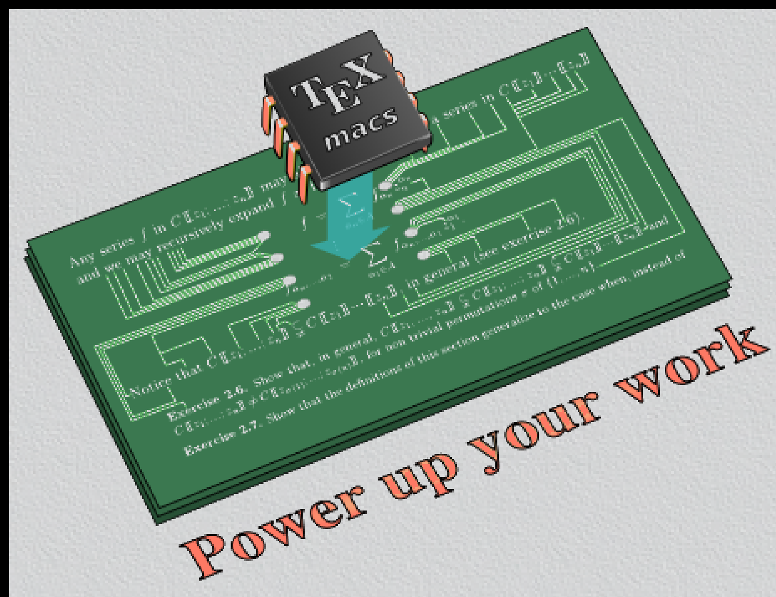
Sparse polynomial interpolation

Joris van der Hoeven

CNRS, LIX

Parts in joint work with Grégoire Lecerf

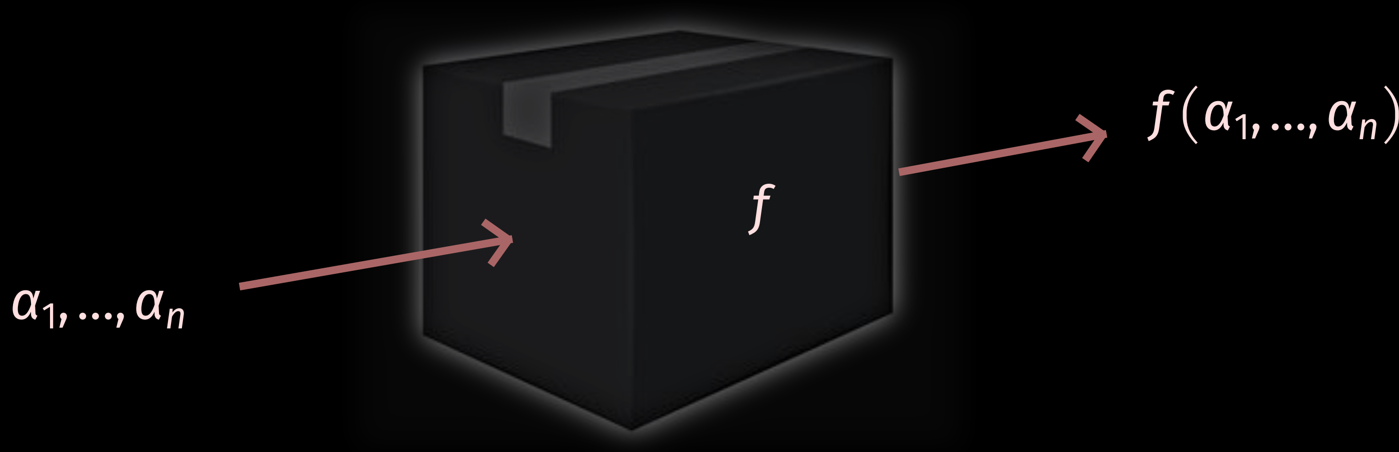


École polytechnique **December 12, 2022**

Part I

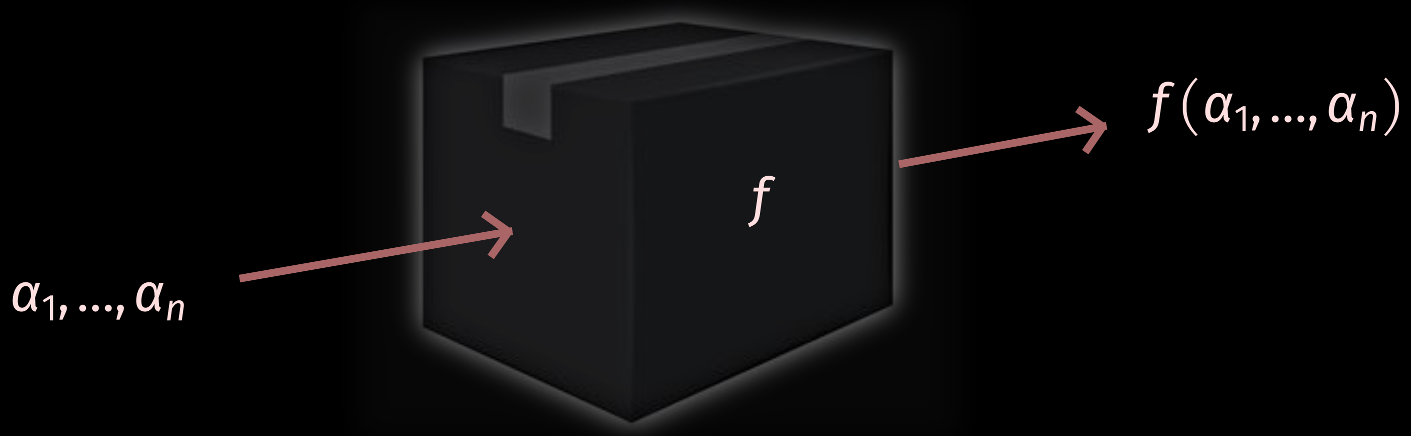
Statement of the problem

Input



Black box functions and their interpolation

Input



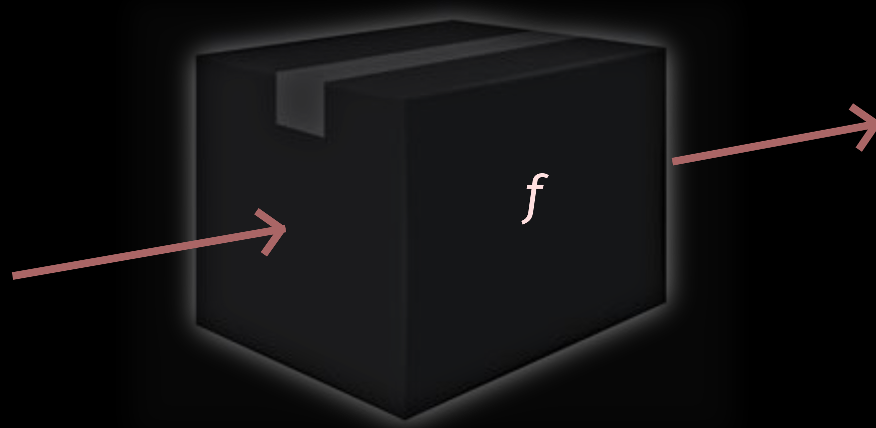
Output

$$f(x_1, \ldots, x_n) = c_1 x_1^{e_{1,1}} \cdots x_n^{e_{1,n}} + \cdots + c_t x_1^{e_{t,1}} \cdots x_n^{e_{t,n}}$$

Example

Input

$$\alpha_{1,1}, \alpha_{1,2}, \alpha_{1,3},\\ \alpha_{2,1}, \alpha_{2,2}, \alpha_{2,3},\\ \alpha_{3,1}, \alpha_{3,2}, \alpha_{3,3}$$



$$\begin{vmatrix} \alpha_{1,1} & \alpha_{1,2} & \alpha_{1,3} \\ \alpha_{2,1} & \alpha_{2,2} & \alpha_{2,3} \\ \alpha_{3,1} & \alpha_{3,2} & \alpha_{3,3} \end{vmatrix}$$

Input

$\alpha_{1,1}, \alpha_{1,2}, \alpha_{1,3},$
$\alpha_{2,1}, \alpha_{2,2}, \alpha_{2,3},$
$\alpha_{3,1}, \alpha_{3,2}, \alpha_{3,3}$

$$\begin{vmatrix} \alpha_{1,1} & \alpha_{1,2} & \alpha_{1,3} \\ \alpha_{2,1} & \alpha_{2,2} & \alpha_{2,3} \\ \alpha_{3,1} & \alpha_{3,2} & \alpha_{3,3} \end{vmatrix}$$

Example

Input

Gaussian elimination

$$\alpha_{1,1}, \alpha_{1,2}, \alpha_{1,3},$$
$$\alpha_{2,1}, \alpha_{2,2}, \alpha_{2,3},$$
$$\alpha_{3,1}, \alpha_{3,2}, \alpha_{3,3}$$

$$\begin{vmatrix} \alpha_{1,1} & \alpha_{1,2} & \alpha_{1,3} \\ \alpha_{2,1} & \alpha_{2,2} & \alpha_{2,3} \\ \alpha_{3,1} & \alpha_{3,2} & \alpha_{3,3} \end{vmatrix}$$

Output

$$x_{1,1}x_{2,2}x_{3,3} - x_{1,1}x_{2,3}x_{3,2} + x_{1,2}x_{2,3}x_{3,1} - x_{1,2}x_{2,1}x_{3,3} + x_{1,3}x_{2,1}x_{3,2} - x_{1,3}x_{2,2}x_{3,1}$$

Variants

Coefficient ring or field $\mathbb{K}$

- A field from analysis such as $\mathbb{K} = \mathbb{C}$.
- A discrete field such as $\mathbb{K} = \mathbb{Q}$ or a finite field $\mathbb{K} = \mathbb{F}_q$.

Variants

Coefficient ring or field $\mathbb{K}$

- A field from analysis such as $\mathbb{K} = \mathbb{C}$.
- A discrete field such as $\mathbb{K} = \mathbb{Q}$ or a finite field $\mathbb{K} = \mathbb{F}_q$.

Complexity model

- Algebraic *versus* bit complexity.
- Deterministic (needs bounds) *versus* probabilistic.
- Theoretic (asymptotic) *versus* practical complexity.
- Divisions in $\mathbb{K}$ allowed for evaluation of f ?
- Allow evaluations at points in $\mathbb{A}^n$ for some $\mathbb{K}$-algebra $\mathbb{A}$?

Variants

Coefficient ring or field $\mathbb{K}$

- A field from analysis such as $\mathbb{K} = \mathbb{C}$.
- A discrete field such as $\mathbb{K} = \mathbb{Q}$ or a finite field $\mathbb{K} = \mathbb{F}_q$.

Complexity model

- Algebraic *versus* bit complexity.
- Deterministic (needs bounds) *versus* probabilistic.
- Theoretic (asymptotic) *versus* practical complexity.
- Divisions in $\mathbb{K}$ allowed for evaluation of f?
- Allow evaluations at points in $\mathbb{A}^n$ for some $\mathbb{K}$-algebra $\mathbb{A}$?

How sparse?

- Weakly sparse: total degrees d of the order $O(\log t)$.
- Normally sparse: total degrees d of the order $t^{O(1)}$.
- Super sparse: total degrees of order d with $\log t = o(\log d)$.

Short history

Old work

- Prony [1795]
- Zippel [1979, 1990]

Old work

- Prony [1795]
- Zippel [1979, 1990]

Rediscovery and early work in computer algebra

- Ben-Or Tiwari [1988]
- Kaltofen-Yagati [1988], Canny-Kaltofen-Lakshman [1989], Kaltofen-Trager [1990], Kaltofen-Lakshman-Wiley [1990]
- Huang-Rao [1996], Murao-Fujise [1996]

Short history

Old work

- Prony [1795]
- Zippel [1979, 1990]

Rediscovery and early work in computer algebra

- Ben-Or Tiwari [1988]
- Kaltofen-Yagati [1988], Canny-Kaltofen-Lakshman [1989], Kaltofen-Trager [1990], Kaltofen-Lakshman-Wiley [1990]
- Huang-Rao [1996], Murao-Fujise [1996]

Early implementations

- Diaz-Kaltofen [1988] FOXFOX
- Freeman-Imirzian-Kaltofen-Lakshman [1988] Dagwood

Short history continued...

Recent work

- Garg-Schost [2009]
- Javadi-Monagan [2010], Hu-Monagan [2013, 2016], Monagan-Tuncer [2015, 2019], Monagan-Wong [2016]
- Giesbrecht-Roche [2011], Arnold-Giesbrecht-Roche [2014, 2016], Arnold-Roche [2014], Roche [2018]
- vdH-Lecerf [2009, 2013, 2015, 2019], Grenet-vdH-Lecerf [2015, 2016]
- Huang-Gao [2017], Huang [2019]

Short history continued...

