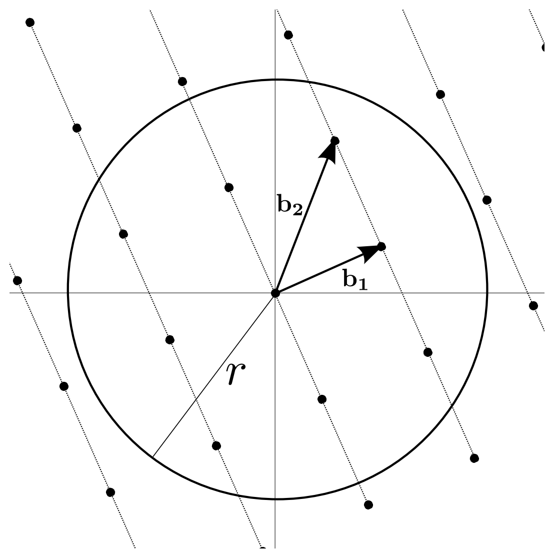
The Preprocessing of Lattice Point Enumeration

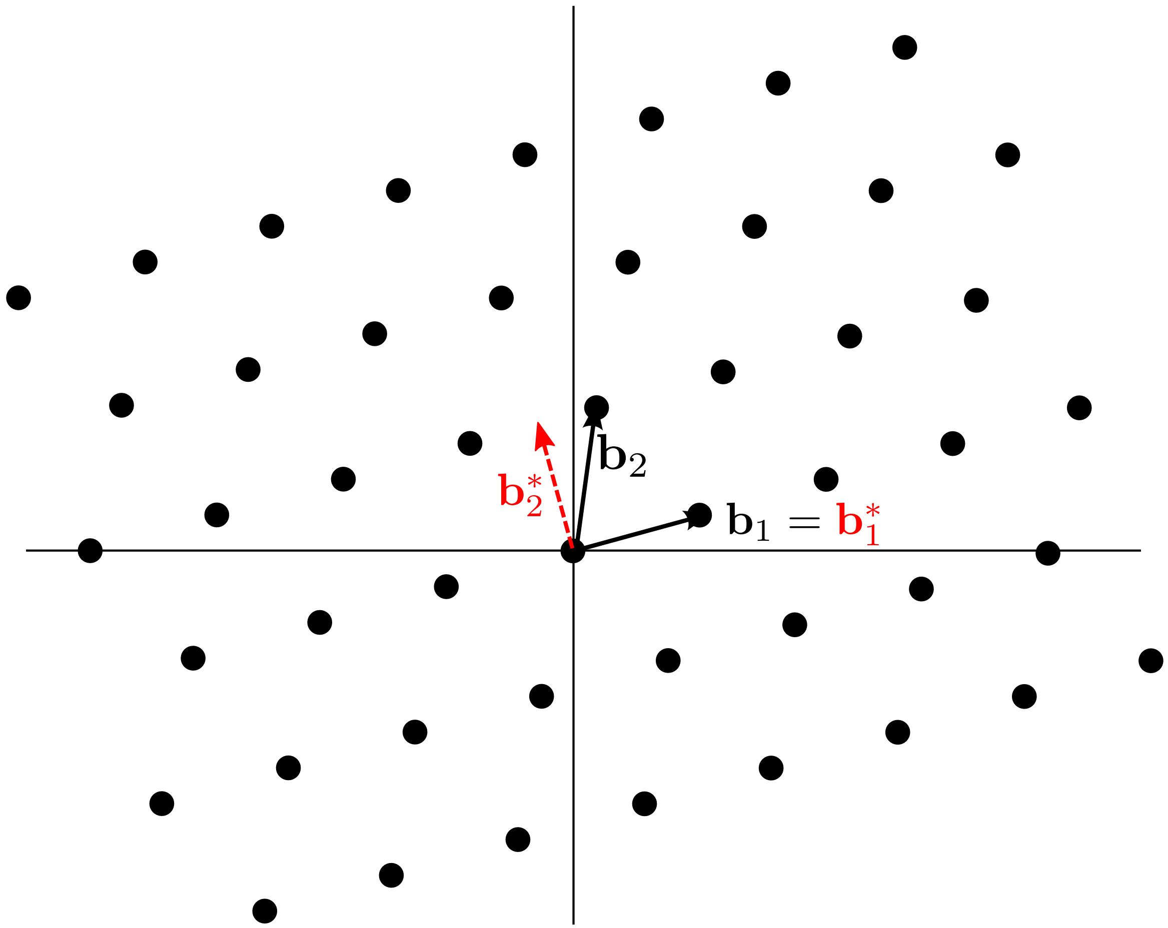


Daniele Micciancio

Michael Walter

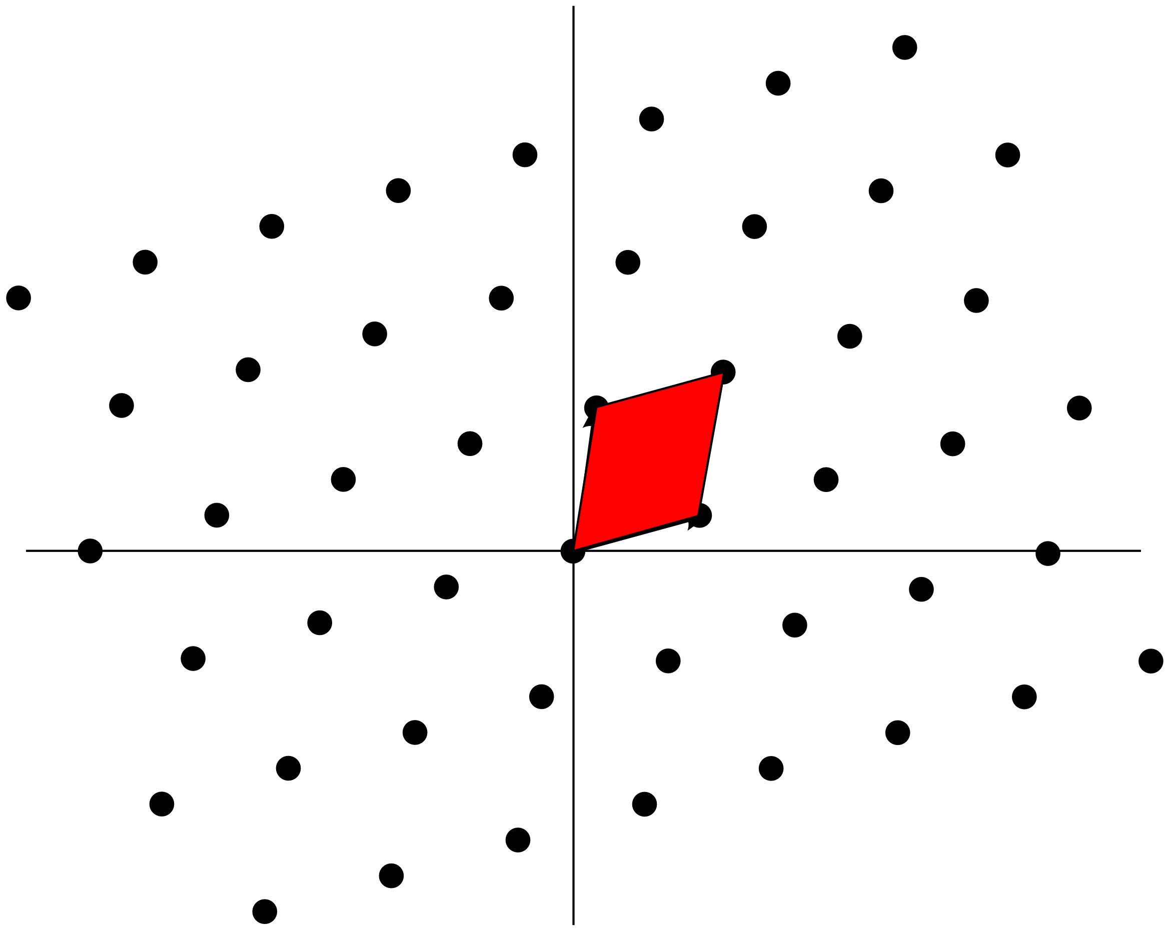
