Expansions, Decompositions, and 2-Variable Logic

Conference dedicated to the scientific legacy of M.-P. Schützenberger

Howard Straubing
Boston College

Deterministic Finite Automaton

$$\mathcal{A} = (Q, \Sigma, q_0, F)$$

$$w = \sigma_1 \cdots \sigma_n \in \Sigma^*$$

$$\begin{aligned} w &\mapsto q_0\sigma_1 \cdots \sigma_n \\ &= qw \in Q \end{aligned}$$

$$L_{\mathcal{A}} = \{w \in \Sigma^* : q_0 w \in F\}$$

is a *recognizable* (= regular) *language*

DFA

$\mathcal{A} = (Q, \Sigma, q_0, F)$

$w = \sigma_1 \cdots \sigma_n \in \Sigma^*$

$$\begin{aligned} w &\mapsto q_0\sigma_1 \cdots \sigma_n \\ &= qw \in Q \end{aligned}$$

$L_{\mathcal{A}} = \{w \in \Sigma^* : q_0 w \in F\}$
is a *recognizable* (= regular) *language*

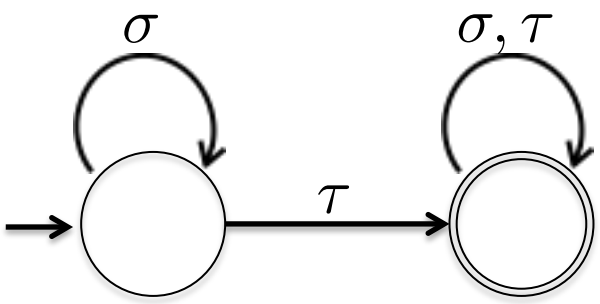
Homomorphism into finite monoid

$\phi : \Sigma^* \to M$

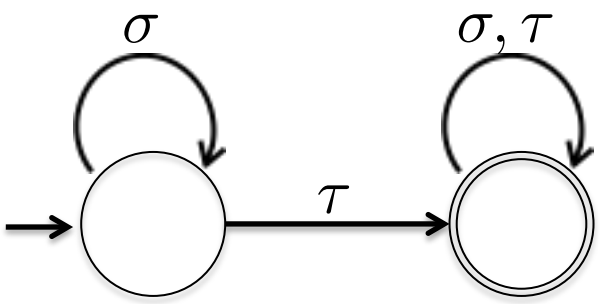
$X \subseteq M$

$$\begin{aligned} w &\mapsto \phi(\sigma_1) \cdots \phi(\sigma_n) \\ &= \phi(w) \in M \end{aligned}$$

$L_{\mathcal{A}} = \{w \in \Sigma^* : \phi(w) \in X\}$
is a *recognizable* (= regular) *language*



Recognizes $L = \{\sigma, \tau\}^* \tau \{\sigma, \tau\}^*$
set of words that contain a τ



Recognizes $L = \{\sigma, \tau\}^* \tau \{\sigma, \tau\}^*$
set of words that contain a τ

$M = U_1 = \{0, 1\}$

$X = \{0\}$

$\phi(\sigma) = 1, \phi(\tau) = 0$

$\times$	1	0
1	1	0
0	0	0

Recognizes the same language.

The Schützenberger Product

(1963-1966)

'On finite monoids having only trivial subgroups', *Information and Control*, 1965
(and at least four others from same era)

The Schützenberger Product

$\phi : \Sigma^* \to M$ homomorphism onto finite monoid

$$w = \sigma_1 \cdots \sigma_n \overset{\Psi}{\mapsto} \prod_{w=u\sigma v} (\phi(u), \sigma, \phi(v)) =$$

$$\big(1, \sigma_1, \phi(\sigma_2 \cdots \sigma_n)\big)\big(\phi(\sigma_1), \sigma_2, \phi(\sigma_3 \cdots \sigma_n)\big) \cdots \big(\phi(\sigma_1 \cdots \sigma_{n-1}), \sigma_n\, 1\big)$$

