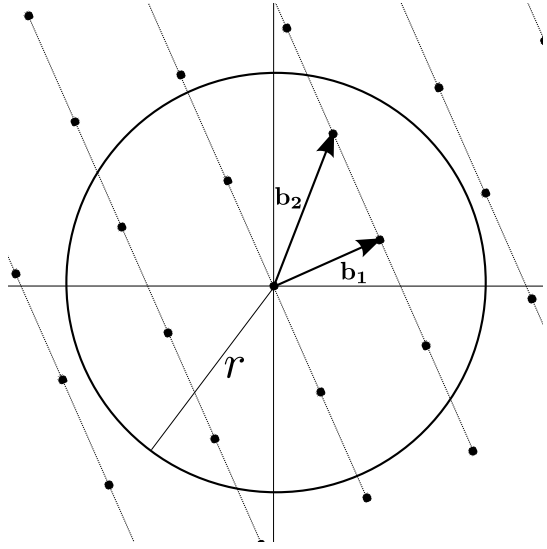
# SVP by Enumeration

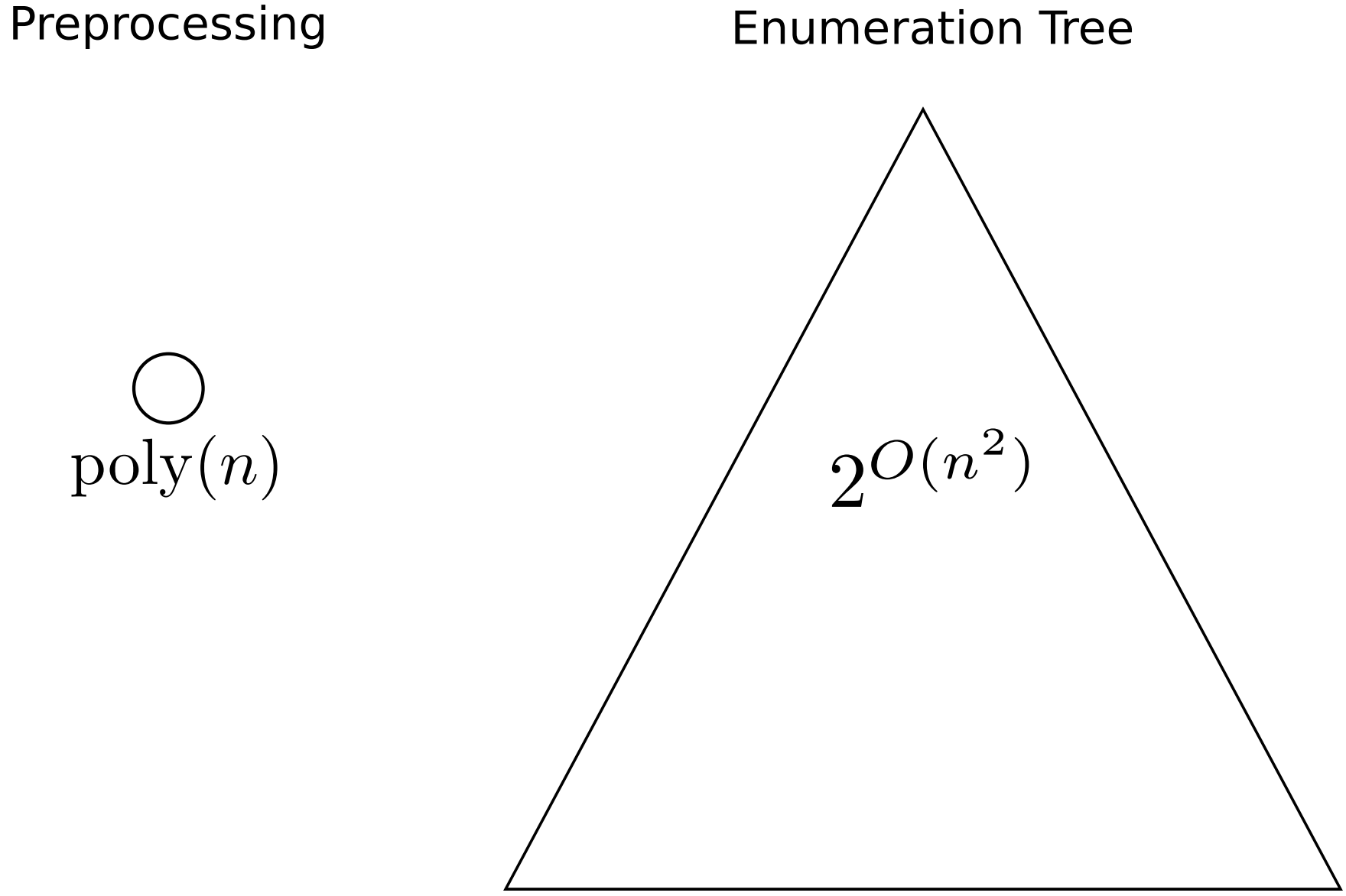
## Bridging the Gap between Theory and Practice