Mathematics of Modern Cryptography

Gram-Schmidt-Orthogonalization



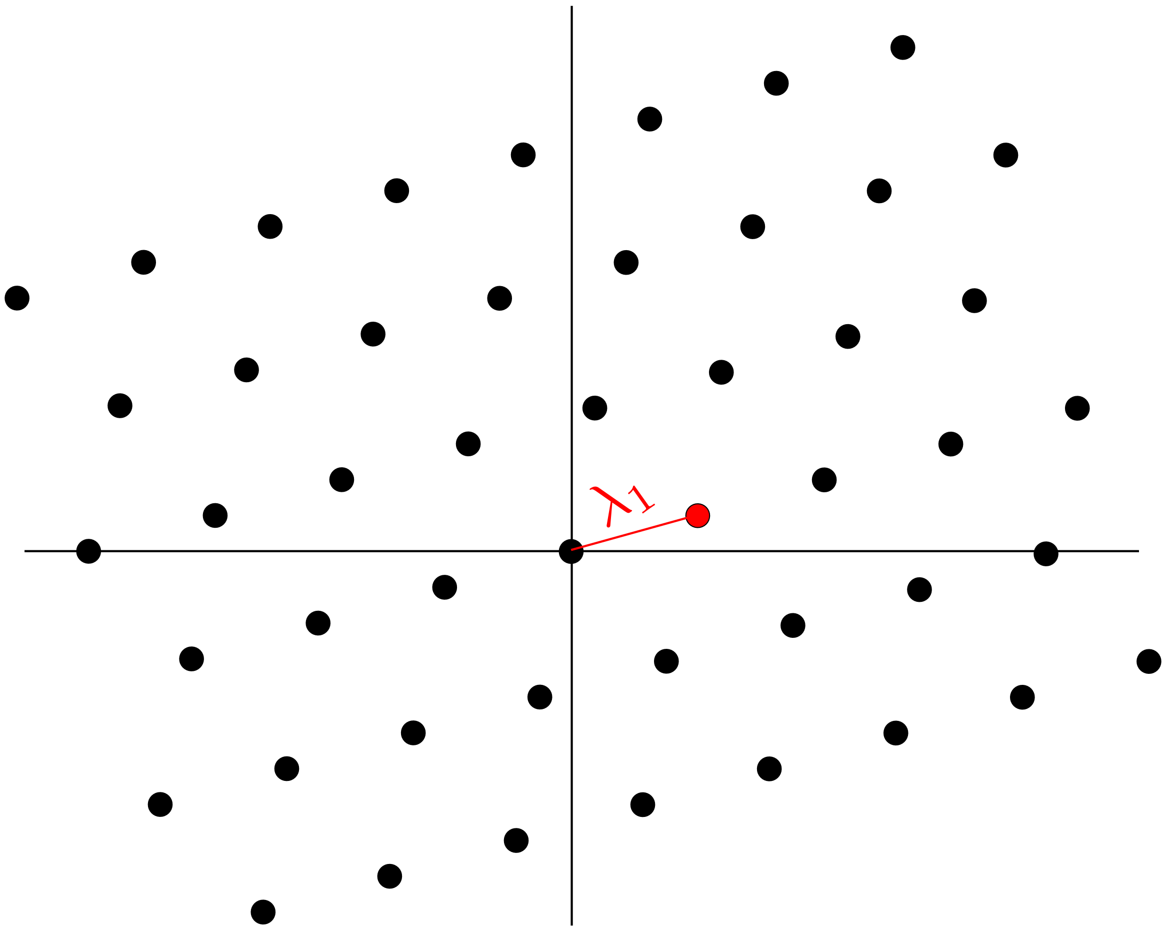
$$\mathbf{b}_i^* = \underbrace{\pi_{[\mathbf{b}_1,\ldots,\mathbf{b}_{i-1}]^\perp}}_{\pi_i}(\mathbf{b}_i)$$

