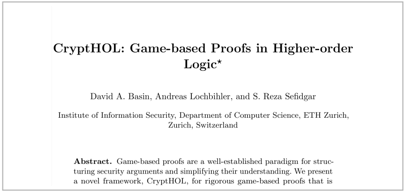
A Mechanized Proof of the Max-Flow-Min-Cut Theorem for Countable Networks

Andreas Lochbihler

Digital Asset

Motivation

CryptHOL



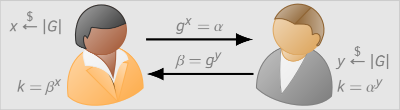
CryptHOL: Game-based Proofs in Higher-order Logic*

David A. Basin, Andreas Lochbihler, and S. Reza Sefidgar

Institute of Information Security, Department of Computer Science, ETH Zurich, Zurich, Switzerland

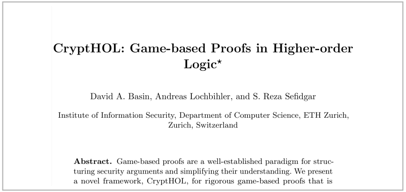
Abstract. Game-based proofs are a well-established paradigm for structuring security arguments and simplifying their understanding. We present a novel framework, CryptHOL, for rigorous game-based proofs that is

Relational logic for discrete probability distributions



Motivation

CryptHOL



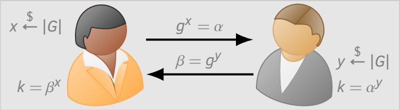
CryptHOL: Game-based Proofs in Higher-order Logic*

David A. Basin, Andreas Lochbihler, and S. Reza Sefidgar

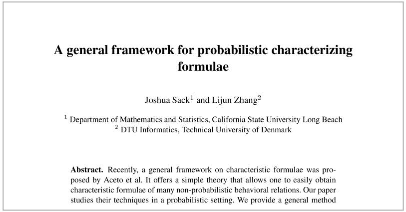
Institute of Information Security, Department of Computer Science, ETH Zurich, Zurich, Switzerland

Abstract. Game-based proofs are a well-established paradigm for structuring security arguments and simplifying their understanding. We present a novel framework, CryptHOL, for rigorous game-based proofs that is

Relational logic for discrete probability distributions



Lifting operator



A general framework for probabilistic characterizing formulae

Joshua Sack[1] and Lijun Zhang[2]

[1] Department of Mathematics and Statistics, California State University Long Beach
[2] DTU Informatics, Technical University of Denmark

Abstract. Recently, a general framework on characteristic formulae was proposed by Aceto et al. It offers a simple theory that allows one to easily obtain characteristic formulae of many non-probabilistic behavioral relations. Our paper studies their techniques in a probabilistic setting. We provide a general method

Motivation

CryptHOL

CryptHOL: Game-based Proofs in Higher-order Logic*

David A. Basin, Andreas Lochbihler, and S. Reza Sefidgar

Institute of Information Security, Department of Computer Science, ETH Zurich, Zurich, Switzerland

Abstract. Game-based proofs are a well-established paradigm for structuring security arguments and simplifying their understanding. We present a novel framework, CryptHOL, for rigorous game-based proofs that is

Lifting operator

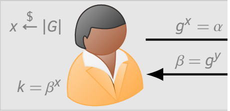
A general framework for probabilistic characterizing formulae

Joshua Sack[1] and Lijun Zhang[2]

[1] Department of Mathematics and Statistics, California State University Long Beach
[2] DTU Informatics, Technical University of Denmark

Abstract. Recently, a general framework on characteristic formulae was proposed by Aceto et al. It offers a simple theory that allows one to easily obtain characteristic formulae of many non-probabilistic behavioral relations. Our paper ... babilistic setting. We provide a general method

Relational logic fc probability distrib



The Max-Flow Min-Cut theorem for countable networks

Ron Aharoni[a,1,3], Eli Berger[b,2], Agelos Georgakopoulos[c,3], Amitai Perlstein[a], Philipp Sprüssel[c,3]

[a] *Department of Mathematics, Technion, Haifa, Israel 32000*
[b] *Department of Mathematics, Faculty of Science and Science Education, Haifa University, Israel 32000*
[c] *Universität Hamburg, Germany*

A R T I C L E I N F O

Article history:
Received 4 December 2007

Keywords:

A B S T R A C T

We prove a strong version of the Max-Flow Min-Cut theorem for countable networks, namely that in every such network there exist a flow and a cut that are “orthogonal” to each other, in the sense that the flow saturates the cut and is zero on the reverse cut. If

Motivation

CryptHOL

CryptHOL: Game-based Proofs i[...]
Logic*

David A. Basin, Andreas Lochbihler, and S[...]

Institute of Information Security, Department of Compu[...]
Zurich, Switzerland

Abstract. Game-based proofs are a well-established paradigm for structuring security arguments and simplifying their understanding. We present a novel framework, CryptHOL, for rigorous game-based proofs that is

Lifting operator

A recent mathematical theorem

✓ formalized in Isabelle/HOL

✓ found and fixed many mistakes and glitches

✓ simpler variant with additional assumptions

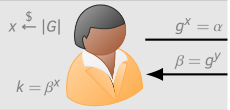
[...]work for probabilistic characterizing formulae

[...]Joshua Sack[1] and Lijun Zhang[2]

[...]atics and Statistics, California State University Long Beach
[...]formatics, Technical University of Denmark

Abstract. Recently, a general framework on characteristic formulae was proposed by Aceto et al. It offers a simple theory that allows one to easily obtain characteristic formulae of many non-probabilistic behavioral relations. Our paper [...]babilistic setting. We provide a general method

Relational logic fo[...]
probability distrib[...]



The Max-Flow Min-Cut theorem for countable networks

Ron Aharoni[a,1,3], Eli Berger[b,2], Agelos Georgakopoulos[c,3], Amitai Perlstein[a], Philipp Sprüssel[c,3]

[a] Department of Mathematics, Technion, Haifa, Israel 32000
[b] Department of Mathematics, Faculty of Science and Science Education, Haifa University, Israel 32000
[c] Universität Hamburg, Germany

ARTICLE INFO

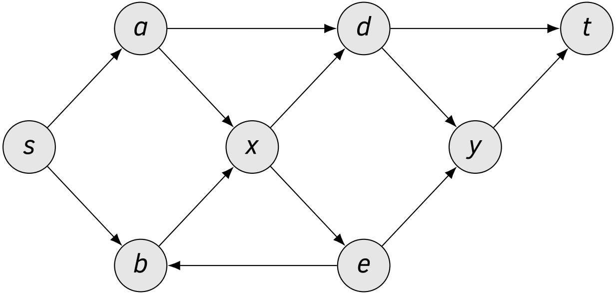
Article history:
Received 4 December 2007

Keywords:

ABSTRACT

We prove a strong version of the Max-Flow Min-Cut theorem for countable networks, namely that in every such network there exist a flow and a cut that are "orthogonal" to each other, in the sense that the flow saturates the cut and is zero on the reverse cut. If

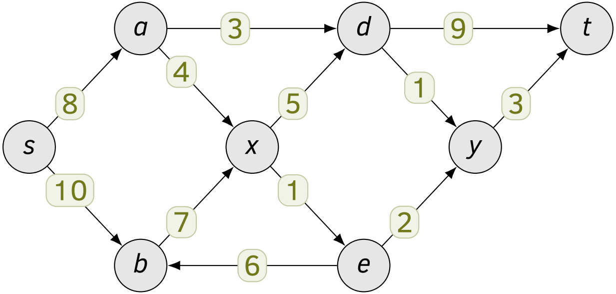
The Max-Flow-Min-Cut Theorem for Finite Networks



