# Noncommutative Rational Pólya Series

Jason Bell, University of Waterloo, Canada (joint with Daniel Smertnig)

COW, December 2022

Let $K$ be a field. A univariate formal power series

$$S = \sum_{n \geq 0} s(n) x^n \in K[[x]]$$

is a *rational series* if it is the power series expansion of a rational function at 0. Necessarily, this rational function does not have a pole at 0. Equivalently, the coefficients of a rational series satisfy a *linear recurrence relation*, that is, there exist $\alpha_1, \ldots, \alpha_m \in K$ such that

$$s(n+m) = \alpha_1 s(n+m-1) + \cdots + \alpha_m s(n) \quad \text{for all } n \geq 0.$$

# Pólya's theorem

$G \leq \mathbb{Q}^*$

$\langle 2, 3, 5 \rangle$

Pólya considered arithmetical properties of rational series over $K = \mathbb{Q}$, and characterized the univariate rational series whose coefficients are supported at finitely many prime numbers. This was later extended to number fields by Benzaghou, and to arbitrary fields by Bézivin.

We call a rational series $S \in K[[x]]$ a *Pólya series* if there exists a finitely generated subgroup $G \leq K^\times$, such that all coefficients of $S$ are contained in $G \cup \{0\}$.

## Theorem (Pólya; Benzaghou; Bézivin)

*Let $K$ be a field, let $S = P/Q \in K(x)$ be a rational function with $Q(0) \neq 0$, and let*

$$S = \sum_{n=0}^{\infty} s(n)x^n \in K[[x]]$$

*be the power series expansion of $S$ at 0. Suppose that $S$ is a Pólya series. Then there exist a polynomial $T \in K[x]$, $d \in \mathbb{Z}_{\geq 0}$, and for each $r \in [0, d-1]$ elements $\alpha_r \in K$, $\beta_r \in K^\times$ such that*

$$S = T + \sum_{r=0}^{d-1} \frac{\alpha_r x^r}{1 - \beta_r x^d}.$$

*Equivalently, there exists a finite set $F \subseteq \mathbb{Z}_{\geq 0}$ such that*

$$s(kd+r) = \alpha_r \beta_r^k \qquad \text{for all } k \geq 0 \text{ and } r \in [0, d-1] \text{ with } kd + r \notin F.$$

# Example

[

$$11 + \frac{3x}{1-2x^3} + \frac{5x^2}{1-7x^3}$$

$$= 11 + 3x + 6x^4 + \cdots$$
$$+ 5x^2 + 35x^5 + \cdots$$

$\{0, 11, 3\cdot 2^i, 5\cdot 7^i\}$

$G = \langle 11, 3, 2, 5, 7 \rangle \cup \{0\}$

$\sum a_n x^n \quad \exists r > 0 \quad a_n \neq 0 \quad \frac{a_{n+r}}{a_n} \in T \leftarrow$ finite set

$1 + x + 2x^2 + 3x^3 + 5x^4 + \cdots \quad \frac{a_{n+r}}{a_n} \to \rho^r \notin \mathbb{Q}$

# Berstel-Reutenauer theory

Let $R$ be a (commutative) integral domain. A noncommutative formal power series $S = \sum_{w \in X^*} S(w)w \in R\langle\langle X\rangle\rangle$ is *rational* if it can be obtained from noncommutative polynomials in $R\langle X\rangle$ by successive applications of addition, multiplication, and the star operation $S^* = (1 - S)^{-1} = \sum_{n \geq 0} S^n$ (if $S$ has zero constant coefficient).

6

**Ex** $X = \{x, y\}$

$$y \cdot \underline{(1 - \underline{xy})^{-1}} \cdot x$$

$$= y(1 + xy + xyxy + xyxyxy + \cdots)x$$

$$= yx + yxyx + \cdots$$

$$= yx(1 - yx)^{-1}$$

Recall that for univariate rational series the coefficients satisfy a linear recurrence relations. Schützenberger shows we can extend this to the noncommutative setting

The series $S$ is rational if and only if it has a linear representation, or, equivalently, is recognized by a weighted finite automaton.

