Building 3-Variable Homogeneous Integer-valued Polynomials Using Projective Planes

Marie-Andrée B.Langlois

Dalhousie University

March 2018

Homogeneous Polynomials

Definition

A 3-variable homogeneous polynomial of degree m is one of the form

$$f(x,y,z) = \sum_{i+j+k=m} c_{ijk} x^i y^j z^k.$$

For degree m they have the property that for a constant h :

$$f(hx,hy,hz) = h^m f(x,y,z).$$

Homogeneous Integer-Valued Polynomials

Definition

A polynomial $f(x, y, z) \in \mathbb{Q}[x, y, z]$ *is said to be integer-valued if* $f(a, b, c) \in \mathbb{Z}$ *for all* $(a, b, c) \in \mathbb{Z}^3$.

- This talk has for goal to construct homogeneous 3-variable IVPs, with denominators as large as possible.
- We work locally at $p = 2$, hence we want to have the largest k such that 2^k is the denominator of a HomIVP.
- **Goals :** (1) Produce HomIVPs, (2) such that they can be written as a product of linear factors.

Today's Plan

We will go over the following :

- Finite projective planes, especially the Fano plane.
- It is sufficient to evaluate at points on the projective planes.
- Use the Fano plane to build HomIVPs.
- What is known about 2-variable and 3-variable HomIVPs.
- Finite projective Hjelmslev-planes.
- Using H-planes to construct HomIVPs.

Projective Planes

Definition

A projective plane consists of a set of lines $\mathcal{L}$, a set of points $\mathcal{P}$, and a relationship between the lines and points called incidence $\mathcal{I}$, having the following properties :

I *Given any two distinct points, there is exactly one line incident to both of them.*

II *Given any two distinct lines there is exactly one point incident with both of them.*

III *There exists three non-collinear points.*

IV *Every line contains at least three points.*

Finite Projective Planes

Definition

The finite projective plane over $\mathbb{F}_p$ denoted $\mathbb{F}_p\mathbf{P}^2$, is defined as the set of triples $(x, y, z) \in \mathbb{F}_p^3 \backslash \{(0, 0, 0)\}$ with the equivalence relation $(x, y, z) \sim \lambda(x, y, z)$ for λ non-zero in $\mathbb{F}_p$.

Definition

A line $L = (a, b, c)$ in $\mathbb{F}_p\mathbf{P}^2$ is determined by a linear polynomial $ax + by + cz$, with at least one of a, b or c not divisible by p. Such that the points incident to it are

$$L_{(a,b,c)} = \{(x, y, z) \mid ax + by + cz \equiv 0 \pmod{p}\}.$$

Duality

Proposition

Given the incidence relation, the point $P = (x, y, z)$ and the line $L = (a, b, c)$ we also have that $P_1 = (a, b, c)$ is incident to $L_1 = (x, y, z)$. This is referred to as the duality of projective planes.

Number of Points/Lines

Proposition

The projective plane $\mathbb{F}_p\mathbf{P}^2$ has p^2+p+1 distinct points and p^2+p+1 distinct lines.

Proof :