$$\in (M \times \Sigma \times M)^*$$

The Schützenberger Product

$\phi : \Sigma^* \to M$ homomorphism onto finite monoid

$$w = \sigma_1 \cdots \sigma_n \overset{\Psi}{\mapsto} \prod_{w=u\sigma v} (\phi(u), \sigma, \phi(v)) =$$

$$\big(1, \sigma_1, \phi(\sigma_2 \cdots \sigma_n)\big)\big(\phi(\sigma_1), \sigma_2, \phi(\sigma_3 \cdots \sigma_n)\big) \cdots \big(\phi(\sigma_1 \cdots \sigma_{n-1}), \sigma_n\, 1\big)$$

$$\in (M \times \Sigma \times M)^*$$

Set $w_1 \cong w_2$ if $\phi(w_1) = \phi(w_2)$, and
$\Psi(w_1)$ and $\Psi(w_2)$ have the same set of letters.

$\cong$ is a congruence of finite index on on Σ^*.

The Schützenberger Product

$\phi : \Sigma^* \to M$ homomorphism onto finite monoid

$$w = \sigma_1 \cdots \sigma_n \overset{\Psi}{\mapsto} \prod_{w=u\sigma v} (\phi(u), \sigma, \phi(v)) =$$

$$\big(1, \sigma_1, \phi(\sigma_2 \cdots \sigma_n)\big)\big(\phi(\sigma_1), \sigma_2, \phi(\sigma_3 \cdots \sigma_n)\big) \cdots \big(\phi(\sigma_1 \cdots \sigma_{n-1}), \sigma_n\, 1\big)$$

$$\in (M \times \Sigma \times M)^*$$

Set $w_1 \cong w_2$ if $\phi(w_1) = \phi(w_2)$, and
$\Psi(w_1)$ and $\Psi(w_2)$ have the same set of letters.

$\cong$ is a congruence of finite index on on Σ^*.

$\Diamond M$ ‘ = ’ $\Sigma^* / \cong$ (more or less the Schützenberger product)
$\Diamond\phi : \Sigma^* \to \Diamond M$ projection homomorphism

Not exactly...

The Schützenberger product is

$$M_1 \Diamond M_2 = M_1 \times \mathcal{P}(M_1 \times M_2) \times M_2$$

where

$$(m_1, X, m_2)(n_1, Y, n_2) = (m_1 m_2, Z, n_1 n_2)$$

with

$$Z = \{(m_1 s, t) : (s, t) \in X\} \cup \{(s, t n_2) : (s, t) \in Y\}$$

$L_1 \sigma L_2$ is recognized by the homomorphism

$$\sigma \mapsto (\phi(\sigma), \{(1, 1)\}, \phi(\sigma))$$

$$\tau \mapsto (\phi(\tau), \emptyset, \phi(\tau))$$

if $\tau \neq \sigma$.

$\Diamond\phi : \Sigma^* \to \Diamond M$ is an *expansion* of $\phi : \Sigma^* \to M$.
(terminology due to Birget and Rhodes)

$\Diamond M$ admits simple *coordinates*.

$\Diamond M$ is *close* to M.

$\Diamond\phi : \Sigma^* \to \Diamond M$ is an *expansion* of $\phi : \Sigma^* \to M$.

$\Diamond M$ admits simple *coordinates*.

$\Diamond\phi(w) =$ (factorizations of $w, \phi(w)$)

If $\phi : \Sigma^* \to M$ recognizes $L_1, L_2 \subseteq \Sigma^*$
then $\Diamond\phi$ recognizes $L_1 \sigma L_2$ for any $\sigma \in \Sigma$.

$\Diamond M$ is *close* to M.

Every group in $\Diamond M$ is isomorphic to a group in M.

Consequence: If $L \subseteq \Sigma^*$ is built starting with $\emptyset$, and closing under boolean operations and $(L_1, L_2) \mapsto L_1 \sigma L_2$ (*i.e., L is star-free)* then L is recognized by a monoid M with no nontrivial groups (*aperiodic* monoid).

(one direction of that famous theorem..)

