Local Rees extensions

Volker Diekert[1]

Universität Stuttgart

CSA 2106, Lisbon, June 24th, 2016

Celebrating the 60th birthdays
of Jorge Almeida and Gracinda Gomes

[1] Joint work with Tobias Walter

- Part I: semigroups: here monoids.
- Commercial break
- Part II: automata: here formal languages.

Part I: Varieties of finite monoids

A variety is a class of finite monoids which is closed under finite direct products and divisors. A monoid N is a divisor of M if N is the homomorphic image of a submonoid of M. Notation: $N \preceq M$.

Example

$\mathbf{1}$, $\mathbf{Ab}$, $\mathbf{Sol}$, $\mathbf{G}$ are varieties of groups.

If $\mathbf{V}$ is a variety, then

$$\mathbf{V} \cap \mathbf{G} = \{G \in \mathbf{V} \mid G \text{ is a group}\}$$

is a variety of groups.

If $\mathbf{H}$ is a variety of groups, then we let

$$\overline{\mathbf{H}} = \{M \in \mathbf{Mon} \mid \text{ all subgroups of } M \text{ are in } \mathbf{H}\}.$$

Example

$\overline{\mathbf{1}} = \mathbf{AP}, \quad \overline{\mathbf{G}} = \mathbf{Mon}, \quad \mathbf{V} \subseteq \overline{\mathbf{V} \cap \mathbf{G}}.$

Jorge Almeida and Ondřej Klíma defined the bullet operation $\mathrm{Rees}(\mathbf{U}, \mathbf{V})$ as the least variety of monoids containing all Rees extensions $\mathrm{Rees}(N, L, \rho)$ for $N \in \mathbf{U}$, $L \in \mathbf{V}$, and $\rho : N \to L$.

A variety $\mathbf{V}$ is called bullet idempotent if $\mathbf{V} = \mathrm{Rees}(\mathbf{V}, \mathbf{V})$.

Almeida, Klíma, **J. Pure Appl. Algebra**, 220:1517 – 1524, 2016

$\overline{\mathbf{H}}$ is bullet idempotent.

Question. Is it true that all bullet idempotent varieties are of the form $\overline{\mathbf{H}}$?

Answer. (D., Walter): **Yes.**

This shows that $\overline{\mathbf{H}}$ is a robust variety admitting many other characterizations. This relates, in particular, to classical results by Schützenberger.

Rees extensions

Let N, L be monoids and $\rho : N \to L$ be any mapping.

As a set we define

$$\mathrm{Rees(N, L, \rho)} = N \cup (N \times L \times N)\,.$$

The multiplication $\cdot$ on $\mathrm{Rees(N, L, \rho)}$ is given by

$$\begin{aligned} n \cdot n' &= nn' \\ n \cdot (n_1, m, n_2) \cdot n' &= (nn_1, m, n_2 n') \\ (n_1, m, n_2) \cdot (n_1', m', n_2') &= (n_1, m\rho(n_2 n_1')m', n_2'). \end{aligned}$$

Lemma

Let $N \preceq N'$ and $L \preceq L'$. Given $\rho : N \to L$, there exists a mapping $\rho' : N' \to L'$ such that $\mathrm{Rees(N, L, \rho)}$ is a divisor of $\mathrm{Rees(N', L', \rho')}$.

Emil Artin, Geometric algebra (1957), page 14, paragraph 3

"It is my experience that proofs involving matrices can be shortened by 50% if one throws the matrices out."

Local divisor technique

The local divisor technique was established in finite semigroup theory around 2004 as a tool to simplify inductive proofs. (In associative algebra the concept is due to Kurt Meyberg 1972.[2])

Let M be a monoid and $c \in M$. Consider the set $cM \cap Mc$ and define a new multiplication

$$xc \circ cy = xcy.$$

Then $M_c = (cM \cap Mc, \circ, c)$ is monoid: the local divisor at c.

