Structure of Finite Semigroups and Language Equations

Michal Kunc

Masaryk University Brno

Outline

Structure of finite semigroups:

1) Green's relations
2) Factorization forests
3) Examples of applications to regular languages

Well quasiorders

Systems of language equations:

1) Explicit
2) Implicit

Basic Notions

Semigroup S: set equipped with an associative binary operation $\cdot$

Monoid M: semigroup with identity element 1 $\quad$ ($x \cdot 1 = 1 \cdot x = x$)

Group G: monoid where every element has an inverse $\quad$ ($x \cdot x^{-1} = x^{-1} \cdot x = 1$)

Subgroup of a semigroup $=$ subsemigroup which is a group

(identity element of the subgroup need not be 1, but has to be idempotent, i.e. $x \cdot x = x$)

Smallest monoid containing a semigroup S:

$$S^1 = \begin{cases} S & \text{if } S \text{ is a monoid} \\ S \cup \{1\} & \text{if } S \text{ contains no identity element} \end{cases}$$

Homomorphism $\varphi\colon S \to T$ $\ldots$ $\varphi(xy) = \varphi(x)\varphi(y)$

Monoid homomorphism $\ldots$ additionally $\varphi(1) = 1$

Congruence ρ on S: $\quad$ equivalence $\rho \subseteq S \times S$ satisfying $x \mathrel{\rho} x' \;\&\; y \mathrel{\rho} y' \implies xy \mathrel{\rho} x'y'$

Kernel of a homomorphism $\varphi\colon S \to T$:

$$\ker(\varphi) = \{\, (x, y) \in S \times S \mid \varphi(x) = \varphi(y) \,\}$$

Congruences $=$ kernels of homomorphisms.

Words

A ... finite alphabet

A^* ... monoid of all finite words over A with concatenation as operation
semigroup $A^+ \subseteq A^*$ ... empty word ε excluded

Homomorphisms $A^* \longrightarrow M$ and $A^+ \longrightarrow S$ uniquely defined by any choice of images of letters.

Language $L \subseteq A^*$ recognized by a homomorphism $\varphi\colon A^* \longrightarrow M$ to a finite monoid, if $L = \varphi^{-1}(F)$ for some $F \subseteq M$.

Language $L \subseteq A^+$ recognized by a homomorphism $\varphi\colon A^+ \longrightarrow S$ to a finite semigroup, if $L = \varphi^{-1}(F)$ for some $F \subseteq S$.

recognizable $=$ regular

recognizing homomorphism provides a deterministic automaton for both L and its reverse:

- set of states M
- $\delta_a(x) = x \cdot \varphi(a)$
- $\delta_a^{\mathrm{r}}(x) = \varphi(a) \cdot x$
- initial state 1, accepting states F

Ordered Semigroups

Ordered semigroup: monotone partial order $\leq$ on S, i.e. $x \leq x'$ & $y \leq y' \implies xy \leq x'y'$
(ordinary semigroup ordered by $=$)

$F \subseteq S$ upward closed w.r.t. $\leq$ ... if $x \leq y$ and $x \in F$, then $y \in F$

Language $L \subseteq A^*$ recognized by a homomorphism $\varphi\colon A^* \to M$ to a finite ordered monoid $(M, \leq)$, if $L = \varphi^{-1}(F)$ for some $F \subseteq M$ upward closed w.r.t. $\leq$.

Homomorphism $\varphi\colon A^* \to (M, \leq)$ induces a monotone quasiorder on A^*:

$$u \leq_\varphi v \iff \varphi(u) \leq \varphi(v)$$

(quasiorder $=$ reflexive and transitive relation)

$L \subseteq A^*$ recognized by $\varphi \iff L$ upward closed w.r.t. $\leq_\varphi$

Conversely, any monotone quasiorder $\leq$ on A^* determines a congruence on A^*:

$$w \sim w' \iff w \leq w' \;\&\; w' \leq w$$

$A^*/\sim$ ordered monoid: $\quad w{\sim} \leq w'{\sim} \iff w \leq w'$

projection homomorphism $\nu\colon A^* \to A^*/{\sim}$

Syntactic Homomorphism

$L \ldots$ a language over A

contexts of $w \in A^*$ in L: $\quad \mathrm{C}_L(w) = \{ (u,v) \mid u,v \in A^*,\ uwv \in L \}$

Syntactic monotone quasiorder of L on A^*:

for $w, w' \in A^*$, $\quad w \leq_L w' \iff \mathrm{C}_L(w) \subseteq \mathrm{C}_L(w')$

Syntactic congruence $=$ the corresponding equivalence relation:

$w \sim_L w' \iff w \leq_L w' \;\&\; w' \leq_L w$

$M_L = A^*/\sim_L$ syntactic (ordered) monoid (with ordering induced by $\leq_L$)

$\varphi_L \colon A^* \to A^*/\sim_L$ syntactic homomorphism

M_L smallest (ordered) monoid recognizing L with respect to division (quotient of a submonoid)

M_L finite $\iff$ L regular

for $L \subseteq A^+$: $\quad S_L = A^+/\sim_L$ syntactic semigroup

additional letters in alphabet $\Longrightarrow$ new zero in the syntactic monoid ($0 \cdot x = x \cdot 0 = 0$)

$\varphi_L(w)$ is idempotent if and only if $\forall u, v \in A^*, n \in \mathbb{N} \colon uwv \in L \iff uw^n v \in L$

Products of elements of semigroups versus recognizing languages:

evaluation homomorphism:

$$\mathrm{eval}\colon M^* \to M \qquad \mathrm{eval}(x_1 \ldots x_n) = x_1 \cdots x_n$$

$\varphi\colon A^* \to M$ homomorphism

substitution f from M^* to A^* defined by $f(x) = \{ a \in A \mid \varphi(a) = x \}$

Then $\varphi^{-1}(x) = f(\{ x_1 \ldots x_n \in M^* \mid x_1 \cdots x_n = x \})$

Transformations

Q ... a (finite) set

Full transformation monoid $\mathcal{T}(Q)$ ... all mappings $Q \to Q$ with composition as operation

$\mathcal{A} = (Q, A, \delta)$ deterministic automaton without initial and final states

$\delta_a \colon Q \to Q$ action of $a \in A$

determines homomorphism $\varphi \colon A^* \to \mathcal{T}(Q)$, where $\varphi(a) = \delta_a$

$\varphi(w) = \delta_w^*$ extended transition function

$\{ \delta_w^* \mid w \in A^+ \}$ subsemigroup of $\mathcal{T}(Q)$ ... transition semigroup $\mathcal{T}(\mathcal{A})$ of $\mathcal{A}$

- generated by δ_a for $a \in A$
- recognizes all languages accepted by $\mathcal{A}$

transition monoid $= \mathcal{T}(\mathcal{A}) \cup \{\mathrm{id}_Q\}$

syntactic semigroup $=$ transition semigroup of the minimal automaton

Every semigroup S is isomorphic to a subsemigroup of $\mathcal{T}(S^1)$:

$$\delta_x(y) = y \cdot x \qquad\qquad S \cong \{ \delta_x \mid x \in S \}$$

Partial transformations: $\mathcal{PT}(Q) \subseteq \mathcal{T}(Q \cup \{s\})$, where s is a new sink state

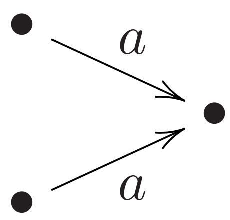
Group Languages

Finite transformation semigroup is a group

$\iff$ contains only permutations

$\iff$ minimal automaton is dually deterministic

$\iff$ minimal automaton does not contain the pattern



(automaton cannot remember letters, only counts)

Relations

Full relation monoid $\mathcal{R}(Q) \supseteq \mathcal{T}(Q)$ ... all binary relations on Q with composition as operation

$(p,q) \in \sigma \circ \delta \iff \exists r \in Q\colon (p,r) \in \sigma \;\&\; (r,q) \in \delta$

$\mathcal{A} = (Q, A, \delta)$ non-deterministic automaton without initial and final states

$\delta_a = \{\, (p,q) \in Q \times Q \mid (p,a,q) \in \delta \,\}$ for all $a \in A$

determines homomorphism $\varphi\colon\ A^* \to \mathcal{R}(Q)$, where $\varphi(a) = \delta_a$

subsemigroup of $\mathcal{R}(Q)$ generated by mappings δ_a recognizes all languages accepted by $\mathcal{A}$

Monogenic Subsemigroups

$x \in S$ generates the subsemigroup $\langle x \rangle = \{\, x^n \mid n \in \mathbb{N} \,\}$

Case 1: $\langle x \rangle$ infinite, isomorphic to $(\mathbb{N}, +)$

$$x \longrightarrow x^2 \longrightarrow x^3 \longrightarrow \cdots$$

Case 2: there exist smallest index $i \geq 1$ and period $p \geq 1$ such that $x^{i+p} = x^i$

$$\begin{tikzcd}
& & & & x^{i+1} \arrow[r] & \cdots \arrow[dr] & \\
x \arrow[r] & x^2 \arrow[r] & \cdots \arrow[r] & x^i = x^{i+p} \arrow[ur] & & & \vdots \arrow[dl] \\
& & & & x^{i+p-1} \arrow[ul] & \cdots \arrow[l] &
\end{tikzcd}$$

$\{x^i, \ldots, x^{i+p-1}\}$ cyclic subgroup of S

$x^\omega = \lim\limits_{n \to \infty} x^{n!} = x^{|S|!}$ unique idempotent in $\langle x \rangle$, identity element of the subgroup

periodic semigroup $=$ all monogenic subsemigroups are finite

finite $\Longrightarrow$ periodic

idempotents are exactly elements x^ω for $x \in S$

Green's Relations

$I \subseteq S$ left (right) ideal of S ... $SI \subseteq I$ ($IS \subseteq I$)

$I \subseteq S$ ideal of S ... $SIS \subseteq I$

left (right) ideal generated by $x \in S$ ... S^1x (xS^1)

ideal generated by $x \in S$ ... S^1xS^1

Green's quasiorders:

$$y \leq_{\mathcal{L}} x \iff S^1y \subseteq S^1x \iff y \in S^1x$$

$$y \leq_{\mathcal{R}} x \iff yS^1 \subseteq xS^1 \iff y \in xS^1$$

$$y \leq_{\mathcal{J}} x \iff S^1yS^1 \subseteq S^1xS^1 \iff y \in S^1xS^1$$

$$y \leq_{\mathcal{L}} x \implies yz \leq_{\mathcal{L}} xz$$

$$y \leq_{\mathcal{R}} x \implies zy \leq_{\mathcal{R}} zx$$

$$S^1xS^1 = \{\, y \in S \mid y \leq_{\mathcal{J}} x \,\}$$

Green's equivalence relations:

$$x \mathrel{\mathcal{L}} y \iff y \leq_{\mathcal{L}} x \,\&\, y \leq_{\mathcal{L}} x \iff S^1x = S^1y$$

$$x \mathrel{\mathcal{R}} y \iff y \leq_{\mathcal{R}} x \,\&\, y \leq_{\mathcal{R}} x \iff xS^1 = yS^1$$

$$x \mathrel{\mathcal{J}} y \iff y \leq_{\mathcal{J}} x \,\&\, y \leq_{\mathcal{J}} x \iff S^1xS^1 = S^1yS^1$$

quasiorders induce partial ordering of the corresponding classes

multiplying element from any side $\rightsquigarrow$ descending in the ordering of $\mathcal{J}$-classes

multiplying element from the left (right) $\rightsquigarrow$ descending in the ordering of $\mathcal{L}(\mathcal{R})$-classes

In a monoid, invertible elements form the top $\mathcal{J}$-class, which is a group.

Zero always forms a one-element bottom $\mathcal{J}$-class.

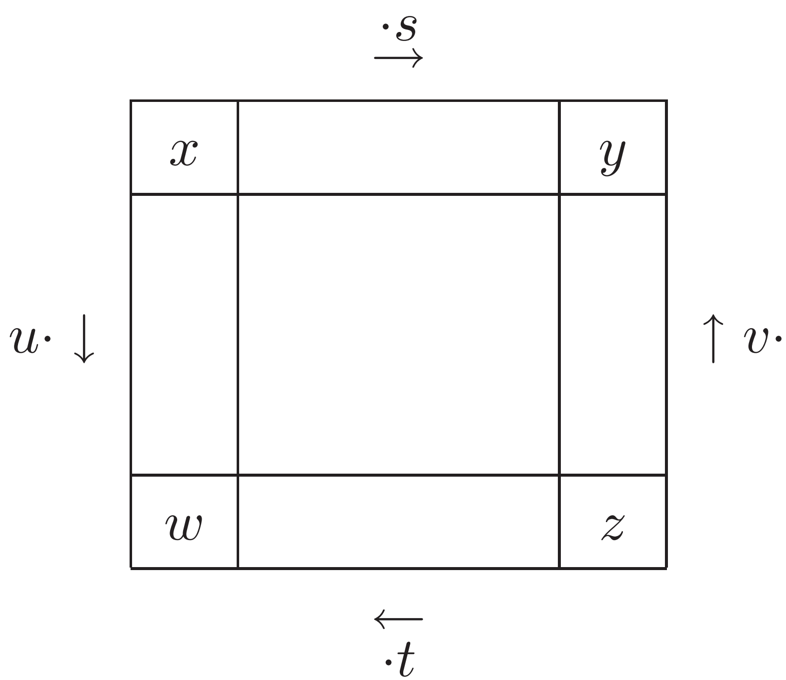
Every semigroup has at most one minimal $\mathcal{J}$-class.