Determinant

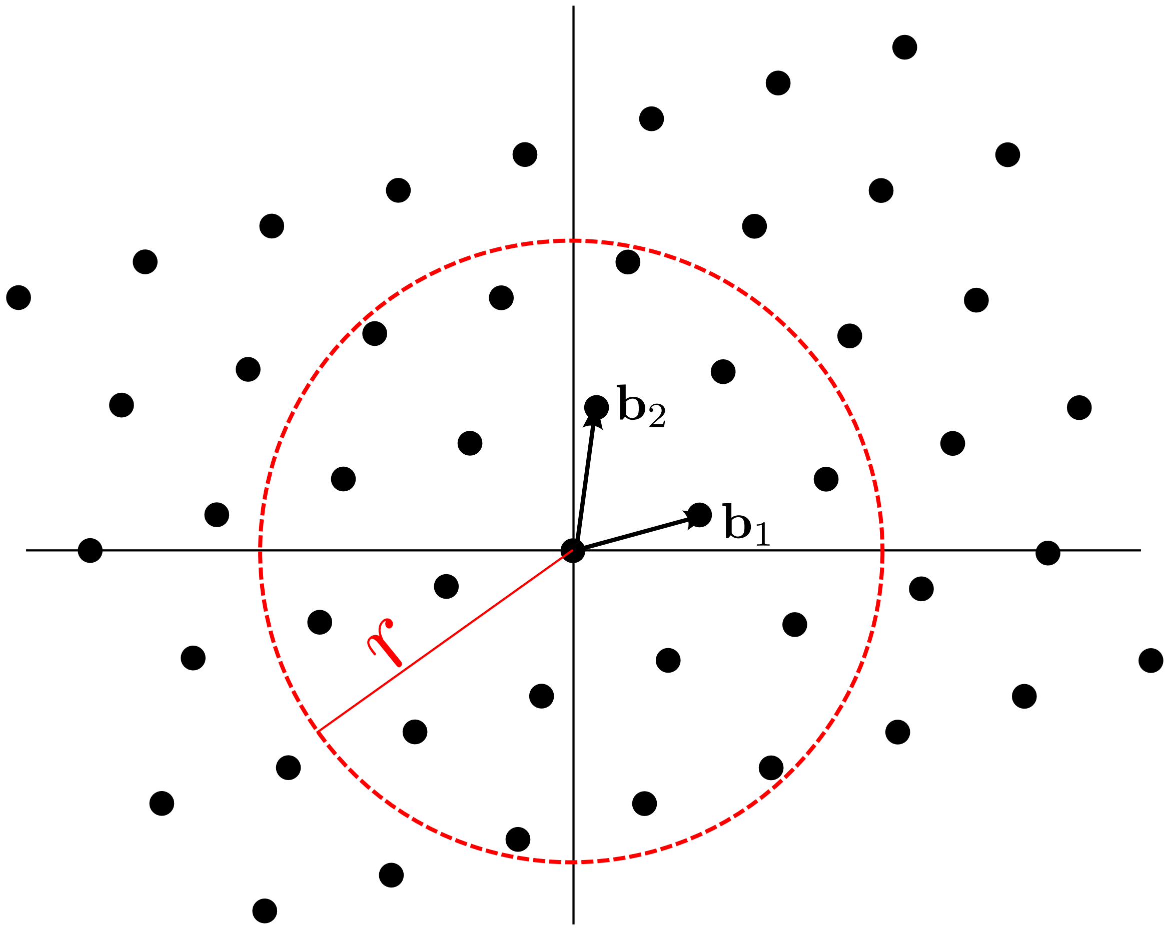


$$\det(\mathcal{L}(\mathbf{B})) = \prod_i \|\mathbf{b}_i^*\|$$

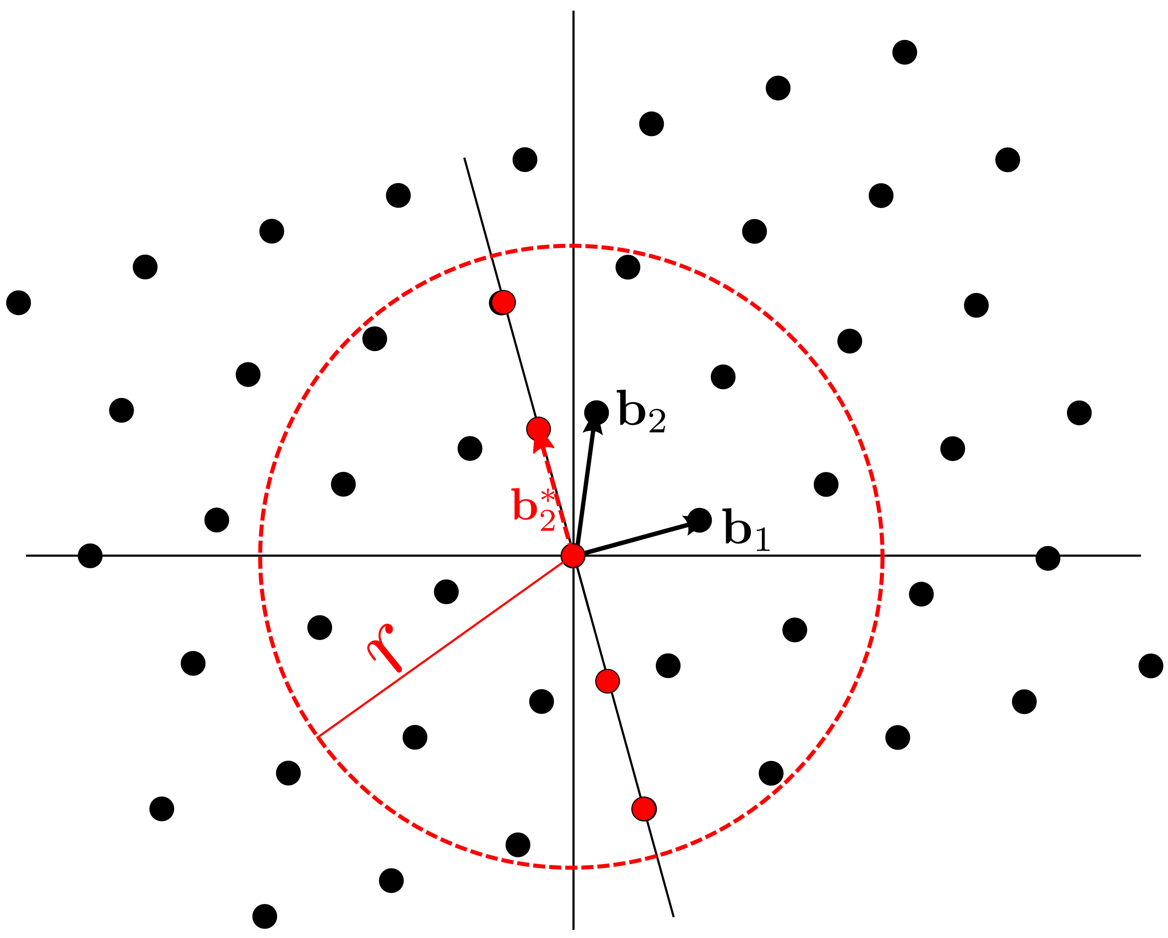
The Shortest Vector Problem



Enumeration

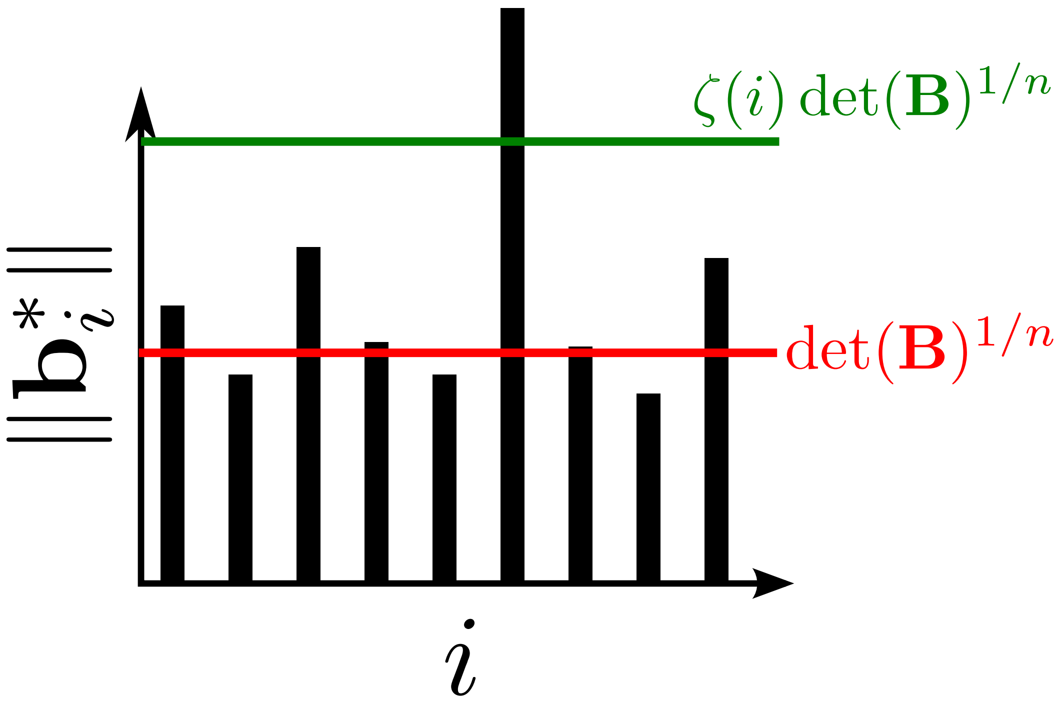


Enumeration



ζ-Reduction: Definition

