Counting points on curves

Edgar Costa

Dartmouth College

Québec-Maine Number Theory conference, 8th October 2016

(joint work with David Harvey, UNSW)

Setup

$p =$ prime

$C \subset \mathbb{P}^n_{\mathbb{F}_p} =$ algebraic curve defined over $\mathbb{F}_p$

The Hasse–Weil zeta function of C is the generating function

$$Z_C(t) := exp\left(\sum_{a>0} \frac{\#C(\mathbb{F}_{p^a})t^a}{a}\right)$$

Example

Let $p = 5$ and C be genus 3 curve given in $\mathbb{P}^2$ by

$$x^4 + xy^3 + 2y^4 - z^4 = 0$$

Example

Let $p = 5$ and C be genus 3 curve given in $\mathbb{P}^2$ by

$$x^4 + xy^3 + 2y^4 - z^4 = 0$$

By naive point enumeration, we find that

$$\begin{aligned} \#C(\mathbb{F}_p) &= 9, & \#C(\mathbb{F}_{p^4}) &= 581, \\ \#C(\mathbb{F}_{p^2}) &= 29, & \#C(\mathbb{F}_{p^5}) &= 3309, \\ \#C(\mathbb{F}_{p^3}) &= 156, & &\dots \end{aligned}$$

Example

Let $p = 5$ and C be genus 3 curve given in $\mathbb{P}^2$ by

$$x^4 + xy^3 + 2y^4 - z^4 = 0$$

By naive point enumeration, we find that

$$\begin{aligned} \#C(\mathbb{F}_p) &= 9, & \#C(\mathbb{F}_{p^4}) &= 581, \\ \#C(\mathbb{F}_{p^2}) &= 29, & \#C(\mathbb{F}_{p^5}) &= 3309, \\ \#C(\mathbb{F}_{p^3}) &= 156, & &\dots \end{aligned}$$

thus:

$$Z_C(t) = 1 + 9t + 55t^2 + 304t^3 + 1579t^4 + 8029t^5 + 40404t^6 + \cdots$$

Example

Let $p = 5$ and C be genus 3 curve given in $\mathbb{P}^2$ by

$$x^4 + xy^3 + 2y^4 - z^4 = 0$$

By naive point enumeration, we find that

$$\begin{aligned} \#C(\mathbb{F}_p) &= 9, & \#C(\mathbb{F}_{p^4}) &= 581, \\ \#C(\mathbb{F}_{p^2}) &= 29, & \#C(\mathbb{F}_{p^5}) &= 3309, \\ \#C(\mathbb{F}_{p^3}) &= 156, & &\dots \end{aligned}$$

thus:

$$\begin{aligned} Z_C(t) &= 1 + 9t + 55t^2 + 304t^3 + 1579t^4 + 8029t^5 + 40404t^6 + \cdots \\ &= \frac{1 + 3t + 6t^2 + 19t^3 + 6 \cdot 5t^4 + 3 \cdot 5^2 t^5 + 1 \cdot 5^3 t^6}{(1-t)(1-5t)} \end{aligned}$$

Typical algorithms

Naively computing

$$\#C(\mathbb{F}_p), \#C(\mathbb{F}_{p^2}), \cdots, \#C(\mathbb{F}_{p^g})$$

is not practical!

Looping over $\mathbb{F}_{p^g}$ takes at least $O(p^g)$ time.

Typical algorithms

Naively computing

$$\#C(\mathbb{F}_p), \#C(\mathbb{F}_{p^2}), \cdots, \#C(\mathbb{F}_{p^g})$$

is not practical!

Looping over $\mathbb{F}_{p^g}$ takes at least $O(p^g)$ time.

One can them compute the last line with variety of methods.

- ℓ-adic cohomology
- p-adic cohomology

New method

Today I will overview a new elementary method to compute $L_C(t)$.

New method

Today I will overview a new elementary method to compute $L_C(t)$.

- Simple
- Practical
- Cohomology free!

New method - Input/Output

Input: $F(x, y, z)$ homogeneous polynomial of degree d

Output: $L_C(t)$, where C is the **desingularization** of the zero locus of $F(x, y, z)$ in $\mathbb{P}^2$

New method - Input/Output

Input: $F(x, y, z)$ homogeneous polynomial of degree d

Output: $L_C(t)$, where C is the **desingularization** of the zero locus of $F(x, y, z)$ in $\mathbb{P}^2$

Assumption: The polynomials $F(0, y, z)$, $F(x, 0, y)$ and $F(x, y, 0)$ have no repeated factors.

Geometrically, the curve given by F intersects the coordinate axes ($x = 0$, $y = 0$, and $z = 0$) transversally.

New method - Ingredients

C curve of genus g that is the desingularization of $\{F = 0\} \subset \mathbb{P}^2$

Goal: compute $\#C(\mathbb{F}_{p^a})$

New method - Ingredients

C curve of genus g that is the desingularization of $\{F = 0\} \subset \mathbb{P}^2$

Goal: compute $\#C(\mathbb{F}_{p^a})$

Approach:

- Compute $\#\{F(x, y, z) = 0 : (x, y, z) \in \mathbb{P}^2(\mathbb{F}_{p^a}),\ xyz \neq 0\}$
- Compute $\#\{F(x, y, z) = 0 : (x, y, z) \in \mathbb{P}^2(\mathbb{F}_{p^a}),\ xyz = 0\}$
- Resolve the singularities of $F(x, y, z) = 0$ (over $\overline{\mathbb{F}_p}$)

Altogether, we can deduce $\#C(\mathbb{F}_{p^a})$.

New method - Ingredients

C curve of genus g that is the desingularization of $\{F = 0\} \subset \mathbb{P}^2$

Goal: compute $\#C(\mathbb{F}_{p^a})$

Approach:

- $\Rightarrow$Compute $\#\{F(x, y, z) = 0 : (x, y, z) \in \mathbb{P}^2(\mathbb{F}_{p^a}),\ xyz \neq 0\}$
- Compute $\#\{F(x, y, z) = 0 : (x, y, z) \in \mathbb{P}^2(\mathbb{F}_{p^a}),\ xyz = 0\}$
- Resolve the singularities of $F(x, y, z) = 0$ (over $\overline{\mathbb{F}_p}$)

Altogether, we can deduce $\#C(\mathbb{F}_{p^a})$.

New method - Trace formula

Let $B_\ell = \{u \in \mathbb{N}^3 : \sum_i u_i = \ell\}$.

