50 years of the Krohn-Rhodes theorem

Kamal Lodaya

The Institute of Mathematical Sciences, Chennai

50 years of IMSc

Awkward example (Pitts and Stark 1998)

```
class K1 (m1:comm → comm) =
local int x; init x := 0;
method m1(c) =
(x := 1; c; if x ≠ 1 then diverge)
end K1

class K2 (m2:comm → comm) =
local int x; init x := 0;
method m2(c) = (c)
end K2
```

Claim. K1, K2 have the same meaning.
How do we prove this?

More awkward example (Dreyer et al 2010)

```
class K1 (m1:comm → comm) =
local int x; init x := 0;
method m1(c) =
(x := 0; c; x := 1; c; if x ≠ 1 then diverge)
end K1

class K2 (m2:comm → comm)
local int x; init x := 0;
method m2(c) = (c;c)
end K2
```

Claim. K1, K2 have the same meaning.
How do we prove this?

More awkward example (Dreyer et al 2010)

```
class K1 (m1:comm → comm) =
local int x; init x := 0;
method m1(c) =
(x := 0; c; x := 1; c; if x ≠ 1 then diverge)
end K1

class K2 (m2:comm → comm)
local int x; init x := 0;
method m2(c) = (c;c)
end K2
```

Claim. K1, K2 have the same meaning.
How do we prove this?
Solved by (Dreyer, Neis and Birkedal, ICFP 2010) using operational methods, and by (Reddy and Dunphy, Icalp 2012) using denotational methods.

Some dates

- Reddy and Dunphy in 2012 extend a semantics developed by (Reynolds, 1981) and (Oles, 1985)
- They use the idea of parametric polymorphism developed by (Reynolds, IFIP 1983), first used in this kind of semantics by (O'Hearn and Tennent, 1992)
- Parametricity uses logical relations developed in Plotkin's notes, 1973, based on ideas in (Tait, 1967)

Some dates

- Reddy and Dunphy in 2012 extend a semantics developed by (Reynolds, 1981) and (Oles, 1985)
- They use the idea of parametric polymorphism developed by (Reynolds, IFIP 1983), first used in this kind of semantics by (O'Hearn and Tennent, 1992)
- Parametricity uses logical relations developed in Plotkin's notes, 1973, based on ideas in (Tait, 1967)
- Bisimulation developed by Park around 1980 is a close relative of logical relations
- An earlier idea was zigzag relations in van Benthem's thesis, 1974, 1983
- van Benthem's definition is a relational generalization of that of p-morphisms in Segerberg's thesis, 1968, 1970
- One of the first ideas in this direction is that of weak homomorphisms of automata (Ginzburg and Yoeli, 1965)

Some dates

- Reddy and Dunphy in 2012 extend a semantics developed by (Reynolds, 1981) and (Oles, 1985)
- They use the idea of parametric polymorphism developed by (Reynolds, IFIP 1983), first used in this kind of semantics by (O'Hearn and Tennent, 1992)
- Parametricity uses logical relations developed in Plotkin's notes, 1973, based on ideas in (Tait, 1967)
- Bisimulation developed by Park around 1980 is a close relative of logical relations
- An earlier idea was zigzag relations in van Benthem's thesis, 1974, 1983
- van Benthem's definition is a relational generalization of that of p-morphisms in Segerberg's thesis, 1968, 1970
- One of the first ideas in this direction is that of weak homomorphisms of automata (Ginzburg and Yoeli, 1965)
- The corresponding idea of division of monoids appears in the theses of Krohn and of Rhodes, 1962

Some dates

- 1954-55 Edwin Moore and George Mealy (automata)
- 1956 Stephen Kleene (expressions)
- 1957-58 John Myhill and Anil Nerode (monoids)
- 1958 Michael Rabin and Dana Scott (automata)
- 1960-62 Richard Büchi (logic)
- 1962-65 Kenneth Krohn and John Rhodes (monoids)
- 1965 Marcel-Paul Schützenberger (monoids)
- 1966 Robert McNaughton (logic)
- 1965-66 Stål Aanderaa and Arto Salomaa (expressions)
- 1966 Corrado Böhm and Giuseppe Jacopini (expressions)
- 1970 Charles Wells (categories)