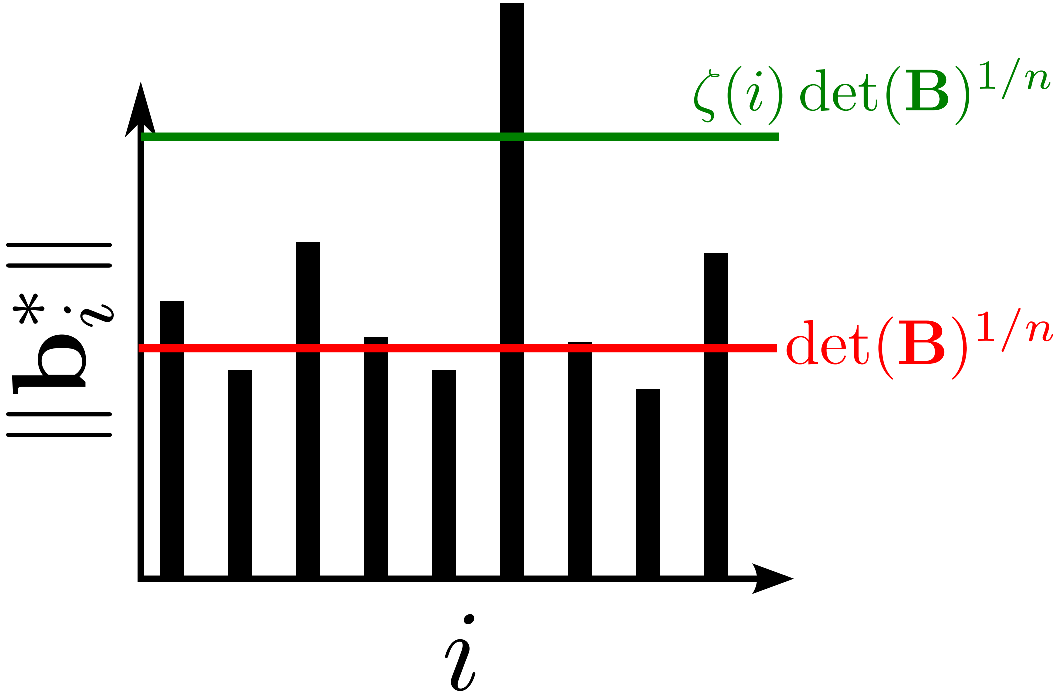
$$\|\mathbf{b}_i^*\| > \zeta(i)\det(\mathbf{B})^{1/n}$$



ζ-Reduction: Definition

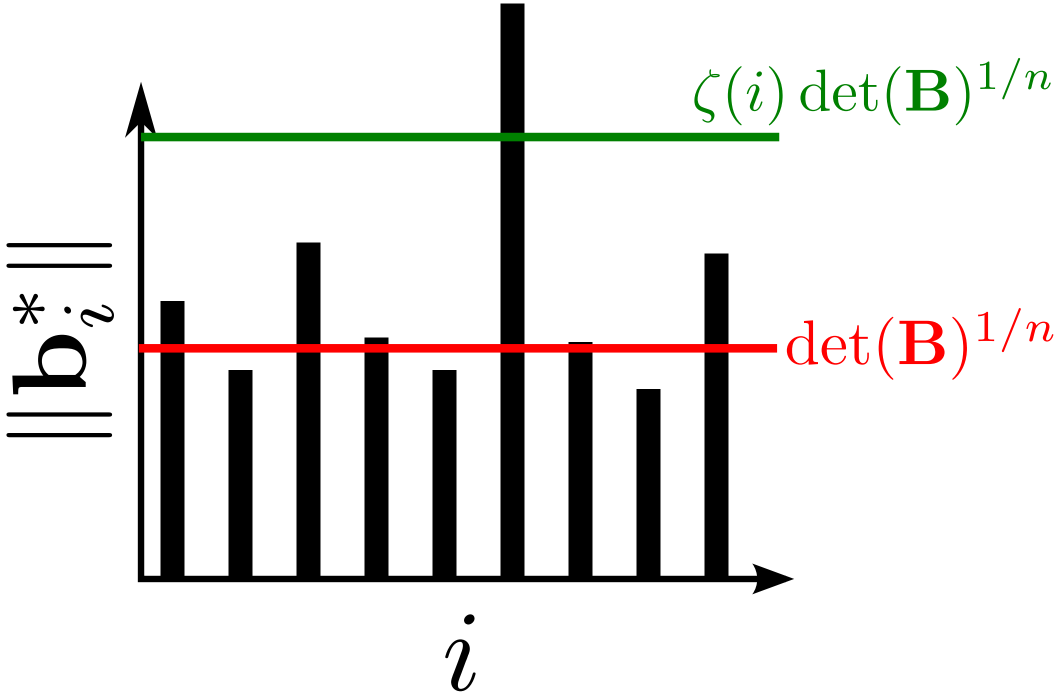
$$\|\mathbf{b}_i^*\| > \zeta(i)\det(\mathbf{B})^{1/n}$$

$$\Longrightarrow$$



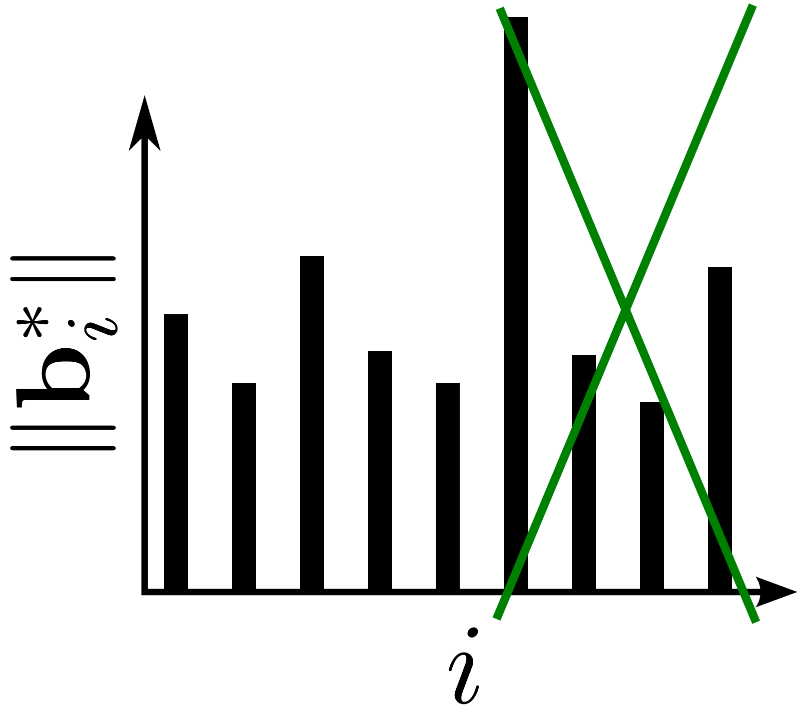
ζ-Reduction: Definition

$$\|\mathbf{b}_i^*\| > \zeta(i)\det(\mathbf{B})^{1/n}$$



$$\Longrightarrow$$

$$\lambda_1(\pi_i(\mathbf{B})) > \lambda_1(\mathbf{B})$$



ζ-Reduction: Theorem

$\mathbf{B}$ is ζ-reduced

$$\Longrightarrow$$

Enumeration solves SVP in $\mathcal{L}(\mathbf{B})$ in time $2^{O(n)}\Pi_i\zeta(i)$