Lemma: $\mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$

Proof:

$$x \, \mathcal{R} \, y \, \mathcal{L} \, z \implies y = xs, x = yt, z = uy, y = vz$$

$$w = uyt = ux = zt \implies x = yt = vzt = vuyt = vw, z = uy = uxs = uyts = ws$$



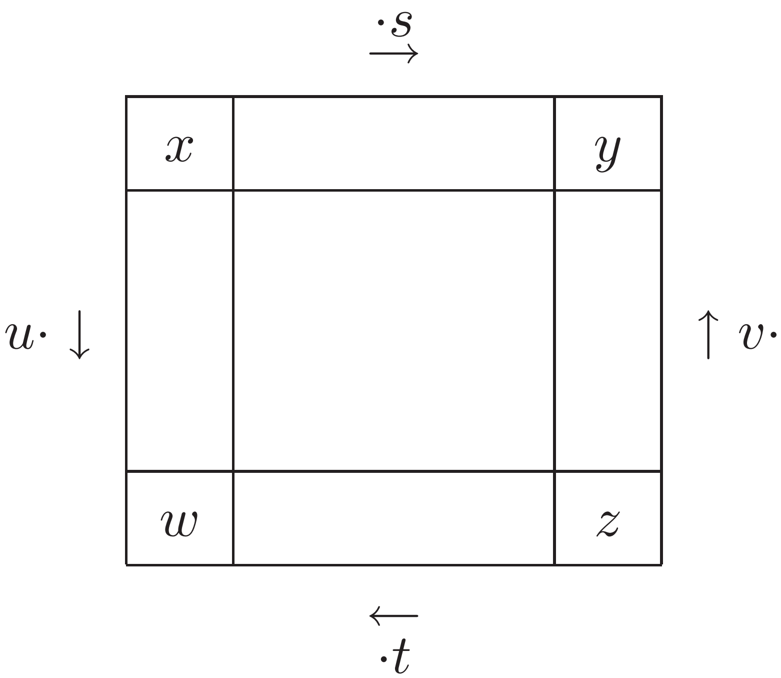
Remaining Green's equivalences: $\mathcal{H} = \mathcal{L} \cap \mathcal{R}, \quad \mathcal{D} = \mathcal{L} \circ \mathcal{R}$

$$x \, \mathcal{D} \, y \iff x\mathcal{R} \cap y\mathcal{L} \neq \emptyset \iff x\mathcal{L} \cap y\mathcal{R} \neq \emptyset$$

$$\mathcal{H} \subseteq \mathcal{L}(\mathcal{R}) \subseteq \mathcal{D} \subseteq \mathcal{J}$$

eggbox . . . $\mathcal{D}$-class row . . . $\mathcal{R}$-class column . . . $\mathcal{L}$-class cell . . . $\mathcal{H}$-class

Bijections Between $\mathcal{H}$-Classes



$\cdot s$ and $\cdot t$ mutually inverse bijections between $\mathcal{L}$-classes of x and y, which preserve $\mathcal{R}$-classes

$u\cdot$ and $v\cdot$ mutually inverse bijections between $\mathcal{R}$-classes of x and w, which preserve $\mathcal{L}$-classes

$\rightsquigarrow$ bijections between all $\mathcal{H}$-classes in a $\mathcal{D}$-class

Examples:

A^*:

$u \leq_{\mathcal{L}} v \iff v$ is a suffix of u

$u \leq_{\mathcal{R}} v \iff v$ is a prefix of u

$u \leq_{\mathcal{J}} v \iff v$ is a factor of u

$u \mathrel{\mathcal{J}} v \iff u \mathrel{\mathcal{D}} v \iff u \mathrel{\mathcal{L}} v \iff u \mathrel{\mathcal{R}} v \iff u \mathrel{\mathcal{H}} v \iff u = v$

($\mathcal{J}$-trivial semigroup)

$\mathcal{T}(Q)$:

$\rho \leq_{\mathcal{L}} \sigma \iff \mathrm{Im}(\rho) \subseteq \mathrm{Im}(\sigma)$ $\qquad$ $\rho \mathrel{\mathcal{L}} \sigma \iff \mathrm{Im}(\rho) = \mathrm{Im}(\sigma)$

$\rho \leq_{\mathcal{R}} \sigma \iff \ker(\rho) \supseteq \ker(\sigma)$ $\qquad$ $\rho \mathrel{\mathcal{R}} \sigma \iff \ker(\rho) = \ker(\sigma)$

$\rho \leq_{\mathcal{J}} \sigma \iff |\mathrm{Im}(\rho)| \leq |\mathrm{Im}(\sigma)|$

$\rho \mathrel{\mathcal{D}} \sigma \iff \rho \mathrel{\mathcal{J}} \sigma \iff |\mathrm{Im}(\rho)| = |\mathrm{Im}(\sigma)|$

Schützenberger Groups

M monoid, H $\mathcal{H}$-class of M

(right) Schützenberger group $\Gamma(H)$: all bijections of H of the form $x \mapsto xs$, where $s \in M$

$|\Gamma(H)| = |H|$

Schützenberger groups of $\mathcal{H}$-classes in the same $\mathcal{D}$-class are isomorphic.

For every $\mathcal{H}$-class H, either $H^2 \cap H = \emptyset$ or H is a subgroup maximal w.r.t. inclusion and isomorphic to its Schützenberger group.

Maximal subgroups are precisely $\mathcal{H}$-classes containing an idempotent.

Theorem: In every finite (periodic) semigroup, $\mathcal{D} = \mathcal{J}$.

Proof:

$$x \; \mathcal{J} \; y \implies \exists p, q, s, t \in S^1 : x = pyq, \; y = sxt$$

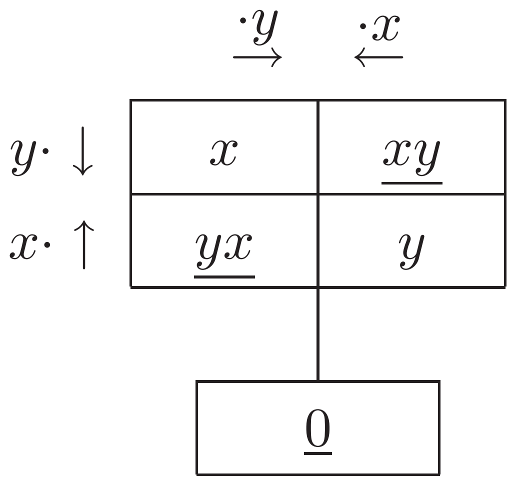
$$y = spyqt = (sp)^2 y (qt)^2 = \cdots = (sp)^\omega y (qt)^\omega = (sp)^\omega (sp)^\omega y (qt)^\omega = (sp)^\omega y$$

$x \; \mathcal{L} \; yq$: $\quad x = p \cdot yq$

$$yq = (sp)^\omega yq = (sp)^{\omega-1} spyq = (sp)^{\omega-1} s \cdot x$$

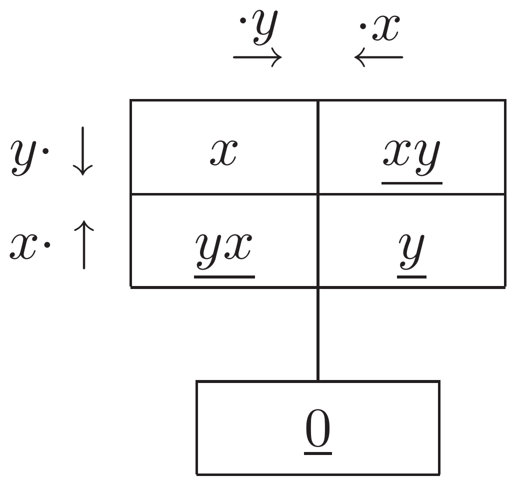
$y \; \mathcal{R} \; yq$: $\quad y = y(qt)^\omega = yq \cdot t(qt)^{\omega-1}$

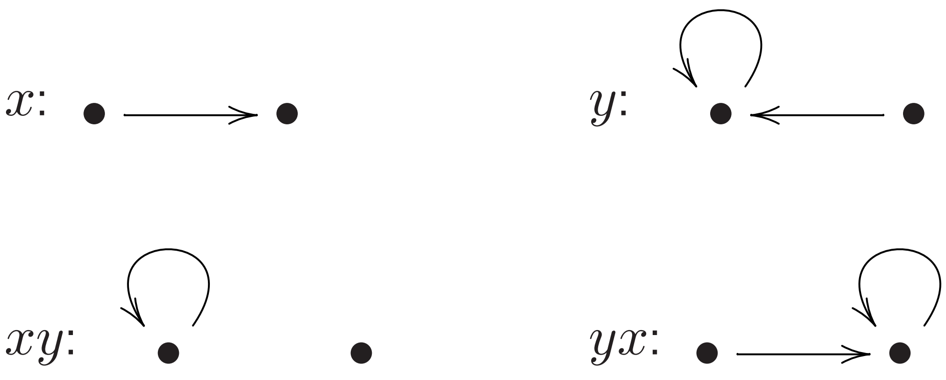
Example: subsemigroup of $\mathcal{PT}(2)$



$x^2 = y^2 = 0$ $\qquad$ $xyx = x$ $\qquad$ $yxy = y$

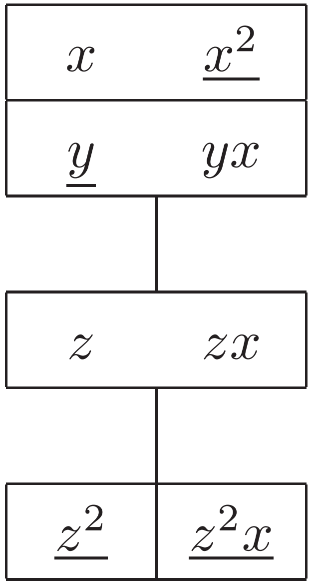
Similar example: subsemigroup of $\mathcal{PT}(2)$

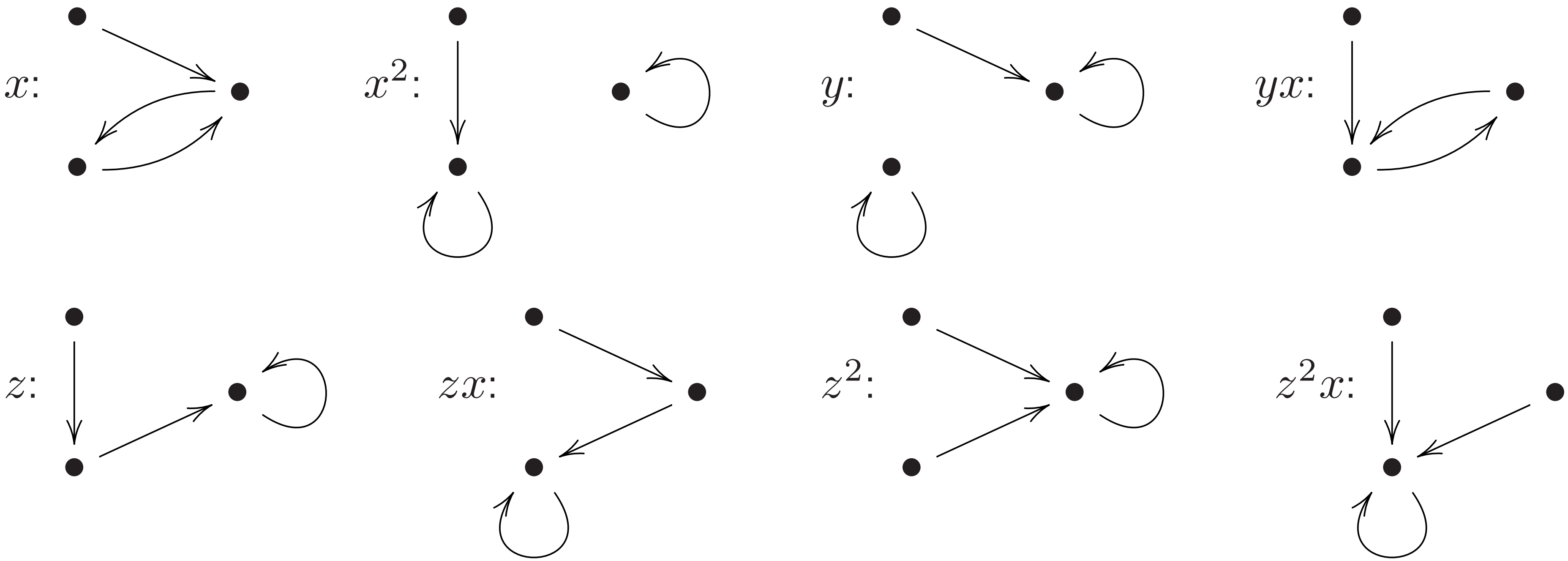




$x^2 = 0$ $\qquad xyx = x$ $\qquad yxy = y$

More interesting example: subsemigroup of $\mathcal{T}(3)$





x and z belong to the same $\mathcal{L}$-class of $\mathcal{T}(3)$

Basic Properties of Green's Relations in Finite Semigroups

Lemma: S finite semigroup, $x, y \in S$ such that $x \leq_{\mathcal{L}} y$ and $x \mathrel{\mathcal{J}} y$. Then $x \mathrel{\mathcal{L}} y$.

Proof: $x = sy \implies y = txu = tsyu = (ts)^\omega yu^\omega = (ts)^{\omega-1}tsy = (ts)^{\omega-1}tx$.

Reformulations: In any finite semigroup:

- $x \leq_{\mathcal{J}} xs \implies x \mathrel{\mathcal{R}} xs$
- $x <_{\mathcal{L}} y \implies x <_{\mathcal{J}} y$

Corollary: In any finite semigroup, $sxt \mathrel{\mathcal{H}} x \implies sx \mathrel{\mathcal{H}} xt \mathrel{\mathcal{H}} x$.