# What do we mean by linear representation?

Specifically, we have a monoid homomorphism $\mu : X^* \to M_d(K)$, a row vector $u \in K^{1\times d}$, and a column vector $v \in K^{d\times 1}$ such that $S(w) = u \cdot \mu(w) \cdot v$ for all $w \in X^*$.

$1\times d \quad d\times d \quad d\times 1$

If you are familiar with $k$-regular series this is exactly the same thing when we take $X = \{0, 1, \ldots, k-1\}$.

Notation: We'll let $(u, \mu, v)$ denote this linear representation

$$\{ w \longmapsto u \cdot \mu(w) \cdot v \in K$$

$$X = \{x\}$$

$$\sum_{n \geq 0} S(x^n)\, x^n \in K[[x]]$$

$$\mu(x) = A$$

$$S(x^n) = u \cdot A^n \cdot v \qquad \mu(x^n) = A^n$$

$$A^d + c_{d-1} A^{d-1} + \cdots + c_1 A + c_0 I = 0$$

$$S(x^{n+d}) + \cdots + c_1 S(x^{n+1}) + c_0 S(x^n) = 0$$

A linear representation $(u, \mu, v)$ with $\mu : X^* \to M_d(K)$ is *minimal* if we cannot find an equivalent representation $(u', \mu', v')$ with $\mu' : X^* \to M_e(K)$ with $e < d$.

There is a graph theoretical way to view noncommutative rational series over a field $K$ via weighted automata.

A *weighted (finite) automaton* $\mathcal{A} = (Q, I, E, T)$ over the alphabet $X$ with weights in $K$ consists of a finite set of *states* $Q$ and three maps

initial                                             terminal

$$I : Q \to K, \quad E : Q \times X \times Q \to K, \quad T : Q \to K.$$

A triple $(p, x, q) \in Q \times X \times Q$ is an *edge* if $E(p, x, q) \neq 0$.

$q \xrightarrow{x} q'$    wt $= E(q, x, q')$

We say that there is an edge from $p$ to $q$ labeled by $x$ and with weight $E(p, x, q)$. A state $p \in Q$ is *initial* if $I(p) \neq 0$ and *terminal* if $T(p) \neq 0$.

A *path* is a sequence of edges

$p_0 \xrightarrow{x_1} p_1 \xrightarrow{x_2} \cdots \xrightarrow{x_l} p_l$

$$P = (p_0, x_1, p_1)(p_1, x_2, p_2) \cdots (p_{l-1}, x_l, p_l).$$

Its *weight* is $E(P) = \prod_{i=1}^{l} E(p_{i-1}, x_i, p_i)$ and its *label* is the word $x_1 \cdots x_l \in X^*$. The path is *accepting* if $p_0$ is an initial state and $p_l$ is a terminal state.

# Example

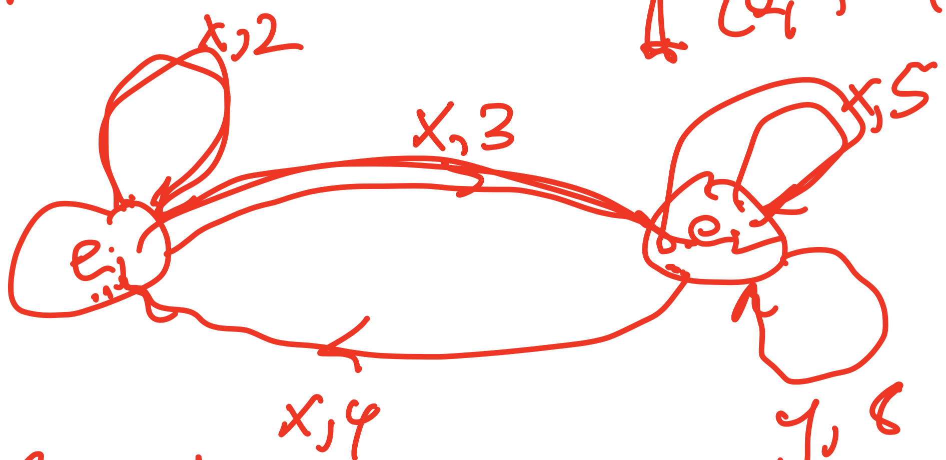
$u = [1 \ 0]$ $\quad v = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ $\quad X = \{x, y\}$

