Circuit Evaluation for Finite Semirings

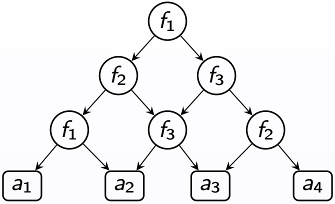
CSA 2016

Markus Lohrey
University of Siegen

joint work with Moses Ganardi, Danny Hucke, and Daniel König

Circuits over algebraic structures

$\mathcal{A} = (A, f_1, \dots, f_m), \quad f_i : A^{r_i} \to A$



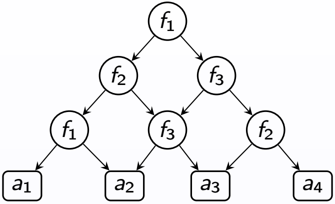
Circuit $\mathcal{C}$ over $\mathcal{A}$

- set of gates
- output gate
- $X = a \quad (a \in A)$ or $X = f_i(X_1, \dots, X_r)$

  constant gates inner gates

Circuits over algebraic structures

$\mathcal{A} = (A, f_1, \ldots, f_m), \quad f_i : A^{r_i} \to A$



Circuit $\mathcal{C}$ over $\mathcal{A}$

- set of gates
- output gate
- $X = a \quad (a \in A)$ or $X = f_i(X_1, \ldots, X_r)$

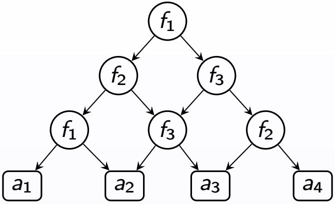
constant gates inner gates

Circuit Evaluation Problem CEP($\mathcal{A}$)

Input: circuit $\mathcal{C}$ over $\mathcal{A}$
Compute: value of output gate of $\mathcal{C}$

Circuits over algebraic structures

$\mathcal{A} = (A, f_1, \ldots, f_m), \quad f_i : A^{r_i} \to A$



Circuit $\mathcal{C}$ over $\mathcal{A}$

- set of gates
- output gate
- $X = a \quad (a \in A)$ or $X = f_i(X_1, \ldots, X_r)$

constant gates inner gates

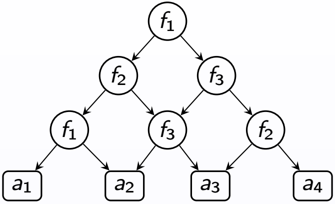
Circuit Evaluation Problem CEP($\mathcal{A}$)

Input: circuit $\mathcal{C}$ over $\mathcal{A}$
Compute: value of output gate of $\mathcal{C}$

Goal: Classify structures $\mathcal{A}$ according to the complexity of CEP($\mathcal{A}$)

Circuits over algebraic structures

$\mathcal{A} = (A, f_1, \ldots, f_m), \quad f_i : A^{r_i} \to A$



Circuit $\mathcal{C}$ over $\mathcal{A}$

- set of gates
- output gate
- $\underbrace{X = a \quad (a \in A)}_{\text{constant gates}}$ or $\underbrace{X = f_i(X_1, \ldots, X_r)}_{\text{inner gates}}$

Circuit Evaluation Problem CEP($\mathcal{A}$)

Input: circuit $\mathcal{C}$ over $\mathcal{A}$
Compute: value of output gate of $\mathcal{C}$

Goal: Classify structures $\mathcal{A}$ according to the complexity of CEP($\mathcal{A}$)

If $\mathcal{A}$ is finite, then CEP($\mathcal{A}$) is clearly in **P** (= polynomial time).

Parallel Complexity Theory

- **P** class of problems which can be solved in time $n^{O(1)}$.

Parallel Complexity Theory

- **P** class of problems which can be solved in time $n^{O(1)}$.
- **NC** class of problems which have efficient parallel algorithms

Parallel Complexity Theory

- **P** class of problems which can be solved in time $n^{O(1)}$.
- **NC** class of problems which have efficient parallel algorithms
- efficient parallel algorithm: time $(\log n)^{O(1)}$ on a PRAM with $n^{O(1)}$ processors

Parallel Complexity Theory

- **P** class of problems which can be solved in time $n^{O(1)}$.
- **NC** class of problems which have efficient parallel algorithms
- efficient parallel algorithm: time $(\log n)^{O(1)}$ on a PRAM with $n^{O(1)}$ processors
- Clearly $\mathbf{NC} \subseteq \mathbf{P}$

Parallel Complexity Theory

- **P** class of problems which can be solved in time $n^{O(1)}$.
- **NC** class of problems which have efficient parallel algorithms
- efficient parallel algorithm: time $(\log n)^{O(1)}$ on a PRAM with $n^{O(1)}$ processors
- Clearly $\mathbf{NC} \subseteq \mathbf{P}$
- The big open problem of parallel complexity theory: $\mathbf{NC} \subsetneq \mathbf{P}$?