For $u \in B_{dn}$, let $(F^n)_u$ be the coefficient of $x^{u_0} y^{u_1} z^{u_2}$ in F^n.

$$(M_s)_{v,u} := \left(F^{s(p-1)}\right)_{pv-u} \quad \text{for } v, u \in B_{ds}.$$

New method - Trace formula

Let $B_\ell = \{u \in \mathbb{N}^3 : \sum_i u_i = \ell\}$.

For $u \in B_{dn}$, let $(F^n)_u$ be the coefficient of $x^{u_0} y^{u_1} z^{u_2}$ in F^n.

$$(M_s)_{v,u} := \left(F^{s(p-1)}\right)_{pv-u} \quad \text{for } v, u \in B_{ds}.$$

$$M_0, M_1, \ldots, M_\lambda \rightsquigarrow \#C(\mathbb{F}_{p^a}) \bmod p^\lambda \quad \forall_a$$

New method - Trace formula

Let $B_\ell = \{u \in \mathbb{N}^3 : \sum_i u_i = \ell\}$.

For $u \in B_{dn}$, let $(F^n)_u$ be the coefficient of $x^{u_0} y^{u_1} z^{u_2}$ in F^n.

$$(M_s)_{v,u} := \left(F^{s(p-1)}\right)_{pv-u} \quad \text{for } v, u \in B_{ds}.$$

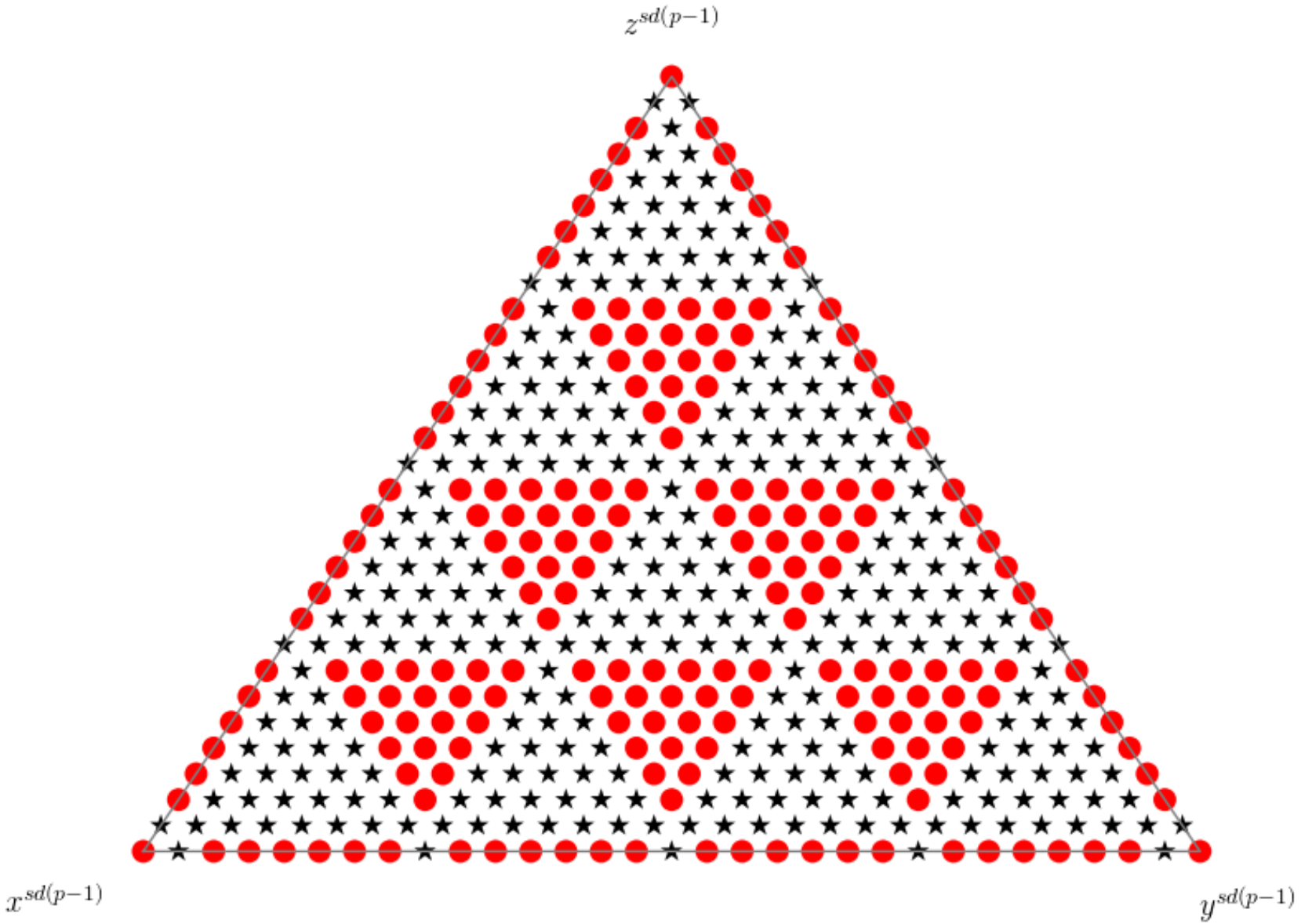
$$M_0, M_1, \ldots, M_\lambda \rightsquigarrow \#C(\mathbb{F}_{p^a}) \bmod p^\lambda \quad \forall_a$$

Harvey (2015)