Bilateral Transducers ('bimachines')

'A remark on finite transducers', *Information and Control*, 1961

Bilateral Transducers ('bimachines')

Q, Q' left and right finite state sets.

$(q, \sigma) \mapsto q\sigma, (\sigma, q') \mapsto \sigma q' \quad \text{for } q \in Q, q' \in Q'.$

$$w = \sigma_1 \cdots \sigma_n \overset{\Psi}{\mapsto} \prod_{w=u\sigma v} (q_0 u, \sigma, v q_0')$$

$$= (q_0, \sigma_1, \sigma_2 \cdots \sigma_n q_0')(q_0\sigma_1, \sigma_2, \sigma_3 \cdots \sigma_n q_0') \cdots (q_0\sigma_1 \cdots \sigma_{n-1}, \sigma_n, q_0')$$

$$\in (Q \times \Sigma \times Q')^* = \Gamma^*.$$

Bilateral Transducers ('bimachines')

Q, Q' left and right finite state sets.

$(q, \sigma) \mapsto q\sigma, (\sigma, q') \mapsto \sigma q' \quad \text{for } q \in Q, q' \in Q'.$

$$w = \sigma_1 \cdots \sigma_n \overset{\Psi}{\mapsto} \prod_{w=u\sigma v} (q_0 u, \sigma, v q_0')$$

$$= (q_0, \sigma_1, \sigma_2 \cdots \sigma_n q_0')(q_0\sigma_1, \sigma_2, \sigma_3 \cdots \sigma_n q_0') \cdots (q_0\sigma_1 \cdots \sigma_{n-1}, \sigma_n, q_0')$$

$$\in (Q \times \Sigma \times Q')^* = \Gamma^*.$$

(We should really map $Q \times \Sigma \times Q'$ to a separate output alphabet.)

Bimachine transductions via finite monoids:

$$\phi : \Sigma^* \to M$$

$$w = \sigma_1 \cdots \sigma_n \overset{\Psi}{\mapsto} \prod_{w=u\sigma v} (\phi(u), \sigma, \phi(v))$$

$$= (1, \sigma_1, \phi(\sigma_2 \cdots \sigma_n))(\phi(\sigma_1), \sigma_2, \phi(\sigma_3 \cdots \sigma_n)) \cdots (\phi(\sigma_1 \cdots \sigma_{n-1}), \sigma_n, 1)$$

$$\in (M \times \Sigma \times M)^*$$

(Take $M = M_1 \times M_2$, where M_1 is transition monoid of (Q, Σ),

M_2 is (left) transition monoid of (Q', Σ).)

Theorem. (*Schützenberger (1961)*) The composition of two bimachine transductions is a bimachine transduction.

Homomorphisms
$\phi : \Sigma^* \to M$
$\psi : (M \times \Sigma \times M)^* \to N$

Composite transduction computed by *block product* $N \square M$.

Theorem. (*Schützenberger (1961)*) The composition of two bimachine transductions is a bimachine transduction.

Homomorphisms
$\phi : \Sigma^* \to M$
$\psi : (M \times \Sigma \times M)^* \to N$

Composite transduction computed by *block product* $N \Box M$.

(Block product formally introduced by Rhodes and Tilson much later, but it is implicit in Schützenberger's proof of this theorem.)

Block product. Don't spend a lot of time trying to understand the definition!

$$N \Box M = N^{M \times M} \times M$$

with multiplication

$$(F_1, m_1) \cdot (F_2, m_2) = (G, m_1 m_2)$$

where

$$G(m, m') = F_1(m, m_2 m') \cdot F_2(m m_1, m').$$

If

$$\psi : \sigma_i \mapsto (F_i, \phi(\sigma_i),$$

then

$$w = \sigma_1 \cdots \sigma_n \mapsto (G, \phi(w)),$$

where

$$G(1,1) = \prod_{i=1}^{n} F_i(\phi(\sigma_1 \cdots \sigma_{i-1}), \phi(\sigma_{i+1} \cdots \sigma_n)).$$

The Schützenberger Product

$\Diamond M$ ‘ = ’ $U_1 \Box M$. (Recall $U_1 = \{0, 1\}$.)