Network

- graph $G = (V, E)$

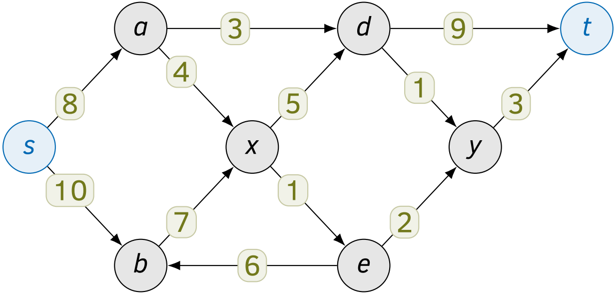
The Max-Flow-Min-Cut Theorem for Finite Networks



Network

- graph $G = (V, E)$
- capacity $c : E \longrightarrow \mathbb{R}_{\geq 0}$

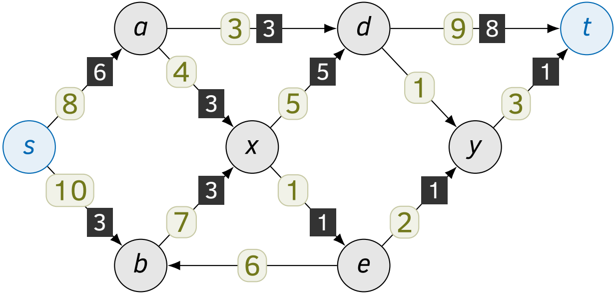
The Max-Flow-Min-Cut Theorem for Finite Networks



Network

- graph $G = (V, E)$
- capacity $c : E \longrightarrow \mathbb{R}_{\geq 0}$
- source s, sink t

The Max-Flow-Min-Cut Theorem for Finite Networks



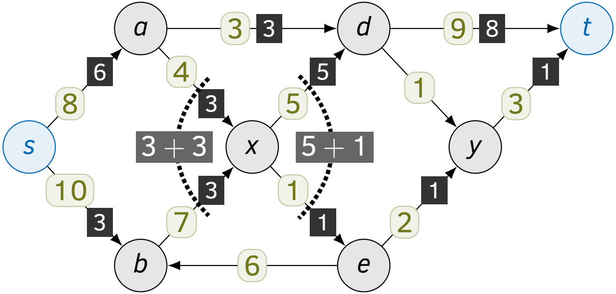
Network

- graph $G = (V, E)$
- capacity $c : E \longrightarrow \mathbb{R}_{\geq 0}$
- source s, sink t

Flow $f : E \longrightarrow \mathbb{R}_{\geq 0}$

- Capacity $f(e) \leq c(e)$
- Preservation $\sum_{e \in \text{in}(x)} f(e) = \sum_{e \in \text{out}(x)} f(e)$ for $x \in V - \{s, t\}$

The Max-Flow-Min-Cut Theorem for Finite Networks



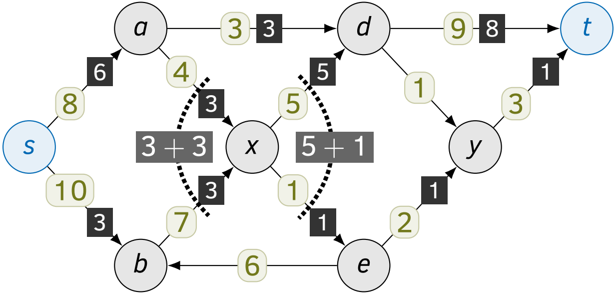
Network

- graph $G = (V, E)$
- capacity $c : E \longrightarrow \mathbb{R}_{\geq 0}$
- source s, sink t

Flow $f : E \longrightarrow \mathbb{R}_{\geq 0}$

- Capacity $f(e) \leq c(e)$
- Preservation $\sum_{e \in \mathrm{in}(x)} f(e) = \sum_{e \in \mathrm{out}(x)} f(e)$
  for $x \in V - \{s, t\}$

The Max-Flow-Min-Cut Theorem for Finite Networks



Network

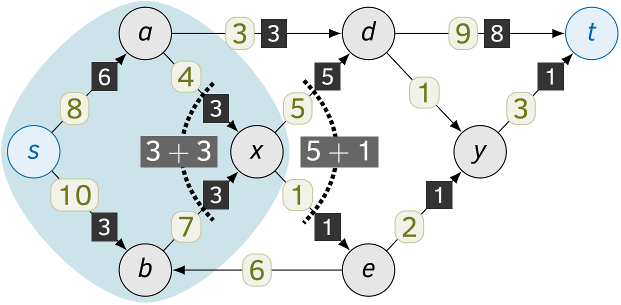
- graph $G = (V, E)$
- capacity $c : E \longrightarrow \mathbb{R}_{\geq 0}$
- source s, sink t

Flow $f : E \longrightarrow \mathbb{R}_{\geq 0}$

- Capacity $f(e) \leq c(e)$
- Preservation $\sum_{e \in \mathrm{in}(x)} f(e) = \sum_{e \in \mathrm{out}(x)} f(e)$ for $x \in V - \{s, t\}$
- Value $|f| = \sum_{e \in \mathrm{out}(s)} f(e) = \sum_{e \in \mathrm{in}(t)} f(e)$

$|f| = 6 + 3 = 8 + 1$

The Max-Flow-Min-Cut Theorem for Finite Networks



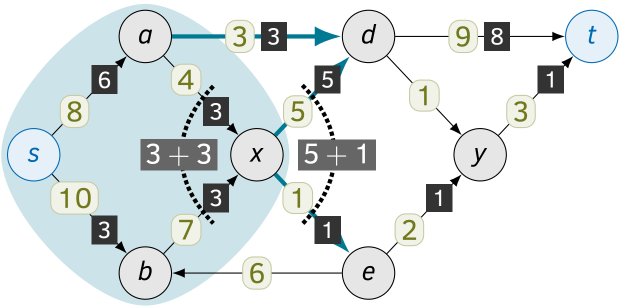
Cut $C \subseteq V$
- $s \in C$, $t \notin C$
- Value $|C| = \sum_{(x,y) \in E, x \in C, y \notin C} c(x,y)$

Network
- graph $G = (V, E)$
- capacity $c : E \longrightarrow \mathbb{R}_{\geq 0}$
- source s, sink t

Flow $f : E \longrightarrow \mathbb{R}_{\geq 0}$
- Capacity $f(e) \leq c(e)$
- Preservation $\sum_{e \in \text{in}(x)} f(e) = \sum_{e \in \text{out}(x)} f(e)$ for $x \in V - \{s, t\}$
- Value $|f| = \sum_{e \in \text{out}(s)} f(e) = \sum_{e \in \text{in}(t)} f(e)$

$|f| = 6 + 3 = 8 + 1$

The Max-Flow-Min-Cut Theorem for Finite Networks



Cut $C \subseteq V$

- $s \in C$, $t \notin C$
- Value $|C| = \sum_{(x,y)\in E, x\in C, y\notin C} c(x,y)$

$|C| = 3 + 5 + 1$

Network

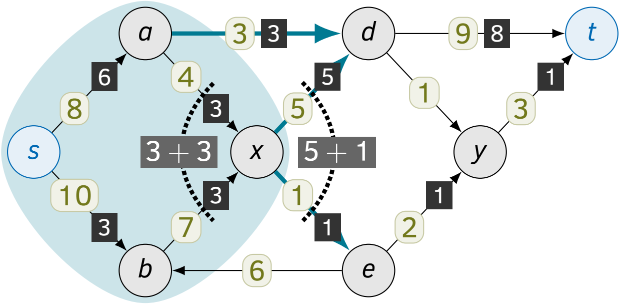
- graph $G = (V, E)$
- capacity $c : E \longrightarrow \mathbb{R}_{\geq 0}$
- source s, sink t

Flow $f : E \longrightarrow \mathbb{R}_{\geq 0}$

- Capacity $f(e) \leq c(e)$
- Preservation $\sum_{e\in \mathrm{in}(x)} f(e) = \sum_{e\in \mathrm{out}(x)} f(e)$ for $x \in V - \{s, t\}$
- Value $|f| = \sum_{e\in \mathrm{out}(s)} f(e) = \sum_{e\in \mathrm{in}(t)} f(e)$

$|f| = 6 + 3 = 8 + 1$

The Max-Flow-Min-Cut Theorem for Finite Networks



Max-Flow Min-Cut Theorem
In every finite network, there exist a cut C and a flow f s.t. $|C| = |f|$.