Facts

- $\lambda_c : \{x \in M \mid cx \in Mc\} \to M_c$ given by $\lambda_c(x) = cx$ is a surjective homomorphism. Hence, M_c is a divisor of M.
- If c is a unit, then M_c is isomorphic to M.
- If $c = c^2$, then M_c is the standard "local monoid".
- If c is not a unit, then $1 \notin M_c$. Hence, if c is not a unit and if M is finite, then $|M_c| < |M|$.

[2]As I learned from Ben Steinberg

Local Rees extensions

Let $N \subseteq M$ be a proper submonoid and $c \in M \setminus N$ which is not a unit such that $N \cup \{c\}$ generate M. Hence, N and M_c are divisors of M and $|N|, |M_c| < |M|$. Let $\rho(x) = cxc$.

$\mathrm{LocRees(N, c)} = \mathrm{Rees(N, M_c, \rho)}$ is called a local Rees extension.

Lemma

M is a quotient monoid of $\mathrm{LocRees(N, c)}$.

Proof.

Define $\varphi : \mathrm{LocRees(N, c)} \to M$ by $\varphi(n) = n$ for $n \in N$ and $\varphi(u, x, v) = uxv$ for $(u, x, v) \in N \times M_c \times N$. Since

$$\begin{aligned}\varphi((u, x, v)(s, y, t)) &= \varphi(u, x \circ cvsc \circ y, t) = \varphi(u, xvsy, t) \\ &= (uxv)(syt) = \varphi(u, x, v)\varphi(s, y, t),\end{aligned}$$

φ is a homomorphism. Obviously, $M = N \cup NM_cN$ and thus φ is surjective. $\square$

Theorem

Let $\mathbf{H}$ be a variety of groups and $\mathbf{V}$ be the smallest variety which is closed under local Rees extensions and which contains $\mathbf{H}$. Then we have $\mathbf{V} = \overline{\mathbf{H}}$.

Proof.

The inclusion $\mathbf{V} \subseteq \overline{\mathbf{H}}$ follows from Almeida and Klíma. For the other direction, let $M \in \overline{\mathbf{H}}$. If M is a group, then $M \in \mathbf{H}$ and we are done. Otherwise choose a minimal set of generators $c, c_1, \ldots, c_k$. Wlog. c is not a unit. Consider $N = \langle c_1, \ldots, c_k \rangle$ and M_c. By induction, N, $M_c \in \mathbf{V}$ and hence $\mathrm{LocRees(N, c)} \in \mathbf{V}$. Hence, the divisor M is in $\mathbf{V}$. □

Every bullet idempotent variety is of the form $\overline{\mathbf{H}}$. More precisely:

Corollary

Let $\mathbf{V}$ be a variety and $\mathbf{H} = \mathbf{V} \cap \mathbf{G}$, then

$$\mathbf{V} \subseteq \mathrm{LocRees}(\mathbf{H}) = \mathrm{Rees}(\mathbf{V}) = \overline{\mathbf{H}} = \mathrm{Rees}(\overline{\mathbf{H}}).$$

Example

Let $B = \{1, a, b, 0\}$ with $xy = 0$ unless $x = 1$ or $y = 1$ and $\mathfrak{S}_3 = \langle \delta, \sigma \rangle$ where δ is a “Drehung” (rotation: $\delta^3 = 1$) and σ is a “Spiegelung” (reflection: $\sigma^2 = 1$). Define

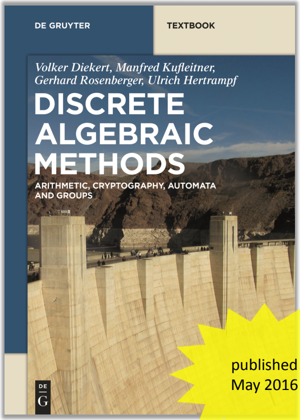
$$M = (\mathfrak{S}_3 \times B) / \left\{ (\delta, a) = (1, a) \right\}.$$

Then $M = \{0\} \cup \mathfrak{S}_3 \cup a \langle \sigma \rangle \cup b\mathfrak{S}_3$ has fifteen elements. The local Rees decomposition is as follows.

