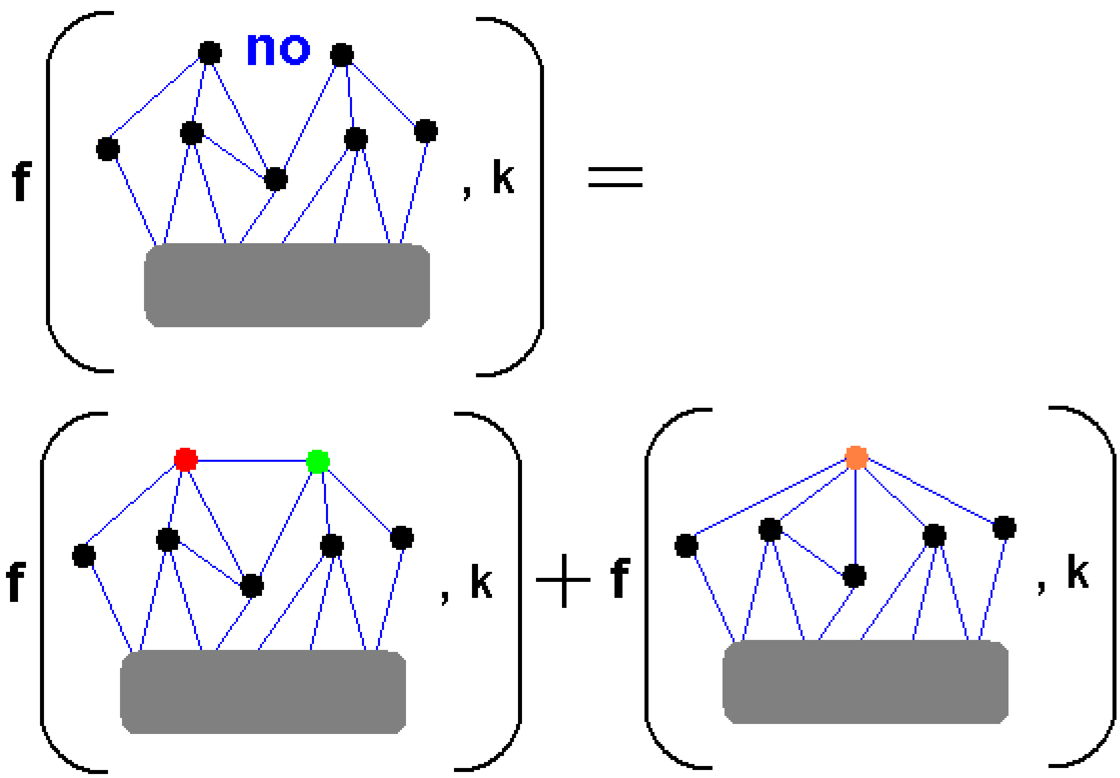
Rings of "Integer"-Valued Polynomials

David Lantz
Colgate University
dlantz@mail.colgate.edu

An *integer-valued polynomial* is a function from the integers to the integers that is given by a polynomial.

Ex: The number of (vertex-)colorings of a given graph (so that vertices connected by an edge have different colors), using a set of k colors, is a polynomial in k.

Proof: $f(K_n, k) = k(k-1)(k-2)\cdots(k-n+1)$.



So $f(G, k)$ has integer coefficients, leading coefficient 1, and degree $|V(G)|$.

Ex: F a field, $x_1, x_2, \ldots, x_n$ indeterminates (variables). Dimension of the F-v.s. of all polynomials of total degree k is

$$\binom{k+n-1}{n-1}$$

(In $k+n-1$ positions to be filled with either "another of the same variable" or "switch to a new variable", pick the second $n-1$ times.)

So

$$\dim_F\left(\frac{F[x_1, x_2, \ldots, x_n]}{\text{polynomials of degree } > n}\right) = \binom{k+n}{n}$$

— coefficients are integers over $n!$, leading coefficient is $1/n!$, and degree is n.