Lammich and Sefidgar [ITP 2016]

Cut $C \subseteq V$

- $s \in C$, $t \notin C$
- Value $|C| = \sum_{(x,y)\in E, x\in C, y\notin C} c(x,y)$

$|C| = 3 + 5 + 1$

Network

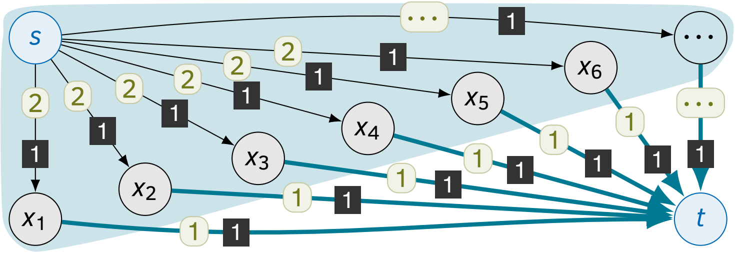
- graph $G = (V, E)$
- capacity $c : E \longrightarrow \mathbb{R}_{\geq 0}$
- source s, sink t

Flow $f : E \longrightarrow \mathbb{R}_{\geq 0}$

- Capacity $f(e) \leq c(e)$
- Preservation $\sum_{e\in \text{in}(x)} f(e) = \sum_{e\in \text{out}(x)} f(e)$ for $x \in V - \{s, t\}$
- Value $|f| = \sum_{e\in \text{out}(s)} f(e) = \sum_{e\in \text{in}(t)} f(e)$

$|f| = 6 + 3 = 8 + 1$

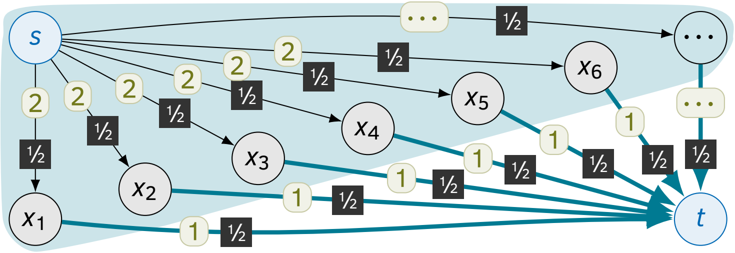
Challenges with Countable Networks



$C = \{s, x_1, x_2, \ldots\}$ $\quad |C| = \infty$

$f(e) = 1$ $\quad |f| = \infty$

Challenges with Countable Networks

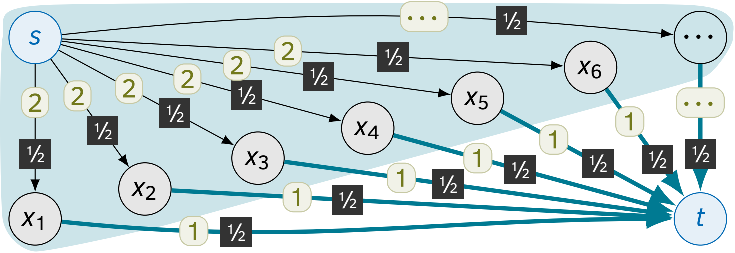


$C = \{s, x_1, x_2, \ldots\}$ $\quad |C| = \infty$

$f(e) = 1$ $\quad |f| = \infty$

$g(e) = 1/2$ $\quad |g| = \infty$

Challenges with Countable Networks



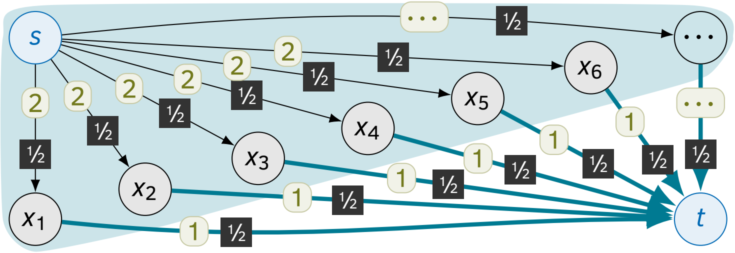
$C = \{s, x_1, x_2, \ldots\}$ $\quad |C| = \infty$

$f(e) = 1$ $\quad |f| = \infty$

$g(e) = 1/2$ $\quad |g| = \infty$

Avoid infinite sums!

Challenges with Countable Networks



$C = \{s, x_1, x_2, \dots\}$ $|C| = \infty$

$f(e) = 1$ $|f| = \infty$

$\cancel{g(e) = 1/2}$ $\cancel{|g| = \infty}$

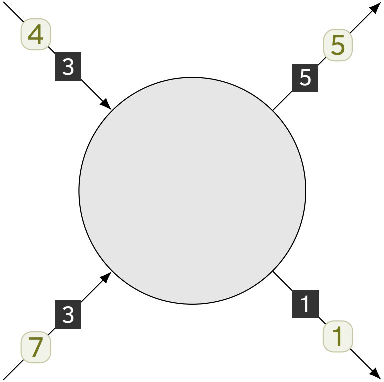
Avoid infinite sums!

Max-Flow Min-Cut Theorem [Aharoni et al.]

There exist a cut C and a flow f s.t.

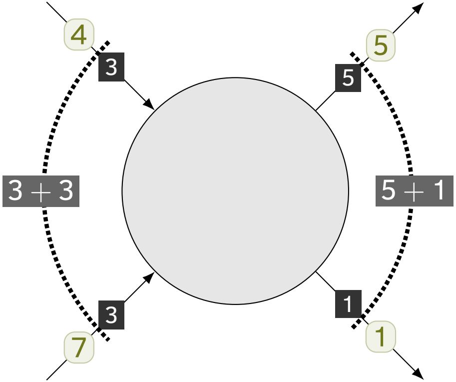
- $f(x,y) = c(x,y)$ for $(x,y) \in E, x \in C, y \notin C$
- $f(x,y) = 0$ for $(x,y) \in E, x \notin C, y \in C$