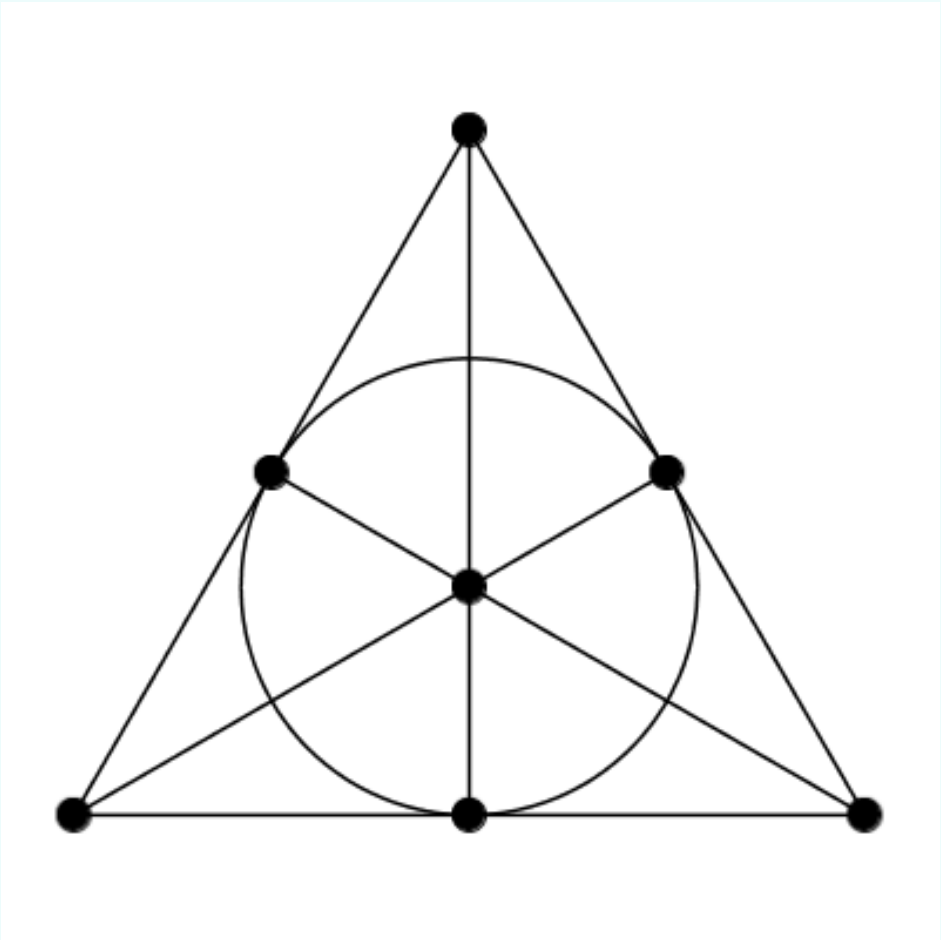
- The set $\mathbb{F}_p$ has p points. The set $(\mathbb{F}_p)^3\backslash(0,0,0)$ has p^3-1 points.

- Since there are $p-1$ units in $\mathbb{F}_p$ and we get an equivalence class for each of these, we have $\frac{p^3-1}{p-1} = p^2+p+1$ points.

The Fano Plane

- The smallest finite projective plane is $\mathbb{F}_2\mathbf{P}^2$ and is called the Fano plane.
- It has $2^2 + 2 + 1 = 7$ points and lines.
- The triples representing these are $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, $(1, 1, 0)$, $(1, 0, 1)$, $(0, 1, 1)$ and $(1, 1, 1)$.

