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  \( (x \cdot 1 = 1 \cdot x = x) \)

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

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 $\varphi: S \to T$  \( \varphi(xy) = \varphi(x)\varphi(y) \)

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

Congruence $\rho$ on $S$:  equivalence $\rho \subseteq S \times S$ satisfying $x \rho x' \& y \rho y' \implies xy \rho x'y'$

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

\[\ker(\varphi) = \{(x, y) \in S \times S | \varphi(x) = \varphi(y)\}\]

Congruences = kernels of homomorphisms.
Words

A . . . finite alphabet

$A^* . . . \text{monoid of all finite words over } A \text{ with concatenation as operation}$

semigroup $A^+ \subseteq A^* . . . \text{empty word } \varepsilon \text{ excluded}$

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

Language $L \subseteq A^*$ recognized by a homomorphism $\varphi : A^* \rightarrow M$ to a finite monoid, if

$L = \varphi^{-1}(F)$ for some $F \subseteq M$.

Language $L \subseteq A^+$ recognized by a homomorphism $\varphi : A^+ \rightarrow S$ 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 $M$

$\delta_a(x) = x \cdot \varphi(a)$

$\delta^r_a(x) = \varphi(a) \cdot x$

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. \( \leq \) \( \ldots \) if \( x \leq y \) and \( x \in F \), then \( y \in F \)

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

Homomorphism \( \varphi : A^* \rightarrow (M, \leq) \) 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: \( w \sim \leq w' \sim \iff w \leq w' \)

projection homomorphism \( \nu : A^* \rightarrow A^*/\sim \)
Syntactic Homomorphism

$L \ldots$ a language over $A$

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

Syntactic monotone quasiorder of $L$ on $A^*$:

for $w, w' \in A^*$, $w \leq_L w' \iff C_L(w) \subseteq C_L(w')$

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 $\leq_L$)

$\varphi_L: A^* \rightarrow A^*/\sim_L$ syntactic homomorphism

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

$M_L$ finite $\iff L$ regular

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

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

$\varphi_L(w)$ is idempotent if and only if $\forall u, v \in A^*, n \in \mathbb{N}: uwv \in L \iff uw^nv \in L$
Products of elements of semigroups versus recognizing languages:

evaluation homomorphism:

\[ \text{eval}: M^* \to M \quad \text{eval}(x_1 \ldots x_n) = x_1 \cdots x_n \]

\( \varphi: A^* \to M \) 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 $Q \rightarrow Q$ with composition as operation

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

$\delta_a : Q \rightarrow Q$ action of $a \in A$

determines homomorphism $\varphi : A^* \rightarrow \mathcal{T}(Q)$, 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 $\delta_a$ for $a \in A$

• recognizes all languages accepted by $\mathcal{A}$

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

syntactic semigroup $= \text{transition semigroup of the minimal automaton}$

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

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

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

\[
\iff \text{contains only permutations}
\iff \text{minimal automaton is dually deterministic}
\iff \text{minimal automaton does not contain the pattern}
\]

(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
\[
(p, q) \in \sigma \circ \delta \iff \exists r \in Q: (p, r) \in \sigma \land (r, q) \in \delta
\]

\( A = (Q, A, \delta) \) non-deterministic automaton without initial and final states
\[
\delta_a = \{ (p, q) \in Q \times Q \mid (p, a, q) \in \delta \} \text{ for all } a \in A
\]
determines homomorphism \( \varphi: A^* \to \mathcal{R}(Q) \), where \( \varphi(a) = \delta_a \)
subsemigroup of \( \mathcal{R}(Q) \) generated by mappings \( \delta_a \) recognizes all languages accepted by \( A \)
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 $(\mathbb{N}, +)$

\[
\begin{array}{c}
x \\
\rightarrow x^2 \\
\rightarrow x^3 \\
\rightarrow \cdots
\end{array}
\]

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

\[
\begin{array}{c}
x \\
\rightarrow x^2 \\
\rightarrow \cdots \\
\rightarrow x^i = x^{i+p} \\
\rightarrow \cdots
\end{array}
\]

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

\[
x^\omega = \lim_{n \to \infty} x^n = x^{|S|!} \text{ unique idempotent in } \langle x \rangle, \text{ identity element of the subgroup}
\]

periodic semigroup $= \text{ all monogenic subsemigroups are finite}$

finite $\implies$ periodic

idempotents are exactly elements $x^\omega$ 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:

$y \leq_L x \iff S^1y \subseteq S^1x \iff y \in S^1x$
$y \leq_R x \iff yS^1 \subseteq xS^1 \iff y \in xS^1$
$y \leq_J x \iff S^1yS^1 \subseteq S^1xS^1 \iff y \in S^1xS^1$

