An Introduction to Integer Valued Polynomials

Marie-Andrée B.Langlois

Dalhousie University

February 2018

What are Integer Valued Polynomials?

For this talk

Definition

For any subset S of $\mathbb{Z}$ the ring of integer valued polynomials on S is defined to be $\mathrm{Int}(S) = \{f(x) \in \mathbb{Q}[x] \mid f(S) \subseteq \mathbb{Z}\}$.

What are Integer Valued Polynomials?

For this talk

Definition

For any subset S of $\mathbb{Z}$ the ring of integer valued polynomials on S is defined to be $\text{Int}(S) = \{f(x) \in \mathbb{Q}[x] \mid f(S) \subseteq \mathbb{Z}\}$.

The formal definition is for a domain D and field of fractions K.

Definition

For any subset S of D the ring of integer valued polynomials on S is defined to be $\text{Int}(S, D) = \{f(x) \in K[x] \mid f(S) \subseteq D\}$.

What are Integer Valued Polynomials ?

Lets start with $\text{Int}(\mathbb{Z})$ and find some examples :

- $25x^5 - 13x^3 + 7x - 23$

What are Integer Valued Polynomials ?

Lets start with $\text{Int}(\mathbb{Z})$ and find some examples :

- $25x^5 - 13x^3 + 7x - 23$
- is a boring example, we want non-integer coefficients !

What are Integer Valued Polynomials ?

Lets start with $\text{Int}(\mathbb{Z})$ and find some examples :

- $25x^5 - 13x^3 + 7x - 23$
- is a boring example, we want non-integer coefficients !
- Degree 1, can we do better than x ?

What are Integer Valued Polynomials ?

Lets start with $\mathrm{Int}(\mathbb{Z})$ and find some examples :

- $25x^5 - 13x^3 + 7x - 23$
- is a boring example, we want non-integer coefficients !
- Degree 1, can we do better than x ?
- Degree 2, $\frac{x(x-1)}{2}$

What are Integer Valued Polynomials?

Lets start with $\text{Int}(\mathbb{Z})$ and find some examples :

- $25x^5 - 13x^3 + 7x - 23$
- is a boring example, we want non-integer coefficients!
- Degree 1, can we do better than x?
- Degree 2, $\frac{x(x-1)}{2}$
- Degree 3, $\frac{x(x-1)(x-2)}{2 \cdot 3}$

What are Integer Valued Polynomials?

In general, for degree n :

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$$

Theorem

A polynomial is integer valued on $\mathbb{Z}$ if and only if it can be written as a $\mathbb{Z}$-linear combination of the polynomials

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-k+1)}{n!},$$

for $n = 0, 1, 2, \ldots$.

Today's Plan

We will go over the following :

- Bases and IVPs on subsets of the integers.
- p-orderings, p-sequences and invariants of $\text{Int}(S)$.
- Multivariable and homogeneous case.

Int(S) is a Ring

- Most of the axioms follow from $\mathbb{Q}[x]$ being a ring.
- Int(S) is also closed under addition and multiplication.
- Int(S) is a $\mathbb{Z}$-module.

Int(S) is a Module

Definition

An R-module M, over the ring R consist of an abelian group $(M,+)$ and an operation $R \times M \to M$ (scalar multiplication). For all $r, s \in R$, $x, y \in M$ we have

1. $r(x+y) = rx + ry$.
2. $(r+s)x = rx + sx$.
3. $(rs)(x) = r(sx)$.
4. $1_R x = x$.

Int(S) is a $\mathbb{Z}$-module

In this case $R = \mathbb{Z}$, we want for all $m, n \in \mathbb{Z}$ and $f(x), g(x) \in \text{Int}(S)$:

1. $m(f(x) + g(x)) = m \cdot f(x) + m \cdot g(x)$.
2. $(m + n)f(x) = m \cdot f(x) + n \cdot f(x)$.
3. $(mn)f(x) = m(n \cdot f(x))$.
4. $1 \cdot f(x) = f(x)$.

Multiply $f(x)$ an IVP by an integer n will preserve its integer valued property.