Michael Walter Daniele Micciancio

UCSD

# Preprocessing LLL: Fincke-Pohst



# Recursive Preprocessing: Kannan

Preprocessing

$\underbrace{2^{O(n \log \log n)}}$

# recursive calls

Enumeration Tree

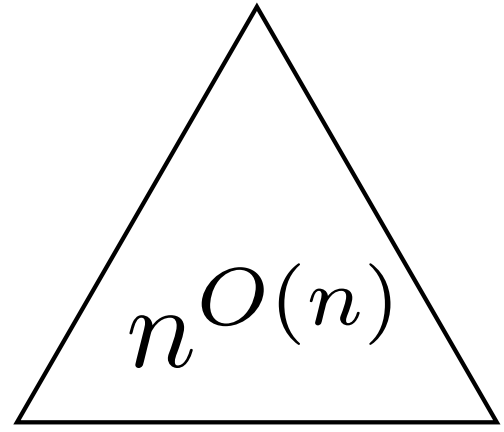
$n^{O(n)}$

# Recursive Preprocessing: Kannan

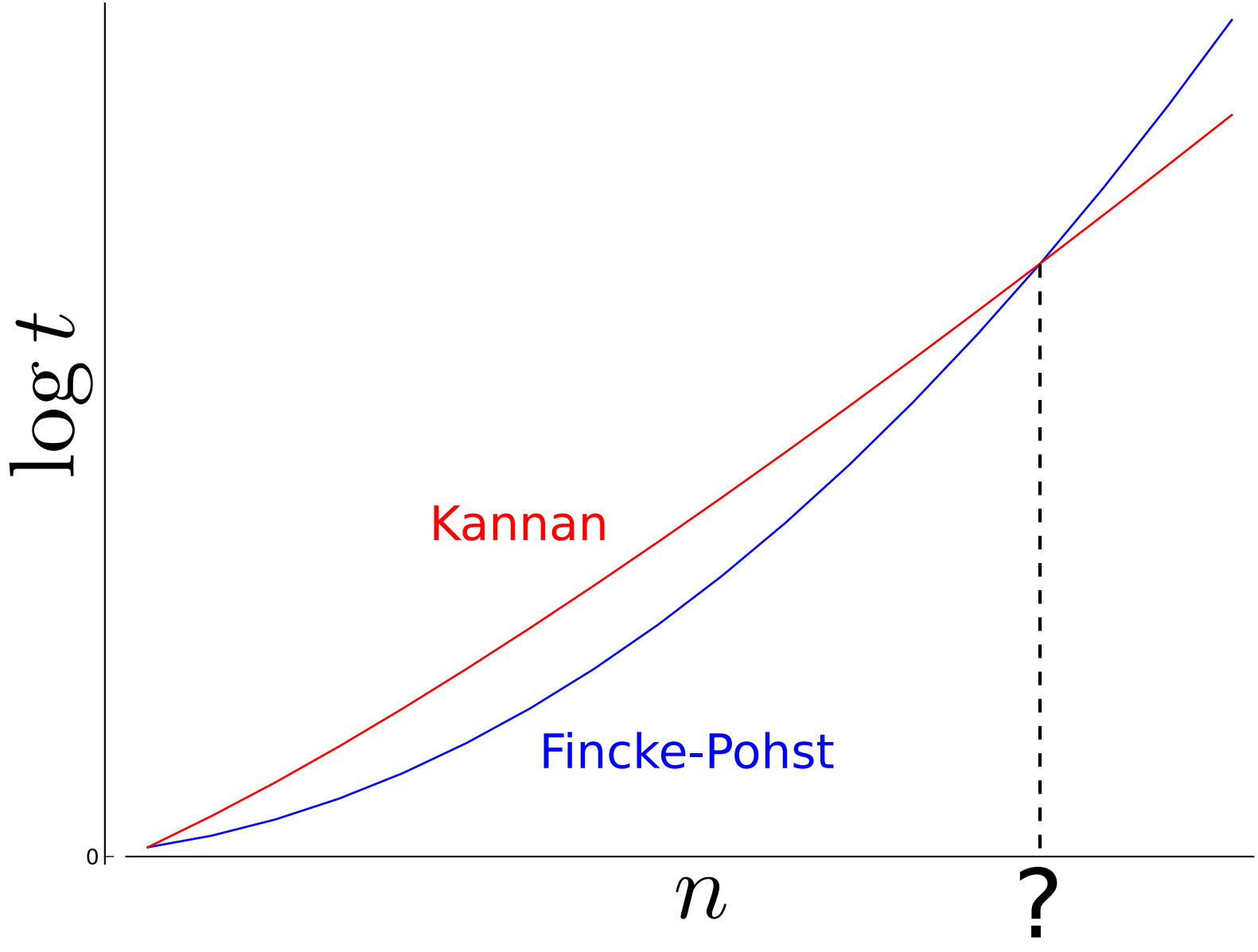
Preprocessing

$$\underbrace{2^{O(n \log \log n)}}_{\text{\# recursive calls}} n^{O(n)}$$

Enumeration Tree

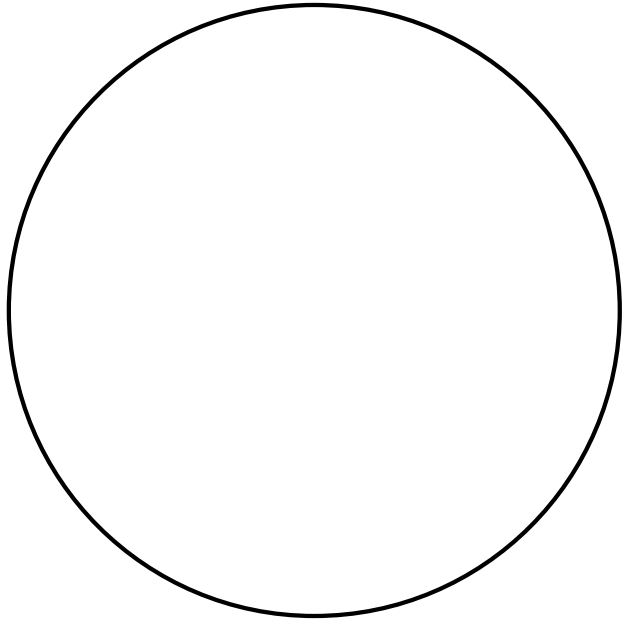