The Schützenberger Product

$\Diamond M$ ‘ = ’ $U_1 \Box M$. (Recall $U_1 = \{0, 1\}$.)

Well, not *exactly*, but close enough.
The two generate the same variety, and both are equal to semidirect products of M with an idempotent and commutative monoid on the left.
(Schützenberger: ‘boolean semidirect product’.)

The other half of that famous theorem.

If $L \subseteq \Sigma^*$ is built starting with $\emptyset$, and closing under boolean operations and

$$(L_1, L_2) \mapsto L_1 \sigma L_2$$

(i.e., L is star-free) then L is recognized by a monoid M with no nontrivial groups (*aperiodic* monoid).

Conversely, if L is recognized by a finite aperiodic monoid, then L is star-free.

'Next to Kleene's Theorem, probably the most important result dealing with recognizable sets.'

–Samuel Eilenberg

This yields a *decomposition:*

Every finite aperiodic monoid M *divides*
(is a quotient of a submonoid of)

$$U_1 \Box \cdots (U_1 \Box (U_1 \Box U_1)) \cdots)$$

Compare work of Krohn, Rhodes (1962-1965)

Sequential function computed by monoid.

$$w = \sigma_1 \cdots \sigma_n \overset{\Psi}{\mapsto} \prod_{w=u\sigma v}^{n} (\phi(u), \sigma)$$

$$= (1, \sigma_1)(\phi(\sigma_1), \sigma_2) \cdots (\phi(\sigma_1 \cdots \sigma_{n-1}), \sigma_n) \in (M \times \Sigma)^*$$

Composition computed by *wreath product* $N \circ M$.

Every aperiodic monoid divides

$$U_2 \circ U_2 \circ \cdots U_2$$

where $U_2 = \{1, a, b\}$ with $b = U_2 b, a = U_2 a$

The block product (in contrast to the wreath product) is not associative.

What if we turn it inside-out?

What do we get from

$$(\cdots((U_1 \square U_1) \square U_1)\cdots) \square U_1 \ ?$$

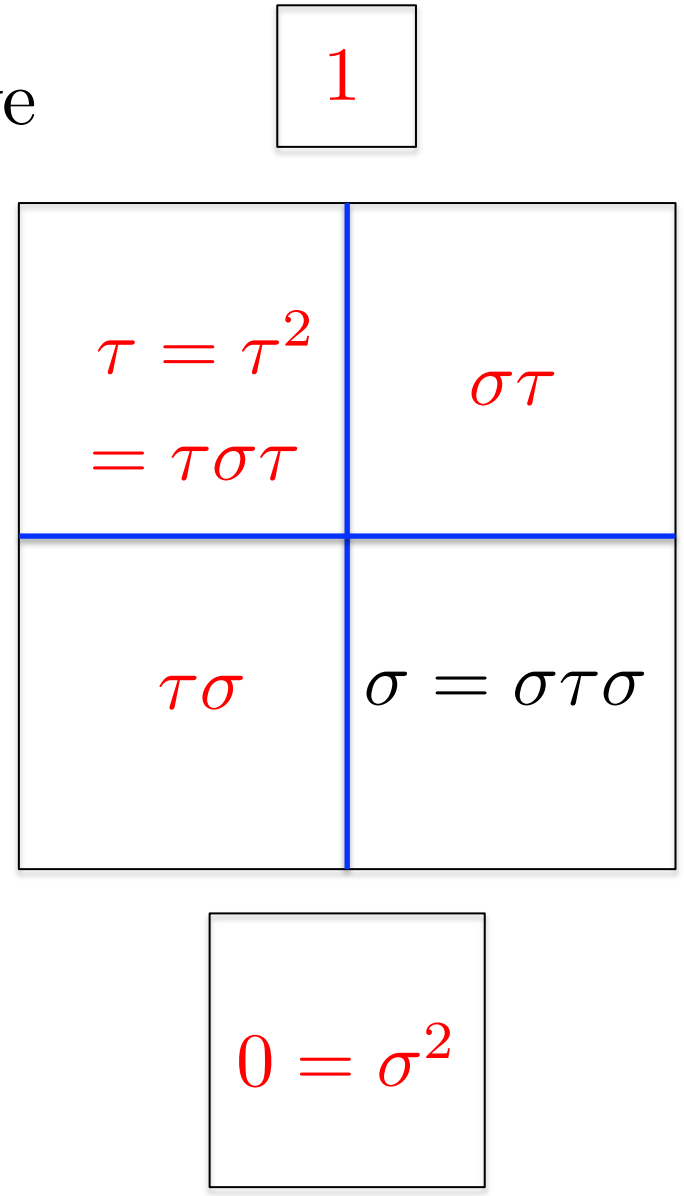
‘Le Produit de Concatenation Non-ambigu’ (1976)