Bases

Definition

A basis $\mathcal{B}$ of the R-module $\mathbb{B}$ is said to be a regular basis if it is formed by one and only one polynomial of each degree.

- A regular basis for $\mathrm{Int}(\mathbb{Z})$ is $\{1\} \cup \left\{ \binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!} \right\}_{n \geq 1}$.

What if $S \subset \mathbb{Z}$

We will look at Int(S) for $S \subset \mathbb{Z}$, to motivate why we need better tools to find bases. Here are examples of sets we can consider

- Even/Odd integers
- Prime numbers
- Fibonacci Numbers
- Sum of ℓ d-th powers

$$x = x_1^d + x_2^d + \cdots + x_\ell^d$$

Even/Odd Integers

Even/Odd Integers

- For $S = 2\mathbb{Z}$, a basis for $\mathrm{Int}(S)$ is made of the polynomials $\binom{x/2}{n}$

$$\left\{1,\ \frac{x}{2},\ \frac{x(x-2)}{8},\ \frac{x(x-2)(x-4)}{48},\ \ldots\right\}$$

Even/Odd Integers

- For $S = 2\mathbb{Z}$, a basis for $\mathrm{Int}(S)$ is made of the polynomials $\binom{x/2}{n}$

$$\left\{1,\ \frac{x}{2},\ \frac{x(x-2)}{8},\ \frac{x(x-2)(x-4)}{48},\ \dots\right\}$$

- For $S = 1 + 2\mathbb{Z}$, a basis for $\mathrm{Int}(S)$ is made of the polynomials $\binom{(x-1)/2}{n}$

$$\left\{1,\ \frac{(x-1)}{2},\ \frac{(x-1)(x-3)}{8},\ \frac{(x-1)(x-3)(x-5)}{48},\ \dots\right\}$$

Prime Numbers

The beginning of a basis for $\text{Int}(\mathbb{P})$:

$$f_0 = 1,\ f_1 = (x-1),\ f_2 = \frac{(x-1)(x-2)}{2},$$

$$f_3 = \frac{(x-1)(x-2)(x-3)}{24},\ f_4 = \frac{(x-1)^2(x-2)(x-3)}{48},$$

$$f_5 = \frac{(x-1)(x-2)(x-3)(x-5)(x-79)}{5760},\ \ldots$$

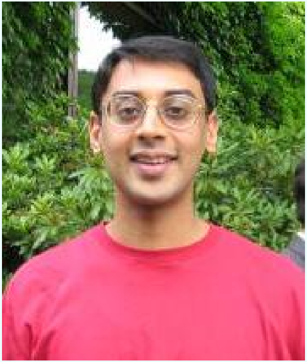
and $f_3(4) = \frac{1}{4}$, $f_4(4) = \frac{3}{4}$ and $f_5(4) = \frac{5}{64}$.

Manjul Bhargava

We will go over some work that Bhargava did during his undergraduate degree and define

- *p*-orderings
- *p*-sequences.

For the next part of the presentation we will work locally at a prime p.



Source of Image : https://opc.mfo.de/detail?photo_id=7108

A Game Called p-orderings

Fix a prime p.

Definition (Bhargava)

A p-ordering of S a subset of $\mathbb{Z}$ is a sequence $(a_n)_{n\geq 0}$, such that a_0 is arbitrarily chosen and for each $n > 0$, $a_n \in S$ is chosen to minimize

$$\nu_p((a_0 - a_n)\cdots(a_{n-1} - a_n)).$$

where

$$\nu_p(n) = \begin{cases} \max\{\nu \in \mathbb{N} \colon p^\nu | n\} & n \geq 0 \\ \infty & n = 0 \end{cases}$$

Lets play !

Let $p = 2$ and $S = \{0, 1, 2, 3, 4\}$

Lets play !

Let $p = 2$ and $S = \{0, 1, 2, 3, 4\}$

- $a_0 = 0$

Lets play !

Let $p = 2$ and $S = \{0, 1, 2, 3, 4\}$

- $a_0 = 0$
- for a_1 we want to minimize the power of 2 dividing $(0 - a_1)$ take any odd number, $a_1 = 1$

Lets play !