The Fano Plane



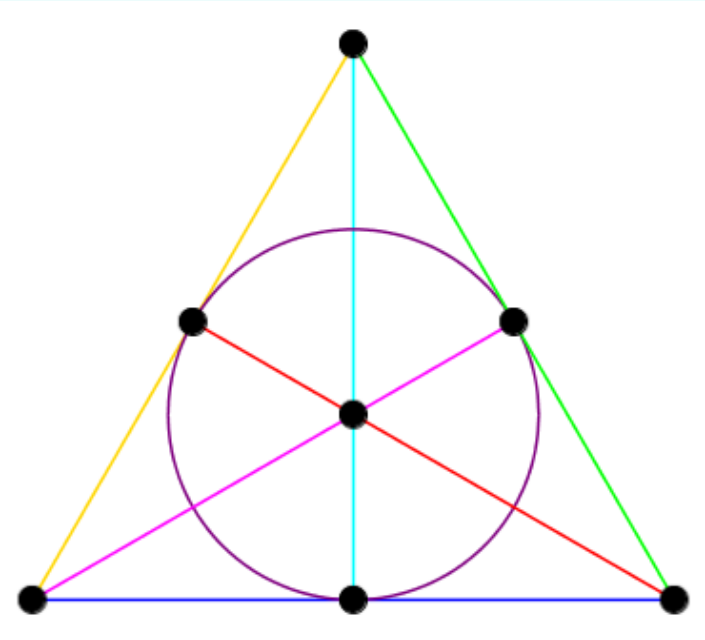
Number of lines

Proposition

(i) *Each point in* $\mathbb{F}_p\mathbf{P}^2$ *is incident to* $p+1$ *lines.*

(ii) *Each line in* $\mathbb{F}_p\mathbf{P}^2$ *is incident to* $p+1$ *points.*

Each point on the Fano plane is on 3 lines.



