Course Notes

Selected Topics in Computational Mathematics: Weighted Finite Automata and Noncommutative Rational Series

Daniel Smertnig

Winter Term 2024/25
University of Ljubljana

for the 2nd cycle (master's students), 3h/week

made available online: 17.5.2026

WFA & Nc rational series

↑ weighted (finite) automata

0. Introduction

- WFA are a simple computational model, computing functions

$$f: A^* \longrightarrow K \quad \text{↩ semiring}$$

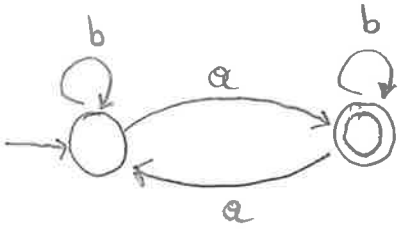
↑ words on alphabet A

- Many questions on WFA are on the boundary of decidability/undecidability; in the case where K is a field (e.g. $K=\mathbb{Q}$) there are connections to number theory
- WFA generalize: finite automata & linear recurrence sequences (LRS)

related to: probabilistic automata, quantum automata

Finite automata (= finite state machine)

E.g. $A=\{a,b\}$



- Accepts a word w, if the number of "a"s in w is odd.

- Language: subset of A^*
- Languages recognized by F.A. are precisely the regular languages ($\emptyset$, singletons $\{a\}$ with $a \in A$, and everything constructed from the with union $(L_1 \cup L_2)$, concatenation $(L_1 \cdot L_2 = \{w_1 w_2 : w_i \in L_i\})$

Kleene star $L^* = \bigcup_{n \geq 0} L^n = \{w_1 \cdots w_n : n \geq 0,\ w_i \in L\}$

⇝ F.A. $\triangleq$ WFA over Boolean semiring $\mathbb{B}=\{0,1\}$

↑ $1+1=1$

LRS ($/\mathbb{Q}$): $a_0, \dots, a_{m-1} \in \mathbb{Q}$, $\lambda_1, \dots, \lambda_m \in \mathbb{Q}$

$$\forall n \geq m: \quad a_n = \sum_{i=1}^{m} \lambda_i a_{n-i}$$

E.g. Fibonacci numbers: $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$. $\forall n \geq 2$.

$\rightsquigarrow$ LRS $\hat{=}$ WFA over $\mathbb{Q}$ on a single-letter alphabet $A = \{x\}$ (input x^n $\rightsquigarrow$ output a_n).

1. WFA, Linear Representations, Rational Series [→ Berstel, Reutenauer Ch. 1]

Def. A semiring is a set K with binary operations $+, \cdot$ and elements $0, 1 \in K$ s.t.

(1) $(K, +, 0)$ is a commutative monoid

(2) $(K, \cdot, 1)$ is a monoid

(3) $\forall a, b, c \in K$: $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$

(4) $\forall a \in K$: $0 \cdot a = 0 = a \cdot 0$

A semiring K is commutative if $(K, \cdot)$ is commutative (mostly we will deal with these). $K' \subseteq K$ is a subsemiring if $0, 1 \in K'$ and K' is closed wrt. $+, \cdot$. A semiring (homo)morphism of semirings K, K' is a map $f: K \to K'$ that respects $0, 1, +, \cdot$.

Exm:
- Rings
- $(\mathbb{N}_0, +, \cdot)$ (no subtraction)
- $(\mathbb{Z} \cup \{-\infty\}, \max, +)$, $(\mathbb{Z} \cup \{+\infty\}, \min, +)$ or with $\mathbb{N}_0, \mathbb{Q}, \mathbb{R}, \mathbb{R}_{\geq 0}, \dots$ instead of $\mathbb{Z}$: (Tropical semirings)
- $\mathbb{B} = \{0, 1\}$ with $1 + 1 = 1$ Boolean semiring

- Let $(M, \cdot, 1)$ be a monoid, $\mathcal{P}(M) = \{X : X \subseteq M\}$ powerset

With $X \cdot Y := \{xy : x \in X, y \in Y\}$ as multiplication,
$X \cup Y$ as addition, $\mathcal{P}(M)$ is a semiring

- Nc polynomials, nc series — A an alphabet (nonempty, finite set)

A (formal) series S is a function $A^* \to K$ (A^* = free monoid)

we write (S, w) for the image of w under S

((S, w) .. coefficient of w)

$$(S+T, w) = (S, w) + (T, w), \qquad (ST, w) = \sum_{\substack{x,y \in A^* \\ w = xy}} (S, x)(T, y)$$

(finite sum)

Notation: $S = \sum_{w \in A^*} (S, w) w$

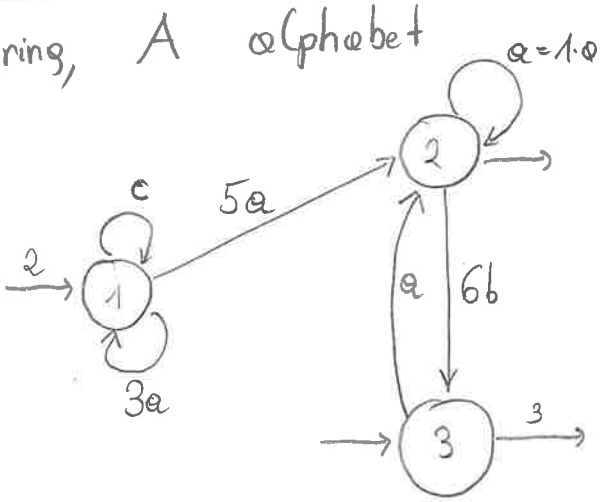
$$\mathrm{supp}(S) = \{w \in A^* : (S, w) \neq 0\}$$

$K\langle\langle A \rangle\rangle$ ... semiring of nc series

$K\langle A \rangle$ ... subsemiring of nc polynomials ($\mathrm{supp}(S)$ finite)

1.1 WFA

K semiring, A alphabet



(*)

Def: (1) A weighted (finite) automaton (= WFA, = WA, = K-automaton) with weights in K is a tuple (Q, I, E, T) consisting of a finite set Q of states, and maps

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

(initial weights) (transition function) (terminal weights)

(2) A triple (p, a, q) with $E(p, a, q) \neq 0$ is an edge (= transition) with label a, start state p, end state q, weight $E(p, a, q) \in K$

(3) A path (= run) is a sequence of edges

$$c = (q_0, a_1, q_1)(q_1, a_2, q_2) \cdots (q_{n-1}, a_n, q_n),$$

its weight is $E(c) = E(q_0, a_1, q_1) E(q_1, a_2, q_2) \cdots E(q_{n-1}, a_n, q_n)$

its label is $w = a_1 a_2 \cdots a_n \in A^*$

(4) The behaviour of $\mathcal{A}$ is the nc series $[\![\mathcal{A}]\!] \in K\langle\langle A \rangle\rangle$ defined by

$$([\![\mathcal{A}]\!], w) = \sum_{q_0, \ldots, q_n \in Q} I(q_0) E(q_0, a_1, q_1) \cdots E(q_{n-1}, a_n, q_n) T(q_n)$$

$w = a_1 \cdots a_n, \ a_i \in A$

Terminology:

- A state q is initial if $I(q) \neq 0$, terminal if $T(q) \neq 0$.
- A successful run (= accepting path) is a run from an initial to a terminal state

Computational interpretation: Given $w \in A^*$, compute $([\![\mathcal{A}]\!], w)$ by

- finding all successful runs for w
- for each such run, take the product over weights (incl. $I(q_0), T(q_n)$)

• sum up all those values

Exm: (1) $A=\{a,b\}$, $K=\mathbb{Q}$, $Q=\{1,2\}$

$I(1)=1$, $I(2)=0$

$T(1)=0$, $T(2)=1$

$E(1,a,1)=1$, $E(1,b,1)=1$

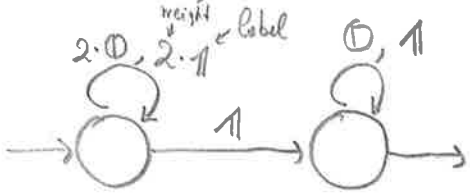
$E(1,a,2)=1$, $E(1,b,2)=0$

$E(2,a,2)=1$, $E(2,b,2)=1$

w	1 (empty word)	a	b	aa	ab	ba	bb	
$(\mathbb{A}, w)$	0	1	0	1+1 = 2	1	1	0	...

$(\mathbb{A}, w)$ = # of „a"s in w

(2) $A=\{\textcircled{0}, \textcircled{1}\}$



$\mathcal{B}$

w	1	0	1	00	01	10	11	001
	0	0	1	0	2	1	2+1 = 3	4

output: $[\![\mathcal{B}]\!](b_0 \dots b_n) = \bar{b}_0 + 2\bar{b}_1 + 4\bar{b}_2 + \dots + 2^{n-1}\bar{b}_n$ with $\bar{0}=0$, $\bar{1}=1$

i.e., number with binary digits $(b_0 \dots b_n)$ (b_0: LSB, b_n: MSB)

Exc: Create a WFA that reads MSB first (also possible with 2 states)

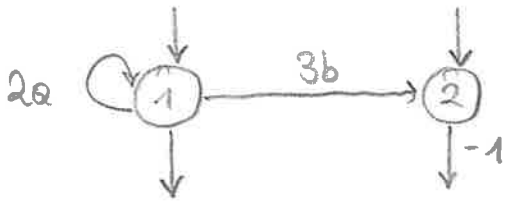
(3) Same WFA as in (1) but with $K = \mathbb{B}$

Output: $\begin{cases} 1 & \text{if } w \text{ contains } a \\ 0 & \text{otherwise} \end{cases}$

$\hat{=}$ unweighted automaton

Remark: finite (unweighted) automata $\hat{=}$ $\mathbb{B}$-automata
(output $= 1 \Leftrightarrow \exists$ successful run).

(4) $K = \mathbb{Z}$



$$[\![A]\!] = \sum_{n \geq 1} 2^n a^n - 3 \sum_{n \geq 0} 2^n a^n b$$

1.2 Linear repr. / Recognizable series

K semiring, A alphabet.

Can also represent the data in (*) using adjacency matrices:

$\lambda = (2, 0, 1)$ initial weights, $\gamma = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$

$$\mu(a) = \begin{pmatrix} 3 & 5 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{matrix} 1 \to \\ 2 \to \\ 3 \to \end{matrix} \qquad \mu(b) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix} \qquad \mu(c) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Def (1) A series $S \in K\langle\langle A \rangle\rangle$ is (K-)recognizable if $\exists n \geq 0$, $\lambda \in K^{1 \times n}$, $\gamma \in K^{n \times 1}$, and a monoid morphism $A^* \to K^{n \times n}$ s.t.

$$\forall w \in A^* : (S, w) = \lambda \mu(w) \gamma$$

(2) The triple (λ, μ, γ) is a linear representation of S, n is its dimension.

Proposition 1.1 $S \in K\langle\langle A \rangle\rangle$ is recognizable $\Leftrightarrow \exists$ WFA $\mathcal{A}$ s.t. $S = [\![\mathcal{A}]\!]$

Proof: „$\Leftarrow$": Suppose $S = [\![\mathcal{A}]\!]$ with $\mathcal{A} = (Q, I, E, T)$

W.l.o.g $Q = \{1, \dots, n\}$.

Define: $\lambda = (I(1), \dots, I(n))$, $\gamma = \begin{pmatrix} T(1) \\ \vdots \\ T(n) \end{pmatrix}$,

$\forall a \in A$: $\mu(a) = \begin{pmatrix} E(1,a,1) & \dots & E(1,a,n) \\ \vdots & & \\ E(n,a,1) & \dots & E(n,a,n) \end{pmatrix}$, extends to morphism $\mu: A^* \to K^{n \times n}$ by $\mu(a_1 \cdots a_m) = \mu(a_1) \cdots \mu(a_m)$

Then, for $p, q \in Q$, $w = a_1 \cdots a_m$,

$$\mu(w)_{p,q} = (\mu(a_1) \cdot \ldots \cdot \mu(a_m))_{p,q} = \sum_{p_1, \dots, p_{m-1} = 1}^{n} \mu(a_1)_{p p_1} \mu(a_2)_{p_1 p_2} \cdots \mu(a_m)_{p_{m-1} q},$$

and

$$\lambda \mu(w) \gamma = \sum_{p, p_1, \dots, p_{m-1}, q = 1}^{n} \lambda_p \mu(a_1)_{p p_1} \mu(a_2)_{p_1 p_2} \cdots \mu(a_m)_{p_{m-1} q} \gamma_q$$

$$= \sum_{p, p_1, \dots, p_{m-1}, q = 1}^{n} I(p) E(p, a_1, p_1) E(p_1, a_2, p_2) \cdots E(p_{m-1}, a_m, q) T(q)$$

$$= (\![\mathcal{A}]\!, w)$$

„$\Rightarrow$": Let (λ, μ, γ) be a lin repr. recognizing S.

Set $Q = \{1, \dots, n\}$, $I(p) := \lambda_p$, $T(q) := \gamma_q$,

$E(p, a, q) := \mu(a)_{pq}$ $(p, q \in Q, a \in A)$.

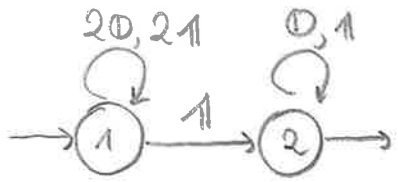
Same computation as in „$\Leftarrow$" shows that S is the behaviour of $\mathcal{A} = (Q, I, E, T)$. □

Cor: There is a bijection

$$\left\{ \frac{\text{WFA}}{\text{renaming of states}} \right\} \longleftrightarrow \left\{ \frac{\text{Linear representation}}{\text{permutation of standard basis vectors}} \right\}$$

Remark Permuting the standard basis vectors changes (λ, μ, γ) into $(\lambda P^{-1}, P\mu P^{-1}, P\gamma)$ via P a permutation matrix (observe $P\mu(w)P^{-1} = (P\mu(a_1)P^{-1})(P\mu(a_2)P^{-1}) \cdots (P\mu(a_m)P^{-1})$ if $w = a_1 \cdots a_m$)

Exm:



corresponds to

$$\lambda = (1,0), \quad \gamma = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \mu(\mathbb{D}) = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad \mu(\mathbb{I}) = \begin{pmatrix} 2 & 1 \\ & 1 \end{pmatrix}$$

Computational Interpretation:

- We have n registers, each holding a value in K
- λ is the initial state of the registers
- Reading the letters of w (left to right), we make linear updates of the registers
- At the end we output a linear combination of the register values (defined by γ)

Remark (left/right symmetry) We could also think of γ as initial state, reading letters right to left;

Transposition of matrices reduces one POV to the other:

$$\lambda\mu(a_1)\cdots\mu(a_m)\gamma = \gamma^T\mu(a_m)^T\cdots\mu(a_1)^T\lambda^T.$$

1.3 Module-theoretic Characterization

K semiring, A alphabet

A **left K-module** is a commutative monoid $(M, +, 0)$ together with a map $K \times M \to M$, $(k, x) \mapsto kx$ (scalar multiplication) s.t. $\forall k, \ell \in K \; \forall x, y \in M$:

$$k(x+y) = kx + ky, \quad (k+\ell)x = kx + \ell x,$$
$$k(\ell x) = (k\ell)x, \quad 1x = x$$
$$0x = 0, \quad k0 = 0 \quad \text{[new!]}$$

Submodule: submonoid closed under scalar mult.

$K\langle\langle A^* \rangle\rangle$ is a K-module with $(kS; w) := kS(w)$

Def: For $x \in A^*$, $S \in K\langle\langle A^* \rangle\rangle$ the **left quotient** (of S by x) is

$$x^{-1}S := \sum_{w \in A^*} (S, xw)\, w \qquad (\Leftrightarrow (x^{-1}S, w) = (S, xw) \; \forall x, w \in A^*)$$

Lemma

(1) For each $x \in A^*$, the map $S \mapsto x^{-1}S$ is a **K-module morphism**

(i.e. $x^{-1}(S+T) = x^{-1}S + x^{-1}T$, $x^{-1}(kS) = k(x^{-1}S)$, $x^{-1}0 = 0$ $\forall S, T \in K\langle\langle A^* \rangle\rangle, k \in K$)

(2) $\forall x, y \in A^* \; \forall S \in K\langle\langle A^* \rangle\rangle$: $(xy)^{-1}S = y^{-1}(x^{-1}S)$

Exm: $(ab)^{-1}\left(a^2 - b^2 + 2aba^2 + 5ab + 3baab + 7abbab\right)$

$$= 2a^2 + 5 + 7ab.$$

Def. $M \subseteq K\langle\langle A\rangle\rangle$ is stable if

$\forall S \in M \; \forall x \in A^* : \; x^{-1}S \in M$

$(\Leftrightarrow \; \forall a \in A : \; a^{-1}M \subseteq M)$

Thm 1.2 $S \in K\langle\langle A\rangle\rangle$ is recognizable $\Leftrightarrow$ stable f.g. left submodule $M \subseteq K\langle\langle A\rangle\rangle$ s.t. $S \in M$.

Proof „$\Rightarrow$" Let (λ, μ, γ) be a lin. repr of dimension n s.t. $(S,w) = \lambda\mu(w)\gamma \quad \forall w \in A^*$.

For $i = 1, \dots, n$ let $S_i := (\mu(w)\gamma)_i = e_i^T \mu(w)\gamma$. ($e_i^T$: standard basis vector)

Let $M = {}_K\langle S_1, \dots, S_n\rangle \in K\langle\langle A\rangle\rangle$.

$\rightarrow (S,w) = \sum_{i=1}^{n} \lambda_i (\mu(w)\gamma)_i$, so $S = \sum_{i=1}^{n} \lambda_i S_i$

M is stable: Let $x \in A^*$. Since $T \mapsto x^{-1}T$ is K-linear, it suffices to show $x^{-1}S_1, \dots, x^{-1}S_n \in M$.

$$(x^{-1}S_i, w) = (S_i, xw) = (\mu(xw)\gamma)_i = (\mu(x)\cdot\mu(w)\gamma)_i$$

$$= \sum_{j=1}^{n} \mu(x)_{ij} (\mu(w)\gamma)_j = \sum_{j=1}^{n} \mu(x)_{ij} (S_j, w)$$

$$\Rightarrow x^{-1}S_i = \sum_{j=1}^{n} \mu(x)_{ij} S_j \in M.$$

„$\Leftarrow$": Let $M \subseteq K\langle\langle A\rangle\rangle$ be a stable f.g. K-module containing S. Suppose $M = \langle S_1, \dots, S_n\rangle$, $S = \sum_{i=1}^{n} \lambda_i S_i$ $(\lambda_i \in K)$.

Let $a \in A$. Since $a^{-1}S_i \in M$ (stability), $\exists \mu(a) \in K^{n\times n}$: $a^{-1}S_i = \sum_{j=1}^{n} \mu(a)_{ij} S_j$.

Def. $M \subseteq K\langle\langle A\rangle\rangle$ is stable if

$\forall S \in M \; \forall x \in A^* : \; x^{-1}S \in M$

$(\Leftrightarrow \; \forall a \in A : \; a^{-1}M \subseteq M)$

Thm 1.2 $S \in K\langle\langle A\rangle\rangle$ is recognizable $\Leftrightarrow$

$\exists$ stable f.g. left submodule $M \subseteq K\langle\langle A\rangle\rangle$ s.t. $S \in M$.

Proof: „$\Rightarrow$" Let (λ, μ, γ) be a lin. repr of dimension n

s.t. $(S,w) = \lambda\mu(w)\gamma \quad \forall w \in A^*$.

(e_i^T: standard basis vector)

For $i = 1, \dots, n$ let $(S_i, w) = (\mu(w)\gamma)_i = e_i^T \mu(w)\gamma$.

Let $M = {}_K\langle S_1, \dots, S_n\rangle \subseteq K\langle\langle A\rangle\rangle$.

$\rightarrow (S,w) = \sum_{i=1}^{n} \lambda_i (\mu(w)\gamma)_i$, so $S = \sum_{i=1}^{n} \lambda_i S_i$

M is stable: Let $x \in A^*$. Since $T \mapsto x^{-1}T$ is K-linear,

it suffices to show $x^{-1}S_1, \dots, x^{-1}S_n \in M$.

$$(x^{-1}S_i, w) = (S_i, xw) = (\mu(xw)\gamma)_i = (\mu(x)\cdot\mu(w)\gamma)_i$$

$$= \sum_{j=1}^{n} \mu(x)_{ij} (\mu(w)\gamma)_j = \sum_{j=1}^{n} \mu(x)_{ij} (S_j, w) \quad \forall w \in A^*$$

$$\Rightarrow x^{-1}S_i = \sum_{j=1}^{n} \mu(x)_{ij} S_j \in M.$$

„$\Leftarrow$": Let $M \subseteq K\langle\langle A\rangle\rangle$ be a stable f.g. K-module containing

S. Suppose $M = \langle S_1, \dots, S_n\rangle$, $S = \sum_{i=1}^{n} \lambda_i S_i$ $(\lambda_i \in K)$.

Let $a \in A$. Since $a^{-1}S_i \in M$ (stability),

$\exists \mu(a) \in K^{n\times n}$: $a^{-1}S_i = \sum_{j=1}^{n} \mu(a)_{ij} S_j$.

μ extends to a monoid morphism $\mu: A^* \to K^{d\times d}$

Claim: $w^{-1} S_i = \sum_{j=1}^{n} \mu(w)_{ij} S_j$

Proof by induction on $|w|$, $w = 1$ ✓

$$(wa)^{-1} S_i = a^{-1} w^{-1} S_i \overset{(IH)}{=} a^{-1} \left(\sum_{j=1}^{n} \mu(w)_{ij} S_j \right) =$$

$$= \sum_{j=1}^{n} \mu(w)_{ij} a^{-1} S_j = \sum_{j=1}^{n} \mu(w)_{ij} \sum_{k=1}^{n} \mu(a)_{jk} S_k$$

$$= \sum_{j,k=1}^{n} \mu(w)_{ij} \mu(a)_{jk} S_k = \sum_{k=1}^{n} \mu(wa)_{ik} S_k \qquad (**)$$

Set $g := \begin{pmatrix} (S_1, 1) \\ \vdots \\ (S_n, 1) \end{pmatrix}$

$$\Rightarrow \quad (\mu(w)\, g)_i = \sum_{j=1}^{n} \mu(w)_{ij} g_j = \sum_{j=1}^{n} \mu(w)_{ij} (S_j, 1)$$

$$= \left(\sum_{j=1}^{n} \mu(w)_{ij} S_j , 1 \right) \overset{(**)}{=} (w^{-1} S_i, 1) = (S_i, w)$$

$$\Rightarrow \quad \lambda\, \mu(w)\, g = \sum_{i=1}^{n} \lambda_i (S_i, w) = (S, w) \qquad \square$$

✱ Exm: $A = \{0, 1\}$, (S, w) is binary number represented by w (LSB on left).

$$S = 1 + 2 \cdot 01 + 10 + 3 \cdot 11 + \dots$$

$$\Rightarrow \quad (0^{-1} S, w) = (S, 0w) = 2 \cdot (S, w)$$

$$(1^{-1} S, w) = (S, 1w) = 1 + 2 \cdot (S, w)$$

$$\Rightarrow \quad 1^{-1} S = T + 2 \cdot S \quad \text{with} \quad T(w) = 1 \quad \forall w \in A^*$$

Since $\mathbb{Q}^{-1}T = T$, $\mathbb{Q}^{2}T = T$, $\mathbb{Q}\langle S, T\rangle \leq \mathbb{Q}\langle\langle A\rangle\rangle$ is stable

$\mathbb{Q}$-vector space

$\Rightarrow$ S is recognizable.

Cor 1.3: Left and right K-linear combinations of K-recognizable series are K-recognizable

Proof Let $k \in K$, $S, T \in K\langle\langle A\rangle\rangle$ K-recognizable.

Suffices to show: (i) kS, Sk are K-recognizable

(ii) $S+T$ is K-recognizable

(i) Let ${}_KM \leq K\langle\langle A\rangle\rangle$ be f.g. stable with $S \in M$.

$kM \subseteq M \Rightarrow kS$ K-recognizable

$Mk = \{S'k : S' \in M\}$ is stable f.g. left K-module

$\Rightarrow Sk$ K-recognizable.

(ii) ${}_KM, {}_KN \leq K\langle\langle A\rangle\rangle$ f.g. stable, $S \in M$, $T \in N$

$\Rightarrow S+T \in M+N = \{S'+T' : S' \in M, T' \in N\}$

$\uparrow$ f.g., stable (suffices to check on generators) $\square$

Alternatively: using linear representations:

S recognized by (λ, μ, γ), T by $(\lambda', \mu', \gamma')$

$\Rightarrow kS \hookleftarrow (k\lambda, \mu, \gamma)$, $Sk \hookleftarrow (\lambda, \mu, \gamma k)$

$S+T \hookleftarrow \left((\lambda\ \lambda'), \begin{pmatrix} \mu & \\ & \mu' \end{pmatrix}, \begin{pmatrix} \gamma \\ \gamma' \end{pmatrix}\right)$

Def: The Hadamard product of $S, T \in K\langle\langle A \rangle\rangle$, denoted $S \odot T$ is defined by.

$$(S \odot T, w) = (S, w)(T, w)$$

Thm 1.4 (Schützenberger) Let $K_1, K_2 \leq K$ be subsemirings s.t. $k_1 k_2 = k_2 k_1 \ \forall k_i \in K_i$.
If S_i is K_i-recognizable, then $S_1 \odot S_2$ is K-recognizable.