$y \leq_L x \implies yz \leq_L xz$
$y \leq_R x \implies zy \leq_R zx$

$S^1xS^1 = \{ y \in S \mid y \leq_J x \}$

Green’s equivalence relations:

$x \mathcal{L} y \iff y \leq_L x \& y \leq_L x \iff S^1x = S^1y$
$x \mathcal{R} y \iff y \leq_R x \& y \leq_R x \iff xS^1 = yS^1$
$x \mathcal{J} y \iff y \leq_J x \& y \leq_J x \iff S^1xS^1 = S^1yS^1$
quasiorders induce partial ordering of the corresponding classes
multiplying element from any side \( \leadsto \) descending in the ordering of \( J \)-classes
multiplying element from the left (right) \( \leadsto \) descending in the ordering of \( L(R) \)-classes

In a monoid, invertible elements form the top \( J \)-class, which is a group.
Zero always forms a one-element bottom \( J \)-class.
Every semigroup has at most one minimal \( J \)-class.
Lemma: $\mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$

Proof:
\[ x \mathcal{R} y \mathcal{L} z \implies y = xs, x = yt, z = uy, y = vz \]
\[ w = uyt = ux = zt \implies x = yt = vzt = vuyt = vw, z = uy = uxs = uyts = ws \]

\[
\begin{array}{cc}
  x & y \\
  u \downarrow & \uparrow v \\
  w & z \\
\end{array}
\]

\[
\begin{array}{cc}
  & u \downarrow \\
  w & \leftarrow t \\
  & \uparrow v \\
\end{array}
\]

Remaining Green's equivalences:
\[ H = \mathcal{L} \cap \mathcal{R}, \quad D = \mathcal{L} \circ \mathcal{R} \]
\[ x \mathcal{D} y \iff x\mathcal{R} \cap y\mathcal{L} \neq \emptyset \iff x\mathcal{L} \cap y\mathcal{R} \neq \emptyset \]
\[ H \subseteq \mathcal{L}(\mathcal{R}) \subseteq \mathcal{D} \subseteq \mathcal{J} \]

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

- $s$ and $t$ 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
- $\sim$ bijections between all $\mathcal{H}$-classes in a $\mathcal{D}$-class
Examples:

\(A^*:\)

\[u \leq_L v \iff v \text{ is a suffix of } u\]

\[u \leq_R v \iff v \text{ is a prefix of } u\]

\[u \leq_J v \iff v \text{ is a factor of } u\]

\[u \mathcal{J} v \iff u \mathcal{D} v \iff u \mathcal{L} v \iff u \mathcal{R} v \iff u \mathcal{H} v \iff u = v\]

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

\(\mathcal{T}(Q):\)

\[\rho \leq_L \sigma \iff \text{Im}(\rho) \subseteq \text{Im}(\sigma)\]

\[\rho \leq_R \sigma \iff \ker(\rho) \supseteq \ker(\sigma)\]

\[\rho \leq_J \sigma \iff |\text{Im}(\rho)| \leq |\text{Im}(\sigma)|\]

\[\rho \mathcal{D} \sigma \iff \rho \mathcal{J} \sigma \iff |\text{Im}(\rho)| = |\text{Im}(\sigma)|\]
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, $D = J$.

Proof:

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

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

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

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

$y \mathcal{R} yq: \quad y = y(qt)^\omega = yq \cdot t(qt)^{\omega - 1}$
Example: subsemigroup of $\mathcal{PT}(2)$

\[ x^2 = y^2 = 0 \quad xyx = x \quad yxy = y \]
Similar example: subsemigroup of $\mathcal{PT}(2)$

\[
\begin{array}{c|cc}
\cdot y & \cdot x \\
\hline
y \cdot & x & xy \\
\hline
x \cdot & yx & y \\
\hline
0 \\
\end{array}
\]

\[
x: \bullet \rightarrow \bullet \quad y: \bullet \leftarrow \bullet
\]

\[
xy: \bullet \quad \bullet \quad yx: \bullet \rightarrow \bullet
\]

\[
x^2 = 0 \quad xyx = x \quad yxy = y
\]
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 $x \leq_L y$ and $x \unlhd y$. Then $x \equiv_L y$.

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

Reformulations: In any finite semigroup:

- $x \leq_J xs \implies x \equiv_R xs$
- $x <_L y \implies x <_J y$

Corollary: In any finite semigroup, $sxHx \implies sxHxtHx$.

