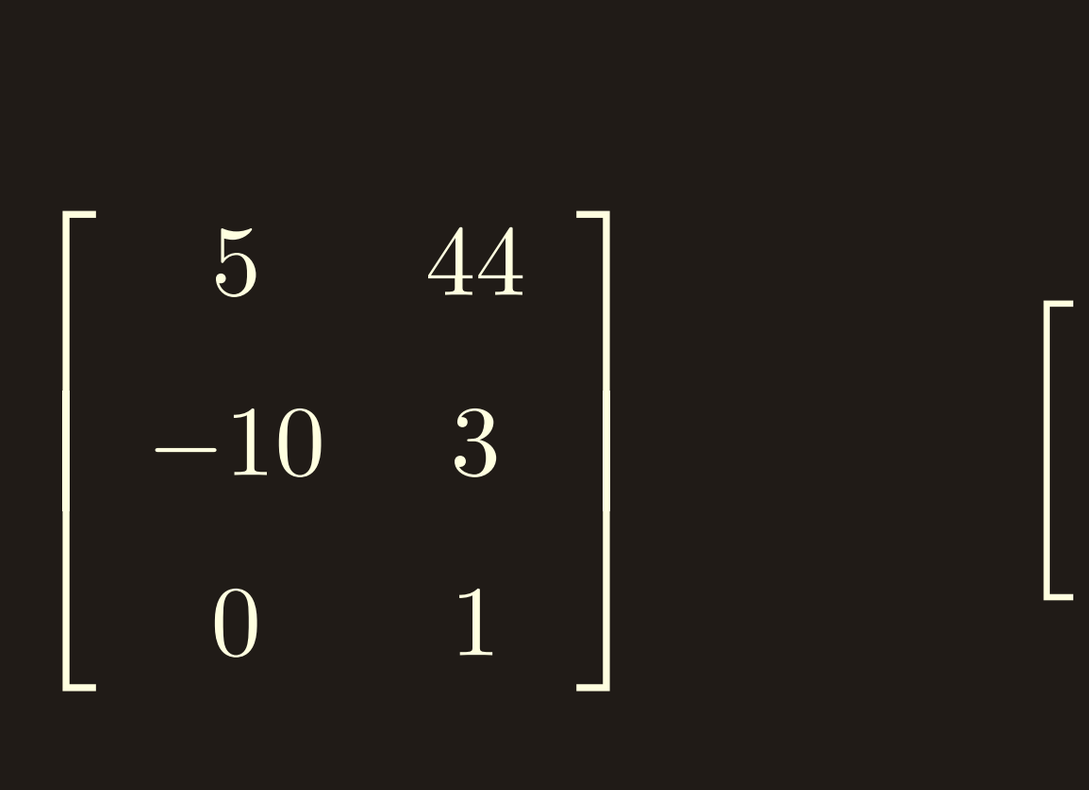
$$\begin{bmatrix} 5 & 44 \\ -10 & 3 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 11.180 & 16.994 \\ 0.0 & 40.709 \end{bmatrix}$$



$$\begin{bmatrix} 5 & 44 \\ -10 & 3 \\ 0 & 1 \end{bmatrix}$$

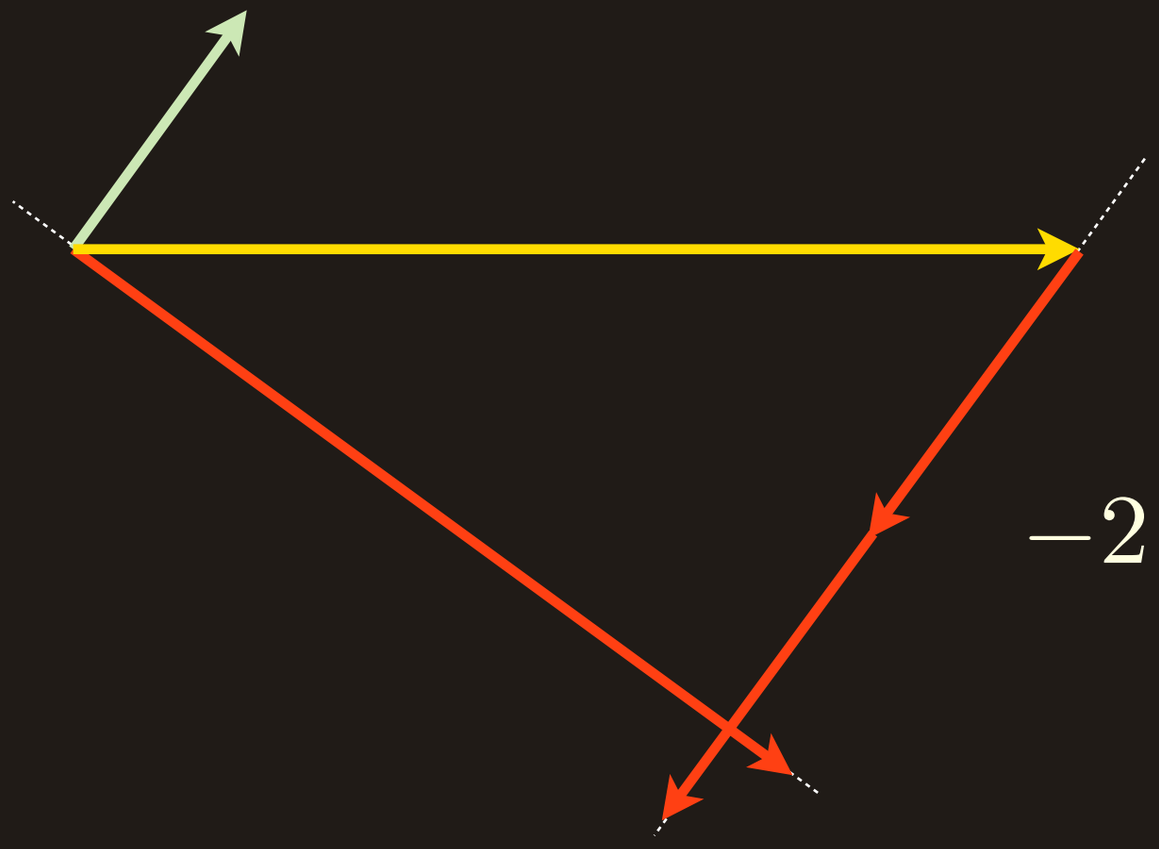
$$\begin{bmatrix} 11.180 & 16.994 \\ 0.0 & 40.709 \end{bmatrix}$$



$$\begin{bmatrix} 5 & 44 \\ -10 & 3 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 11.180 & 16.994 \\ 0.0 & 40.709 \end{bmatrix}$$

“Quotient” (translation)

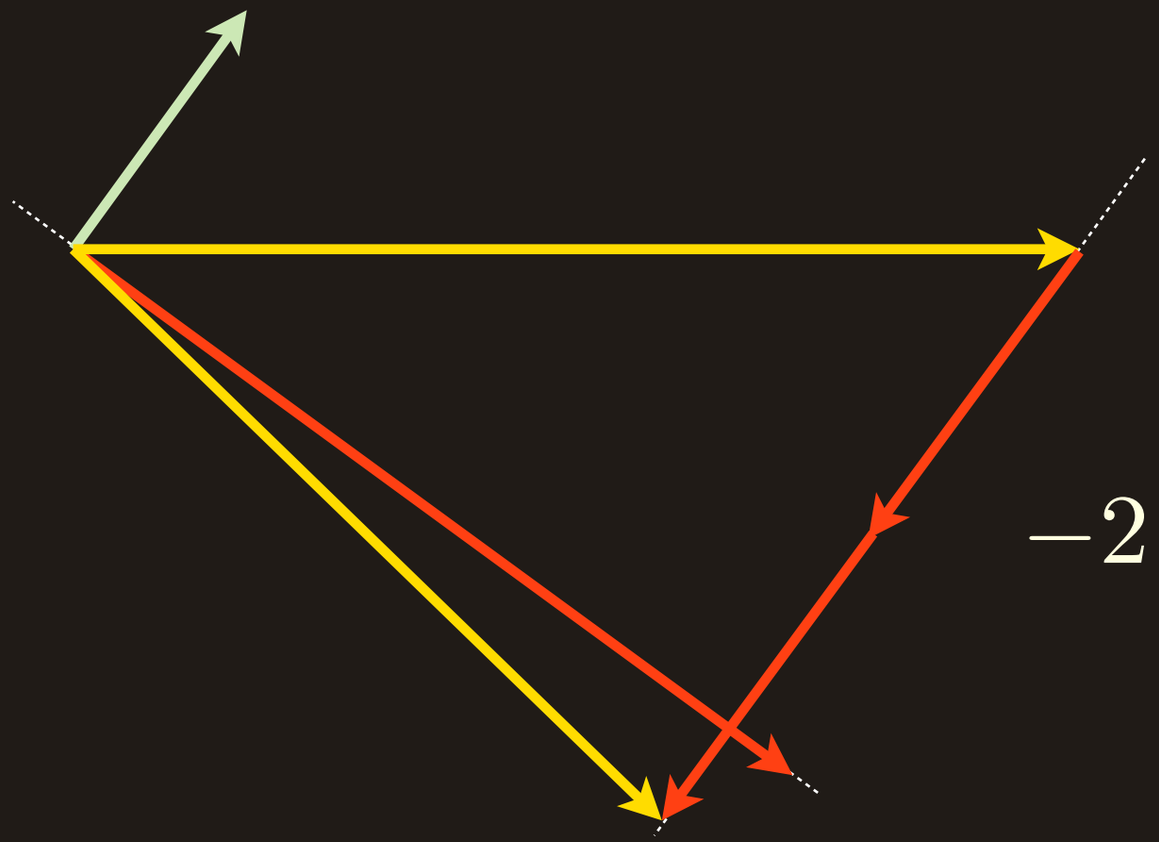


-2

$$\begin{bmatrix} 5 & 44 \\ -10 & 3 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 11.180 & 16.994 \\ 0.0 & 40.709 \end{bmatrix}$$

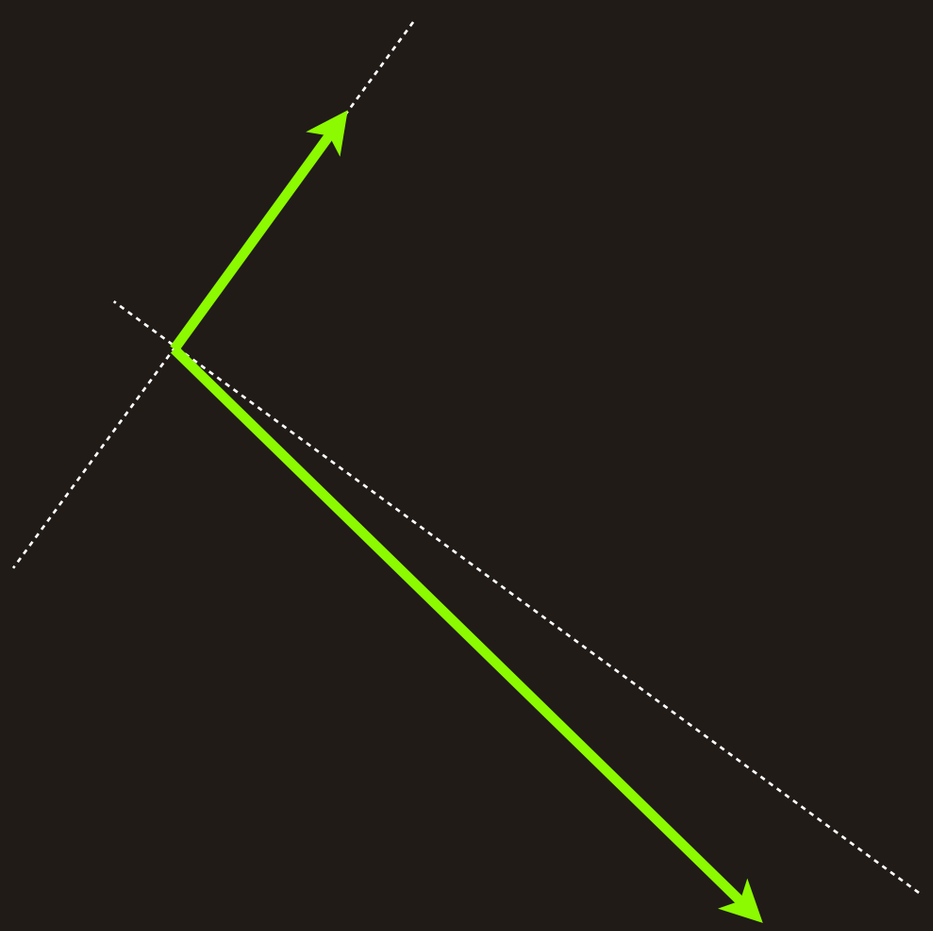
“Quotient” (translation)



-2

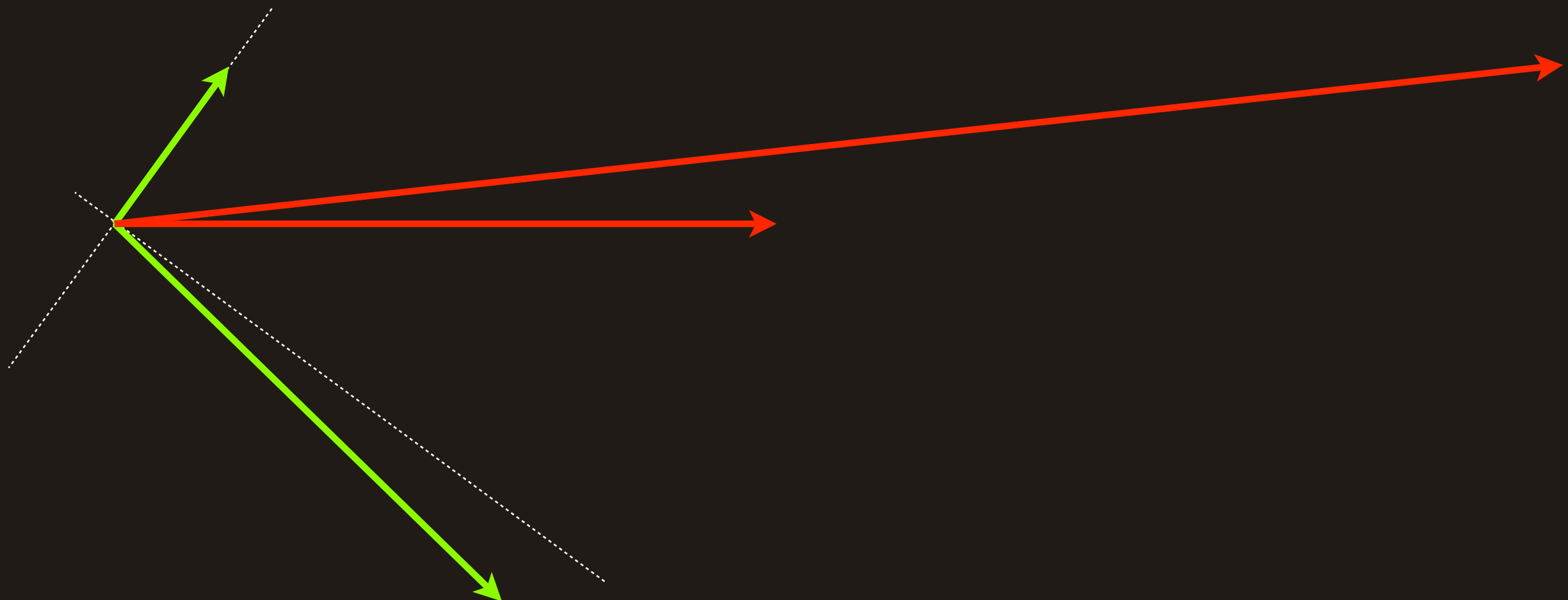
$$\begin{bmatrix} 5 & 34 \\ -10 & 23 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 11.180 & -5.3666 \\ 0.0 & 40.709 \end{bmatrix}$$



$$\begin{bmatrix} 5 & 34 \\ -10 & 23 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 11.180 & -5.3666 \\ 0.0 & 40.709 \end{bmatrix}$$



