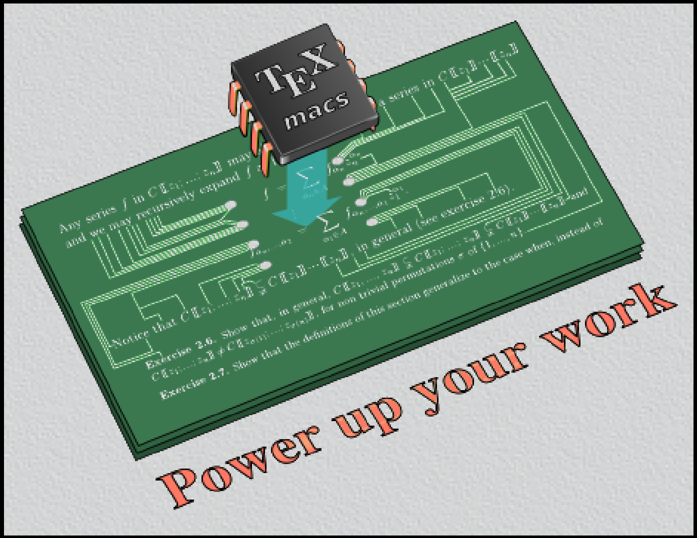
Sparse multiplication of multivariate polynomials

Joris van der Hoeven

CNRS, LIX, Parts in joint work with Grégoire Lecerf



RTCA, ENS Lyon

June 27, 2023

Part I

Statement of the problem

Sparse multiplication

$$\mathbb{K}[x] := \mathbb{K}[x_1, \ldots, x_n]$$
$$x^e := x_1^{e_1} \cdots x_n^{e_n}$$

$$\mathbb{K}[x] := \mathbb{K}[x_1, \ldots, x_n]$$
$$x^e := x_1^{e_1} \cdots x_n^{e_n}$$

Sparse polynomials

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

$$\mathbb{K}[x] := \mathbb{K}[x_1, \ldots, x_n]$$
$$x^e := x_1^{e_1} \cdots x_n^{e_n}$$

Sparse polynomials

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

Sparse multiplication

Given sparse $g, h \in \mathbb{K}[x]$, compute $f := g\, h$.

$$\mathbb{K}[x] := \mathbb{K}[x_1, \ldots, x_n]$$
$$x^e := x_1^{e_1} \cdots x_n^{e_n}$$

Sparse polynomials

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

Sparse multiplication

Given sparse $g, h \in \mathbb{K}[x]$, compute $f := g\, h$.

Complexity in terms of t_f, t_g, t_h, $d := \deg R$, and n.

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 *versus* probabilistic.
- Theoretic (asymptotic) *versus* practical complexity.

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 *versus* probabilistic.
- Theoretic (asymptotic) *versus* practical complexity.

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 $\log t = o(\log d)$.

Remark

$t_f \approx t_g t_h \implies$ naive multiplication performs best.

This talk

Remark

$t_f \approx t_g t_h \implies$ naive multiplication performs best.

Our focus

- Fast algorithms when $t_f \ll t_g t_h$.
- Weakly or normally sparse setting.
- $\mathbb{K} = \mathbb{F}_p$ (in practice, $p \approx 2^{48}$, possibly an FFT prime).

Remark

$t_f \approx t_g\, t_h \implies$ naive multiplication performs best.

Our focus

- Fast algorithms when $t_f \ll t_g\, t_h$.
- Weakly or normally sparse setting.
- $\mathbb{K} = \mathbb{F}_p$ (in practice, $p \approx 2^{48}$, possibly an FFT prime).

Note

- Packing of exponents $e = (e_1, \ldots, e_n)$ important in practice.
- $\mathbb{K} = \mathbb{Z}$ and $\mathbb{K} = \mathbb{Q}$ recovered using Chinese remaindering.
- Extensible to $\mathbb{K} = \mathbb{C}$ using similar techniques.

Part II

The geometric sequence approach

Geometric sequence approach

- $\alpha \in \mathbb{K}^n$ is such that we can efficiently recover $e \in \mathbb{N}^n$ from α^n.
- (an upper bound for) t is known and that $1, \ldots, \alpha^{2t-1}$ pairwise distinct.

Geometric sequence approach

- $\alpha \in \mathbb{K}^n$ is such that we can efficiently recover $e \in \mathbb{N}^n$ from α^n.
- (an upper bound for) t is known and that $1, \ldots, \alpha^{2t-1}$ pairwise distinct.

Evaluate

Compute $g(\alpha^k)$ and $h(\alpha^k)$ for $k = 0, \ldots, 2t-1$.

Geometric sequence approach

- $\alpha \in \mathbb{K}^n$ is such that we can efficiently recover $e \in \mathbb{N}^n$ from α^n.
- (an upper bound for) t is known and that $1, \ldots, \alpha^{2t-1}$ pairwise distinct.

Evaluate

Compute $g(\alpha^k)$ and $h(\alpha^k)$ for $k = 0, \ldots, 2t-1$.

Multiply

Multiply $f(\alpha^k) := g(\alpha^k)\, h(\alpha^k)$ for $k = 0, \ldots, 2t-1$.

- $\alpha \in \mathbb{K}^n$ is such that we can efficiently recover $e \in \mathbb{N}^n$ from α^n.
- (an upper bound for) t is known and that $1, \ldots, \alpha^{2t-1}$ pairwise distinct.

Evaluate

Compute $g(\alpha^k)$ and $h(\alpha^k)$ for $k = 0, \ldots, 2t - 1$.

Multiply

Multiply $f(\alpha^k) := g(\alpha^k)\, h(\alpha^k)$ for $k = 0, \ldots, 2t - 1$.

Interpolate

Recover f from $f(1), f(\alpha), \ldots, f(\alpha^{2t-1})$.

Geometric sequence approach

- $\alpha \in \mathbb{K}^n$ is such that we can efficiently recover $e \in \mathbb{N}^n$ from α^n.
- (an upper bound for) t is known and that $1, \ldots, \alpha^{2t-1}$ pairwise distinct.

Evaluate

Compute $g(\alpha^k)$ and $h(\alpha^k)$ for $k = 0, \ldots, 2t-1$.

Multiply

Multiply $f(\alpha^k) := g(\alpha^k)\, h(\alpha^k)$ for $k = 0, \ldots, 2t-1$.

Interpolate

Recover f from $f(1), f(\alpha), \ldots, f(\alpha^{2t-1})$.

Complexity

$O(\mathsf{M}(t) \log t)$ in most favorable case (using tangent Graeffe).

Part III

The cyclic extension approach

Idea

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

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

Main idea (univariate case)

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

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

Match corresponding terms to find the e_i and next the c_i

Idea

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

Main idea (univariate case)

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

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

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

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 $x^{10} - 1$

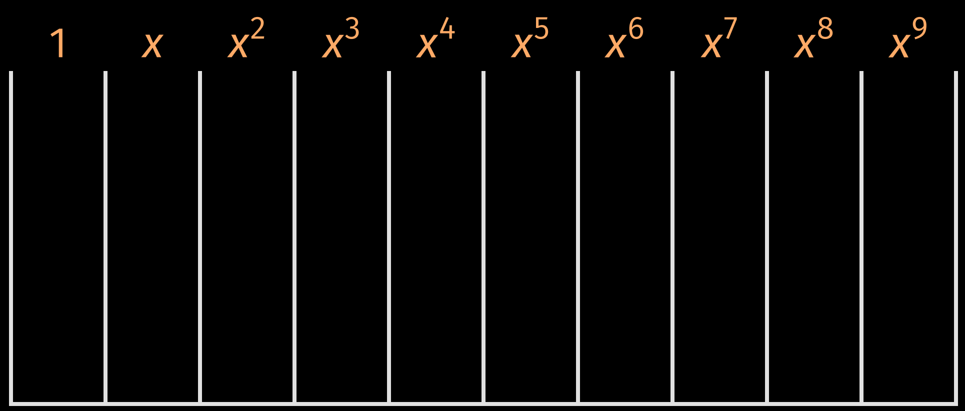
$$\begin{aligned} f &\equiv 18x^0 + 33x^2 + 2x^7 + x^2 + 7x^1 + 4x^8 + 11x^3 + 28 \\ &\equiv 4x^8 + 2x^7 + 11x^3 + (33+1)x^2 + 7x^1 + (28+18)x^0 \\ xf' &\equiv 4500x^0 + 7656x^2 + 394x^7 + 152x^2 + 847x^1 + 472x^8 + 693x^3 + 0 \\ &\equiv 472x^8 + 394x^7 + 693x^3 + (7656+152)x^2 + 847x^1 + (4500+0)x^0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

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

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

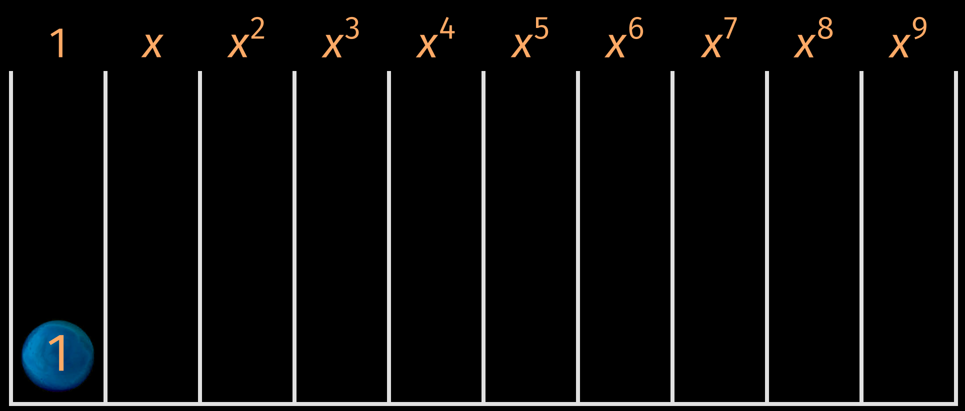
A combinatorial ball model

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



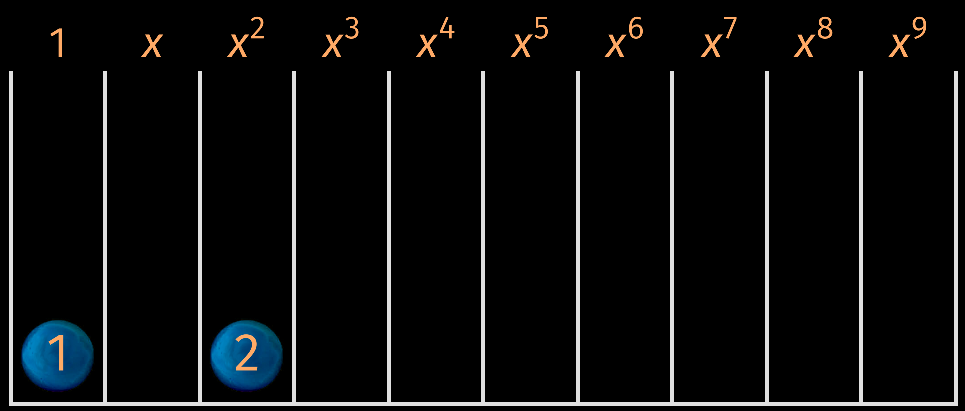
A combinatorial ball model

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

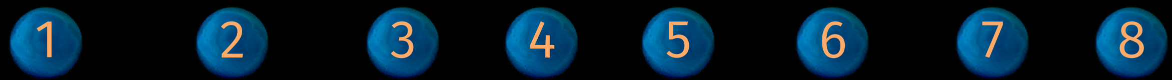


A combinatorial ball model

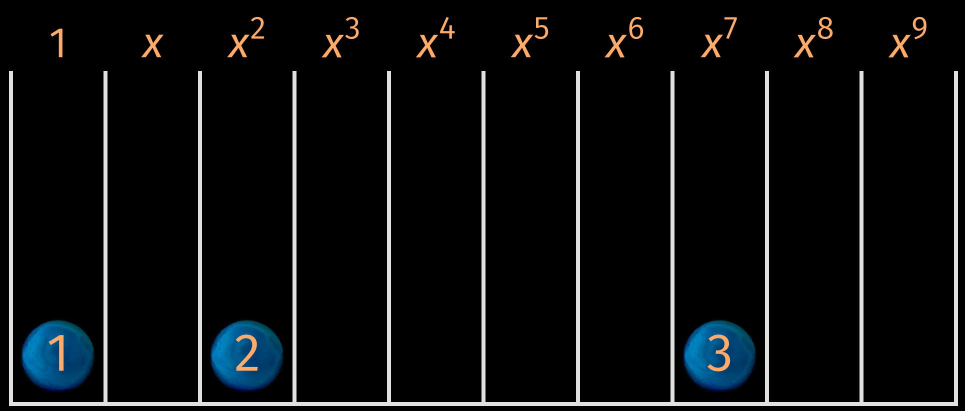
$$f = \overbrace{18\,x^{250}}^{1} + \overbrace{33\,x^{232}}^{2} + \overbrace{2\,x^{197}}^{3} + \overbrace{x^{152}}^{4} + \overbrace{7\,x^{121}}^{5} + \overbrace{4\,x^{118}}^{6} + \overbrace{11\,x^{63}}^{7} + \overbrace{28}^{8}$$