Let $p = 2$ and $S = \{0, 1, 2, 3, 4\}$

- $a_0 = 0$
- for a_1 we want to minimize the power of 2 dividing $(0 - a_1)$ take any odd number, $a_1 = 1$
- a_2 $(0 - a_2)(1 - a_2)$ pick 2 or 3, $a_2 = 2$

Lets play !

Let $p = 2$ and $S = \{0, 1, 2, 3, 4\}$

- $a_0 = 0$
- for a_1 we want to minimize the power of 2 dividing $(0 - a_1)$ take any odd number, $a_1 = 1$
- a_2 $(0 - a_2)(1 - a_2)$ pick 2 or 3, $a_2 = 2$
- a_3 $(0 - a_3)(1 - a_3)(2 - a_3)$, need to pick an odd value $a_3 = 3$

Lets play !

Let $p = 2$ and $S = \{0, 1, 2, 3, 4\}$

- $a_0 = 0$
- for a_1 we want to minimize the power of 2 dividing $(0 - a_1)$ take any odd number, $a_1 = 1$
- $a_2 \quad (0 - a_2)(1 - a_2)$ pick 2 or 3, $a_2 = 2$
- $a_3 \quad (0 - a_3)(1 - a_3)(2 - a_3)$, need to pick an odd value $a_3 = 3$
- $a_4 = 4$.

Our p-ordering of S is $\{0, 1, 2, 3, 4\}$.

In General

Proposition (Bhargava)

The natural ordering of $\mathbb{Z}_{\geq 0}$ with $a_i = i$ is a p-ordering of $\mathbb{Z}$ for all primes p.

Are p-orderings unique ?

In General

Proposition (Bhargava)

The natural ordering of $\mathbb{Z}_{\geq 0}$ with $a_i = i$ is a p-ordering of $\mathbb{Z}$ for all primes p.

Are p-orderings unique ? No, we made some choices in the previous example.

p-sequences

Definition (Bhargava)

Given $(a_n)_{n\geq 0}$ a p-ordering of S a subset of $\mathbb{Z}$ with $\alpha_0 = 0$ and $\alpha_n(S,p) = \nu_p((a_0 - a_n)\cdots(a_{n-1} - a_n))$, $\{\alpha_n(S,p)\}$ is the associated p-sequence of S.

A nice property for a set S is that the p-sequence is independent of the choice of p-ordering.

Example : $\{\alpha_n(\mathbb{Z},p)\} = \{\nu_p(n!)\}$.

A More Interesting Version of the Game

Let $p = 2$ and $S = \{0, 1, 8, 27, 64, 125\}$

A More Interesting Version of the Game

Let $p = 2$ and $S = \{0, 1, 8, 27, 64, 125\}$

- $a_0 = 0$ and $\alpha_0 = 0$

A More Interesting Version of the Game

Let $p = 2$ and $S = \{0, 1, 8, 27, 64, 125\}$

- $a_0 = 0$ and $\alpha_0 = 0$
- for a_1 we want to minimize the power of 2 dividing $(0 - a_1)$ take any odd number, $a_1 = 1$ and $\alpha_1 = 0$

A More Interesting Version of the Game

Let $p = 2$ and $S = \{0, 1, 8, 27, 64, 125\}$

- $a_0 = 0$ and $\alpha_0 = 0$
- for a_1 we want to minimize the power of 2 dividing $(0 - a_1)$ take any odd number, $a_1 = 1$ and $\alpha_1 = 0$
- a_2 $(0 - a_2)(1 - a_2)$, $a_2 = 27$ is the best choice and $\alpha_2 = 1$.

A More Interesting Version of the Game

Let $p = 2$ and $S = \{0, 1, 8, 27, 64, 125\}$

- $a_0 = 0$ and $\alpha_0 = 0$
- for a_1 we want to minimize the power of 2 dividing $(0 - a_1)$ take any odd number, $a_1 = 1$ and $\alpha_1 = 0$
- a_2 $(0 - a_2)(1 - a_2)$, $a_2 = 27$ is the best choice and $\alpha_2 = 1$.
- a_3 $(0 - a_3)(1 - a_3)(27 - a_3)$, we can choose between 8 and 125, $a_3 = 8$ and $\alpha_3 = 3$.