Recent work

- Garg-Schost [2009]
- Javadi-Monagan [2010], Hu-Monagan [2013, 2016], Monagan-Tuncer [2015, 2019], Monagan-Wong [2016]
- Giesbrecht-Roche [2011], Arnold-Giesbrecht-Roche [2014, 2016], Arnold-Roche [2014], Roche [2018]
- vdH-Lecerf [2009, 2013, 2015, 2019], Grenet-vdH-Lecerf [2015, 2016]
- Huang-Gao [2017], Huang [2019]

Modern implementations

- Monagan [2010–] Maple
- vdH-Lecerf [2009, 2015–] Mathemagix
- Demin [2022-] Julia

Part II

Reductions

Probabilistic verification of correctness

Lemma (Schwartz–Zippel)

Let $f \in \mathbb{K}[x_1, \ldots, x_n]$ *be non-zero of total degree* $d > 0$

Let $S \subseteq \mathbb{K}$ *be a finite set with* $|S|$ *elements*

For a random $(x_1, \ldots, x_n) \in S^n$*, we have*

$$\Pr(f(x_1, \ldots, x_n) = 0) \leqslant \frac{d}{|S|}$$

Probabilistic verification of correctness

Lemma (Schwartz–Zippel)

Let $f \in \mathbb{K}[x_1, \ldots, x_n]$ *be non-zero of total degree* $d > 0$

Let $S \subseteq \mathbb{K}$ *be a finite set with* $|S|$ *elements*

For a random $(x_1, \ldots, x_n) \in S^n$*, we have*

$$\Pr(f(x_1, \ldots, x_n) = 0) \leqslant \frac{d}{|S|}$$

Fast collection of information

Probabilistic verification of correctness

Lemma (Schwartz–Zippel)

Let $f \in \mathbb{K}[x_1, \ldots, x_n]$ *be non-zero of total degree* $d > 0$

Let $S \subseteq \mathbb{K}$ *be a finite set with* $|S|$ *elements*

For a random $(x_1, \ldots, x_n) \in S^n$*, we have*

$$\Pr(f(x_1, \ldots, x_n) = 0) \leqslant \frac{d}{|S|}$$

Fast collection of information

- f is a constant in $\mathbb{K}$? $f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$ for random $x, y \in \mathbb{K}^n$

Probabilistic verification of correctness

Lemma (Schwartz–Zippel)

Let $f \in \mathbb{K}[x_1, \dots, x_n]$ be non-zero of total degree $d > 0$

Let $S \subseteq \mathbb{K}$ be a finite set with $|S|$ elements

For a random $(x_1, \dots, x_n) \in S^n$, we have

$$\Pr(f(x_1, \dots, x_n) = 0) \leqslant \frac{d}{|S|}$$

Fast collection of information

- f is a constant in $\mathbb{K}$? $\quad f(x_1, \dots, x_n) = f(y_1, \dots, y_n)$ for random $x, y \in \mathbb{K}^n$
- f is linear in x_1? $\quad \begin{vmatrix} \alpha & f(\alpha, x_2, \dots, x_n) - f(0, x_2, \dots, x_n) \\ \beta & f(\beta, x_2, \dots, x_n) - f(0, x_2, \dots, x_n) \end{vmatrix} = 0$ for random $\alpha, \beta \in \mathbb{K}$, $x \in \mathbb{K}^n$

Reduction to case with known bounds

Algorithm

Input: a polynomial black box function $f(x_1, \ldots, x_n)$

Output: the sparse interpolation f^* of f

1. Set initial bounds $T := 1$ and $D := 1$ for t and the total degree d of f
2. Determine the sparse interpolation f^* of f using these bounds
3. If $f = f^*$ with high probability, then return f^*
4. Increase T and/or D and return to step 2

Algorithm

Input: a polynomial black box function $f(x_1, \ldots, x_n)$

Output: the sparse interpolation f^* of f

1. Let $f^* := 0$ be an initial approximation of f
2. Determine the approximate sparse interpolation δ^* of $\delta := f - f^*$
3. Set $f^* := f^* + \delta^*$
4. If $f = f^*$ with high probability, then return f^*
5. Return to step 3

Modular reduction

$$f = c_1 x_1^{e_{1,1}} \cdots x_n^{e_{1,n}} + \cdots + c_t x_1^{e_{t,1}} \cdots x_n^{e_{t,n}}$$

Chinese remaindering

- $f \in \mathbb{Z}[x_1, \ldots, x_n]$
- $|c_i| < B$ for all i
- $p_1 \cdots p_k > 2B$ for coprime primes $p_1, \ldots, p_k$

Reconstruct f from $f \bmod p_1, \ldots, f \bmod p_k$

Modular reduction

$$f = c_1 x_1^{e_{1,1}} \cdots x_n^{e_{1,n}} + \cdots + c_t x_1^{e_{t,1}} \cdots x_n^{e_{t,n}}$$

Chinese remaindering

- $f \in \mathbb{Z}[x_1, \dots, x_n]$
- $|c_i| < B$ for all i
- $p_1 \cdots p_k > 2B$ for coprime primes $p_1, \dots, p_k$

Reconstruct f from $f \bmod p_1$, …, $f \bmod p_k$

Also works for $f \in \mathbb{Q}[x_1, \dots, x_n]$, using “rational number reconstruction”

Modular reduction

$$f = c_1 x_1^{e_{1,1}} \cdots x_n^{e_{1,n}} + \cdots + c_t x_1^{e_{t,1}} \cdots x_n^{e_{t,n}}$$

Chinese remaindering

- $f \in \mathbb{Z}[x_1, \ldots, x_n]$
- $|c_i| < B$ for all i
- $p_1 \cdots p_k > 2B$ for coprime primes $p_1, \ldots, p_k$

Reconstruct f from f mod p_1, ..., f mod p_k

Also works for $f \in \mathbb{Q}[x_1, \ldots, x_n]$, using "rational number reconstruction"

Smooth primes

- We are free to chose $p_1, \ldots, p_k$ as we please
- $p - 1$ has many small prime factors $\Rightarrow$ fast arithmetic in $\mathbb{F}_p[x]$
- E.g. $p = 3 \times 2^{30} + 1$

Reduction to the univariate case

$$f = c_1 x_1^{e_{1,1}} \cdots x_n^{e_{1,n}} + \cdots + c_t x_1^{e_{t,1}} \cdots x_n^{e_{t,n}}$$

$$\deg_{x_j} f = \max_i e_{i,j} < d_j$$

Kronecker substitution

$$g(z) = f(u, u^{d_1}, u^{d_1 d_2}, \ldots, u^{d_1 \cdots d_{n-1}})$$

Reduction to the univariate case

$$f = c_1 x_1^{e_{1,1}} \cdots x_n^{e_{1,n}} + \cdots + c_t x_1^{e_{t,1}} \cdots x_n^{e_{t,n}}$$
$$\deg_{x_j} f = \max_i e_{i,j} < d_j$$

Kronecker substitution

$$g(z) = f(u, u^{d_1}, u^{d_1 d_2}, \ldots, u^{d_1 \cdots d_{n-1}})$$

Example $(d_1 = d_2 = 10)$

$$f(x_1, x_2) = 3 x_1^7 x_2^8 - 11 x_1^3 x_2^5 + 8 x_2^3 - 7 x_1^8$$
$$g(u) = 3 u^{87} - 11 u^{53} + 8 u^{30} - 7 u^8$$

Part III

The geometric progression approach

The method

$$f = c_1 x^{e_1} + \cdots + c_t x^{e_t} \in \mathbb{F}_p[x]$$

The method

$$f = c_1 x^{e_1} + \cdots + c_t x^{e_t} \in \mathbb{F}_p[x]$$

For some number $\omega \in K$ of high multiplicative order, compute

$$\begin{aligned} f(\omega^0) &= c_1 \omega^{0e_1} + \cdots + c_t \omega^{0e_t} \\ f(\omega^1) &= c_1 \omega^{1e_1} + \cdots + c_t \omega^{1e_t} \\ f(\omega^2) &= c_1 \omega^{2e_1} + \cdots + c_t \omega^{2e_t} \\ &\vdots \end{aligned}$$

The method

$$f = c_1 x^{e_1} + \cdots + c_t x^{e_t} \in \mathbb{F}_p[x]$$

For some number $\omega \in K$ of high multiplicative order, compute

$$\begin{aligned}
f(\omega^0) &= c_1 \omega^{0e_1} + \cdots + c_t \omega^{0e_t} \\
f(\omega^1)\, z &= c_1 \omega^{1e_1} z + \cdots + c_t \omega^{1e_t} z \\
f(\omega^2)\, z^2 &= c_1 \omega^{2e_1} z^2 + \cdots + c_t \omega^{2e_t} z^2 \\
&\vdots
\end{aligned}$$

The method

$$f = c_1 x^{e_1} + \cdots + c_t x^{e_t} \in \mathbb{F}_p[x]$$

For some number $\omega \in \mathbb{F}_q$ of high multiplicative order, compute

$$\begin{aligned}
f(\omega^0) &= c_1 \omega^{0e_1} + \cdots + c_t \omega^{0e_t} \\
f(\omega^1)\, z &= c_1 \omega^{1e_1} z + \cdots + c_t \omega^{1e_t} z \\
f(\omega^2)\, z^2 &= c_1 \omega^{2e_1} z^2 + \cdots + c_t \omega^{2e_t} z^2 \\
&\vdots \\
\sum_{k=0}^{\infty} f(\omega^k)\, z^k &= \frac{c_1}{1-\omega^{e_1} z} + \cdots + \frac{c_t}{1-\omega^{e_t} z} = \frac{N(z)}{\Lambda(z)}
\end{aligned}$$

The method

$$f = c_1 x^{e_1} + \cdots + c_t x^{e_t} \in \mathbb{F}_p[x]$$

For some number $\omega \in \mathbb{F}_q$ of high multiplicative order, compute

$$\begin{aligned}
f(\omega^0) &= c_1 \omega^{0e_1} + \cdots + c_t \omega^{0e_t} \\
f(\omega^1)\, z &= c_1 \omega^{1e_1} z + \cdots + c_t \omega^{1e_t} z \\
f(\omega^2)\, z^2 &= c_1 \omega^{2e_1} z^2 + \cdots + c_t \omega^{2e_t} z^2 \\
&\vdots \\
\sum_{k=0}^{\infty} f(\omega^k)\, z^k &= \frac{c_1}{1-\omega^{e_1} z} + \cdots + \frac{c_t}{1-\omega^{e_t} z} = \frac{N(z)}{\Lambda(z)}
\end{aligned}$$

- Recover N and Λ from the first $2t-1$ evaluations

The method

$$f = c_1 x^{e_1} + \cdots + c_t x^{e_t} \in \mathbb{F}_p[x]$$

For some number $\omega \in \mathbb{F}_q$ of high multiplicative order, compute

$$\begin{aligned}
f(\omega^0) &= c_1 \omega^{0e_1} + \cdots + c_t \omega^{0e_t} \\
f(\omega^1)\, z &= c_1 \omega^{1e_1} z + \cdots + c_t \omega^{1e_t} z \\
f(\omega^2)\, z^2 &= c_1 \omega^{2e_1} z^2 + \cdots + c_t \omega^{2e_t} z^2 \\
&\vdots \\
\sum_{k=0}^{\infty} f(\omega^k)\, z^k &= \frac{c_1}{1 - \omega^{e_1} z} + \cdots + \frac{c_t}{1 - \omega^{e_t} z} = \frac{N(z)}{\Lambda(z)}
\end{aligned}$$

- Recover N and Λ from the first $2t-1$ evaluations
- Determine the roots ω^{-e_i} of Λ

The method

$$f = c_1 x^{e_1} + \cdots + c_t x^{e_t} \in \mathbb{F}_p[x]$$

For some number $\omega \in \mathbb{F}_q$ of high multiplicative order, compute

$$\begin{aligned}
f(\omega^0) &= c_1 \omega^{0e_1} + \cdots + c_t \omega^{0e_t} \\
f(\omega^1)\, z &= c_1 \omega^{1e_1} z + \cdots + c_t \omega^{1e_t} z \\
f(\omega^2)\, z^2 &= c_1 \omega^{2e_1} z^2 + \cdots + c_t \omega^{2e_t} z^2 \\
&\vdots \\
\sum_{k=0}^{\infty} f(\omega^k)\, z^k &= \frac{c_1}{1-\omega^{e_1} z} + \cdots + \frac{c_t}{1-\omega^{e_t} z} = \frac{N(z)}{\Lambda(z)}
\end{aligned}$$

- Recover N and Λ from the first $2t-1$ evaluations
- Determine the roots ω^{-e_i} of Λ
- Compute the discrete logarithms e_i of ω^{e_i} w.r.t. ω

The method

$$f = c_1 x^{e_1} + \cdots + c_t x^{e_t} \in \mathbb{F}_p[x]$$

For some number $\omega \in \mathbb{F}_q$ of high multiplicative order, compute

$$\begin{aligned}
f(\omega^0) &= c_1 \omega^{0e_1} + \cdots + c_t \omega^{0e_t} \\
f(\omega^1)\, z &= c_1 \omega^{1e_1} z + \cdots + c_t \omega^{1e_t} z \\
f(\omega^2)\, z^2 &= c_1 \omega^{2e_1} z^2 + \cdots + c_t \omega^{2e_t} z^2 \\
&\vdots \\
\sum_{k=0}^{\infty} f(\omega^k)\, z^k &= \frac{c_1}{1 - \omega^{e_1} z} + \cdots + \frac{c_t}{1 - \omega^{e_t} z} = \frac{N(z)}{\Lambda(z)}
\end{aligned}$$

- Recover N and Λ from the first $2t - 1$ evaluations
- Determine the roots ω^{-e_i} of Λ
- Compute the discrete logarithms e_i of ω^{e_i} w.r.t. ω
- Compute the coefficients c_i using linear algebra

Complexity analysis

- Evaluate $f(\omega^0), f(\omega^1), \ldots, f(\omega^{2t-1})$ $O^\flat(Lt \log p)$

Complexity analysis

- Evaluate $f(\omega^0), f(\omega^1), \ldots, f(\omega^{2t-1})$ $O^\flat(L\, t \log p)$
- Recover N and Λ
  - Half-gcd $O^\flat(M_p(t) \log t)$

Complexity analysis

- Evaluate $f(\omega^0), f(\omega^1), \ldots, f(\omega^{2t-1})$ $O^\flat(L\,t \log p)$
- Recover N and Λ
  - Half-gcd $O^\flat(t\,(\log t)^2 \log p)$

Complexity analysis

- Evaluate $f(\omega^0), f(\omega^1), \ldots, f(\omega^{2t-1})$ $\quad O^\flat(L\, t \log p)$
- Recover N and Λ
  - Half-gcd $\quad O^\flat(t\,(\log t)^2 \log p)$
- Determine the roots ω^{-e_i} of Λ
  - Cantor–Zassenhaus $\quad O^\flat(t\,(\log t)^2\,(\log p)^2)$
  - Tangent-Graeffe, $p-1$ large smooth factor $\quad O^\flat(t\,(\log t)^2 \log p)$

Complexity analysis

- Evaluate $f(\omega^0), f(\omega^1), \ldots, f(\omega^{2t-1})$ $\quad O^\flat(L\,t\log p)$
- Recover N and Λ
  - Half-gcd $\quad O^\flat(t\,(\log t)^2\log p)$
- Determine the roots ω^{-e_i} of Λ
  - Cantor–Zassenhaus $\quad O^\flat(t\,(\log t)^2\,(\log p)^2)$
  - Tangent-Graeffe, $p-1$ large smooth factor $\quad O^\flat(t\,(\log t)^2\log p)$
- Compute the discrete logarithms e_i of ω^{e_i} w.r.t. ω
  - Pohlig-Helmann, $p-1$ large smooth factor $\quad O^\flat(t\log t\log p)$

Complexity analysis

- Evaluate $f(\omega^0), f(\omega^1), \ldots, f(\omega^{2t-1})$ — $O^\flat(L\,t\log p)$
- Recover N and Λ
  - Half-gcd — $O^\flat(t(\log t)^2\log p)$
- Determine the roots ω^{-e_i} of Λ
  - Cantor–Zassenhaus — $O^\flat(t(\log t)^2(\log p)^2)$
  - Tangent-Graeffe, $p-1$ large smooth factor — $O^\flat(t(\log t)^2\log p)$
- Compute the discrete logarithms e_i of ω^{e_i} w.r.t. ω
  - Pohlig-Helmann, $p-1$ large smooth factor — $O^\flat(t\log t\log p)$
- Compute the coefficients c_i using linear algebra
  - Transposed fast multi-point interpolation — $O^\flat(t(\log t)^2\log p)$