Kannan

- HKZ: $\|\mathbf{b}_1\| = \lambda_1$, $\pi_1(\mathbf{B})$ is HKZ

Kannan

- HKZ: $\|\mathbf{b}_1\| = \lambda_1$, $\pi_1(\mathbf{B})$ is HKZ
- quasi-HKZ: $\|\mathbf{b}_1\| \leq 2\|\mathbf{b}_2^*\|$, $\pi_1(\mathbf{B})$ is HKZ

Kannan

- HKZ: $\|\mathbf{b}_1\| = \lambda_1$, $\pi_1(\mathbf{B})$ is HKZ

- quasi-HKZ: $\|\mathbf{b}_1\| \leq 2\|\mathbf{b}_2^*\|$, $\pi_1(\mathbf{B})$ is HKZ

$\|\mathbf{b}_1\| > 2\|\mathbf{b}_2^*\|$ (loops back to LLL)

`LLL`

`Recurse on` $\pi_1(\mathbf{B})$

`Enumerate to find` $\mathbf{v}$

`Recurse on` $\pi_{\mathbf{v}}(\mathbf{B})$

Kannan

$\|\mathbf{b}_1\| > 2\|\mathbf{b}_2^*\|$

`LLL`

`Recurse on` $\pi_1(\mathbf{B})$

`Enumerate to find` $\mathbf{v}$

`Recurse on` $\pi_{\mathbf{v}}(\mathbf{B})$

Kannan

$\|\mathbf{b}_1\| > 2\|\mathbf{b}_2^*\|$

LLL

Recurse on $\pi_1(\mathbf{B})$

Enumerate to find $\mathbf{v}$