A combinatorial ball model

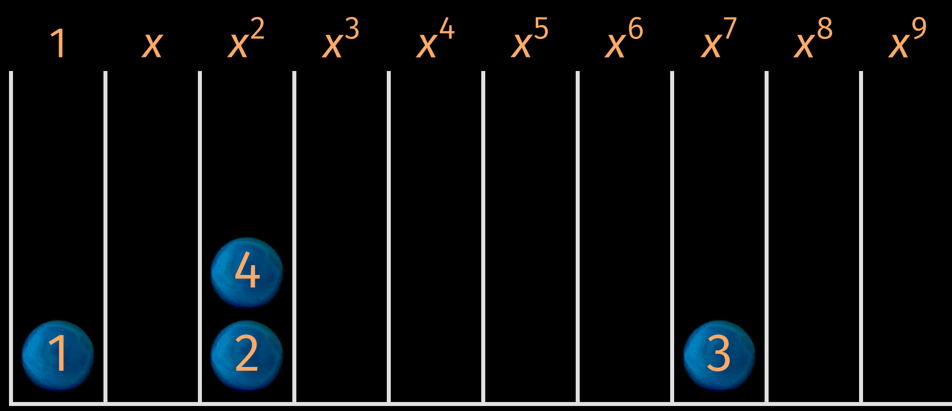


$$f = \overline{18x^{250}} + \overline{33x^{232}} + \overline{2x^{197}} + \overline{x^{152}} + \overline{7x^{121}} + \overline{4x^{118}} + \overline{11x^{63}} + \overline{28}$$



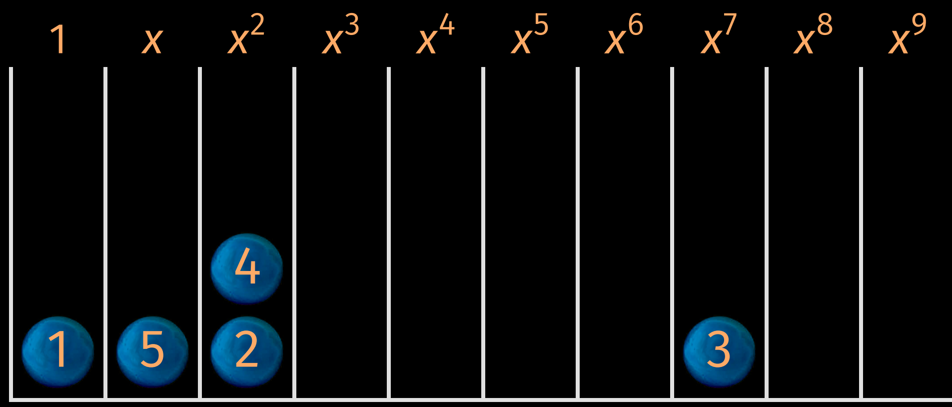
A combinatorial ball model

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



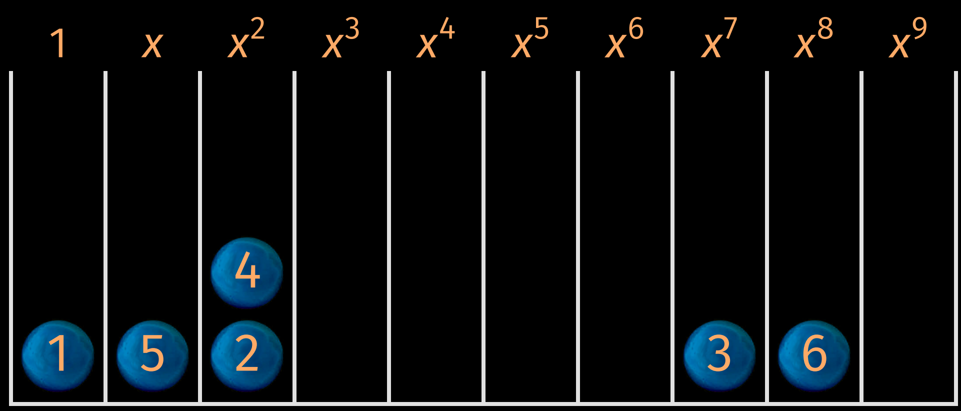
A combinatorial ball model

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



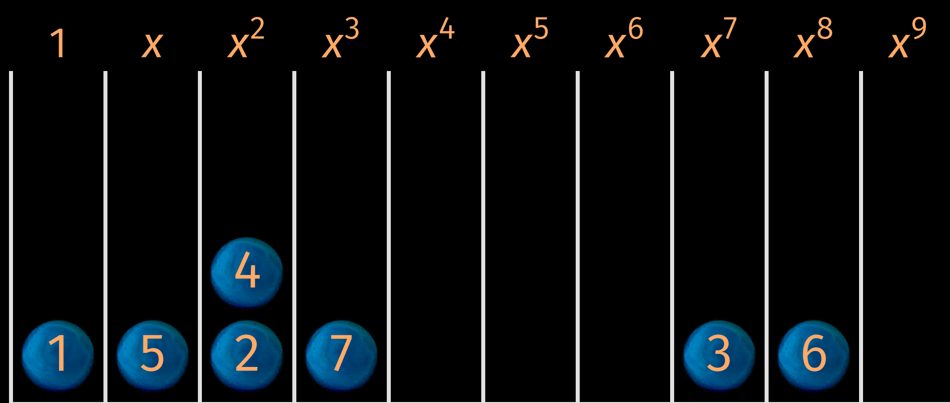
A combinatorial ball model

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



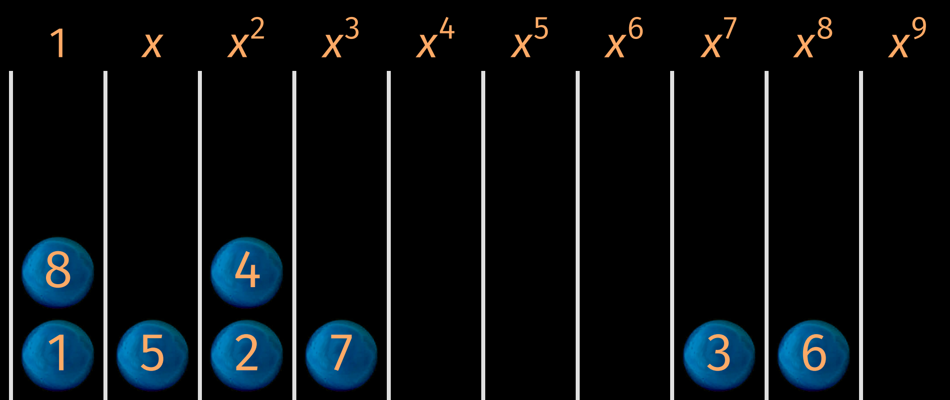
A combinatorial ball model

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



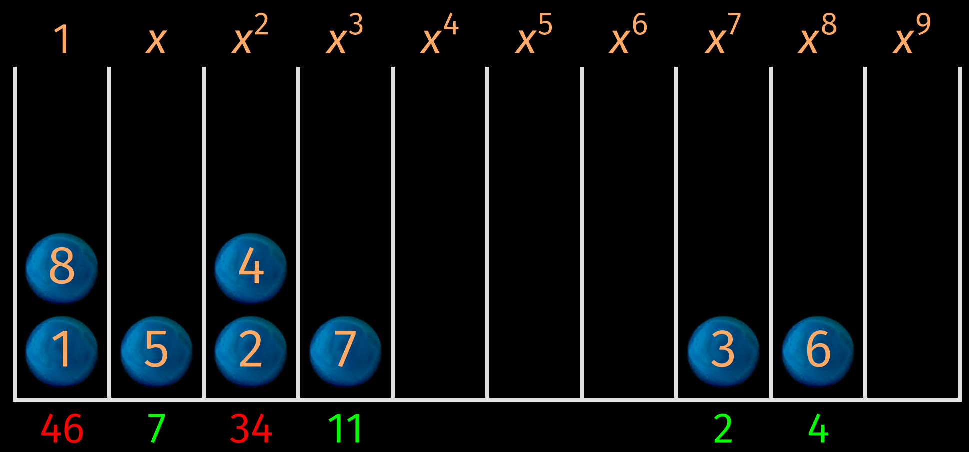
A combinatorial ball model

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



A combinatorial ball model

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



Probabilistic analysis

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:

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

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 $f(x)$, $xf'(x)$ modulo $x^r-1 \xrightarrow{\text{ops in } \mathbb{F}_p} 3\,\mathsf{M}(r)+O(r)$

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:

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

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

Computational cost

- Evaluating $f(x), xf'(x)$ modulo $x^r-1 \xrightarrow{\text{ops in } \mathbb{F}_p} 3\,\mathsf{M}(r)+O(r)$
- 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 $f(x), xf'(x)$ modulo $x^r-1 \xrightarrow{\text{ops in } \mathbb{F}_p} 3\,\mathsf{M}(r)+O(r)$
- 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 IV

FFT-based approach

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

Compute gh modulo $x^r - 1$ using two DFTs and one inverse DFT.

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

Compute $g\,h$ modulo $x^r - 1$ using two DFTs and one inverse DFT.

Complex coefficients

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

Rough summary

	General	Known exponents
Geometric sequences	$O(\mathrm{M}(t)\log t)$	$O(\mathrm{M}(t)\log t)$
Cyclic extensions	$3\,\mathrm{e}\,\mathrm{M}(t)+O(t)$	$\mathrm{e}\,\mathrm{M}(t)+O(t)$
FFT-based approach	$\mathrm{e}\,\mathrm{M}(t)+O(t)$	$^1/_2\,\mathrm{e}\,\mathrm{M}(t)+O(t)$

Complexity

Rough summary

	General	Known exponents
Geometric sequences	$O(\mathsf{M}(t)\log t)$	$O(\mathsf{M}(t)\log t)$
Cyclic extensions	$3\,\mathrm{e}\,\mathsf{M}(t)+O(t)$	$\mathrm{e}\,\mathsf{M}(t)+O(t)$
FFT-based approach	$\mathrm{e}\,\mathsf{M}(t)+O(t)$	${}^1\!/_2\,\mathrm{e}\,\mathsf{M}(t)+O(t)$

Notes

Rough summary

	General	Known exponents
Geometric sequences	$O(\mathrm{M}(t)\log t)$	$O(\mathrm{M}(t)\log t)$
Cyclic extensions	$3\,\mathrm{e}\,\mathrm{M}(t)+O(t)$	$\mathrm{e}\,\mathrm{M}(t)+O(t)$
FFT-based approach	$\mathrm{e}\,\mathrm{M}(t)+O(t)$	$^1/_2\,\mathrm{e}\,\mathrm{M}(t)+O(t)$

Notes

- Heuristic/expected complexities in terms of operations in $\mathbb{F}_p$.