Parallel Complexity Theory

- **P** class of problems which can be solved in time $n^{O(1)}$.
- **NC** class of problems which have efficient parallel algorithms
- efficient parallel algorithm: time $(\log n)^{O(1)}$ on a PRAM with $n^{O(1)}$ processors
- Clearly $\mathbf{NC} \subseteq \mathbf{P}$
- The big open problem of parallel complexity theory: $\mathbf{NC} \subsetneq \mathbf{P}$?
- A problem A is **P**-complete if (i) it belongs to **P** and (ii) every problem in **P** can be reduced to A.

Parallel Complexity Theory

- **P** class of problems which can be solved in time $n^{O(1)}$.
- **NC** class of problems which have efficient parallel algorithms
- efficient parallel algorithm: time $(\log n)^{O(1)}$ on a PRAM with $n^{O(1)}$ processors
- Clearly $\mathbf{NC} \subseteq \mathbf{P}$
- The big open problem of parallel complexity theory: $\mathbf{NC} \subsetneq \mathbf{P}$?
- A problem A is **P**-complete if (i) it belongs to **P** and (ii) every problem in **P** can be reduced to A.
- If $\mathbf{NC} \subsetneq \mathbf{P}$ then **P**-complete do not belong to **NC** (inherently sequential problems)

Parallel Complexity Theory

- **P** class of problems which can be solved in time $n^{O(1)}$.
- **NC** class of problems which have efficient parallel algorithms
- efficient parallel algorithm: time $(\log n)^{O(1)}$ on a PRAM with $n^{O(1)}$ processors
- Clearly $\mathbf{NC} \subseteq \mathbf{P}$
- The big open problem of parallel complexity theory: $\mathbf{NC} \subsetneq \mathbf{P}$?
- A problem A is **P**-complete if (i) it belongs to **P** and (ii) every problem in **P** can be reduced to A.
- If $\mathbf{NC} \subsetneq \mathbf{P}$ then **P**-complete do not belong to **NC** (inherently sequential problems)

New goal: For which structures $\mathcal{A}$ is $\mathrm{CEP}(\mathcal{A})$ in **NC** (resp., **P**-complete)?

Parallel Complexity Theory

- **P** class of problems which can be solved in time $n^{O(1)}$.
- **NC** class of problems which have efficient parallel algorithms
- efficient parallel algorithm: time $(\log n)^{O(1)}$ on a PRAM with $n^{O(1)}$ processors
- Clearly $\mathbf{NC} \subseteq \mathbf{P}$
- The big open problem of parallel complexity theory: $\mathbf{NC} \subsetneq \mathbf{P}$?
- A problem A is **P**-complete if (i) it belongs to **P** and (ii) every problem in **P** can be reduced to A.
- If $\mathbf{NC} \subsetneq \mathbf{P}$ then **P**-complete do not belong to **NC** (inherently sequential problems)

New goal: For which structures $\mathcal{A}$ is $\mathrm{CEP}(\mathcal{A})$ in **NC** (resp., **P**-complete)?

Are there structures $\mathcal{A}$ such that $\mathrm{CEP}(\mathcal{A})$ is neither in **NC** nor **P**-complete?

P-complete circuit evulation problems.

Theorem [Ladner, 1975]

Circuit evaluation problem for the boolean semiring $\mathbb{B}_2 = (\{0,1\}, \vee, \wedge)$ is **P**-complete.

$\mathbf{P}$-complete circuit evulation problems.

Theorem [Ladner, 1975]

Circuit evaluation problem for the boolean semiring $\mathbb{B}_2 = (\{0, 1\}, \vee, \wedge)$ is $\mathbf{P}$-complete.

A semigroup S is solvable if every group in S is solvable.

Theorem [Beaudry et al., 1993, based on Krohn, Maurer, Rhodes, 1966]

Let $\mathcal{S}$ be a finite semigroup.

- If $\mathcal{S}$ is solvable, then CEP($\mathcal{S}$) is in $\mathbf{NC}$
- otherwise it is $\mathbf{P}$-complete.