$\mu(x) = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$ $\quad \mu(y) = \begin{pmatrix} 0 & 0 \\ 0 & 8 \end{pmatrix}$

$Q = \{e_1, e_2\}$

$I(e_1) = 1$ $\quad I(e_2) = 0$

$T(e_1) = 1$ $\quad T(e_2) = 1$




$x^2$

$6 + 15 = 21$

$$U = \begin{bmatrix} I(e_1) & \cdots & I(e_n) \end{bmatrix}$$

$$V = \begin{bmatrix} T(e_1) \\ \vdots \\ T(e_n) \end{bmatrix}$$

$$\mu(x) = \left( E(e_i, x, e_j) \right)$$

# Unambiguous weighted automata

$$\sum_{w \in X^*} w(P)$$

## Definition

Let $\mathcal{A}$ be a weighted automaton. Then $\mathcal{A}$ is *unambiguous* if each $w \in X^*$ labels at most one accepting path. It is *deterministic* if

- there exists at most one initial state; and
- for each $(p, x) \in Q \times X$, there exists at most one $q \in Q$ with $E(p, x, q) \neq 0$.

# Example

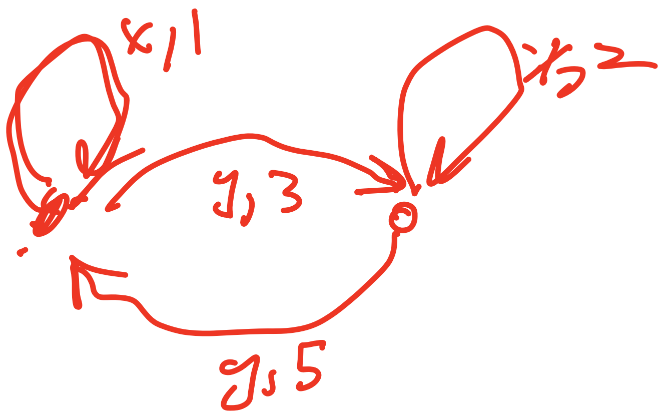
$X = \{x, y\}$

$u = [1 \;\; 1]$

$v = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

$\mu(x) = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ $\mu(y) = \begin{pmatrix} 0 & 3 \\ 5 & 0 \end{pmatrix}$

$u$




$xyx$

Reutenauer introduced the notion of noncommutative Pólya series.

A rational series $S \in R\langle\langle X \rangle\rangle$ is a *Pólya series* if its nonzero coefficients are contained in a finitely generated subgroup $G \leq K^{\times}$ of the quotient field $K$ of $R$.

$G \cup \{0\}$

Reutenauer also introduced the notion of an *unambiguous* rational series and conjectured that these should be precisely the rational Pólya series.

# Unambiguous Rational Series

A rational series is *unambiguous* if it can be obtained from noncommutative polynomials and the operations of addition, multiplication, and the star operation $S^* = (1 - S)^{-1} = \sum_{n \geq 0} S^n$ in such a way that, in these operations, one never forms a sum of two nonzero coefficients.