Lagrange Interpolation: $a_1, a_2, \ldots, a_n$ distinct, any $r_1, r_2, \ldots, r_n$:

$$f(X) = \sum_{j=1}^{n} r_j \prod_{i \neq j} \frac{X - a_i}{a_j - a_i} .$$

has $f(a_i) = r_i$ (and is unique of degree at most n)

So if the a_i's are consecutive integers, the denominator is (no worse than) $(n-1)!$.

In fact, it's better to write an integer-valued polynomial, not in powers of k, but in the "binomial coefficient" functions

$$\binom{k+n-1}{n} = B_n(k) \quad :$$

$$B_0(k) = 1\,,\ B_1(k) = k\,,\ B_2(k) = \frac{1}{2}k(k+1)\,,\ \ldots$$

$$P(k) = e_0 B_0(k) + e_1 B_1(k) + \ldots + e_d B_d(k)$$

where the e_i's are integers and $d = \deg(P)$

From

$$B_n(k+1) - B_n(k) = B_{n-1}(k+1)$$

we get

$$\begin{aligned} P(k+1) - P(k) \\ &= e_1 B_0(k+1) + e_2 B_1(k+1) \\ &\quad + \ldots + e_d B_{d-1}(k+1) \end{aligned}$$

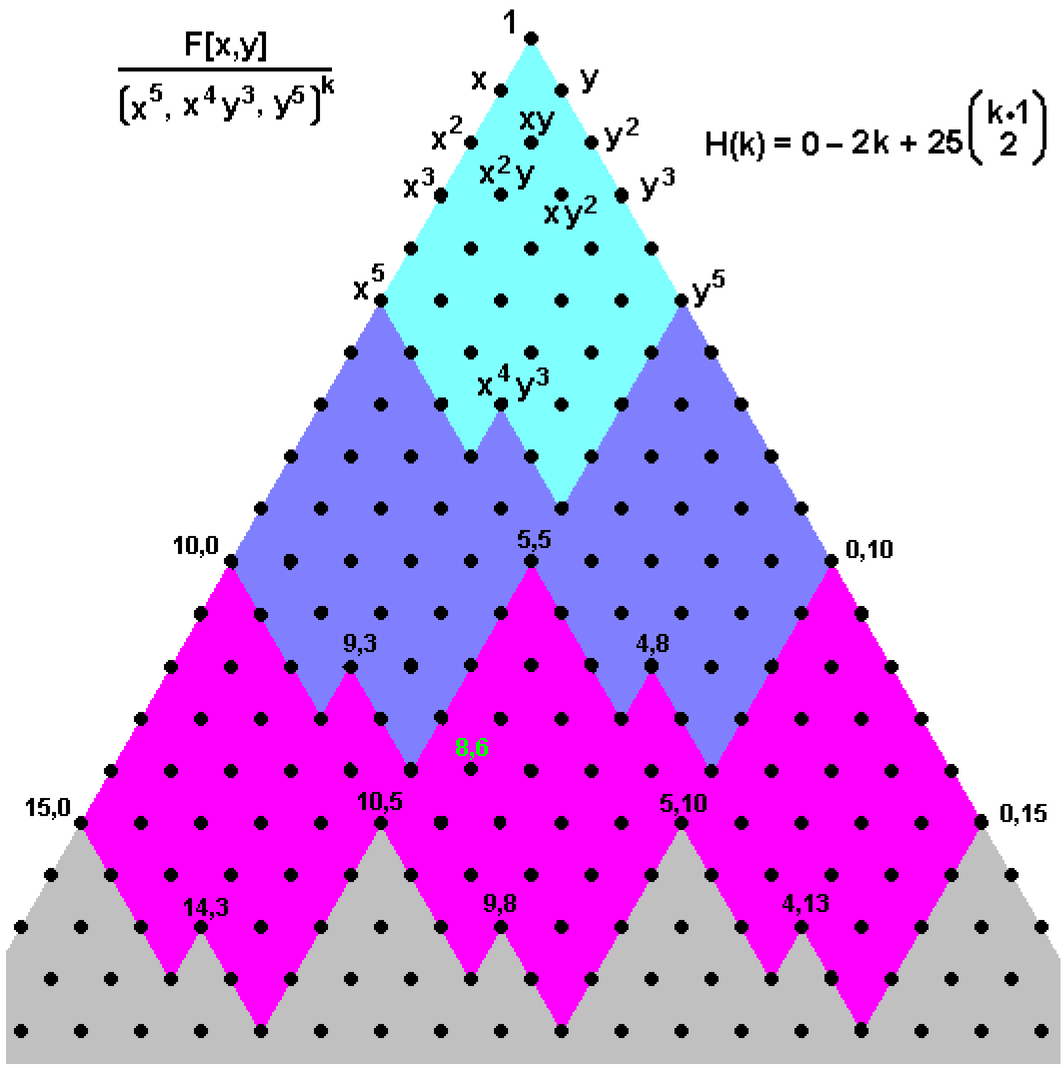
Repeating this, we can get e_d, then subtract $e_d B_d(k)$ and repeat to find the other e_i's. (Example shortly.)