Complexity analysis

- Evaluate $f(\omega^0), f(\omega^1), \ldots, f(\omega^{2t-1})$ — $O^\flat(L\,t \log p)$
- Recover N and Λ
  - Half-gcd — $O^\flat(t(\log t)^2 \log p)$
- Determine the roots ω^{-e_i} of Λ
  - Cantor–Zassenhaus — $O^\flat(t(\log t)^2 (\log p)^2)$
  - Tangent-Graeffe, $p-1$ large smooth factor — $O^\flat(t(\log t)^2 \log p)$
- Compute the discrete logarithms e_i of ω^{e_i} w.r.t. ω
  - Pohlig-Helmann, $p-1$ large smooth factor — $O^\flat(t \log t \log p)$
- Compute the coefficients c_i using linear algebra
  - Transposed fast multi-point interpolation — $O^\flat(t(\log t)^2 \log p)$

Total — $O((L + (\log t)^2)\, t \log p)$

Part IV

The cyclic extension approach

Idea

$$f = c_1 x^{e_1} + \cdots + c_t x^{e_t}$$

Idea

$$f = c_1 x^{e_1} + \cdots + c_t x^{e_t}$$

Main idea

For $r \geqslant T$ evaluate f and xf' at $\bar{x} \in \mathbb{F}_p[x]/(x^r - 1)$, which yields

$$\begin{aligned} f \operatorname{rem} (x^r - 1) &= c_1 \quad x^{e_1 \operatorname{rem} r} + \cdots + c_t \quad x^{e_t \operatorname{rem} r} \\ (xf') \operatorname{rem} (x^r - 1) &= c_1 e_1 x^{e_1 \operatorname{rem} r} + \cdots + c_t e_t x^{e_t \operatorname{rem} r} \end{aligned}$$

Match corresponding terms to find the e_i and next the c_i

$$f = c_1 x^{e_1} + \cdots + c_t x^{e_t}$$

Main idea

For $r \geqslant T$ evaluate f and xf' at $\bar{x} \in \mathbb{F}_p[x]/(x^r - 1)$, which yields

$$\begin{aligned} f \operatorname{rem} (x^r - 1) &= c_1 \quad x^{e_1 \operatorname{rem} r} + \cdots + c_t \quad x^{e_t \operatorname{rem} r} \\ (xf') \operatorname{rem} (x^r - 1) &= c_1 e_1 x^{e_1 \operatorname{rem} r} + \cdots + c_t e_t x^{e_t \operatorname{rem} r} \end{aligned}$$

Match corresponding terms to find the e_i and next the c_i

Note

If we interpolate $f \in \mathbb{Q}[x]$ modulo many primes $p_1, \ldots, p_k$,
then the exponents e_i need only be determined modulo p_1

Example

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$

Evaluation modulo $x^{10} - 1$

$$\begin{aligned} f &\equiv 18x^0 + 33x^2 + 2x^7 + x^2 + 7x^1 + 4x^8 + 11x^3 + 28 \\ &\equiv 4x^8 + 2x^7 + 11x^3 + (33+1)x^2 + 7x^1 + (28+18)x^0 \\ xf' &\equiv 4500x^0 + 7656x^2 + 394x^7 + 152x^2 + 847x^1 + 472x^8 + 693x^3 + 0 \\ &\equiv 472x^8 + 394x^7 + 693x^3 + (7656+152)x^2 + 847x^1 + (4500+0)x^0 \end{aligned}$$

Example

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$

Evaluation modulo $x^{10} - 1$

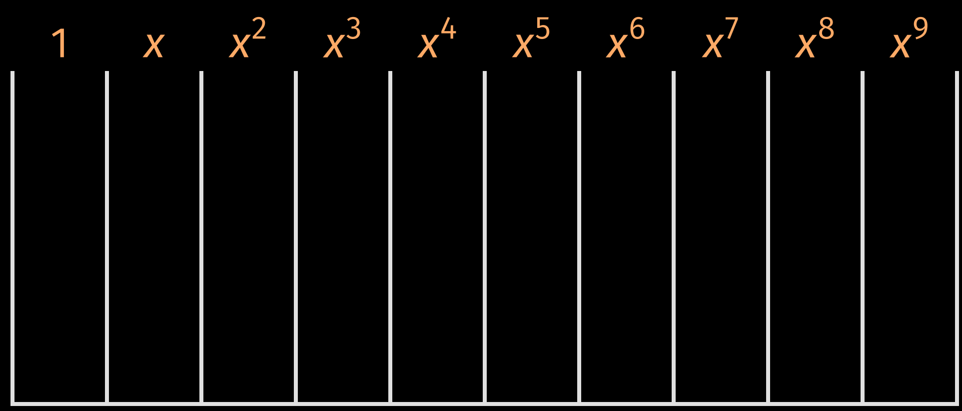
$$\begin{aligned} f &\equiv 18x^0 + 33x^2 + 2x^7 + x^2 + 7x^1 + 4x^8 + 11x^3 + 28 \\ &\equiv 4x^8 + 2x^7 + 11x^3 + (33+1)x^2 + 7x^1 + (28+18)x^0 \\ xf' &\equiv 4500x^0 + 7656x^2 + 394x^7 + 152x^2 + 847x^1 + 472x^8 + 693x^3 + 0 \\ &\equiv 472x^8 + 394x^7 + 693x^3 + (7656+152)x^2 + 847x^1 + (4500+0)x^0 \end{aligned}$$

Quotients for $p = 3 \times 2^{30} + 1$

$$\frac{472}{4} = 118, \quad \frac{394}{2} = 197, \quad \ldots \quad , \frac{4500}{46} = 700266505, \quad \ldots$$

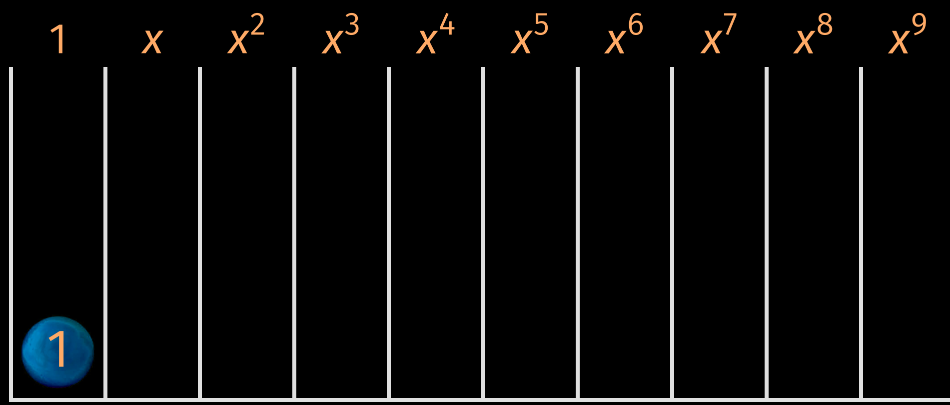
A combinatorial ball model

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$



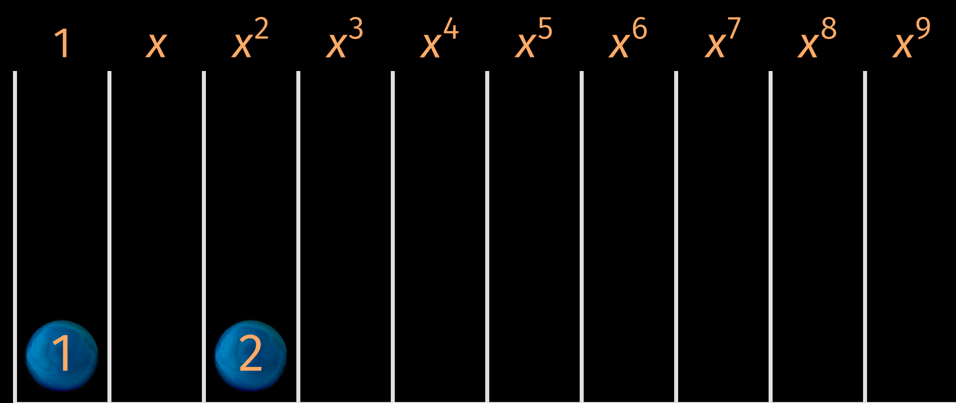
A combinatorial ball model

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$



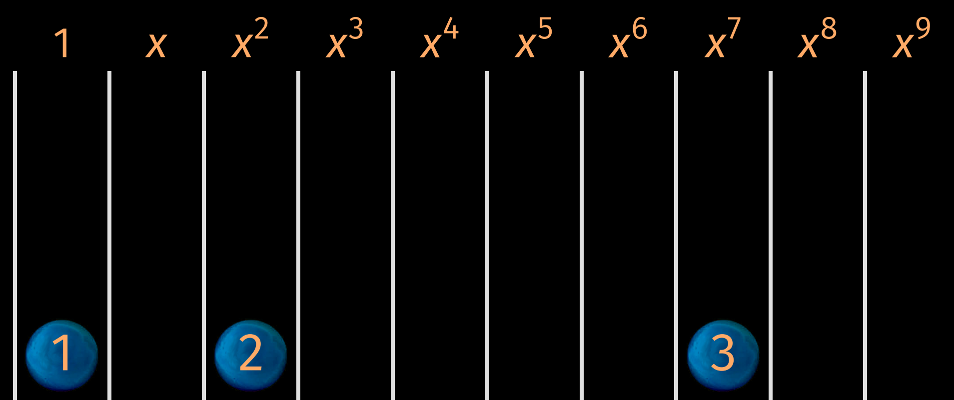
A combinatorial ball model

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$



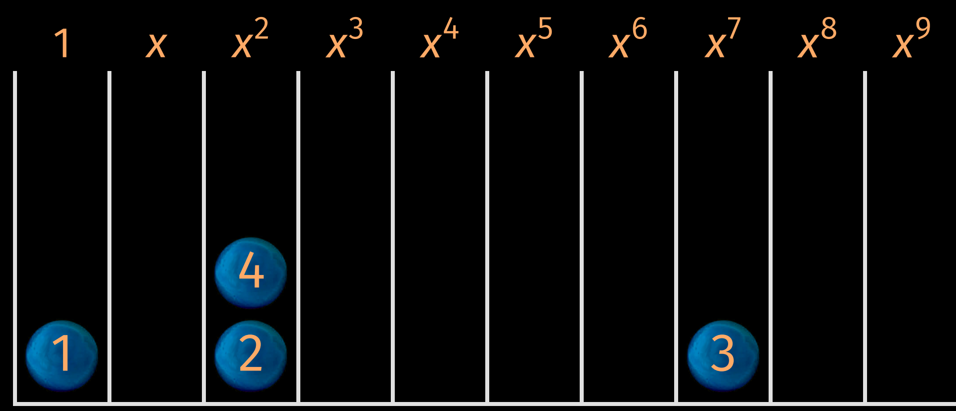
A combinatorial ball model

$$f = \overbrace{18\,x^{250}}^{1} + \overbrace{33\,x^{232}}^{2} + \overbrace{2\,x^{197}}^{3} + \overbrace{x^{152}}^{4} + \overbrace{7\,x^{121}}^{5} + \overbrace{4\,x^{118}}^{6} + \overbrace{11\,x^{63}}^{7} + \overbrace{28}^{8}$$



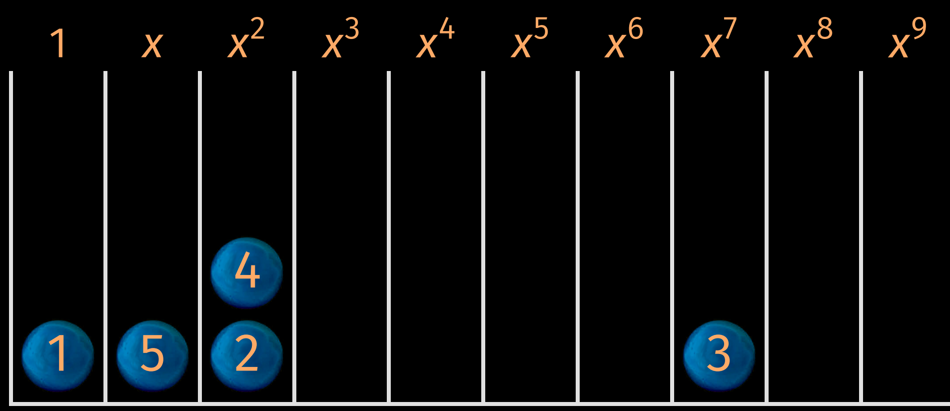
A combinatorial ball model

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$



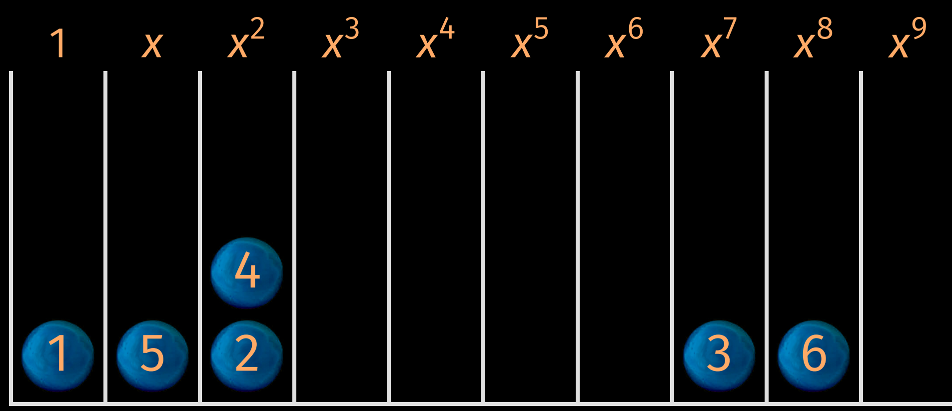
A combinatorial ball model

$$f = \overbrace{18x^{250}}^{1} + \overbrace{33x^{232}}^{2} + \overbrace{2x^{197}}^{3} + \overbrace{x^{152}}^{4} + \overbrace{7x^{121}}^{5} + \overbrace{4x^{118}}^{6} + \overbrace{11x^{63}}^{7} + \overbrace{28}^{8}$$