$\Sigma = \{\sigma, \tau\}$, $L = \overline{\Sigma^* \sigma\sigma \Sigma^*}$
(words without two consecutive occurrences of σ.)

$M(L) =$ minimum recognizing monoid (syntactic monoid)

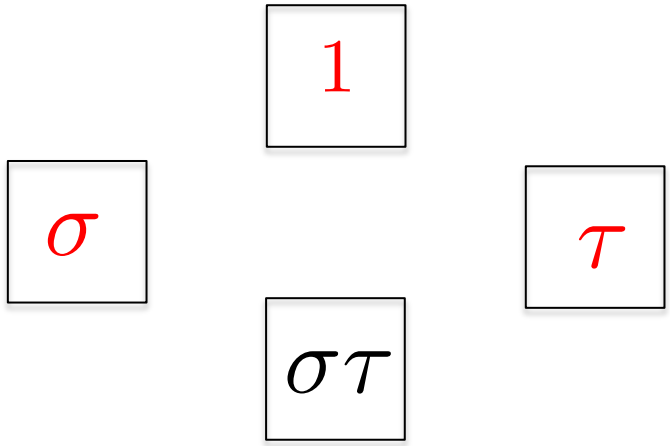
Boxes are classes of elements that generate same ideal ($\mathcal{J}$-classes)

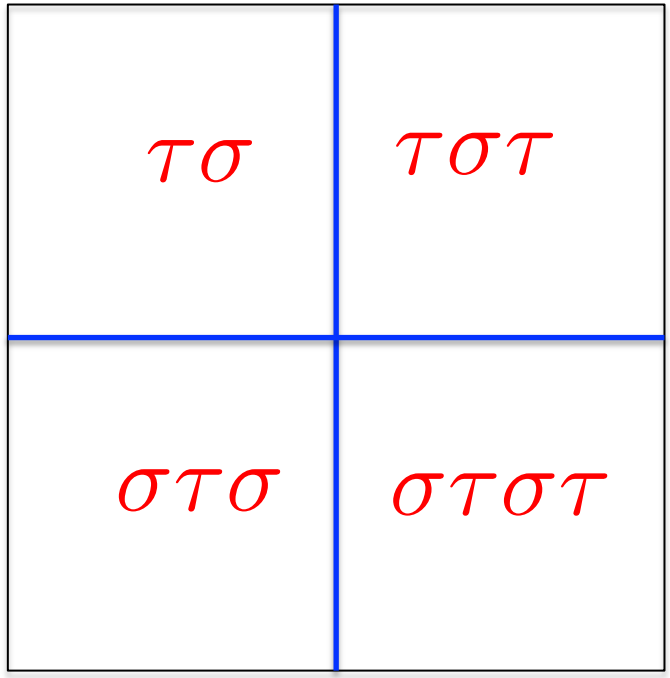
Idempotents in red.



$$L = \sigma^+ \tau \Sigma^* \sigma \tau^+$$

concatenation is *unambiguous*





(Schützenberger, 1976) Variety **DA** of finite monoids.

Every $\mathcal{J}$-class with an idempotent
contains only idempotents.