Proof: Let $M_i \leq_{K_i} K_i\langle\langle A \rangle\rangle$ be stable K_i-f.g. s.t. $S_i \in M_i$.
Let $M \leq_K K\langle\langle A \rangle\rangle$ be generated by $\{T_1 \odot T_2 : T_1 \in M_1, T_2 \in M_2\}$
$\Rightarrow S_1 \odot S_2 \in M$

M is f.g: Let $U_1, \dots, U_m \in M_1$, $V_1, \dots, V_n \in M_2$ s.t. they generate the respective module.
Let $T_i \in M_i$,

$$T_1 = \sum_{i=1}^{m} k_i U_i \quad (k_i \in K_1), \quad T_2 = \sum_{j=1}^{n} \ell_j V_j \quad (\ell_j \in K_2)$$

$$(T_1 \odot T_2, w) = \left(\sum_{i=1}^{m} k_i (U_i, w)\right)\left(\sum_{j=1}^{n} \ell_j (V_j, w)\right)$$

$$= \sum_{i,j} k_i \underbrace{(U_i, w)}_{\in K_1} \underbrace{\ell_j}_{\in K_2} (V_j, w) = \sum_{i,j} k_i \ell_j (U_i, w)(V_j, w)$$

$$= \sum_{i,j} k_i \ell_j (U_i \odot V_j, w)$$

M is stable: $x \in A^*$, $T_1 \in M_1$, $T_2 \in M_2$

$$\Rightarrow (x^{-1}(T_1 \odot T_2), w) = (T_1 \odot T_2, xw) = T_1(xw)\, T_2(x, w)$$

$$= (x^{-1} T_1, w) \cdot (x^{-1} T_2, w)$$

$$\Rightarrow x^{-1}(T_1 \odot T_2) = x^{-1} T_1 \odot x^{-1} T_2$$

□

W.l.o.g. $K = \mathbb{N}_0$ (or $K = \mathbb{Q}$)

Exm: For $w \in A^*$, $a \in A$ let $|w|_a :=$ # of „a"s in w.

We saw $S_a = \sum_{w \in A^*} |w|_a w$ is K-recognizable.

$\Rightarrow S_a^{\odot n} = \underbrace{S_a \odot \dots \odot S_a}_{n \text{ times}} = \sum_{w \in A^*} |w|_a^n w$ is K-recognizable. (Thm 1.4)

$\Rightarrow S_{a_1}^{\odot n_1} \odot \dots \odot S_{a_e}^{\odot n_e} = \sum_{w \in A^*} |w|_{a_1}^{n_1} \cdots |w|_{a_e}^{n_e} w$ is K-recognizable (Thm 1.4)

Cor 1.3 $\Rightarrow$ If $A = \{a_1, \dots, a_e\}$ and $P \in K[X_1, \dots, X_e]$ is a (commutative) polynomial, then

$$\sum_{w \in A^*} P(|w|_{a_1}, \dots, |w|_{a_e})\, w \text{ is } K\text{-recognizable.}$$

Let $S \in K\langle\langle A \rangle\rangle$. Then $M := {}_K\langle \{ x^{-1}S : x \in A^* \} \rangle$ is the smallest stable module containing S.

Careful: Even if S is recognizable, M may not be f.g.! It is only a submodule of a f.g. stable module.

Prop 1.5 Let K be a finite semiring or a commutative ring.

Then $S \in K\langle\langle A \rangle\rangle$ is recognizable
$\Leftrightarrow M := {}_K\langle \{ x^{-1}S : x \in A^* \} \rangle$ is f.g.

In particular, we can then choose generators of the form $x_1^{-1}S, \dots, x_n^{-1}S$.

Proof: „$\Leftarrow$": Theorem 1.2

„$\Rightarrow$" K finite: Let $N \leq_K K\langle\langle A \rangle\rangle$ be f.g. stable with $S \in N$

$\Rightarrow S \in M \subseteq N$.

N f.g. + K finite $\Rightarrow N$ finite $\Rightarrow M$ finite $\Rightarrow M$ f.g.

K commutative ring: Let (λ, μ, γ) be a linear representation for S.

Let $R \subseteq K$ be the subring generated by entries of λ, γ, $\mu(a)$, $a \in A$. Then R is finitely generated and $\mu(w) \in R^{d \times d}$ for all $w \in A^*$.

$\Rightarrow S$ is R-recognizable $\overset{(1.2)}{\Rightarrow} \exists$ f.g. stable $N \leq_R R\langle\langle A \rangle\rangle$ s.t. $S \subseteq N$.

Since R is f.g. & commutative it is noetherian

[$\exists$ ring epimorphism $\mathbb{Z}[X_1, \dots, X_N] \twoheadrightarrow R$, $\mathbb{Z}[X_1, \dots, X_N]$ is noetherian by Hilbert's basis theorem, & quotients of noetherian rings are noetherian]

$\Rightarrow {}_R\langle \{ x^{-1}S : x \in A^* \} \rangle \leq N$ is f.g. as R-module.

$\Rightarrow M = {}_K\langle \{ \overleftarrow{x} S : x \in A^* \} \rangle$ is f.g. as K-module

---

„In particular": Suppose M is f.g. by $T_1, \dots, T_n$

$\Rightarrow T_i = \sum_{j=1}^{m_i} k_j \left(\overleftarrow{x_{ij}} S \right)$ with $k_j \in K$, $x_{ij} \in A^*$

$\Rightarrow \{ \overleftarrow{x_{ij}} S : 1 \le i \le n,\ 1 \le j \le m_i \}$ generate M. $\square$

1.4 Rational Series

K semiring, A alphabet

$S \in K\langle\langle A \rangle\rangle$ is proper if $(S, 1) = 0$ (constant term is 0)

Def: For proper $S \in K\langle\langle A \rangle\rangle$, let

$$S^* := \sum_{n \ge 0} S^n = 1 + S + S^2 + \dots, \quad S^+ = \sum_{n \ge 1} S^n$$

Makes sense, because in S^n all words w with $|w| < n$ have coefficient zero, so

$$(S^*, w) = \sum_{m=0}^{n} (S^m, w) \quad \text{for all } w \text{ with } |w| \le n$$

is a finite sum.

Lemma 1.6

(1) If K is a ring, and S is proper, then $S^* = (1 - S)^{-1}$

(2) If $U, V \in K\langle\langle A \rangle\rangle$ and V is proper, then

$S := V^* U$ is the unique solution of $S = U + VS$,

$S' := UV^*$ ——— " ——— $S' = U + S'V$.

Proof: (1) $S^*S = S^+ = S^* - 1$

$\Rightarrow S^*(S-1) = -1 \Rightarrow S^*(1-S) = 1$

and similarly $(1-S)S^* = 1$.

(2) We show this for S.

S is a solution: $U + \underbrace{V^*V}_{=V^+}U = U + V^+U = \underbrace{(1+V^+)}_{=V^*}U = V^*U.$

Uniqueness: Suppose $T = U + VT$

$\Rightarrow T = U + V(U+VT) = U + VU + V^2T = U + VU + V^2(U+VT)$

$= U + VU + V^2U + V^3T$

$\overset{\text{induction}}{=} U + VU + V^2U + \dots + V^nU + V^{n+1}T$

Since V is proper, $\operatorname{supp}(V^{n+1}T)$ only contains words w with $|w| \geq n+1$.

$\Rightarrow (T,w) = \left(\left(\sum_{i=0}^{n} V^i\right)U, w\right)$ whenever $|w| \leq n$.

$\Rightarrow T = V^*U = S.$ □

Definition The smallest subset of $K\langle\langle A\rangle\rangle$ that contains $K\langle A\rangle$ (polynomials), and is closed under products, left and right K-linear combinations, and the star operation (in proper sense) is called the Semiring of **K-rational series**.

Remark (1) If K is a ring, then $S \in K\langle\langle A\rangle\rangle^{\times}$ ($\times$ = invertible)
$\Leftrightarrow (S,1) \in K^{\times}$.

Then the ring of rational series is the smallest subring of $K\langle\langle A\rangle\rangle$ that contains $K\langle A\rangle$ and is closed under inversion (i.e. whenever S has an inverse in $K\langle\langle A\rangle\rangle$, then S^{-1} is in the subring).

[„$\subseteq$": S rational, $k := (S,1) \in K^{\times} \Rightarrow (1 - Sk^{-1})$ proper
$\Rightarrow (1 - Sk^{-1})^*$ rational & inverse of $1 - (1 - Sk^{-1}) = Sk^{-1}$
$\Rightarrow kS^{-1}$ rational $\Rightarrow S^{-1}$ rational.

„$\supseteq$": T proper $\Rightarrow 1 - T \in K\langle\langle A\rangle\rangle \Rightarrow T^* = (1-T)^{-1}$]

(2) Let K be a field, $\operatorname{char} K = 0$.

$R_0 := \left\{ \frac{P}{Q} : P, Q \in K[x],\ Q(0) \neq 0 \right\} \subseteq K(x)$ rational (in the sense of „quotients of polynomials") functions w/o pole at 0.

R_0 is a commutative ring, $R_0^{\times} = \left\{ \frac{P}{Q} : P(0) \neq 0,\ Q(0) \neq 0 \right\}$

$\iota : R_0 \hookrightarrow K[\![x]\!]$ by (formal) Taylor expansion around 0

$$F = \frac{P}{Q} \longmapsto F(0) + F'(0)x + \frac{F''(0)}{2}x^2 + \dots + \frac{F^{(n)}(0)}{n!}x^n + \dots \quad (*)$$

Then $\iota(R_0)$ consists precisely of the rational series in the sense of the previous definition!
(It is the smallest subring containing polynomials & closed under inverses in $K[\![x]\!]$)

In fact: holds for every commutative ring, but we have to be a bit careful to interpret (*) correctly.

Easy algebraic way: $K[x] \hookrightarrow K[\![x]\!]$,

$M := \{ P \in K[x],\ P(0) \neq 0 \}$ multiplicative set,

$R_0 = M^{-1}K[x]$ (localization)

$\xrightarrow[\text{of localization}]{\text{U.P.}}$ $M^{-1}K[x] \hookrightarrow K[\![x]\!]$

skipped

Thm 1.7 ((Kleene-)Schützenberger) *Let $S \in K\langle\langle A \rangle\rangle$. Then*

S recognizable $\Leftrightarrow$ S rational

Lemma 1.8 *Let $S, T \in K\langle\langle A \rangle\rangle$, $a \in A$*

(1) $a^{-1}(ST) = (a^{-1}S)T + (S,1)(a^{-1}T)$

(2) *If S is proper, then* $a^{-1}(S^*) = (a^{-1}S)S^*$

Proof: (1) $(a^{-1}(ST), w) = (ST, aw) = \sum_{\substack{uv \in A^* \\ uv = aw}} (S,u)(T,v)$

$$= \overbrace{(S,1)(T,aw)}^{v=1} + \sum_{\substack{u'v=w \\ u',v \in A^*}} \overbrace{(S,au')(T,v)}^{u=au'}$$

$$= (S,1)(a^{-1}T, w) + ((a^{-1}S)\cdot T, w)$$

(2) $S^* = 1 + SS^* \xrightarrow{(1)} a^{-1}S^* = (a^{-1}S)S^* + \underbrace{(S,1)}_{=0}(a^{-1}S^*)$ □

Note: $\Phi : \begin{cases} K\langle\langle A \rangle\rangle^{n\times n} \longrightarrow K^{n\times n}\langle\langle A \rangle\rangle \\ M = (\underbrace{M_{ij}}_{\in K\langle\langle A \rangle\rangle})_{1\le i,j\le n} \longmapsto \sum_{w \in A^*} (M_{ij}, w)_{i,j}\, w \end{cases}$

is a semiring isomorphism

M proper $:\Leftrightarrow$ $\Phi(M)$ proper $\Leftrightarrow$ $(M_{ij}, 1) = 0 \ \forall i,j$

$\Leftrightarrow$ M_{ij} proper $\forall i,j$

$M^* := \Phi^{-1}(\Phi(M)^*) = \sum_{n\ge 0} M^n$ if M proper.

$\Rightarrow$ $M^* = \underbrace{I}_{\text{identity}} + MM^*$

Lemma 1.9 If $M = (M_{ij}) \in K\langle\langle A \rangle\rangle^{n\times n}$ is proper, then all entries of M^* can be obtained from the M_{ij} by repeated application of: K-linear combination, product, *.

In particular: If M_{ij} is rational for all i,j, then the entries of M^* are rational.

Proof: Induction on n. $n=1$ ✓

$n>1$: Choose some non-trivial block decomposition

$$M =: \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{matrix} \}m \\ \}n-m \end{matrix} \qquad 1 \le m < n \text{ (arbitrary, e.g. } m=1)$$

$$\underbrace{}_{m} \quad \underbrace{}_{n-m}$$

$$M^* =: \begin{pmatrix} \tilde{A} & \tilde{B} \\ \tilde{C} & \tilde{D} \end{pmatrix}$$

Recursive equation: $M^* = I + MM^* =$

$$\begin{pmatrix} I + A\tilde{A} + B\tilde{C} & A\tilde{B} + B\tilde{D} \\ C\tilde{A} + D\tilde{C} & I + C\tilde{B} + D\tilde{D} \end{pmatrix}$$

($\tilde{A}$ = upper-left block; $\tilde{B}$ = upper-right block; $\tilde{C}$ = lower-left block; $\tilde{D}$ = lower-right block)

$$\xRightarrow[A,D \text{ proper}]{L1.6 + \text{iso } \Phi} \tilde{C} = D^*(C\tilde{A}), \quad \tilde{B} = A^*(B\tilde{D})$$

$$\Rightarrow \tilde{A} = I + A\tilde{A} + BD^*C\tilde{A} = I + \overbrace{(A + BD^*C)}^{\text{proper}}\tilde{A}$$

$$\tilde{D} = I + CA^*B\tilde{D} + D\tilde{D} = I + (CA^*B + D)\tilde{D}$$

$$\xRightarrow{L1.6} \tilde{A} = (A + BD^*C)^*, \quad \tilde{D} = \underbrace{(CA^*B + D)^*}_{\text{proper}}$$

$$\tilde{B} = A^*B(CA^*B + D)^*, \quad \tilde{C} = D^*C(A + BD^*C)^*$$

By IH entries of A^*, D^* are rational expr in entries of A, D. (IH) again: similar result holds for

$(CA^*B + D)^*$, $(A + BD^*C)^*$ $\Rightarrow$ entries of $\tilde{A}, \tilde{B}, \tilde{C}, \tilde{D}$ are rational expr in entries of A, B, C, D. $\square$

Proof of Thm 1.7

„⇐": Using module-theoretic characterization:

(i) $P \in K\langle\langle A\rangle\rangle \Rightarrow w^{-1}P = 0$ if $|w| > \deg(P)$

$\Rightarrow \{w^{-1}P : w \in A^*\}$ is finite & stable

$\Rightarrow {}_K\langle\{w^{-1}P : w \in A^*\}\rangle$ is f.g. stable K-module containing P

$\Rightarrow P$ recognizable

(ii) Cor 1.3: S, T recognizable $\Rightarrow \forall k, \ell \in K$: $kS + \ell T$ recognizable

(iii) Let S, T be recognizable, $S \in {}_K M$, $T \in {}_K N$, M, N f.g. stable modules.

$\Rightarrow {}_K MT + {}_K N$ is f.g. K-module

If $U \in M$, $V \in N$, $w \in A^*$: $w^{-1}(UT + V) \overset{(1.8)}{=} \underbrace{(w^{-1}U)}_{\in M} T + (U,1)\underbrace{(w^{-1}T)}_{\in N} + \underbrace{w^{-1}V}_{\in N}$

$\in MT + N$

$\Rightarrow MT + N$ is stable, and $ST \in MT + N$

$\Rightarrow ST$ recognizable

(iv) Let S be proper, $S \in {}_K M$ with M stable f.g.

${}_K N := MS^* + K \leq {}_K K\langle\langle A\rangle\rangle$ f.g., $S^* = SS^* + 1 \in N$

$\forall U \in M\ \forall k \in K\ \forall w \in A^*$: $w^{-1}(US^* + k) \overset{(1.8)}{=} \underbrace{(w^{-1}U)}_{\in M} S^* + (U,1)(w^{-1}S^*) + \underbrace{w^{-1}k}_{\in K}$

$= \underbrace{(w^{-1}U)}_{\in M} S^* + \underbrace{(U,1)(w^{-1}S)}_{\in M} S^* + \underbrace{w^{-1}k}_{\in K} \in MS^* + K = N.$

So: nc polynomials are recognizable, and the set of recognizable series is closed under $+$, scalar mult., products, sums, star.

Since the rational series form the smallest such set:

rational $\Rightarrow$ recognizable.

"$\Rightarrow$" Let S be recognizable with lin repr. (λ, μ, γ), dimension n.

$$M := \sum_{a \in A} \mu(a)\, a \quad \in K^{n \times n} \langle\langle A \rangle\rangle \text{ is a proper matrix}$$

$$\Rightarrow M^* = \sum_{\ell \geq 0} M^\ell = \sum_{\ell \geq 0} \left(\sum_{a \in A} \mu(a)\, a \right)^\ell = \sum_{\ell \geq 0} \sum_{\substack{w \in A^* \\ |w| = \ell}} \mu(w)\, w = \sum_{w \in A^*} \mu(w)\, w.$$

$$\overset{\text{Iso } \textcircled{1}}{\Rightarrow} \quad (M^*)_{ij} = \sum_{w \in A^*} (\mu(w))_{ij}\, w.$$

By L.1.9. each $(M^*)_{ij}$ is rational.

$$S = \sum_{i,j=1}^{n} \lambda_i \, (\mu(w))_{ij} \, \gamma_j \, w \quad \Rightarrow \quad S \text{ rational.} \qquad \square$$

Corollary 1.10 K semiring, A alphabet; $S \in K\langle\langle A \rangle\rangle$. TFAE

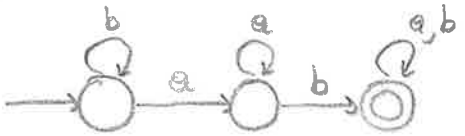
(1) S is recognizable by a WFA
(2) — " — linear repr.
(3) S is contained in a stable, f.g. submodul of $K\langle\langle A \rangle\rangle$
(4) S is rational.

2. The unweighted case (some proofs omitted)

Set now $K = \mathbb{B}$, A an alphabet

Then: $S \in \mathbb{B}\langle\langle A^* \rangle\rangle$ $\mathbb{B}$-recognizable $\Leftrightarrow$ $\mathrm{supp}(S)$ accepted by an (unweighted) automaton

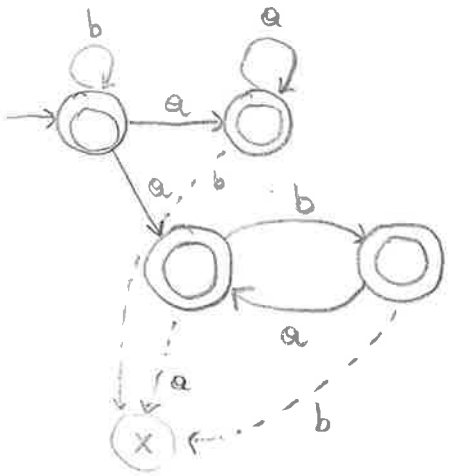
Exm 2.1: (1) $A = \{a, b\}$, $L \subseteq A^*$ (formal) language of all words in which there is some a, after which there is some b



(2) Every a only followed either only by a's, or by $bab\ldots$ alternating

(So: $b^n a^m$, or $b^n abab\ldots ab$
or $b^n abab\ldots a$)

(non-deterministic)



Regular languages: ·) $\emptyset$, $\{a\}$ for $a \in A$ are regular

·) L_1, L_2 regular $\Rightarrow$ $L_1 \cup L_2$, $L_1 \cdot L_2$ regular

·) L regular $\Rightarrow$ $L^* = \bigcup_{n \geq 0} L^n$ (Kleene star, ⚠ empty word $1 = \varepsilon \in L$ allowed)

·) Set of reg. languages is the smallest set closed under these properties.

Note: · $\{1\} = \emptyset^*$ (bec. $L^0 = \{1\}$ by definition)

· $(L \setminus \{1\})^* = L^*$

So: L regular $\Leftrightarrow$ L accepted by an automaton by Cor. 1.10

Exm 2.1 cont'd: (1) $\{b\}^* a \{a\}^* b \{a,b\}^*$

$= A^* a A^* b A^*$

(2) $\{b\}^* \cup \{b\}^* a \{a\}^* \cup \{b\}^* a (ba)^* \cup \{b\}^* a (ba)^* b$

Algebraic P.o.V. $L \subseteq A^*$ Language

left syntactic equivalence: $\forall x,y \in A^*$: $x \equiv_{L,e} y \Leftrightarrow x^{-1}L = y^{-1}L$

$\Leftrightarrow \forall w \in A^*: xw \in L \Leftrightarrow yw \in L$

Then: L regular $\overset{\text{Cor. 1.10}}{\Leftrightarrow} \{x^{-1}L : x \in A^*\}$ is a finite set ($\mathbb{B}$-module is fg $\Leftrightarrow$ finite)

$\Leftrightarrow A^*/_{\equiv_{L,e}}$ is finite

Given a regular $L \subseteq A^*$, define ($\mathbb{B}$-) automaton $\mathcal{A}$

states: $Q = \{x^{-1}L : x \in A^*\}$

$I = \{L\}$

$T = \{x^{-1}L : x \in A^*, \ 1 \in x^{-1}L\}$

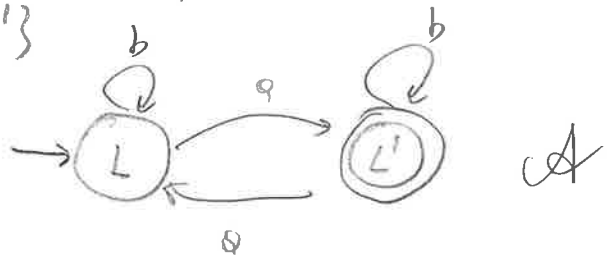
$Q \times A \times Q \supseteq E = \{(x^{-1}L, a, y^{-1}L) : \underbrace{a^{-1}x^{-1}L}_{=(xa)^{-1}L} = y^{-1}L\}$

Exm: L ... words with odd number of „a", $A = \{a,b\}$:

$\Rightarrow b^{-1}L = L$, $a^{-1}L =: L'$ ... even number of „a"s

$b^{-1}L' = L'$, $a^{-1}L' = L$

$Q = \{L, L'\}$



$\mathcal{A}$

Prop 2.2: The automaton constructed from the left syntactic equivalence accepts L.

Exm: # left quotients ≠ # right quotients in general:

E.g. $L = \{a^2, ba, a\}$

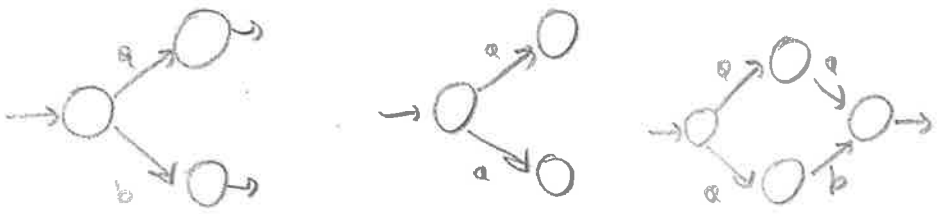
left quotients: $L, \{a, 1\}, \{a\}, \{1\}, \emptyset$

right quotients: $L, \{a, b, 1\}, \emptyset, \{1\}$

An automaton is **deterministic** (DFA) if:

- has ≤ 1 initial state
- for every state p, letter a, there is ≤ 1 state q with a transition $p \xrightarrow{a} q$

E.g.



deterministic — not — not (but codeterministic)

Determinization: Every non-deterministic FA (NFA) is equivalent to a deterministic FA (DFA)

Powerset Construction: Starting from NFA (Q, I, E, T), $I, T \subseteq Q$, $E \subseteq Q \times A \times Q$

new set of states: $\tilde{Q} := \{X : X \subseteq Q\}$

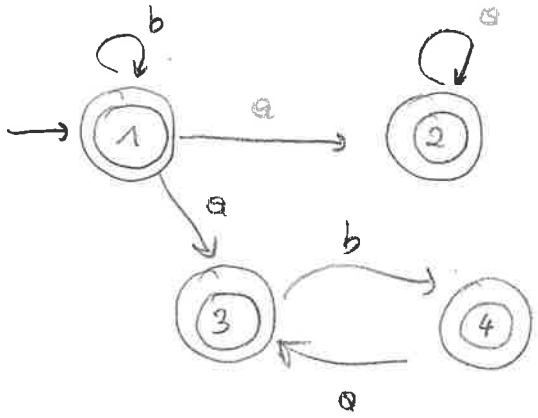
$\tilde{I} = \{I\}$

transition: Given $X_1 \subseteq Q$, $a \in A$, there is a transition to

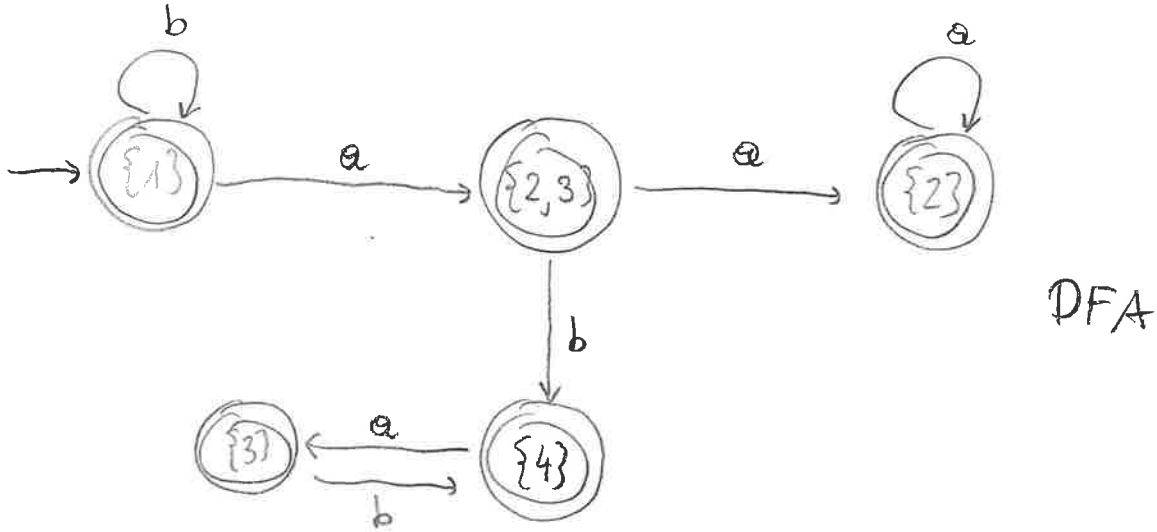
$X_2 := \{q \in Q : \exists x_1 \in X_1 : (x_1, a, q) \in E\}$

$\tilde{T} = \{X \subseteq Q : Q \cap T \neq \emptyset\}$,

Exm:



NFA



DFA

Def: •) For $L \subseteq A^*$ the syntactic congruence (Nerode congruence) is defined by $u \equiv_L v \iff [\forall x,y \in L: xuy \in L \iff xvy \in L]$

•) $A^*/\equiv_L$ is the syntactic monoid

Note: $\equiv_L$ is indeed a congruence, i.e. an equivalence relation and $u \equiv_L v \Rightarrow \forall x,y \in L: xuy \equiv_L xvy$.
Therefore $A^*/\equiv_L$ really is a monoid.