$$\begin{tikzcd}[column sep=small]
 & & & M \arrow[dll, dash] \arrow[drr, dash] & & & \\
 & M[a,\sigma,\delta] \arrow[dl, dash] \arrow[dr, dash] & & & & M_b \simeq \mathfrak{S}_3 \cup \{0\} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathfrak{S}_3 & & M[a,\sigma,\delta]_a \simeq \mathbb{Z}/2\mathbb{Z} \cup \{0\} \arrow[dl, dash] \arrow[dr, dash] & & \mathfrak{S}_3 & & (M_b)_0 \simeq \{1\} \\
 & \mathbb{Z}/2\mathbb{Z} & & (M[a,\sigma,\delta]_a)_0 \simeq \{1\} & & &
\end{tikzcd}$$

Commercial break

Free inspection copies available using deGruyter's page
http://www.degruyter.com/page/640
If you are interested please contact the speaker.



published
May 2016

From the Content:

- Cryptography
- Number theoretic algorithms
- Polynomial time primality test
- Elliptic curves
- Combinatorics on words
- Discrete infinite groups

Retail price: € 34.95 / US$ 49.00

340 pages, 60 illustrations

paperback isbn 978-3-11-041332-8
eBook isbn 978-3-11-041333-5

http://www.degruyter.com/books/ 978-3-11-041332-8

1

Prefix codes of bounded synchronization delay

$K \subseteq A^+$ is called prefix code if it is prefix-free. That is: $u, uv \in K$ implies $u = uv$.

A prefix-free language K is a code since every word $u \in K^*$ admits a unique factorization $u = u_1 \cdots u_k$ with $k \geq 0$ and $u_i \in K$.

A prefix code K has bounded synchronization delay if for some $d \in \mathbb{N}$ and for all $u, v, w \in A^*$ we have:
if $uvw \in K^*$ and $v \in K^d$, then $uv \in K^*$.

Example

$B \subseteq A$ yields a prefix code with synchronization delay 0. If $c \in A \setminus B$, then B^*c is a prefix code with synchronization delay 1.

Application

Assume that Alice sends a message using a prefix code K with synchronization delay d of the form

$$m = c_1 \cdots c_k$$

where $c_i \in K$. Bob is late and receives a suffix of m, only:

$$?uvw.$$

such that $v \in K^d$. Then Bob can recover the suffix w as suffix

$$w = c_p \cdots c_k$$

with $d \leq p \leq k$.

Notation

- A = finite alphabet
- A^* = finite words, A^ω = infinite words, $A^\infty = A^* \cup A^\omega$.
- $h : A^* \to M$ recognizes $L \subseteq A^*$ if $h^{-1}(h(L)) = L$.
- If $\mathbf{V}$ is a variety, then
  $\mathbf{V}(A^*) = \{L \subseteq A^* \mid \text{some } h : A^* \to M \text{ recognizes } L\}$
- M is aperiodic if all subgroups are trivial.
- Regular languages: finite subsets & closure under union, concatenation, and Kleene-star
  = recognizable by a finite monoid.
- Star-free languages: finite subsets & closure under union, concatenation, complementation, but no Kleene-star
  = recognizable by a finite aperiodic monoid.

Lemma (Schützenberger)

Let $K \in \overline{\mathbf{H}}(A^*)$ be a prefix code of bounded synchronization delay. Then: $K^* \in \overline{\mathbf{H}}(A^*)$.

Proof.

We have

$$A^* \setminus K^* = \bigcup_{0 \leq i} \left(K^i AA^* \setminus K^{i+1} A^*\right).$$

Now, let d be the synchronization delay of K. Then we can write

$$A^* \setminus K^* = A^* K^d (AA^* \setminus KA^*) \cup \bigcup_{0 \leq i < d} (K^i AA^* \setminus K^{i+1} A^*).$$

$\square$

$\mathbf{H}$-controlled star
Cet obscur objet du désir (Luis Buñuel 1977)

Let $\mathbf{H}$ be a variety of groups and $G \in \mathbf{H}$. Let $K \subseteq A^+$ be a prefix code of bounded synchronization delay. Consider any mapping $\gamma : K \to G$ and define $K_g = \gamma^{-1}(g)$. Assume further that $K_g \in \overline{\mathbf{H}}(A^*)$ for all $g \in G$.