L is recognized by a monoid in **DA** if and only if
L is built from letters, Γ^* for $\Gamma \subseteq \Sigma$,
by closing under boolean operations and unambiguous
concatenation $L_1, L_2 \mapsto L_1 L_2$.

The block product (in contrast to the wreath product) is not associative.

What if we turn it inside-out?

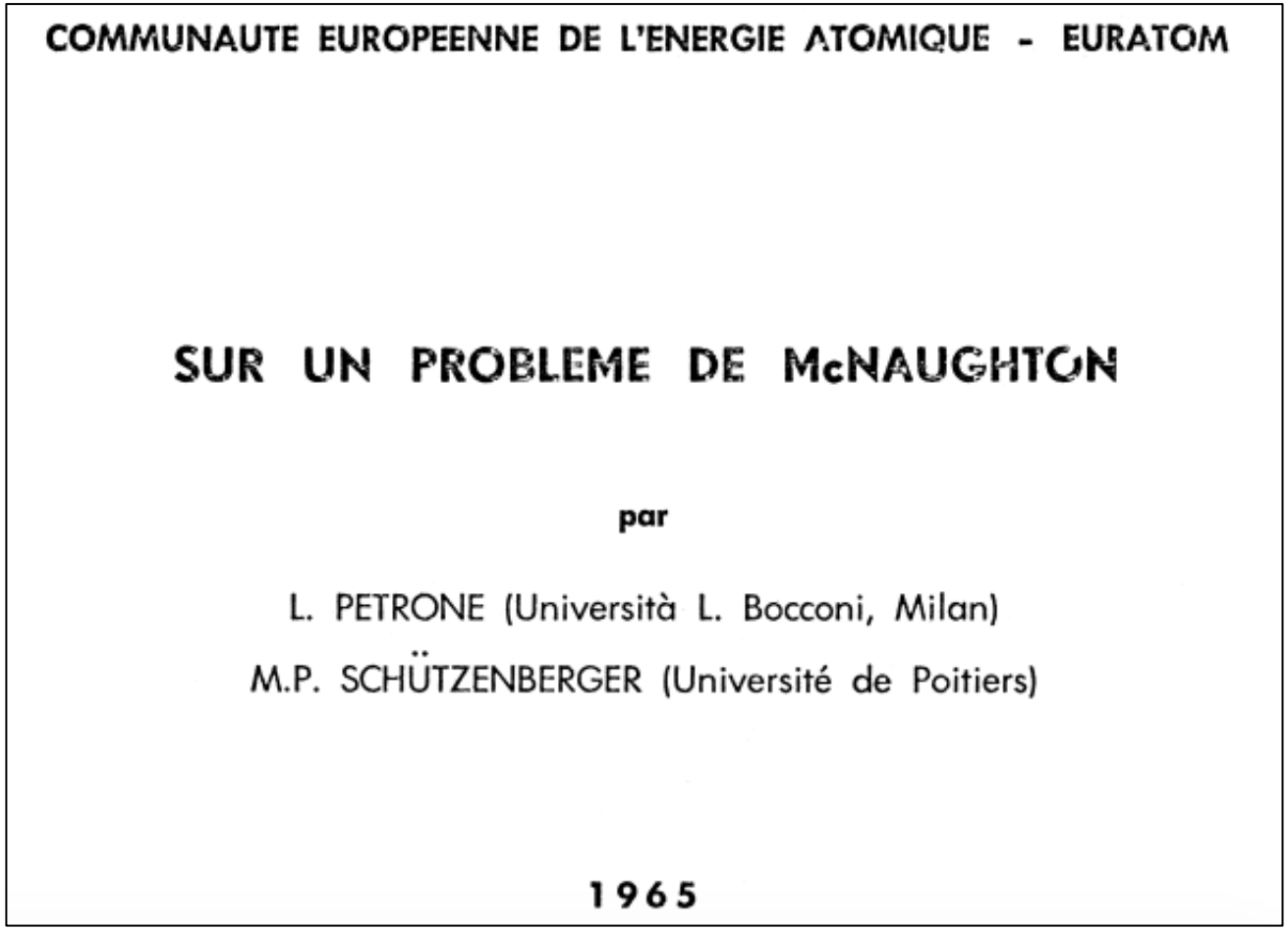
What do we get from

$$(\cdots((U_1 \square U_1)\square U_1)\cdots)\square U_1 \ ?$$

Answer: **DA** *(Straubing and Thérien, 2002)*

Connections with Logic

Connections with Logic



COMMUNAUTE EUROPEENNE DE L'ENERGIE ATOMIQUE - EURATOM

SUR UN PROBLEME DE McNAUGHTON

par

L. PETRONE (Università L. Bocconi, Milan)

M.P. SCHÜTZENBERGER (Université de Poitiers)

1965

First-order descriptions of regular languages

$\Sigma^*\sigma\Sigma^*$: $\quad \exists x \sigma(x)$

$\overline{\Sigma^*\sigma\sigma\Sigma^*}$: $\neg\exists x \exists y \big[\sigma(x) \wedge \sigma(y) \wedge x < y \wedge \forall z(z \leq x \vee y \leq z)\big]$

$L \subseteq \Sigma^*$ is star-free if and only if L is first-order definable

$L, L' \subseteq \Sigma^*$ defined by ψ_1, ψ_2

$L\sigma L'$ defined by $\exists x(\sigma(x) \wedge \psi_1^{<x} \wedge \psi_2^{>x})$

where $\psi^{<x}$ is obtained from ψ by globally replacing
$\exists t\phi$ by $\exists t(t < x \wedge \phi)$
and
$\forall t\phi$ by $\forall t(t < x \rightarrow \phi)$

(Immerman, Kozen) Every first-order sentence over $<$ is equivalent to one using only three variables.

What can you define with *two* variables?

$\sigma^+\tau\Sigma^*\tau\sigma^+$:

$$\begin{aligned}
\exists x\big[\tau(x) \quad &\wedge \quad \forall y(y < x \to \sigma(y)) \\