A More Interesting Version of the Game

Let $p = 2$ and $S = \{0, 1, 8, 27, 64, 125\}$

- $a_0 = 0$ and $\alpha_0 = 0$
- for a_1 we want to minimize the power of 2 dividing $(0 - a_1)$ take any odd number, $a_1 = 1$ and $\alpha_1 = 0$
- a_2 $(0 - a_2)(1 - a_2)$, $a_2 = 27$ is the best choice and $\alpha_2 = 1$.
- a_3 $(0 - a_3)(1 - a_3)(27 - a_3)$, we can choose between 8 and 125, $a_3 = 8$ and $\alpha_3 = 3$.
- a_4 $(0 - a_4)(1 - a_4)(27 - a_4)(8 - a_4)$ start checking with 125, since we hope for $\alpha < 6$, we obtain $a_4 = 125$ and $\alpha_4 = 3$

A More Interesting Version of the Game

Let $p = 2$ and $S = \{0, 1, 8, 27, 64, 125\}$

- $a_0 = 0$ and $\alpha_0 = 0$
- for a_1 we want to minimize the power of 2 dividing $(0 - a_1)$ take any odd number, $a_1 = 1$ and $\alpha_1 = 0$
- a_2 $(0 - a_2)(1 - a_2)$, $a_2 = 27$ is the best choice and $\alpha_2 = 1$.
- a_3 $(0 - a_3)(1 - a_3)(27 - a_3)$, we can choose between 8 and 125, $a_3 = 8$ and $\alpha_3 = 3$.
- a_4 $(0 - a_4)(1 - a_4)(27 - a_4)(8 - a_4)$ start checking with 125, since we hope for $\alpha < 6$, we obtain $a_4 = 125$ and $\alpha_4 = 3$
- $a_5 = 64$ and $(0 - 64)(1 - 64)(27 - 64)(8 - 64)(125 - 64) = 2^6(-63)(-37)(-56)(61)$ and $\alpha_5 = 9$.

Our p-ordering of S is $\{0, 1, 27, 8, 125, 64\}$ and the p-sequence is $\{0, 0, 1, 3, 3, 9\}$.

Factorial Function

The factorial function is very important when working with IVPs. It was in the denominators of the basis elements of Int($\mathbb{Z}$) and in the p-sequence of $\mathbb{Z}$.

What is the factorial function when working with S not $\mathbb{Z}$?

Proposition

- *For any non-negative k and ℓ, $(k+\ell)!$ is still a multiple of $k!\ell!$.*
- *Let f be a primitive polynomial with integer coefficients of degree k, and let $d(\mathbb{Z}, f) = gcd\{f(a) \mid a \in \mathbb{Z}\}$. Then $d(\mathbb{Z}, f)$ divides $k!$.*

  This is called the **fixed divisor** *of f.*

Generalized Factorial Function

Definition (Bhargava)

Let S be any subset of $\mathbb{Z}$. the the factorial function on S denoted $k!_S$ is defined by $k!_S = \prod_p p^{\alpha_k(S,p)}$.

This definition preserves many properties of the factorial function on $\mathbb{Z}$:

- For any non-negative k and ℓ, $(k+\ell)!_S$ is still a multiple of $k!_S \ell!_S$.
- Let f be a primitive polynomial of degree k, and let $d(S,f) = gcd\{f(a) \mid a \in S\}$. Then $d(S,f)$ divides $k!_S$.

Generalized Factorial is the Same on $\mathbb{Z}$

We know that $6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$, we use the generalized factorial instead :

$$\alpha_n(\mathbb{Z}, 2) = \{0, 0, 1, 1, 3, 3, 4, 4, 7, 8, \ldots\}$$
$$\alpha_n(\mathbb{Z}, 3) = \{0, 0, 0, 1, 1, 1, 2, 2, 2, 4, \ldots\}$$
$$\alpha_n(\mathbb{Z}, 5) = \{0, 0, 0, 0, 0, 1, 1, 1, 1, 1, \ldots\}$$

$$6! = 2^4 \cdot 3^2 \cdot 5$$

Generalized Factorial is the Same on $\mathbb{Z}$

We know that $6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$, we use the generalized factorial instead :