# Examples

''

<u>Ex</u> $X = \{x, y\}$

$$y(1-xy)^{-1}x + 2(1-yx)^{-1}$$

$$= yx + yxyx + yxyxyx + \cdots \qquad 2 + 2yx + 2yxyx + \cdots$$

$$= 2 + 3yx(1-yx)^{-1}$$ ← unambiguous

$X = \{x\}$

$$\frac{1}{1-\underline{2}x} + \frac{1}{1-\underline{3}x} + \sum_{j<i} \frac{\cancel{?}\,;}{1-\alpha x^i}$$

$$= 1 + 2x + 4x^2 + \cdots \quad + 1 + 3x + 9x^2 + \cdots$$

$$= \underline{2} + 5x + 13x^2 + \cdots$$

$\leftarrow$ not $\underline{\text{unambiguous}}$

$2^n + 3^n \quad \forall n \geq 1$

$$\frac{2^{n+1} + 3^{n+1}}{2^n + 3^n} \notin F$$

$\mathbb{Z}$ $\mathbb{F}_p[t]$, fields

## Theorem

*(B-Smertnig) Let $R$ be a completely integrally closed domain with quotient field $K$. Let $X$ be a finite non-empty set, and let $S \in R\langle\langle X\rangle\rangle$ be a rational series. Then the following statements are equivalent.*

1. *$S$ is a Pólya series.* $\Downarrow$ hard
2. *$S$ is recognized by an unambiguous weighted finite automaton with weights in $R$.* $\Updownarrow$
3. *$S$ is unambiguous (over $R$).*

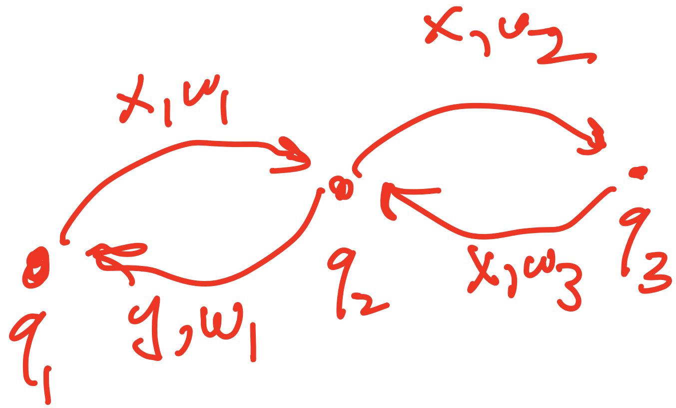
$2 \Leftrightarrow 3$ (Reutenauer)

$3 \Rightarrow 1$ (Not hard)

The 'hard' part of our theorem is showing $1 \Rightarrow 2$ in the case where $R = K$ is a field. (The other parts were already known!)

Notice that $(3) \implies (1)$ is more or less immediate.

$(2) \Rightarrow (1)$




$S(w) = \omega(P)$ or $\exists \leq 1$ path $P$ with label $w$

$\parallel$

$0$ ✓

$\omega(P) \in \langle \omega_1, \omega_2, \ldots, \omega_r \rangle$

f.g. group

# The Linear Hull

$$\phi : \underset{\text{group}}{G} \longrightarrow GL_n(\mathbb{C})$$

$$\phi(g) = \begin{pmatrix} A_1(g) & & & 0 \\ & \boxed{A_2(g)} & & \\ & & \ddots & \\ 0 & & & \boxed{A_d(g)} \end{pmatrix}$$

$$(u, \mu, v)$$

$$u = [1 \ 0 \ 0] \qquad \mu(x) = \begin{pmatrix} 2 & 3 & 0 \\ 1 & 4 & 0 \\ 0 & 0 & 5 \end{pmatrix} \qquad \mu(y) = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 2 & 0 \\ 0 & 0 & 8 \end{pmatrix}$$

$$v = \begin{bmatrix} 1 \\ 3 \\ 5 \end{bmatrix}$$

# Second Example

$u = [1\ 0]$ $\quad \mu(x) = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ $\quad \mu(y) = \begin{pmatrix} 0 & 3 \\ 5 & 0 \end{pmatrix}$

$\in \mathcal{F}(\mathbb{C}^2)$

$v = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

$u\,\mu(x) = [1\ 0]$

$\vdots$

$u\,\mu(y) = [0\ 3]$

$u\,\mu(y^2) = [15\ 0]$

$u\,\mu(x^2) = [1\ 0]$


$X^* = \underline{\{\text{even } \# y\text{'s}\}} \cup \underline{\{\text{odd } \# y\text{'s}\}}$

The linear hull captures the idea of breaking up the representation into these essential components.