Proof: $sx \leq_L x, x \leq_R sx, sx \unlhd x$
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 “\( \Leftarrow \)”:

\[ x = se, \quad y = et \quad \Rightarrow \quad xy = seet = xt \]

\[
\begin{array}{c|c|c}
  x & xy \\
  \hline
  e & y \\
  \hline
\end{array}
\]

\[ s \cdot \uparrow \]

\[ t \rightarrow \]
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 “$\Longrightarrow$”:

\[
xy \leq \mathcal{R} x \& xy \mathcal{J} x \Longrightarrow xy \mathcal{R} x
\]

\[
xy \leq \mathcal{L} y \& xy \mathcal{J} y \Longrightarrow xy \mathcal{L} y
\]

\[
x = xys \& y = txy \Longrightarrow (tx)^2 = ttxys = txys = tx
\]
Recalling example: subsemigroup of $\mathcal{PT}(2)$

<table>
<thead>
<tr>
<th></th>
<th>$x$</th>
<th>$xy$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$y$</td>
<td>$xy$</td>
<td>$y$</td>
</tr>
<tr>
<td>$x$</td>
<td>$yx$</td>
<td>$y$</td>
</tr>
<tr>
<td></td>
<td>$0$</td>
<td></td>
</tr>
</tbody>
</table>

$x^2 = 0$  
$xyx = x$  
$yxy = y$
Regular Elements

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

$x \in S$ is regular $= \text{has an inverse}$

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

$y$ inverse of $x$ $\Rightarrow xy$ and $yx$ are idempotents in the same $D$-class

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

$A^+$: no regular elements

$T(Q)$:

$\rho$ is idempotent $\iff \forall q \in \text{Im}(\rho) : \rho(q) = q$

$\rho$ belongs to a subgroup $\iff \rho|_{\text{Im}(\rho)} : \text{Im}(\rho) \to \text{Im}(\rho)$ is a bijection

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

every element is regular
Regular $\mathcal{D}$-Classes

Example:

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

<table>
<thead>
<tr>
<th></th>
<th>$x$</th>
<th>$y$</th>
<th>$z$</th>
<th>$u$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td></td>
<td></td>
<td>$f$</td>
<td></td>
</tr>
<tr>
<td>$g$</td>
<td></td>
<td></td>
<td></td>
<td>$\Box$</td>
</tr>
</tbody>
</table>

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), $y$, $z$, $u$. 

\[x\] 
\[e\] 
\[f\] 
\[g\]
Regular $D$-Classes

Regular $D$-class — equivalent definitions:

1) Contains an idempotent.
2) Contains a regular element.
3) Every element is regular.
4) Every $L$-class and every $R$-class contains an idempotent.

2 $\implies$ 3:

\[
xyx = x, \quad yxy = y, \quad z = xs, \quad x = zt
\]

\[
z \cdot t x \rightarrow y xy
\]

\[
z(ty)z = xyxs = xs = z, \quad (ty)z(ty) = tyxy = ty
\]

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

Every idempotent is a left identity for its $R$-class and a right identity for its $L$-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 $y = fs$

\[
\begin{align*}
x(fs)x &= xsx = ex = x \\
(fs)x(fs) &= fsex = fse = fs
\end{align*}
\]

\[
\begin{array}{c|c}
  x & e \\
  \hline
  f & y \\
\end{array}
\]

\[
\begin{array}{c|c}
  & s \\
  \hline
  s & \\
\end{array}
\]
Consequence:
Idempotents $e$ and $f$ belong to the same $D$-class if and only if there exist mutually inverse elements $x$ and $y$ such that $e = xy$ and $f = yx$.

\[
\begin{array}{c|c|c}
 x & e = xy & f = yx \\
\hline
 y \cdot & & y \\
\hline
 f = yx & y & \\
\hline
 x \cdot & & \\
\end{array}
\]

Consequence:
Two $H$-classes in the same $D$-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 \( \iff \) \( \forall x, y \in S : x^{\omega+1} = x \) & \( (xyx)^\omega = x^\omega \).