$$\alpha_n(\mathbb{Z}, 2) = \{0, 0, 1, 1, 3, 3, 4, 4, 7, 8, \ldots\}$$
$$\alpha_n(\mathbb{Z}, 3) = \{0, 0, 0, 1, 1, 1, 2, 2, 2, 4, \ldots\}$$
$$\alpha_n(\mathbb{Z}, 5) = \{0, 0, 0, 0, 0, 1, 1, 1, 1, 1, \ldots\}$$

$$6! = 2^4 \cdot 3^2 \cdot 5$$

Generalized Factorial on S

Let $S = \{0, 1, 8, 27, 64, 125\}$, we will calculate $3!_S$, the factorial of an element with index 3 in our p-ordering, in out case this was 8 :

$$\alpha_n(\mathbb{Z}, 2) = \{0, 0, 1, 3, 3, 9\}$$
$$\alpha_n(\mathbb{Z}, 3) = \{0, 0, 0, 2, 2, 3\}$$
$$\alpha_n(\mathbb{Z}, 5) = \{0, 0, 0, 0, 0, 3\}$$
$$\alpha_n(\mathbb{Z}, 7) = \{0, 0, 0, 1, 2, 2\}$$

$$3!_S = 2^3 \cdot 3^2 \cdot 5^0 \cdot 7^1$$

Generalized Factorial on S

Let $S = \{0, 1, 8, 27, 64, 125\}$, we will calculate $3!_S$, the factorial of an element with index 3 in our p-ordering, in out case this was 8 :

$$\alpha_n(\mathbb{Z}, 2) = \{0, 0, 1, 3, 3, 9\}$$
$$\alpha_n(\mathbb{Z}, 3) = \{0, 0, 0, 2, 2, 3\}$$
$$\alpha_n(\mathbb{Z}, 5) = \{0, 0, 0, 0, 0, 3\}$$
$$\alpha_n(\mathbb{Z}, 7) = \{0, 0, 0, 1, 2, 2\}$$

$$3!_S = 2^3 \cdot 3^2 \cdot 5^0 \cdot 7^1$$

Basis for IVPs on a subset of $\mathbb{Z}$

Theorem (Bhargava)

A polynomial is integer valued on a subset S of $\mathbb{Z}$ if and only if it can be written as a $\mathbb{Z}$-linear combination of the polynomials

$$\frac{B_{k,S}}{k!_S} = \frac{(x-a_{0,k})(x-a_{1,k})\cdots(x-a_{k-1,k})}{k!_S},$$

for $k = 0, 1, 2, \ldots$ where the $B_{k,S}(x)$ are the polynomials defined by

$$(x-a_{0,k})(x-a_{1,k})\cdots(x-a_{k-1,k}),$$

where $\{a_{i,k}\}_{i=0}^{\infty}$ is a sequence in $\mathbb{Z}$ that, for each prime p dividing $k!_S$, is term-wise congruent modulo $\alpha_k(S,p)$ to some p-ordering of S.

Characteristic Ideal

Definition (Chabert)

The characteristic ideal of index n of $\mathbb{Z}$ is the set $\mathfrak{J}_n(\mathbb{Z})$ formed by 0 and the leading coefficients of the polynomials in $\mathrm{Int}(S,\mathbb{Z})$ of degree n.

For example, when $S = \mathbb{Z}$, $\mathfrak{J}_n(\mathbb{Z}) = \frac{1}{n!}\mathbb{Z}$.

Definition (Chabert)

The characteristic sequence of S with respect to a fixed prime p is the sequence of negatives of the p-adic valuations of these ideals, denoted by $\alpha_n(S,p)$.