To do this carefully, we introduce a topology and a related invariant of a linear representation

**Definition**

For a finite-dimensional vector space $V$, let $\mathcal{F}(V)$ be the collection of all subsets $Y \subseteq V$ of the form $Y = V_1 \cup \cdots \cup V_l$ with $l \in \mathbb{Z}_{\geq 0}$ and $V_i \subseteq V$ vector subspaces.

## Lemma

*Every finite-dimensional vector space $V$ has a noetherian topology for which $\mathcal{F}(V)$ is the collection of closed sets.*

The proof of this lemma is the same as the proof that the Zariski topology is a topology.

$C_1 \supseteq C_2 \supseteq C_3 \supseteq \cdots$

terminates

# Example

## Definition

Let $(u, \mu, v)$ be a linear representation over the field $K$, and let

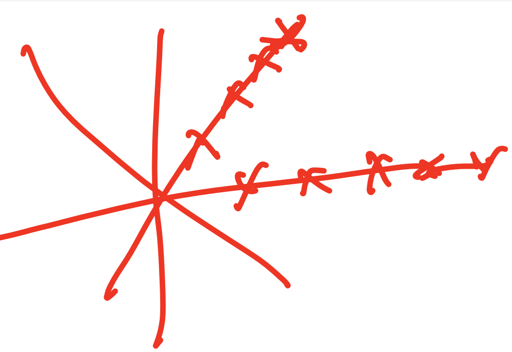
$$\Omega := u\mu(X^*) = \{\, u\mu(w) : w \in X^* \,\}$$

be the *(left) reachability set*. The closed set $\overline{\Omega}$ is the (*left*) *linear hull* of $(u, \mu, v)$. We can also define the right linear hull.