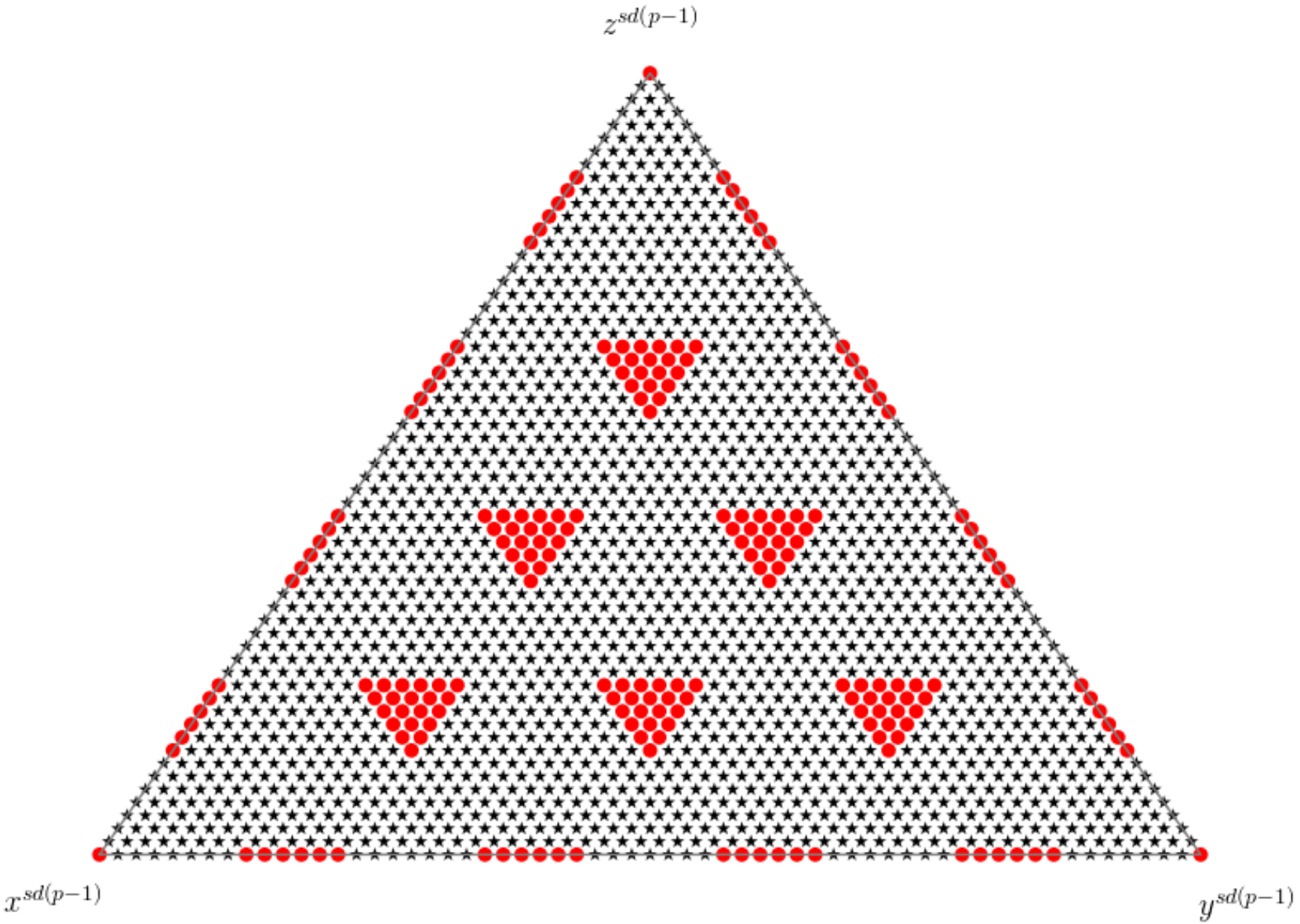
For p not small:

$$\#\{F(x,y,z) = 0 : (x,y,z) \in \mathbb{P}^2(\mathbb{F}_{p^a}),\ xyz \neq 0\}$$
$$= (p^a - 1)^2 \sum_{s=0}^{\lambda} \binom{\lambda}{s} \operatorname{Tr}(M_s^a) \bmod p^\lambda$$