Rough summary

	General	Known exponents
Geometric sequences	$O(\mathsf{M}(t)\log t)$	$O(\mathsf{M}(t)\log t)$
Cyclic extensions	$3\,\mathrm{e}\,\mathsf{M}(t)+O(t)$	$\mathrm{e}\,\mathsf{M}(t)+O(t)$
FFT-based approach	$\mathrm{e}\,\mathsf{M}(t)+O(t)$	${}^{1}\!/_{2}\,\mathrm{e}\,\mathsf{M}(t)+O(t)$

Notes

- Heuristic/expected complexities in terms of operations in $\mathbb{F}_p$.
- Discarded dependence on d and n.

Part V

A game of mystery balls

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

Multiplication of sparse polynomials

Example

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

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

Idea

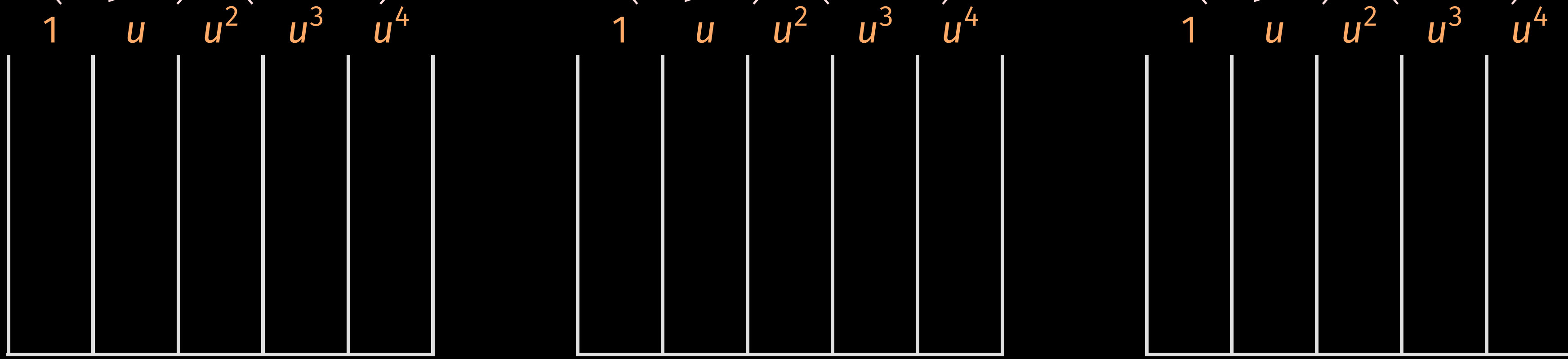
- For “random” $(\alpha,\beta,\gamma)\in\mathbb{N}^3$, evaluate $f(u^\alpha,u^\beta,u^\gamma)$ modulo u^r-1
- *Three* directions $(\alpha_i,\beta_i,\gamma_i)_{i=1,2,3}$ instead of a single one $\longrightarrow$ smaller r

Assumption

Exponents already known

The game of mystery balls

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

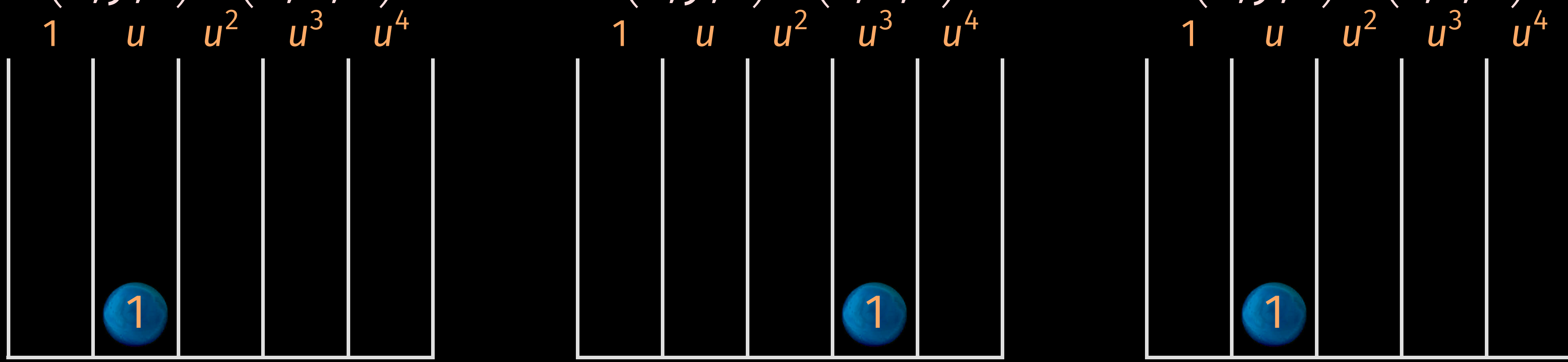


$$f = \overset{1}{\overbrace{3x^{12}y^{18}z^{6}}} + \overset{2}{\overbrace{1x^{10}y^{15}z^{4}}} + \overset{3}{\overbrace{9x^{3}y^{10}z^{4}}} + \overset{4}{\overbrace{3x^{3}y^{9}z^{3}}} + \overset{5}{\overbrace{(-4)x^{10}y^{14}z^{3}}} +$$

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

The game of mystery balls

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

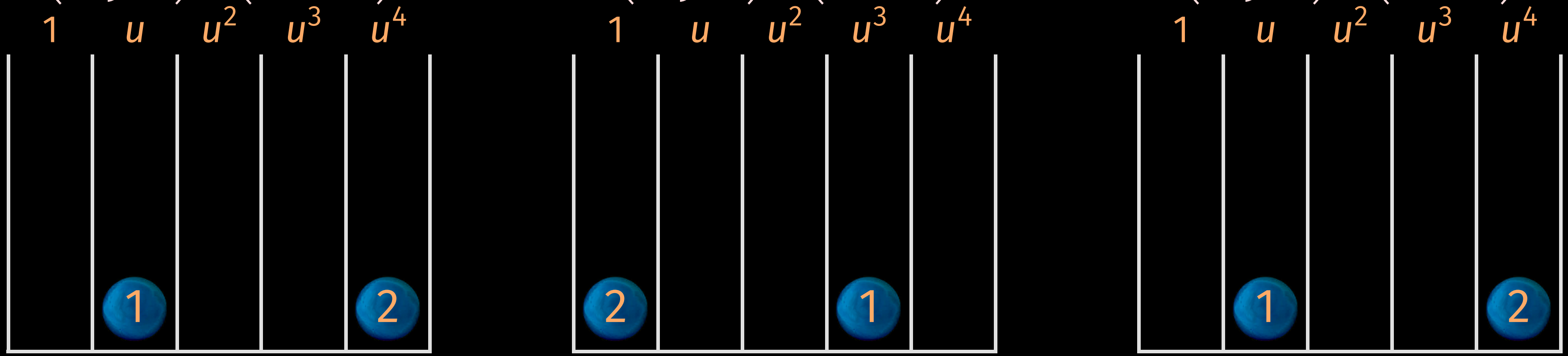


$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

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

The game of mystery balls

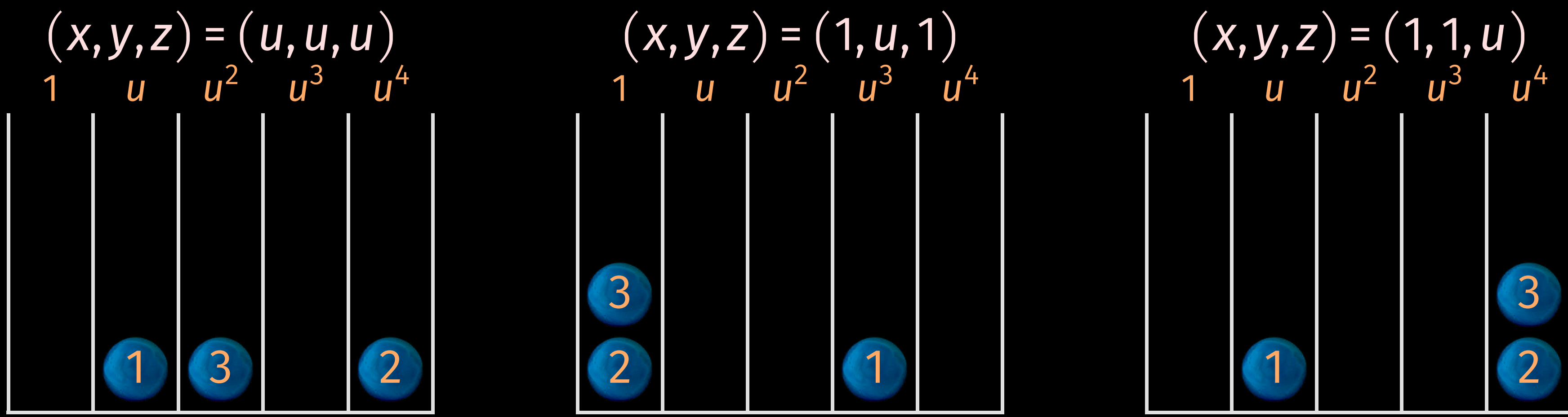
$(x,y,z) = (u,u,u)$ $\qquad$ $(x,y,z) = (1,u,1)$ $\qquad$ $(x,y,z) = (1,1,u)$



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

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

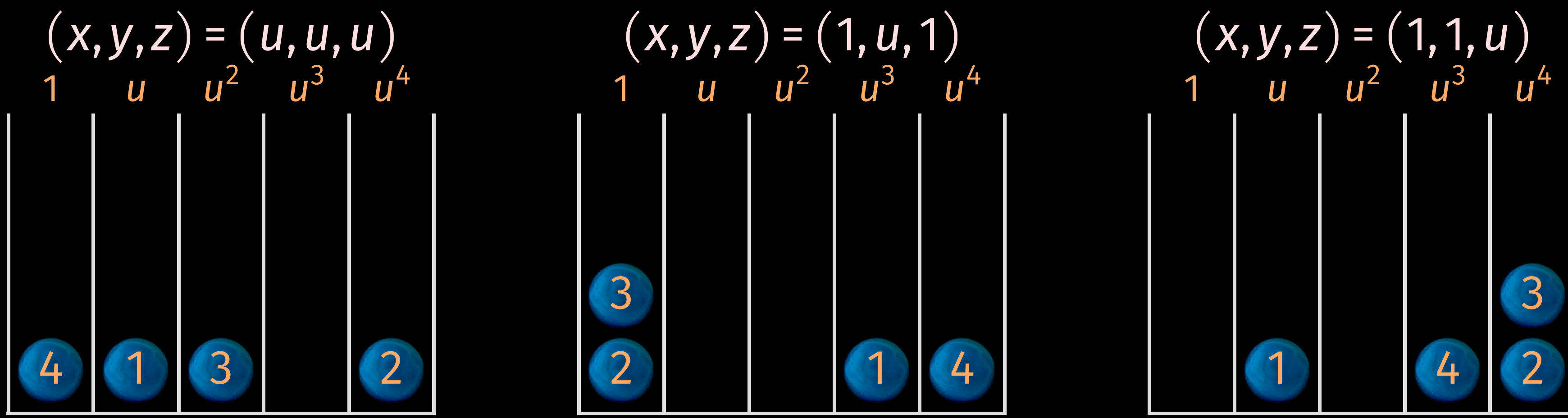
The game of mystery balls



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

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

The game of mystery balls

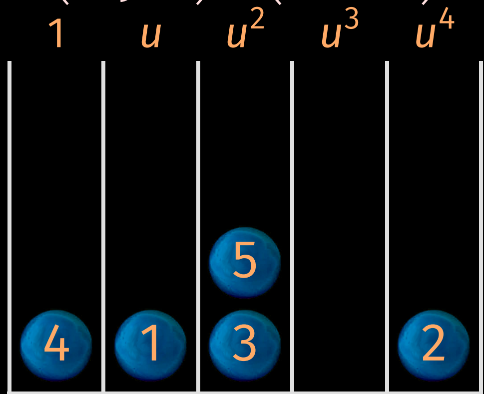


$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)\,x^{10}y^{14}z^{3}}^{5} +$$