$\overline{\{u \cdot \mu(w) : w \in X^*\}}$

$1 \times d \quad d \times d$

$\overline{\{\mu(w) v : w \in X^*\}}$



# Example

$u = [1 \quad 0]$

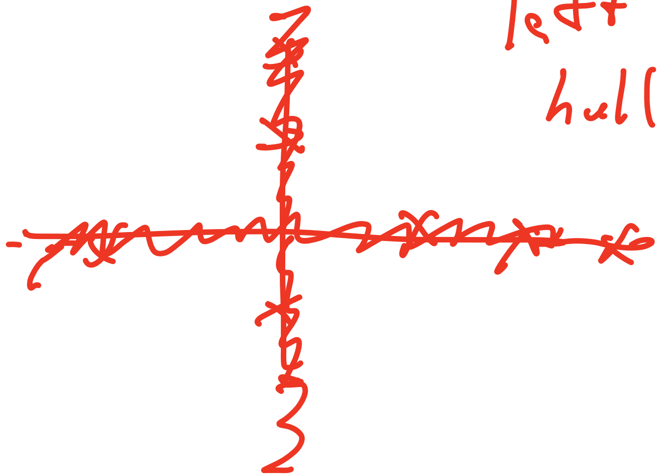
$X = \{x, y\}$

$\mu(x) = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$

$\mu(y) = \begin{bmatrix} 0 & 1 \\ 3 & 0 \end{bmatrix}$

$v = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

left linear hull



$u \cdot \mu(x) = [2 \quad 0]$

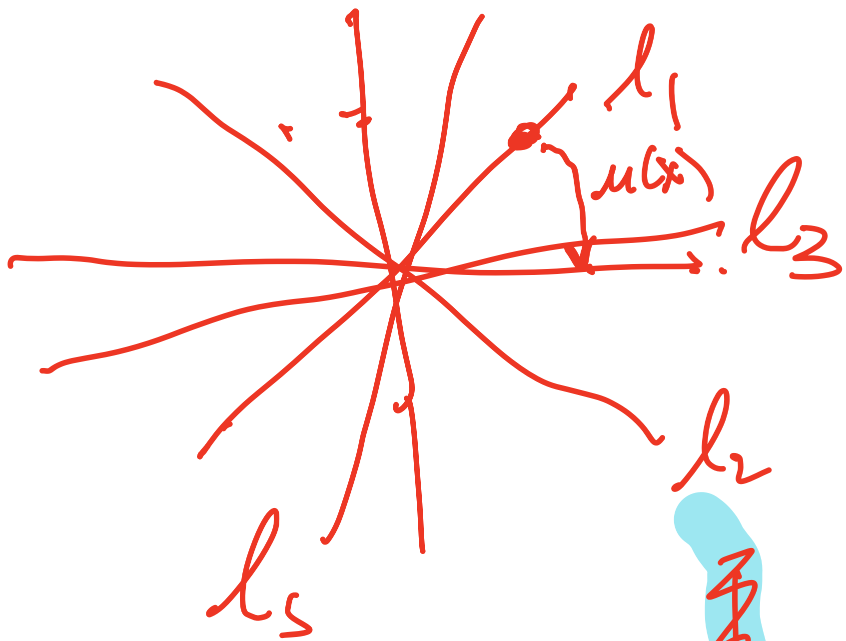
$u \cdot \mu(y) = [0 \quad 1]$

$\vdots$

$v = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ $\quad \mu(x)\, v = \begin{bmatrix} 2 \\ 3 \end{bmatrix}$ $\quad \mu(y) \cdot v = \begin{bmatrix} 1 \\ 3 \end{bmatrix}$

$$\mu(w)\cdot v = \begin{bmatrix} \neq 0 \\ \neq 0 \end{bmatrix}$$

right linear hull $= \mathbb{C}^2$

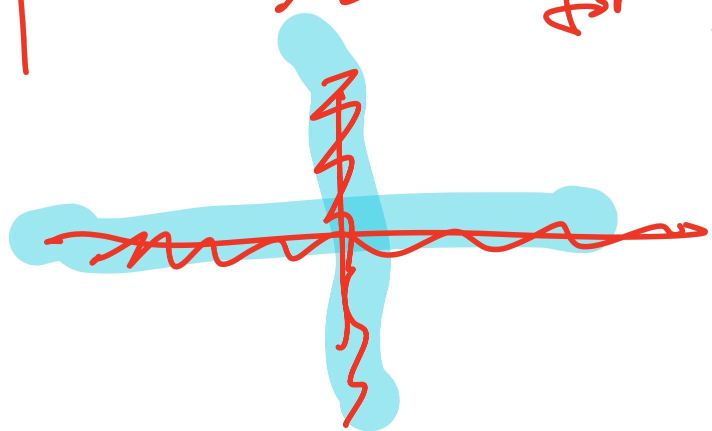



$$\mu(x)\cdot \ell_i = \ell_{\sigma(i)}$$

$$\mu(x^n)\,\ell_i = \ell_i$$

$\ell_i =$ eigenspace

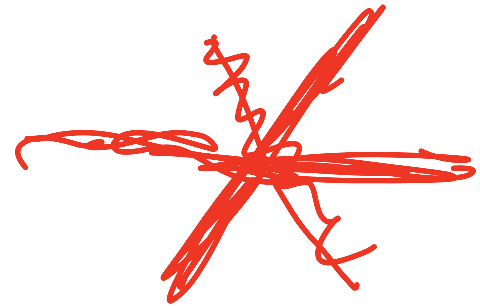
for $\mu(x^n) = \begin{pmatrix} 2^n & 0 \\ 0 & 3^n \end{pmatrix}$



Working with the linear hull allows us to break up the supports of noncommutative Pólya series into sets where the our linear representations are in some sense strongly irreducible.