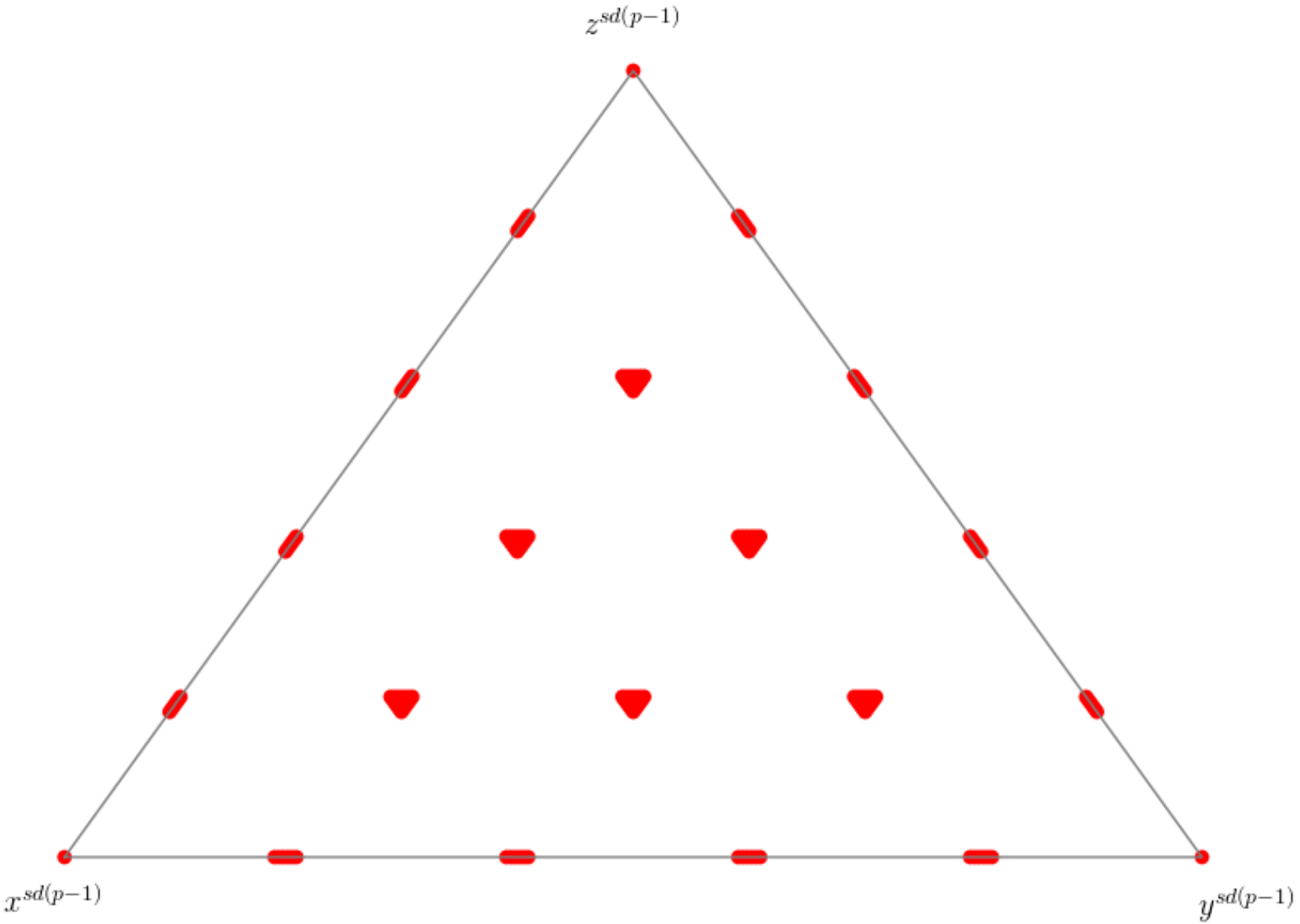
M_1 for $p = 7, d = 5$



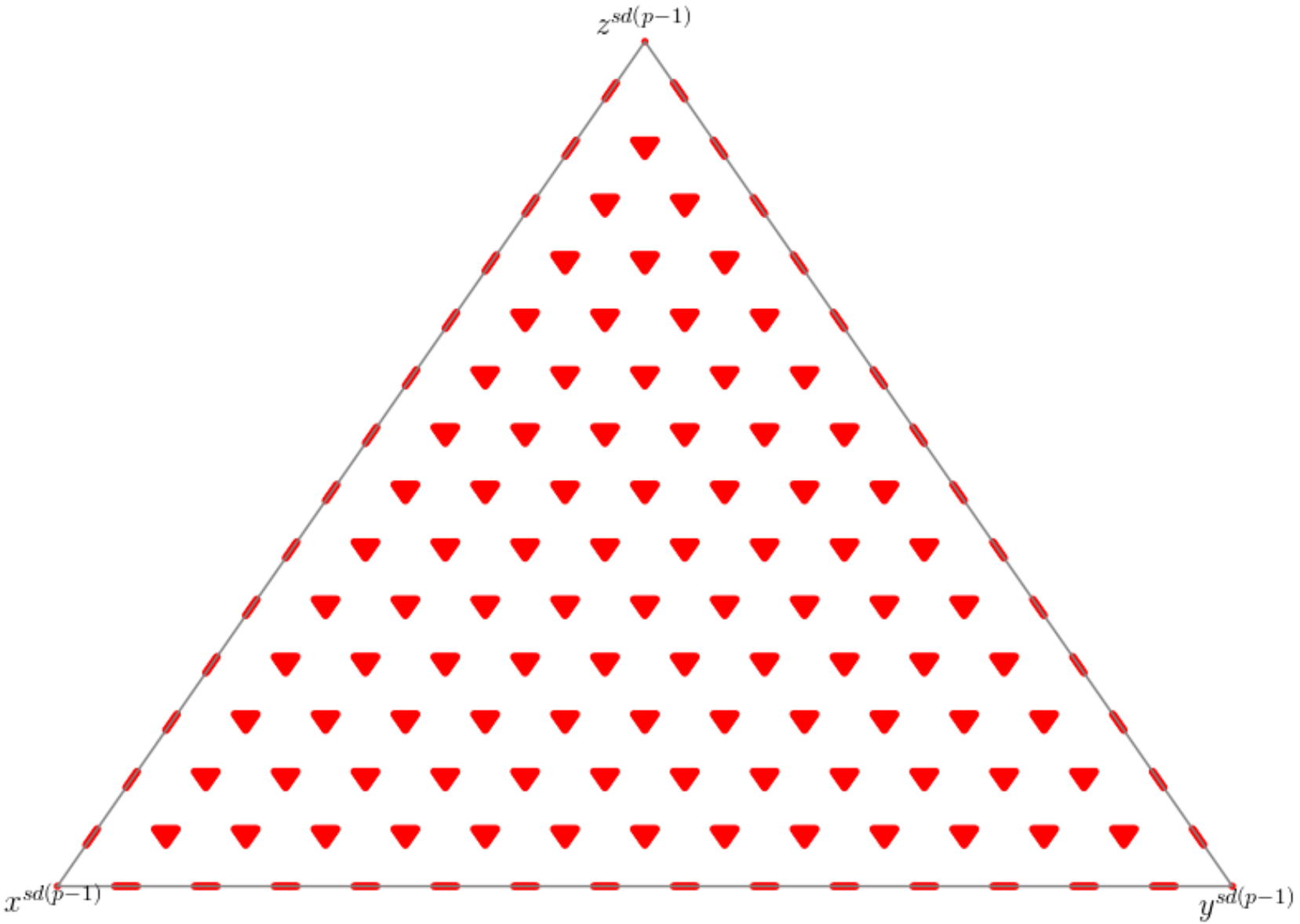
M_1 for $p = 13, d = 5$



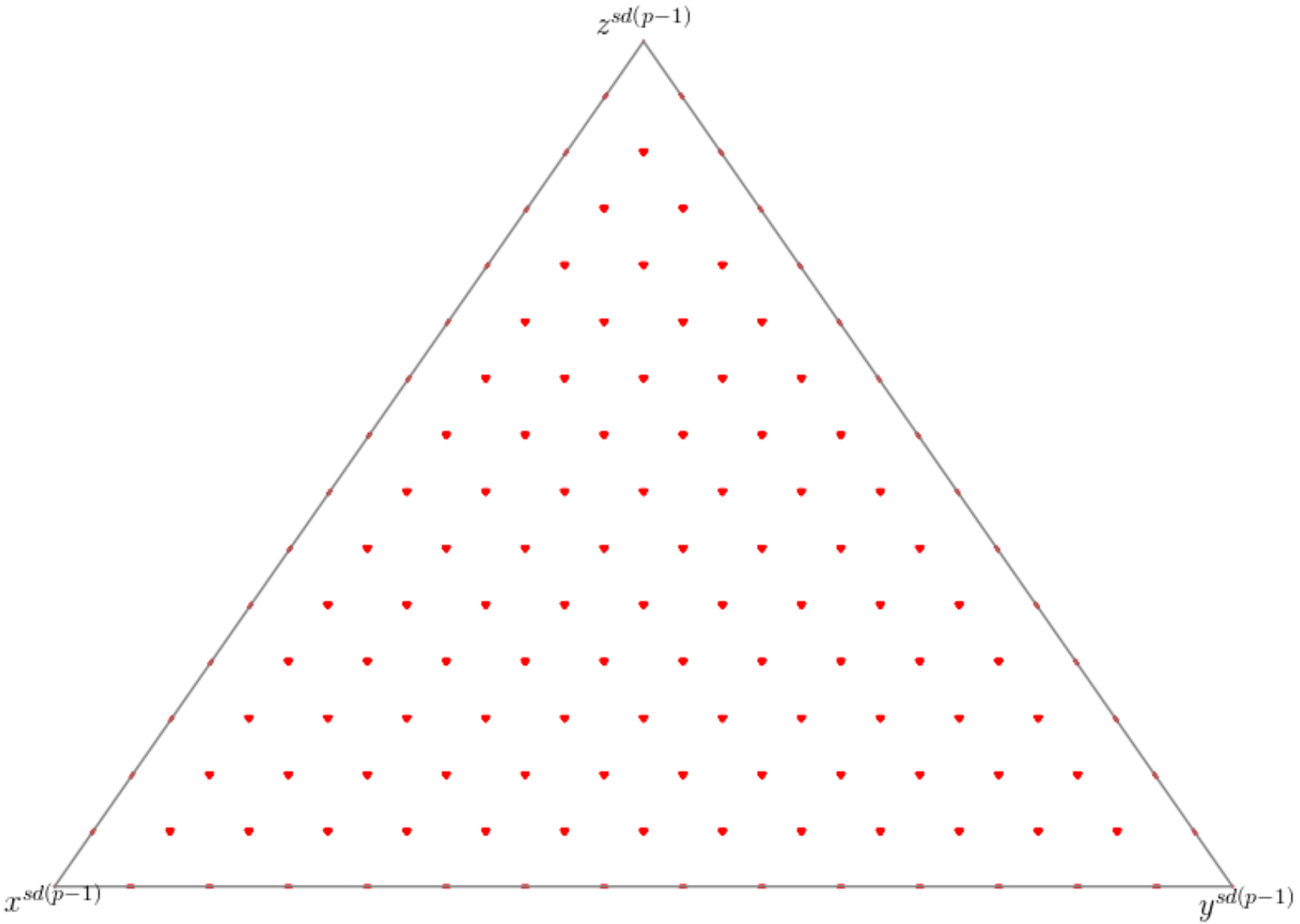
M_1 for $p = 53, d = 5$



M_3 for $p = 53, d = 5$



M_3 for $p = 199, d = 5$