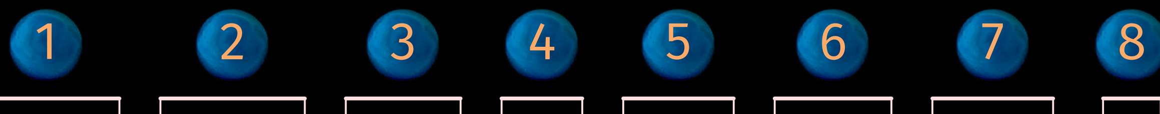


A combinatorial ball model

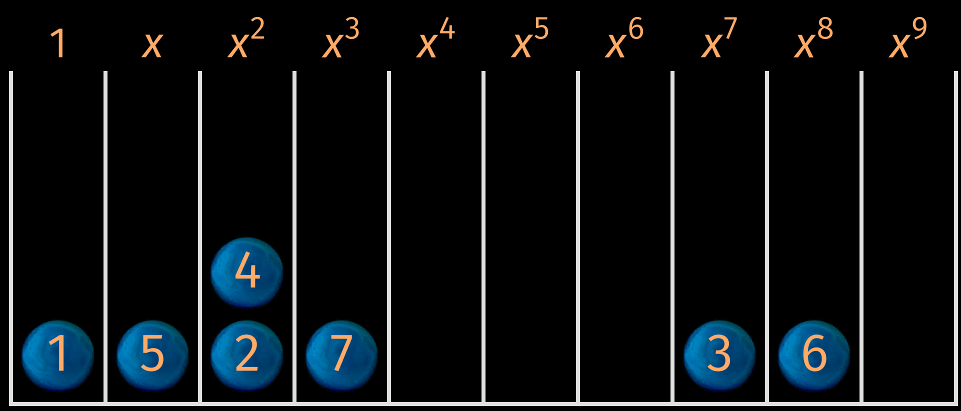
$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$



A combinatorial ball model

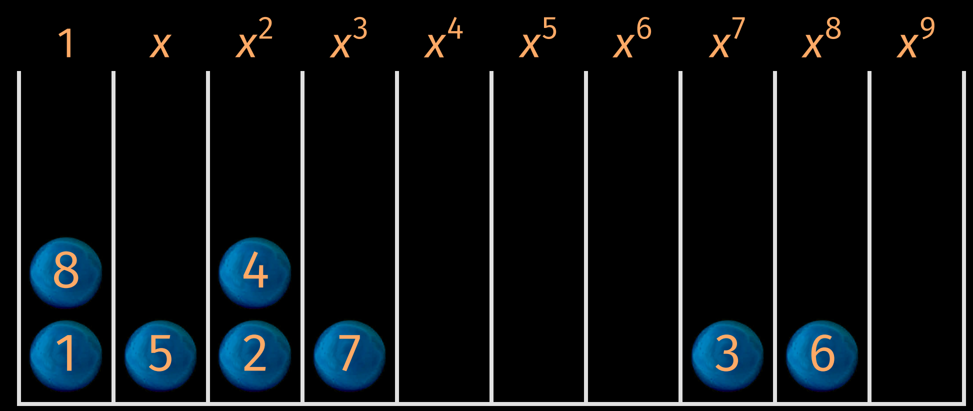


$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$



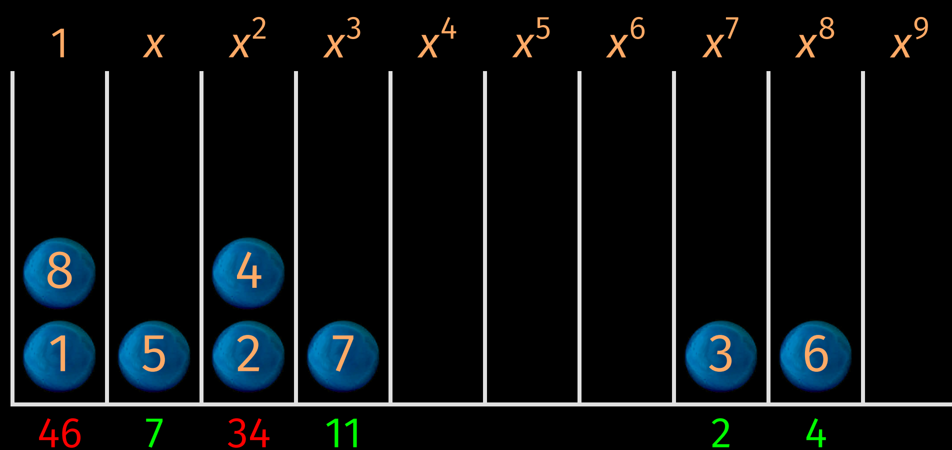
A combinatorial ball model

$$f = \overbrace{18x^{250}}^{1} + \overbrace{33x^{232}}^{2} + \overbrace{2x^{197}}^{3} + \overbrace{x^{152}}^{4} + \overbrace{7x^{121}}^{5} + \overbrace{4x^{118}}^{6} + \overbrace{11x^{63}}^{7} + \overbrace{28}^{8}$$



A combinatorial ball model

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$



Heuristic assumption

The distribution of $e_i \bmod r$ is uniform in $\mathbb{Z}/r\mathbb{Z}$

Heuristic assumption

The distribution of $e_i \bmod r$ is uniform in $\mathbb{Z}/r\mathbb{Z}$

Throwing *t* balls in *r* boxes

- Probability that a ball ends up in a box of its own:

$$\left(1-\frac{1}{r}\right)^{t-1} \approx \left(1-\frac{1}{r}\right)^{t} = e^{\log\left(1-\frac{1}{r}\right)t} = e^{\left(-\frac{1}{r}-\frac{1}{2r^2}+\cdots\right)t} \approx e^{-t/r}$$

Heuristic assumption

The distribution of $e_i \bmod r$ is uniform in $\mathbb{Z}/r\mathbb{Z}$

Throwing *t* balls in *r* boxes

- Probability that a ball ends up in a box of its own:

$$\left(1-\frac{1}{r}\right)^{t-1} \approx \left(1-\frac{1}{r}\right)^{t} = \mathrm{e}^{\log\left(1-\frac{1}{r}\right)t} = \mathrm{e}^{\left(-\frac{1}{r}-\frac{1}{2r^2}+\cdots\right)t} \approx \mathrm{e}^{-t/r}$$

- $\mathrm{e}^{-t/r}\,T$ non-colliding terms in $f(x) \operatorname{rem} (x^r - 1)$ on average

Heuristic assumption

The distribution of $e_i \bmod r$ is uniform in $\mathbb{Z}/r\mathbb{Z}$

Throwing *t* balls in *r* boxes

- Probability that a ball ends up in a box of its own:

$$\left(1-\frac{1}{r}\right)^{t-1} \approx \left(1-\frac{1}{r}\right)^{t} = \mathrm{e}^{\log\left(1-\frac{1}{r}\right)t} = \mathrm{e}^{\left(-\frac{1}{r}-\frac{1}{2r^2}+\cdots\right)t} \approx \mathrm{e}^{-t/r}$$

- $\mathrm{e}^{-t/r}T$ non-colliding terms in $f(x) \operatorname{rem} (x^r-1)$ on average

Computational cost

- Evaluating $f(x)$ modulo $x^r-1 \xrightarrow{\text{ops in } \mathbb{F}_p} O(L\,\mathsf{M}(r)) = O(L\,r\log r)$

Probabilistic analysis

Heuristic assumption

The distribution of $e_i \bmod r$ is uniform in $\mathbb{Z}/r\mathbb{Z}$

Throwing *t* balls in *r* boxes

- Probability that a ball ends up in a box of its own:

$$\left(1-\frac{1}{r}\right)^{t-1} \approx \left(1-\frac{1}{r}\right)^{t} = e^{\log\left(1-\frac{1}{r}\right)t} = e^{\left(-\frac{1}{r}-\frac{1}{2r^2}+\cdots\right)t} \approx e^{-t/r}$$

- $e^{-t/r}T$ non-colliding terms in $f(x) \operatorname{rem} (x^r-1)$ on average

Computational cost

- Evaluating $f(x)$ modulo $x^r-1 \xrightarrow{\text{ops in } \mathbb{F}_p} O(L\,\mathsf{M}(r)) = O(L\,r\log r)$
- Expected number of correct terms $\longrightarrow e^{-t/r}t$

Heuristic assumption

The distribution of $e_i \bmod r$ is uniform in $\mathbb{Z}/r\mathbb{Z}$

Throwing *t* balls in *r* boxes

- Probability that a ball ends up in a box of its own:

$$\left(1-\frac{1}{r}\right)^{t-1} \approx \left(1-\frac{1}{r}\right)^{t} = \mathrm{e}^{\log\left(1-\frac{1}{r}\right)t} = \mathrm{e}^{\left(-\frac{1}{r}-\frac{1}{2r^2}+\cdots\right)t} \approx \mathrm{e}^{-t/r}$$

- $\mathrm{e}^{-t/r}T$ non-colliding terms in $f(x) \operatorname{rem} (x^r-1)$ on average

Computational cost

- Evaluating $f(x)$ modulo $x^r-1 \xrightarrow{\text{ops in } \mathbb{F}_p} O(L\,\mathsf{M}(r)) = O(L\,r\log r)$
- Expected number of correct terms $\longrightarrow \mathrm{e}^{-t/r}t$
- Cost proportional to $\mathrm{e}^{t/r}r \Rightarrow$ maximal efficiency for $r \approx t$

Part V

FFT-based approach

Idea

Choice of *p* and *r*

- Take p to be smooth, e.g. $p-1$ is a product of many small primes
- Take $r \approx t$ such that $r \mid (p-1)$
- Now $x^r - 1 = (x-1)(x-\omega)\cdots(x-\omega^{r-1})$ for some $\omega \in \mathbb{F}_p$

Idea

Choice of p and r

- Take p to be smooth, e.g. $p-1$ is a product of many small primes
- Take $r \approx t$ such that $r \mid (p-1)$
- Now $x^r - 1 = (x-1)(x-\omega)\cdots(x-\omega^{r-1})$ for some $\omega \in \mathbb{F}_p$

Boosting the cyclic extension approach

Instead of directly evaluating f at $\bar{x}$ over $\mathbb{K}[x]/(x^r-1)$:

- Evaluate f at $1, \omega, \ldots, \omega^{r-1}$
- Reconstruct f modulo $x^r - 1$ from $f(1), \ldots, f(\omega^{r-1})$ using an inverse FFT

Choice of p and r

- Take p to be smooth, e.g. $p-1$ is a product of many small primes
- Take $r \approx t$ such that $r \mid (p-1)$
- Now $x^r - 1 = (x-1)(x-\omega)\cdots(x-\omega^{r-1})$ for some $\omega \in \mathbb{F}_p$

Boosting the cyclic extension approach

Instead of directly evaluating f at $\bar{x}$ over $\mathbb{K}[x]/(x^r-1)$:

- Evaluate f at $1, \omega, \ldots, \omega^{r-1}$
- Reconstruct f modulo $x^r - 1$ from $f(1), \ldots, f(\omega^{r-1})$ using an inverse FFT

Complex coefficients

- Also works “approximately” over $\mathbb{C}$ by taking $\omega = \mathrm{e}^{2\pi \mathrm{i}/r}$
- C.f. “sparse Fourier transforms”, special cases of “compressed sensing”

Complexity analysis

Heuristic probabilistic complexity

- Expected evaluation time $O^\flat(L\,t\log p)$
- Expected interpolation time $O^\flat(t\log t\log p)$
- Total: $O^\flat((L+\log t)\,t\log p)$

Complexity analysis

Heuristic probabilistic complexity

- Expected evaluation time $O^\flat(L\,t\log p)$
- Expected interpolation time $O^\flat(t\log t\log p)$
- Total: $O^\flat((L+\log t)\,t\log p)$

Comparison with geometric sequence approach

	geometric sequence	FFT
Number of evaluations	$2t-1$	$\in(2\,e\,t, 5\,e\,t)$
„ known exponents	t	$e\,t$
Interpolation time	$O^\flat(t\log^2 t\log p)$	$O^\flat(t\log t\log p)$

Heuristic probabilistic complexity

- Expected evaluation time $O^{\flat}(L\, t \log p)$
- Expected interpolation time $O^{\flat}(t \log t \log p)$
- Total: $O^{\flat}((L + \log t)\, t \log p)$

Comparison with geometric sequence approach

	geometric sequence	FFT
Number of evaluations	$2t-1$	$\in (2\,\mathrm{e}\,t, 5\,\mathrm{e}\,t)$
„ known exponents	t	$\mathrm{e}\,t$
Interpolation time	$O^{\flat}(t \log^2 t \log p)$	$O^{\flat}(t \log t \log p)$

Multiplication $f = g\,h$ of sparse polynomials

- Evaluating f at a geometric sequence: $O^{\flat}(t \log^2 t \log p)$
- Evaluating g, h modulo $x^r - 1$: $O(t \log p)$
- FFT multication of g, h modulo $x^r - 1$: $O^{\flat}(t \log t \log p)$

Part VI

A game of mystery balls

Multiplication of sparse polynomials

Example

$$g = xy^5 + 3xy^6z - 2x^8y^{10} + x^{10}y^{14}z^3$$
$$h = 2 + yz + 3x^2y^4z^3$$

$$f = gh = 3x^{12}y^{18}z^6 + x^{10}y^{15}z^4 + 9x^3y^{10}z^4 + 3x^3y^9z^3 - 4x^{10}y^{14}z^3 + 3xy^7z^2 + 7xy^6z - 2x^8y^{11}z + 2xy^5 - 4x^8y^{10}$$

Multiplication of sparse polynomials

Example

$$g = xy^5 + 3xy^6z - 2x^8y^{10} + x^{10}y^{14}z^3$$
$$h = 2 + yz + 3x^2y^4z^3$$

$$f = gh = 3x^{12}y^{18}z^6 + x^{10}y^{15}z^4 + 9x^3y^{10}z^4 + 3x^3y^9z^3 - 4x^{10}y^{14}z^3 + 3xy^7z^2 + 7xy^6z - 2x^8y^{11}z + 2xy^5 - 4x^8y^{10}$$

Idea

- For “random” $(\alpha,\beta,\gamma) \in \mathbb{N}^3$, evaluate $f(u^\alpha, u^\beta, u^\gamma)$ modulo $u^r - 1$

Example

$$g = xy^5 + 3xy^6z - 2x^8y^{10} + x^{10}y^{14}z^3$$
$$h = 2 + yz + 3x^2y^4z^3$$

$$f = gh = 3x^{12}y^{18}z^6 + x^{10}y^{15}z^4 + 9x^3y^{10}z^4 + 3x^3y^9z^3 - 4x^{10}y^{14}z^3 + 3xy^7z^2 + 7xy^6z - 2x^8y^{11}z + 2xy^5 - 4x^8y^{10}$$

Idea

- For "random" $(\alpha, \beta, \gamma) \in \mathbb{N}^3$, evaluate $f(u^\alpha, u^\beta, u^\gamma)$ modulo $u^r - 1$
- *Three* directions $(\alpha_i, \beta_i, \gamma_i)_{i=1,2,3}$ instead of a single one $\longrightarrow$ smaller r

Example

$$\begin{aligned} g &= xy^5 + 3xy^6z - 2x^8y^{10} + x^{10}y^{14}z^3 \\ h &= 2 + yz + 3x^2y^4z^3 \end{aligned}$$

$$\begin{aligned} f = gh = {} & 3x^{12}y^{18}z^6 + x^{10}y^{15}z^4 + 9x^3y^{10}z^4 + 3x^3y^9z^3 - 4x^{10}y^{14}z^3 + \\ & 3xy^7z^2 + 7xy^6z - 2x^8y^{11}z + 2xy^5 - 4x^8y^{10} \end{aligned}$$