Proof: $sx \leq_{\mathcal{L}} x$, $x \leq_{\mathcal{R}} sx$, $sx \mathrel{\mathcal{J}} x$

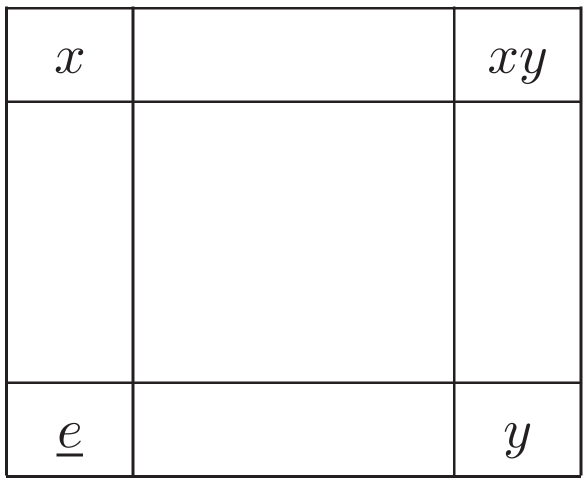
Lemma: If x and y are $\mathcal{J}$-equivalent elements of a finite semigroup, then $xy \; \mathcal{J} \; x$ if and only if there exists an idempotent e such that $x \; \mathcal{L} \; e \; \mathcal{R} \; y$. In that case, we have $x \; \mathcal{R} \; xy \; \mathcal{L} \; y$.

Proof of "$\Longleftarrow$" :

$x = se$, $y = et \implies xy = seet = xt$

$\xrightarrow{\cdot t}$

$s\cdot \uparrow$



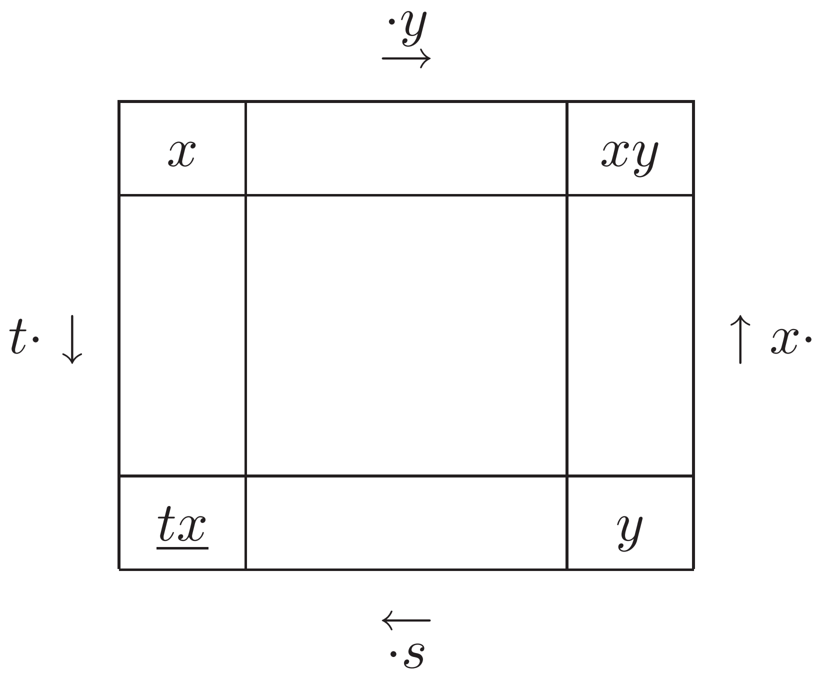
Lemma: If x and y are $\mathcal{J}$-equivalent elements of a finite semigroup, then $xy \mathrel{\mathcal{J}} x$ if and only if there exists an idempotent e such that $x \mathrel{\mathcal{L}} e \mathrel{\mathcal{R}} y$. In that case, we have $x \mathrel{\mathcal{R}} xy \mathrel{\mathcal{L}} y$.

Proof of "$\Longrightarrow$" :

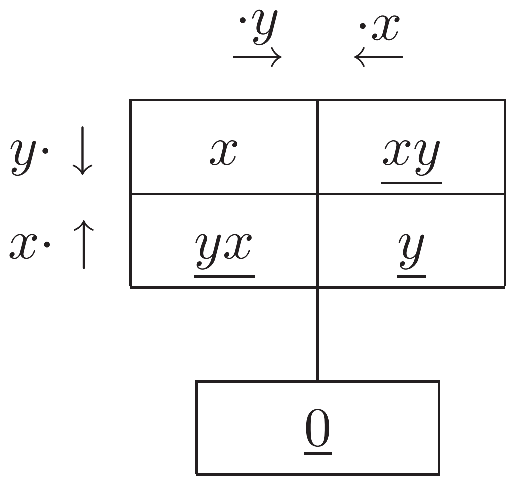
$$xy \leq_{\mathcal{R}} x \text{ \& } xy \mathrel{\mathcal{J}} x \implies xy \mathrel{\mathcal{R}} x$$

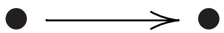
$$xy \leq_{\mathcal{L}} y \text{ \& } xy \mathrel{\mathcal{J}} y \implies xy \mathrel{\mathcal{L}} y$$

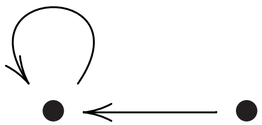
$$x = xys \text{ \& } y = txy \implies (tx)^2 = txtxys = txys = tx$$



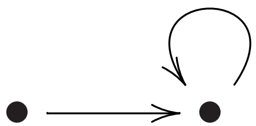
Recalling example: subsemigroup of $\mathcal{PT}(2)$



x: 

y: 

xy: 

yx: 

$x^2 = 0$ $\qquad xyx = x$ $\qquad yxy = y$

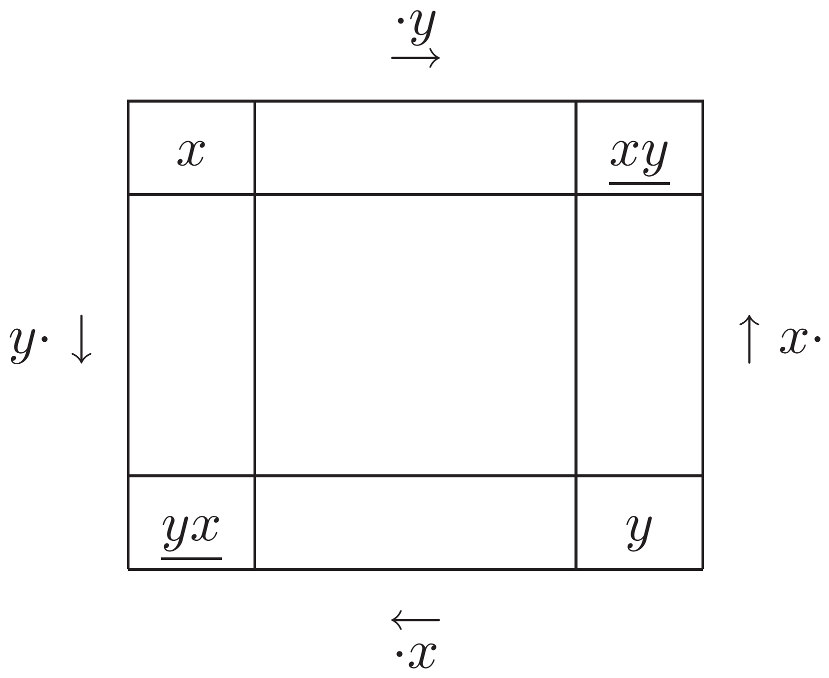
Regular Elements

y is a (semigroup) inverse of x, if $xyx = x$ & $yxy = y$

$x \in S$ is regular $=$ has an inverse

x belongs to a subgroup $\implies$ x is regular

y inverse of x $\implies$ xy and yx are idempotents in the same $\mathcal{D}$-class



$x \in S$ regular $\iff$ $\exists y, z \in S : x = (yz)^{\omega} y$ (inverse is $z(yz)^{\omega-1}$)

Examples:

A^+: no regular elements

$\mathcal{T}(Q)$:

ρ is idempotent $\iff \forall q \in \mathrm{Im}(\rho)\colon \rho(q) = q$

ρ belongs to a subgroup $\iff \rho|_{\mathrm{Im}(\rho)}\colon \mathrm{Im}(\rho) \to \mathrm{Im}(\rho)$ is a bijection

$\iff \mathrm{Im}(\rho)$ forms a transversal (set of representatives) of $\ker(\rho)$

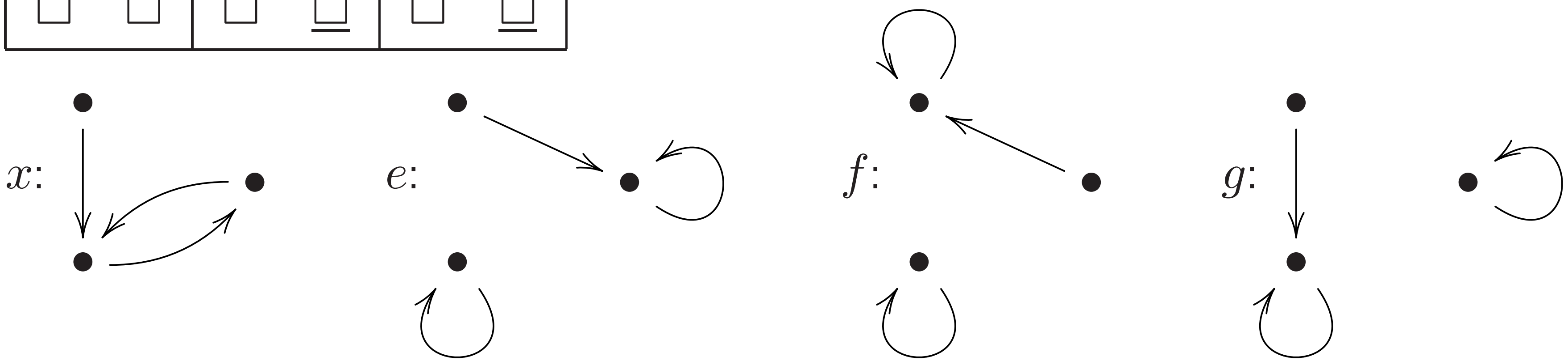
every element is regular

Regular $\mathcal{D}$-Classes

Example:

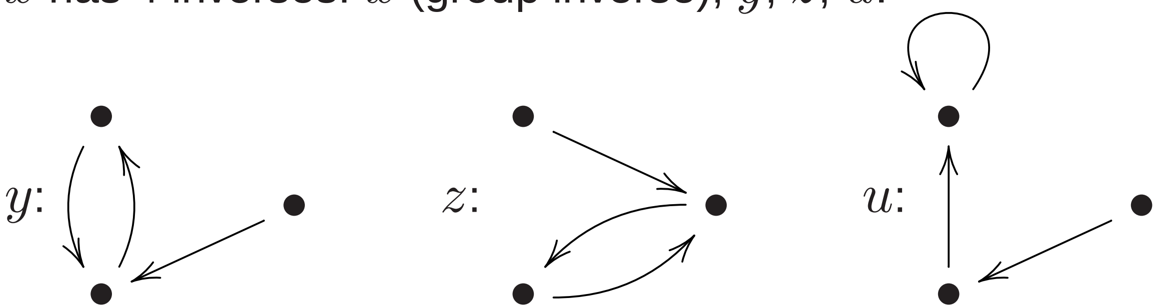
a $\mathcal{D}$-class of $\mathcal{T}(3)$ with two-element $\mathcal{H}$-classes

$x \quad \underline{e}$	$y \quad \underline{f}$	$\square \quad \square$
$z \quad \underline{g}$	$u \quad \square$	$\square \quad \underline{\square}$
$\square \quad \square$	$\square \quad \underline{\square}$	$\square \quad \underline{\square}$



Idempotents $\mathcal{R}$-related to x are e and f. Idempotents $\mathcal{L}$-related to x are e and g.

x has 4 inverses: x (group inverse), y, z, u.



Regular $\mathcal{D}$-Classes

Regular $\mathcal{D}$-class — equivalent definitions:

1) Contains an idempotent.

2) Contains a regular element.

3) Every element is regular.

4) Every $\mathcal{L}$-class and every $\mathcal{R}$-class contains an idempotent.

2 $\implies$ 3: $xyx = x$, $yxy = y$, $z = xs$, $x = zt$

$$z \xrightarrow{\cdot t} x \xrightarrow{\cdot y} xy$$

$$z(ty)z = xyxs = xs = z,\ (ty)z(ty) = tyxy = ty$$

In a finite semigroup, a $\mathcal{D}$-class is regular if and only if it contains some elements x and y together with their product xy.

regular $\mathcal{D}$-class ... products can stay there for arbitrarily many multiplications

Every idempotent is a left identity for its $\mathcal{R}$-class and a right identity for its $\mathcal{L}$-class.

Proof: $x = es \implies ex = ees = es = x$

Theorem: (Miller & Clifford 1956)

There is a bijection between inverses of x and pairs of idempotents (e, f) such that $e \mathcal{R} x \mathcal{L} f$; there exists exactly one inverse y such that $e \mathcal{L} y \mathcal{R} f$, and it satisfies $xy = e$ and $yx = f$.

Proof: if $e = xs$, take $y = fs$

$$\underline{x(fs)}x = \underline{xs}x = ex = x$$

$$(fs)\underline{x(fs)} = fs\underline{xs} = fse = fs$$

$$\xrightarrow{\cdot s}$$

x		$\underline{e}$
$\underline{f}$		y

$$\xrightarrow[\cdot s]{}$$

Consequence:

Idempotents e and f belong to the same $\mathcal{D}$-class if and only if there exist mutually inverse elements x and y such that $e = xy$ and $f = yx$.

$$
\begin{array}{ccc}
 & \xrightarrow{\cdot y} & \\
y\cdot \downarrow & \begin{array}{|c|c|c|}\hline x & & \underline{e = xy} \\ \hline & & \\ & & \\ \hline \underline{f = yx} & & y \\ \hline\end{array} & \uparrow x\cdot \\
 & \xleftarrow[\cdot x]{} &
\end{array}
$$

Consequence:

Two $\mathcal{H}$-classes in the same $\mathcal{D}$-class, which contain an idempotent, are isomorphic subgroups.

Proof: isomorphism $z \mapsto yzx$, where x and y are mutually inverse elements such that $e = xy$ and $f = yx$.