Circuits over Semirings

Question: For which semirings $\mathcal{R}$ is $\mathsf{CEP}(\mathcal{R})$ in **NC**?

Circuits over Semirings

Question: For which semirings $\mathcal{R}$ is CEP($\mathcal{R}$) in **NC**?

Semiring $\mathcal{R} = (R, +, \cdot)$

- $(R, +)$ commutative semigroup
- $(R, \cdot)$ semigroup
- left- and right-distributivity

Circuits over Semirings

Question: For which semirings $\mathcal{R}$ is CEP($\mathcal{R}$) in **NC**?

Semiring $\mathcal{R} = (R, +, \cdot)$

- $(R, +)$ commutative semigroup
- $(R, \cdot)$ semigroup
- left- and right-distributivity

Example: Power semirings

finite semigroup $\mathcal{S}$ $\longmapsto$ $\mathcal{P}(\mathcal{S}) = (2^S \setminus \{\varnothing\}, \cup, \cdot)$
where $A \cdot B = \{ab \mid a \in A,\ b \in B\}$

Circuits over Semirings

Question: For which semirings $\mathcal{R}$ is $\mathsf{CEP}(\mathcal{R})$ in **NC**?

Semiring $\mathcal{R} = (R, +, \cdot)$

- $(R, +)$ commutative semigroup
- $(R, \cdot)$ semigroup
- left- and right-distributivity

Example: Power semirings

finite semigroup $\mathcal{S}$ $\quad\longmapsto\quad$ $\mathcal{P}(\mathcal{S}) = (2^S \setminus \{\varnothing\}, \cup, \cdot)$

where $A \cdot B = \{ab \mid a \in A,\ b \in B\}$

Why exclude $\varnothing$?

Let $e \in S$ be an idempotent element, i.e. $e \cdot e = e$.

Circuits over Semirings

Question: For which semirings $\mathcal{R}$ is CEP($\mathcal{R}$) in **NC**?

Semiring $\mathcal{R} = (R, +, \cdot)$

- $(R, +)$ commutative semigroup
- $(R, \cdot)$ semigroup
- left- and right-distributivity

Example: Power semirings

finite semigroup $\mathcal{S}$ $\longmapsto$ $\mathcal{P}(\mathcal{S}) = (2^S \setminus \{\varnothing\}, \cup, \cdot)$

where $A \cdot B = \{ab \mid a \in A,\ b \in B\}$

Why exclude $\varnothing$?

Let $e \in S$ be an idempotent element, i.e. $e \cdot e = e$.
Then $\{\varnothing, \{e\}\} \cong \mathbb{B}_2$!

Circuits over Semirings

Question: For which semirings $\mathcal{R}$ is $\mathrm{CEP}(\mathcal{R})$ in **NC**?

Semiring $\mathcal{R} = (R, +, \cdot)$

- $(R, +)$ commutative semigroup
- $(R, \cdot)$ semigroup
- left- and right-distributivity

Example: Power semirings

finite semigroup $\mathcal{S}$ $\longmapsto$ $\mathcal{P}(\mathcal{S}) = (2^S \setminus \{\varnothing\}, \cup, \cdot)$

where $A \cdot B = \{ab \mid a \in A,\ b \in B\}$

Why exclude $\varnothing$?

Let $e \in S$ be an idempotent element, i.e. $e \cdot e = e$.
Then $\big\{\varnothing, \{e\}\big\} \cong \mathbb{B}_2$!

Question: For which semigroups $\mathcal{S}$ is $\mathrm{CEP}(\mathcal{P}(\mathcal{S}))$ in **NC**?

Circuits over Semirings

(Easy) **P**-complete examples

- $\mathbb{B}_2 = (\{0, 1\}, \vee, \wedge)$

Circuits over Semirings

(Easy) **P**-complete examples

- $\mathbb{B}_2 = (\{0,1\}, \vee, \wedge)$
- $(\mathbb{Z}_d, +, \cdot)$ for $d \geq 2$

Circuits over Semirings

(Easy) **P**-complete examples

- $\mathbb{B}_2 = (\{0,1\}, \vee, \wedge)$
- $(\mathbb{Z}_d, +, \cdot)$ for $d \geq 2$

$$x \wedge y \;\to\; x \cdot y \qquad\qquad \neg x \;\to\; 1 + (d-1) \cdot x$$

Circuits over Semirings

(Easy) **P**-complete examples

- $\mathbb{B}_2 = (\{0,1\}, \vee, \wedge)$
- $(\mathbb{Z}_d, +, \cdot)$ for $d \geq 2$

$$x \wedge y \;\to\; x \cdot y \qquad\qquad \neg x \;\to\; 1 + (d-1) \cdot x$$

- finite semirings with additive identity 0
  and multiplicative identity $1 \neq 0$