Transition systems and monoids

- $(Q, \delta : Q \times A \to Q)$
- Alternately $\delta : A \to Q^Q$
- Morphism $\delta^* : (A^*, ., \varepsilon) \to (Q^Q, \circ, Id)$
  $\delta^*(\varepsilon) = Id, \delta^*(wx) = \delta^*(w)\delta^*(x)$
- Subset construction: $(Q, \delta \subseteq Q \times A \times Q)$, morphism
  $\delta^* : (A^*, ., \varepsilon) \to (\wp(Q \times Q), \circ, Id)$

Transition systems and monoids

- $(Q, \delta : Q \times A \to Q)$
- Alternately $\delta : A \to Q^Q$
- Morphism $\delta^* : (A^*, ., \varepsilon) \to (Q^Q, \circ, Id)$
  $\delta^*(\varepsilon) = Id, \delta^*(wx) = \delta^*(w)\delta^*(x)$
- Subset construction: $(Q, \delta \subseteq Q \times A \times Q)$, morphism
  $\delta^* : (A^*, ., \varepsilon) \to (\wp(Q \times Q), \circ, Id)$
- Right action $(Q, .)$ of monoid A^* acting on Q
  $q.1 = q, q.(wx) = (q.w).x$
- Product construction: Given $(P, .)$ and $(Q, .)$, right action on $P \times Q$ given by $(p, q).a = (p.a, q.a)$

Transition systems and monoids

- $(Q, \delta : Q \times A \to Q)$
- Alternately $\delta : A \to Q^Q$
- Morphism $\delta^* : (A^*, ., \varepsilon) \to (Q^Q, \circ, Id)$
  $\delta^*(\varepsilon) = Id, \delta^*(wx) = \delta^*(w)\delta^*(x)$
- Subset construction: $(Q, \delta \subseteq Q \times A \times Q)$, morphism
  $\delta^* : (A^*, ., \varepsilon) \to (\wp(Q \times Q), \circ, Id)$
- Right action $(Q, .)$ of monoid A^* acting on Q
  $q.1 = q, q.(wx) = (q.w).x$
- Product construction: Given $(P, .)$ and $(Q, .)$, right action on $P \times Q$ given by $(p, q).a = (p.a, q.a)$
- $L \subseteq A^*$ is recognized by $L = (\delta^*)^{-1}(\{q_0\} \times Q_f)$
- Generalizing, L recognized by morphism h from a finitely generated monoid into monoid S if for some $S_f \subseteq S$,
  $L = h^{-1}(S_f)$

Mealy machines and transducers

- $(Q, \delta, \beta : Q \times A \to B^*)$
- Alternately $\beta : A \to (B^*)^Q$
- Morphism $\beta^* : (A^*, ., \varepsilon) \to ((B^*)^Q, \circ, \overline{\varepsilon})$,
  $\beta^*(\varepsilon)(q) = \overline{\varepsilon}, \beta^*(wx)(q) = \beta^*(w)(q)\beta^*(x)(\delta^*(w)(q))$
- Right actions $(Q, ., *)$, monoid A^* acting on $(B^*)^Q$
  $q * 1 = \overline{1}, q * (wx) = (q * w)((q.w) * x)$, realizing a sequential function from A^* to B^*
- Alternately right action of monoid A^* acting on $(B^*)^Q \times Q$
  $(f, q).1 = (f, q), (f, q).(wx) = (f(q)(w)f(q.w)(x), (q.w).x)$

Composition of Mealy machines

- Let $M_{BC} = (P, ., *)$ realize a sequential function from B^* to C^* and $M_{AB} = (Q, ., *)$ realize a sequential function from A^* to B^*
- Their composition from A^* to C^* is realized by $(P \times Q, ., *)$ $(p, q).a = (p.(q * a), q.a), (p, q) * a = p * (q * a)$
- Internalizing the intermediate alphabet we get a right action $(B^*)^Q \times A^*$ acting on the product $P \times Q$ using $(p, q).(f, a) = (p.f(q), q.a)$
- If M_{BC}, M_{AB} are minimal automata, we can think of their state sets P, Q as being equivalence classes labelled by $(B^*)^Q$ and A^* respectively, hence $(B^*)^{A^*}$ and A^*
- More generally, given monoids S and T, we have to consider for the composition $S^T \times T$