0-Simple Semigroups

Simple semigroup $=$ has no proper ideal $=$ has only one $\mathcal{J}$-class

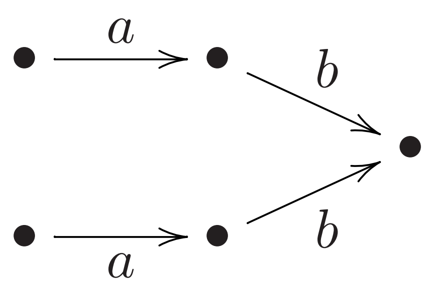
Null semigroup ... $S^2 = \{0\}$

0-simple semigroup ... $S^2 \neq \{0\}$ & exactly two ideals $\{0\}$, S (two $\mathcal{J}$-classes $\{0\}$, $S \setminus \{0\}$)

S simple $\implies$ $S \cup \{0\}$ 0-simple

A finite semigroup S is simple $\iff$ $\forall x, y \in S \colon x^{\omega+1} = x \;\&\; (xyx)^{\omega} = x^{\omega}$.

Regular language is recognizable by a finite simple semigroup if and only if its minimal automaton does not contain the pattern



Equivalent formulation:

For any letters $a, b \in A$, $\mathrm{Im}(\delta_a)$ forms a transversal (set of representatives) of $\ker(\delta_b)$.

Structure of $\mathcal{D}$-Classes

Rees quotient:

I ideal of S, $\qquad S/I = (S \setminus I) \cup \{0\}$

(subset $I \subseteq S$ downward closed w.r.t. $\mathcal{J}$ becomes zero of S/I)

corresponds to congruences of the form $\mathrm{id}_S \cup I \times I$

Divisibility in regular $\mathcal{D}$-classes:

D regular $\mathcal{D}$-class, $e \in D$ idempotent, $x \mathrel{\mathcal{R}} e \implies x \in eD$ and $e \in xD$

$$\xrightarrow{\cdot y}$$

x		$\underline{e = xy}$
$\underline{f = yx}$		y

$$\xleftarrow[\cdot x]{}$$

Consequence:

D regular $\mathcal{D}$-class, $x, y \in D \implies \exists z \in D\colon x \in zD \;\&\; z \in xD \;\&\; y \in Dz \;\&\; z \in Dy$

Principal Factors

Principal factors of a finite semigroup S:

- bottom $\mathcal{D}$-class ($=$ least ideal) is a simple semigroup
- D non-regular $\mathcal{D}$-class $\implies D \cup \{0\} = S^1 D S^1 / (S^1 D S^1 \setminus D)$ is a null-semigroup
- D regular $\mathcal{D}$-class $\implies D \cup \{0\} = SDS/(SDS \setminus D)$ is a 0-simple semigroup

Principal factors of homomorphic images:

S, T finite semigroups, $\varphi\colon S \twoheadrightarrow T$ onto homomorphism

$\forall x \in S,\ z \in T\colon\ z \leq_{\mathcal{J}} \varphi(x) \iff \exists y \leq_{\mathcal{J}} x\colon \varphi(y) = z$

D a $\mathcal{D}$-class of T, choose x $\mathcal{J}$-minimal in $\varphi^{-1}(D)$

Then $y <_{\mathcal{J}} x \implies \varphi(y) <_{\mathcal{J}} \varphi(x)$. $\qquad \implies D$ is the image of $x\mathcal{D}$

Every principal factor of T is image of a principal factor of S via homomorphism induced by φ.

Every (maximal) subgroup of T is of the form $\varphi(G)$ for a (maximal) subgroup G of S.

Proof:

$e \in T$ idempotent $\implies$ exists idempotent $f \in S\colon \varphi(f) = e$ & f $\mathcal{J}$-minimal in $\varphi^{-1}(e\mathcal{H})$

($\varphi(y)\ \mathcal{H}\ e \implies \varphi(y^\omega) = e$)

$e\mathcal{H} = \varphi(f\mathcal{H})$: $\quad x \in S$ satisfies $\varphi(x)\ \mathcal{H}\ e \implies \varphi(fxf) = \varphi(x)$ & $fxf\ \mathcal{H}\ f$

Classification of Finite 0-Simple Semigroups

Rectangular bands: R and L arbitrary finite sets

multiplication on $R \times L$: $(r, \ell) \cdot (r', \ell') = (r, \ell')$

$(r, \ell) \, \mathcal{R} \, (r', \ell') \iff r = r'$ $\qquad$ $(r, \ell) \, \mathcal{L} \, (r', \ell') \iff \ell = \ell'$

all $\mathcal{H}$-classes are trivial groups

S simple $\implies$ $\mathcal{H}$ is a congruence, $S/\mathcal{H}$ is a rectangular band and all $\mathcal{H}$-classes are isomorphic groups

Rees matrix semigroup: R and L finite sets, G finite group

$P = (p_{\ell r})_{\ell \in L,\, r \in R}$ ... $L \times R$-matrix with entries in $G \cup \{0\}$ and with at least one non-zero entry in every row and every column

multiplication on $\mathfrak{M}^0(R, L, G, P) = (R \times G \times L) \cup \{0\}$:

$$(r, g, \ell) \cdot (r', g', \ell') = \begin{cases} (r, g \cdot p_{\ell r'} \cdot g', \ell') & \text{if } p_{\ell r'} \neq 0 \\ 0 & \text{if } p_{\ell r'} = 0 \end{cases}$$

Matrix representation of $\mathfrak{M}^0(R, L, G, P)$:

(r, g, ℓ) corresponds to the matrix with only one non-zero entry g in the position (r, ℓ)

sandwich multiplication: $M \cdot N = MPN$

Theorem: (Rees 1940)

A finite semigroup is 0-simple if and only if it is isomorphic to some $\mathfrak{M}^0(R, L, G, P)$.

Proof:

S ... 0-simple semigroup

G ... Schützenberger group of the non-zero $\mathcal{D}$-class

R ... the set of $\mathcal{R}$-classes, L ... the set of $\mathcal{L}$-classes

choose a group $\mathcal{H}$-class and elements t_r and s_ℓ, for $r \in R$ and $\ell \in L$

$$\begin{array}{c|c|c|c|}
 & & \xrightarrow{\cdot s_\ell} & \ell \\
\hline
 & G & & s_\ell \\
\hline
t_r \cdot \downarrow & & & \\
\hline
r & t_r & & t_r g s_\ell \\
\hline
\end{array}$$

Every element can be uniquely expressed in the form $t_r g s_\ell$, for $r \in R$, $g \in G$ and $\ell \in L$.

$(t_r g s_\ell)(t_{r'} g' s_{\ell'}) = t_r (g s_\ell t_{r'} g') s_{\ell'} \quad \rightsquigarrow \quad$ set $p_{\ell r} = s_\ell t_r \in G \cup \{0\}$

Finite simple semigroups: all entries of P belong to G

Repetitions in Products

Lemma: (cancellation rule in a $\mathcal{J}$-class)

In every finite semigroup: $x \mathrel{\mathcal{J}} y \mathrel{\mathcal{J}} z \mathrel{\mathcal{J}} xy = xyz \implies y = yz$.

Proof: $y \mathrel{\mathcal{R}} yz$, $x\cdot$ is a bijection between $\mathcal{R}$-classes of y and xy

Repetitions in products staying in the same $\mathcal{J}$-class:

Lemma: J a $\mathcal{J}$-class of a finite semigroup, $x_1 \cdots x_n \in J$, $|\{ i \mid x_i \in J \}| > |J|$.

Then there exist $i < j$ such that $x_i, x_j \in J$ and $x_i \cdots x_j = x_i$.

Proof:

k smallest such that $x_k \in J$

$\forall j \geq k \colon x_k \cdots x_j \in J \implies$

$\exists k \leq i < j \colon x_i, x_j \in J \;\&\; x_k \cdots x_i = x_k \cdots x_j$ (by pigeonhole principle)

$x_k \cdots x_{i-1} \mathrel{\mathcal{J}} x_i \mathrel{\mathcal{J}} x_{i+1} \cdots x_j \mathrel{\mathcal{J}} (x_k \cdots x_{i-1}) x_i (x_{i+1} \cdots x_j)$

cancellation rule $\implies x_i \cdots x_j = x_i$

Finite Power Property

L possesses the finite power property $\iff \exists n\colon L^+ = L \cup L^2 \cup \cdots \cup L^n$

Does a given regular language L have the finite power property?

decidable (Hashiguchi 1979, Simon 1978)

Construction: (Birget & Rhodes 1984)

$\varphi\colon A^+ \longrightarrow S$ homomorphism recognizing L and L^+

define mapping $\tau\colon A^+ \longrightarrow \wp(S^3)$

$$\tau(w) = \{\, (\varphi(t), \varphi(u), \varphi(v)) \mid t, u, v \in A^+,\ w = tuv \,\}$$

τ induces a semigroup operation on $\tau(L^+) \subseteq \wp(S^3)$ $\rightsquigarrow$ τ homomorphism

Theorem: For a regular language L, the following conditions are equivalent: (MK 2006)

- L possesses the finite power property.
- For all $w \in L^+$, there exists n such that $w^n \in L \cup \cdots \cup L^n$.
- Every regular $\mathcal{D}$-class of $\tau(L^+)$ contains some element of $\tau(L)$.
- $L^+ = L \cup \cdots \cup L^{(j+1)^h}$

  j … maximal size of a $\mathcal{J}$-class of S

  h … length of the longest chain of $\mathcal{J}$-classes in $\tau(L^+)$

Star-Free Languages and Aperiodic Semigroups

star-free language $=$ definable by rational expression with union, concatenation and complementation (without Kleene star)

Example: $A = \{a, b\}, \quad (ab)^+ = a\overline{\emptyset} \cap \overline{\emptyset}b \cap \overline{\overline{\emptyset}aa\overline{\emptyset}} \cap \overline{\overline{\emptyset}bb\overline{\emptyset}}$ is star-free

Aperiodic semigroup S — equivalent definitions:

- $\forall x \in S\, \exists n \colon x^{n+1} = x^n \quad (x^{\omega+1} = x^{\omega})$
- periodic semigroup where all subgroups are trivial

Prohibited pattern in minimal automaton:

cycle labelled by a non-primitive word w^n, $n \geq 2$ (counter-free automaton)

Lemma: Periodic semigroup is aperiodic $\iff$ $\mathcal{H}$ is trivial.

Proof: $y = xs \;\&\; x = ty \implies y = tys = t^{\omega}ys^{\omega} = t^{\omega+1}ys^{\omega} = ty = x$

M finite monoid, $x, x_1, \ldots, x_n \in M$.

Task: Describe all products $y = x_1 \cdots x_n$ satisfying $y \mathrel{\mathcal{H}} x$ using union, concatenation, complementation and descriptions of products belonging to higher $\mathcal{J}$-classes.

Lemma: $x_1 \cdots x_n \mathrel{\mathcal{H}} x \iff$

1. $x_1 \cdots x_i \mathrel{\mathcal{R}} x$ for some $i \leq n$,
2. $x_i \cdots x_n \mathrel{\mathcal{L}} x$ for some $i \leq n$,
3. $x_1 \cdots x_n \geq_{\mathcal{J}} x$.

Proof of "$\Longleftarrow$" : $y = x_1 \cdots x_n$

$y \geq_{\mathcal{J}} x$ & $y \leq_{\mathcal{R}} x$ & $y \leq_{\mathcal{L}} x \implies y \mathrel{\mathcal{R}} x$ & $y \mathrel{\mathcal{L}} x$

These three conditions can be expressed using characterizations for higher $\mathcal{J}$-classes by considering positions i, where they become true (1 and 2) or false (3). This is a local event.

Lemma:

$x_1 \cdots x_i \mathrel{\mathcal{R}} x$ for some $i \iff$ exists i such that $x_1 \cdots x_{i-1} >_{\mathcal{J}} x$ and $x_1 \cdots x_i \mathrel{\mathcal{R}} x$.

Proof of "$\Longrightarrow$" : take the smallest i such that $x_1 \cdots x_i \mathrel{\mathcal{R}} x$

Lemma: $x_1 \cdots x_n \not\geq_{\mathcal{J}} x \iff$ either $x_i \not\geq_{\mathcal{J}} x$ for some i

or $x_{i+1} \cdots x_{j-1} >_{\mathcal{J}} x$ and $x_i \cdots x_j \not\geq_{\mathcal{J}} x$ for some $i < j$.

Proof of "$\Longrightarrow$" : Take $i \leq j$ such that $x_i \cdots x_j \not\geq_{\mathcal{J}} x$ and $j - i$ is smallest possible.

$i = j \implies x_i \not\geq_{\mathcal{J}} x$

$i < j \implies y = x_{i+1} \cdots x_{j-1} \geq_{\mathcal{J}} x$

$y \geq_{\mathcal{L}} x_i y \geq_{\mathcal{J}} x$ and $y \geq_{\mathcal{R}} y x_j \geq_{\mathcal{J}} x$ (minimality of $x_i y x_j$)

Assume $y \mathrel{\mathcal{J}} x$. Then $x_i y \mathrel{\mathcal{J}} y x_j \mathrel{\mathcal{J}} y$, and so $x_i y \mathrel{\mathcal{L}} y$ and $y x_j \mathrel{\mathcal{R}} y$.

$\xrightarrow{\cdot x_j}$

	y		yx_j
$x_i \cdot \downarrow$			
	$x_i y$		$x_i y x_j$

$x_i \cdots x_j = x_i y x_j \mathrel{\mathcal{J}} y \mathrel{\mathcal{J}} x$, contradiction

Therefore $y >_{\mathcal{J}} x$.