Thm 2.3 (Myhill-Nerode) $L \subseteq A^*$

(1) L is regular $\iff$ Syntactic monoid is finite

(2) Every minimal DFA is equivalent do:

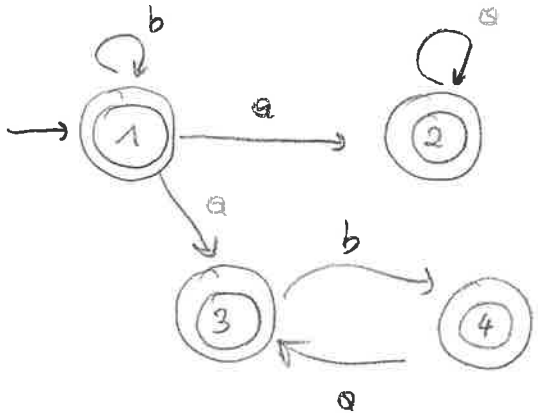
$Q = \{[x]_L : x \in A^*\}$ (equiv. classes)

$I = \{[1]_L\}$, $T = \{[x]_L : x \in L\}$,

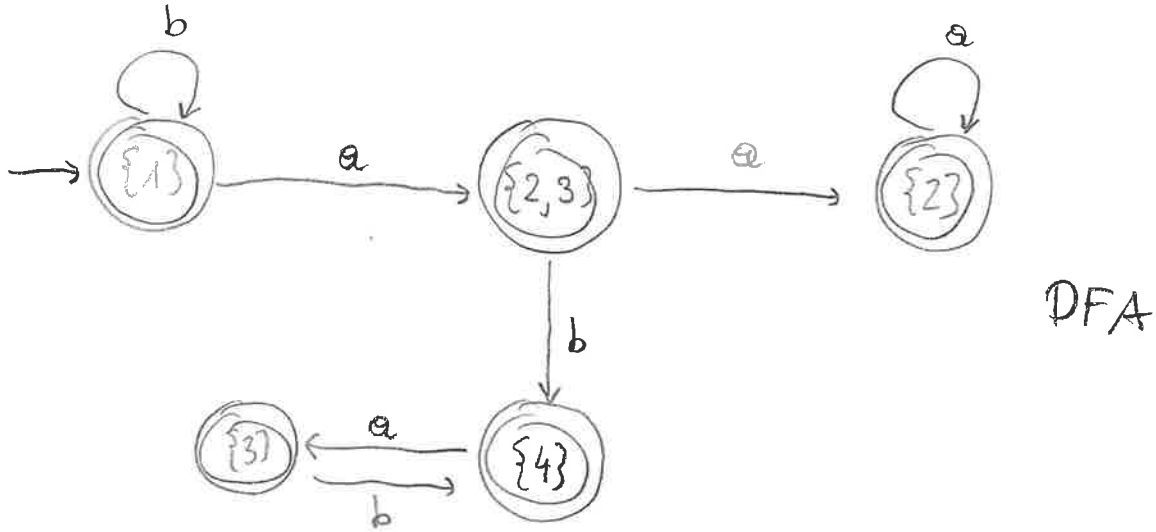
transitions: $[x]_L \to [xa]_L$ for all $x \in A^*$, $a \in A$.

In particular: $|A^*/\equiv_L|$ = number of states of min. DFA.

Exm:



NFA



DFA

Def: •) For $L \subseteq A^*$ the syntactic congruence (Nerode congruence) is defined by $u \equiv_L v \iff [\forall x,y \in L: xuy \in L \iff xvy \in L]$

•) $A^*/\equiv_L$ is the syntactic monoid

Note: $\equiv_L$ is indeed a congruence, i.e. an equivalence relation and $u \equiv_L v \Rightarrow \forall x,y \in L: xuy \equiv_L xvy$, therefore $A^*/\equiv_L$ really is a monoid.

Thm 23 (Myhill-Nerode) $L \subseteq A^*$

(1) L is regular $\iff$ Syntactic monoid is finite

(2) Every minimal DFA is equivalent do:

$Q = \{[x]_L : x \in A^*\}$ (equiv. classes)

$I = \{[1]_L\}$, $T = \{[x]_L : x \in L\}$,

transitions: $[x]_L \to [xa]_L$ for all $x \in A^*$, $a \in A$.

minimal # of states among all DFAs which have an initial state $\geq$ $\forall p \in Q \, \forall x \in A \, \exists! q : p \cdot x = q$, i.e.

In particular: $|A^*/\equiv_L|$ = number of states of min. DFA.

Proof (Sketch)

(1) „$\Leftarrow$" If $u \equiv_L v$, then $u^{-1}L = v^{-1}L$.

So finite syntactic monoid $\Rightarrow$ finitely many left quotients

$\overset{\text{Cor 1.10}}{\Rightarrow}$ L regular.

„$\Rightarrow$" Suppose L is recognized by some $\mathbb{B}$-linear repr. (λ, μ, γ) with $\mu: A^* \to \mathbb{B}^{d\times d}$. Then $\mu(A^*)$ is finite.

Define $u \sim v :\Leftrightarrow \mu(u) = \mu(v)$. Then $\sim$ is a congruence on A^* with finite quotient $A^*/_\sim \cong \mu(A^*)$.

Now: $u \sim v \Rightarrow \forall x,y \in A^*: \mu(xuy) = \mu(xvy)$

$\Rightarrow [xuy \in L \Leftrightarrow \lambda \underbrace{\mu(xuy)}_{=\mu(xvy)} \gamma = 1 \Leftrightarrow xvy \in L]$

Since $\equiv_L$ is the coarsest congruence wrt this property, (i.e. $\sim \subseteq \equiv_L$), there is a surjective hom.

$\varphi: \mu(A^*) \to A/_{\equiv_L}$

$\Rightarrow A/_{\equiv_L}$ is finite.

(2) Check that the given automaton is well-defined & accepts L (note: after reading x, it is in state $[x]_L$)

Minimality: Suppose we have a minimal DFA (q_0, E, T). We show $\mu(A^*) \xrightarrow{\varphi} A/_{\equiv_L}$ from (1) is injective.

Suppose $u \equiv_L v$ and $p \in \{1,\dots,d\} = Q$, q_0 initial state

Minimality $\Rightarrow \exists x \in A^*$: s.t. $q_0 \cdot x = p$ [(letters act on states); after reading x we are in state p, $\exists!$ since deterministic]

SHOW: $\mu(u)_{p*} = \mu(v)_{p*}$ [note: row has ≤ 1 nonzero entry]

Now: $\forall y \in A^*$: $xuy \in L \Leftrightarrow xvy \in L$

Suppose $p \cdot u =: q_u$, $p \cdot v =: q_v$

Then $\{y \in A^* : q_u \cdot y \in T\} = \{y \in A^* : q_v \cdot y \in T\}$.

So from q_u, q_v on we accept exactly the same words!

Minimality $\Rightarrow$ $q_u = q_v$.

$\Rightarrow p \cdot u = p \cdot v \overset{(\forall p)}{\Longrightarrow} \underline{\mu(u) = \mu(v)}$. □

Cor: In a minimal deterministic automaton $\mathcal{A}$ for L, the transition monoid $\mu(A^*)$ is isomorphic to the syntactic monoid $\mu(A^*) \cong A^*/\equiv_L$.

Connection with Logic (Informal)

First order logic, syntax: $\forall x, \exists x$ (quantification over elements of a universe), $\varphi \wedge \psi$, $\varphi \vee \psi$, $\neg\varphi$, $x = y$, $R(x_1, \dots, x_n)$ (↑ relations)

Monadic second order (MSO) logic: also:

$\forall X, \exists Y$ (quantifies over subsets of universe ($\to$ 2nd order)) $\qquad$ $x \in X$ (membership ($\to$ binary relation))

monadic: no quantification over binary, ternary, ... relations

MSO logic on words: universe = set of positions of word

relations: $x \leq y$ (↑ pos. x comes before y), $a(x)$ for all $a \in A$ (↑ letter in pos x is „a") ← alphabet (fixed)

A sentence in MSO-logic defines a language of all words satisfying it

Cor: $L \subseteq A^*$ is regular if and only if there exists a finite monoid M, a homomorphism $\varphi: A^* \to M$, and a subset $P \subseteq M$ s.t. $L = \varphi^{-1}(P)$.

Exm: $A = \{a, b, c\}$

- $\exists x: a(x) \wedge \exists y: b(y) \wedge \exists z: c(z)$ ... all letters occur
- $\forall x, y: [x \leq y \wedge a(y)] \Rightarrow a(x)$ ... "a" cannot follow any other letter
- Can also refer to "$x+1$": $y = x+1$ iff $x \leq y \wedge [\forall z: z \leq x \vee y \leq z]$
  also $x-1$, $x-2$, $x+2$, ... first / last position etc.

Remark: Complement of a regular language is regular.

Theorem 2.4 (Trakhtenbrot - Büchi - Elgot) $L \subseteq A^*$

L is MSO - definable $\Leftrightarrow$ L is regular.

A regular language is star-free if it can be constructed from $\emptyset$, $\{a\}$ $a \in A$, using Boolean operations $\cup, \cap, L \mapsto \bar{L}$ (↑ complement) and $\cdot$ (↑ concatenation)

Theorem 2.5 For a regular $L \subseteq A^*$ TFAE

(a) L is star-free

(b) The syntactic monoid of L is aperiodic
($\forall x \; \exists n \geq 1: \; x^n = x^{n+1}$)

(c) L is definable in first-order logic

(Schützenberger: (a) ↔ (b); McNaughton - Papert: (a) ↔ (c))

---

first(x) := $\forall y: y \geq x$ last(x) := $\forall y: y \leq x$

- $(aa)^*a$ ... words of odd length:

there is a set of pos containing first & last pos.

$\exists X \; \forall x: (\text{first}(x) \vee \text{last}(x)) \Rightarrow x \in X$

$\wedge \; \forall x \forall y: y = x+1 \Rightarrow (x \in X \Leftrightarrow y \notin X)$

contains every 2nd pos

Using Thm 25 we can see that $L=(aa)^* \subseteq$ is not first order definable:

$$a^n \equiv_L a^m \iff n \equiv m \bmod 2$$

$$\Rightarrow \begin{cases} \left(A^*/\equiv_L, \cdot\right) \cong \left(\mathbb{Z}/2\mathbb{Z}, +\right) \\ a^n \longmapsto n+2\mathbb{Z} \end{cases}$$

not aperiodic:

$1+1 \equiv 0, \quad 1+1+1 \equiv 1, \ldots \bmod 2$

Rem: Star height problem (deciding # of nested stars needed to define a regular language)

Q: 1963

Decidable 1988 → Hashiguchi

2005 → Kirsten: 2EXPSPACE

3. Syntactic Algebras & Minimization

K commutative ring (e.g. field), A alphabet.

Recall: •) If $S \in K\langle\langle A\rangle\rangle$ recognizable, then $\langle\{w^{-1}S : w \in A^*\}\rangle_K$ is f.g. (Prop 1.5)

•) A **K-algebra** is a ring B that is also a K-module, and where $k(bb') = b(kb') = (kb)b' \quad \forall k \in K,\ b, b' \in B$.

E.g.: $\mathbb{Q}[X,Y]$, $\mathbb{Q}\langle A\rangle$, $\mathbb{Q}\langle\langle A\rangle\rangle$, $\mathbb{R}$, $\mathbb{Q}^{d\times d}$ are $\mathbb{Q}$-algebras

($\Leftrightarrow$ B is a ring together with a ring homomorphism $K \to Z(B)$ (↑ center))

Fix $S \in K\langle\langle A\rangle\rangle$. For $P = \sum_{i=1}^{m} c_i w_i \in K\langle A\rangle$, $c_i \in K$, $w_i \in A^*$ distinct,

let $(S,P) := \sum_{w\in A^*} (S,w)(P,w) = \sum_{i=1}^{m} c_i (S,w_i) \in K$

Induces a K-bilinear map

$$\begin{array}{ccc} K\langle\langle A\rangle\rangle \times K\langle A\rangle & \longrightarrow & K \\ (S,\ P) & \longmapsto & (S,P) \end{array}$$

(↑ tuple; ↑ as just defined)

So: $(S,-) : \begin{cases} K\langle A\rangle \longrightarrow K \\ P \longmapsto (S,P) \end{cases}$ is K-linear

$\Rightarrow K\langle\langle A\rangle\rangle \cong K\langle A\rangle^* = \mathrm{Hom}_K(K\langle A\rangle, K)$ (dual module).

[Surjectivity: A^* is a basis of $K\langle A\rangle$ and

$K\langle\langle A\rangle\rangle = \{\text{maps } P : A^* \to K\}$

$\cong \{\text{linear maps } F : K\langle A\rangle \to K\}$

Injectivity: $(S,-) = 0 \Rightarrow \forall w \in A^*,\ (S,w) = 0 \Rightarrow S = 0$]

The quotient operation $S \mapsto w^{-1}S$ extends to a right $K\langle A\rangle$-module structure on $K\langle\langle A\rangle\rangle$:

If $P = c_1 w_1 + \dots + c_m w_m$, define

$$\boxed{S \circ P := \sum_{i=1}^{m} c_i w_i^{-1} S}$$

$\left(S \circ w = w^{-1}S, \quad (S\circ x)\circ y = S\circ(xy)\right)$

Then: $(S\circ P, Q) = (S, PQ)$

[$S\circ -\circ P : K\langle\langle A\rangle\rangle \to K\langle\langle A\rangle\rangle$, $S \mapsto S\circ P$ is the adjoint of the multiplication-by-P linear map $K\langle A\rangle \to K\langle A\rangle$, $Q \mapsto PQ$:

$$\begin{array}{ccccc} K\langle A\rangle & \xrightarrow{m_P} & K\langle A\rangle & \overset{\mathrm{Hom}(-,K)}{\rightsquigarrow} & K\langle\langle A\rangle\rangle \xleftarrow[m_P^*]{\mathrm{Hom}(m_P,K)} K\langle\langle A\rangle\rangle \\ Q & \longmapsto & PQ & & S\circ P \longleftarrow S \end{array}$$

]

Def: Let $S \in K\langle\langle A\rangle\rangle$. The <u>syntactic right ideal</u> I_S^r of S is the largest right ideal contained in

$$\{P \in K\langle A\rangle : (S,P) = 0\} =: \mathrm{Ker}(S)$$

[Exists: $I_S^r = \sum\{I : I \text{ right ideal of } K\langle A\rangle,\ I \subseteq \mathrm{Ker}(S)\}$ ($\uparrow$ K-module, but not $K\langle A\rangle$-module!)

<u>Lemma 2.1</u> (1) $I_S^r = \{P \in K\langle A\rangle : S\circ P = 0\}$

$$= \mathrm{Ker}(P \mapsto S\circ P)$$

(2) $K\langle A\rangle / I_S^r \underset{(*)}{\cong} S\circ K\langle A\rangle \underset{(**)}{\subseteq} K^{\langle\{w^{-1}S : w \in A^*\}\rangle}$ (as right $K\langle A\rangle$-modules)

<u>Proof</u>: (1) „$\supseteq$": If $S\circ P = 0$ and $Q \in K\langle A\rangle$, then $S\circ(PQ) = (S\circ P)\circ Q = 0$, so $\{P \in K\langle A\rangle : S\circ P = 0\}$ is a right $K\langle A\rangle$-ideal.

Also $S\circ P = 0 \Rightarrow (S\circ P, 1) = 0 \Rightarrow (S, P\cdot 1) = (S,P) = 0 \Rightarrow P \in \mathrm{Ker}(S)$, so the set is contained in I_S^r.

$\subseteq$: Suppose $P \in I_S^r$. To show: $S \circ P = 0$

Since I_S^r is a right $K\langle A\rangle$-ideal, also $PQ \in I_S^r$ $\forall Q \in K\langle A\rangle$,

$\Rightarrow \forall Q \in K\langle A\rangle$: $PQ \in \mathrm{Ker}(S)$. So $\forall Q \in K\langle A\rangle$

$\Rightarrow (S, PQ) = 0 \Rightarrow (S \circ P, Q) = 0$.

In particular: $\forall w \in A^*$: $(S \circ P, w) = 0 \Rightarrow$ $S \circ P = 0$.

(2) (*): rhs is image of K-linear map $P \mapsto S \circ P$, and I_S^r is its kernel.

(**) Look at def of $S \circ P$.

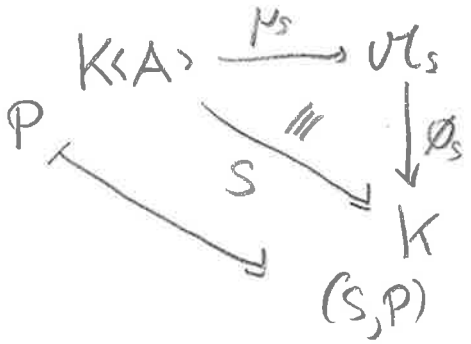
□

So: S recognizable $\Leftrightarrow$ $K\langle A\rangle / I_S^r$ finitely generated K-module.

Def: The syntactic ideal I_S of $S \in K\langle\langle A\rangle\rangle$ is the largest two-sided of $K\langle A\rangle$ contained in $\mathrm{Ker}(S) = \{P \in K\langle A\rangle : S \circ P = 0\}$

The syntactic algebra is $\mathcal{M}_S := K\langle A\rangle / I_S$.

There is a canonical algebra morphism $\mu_S : K\langle A\rangle \to \mathcal{M}_S$ and a linear map $\varphi_S : \mathcal{M}_S \to K$ s.t. $S = \varphi_S \circ \mu_S$



(K-linear)

The quotient operation $S \mapsto w^{-1}S$ extends to a right $K\langle A\rangle$-module structure on $K\langle\langle A\rangle\rangle$:

If $P = c_1 w_1 + \dots + c_m w_m$, define

$$\boxed{S \circ P := \sum_{i=1}^{m} c_i w_i^{-1} S}$$

$\left(S \circ w = w^{-1}S, \quad (S\circ x)\circ y = S\circ(xy)\right)$

Then: $(S\circ P, Q) = (S, PQ)$

[$S\circ -\circ P : K\langle\langle A\rangle\rangle \to K\langle\langle A\rangle\rangle$, $S \mapsto S\circ P$ is the adjoint of the multiplication-by-P linear map $K\langle A\rangle \to K\langle A\rangle$, $Q \mapsto PQ$:

$$\begin{array}{ccc} K\langle A\rangle & \xrightarrow{m_P} & K\langle A\rangle \\ Q & \longmapsto & PQ \end{array} \qquad \begin{array}{ccc} K\langle\langle A\rangle\rangle & \xleftarrow[m_P^*]{\mathrm{Hom}(m_P,K)} & K\langle\langle A\rangle\rangle \\ S\circ P & \longleftarrow & S \end{array}$$

$\mathrm{Hom}_K(-,K)$]

Def: Let $S \in K\langle\langle A\rangle\rangle$. The <u>syntactic right ideal</u> I_S^r of S is the largest right ideal contained in

$$\{P \in K\langle A\rangle : (S,P) = 0\} =: \mathrm{Ker}(S)$$

[Exists: $I_S^r = \sum\{I : I \text{ right ideal of } K\langle A\rangle,\ I \subseteq \mathrm{Ker}(S)\}$ (K-module, but not $K\langle A\rangle$-module!)

Lemma 3.1 (1) $I_S^r = \{P \in K\langle A\rangle : S\circ P = 0\}$

$= \mathrm{Ker}(P \mapsto S\circ P)$

(2) $K\langle A\rangle / I_S^r \underset{(*)}{\cong} S\circ K\langle A\rangle \underset{(**)}{=} K^{\langle\{w^{-1}S : w \in A^*\}\rangle}$ (as right $K\langle A\rangle$-modules)

Proof: (1) „$\supseteq$": If $S\circ P = 0$ and $Q \in K\langle A\rangle$, then $S\circ(PQ) = (S\circ P)\circ Q = 0$, so $\{P \in K\langle A\rangle : S\circ P = 0\}$ is a right $K\langle A\rangle$-ideal.

Also $S\circ P = 0 \Rightarrow (S\circ P, 1) = 0 \Rightarrow (S, P1) = (S,P) = 0 \Rightarrow P \in \mathrm{Ker}(S)$, so the set is contained in I_S^r.

"$\subseteq$": Suppose $P \in I_S^r$. To show: $S \circ P = 0$

Since I_S^r is a right $K\langle A\rangle$-ideal, also $PQ \in I_S^r$ $\forall Q \in K\langle A\rangle$,

$\Rightarrow \forall Q \in K\langle A\rangle$: $PQ \in \ker(S)$. So $\forall Q \in K\langle A\rangle$

$\Rightarrow (S, PQ) = 0 \Rightarrow (S \circ P, Q) = 0$.

In particular: $\forall w \in A^*$: $(S \circ P, w) = 0 \Rightarrow \underline{S \circ P = 0}$.

(2) (*): rhs is image of K-linear map $P \mapsto S \circ P$, and I_S^r is its kernel.

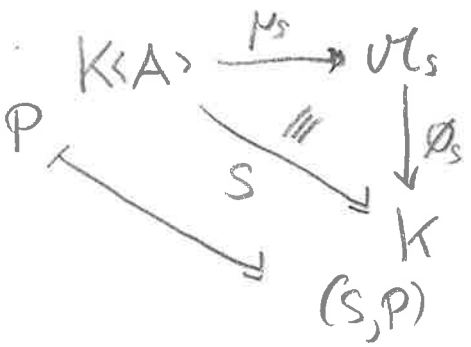
(**) Look at def of $S \circ P$ □

So: S recognizable $\Leftrightarrow$ $K\langle A\rangle / I_S^r$ finitely generated K-module.

Def: The syntactic ideal I_S of $S \in K\langle\langle A\rangle\rangle$ is the largest two-sided ideal of $K\langle A\rangle$ contained in $\ker(S) = \{P \in K\langle A\rangle : S \circ P = 0\}$

The syntactic algebra is $\mathcal{M}_S := K\langle A\rangle / I_S$.

There is a canonical algebra morphism $\mu_S : K\langle A\rangle \to \mathcal{M}_S$ and a linear map $\varphi_S : \mathcal{M}_S \to K$ s.t. $S = \varphi_S \circ \mu_S$



(K-linear)

Lemma 3.2 $I_S = \{Q \in K\langle A\rangle : \forall P,R \in K\langle A\rangle \ (S, PQR) = 0\} =: J$

$= \{Q \in K\langle A\rangle : \forall x,y \in A^* : (S, xQy) = 0\} =: J'$

Proof: $I_S \subseteq J \subseteq J'$ ✓ (since I_S is an ideal)

$J' \subseteq I_S$: Let $Q \in J'$. To show: $K\langle A\rangle Q K\langle A\rangle \subseteq \mathrm{Ker}(S)$, i.e.

$\forall P,R \in K\langle A\rangle$: $(S, PQR) = 0$.

Clear using bilinearity + def. of J'. □

Note: $I_S^r = \{Q \in K\langle A\rangle : \forall P \in K\langle A\rangle \ (S, QP) = 0\}$

$= \{Q \in K\langle A\rangle : \forall x \in A^* \ (S, Qx) = 0\}$

Lemma 3.3 ("basis-free linear repr") Let M_K be f.g. right K-module, $\varnothing : M \to K$ K-linear, $m_0 \in M$, $\nu : A^* \to \mathrm{End}(M_K)$ monoid morphism. Then

$$S = \sum_{w \in A^*} \varnothing(\nu(w)(m_0))\, w \quad \in K\langle\langle A\rangle\rangle$$

is recognizable. If M is n-generated, S has a lin. repn of dimension n.

Proof (Sketch): Let $M = \langle m_1, \dots, m_d\rangle_K$.

For $a \in A$, $1 \le i,j \le d$ there exist $\alpha_{ij} \in K$ such that

$$\nu(a)(m_j) = \sum_{i=1}^{d} m_i \alpha_{ij} \qquad \text{(in general, } \alpha_{ij} \text{ are not unique!)}$$

Define $\mu(a) := (\alpha_{ij})_{i,j} \in K^{d\times d}$, and extend to $\mu : A^* \to K^{d\times d}$ multiplicatively.

Then (check) $\nu(w)(m_j) = \sum_{i=1}^{d} m_i \mu(w)_{ij}$ $\forall w \in A^*$, $1 \le j \le d$.

Let $\lambda = (\lambda_1, \dots, \lambda_d)^T$ with $\lambda_i := \varnothing(m_i)$,
$\gamma = (\gamma_1, \dots, \gamma_d)$ and $m_0 = \sum_{j=1}^{d} m_j \gamma_j$

$\overset{\text{(Check)}}{\Longrightarrow}$ $\gamma\, \mu(w)\, \lambda = \varnothing(\upsilon(w)(m_0))$ $\forall w \in A^*$. $\square$

Thm 3.4 (Reutenauer) $S \in K\langle\langle A \rangle\rangle$ is rational $\Leftrightarrow$ $\mathcal{M}_S$ is a f.g. K-module

Proof: "$\Rightarrow$": Let (λ, μ, γ) be a lin. repr. for S.

Let K_0 be the subring of K generated by entries of $\lambda, \gamma, \mu(a), a \in A$
$\Rightarrow$ $\mu(w)$ has entries in K_0 $\forall w \in A^*$; K_0 is noetherian (cf. Prop 1.5)

$\mu(K_0\langle A \rangle) \subseteq K_0^{d \times d}$ is a K_0-submodule, $K_0^{d\times d}$ is f.g., K_0 noetherian

$\Rightarrow$ $\mu(K_0\langle A \rangle)$ is finitely generated / K_0 $\Rightarrow$ $\mu(K\langle A \rangle)$ f.g. over K.

If $\mu(w) = 0$, then $(S, w) = 0$, so $\ker(\mu) \subseteq \ker(S)$ and $\ker(\mu)$ is an ideal $\Rightarrow$ $\ker(\mu) \subseteq I_S$ by def of I_S

$\Rightarrow$ $\exists$ K-algebra epi $\dfrac{K\langle A \rangle}{\ker(\mu)} \twoheadrightarrow \dfrac{K\langle A \rangle}{I_S} = \mathcal{M}_S$.

$\dfrac{K\langle A \rangle}{\ker(\mu)} \cong \mu(K\langle A \rangle)$

$\Rightarrow$ $\mathcal{M}_S$ is f.g. as K-module.