Coverings of Projective Planes

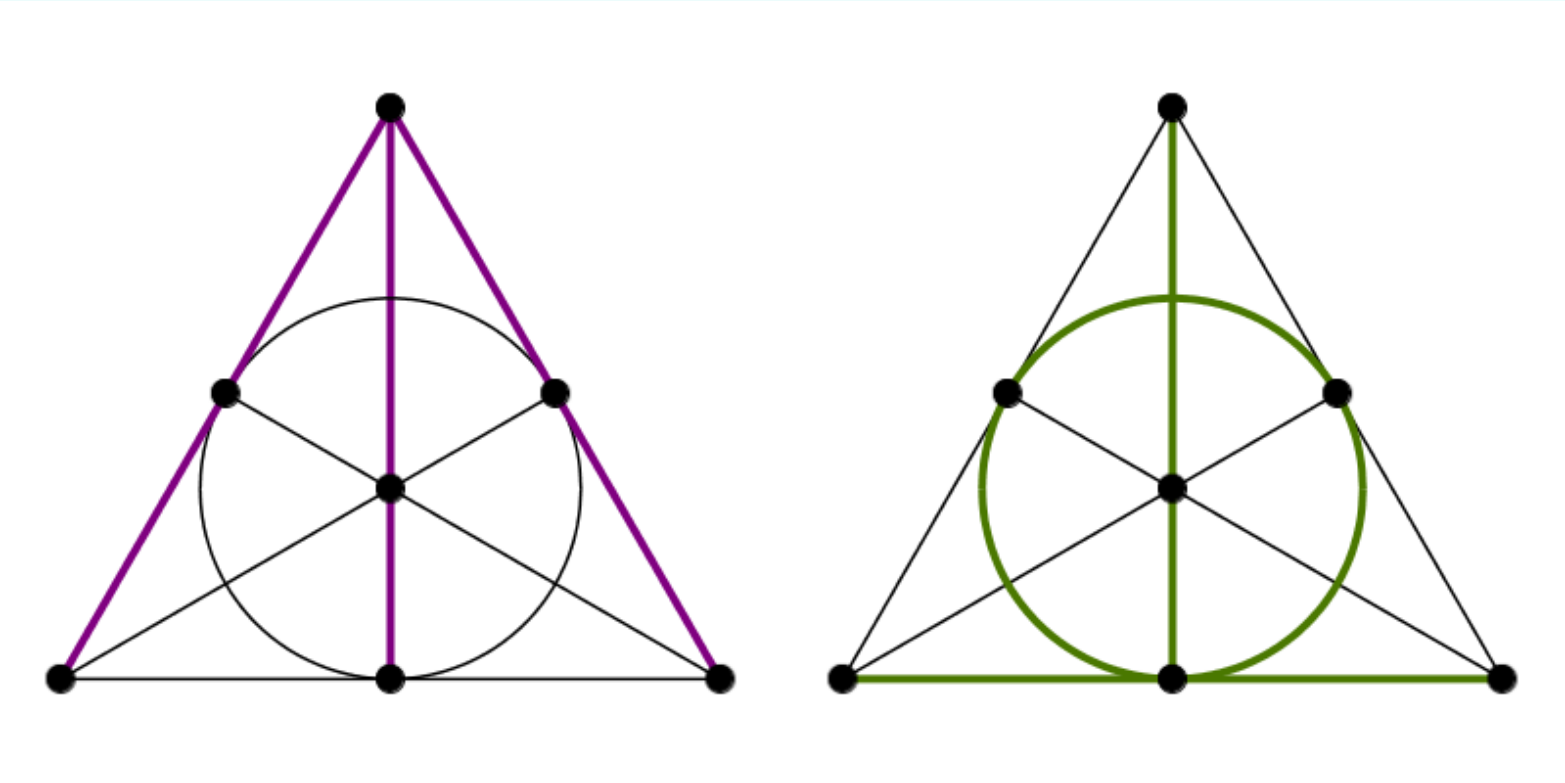
Proposition

When picking all $p+1$ lines that are incident to a point over $\mathbb{F}_p\mathbf{P}^2$, these lines will cover all of $\mathbb{F}_p\mathbf{P}^2$.

When taking all three lines that go through any point of the Fano plane, we will cover all seven points.

Note that this is not possible when taking fewer lines.

Coverings of the Fano Plane



Why is it Sufficient to Consider Points over $\mathbb{F}_p\mathbf{P}^2$?

When wanting to check if $\frac{f(x,y,z)}{p}$, a polynomial of degree m, is a HomIVP, one needs to evaluate $f(i,j,k)$ at $0 \leq i,j,k, \leq p-1$ and verify that $\frac{f(i,j,k)}{p} \in \mathbb{Z}$.

It is actually sufficient to evaluate f at the points of $\mathbb{F}_p\mathbf{P}^2$.

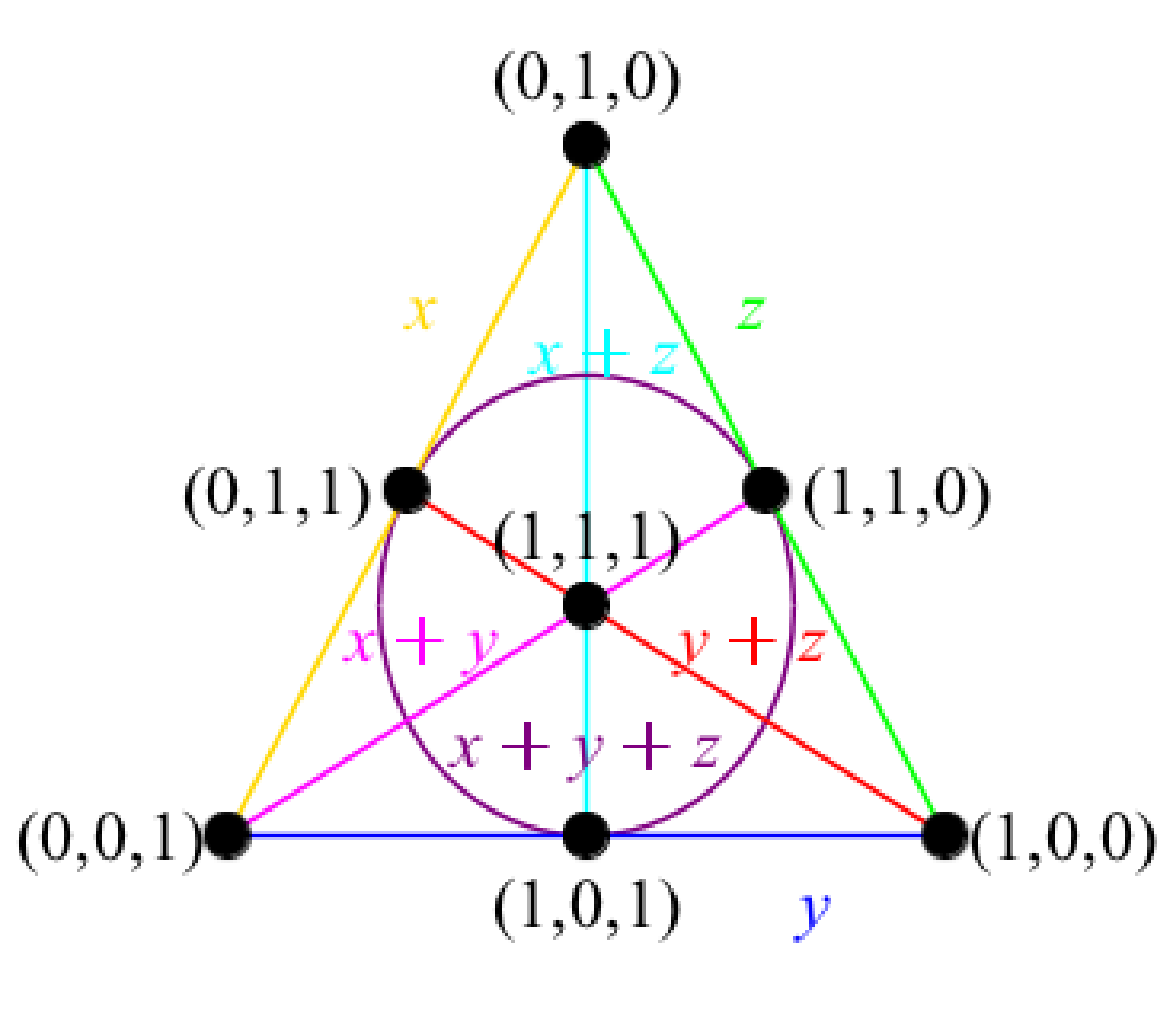
- $f(0,0,0) = 0$ since f is homogeneous.
- We don't need to test at $(0,0,0)$.