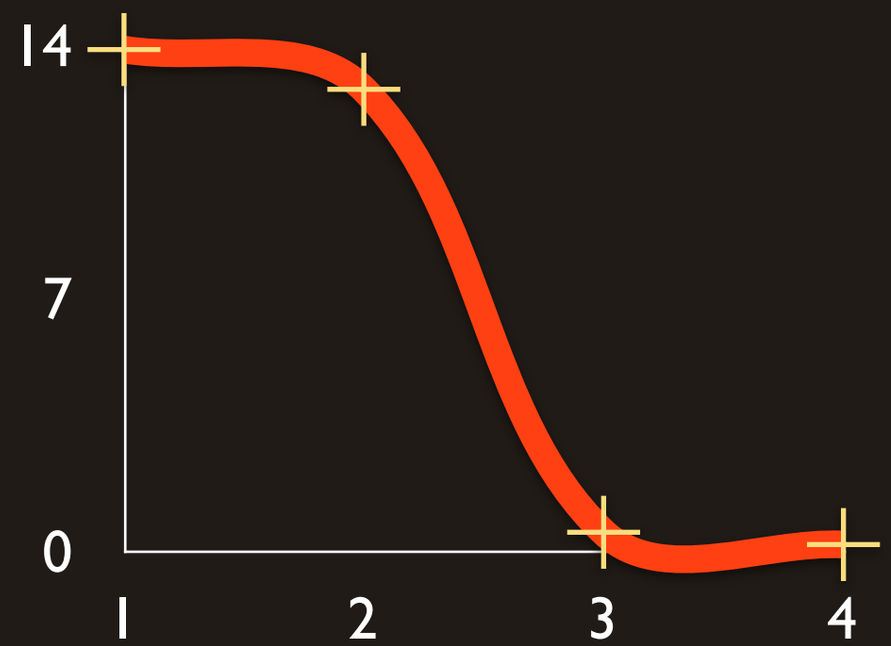
LLL reduction

(a) **“Quotient”** (translation) $|r_{i,j}| \leq \eta \|b_i^*\| + \theta \|b_j^*\|$

(b) If $\|b_i^*\|^2 > \left(r_{i,i+1}^2 + \|b_{i+1}^*\|^2\right)/\delta$ then **swap**

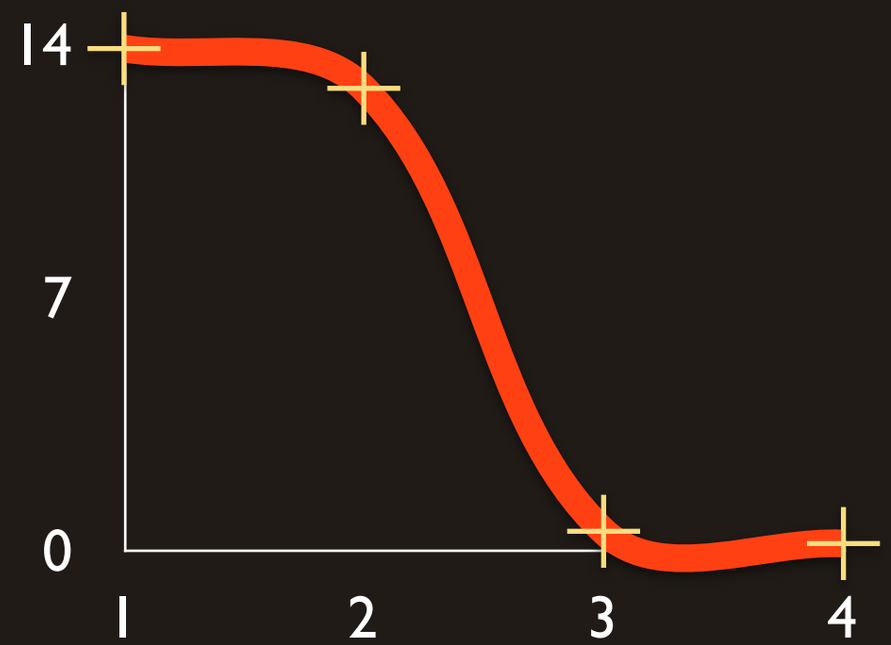
Gram-Schmidt length diagrams

$$\begin{bmatrix} 829556 & 161099 & 11567 & 521155 \\ 769480 & 639201 & 689979 & 53629 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$



Gram-Schmidt length diagrams

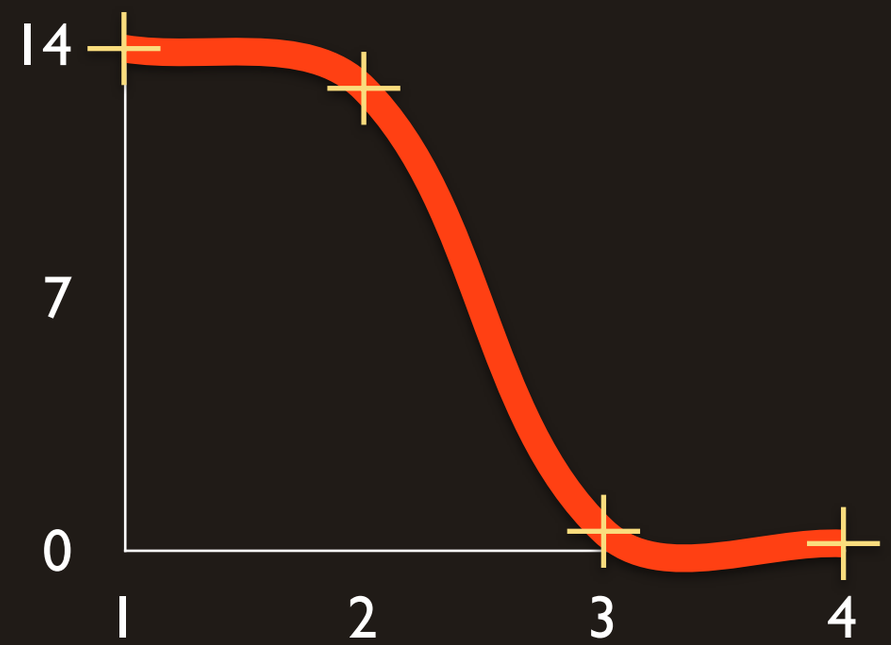
$$\begin{bmatrix} 829556 & 161099 & 11567 & 521155 \\ 769480 & 639201 & 689979 & 53629 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$



LLL reduction ↓

Gram-Schmidt length diagrams

$$\begin{bmatrix} 829556 & 161099 & 11567 & 521155 \\ 769480 & 639201 & 689979 & 53629 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

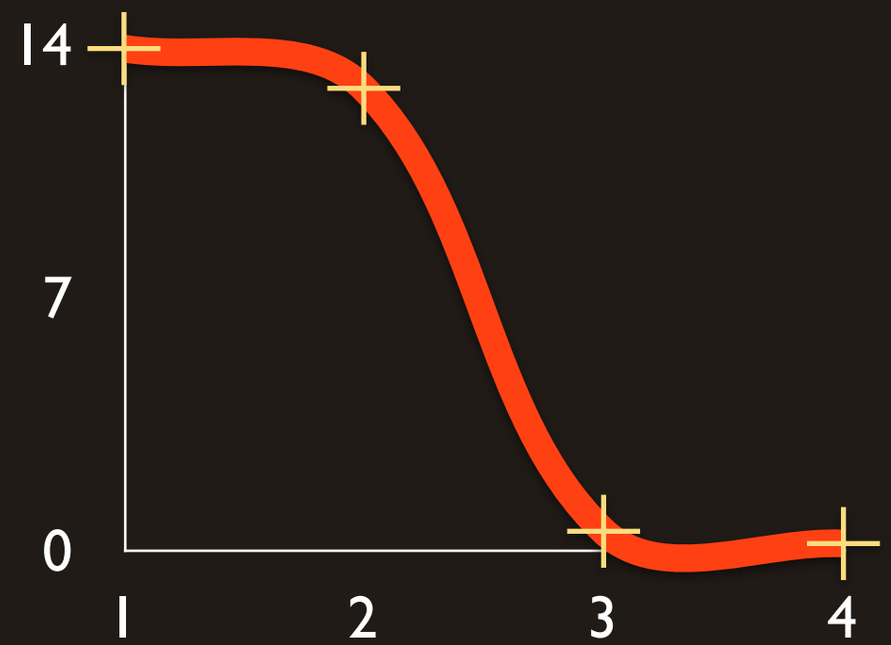


LLL reduction ↓

$$\begin{bmatrix} -158 & -827 & 481 & -532 \\ -344 & -143 & 103 & 774 \\ 342 & -199 & -418 & 251 \\ 132 & 368 & 727 & 128 \\ -459 & -135 & -242 & -365 \\ -575 & 206 & 446 & -431 \end{bmatrix}$$

Gram-Schmidt length diagrams

$$\begin{bmatrix} 829556 & 161099 & 11567 & 521155 \\ 769480 & 639201 & 689979 & 53629 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

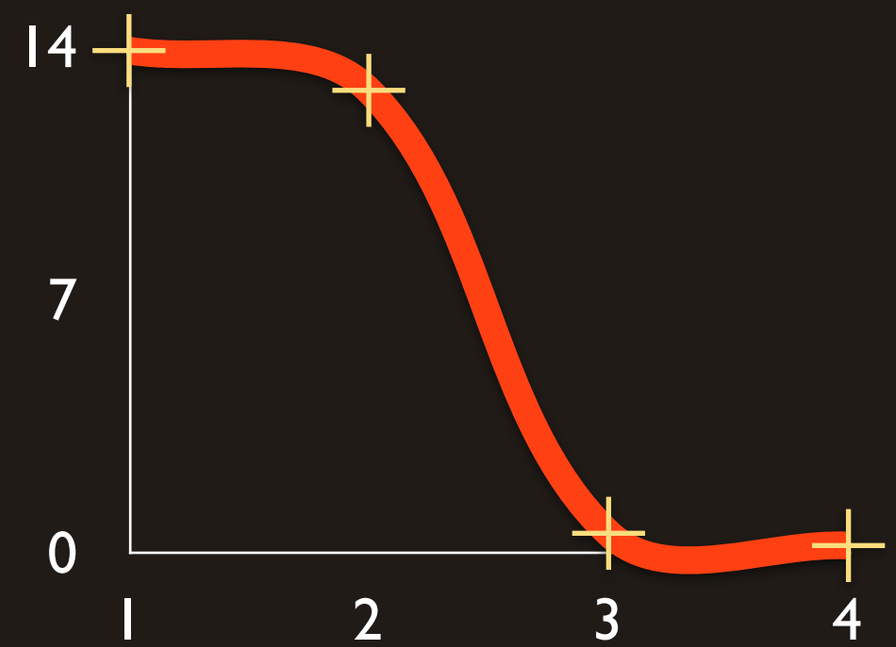


LLL reduction ↓

$$\begin{bmatrix} 904.983 & 114.799 & -335.690 & 371.165 \\ 0.0 & -962.749 & -105.204 & -253.770 \\ 0.0 & 0.0 & 1038.72 & -186.796 \\ 0.0 & 0.0 & 0.0 & -1021.48 \end{bmatrix}$$

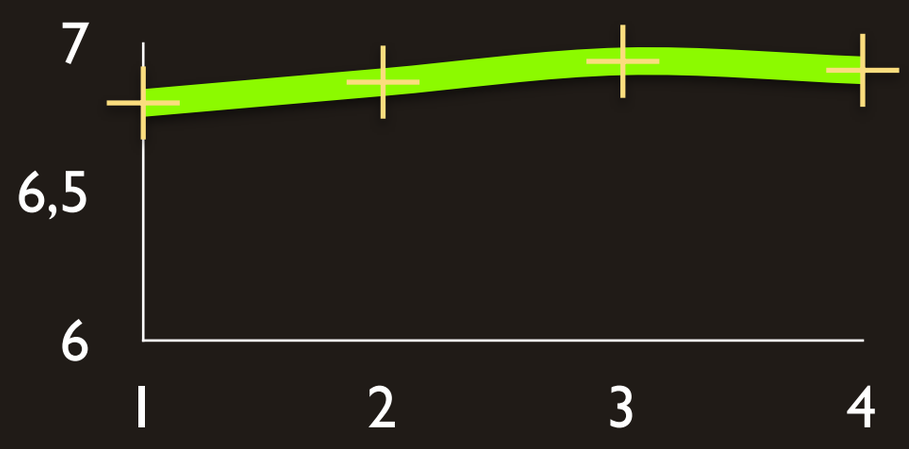
Gram-Schmidt length diagrams

$$\begin{bmatrix} 829556 & 161099 & 11567 & 521155 \\ 769480 & 639201 & 689979 & 53629 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$



LLL reduction ↓

$$\begin{bmatrix} 904.983 & 114.799 & -335.690 & 371.165 \\ 0.0 & -962.749 & -105.204 & -253.770 \\ 0.0 & 0.0 & 1038.72 & -186.796 \\ 0.0 & 0.0 & 0.0 & -1021.48 \end{bmatrix}$$



Reduced bases are fairly “well” conditioned

$$B \in \mathbb{R}^{n \times n} \text{ reduced} \quad \Rightarrow \quad \log \mathrm{cond}(R) \leq c \cdot n$$

$$r_{i,i} \leq \alpha r_{i+1,i+1}$$

[Chang, Stehlé, V. 2009-2011]