New method - Key idea

There are relations between neighbouring coefficients of F^n.

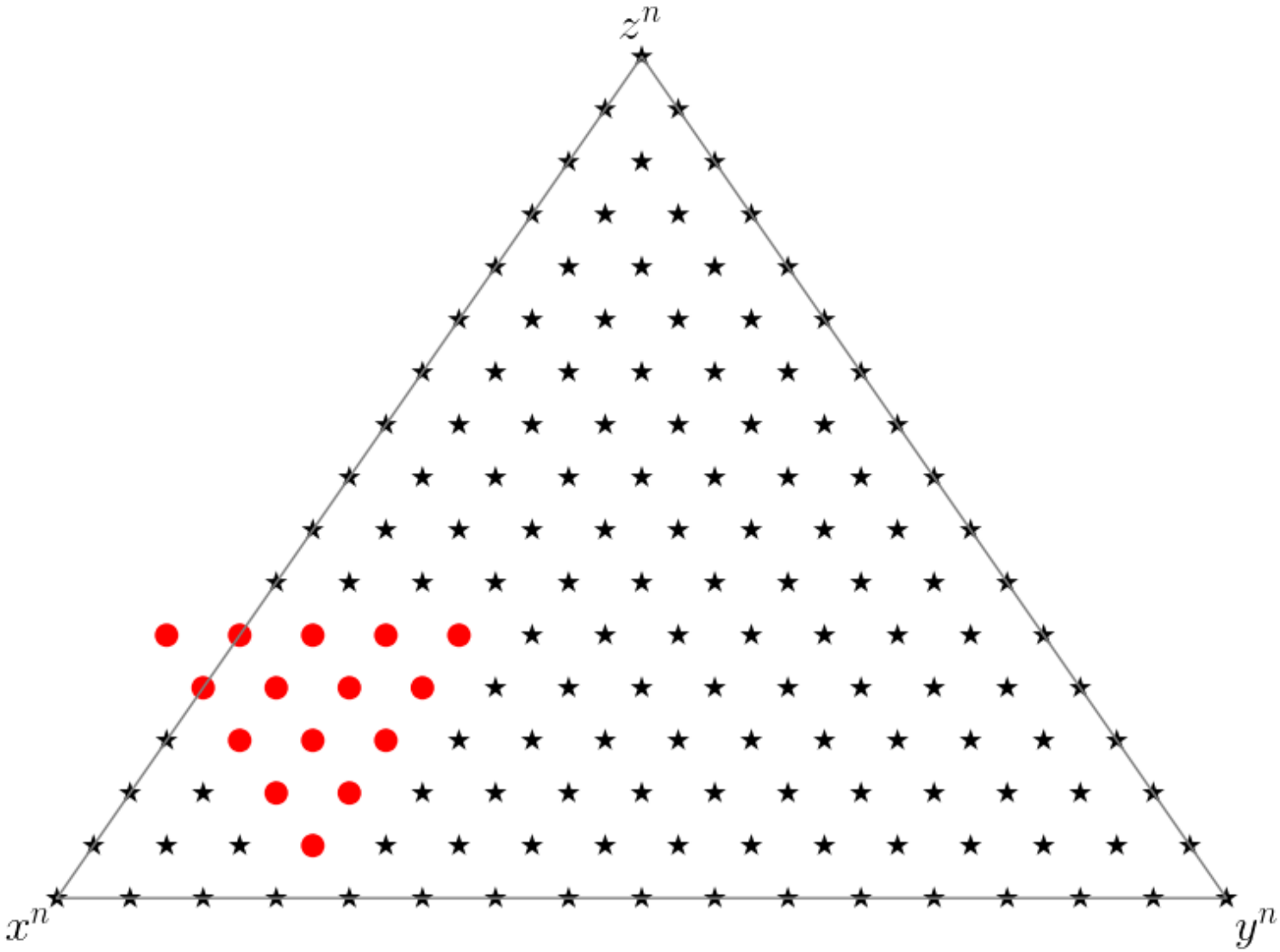
We can derive these relations from:

$$F^{n+1} = F \cdot F^n$$
$$\partial_x F^{n+1} = (n+1)\partial_x F \cdot F^n$$

or any other derivative.