Theorem: Regular language L is star-free $\iff$ $\mathcal{M}(L)$ is aperiodic. (Schützenberger 1965)

Proof: "$\Longrightarrow$" direct verification

"$\Longleftarrow$" $\varphi\colon A^* \to M$ homomorphism, where M is a finite aperiodic monoid, i.e. $\mathcal{H}$-trivial

We prove that $\varphi^{-1}(x)$ is star-free for all $x \in M$ by induction downwards on $\geq_{\mathcal{J}}$:

- highest $\mathcal{J}$-class = $\{1\}$:

$\varphi^{-1}(1) = A^* \setminus (A^* \cdot \{\, a \in A \mid \varphi(a) \neq 1 \,\} \cdot A^*)$

- induction step:

$\varphi(w) = x \iff \varphi(w)\ \mathcal{H}\ x$

$\varphi^{-1}(x) = (RA^* \cap A^*L) \setminus A^*JA^*$

$$R = \bigcup \{\, \varphi^{-1}(y)a \mid y \in M,\ a \in A,\ y >_{\mathcal{J}} x,\ y\varphi(a)\ \mathcal{R}\ x \,\}$$

$$L = \bigcup \{\, a\varphi^{-1}(y) \mid y \in M,\ a \in A,\ y >_{\mathcal{J}} x,\ \varphi(a)y\ \mathcal{L}\ x \,\}$$

$$J = \{\, a \in A \mid \varphi(a) \not\geq_{\mathcal{J}} x \,\}$$
$$\cup \bigcup \{\, a\varphi^{-1}(y)b \mid y \in M,\ a, b \in A,\ y >_{\mathcal{J}} x,\ \varphi(a)y\varphi(b) \not\geq_{\mathcal{J}} x \,\}$$

M is $\mathcal{H}$-trivial $\Longrightarrow$ $\varphi^{-1}(y)$ definable by induction assumption

Example: $\mathcal{M}((a^2)^*)$ is a two-element group $\Longrightarrow$ $(a^2)^*$ is not star-free

Occurrences of Idempotents in Products

S finite semigroup, $E(S)$ the set of idempotents of S

Lemma: $\forall n \geq |S|\colon S^n = S \cdot E(S) \cdot S$

Proof: $x_1, \ldots, x_n \in S$

case 1: $x_1 \cdots x_i$ all different $\implies$ some of them is idempotent

case 2: $x_1 \cdots x_i = x_1 \cdots x_i x_{i+1} \cdots x_j \implies x_1 \cdots x_i = x_1 \cdots x_i (x_{i+1} \cdots x_j)^\omega$

Theorem: For every finite semigroup S and $k \geq 2$ there exists n such that for every $x_1, \ldots, x_n \in S$ there is an idempotent $e \in E(S)$ and $0 \leq i_1 < \cdots < i_k \leq n$ satisfying $x_{i_j+1} \cdots x_{i_\ell} = e$ for all $1 \leq j < \ell \leq n$.

follows directly from Ramsey's theorem: graph nodes = positions in the word $x_1 \ldots x_n$

colours = elements of S

Hall & Sapir 1996: S has n non-idempotent elements $\implies$ every sequence of 2^n elements contains a factor evaluating to an idempotent (optimal value)

Factorization Forests

$\varphi\colon A^* \to M$ homomorphism to a finite monoid

factorization forest of φ:

$d\colon \{\, w \in A^* \mid |w| \geq 2 \,\} \to (A^+)^+$ such that

if $d(w) = (w_1, \ldots, w_n)$ then:

1) $w = w_1 \ldots w_n$
2) $|w_i| < |w|$
3) $n \geq 3 \implies \varphi(w) = \varphi(w_1) = \cdots = \varphi(w_n)$ is idempotent

d provides for every word w a tree with root labelled by w, nodes labelled by its factors and leaves by letters, which expresses successive factorizations of w up to letters.

Node with more than two successors $\implies$ all labels evaluate to the same idempotent.

height of d: (height of the highest tree)

$$h(a) = 0 \quad \text{for } a \in A$$

$$h(w) = \max\{h(w_1), \ldots, h(w_n)\} + 1 \quad \text{if } d(w) = (w_1, \ldots, w_n)$$

$$h(d) = \sup\{\, h(w) \mid w \in A^+ \,\}$$

Example:

$M = (\mathbb{Z}, +)/2\mathbb{Z}$ (two-element group)

$\varphi\colon \{a, b\}^+ \to M$ $\varphi(a) = 1, \varphi(b) = 0$ (identity element)

Minimal height of a factorization forest for φ is 5:

if $|w|_a$ odd, $w = b^k a \hat{w}$, then

$$d(w) = \begin{cases} (b^k, a) & \text{if } \hat{w} = \varepsilon \\ (b^k a, \hat{w}) & \text{if } \hat{w} \neq \varepsilon \end{cases}$$

if $|w|_a$ even, $w = b^{k_0} a b^{k_1} \dots a b^{k_n}$, then

$$d(w) = \begin{cases} (a, b^{k_1} a) & \text{if } n = 2, k_0 = k_2 = 0 \\ (\underbrace{b, \dots, b}_{k_0}, a b^{k_1} a, \underbrace{b, \dots, b}_{k_2}, \dots, a b^{k_{n-1}} a, \underbrace{b, \dots, b}_{k_n}) & \text{otherwise} \end{cases}$$

word $abbbabbbabbbabbba$ requires tree of height 5

Theorem: (Simon 1990, Kufleitner 2008)

Every morphism from A^* to a finite monoid M has a factorization forest of height $3|M| - 1$.

(tight bound for all finite groups; for aperiodic monoids height $2|M|$ is sufficient)

Proof idea: inductive construction w.r.t. $\mathcal{J}$-classes

long products staying in the same $\mathcal{J}$-class:

$x_1, \ldots, x_n, x_1 \cdots x_n$ belong to the same $\mathcal{J}$-class $\Longrightarrow$

$\mathcal{H}$-class of $x_{i+1} \cdots x_j$ uniquely determined by $\mathcal{R}$-class of x_{i+1} and $\mathcal{L}$-class of x_j

($x_{i+1} \cdots x_j \; \mathcal{J} \; x_j$ & $x_{i+1} \cdots x_j \leq_{\mathcal{L}} x_j \Longrightarrow x_{i+1} \cdots x_j \; \mathcal{L} \; x_j$)

consider repetitions of the pairs $(x_i\mathcal{L}, x_{i+1}\mathcal{R})$

factors between places with the same pair belong to the same $\mathcal{H}$-class

Equivalent formulation: For every homomorphism φ to a finite monoid there exists a regular expression representing A^* where Kleene star is applied only to languages L satisfying $\varphi(L) = \{e\}$ for some idempotent e.

Example of application: decidability of limitedness of distance automata (Simon 1990)

Polynomials

monomial of degree k over A

... language of the form $A_0^* a_1 A_1^* \cdots a_k A_k^*$, where $a_i \in A$ and $A_i \subseteq A$

polynomial $=$ finite union of monomials

(languages of level 3/2 of the Straubing-Thérien concatenation hierarchy)

Factorization forest d gives for every $w \in A^+$ a monomial $P_d(w)$ of degree at most $2^{h(d)}$:

$P_d(a) = \{a\}$ for $a \in A$

$P_d(w) = P_d(w_1) \cdot P_d(w_2)$ if $d(w) = (w_1, w_2)$

$P_d(w) = P_d(w_1) \cdot \mathrm{alph}(w)^* \cdot P_d(w_n)$ if $d(w) = (w_1, \ldots, w_n)$ with $n \geq 3$

Theorem: (Arfi 1991)

For a regular language $L \subseteq A^*$ the following conditions are equivalent:

1) L is a polynomial.

2) L is recognizable by a finite ordered monoid $(M, \leq)$ where every idempotent $e \in E(M)$ is the least element of the subsemigroup $e \cdot \{\, x \in M \mid e \leq_{\mathcal{J}} x \,\}^* \cdot e$.

3) $\forall v, w \in A^* \colon \varphi_L(w) = \varphi_L(w^2) \;\&\; \mathrm{alph}(v) \subseteq \mathrm{alph}(w) \implies w \leq_L wvw$

Proof of "2 $\implies$ 1":

$\varphi\colon A^* \to M$ recognizes finite unions of languages $\{\, w \in A^* \mid \varphi(w) \geq x \,\}$ for $x \in M$.

$d \ldots$ factorization forest of φ of height $3|M|$

We verify $\{\, w \in A^* \mid \varphi(w) \geq x \,\} = \displaystyle\bigcup_{\varphi(w)\geq x} P_d(w)$

(this is a polynomial because degrees are bounded by $2^{3|M|}$)

$\subseteq$: $\quad w \in P_d(w)$

$\supseteq$: $\quad$ It is sufficient to prove by induction that $v \in P_d(w) \implies \varphi(v) \geq \varphi(w)$.

If $d(w) = (w_1, w_2)$ then $v \in P_d(w) = P_d(w_1) \cdot P_d(w_2)$

$\implies v = v_1 v_2, \varphi(v_1) \geq \varphi(w_1), \varphi(v_2) \geq \varphi(w_2)$

$\implies \varphi(v) = \varphi(v_1 v_2) \geq \varphi(w_1 w_2) = \varphi(w)$

If $d(w) = (w_1, \ldots, w_n)$ with $n \geq 3$ then $v \in P_d(w) = P_d(w_1) \cdot \mathrm{alph}(w)^* \cdot P_d(w_n)$

$\implies v = v_1 u v_n, \varphi(v_1) \geq \varphi(w_1), \varphi(v_n) \geq \varphi(w_n), \mathrm{alph}(u) \subseteq \mathrm{alph}(w)$

$\implies \varphi(u) \in \{\, x \in M \mid \varphi(w) \leq_{\mathcal{J}} x \,\}^*$

$\implies \varphi(v) = \varphi(v_1)\varphi(u)\varphi(v_n) \geq \varphi(w_1)\varphi(u)\varphi(w_n) = \varphi(w)\varphi(u)\varphi(w) \geq \varphi(w)$

Well Quasiorders

Recognizing Languages by Monotone Quasiorders

Monotone quasiorder $\leq$ on A^*: $\quad u \leq v \,\&\, \tilde{u} \leq \tilde{v} \implies u\tilde{u} \leq v\tilde{v}$

L recognized by $\leq$ ... L upward closed w.r.t. $\leq$

monotone quasiorder $\leq$ recognizes $L \iff \leq$ contained in the syntactic quasi-order of L

$(u \leq v \implies \mathrm{C}_L(u) \subseteq \mathrm{C}_L(v) \implies u \leq_L v)$

Special case:

recognized by a congruence $=$ union of its classes $=$ recognized by the quotient monoid

recognizing by finite ordered monoids $=$ recognizing by monotone quasiorders with finite index

Are there quasiorders on A^* with infinite index which recognize only regular languages?

all upward closed languages are regular $\iff$ all downward closed languages are regular

(closure under complementation)

Well Quasiorders (Wqo)

$w \in L$ minimal in $L \subseteq A^*$ w.r.t. $\leq \iff (\forall u \in L\colon u \leq w \implies w \leq u)$

Equivalent definitions of well quasiorder $\leq$ on A^*:

- Every infinite sequence of words contains an infinite ascending subsequence.
- For every infinite sequence $(w_i)_{i=1}^{\infty}$ there exist $i < j$ such that $w_i \leq w_j$.
- Contains neither infinite descending chains nor infinite antichains $\bullet \; \bullet \; \bullet \cdots$
- Every upward closed language over A is finitely generated.
- Every non-empty language over A has some minimal element, but only finitely many non-equivalent minimal elements.
- There is no infinite ascending sequence of upward closed languages.

Special case: Congruence of finite index is a monotone well quasiorder.

recognizing by monotone well quasiorders $=$ recognizing by well partially ordered monoids

Theorem: (Ehrenfeucht & Haussler & Rozenberg 1983, de Luca & Varricchio 1994)

For any language $L \subseteq A^*$ the following conditions are equivalent:

1) L is regular.

2) L is upward closed w.r.t. a monotone wqo on A^*.

3) L is upward closed w.r.t. a left-monotone wqo on A^* and w.r.t. a right-monotone wqo on A^*.

(language upward closed w.r.t. a right-monotone wqo need not be regular)

Proof of "3 $\Longrightarrow$ 1":

Left and right syntactic quasiorders $\leq_L^\ell$ and $\leq_L^r$ are wqos.

$w \leq_L^\ell w' \iff (\forall u \in A^*\colon uw \in L \implies uw' \in L) \iff \mathrm{C}_L^\ell(w) \subseteq \mathrm{C}_L^\ell(w')$

$w \leq_L^r w' \iff (\forall v \in A^*\colon wv \in L \implies w'v \in L) \iff \mathrm{C}_L^r(w) \subseteq \mathrm{C}_L^r(w')$

L non-regular $\implies$ exists infinite sequence $(w_i)_{i=1}^\infty$, where $\mathrm{C}_L^\ell(w_i) \neq \mathrm{C}_L^\ell(w_j)$

contains subsequence $(u_i)_{i=1}^\infty$ strictly increasing w.r.t. $<_L^\ell$

i.e. $i < j \implies \mathrm{C}_L^\ell(u_i) \subset \mathrm{C}_L^\ell(u_j)$

$\mathrm{C}_L^\ell(u_i)$ is upward closed w.r.t. $\leq_L^r$:

$v \in \mathrm{C}_L^\ell(u_i) \mathbin{\&} v \leq_L^r v' \implies u_i \in \mathrm{C}_L^r(v) \subseteq \mathrm{C}_L^r(v') \implies v' \in \mathrm{C}_L^\ell(u_i)$

$(\mathrm{C}_L^\ell(u_i))_{i=1}^\infty$ strictly increasing sequence of languages upward closed w.r.t. $\leq_L^r$

contradicts that $\leq_L^r$ is wqo

Nash-Williams Minimal Bad Sequence Argument

How to prove a quasiorder to be wqo?

$(X, \leq)$ ... a quasiordered set

X^ω ... the set of infinite sequences $(x_i)_{i=1}^\infty$, where $x_i \in X$

$(x_i)_{i=1}^\infty \in X^\omega$ bad sequence ... $\forall i, j\colon i < j \implies x_i \not\leq x_j$

$\trianglelefteq$ another quasiordering on X, $\sim$ the corresponding equivalence relation

quasiorder X^ω lexicographically w.r.t. $\trianglelefteq$:

$$(x_i)_{i=1}^\infty \trianglelefteq (y_i)_{i=1}^\infty \iff \begin{array}{l} \text{either } \forall i\colon x_i \sim y_i \\ \text{or } \exists n\colon x_n \triangleleft y_n \;\&\; \forall i < n\colon x_i \sim y_i \end{array}$$

Lemma:

If X contains no infinite descending sequence w.r.t. $\trianglelefteq$ and $\leq$ is not a wqo,

then there exists a bad sequence for $\leq$ minimal w.r.t. $\trianglelefteq$.