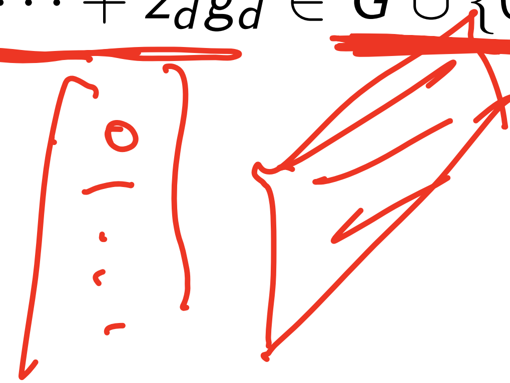
As it turns out, for Pólya series we can show we can always reduce to the case where the linear hull is made up of one-dimensional subspaces.

# Idea



We have a linear representation $(u, \mu, v)$. Once we are working in a component of the linear hull we can reduce further to the case where the vectors $u\mu(w)$ and $v$ have all of their coordinates in the group $G \cup \{0\}$ and $v$ has all nonzero coordinates.

Then suppose that $v = [g_1, \ldots, g_d]^T$. Then if $u\mu(w)v \in G \cup \{0\}$, we get an equation $z_1 g_1 + \cdots + z_d g_d \in G \cup \{0\}$ with the $z_i \in G \cup \{0\}$.



$u\mu(w) = [z_1 \ldots z_d]$

$v$

$G \cup \{0\}$

Now we use a big hammer.

### Theorem

*Let $G \leq K^*$ be a finitely generated multiplicative subgroup of a field $K$ of characteristic zero. Then there are only finitely many solutions to $z_1 + \cdots + z_d = 1$ with $(z_1, \ldots, z_d) \in G^d$ such that no non-trivial subsum of $z_1 + \cdots + z_d$ vanishes.*

Char = 0 ✓

$x + y = 1$

$K = \mathbb{F}_p(t)$

$(1+t)^{p^j} + (-1) \cdot t^{p^j} = 1$

$G = \langle 1+t, t, -1 \rangle$

$((1+t) \supset t)$

$1 + t^{p^j} + (-1) \cdot t^{p^j} = 1$

# Why is this relevant?

$z_1 g_1 + \dots + z_d g_d \in G \cup \{0\}$

Case 1: proper subsum vanishes

$z_{i_1} g_{i_1} + \dots + z_{i_r} g_{i_r} = 0$

reduce to no proper subsum vanishing

reduce linear hull $(z_1, \dots, z_d)$

$z_1 g_1 + \dots + z_d g_d = 0$

$= g \in G$

$g$

linear hull = union of lines

$\mu: X^* \to M_1(K) = K$

$u, v \in K$

$u \cdot \mu(w) v = u \cdot \mu(x_{i_1}) \cdots \mu(x_{i_\ell}) v \in K^* \cup \{0\}$

In positive characteristic we do not have the strong $S$-unit theorem, but Derksen and Masser have a version, which when combined with careful height estimates is enough to handle the positive characteristic case.

As it turns out, we are able to give an algorithm to compute the linear hull of a linear representation $(u, \mu, v)$. In particular, we can use this to show that the question of whether a weighted automaton is equivalent to an unambiguous weighted automaton is decidable.

$\langle \lambda_1, \dots, \lambda_s \rangle \in K^*$

$S(w) = \lambda_1^{a_1(w)} \cdots \lambda_s^{a_s(w)}$

$a_i(w) \in \mathbb{Z}$ linearly bounded

$\sum a_i(w)\, w$ rational series

Thanks!