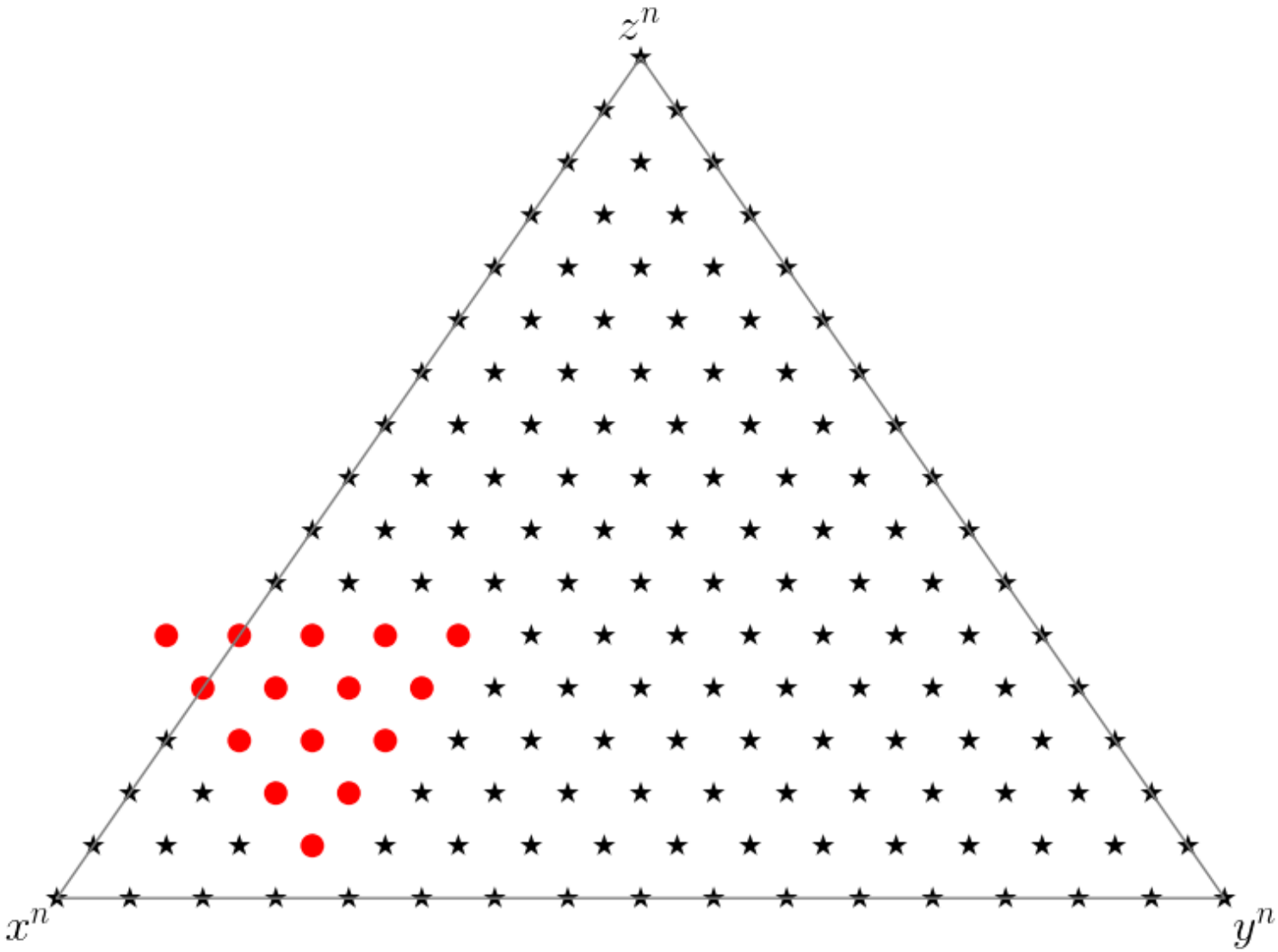
Example, $d = 4$ and $n = 4$

The coefficient $(F^{n+1})_{(12,3,5)}$ is known if given F^n on:



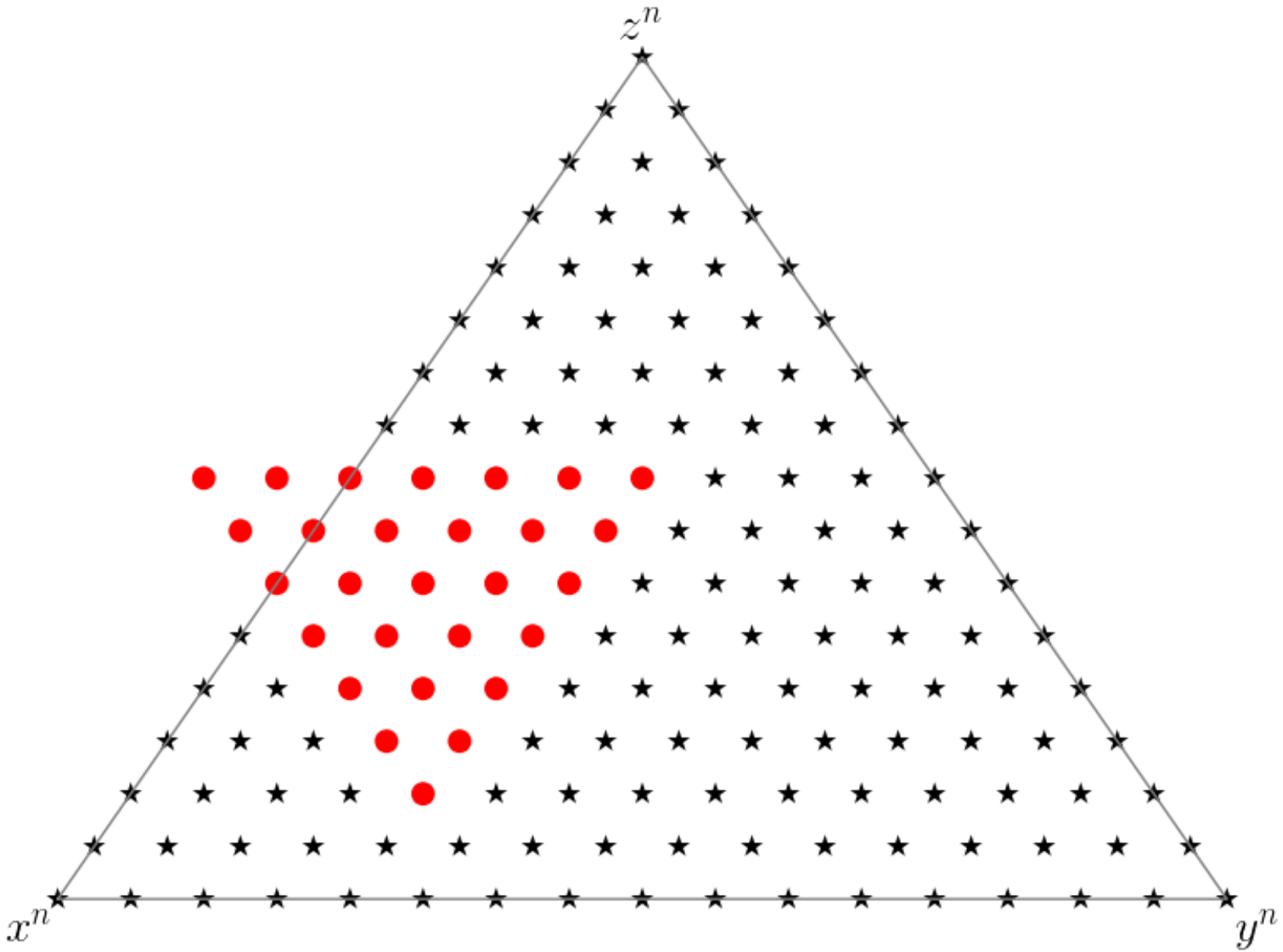
Example, $d = 4$ and $n = 4$

Indeed, there are 2 independent equations involving the red dots



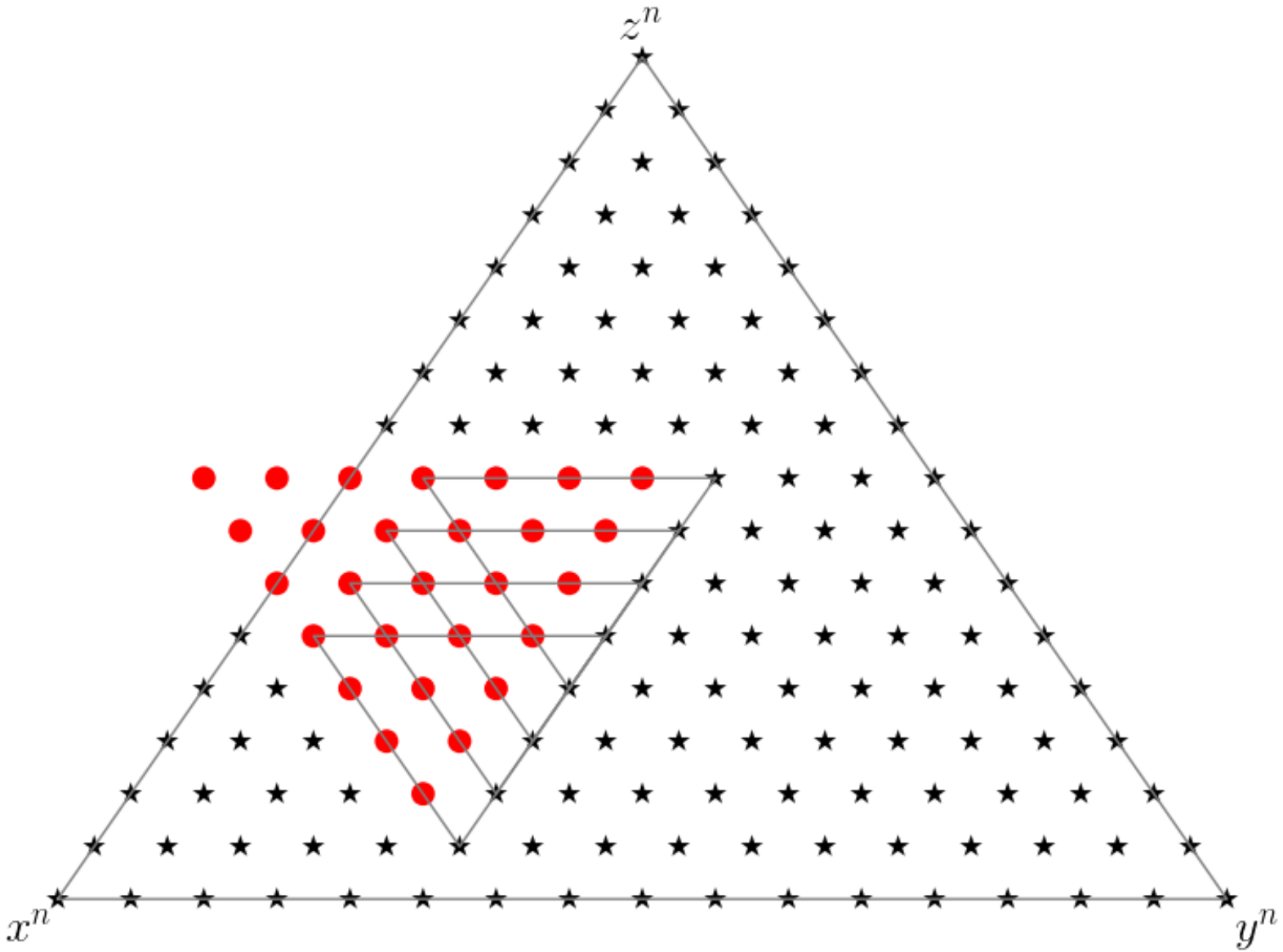
Example, $d = 4$ and $n = 4$

Combining enough relations we can move a larger triangle.