Proof: Inductively choose x_i minimal w.r.t. $\trianglelefteq$ such that $x_1, \ldots, x_i$ can be prolonged into a bad sequence.

Proof method for wqo property:

Take a bad sequence and construct a smaller one.

Derivation Relations of Context-Free Rewriting Systems

Example: “scattered subword” relation

$a_1 \ldots a_n \leq u_0 a_1 u_1 \ldots a_n u_n$

context-free rewriting system $R = \{\, \varepsilon \longrightarrow a \mid a \in A \,\}$

$\leq$ is the derivation relation $\Rightarrow_R^*$ of R

$\leq$ is wqo (Higman 1952):

$(w_i)_{i=1}^{\infty}$ bad sequence minimal w.r.t. length quasiorder

infinitely many w_i start with the same letter a: $w_{i_k} = a v_k$ for $k = 1, \ldots, \infty$

$w_1, \ldots, w_{i_1 - 1}, v_1, v_2, \ldots$ is a bad sequence smaller than the original one

$\Longrightarrow$ every language closed under inserting letters is regular

Unitary context-free systems:

$R = \{\, \varepsilon \longrightarrow w \mid w \in I \,\}$, where $I \subseteq A^*$ finite

(to obtain standard context-free system, replace every rule $\varepsilon \longrightarrow w$ with rules $a \longrightarrow aw$ and $a \longrightarrow wa$ for all $a \in A$)

Examples:

$I = A$: “scattered subword” relation

$I = \{\, a\bar{a} \mid a \in A \,\}$: generates Dyck language

Unitary Context-Free Systems

Theorem: (Ehrenfeucht & Haussler & Rozenberg 1983, D'Alessandro & Varricchio 2005)

For every unitary system $R = \{ \varepsilon \to w \mid w \in I \}$, the following conditions are equivalent:

- $\Rightarrow_R^*$ is a wqo on $(\mathrm{alph}(I))^*$
- $\Rightarrow_R^*$ is a wqo on $\{ w \mid \varepsilon \Rightarrow_R^* w \}$
- $\{ w \mid \varepsilon \Rightarrow_R^* w \}$ is regular
- I is unavoidable over $\mathrm{alph}(I)$

$I \subseteq A^+$ unavoidable over A — equivalent definitions:

- every infinite word over A has a factor belonging to I
- there are only finitely many finite words over A without factors from I
- $\exists n\colon A^n \subseteq A^* I A^*$

Examples: $A = \{a, b\}$

$I = \{a^2, b^2\}$ avoidable, $\quad I = \{a^2, b^2, ab\}$ unavoidable

General Context-Free Systems

Theorem: (Bucher & Ehrenfeucht & Haussler 1985)

For every context-free rewriting system R, the following conditions are equivalent:

- $\Rightarrow_R^*$ is a wqo on A^*
- $\{\, awa \mid a \in A,\ w \in A^*,\ a \Rightarrow_R^* awa \,\}$ is unavoidable over A
- $\{\, aw \mid a \in A,\ w \in A^+,\ a \Rightarrow_R^* aw \,\} \cup \{\, wa \mid a \in A,\ w \in A^+,\ a \Rightarrow_R^* wa \,\}$ is unavoidable over A

Are these conditions decidable?

Unavoidability is decidable for regular sets: I unavoidable $\iff$ $A^* \setminus A^* I A^*$ finite

But sets in these conditions are context-free.

Context-Free Derivations Defined by Homomorphisms

$\varphi\colon A^* \longrightarrow (M, \leq)$ homomorphism

$R = \{\, a \rightarrow w \mid a \in A,\ w \in A^+,\ \varphi(a) \leq \varphi(w) \,\}$

notation: $\Rightarrow^*_\varphi \;\equiv\; \Rightarrow^*_R$

$$\begin{aligned} u \Rightarrow^*_\varphi v \iff\ & u = a_1 \ldots a_n, a_i \in A \\ & \&\ v = v_1 \ldots v_n, v_i \in A^+ \\ & \&\ \varphi(a_i) \leq \varphi(v_i) \end{aligned}$$

$\Rightarrow^*_\varphi \;\subseteq\; \leq_\varphi$

$\varphi(A) = M \implies$ sufficient to take finite

$$R = \{\, a \rightarrow bc \mid a, b, c \in A,\ \varphi(a) = \varphi(bc) \,\} \cup \{\, a \rightarrow b \mid \varphi(a) \leq \varphi(b) \,\}$$

$\Rightarrow^*_\varphi$ is a wqo $\implies$ sufficient to take finite

$$R = \{\, a \rightarrow w \mid a \in A,\ w \in \min\{\, u \in A^+ \mid |u| \geq 2,\ \varphi(a) \leq \varphi(u) \,\} \,\}$$

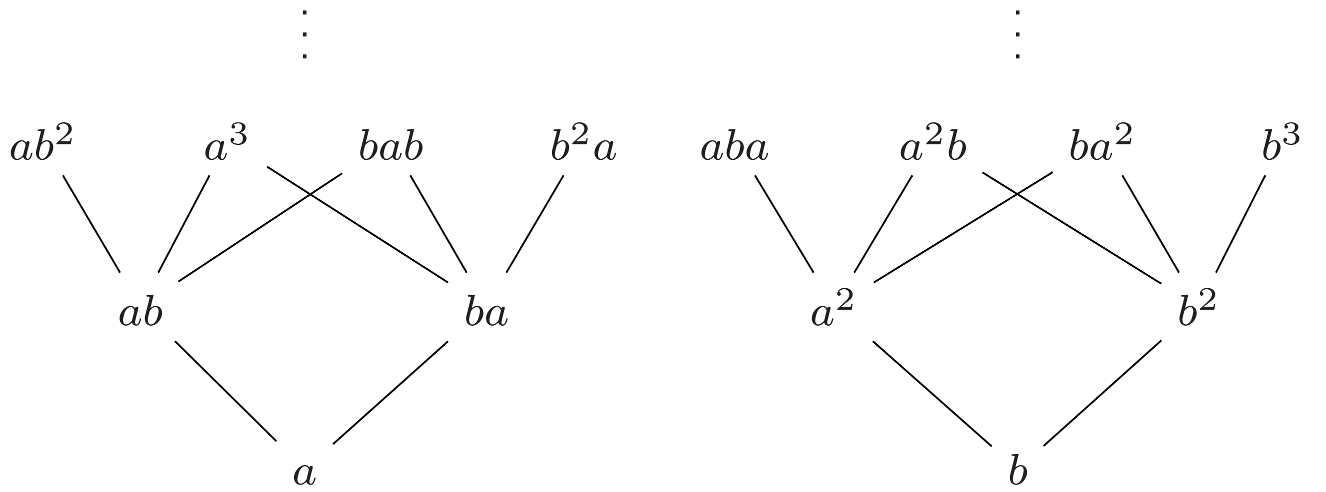
Example:

$M = (\mathbb{Z}, +)/2\mathbb{Z}$ (two-element group)

$\leq$ is $=$

$\varphi\colon \{a, b\}^+ \to M$ $\varphi(a) = 1, \varphi(b) = 0$ (identity element)

$\Rightarrow_\varphi^*$:



$a \Rightarrow_\varphi^* a^3$, $b \Rightarrow_\varphi^* b^2 \mid ba^2b \mid babab$ $\{a^3, b^2, ba^2b, babab\}$ is unavoidable

Therefore $\Rightarrow_\varphi^*$ is a wqo.

Example:

$\varphi(a) \neq \varphi(a^2) = 0$, two incomparable elements

$\Rightarrow_\varphi^*$ is not wqo: a^k cannot be rewritten; a^ω avoids all awa such that $a \Rightarrow_\varphi^* awa$

Theorem: (Bucher & Ehrenfeucht & Haussler 1985)

For every context-free rewriting system R, the following conditions are equivalent:

1) For every regular $L \subseteq A^*$, $\{\, w \mid \exists u \in L \colon u \Rightarrow_R^* w \,\}$ is regular.

2) For every $a \in A$, $\{\, w \mid a \Rightarrow_R^* w \,\}$ is regular.

3) There exists homomorphism $\varphi \colon A^* \to M$ to a finite ordered monoid such that $\Rightarrow_R^* = \Rightarrow_\varphi^*$.

Proof:

3 $\Longrightarrow$ 2: $a \Rightarrow_R^* w \iff \varphi(w) \in \{\, x \in M \mid x \geq \varphi(a) \,\}$

2 $\Longrightarrow$ 1: substitute $\{\, w \mid a \Rightarrow_R^* w \,\}$ for every $a \in A$ in L

1 $\Longrightarrow$ 3: $\varphi_a \colon A^+ \to M_a$ syntactic homomorphism to ordered monoid for $\{\, w \mid a \Rightarrow_R^* w \,\}$

$$\varphi \colon A^+ \to M = \prod_{a \in A} M_a \qquad \varphi(w) = (\varphi_a(w))_{a \in A}$$

$$\varphi(b) \leq \varphi(w) \iff \forall a \in A\, \forall u, v \in A^* \colon a \Rightarrow_R^* ubv \implies a \Rightarrow_R^* uwv$$

$$\iff b \Rightarrow_R^* w$$

Problem: For which homomorphisms $\varphi\colon A^* \to M$ to a finite ordered monoid is $\Rightarrow_\varphi^*$ wqo?

Theorem: (MK 2005)

For every homomorphism $\varphi\colon A^* \to M$ to a finite unordered monoid (i.e. $\leq$ is $=$),

$\Rightarrow_\varphi^*$ is a wqo $\iff$ $\varphi(A^*)$ is a chain of simple semigroups.

Chain of simple semigroups S — equivalent definitions:

- $S = S_1 \cup \cdots \cup S_n$, where S_i are pairwise disjoint, $S_i \cdot S_j \subseteq S_{\max\{i,j\}}$
- For every $x, y \in S$ either $xy \mathrel{\mathcal{J}} x$ or $xy \mathrel{\mathcal{J}} y$.

S_i ... simple semigroups, $\mathcal{J}$-classes of S

Open problem: What about for arbitrary ordered monoids?

Computability of Closure

Is the upward closure of languages w.r.t. wqo $\Rightarrow_R^*$ computable?

closure computable $\Longrightarrow$ emptiness problem decidable

For scattered subword ordering:

emptiness problem decidable & effective intersection with regular languages $\Longrightarrow$ computable

(van Leeuwen 1978)

(holds, in particular, for context-free languages)

In general: unknown even for closure of one letter.

Are there other monotone quasiorders than wqos that recognize only regular languages?

Theorem: (Bucher & Ehrenfeucht & Haussler 1985)

For every decidable monotone quasiorder $\leq$ on A^* satisfying $u \leq v \implies |u| \leq |v|$,

the following conditions are equivalent:

- All upward closed languages are regular.
- All upward closed languages are recursive.
- $\leq$ is a wqo.

(applies to all derivation relations of non-erasing context-free systems)

Wqos Defined by Other Rewriting Systems

Shuffle analogue:

rewriting rules $w \longrightarrow w \sqcup\!\sqcup u$, for $u \in I$,

i.e. $w_0 \ldots w_n \longrightarrow w_0 u_1 w_1 \ldots u_n w_n$, for $u_1 \ldots u_n \in I$

Theorem: (Haussler 1985)

$\longrightarrow^*$ is a wqo $\iff$ I is subsequence unavoidable

regularity conditions for permutable and periodic languages based on wqos defined by rewriting

(de Luca & Varricchio)

Closure Properties of Well Quasiorders

Closure properties corresponding to operations on finite monoids:

substructures: $\leq$ monotone wqo on A^* and $f\colon B^* \to A^*$ homomorphism

$\sqsubseteq$ quasiorder induced on B^*: $\quad u \sqsubseteq v \iff f(u) \leq f(v)$

Then $\sqsubseteq$ is a monotone wqo on B^*.

quotients: $\leq$ wqo on A^* and $\sqsubseteq\ \supseteq\ \leq$ quasiorder on A^* $\implies$ $\sqsubseteq$ wqo on A^*

products: $\leq$ and $\sqsubseteq$ monotone wqos on A^* $\implies$ $\leq \cap \sqsubseteq$ monotone wqo on A^*

$\leq$ wqo on X and $\sqsubseteq$ quasiorder on Y

$f\colon X \twoheadrightarrow Y$ onto mapping satisfying $x \leq y \implies f(x) \sqsubseteq f(y)$

Then $\sqsubseteq$ is a wqo on Y.

$\leq$ wqo on X and $\sqsubseteq$ wqo on Y $\implies$ componentwise quasiordering on $X \times Y$ is a wqo

$\leq$ wqo on X

quasiordering of X^*:

$a_1 \ldots a_m \sqsubseteq b_1 \ldots b_n \iff \exists 1 \leq i_1 < \cdots < i_m \leq n$ such that $a_j \leq b_{i_j}$

(infinite rewriting system: $\varepsilon \longrightarrow a$, $a \longrightarrow b$, for $a \leq b$, $a, b \in X$)

Higman 1952: $\sqsubseteq$ is a wqo on X^*

$\mathcal{F}$ ... the set of subsets of X upward closed w.r.t. $\leq$

$\supseteq$ is not in general wqo on $\mathcal{F}$ $\quad\rightsquigarrow\quad$ better quasiorders

$\subseteq$ is a wqo on the set of finitely generated downward closed subsets of X

(isomorphic to a subset of $(\mathcal{F}, \supseteq)$)

Language Equations

Language equation $=$ equation over some algebra of languages

- constants: languages over A
- operations: concatenation, Boolean operations, ...
- finite set of variables $\mathcal{V} = \{X_1, \ldots, X_n\}$
- solution: mapping $\alpha\colon \mathcal{V} \longrightarrow \wp(A^*)$

- long ago: explicit systems of polynomial equations — context-free languages
- today: renewed interest, surprising recent results

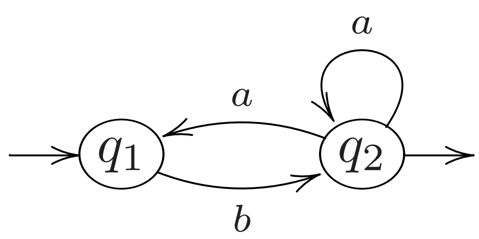
What are we interested in?