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

\[
\begin{align*}
&\bullet \xrightarrow{a} \bullet \xrightarrow{b} \bullet \\
&\bullet \xrightarrow{a} \bullet \xrightarrow{b} \bullet
\end{align*}
\]

Equivalent formulation:

For any letters \( a, b \in A \), \( \text{Im}(\delta_a) \) forms a transversal (set of representatives) of \( \ker(\delta_b) \).
Structure of $\mathcal{D}$-Classes

Rees quotient:
$I$ ideal of $S$, \[ S/I = (S \setminus I) \cup \{0\} \]
(subset $I \subseteq S$ downward closed w.r.t. $\mathcal{J}$ becomes zero of $S/I$)
corresponds to congruences of the form $\text{id}_S \cup I \times I$

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

Consequence:
$D$ regular $\mathcal{D}$-class, $x, y \in D \implies \exists z \in D : x \in zD \& z \in xD \& y \in Dz \& z \in Dy$
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 $\implies D \cup \{0\} = S^1 DS^1 / (S^1 DS^1 \setminus D)$ 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, $\varphi : S \to T$ onto homomorphism

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

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

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

Every principal factor of $T$ is image of a principal factor of $S$ via homomorphism induced by $\varphi$.

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 $f \in S : \varphi(f) = e$ & $f \mathcal{J}$-minimal in $\varphi^{-1}(e\mathcal{H})$

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

e\mathcal{H} = \varphi(f\mathcal{H}) : 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 \( R \times L \):
\[
(r, \ell) \cdot (r', \ell') = (r, \ell')
\]
\[
(r, \ell) R (r', \ell') \iff r = r'
\]
\[
(r, \ell) L (r', \ell') \iff \ell = \ell'
\]
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 \( \mathcal{M}^0(R, L, G, P) = (R \times G \times L) \cup \{0\} \):
\[
(r, g, \ell) \cdot (r', g', \ell') = \begin{cases} 
(r, g \cdot p_{\ell r'} \cdot g', \ell') & \text{if } p_{\ell r'} \neq 0 \\
0 & \text{if } p_{\ell r'} = 0
\end{cases}
\]

Matrix representation of \( \mathcal{M}^0(R, L, G, P) \):
\((r, g, \ell)\) corresponds to the matrix with only one non-zero entry \( g \) in the position \((r, \ell)\)
sandwich multiplication: \( M \cdot N = MPN \)
Theorem: (Rees 1940)

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

Proof:

$S$ . . . 0-simple semigroup

$G$ . . . Schützenberger group of the non-zero $D$-class

$R$ . . . the set of $R$-classes, $L$ . . . the set of $L$-classes

choose a group $H$-class and elements $t_r$ and $s_\ell$, for $r \in R$ and $\ell \in L$

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

$(t_r g s_\ell)(t_r' g' s_\ell') = t_r (g s_\ell t_r' g') s_\ell' \leadsto \text{ set } p_{\ell r} = s_\ell t_r \in G \cup \{0\}$

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: $x \mathcal{J} y \mathcal{J} z \mathcal{J} xy = xyz \implies y = yz.$

Proof: $y \mathcal{R} yz$, $x \cdot$ 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 $x_k \in J$
$\forall j \geq k: x_k \cdots x_j \in J \implies$
$\exists k \leq i < j: x_i, x_j \in J \& x_k \cdots x_i = x_k \cdots x_j$ (by pigeonhole principle)
$x_k \cdots x_{i-1} \mathcal{J} x_i \mathcal{J} x_{i+1} \cdots x_j \mathcal{J} (x_k \cdots x_{i-1})x_i(x_{i+1} \cdots x_j)$
cancellation rule $\implies x_i \cdots x_j = x_i$
Finite Power Property

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

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

decidable (Hashiguchi 1979, Simon 1978)

Construction: (Birget & Rhodes 1984)

$\varphi: A^+ \rightarrow S$ homomorphism recognizing $L$ and $L^+$

define mapping $\tau: A^+ \rightarrow \varphi(S^3)$

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

$\tau$ induces a semigroup operation on $\tau(L^+) \subseteq \varphi(S^3)$ \sim \tau$ 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 $D$-class of $\tau(L^+)$ contains some element of $\tau(L)$.
- $L^+ = L \cup \cdots \cup L^{(j+1)^h}$

$j$ ... maximal size of a $J$-class of $S$

$h$ ... length of the longest chain of $J$-classes in $\tau(L^+)$
Star-Free Languages and Aperiodic Semigroups

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

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

Aperiodic semigroup $S$ — equivalent definitions:

• $\forall x \in S \exists n: x^{n+1} = x^n \ (x^\omega+1 = x^\omega)$

• 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 $y \mathcal{H} x$ using union, concatenation, complementation and descriptions of products belonging to higher $\mathcal{J}$-classes.