Def: R is *Noetherian* if (1) every ideal is fin gen; or (2) every ($\neq \emptyset$) set of ideals has max elts.

R Noetherian, M max ideal, I M-primary ideal (contains a power of M). Then

$$\text{length}(R/I^k) = H_I(k)$$

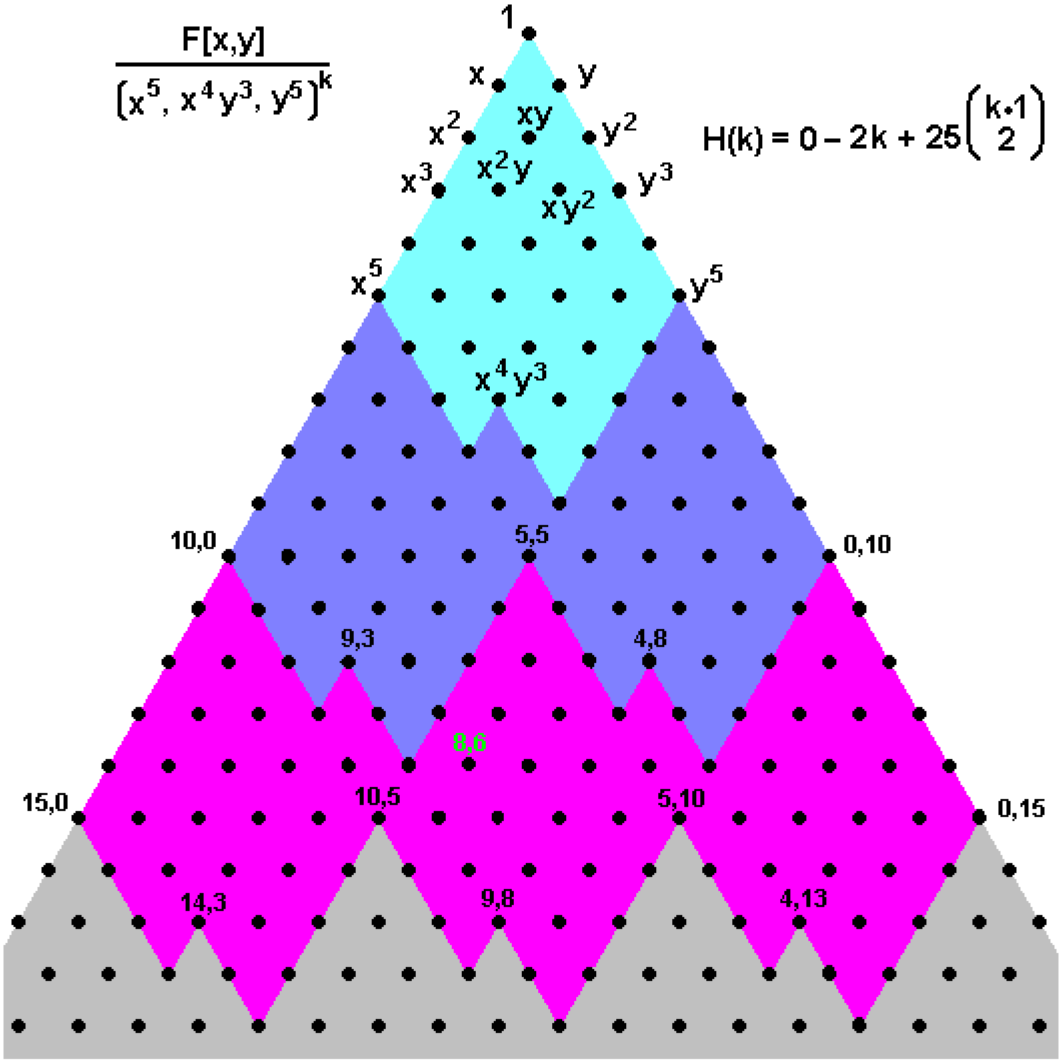
is a polynomial in k for $k >> 0$.