Circuits over Semirings

(Easy) **P**-complete examples

- $\mathbb{B}_2 = (\{0,1\}, \vee, \wedge)$
- $(\mathbb{Z}_d, +, \cdot)$ for $d \geq 2$

$$x \wedge y \;\rightarrow\; x \cdot y \qquad\qquad \neg x \;\rightarrow\; 1 + (d-1) \cdot x$$

- finite semirings with additive identity 0
  and multiplicative identity $1 \neq 0$

Circuits over Semirings

(Easy) **P**-complete examples

- $\mathbb{B}_2 = (\{0,1\}, \vee, \wedge)$
- $(\mathbb{Z}_d, +, \cdot)$ for $d \geq 2$

$$x \wedge y \ \rightarrow \ x \cdot y \qquad\qquad \neg x \ \rightarrow \ 1 + (d-1) \cdot x$$

- finite semirings with additive identity 0
  and multiplicative identity $1 \neq 0$

contains either $\mathbb{B}_2$ or $\mathbb{Z}_d$ for some $d \geq 2$

Circuits over Semirings

(Easy) **P**-complete examples

- $\mathbb{B}_2 = (\{0,1\}, \vee, \wedge)$
- $(\mathbb{Z}_d, +, \cdot)$ for $d \geq 2$

$$x \wedge y \;\to\; x \cdot y \qquad\qquad \neg x \;\to\; 1 + (d-1) \cdot x$$

- finite semirings with additive identity 0
  and multiplicative identity $1 \neq 0$

contains either $\mathbb{B}_2$ or $\mathbb{Z}_d$ for some $d \geq 2$

The semiring $\mathcal{R} = (R, +, \cdot)$ is $\{0,1\}$-free if it contains no subsemiring with an additive 0 and a multiplicative $1 \neq 0$.

Main Theorem

Theorem

Let $\mathcal{R}$ be a finite semiring.

- If $\mathcal{R}$ is $\{0, 1\}$-free and $(R, \cdot)$ is solvable, then $\mathrm{CEP}(\mathcal{R})$ is in **NC**
- otherwise it is **P**-complete.

Main Theorem

Theorem

Let $\mathcal{R}$ be a finite semiring.

- If $\mathcal{R}$ is $\{0,1\}$-free and $(R,\cdot)$ is solvable, then $\mathsf{CEP}(\mathcal{R})$ is in **NC**
- otherwise it is **P**-complete.

Using results from semigroup theory:

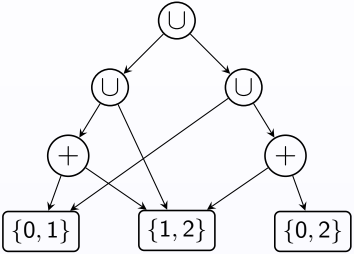
Corollary

Let $\mathcal{S}$ be a finite semigroup.

- If $\mathcal{S}$ is a local group and solvable, then $\mathsf{CEP}(\mathcal{P}(\mathcal{S}))$ is in **NC**
- otherwise it is **P**-complete.