&\wedge \quad \exists y(y < x) \\
&\wedge \quad \exists y\{x < y \wedge \tau(y) \\
&\qquad \wedge \forall x(y < x \to \sigma(y)) \\
&\qquad \wedge \exists x(y < x)\}\big]
\end{aligned}$$

(*Thérien-Wilke*) L is definable by a two-variable sentence if and only if it is recognized by a monoid in **DA**.

How this follows from our block-product decomposition:

L recognized by $M \square U_1$:

$\sigma_1 \cdots \sigma_n \mapsto b_1 \cdots b_n \in \{0,1\}^*$
$\mapsto (1, b_1, b_2 \cdots b_n) \cdots (b_1 \cdots b_{n-1}, b_n, 1) \in (U_1 \times \{0,1\} \times U_1)^* = \Gamma^*$
$\to M$

Accepted if and only if result satisfies a two-variable sentence ψ over Γ

Replace each atomic formula $\gamma(x)$, $\gamma \in \Gamma$ of ψ by

(supposing $\gamma = (0, 1, 1)$):

$$\exists y(y < x \wedge 0(y)) \wedge 1(x) \wedge \forall y(x < y \rightarrow 1(y)).$$

The result is still a two-variable sentence.

Variations on a Theme:

(Krebs, Straubing, 2012): Algebraic characterization of quantifier alternation depth in two-variable logic.

L has alternation depth $\leq k$ if and only if recognized by

$$(\cdots(M\Box M)\cdots\Box M)\Box M)$$

where M has 1-element $\mathcal{J}$-classes.

Used to prove computability of alternation depth for 2-variable logic.
(Independently proved by Kufleitner and Weil.)

Variations on a Theme:

What can you define if you sneak betweenness back into 2-variable logic?

New relation symbols:

$\sigma(x, y)$

means

$\exists z(x < z < y \wedge \sigma(z))$

(Krebs, Lodaya, Pandya, Straubing, 2016):
(Partial) algebraic characterization of this logic.