$\frac{F[x,y]}{(x^5, x^4y^3, y^5)^k}$
$H(k) = 0 - 2k + 25\binom{k+1}{2}$
1
x
y
xy
x^2
y^2
x^2y
x^3
y^3
xy^2
x^5
y^5
x^4y^3
10,0
5,5
0,10
9,3
4,8
8,6
15,0
10,5
5,10
0,15
14,3
9,8
4,13

$$\frac{F[x,y]}{\left(x^5,\ x^4y^3,\ y^5\right)^k}$$

$$H(k) = 0 - 2k + 25\binom{k+1}{2}$$



But the polynomial may not kick in immediately:

Ex: $R = F[x, y]$, $M = (x, y)$, $I = (x^5, x^3y^2, y^5)$:

k	1	2	3	4	5	6
$H(k)$	19	61	127	217	332	472
1st diffs $H(k+1) - H(k)$	42	66	90	115	140	
2nd diffs	24	24	25	25		
$H(k) - 25B_2(k)$	-6	-14	-23	-33	-43	-53
1st diffs	-8	-9	-10	-10	-10	
$H(k) - (25B_2(k) - 10B_1(k))$	4	6	7	7	7	7
$H(k) - (25B_2(k) - 10B_1(k) + 7B_0(k))$	-3	-1	0	0	0	0

So $H_I(k) = 7B_0(k) - 10B_1(k) + 25B_2(k)$ for $k \geq 3$.

Notation:

$$\begin{aligned} H_I(k) &= e_0(I)B_0(k) + e_1(I)B_1(k) \\ &\qquad + \cdots + e_d(I)B_d(k) \end{aligned}$$

(reverses the usual).

First k s.t. H_I agrees with the polynomial is the *postulation number* of I.

Notation: $I : J = \{r \in R \mid rJ \subseteq I\}$

Ratliff and Rush: R Noetherian, I contains a nonzerodivisor. Then

$$\tilde{I} = \cup\{I^{k+1} : I^k \mid k \geq 1\}$$

is largest ideal $\supseteq I$ s.t. $(\tilde{I})^k = I^k$ for $k >> 0$ (so $H_{\tilde{I}}(k) = H_I(k)$ for $k >> 0$, so $e_j(\tilde{I}) = e_j(I)$ for $j = 0, 1, \ldots, d$).

K. Shah: R Noeth, only 1 max M (dim $d > 0$ q-unmixed, R/M inf), I M-primary. Then there is a largest ideal $I_{\{s\}} \supseteq I$ s.t.

$$e_j(I_{\{s\}}) = e_j(I)$$

for $j = s, s+1, \ldots, d$ (so $\tilde{I} = I_{\{0\}}$ and $I_{\{d\}}$ is the "integral closure" of I, the largest ideal $\supseteq I$ with the same "multiplicity" e_d).