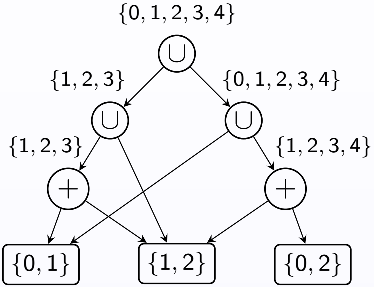
Power semiring over a finite group G

Example: $G = (\mathbb{Z}_5, +)$



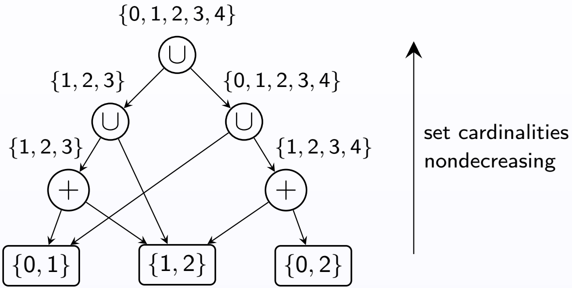
Power semiring over a finite group G

Example: $G = (\mathbb{Z}_5, +)$



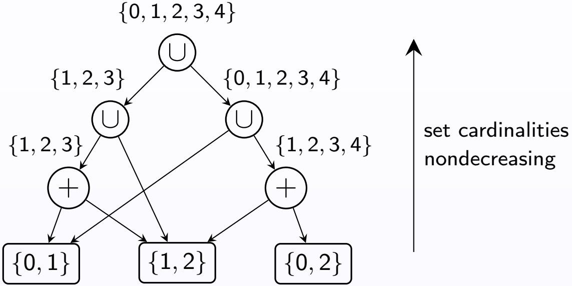
Power semiring over a finite group G

Example: $G = (\mathbb{Z}_5, +)$



Power semiring over a finite group G

Example: $G = (\mathbb{Z}_5, +)$



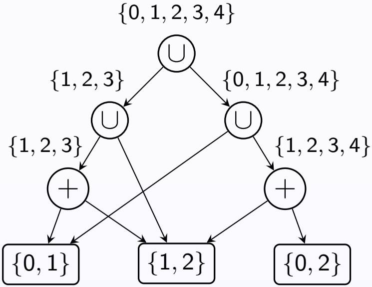
Parallel Evaluation Algorithm

for $k = 1, \ldots, |G|$ **do**

evaluate all gates whose value has size k

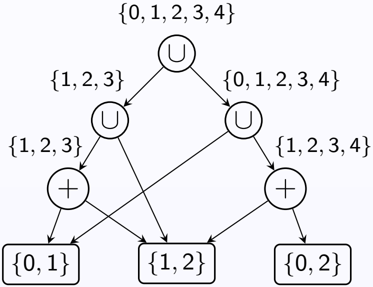
endfor

Invariant: After k-th round all sets of size $\leq k$ are evaluated.



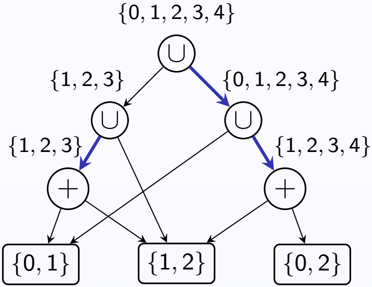
Invariant: After k-th round all sets of size $\leq k$ are evaluated.

1. Evaluate maximal $\cup$-subcircuits



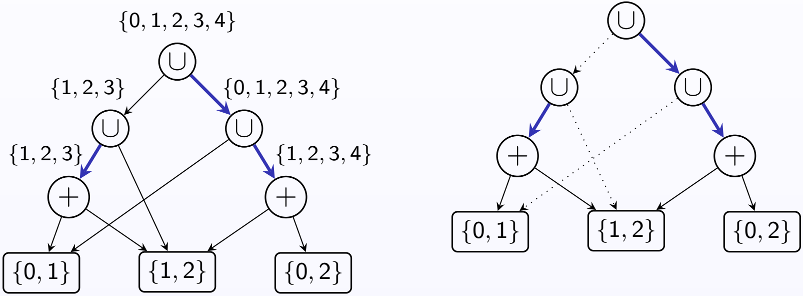
Invariant: After k-th round all sets of size $\leq k$ are evaluated.

1. Evaluate maximal $\cup$-subcircuits
   $\Longrightarrow$ every $\cup$-gate has inner input gate



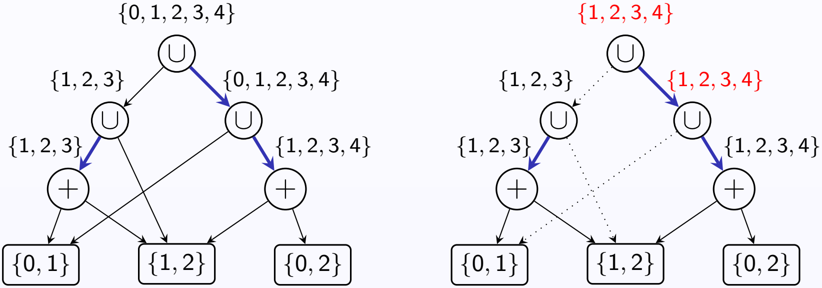
Invariant: After k-th round all sets of size $\leq k$ are evaluated.