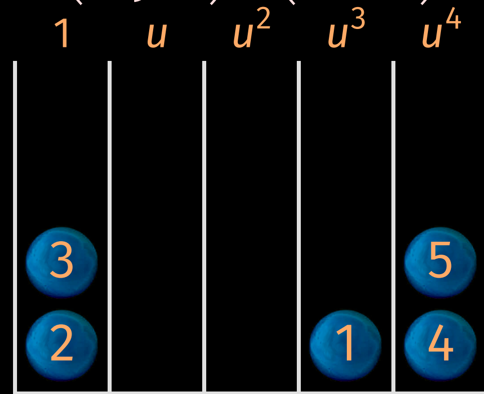
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)\,x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)\,x^{8}y^{10}}^{10}$$

The game of mystery balls

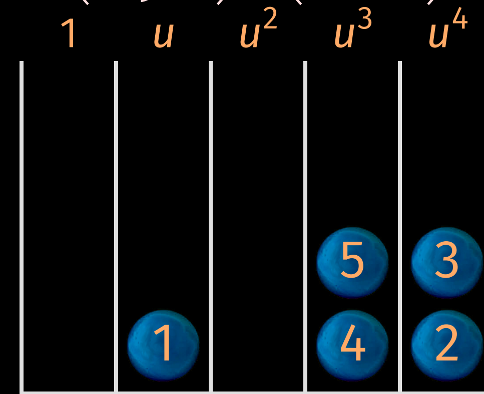
$(x, y, z) = (u, u, u)$



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



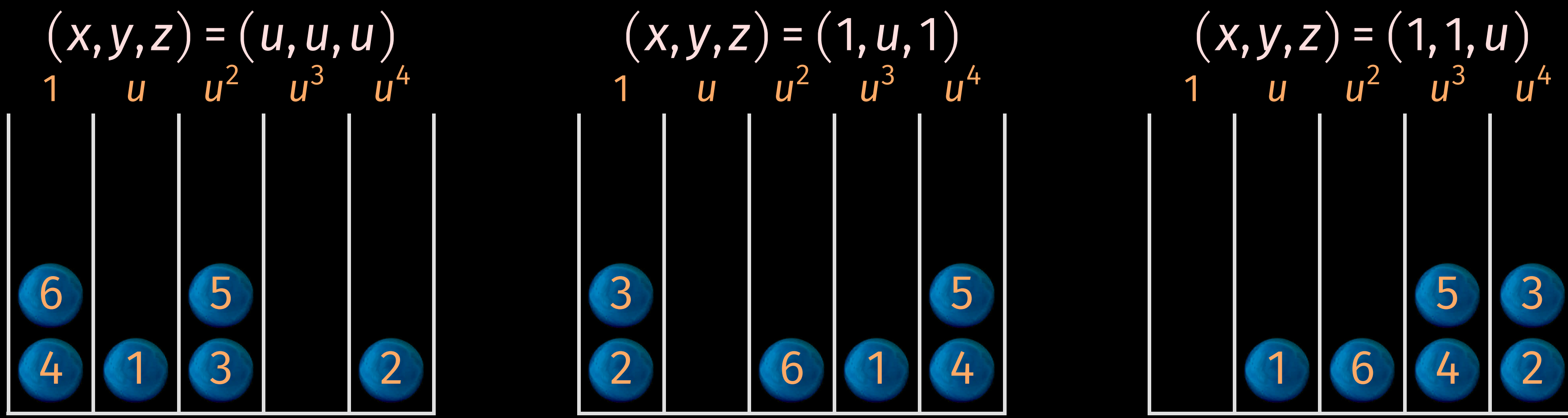
$(x, y, z) = (1, 1, u)$



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

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

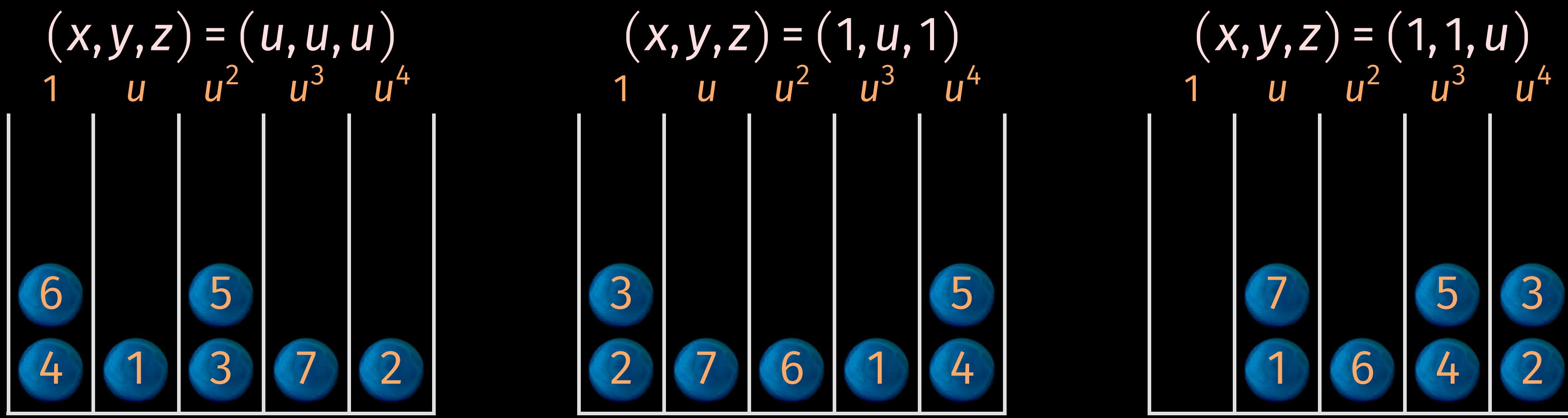
The game of mystery balls



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

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

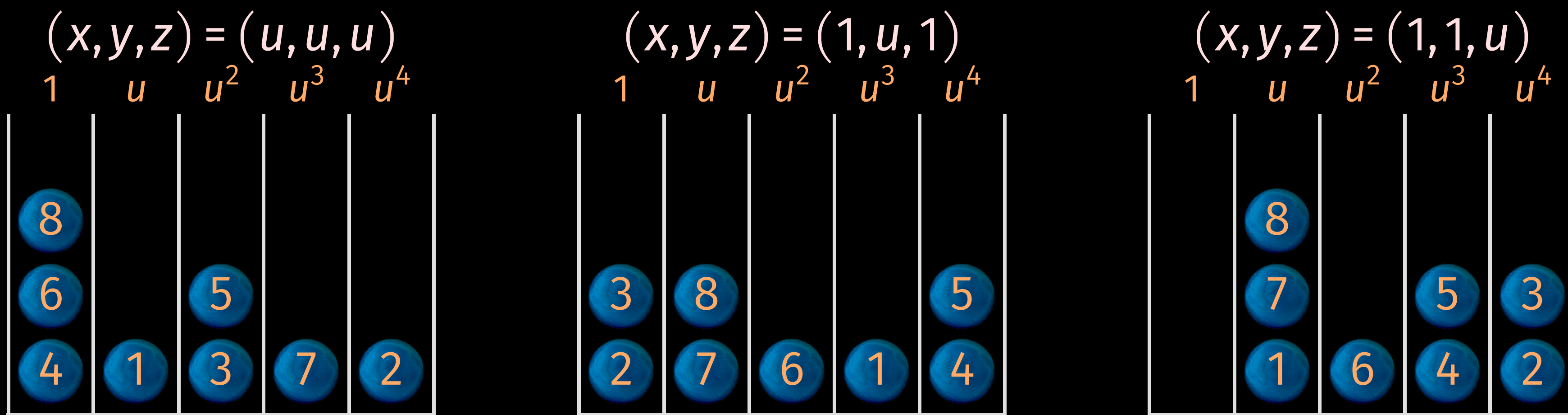
The game of mystery balls



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

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

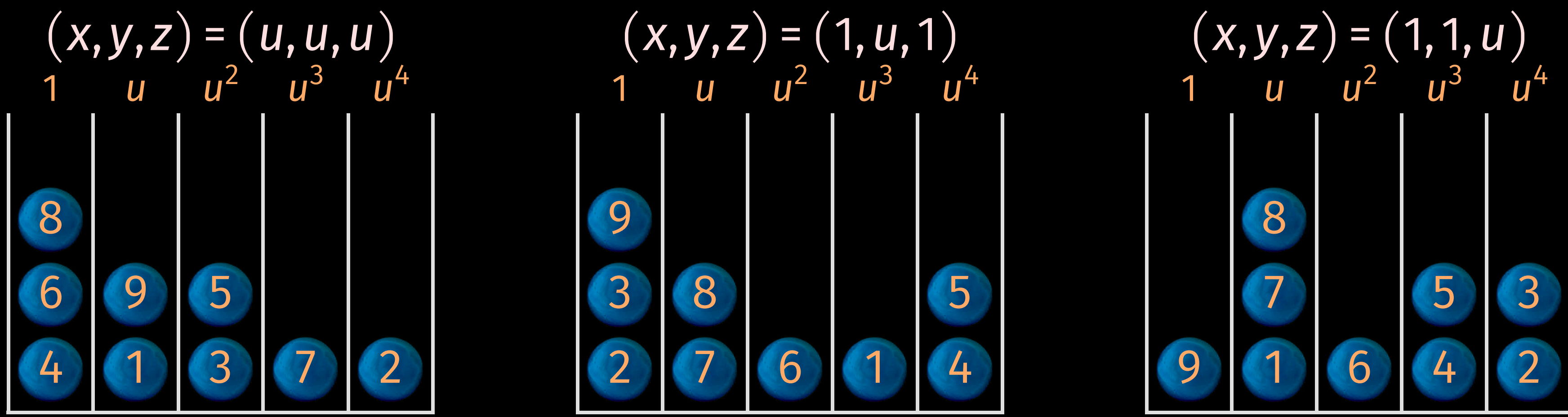
The game of mystery balls



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

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

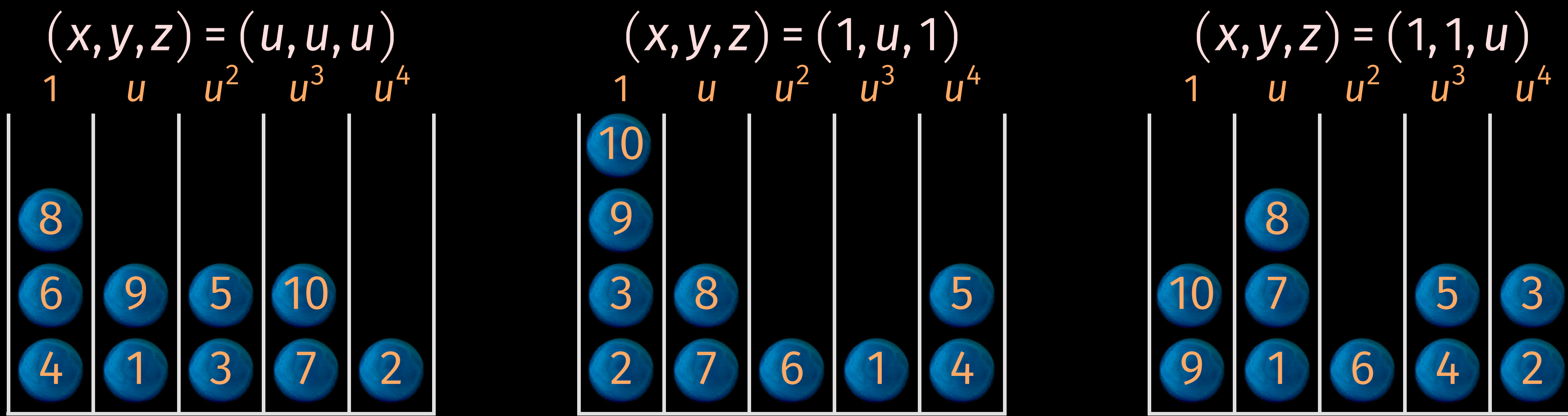
The game of mystery balls



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

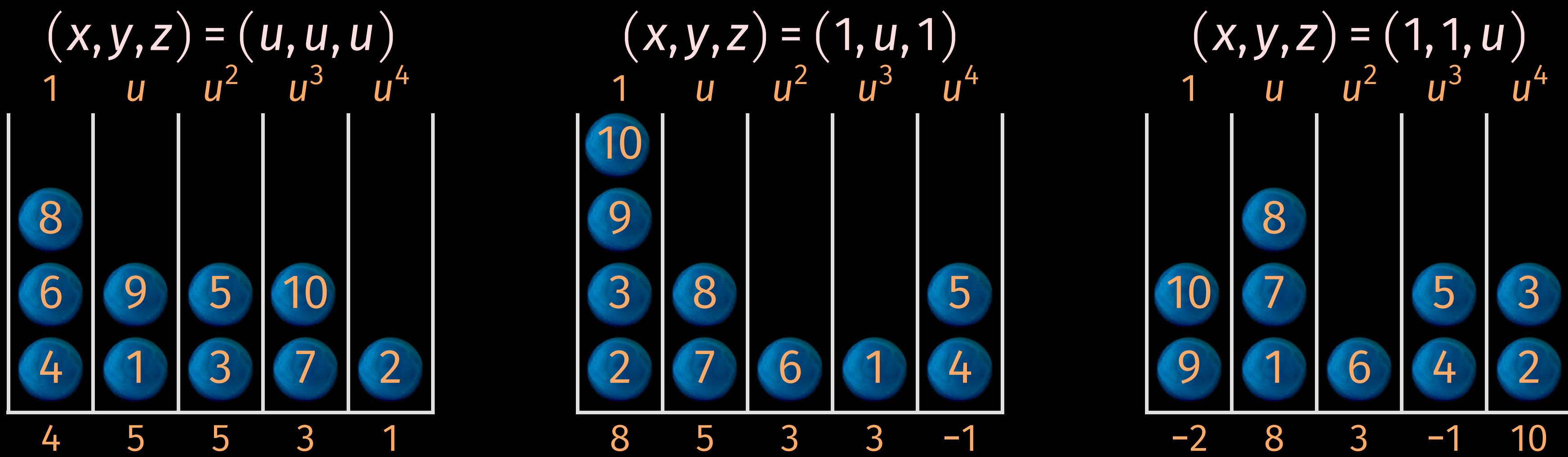
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

The game of mystery balls



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

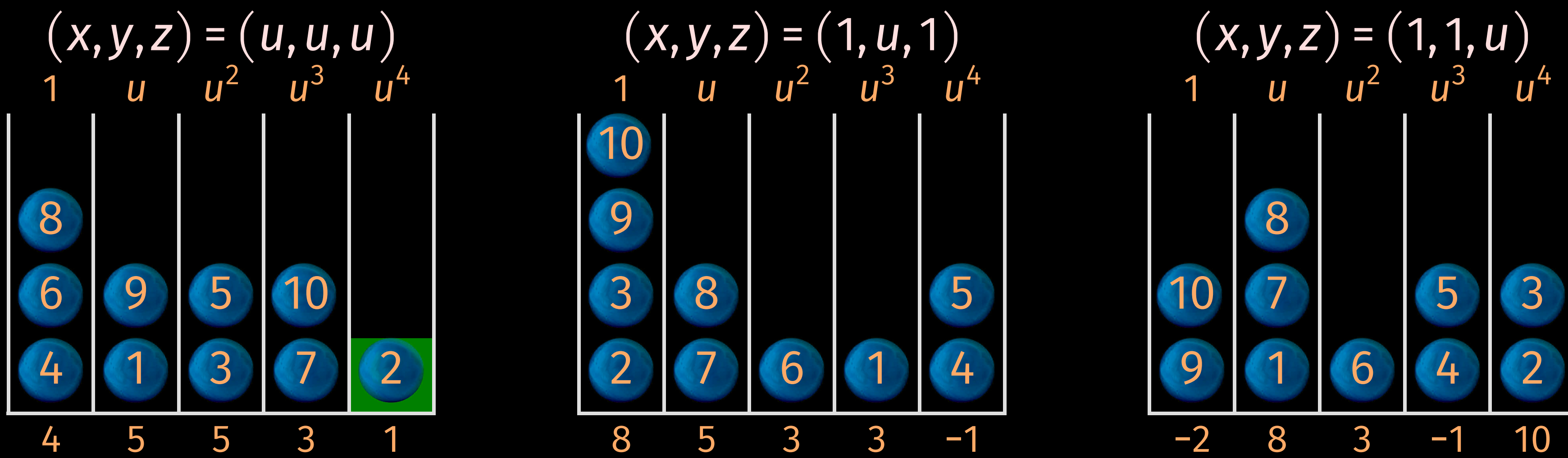
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$