More Infinite Sums



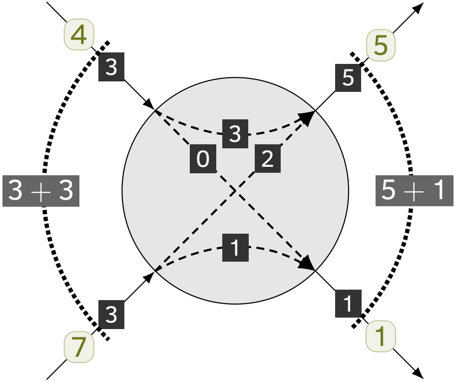
More Infinite Sums

Flow preservation

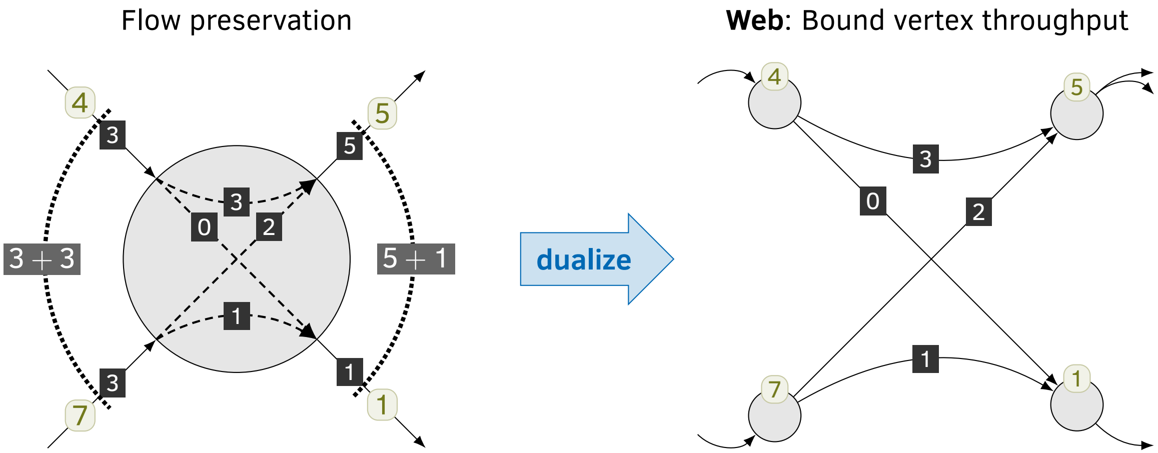


More Infinite Sums

Flow preservation

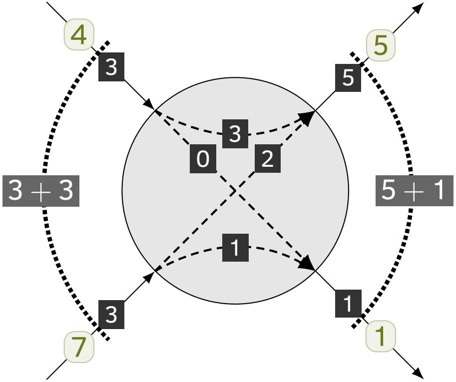


More Infinite Sums



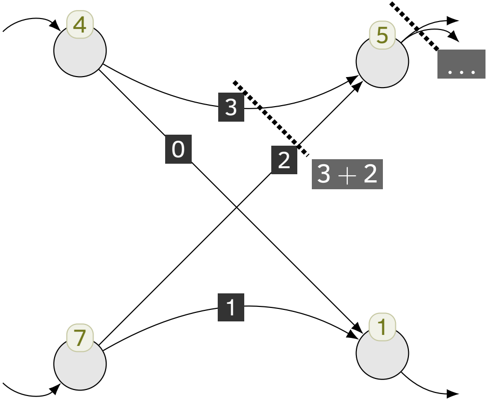
More Infinite Sums

Flow preservation



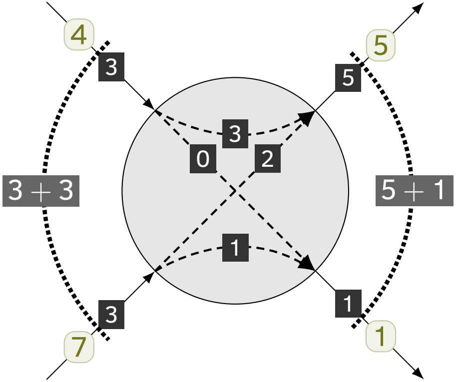
dualize