"$\Leftarrow$": Suppose $\mathcal{M}_S$ is f.g. over K, $\mu_S : K\langle A \rangle \twoheadrightarrow \mathcal{M}_S$ with $\ker(\mu_S) = I_S$. For all $w \in A^*$, define

$$\upsilon(w) : \begin{cases} \mathcal{M}_S \longrightarrow \mathcal{M}_S \\ x \longmapsto \mu_S(w)\, x \end{cases} \quad \Rightarrow \quad \upsilon(ww')x = \mu_S(ww')x = \mu_S(w)\mu_S(w')x = \upsilon(w)(\upsilon(w')x)$$

$\Rightarrow$ $\upsilon : A^* \to \mathrm{End}(\mathcal{M}_S)$ is a monoid morphism.

$$\varphi_S(\nu(w)(1)) = \varphi_S(\mu_S(w)\cdot 1) = \varphi_S(\mu_S(w)) = (S,w).$$

(μ_S over the first $=$; $\mu_S : M_S \to K$, from Def. of syntactic algebra)

Lemma 2.3 $\Rightarrow$ S is recognizable. $\square$

3.1 The Hankel matrix

Let K be a field, A alphabet.

Def: Let $S \in K\langle\langle A \rangle\rangle$. The Hankel matrix $H = H_S$ of S is

the infinite matrix with rows & columns indexed by A^* and

$$H(x,y) = (S, xy) \qquad \forall x,y \in A^*.$$

Remark rank H = largest non-vanishing subdeterminant

= max. # of independent rows

= — " — columns

rank $H \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$.

Lemma 3.5 $\dim_K(S \circ K\langle A \rangle) = \dim_K\left(K\langle A \rangle / I_S^r\right) = \text{rank}(H_S) \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$.

Proof: $S \circ K\langle A \rangle \cong K\langle A \rangle / I_S^r$ shows the first equality.

$$S \circ K\langle A \rangle = \langle \{ S \circ x : x \in A^* \} \rangle_K$$

($S \circ x = x^{-1}S$)

Each $x^{-1}S$ is the row with index x in H, so

$$\dim(S \circ K\langle A \rangle) = \text{rank}(H). \qquad \square$$

Def: $\dim_K(S \circ K\langle A \rangle)$ is the rank of S.

Theorem 3.6 (Carlyle-Paz ; Fliess)

$S \in K\langle\langle A \rangle\rangle$ is rational $\Leftrightarrow$ $\operatorname{rank} S < \infty$

If $r = \operatorname{rank} S < \infty$ then r is the minimum dimension of the lin. repr's of S.

Proof: "$\Rightarrow$" Let (λ, μ, γ) be a lin repr. for S of dimension d,

Extend $\mu: A^* \to K^{d\times d}$ to a K-algebra hom $\mu: K\langle A\rangle \to K^{d\times d}$

$I := \{P \in K\langle A\rangle : \lambda\mu(P) = 0\}$ is a right ideal of $K\langle A\rangle$,

$I \subseteq \operatorname{Ker}(S)$

$\Longrightarrow I \subseteq I_s^r$ syndactic right ideal

$I = \operatorname{Ker}(K\langle A\rangle \to K^{1\times d},\ P \mapsto \lambda\mu(P)) \Rightarrow \dim K\langle A\rangle/I \leq \dim K^{1\times d} = d.$

$\Rightarrow \dim K\langle A\rangle/I \leq d \Rightarrow \dim K\langle A\rangle/I_s^r \leq d \Rightarrow \operatorname{rank} S \leq d.$

"$\Leftarrow$": $d := \operatorname{rank}(S) = \dim(S \circ K\langle A\rangle) < \infty$. Define a K-linear

$$\varphi: \begin{cases} \overline{S \circ K\langle A\rangle} =: V_K \to K \\ T \mapsto (T, 1) \end{cases}$$

$\Rightarrow \forall w \in A^*$: $\varphi(S \circ w) = (S \circ w, 1) = (S, w)$

Fix a basis of $V \xrightarrow{\psi} K^{1\times d}$.

For each $w \in A^*$, let $\mu(w) \in K^{d\times d}$ be the matrix representing the linear map $V \to V$, $T \mapsto T \circ w$, acting on the right (i.e. $\psi(T)\mu(w) = \psi(T \circ w)$)

↑ row vector

Define $\lambda := \psi(S)$ and let $\gamma \in K^{d\times 1}$ be such that $\varphi(T) = \psi(T)\gamma$ $\forall T$ (i.e. γ represents $\varphi \in V^*$).

Then: $\psi(T)\mu(ww') = \psi(T \circ ww') = \psi((T \circ w) \circ w') = \psi(T \circ w)\mu(w')$

$= \psi(T)\mu(w)\mu(w')$ $\forall T \in V$

$\Rightarrow \mu(ww') = \mu(w)\mu(w')$ $\forall w, w' \in A^*$

Shorter: If $\operatorname{rank}(S) = d$, then $\dim\left(K\langle A\rangle / I_s^r\right) = d$ ($\{x^{-1}S : x \in A^*\}_K$)

Thm 1.2 $\Rightarrow$ S has a d-dim lin repr

and: $\lambda\mu(w)\gamma = \lambda\mu(s)\mu(w)\gamma = \lambda\mu(sow)\gamma = \varphi(sow) = (s,w)$

□

3.3 Minimal lin. repr.

K field

Def: A d-dim lin repr (λ,μ,γ) is minimal if its dimension is minimal among all lin. repr for the series recognized by (λ,μ,γ).

Prop 3.7 Let (λ,μ,γ) be a lin. repr. of dimension $d \geq 0$, set $\mathcal{H} := \mu(K\langle A\rangle) \subseteq K^{d\times d}$.

Then: (λ,μ,γ) minimal $\Leftrightarrow \lambda\mathcal{H} = K^{1\times d}$ and $\mathcal{H}\gamma = K^{d\times 1}$
("(λ,μ,γ) is left and right reduced")

Proof: "$\Leftarrow$" Let $x_1,\dots,x_d, y_1,\dots,y_d \in A^*$ s.t.
$(\lambda\mu(x_1),\dots,\lambda\mu(x_d))$ is a basis of $K^{1\times d}$, and
$(\mu(y_1)\gamma,\dots,\mu(y_d)\gamma)$ is a basis of $K^{d\times 1}$.

Then $\det(\lambda\mu(x_i y_j)\gamma)_{1\leq i,j\leq d} \neq 0$

[**Proof:** Suppose $\exists \alpha_1,\dots,\alpha_d \in K\ \forall j\in\{1,\dots,d\}: \sum_{i=1}^{d} \alpha_i \lambda\mu(x_i)\mu(y_j)\lambda = 0$

Since $(\mu(y_j)\lambda)_{1\leq j\leq d}$ is a basis of $K^{d\times n} = (K^{1\times d})^*$,
$\sum_{i=1}^{d} \alpha_i \lambda\mu(x_i) = 0 \Rightarrow \alpha_1 = \dots = \alpha_d = 0$]

Since $(S, x_i y_j) = \lambda\mu(x_i y_j)\gamma$, the Hankel matrix has rank $\geq d$ $\xRightarrow{\text{Thm 36}}$ rank $S \geq d$.

„⇒": $I := \{P \in K\langle A\rangle : \lambda\mu(P) = 0\}$ right ideal of $K\langle A\rangle$.

$I = \ker(\varphi)$ with $\varphi: K\langle A\rangle \longrightarrow K^{1\times d}$, $P \mapsto \lambda\mu(P)$

$\operatorname{im}\varphi = \lambda\mathcal{U}$, $\dim \lambda\mathcal{U} \leq d$

$$I \subseteq I_s^r \Rightarrow d \geq \dim(\lambda\mathcal{U}) = \dim\left(K\langle A\rangle / I\right) \geq \dim\left(K\langle A\rangle / I_r\right) = d.$$

(Lemma 3.5)

$\Rightarrow \dim(\lambda\mathcal{U}) = d \Rightarrow \underline{\lambda\mathcal{U} = K^{1\times d}}$ and $I = I_s^r$.

Symmetrically: $\mathcal{U}_\gamma = K^{d\times 1}$. □

Cor 3.8 If (λ, μ, γ) is minimal, then

(1) $\ker(P \mapsto \lambda\mu(P)) = I_s^r$, $\ker(P \mapsto \mu(P)\gamma) = I_s^\ell$

(2) $\ker(\mu) = I_s$. (syntactic ideal)

$\Rightarrow \mu(K\langle A\rangle) = K\langle \mu(A^*)\rangle \cong \mathcal{M}_s$ (syntactic algebra)

Proof: (1) By proof of Prop 3.7.

(2) $\ker(\mu) \subseteq \ker(s)$ is an ideal, so $\ker(\mu) \subseteq I_s$.

$I_s \subseteq \ker(\mu)$: Let $Q \in I_s \Rightarrow \forall P, R \in K\langle A\rangle : PQR \in I_s$

$\Rightarrow (s, PQR) = 0 \Rightarrow \lambda\mu(PQR)\gamma = 0$

$\overset{\text{P. 37}}{\Rightarrow} \underbrace{\lambda\mu(K\langle A\rangle)}_{K^{1\times d}}\, \mu(Q)\, \underbrace{\mu(K\langle A\rangle)\gamma}_{K^{d\times 1}} = 0 \Rightarrow \mu(Q) = 0$. □

Cor 3.9 If (λ, μ, γ) is a minimal lin repr of s, $\dim d$, then there are $P_i, Q_j \in K\langle A\rangle$ s.t.

$$\forall w \in A^*: \quad \mu(w) = \left((s, P_i w Q_j)\right)_{1\leq i,j\leq d}.$$

Proof: Pick P_i, Q_j s.t. $(\lambda\mu(P_i))_{1\leq i\leq d}$ is the standard basis of $K^{1\times d}$, $(\mu(Q_j)\gamma)_{1\leq j\leq d}$ standard basis of $\mu(Q_i)\gamma$.

$\Rightarrow \mu(w)_{ij} = (\lambda_\mu(P_i))\,\mu(w)(\mu(Q_j)\gamma) = \lambda_\mu(P_i w Q_j)\gamma = (S, P_i w Q_j)$ □

Def (λ,μ,γ), (λ',μ',γ') are **similar** if they have the same dimension d and there exists $T \in GL_d(K)$ s.t.

$$\lambda' = \lambda T, \quad \mu'(w) = T^{-1}\mu(w)T \ \ \forall w \in A^*, \quad \gamma' = T^{-1}\gamma$$

Similar rep's recognize the same series!

Thm 3.10 (Schützenberger) Minimal linear reps of a series S are unique up to similarity.

Proof: Let (λ,μ,γ) be a minimal linear repr of S, of dimension d. By 3.8, $I_S^r = \{P \in K\langle A\rangle : \lambda_\mu(P) = 0\}$

$\Rightarrow$ There is a right $K\langle A\rangle$-module iso

$$F: \begin{cases} K^{1\times d} = \lambda_\mu(K\langle A\rangle) \xrightarrow{\sim} K\langle A\rangle / I_S^r \cong S \circ K\langle A\rangle = \langle \{ w^{-1}S : w \in A^*\}\rangle_K \\ \lambda_\mu(P),\ P \in K\langle A\rangle \longmapsto S \circ P \end{cases}$$

(3.7: $K^{1\times d} = \lambda_\mu(K\langle A\rangle)$; $= \langle \lambda_\mu(w) : w \in A^*\rangle_K$; 3.1: $K\langle A\rangle/I_S^r \cong S \circ K\langle A\rangle$)

right $K\langle A\rangle$-action: Q acts on $\lambda_\mu(P)$ by $\lambda_\mu(PQ)$, on $S \circ P$ by $S \circ PQ$

Note: $F(\lambda) = S$ and define $\varphi: S \circ K\langle A\rangle \to K$, $T \mapsto (T, 1)$.

Then "everything commutes":

$$\begin{array}{ccc} \lambda_\mu(w) & \longmapsto & \lambda_\mu(w)\gamma \\ K^{1\times d} & \xrightarrow{\cdot\gamma} & K \\ F \downarrow \lambda & = & \| \\ S \circ K\langle A\rangle & \xrightarrow{\varphi} & K \\ S \circ w & \longmapsto & (S \circ w, 1) = (S, w) \end{array}$$

Now same for (λ',μ',γ'):

$$\begin{array}{ccc} F' \uparrow \lambda' & = & \| \\ K^{1\times d} & \xrightarrow{\cdot\gamma'} & K \end{array}$$

$\forall w \in A^*$:

$$\begin{array}{ccc} \lambda_\mu(x) & \longmapsto & \lambda_\mu(xw) \\ K^{1\times d} & \xrightarrow{\cdot\mu(w)} & K^{1\times d} \\ F \downarrow & = & \downarrow F \\ S \circ K\langle A\rangle & \longrightarrow & S \circ K\langle A\rangle \\ S \circ x & \longmapsto & S \circ xw \end{array}$$

$$\begin{array}{ccc} F' \uparrow \lambda' & = & F' \uparrow \lambda' \\ K^{1\times d} & \xrightarrow{\cdot\mu'(w)} & K^{1\times d} \\ \lambda'\mu'(x) & \longmapsto & \lambda'\mu'(xw) \end{array}$$

$\Rightarrow \mu(w)_{ij} = (\lambda_\mu(P_i))\,\mu(w)(\mu(Q_j)\gamma) = \lambda_\mu(P_i w Q_j)\gamma = (S, P_i w Q_j)$ □

Def (λ,μ,γ), (λ',μ',γ') are *similar* if they have the same dimension d and there exists $T \in GL_d(K)$ s.t.

$$\lambda' = \lambda T, \quad \mu'(w) = T^{-1}\mu(w)T \ \forall w \in A^*, \quad \gamma' = T^{-1}\gamma$$

Similar rep's recognize the same series!

Thm 3.10 (Schützenberger) Minimal linear reps of a series S are unique up to similarity.

Proof: Let (λ,μ,γ) be a minimal linear repr of S, of dimension d. By 3.8, $I_S^r = \{P \in K\langle A\rangle : \lambda_\mu(P) = 0\}$

$\Rightarrow$ There is a right $K\langle A\rangle$-module iso

$$F: \begin{cases} K^{1\times d} \overset{3.7}{=} \lambda_\mu(K\langle A\rangle) \xrightarrow{\sim} K\langle A\rangle / I_S^r \overset{3.1}{\cong} S\circ K\langle A\rangle = \langle\{w^{-1}S : w\in A^*\}\rangle_K \\ \lambda_\mu(P),\ P\in K\langle A\rangle \longmapsto S\circ P \end{cases}$$

($\lambda_\mu(w) : w\in A^*\rangle_K$)

right $K\langle A\rangle$-action: Q acts on $\lambda_\mu(P)$ by $\lambda_\mu(PQ)$, on $S\circ P$ by $S\circ PQ$

Note: $F(\lambda) = S$ and define $\varnothing: S\circ K\langle A\rangle \to K$, $T \mapsto (T,1)$.

Then "everything commutes":

$$\begin{array}{ccc} \lambda_\mu(w) & \longmapsto & \lambda_\mu(w)\gamma \\ K^{1\times d} & \xrightarrow{\cdot\gamma} & K \\ F\downarrow & = & \| \\ S\circ K\langle A\rangle & \xrightarrow{\varnothing} & K \\ S\circ w & \longmapsto & (S\circ w, 1) = (S, w) \end{array}$$

Now same for (λ',μ',γ'):

$$\begin{array}{ccc} F'\uparrow & = & \| \\ K^{1\times d} & \xrightarrow{\cdot\gamma'} & K \\ \lambda'_{\mu'}(w) & \longmapsto & \lambda'_{\mu'}(w)\gamma' \end{array}$$

$\forall w\in A^*$:

$$\begin{array}{ccc} \lambda_\mu(x) & \longmapsto & \lambda_\mu(xw) \\ K^{1\times d} & \xrightarrow{\cdot\mu(w)} & K^{1\times d} \\ F\downarrow & = & \downarrow F \\ S\circ K\langle A\rangle & \longrightarrow & S\circ K\langle A\rangle \\ S\circ x & \longmapsto & S\circ xw \end{array}$$

$$\begin{array}{ccc} F'\uparrow & = & F'\uparrow \\ K^{1\times d} & \xrightarrow{\cdot\mu'(w)} & K^{1\times d} \\ \lambda'_{\mu'}(x) & \longmapsto & \lambda'_{\mu'}(xw) \end{array}$$

$\Rightarrow$ $(F')^{-1} \circ F : K^{1\times d} \xrightarrow{\sim} K^{1\times d}$ induces the desired similarity.
Write T for its matrix (acting from right)

$\Rightarrow$ $\lambda T = \lambda'$, $\gamma' = T^{-1}\gamma$

$\mu'(w) = T^{-1}\mu(w)T$

□

Corollary 3.11 Let (λ, μ, γ), $(\lambda', \mu', \gamma')$ be two lin. repr of S. Suppose $(\lambda', \mu', \gamma')$ is minimal. Then, up to similarity, (λ, μ, γ) has a block decomposition

$$\lambda = (*, \boxed{\lambda'}, 0) \quad \mu = \begin{pmatrix} \mu_1 & 0 & 0 \\ * & \boxed{\mu'} & 0 \\ * & * & \mu_2 \end{pmatrix} \quad \gamma = \begin{pmatrix} 0 \\ \boxed{\gamma'} \\ * \end{pmatrix}$$

with $\mu_i : A^* \to K^{d\times d}$ morphisms.

Proof: Let n be the dimension of (λ, μ, γ).

Define $V_1 := \lambda\mu(K\langle A\rangle) \cap \{v \in K^{1\times n} : v\mu(K\langle A\rangle)\gamma = 0\}$

and V_2 s.t. $V_1 \oplus V_2 = \lambda\mu(K\langle A\rangle)$ as K-v.s.

Finally choose V_3 s.t. $V_1 \oplus V_2 \oplus V_3 = K^{1\times n}$.

Then (i) $V_1 \oplus V_2$ and V_1 are invariant under right $K\langle A\rangle$-operation (i.e. right $K\langle A\rangle$-submodules)

(ii) $\lambda \in V_1 \oplus V_2$

(iii) $V_1\gamma = 0$.

So, after fixing bases on V_1, V_2, V_3 ($\to$ similarity):

$$\lambda = (*, \tilde{\lambda}, 0), \quad \mu = \begin{pmatrix} \mu_1 & 0 & 0 \\ * & \tilde{\mu} & 0 \\ * & * & * \end{pmatrix}, \quad \gamma = \begin{pmatrix} 0 \\ \tilde{\gamma} \\ * \end{pmatrix}$$

To finish, we show $(\tilde{\lambda}, \tilde{\mu}, \tilde{\gamma})$ is a minimal lin. repr of S. Then, after a base change on V_2, $(\tilde{\lambda}, \tilde{\mu}, \tilde{\gamma}) = (\lambda', \mu', \gamma')$

Since $\lambda\mu(w)\gamma = \tilde{\lambda}\tilde{\mu}(w)\tilde{\gamma}$, $(\tilde{\lambda}, \tilde{\mu}, \tilde{\gamma})$ is a lin. repr of S.

(i) $\tilde{\lambda}\tilde{\mu}(K\langle A\rangle) = V_2$:

$$(*, \tilde{\lambda}) \begin{pmatrix} \mu_1(p) & 0 \\ * & \tilde{\mu}(p) \end{pmatrix} = (*, \tilde{\lambda}\tilde{\mu}(p)) \in \text{spans } V_1 \oplus V_2 \text{ by def}$$

$$\Rightarrow \tilde{\lambda}\tilde{\mu}(K\langle A\rangle) = V_2$$

(ii) $\tilde{\mu}(K\langle A\rangle)\tilde{y} = V_2^*$:

Let $v \in V_2$ s.t. $v\tilde{\mu}(K\langle A\rangle)\tilde{y} = 0$. Show: $v = 0$.

But $v\tilde{\mu}(K\langle A\rangle)\tilde{y} = 0 \Rightarrow v\mu(K\langle A\rangle)y = 0 \overset{\text{Def. } V_1}{\Longrightarrow} v \in V_1 \cap V_2 = 0$.

$$(0, v, 0) \begin{pmatrix} \mu_1 & \circ & \circ \\ * & \tilde{\mu} & \circ \\ * & \bullet & \mu_2 \end{pmatrix} = (*, \tilde{v}, 0)$$

Prop 3.7 $\Longrightarrow$ $(\tilde{\lambda}, \tilde{\mu}, \tilde{y})$ is minimal. □

3.4 Minimization Algorithm (K field)

Prop 3.7 leads to a minimization algorithm:

Given a lin repr (λ, μ, y) of S

(1) Find a basis of $V := \mu(K\langle A\rangle)y = \langle\{\mu(w)y : w \in A^*\}\rangle$ of the form $\mu(w_1)y, \ldots, \mu(w_n)y$.

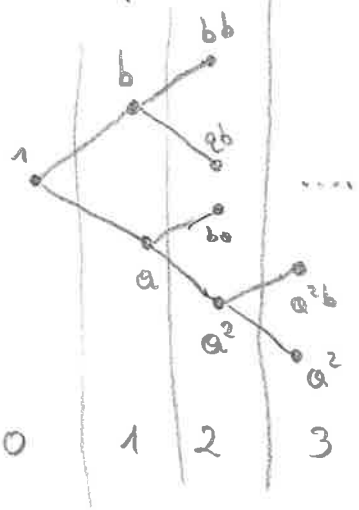
(2) Viewing $\mu(a): K^{d\times 1} \to K^{d\times 1}$, $\lambda: K^{d\times 1} \to K$, restrict to V (note $\mu(w)V \subseteq V$) to find a lin repr (λ', μ', y') of S with $\mu'(K\langle A\rangle)y' = K^{d'\times 1}$.

(3) Repeat analogously on the other side to get (λ'', μ'', y'') with $\lambda''\mu''(K\langle A\rangle) = K^{1\times d''}$, $\mu''(K\langle A\rangle)y'' = K^{d''\times 1}$.

Then (λ'', μ'', y'') is minimal by Prop 3.7.

How to find bases of $\lambda\mu(K\langle A\rangle)$, $\mu(K\langle A\rangle)y$?:

Breadth first search on words: , e.g. $A = \{a, b\}$



Claim: If $\ell \geq 0$ and for every $w \in A^*$ with $|w| = \ell$,

$$\lambda\mu(w) \in \langle \{\lambda\mu(x) : x \in A^*, |x| < \ell\} \rangle_K,$$

then $\lambda\mu(K\langle A \rangle) = \langle \{\lambda\mu(x) : |x| < \ell\} \rangle_K$.

So, at every length we either find at least one new lin indep vector, or we know we are done!

Proof of Claim: By induction on $|w|$.

Suppose $|w| \geq \ell$, $|w| = \ell$ ✓ by assumption.

$|w| > \ell$: $w = w'a$, $|w'| \geq \ell$, $a \in A$,

$$|w'| < |w| \overset{IH}{\Longrightarrow} \lambda\mu(w') = \sum_{\substack{|x| < \ell \\ x \in A^*}} \alpha_{w',x} \lambda\mu(x).$$

$$\Rightarrow \lambda\mu(w) = \lambda\mu(w')\mu(a) = \sum_{|x| < \ell} \alpha_{w',x} \lambda\mu(x)\mu(a) = \sum_{|x| < \ell} \alpha_{w',x} \lambda\mu(xa)$$

Since $|xa| < |w|$, $\lambda\mu(xa) \in \langle \{\lambda\mu(y) : y \in A^*\} \rangle_K$,

so $\lambda\mu(w)$ is in the same set. □

Cor 3.12: Over fields, equality of WFA is decidable.

Proof: From lin reps for S and T, we can construct a lin rep (λ, μ, γ) for $S - T$. Minimize (λ, μ, γ) to get $(\lambda', \mu', \gamma')$. Uniqueness of min. lin. repr $\Rightarrow$ ($S - T = 0 \iff$ $(\lambda', \mu', \gamma')$ has dimension 0). □

Remark: (1) A refinement of this using prefix-sets & prefix-closed sets gives a polynomial time algorithm for minimization

(2) Same idea allows to show: every right [left] ideal of $K\langle A\rangle$ is free (but arbitrary ranks, incl. infinite ranks, are possible)

4. Undecidability of Equality for Tropical Semirings

Thm 4.1 (Krob '94) Let $K = (\mathbb{N}_0 \cup \{-\infty\}, \max, +)$ or $K = (\mathbb{Z} \cup \{-\infty\}, \max, +)$, and $|A| \geq 2$.

If $\mathcal{A}, \mathcal{A}'$ are WFA over K, in general it is undecidable whether $[\![\mathcal{A}]\!] = [\![\mathcal{A}']\!]$.

Remark: (1) Since $\{a,b\}^*$ contains free monoids of arbitrary finite, even countable rank (e.g. the monoid generated by $\{a^i b : i \geq 0\}$), it suffices to prove the claim for some arbitrary finite alphabet A (i.e. we can use more than two letters)

(2) Krob's proof reduces Hilbert-10 (non-decidability of the existence of solutions of Diophantine equations, $P(x_1, \dots, x_n) = 1$, $P \in \mathbb{Z}[x_1, \dots, x_n]$, P homogeneous of degree ≤ 4)

Almagor, Baker, Kuperman (2011) gave an easier automata-theoretic proof using non-decidability of the halting problem for 2-counter machines (2CM) (Minsky machines).

Simplified by Droste, Kuske (2021). ("locations", "lines of code")

2CM: Idea: - Machine will finitely many states PLUS two nonnegative counters ($\in \mathbb{N}_0$)

- Counters can be incremented, decremented (only if positive), and tested for zero (in which case some transition is made)

Formally (one possible formalization)

- A 2CM is a DFA $\mathcal{M}$ over the alphabet $C = \{a_+, a_-, a_?, b_+, b_-, b_?\}$

  [for $x \in \{a,b\}$: x_+, x_- increment / decrement, $x_?$ – only possible if $x=0$].
  (x_-: only possible if $x=0$)

- The 2CM $\mathcal{M}$ halts (from the empty configuration) if it accepts some $w \in C^*$ s.t.
  (i) $|u|_{x_-} \leq |u|_{x_+}$ for every prefix u of w and $x \in \{a,b\}$
  (ii) $|u|_{x_-} = |u|_{x_+}$ for every prefix $ux_?$ of w and $x \in \{a,b\}$

- Words satisfying (i) & (ii) (but not necessarily accepted by $\mathcal{M}$) are potential computations.

Remark: $x_?$ tests for counter x being zero; $x_- x_+$ for counter x being nonzero.