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

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

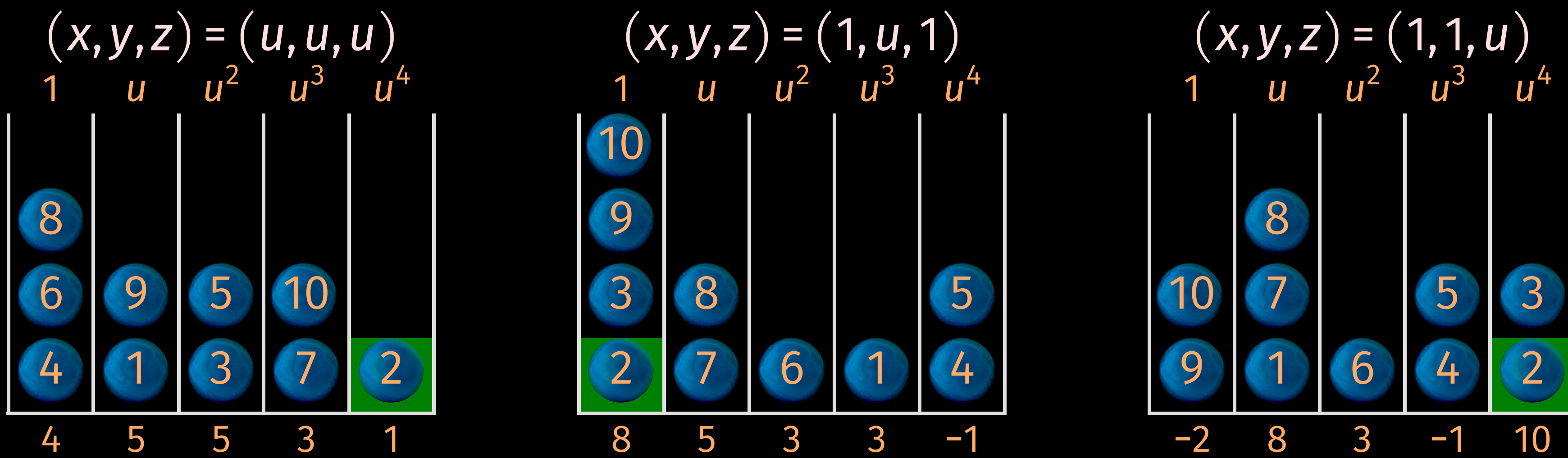
The game of mystery balls



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

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

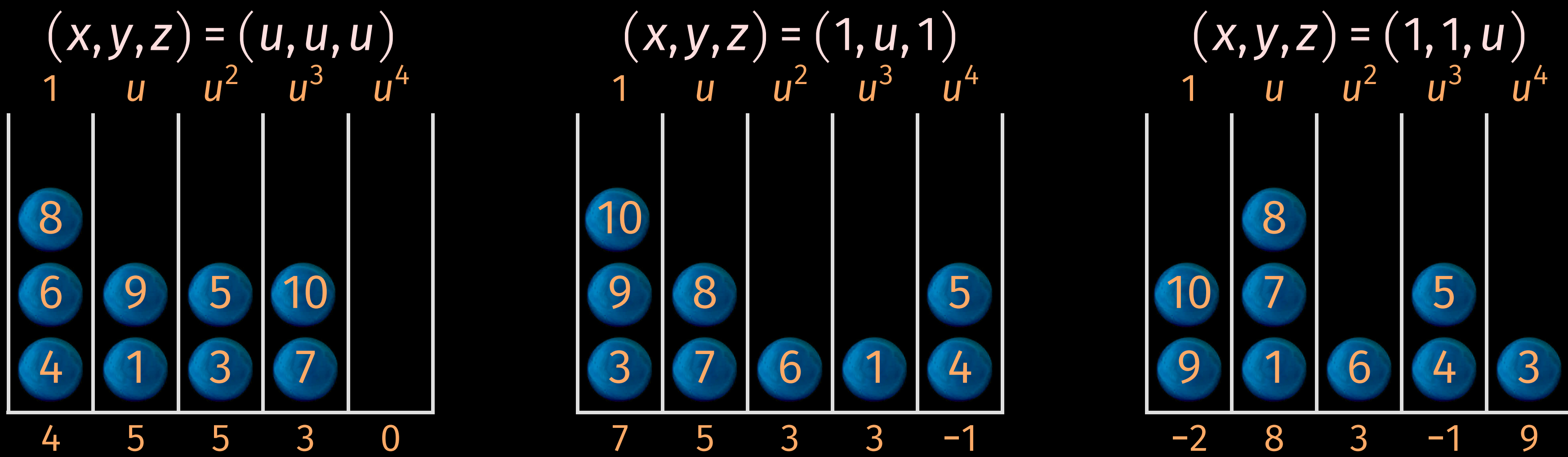
The game of mystery balls



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

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

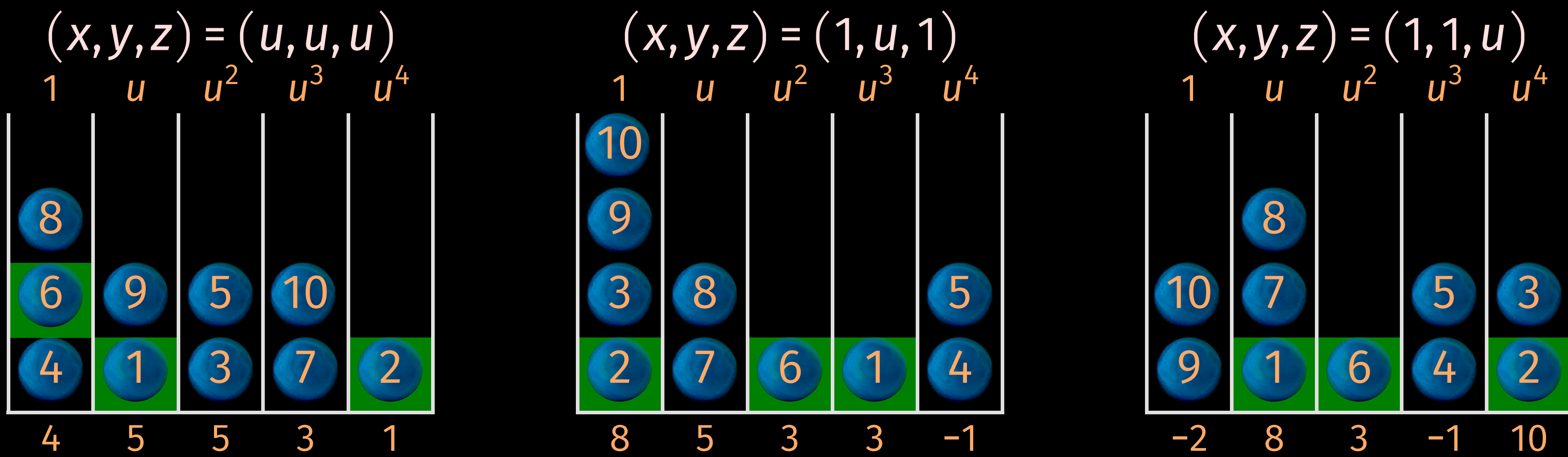
The game of mystery balls



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

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

The game of mystery balls

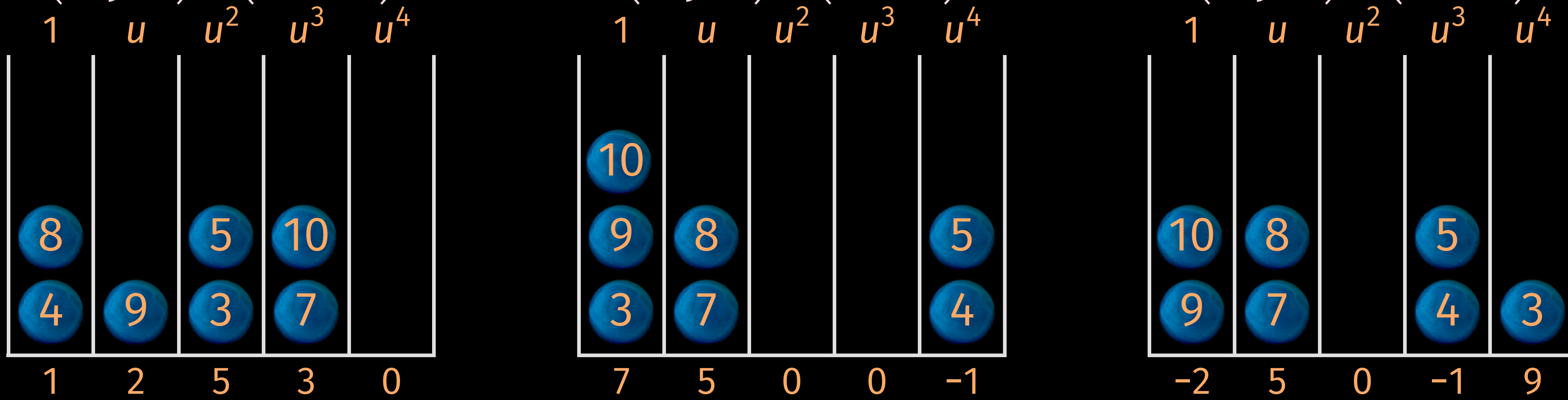


$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

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

The game of mystery balls

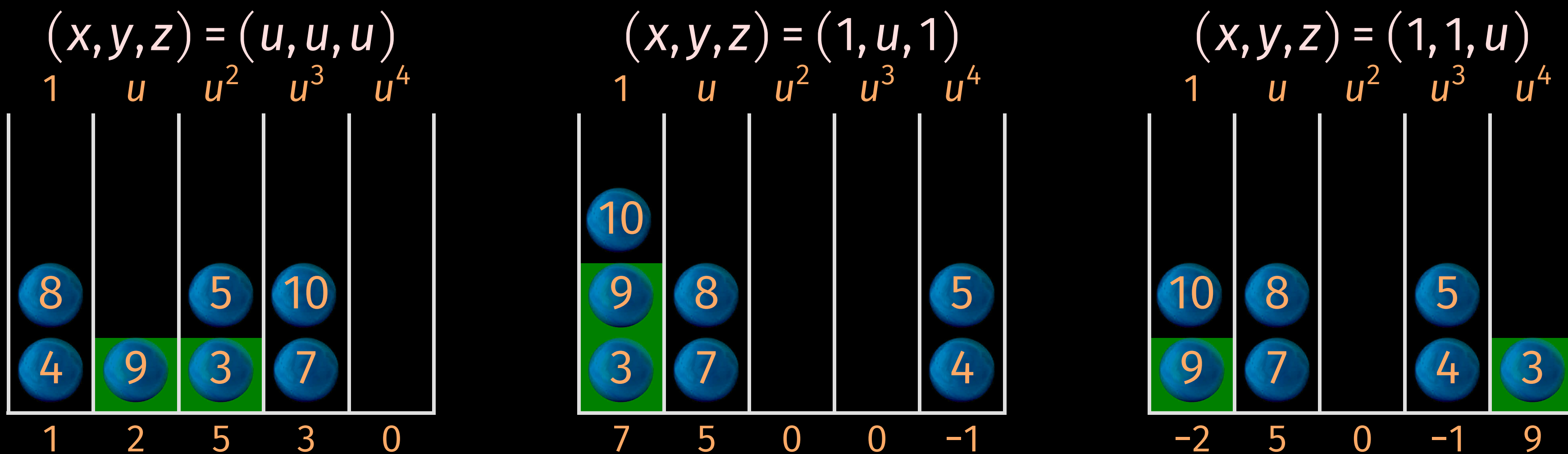
$(x,y,z)=(u,u,u)$ $\quad$ $(x,y,z)=(1,u,1)$ $\quad$ $(x,y,z)=(1,1,u)$