Elias: Pick a "minimal reduction" $a_1, a_2, ..., a_d$ of I ($a_i \in I$, $\overline{a}I^k = I^{k+1}$ for $k >> 0$). Then $\tilde{I} = I^{k+1} : (a_1^k, a_2^k, \ldots, a_d^k)$ if

$k \geq 1+\max\{\mathrm{pn}(I), \mathrm{pn}(I/(a_1)), \ldots, \mathrm{pn}(I/(a_d))\}$.

Moreover, if

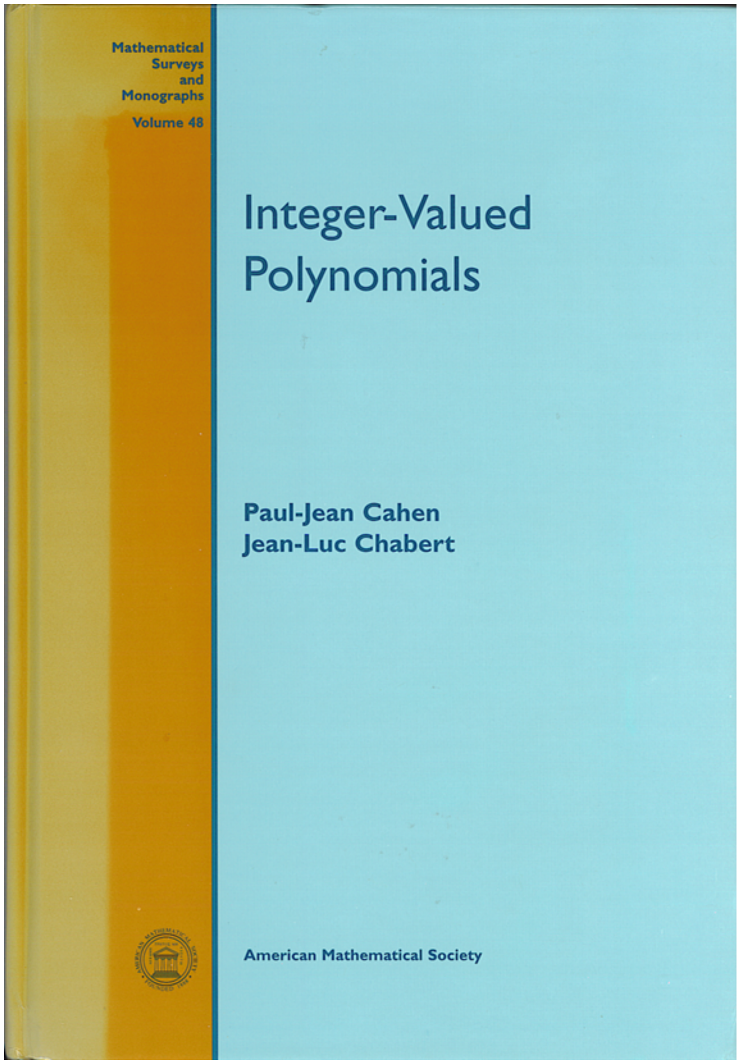
$$f(e,d) := \begin{cases} e-1 & \text{if } d=1 \\ e^{2(d-1)!-1}(e-1)^{(d-1)!} & \text{if } d>1 \end{cases}$$

then $\tilde{I} = I^{k+1} : I^k$ for

$$k \geq (d+1)(f(e_d(I),d)+2) \ .$$

For $d=2$ and $e_2(I)=49$, the bound is 7062.
I had the computer check all the <u>monomial</u> ideals in $F[x,y]$ with minimal reduction x^7, y^7, and none needed a $k > 4$.
It's a long way from 4 to 7062. Is there a theorem here?

For more on *coefficient ideals,* see Shah, or several papers by Heinzer, L., Johnston and Shah (in various combinations).