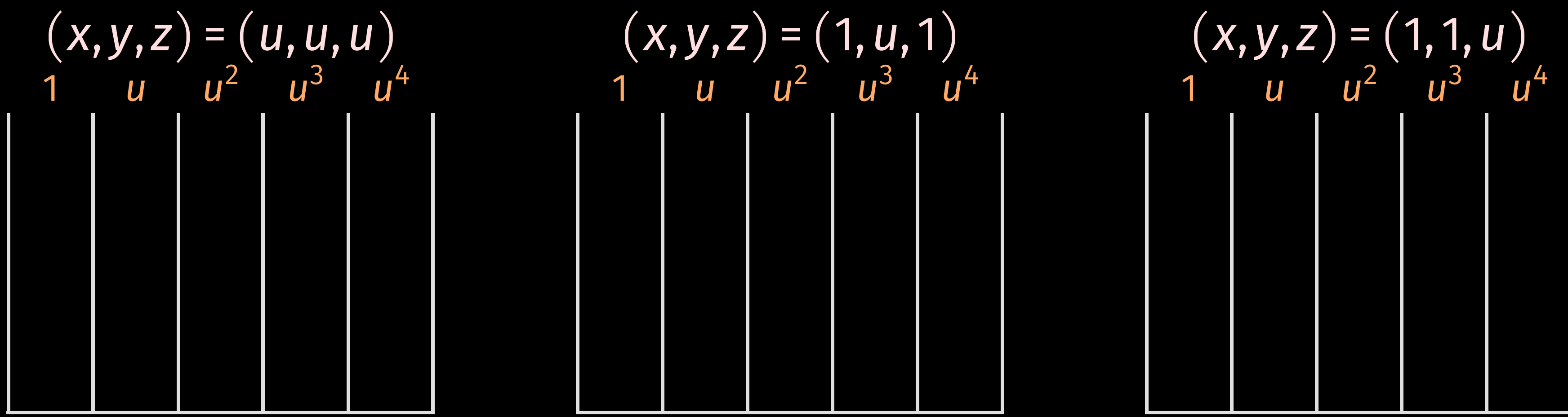
Idea

- For “random” $(\alpha,\beta,\gamma) \in \mathbb{N}^3$, evaluate $f(u^\alpha, u^\beta, u^\gamma)$ modulo $u^r - 1$
- *Three* directions $(\alpha_i, \beta_i, \gamma_i)_{i=1,2,3}$ instead of a single one $\longrightarrow$ smaller r

Assumption

Exponents already known

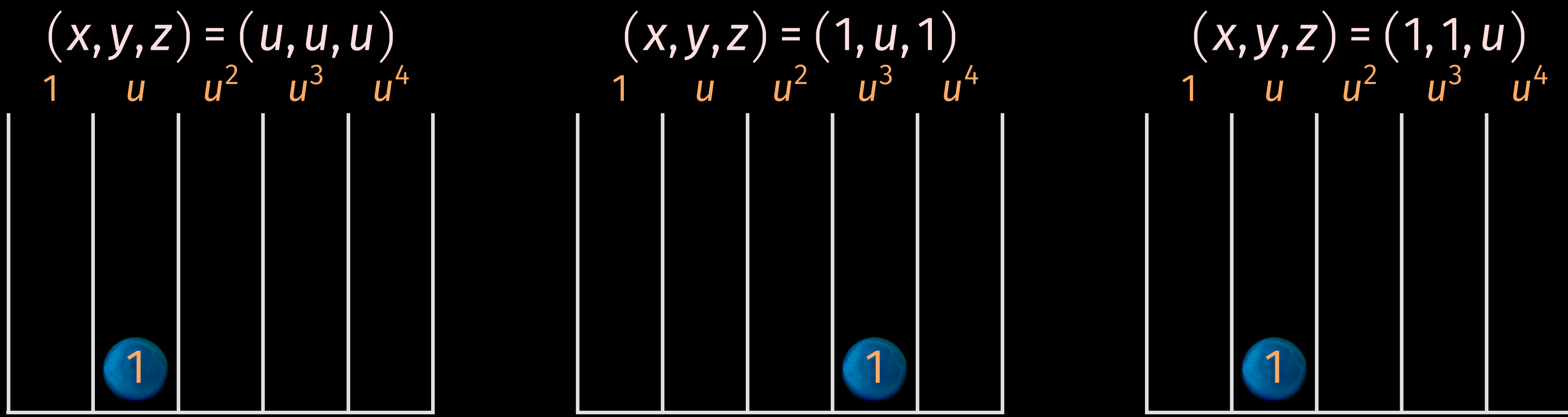
The game of mystery balls



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

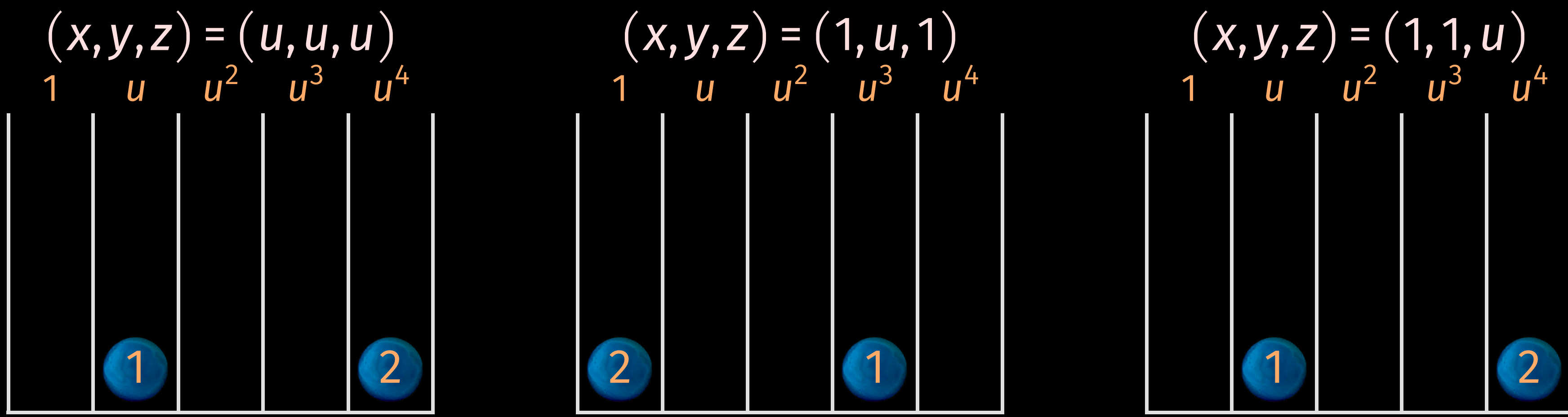
The game of mystery balls



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

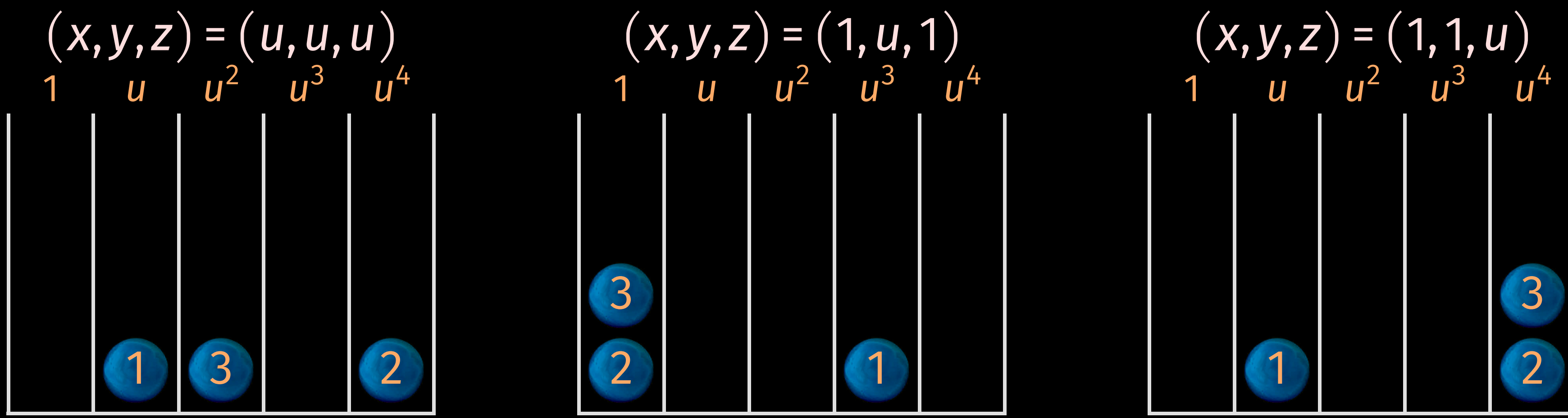
The game of mystery balls



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

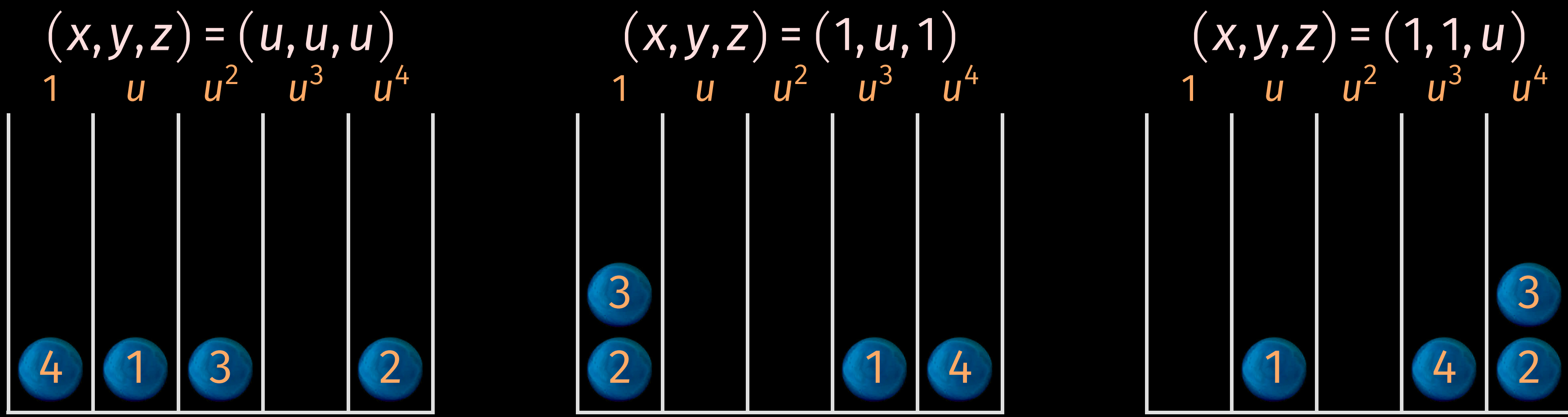
The game of mystery balls



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

The game of mystery balls

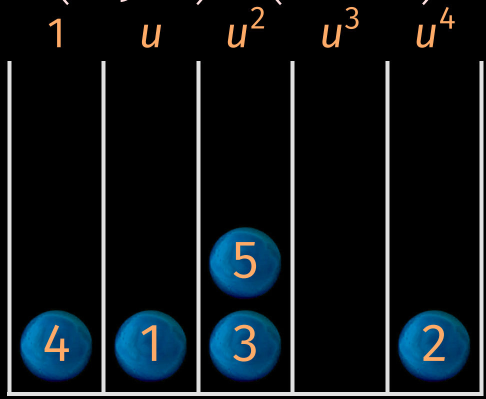


$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

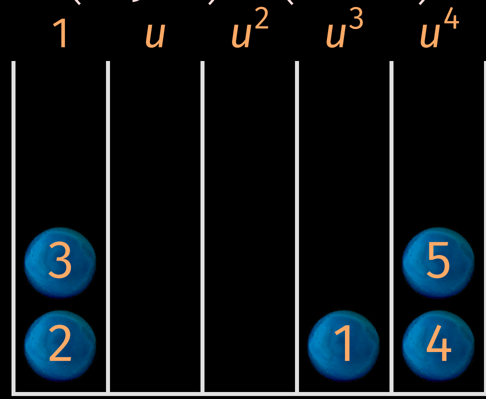
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

The game of mystery balls

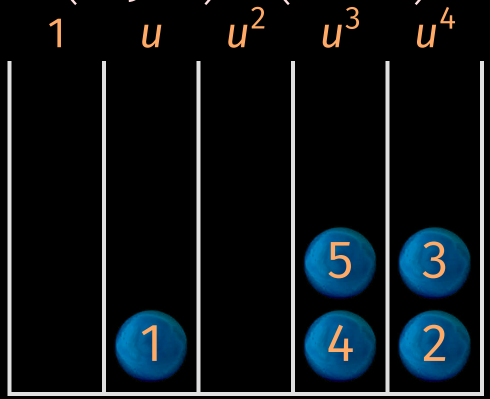
$(x,y,z)=(u,u,u)$



$(x,y,z)=(1,u,1)$



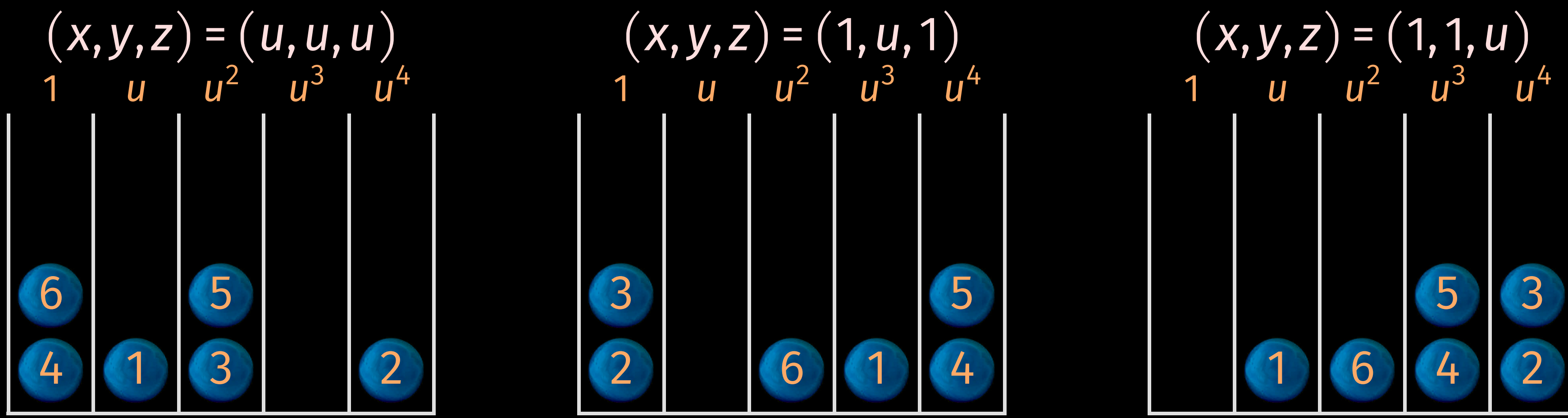
$(x,y,z)=(1,1,u)$



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)\,x^{10}y^{14}z^{3}}^{5} +$$