Web: Bound vertex throughput



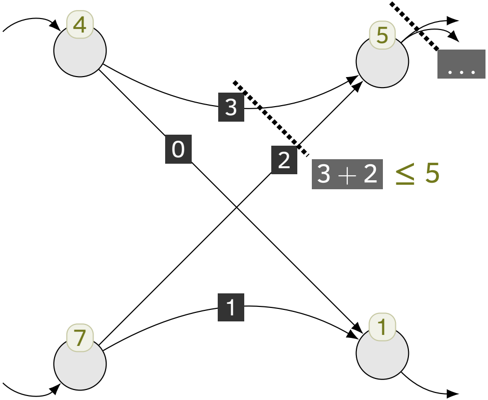
More Infinite Sums

Flow preservation

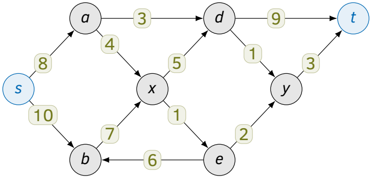


dualize

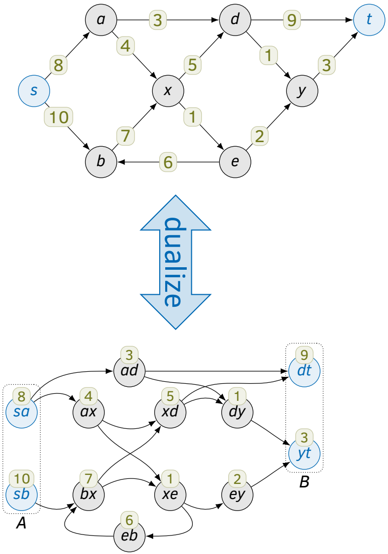
Web: Bound vertex throughput



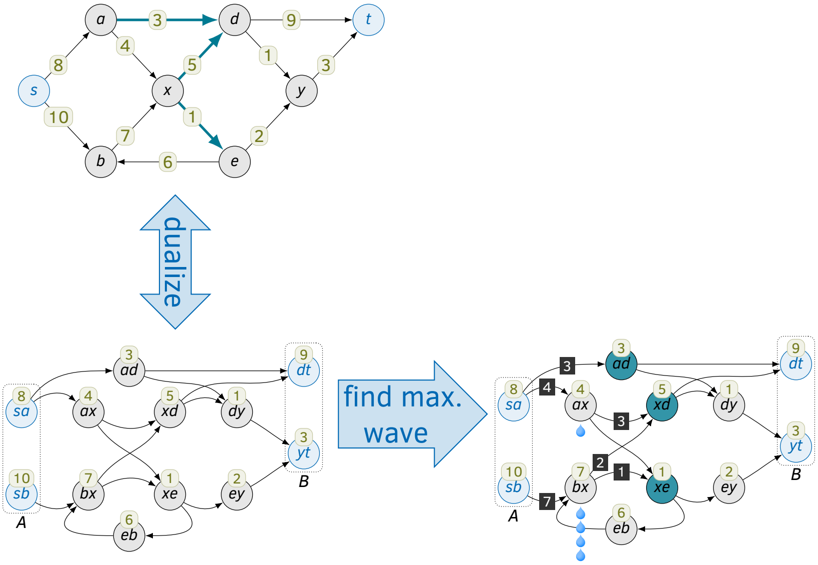
Transformations



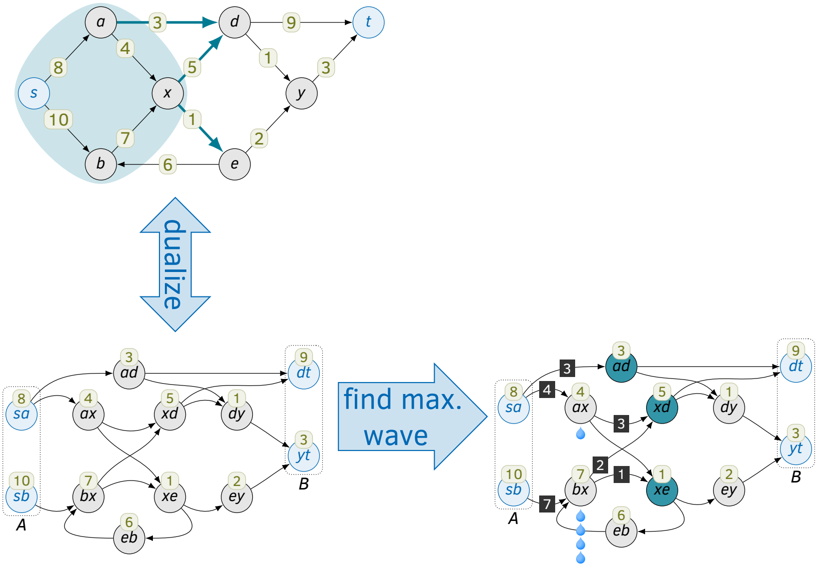
Transformations



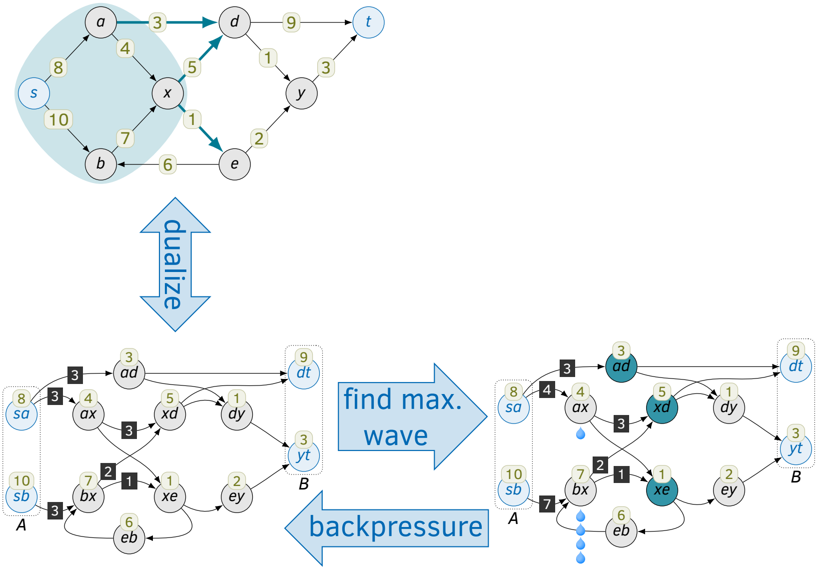