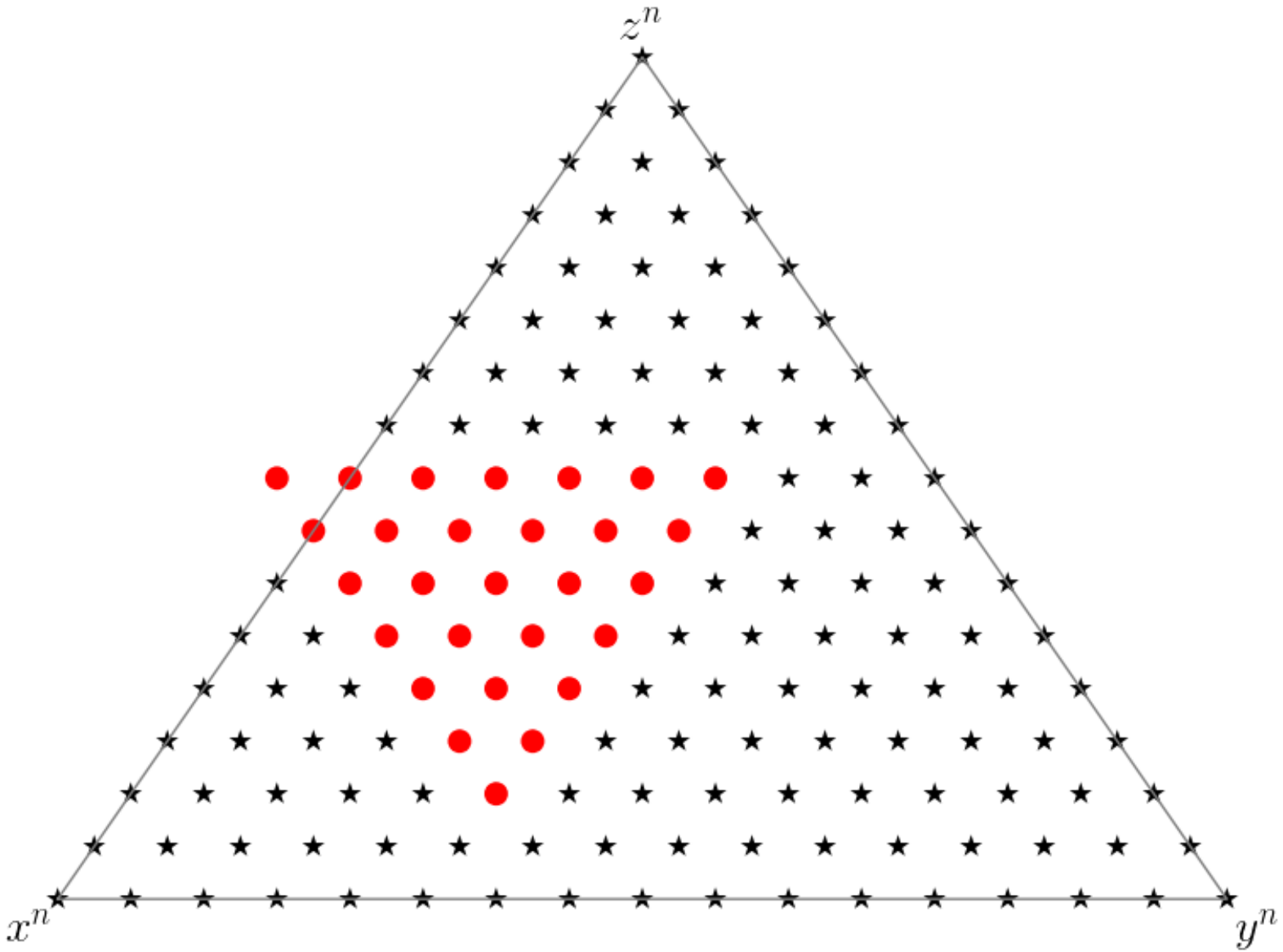
Example, $d = 4$ and $n = 4$

Combining enough relations we can move a larger triangle.



Example, $d = 4$ and $n = 4$

Combining enough relations we can move a larger triangle.

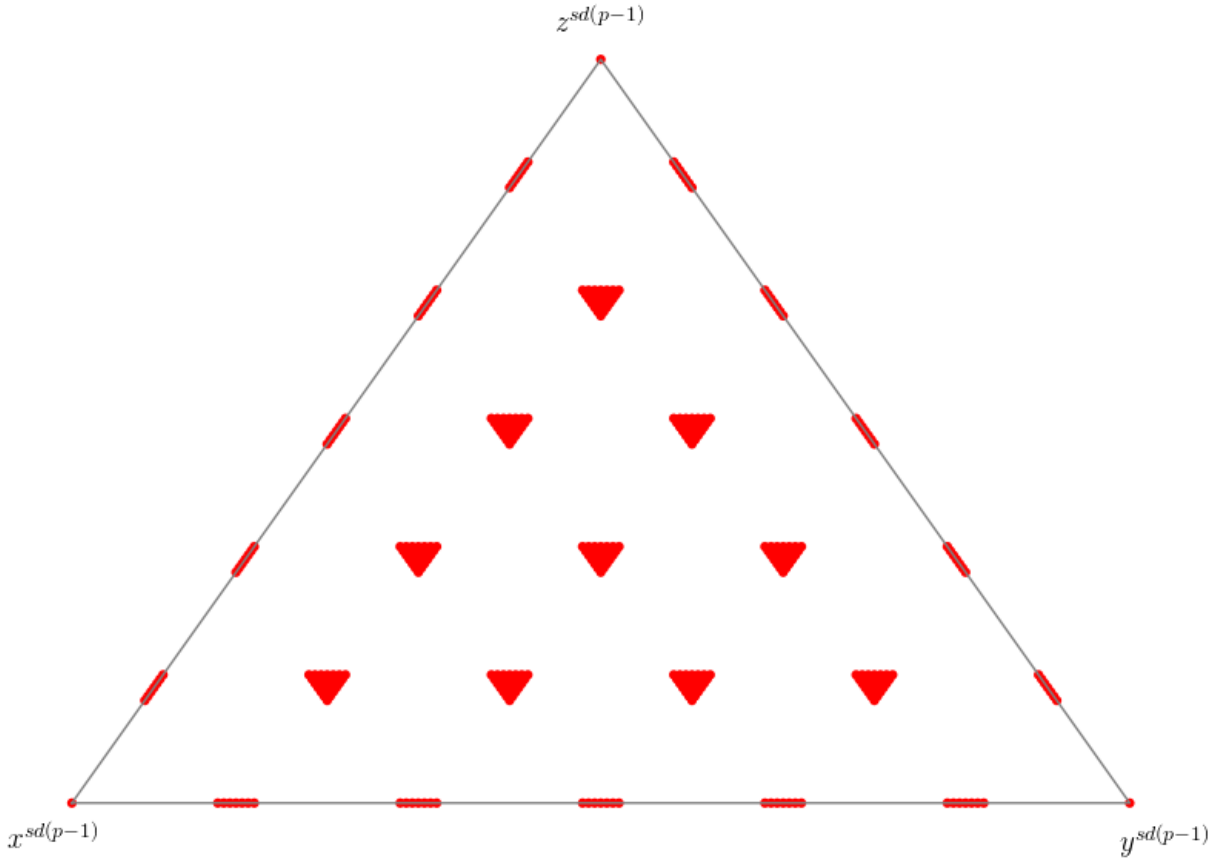


New method - Altogether

Start with a triangle at one of the vertices, where the coefficients of $F^{s(p-1)}$ are trivial to compute.

Move it around until we have computed by all the target coefficients.

Assemble M_s in $O(p)$ time



Toy implementation in sage

Setup: $d = 6$ and genus $= 5$

$p = 1009$: 7 minutes

$p = 1999$: 14 minutes

Toy implementation in sage

Setup: $d = 6$ and genus $= 5$

$p = 1009$: 7 minutes

$p = 1999$: 14 minutes

Tuitman's algorithm in Magma:

$p = 1009$: 8 minutes

$p = 1999$: 24 minutes

Disclaimer: this is **NOT** a fair comparison.

Future

Short term:

- Finish C++ implementation
- precision bounds

Long term, perhaps consider the two obvious improvements:

- reduce the running time to $p^{1/2+o(1)}$.
- average polynomial time

Future

Short term:

- Finish C++ implementation
- precision bounds

Long term, perhaps consider the two obvious improvements:

- reduce the running time to $p^{1/2+o(1)}$.
- average polynomial time

Thank you!