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

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

**Proof of “$\iff$”:** $y = x_1 \cdots x_n$

$y \geq \mathcal{J} x \& y \leq \mathcal{R} x \& y \leq \mathcal{L} x \implies y \mathcal{R} x \& y \mathcal{L} x$

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:**

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

**Proof of “$\iff$”:** take the smallest $i$ such that $x_1 \cdots x_i \mathcal{R} x$.
Lemma: \( x_1 \cdots x_n \not\in \mathcal{J} \ x \iff \) either \( x_i \not\in \mathcal{J} \ x \) for some \( i \)
\[\text{or} \ x_{i+1} \cdots x_{j-1} > \mathcal{J} \ x \ \text{and} \ x_i \cdots x_j \not\in \mathcal{J} \ x \ \text{for some} \ i < j.\]

Proof of \( \implies \): Take \( i \leq j \) such that \( x_i \cdots x_j \not\in \mathcal{J} \ x \) and \( j - i \) is smallest possible.

<table>
<thead>
<tr>
<th></th>
<th>( y )</th>
<th>( yx_j )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x_i \downarrow )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( x_i y )</td>
<td>( x_i yx_j )</td>
<td></td>
</tr>
</tbody>
</table>

\[x_i \cdots x_j = x_i y x_j \in \mathcal{J} \ y \in \mathcal{J} \ x, \ \text{contradiction}\]

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

Proof: “$\implies$” direct verification

“$\impliedby$” $\varphi: A^* \to M$ 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:

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

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

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

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

$J = \{ a \in A \mid \varphi(a) \notin \mathcal{J} x \}$

$\cup \bigcup \{ a\varphi^{-1}(y)b \mid y \in M, a, b \in A, y > \mathcal{J} x, \varphi(a)y\varphi(b) \notin \mathcal{J} x \}$

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

Example: $M((a^2)^*)$ is a two-element group $\implies (a^2)^*$ is not star-free
Occurrences of Idempotents in Products

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

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

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

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

factorization forest of $$\varphi$$:

d: \{ w \in A^* \mid |w| \geq 2 \} \to (A^+)^+ \text{ 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:

\[ M = \left( \mathbb{Z}, + \right) / 2\mathbb{Z} \] (two-element group)

\[ \varphi: \{a, b\}^+ \to M \quad \varphi(a) = 1, \varphi(b) = 0 \] (identity element)

Minimal height of a factorization forest for \( \varphi \) 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, \( w = b^{k_0} a b^{k_1} \ldots a b^{k_n} \), then

\[
d(w) = \begin{cases} 
(a, b^{k_1} a) & \text{if } n = 2, k_0 = k_2 = 0 \\
(b, \ldots, b, a b^{k_1} a, b, \ldots, b, \ldots, a b^{k_n-1} a, b, \ldots, b) & \text{otherwise}
\end{cases}
\]

word \( abbbabbbabbbabbbabba \) 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. $J$-classes

long products staying in the same $J$-class:

- $x_1, \ldots, x_n, x_1 \cdots x_n$ belong to the same $J$-class $\implies$
- $H$-class of $x_{i+1} \cdots x_j$ uniquely determined by $R$-class of $x_{i+1}$ and $L$-class of $x_j$

$$(x_{i+1} \cdots x_j J x_j \& x_{i+1} \cdots x_j \leq L x_j \implies x_{i+1} \cdots x_j L x_j)$$

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

factors between places with the same pair belong to the same $H$-class

Equivalent formulation: For every homomorphism $\varphi$ 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 $= \text{finite union of monomials}$

(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 $d(w) = (w_1, w_2)$

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

Theorem: 

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 $e \cdot \{x \in M \mid e \leq_J x\}^* \cdot e$.

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

(Arfi 1991)
Proof of “2 $\implies$ 1”: 
\( \varphi : A^* \to M \) recognizes finite unions of languages \( \{ w \in A^* \mid \varphi(w) \geq x \} \) for \( x \in M \).

d \ldots factorization forest of \( \varphi \) of height \( 3|M| \)
We verify \( \{ w \in A^* \mid \varphi(w) \geq x \} = \bigcup_{\varphi(w) \geq x} P_d(w) \)
    (this is a polynomial because degrees are bounded by \( 2^{3|M|} \))
\( \subseteq: \) \( w \in P_d(w) \)
\( \supseteq: \) 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 \( v \in P_d(w) = P_d(w_1) \cdot P_d(w_2) \)
    \( \implies v = v_1v_2, \varphi(v_1) \geq \varphi(w_1), \varphi(v_2) \geq \varphi(w_2) \)
    \( \implies \varphi(v) = \varphi(v_1v_2) \geq \varphi(w_1w_2) = \varphi(w) \)