Transformations



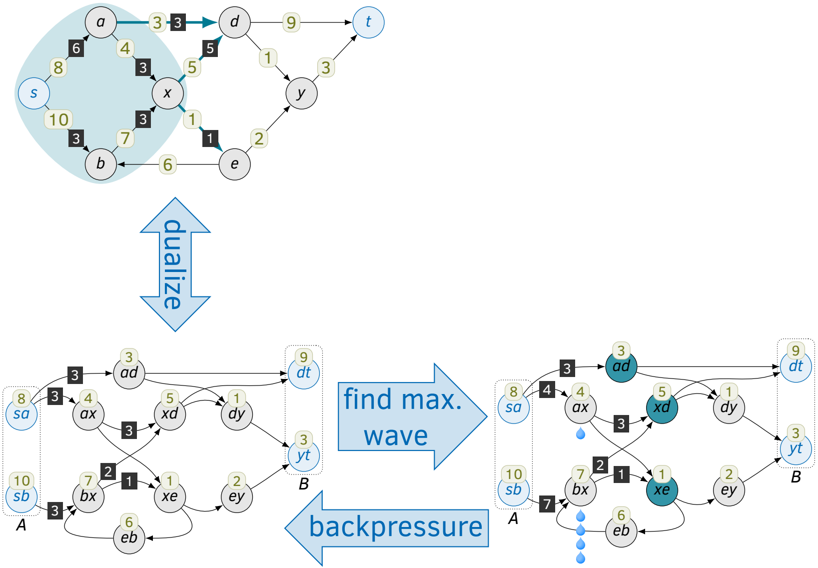
Transformations



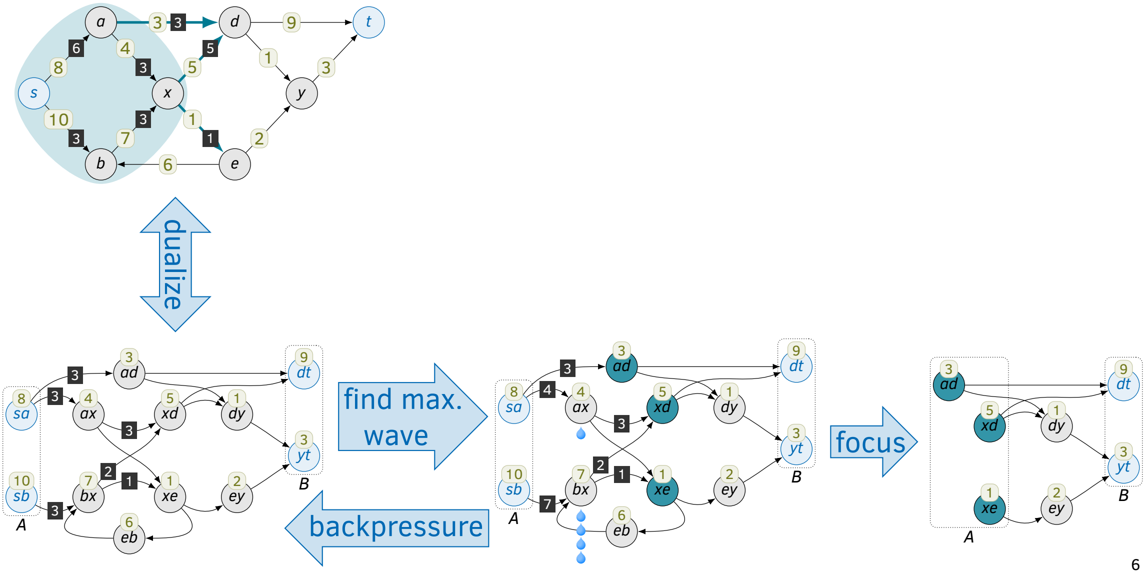
Transformations



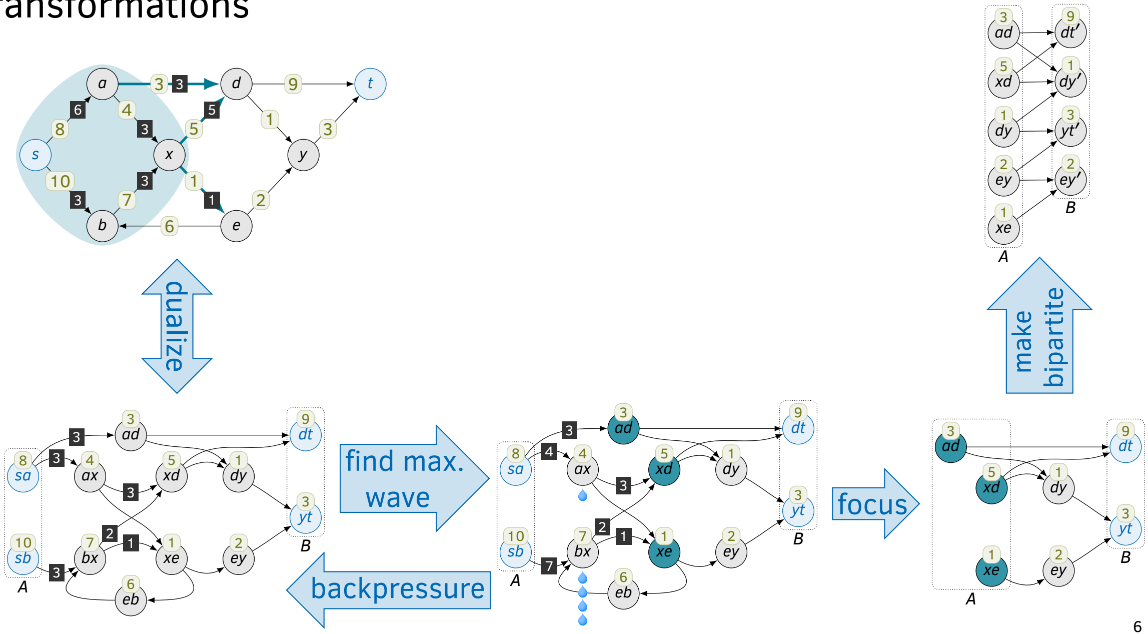
Transformations



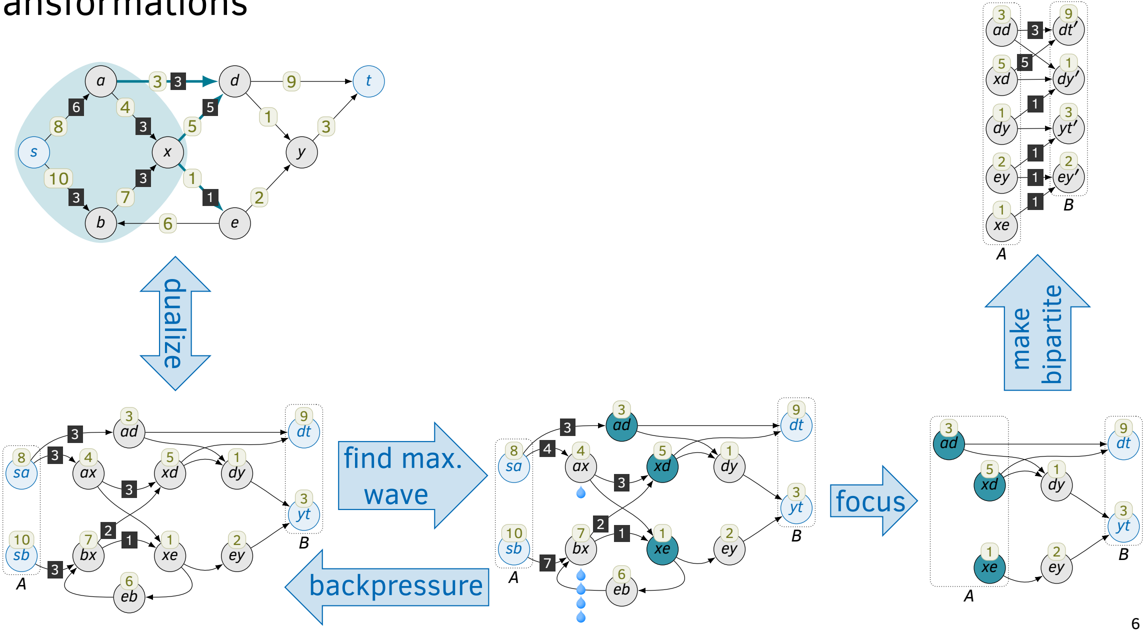
Transformations



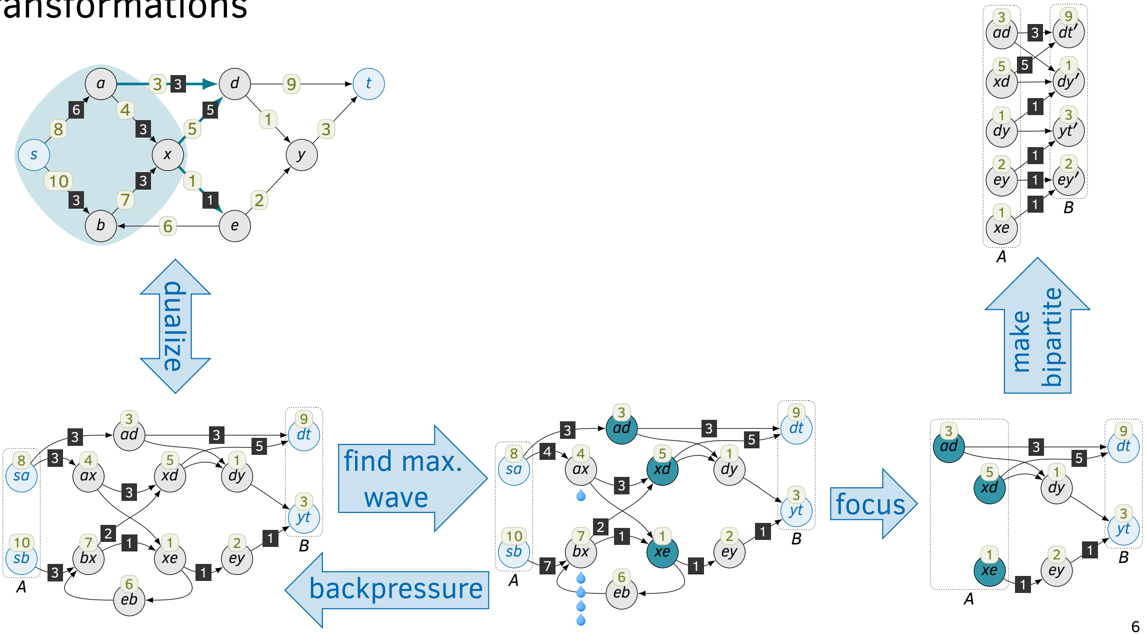
Transformations



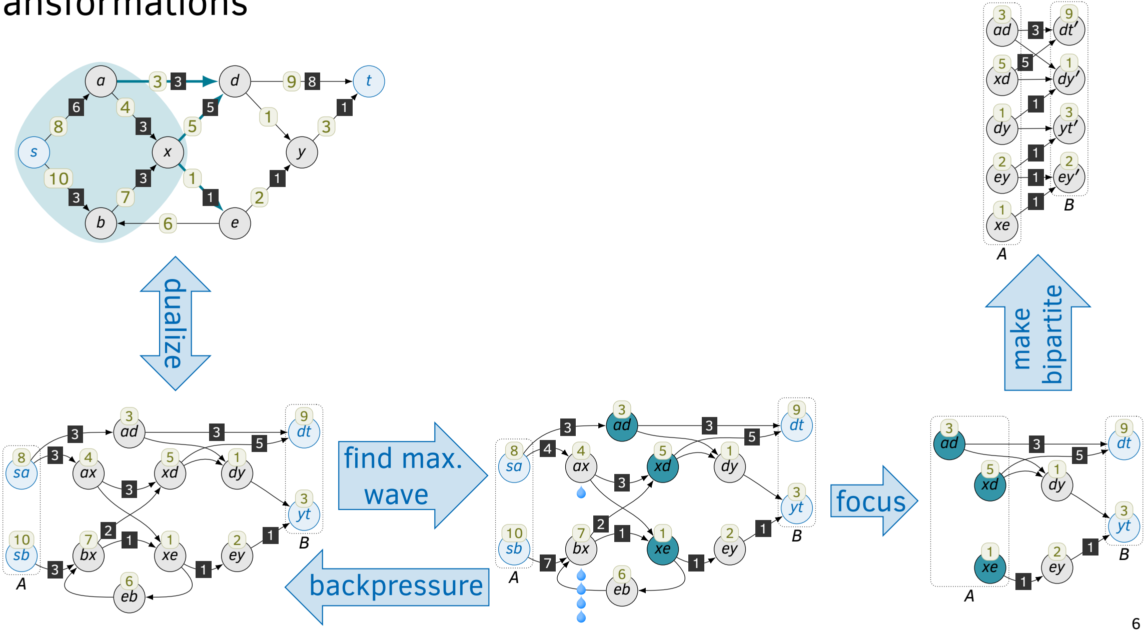
Transformations