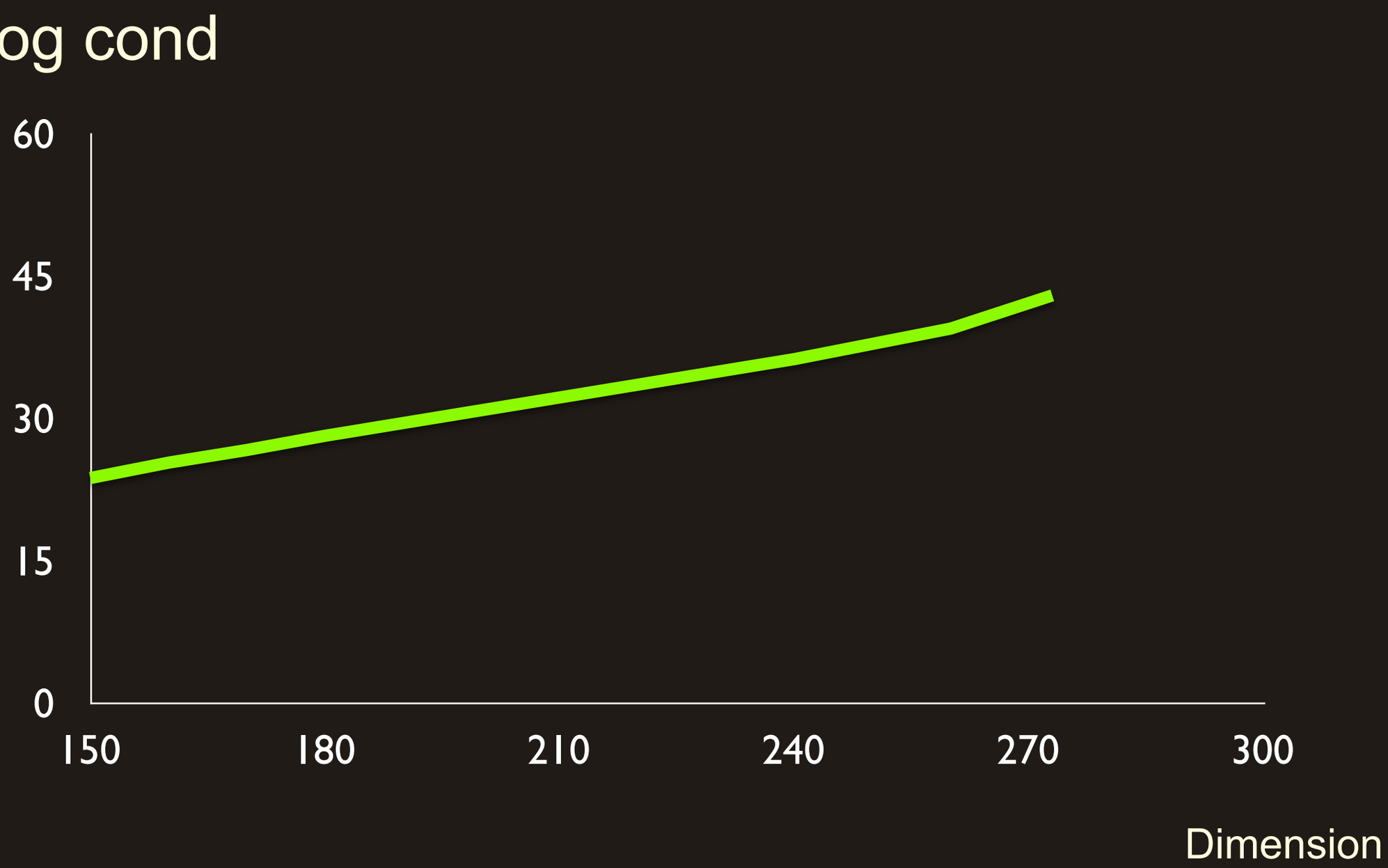
Reduced bases are fairly “well” conditioned

$$B \in \mathbb{R}^{n \times n} \text{ reduced} \quad \Rightarrow \quad \log \mathrm{cond}(R) \leq c \cdot n$$

$$r_{i,i} \leq \alpha r_{i+1,i+1}$$

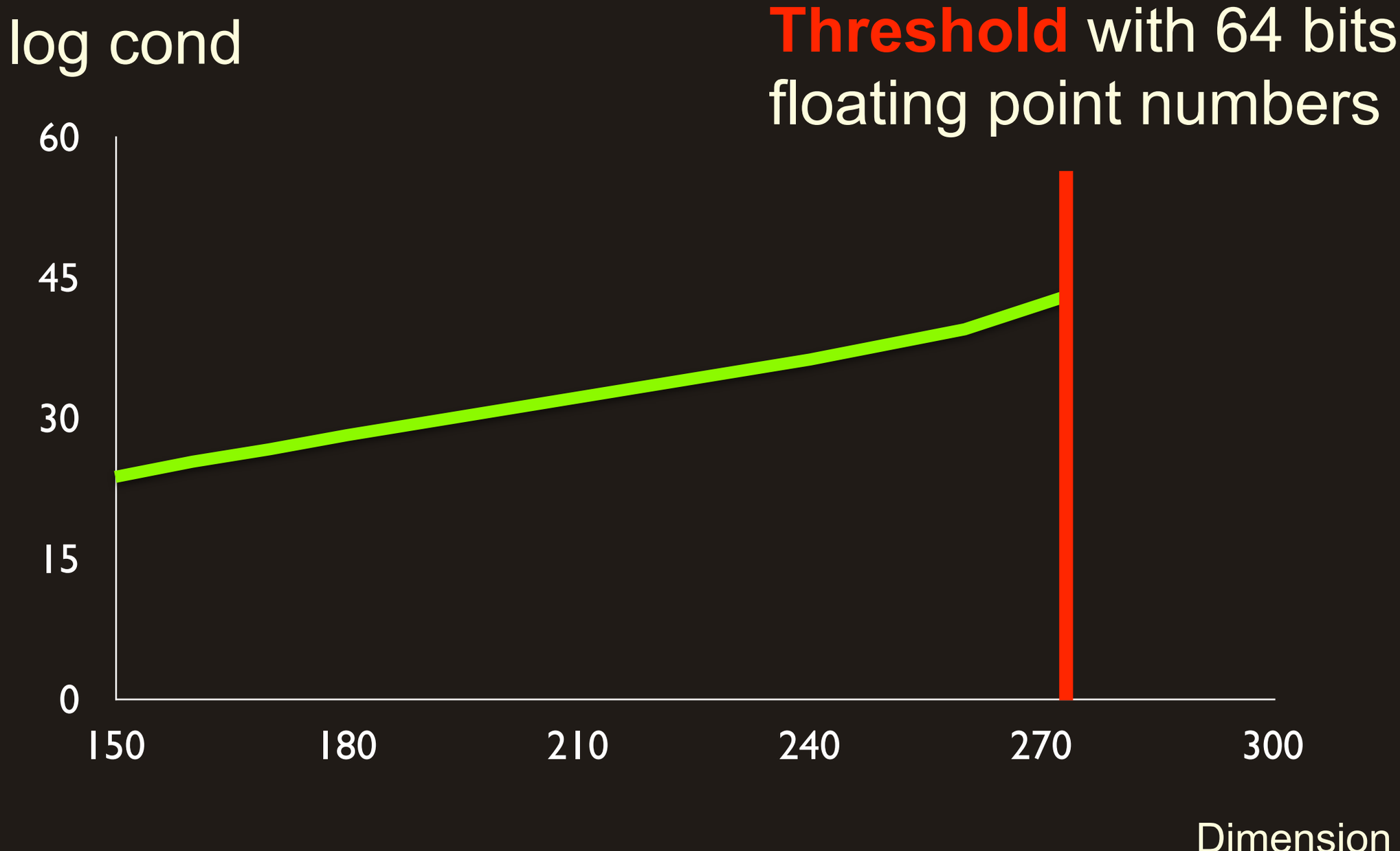
[Chang, Stehlé, V. 2009-2011]

bits > 10000



LLL Householder based algorithm

bits > 10000



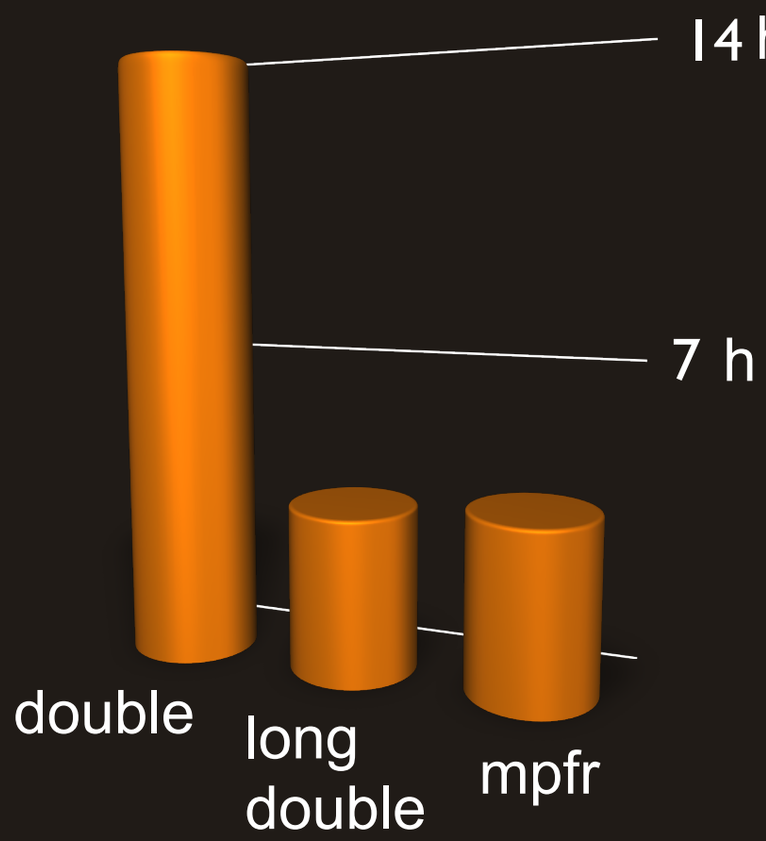
L2 type hybrid approach

[Nguyen & Stehlé 2005]

Choice of QR algorithm depending on the arithmetic precision and the dimension

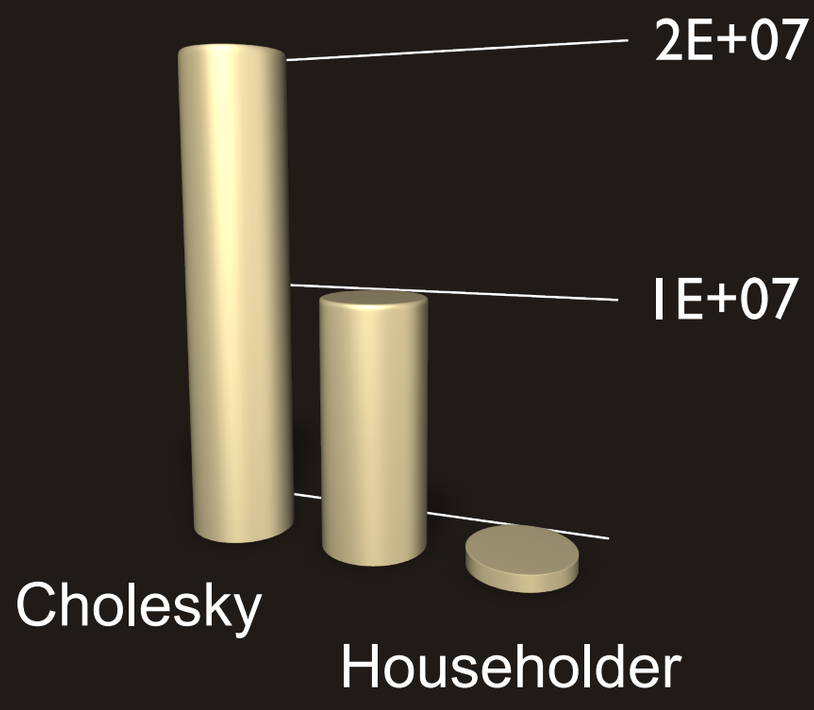
+

Numerical certificate/heuristic for switching



Time spend with the different precisions

$d = 400$, 10000 bits



Lovász tests

$n \times n$ $\quad \max \log \|A_j\| \leq \beta$

[Lenstra, Lenstra, Lovász 1982]

[Kaltofen 1983]

[Schnorr 1988]

[Schönhage 1984]

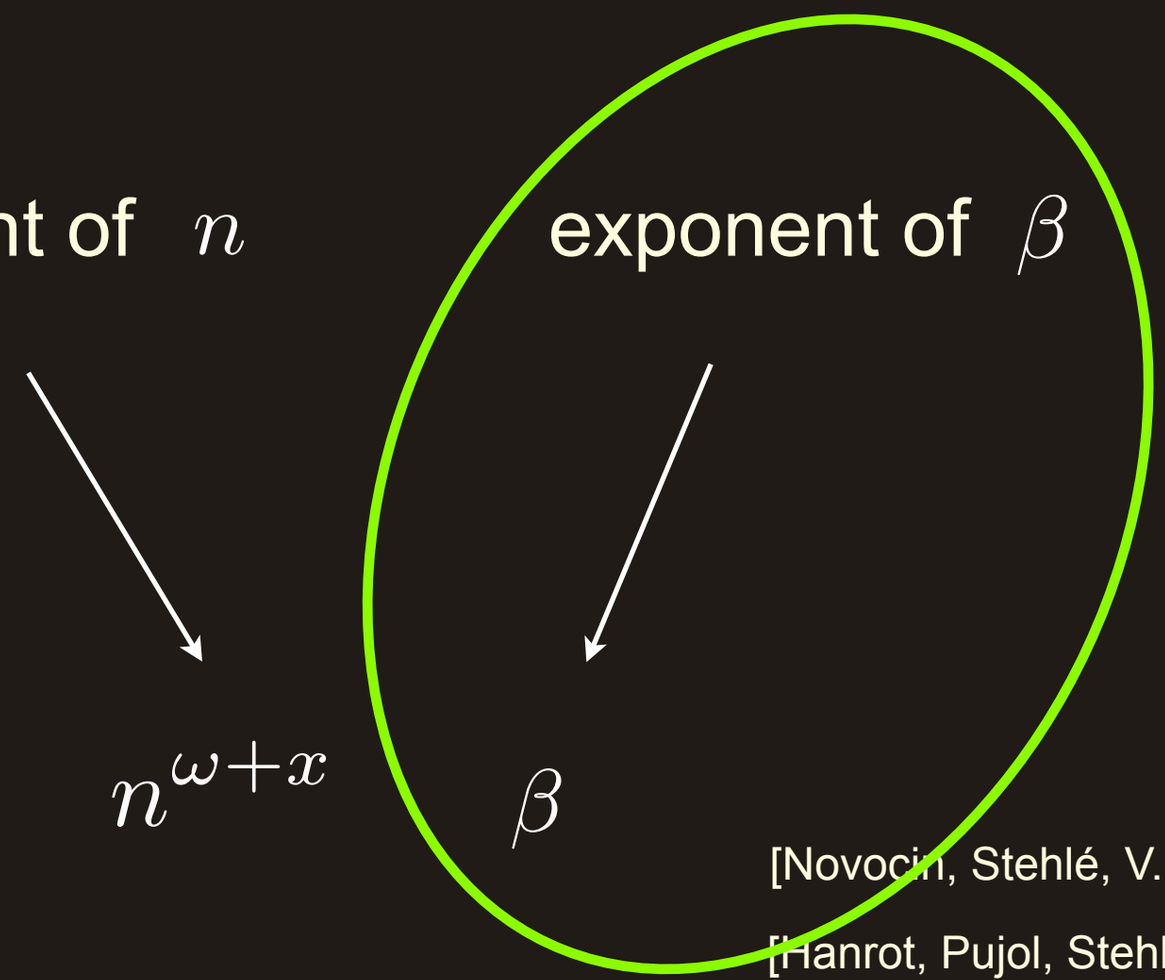
[Storjohann 1996] (relaxed)

[Schnorr 2006] (relaxed)

[Nguyen, Stehlé 2006]

$$O^{\sim}(n^{3.5}\beta^2)$$

$$O^{\sim}(n^4)\beta(n+\beta)$$



[Novocin, Stehlé, V. 2010-2011]

[Hanrot, Pujol, Stehlé, V. 2010-]

Numerical matrix techniques

$$\begin{bmatrix} 43233244567554319986453 & 764435432278876556777 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 4323324456 & 764435432 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot 10^{11} + \Delta M$$

Decoupling
L2 algorithm and beyond

[Odlyzko 1984] [Schnorr 1988] [Nguyen, Stehlé 2005]

Unimodular operations

Approximate QR factorization (orthogonalization)

Modified Gram-Schmidt, Cholesky, Householder, etc.

