Lightweight Formal Methods for the Development of High-Assurance Network Systems

Assaf Kfoury

with contributions from

Azer Bestavros, Adam Bradley, Andrei Lapets, and Michael Ocean

iBench Initiative
http://www.cs.bu.edu/groups/ibench/
snBench
http://csr.bu.edu/snbench/

Computer Science

More Formal Methods ...

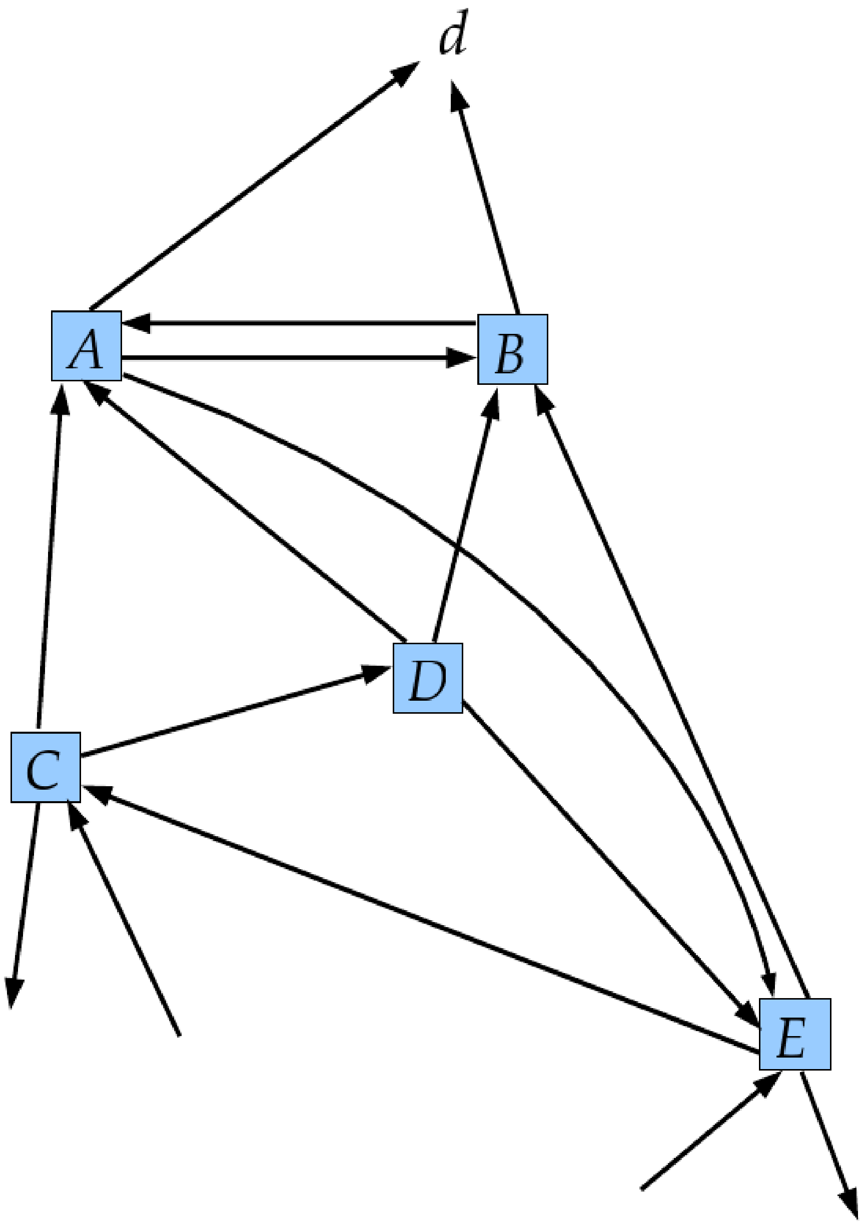
for the development of a rigorous discipline of *specification, analysis, programming* and *maintenance* of network systems

1. Compositional Analysis/Specification and its Benefits
(mostly with **Azer Bestavros**)
iBench Initiative – http://www.cs.bu.edu/groups/ibench/