With these data the $\mathbf{H}$-controlled star $K^{\gamma\star}$ is defined as:

$$K^{\gamma\star} = \{u_{g_1} \cdots u_{g_k} \in K^* \mid u_{g_i} \in K_{g_i} \wedge g_1 \cdots g_k = 1 \in G\}\,.$$

Example

If G is the trivial group $\{1\}$, then $K^{\gamma\star} = K^*$ is the usual star.

Proposition (Schützenberger, **RAIRO**, 8:55–61, 1974.)

$\overline{\mathbf{H}}(A^*)$ *is closed under the* $\mathbf{H}$*-controlled star.*

Schützenberger's $\mathrm{SD}_{\mathbf{H}}$ classes

By $\mathrm{SD}_{\mathbf{H}}(A^*)$ we denote the set of regular languages which is inductively defined as follows.

1. Finite subsets of A^* are in $\mathrm{SD}_{\mathbf{H}}(A^*)$.
2. If $L, K \in \mathrm{SD}_{\mathbf{H}}(A^*)$, then $L \cup K, L \cdot K \in \mathrm{SD}_{\mathbf{H}}(A^*)$.
3. Let $K \subseteq A^+$ be a prefix code of bounded synchronization delay, $\gamma : K \to G \in \mathbf{H}$, and $\gamma^{-1}(g) \in \mathrm{SD}_{\mathbf{H}}(A^*)$ for all g. Then the $\mathbf{H}$-controlled star $K^{\gamma\star}$ is in $\mathrm{SD}_{\mathbf{H}}(A^*)$.

Note: the definition doesn't involve any complementation!

Proposition (Schützenberger (1974) reformulated)

$$\mathrm{SD}_{\mathbf{H}}(A^*) \subseteq \overline{\mathbf{H}}(A^*)$$

Theorem (Schützenberger (1975) and (1974))

$$\mathrm{SD}_{\mathbf{1}}(A^*) = \overline{\mathbf{1}}(A^*) = \mathbf{AP}(A^*) \textit{ and } \mathrm{SD}_{\mathbf{Ab}}(A^*) = \overline{\mathbf{Ab}}(A^*)$$

Schützenberger's result holds for all varieties.

Theorem (D., Walter. To appear ICALP, Rome, July 12-15, 2016)

Let $\mathbf{H}$ be any variety of finite groups. Then we have

$$\mathrm{SD}_{\mathbf{H}}(A^*) = \overline{\mathbf{H}}(A^*).$$

Remarks on the proof

- The proof uses an induction based on the "local divisor technique".
- The result that all bullet idempotent varieties are of the form $\overline{\mathbf{H}}(A^*)$ is an off-spring of that proof.

Applications of the local divisor technique

- Simplified proof for $\mathrm{LTL} = \mathrm{FO} = \mathbf{AP}$ for finite and infinite words and "traces". D. and Gastin (2006)
- "One-page-proof" for $\mathrm{SF} = \mathbf{AP}$. Kufleitner (2010)
- Aperiodic languages are Church-Rosser congruential. D., Kufleitner, and Weil (2011)
- Regular languages are Church-Rosser congruential. D., Kufleitner, Reinhardt, and Walter (2012)
- Simplified proof for the Krohn-Rhodes Theorem. D., Kufleitner, and Steinberg (2012)
- $\mathrm{SD}(A^\omega) = \mathbf{AP}(A^\omega)$. D. and Kufleitner (2013)
- New interpretation of Green's Lemma: Schützenberger categories. Costa and Steinberg (2014)
- $\mathrm{SD}_{\mathbf{H}}(A^\infty) = \overline{\mathbf{H}}(A^\infty)$. D. and Walter (2016)
- Thank you and "Happy birthday" to Cracinda and Jorge!