Adequation of the definition of reduction with the numerical errors?

“Incompatibility” between QR algorithms and the reduction definition

Backward stability

[Higham 1996]

Floating point Householder algorithm

$$B \longrightarrow \tilde{R}$$

Backward stability

[Higham 1996]

Floating point Householder algorithm

$$B \longrightarrow \tilde{R}$$

$$B + \Delta B = Q\tilde{R}$$

Backward stability

[Higham 1996]

Floating point Householder algorithm

$$B \longrightarrow \tilde{R}$$

$$B + \Delta B = Q\tilde{R}$$

QR perturbation theory

$$\tilde{R} = R + \Delta R \qquad \frac{\|\Delta r_j\|}{\|r_j\|} \leq \varkappa_j \epsilon$$

Backward stability

[Higham 1996]

Floating point Householder algorithm

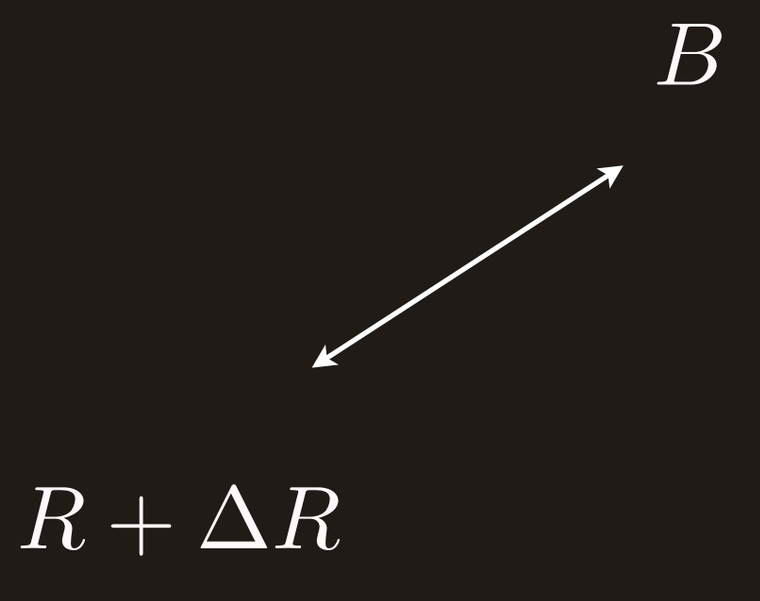
$$B \longrightarrow \tilde{R}$$

$$B + \Delta B = Q\tilde{R}$$

QR perturbation theory

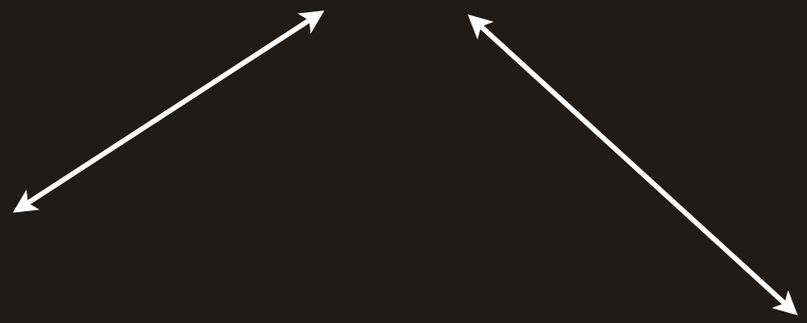
$$\tilde{R} = R + \Delta R$$

$$\frac{\|\Delta r_j\|}{\|r_j\|} \leq \varkappa_j \epsilon$$



$$\frac{\|\Delta r_j\|}{\|r_j\|} \leq \varkappa_j \epsilon$$

$$B$$



$$R + \Delta R$$

$$|r_{i,j}| \leq \eta |r_{i,i}|$$

$$\frac{\|\Delta r_j\|}{\|r_j\|} \leq \varkappa_j \epsilon$$

$$B$$

$$R + \Delta R$$

$$\frac{\|\Delta r_j\|}{\|r_j\|} \leq \varkappa_j \epsilon$$

$$|r_{i,j}| \leq \eta |r_{i,i}|$$

Tool 1 **Elementary step: ”from reduced to reduced”**

$$\begin{bmatrix} 392554592838 & 836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

New, robust LLL reduction definition

$$|r_{i,j}| \leq \eta \|b_i^*\| + \theta \|b_j^*\|$$

$$B \in \mathbb{R}^{n \times n} \quad \Xi_1\text{-reduced}$$

$$\max \frac{\Delta \|b_i\|}{\|b_i\|} \leq 2^{-cn} \quad \Rightarrow \quad B + \Delta B \quad \Xi_2\text{-reduced}$$

[Chang, Stehlé, V. 2009-2011]

Tool 1 **Elementary step: ”from reduced to reduced”**

$$\begin{bmatrix} 392554592838 & 836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \sigma^{12} \begin{bmatrix} 0.392554592838 & 0.836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Tool 1 **Elementary step: ”from reduced to reduced”**

$$\begin{bmatrix} 0.392554592838 & 0.836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

B reduced

Tool 1 **Elementary step: ”from reduced to reduced”**

$$\begin{bmatrix} 0.392554592838 & 0.836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

B reduced

$$\sigma^{12} \begin{bmatrix} 0.392554592838 & 0.836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\sigma^l B = \mathrm{diag}(2^l, 1, \ldots, 1) B$$

[Belabas 2004] [van Hoeij, Novocin 2010]

Tool 1 **Elementary step: "from reduced to reduced"**

$$\begin{bmatrix} 0.392554592838 & 0.836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

B reduced

$$\sigma^{12} \begin{bmatrix} 0.392554592838 & 0.836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$\sigma^l B = \mathrm{diag}(2^l, 1, \ldots, 1)B$

[Belabas 2004] [van Hoeij, Novocin 2010]

"LLL quotient": U unimodular such that

$C = \sigma^l BU$ is reduced

[Stehlé, Novocin, V. 2010]

Euclid's algorithm

$$\begin{bmatrix} 392554592838 & 836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Euclid's algorithm

$$\begin{bmatrix} 392554592838 & 836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

↓ a few steps

Euclid's algorithm

$$\begin{bmatrix} 392554592838 & 836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

↓ a few steps

$$\begin{bmatrix} 15676304061 & 2133306629 \\ 32 & -49 \\ -15 & 23 \end{bmatrix}$$

Euclid's algorithm

$$\begin{bmatrix} 392554592838 & 836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

↓ a few steps

$$\begin{bmatrix} 15676304061 & 2133306629 \\ 32 & -49 \\ -15 & 23 \end{bmatrix}$$

Lift LLL

$$\begin{bmatrix} 0.392554592838 & 0.836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Euclid's algorithm

$$\begin{bmatrix} 392554592838 & 8364047111117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

a few steps

$$\begin{bmatrix} 15676304061 & 2133306629 \\ 32 & -49 \\ -15 & 23 \end{bmatrix}$$

Lift LLL

$$\sigma^4 \begin{bmatrix} 0.392554592838 & 0.8364047111117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Euclid's algorithm

$$\begin{bmatrix} 392554592838 & 836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

↓ a few steps

$$\begin{bmatrix} 15676304061 & 2133306629 \\ 32 & -49 \\ -15 & 23 \end{bmatrix}$$

Lift LLL

$$\sigma^4 \begin{bmatrix} 0.392554592838 & 0.836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\approx$$

$$\begin{bmatrix} 3925.545 & 8364.047 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Euclid's algorithm

$$\begin{bmatrix} 392554592838 & 836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

↓ a few steps

$$\begin{bmatrix} 15676304061 & 2133306629 \\ 32 & -49 \\ -15 & 23 \end{bmatrix}$$

Lift LLL

$$\sigma^4 \begin{bmatrix} 0.392554592838 & 0.836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\wr$$

$$\begin{bmatrix} 3925.545 & 8364.047 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

↓ reduction

Euclid's algorithm

$$\begin{bmatrix} 392554592838 & 836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

↓ a few steps

$$\begin{bmatrix} 15676304061 & 2133306629 \\ 32 & -49 \\ -15 & 23 \end{bmatrix}$$

Lift LLL

$$\sigma^4 \begin{bmatrix} 0.392554592838 & 0.836404711117 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\wr$$

$$\begin{bmatrix} 3925.545 & 8364.047 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

↓ reduction

$$\begin{bmatrix} -21.333 & -156.763 \\ 49 & -32 \\ -23 & 15 \end{bmatrix}$$

Tool 2 **The most signigicant bits of B suffice**

Progress: lifted by σ^l

Tool 2 **The most signigicant bits of B suffice**

Progress: lifted by σ^l

$B \in \mathbb{R}^{d \times d}$ Ξ_1-reduced $\max \frac{\Delta \|b_i\|}{\|b_i\|} \leq 2^{-l-cd}$

$\sigma^l(B + \Delta B)U, \quad \Xi_2$-reduced

$\Downarrow$

$\sigma^l BU, \quad \Xi_3$-reduced

Hint: bounds on U and robust reduction

[Lehmer 1938]

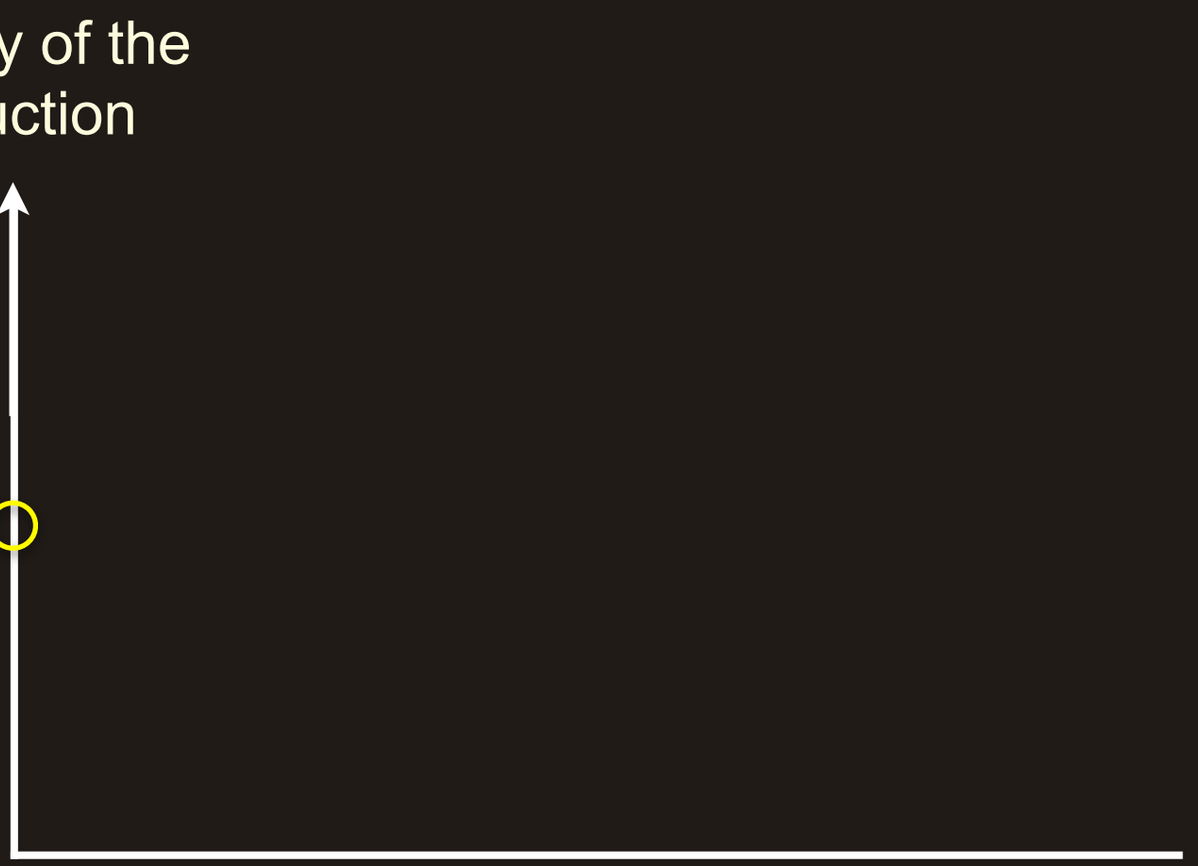
[Novocin, Stehlé, V. 2010]

One step of Lehmer lift reduction

(Low cost unimodular transformaitons and reduction strengthening)