Theorem 4.2 (Minsky 1961) Halting Problem for 2CM is undecidable

(Sketch of proof later)

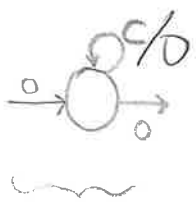
Proof of Thm 4.1 For $w \in C^*$, the maximal error $E(w)$ is the maximum of 0 and

- $|u|_{x_-} - |u|_{x_+}$ over all prefixes u of w, $x \in \{a,b\}$
- $|u|_{x_+} - |u|_{x_-}$ over all prefixes $ux_?$ of w, $x \in \{a,b\}$.

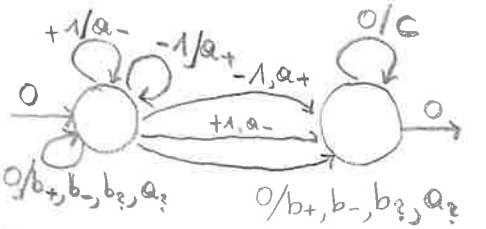
(E.g. $E(\overrightarrow{a_+^{-1}}\ \overrightarrow{a_?^{1}}\ \overrightarrow{a_-^{0}}\ \overrightarrow{a_-^{1}}) = 1$)

Then $E(w) = 0 \iff w$ is a potential computation.

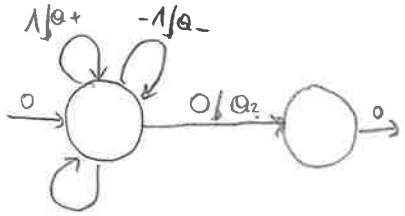
Considered as a series over $(\mathbb{Z} \cup \{-\infty\}, \max, +)$ E is recognizable:



≥ 0



$\max\{|u|_{a_-} - |u|_{a_+} : u\}$
plus a similar fragment with a, b swapped



$\max\{|u|_{a_+} - |u|_{a_-} : ua_? \text{ prefix}\}$
plus fragment with a, b swapped

Formally (one possible formalization)

- A 2CM is a DFA $\mathcal{M}$ over the alphabet $C = \{a_+, a_-, a_?, b_+, b_-, b_?\}$

  [for $x \in \{a,b\}$: x_+, x_- increment / decrement, $x_?$ – only possible if $x=0$; x_- only possible if $x=0$]

- The 2CM $\mathcal{M}$ halts (from the empty configuration) if it accepts some $w \in C^*$ s.t.
  (i) $|u|_{x_-} \leq |u|_{x_+}$ for every prefix u of w and $x \in \{a,b\}$
  (ii) $|u|_{x_-} = |u|_{x_+}$ for every prefix $ux_?$ of w and $x \in \{a,b\}$
- Words satisfying (i) & (ii) (but not necessarily accepted by $\mathcal{M}$) are potential computations.

Remark: $x_?$ tests for counter x being zero ; $x_- x_+$ for counter x being nonzero.

Theorem 4.2 (Minsky 1961) Halting Problem for 2CM is undecidable

(Sketch of proof below)

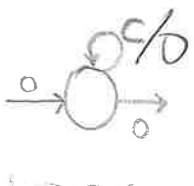
Proof of Thm 4.1 For $w \in C^*$, the maximal error (E,w) is the maximum of 0 and

- $|u|_{x_-} - |u|_{x_+}$ over all prefixes u of w, $x \in \{a,b\}$
- $|u|_{x_+} - |u|_{x_-}$ over all prefixes $ux_?$ of w, $x \in \{a,b\}$

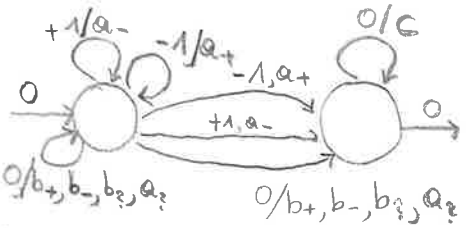
$(E.g.\ (E, a_+^{-1} a_?^{1} a_-^{0} a_-^{1}) = 1)$

Then $(E,w)=0 \iff w$ is a potential computation.

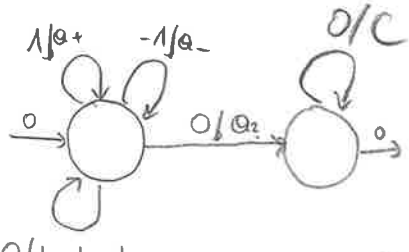
Considered as a series over $(\mathbb{Z} \cup \{-\infty\}, \max, +)$ E is recognizable:



ε



$\max\{|u|_{a_-} - |u|_{a_+} : u\}$
plus a similar fragment with a,b swapped



$\max\{|u|_{a_+} - |u|_{a_-} : ua_? \text{ prefix}\}$
plus fragment with a,b swapped

Let $\mathcal{A}$ be a 2CM.

Idea: Construct a recognizable $S_{\mathcal{A}}$ s.t.

$$E = S_{\mathcal{A}} \Leftrightarrow \mathcal{A} \text{ does not halt}$$

Then $E = S_{\mathcal{A}}$ is undecidable by Thm 4.2

Define $(S_{\mathcal{A}}, w) = \begin{cases} \max\{(E,w), 1\} & \text{if } w \text{ accepted by } \mathcal{A} \\ (E,w) & \text{if } w \text{ rejected by } \mathcal{A} \end{cases}$

$S_{\mathcal{A}}$ is recognizable: Let $L \subseteq C^*$ be the regular language accepted by $\mathcal{A}$. Then $\mathbb{1}_L$ with $(\mathbb{1}_L, w) = \begin{cases} 0 & \text{if } w \in L \\ -\infty & \text{if } w \notin L \end{cases}$ (indicator function) is recognizable (standing with the boolean automaton, set all weights to 0).

⚠ Hadamard product in this semiring, Thm 1.4

$$\Rightarrow S_{\mathcal{A}} = \max\{\max\{E, 1 + \mathbb{1}_{C^*}\} + \mathbb{1}_L \;,\; E + \mathbb{1}_{C^* \setminus L}\}$$

"plus" in $(\mathbb{Z} \cup \{\infty\}, \max, +)$; "product" in $(\mathbb{Z} \cup \{\infty\}, \max, +)$

$$= \left(\left(E \boxplus (1 \boxdot \mathbb{1}_{C^*})\right) \odot \mathbb{1}_L\right) \boxplus (E \odot \mathbb{1}_{C^* \setminus L})$$

with $\boxplus = \max$, $\boxdot = +$, $\odot$ = "Hadamard product" (elementwise $\boxdot = +$)

Now: $(S_{\mathcal{A}}, w) = (E, w) \Leftrightarrow w \notin L$ or $(E, w) > 0$

$\Leftrightarrow w \notin L$ or w is no potential computation

So $S_{\mathcal{A}} \neq E \Leftrightarrow \mathcal{A}$ accepts some potential computation

$\Leftrightarrow \mathcal{A}$ halts

Now over $\mathbb{N}_0 \cup \{-\infty\}$: Set $(E', w) := (E, w) + |w|$,

$(S_{\mathcal{A}}', w) := (S_{\mathcal{A}}, w) + |w|$

The WFA for E, $S_{\mathcal{A}}$ only use transition weights $0, 1, -1, -\infty$

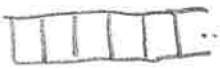
$\Rightarrow$ adding 1 to each transition weight produces WFA over $(\mathbb{N}_0 \cup \{-\infty\}, \max, +)$ recognizing E', $S_{\mathcal{A}}'$ $\square$

To show Thm 4.2 one proves universality of 2CM:

a 2CM can simulate an arbitrary Turing machine (TM) if the input/output is encoded in a suitable clever way.

SKETCH:

- TM: „computer program" consists of
  - finitely many states q_i with deterministic transitions (= a finite automaton) (= „locations in the code", „instructions")
  - a read/write tape that is infinite in one direction



  each cell contains 0 or 1; initialized to 0
  - current position on tape („head")
  - Can:
    - Move head one position left/right
    - Write 0 or 1 in current position
    - Read the tape and goto a different state depending on whether it is 0 or 1
    - Sense the end of the tape.

[Formally: Finite list of 5-tuples $q_i\, S_j \to S_{ij}\, q_{ij}\, d_{ij}$

q_* -- FA state (↑ location), S_* -- symbols (0/1), d_* direction (left/right)

- „If state is q_i and current symbol is S_j, write S_{ij} in current position, goto state q_{ij}, and move tape head in direction d_{ij}"
- If current state & symbol q_i, S_j don't match any 5-tuple, HALT]

The halting problem for TM is undecidable!

Complete state of TM at any moment:

(TM) current FA state (q) ⇝ (2CM) current FA state (q')

(finite) data on tape: $b_0 b_1 b_2 \dots b_m$ ⇝ counter a: $2^k 3^{2^x} = n$

position x of tape head ⇝ will $k = b_0 + b_1 2 + \dots + b_m 2^m$

Note: - Since 2, 3 are distinct primes, their exponents $(k, 2^x)$ are uniquely determined by n:

$$(\mathbb{N}, \cdot) \xrightarrow{\sim} (\mathbb{N}_0, +)^{(\mathbb{P})}$$

$$2^{n_1} 3^{n_2} 5^{n_3} 7^{n_4} \dots \longmapsto (n_1, n_2, n_3, n_4, \dots)$$

Using ℓ primes, we can embed $\mathbb{N}_0^\ell \hookrightarrow \mathbb{N}$.
In this way we can encode an ordered vector of nonnegative numbers into one counter
(But we also need to be able to compute with this data!)

- At any given moment, there is only a finite amount of data on the tape. k encodes this data by interpreting it as digits of a binary number.

Now: Instruction on TM ⇝ Sequence of Instructions on 2CM ("subroutine")

1st counter will hold the state of TM,
2nd counter is a "temporary register" that is 0 at the beginning & end of each subroutine simulating a TM instruction

Key Idea: For k and $\ell \in \mathbb{N}$ with $\gcd(k,\ell)=1$,
we can construct a subroutine $C(k,\ell)$ that replaces each k-factor in counter a by ℓ.

E.g. $2^k 3^{2^x} \xrightarrow{C(3,5)} 2^k 5^{2^x}$

How: We first create routines

- $MUL(\ell, q)$.. multiply counter a by the (constant) ℓ; then goto q
- $DIV(k, q_1, q_2)$ divide counter a by k; if not divisible by k, goto state q_1 (leaving a unchanged), otherwise goto q_2

E.g., $MUL(\ell)$ looks like:

```
            increment a
mulloop :   decrement a
            if a=0 goto copyback
            inc b
            inc b
              ⋮        } ℓ times
            inc b
            goto mulloop

copyback:   inc a
            dec b
            if b=0 goto q
            goto copyback
```

NOTE: $\ell, k, q, \ldots$ are not parameters but part of the name of the routine. We need a different routine for each set of these values that we are using

$DIV(k, q_1, q_2)$ looks similar, but we decrement a in the loop and each time have to check if it is 0. If we hit 0 in the middle of the loop, we can restore the previous state, because the exact point where we hit 0 tells us the remainder of counter a modulo k. (many gotos.. skipped)

Now: for $C(k,\ell)$: Repeatedly divide counter a by k and multiply it by ℓ

Eg. $2^3 3^{2^2} \xrightarrow{\text{DIV}(2)} 2^2 3^{2^2} \xrightarrow{\text{MUL}(5)} 5\cdot 2^2 3^{2^2} \xrightarrow{\text{DIV}(2)} 5\cdot 2\cdot 3^{2^2}$

$\xrightarrow{\text{MUL}(5)} 5^2\cdot 2\cdot 3^{2^2} \xrightarrow{\text{DIV}(2)} 5^2 3^{2^2} \xrightarrow{\text{MUL}(5)} 5^3\cdot 3^{2^2}$

Since k, ℓ are coprime this works without messing up the state.

Simulating TM-instructions:

(1) Moving the tape head

Position is „x" in $2^k 3^{2^x}$

Moving to the right $\hat{=}$ incrementing x . $2^k 3^{2^{x+1}} = 2^k 3^{2^x\cdot 2} = 2^k 9^{2^x}$

$\hat{=}$ squaring the 3

This would be „$C(3,9)$" but since 3 divides 9, we can't do that directly, use an extra prime temporarily:

$2^k 3^{2^x} \xrightarrow{C(3,5)} 2^k 5^{2^x} \xrightarrow{C(5,9)} 2^k 9^{2^x} = 2^k 3^{2^{x+1}}$

Moving to the left: - Can check end of tape ($x=0$) using DIV subroutine

- If $x>0$: $2^k 3^{2^x} \xrightarrow{C(9,5)} 2^k 5^{2^{x-1}} \xrightarrow{C(5,3)} 2^k 3^{2^{x-1}}$

$2^k 3^{2^x} = 2^k (9)^{2^{x-1}}$

(2) Writing on the tape:

state: $2^k 3^{2^x}$ $\quad k = k_0 + k_1 2 + k_2 4 + \dots + k_m 2^m$, $k_i \in \{0,1\}$

- If $k_x = 0$, and we want to change it to 1, we need to add 2^x to k, i.e. multiply counter a by 2^{2^x}.

„C(3,6)": $2^k 3^{2^x} \xrightarrow{C(3,5)} 2^k 5^{2^x} \xrightarrow{C(5,6)} 2^k 6^{2^x} = 2^k 2^{2^x} \cdot 3^{2^x}$

- If $k_x = 1$, and we want to change it to 0, we need to divide counter a by 2^{2^x}.

$$2^k 3^{2^x} = 2^{k-2^x} 6^{2^x} \xrightarrow{C(6,5)} 2^{k-2^x} 5^{2^x} \xrightarrow{C(5,3)} 2^{k-2^x} 3^{2^x}$$

(3) Reading the tape:

Need to determine if $k_x = 0$ or $k_x = 1$.

$$k = \sum_{j=0}^{m} k_j 2^j = \underbrace{\sum_{j=x+1}^{m} k_j 2^j}_{\text{divisible by } 2^x \text{ on an even number of times } (2^j = 2^{j-x} \cdot 2^x)} + k_x 2^x + \underbrace{\sum_{j=0}^{x-1} k_j 2^j}_{< 2^x, \text{ not div by } 2^x}$$

So $k_x = 1 \iff 2^x$ divides k on an odd number of times (division will remainder)

So:
- Repeatedly subtract 2^x from k, and keep track of parity of # of subtractions
- This will destroy 2^k, so we work on a copy

$$2^k 3^{2^x} \xrightarrow{C(2,5,7)} 5^k 7^k 3^{2^x} \xrightarrow{C(7,2)} 2^k 5^k 3^{2^x}$$

Now repeated application of what we did for writing ($k \rightsquigarrow k - 2^x$):

$$2^k 5^k 3^{2^x} \xrightarrow{C(5\cdot 3, 7)} 2^k 5^{k-2^x} 7^{2^x} \xrightarrow{C(5\cdot 7, 3)} 2^k 5^{k-2\cdot 2^x} \cdot 3^{2^x}$$

$\rightarrow \ldots$

- Termination of loop: need to check if $k \leq 2^x$ – in this case both 3 & 7 show up as not all of them can be substituted;

  E.g. $2 \cdot 5 \cdot 3^{2^2} \xrightarrow{C(5\cdot 3, 7)} 2 \cdot 3^{2^2-1} \cdot 7$

  Can test this with DIV
- Final state of termination encodes parity.

In conclusion: 2CM are Turing-complete, hence their halting problem is undecidable.

Remark: Many WFA properties lie right of the boundary between decidable & undecidable; often this is sensitive to the semiring, e.g.

	TROPICAL $(\mathbb{N}\cup\{\infty\}, \min, +)$	TROPICAL $(\mathbb{Z}\cup\{\infty\}, \min, +)$	FIELD $(\mathbb{Q}, +, \cdot)$
Non-emptiness $(\exists w: (S,w) \neq \infty)$	PTIME		PTIME
$\forall$-Universality $(\forall w: (S,w) < \infty)$	PSPACE	∪	∪ (here: $\mathrm{supp}(S) = A^*$)
Equality	∪		PTIME
Abs. upper boundedness $(\exists M \forall w: \lvert(S,w)\rvert < M)$	PSPACE-C		∪ (but decidable / $\mathbb{Z}$)

See: Almagor, Boker, Kupferman, "What is decidable about weighted automata?", 2020 for many more.

Sometimes properties become decidable if one restricts to a "nice" subclass of WFA (e.g. deterministic).
E.g. Universality in the trop. case becomes PTIME.

4 Rational Series in One Variable: Linear Recurrence Sequences

Let K be a field.

Def: A sequence $(a_n)_{n\geq 0}$, $a_n \in K$ is a linear recurrence sequence (LRS) if there exist $\alpha_1, \dots, \alpha_\ell \in K$ s.t.

$\forall n \geq \ell$: $a_n = \alpha_1 a_{n-1} + \dots + \alpha_\ell a_{n-\ell}$ (*).

A relation of the form (*) is a linear recurrence relation (LRR) of degree ℓ.

Let $A = \{x\}$, $K[\![x]\!] := K\langle\langle x \rangle\rangle$, $K[x] := K\langle x \rangle$. Elements of $K[\![x]\!]$ are formal (power) series in one variable

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

Note $S \in K[\![x]\!]^\times \iff (S, x^0) \in K^\times$

Prop 4.1: Let $S = \sum_{n=0}^{\infty} s_n x^n \in K[\![x]\!]$. TFAE:

(a) S is rational (i.e., contained in the smallest K-subalgebra of $K[\![x]\!]$ that contains $K[x]$ and is closed under inverses that exist in $K[\![x]\!]$)

(b) S is the formal power series expansion of P/Q with $P, Q \in K[x]$, $Q(0) \neq 0$.

(c) $(s_n)_{n\geq 0}$ is a LRS.

Proof: (a) $\Leftrightarrow$ (b) $R := \left\{ \frac{P}{Q} \in K(x) : Q(0) = 1 \right\}$ is closed under multiplication, addition, multiplication by scalars.

Since $Q \in K[x]$ with $Q(0) \neq 0$ is invertible in $K[\![x]\!]$, there is a monomorphism of K-algebras

$$R \hookrightarrow K[\![x]\!].$$

Since $K[x] \subseteq R$, and every element of R is rational (in the sense of (a)), it suffices to show that R is closed under inversion in $K[\![x]\!]$.

W.l.o.g. $P/Q \in R \cap K[\![x]\!]^\times$ with $Q(0) = 1$. Considering P/Q as power series, the constant coeff. is $\frac{P(0)}{Q(0)} = P(0) =: \lambda \in K^\times$.

$$\Rightarrow \frac{P}{Q} - \frac{\lambda^{-1} P}{\lambda^{-1} Q} \text{ and } \frac{\lambda^{-1} Q}{\lambda^{-1} P} \in R.$$

(a) $\Leftrightarrow$ (c) W.l.o.g. $I_S \trianglelefteq K[x]$ be the syndodic (right) ideal of S.

Then S rational $\overset{L3.1}{\Leftrightarrow}$ $K[x]/I_S$ finitely dimensional K-v.s.

$$\Leftrightarrow I_S \neq 0.$$

If $P = a_0 x^\ell - a_1 x^{\ell-1} - \ldots - a_\ell \in K[x]$, $a_0 \neq 0$, then

$$P \in I_S \Leftrightarrow 0 = S \circ P = \sum_{j=0}^{\ell} a_j (S \circ x^j) = \sum_{j=0}^{\ell} a_j \sum_{n=0}^{\infty} s_{n+j} x^j$$

$$= \sum_{n=0}^{\infty} \left(\sum_{j=0}^{\ell} a_j s_{n+j} \right) x^j$$

$$\Leftrightarrow \forall n \geq \ell: \quad a_0 s_n = -\sum_{j=1}^{\ell} a_j s_{n-j}.$$

So: S rational $\Leftrightarrow$ $(s_n)_{n \geq 0}$ LRS. $\square$

Cor 4.2 The monic elements of the syndactic ideal correspond bijectively to LRR satisfied by $(s_n)_{n\geq 0}$. There is a unique LRR of minimal degree (since $K[x]$ is a PID).

Def: The polynomial associated to the minimal LRR of S is called the minimal polynomial of S. Its roots are the eigenvalues of S.

Exercise: Prove (b) $\Leftrightarrow$ (c) of Thm 4.1 directly.

By Thm 4.1, every LRS has a (minimal) lin repr. Explicitly, there exist $\gamma \in K^{1\times d}$, $A \in K^{d\times d}$, $\lambda \in K^{d\times 1}$ s.t. $s_n = \gamma A^n \lambda \quad \forall n \geq 0$.

We give a direct proof as well.

Prop 4.3 Suppose $(s_n)_{n\geq 0}$ satisfies a LRR with associated polynomial $P = x^d - a_1 x^{d-1} - \dots - a_d \in K[x]$. Then $s_n = \gamma A^n \lambda$ with

$$\gamma = (1, 0, \dots, 0) \in K^{1\times d}, \quad A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & 1 & \ddots & 0 \\ & & \ddots & \ddots & \vdots \\ & & & \ddots & 0 \\ 0 & & & & 1 \\ a_d & a_{d-1} & \cdots & & a_1 \end{pmatrix} \in K^{d\times d}, \quad \lambda = \begin{pmatrix} s_0 \\ \vdots \\ s_{d-1} \end{pmatrix} \in K^{d\times 1}$$

(companion matrix of P)

Further, if P is the minimal polynomial of $S = \sum_{n\geq 0} s_n x^n$, then $(\gamma, x \mapsto A, \lambda)$ is a minimal lin. repr of S.

Proof: Note $A\lambda = \begin{pmatrix} s_1 \\ \vdots \\ s_{d-1} \\ s_d \end{pmatrix}$ since $s_d = a_d s_0 + \dots + a_1 s_{d-1}$

By induction, $A^n \lambda = \begin{pmatrix} s_n \\ \vdots \\ s_{n+d-1} \end{pmatrix}$ for all $n \geq 0$.

Hence $\forall n \geq 0: \gamma A^n \lambda = s_n$. Note that the minimal & characteristic polynomial of A are both P.

To show minimality: if P is minimal, suppose

$s_n = \gamma' (A')^n \lambda'$ for some $\gamma' \in K^{1 \times d'}$, $A' \in K^{d' \times d'}$, $\lambda' \in K^{d' \times 1}$.

Let P' be the characteristic polynomial of A', i.e.

$P' = \det(xI - A')$, say $P' = x^{d'} - \alpha'_1 x^{d'-1} - \cdots - \alpha'_{d'}$.

By Cayley-Hamilton, $P'(A') = 0$.

$\Rightarrow \forall n \geq 0: \quad 0 = \gamma' A^n P'(A') \lambda' = \gamma' A^{n+d'} \lambda' - \alpha'_1 \gamma' A^{n+d'-1} \lambda' - \cdots - \alpha'_{d'} \gamma' A^n \lambda'$

$\Rightarrow \forall n \geq 0: \quad s_{n+d'} = \alpha'_1 s_{n+d'-1} + \cdots + \alpha'_{d'} s_n$.

$\rightarrow (s_n)_{n \geq 0}$ satisfies a LRR of degree $d' \Rightarrow d' \geq d = \deg(P)$. □

Remark: Observe $A \in GL_d(K) \Leftrightarrow \det(A) \neq 0 \Leftrightarrow \alpha_d \neq 0$.

An LRR $s_n = \alpha_1 s_{n-1} + \cdots + \alpha_d s_{n-d}$ is strict if $\alpha_d \neq 0$;

A rational series S / LRS is strict if it satisfies some strict LRR.

Prop 44 Let $S = \sum_{n \geq 0} s_n x^n$ be a rational series. TFAE:

(a) S is strict
(b) the shortest LRR satisfied by S is strict
(c) $\exists P \in K[x]: \quad S \circ P = 0, \quad P(0) \neq 0$
(d) The min. poly of S has nonzero constant term

(e) The eigenvalues of S are nonzero

(f) S has a lin repr (λ, μ, γ) with $\mu(x)$ invertible

(g) In any minimal lin repr (λ, μ, γ) of S, $\mu(x)$ is invertible

(h) $S = P/Q$ with $P, Q \in K[X]$, $Q(0) \neq 0$, $\deg P < \deg Q$

(i) If $S = P/Q$ with P, Q coprime, then $\deg P < \deg Q$

Proof: Let P_0 be the minimal polynomial of S.

(a) $\Rightarrow$ (b) If P is the polynomial associated to a strict LRR for S, then $P(0) \neq 0$. Since P_0 divides P, also $P_0(0) \neq 0$

(b) $\Rightarrow$ (c) $S \cdot P_0 = 0$ and $P_0(0) = 0$.

(c) $\Rightarrow$ (a) ✓

(b) $\Leftarrow$ (d) $\Leftrightarrow$ (e) P_0 is the polynomial associated to the shortest LRR of S; its roots are the eigenvalues of S

(d) $\Rightarrow$ (g) By Prop 4.3 $\mu(x)$ is invertible for a minimal lin. repr. (and hence, for all minimal lin repr)

(g) $\rightarrow$ (f) ✓

(f) $\Rightarrow$ (d) Again by Prop 4.3,

(a) $\Rightarrow$ (h) Suppose $\exists d \geq 0$, $\alpha_1, \dots, \alpha_d \in K$, $\alpha_d \neq 0$ s.t.

$$\forall n \geq d: \quad s_n = \alpha_1 s_{n-1} + \dots + \alpha_d s_{n-d}$$

$$\Rightarrow \quad S - \alpha_1 X S - \dots - \alpha_d X^d S = (1 - \alpha_1 X - \dots - \alpha_d X^d) S$$

is a polynomial of degree $< d$

(h) $\Rightarrow$ (i) Cancelling common terms preserves $\deg P < \deg Q$

(i) $\Rightarrow$ (a) Wlog $Q = 1 - \alpha_1 X - \dots - \alpha_d X^d$ since $Q(0) \neq 0$.

$\Rightarrow QS = P$ with $\deg P < d \Rightarrow \forall n \geq d: s_n = \alpha_1 s_{n-1} + \dots + \alpha_d s_{n-d}$ □

Cor 4.5 If $S = P/Q$ with P, Q coprime, $Q(0)=1$ and $\deg P < \deg Q$, then Q is the reciprocal of the minimal polynomial of S, i.e. If $P_0 = X^d - a_1 X^{d-1} - \dots - a_d$ is the min. poly of S, then $Q = 1 - a_1 X - \dots - a_d X^d = X^d P_0(\frac{1}{X})$.

In a strict LRR, the recurrence can be used to compute coefficients forwards and backwards (for all $n \in \mathbb{Z}$).
In particular: If S satisfies an LRR of degree d, then any d consecutive coefficients of S determine all the others.