The Valuative Capacity

Definition (Chabert)

For S a subset of $\mathbb{Z}$ and p a fixed prime, the valuative capacity of S with respect to the prime p is the following limit :

$$L_{S,p} = \lim_{n\to\infty} \frac{\alpha_n(S,p)}{n}.$$

The positive integers in increasing order are a p-ordering of $\mathbb{Z}$ and we have that $\alpha_n(\mathbb{Z},p) = \nu_p(n!)$. By Legendre's formula $\nu_p(n!) = \frac{n-\sum n_i}{p-1}$, we can compute

$$L_{\mathbb{Z},p} = \lim_{n\to\infty} \frac{\alpha_n(\mathbb{Z},p)}{n} = \frac{1}{p-1}.$$

Sums of Two and Three Squares

Let S be the set of perfect squares in $\mathbb{Z}$ and

$$E = S + S \quad F = S + S + S$$

Theorem (Fares, Johnson)

$$L_{E,p} = \begin{cases} \frac{1}{p-1} & \text{if } p \equiv 1 \pmod 4 \\ -1 + \sqrt{1 + \frac{2p}{(p-1)^2}} & \text{if } p \equiv 3 \pmod 4 \\ \frac{-1+\sqrt{13}}{2} & \text{if } p = 2 \end{cases}$$

$$L_{F,p} = \begin{cases} \frac{1}{p-1} & \text{if } p > 2 \\ \frac{-25+3\sqrt{705}}{52} & \text{if } p = 2 \end{cases}$$

Sums of ℓ Elements to the Power of d

For $D = \{x^d \mid x \in \mathbb{Z}\}$ and we let $\ell D = D + \cdots + D$, for ℓ terms in the sum.

Theorem (B.)

Suppose p is a prime and $d = p^j d'$ a positive integer not equal to 4, where $p \nmid d'$ and let $e = 2j + 1$.

Then, $L_{\ell D,p}$ is an algebraic number of degree at most 2.

When 0 can be written non-trivially as a sum of ℓ elements to the power of $d \pmod{p^e}$, $L_{\ell D,p}$ is a rational number.

Corollary (B.)

For a fixed ℓ, if d is odd and p is a prime, then $L_{\ell D,p} \in \mathbb{Q}$.

Timeline of IVPs

- Pólya in 1915
- Cahen and Chabert wrote a textbook on the subject, mid 90's
- Bhargava, *p*-sequences, late 90's
- Chabert, valuative capacity 2001
- Chabert, survey article 2014

Generalization

- Recall that the official definition is $\text{Int}(S, D)$.
- IVPs over quaternions. [Werner] [Johnson and Pavlovski]
- IVPs over matrix rings. [Evrard, Fares and Johnson] [Frisch] [Werner]
- Multivariable case. [Bhargava] [Evrard]
- Homogeneous 2-variable case. [Johnson and Patterson]

Multivariable

Let n be a positive integer, let $\underline{S}$ be a subset of $\mathbb{Z}^n$ and let $m_0, m_1, \ldots$ be an ordering of the monomials of $\mathbb{Z}^n[\underline{X}]$, and consider the $\mathbb{Z}$-algebra

$$\text{Int}(\underline{S}) = \{f(X_1, \ldots, X_n) \in \mathbb{Q}[X_1, \ldots, X_n] \mid f(\underline{S}) \subseteq \mathbb{Z}\}.$$

Using matrices, p-orderings and p-sequences can be generalized to the multivariable case.

Multivariable - A Basis $\mathrm{Int}(\mathbb{Z}^n)$

Proposition

The polynomials $\left\{ \binom{x_1}{r_1}\binom{x_2}{r_2}\cdots\binom{x_n}{r_n} \mid r_1,\ldots,r_n \in \mathbb{Z},\ r_1,\ldots,r_n \geq 0 \right\}$ *form a basis of the* $\mathbb{Z}$*-module of* $\mathrm{Int}(\mathbb{Z}^n)$*.*

In the three variable case, the elements of degree 3 are

$$\binom{x}{3}, \binom{y}{3}, \binom{z}{3}, \binom{x}{2}\binom{y}{1}, \binom{x}{2}\binom{z}{1}, \binom{x}{1}\binom{y}{2}, \binom{y}{2}\binom{z}{1}$$

$$\binom{x}{1}\binom{z}{2}, \binom{y}{1}\binom{z}{2}, \binom{x}{1}\binom{y}{1}\binom{z}{1}$$

Homogeneous Polynomials

A homogeneous polynomial is one of the form

$$f(x_1, \ldots, x_n) = \sum_{i_1+i_2+\cdots+i_n=m} c_1 x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}.$$

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

$$f(hx_1, \ldots, hx_n) = h^m f(x_1, \ldots, x_n)$$

Homogeneous as a Product of Linears

- When written as a product of linear factors each term must contain a variable, we can't have $(x-2)$ we would need $(x-2y)$.