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

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

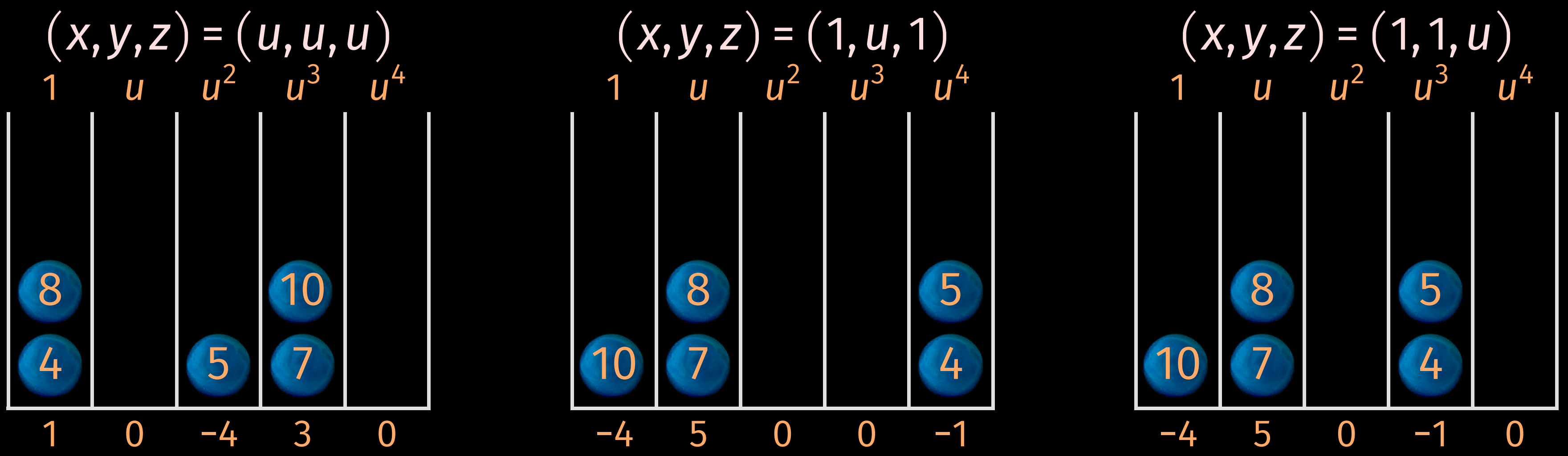
The game of mystery balls



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

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

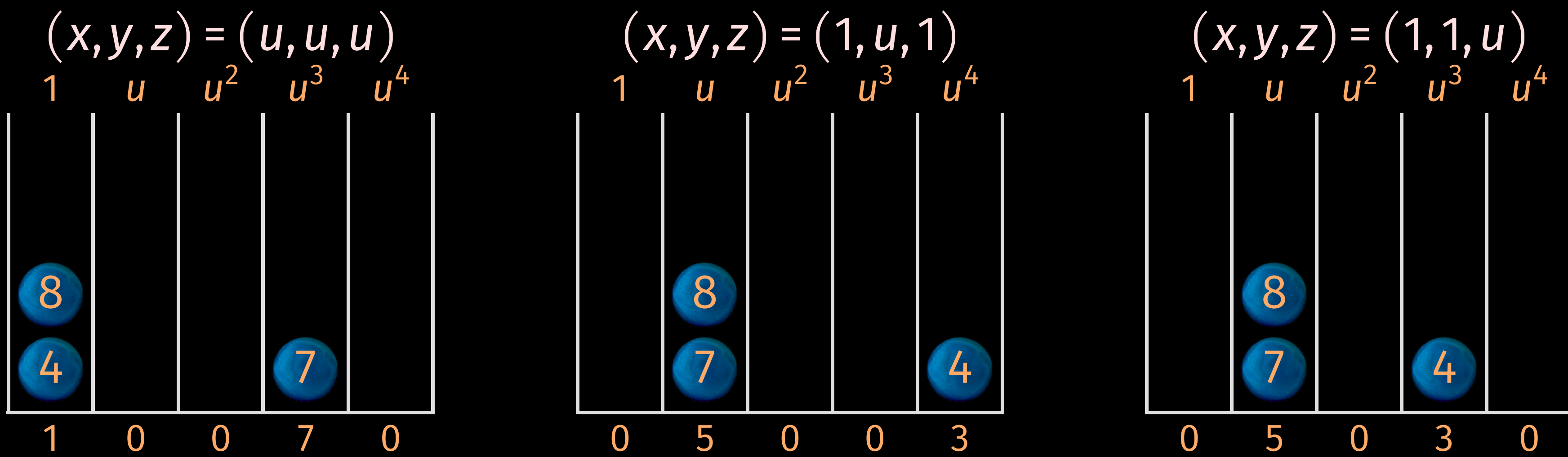
The game of mystery balls



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

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

The game of mystery balls

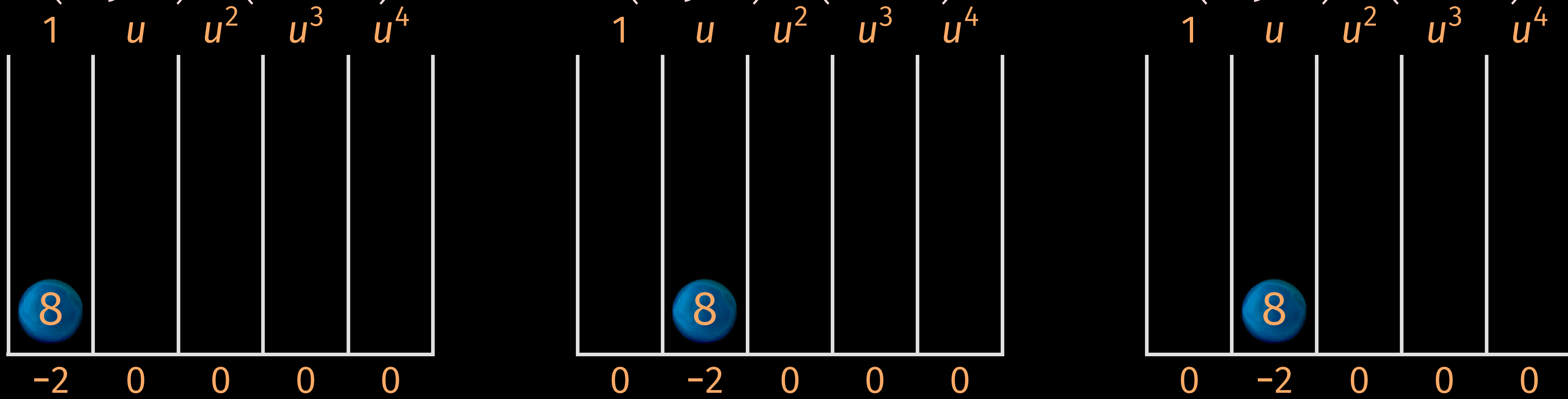


$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

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

The game of mystery balls

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

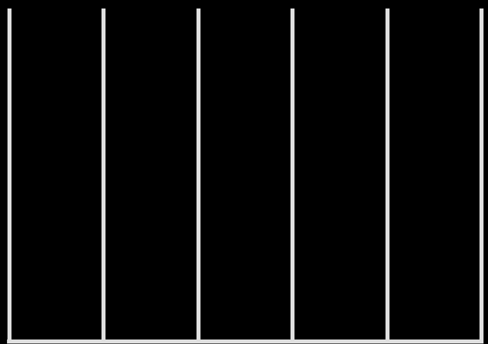


$$f = \overbrace{3x^{12}y^{18}z^{6}}^{1} + \overbrace{1x^{10}y^{15}z^{4}}^{2} + \overbrace{9x^{3}y^{10}z^{4}}^{3} + \overbrace{3x^{3}y^{9}z^{3}}^{4} + \overbrace{(-4)x^{10}y^{14}z^{3}}^{5} +$$

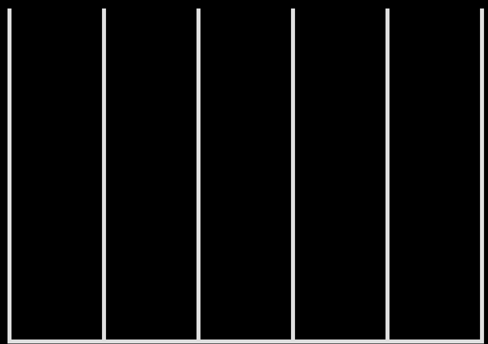
$$\overbrace{3xy^{7}z^{2}}^{6} + \overbrace{7xy^{6}z}^{7} + \overbrace{(-2)x^{8}y^{11}z}^{8} + \overbrace{2xy^{5}}^{9} + \overbrace{(-4)x^{8}y^{10}}^{10}$$

The game of mystery balls

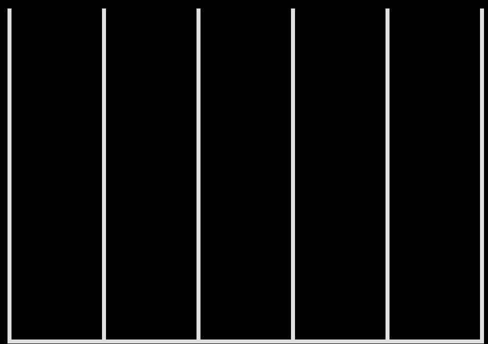
$(x,y,z)=(u,u,u)$



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



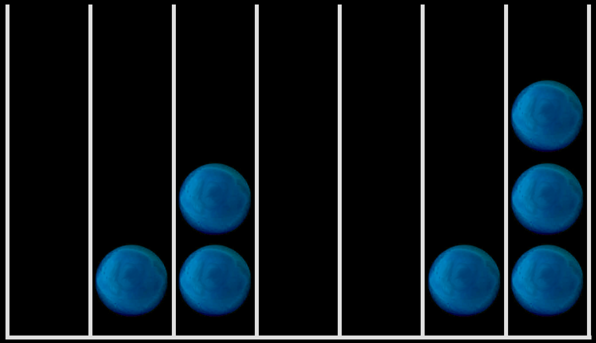
$(x,y,z)=(1,1,u)$



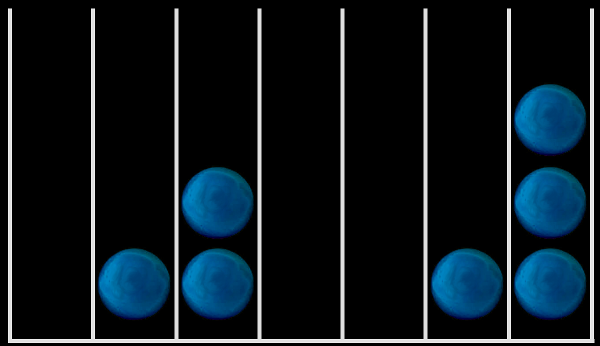
$$f = \overbrace{3x^{12}y^{18}z^6}^{1} + \overbrace{1x^{10}y^{15}z^4}^{2} + \overbrace{9x^3y^{10}z^4}^{3} + \overbrace{3x^3y^9z^3}^{4} + \overbrace{(-4)x^{10}y^{14}z^3}^{5} +$$

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

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