4.1 Exponential Polynomials

One way to solve a LRR (= obtaining a closed form expression for an LRS satisfying the LRR) is by taking a linear repr. and making the matrix A triangular, e.g. using Jordan normal form.
Another uses partial fraction decompositions + geometric series (& their derivatives).

Exm 4.6 (Fibonacci numbers) $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ $(n \geq 2)$ is a strict LRR. $F := \sum_{n \geq 0} F_n X^n$.

$$\Rightarrow F = 0 + X + \sum_{n \geq 2} F_n X^n = X + \sum_{n \geq 2} F_{n-1} X^n + \sum_{n \geq 2} F_{n-2} X^n$$

$$= X + X \sum_{n \geq 2} F_{n-1} X^{n-1} + X^2 \sum_{n \geq 2} F_{n-2} X^{n-2}$$

$\Rightarrow F = x + xF + x^2F$

$\Rightarrow (1-x-x^2)F = x \quad \Rightarrow \quad F = \frac{x}{1-x-x^2}$

roots of $1-x-x^2$ are $\varphi_1 = \frac{1+\sqrt{5}}{2}$ and $\frac{-3-\sqrt{5}}{2} = \bar{\varphi}-1$, with $\bar{\varphi} = \frac{1-\sqrt{5}}{2}$

$(\varphi^2 = \varphi+1, \quad \bar{\varphi}^2 = \bar{\varphi}+1, \quad \varphi+\bar{\varphi}=1, \quad \varphi\bar{\varphi} = -1)$

Partial Frac. Decomposition $\Rightarrow F = \frac{1}{\sqrt{5}} \frac{1}{1-\varphi x} - \frac{1}{\sqrt{5}} \frac{1}{1-\bar{\varphi}x}$

Geometric series expansion

$\Rightarrow F_n = \frac{1}{\sqrt{5}} (\varphi^n - \bar{\varphi}^n)$.

Prop 4.7 For every rational series $S \in K[[x]]$ there exists a unique polynomial P and a unique strict rational series T s.t. $S = P+T$

Proof: **Ex:** Suppose $S = A/Q$ with $A, Q \in K[x]$, $Q(0) \neq 1$

$\Rightarrow A = BQ + R$ with $\deg(R) < \deg(Q)$ (polynomial division)

$\Rightarrow S = B + R/Q$

Uniqueness: Suppose $S = P_i + \frac{R_i}{Q_i}$ $i=1,2$ with $\deg(R_i) < \deg(Q_i)$

replacing Q_i by Q_1Q_2 wlog $Q_1 = Q_2 =: Q$

$\Rightarrow SQ = P_iQ + R_i$, $i=1,2$, $\deg(R_i) < \deg(Q)$

$\Rightarrow P_1 = P_2$, $R_1 = R_2$ by uniqueness of polynomial division

□

Suppose now: **char K = 0**

Let $\Lambda := K^\times$ (multiplicative group), t an indeterminate

We consider the group algebra of Λ over the polynomial ring $K[t]$, i.e. $K[t][\Lambda]$ consists of sums of the form

$$P_1(t)\lambda_1 + \dots + P_e(t)\lambda_e \quad \text{with } P_i \in K[t],\ \lambda_i \in \Lambda$$

If we take λ_i pairwise distinct, these representations are (by definition) unique; they are added and multiplied in the obvious way. Elements of $K[t][\Lambda]$ are called exponential polynomials.

Theorem 4.8 Let K be algebraically closed (and char $K=0$):

There is a K-vector space isomorphism

$$\Phi: \begin{cases} K[t][\Lambda] \longrightarrow \{\text{strict rational series}\} \\ \sum_{\lambda\in\Lambda} P_\lambda(t)\lambda \longmapsto \sum_{n\geq 0} s_n x^n, \quad s_n = \sum_{\lambda\in\Lambda} P_\lambda(n)\lambda^n. \end{cases}$$

Multiplication of exponential polynomials corresponds to the Hadamard product of strict rational series. In particular, strict rational series are closed under the Hadamard product.

Exm: $\dfrac{1}{(1-\alpha x)} = \sum_{n\geq 0} \alpha^n x^n$, exp poly: α

$$\frac{1}{(1-x)^2} = \sum_{n\geq 0} (n+1)x^n, \quad \text{exp poly } n+1$$

Suppose now: **char K = 0**

Let $\Lambda := K^\times$ (multiplicative group), t an indeterminate.

We consider the group algebra of Λ over the polynomial ring $K[t]$, i.e. $K[t][\Lambda]$ consists of sums of the form

$$P_1(t)\lambda_1 + \dots + P_e(t)\lambda_e \quad \text{with } P_i \in K[t],\ \lambda_i \in \Lambda$$

If we take λ_i pairwise distinct, these representations are (by definition) unique; they are added and multiplied in the obvious way. Elements of $K[t][\Lambda]$ are called exponential polynomials.

Theorem 4.8 Let K be algebraically closed (and char $K=0$).

There is a K-vector space isomorphism

$$\Phi: \begin{cases} K[t][\Lambda] \longrightarrow \{\text{strict rational series}\} \\ \sum_{\lambda\in\Lambda} P_\lambda(t)\lambda \longmapsto \sum_{n\geq 0} s_n x^n, \quad s_n = \sum_{\lambda\in\Lambda} P_\lambda(n)\lambda^n. \end{cases}$$

Multiplication of exponential polynomials corresponds to the Hadamard product of strict rational series. In particular, strict rational series are closed under the Hadamard product.

Exm: $\dfrac{1}{(1-\alpha x)} = \sum_{n\geq 0} \alpha^n x^n$, exp poly: α

$$\frac{1}{(1-x)^2} = \sum_{n\geq 0} (n+1)x^n, \quad \text{exp poly } n+1$$

Proof: $\overline{\Phi}(P+Q) = \overline{\Phi}(P) + \overline{\Phi}(Q)$, $\overline{\Phi}(PQ) = \overline{\Phi}(P) \odot \overline{\Phi}(Q)$ are easy to see, so we just need to show that $\overline{\Phi}$ is a bijection.

Fix $d \geq 1$, $\alpha_1, \dots, \alpha_d \in K$, $\alpha_d \neq 0$ and let $V \subseteq K[[x]]$ consist of all series whose coefficients $(s_n)_{n \geq 0}$ satisfy the LRR

$$(*) \quad s_n = \alpha_1 s_{n-1} + \dots + \alpha_d s_{n-d} \qquad \forall n \geq d.$$

Then V is a K-vector space. Further $\dim V = d$.
(a basis can be obtained by setting for each $0 \leq i \leq d-1$, $s_i = 1$, $s_j = 0$ if $j \neq i$, $0 \leq j \leq d-1$, and s_n according to $(*)$ for $n \geq d$)

Let $\lambda_1, \dots, \lambda_e \in K$ be the (pairwise distinct) roots of

$$x^d - \alpha_1 x^{d-1} - \dots - \alpha_d \in K[x],$$ and m_i the multiplicity of λ_i.
Let

$$W = \left\{ \sum_{i=1}^{e} P_i(t) \lambda_i \in K[t][\Lambda] : \deg P_i \leq m_i - 1 \right\}$$

Then $W \subseteq K[t][\Lambda]$ is a vector space of dimension $m_1 + \dots + m_e = d$.

To conclude, we show $\overline{\Phi}|_W : W \to V$ is surjective (and hence an isomorphism).
Let $S = \sum_{n \geq 0} s_n x^n \in V$. Then $S = P/Q$ with

$$Q = 1 - \alpha_1 x - \dots - \alpha_d x^d \quad \text{(reciprocal)}$$

The roots of Q are $1/\lambda_1, \dots, 1/\lambda_e$, so partial fraction decomposition gives

$$S = \sum_{j=1}^{e} \sum_{i=1}^{m_j} \frac{\gamma_{j,i}}{(1-x\lambda_j)^i} \quad \text{with } \gamma_{j,i} \in K$$

Now $\frac{1}{(1-x\lambda_j)^i} = \sum_{n=0}^{\infty} \binom{n+i-1}{i-1} \lambda_j^n x^n$ (since $\frac{1}{1-x\lambda_j} = \sum_{n=0}^{\infty} \lambda_j^n x^n$, then use induction + formal differentiation)

$n \longmapsto \binom{n+i-1}{i-1} = \frac{(n+i-1)\cdots(n+1)}{(i-1)!}$ is a polynomial function in n of degree $i-1 \leq m_i - 1$

$\Rightarrow \frac{1}{(1-x\lambda_j)^i} \in \mathbb{D}(W)$ and hence $S \in \mathbb{D}(W)$. □

Cor 4.9 Let $S = \sum_{n=0}^{\infty} s_n x^n$ be a rational series over an alg. closed field K of characteristic 0.

(1) For sufficiently large n,

$$s_n = \sum_{i=1}^{e} P_i(n) \lambda_i^n \quad \text{with } \lambda_i \in K^\times,\ P_i \in K[t]$$

(2) The expression in (1) is unique if the λ_i are pairwise distinct.
In particular: The λ_i's with $P_i \neq 0$ are the eigenvalues of S.

Proof: By 4.7 and 4.8 (including the respective uniqueness statements) □

4.3 The Skolem - Mahler - Lech Theorem

An (infinite) arithmetic progression is a set of the form $A_{m,n} := \{mk+n : k \in \mathbb{N}_0\}$ where $m \in \mathbb{N}$, $n \in \mathbb{N}_0$

$$\{n, n+m, n+2m, \dots\} = n + m\mathbb{N}_0$$

Theorem 4.10 (SML) Let K be a field of characteristic 0, $S = \sum_{n \geq 0} s_n x^n \in K[[x]]$ rational. Then

$$\{n \in \mathbb{N}_0 : s_n = 0\}$$

is a union of a finite set and finitely many arithmetic progressions.

History: Skolem (1934) for $K = \mathbb{Z}$; Mahler (1935) for number fields; Lech (1953) for all fields of characteristic 0.

The proof uses some number theory (p-adic analysis), but can be recast in an elementary way.

Def: (1) $A \subseteq \mathbb{N}_0$ is purely periodic if $\exists N \geq 0$ and $0 \leq k_1, \dots, k_r \leq N-1$ s.t.

$$A = \{k_i + nN : n \in \mathbb{N}_0,\ 1 \leq i \leq r\} = \{k_1, \dots, k_r\} + N\mathbb{N}_0$$

N is called a period of A

(2) $A \subseteq \mathbb{N}_0$ is quasi-periodic (of period N) if it is a union of a finite set and a purely periodic set (of period N)

Lemma 4.11 If $(A_i)_{i\in I}$ is a family of quasi-periodic sets of period N, then $\bigcap_{i\in I} A_i$ is quasi-periodic of period N.

Proof: For $0 \le j \le N-1$ and $i \in I$, the set

$$(j + N\mathbb{N}_0) \cap A_i$$

is either finite or equal to $j + N\mathbb{N}_0$.

Then
$$(j+N\mathbb{N}_0) \cap \left(\bigcap_{i\in I} A_i\right) = \begin{cases} j+N\mathbb{N}_0 & \text{if } (j+N\mathbb{N}_0)\cap A_i = j+N\mathbb{N}_0 \text{ for all } i\in I \\ \text{finite} & \text{otherwise.} \end{cases}$$

But then $\bigcap_{i\in I} A_i$ is quasi-periodic of period N. □

Def: For $S = \sum_{n\ge 0} s_n x^n \in K[[x]]$, let

$$\mathrm{ann}(S) = \{ n \in \mathbb{N}_0 : a_n = 0 \} = \mathbb{N}_0 \setminus \{ n : x^n \in \mathrm{supp}(S) \}$$

Prop 4.12 (Key Prop for SHL) If $S = \sum_{n\ge 0} s_n x^n \in \mathbb{Q}[[x]]$ is a strict rational series, then $\mathrm{ann}(S)$ is quasi-periodic.

Proving Prop 4.12 is the hardest part of SHL. We need several preparatory Lemmas.

Fix a prime number p. Every $a \in \mathbb{Q}\setminus\{0\}$ can be written as

$$a = p^e \frac{m}{n} \quad \text{with } m,n \in \mathbb{Z}\setminus\{0\},\ p\nmid m,\ p\nmid n,\ e\in\mathbb{Z}.$$

The **p-adic valuation** of a is

$$v_p(a) = \begin{cases} e & \text{if } a \neq 0 \\ \infty & \text{if } a = 0. \end{cases}$$

$v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is a discrete valuation, i.e.

(1) $v_p(ab) = v_p(a) + v_p(b)$ for all $a, b \in \mathbb{Q}$

(2) $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$ for all $a, b \in \mathbb{Q}$

(3) $v_p(a) = \infty \iff a = 0$

[Here $a + \infty = \infty + \infty = \infty$ and $a < \infty$ for all $a \in \mathbb{Q}$]

Lemma 4.13 (Legendre) $v_p(n!) = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor = \frac{n - s_p(n)}{p-1} \leq \frac{n}{p-1}$

Here $s_p(n)$ is the digit sum of n in base p.

Proof: (i) $n! = n \cdot (n-1) \cdots 2 \cdot 1$

So each multiple of p that is $\leq n$ contributes at least one p-factor to $n!$: $kp \leq n \iff k \leq \left\lfloor \frac{n}{p} \right\rfloor$, so there are $\left\lfloor \frac{n}{p} \right\rfloor$ of those.

Each multiple of p^2 contributes at least one extra factor p $\rightsquigarrow$ $\left\lfloor \frac{n}{p^2} \right\rfloor$ of those, and so on ...

(Note the "infinite sum" is actually finite bec. $\left\lfloor \frac{n}{p^j} \right\rfloor = 0$ if $p^j \geq n$)

(ii) Let $n = \sum_{j=0}^{k} n_j p^j$ with $n_j \in \{0, \ldots, p-1\}$.

Then $s_p(n) = \sum_{j=0}^{k} n_j$.

$$\sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor = \sum_{j=1}^{k} \left\lfloor \frac{n_k p^k + \ldots + n_1 p + n_0}{p^j} \right\rfloor = \sum_{j=1}^{k} \left(n_k p^k + \ldots + n_j p^j\right) p^{-j}$$

$$= \sum_{j=1}^{k} \sum_{i=j}^{k} n_i p^{i-j} = \sum_{i=1}^{k} \sum_{j=1}^{i} n_i p^{i-j} = \sum_{i=1}^{k} n_i \left(\frac{p^i - 1}{p-1}\right) =$$

↑ geom. sum

$$\frac{1}{p-1}\left(\sum_{i=1}^{k} n_i p^i - \sum_{i=1}^{k} n_i\right) = \frac{n - s_p(n)}{p-1}.$$

□

As consequence: $\underline{v_p\left(\frac{p^n}{n!}\right) = n - v_p(n!) \geq n - \frac{n}{p-1} = n\frac{(p-2)}{(p-1)}}$.

For a polynomial $P = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Q}[x]$ and $k \geq 0$, let

$$\omega_k(P) := \min\{ v_p(a_j) : j \geq k \}.$$

Then: (i) $\omega_0(P) \leq \omega_1(P) \leq \dots$ and $\omega_k(P) = \infty$ if $k > n$.

(ii) $\forall m \in \mathbb{Z}$: $\underline{v_p(P(m)) \geq \omega_0(P)}$

[Since: $v_p(P(m)) \geq \min\{ v_p(a_0), v_p(a_1 m), \dots, v_p(a_n m^n) \}$

$\geq \min\{ v_p(a_0), v_p(a_1), \dots, v_p(a_n) \} = \omega_0(P)$]

Lemma 4.14 Let $Q \in \mathbb{Q}[x]$, $t_1, \dots, t_k \in \mathbb{Z}$ and

$$P = (x - t_1) \cdots (x - t_k) Q \quad \in \mathbb{Q}[x].$$

Then $\omega_k(P) \leq \omega_0(Q)$.

Proof: It suffices to show: If $P = (x-t)Q$ with $t \in \mathbb{Z}$, then $\omega_{k+1}(P) \leq \omega_k(Q)$ for all $k \geq 0$.

(Then $\omega_k(P) \leq \omega_{k-1}\left((x-t_2)\cdots(x-t_k)Q\right)\right) \leq \dots \leq \omega_0(Q)$)

Suppose $Q = a_0 + a_1 x + \dots + a_n x^n$, $P = b_0 + b_1 x + \dots + b_{n+1} x^{n+1}$, and $P = (x-t)Q$.

$\Rightarrow$ $\underline{b_{n+1} = a_n}$, $\underline{b_{j+1} = a_j - t a_{j+1}}$ for $0 \leq j \leq n-1$.

$$\Rightarrow \quad a_j = b_{j+1} + t b_{j+2} + \dots + t^{n-j} b_{n+1} \qquad (0 \le j \le n)$$

$$\Rightarrow \quad v_p(a_j) \ge \min\{ v_p(b_{j+1}),\ v_p(t b_{j+2}),\ \dots,\ v_p(t^{n-j} b_{n+j}) \}$$
$$\ge \omega_{j+1}(P) \quad \text{for } \underline{\text{all } j}$$

$$\Rightarrow \forall j \ge k: \quad v_p(a_j) \ge \omega_{j+1}(P) \ge \omega_{k+1}(P)$$

$$\Rightarrow \quad \omega_k(Q) \ge \omega_{k+1}(P).$$

□

Lemma 4.15 Let $(d_n)_{n\ge 0}$ be a sequence of integers and p an odd prime. Let

$$b_n := \sum_{i=0}^{n} \binom{n}{i} p^i d_i \qquad \text{for } n \ge 0.$$

If $b_n = 0$ for infinitely many n, then $b_n = 0$ for all $n \ge 0$.

Proof: We can think of $\binom{n}{i}$ as the evaluation of a polynomial

$$\binom{x}{i} = \frac{x(x-1)\cdots(x-i+1)}{i!} \in \mathbb{Q}[x] \quad \text{at } x = n.$$

Define $$R_n := \sum_{i=0}^{n} d_i p^i \binom{x}{i} \in \mathbb{Q}[x].$$

If $t \in \mathbb{N}_0$ and $i \ge t$, then $\binom{t}{i} = 0$.

So $$b_t = R_t(t) = R_n(t) \quad \text{for all } n \ge t.$$

Claims: (i) $\forall k, n \ge 0$: $\omega_k(R_n) \ge k\,\frac{p-2}{p-1}$

(ii) $\forall k, t \ge 0$: $v_p(b_t) \ge k\,\frac{p-2}{p-1}$

By taking $k \to \infty$ in (ii), then necessarily $b_t = 0$ for all $t \ge 0$.

(i) Let $R_n = \sum_{k=0}^{n} c_{n,k} x^k$ with $c_{n,k} \in \mathbb{Q}$

Each $c_{n,k}$ is an integral linear combination of numbers of the form $\frac{d_i p^i}{i!}$ with $k \le i \le n$.

$$\Rightarrow v_p(c_{n,k}) \ge \min\left\{ v_p\left(\underbrace{d_i}_{\in \mathbb{Z}} \frac{p^i}{i!}\right) : k \le i \le n \right\}$$

$$\ge \min\left\{ i \frac{p-2}{p-1} : k \le i \le n \right\} \ge k \frac{p-2}{p-1}$$

↑ Legendre formula

$$\Rightarrow \omega_k(R_n) \ge k \frac{p-2}{p-1}$$

(ii) Fix $k \ge 0$. Since $b_t = 0$ for infinitely many $t \ge 0$, we can take the first $0 \le t_1 < t_2 < \dots < t_k$ s.t. $b_{t_i} = 0$.

Let $n \ge \max\{t, t_k\}$

$$\Rightarrow R_n(t_i) = b_{t_i} = 0 \quad \forall 1 \le i \le k$$

$$\Rightarrow R_n = (x - t_1) \cdots (x - t_k) Q \quad \text{with } Q \in \mathbb{Q}[x]$$

$$\Rightarrow \omega_k(R_n) \overset{L4.14}{\le} \omega_0(Q).$$

$$v_p(b_t) = v_p(R_n(t)) \ge v_p(Q(t)) \ge \omega_0(Q) \ge \omega_k(R_n) \overset{(i)}{\ge} k \frac{p-2}{p-1}$$

↑ $n \ge t$; ↑ $Q(t)$ divides $R_n(t)$

□

Prop 4.16 (SML for $K = \mathbb{Z}$) Let $S = \sum_{n \ge 0} s_n x^n \in \mathbb{Z}[\![x]\!]$ be a strict rational series, and (λ, μ, γ) a linear representation of S of dimension d (w/ all coefficients in $\mathbb{Z}$).

If p is an odd prime with $p \nmid \det(\mu(x))$, then $\operatorname{ann}(S)$ is quasi-periodic of period $N = |GL_d(\mathbb{Z}/p\mathbb{Z})|$.

(i) Let $R_n = \sum_{k=0}^{n} c_{n,k} x^k$ with $c_{n,k} \in \mathbb{Q}$

Each $c_{n,k}$ is an integral linear combination of numbers of the form $\frac{d_i p^i}{i!}$ with $k \le i \le n$.

$$\Rightarrow v_p(c_{n,k}) \geq \min\left\{ \underbrace{v_p\left(d_i \frac{p^i}{i!}\right)}_{\in \mathbb{Z}} : k \le i \le n \right\}$$

$$\geq \min\left\{ i \frac{p-2}{p-1} : k \le i \le n \right\} \geq k \frac{p-2}{p-1}$$

↑ Legendre formula

$$\Rightarrow \omega_k(R_n) \geq k \frac{p-2}{p-1}$$

(ii) Fix $k \geq 0$. Since $b_t = 0$ for infinitely many $t \geq 0$, we can take the first $0 \le t_1 < t_2 < \dots < t_k$ s.t. $b_{t_i} = 0$.

Let $n \geq \max\{t, t_k\}$

$$\Rightarrow R_n(t_i) = b_{t_i}^{(i)} = 0 \quad \forall 1 \le i \le k$$

$$\Rightarrow R_n = (x - t_1) \cdots (x - t_k) Q \quad \text{with } Q \in \mathbb{Q}[x]$$

$$\Rightarrow \omega_k(R_n) \overset{L4.14}{\leq} \omega_0(Q).$$

$$v_p(b_t) \overset{n \geq t}{=} v_p(R_n(t)) \geqslant v_p(Q(t)) \geqslant \omega_0(Q) \geqslant \omega_k(R_n) \overset{(i)}{\geq} k \frac{p-2}{p-1}$$

↑ $Q(t)$ divides $R_n(t)$

□

Prop 4.16 (SML for $K = \mathbb{Z}$) Let $S = \sum_{n \geq 0} s_n x^n \in \mathbb{Z}[\![x]\!]$ be a strict rational series, and (λ, μ, γ) a linear representation of S of dimension d (with all coefficients in $\mathbb{Z}$).

If p is an odd prime with $p \nmid \det(\mu(x))$, then $\operatorname{ann}(S)$ is quasi-periodic of period $N = |GL_d(\mathbb{Z}/p\mathbb{Z})|$.

Proof: Let $n \mapsto \bar{n}$ denote the canonical epimorphism from $\mathbb{Z}$ to the field $\mathbb{Z}/p\mathbb{Z}$.

Since $\det(\overline{\mu(x)}) = \overline{\det(\mu(x))}$, $\overline{\mu(x)} \in GL_d(\mathbb{Z}/p\mathbb{Z})$.

Since $GL_d(\mathbb{Z}/p\mathbb{Z})$ is a finite group of cardinality N, then $\overline{\mu(x^N)} = \bar{I}$.

$\Longrightarrow \mu(x^N) = I + pB$ for some $B \in \mathbb{Z}^{d \times d}$.

For $0 \leq j \leq N-1$, $n \geq 0$

$$a_{j+nN} = \lambda \mu(x^{j+nN}) \gamma = \lambda \mu(x^j) (I + pB)^n \gamma =$$

$$= \sum_{i=0}^{n} \binom{n}{i} p^i \underbrace{\lambda \mu(x^j) B^i \gamma}_{=: d_i \in \mathbb{Z}}$$

binomial theorem (works bec. I, B commute)

Set $b_n := a_{j+nN}$ (j, N fixed)

$$\Longrightarrow b_n = \sum_{i=0}^{n} \binom{n}{i} p^i d_i$$

By Lemma 4.15, $(b_n)_{n \geq 0}$ either contains finitely many zero terms or vanishes completely. Since this is true for all $0 \leq j \leq N$, $\mathrm{ann}(S)$ is quasi-periodic with period N. $\square$

Proof of Prop 4.12 (SML for strict series $/\mathbb{Q}$)

Let (λ, μ, γ) be a lin repr of S, with $\mu(x)$ invertible (by strictness, Prop 4.4). Let $m \in \mathbb{N}$ be a common denominator of all entries of λ, μ, γ.

Then $(m\lambda, m\mu, m\gamma)$ is a strict $\mathbb{Z}$-linear representation, recognizing S' with $(S', x^n) = m^{n+2}(S, x^n)$.

Since $\mathrm{ann}(S) = \mathrm{ann}(S')$, the claim follows from Prop. 4.16. □

Intermezzo: p-adic analysis (i.e., where is Lemma 4.15 coming from)

Fix $p \in \mathbb{P}$, for $a \in \mathbb{Q}$ define $|a|_p := p^{-v_p(a)}$.

Then $|a|_p = 0 \Leftrightarrow a = 0$ $(\Leftrightarrow v_p(a) = \infty)$,

$|ab|_p = |a|_p |b|_p$,

$|a+b|_p \leq \max\{|a|_p, |b|_p\} \leq |a|_p + |b|_p$

↑ stronger than Δ-inequality!

So $|\cdot|_p : \mathbb{Q} \longrightarrow \mathbb{R}_{\geq 0}$ is an absolute value. Since $|a+b|_p \leq \max\{|a|_p, |b|_p\}$ it is called non-archimedean.

Here a is p-adically "small" if it is often divisible by p, e.g. $|p^n|_p = p^{-n} \to 0$ as $n \to \infty$

$|\cdot|_p$ induces an (ultra) metric: $d_p(a,b) := |a-b|_p$, and hence a topology on $\mathbb{Q}$.

FACT: Up to equivalence (= inducing the same topology), the abs. values on $\mathbb{Q}$ are precisely the archimedean (= usual) absolute value $|\cdot| = |\cdot|_\infty$ and $\{|\cdot|_p : p \in \mathbb{P}\}$ (Ostrowski's Theorem).

One can define convergence of sequences $\left((a_n)_{n\geq 0} \to 0 \Leftrightarrow (|a_n|_p)_{n\geq 0} \to 0\right)$ and Cauchy sequences w.r.t. $|\cdot|_p$.