- Start by focusing on how big of a power of $p=2$ we can get. How can we construct 2-variable IVPs ?

- In degree 1 and 2 we need integer coefficients : $x,\ y,\ xy$.

- Can we obtain a denominator in degree 3 ?

Homogeneous as a Product of Linears

- When written as a product of linear factors each term must contain a variable, we can't have $(x-2)$ we would need $(x-2y)$.
- Start by focusing on how big of a power of $p=2$ we can get. How can we construct 2-variable IVPs ?
- In degree 1 and 2 we need integer coefficients : $x,\ y,\ xy$.
- Can we obtain a denominator in degree 3 ?
- Yes ! $\frac{xy(x-y)}{2}$

Basis for Degree 3, 3 Variables

In degree m we will have $\frac{(m+1)(m+2)}{2}$ basis elements.

$$\left\{xyz, \frac{xy(x-y)}{2}, \frac{xz(x-z)}{2}, \frac{yz(y-z)}{2}, x^2(x-y), x^2(x-z), y^2(y-x), y^2(y-z), z^2(z-x), z^3\right\}.$$

Another Example

- For example when $m = 6$, we have 7 elements with a 2^0, 14 with a 2^1, 4 with a 2^2 and 3 with a 2^3 in their denominators.

- The polynomials with a 2^3 in their denominator are :

$$f = \frac{1}{4}x^5y + \frac{7}{8}x^4y^2 + \frac{1}{8}x^2y^4 + \frac{3}{4}xy^5$$

$$g = \frac{3}{4}x^5z + \frac{1}{8}x^4z^2 + \frac{7}{8}x^2z^4 + \frac{1}{4}xz^5$$

$$h = \frac{1}{4}x^5y + \frac{1}{2}x^5z + \frac{3}{8}x^4y^2 + \frac{3}{4}x^4z^2 + \frac{5}{8}x^2y^4 + \frac{1}{4}x^2z^4 + \frac{3}{4}xy^5 + \frac{1}{2}xz^5 + \frac{3}{4}y^5z + \frac{1}{8}y^4z^2 + \frac{7}{8}y^2z^4 + \frac{1}{4}yz^5$$

Counting the Basis Elements

	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9
1	3	0	0	0	0	0	0	0	0	0
2	6	0	0	0	0	0	0	0	0	0
3	7	3	0	0	0	0	0	0	0	0
4	7	8	0	0	0	0	0	0	0	0
5	7	14	0	0	0	0	0	0	0	0
6	7	14	4	3	0	0	0	0	0	0
7	7	14	6	9	0	0	0	0	0	0
8	7	14	7	14	3	0	0	0	0	0
9	7	14	7	14	13	0	0	0	0	0
10	7	14	7	14	21	3	0	0	0	0
11	7	14	7	14	28	8	0	0	0	0
12	7	14	7	14	28	14	4	3	0	0
13	7	14	7	14	28	14	6	15	0	0
14	7	14	7	14	28	14	7	25	3	1

Counting the Basis Elements

	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9
1	3	0	0	0	0	0	0	0	0	0
2	6	0	0	0	0	0	0	0	0	0
3	7	3	0	0	0	0	0	0	0	0
4	7	8	0	0	0	0	0	0	0	0
5	7	14	0	0	0	0	0	0	0	0
6	7	14	4	3	0	0	0	0	0	0
7	7	14	6	9	0	0	0	0	0	0
8	7	14	7	14	3	0	0	0	0	0
9	7	14	7	14	13	0	0	0	0	0
10	7	14	7	14	21	3	0	0	0	0
11	7	14	7	14	28	8	0	0	0	0
12	7	14	7	14	28	14	4	3	0	0
13	7	14	7	14	28	14	6	15	0	0
14	7	14	7	14	28	14	7	25	3	1

Thank you

Thanks for listening to this presentation.