Input: B

Ξ-reduced

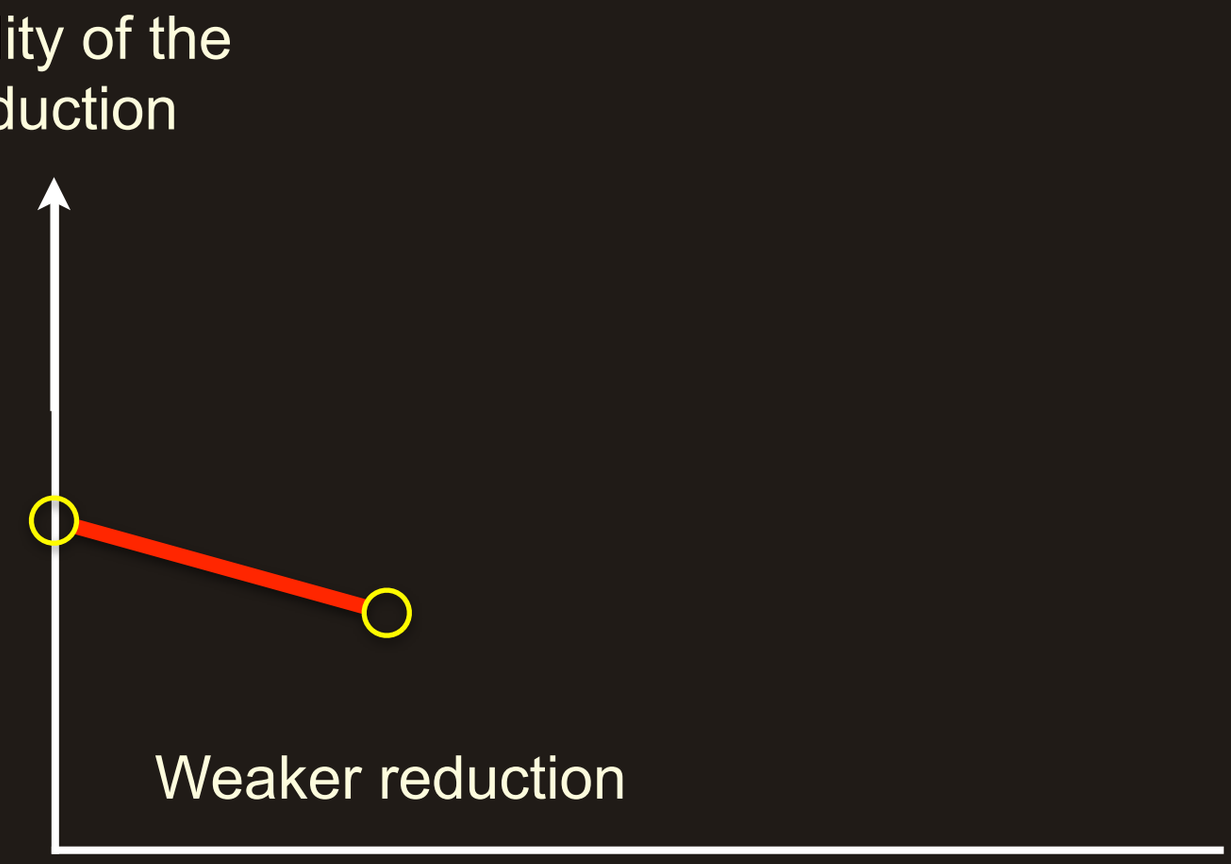


One step of Lehmer lift reduction

(Low cost unimodular transformaitons and reduction strengthening)

Input: B
Ξ-reduced

Truncation: $l + cd$ bits B'
Ξ'-reduced



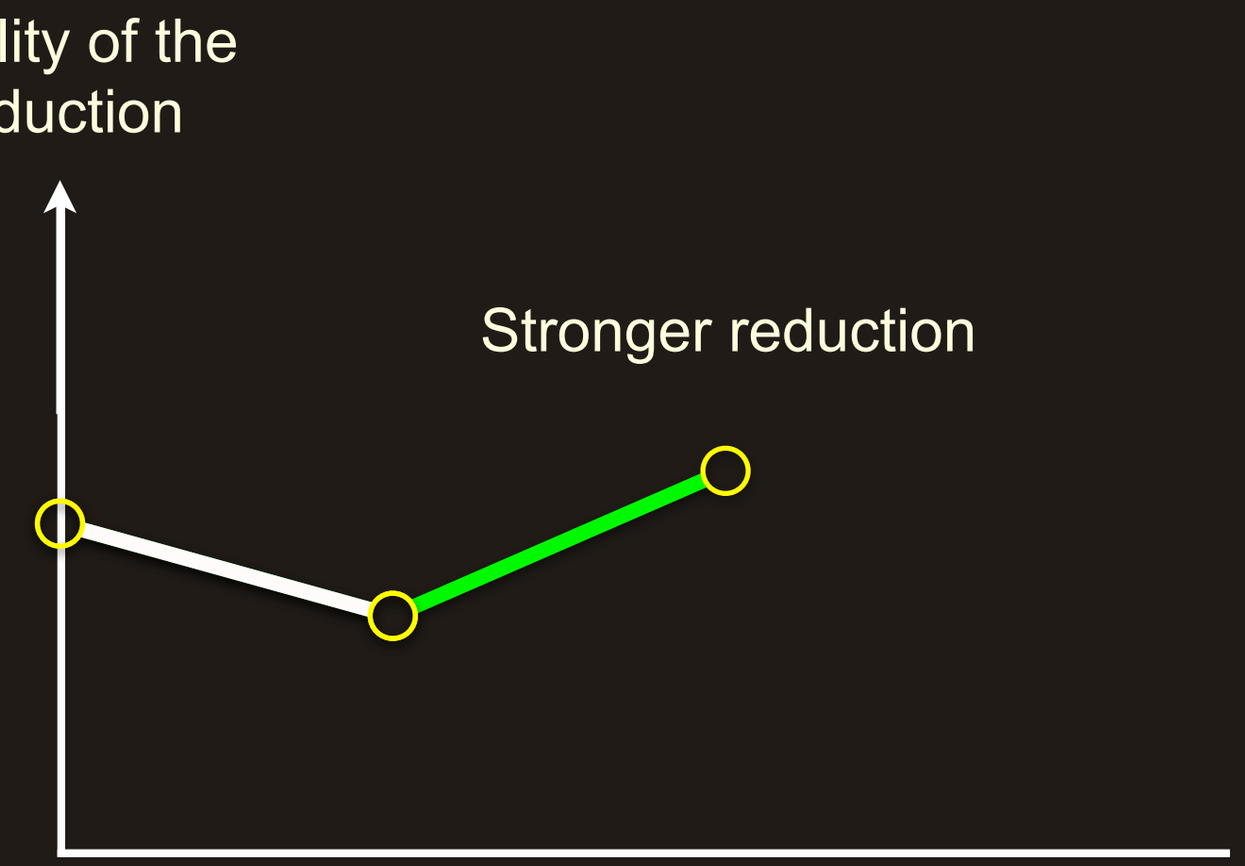
One step of Lehmer lift reduction

(Low cost unimodular transformaitons and reduction strengthening)

Input: B
Ξ-reduced

Truncation: $l + cd$ bits B'
Ξ'-reduced

Reduction: $\sigma^l B' U$
Ξ''-reduced



One step of Lehmer lift reduction

(Low cost unimodular transformaitons and reduction strengthening)

Input: B
Ξ-reduced

Truncation: $l + cd$ bits B'
Ξ'-reduced

Reduction: $\sigma^l B' U$
Ξ''-reduced

Return: $\sigma^l BU$
Ξ-reduced

One step of Lehmer lift reduction

(Low cost unimodular transformaitons and reduction strengthening)

Input: B

Ξ-reduced

Return: $\sigma^l BU$

Ξ-reduced

Lehmer lift reduction

$$\sigma^{\beta} BU$$

$$\sigma^{l} \cdot (\sigma^{l} \cdot (\ldots (\sigma^{l} \cdot B \cdot U_1) \ldots) \cdot U_{\beta/l-1}) \cdot U_{\beta/l}$$

Tool 2. $l + cd$ digits of the basis for each lift

Cost $\approx (\beta/l) \times \mathcal{P}(d) l^2$

$$l = \sqrt{\beta}$$

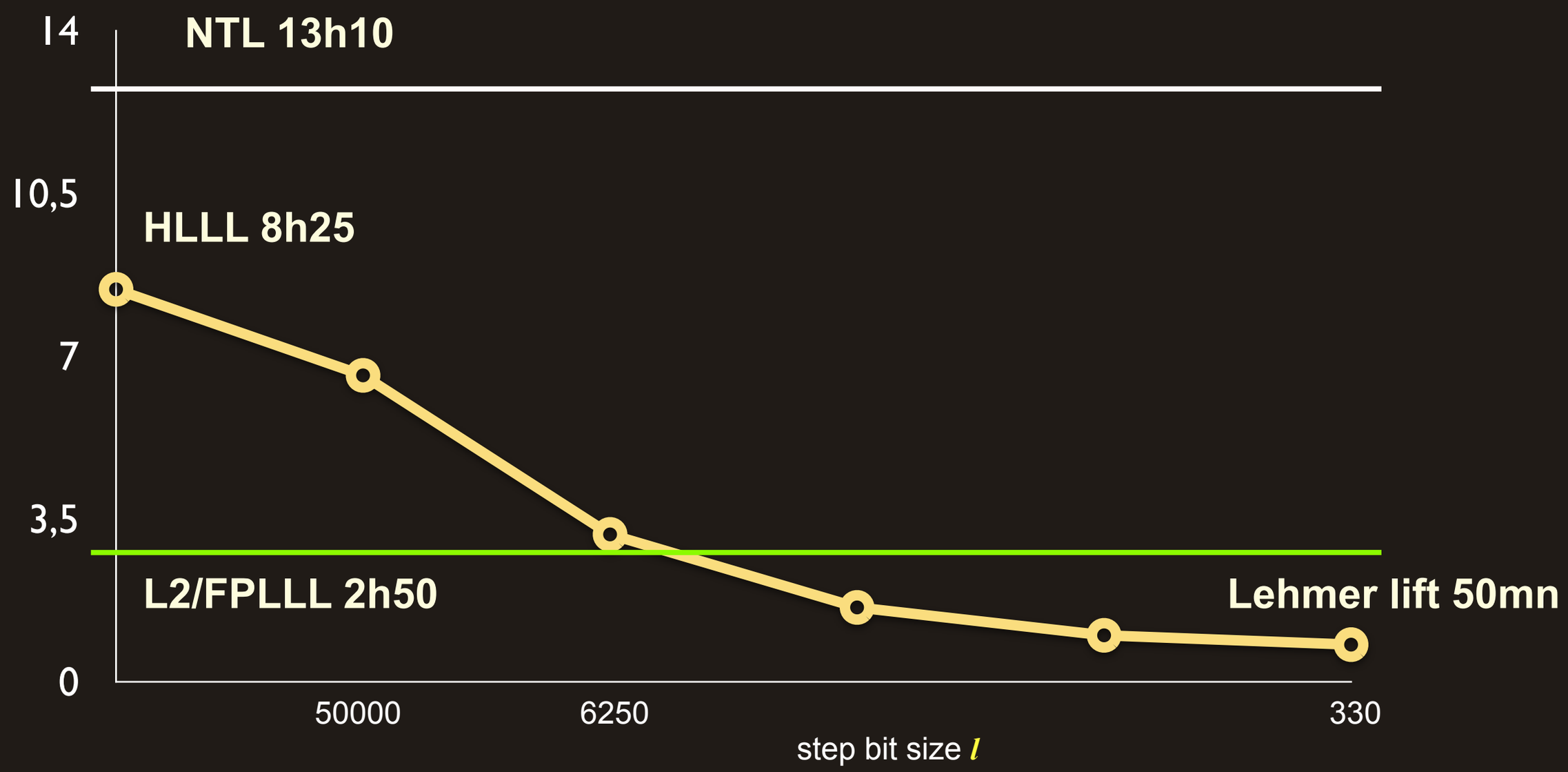
Tool 3. Low cost transformations

Cost $\approx (\beta/l) \times \mathcal{Q}(d) \beta^{1+\epsilon}$

$$\mathcal{P}oly(d) \beta^{1.5+\epsilon}$$

Timings

d=120 100,000 bits



The talk

Symbolic linear algebra

LLL: a “testbed” for exact-numerical computation

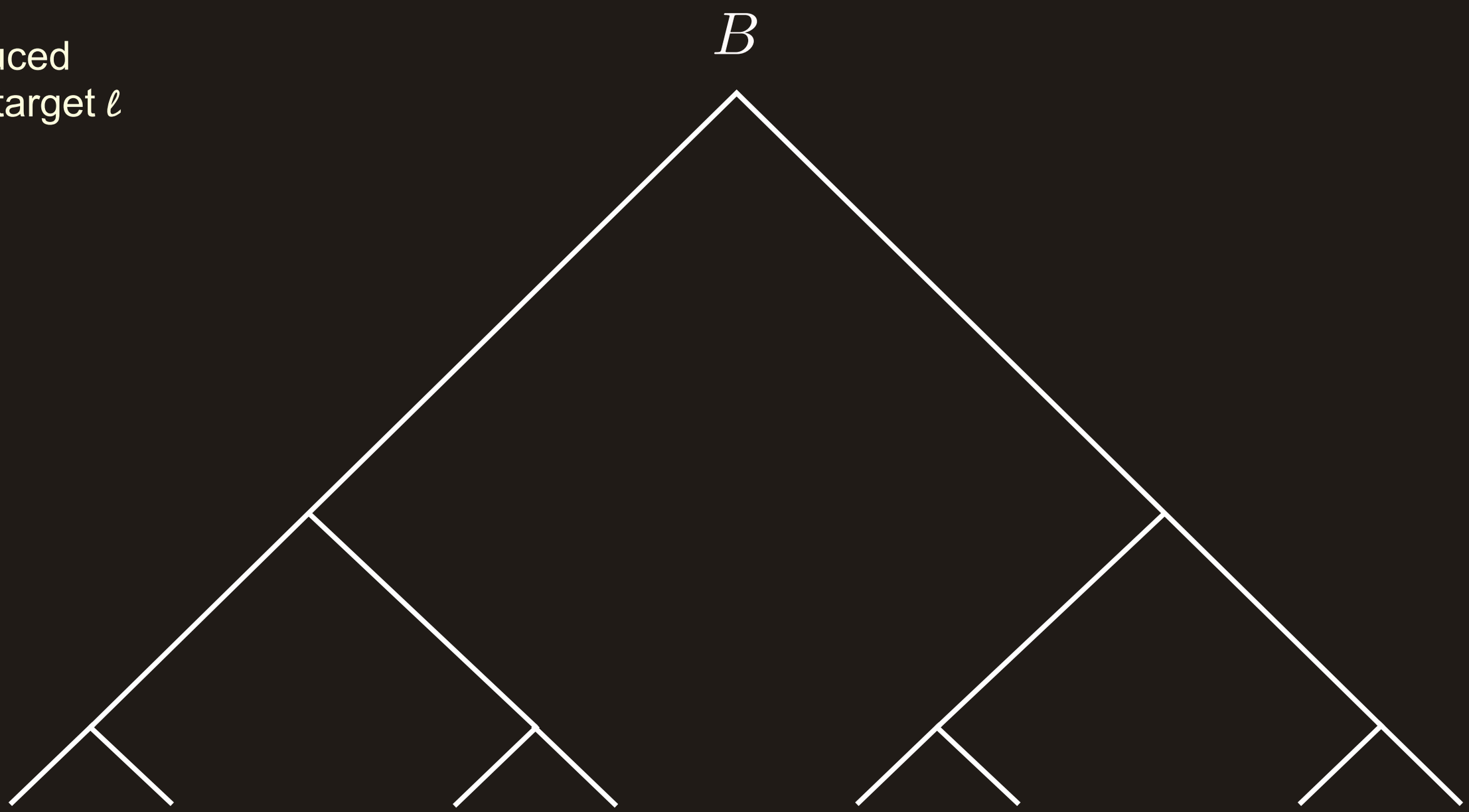
Tool box for an iterative reduction approach