$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)\,x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)\,x^{8}y^{10}}^{10}$$

The game of mystery balls

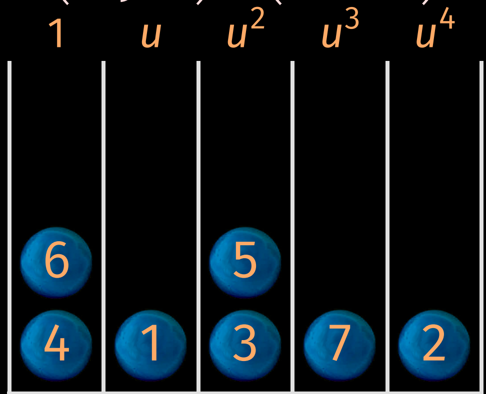


$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)\,x^{10}y^{14}z^{3}}^{5} +$$

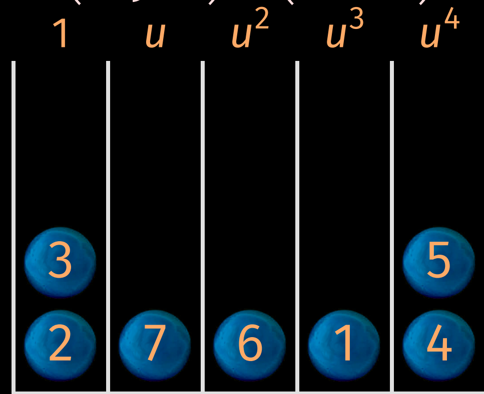
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)\,x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)\,x^{8}y^{10}}^{10}$$

The game of mystery balls

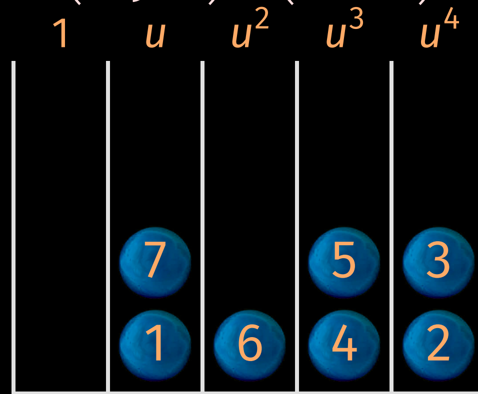
$(x,y,z) = (u,u,u)$



$(x,y,z) = (1,u,1)$



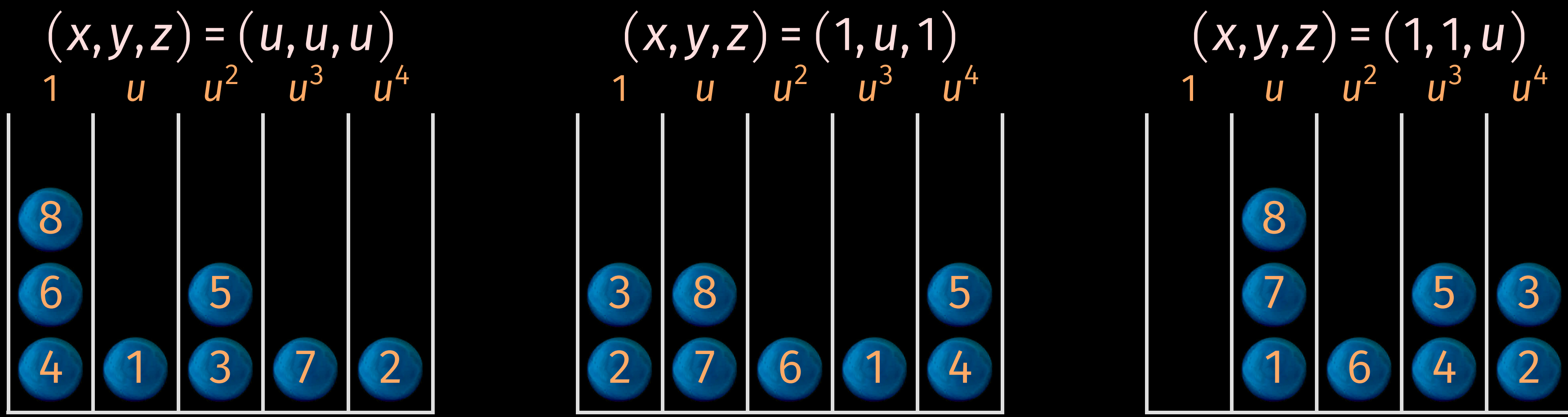
$(x,y,z) = (1,1,u)$



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

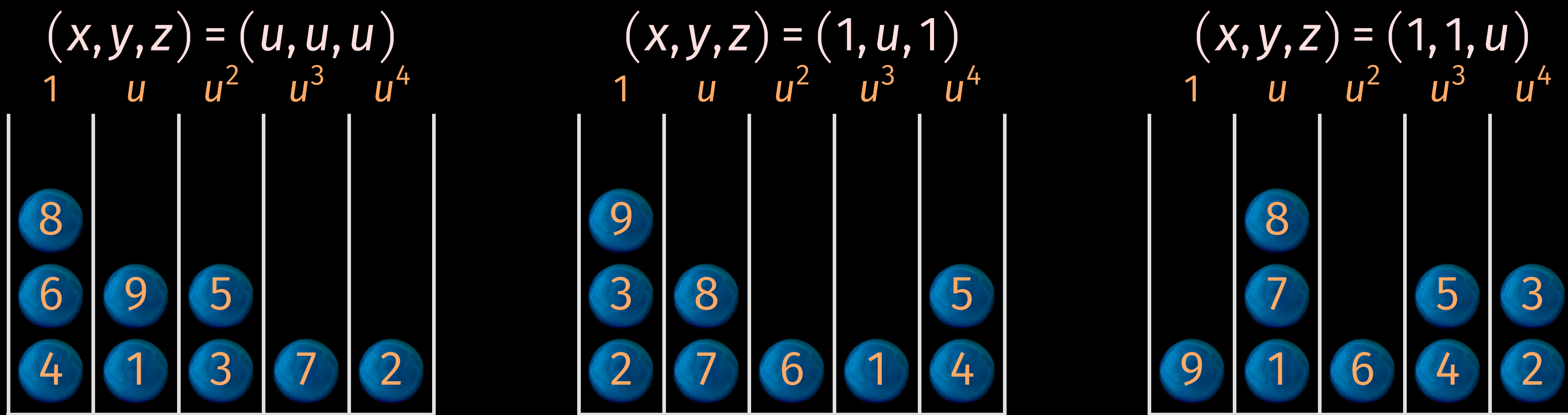
The game of mystery balls



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)\,x^{10}y^{14}z^{3}}^{5} +$$

$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)\,x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)\,x^{8}y^{10}}^{10}$$

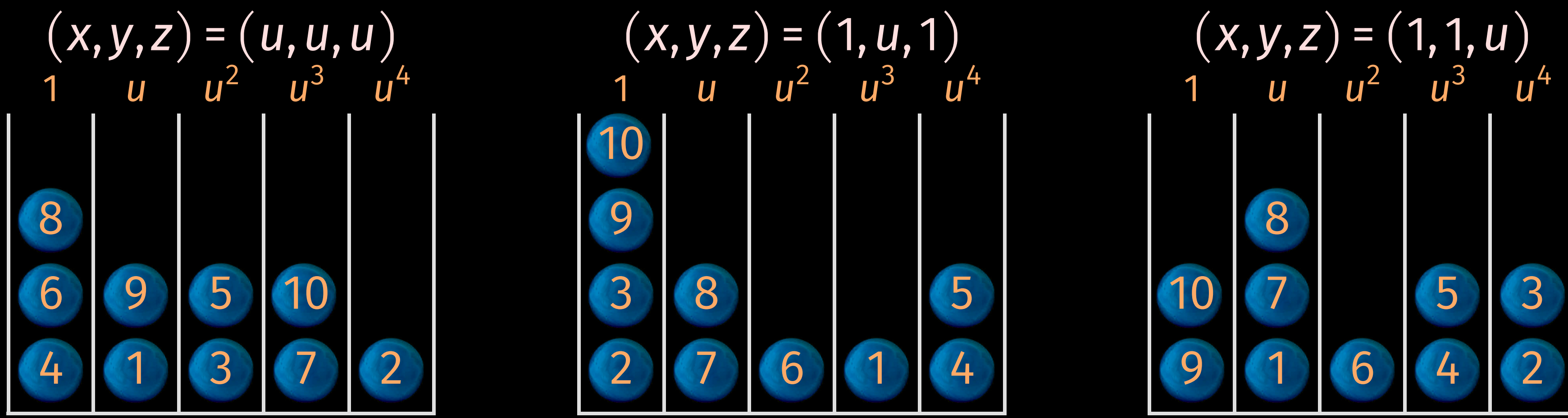
The game of mystery balls



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)\,x^{10}y^{14}z^{3}}^{5} +$$

$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)\,x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)\,x^{8}y^{10}}^{10}$$

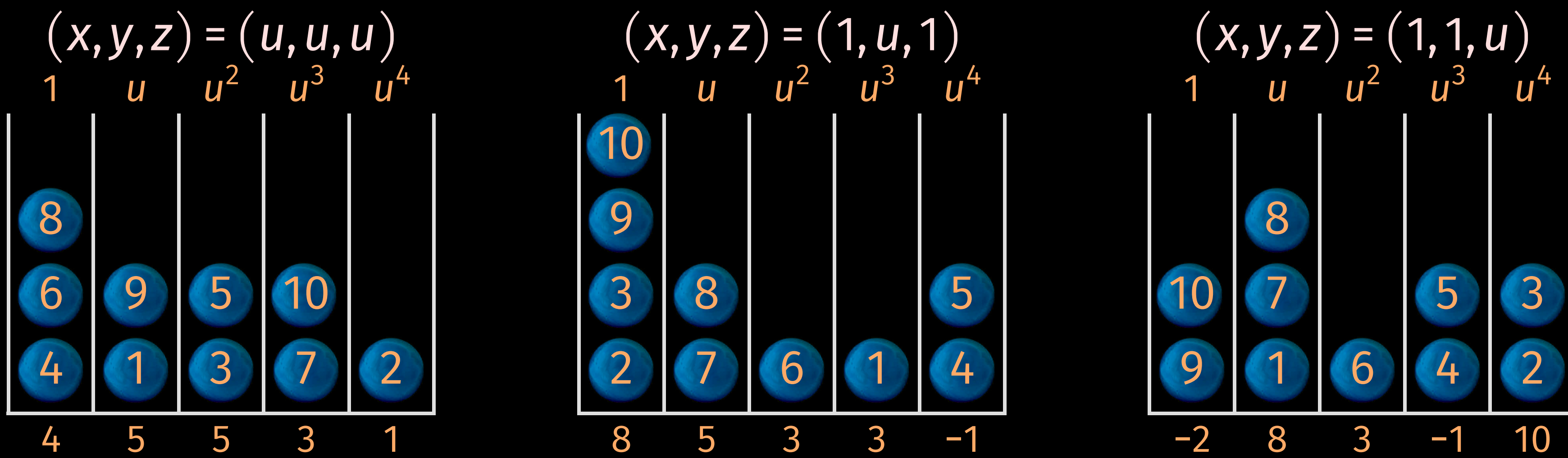
The game of mystery balls



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

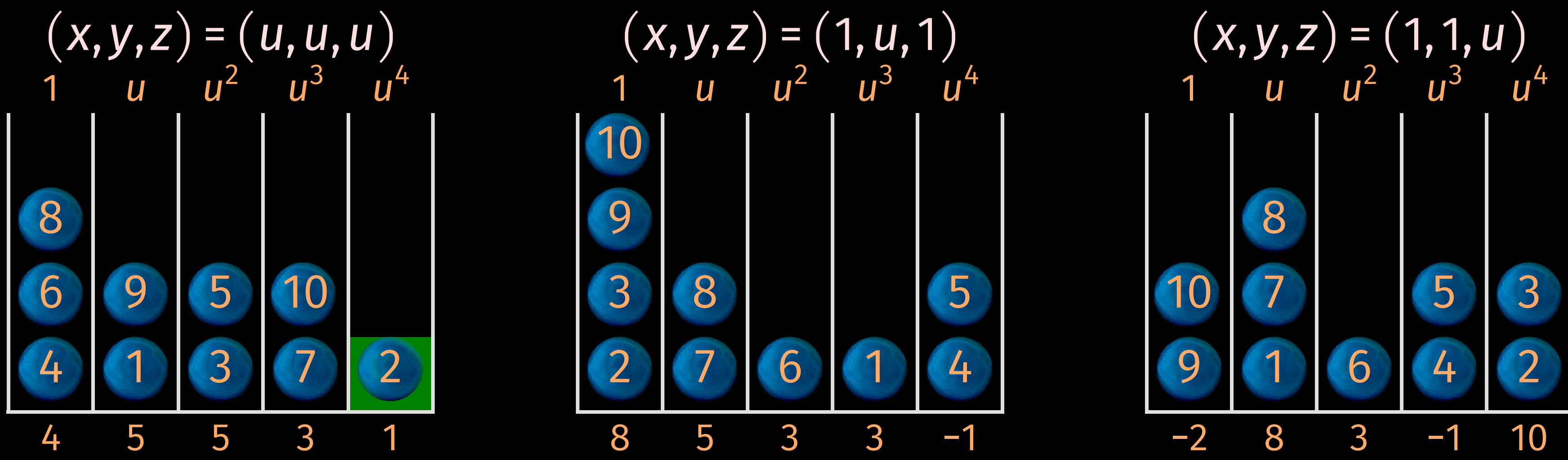
The game of mystery balls



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)\,x^{10}y^{14}z^{3}}^{5} +$$