In the same way $\mathbb{R}$ is constructed from $\mathbb{Q}$ as a completion using Cauchy sequences (ring of Cauchy sequences, modulo ideal of sequences converging to 0), the p-adic field $\mathbb{Q}_p$ is obtained from $|\cdot|_p$:

$$\{(a_n)_{n\geq 0} : (a_n)_{n\geq 0} \text{ p-adic Cauchy seq. over } \mathbb{Q}\} \Big/ \{(a_n)_{n\geq 0} : (a_n)_{n\geq 0} \xrightarrow{\text{p-adically}} 0\}.$$

This gives a field $\mathbb{Q}_p$ (p-adic numbers), elements can be represented as

$$\sum_{n=-m}^{\infty} a_n p^n, \qquad a_n \in \{0, \dots, p-1\}.$$

↑ converges, bec $p^n \to 0$

[Fun fact: $\sum_{n=0}^{\infty} b_n$ converges $\iff (b_n)_{n\geq 0} \to 0$ bec. of non archimedean property]

E.g. in $\mathbb{Q}_2$: $-1 = \frac{1}{1-2} = \sum_{n=0}^{\infty} 2^n$.

⚠ char $\mathbb{Q}_p = 0$, not p!

$|\cdot|_p$ extends to $\mathbb{Q}_p$ by $\left|\sum_{n=-m}^{\infty} a_n p^n\right|_p = p^m$ if $a_m \neq 0$

$\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a|_p \leq 1\} = \left\{\sum_{n=0}^{\infty} a_n p^n : a_n \in \{0, \dots, p-1\}\right\}$

is a subring. (p-adic integers)

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathbb{Z}_p \\ \downarrow & \text{dense} \uparrow\downarrow & \downarrow \\ \mathbb{Q} & \hookrightarrow & \mathbb{Q}_p \end{array}$$

$\mathbb{Q}_p$ is complete, Hausdorff, locally compact, totally disconnected

Algebraic closure $\overline{\mathbb{Q}_p}$: alg. closed, no longer complete wrt $|\cdot|_p$,

$\dim_{\mathbb{Q}_p} \overline{\mathbb{Q}}_p = \infty$

(Compare: $\dim_{\mathbb{R}} \mathbb{C} = 2$, $\mathbb{C}$ is alg. closed AND complete)

Take completion of $\overline{\mathbb{Q}}_p$ again $\rightsquigarrow \mathbb{C}_p$ complete and also still algebraically closed! (But $\mathbb{C}_p$ is not locally compact)

In $\mathbb{C}_p$ one can do analysis!

There is a notion of power series, and we can use it to define $\exp_p$ and $\log_p$

$$\exp_p : \begin{cases} \{x \in \mathbb{C}_p : |x|_p < p^{\frac{-1}{p-1}}\} & \longrightarrow \mathbb{C}_p \\ x & \longmapsto \sum_{n=0}^{\infty} \frac{x^n}{n!} \end{cases}$$

$$\log_p : \begin{cases} \{x \in \mathbb{C}_p : |x-1|_p < 1\} & \longrightarrow \mathbb{C}_p \\ x & \longmapsto \log_p(1+(x-1)) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n} \end{cases}$$

⚠ Because $\left|\frac{1}{n!}\right|_p \to \infty$ as $n \to \infty$, the series for $\exp_p$ does not converge on all of $\mathbb{C}_p$.

FACT: If $f = \sum_{n=0}^{\infty} a_n x^n$ converges in some open disc $D \subseteq \mathbb{C}_p$, and there is a convergent sequence $(x_n)_{n \geq 0}$ in D s.t. $f(x_n) = 0 \ \forall n \geq 0$, then $f \equiv 0$.

Note: $\mathbb{Z}$ contains convergent sequences (e.g. $(p^n)_{n \geq 0} \to 0$), so if f vanishes on $\mathbb{Z}$, it vanishes everywhere ($\mathbb{Z}$ is p-adically dense in $\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$)

Back to SHL: Consider $(a_n)_{n \geq 0}$ a strict $\mathbb{Z}$-LRS, as in Prop 4.16

$$\Rightarrow \quad a_n = P_1(n)\lambda_1^n + \dots + P_e(n)\lambda_e^n \quad \text{with } \lambda_i \in \mathbb{C}_p, \ P_i \in \mathbb{Q}[x]$$

Taking N as in 4.16 ($A^N \equiv I \bmod p$) $\Rightarrow |\lambda_i^N - 1|_p < 1$

$$\Rightarrow \quad a_{nN} = \sum_{i=1}^{e} P_i(n) \exp_p\left(n \log_p(\lambda_i^N)\right)$$

Define p-adic power series: $f(x) := \sum_{i=1}^{e} P_i(x) \exp_p\left(x \log_p(\lambda_i^N)\right)$

(so $f(n) = a_{nN}$ interpolates the subsequence $(a_{nN})_{n \geq 0}$)

Now f converges on a disc around 0.
So either $f(nN) \neq 0$ for all suff. large n or
$f(nN) = 0$ for all sufficiently large n.
(Deal with $f(j+nN)$ similarly).

Thus: SML follows from an identity theorem for p-adic power series.

(END OF INTERMEZZO) (Good Intro: F.Q. Gouvêa: p-adic Numbers - An Introduction)

Still have to do SML for other fields of char 0!

From field theory we know that if $K \subseteq L$ is a field extension, then exists an intermediate field M

s.t.
$$\left.\begin{matrix} L \\ | \\ M \end{matrix}\right\} \text{algebraic}$$
$$\left.\begin{matrix} M \\ | \\ K \end{matrix}\right\} \text{purely transcendental, i.e. } M = K(X) \text{ rational function field in the indeterminate } X$$

If L/K is f.g. as field ext, then $M = K(x_1, \dots, x_n) = \left\{ \frac{P}{Q} : P, Q \in K[x_1, \dots, x_n], Q \neq 0 \right\}$

and L/M is finite-dimensional (as M-vector space)

→ 2 steps (transcendental, then algebraic)

Def: A field K is an SML-field if it satisfies the conclusion of Thm 4.10 (SML)

By 4.12, $\mathbb{Q}$ is an SML-field

Lemma 4.17 K field, $P \in K[x_1, \dots, x_n]$, $d_i := \deg_{x_i}(P)$.
If $A_1, \dots, A_n \subseteq K$ are such that $|A_i| \geq d_i$ and

$$f(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in A_1 \times \dots \times A_n,$$

then $f = 0$.

Now f converges on a disc around 0.
So either $f(nN) \neq 0$ for all suff. large n or
$f(nN) = 0$ for all sufficiently large n.
(Deal with $f(j+nN)$ similarly).

Thus: SML follows from an identity theorem for p-adic power series.

(END OF INTERMEZZO) (Good Intro: F.Q. Gouvêa: p-adic Numbers - An Introduction)

Still have to do SML for other fields of char 0!

From field theory we know that if $K \subseteq L$ is a field extension, there exists an intermediate field M

s.t. $\left.\begin{matrix} L \\ | \\ M \end{matrix}\right\}$ algebraic

$\left.\begin{matrix} M \\ | \\ K \end{matrix}\right\}$ purely transcendental, i.e. $M = K(X)$ rational function field in the indeterminates

X

If L/K is f.g. as field ext, then $M = K(x_1, \dots, x_n) = \left\{ \frac{P}{Q} : P, Q \in K[x_1, \dots, x_n], Q \neq 0 \right\}$

and L/M is finite-dimensional (as M-vector space)

→ 2 Steps (transcendal, then algebraic)

Def: A field K is an SML-field if it satisfies the conclusion of Thm 4.10 (SML)

Eg 4.12, $\mathbb{Q}$ is an SML-field

Lemma 4.17 K field, $P \in K[x_1, \dots, x_n]$, $d_i := \deg_{x_i}(P)$.
If $A_1, \dots, A_n \subseteq K$ are such that $|A_i| > d_i$ and

$$f(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in A_1 \times \dots \times A_n,$$

then $f = 0$.

Proof: Exc, by induction from the univariate case

(N.B.: The assumption can be made weaker, leading to Noga Alon's Combinatorial Nullstellensatz)

Lemma 4.18 Let $0 \neq P \in \mathbb{Z}[x_1, \dots, x_n]$. For all but finitely many primes p, there exist $a_1, \dots, a_n \in \mathbb{Z}$ s.t.

$$P(a_1, \dots, a_n) \not\equiv 0 \mod p.$$

Proof: Let $P = \sum_{(i_1, \dots, i_n)} c_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n}$.

Let $p \in \mathbb{P}$ be s.t. $p > \max\{d_1, \dots, d_n\}$ and $\exists (i_1, \dots, i_n): p \nmid c_{i_1, \dots, i_n}$.
(This will be true for all sufficiently large primes, if $d_i = \deg_{x_i}(P)$)

The canonical epi $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $a \mapsto \bar{a}$, induces a ring epi $\mathbb{Z}[x_1, \dots, x_n] \to \mathbb{Z}/p\mathbb{Z}[x_1, \dots, x_n]$ (acting on coefficients), so

$$0 \neq \bar{P} = \sum_{(i_1, \dots, i_n)} \overline{c_{i_1, \dots, i_n}}\, x_1^{i_1} \cdots x_n^{i_n}.$$

Since $|\mathbb{Z}/p\mathbb{Z}| > p > d_i$, Lemma 4.17 implies that there exist $a_1, \dots, a_n \in \mathbb{Z}$ with $\bar{P}(\bar{a}_1, \dots, \bar{a}_n) \neq 0$. □

Prop 4.19 If S is a strict rational series over $\mathbb{Q}(x_1, \dots, x_n)$, then $\mathrm{conn}(S)$ is quasi-periodic. In particular, $\mathbb{Q}(x_1, \dots, x_n)$ is an SMC-field.

Proof: Let (λ, μ, γ) be a lin. repr of S with $\mu(x)$ invertible. Multiplying everything by some common denominator from $\mathbb{Z}[x_1, \dots, x_n]$, we can assume all coefficients to be in $\mathbb{Z}[x_1, \dots, x_n]$ (as in Proof of Prop 4.12),

Let $P := \det(\mu(x)) \in \mathbb{Z}[x_1, \dots, x_n]$. Then $P \neq 0$ since $\mu(x)$ is invertible.

$\xrightarrow{4.18}$ $\exists a_1, \dots a_n \in \mathbb{Z}$: $\det(\mu(x)(a_1, \dots a_n)) \not\equiv 0 \mod p$.

Let $H := (a_1, \dots a_n) + p\mathbb{Z}^n$. Then

$$\det(\mu(x)(b_1, \dots, b_n)) \equiv \det(\mu(x)(a_1, \dots a_n)) \not\equiv 0 \mod p$$

for all $(b_1, \dots b_n) \in H$.

Suppose $S = \sum_{m=0}^{\infty} s_m x^m$ with $s_n \in \mathbb{Z}[x_1, \dots x_n]$

Define $S_{b_1, \dots b_n} := \sum_{m=0}^{\infty} s_m(b_1, \dots b_n) x^m \in \mathbb{Z}[x]$. for $(b_1, \dots b_n) \in H$

Each $S_{b_1, \dots b_n}$ is rational as series over $\mathbb{Z}$ (we can substitute in the linear repr for S). with some period $N \leq |GL_d(\mathbb{F}_p)| \leq p^{d^2}|(p^{d^2})!$

$\Rightarrow$ Each $\operatorname{ann}(S_{b_1, \dots b_n})$ is quasi-periodic $\forall$ by Prop 4.12/4.16

$\Rightarrow$ $\bigcap_{(b_1, \dots b_n) \in H} \operatorname{ann}(S_{b_1, \dots b_n})$ is quasi-periodic (Lemma 4.11) with period $(p^{d^2})!$

Claim: $\operatorname{ann}(S) = \bigcap_{(b_1, \dots b_n) \in H} \operatorname{ann}(S_{b_1, \dots b_n})$

„$\subseteq$" ✓ „$\supseteq$" Suppose $s_m(b_1, \dots b_m) = 0$ for all $(b_1, \dots b_m)$.

Then Lemma 4.17 shows $s_m = 0$. □

Prop 4.20 If K is an SNL field and L is a finite extension of K (i.e. $\dim_K L < \infty$), then L is an SNL field.

Proof: $\dim \operatorname{Hom}_K(L, K) = \dim_K L < \infty$. Let $\varphi_1, \dots \varphi_d \in \operatorname{Hom}_K(L, K)$ be a K-basis for $\operatorname{Hom}_K(L, K)$. Then

$$\forall a \in L: \quad a = 0 \iff \varphi_1(a) = \dots = \varphi_d(a) = 0$$

Let $S = \sum_{n=0}^{\infty} s_n x^n \in L[[x]]$ be rational.

For $1 \le i \le d$, let $S_i := \sum_{n=0}^{\infty} \varphi_i(s_n) x^n \in K[[x]]$

$\Rightarrow \operatorname{onn}(S) = \bigcap \operatorname{onn}(S_i)$

Suffices to show: each S_i is rational over K.

S rational $\Rightarrow S$ recognizable $\Rightarrow \exists$ finite-dimensional stable $V \subseteq L[[x]]$ s.t. $S \in V$ (recall: stable means $\forall T \in V: T \circ x = \overleftarrow{x} T \in V$)

($\overleftarrow{x}$: left shift on coefficients)

Now $\varphi_i : L \to K$ extends to a K-linear $\tilde{\varphi}_i : L[[x]] \to K[[x]]$ coefficientwise. Then $\tilde{\varphi}_i(S) \in \tilde{\varphi}_i(V)$ and $\tilde{\varphi}_i(V)$ is stable.

Since V is finite-dim./L and L/K is finite-dim/K, V is also finite-dim over K (if $T_1, \dots, T_m$ is an L-basis of V, $c_1, \dots, c_q$ an K-basis of L, then $c_i T_j$, $1 \le i \le q$, $1 \le j \le m$ generates V, and is in fact a basis)

$\Rightarrow \tilde{\varphi}_i(V)$ is a finite-dim K-vectorspace $\Rightarrow \tilde{\varphi}_i(S) = S_i$ is K-recognizable $\square$

Proof of Thm 4.10 (SMC) Let K be a field of char 0, $S \in K[[x]]$ rational, (λ, μ, γ) a linear repr. of S. $\mathbb{Q} \subseteq K$ (wlog.). The entries of $\lambda, \mu(x), \gamma$ generate a finitely generated field extension K_0 of $\mathbb{Q}$, and $S \in K_0[[x]]$ is K_0-rational.

By Field Theory, K is a finite-dimensional extension of some purely transcendental $\mathbb{Q}(x_1, \dots, x_n)$ (Keyword: Transcendence Basis). By Prop. 4.19, $\mathbb{Q}(x_1, \dots, x_n)$ is an SMC-field, by Prop 4.20 then so is $K_0 \Rightarrow \operatorname{onn}(S)$ is a finite union of α

Finite set and finitely many arithmetic progressions □

Remarks

(1) SML in this form does not hold for fields K with $\mathrm{char} K = p > 0$.

E.g., let $K = \mathbb{F}_p(t)$. Recall $(a+b)^p = a^p + b^p \ \forall a, b \in K$.

Consider

$$S_n := (t+1)^n - t^n - 1$$

Then $(S_n)_{n \geq 0}$ is an LRS $\left(\text{E.g. } \sum_{n=0}^{\infty} S_n x^n = \frac{1}{1-(t+1)x} - \frac{1}{1-tx} - \frac{1}{1-x}\right)$

$$S_n = 0 \Leftrightarrow (t+1)^n = t^n + 1 \Leftrightarrow n = p^k, \ k \in \mathbb{N}_0$$

But $\{p^k : k \geq 0\}$ is not a finite union of a finite set + fin. many arith. progressions (But see below)

(2) SML can be rephrased as a statement about a linear dynamical system: Let $S_n = \lambda A^n y$ with $\lambda \in K^{1 \times d}$, $y \in K^{d \times 1}$, $A \in K^{d \times d}$.

$n \mapsto A^n y$ is a dynamical system with discrete time steps (n)

$H = \{x \in K^{d \times 1} : \lambda x = 0\}$ is a hyperplane.

SML states that the (forward) orbit of y under the action of A hits (=reaches) H in a very regular pattern.

A non-linear version is the (open) Dynamical Mordell-Lang Conjecture (from Arithmetic Dynamics)

Conj: Let X be a quasi-projective variety defined over $\mathbb{C}$. Let Φ be an endomorphism of X, let $a \in X(\mathbb{C})$, and let $V \subseteq X$ be any (closed) subvariety. Then $\{n \in \mathbb{N}_0 : \Phi^n(a) \in V(\mathbb{C})\}$ is a union of a finite set + fin. many arithmetic progressions.

(3) (Effectivity) Given an LRS $(s_n)_{n\geq 0}/\mathbb{Q}$ (or more generally, a f.g. field $/\mathbb{Q}$) it is decidable whether $(s_n)_{n\geq 0}$ has infinitely many zeros, and to find the infinite arithm. progressions on which it is zero. (Berstel - Mignotte 1976)

But the following is a famous open problem (Skolem problem):

[Given an LRS $(s_n)_{n\geq 0}$ over $\mathbb{Q}$ (or $\mathbb{Z}$), is it decidable whether there exists an $n \geq 0$ s.t. $s_n = 0$?

(Then of course one can find all the zeros)

(4) Progress on the Skolem problem

- Some special cases are easy (e.g., if there is a simple dominant eigenvalue λ: $|\lambda| > |\lambda'|$ for all eigenvalues $\lambda' \neq \lambda$, and λ has multiplicity 1)
- If there is a dominant eigenvalue with multiplicity ≤ 3 or the LRS has order ≤ 4, then it is decidable (Mignotte - Shorey - Tijdeman 1984, Vereshchagin 1985). This uses Baker's method on linear forms in logarithms (from Transcendental Number Theory). For order 5 there are only partial results.

- If the LRS has simple eigenvalues, then there is an "algorithm" that produces all zeros + a certificate IF it terminates.

There is a termination proof that depends on two open conjectures from NT:

- Skolem conjecture
- p-adic Schanuel conjecture

(Bilu - Luca - Nieuwveld - Ouaknine - Purser - Worrell, 2022)

- Another new approach: $S \subseteq \mathbb{N}_0$ is a <u>universal Skolem set</u> if it is decidable whether a $\mathbb{Z}$-LRS has a zero in S.

Dependent on the (very strong) Bateman-Horn conjecture on the distribution of prime values taken by polynomials, existence of positive density Skolem sets is proven

(Luca - Maynard - Noubissie - Ouaknine - Worrell 2024)

(5) In <u>positive characteristic</u> the set of zeros of an LRS is <u>p-automatic</u>: there exists a FA taking as input the base p representation of n, and which accepts <u>iff</u> $S_n = 0$.

If K is $\mathbb{Q}_p$ / $\mathbb{F}_p$, then this FA can be computed, and so the Skolem problem here is decidable!

(Derksen 2007).

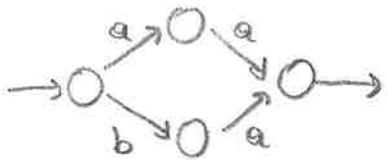
5. Determinizability & Unambiguizability for WFA / Fields

Let K be a field and let (λ, μ, γ) be a lin. repr. of a WFA $\mathcal{A}$.

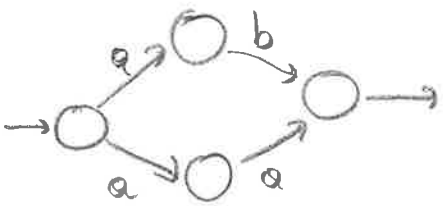
Recall: •) $\mathcal{A}$ is deterministic if it has at most one initial state and given any state p and any letter $x \in A$, there is at most one state q with a transition $p \xrightarrow{x} q$.

[$\Leftrightarrow$ λ has at most one nonzero entry, and each $\mu(x)$ is row-monomial, every row has at most one nonzero entry]

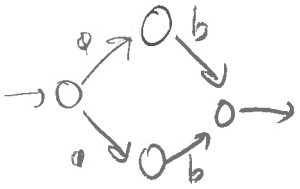
•) $\mathcal{A}$ is unambiguous if every word has at most one successful run.



deterministic



unambiguous, not deterministic



ambiguous

In the unweighted case, every NFA can be determinized ($\rightarrow$ every regular language is recognized by a deterministic finite automaton = DFA)

For WFA this is i.g. no longer true!

So: Which rational series are recognized by deterministic/unambiguous WFA?

As decidability problems: Given a WFA $\mathcal{A}$, does there exist a deterministic / unambiguous WFA $\mathcal{A}'$ with $[\![\mathcal{A}]\!] = [\![\mathcal{A}']\!]$?

This turns out to be decidable over computable fields (e.g. $\mathbb{Q}$), but is still open over tropical semirings.

From now, let K be a field, A an alphabet.

Thm 5.1 Let $S \in K\langle\langle A \rangle\rangle$ be rational, and (λ, μ, γ) a minimal lin. repr. for S of dimension d.

TFAE: (a) S is recognized by a deterministic WFA

(b) The (left) reachability set

$$\lambda\mu(A^*) = \{\lambda\mu(w) \in K^{1\times d} : w \in A^*\}$$

is contained in a finite union of lines through the origin (= 1-dimensional subspaces of $K^{1\times d}$)

Proof: (a) $\Rightarrow$ (b) Let $(\tilde\lambda, \tilde\mu, \tilde\gamma)$ be the lin. repr. corresponding to a deterministic WFA, let m be its dimension, and $e_1, \dots, e_m \in K^{1\times d}$ the standard basis vectors. Then $\tilde\lambda\tilde\mu(w)$ has at most one nonzero entry for each $w \in A^*$

$\Rightarrow \tilde\lambda\tilde\mu(A^*) \subseteq Ke_1 \cup \dots \cup Ke_m$.

By Cor 3.11, there exists an invertible matrix $B \in GL_m(K)$ s.t. there is a block decomposition

$$\tilde\lambda B = (*, \lambda, 0), \quad B^{-1}\tilde\mu(x)B = \begin{pmatrix} \mu_1 & 0 & 0 \\ * & \mu & 0 \\ * & * & \mu_2 \end{pmatrix}, \quad B^{-1}\tilde\gamma = \begin{pmatrix} 0 \\ \gamma \\ * \end{pmatrix}$$

Then $\tilde\lambda\tilde\mu(w)B = (\underbrace{*}_{d_1}, \overbrace{\lambda\mu(w)}^{d}, \overbrace{0}^{d_2}) \subseteq Ke_1B \cup \dots \cup Ke_mB$

Let $\Pi: K^{1\times m} \to K^{1\times d}$, $(x_1, \dots, x_{d_1}, x_{d_1+1}, \dots, x_{d_1+d}, x_{d_1+d+1}, \dots x_{d_1+d+d_2}) \mapsto (x_{d_1+1}, \dots, x_{d_1+d})$

Then $\lambda\mu(w) \subseteq K\Pi(e_1B) \cup \dots \cup K\Pi(e_mB)$.

(b) $\Rightarrow$ (a) Wlog. $S \neq 0$, and hence $\lambda \neq 0$

Let $\alpha_1, \dots, \alpha_m \in K^{1\times d}$ s.t. $\lambda\mu(A^*) \subseteq K\alpha_1 \cup \dots \cup K\alpha_m$.

Wrl. $\alpha_1 = \lambda$ and $\lambda\mu(A^*) \cap K\alpha_i \neq 0$ for all $1 \leq i \leq m$.

For each $1 \leq i \leq m$ and $x \in A$, there exists $j(x,i)$ s.t.

$K\alpha_i \mu(x) \subseteq K\alpha_{j(x,i)}$.

[Indeed: Let $c \in K^\times$, $w \in A^*$ s.t. $c\alpha_i = \lambda\mu(w)$

$\Rightarrow c\alpha_i\mu(x) = \lambda\mu(wx) \subseteq K\alpha_1 \cup \dots \cup K\alpha_m$

$\Rightarrow \exists j(x,i) : c\alpha_i\mu(x) \in K\alpha_{j(x,i)}$

$\Rightarrow K\alpha_i\mu(x) \subseteq K\alpha_{j(x,i)}$]

Let $c(x,i) \in K$ be s.t. $\alpha_i\mu(x) = c(x,i)\,\alpha_{j(x,i)}$.

Define an m-dimensional lin. repr. $(\tilde\lambda, \tilde\mu, \tilde\gamma)$ as follows:

$$\begin{cases} \tilde\lambda = e_1 = (1,0,\dots,0) \\ e_i\tilde\mu(x) = e_{j(x,i)}\, c(x,i) \\ \text{i-th row of } \tilde\mu \\ e_i\tilde\gamma = \alpha_i\gamma. \end{cases}$$

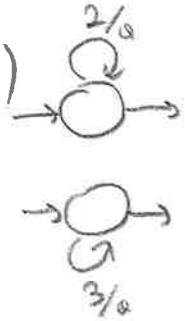
Then the corresponding WFA is deterministic, because $\tilde\lambda, \tilde\mu(x)$ are row-monomial.

Let $w = x_1 \cdots x_n \in A^*$, $x_i \in A$.

Then (easy induction)

$$\begin{aligned} \tilde\lambda\tilde\mu(x_1\cdots x_n)\tilde\gamma &= c(x_1,1)\, c(x_2, j(x_1,1))\, c(x_3, j(x_2, j(x_1,1))) \cdots \\ &\quad \cdots c(x_n, j(x_{n-1}, \dots)))\, e_{j(x_n, j(x_{n-1}, \dots j(x_1,1)))}\,\tilde\gamma \\ &= c(x_1,1)\, c(x_2, j(x_1,1)) \cdots c(x_n, j(x_{n-1}, \dots)) \\ &\quad \alpha_{j(x_n, j(x_{n-1}, \dots, j(x_1,1)))}\,\gamma \\ &= \alpha_1\mu(x_1)\cdots\mu(x_n)\gamma = \lambda\mu(x_1\cdots x_n)\gamma \end{aligned}$$

$\overset{\text{another easy induction}}{=}$ □

Exm (1) 

$A=\{a\}$, $K=\mathbb{Q}$

recognizes

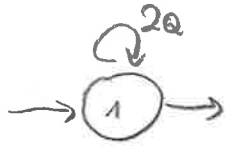
$(S, a^n) = 2^n + 3^n$

$\lambda = (1,1)$, $\mu(a) = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$, $\gamma = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

(λ, μ, γ) is reduced, hence minimal.