Why is it Sufficient to Consider Points over $\mathbb{F}_p\mathbf{P}^2$

- For $\lambda \neq 0 \in \mathbb{F}_p$, if $(x', y', z') = (\lambda x, \lambda y, \lambda z)$, then $f(x', y', z') = \lambda^m f(x, y, z)$.
- Hence if $p|f(x, y, z)$, then $p|f(x', y', z')$.
- It is sufficient to test at one representative per equivalence class.

To verify that $\frac{f(x,y,z)}{2}$ is an IVP we need to test at all points of the Fano plane.

Coordinates and Linear Factors



Using this to build an IVP

- Given $L = (a, b, c)$ a line in the Fano plane, the point $P = (x, y, z)$ is incident to L if

$$ax + by + cz \equiv 0 \pmod 2.$$

- If we take $L = (1, 0, 0)$, that is the line represented by the linear factor x.

- The points incident to L are $(0, 1, 0)$, $(0, 1, 1)$, $(0, 0, 1)$.

- Thus $\frac{x}{2}$ evaluates to an integer at these three points.

Using this to build an IVP

- We need $\frac{f(x,y,z)}{2}$ to be an integer at all seven points of the Fano plane to have an IVP.
- How many lines do we need to take ?
- 3, we need to take all three lines that are incident to a Point.
- Take $P = (0, 1, 0)$, the three lines incident to it are x, $x + z$ and z.
- Thus $\frac{x(x+z)z}{2}$ is an HomIVP.
- What about obtaining $\frac{f(x,y,z)}{2^k}$ as a HomIVP ?

How Big of Denominators Can We Get

The table below displays the largest k such that 2^k is in the denominator of a HomIVP.

Degree	2-variables	3-variables
1	0	0
2	0	0
3	1	1
4	1	1
5	1	1
6	3	3
7	3	3
8	3	4
9	4	4
10	4	5
11	4	5
12	7	7
13	7	7
14	7	9

Projective Hjelmslev-Planes

Definition

The projective H-plane over $\mathbb{Z}/(p^k)$: $\mathbb{Z}/(p^k)\mathbf{P}^2$ is the set of triples from $\mathbb{Z}/(p^k)^3$, such that p does not divide all values in the triple, with the equivalence relation $(x, y, z) \sim (\lambda x, \lambda y, \lambda z)$ for all units λ in $\mathbb{Z}/(p^k)$.