If \( d(w) = (w_1, \ldots, w_n) \) with \( n \geq 3 \) then \( v \in P_d(w) = P_d(w_1) \cdot \operatorname{alph}(w)^* \cdot P_d(w_n) \)
    \( \implies v = v_1uw_n, \varphi(v_1) \geq \varphi(w_1), \varphi(v_n) \geq \varphi(w_n), \operatorname{alph}(u) \subseteq \operatorname{alph}(w) \)
    \( \implies \varphi(u) \in \{ x \in M \mid \varphi(w) \leq \mathcal{J} x \}^* \)
    \( \implies \varphi(v) = \varphi(v_1)\varphi(u)\varphi(v_n) \geq \varphi(w_1)\varphi(u)\varphi(w_n) = \varphi(w)\varphi(u)\varphi(w) \geq \varphi(w) \)
Well Quasiorders
Recognizing Languages by Monotone Quasiorders

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

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

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

$(u \leq v \implies C_L(u) \subseteq C_L(v) \implies u \leq_L v)$

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)

\( w \in L \text{ minimal in } L \subseteq A^* \text{ w.r.t. } \leq \iff (\forall u \in L: u \leq w \Rightarrow w \leq u) \)

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.
- 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 $\implies$ 1”:

Left and right syntactic quasiorders $\leq^L_\ell$ and $\leq^r_L$ are wqos.

$w \leq^L_\ell w' \iff (\forall u \in A^*: uw \in L \implies uw' \in L) \iff C^\ell_L(w) \subseteq C^\ell_L(w')$

$w \leq^r_L w' \iff (\forall v \in A^*: vw \in L \implies w'v \in L) \iff C^r_L(w) \subseteq C^r_L(w')$

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

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

i.e. $i < j \implies C^\ell_L(u_i) \subset C^\ell_L(u_j)$

$C^\ell_L(u_i)$ is upward closed w.r.t. $\leq^r_L$:

$v \in C^\ell_L(u_i) \& v \leq^r_L v' \implies u_i \in C^r_L(v) \subseteq C^r_L(v') \implies v' \in C^\ell_L(u_i)$

$(C^\ell_L(u_i))_{i=1}^\infty$ strictly increasing sequence of languages upward closed w.r.t. $\leq^r_L$

contradicts that $\leq^r_L$ is wqo
Nash-Williams Minimal Bad Sequence Argument

How to prove a quasiorder to be wqo?

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

\(X^\omega\) ... 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 ... \(\forall i, j: i < j \implies x_i \not\leq x_j\)

\(\leq\) another quasiordering on \(X\), \(\sim\) the corresponding equivalence relation

quasiorder \(X^\omega\) lexicographically w.r.t. \(\leq\):

\((x_i)_{i=1}^{\infty} \leq (y_i)_{i=1}^{\infty} \iff\) either \(\forall i: x_i \sim y_i\)

or \(\exists n: x_n \triangleright y_n \land \forall i < n: x_i \sim y_i\)

Lemma:

If \(X\) contains no infinite descending sequence w.r.t. \(\leq\) and \(\leq\) is not a wqo, then there exists a bad sequence for \(\leq\) minimal w.r.t. \(\leq\).

Proof: Inductively choose \(x_i\) minimal w.r.t. \(\leq\) 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 \( R = \{ \varepsilon \to a \mid a \in A \} \)

\( \leq \) 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 \( a \):

\[ w_{i_k} = av_k \text{ for } k = 1, \ldots, \infty \]

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

\[ \implies \] every language closed under inserting letters is regular

Unitary context-free systems:

\[ R = \{ \varepsilon \to w \mid w \in I \}, \text{ where } I \subseteq A^* \text{ finite} \]

(to obtain standard context-free system, replace every rule \( \varepsilon \to w \) with rules \( a \to aw \) and \( a \to wa \) 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 $R = \{ \varepsilon \rightarrow w \mid w \in I \}$, the following conditions are equivalent:

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

$I \subseteq A^+$ 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 $I$
- $\exists n: A^n \subseteq A^*IA^*$

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

$I = \{a^2, b^2\}$ avoidable, $I = \{a^2, b^2, ab\}$ 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 \( \iff A^* \setminus A^*IA^* \) finite

But sets in these conditions are context-free.
Context-Free Derivations Defined by Homomorphisms

\[ \varphi : A^* \rightarrow (M, \leq) \text{ homomorphism} \]

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

notation: \( \Rightarrow^\varphi \equiv \Rightarrow^*_R \)

\[ u \Rightarrow^\varphi v \iff u = a_1 \ldots a_n, a_i \in A \]

\[ \& v = v_1 \ldots v_n, v_i \in A^+ \]

\[ \& \varphi(a_i) \leq \varphi(v_i) \]

\[ \Rightarrow^\varphi \subseteq \leq_\varphi \]

\[ \varphi(A) = M \implies \text{sufficient to take finite} \]