Lehmer: a lift reduction

Knuth-Schönhage: a quasi-linear time reduction

Recursive lift reduction

B reduced lifting target ℓ

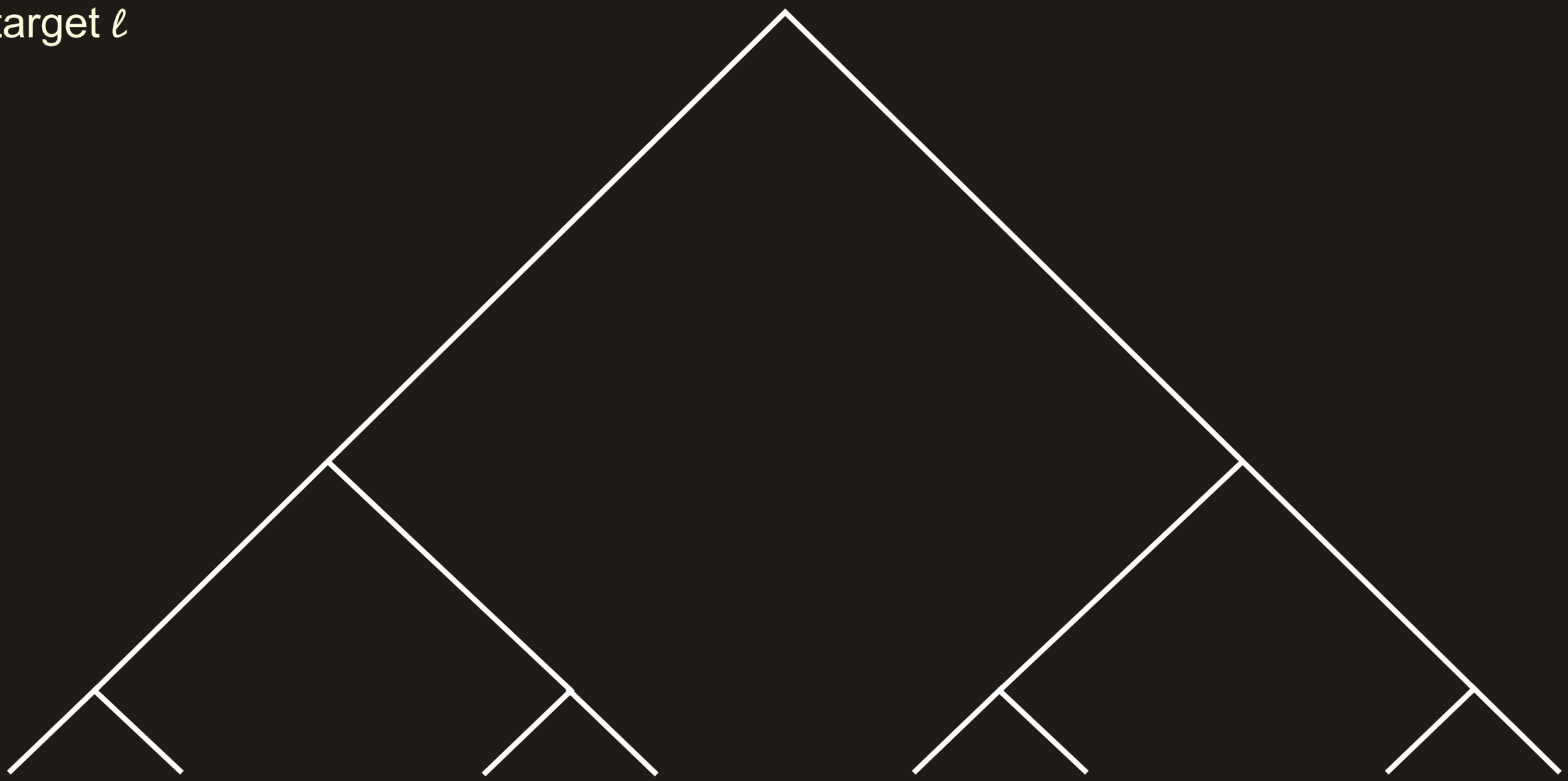


A recursive lifting tree

Recursive lift reduction

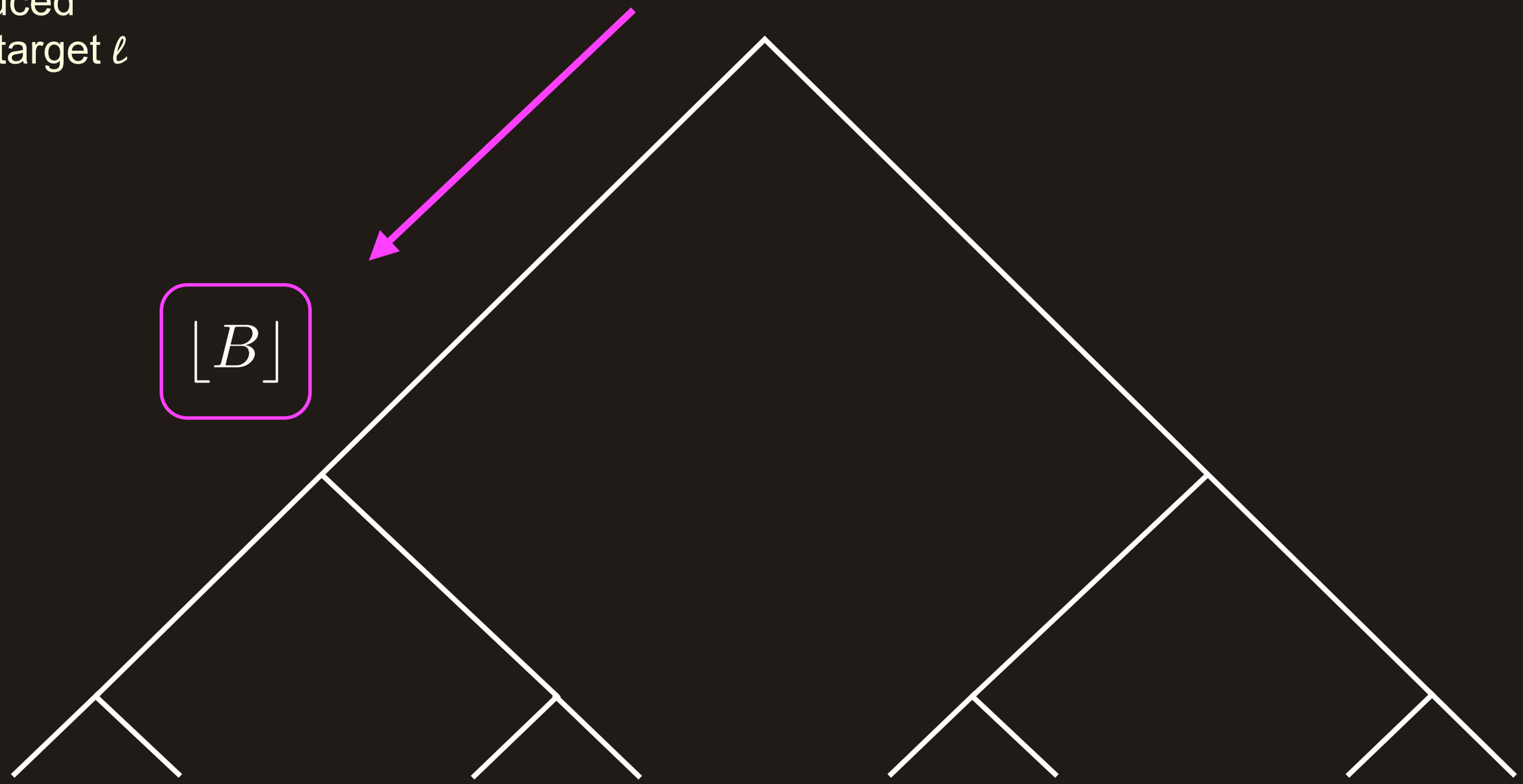
B reduced lifting target ℓ

$\sigma^l BU$?



Recursive lift reduction

B reduced
lifting target ℓ



$$B \text{ reduced} \Rightarrow B + \Delta B \text{ reduced}$$

Recursive lift reduction

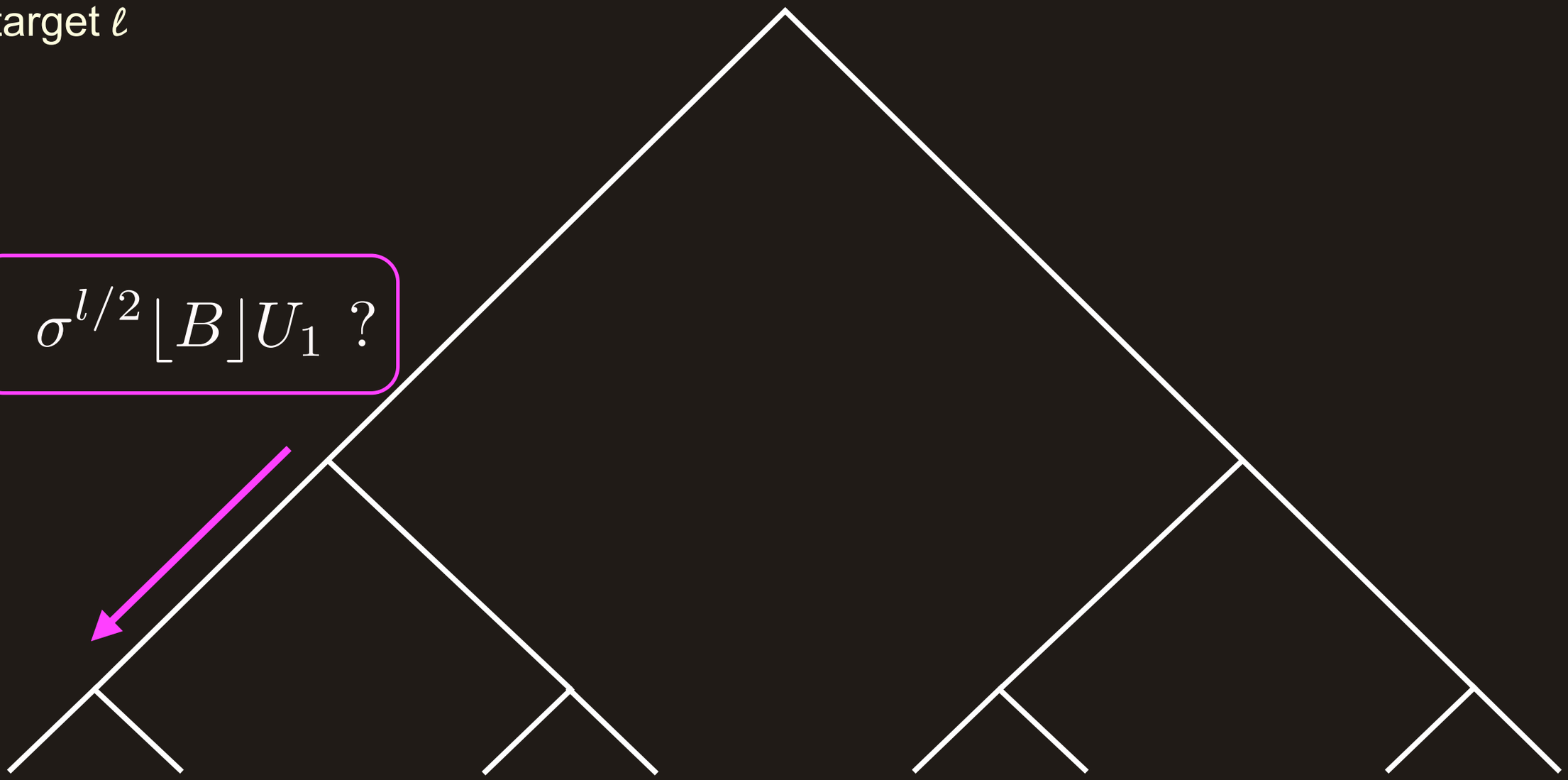
B reduced lifting target ℓ

$\sigma^{l/2}\lfloor B \rfloor U_1 \ ?$

$B + \Delta B$ lifting

Recursive lift reduction

B reduced
lifting target ℓ

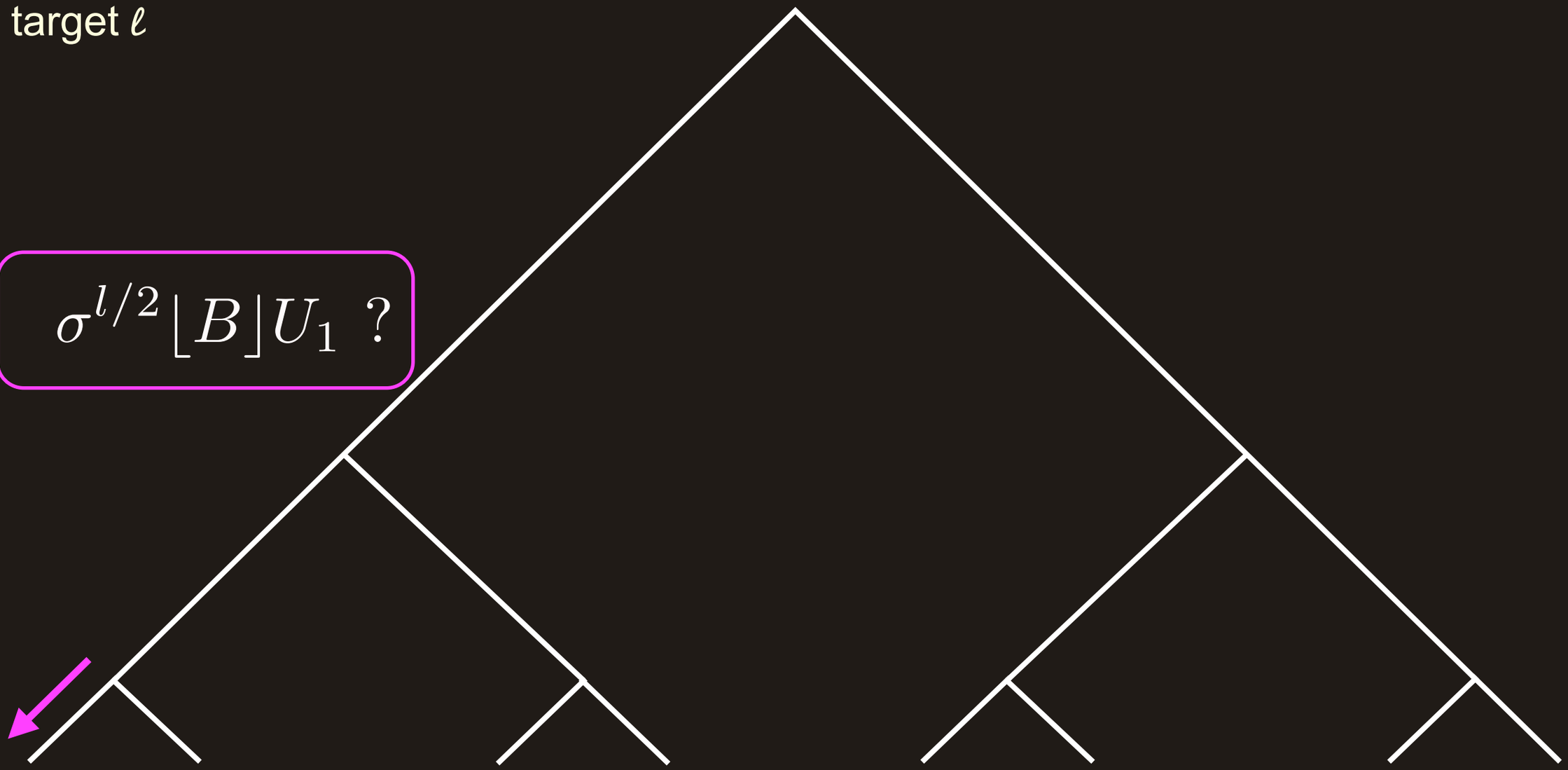


$B + \Delta B$ lifting

Recursive lift reduction

B reduced lifting target ℓ

$\sigma^{l/2}\lfloor B \rfloor U_1$?