I Given any two distinct points, there is ~~exactly~~ one line incident to both of them.

II Given any two distinct lines there is ~~exactly~~ one point incident with both of them.

III There exists three non-collinear points.

IV Every line contains at least three points.

Incidence

Definition

A line $L = (a, b, c)$ in $\mathbb{Z}/(p^k)\mathbf{P}^2$ is determined by a linear polynomial $ax + by + cz$, with at least one of a, b or c not divisible by p. Such that the points incident to it are

$$L_{(a,b,c)} = \{(x, y, z) \mid ax + by + cz \equiv 0 \pmod{p^k}\}.$$

The Duality still holds over $\mathbb{Z}/(p^k)\mathbf{P}^2$.

Lemma

The projective plane $\mathbb{Z}/(p^k)\mathbf{P}^2$ has
$\frac{p^{3k} - (p^{k-1})^3}{p^k - p^{k-1}} = p^{2(k-1)}(p^2 + p + 1)$ *points/lines.*

Number of Points on a Line

Proposition

Each line in $\mathbb{Z}/(2^k)\mathbf{P}^2$ is incident to $2^{k+1} - 2^{k-1}$ points.

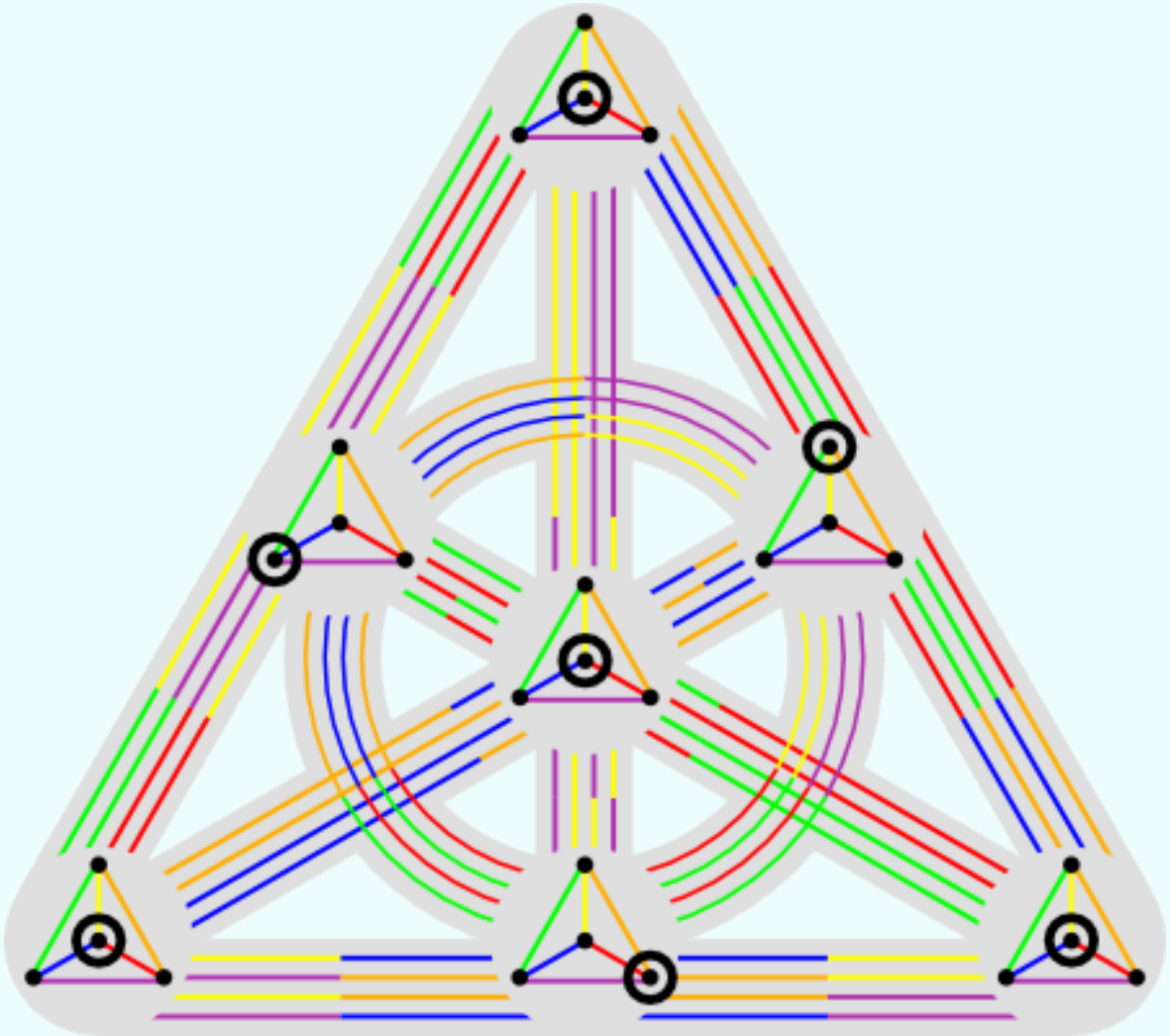
We will work mainly over $\mathbb{Z}/(4)\mathbf{P}^2$:

- $\mathbb{Z}/(2^2)\mathbf{P}^2$ has $\frac{2^6-2^3}{2^2-2} = \frac{64-8}{2} = 28$ points/lines.
- These reduce in fours to the Fano plane.
- Each line has $2^3 - 2^1 = 6$ points on it.

Points Congruent over the Fano Plane

$(0,0,1)$	$(0,2,1)$	$(2,0,1)$	$(2,2,1)$
$(0,1,0)$	$(0,1,2)$	$(2,1,0)$	$(2,1,2)$
$(0,1,1)$	$(0,1,3)$	$(2,1,1)$	$(2,1,3)$
$(1,0,0)$	$(1,0,2)$	$(1,2,0)$	$(1,2,2)$
$(1,0,1)$	$(1,0,3)$	$(1,2,1)$	$(1,2,3)$
$(1,1,0)$	$(1,1,2)$	$(1,3,0)$	$(1,3,2)$
$(1,1,1)$	$(1,1,3)$	$(1,3,1)$	$(1,3,3)$

$\mathbb{Z}/(4)\mathbf{P}^2$



Why is it Sufficient to Consider Points over $\mathbb{Z}/(2^k)\mathbf{P}^2$?

When building a polynomial of degree m through coverings of $\mathbb{Z}/(2^k)\mathbf{P}^2$, it is sufficient to verify that $\frac{f(x,y,z)}{2^h}$ is integer valued at the points of $\mathbb{Z}/(2^k)\mathbf{P}^2$:

- $f(2x', 2y', 2z') = 2^m f(x', y', z')$ since f is homogeneous, triples were all values are even are trivial.
- For $\lambda \in \mathbb{Z}/(2^k)^*$, if $(x', y', z') = (\lambda x, \lambda y, \lambda z)$, then $f(x', y', z') = \lambda^m f(x, y, z)$.
- Hence if $2^\ell | f(x, y, z)$, then $2^\ell | f(x', y', z')$. It is sufficient to test at one representative per equivalence class.

Using Coverings of $\mathbb{Z}/(2^k)\mathbf{P}^2$ to Build HomIVPs

Proposition

When picking six lines that intersect in the same point over $\mathbb{Z}/(4)\mathbf{P}^2$, one can build the homogeneous IVP $\frac{f(x,y,z)}{2^3}$, where 2^3 is the greatest possible denominator.

This won't be that helpful since for degree 6, we can obtain a HomIVP with a 2^3 in its denominator using only two variables.

We will use a different approach.

Using Coverings of $\mathbb{Z}/(2^k)\mathbf{P}^2$ to Build HomIVPs

Instead try seven lines, and pick them such that they reduce (mod 2) to the Fano plane.