Recurse on $\pi_{\mathbf{v}}(\mathbf{B})$

Kannan

$\|\mathbf{b}_1\| > 2\|\mathbf{b}_2^*\|$

LLL

Recurse on $\pi_{k}(\mathbf{B})$

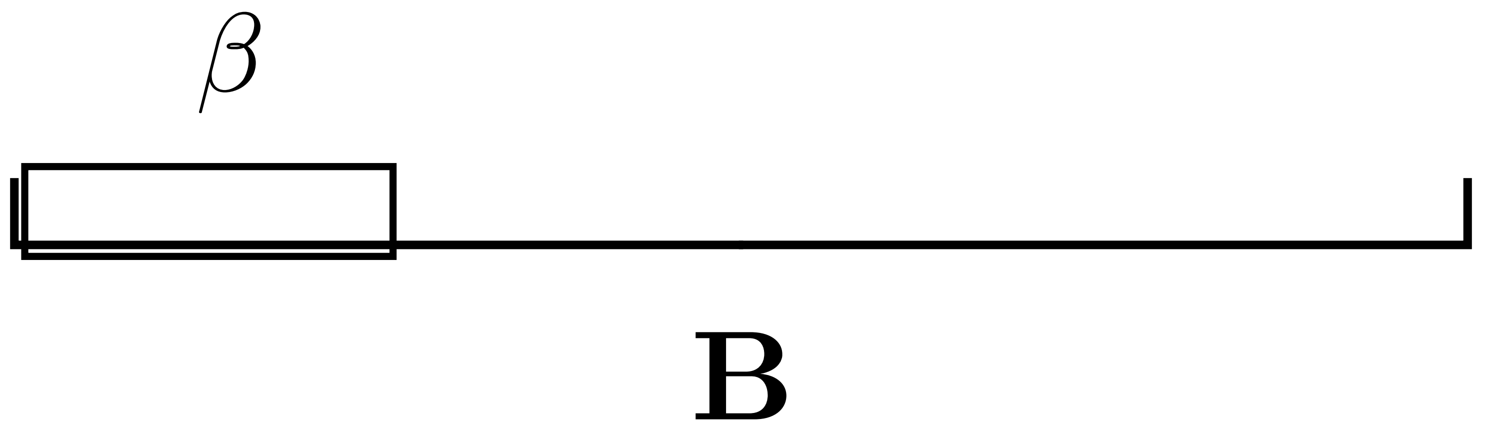
Enumerate to find $\mathbf{v}$

Recurse on $\pi_{\mathbf{v}}(\mathbf{B})$

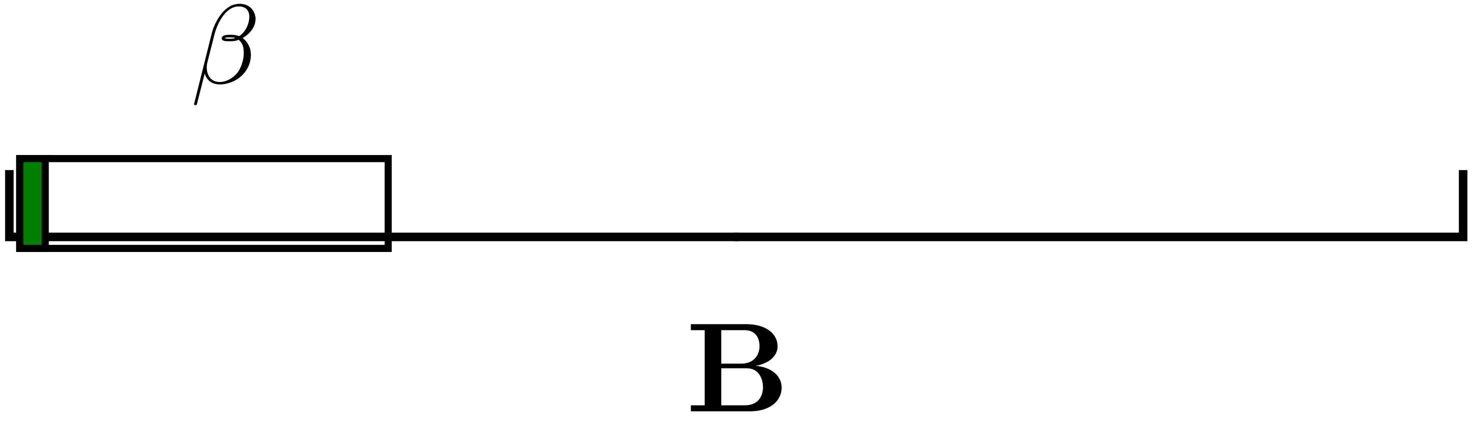
Block Reduction

$$\underbrace{\hspace{10cm}}_{\mathbf{B}}$$

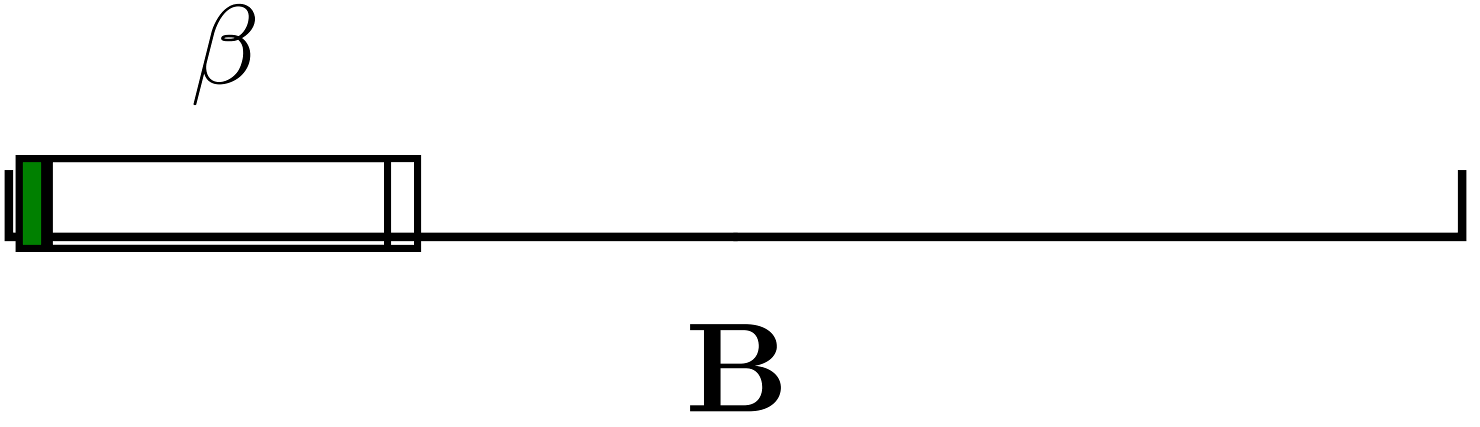
Block Reduction



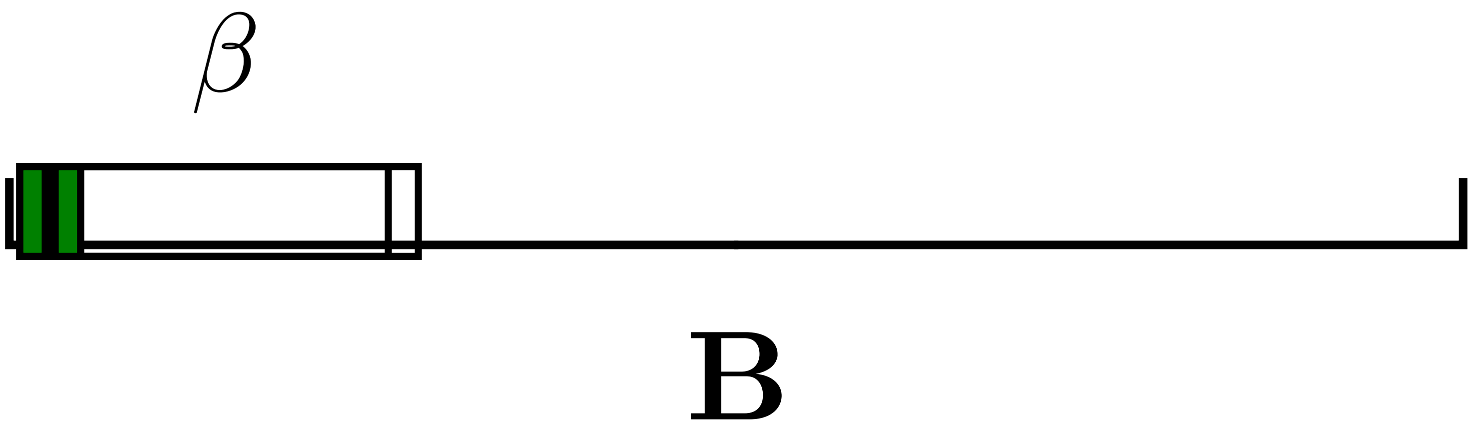
Block Reduction



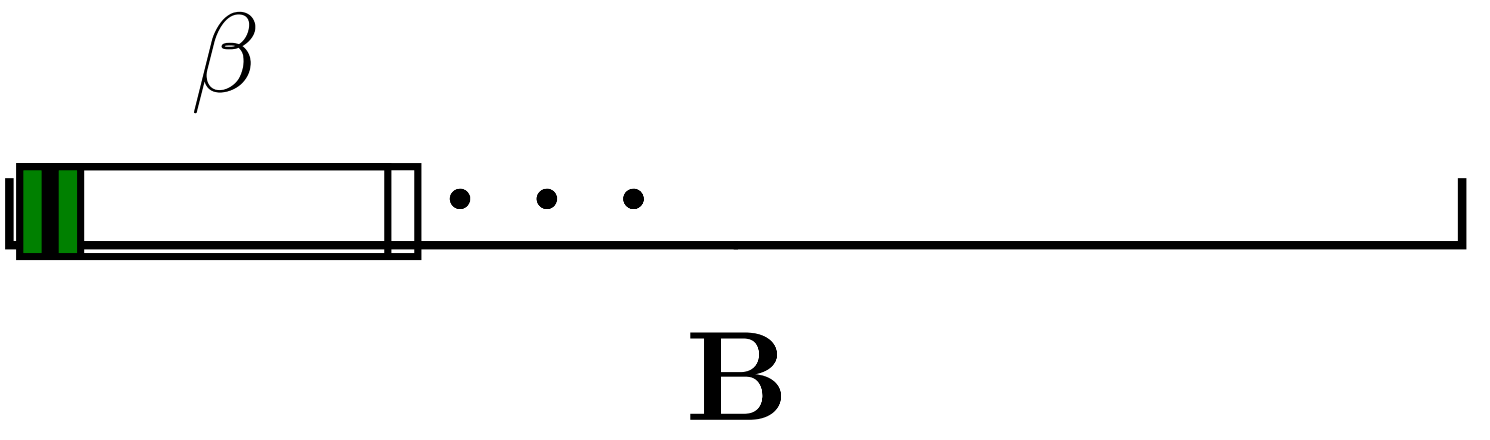
Block Reduction



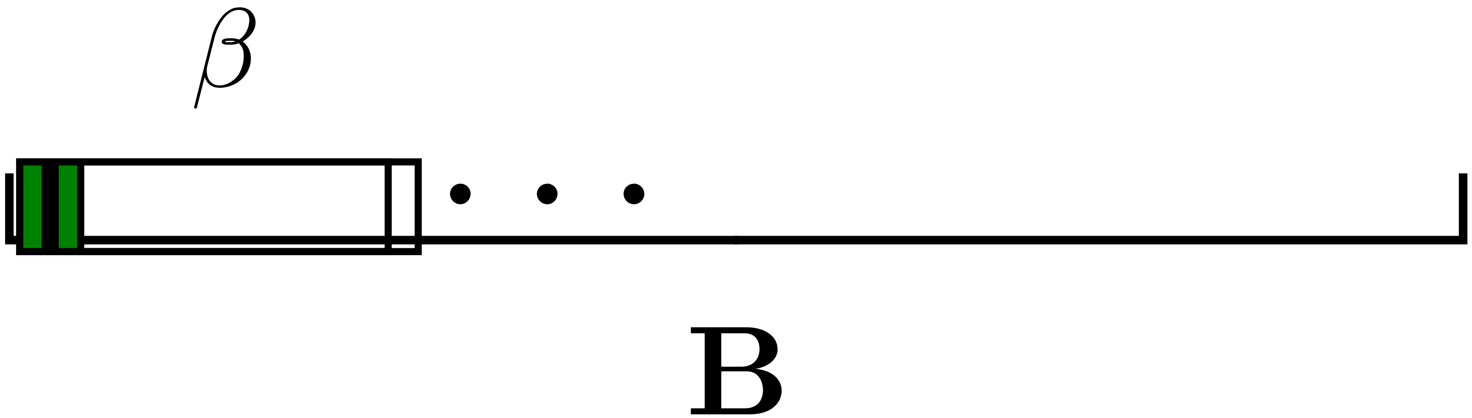
Block Reduction



Block Reduction



Block Reduction



$$\|\mathbf{b}_i^*\| = \lambda_1(\pi_i(\mathbf{B}_{[i,i+\beta]}))$$

Enumeration Complexity

Enumeration Complexity

Block Size: 2 (LLL)

Enumeration Complexity

Block Size: 2 (LLL)

$\zeta(i)$: $2^{O(n)}$