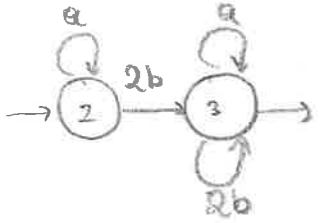
$\lambda\mu(A^*) = \{ (2^n, 3^n) : n \geq 0 \}$ cannot be covered by finitely many lines, bec. $\left(\frac{3}{2}\right)^n$ takes infinitely many distinct values.

$\Rightarrow (\lambda, \mu, \gamma)$ is not determinizable

(2) 

$A=\{a,b\}$

$$(S,w) = \begin{cases} 2^{|w|_a} & \text{if } b \text{ does not appear in } w \\ 2^{|w|_b} & \text{if } b \text{ appears in } w \end{cases}$$



$\lambda = (1,1,0)$ $\mu(a) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $\mu(b) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 2 \end{pmatrix}$

$\gamma = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$

(λ, μ, γ) is minimal, not determinizable bec.

$\lambda\mu(A^*) = \{ (2^n, 1, 0) : n \geq 0 \} \cup \{ (0, 0, 2^m) : m \geq 1 \}$

But the WFA is unambiguous!

Remark: (1) Over a finite field, every WFA is determinizable by Thm 5.1(b)

(2) Over a computable field (e.g. $\mathbb{Q}$), the property in 5.1(b) is decidable (but non-trivially so, see Bok). So determinizability is decidable over such fields.

5.1 Linear Hull, Linear Hull Automaton

Let V be a finite-dimensional K-vector space (we'll consider $V = K^{1\times d}$ and $V = K^{d\times d}$).

Let $\mathcal{C}_V := \{ W_1 \cup \dots \cup W_\ell : \ell \geq 0,\ W_i \leq V \text{ subspace} \}$

Then $\emptyset \in \mathcal{C}_V$, $V \in \mathcal{C}_V$, $\mathcal{C}_V$ is closed under arbitrary intersections (e.g. by induction on dimension) and under finite unions.

$\Rightarrow$ The sets in $\mathcal{C}_V$ are the closed sets of a topology on V (linear Zariski topology)

Given any set $\Omega \subseteq V$, the closure is $\overline{\Omega} := \bigcap_{\substack{X \in \mathcal{C}_V \\ \Omega \subseteq X}} X$.

A non-empty $\Omega \subseteq V$ is irreducible if

$$\forall X, X' \in \mathcal{C}_V:\ \Omega \subseteq X \cup X' \Rightarrow \Omega \subseteq X \text{ or } \Omega \subseteq X'$$

Lemma 5.2: Let $\emptyset \neq X \in \mathcal{C}_V$.

(1) If $|K| < \infty$, then X is irreducible iff X is a subspace with $\dim X \leq 1$.

(2) If $|K| = \infty$, then X is irreducible iff X is a subspace.

Proof: Let $X = W_1 \cup \dots \cup W_\ell$ with $W_i \subseteq V$ subspaces ($\ell \geq 1$)
Wlog. $W_i \not\subseteq W_j$ for $i \neq j$. We can also assume ℓ is minimal.
We claim $\ell = 1$. Suppose $\ell \geq 2$.
$\Rightarrow X \subseteq W_1$ or $X \subseteq W_2 \cup \dots \cup W_\ell$ by irreducibility $\lightning$ ℓ minimal.
So $X = W_1$ is a vector space.

Case $|K| < \infty$: X is either $\{0\}$ or the union of the finitely many lines contained in it. By irreducibility, it must be contained in one line.
Conversely $\{0\}$ and lines are trivially irreducible.

Case $|K| = \infty$: We have to show every vector subspace $W \subseteq V$ is irreducible. But it's an exercise to show that over an infinite field, a vector space cannot be covered by finitely many proper subspaces. □

Lemma 5.3 Every $X \in \mathcal{C}_V$ has an irredundant repr.
$X = W_1 \cup \dots \cup W_\ell$ (meaning $W_i \not\subseteq W_j$ for $i \neq j$)
with W_i irreducible closed. This repr. is unique up to reindexing. The $W_1, \dots, W_\ell$ are the irreducible components of X. The dimension of X is $\max_{1 \leq i \leq \ell} \dim W_i$

Proof: Existence is clear by definition and Lemma 5.2.
Uniqueness: Suppose $W_1 \cup \dots \cup W_\ell = W_1' \cup \dots \cup W_m'$
with W_i, W_j' irreducible and both repr. irredundant.
$W_1 \subseteq W_1' \cup \dots \cup W_m' \Rightarrow \exists j_1 : W_1 \subseteq W_{j_1}' \Rightarrow \exists i_1 : W_{j_1}' \subseteq W_{i_1}$
$\Rightarrow W_1 \subseteq W_{j_1} \subseteq W_{i_1} \Rightarrow i_1 = 1 \Rightarrow W_1 = W_{j_1}$.

Similarly, for every W_i there is a j with $W_i = W_j'$,
by symmetry, for every W_j' there is a i with $W_i = W_j'$.
Irredundancy implies the claim. □

Def Let (λ, μ, ϱ) be a lin. repr.
The **(left) linear hull** of (λ, μ, ϱ) is the closed set $\overline{\lambda\mu(A^*)}$.

Observations

(1) Linear maps are continuous in the linear Zariski topology
(preimages of subspaces are subspaces, the same is true for finite unions of subspaces)

(2) For $f: V \to V'$ continuous, $\Omega \subseteq V$, $f(\overline{\Omega}) \subseteq \overline{f(\Omega)}$

[since preimages of closed sets are closed, and hence
$\overline{\Omega} \subseteq f^{-1}(\overline{f(\Omega)})$]
($\overline{\Omega}$: smallest closed set containing Ω; $\overline{f(\Omega)}$: closed; $f^{-1}(\overline{f(\Omega)})$: closed)

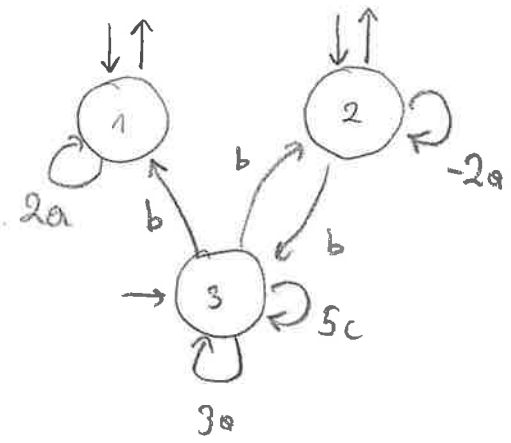
Conclusion: $\lambda\mu(A^*)\mu(x) \subseteq \lambda\mu(A^*)$ implies

$$\boxed{\overline{\lambda\mu(A^*)}\mu(x) \subseteq \overline{\lambda\mu(A^*)}}$$

So, if $\overline{\lambda\mu(A^*)} = W_1 \cup \dots \cup W_m$ is the decomposition into irreducibles
then (i) $(W_1 \cup \dots \cup W_m)\mu(x) \subseteq W_1 \cup \dots \cup W_m$
(ii) $\forall 1 \le i \le m \; \forall x \in A \; \exists j \in \{1, \dots, m\}$: $W_i\mu(x) \subseteq W_j$.
($W_i\mu(x)$: still irreducible)

(j may not be unique)

Exm: $K=\mathbb{Q}$, $A=\{a,b,c\}$



$\lambda = (1,1,1)$

$\mu(a) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$ $\mu(b) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$

$\mu(c) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 5 \end{pmatrix}$, $\gamma = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$

$\lambda\mu(a^n) = (2^n, (-1)^n 2^n, 3^n)$

$\lambda\mu(a^n b) = (3^n, 3^n, (-1)^n 2^n)$

$\lambda\mu(a^n b a^m) = (2^m 3^n, (-1)^m 3^n 2^m, (-1)^n 3^n 2^m)$

Claim: $\overline{\lambda\mu(A^*)} = \overbrace{\langle e_1+e_2, e_3\rangle}^{=W_1} \cup \overbrace{\langle e_1-e_2, e_3\rangle}^{=W_2}$

"$\subseteq$": $\lambda \in W_1 \cup W_2$ and

$W_1\mu(a) \subseteq W_2$, $W_2\mu(a) \subseteq W_1$

$W_1\mu(b) \subseteq W_1$, $W_2\mu(b) \subseteq W_1$

$W_1\mu(c) \subseteq W_1 \cap W_2$, $W_2\mu(c) \subseteq W_1 \cap W_2$

$\Rightarrow \overline{\lambda\mu(A^*)} \subseteq W_1 \cup W_2$

"$\supseteq$": $\{\lambda\mu(a^{2n}) : n \geq 0\}$ is dense in W_1,

$\{\lambda\mu(a^{2n+1}) : n \geq 0\}$ dense in W_2

Remark: By Thm 5.1, $\overset{\circ}{\forall}$ minimal (λ,μ,γ) is determinizable

$\Leftrightarrow \dim \overline{\lambda\mu(A^*)} \leq 1$.

Construction (Linear Hull Automaton)

W.l. (λ, μ, γ) be a lin. repr, $W_1, \dots, W_m$ the irred. components of $\overline{\lambda\mu(A^*)}$. Wlog $\lambda \in W_1$

On each W_i fix a basis $(b_{i1}, \dots b_{id_i})$.

Then $(b_{ij})_{i,j}$ is a basis of $W_1 \oplus \dots \oplus W_m =: W \subseteq K^{1\times(d_1+\dots+d_m)}$

For $x \in A$ choose $f_x : \{1,\dots,m\} \to \{1,\dots,m\}$ s.t.

$W_i \mu(x) \subseteq W_{f_x(i)}$ (exists by Obs. after Lemma 5.2)

Define: For $\beta \in W_i$ define $\pi_i(\beta) = (c_1, \dots, c_{d_i})$ with $\beta = \sum_{j=1}^{d_i} c_j b_{ij}$, $c_j \in K$ $\quad (\pi_i : W_i \xrightarrow{\sim} K^{1\times d_i})$

$\tilde{\lambda} := (\pi_1(\lambda), 0, \dots, 0)$

$\tilde{\mu}(x)$ will a block structure

$$\tilde{\mu}(x) = \begin{bmatrix} d_1 & d_2 & \cdots & \\ & & & d_1 \\ & & & d_2 \\ & & & \vdots \end{bmatrix}$$

s.t. for $i \in \{1,\dots,m\}$ the $(i, f_x(i))$ block contains the matrix repr of $\mu(x)|_{W_i} : W_i \to W_{f_x(i)}$ wrt. the chosen bases. I.e. the $(i,f_x(i))$ block is a $d_i \times d_{f_x(i)}$ matrix whose k-th row is $\pi_{f_x(i)}(b_{ik}\mu(x))$.

All other blocks are zero.

$\tilde{\gamma}$ ... with a block structure of $d_i \times 1$ blocks $\quad \hat{\gamma} = \begin{pmatrix} \vdots \\ \hline \vdots \\ \hline \vdots \end{pmatrix} \begin{matrix} d_1 \\ d_2 \\ \vdots \end{matrix}$

k-th entry of i-th block is $b_{ik}\gamma \in K$

Then $(\tilde{\lambda}, \tilde{\mu}, \tilde{\gamma})$ is a linear repr. of dimension $d_1 + \dots + d_m$, recognizing the same series as (λ, μ, γ). The associated WFA is a **linear hull automaton (LHA)** (depends on choice of f_x, bases)

Sketch of Proof Convince yourself that

$$\tilde{\lambda}\tilde{\mu}(x_1 \cdots x_e) = (0 \,|\, \cdots \,|\, 0 \,|\, \underbrace{\pi_j(\lambda\mu(x_n \cdots x_e))}_{j\text{-th block}} \,|\, 0 \,|\, \cdots \,|\, 0)$$

with $j = f_{x_e} \circ \cdots \circ f_{x_n}(1)$

□ (Sketch)

Exm (cont'd) $\overline{\lambda\mu(A^*)} = \underbrace{\langle e_1+e_2, e_3\rangle}_{=W_1} \cup \underbrace{\langle e_1-e_2, e_3\rangle}_{=W_2}$

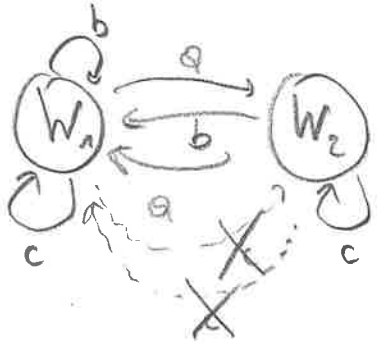
Basis on W_1: $b_{11} := e_1+e_2$, $b_{12} := e_3$

on W_2: $b_{21} := e_1-e_2$, $b_{22} = e_3$

$\lambda = (1,1,1) = b_{11}+b_{12} \Rightarrow \tilde{\lambda} = (\overbrace{1,1}^{W_1} \,|\, \overbrace{0,0}^{W_2})$

(b_{11}, b_{12}, b_{21}, b_{22})

Choose f:



$f_a(1) = 2$, $f_a(2) = 1$

$f_b(2) = f_b(1) = 1$

$f_c(1) = 1$, $f_1(2) = 2$ (choice!)

$$\mu(a) = \begin{pmatrix} 2 & -2 & \\ & & 3 \end{pmatrix} \Rightarrow b_{11}\mu(a) = (2,-2,0) = 2b_{21}$$

(W_1, W_2)

$b_{12}\mu(a) = (0,0,3) = 3b_{22}$

$$\Rightarrow \tilde{\mu}(a) = \left[\begin{array}{cc|cc} & & 2 & 0 \\ & 0 & 0 & 3 \\ \hline 2 & 0 & & \\ 0 & 3 & & 0 \end{array}\right] \begin{matrix} \\ W_1 \\ \\ W_2 \end{matrix}$$

$$\tilde{\mu}(b) = \left[\begin{array}{cc|c} 0 & 1 & \\ 1 & 0 & 0 \\ \hline 0 & -1 & \\ 1 & 0 & 0 \end{array}\right]$$

$b_{11}\mu(b) = (0,0,1) = b_{12}$

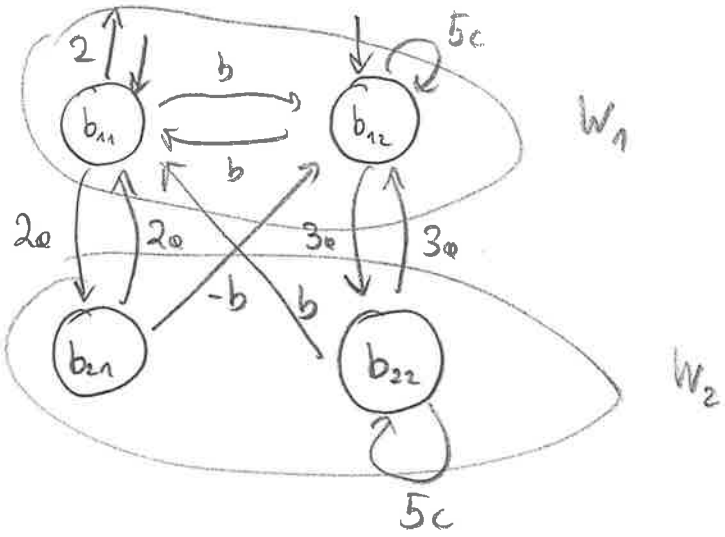
$b_{21}\mu(b) = (1,1,0) = b_{11}$

$b_{21}\mu(b) = (1,-1,0)\mu(b) = (0,0,-1) = -b_{12}$

$$\tilde{\mu}(c) = \left[\begin{array}{cc|c} 0 & 0 & \\ 0 & 5 & 0 \\ \hline & & 0 \\ 0 & & 0 \end{array}\right] \qquad \tilde{\gamma} = \begin{pmatrix} 2 \\ 0 \\ \hline 0 \\ 0 \end{pmatrix}$$

$b_{11}\gamma = 2$ $b_{12}\gamma = 0$

$b_{21}\gamma = 0 = b_{22}\gamma$



Remark: The block structure of the matrices (and $\tilde{\lambda}, \tilde{\rho}$) is semimonomial:

(1) Each row of blocks contains at most one nonzero block

(2) Inside any block, each column contains at most one nonzero entries.

Prop 5.4 Semimonomial linear representations are unambiguous.

Proof: A successful run for $w = x_1 \cdots x_\ell$ corresponds to indices $i_0, i_1, \ldots, i_\ell$ s.t. $\tilde{\lambda}_{i_0} \tilde{\mu}(x_1)_{i_0 i_1} \tilde{\mu}(x_2)_{i_1 i_2} \cdots \tilde{\mu}(x_\ell)_{i_{\ell-1} i_\ell} \tilde{\rho}_{i_\ell} \neq 0$.

By (1), for every $0 \leq j \leq \ell$, there exists a unique block which is nonzero in $\tilde{\lambda}\, \tilde{\mu}(x_1) \cdots \tilde{\mu}(x_j)$. Let $B(j)$ denote the index of that block.

Now i_ℓ is unique, because $\tilde{\rho}$ has a unique nonzero entry in block $B(\ell)$.

But the $B(\ell-1) \times B(\ell)$ block of $\tilde{\mu}(x_\ell)$ has in column i_ℓ a unique nonzero entry (by 2). This row must be $i_{\ell-1}$.

Iterating, $(i_0, \ldots, i_\ell)$ are uniquely determined. □

(Idea: First read w left to right, giving unique sequence of blocks (1), then right to left, giving the states (by (2)))

5.2 Unambiguizability

Suppose $S \in K\langle\langle A \rangle\rangle$ is recognized by some unambiguous WFA $\mathcal{A}$. Let $c_1, \dots, c_N$ be the (finite) set of nonzero weights of $\mathcal{A}$. Then every nonzero (S,w) is a product of the c_i's

Def. $S \in K\langle\langle A \rangle\rangle$ is Pólya if there exists a finitely generated subgroup $\Gamma \leq K^\times$ s.t.

$$\forall w \in A^*: \quad (S,w) \in \Gamma_0 := \Gamma \cup \{0\}.$$

Unambiguizable rational S are always Pólya. We want to show the converse. Suppose $\boxed{\operatorname{char} K = 0}$ (for simplicity)

Theorem 5.5 If $\boxed{\operatorname{char} K = 0}$ and $S \in K\langle\langle A \rangle\rangle$ is a rational Pólya series, then there is an unambiguous WFA recognizing S.

More precisely, we'll sketch that one can take a LHA arising from a minimal lin. repr. + suitable basis.

Lemma 5.6 Let (λ, μ, γ) be a minimal linear repr, $\Gamma_0 \subseteq K$ s.t. $\forall w \in A^*: \lambda\mu(w)\gamma \in \Gamma_0$. By changing to a basis $\mu(w_1)\gamma, \dots, \mu(w_d)\gamma$ of $K^{d\times 1}$, we can find a min. lin. repr. with $\lambda\mu(w) \in \Gamma_0^{1\times d}$ for all $w \in A^*$.

Proof: Let $B = (\mu(w_1)\gamma, \dots, \mu(w_d)\gamma)$.
Then $(\lambda B, B^{-1}\mu B, B^{-1}\gamma)$ has the desired property, because

$$\lambda B B^{-1}\mu(w) B = (\lambda\mu(w)\mu(w_1)\gamma, \dots, \lambda\mu(w)\mu(w_d)\gamma)$$
$$= (\lambda\mu(ww_1)\gamma, \dots, \lambda\mu(ww_d)\gamma) \in \Gamma_0^{1\times d}. \quad \square$$

Lemma 5.7 Let $W \leq V$ be vector spaces, with $e_1, \dots, e_d$ a basis of V. If $\Gamma_0 \leq K^*$, one can choose a basis $b_1, \dots, b_n$ of W s.t.

$$(\Gamma_0 e_1 + \dots + \Gamma_0 e_d) \cap V \leq \Gamma_0 b_1 + \dots + \Gamma_0 b_n$$

Proof: Let $b_1, \dots, b_n$ be an arbitrary basis of W.

Expressing the b_i in terms of $e_1, \dots, e_d$ & using Gaussian elimination & renumbering we can assume $e_i^*(b_i) = 1$, $e_j^*(b_i) = 0$ for $j \in \{1, \dots, n\} \setminus \{i\}$.

$$\left(\begin{array}{c|ccc} & e_1 & & e_d \\ b_1 = & 1 & 0 & 0 \\ b_2 = & 0 & \ddots & 0 \\ \vdots & \vdots & & \vdots \\ b_n = & 0 & \cdots & 1 \end{array} \middle| \begin{array}{ccc} * & \cdots & * \\ \vdots & & \vdots \\ * & \cdots & * \end{array} \right)$$

Suppose $\beta = \sum_{j=1}^{n} \beta_j b_j = \sum_{j=1}^{d} \alpha_j e_j$ with $\alpha_j \in \Gamma_0$.

$$\Rightarrow \alpha_i = e_i^*(\beta) = \sum_{j=1}^{n} \beta_j e_i^*(b_j) = \beta_i \Rightarrow \beta_i \in \Gamma_0 \text{ (for all } i\text{)}$$

□

Cor 5.8 If S is a rational Pólya series, it has a linear repr $(\tilde{\lambda}, \tilde{\mu}, \tilde{\gamma})$ of dim. d s.t. there exists a f.g. $\Gamma \leq K^*$, $\Gamma_0 := \Gamma \cup \{0\}$ s.t. $K^{1 \times d} = W_1 \oplus \dots \oplus W_m$, $\overline{\tilde{\lambda}\tilde{\mu}(A^*)} = W_1 \cup \dots \cup W_m$, $\tilde{\lambda}\tilde{\mu}(A^*) \leq \Gamma_0^{1 \times d}$. In particular, $\Gamma_0^{1 \times d} \cap W_i$ is dense in each W_i (since $\tilde{\lambda}\tilde{\mu}(A^*)$ is).

Proof Sketch: Starting with a minimal linear repr, take a basis as in L5.6; on each component of the linear hull choose a basis as in L5.7. Then the LHA has the desired properties (some easy details omitted). □

The LHA has the required "outer block structure", but we need to prove that every column of every block has at most one nonzero entry.

Suppose from now on $\boxed{\text{char } K = 0}$ (otherwise more difficult)

Unit Eqn's (number theory / Diophantine geometry):

Erdős ('84), van der Poorten-Schlickewei ('82)

Consider a linear equation

$$a_1 X_1 + \dots + a_n X_n = 0 \qquad (*)$$

and a f.g. group $\Gamma \leq K^\times$. Consider solutions to $(*)$ in Γ.

Note: (1) If $(x_1, \dots, x_n)$ solves $(*)$, so does

$$(\gamma x_1, \dots, \gamma x_n) \quad \forall \gamma \in \Gamma$$

(2) If $\emptyset \neq I \subsetneq \{1, \dots, n\}$ s.t. $\sum_{i \in I} a_i x_i = 0$, then also $\sum_{i \in \{1,\dots,n\} \setminus I} a_i x_i = 0$. We can multiply elements in the first set by some $\gamma_1 \in \Gamma$, elts in 2nd set by $\gamma_2 \in \Gamma$.

Def: A solution $(x_1, \dots, x_n)$ is degenerate if $\exists I \subsetneq \{1, \dots, n\}$ s.t. $\sum_{i \in I} a_i x_i = 0$, non-degenerate otherwise.

Theorem 5.9 (Over a field of char $K = 0$), the equation $(*)$ has only finitely many non-degenerate solutions in Γ^n, when considered as projective points ($=$ up to scalar).

(w/o proof)

Key Lemma 5.10 Let V be f.d. vector space with basis $e_1, \dots, e_n$, $\Gamma \leq K^\times$ f.g.. Suppose $\Omega \subseteq \Gamma_0 e_1 + \dots + \Gamma_0 e_n$ is s.t. $\overline{\Omega} = V$. If $\varphi: V \to K$ is linear & $\varphi(\Omega) \subseteq \Gamma_0$, then $\varphi(e_i) \neq 0$ for at most one i.

Proof: Wlog: $n \geq 2$.

Wrt. $e_1, \dots, e_n$, φ takes the form $\varphi(x_1 e_1 + \dots + x_n e_n) = a_1 x_1 + \dots + a_n x_n$, $a_i \in K$.

$I := \{ i \in \{1, \dots, n\} : a_i \neq 0 \}$,

To show $|I| \leq 1$. Wlog $I = \{1, \dots, m\}$. Suppose $m \geq 2$.

For $\emptyset \neq J \subseteq I$, let

$$V_J = \left\{ \sum_{i=1}^{n} \lambda_i e_i \in V : \sum_{j \in J} a_j \lambda_j = 0 \right\} \subsetneq V$$

$$\Rightarrow Y := \bigcup_{\emptyset \neq J \subseteq I} V_J \subsetneq V \quad \text{(since } K \text{ is infinite)}$$

$$\Rightarrow \Omega' := \Omega \setminus Y \text{ is still dense in } V.$$

If $v = \sum_{i=1}^{n} \lambda_i e_i \in \Omega'$, then

$$\sum_{i \in I} a_i \lambda_i = \varphi(v) = \gamma \quad \text{for some } \gamma \in \Gamma$$

$\Rightarrow (\lambda_1, \dots, \lambda_m, \gamma)$ is a non-degenerate solution of $a_1 X_1 + \dots + a_m X_m - X_{m+1} = 0$

$\Rightarrow \{ (\lambda_1, \dots, \lambda_m, \gamma) : v = \sum \lambda_i e_i \in \Omega', \gamma = \varphi(v) \}$ is covered by finitely many lines (Thm 5.9) $\lightning$ $\overline{\Omega'} = V$ since $\dim V \geq 2$.

□

Proof of Thm 5.5 (Sketch)

We work with the LHA from Cor. 5.8.

The columns of a block are now linear maps on $K^{1\times d_i} \cong W_i$.

$\tilde{\lambda}\tilde{\mu}(A^*) \cap W_i =: \Omega \subseteq \Gamma_0^{1\times d_i}$ is dense in W_i.

Since $\tilde{\lambda}\tilde{\mu}(A^*)\mu(x) \subseteq \Gamma_0^{1\times d}$, the assumptions of 5.10 hold & the claim follows. □

Decidability: Except for the computation of the linear hull everything is effective. For computing the LH one needs the following (non trivial) result:

Given finitely many matrices $A_1, \dots, A_n \in K^{d\times d}$, the (linear) Zariski closure of the matrix semigroup generated by $A_1, \dots, A_n$ is computable
(Hrushovski – Ouaknine – Pouly – Worrell 2018).

Thm: Compute $\overline{\mu(A^*)}$, then $\overline{\lambda\mu(A^*)} = \lambda \cdot \overline{\mu(A^*)}$.