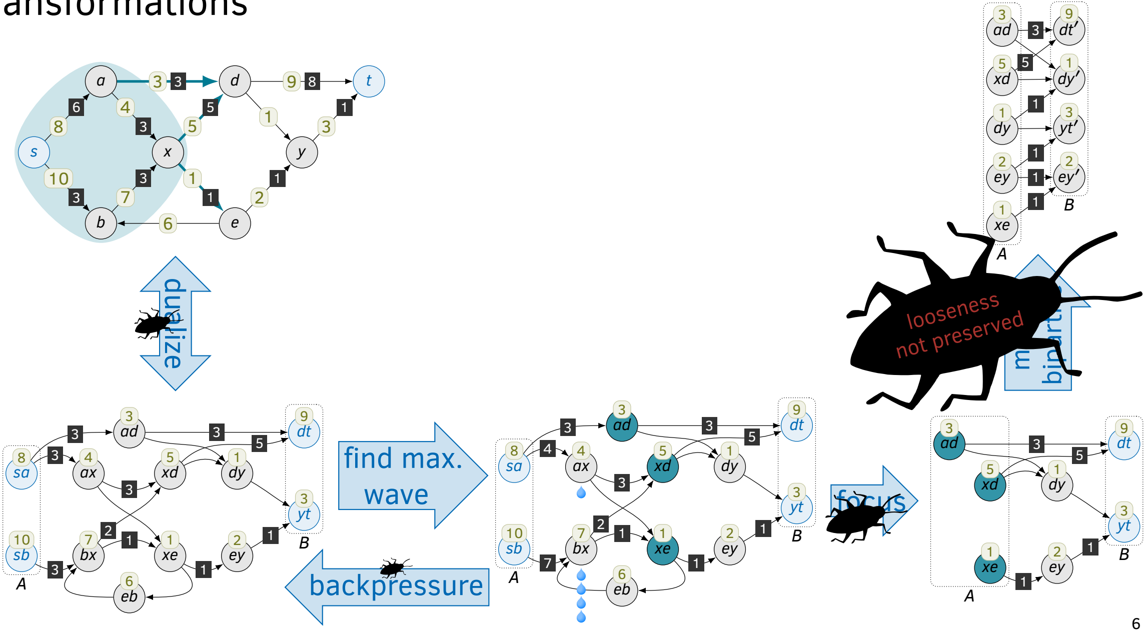
Transformations



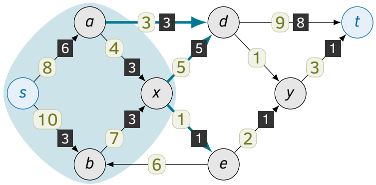
Transformations



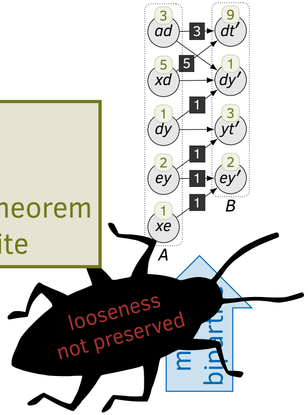
Transformations

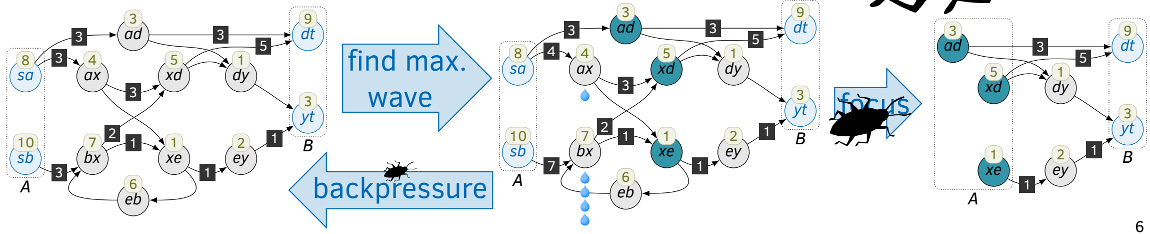


Transformations

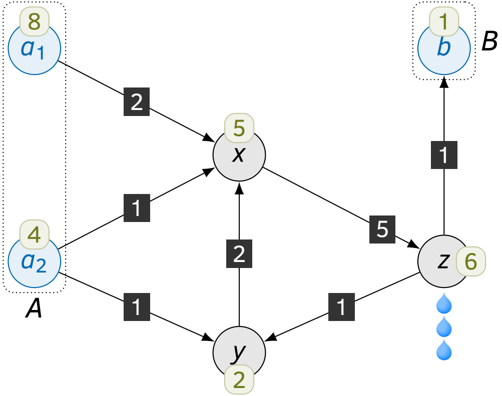


1. adapt proof to weakened induction invariant
2. new proof using finite MFMC theorem if total neighbour weight is finite