Enumeration Complexity

Block Size:	2 (LLL)
$\zeta(i)$:	$2^{O(n)}$
Enumeration:	$2^{O(n^2)}$

Enumeration Complexity

Block Size:	2 (LLL)	$n-1$
$\zeta(i)$:	$2^{O(n)}$	
Enumeration:	$2^{O(n^2)}$	

Enumeration Complexity

Block Size:	2 (LLL)	$n-1$
$\zeta(i)$:	$2^{O(n)}$	$\sqrt{n}$
Enumeration:	$2^{O(n^2)}$	

Enumeration Complexity

Block Size:	2 (LLL)	$n-1$
$\zeta(i)$:	$2^{O(n)}$	$\sqrt{n}$
Enumeration:	$2^{O(n^2)}$	$n^{O(n)}$

Enumeration Complexity

Block Size:	2 (LLL)	β	$n-1$
$\zeta(i)$:	$2^{O(n)}$		$\sqrt{n}$
Enumeration:	$2^{O(n^2)}$		$n^{O(n)}$

Enumeration Complexity

Block Size:	2 (LLL)	β	$n-1$
$\zeta(i)$:	$2^{O(n)}$	$\beta^{O(n/\beta)}$	$\sqrt{n}$
Enumeration:	$2^{O(n^2)}$		$n^{O(n)}$

Enumeration Complexity

Block Size:	2 (LLL)	β	$n-1$
$\zeta(i)$:	$2^{O(n)}$	$\beta^{O(n/\beta)}$	$\sqrt{n}$
Enumeration:	$2^{O(n^2)}$	$\beta^{O(n^2/\beta)}$	$n^{O(n)}$