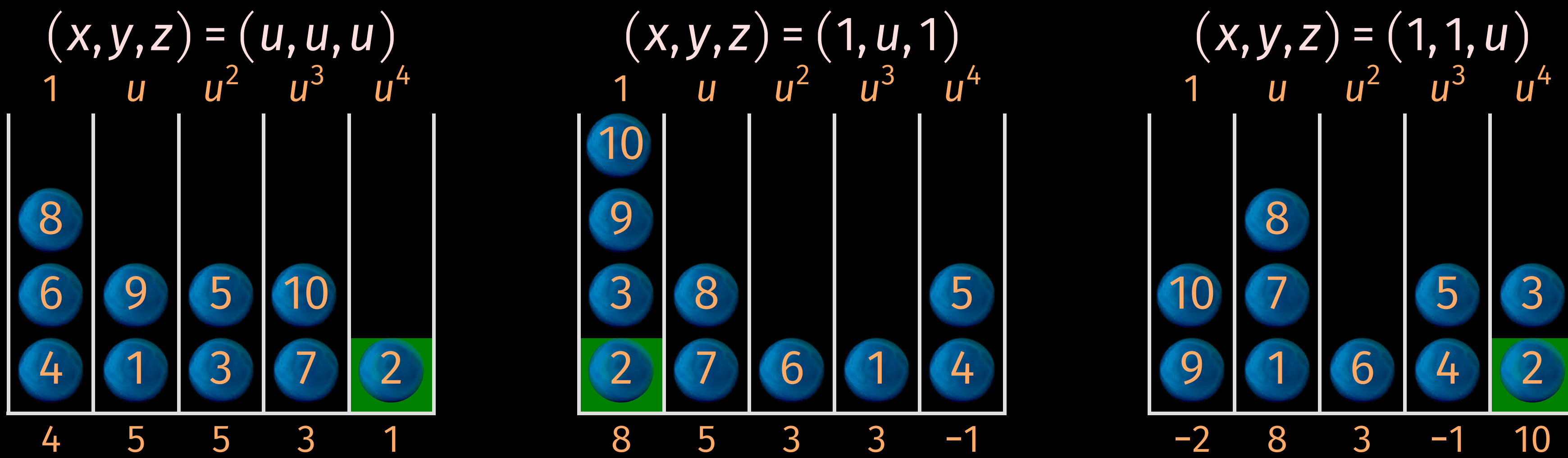
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)\,x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)\,x^{8}y^{10}}^{10}$$

The game of mystery balls



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

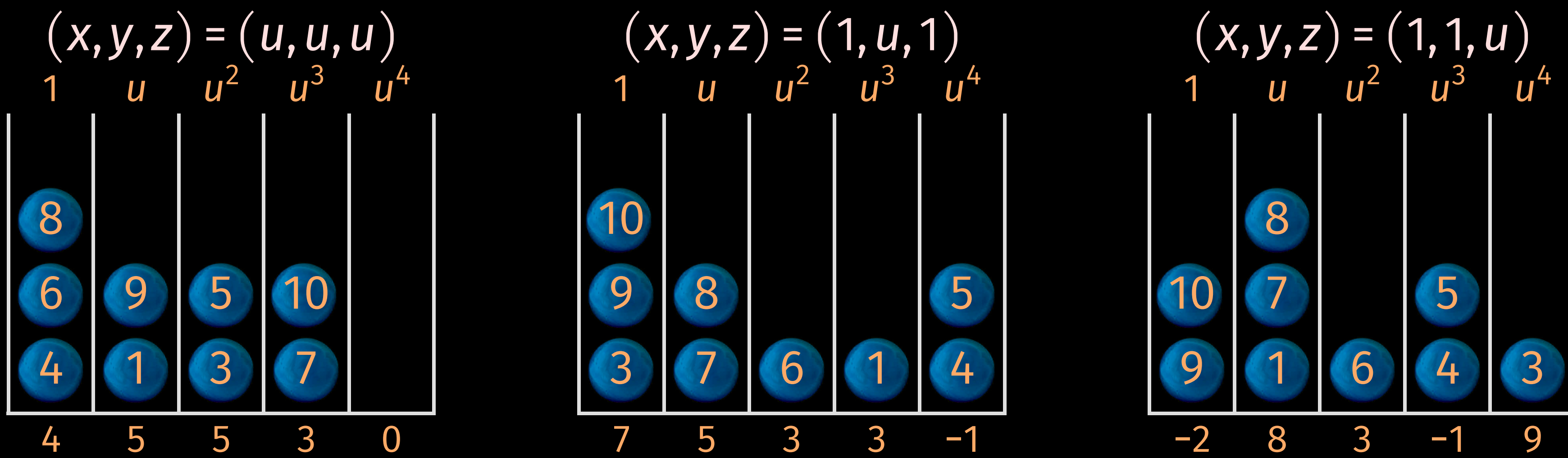
The game of mystery balls



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

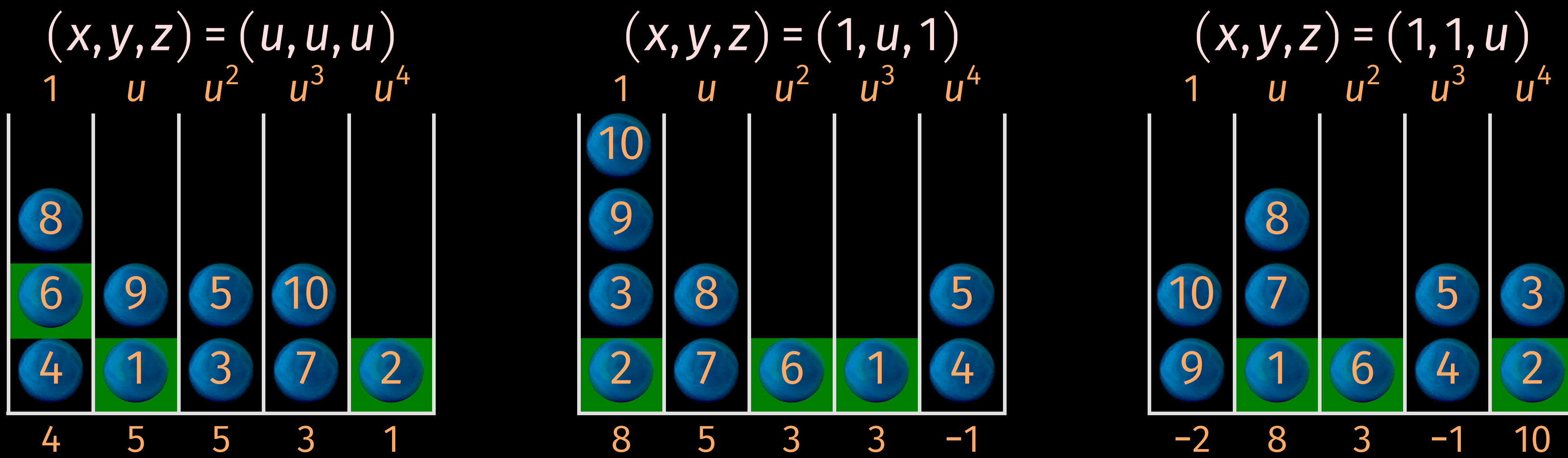
The game of mystery balls



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

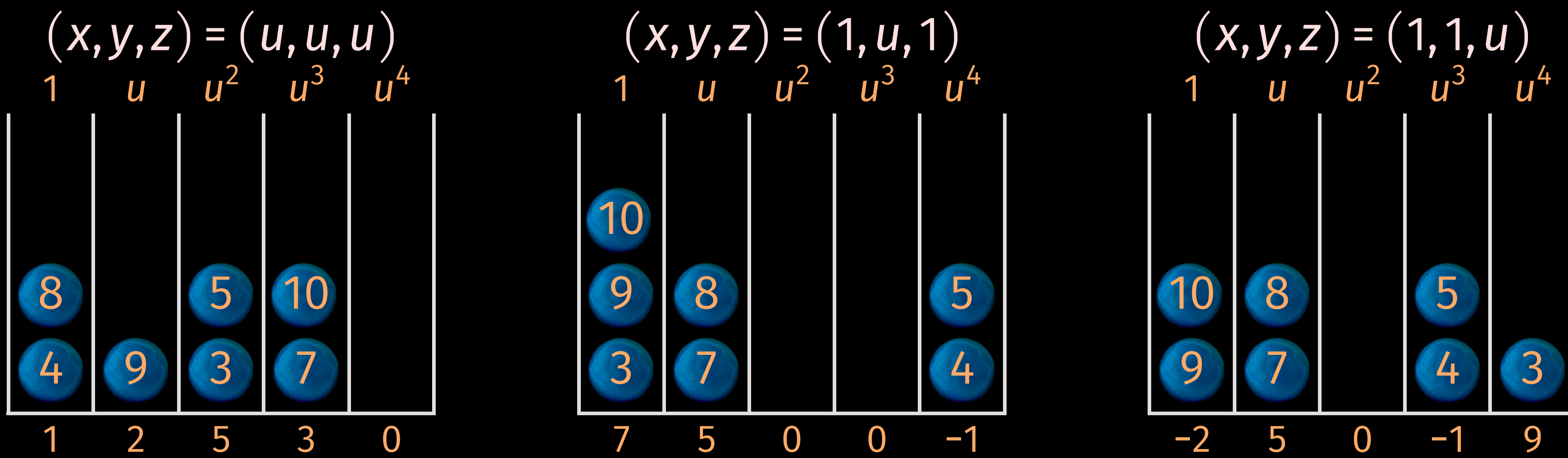
The game of mystery balls



$$f = \overbrace{3\,x^{12}y^{18}z^{6}}^{1} + \overbrace{1\,x^{10}y^{15}z^{4}}^{2} + \overbrace{9\,x^{3}y^{10}z^{4}}^{3} + \overbrace{3\,x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)\,x^{10}y^{14}z^{3}}^{5} +$$

$$\overbrace{3\,xy^{7}z^{2}}^{6} + \overbrace{7\,xy^{6}z}^{7} + \overbrace{(-2)\,x^{8}y^{11}z}^{8} + \overbrace{2\,xy^{5}}^{9} + \overbrace{(-4)\,x^{8}y^{10}}^{10}$$