Wreath product of monoids

- Let (P, S) and (Q, T) be transformation monoids, more generally S a monoid and T a right action on a set Q
- Define $F = S^Q$ and let $(tf)(q) = f(qt)$ for $t \in T$ be the right action T on Q seen as a left action by T on F
- Now we get a monoid $F \times T$ with a right action $F \times T$ (so just a monoid, not necessarily a transformation monoid) $(f, t).(g, u) = (f.(tg), t.u)$
- Associative, so $F \times T$ is a monoid under this operation

Wreath product of monoids

- Let (P, S) and (Q, T) be transformation monoids, more generally S a monoid and T a right action on a set Q
- Define $F = S^Q$ and let $(tf)(q) = f(qt)$ for $t \in T$ be the right action T on Q seen as a left action by T on F
- Now we get a monoid $F \times T$ with a right action $F \times T$ (so just a monoid, not necessarily a transformation monoid) $(f, t).(g, u) = (f.(tg), t.u)$
- Associative, so $F \times T$ is a monoid under this operation
- More generally such a submonoid of $S^T \times T$ is called the wreath product monoid $S \wr T$
- (Straubing 1979) If S recognizes L and T recognizes K, there is a sequential function (realized by a transducer) τ such that $S \wr T$ recognizes $\tau^{-1}(L) \cap K$
- Example: Sequential composition $K; L$

Covering of automata and division of monoids

- $M = (Q, .)$ is covered by $M' = (Q', .)$, written $M \leq M'$, if there is a partial onto function $f : Q' \to Q$ such that when $f(q').a$ is defined, it is equal to $f(q'.a)$
- $M = (Q, .)$ is covered by $M' = (Q', .)$, written $M \leq M'$, if there is an onto relation $r \subseteq Q' \times Q$ such that $r(q').a \subseteq r(q'.a)$
- Generalizing, monoid S divides monoid T, written $S \leq T$, if S is the morphic image of a submonoid of T

Covering of automata and division of monoids

- $M = (Q, .)$ is covered by $M' = (Q', .)$, written $M \leq M'$, if there is a partial onto function $f : Q' \to Q$ such that when $f(q').a$ is defined, it is equal to $f(q'.a)$
- $M = (Q, .)$ is covered by $M' = (Q', .)$, written $M \leq M'$, if there is an onto relation $r \subseteq Q' \times Q$ such that $r(q').a \subseteq r(q'.a)$
- Generalizing, monoid S divides monoid T, written $S \leq T$, if S is the morphic image of a submonoid of T

Theorem (Jordan 1870, Hölder 1890, Krohn-Rhodes)

1. *Every finite group can be written as a composition series of simple groups which are its factors.*
2. *This is unique upto permutation and isomorphism.*
3. *Every finite group divides a series of wreath products of simple groups which divide it; that is,* $G \leq G_1 \wr G_2 \wr \cdots \wr G_n$*, where each* G_i *is a simple group dividing* G*.*

Decomposition

Theorem (Kleene 1956)

The language of any finite automaton can be described by a regular expression using letters, sequencing, choice and iteration operations.

Theorem (Krohn and Rhodes 1962, 1963, 1965)

Every finite monoid divides a series of wreath products of simple groups and the groupfree monoid U2; that is,
$S \leq G_{11} \wr \cdots \wr G_{1j_1} \wr U_{11} \wr \cdots \wr U_{1k_1} \wr \cdots \wr G_{n1} \wr \cdots \wr G_{nj_n} \wr U_{n1} \wr \cdots \wr U_{nk_n}$,
where each G_{ij} is a simple group dividing S and each U_{ij} is a copy of U2.

Theorem (Böhm and Jacopini 1966)

Every flowchart program can be converted into an equivalent program using only assignments, sequencing, choice (if-then-else) and iteration (while-do) commands.