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

\[ \Rightarrow^\varphi \text{ is a wqo} \implies \text{sufficient to take finite} \]

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

\[ M = (\mathbb{Z}, +)/2\mathbb{Z} \quad \text{(two-element group)} \]

\[ \leq \text{is } = \]

\[ \varphi : \{a, b\}^+ \to M \quad \varphi(a) = 1, \varphi(b) = 0 \quad \text{(identity element)} \]

\[ \Rightarrow^* \varphi : \]

\[ \ldots \]

\[
\begin{array}{c}
\text{ab}^2 & a^3 & \text{bab} & b^2a & \text{aba} & a^2b & \text{ba}^2 & b^3 \\
\text{ab} & \text{ba} & \text{a} & \text{a}^2 & b & b^2 & \text{b} & \text{b}^2 \\
\text{a} & \text{b} & \text{a}^3 & \text{b}^2 & \text{babab} & \{a^3, b^2, ba^2b, babab\} \text{ is unavoidable} \\
\end{array}
\]

Therefore \( \Rightarrow^* \varphi \) is a wqo.

Example:

\[ \varphi(a) \neq \varphi(a^2) = 0, \text{two incomparable elements} \]

\[ \Rightarrow^* \varphi \text{ is not wqo: } a^k \text{ cannot be rewritten; } a^{\omega} \text{ avoids all } awa \text{ such that } a \Rightarrow^* \varphi awa \]
Theorem: (Bucher & Ehrenfeucht & Haussler 1985)

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

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

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

3) There exists homomorphism $\varphi : A^* \rightarrow M$ to a finite ordered monoid such that $\Rightarrow^*_R = \Rightarrow^*_\varphi$.

Proof:

3 $\implies$ 2: $a \Rightarrow^*_R w \iff \varphi(w) \in \{ x \in M \mid x \geq \varphi(a) \}$

2 $\implies$ 1: substitute $\{ w \mid a \Rightarrow^*_R w \}$ for every $a \in A$ in $L$

1 $\implies$ 3: $\varphi_a : A^+ \rightarrow M_a$ syntactic homomorphism to ordered monoid for $\{ w \mid a \Rightarrow^*_R w \}$

$\varphi : A^+ \rightarrow M = \prod_{a \in A} M_a \quad \varphi(w) = (\varphi_a(w))_{a \in A}$

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

$\iff b \Rightarrow^*_R w$
Problem: For which homomorphisms $\varphi : A^* \to M$ to a finite ordered monoid is $\Rightarrow^*_\varphi$ wqo?

Theorem: (MK 2005)

For every homomorphism $\varphi : A^* \to M$ 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 $xy \mathcal{J} x$ or $xy \mathcal{J} y$.

$S_i \ldots$ 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 \( \implies \) emptiness problem decidable

For scattered subword ordering:
emptiness problem decidable \& effective intersection with regular languages \( \implies \) 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 \( w \rightarrow w \upharpoonright u \), for \( u \in I \),
i.e. \( w_0 \ldots w_n \rightarrow w_0u_1w_1 \ldots u_nw_n \), for \( u_1 \ldots u_n \in I \)

Theorem: (Haussler 1985)

\( \rightarrow^* \) 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 $f : B^* \to A^*$ homomorphism

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

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 $Y$

$f : X \to Y$ 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: $\varepsilon \rightarrow a$, $a \rightarrow b$, for $a \leq b$, $a, b \in X$)

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

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

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

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

(isomorphic to a subset of $(\mathcal{F}, \sqsupseteq)$)
Language Equations
Language equation = equation over some algebra of languages

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

• 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:

\[ X_1 = \{ \varepsilon \} \cup X_2 \cdot a \quad X_2 = X_1 \cdot b \cup X_2 \cdot a \]

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

\[ X_i = K_i \cup \bigcup_{j=1}^{n} X_j \cdot L_{j,i} \quad i = 1, \ldots, n \]

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 \( R = (L_{j,i}) \)

\[ X = S + X R \]
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 $\ast$.

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: \[ X_1 \rightarrow \varepsilon | X_2X_1 \quad X_2 \rightarrow (X_1) \]

system of language equations: \[ X_1 = \{\varepsilon\} \cup X_2 \cdot X_1 \quad X_2 = \{() \cdot X_1 \cdot ()\} \]

Ginsburg & Rice 1962:
context-free languages = components of smallest (largest, unique) solutions of explicit systems
\[ X_i = P_i \quad i = 1, \ldots, n \]

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 $\varepsilon$-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 EXPTIME and can be 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)

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
• $\subseteq \text{DTIME}(n^3) \cap \text{DSPACE}(n)$
• 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, 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: 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

\[ KM = ML \ldots \text{languages } K \text{ and } L \text{ are conjugated via a language } M \]

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 \( \varepsilon \) 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 \( \varepsilon \)
- 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 \( L_1, \ldots, L_n \)?