1. Evaluate maximal $\cup$-subcircuits
   $\implies$ every $\cup$-gate has inner input gate
2. $\cup$-gate copies inner input gate



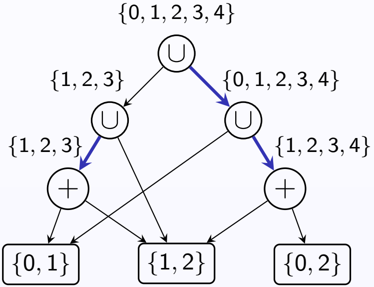
Invariant: After k-th round all sets of size $\leq k$ are evaluated.

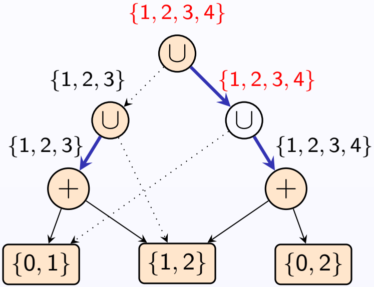
1. Evaluate maximal $\cup$-subcircuits
   $\implies$ every $\cup$-gate has inner input gate
2. $\cup$-gate copies inner input gate
   $\implies$ evaluate multiplicative circuit



Invariant: After k-th round all sets of size $\leq k$ are evaluated.

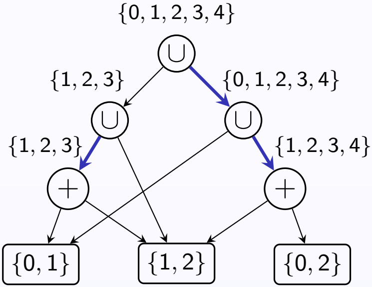
1. Evaluate maximal $\cup$-subcircuits
   $\implies$ every $\cup$-gate has inner input gate
2. $\cup$-gate copies inner input gate
   $\implies$ evaluate multiplicative circuit
3. Find locally correct gates

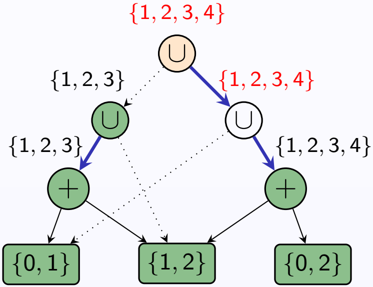




Invariant: After k-th round all sets of size $\leq k$ are evaluated.

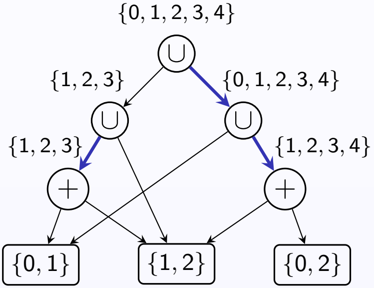
1. Evaluate maximal $\cup$-subcircuits
   $\implies$ every $\cup$-gate has inner input gate
2. $\cup$-gate copies inner input gate
   $\implies$ evaluate multiplicative circuit
3. Find locally correct gates
4. X has correct value if all gates below X are locally correct

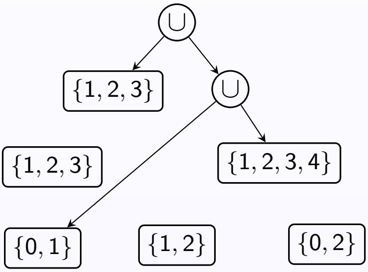




Invariant: After k-th round all sets of size $\leq k$ are evaluated.

1. Evaluate maximal $\cup$-subcircuits
   $\implies$ every $\cup$-gate has inner input gate
2. $\cup$-gate copies inner input gate
   $\implies$ evaluate multiplicative circuit
3. Find locally correct gates
4. X has correct value if all gates below X are locally correct





rank-functions

The algorithm terminates after $|R|$ rounds if $\mathcal{R}$ has a function $\mathbf{rank} : R \to \mathbb{N}$ with

- $\mathbf{rank}(a) \leq \mathbf{rank}(a+b)$
- $\mathbf{rank}(a), \mathbf{rank}(b) \leq \mathbf{rank}(a \cdot b)$
- If $\mathbf{rank}(a) = \mathbf{rank}(a+b)$, then $a = a+b$.

rank-functions

The algorithm terminates after $|R|$ rounds if $\mathcal{R}$ has a function **rank** : $R \to \mathbb{N}$ with

- $\mathbf{rank}(a) \leq \mathbf{rank}(a+b)$
- $\mathbf{rank}(a), \mathbf{rank}(b) \leq \mathbf{rank}(a \cdot b)$
- If $\mathbf{rank}(a) = \mathbf{rank}(a+b)$, then $a = a+b$.