Def: D a(n integral) domain (comm, with 1), F its frac field.

$$\mathrm{Int}(D) = \{g(x) \in F[x] \mid g(d) \in D \;\forall\, d \in D\}$$

Lemma: $f(x) \in \mathrm{Int}(D)$, $\deg d$, $a_0, a_1, \ldots, a_d \in D$,

$$p = \prod_{i<j} (a_j - a_i)\ .$$

Then $pf(x) \in D[x]$.

Pf:

$$\begin{bmatrix} 1 & a_0 & a_0^2 & \ldots & a_0^d \\ 1 & a_1 & a_1^2 & \ldots & a_1^d \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & a_d & a_d^2 & \ldots & a_d^d \end{bmatrix} \begin{bmatrix} f'\mathrm{s} \\ \mathrm{c} \\ \mathrm{o} \\ \mathrm{e} \\ \mathrm{f} \\ \mathrm{f} \\ \mathrm{s} \end{bmatrix} = \begin{bmatrix} f(a_0) \\ f(a_1) \\ \vdots \\ f(a_d) \end{bmatrix}\ .$$

Van der Monde and Cramer. //

Cor: If M max ideal of D with D/M inf, then

$$\mathrm{Int}(D) \subseteq D_M[x]\ .$$

Pf: Pick a_i's from diff cosets of M;
then $p \notin M$. //

Prop: $S \subseteq D - \{0\}$ cl under mult:

$$S^{-1}(\mathrm{Int}(D)) \subseteq \mathrm{Int}(S^{-1}D) \ ,$$

and if D is Noeth, reverse also.

Defs: D domain:

(1) D *valuation* if, $\forall\, a, b \in D - \{0\}$, $a/b \in D$ or $b/a \in D$. (So the nonunits form the only max ideal.)

(2) D *Prüfer* if D_M is valuation $\forall\, M$ max.

(3) D *Dedekind* if Prüfer and Noetherian.

Brizolis; McQuillan; Chabert: If D Dedekind with all D/M finite, then $\mathrm{Int}(D)$ is Prüfer of dimension 2.

E.g.: M max in D, $a \in D$:

$$\begin{aligned} 0 \subseteq \{f \in \mathrm{Int}(D) \mid f(a) = 0\} \\ \subseteq \{f \in \mathrm{Int}(D) \mid f(a) \in M\} \ . \end{aligned}$$

Gilmer, Heinzer and L.: D 1-dim Noeth. Then $\mathrm{Int}(D)$ is Noeth iff it is $D[x]$.

Defs: $D \subseteq R$ domains:

(1) $r \in R$ is *integral over D* if r is a root an elt of $D[x]$ with leading coeff 1.

(2) *Integral closure of D in R* is all integral elements.

(3) *Integral closure* of D is its int cl in its frac field.

Ex: K algebraic extension of $\mathbb{Q}$: Integral closure of $\mathbb{Z}$ in K is the ring of *algebraic integers* in K.
(If $[K : \mathbb{Q}] < \infty$, it's Dedekind with finite residue fields.)

Cahen, Chabert and Frisch: D is an *interpolation domain* iff, given $a_1, a_2, \ldots, a_n \in D$ distinct, any $r_1, r_2, \ldots, r_n \in D$, $\exists\, f(x) \in \mathrm{Int}(D)$ s.t. $f(a_i) = r_i \;\forall\, i$.

Must have $\mathrm{Int}(D) \neq D[x]$, to send 0 to 0 and nonunit to 1.

[CC] D val dom, M max:
$\mathrm{Int}(D) \neq D[x]$ iff M principal and D/M fin.

[CCF] D Noeth or Prüfer and an interp dom: all rings between D and its frac field are interp, too.

Building an interp dom whose int cl isn't an interp dom:

Ordered additive subgroup of $\mathbb{Q}$:

$$G = \{a/2^k \mid a \in \mathbb{Z}, k \in \mathbb{N}\}$$

R = set of finite sums $\Sigma_{g \in G} b_g t^g$ where $g \in G, b_g \in \mathbb{Z}/(2)$ (almost all b's 0). An element $\neq 0$ of R has an "order": smallest g s.t. $b_g \neq 0$. Elements of frac field F of R get orders by subtracting.