- expressive power, properties of solutions
- decidability of existence and uniqueness of solutions
- algorithms for finding (minimal and maximal) solutions

Explicit Systems of Equations
Corresponding to Basic Models of Computation

Description of Regular Languages

Example:



$$X_1 = \{\varepsilon\} \cup X_2 \cdot a \qquad X_2 = X_1 \cdot b \cup X_2 \cdot a$$

Regular languages $=$ components of smallest (largest, unique) solutions of explicit systems

$$X_i = K_i \cup \bigcup_{j=1}^{n} X_j \cdot L_{j,i} \qquad i = 1, \ldots, n$$

of left-linear equations with finite constants K_i and $L_{j,i}$

Matrix notation: union instead of summation

row vectors $X = (X_i)$ and $S = (K_i)$, matrix $R = (L_{j,i})$

$X = S + XR$

Solving Explicit Systems of Left-Linear Equations

Theorem: (one direction of Kleene theorem)

Components of the smallest solution of the system $X = S + XR$ can be constructed from entries of R and S using $\cup$, $\cdot$ and $*$.

The system as an automaton:

- language $R_{j,i}$ labels the transition from state j to state i
- a word from S_i is read when entering the automaton at state i

Proof:

The smallest solution of $X = S + XR$ is SR^*, where $R^* = E + R + R^2 + \cdots$.

Inductive formula for computing R^* as a block matrix:

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}^* = \begin{pmatrix} (A + BD^*C)^* & A^*B(D + CA^*B)^* \\ D^*C(A + BD^*C)^* & (D + CA^*B)^* \end{pmatrix}$$

Description of Context-Free Languages

Example: Dyck language of correct bracketings over $A = \{(,)\}$:

context-free grammar: $X_1 \longrightarrow \varepsilon \mid X_2 X_1 \qquad X_2 \longrightarrow (X_1)$

system of language equations: $X_1 = \{\varepsilon\} \cup X_2 \cdot X_1 \qquad X_2 = \{(\} \cdot X_1 \cdot \{)\}$

Ginsburg & Rice 1962:

context-free languages $=$ components of smallest (largest, unique) solutions of explicit systems

$$X_i = P_i \qquad i = 1, \ldots, n$$

of polynomial equations with finite $P_i \subseteq (A \cup \mathcal{V})^*$

elegant matrix notation for some normal forms

Quadratic Greibach Normal Form

Every context-free grammar generating only non-empty words can be algorithmically modified so that right-hand sides of rules belong to $A\mathcal{V}^2 \cup A\mathcal{V} \cup A$.

Construction: (Rosenkrantz 1967)

Start with Chomsky normal form, i.e. right hand sides in $\mathcal{V}^2 \cup A$.

Matrix notation: $X = S + XR$,

where S is a vector over $\wp(A)$ and R is a matrix over $\wp(\mathcal{V})$.

Equivalently: $X = SR^*$

Replace R^* with matrix of new variables: $X = SY \quad Y = E + RY$

In R replace every occurrence of variable X_k with the set $(SY)_k \subseteq A\mathcal{V}$.

Remove ε-rules.

Generalizations of Context-Free Languages

Conjunctive languages (Okhotin 2001):

- analogy of alternating finite automata and Turing machines for context-free grammars
- additionally intersection allowed in equations
- we can specify that a word satisfies certain syntactic conditions simultaneously
- for unary alphabet, smallest solutions are in $\mathrm{EXPTIME}$ and can be $\mathrm{EXPTIME}$-complete

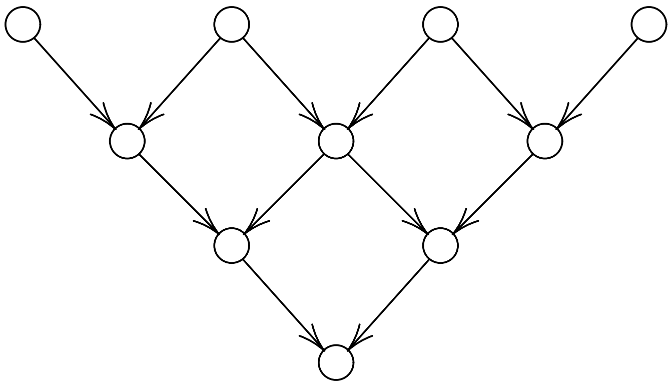
  (Jeż & Okhotin 2008)

  (context-free unary languages are regular = ultimately periodic)

  encoding in positional notation, e.g. binary notation of $\{\, a^{2^n} \mid n \in \mathbb{N} \,\}$ is regular 10^*

Linear conjunctive languages:

exactly languages accepted by one-way real-time cellular automata (Okhotin 2004)



$\longleftarrow$ input word

$\longleftarrow$ output value

Examples:

$\{\, wcw \mid w \in \{a,b\}^* \,\}$, $\{\, a^n b^n c^n \mid n \in \mathbb{N} \,\}$, all computations of a Turing machine

All Boolean Operations

Okhotin 2003:

components of unique (smallest, largest) solutions $=$

$=$ recursive (recursively enumerable, co-recursively enumerable) languages

Boolean grammars (Okhotin 2004):

- semantics defined only for some systems
- generalization of conjunctive languages
- parsing using standard techniques
- $\subseteq \mathrm{DTIME}(n^3) \cap \mathrm{DSPACE}(n)$
- used to give a formal specification of a simple programming language

Okhotin 2007:

equations with concatenation and any clone of Boolean operations

(concatenation and symmetric difference: universal)

Arithmetical hierarchy:

- components of largest and smallest solutions w.r.t. lexicographical ordering
- levels characterized by the number of variables in equations (Okhotin 2005)

Implicit Equations

Equations over Words

- constants are letters, for variables only words are substituted
- for instance, solutions of equation $xba = abx$ are exactly $x = a(ba)^n$, where $n \in \mathbb{N}_0$
- term unification modulo associativity
- PSPACE algorithm deciding satisfiability, $\mathrm{EXPTIME}$ algorithm finding all solutions (Makanin 1977, Plandowski 2006)
- Conjecture: Satisfiability problem is NP-complete.
- satisfiability-equivalent to language equations with only letters as constants and concatenation: $\mathrm{shortlex}$-minimal words of an arbitrary language solution form a word solution

Satisfiability of language equations by arbitrary languages is undecidable for

- equations with finite constants, union and concatenation
- systems of equations with regular constants and concatenation (MK 2007)

Conjugacy of Languages

$KM = ML$ ... languages K and L are conjugated via a language M

Words u and v are conjugated $\iff$ v can be obtained from u by cyclic shift.

MK 2007:

Conjugacy of regular languages via any language containing ε is not decidable.

Satisfiability of systems $KX = XL, A^*X = A^*$ is not decidable for regular languages K, L.

Cassaigne & Karhumäki & Salmela 2007:

Conjugacy of finite bifix codes via any non-empty language is decidable.

Open questions:

- removal of the requirement on ε
- conjugacy of finite languages (satisfiability of equations with finite constants)
- conjugacy via regular or finite languages (satisfiability by regular or finite languages)

Identity checking problem for regular expressions:

f, g regular expressions with variables $X_1, \ldots, X_n$ (union, concatenation, Kleene star, letters)

Does $f(L_1, \ldots, L_n) = g(L_1, \ldots, L_n)$ hold for arbitrary (regular) languages $L_1, \ldots, L_n$?

- trivially decidable (treat variables as letters and compare regular languages)
- decidable also with the shuffle operation (Meyer & Rabinovich 2002)
- open problems for expressions with intersection

Rational systems: (defined by a finite transducer)

Every rational system of word equations is algorithmically equivalent to some of its finite subsystems $\Longrightarrow$ satisfiability of rational systems of word equations is decidable.

(Culik II & Karhumäki 1983, Albert & Lawrence 1985, Guba 1986)

Do given finite languages form a solution of the system $\{\, X^n Z = Y^n Z \mid n \in \mathbb{N} \,\}$?

undecidable (Lisovik 1997, Karhumäki & Lisovik 2003, MK 2007)

Language Inequalities Defining Basic Automata

Minimal automaton of a language L:

state reached by $w \in A^* =$ largest solution of the inequality $w \cdot X_w \subseteq L$

$X_w \xrightarrow{a} X_{wa}$

initial state X_ε

final states X_w, where $w \in L$

Universal automaton of a language L

$=$ smallest non-deterministic automaton admitting morphism from every automaton accepting L

state $=$ maximal solution of the inequality $X \cdot Y \subseteq L$

$(X, Y) \xrightarrow{a} (X', Y') \iff aY' \subseteq Y \iff Xa \subseteq X'$

(X, Y) initial state $\iff \varepsilon \in X$

(X, Y) final state $\iff \varepsilon \in Y$

General Results About Language Inequalities

Jeż & Okhotin 2008: Even for unary alphabet, finite constants, concatenation and union:

components of unique (smallest, largest) solutions $=$

$=$ recursive (recursively enumerable, co-recursively enumerable) languages

Example: Minimal solutions of $X \cup Y = L$ are precisely disjoint decompositions of L.

In the presence of union and concatenation, interesting properties are demonstrated by maximal solutions.

Systems of Inequalities with Constant Right-Hand Sides

$P_i \subseteq L_i$ $\quad L_i \subseteq A^*$ regular, $P_i \subseteq (A \cup \mathcal{V})^*$ arbitrary

maximal solutions: (Conway 1971)

- finitely many, all of them regular
- for context-free expressions P_i: algorithmically regular
- every solution is contained in a maximal one
- all components are recognized by the syntactic homomorphism of the languages L_i

Analogy: preservation of regularity by arbitrary inverse substitutions:

Largest solution of the inequality $\varphi(X) \subseteq A^* \setminus L$ is $X = A^* \setminus (\varphi^{-1}(L))$.

Systems of equations with constant right-hand sides:

$P_i = L_i$ $\quad L_i \subseteq A^*$ regular, $P_i \subseteq (A \cup \mathcal{V})^*$ regular expression

- satisfiability by arbitrary (finite) languages is $\mathrm{EXPSPACE}$-complete (Bala 2006)
- Is satisfiability decidable if P_i can contain intersection?

General Left-Linear Inequalities

$K_0 \cup X_1 K_1 \cup \cdots \cup X_n K_n \subseteq L_0 \cup X_1 L_1 \cup \cdots \cup X_n L_n$

K_j, L_j regular $\implies$ basic properties of the inequality can be expressed using formulae of monadic second-order theory of infinite $|A|$-ary tree

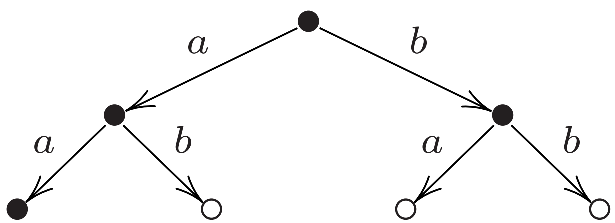
Example: $b \cup Xa \subseteq X \cup Xba$

$$X \text{ is a solution } \iff X(b) \wedge \big(\forall x\colon X(x) \implies (X(xa) \vee \exists y\colon X(y) \wedge x = yb)\big)$$

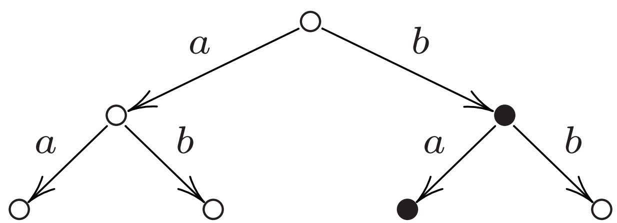
$$X \text{ minimal } \iff \forall Y: (Y \text{ is a solution} \wedge \forall x\colon Y(x) \implies X(x)) \implies$$
$$\implies (\forall x\colon X(x) \implies Y(x))$$

minimal solutions: $\bullet$ = "X holds" $\circ$ = "X does not hold"

$a^* \cup b$:



ba^* :



Rabin 1969 $\implies$ algorithmically solvable using tree automata

very special case of set constraints (letters as unary functions)

$\mathrm{EXPTIME}$-complete (even when complementation is allowed) (1994–2006)

Yet More General Left-Linear Inequalities

$$K_0 \cup X_1 K_1 \cup \cdots \cup X_n K_n \subseteq L_0 \cup X_1 L_1 \cup \cdots \cup X_n L_n$$

K_j arbitrary, L_j regular

largest solution: (MK 2005)

- regular
- for context-free K_j: algorithmically regular
- direct construction of the automaton accepting the solution

Concatenations on the Right

Previous cases:

$\ldots \subseteq L$	constants on the right fix the context
$XK \cup \ldots \subseteq XL \cup \ldots$	local modifications on one side

Next task:

$\ldots \subseteq XLY$	general concatenations on the right

We need to classify words according to their decompositions with respect to constant languages.

A Quasiorder for Dealing with Concatenations on the Right

Applying well-quasiorders to inequalities:

Construct a wqo on A^* such that every solution is contained in an upward closed solution.