Example: Power semiring over finite group

- $|A| \leq |A \cup B|$
- $|A|, |B| \leq |A \cdot B|$
- If $|A| = |A \cup B|$, then $A = A \cup B$.

rank-functions

The algorithm terminates after $|R|$ rounds if $\mathcal{R}$ has a function $\mathbf{rank} : R \to \mathbb{N}$ with

- $\mathbf{rank}(a) \leq \mathbf{rank}(a + b)$
- $\mathbf{rank}(a), \mathbf{rank}(b) \leq \mathbf{rank}(a \cdot b)$
- If $\mathbf{rank}(a) = \mathbf{rank}(a + b)$, then $a = a + b$.

Example: Power semiring over finite group

- $|A| \leq |A \cup B|$
- $|A|, |B| \leq |A \cdot B|$
- If $|A| = |A \cup B|$, then $A = A \cup B$.

Lemma

If $\mathcal{R}$ has a **rank**-function and $\mathrm{CEP}(R, \cdot)$ is solvable, then $\mathrm{CEP}(\mathcal{R})$ belongs to **NC**.

rank-functions

Theorem

If $\mathcal{R}$ is $\{0, 1\}$-free and $(R, \cdot)$ is a monoid, then $\mathcal{R}$ has a **rank**-function.

rank-functions

Theorem

If $\mathcal{R}$ is $\{0,1\}$-free and $(R,\cdot)$ is a monoid, then $\mathcal{R}$ has a **rank**-function.

$a \preceq b \iff b$ can be obtained from a by iterated additions/multiplications with elements from R.

rank-functions

Theorem

If $\mathcal{R}$ is $\{0,1\}$-free and $(R,\cdot)$ is a monoid, then $\mathcal{R}$ has a **rank**-function.

$$a \preceq b \iff b \text{ can be obtained from } a \text{ by iterated additions/multiplications with elements from } R.$$

Induced function $\mathbf{rank} : R \to \mathbb{N}$ with

- $\mathbf{rank}(a) = \mathbf{rank}(b)$ iff $a \preceq b \preceq a$
- $\mathbf{rank}(a) \leq \mathbf{rank}(b)$ if $a \preceq b$

rank-functions

Theorem

If $\mathcal{R}$ is $\{0,1\}$-free and $(R,\cdot)$ is a monoid, then $\mathcal{R}$ has a **rank**-function.

$$a \preceq b \iff b \text{ can be obtained from } a \text{ by iterated additions/multiplications with elements from } R.$$

Induced function $\mathbf{rank} : R \to \mathbb{N}$ with

- $\mathbf{rank}(a) = \mathbf{rank}(b)$ iff $a \preceq b \preceq a$
- $\mathbf{rank}(a) \leq \mathbf{rank}(b)$ if $a \preceq b$

Corollary

If $\mathcal{R}$ is $\{0,1\}$-free and $(R,\cdot)$ is a solvable monoid, then $\mathrm{CEP}(\mathcal{R})$ belongs to **NC**.

What if $(R, \cdot)$ is solvable but not a monoid?

Strategy: Reduce the semigroup S generated by circuit input values

What if $(R, \cdot)$ is solvable but not a monoid?

Strategy: Reduce the semigroup S generated by circuit input values

A few semigroup definitions: Let S be a semigroup.

What if $(R, \cdot)$ is solvable but not a monoid?

Strategy: Reduce the semigroup S generated by circuit input values

A few semigroup definitions: Let S be a semigroup.

- Let $E(S)$ be the set of idempotents of S.

What if $(R, \cdot)$ is solvable but not a monoid?

Strategy: Reduce the semigroup S generated by circuit input values

A few semigroup definitions: Let S be a semigroup.

- Let $E(S)$ be the set of idempotents of S.
- Let $E_{\max}(S) \subseteq E(S)$ be obtained by picking from each maximal (w.r.t. $\mathcal{J}$-order) regular $\mathcal{J}$-class of S an idempotent.

What if $(R, \cdot)$ is solvable but not a monoid?

Strategy: Reduce the semigroup S generated by circuit input values

A few semigroup definitions: Let S be a semigroup.

- Let $E(S)$ be the set of idempotents of S.
- Let $E_{\max}(S) \subseteq E(S)$ be obtained by picking from each maximal (w.r.t. $\mathcal{J}$-order) regular $\mathcal{J}$-class of S an idempotent.
- $\mathcal{H}_e = \mathcal{J}_e \cap eSe$ is the maximal subgroup in S with identity e.