V, set of elts of F with "order" ≥ 0, is val dom. Divisibility looks like G — no smallest positive, so max ideal isn't principal: $\mathrm{Int}(V) = V[x]$, so V isn't an interp dom.

By long division, elements of F are "Laurent series", and exponents have a common denominator:

$$\frac{t^{3/4} + t^{7/8}}{t^{1/4} + t^{1/2} + t^{5/4}} = ?$$

$$\text{Let } z = t^{1/8}: \quad \frac{z^6 + z^7}{z^2 + z^4 + z^{10}} = z^4 \frac{1 + z}{1 + z^2 + z^8}$$

$$\begin{array}{r|l}
 & 1 + z + z^2 \qquad\qquad + z^8 + \cdots \\
\hline
1 + z^2 + z^8 & 1 + z \\
 & 1 \quad + z^2 \qquad\qquad + z^8 \\
\hline
 & \quad z + z^2 \qquad\qquad + z^8 \\
 & \quad z \quad + z^3 \qquad\qquad + z^9 \\
\hline
 & \qquad z^2 + z^3 \qquad + z^8 + z^9 \\
 & \qquad z^2 + z^3 \qquad\qquad + z^{10} \\
\hline
 & \qquad\qquad\qquad z^8 + z^9 + z^{10} \\
 & \qquad\qquad\qquad \vdots
\end{array}$$

$$\begin{aligned}
? &= z^4 \left(1 + z + z^2 + z^8 + \cdots \right) \\
&= t^{1/2} + t^{5/8} + t^{3/4} + t^{3/2} + \cdots
\end{aligned}$$

Additive submonoid of G:

$$S = \left\{ \begin{array}{l} 1, \\ 2, 2\frac{1}{2}, \\ 3, 3\frac{1}{2}, \\ 4, 4\frac{1}{4}, 4\frac{1}{2}, 4\frac{3}{4}, \\ 5, 5\frac{1}{4}, 5\frac{1}{2}, 5\frac{3}{4}, \\ 6, 6\frac{1}{4}, 6\frac{1}{2}, 6\frac{3}{4}, \\ 7, 7\frac{1}{4}, 7\frac{1}{2}, 7\frac{3}{4}, \\ 8, 8\frac{1}{8}, 8\frac{1}{4}, 8\frac{3}{8}, 8\frac{1}{2}, 8\frac{5}{8}, 8\frac{3}{4}, 8\frac{7}{8}, \\ 9, \ldots, \\ \vdots \end{array} \right\}$$

D = Laurent series with all exponents in S. Then
F is frac field of D,
V is int cl of D (because $(a+b)^2 = a^2 + b^2$),
D has ideals (tails of the series) I_s s.t.

- I_s decreases to (0) as $s \to \infty$,
- D/I_s is finite.

For $d \in D$, $d \neq 0$, $d \notin I_s$ for some $s \in S$.
Define polynomial so $d + I_s \mapsto 1$, $I_s \mapsto 0$.
Finish as in Lagrange interp [CCF].

Bibliography

Cahen and Chabert, **Integer-Valued Polynomials,** AMS (1997)
Cahen, Chabert and Frisch, *J Alg* **225** (2000)
Elias, *J Symbolic Computing* **37** (2004)
Gilmer, Heinzer and L., *Trans AMS* **338** (1993)
Gilmer, Heinzer, L. and Smith, *Proc AMS* **108** (1990)
Heinzer, Johnston and L., *Comm Alg* **21** (1993)
Heinzer, Johnston, L. and Shah, *J Algebra* **162** (1993)
Heinzer, L. and Shah, *Comm Alg* **20(2)** (1992)
L., *JPAA* **174** (2002)
Ratliff and Rush, *Indiana Univ Math J* **27** (1978)
Shah, *Trans AMS* **327** (1991)

`http://math.colgate.edu/faculty/dlantz/SeawayS05.pdf`