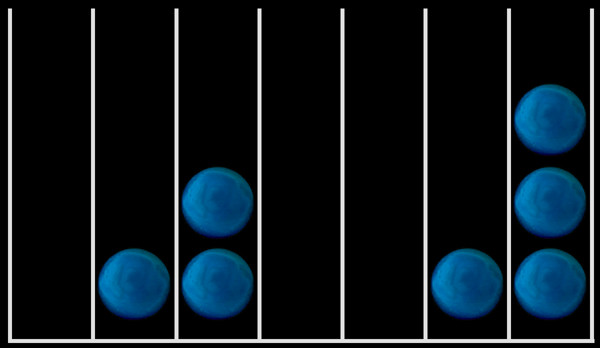


Throwing t balls in $r = \tau t$ drawers



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

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

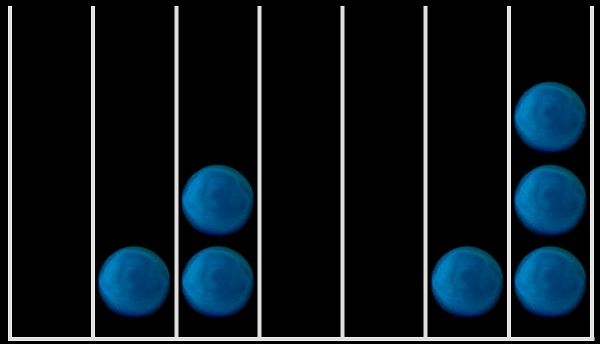


p_k : probability for a ball to end up in a drawer with k balls

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

Probabilistic analysis I

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

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?

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

Gain with respect to previous approach

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

How small can we take τ?

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

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

Gain with respect to previous approach

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

How small can we take τ?

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

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

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

Part VI

Implementation in Mathemagix

Vintage version

- Interpreted language + C++ libraries.

Vintage version

- Interpreted language + C++ libraries.

Version 1

- Compiler (with bugs) + C++ libraries.
- Mathemagix library for symbolic computation.

Vintage version

- Interpreted language + C++ libraries.

Version 1

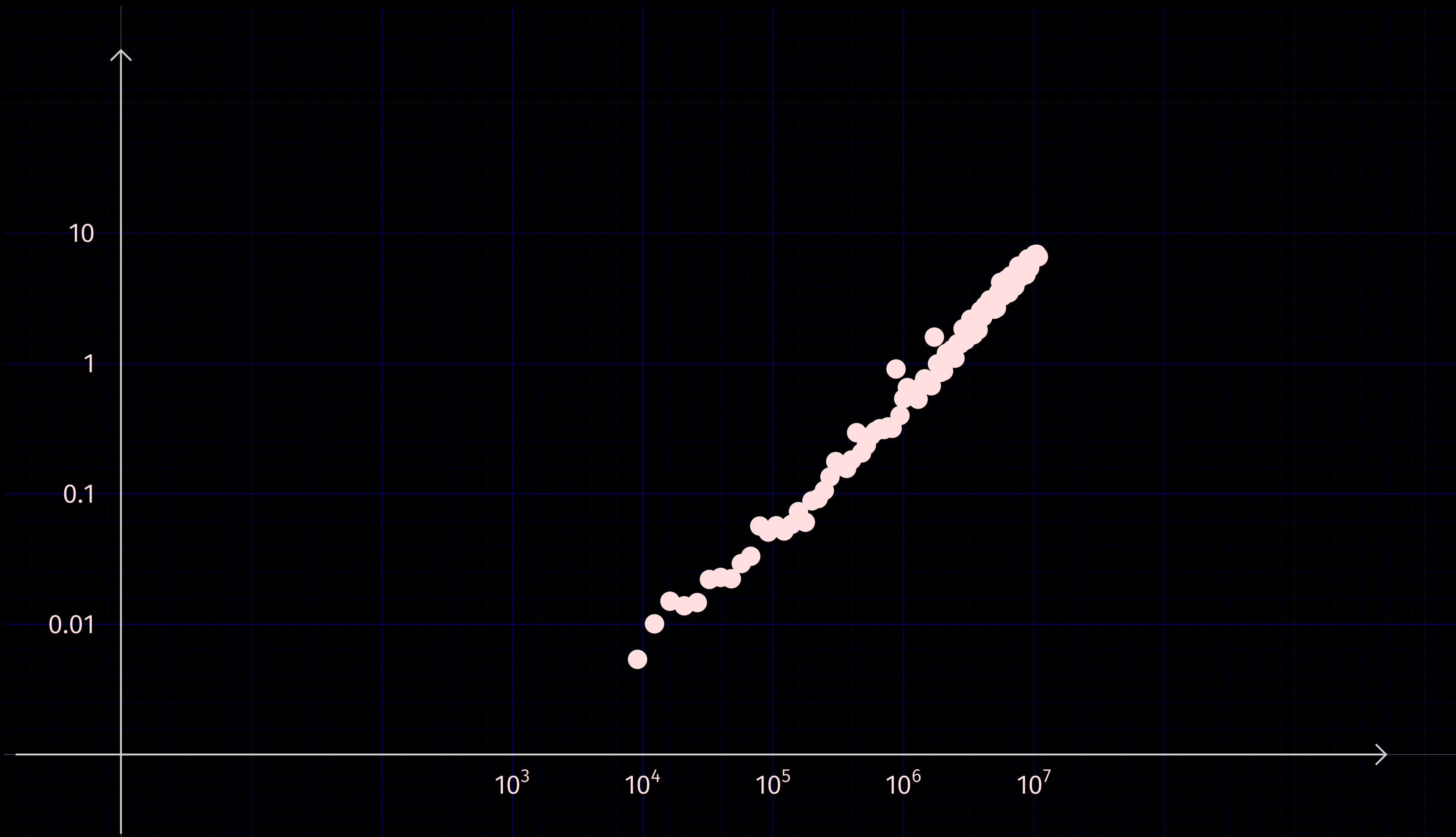
- Compiler (with bugs) + C++ libraries.
- Mathemagix library for symbolic computation.

Version 2

- Compiler (with less bugs) + C++ libraries.
- C++ libraries $\longrightarrow$ Mathemagix libraries (work in progress).