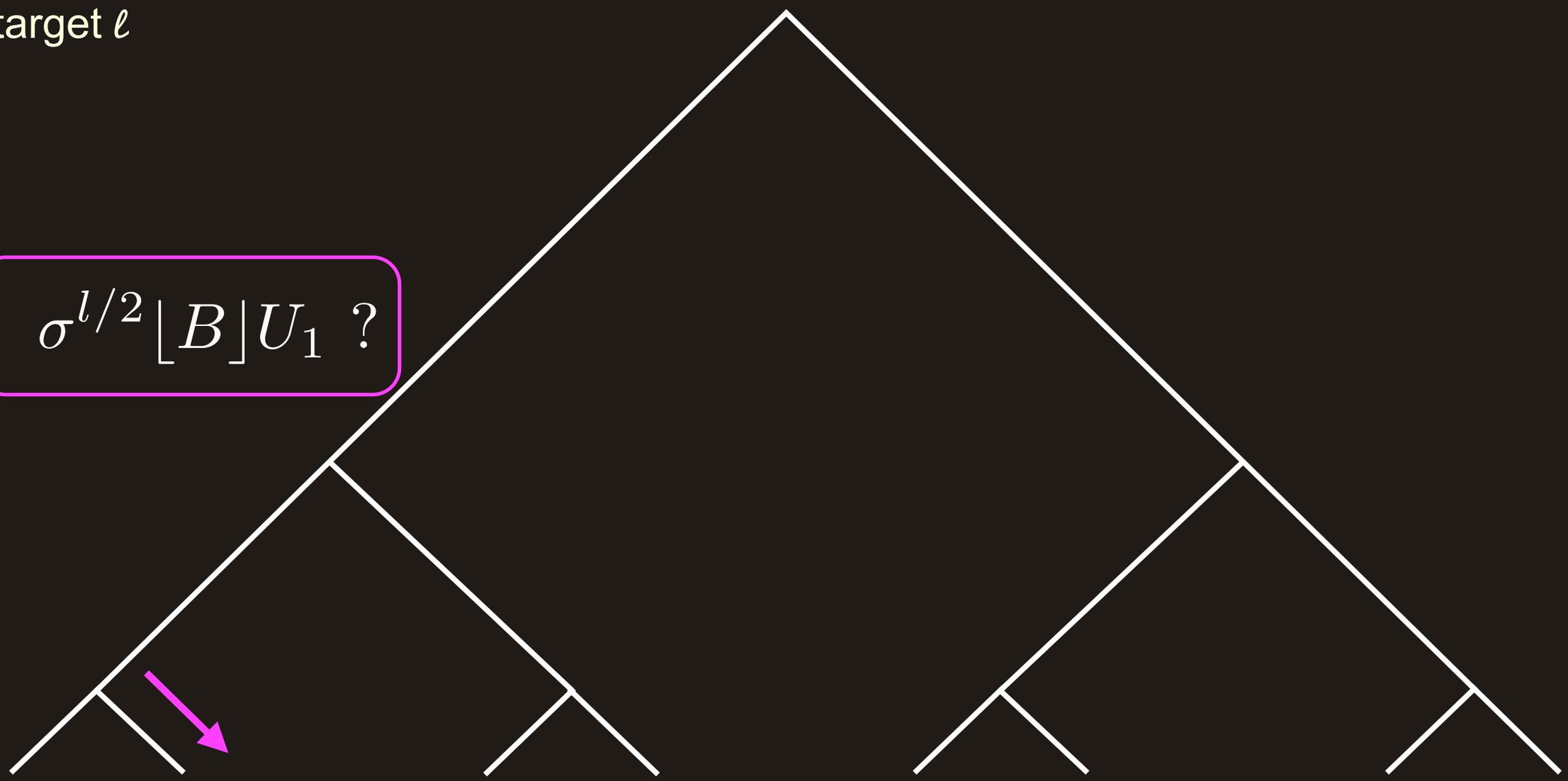


$B + \Delta B$ lifting

Recursive lift reduction

B reduced lifting target ℓ

$\sigma^{l/2}\lfloor B \rfloor U_1 \ ?$



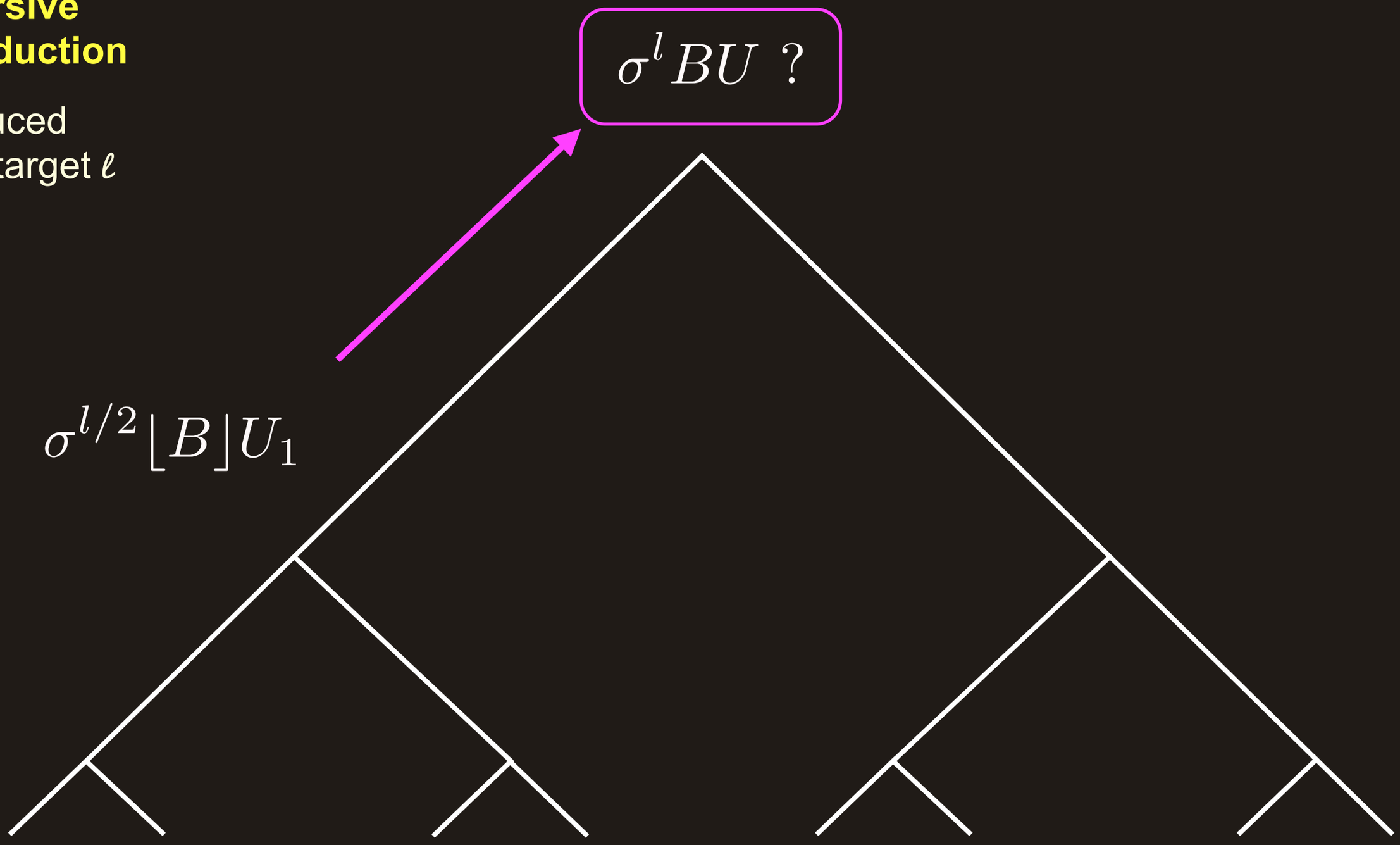
$B + \Delta B$ lifting

Recursive lift reduction

B reduced
lifting target ℓ

Recursive lift reduction

B reduced
lifting target ℓ



$$\sigma^{l/2}(B + \Delta B)U_1 \text{ reduced} \Rightarrow \sigma^{l/2} BU_1 \text{ reduced}$$

Recursive lift reduction

B reduced lifting target ℓ

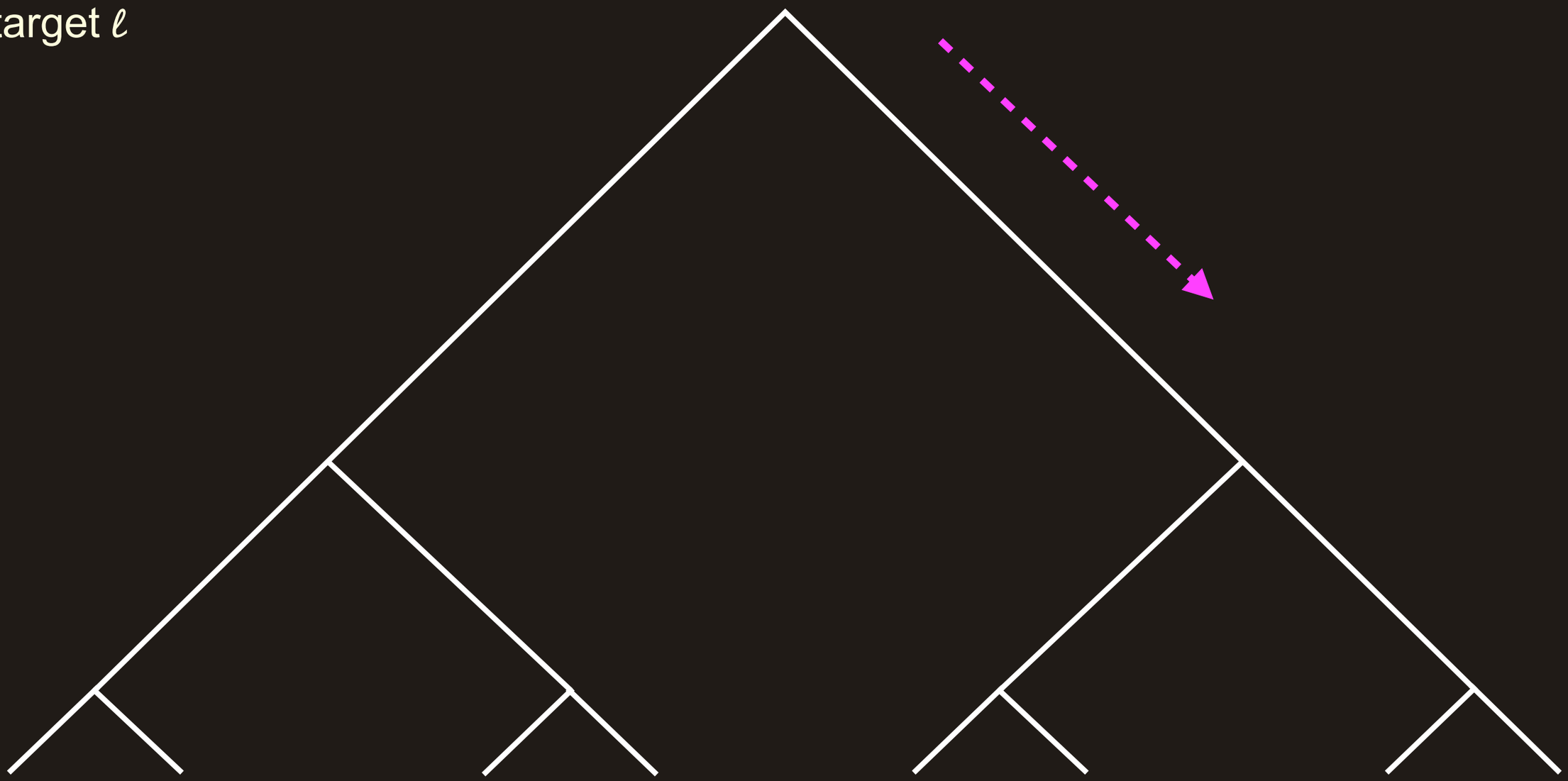
$$\sigma^{l/2}(\sigma^{l/2}BU_1)U_2\ ?$$