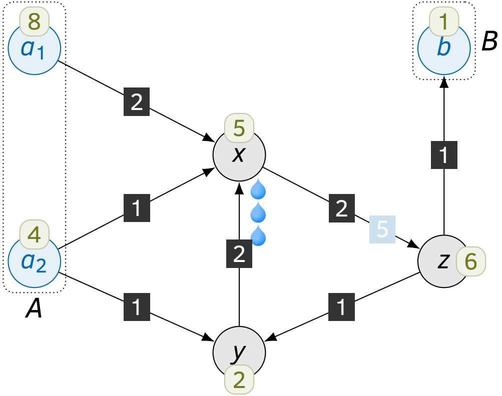




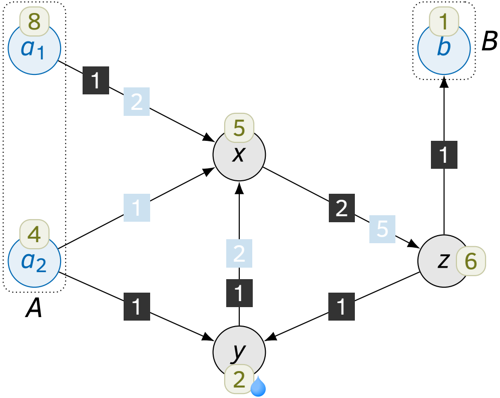
Backpressure fixpoint



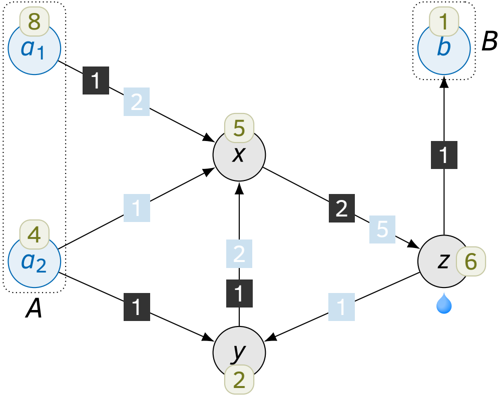
Backpressure fixpoint



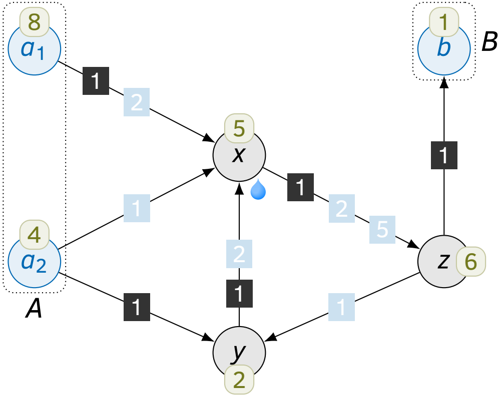
Backpressure fixpoint



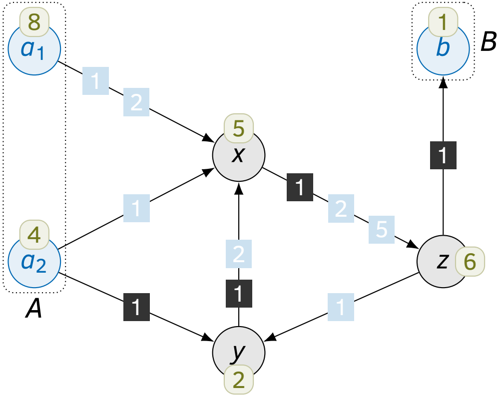
Backpressure fixpoint



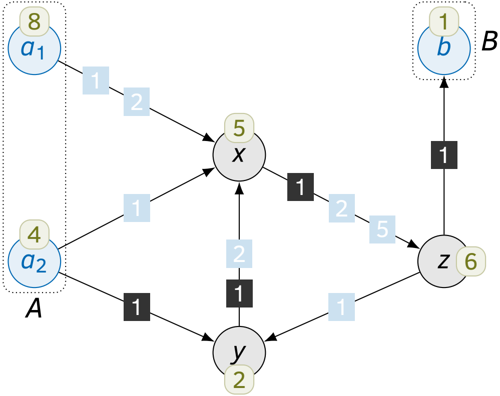
Backpressure fixpoint



Backpressure fixpoint



Backpressure fixpoint

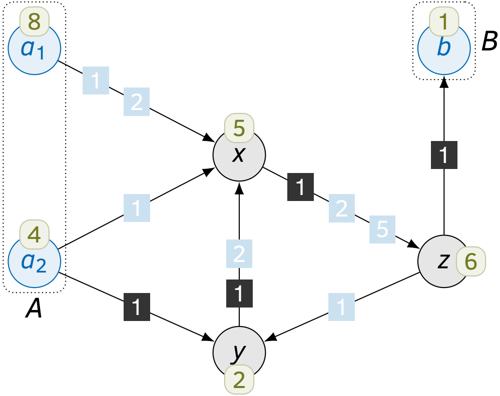


Backpressure $bp_G : Flow \Rightarrow Flow$

Pick a leaking vertex 💧 if any
and reduce incoming flow.

$$f = \mathrm{fix}(bp_G)$$

Backpressure fixpoint



Backpressure $bp_G : Flow \Rightarrow Flow$

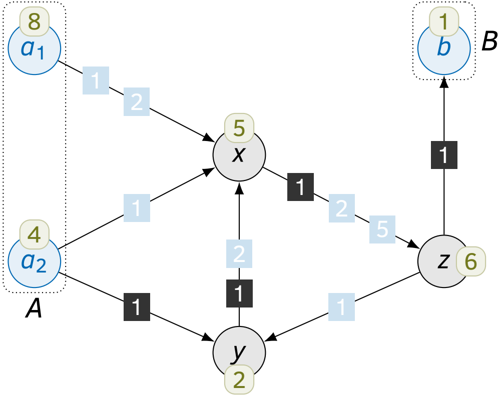
Pick a leaking vertex 💧 if any
and reduce incoming flow.

$f = \mathrm{fix}(bp_G)$

$Flow = (E \Rightarrow \mathbb{R}_{\geq 0}, \geq)$ is a ccpo

Knaster-Tarski?

Backpressure fixpoint



Backpressure $bp_G : \mathit{Flow} \Rightarrow \mathit{Flow}$

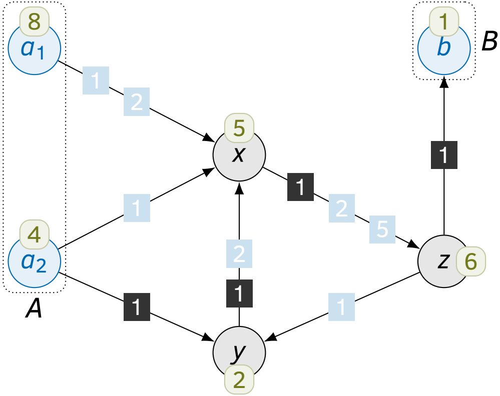
Pick a leaking vertex if any
and reduce incoming flow.

$f = \mathrm{fix}(bp_G)$

$\mathit{Flow} = (E \Rightarrow \mathbb{R}_{\geq 0}, \geq)$ is a ccpo

~~**Knaster-Tarski?**~~ bp_G is not monotone

Backpressure fixpoint



Backpressure $bp_G : \mathit{Flow} \Rightarrow \mathit{Flow}$

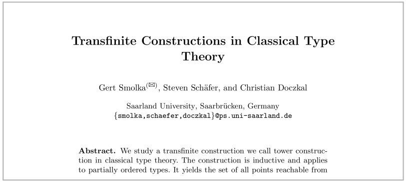
Pick a leaking vertex if any and reduce incoming flow.

$f = \mathrm{fix}(bp_G)$

$\mathit{Flow} = (E \Rightarrow \mathbb{R}_{\geq 0}, \geq)$ is a ccpo

~~Knaster-Tarski?~~ bp_G is not monotone

Bourbaki-Witt! bp_G is decreasing!



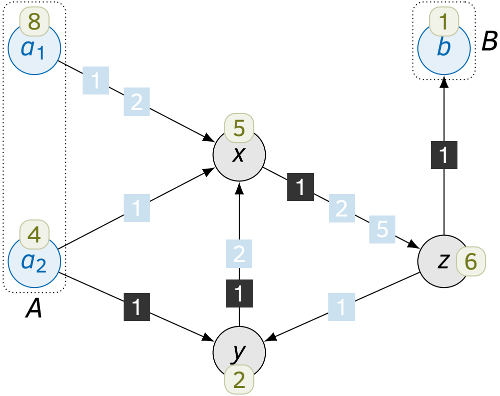
Transfinite Constructions in Classical Type Theory

Gert Smolka[✉], Steven Schäfer, and Christian Doczkal

Saarland University, Saarbrücken, Germany
{smolka,schaefer,doczkal}@ps.uni-saarland.de

Abstract. We study a transfinite construction we call tower construction in classical type theory. The construction is inductive and applies to partially ordered types. It yields the set of all points reachable from

Backpressure fixpoint



Backpressure $bp_G : Flow \Rightarrow Flow$

Pick a leaking vertex if any
and reduce incoming flow.

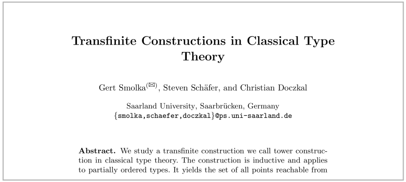
$f = \mathrm{fix}(bp_G)$

$Flow = (E \Rightarrow \mathbb{R}_{\geq 0}, \geq)$ is a ccpo

~~**Knaster-Tarski?**~~ bp_G is not monotone

Bourbaki-Witt! bp_G is decreasing!

translate



Transfinite Constructions in Classical Type Theory

Gert Smolka(✉), Steven Schäfer, and Christian Doczkal

Saarland University, Saarbrücken, Germany
{smolka,schaefer,doczkal}@ps.uni-saarland.de

Abstract. We study a transfinite construction we call tower construction in classical type theory. The construction is inductive and applies to partially ordered types. It yields the set of all points reachable from

Summary: Avoid infinite sums!

Summary: Avoid infinite sums!

Available in the AFP

isa-afp.org/entries/MFMC_Countable.html

Summary: Avoid infinite sums!

Available in the AFP

isa-afp.org/entries/MFMC_Countable.html

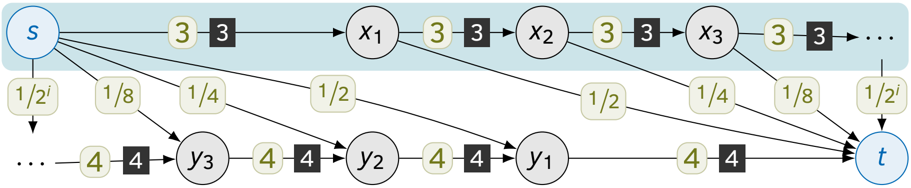
	Line counts
Preliminaries	200
Networks & webs	2214
Transformations	1248
Bounded linkability	1434
Unbounded linkability	5112
Total	**10208**

Summary: Avoid infinite sums!

Available in the AFP

isa-afp.org/entries/MFMC_Countable.html

Line counts	
Preliminaries	200
Networks & webs	2214
Transformations	1248
Bounded linkability	1434
Unbounded linkability	5112
Total	**10208**



	value
cut	2
out-flow	3
in-flow	4