What if $(R, \cdot)$ is solvable but not a monoid?

Strategy: Reduce the semigroup S generated by circuit input values

A few semigroup definitions: Let S be a semigroup.

- Let $E(S)$ be the set of idempotents of S.
- Let $E_{\max}(S) \subseteq E(S)$ be obtained by picking from each maximal (w.r.t. $\mathcal{J}$-order) regular $\mathcal{J}$-class of S an idempotent.
- $\mathcal{H}_e = \mathcal{J}_e \cap eSe$ is the maximal subgroup in S with identity e.

Lemma

Assume that the semiring $\mathcal{R}$ is $\{0, 1\}$-free and $(R, \cdot)$ is solvable.

What if $(R, \cdot)$ is solvable but not a monoid?

Strategy: Reduce the semigroup S generated by circuit input values

A few semigroup definitions: Let S be a semigroup.

- Let $E(S)$ be the set of idempotents of S.
- Let $E_{\text{max}}(S) \subseteq E(S)$ be obtained by picking from each maximal (w.r.t. $\mathcal{J}$-order) regular $\mathcal{J}$-class of S an idempotent.
- $\mathcal{H}_e = \mathcal{J}_e \cap eSe$ is the maximal subgroup in S with identity e.

Lemma

Assume that the semiring $\mathcal{R}$ is $\{0, 1\}$-free and $(R, \cdot)$ is solvable.

Let $\mathcal{C}$ be a circuit, $S =$ be the multiplicative semigroup generated by the input values of $\mathcal{C}$, $F = E_{\text{max}}(S)$ and $e \in F$.

What if $(R, \cdot)$ is solvable but not a monoid?

Strategy: Reduce the semigroup S generated by circuit input values

A few semigroup definitions: Let S be a semigroup.

- Let $E(S)$ be the set of idempotents of S.
- Let $E_{\max}(S) \subseteq E(S)$ be obtained by picking from each maximal (w.r.t. $\mathcal{J}$-order) regular $\mathcal{J}$-class of S an idempotent.
- $\mathcal{H}_e = \mathcal{J}_e \cap eSe$ is the maximal subgroup in S with identity e.

Lemma

Assume that the semiring $\mathcal{R}$ is $\{0, 1\}$-free and $(R, \cdot)$ is solvable.

Let $\mathcal{C}$ be a circuit, $S =$ be the multiplicative semigroup generated by the input values of $\mathcal{C}$, $F = E_{\max}(S)$ and $e \in F$.

Then the evaluation $\mathcal{C}$ can be reduced to the evaluation of (a constant number of) circuits with input values from $FSF \setminus \mathcal{H}_e$ (a subsemigroup!).

What if $(R, \cdot)$ is solvable but not a monoid?

Reduction of the input values from S to $FSF \setminus \mathcal{H}_e$ is done in three steps, where $n = |S|$.

$$S \longrightarrow S^n = SES = SFS \longrightarrow FSF \longrightarrow FSF \setminus \mathcal{H}_e,$$

What if $(R, \cdot)$ is solvable but not a monoid?

Reduction of the input values from S to $FSF \setminus \mathcal{H}_e$ is done in three steps, where $n = |S|$.

$$S \longrightarrow S^n = SES = SFS \longrightarrow FSF \longrightarrow FSF \setminus \mathcal{H}_e,$$

In the last step $FSF \setminus \mathcal{H}_e$, we evaluate subcircuits in the ($\{0, 1\}$-free) subsemiring eRe.

What if $(R, \cdot)$ is solvable but not a monoid?

Reduction of the input values from S to $FSF \setminus \mathcal{H}_e$ is done in three steps, where $n = |S|$.

$$S \longrightarrow S^n = SES = SFS \longrightarrow FSF \longrightarrow FSF \setminus \mathcal{H}_e,$$

In the last step $FSF \setminus \mathcal{H}_e$, we evaluate subcircuits in the ($\{0, 1\}$-free) subsemiring eRe.

Note: eRe is a solvable monoid.

Summary

Theorem

Let $\mathcal{R}$ be a finite semiring.

- If $\mathcal{R}$ is $\{0,1\}$-free and $(R,\cdot)$ is solvable, then $\mathrm{CEP}(\mathcal{R})$ is in **NC** (actually in **DET**).
- otherwise it is **P**-complete.

Outlook

- Intersection problem of a given context-free grammar and a fixed regular language
- Finite "semirings" where $(R,\cdot)$ is a groupoid?
- Evaluating semiring expressions?