- trivally \textbf{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 \textbf{rational system} of word equations is algorithmically equivalent to some of its finite subsystems \( \implies \) satisfiability of rational systems of word equations is \textbf{decidable}.

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

Do given finite languages form a solution of the system \( \{ X^nZ = Y^nZ \mid n \in \mathbb{N} \} \)?

\textbf{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 \( X_\varepsilon \)

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

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

maximal solutions:

- 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 \( L_i \)

(Conway 1971)

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:

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

- satisfiability by arbitrary (finite) languages is 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 \text{basic properties of the inequality can be expressed using formulae of monadic second-order theory of infinite } |A|\text{-ary tree}

**Example:** \( b \cup X a \subseteq X \cup X ba \)

\( X \) is a solution \iff \( X(b) \land (\forall x : X(x) \implies (X(xa) \lor \exists y : X(y) \land x = yb)) \)

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

\[ \implies (\forall x : X(x) \implies Y(x)) \]

**minimal solutions:**

\( \bullet = "X \text{ holds}" \quad \circ = "X \text{ does not hold}" \)

\( a^* \cup b : \)

\[ \begin{array}{c}
  a^* \\
  a \quad b
  \end{array} \]

\( ba^* : \)

\[ \begin{array}{c}
  ba^* \\
  a \quad b
  \end{array} \]

Rabin 1969 \implies \text{algorithmically solvable using tree automata}

very special case of \textit{set constraints} (letters as unary functions)

EXPTIME-complete (even when complementation is allowed) (1994–2006)
Yet More General Left-Linear Inequalities

\[ K_0 \cup X_1K_1 \cup \cdots \cup X_nK_n \subseteq L_0 \cup X_1L_1 \cup \cdots \cup X_nL_n \]

\( K_j \) 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 $P_i \subseteq Q_i$
$P_i \subseteq (A \cup V)^*$ arbitrary
$Q_i \ldots$ regular expressions over variables and languages recognizable by
a homomorphism $\varphi : A^* \rightarrow (M, \leq)$

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: $\alpha$ arbitrary solution

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

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

$\beta$ is a solution:

$u \in \beta(P_i) \implies \exists v \in \alpha(P_i) : v \Rightarrow^\varphi u$ (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 $\beta$
- $e$ 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 $\beta$ 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 $P_i \subseteq Q_i$

$P_i \subseteq (A \cup V)^*$ 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 $N \subseteq N)$
Semi-commutation Inequalities

\[ XK \subseteq LX \]  \( K \) 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 \( w \rightarrow wu \)
  - defender: chooses \( v \in L \)
    - \( wu = vw\hat{w} \)
    - plays \( wu \rightarrow \hat{w} \)

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: $w = abcd$, $L = \{a, ab, abcd, bc, c, cd, da\}$
Well-quasiordering Trees

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

Example:

\[ \begin{array}{ccc}
  & s & \\
  t & & t \\
  & p & q & t \\
  & s & & \\
\end{array} \]

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 $N$.

\[
\begin{align*}
X K & \subseteq LX \\
X & \subseteq M \\
X K & \subseteq LX \\
X M & \subseteq NX \\
X K & \subseteq LX \\
M X & \subseteq XN
\end{align*}
\]

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 $C(L)$ of $XL = LX$ is not recursively enumerable.
Example: \( L \) regular, but \( C(L) \) non-regular

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

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

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

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

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:

$$efga^m ba^n \downarrow$$

$$efga^m ba^n \cdot \hat{gf} \quad \longrightarrow \quad fga^m ba^n \hat{gf} \quad \downarrow$$

$$ga^m ba^n \hat{gf} \quad \quad fga^m ba^n \hat{gf} \cdot c \cdot c \notin L^2 \cdot A^*$$

$$ga a^{m-1} ba^n \hat{gf} \cdot \hat{e} \downarrow$$

$$a^{m-1} ba^n \hat{gf} \hat{e} \downarrow$$

$$\vdots \downarrow$$

$$efga^{m-1} ba^{n-1}$$
Games That Can Be Encoded  
(Jeandel & Ollinger)

Example:

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: (Rato and Romanana 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 $X \uplus Y = L$ of a regular language $L$

• existence of non-trivial unambiguous decompositions of regular languages