Systems of inequalities $P_i \subseteq Q_i$

$P_i \subseteq (A \cup \mathcal{V})^*$ arbitrary

Q_i ... regular expressions over variables and languages recognizable by

a homomorphism $\varphi\colon A^* \to (M, \leq)$

Recalling definition:

$$u \Rightarrow_{\varphi}^{*} v \iff u = a_1 \ldots a_n,\, a_i \in A$$

$$\& \; v = v_1 \ldots v_n,\, v_i \in A^+$$

$$\& \; \varphi(a_i) \leq \varphi(v_i)$$

Theorem: All maximal solutions are recognizable by the quasiorder $\Rightarrow_\varphi^*$. (MK 2005)

Proof: α arbitrary solution

define $\beta(X) = \{\, u \in A^* \mid \exists v \in \alpha(X) \colon v \Rightarrow_\varphi^* u \,\}$, for every $X \in \mathcal{V}$

$\beta(X) \supseteq \alpha(X)$

β is a solution:

$u \in \beta(P_i) \implies \exists v \in \alpha(P_i) \colon v \Rightarrow_\varphi^* u$ (because $\Rightarrow_\varphi^*$ is monotone)

we prove by induction on structure of Q_i:

$$v \in \alpha(Q_i) \;\&\; v \Rightarrow_\varphi^* u \implies u \in \beta(Q_i)$$

e subexpression of Q_i, $v \in \alpha(e)$, $v \Rightarrow_\varphi^* u$

- e variable: $u \in \beta(e)$ by definition of β
- e constant: $u \in \alpha(e) \subseteq \beta(e)$ because $\varphi(u) \geq \varphi(v)$
- e union or intersection: $u \in \beta(e)$ by induction hypothesis
- $e = e_1 \cdot e_2$: $v = v_1 \cdot v_2$, $v_1 \in \alpha(e_1)$, $v_2 \in \alpha(e_2)$

  definition of $\Rightarrow_\varphi^* \implies u = u_1 \cdot u_2$, $v_1 \Rightarrow_\varphi^* u_1$, $v_2 \Rightarrow_\varphi^* u_2$

  induction hypothesis $\implies u_1 \in \beta(e_1)$, $u_2 \in \beta(e_2) \implies u \in \beta(e)$

Every component of β is a finite union of languages of the form

$\langle a_1 \ldots a_n \rangle_{\Rightarrow_\varphi^*} = \varphi^{-1}(\langle \varphi(a_1) \rangle_{\leq}) \cdots \varphi^{-1}(\langle \varphi(a_n) \rangle_{\leq})$, where $a_1, \ldots, a_n \in A$.

Inequalities with Restrictions on Constants

Systems of inequalities $P_i \subseteq Q_i$

$P_i \subseteq (A \cup \mathcal{V})^*$ arbitrary

Q_i ... regular expressions over variables and languages recognizable by finite simple semigroups

(or all together by a finite chain of finite simple semigroups)

(can contain infinite unions and intersections, provided only finitely many constants are used)

MK 2005:

- All maximal solutions are regular.
- The class of polynomials of group languages is closed under taking maximal solutions of such systems.
- If L is recognizable by a finite chain of finite simple semigroups, then every union of powers of L is regular. ($X \subseteq \bigcup_{n \in N} L^n$, for arbitrary $N \subseteq \mathbb{N}$)

Semi-commutation Inequalities

$XK \subseteq LX$ $\quad$ K arbitrary, L regular

largest solution:

- always regular (MK 2005)
- for context-free K: algorithmically recursive
- if K and L finite and all words in K longer than all in L: algorithmically regular (Ly 2007)

Game: position: $w \in A^*$

attacker: chooses $u \in K$

plays $w \longrightarrow wu$

defender: chooses $v \in L$

$wu = v\tilde{w}$

plays $wu \longrightarrow \tilde{w}$

largest solution $=$ all winning positions of the defender

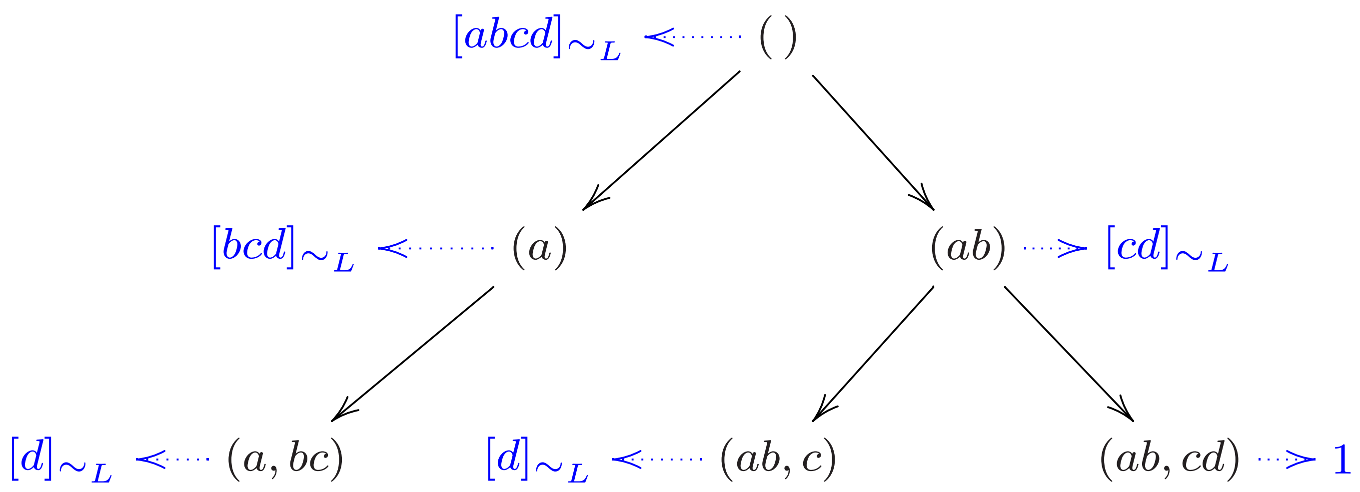
Encoding Defender's Strategies for Initial Word w

Labelled tree:

defender moves along the edges $=$ removes prefixes of w

label $= \sim_L$-class of the current remainder of w

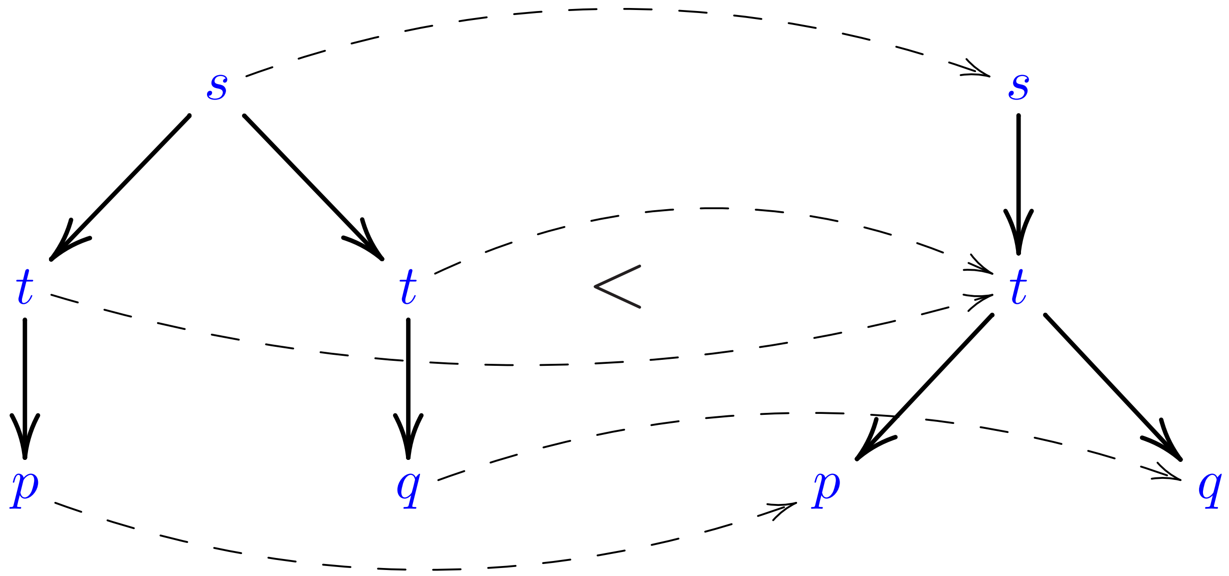
Example: $w = abcd$, $L = \{a, ab, abcde, bc, c, cd, da\}$



Well-quasiordering Trees

$w \leq v \ldots$ winning strategies of the defender for w can be used also for v

Example:



Largest solution is upward closed with respect to $\leq$.

Kruskal 1960: $\leq$ is wqo.

Simple Equations Possessing Universal Power

MK 2005:

Every co-recursively enumerable language can be described as the largest solution of any of the following systems with regular constants K, L, M and N.

$$XK \subseteq LX \qquad XK \subseteq LX \qquad XK \subseteq LX$$
$$X \subseteq M \qquad XM \subseteq NX \qquad MX \subseteq XN$$

Special case: $XL = LX$

- formulated by Conway 1971
- positive results:

  at most three-element languages, regular codes (Karhumäki & Latteux & Petre 2005)

MK 2007:

There exists a finite language L such that the largest solution $\mathcal{C}(L)$ of $XL = LX$ is not recursively enumerable.

Example: L regular, but $\mathcal{C}(L)$ non-regular

$$A = \{a, b, c, e, \hat{e}, f, \hat{f}, g, \hat{g}\}$$

$$\begin{aligned} L = {} & \{c, ef, ga, e, fg, \hat{f}\hat{e}, a\hat{g}, \hat{e}, \hat{g}\hat{f}, fgba\hat{g}\} \cup cM \cup Mc \cup \\ & \cup A^*bA^*bA^* \cup (A \setminus \{c\})^*b(A \setminus \{c\})^* \setminus N \end{aligned}$$

$$M = efga^+ba^* \cup ga^*ba^*\hat{g}\hat{f} \cup a^*ba^*\hat{g}\hat{f}\hat{e} \cup fga^*ba^*\hat{g}$$

$$N = \{efg, fg, g, \varepsilon\} \cdot a^*ba^* \cdot \{\varepsilon, \hat{g}, \hat{g}\hat{f}, \hat{g}\hat{f}\hat{e}\}$$

encodes simultaneous decrementation of two counters and zero-test

Configuration: $[[[e]f]g]a^m ba^n[\hat{g}[\hat{f}[\hat{e}]]]$

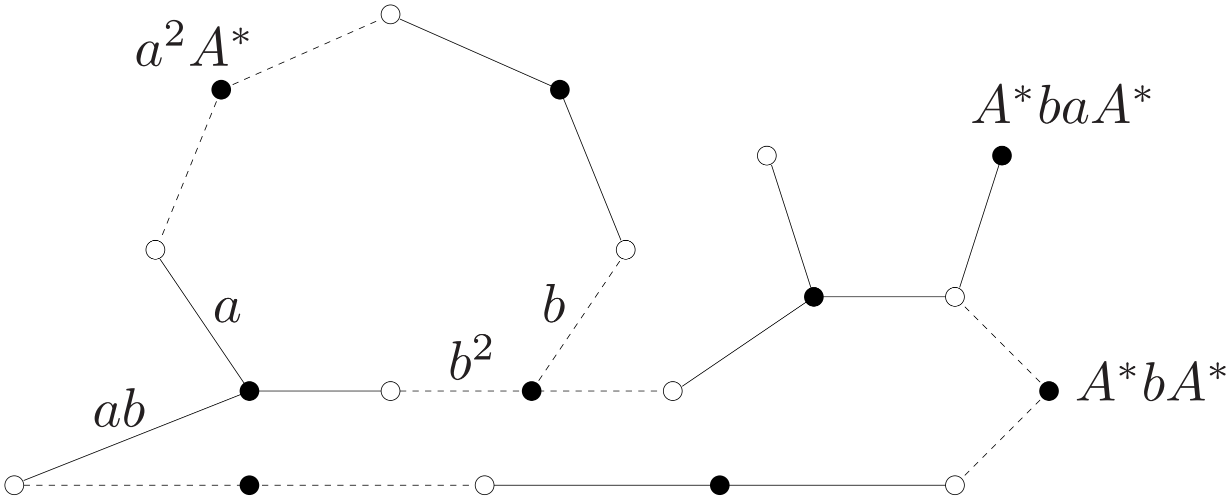
Simultaneous Decrementation of Both Counters

Attacker forces defender to remove one a on each side:

$$
\begin{tikzcd}
efga^mba^n \arrow[d] & \\
\underline{ef}ga^mba^n \cdot \hat{g}\hat{f} \arrow[r] \arrow[d] & fga^mba^n\hat{g}\hat{f} \arrow[d, Rightarrow] \\
ga^mba^n\hat{g}\hat{f} \arrow[d] & fga^mba^n\hat{g}\hat{f} \cdot c \cdot c \notin L^2 \cdot A^* \\
\underline{ga}a^{m-1}ba^n\hat{g}\hat{f} \cdot \hat{e} \arrow[d] & \\
a^{m-1}ba^n\hat{g}\hat{f}\hat{e} \arrow[d] & \\
\vdots \arrow[d] & \\
efga^{m-1}ba^{n-1} &
\end{tikzcd}
$$

Games That Can Be Encoded (Jeandel & Ollinger)

Example:



● = attacker should play —— modification on the left

○ = defender should play – – – modification on the right

position of the game: a vertex of the graph and a word

labels of attacker's vertices: allowed words

labels of edges: words to be added by attacker or removed by defender

- when attacker modifies on one side, defender has to modify on the other
- bipartite graph for each type of edges
- at most one common vertex for any two connected components of different types
- only one type of edges leading from each of attacker's vertices
- non-empty labels of edges only around one attacker's vertex for each type of edges

Some Open Problems

- satisfiability of equations with concatenation (and union) over finite or regular languages
- satisfiability of equations with concatenation and finite constants
- Conjecture: (Ratoandromanana 1989)

  Among codes, equation $XY = YX$ has only solutions of the form $X = L^m$, $Y = L^n$.

  Equivalently: Every code has a primitive root.
- regularity of solutions of other simple systems of inequalities, for example:

  $KXL \subseteq MX$

  $KX \subseteq LX,\ XM \subseteq XN$
- existence of algorithms for finding regular solutions
- methods for proving properties of conjunctive and Boolean grammars
- existence of non-trivial shuffle decomposition $X \sqcup\!\sqcup Y = L$ of a regular language L
- existence of non-trivial unambiguous decompositions of regular languages