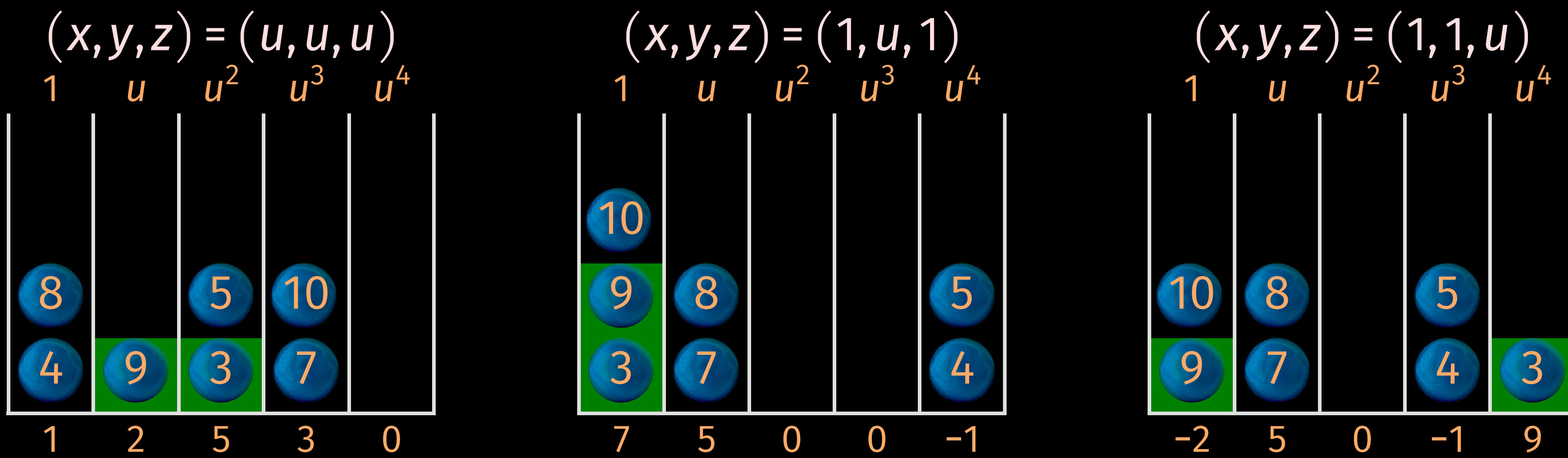
The game of mystery balls



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

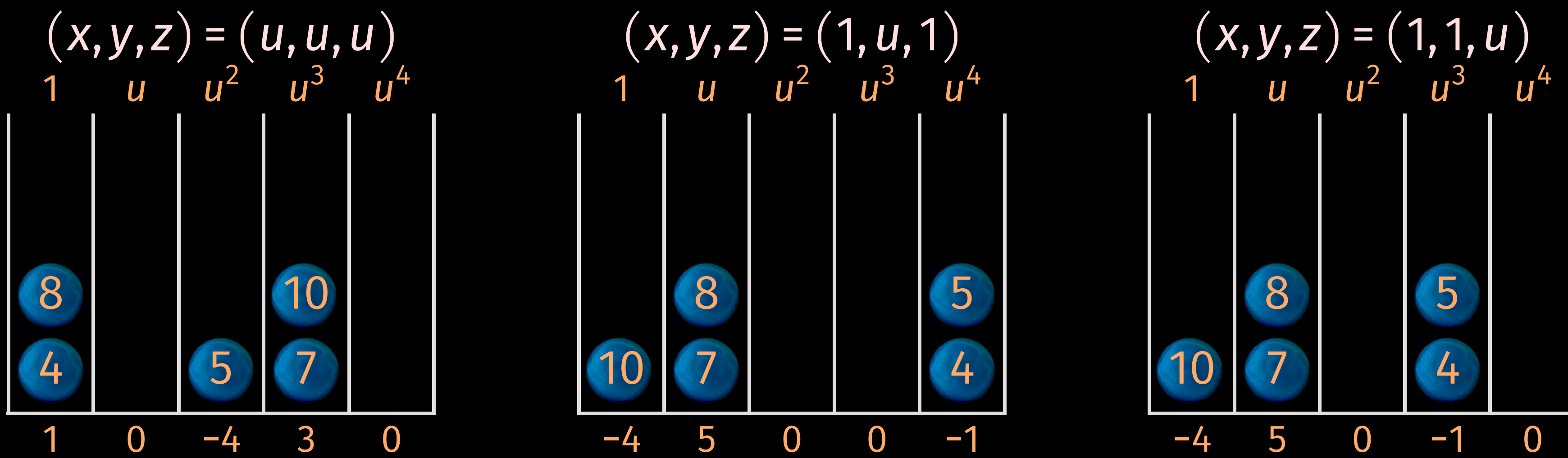
The game of mystery balls



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

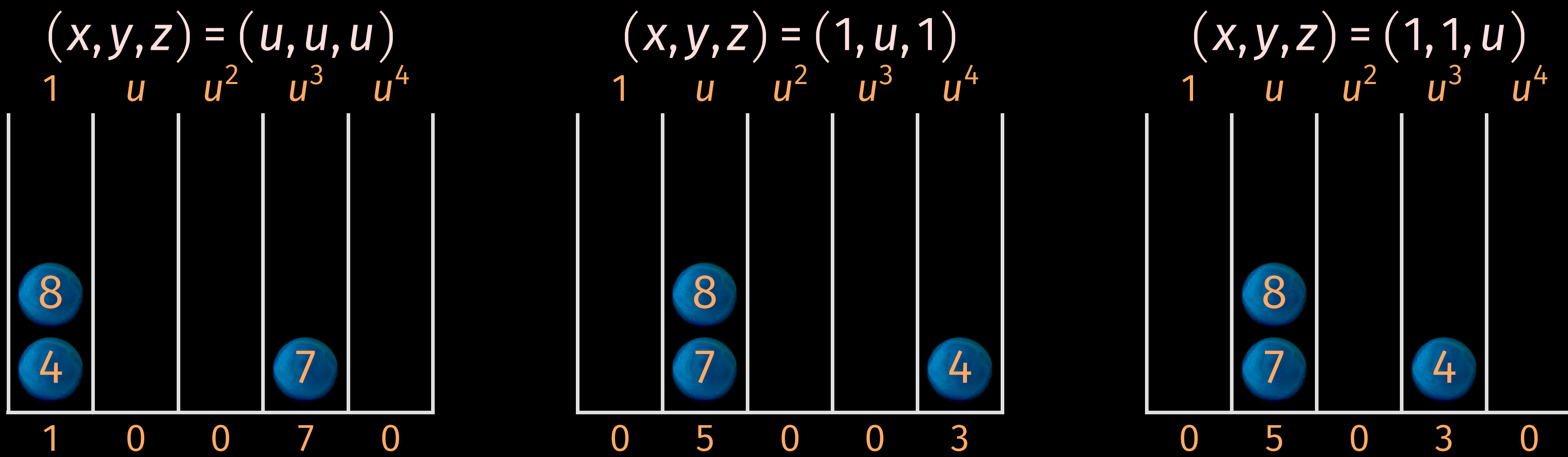
The game of mystery balls



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

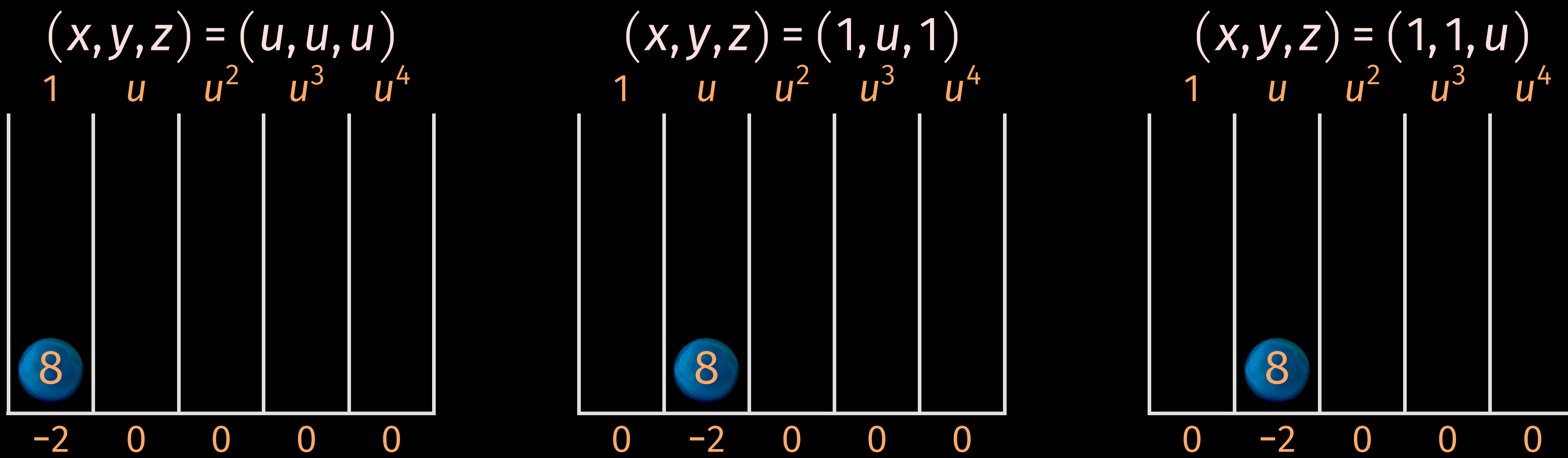
The game of mystery balls



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

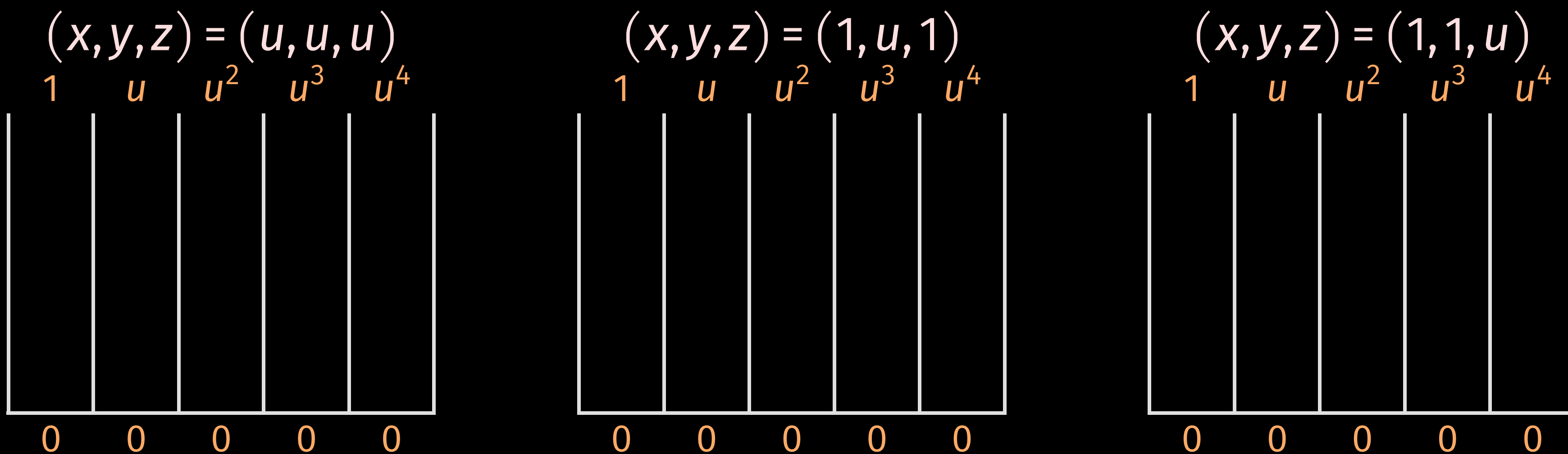
The game of mystery balls



$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)\,x^{10}y^{14}z^{3}}^{5} +$$

$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)\,x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)\,x^{8}y^{10}}^{10}$$

The game of mystery balls



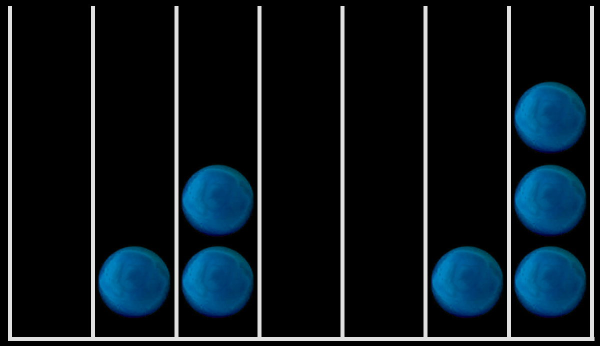
1 2 3 4 5

$$f = 3x^{12}y^{18}z^{6} + 1x^{10}y^{15}z^{4} + 9x^{3}y^{10}z^{4} + 3x^{3}y^{9}z^{3} + (-4)x^{10}y^{14}z^{3} +$$

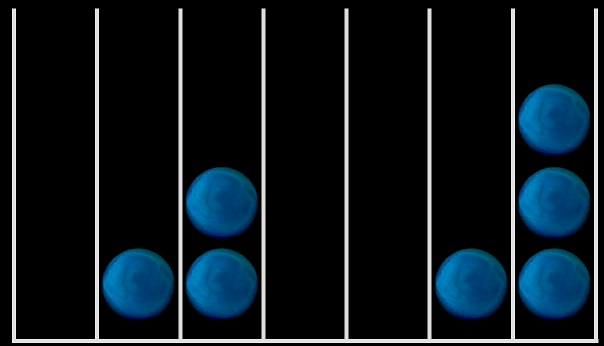
6 7 8 9 10

$$3xy^{7}z^{2} + 7xy^{6}z + (-2)x^{8}y^{11}z + 2xy^{5} + (-4)x^{8}y^{10}$$

Throwing t balls in $r = \tau t$ drawers

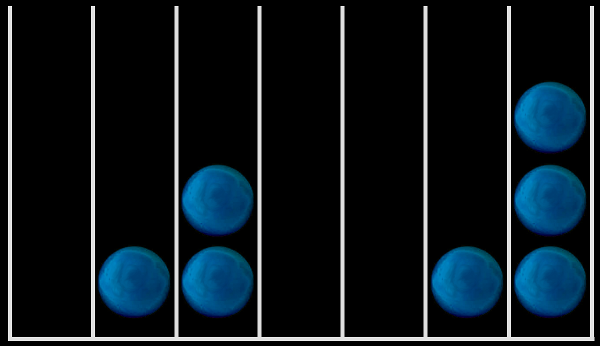


Throwing t balls in $r = \tau t$ drawers



p_k : probability for a ball to end up in a drawer with k balls

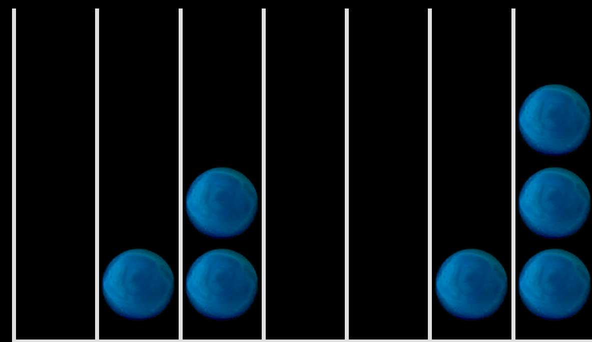
Throwing t balls in $r = \tau t$ drawers



p_k : probability for a ball to end up in a drawer with k balls

$$p_1 = \left(1 - \frac{1}{r}\right)^{t-1} = e^{(t-1)\log\left(1-\frac{1}{\tau t}\right)} = e^{-\frac{1}{\tau}+O\left(\frac{1}{t}\right)} = e^{-\frac{1}{\tau}} + O\left(\frac{1}{t}\right)$$

Throwing t balls in $r = \tau t$ drawers



p_k : probability for a ball to end up in a drawer with k balls

$$p_1 = \left(1 - \frac{1}{r}\right)^{t-1} = e^{(t-1)\log\left(1-\frac{1}{\tau t}\right)} = e^{-\frac{1}{\tau}+O\left(\frac{1}{t}\right)} = e^{-\frac{1}{\tau}} + O\left(\frac{1}{t}\right)$$

$$p_k = \binom{t-1}{k-1}\frac{1}{r^{k-1}}\left(1 - \frac{1}{r}\right)^{t-k} = \frac{e^{-\frac{1}{\tau}}}{(k-1)!\,\tau^{k-1}} + O\left(\frac{1}{t}\right)$$

Probabilistic analysis II

$p_{i,k}$ proportion of balls in a drawer with k balls at start of turn i

$\sigma_i = p_{i,0} + p_{i,1} + p_{i,2} + \cdots$

$$p_{i+1,j} = \sum_{k \geq \max(2,j)} \frac{j}{k} \lambda_{j,k} p_{i,k} \qquad \lambda_{j,k} = \binom{k}{j} \pi_i^{k-j} (1-\pi_i)^j \qquad \pi_i = \left(2 - \frac{p_{i,1}}{\sigma_i}\right) \frac{p_{i,1}}{\sigma_i}$$

$\tau = \frac{1}{2}$

$p_{i,k}$	$k=1$	2	3	4	5	6	7	σ_i
$i=1$	0.13534	0.27067	0.27067	0.18045	0.09022	0.03609	0.01203	1.00000
2	0.06643	0.25063	0.18738	0.09340	0.03491	0.01044	0.00260	0.64646
3	0.04567	0.21741	0.13085	0.05251	0.01580	0.00380	0.00076	0.46696
4	0.03690	0.18019	0.08828	0.02883	0.00706	0.00138	0.00023	0.34292
5	0.03234	0.13952	0.05443	0.01416	0.00276	0.00043	0.00006	0.24371
6	0.02869	0.09578	0.02811	0.00550	0.00081	0.00009	0.00001	0.15899
7	0.02330	0.05240	0.01033	0.00136	0.00013	0.00001	0.00000	0.08752
8	0.01428	0.01823	0.00193	0.00014	0.00001	0.00000	0.00000	0.03459
9	0.00442	0.00249	0.00009	0.00000	0.00000	0.00000	0.00000	0.00700
10	0.00030	0.00005	0.00000	0.00000	0.00000	0.00000	0.00000	0.00035
11	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000

Probabilistic analysis III

Gain with respect to previous approach

Expected number of evaluations: $3\tau t$ instead of $\mathrm{e}t$

Gain with respect to previous approach

Expected number of evaluations: $3\tau t$ instead of $\mathrm{e}\,t$

How small can we take τ?

$$0{,}407264 < \tau_{\mathrm{crit}} < 0{,}407265$$

Probabilistic analysis III

Gain with respect to previous approach

Expected number of evaluations: $3\tau t$ instead of $\mathrm{e}\, t$

How small can we take τ?

$$0{,}407264 \; < \; \tau_{\text{crit}} \; < \; 0{,}407265$$

$$\mathrm{M}_{\mathbb{K}}^{\text{sparse}}(t) \; \leqslant_{\text{heuristic}} \; 1{,}221795\, \mathrm{M}_{\mathbb{K}}^{\circ}(t) + O(t)$$

Gain with respect to previous approach

Expected number of evaluations: $3\tau t$ instead of $\mathrm{e}\,t$

How small can we take τ?

$$0{,}407264 < \tau_{\mathrm{crit}} < 0{,}407265$$

$$\mathsf{M}_{\mathbb{K}}^{\mathrm{sparse}}(t) \leqslant_{\mathrm{heuristic}} 1{,}221795\,\mathsf{M}_{\mathbb{K}}^{\circ}(t) + O(t)$$

Non-generic case of polynomials in *n* variables of total degree *d*

n	2	2	2	3	3	3	4	4	5	7	10
d	100	250	1000	25	50	100	20	40	20	15	10
s	5151	31626	501501	3276	23426	176853	10626	135751	53130	170544	184756
3τ	1.14	1.14	1.14	1.14	1.14	1.14	1.11	1.14	1.14	1.17	1.20

Thank you !

http://www.TeXmacs.org