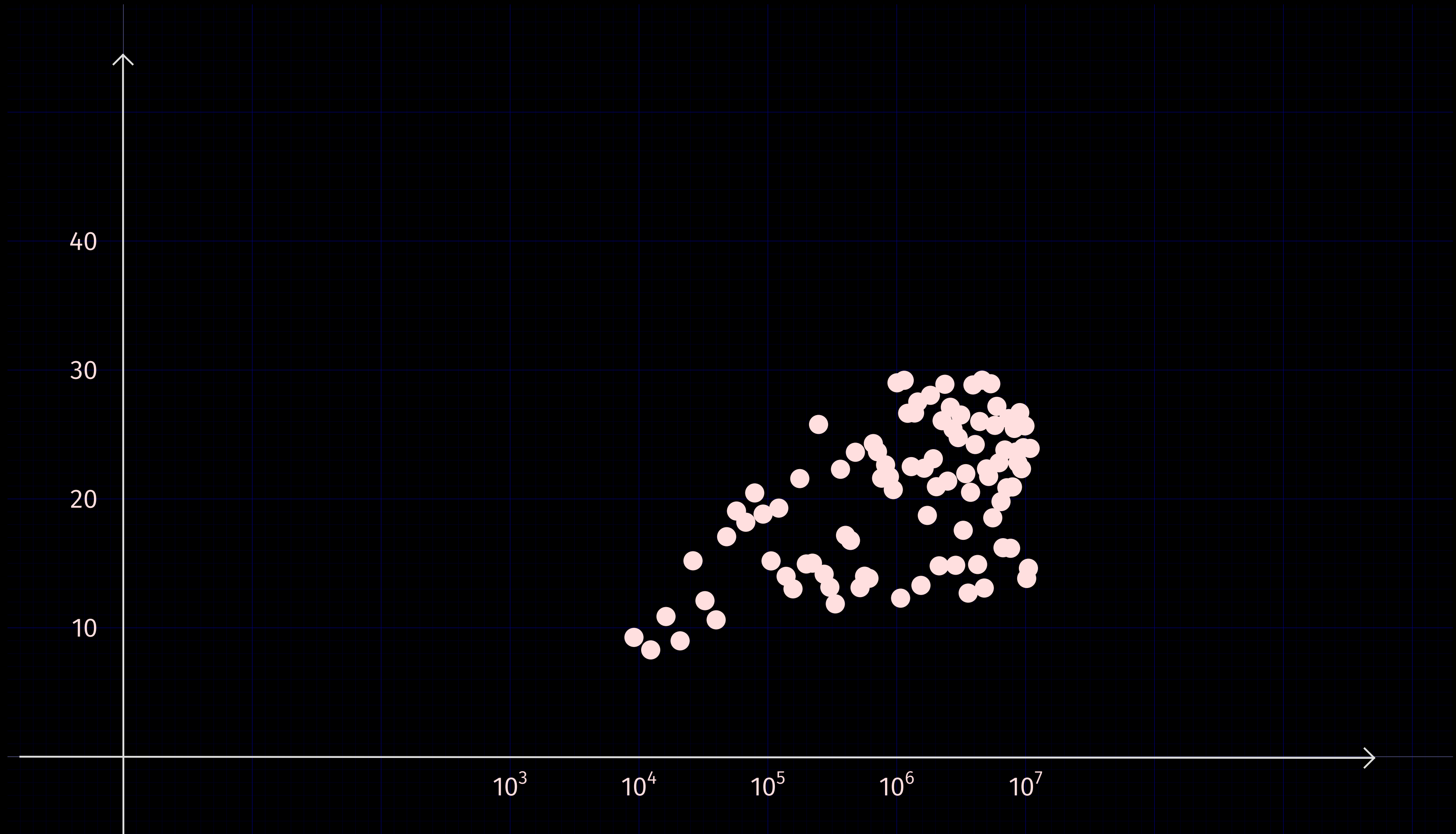
Timings sparse multiplication

$\mathbb{K} = \mathbb{F}_p$ where p is an FFT prime $> 2^{48}$. Time in seconds as a function of $t := t_f$.



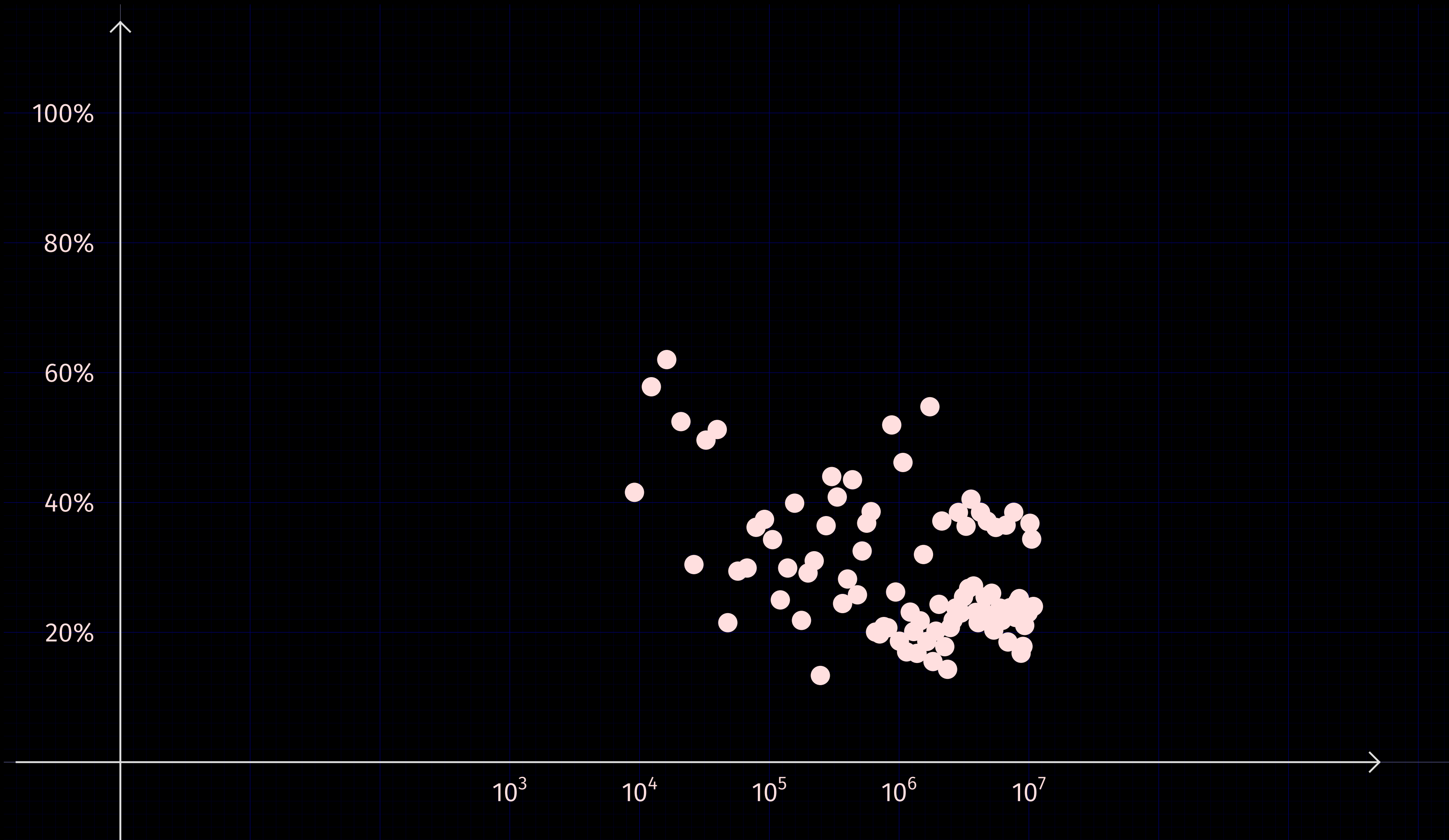
Sparse versus dense multiplication

Ratio with respect to dense multiplication with product of same size t.

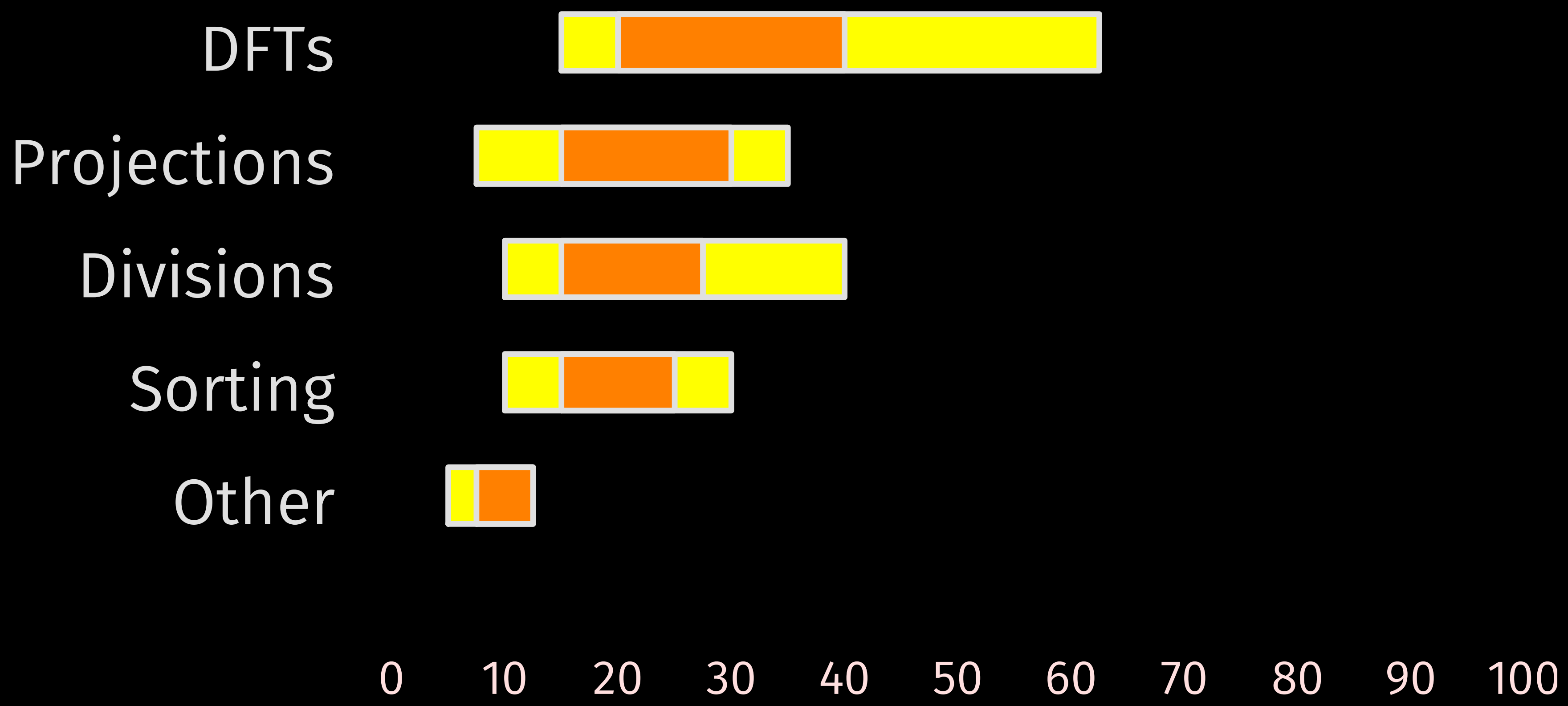


Percentage of time spent on DFTs

Percentage as a function of size t of the product.



How do we spend our time?



Thank you !

http://www.TeXmacs.org