Problem : Over $\mathbb{Z}/(4)\mathbf{P}^2$ we cannot find seven lines that reduce to the Fano plane and cover all of $\mathbb{Z}/(4)\mathbf{P}^2$.

The best one can do is to cover 27 points.

From these linear factors we can get a HomIVPs $\frac{f(x,y,z)}{2^3}$, since when reducing (mod 2) each point will be on three lines.

A Degree 8 HomIVP

L	Points in $\mathbb{Z}/(4)\mathbf{P}^2$ on L
x	(0,0,1), (0,2,1), (0,1,0), (0,1,2), (0,1,1), (0,1,3)
y	(0,0,1), (2,0,1), (1,0,0), (1,0,2), (1,0,1), (1,0,3)
z	(0,1,0), (2,1,0), (1,0,0), (1,2,0), (1,1,0), (3,1,0)
$y+z$	(0,1,3), (2,1,3), (1,0,0), (1,2,2), (1,1,3), (1,3,1)
$x+z$	(0,1,0), (2,1,2), (1,0,3), (1,2,3), (1,1,3), (1,3,3)
$x+y$	(0,0,1), (2,2,1), (3,1,0), (3,1,2), (1,3,1), (1,3,3)
$x+y+z$	(0,1,3), (2,1,1), (1,0,3), (1,2,1), (1,1,2), (3,1,0)

The point $(1,1,1)$ is not on any of the above lines.

We need to find a linear factor that evaluates to an even value at $(1,1,1)$, $x+y$ works, there are 11 others.

A Degree 8 HomIVP

$$\frac{x \cdot y \cdot z \cdot (y+z) \cdot (x+z) \cdot (x+y) \cdot (x+y+z)}{2^3} \cdot \frac{(x+y)}{2}$$

Is a HomIVP of degree 8, and such denominator was not possible using only two variables.

A Degree 14 HomIVP

Proposition

When taking 14 linear factors that correspond to 14 lines over $\mathbb{Z}/(4)\mathbf{P}^2$*, such that they reduce to twice the Fano plane, we obtain* $\frac{f(x,y,z)}{2^8}$.

An example of this polynomial is :

$$(0,1,5),\ (1,1,4),\ (1,1,1),\ (0,1,3),\ (1,4,3),\ (1,0,6),\ (1,1,3),$$
$$(2,0,3),\ (2,1,0),\ (1,6,0),\ (2,6,1),\ (2,1,2),\ (1,2,3),\ (1,3,2).$$

A Degree 28 HomIVP

Proposition

When taking 28 lines from $\mathbb{Z}/(8)\mathbf{P}^2$ that cover all 112 points of $\mathbb{Z}/(8)\mathbf{P}^2$, one can build homogeneous IVPs with a 2^{19} in their denominators.

An example of this polynomial is :

$$(0,0,1),\ (4,1,0),\ (0,1,5),\ (1,0,1),\ (1,1,4),\ (1,0,4),\ (1,1,1),$$
$$(0,2,1),\ (0,1,2),\ (0,1,3),\ (1,4,3),\ (1,1,2),\ (1,0,6),\ (1,1,3),$$
$$(2,0,3),\ (2,1,0),\ (2,3,3),\ (1,6,0),\ (1,6,1),\ (1,3,0),\ (1,3,5),$$
$$(2,6,1),\ (2,1,2),\ (2,1,7),\ (1,2,6),\ (1,2,3),\ (1,3,2),\ (1,7,7).$$

Generalization

By playing a lifting and counting game this can be generalized to higher degrees.

Theorem

There is a one-to-one connection between products of m lines in $\mathbb{Z}/(2^k)\mathbf{P}^2$ *and homogeneous IVPs of degree m that completely factor with denominator* 2^h*, where h depends on the number of coverings of* $\mathbb{Z}/(2^k)\mathbf{P}^2$ *that the lines achieve.*

Thank you

Thank you for listening to this presentation.