# Fincke-Pohst vs Kannan



# Our Algorithm

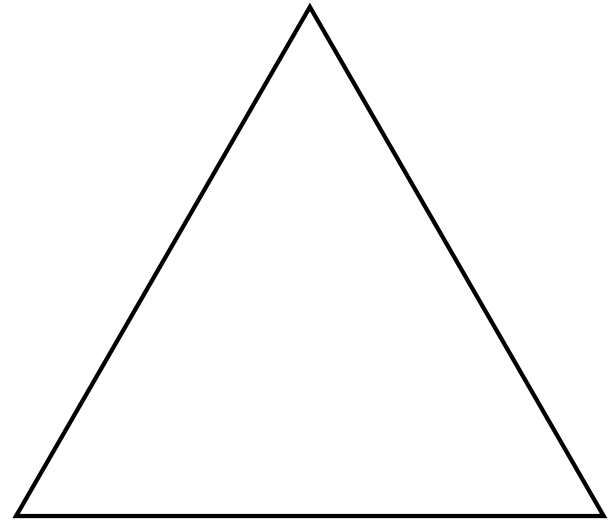
Preprocessing



$\underbrace{2^{O(n/k)}}$

# recursive calls

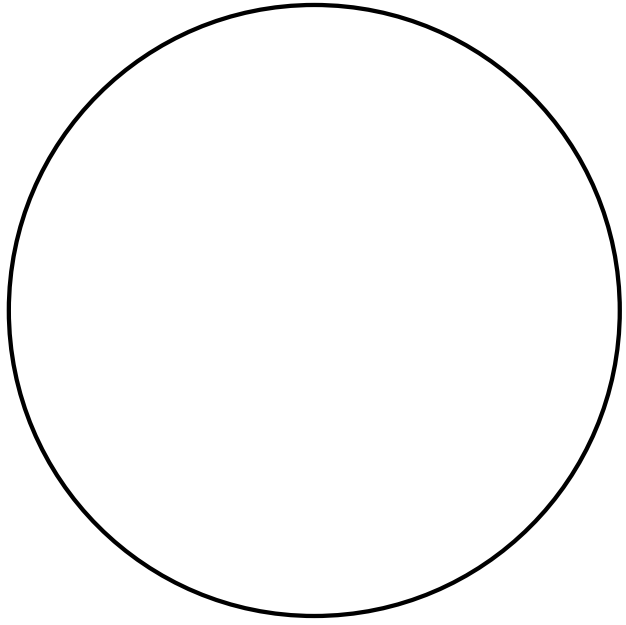
Enumeration Tree



$2^{O(nk)}n^{O(n-k)}$

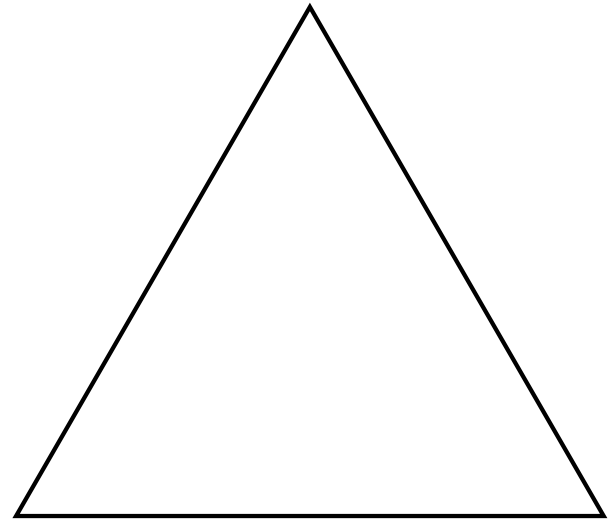
# Our Algorithm

Preprocessing



$$\underbrace{2^{O(n/k)}}_{\text{\# recursive calls}} n^{O(n-k)}$$

Enumeration Tree



$$2^{O(nk)} n^{O(n-k)}$$

# Fincke-Pohst vs Our Algorithm