$$\sigma^l = (\sigma^{l/2})^2,\ \text{now a smaller lift}$$

Recursive lift reduction

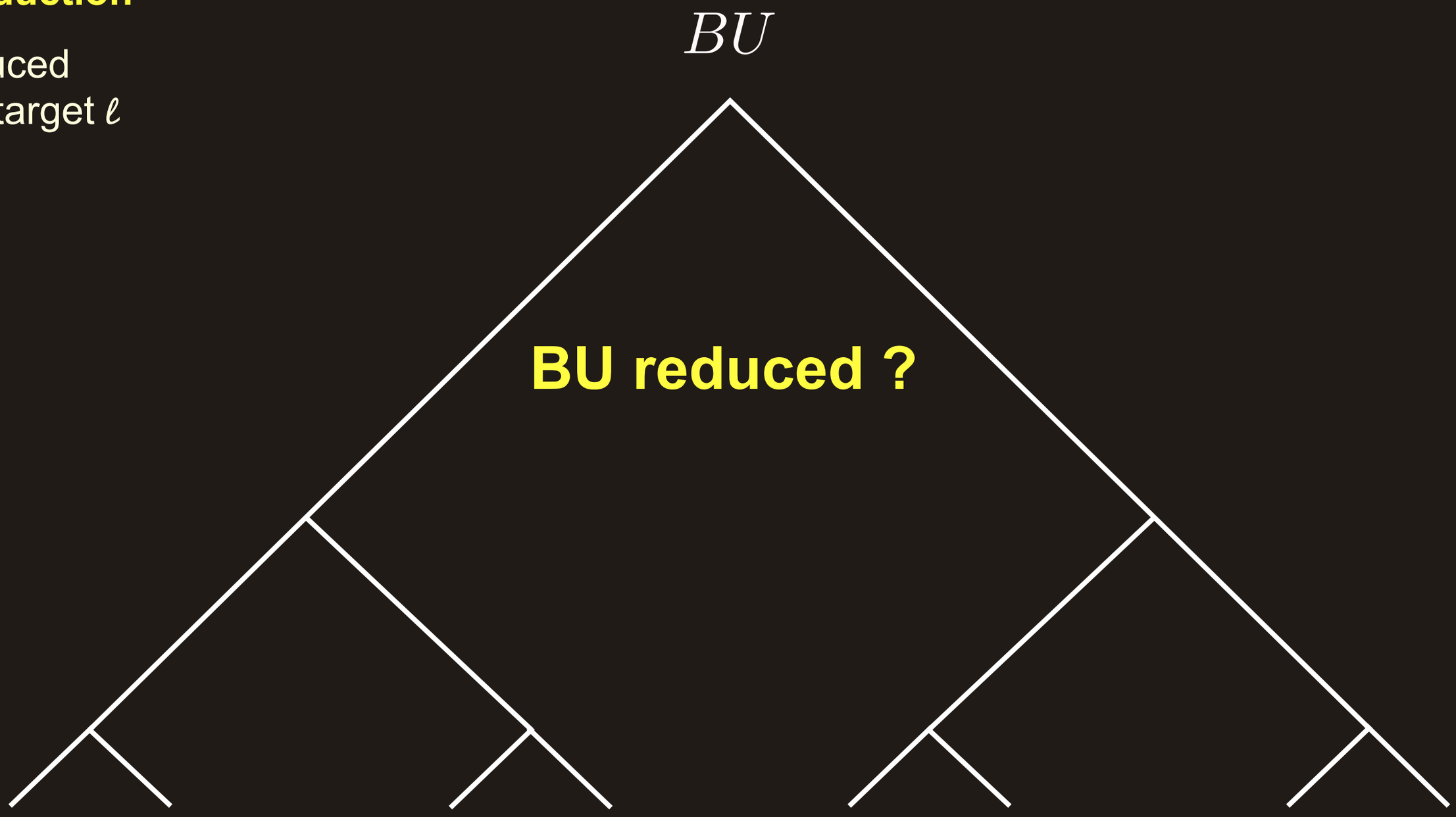
B reduced
lifting target ℓ

$$\sigma^{l/2}(\sigma^{l/2}BU_1)U_2\ ?$$



Recursive lift reduction

B reduced
lifting target ℓ



Recursive lift reduction

B reduced
lifting target ℓ

BU

BU reduced ?

Not quite ...

BU

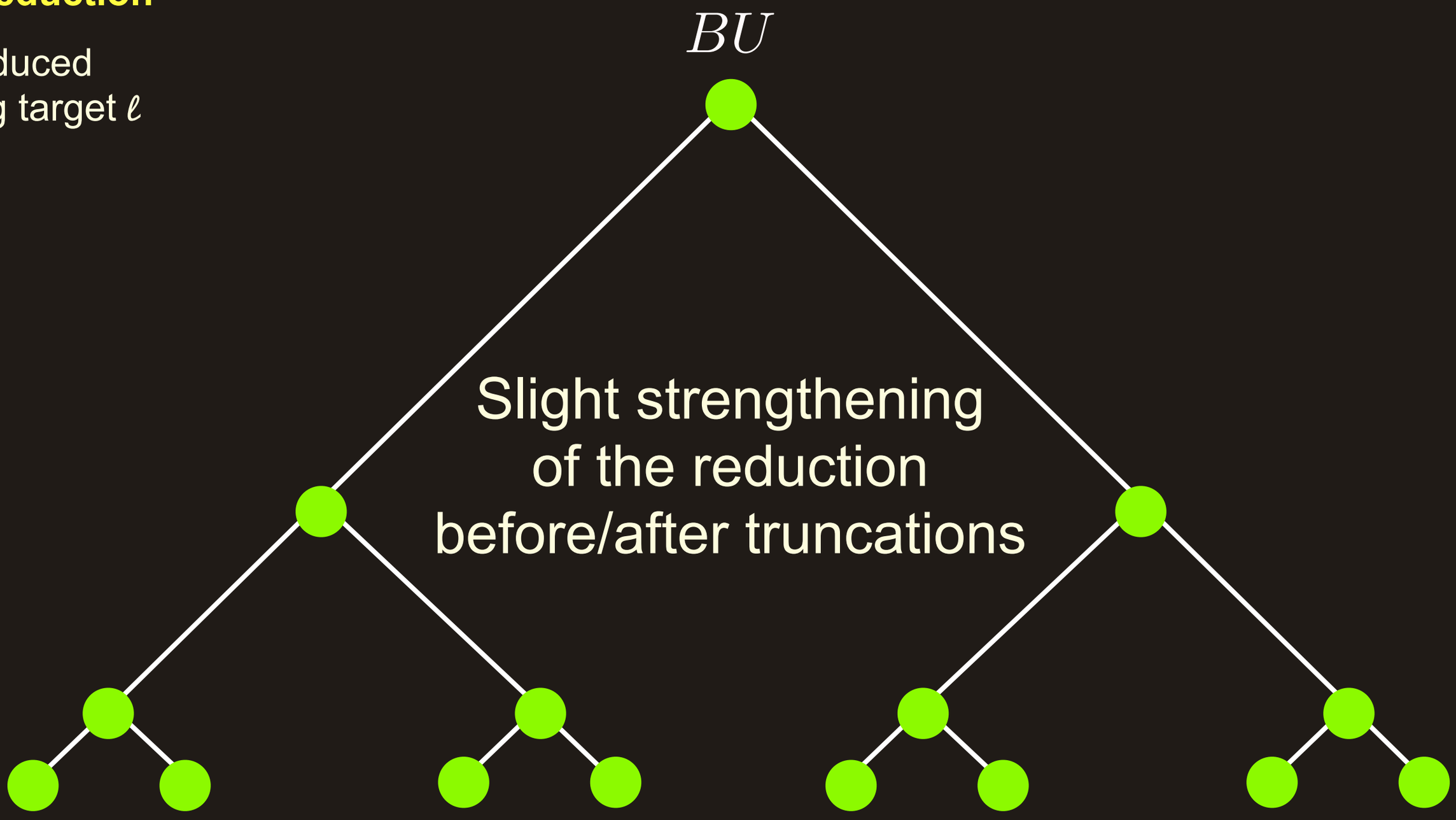
BU reduced ?

Not quite ...

‘’Loss of energy’’ (everywhere) from the precision adjustments

Recursive lift reduction

B reduced lifting target ℓ



+ low cost unimodular matrix product

Knuth-Schönhage: a quasi-linear time reduction

$\tilde{\mathrm{L}}^1$ algorithm Target quality Ξ

Strengthen quality to $\Xi' > \Xi$

First recursive call

$\sigma^{l/2} BU_1$

Strengthen quality to $\Xi'' > \Xi'$

Second recursive call

Strengthen quality to $\Xi''' > \Xi$

$U_1 \odot U_2$

Lift reduction is general

$$B = \begin{bmatrix} -5411049950 & -3092660736 & 22659461114 & -37476723816 \\ 650040948 & 371523735 & -2722105914 & 4502124756 \\ 1046272 & 597995 & -4381426 & 7246500 \\ -31574 & -18046 & 132220 & -218680 \end{bmatrix}$$

Lift reduction is general

$$\begin{bmatrix} 413216 & 20006 & -48 & 14866 \\ 0 & 421008 & -121197 & -181923 \\ 0 & 0 & 283 & -111 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

Via the Hermite normal form

Lift reduction is general

$$\begin{bmatrix} 413216 & 20006 & -48 & 14866 \\ 0 & 421008 & -121197 & -181923 \\ 0 & 0 & 283 & -111 \\ 0 & 0 & 0 & \boxed{2} \end{bmatrix}$$

Reduced

Lift reduction is general

$$\begin{bmatrix} 413216 & 20006 & -48 & 14866 \\ 0 & 421008 & -121197 & -181923 \\ 0 & 0 & 283 & -111 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

Lift reduction is general

$$\begin{bmatrix} 413216 & 20006 & -48 & 14866 \\ 0 & 421008 & -121197 & -181923 \\ 0.0 & 0.0 & 0.28300 & -0.11100 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

Lifting

Lift reduction is general

+ Propagation of the transformations

$$\left[\begin{array}{cc|cc} 413216 & 20006 & -48 & 14866 \\ 0 & 421008 & -121197 & -181923 \\ \hline 0.0 & 0.0 & 0.28300 & -0.11100 \\ 0 & 0 & 0 & 2 \end{array}\right]$$

Lifting

Lift reduction is general

$$\begin{bmatrix} 413216 & 20006 & -134252 & 333060 \\ 0 & 421008 & -111015 & -23928 \\ 0 & 0 & -11 & -28 \\ 0 & 0 & -10 & 26 \end{bmatrix}$$

Reduced

Lift reduction is general

$$\begin{bmatrix} 413216 & -59744 & 89612 & -36114 \\ 0 & 195 & -135 & -681 \\ 0 & 391 & 289 & 407 \\ 0 & -262 & 520 & -196 \end{bmatrix}$$

Reduced

Lift reduction is general

$$\begin{bmatrix} 8 & -1262 & 76 & -4984 \\ -315 & -1671 & 2319 & 1050 \\ -1751 & 101 & -761 & 986 \\ -254 & 2150 & 2344 & -2088 \end{bmatrix}$$

Reduced

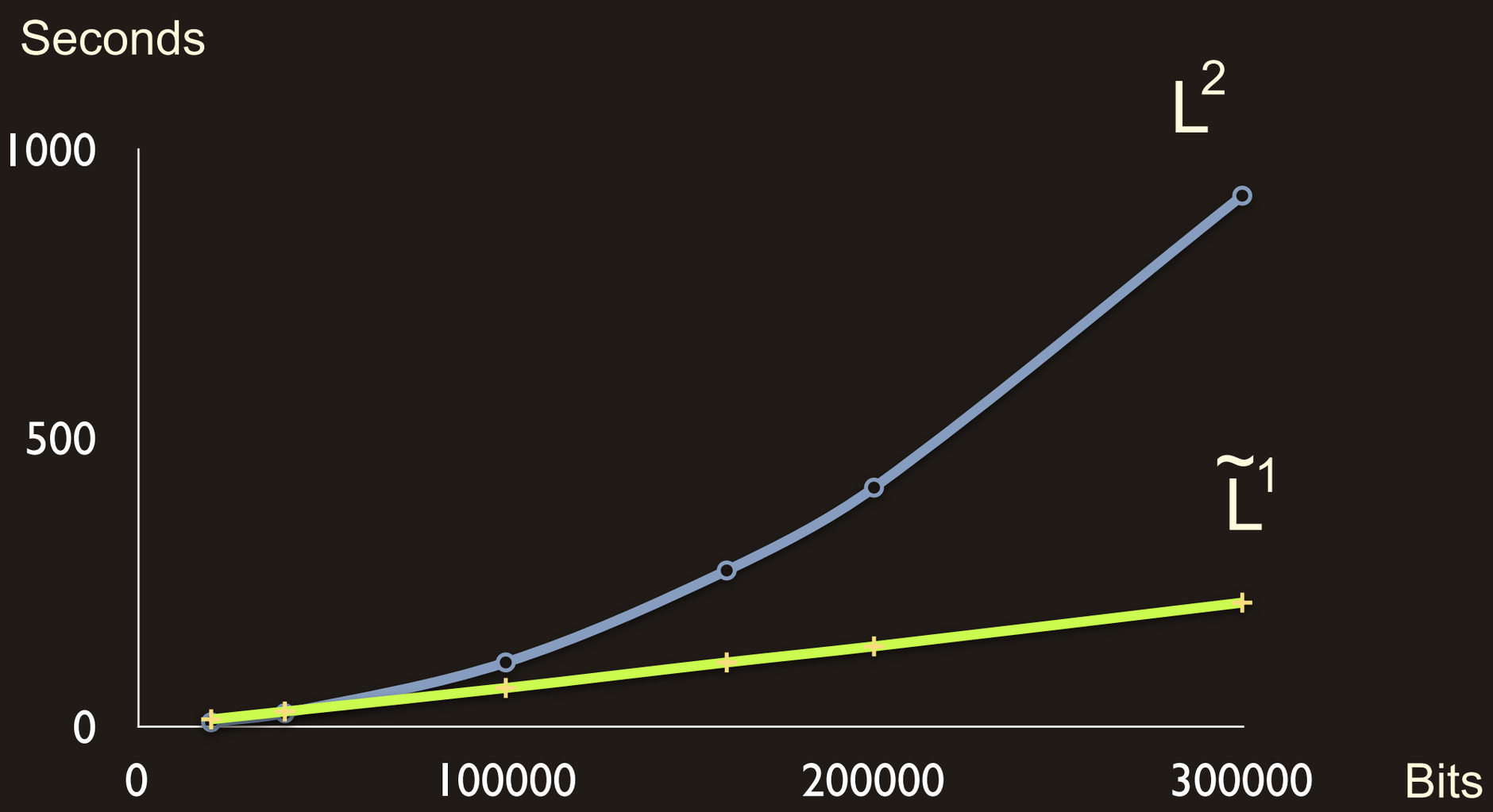
$\tilde{\mathrm{L}}^1$ basis reduction algorithm

$$\mathcal{P}oly(d)\tilde{O}(\beta)$$

[Novocin, Stehlé, V. 2010]

Execution time vs bit-length

Knapsack d=40



Open questions

- Minimal nullspace bases: core problem? Reduction vs relation finding?
- General setting with other new approaches

  [Hanrot, Pujol, Stehlé 2010] [Schnorr 2011]

- New reduction paradigms?
- “Essentially” the matrix product ? Basis reduction algorithm with cost $O^{\sim}(\mathrm{MM}(d, \beta))$?