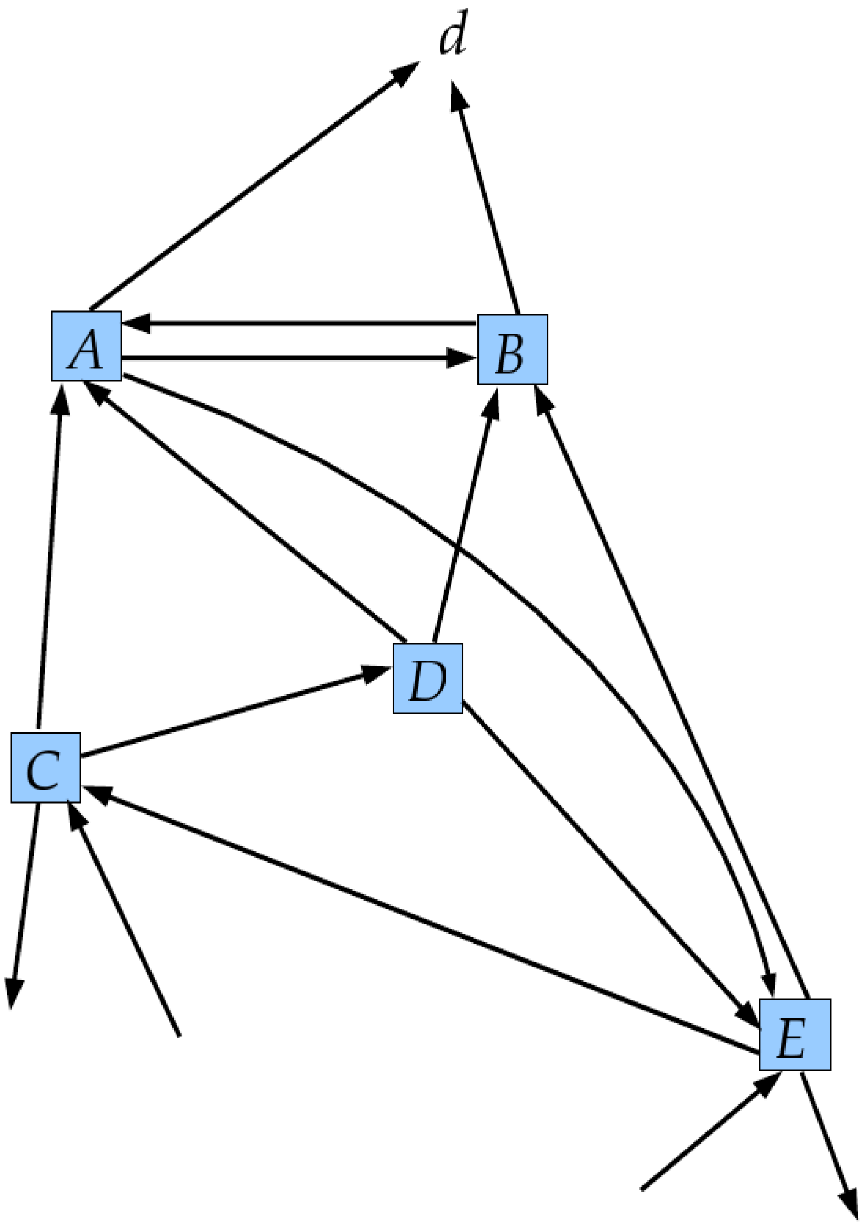
2. An Application of Model Checking:
Safe Composition of Arbitrary Network Protocols
(mostly with **Adam Bradley** and **Azer Bestavros**)
iBench Initiative – http://www.cs.bu.edu/groups/ibench/

3. Resource Allocation in Sensor Networks Using
a Strongly-Typed Domain-Specific Language
(mostly with **Michael Ocean** and **Azer Bestavros**)
snBench – http://csr.bu.edu/snbench/

4. The Stable-Paths Problem and the Promise of
an Automatic Lightweight Proof-Assistant
(mostly with **Kevin Donnelly** and **Andrei Lapets**)

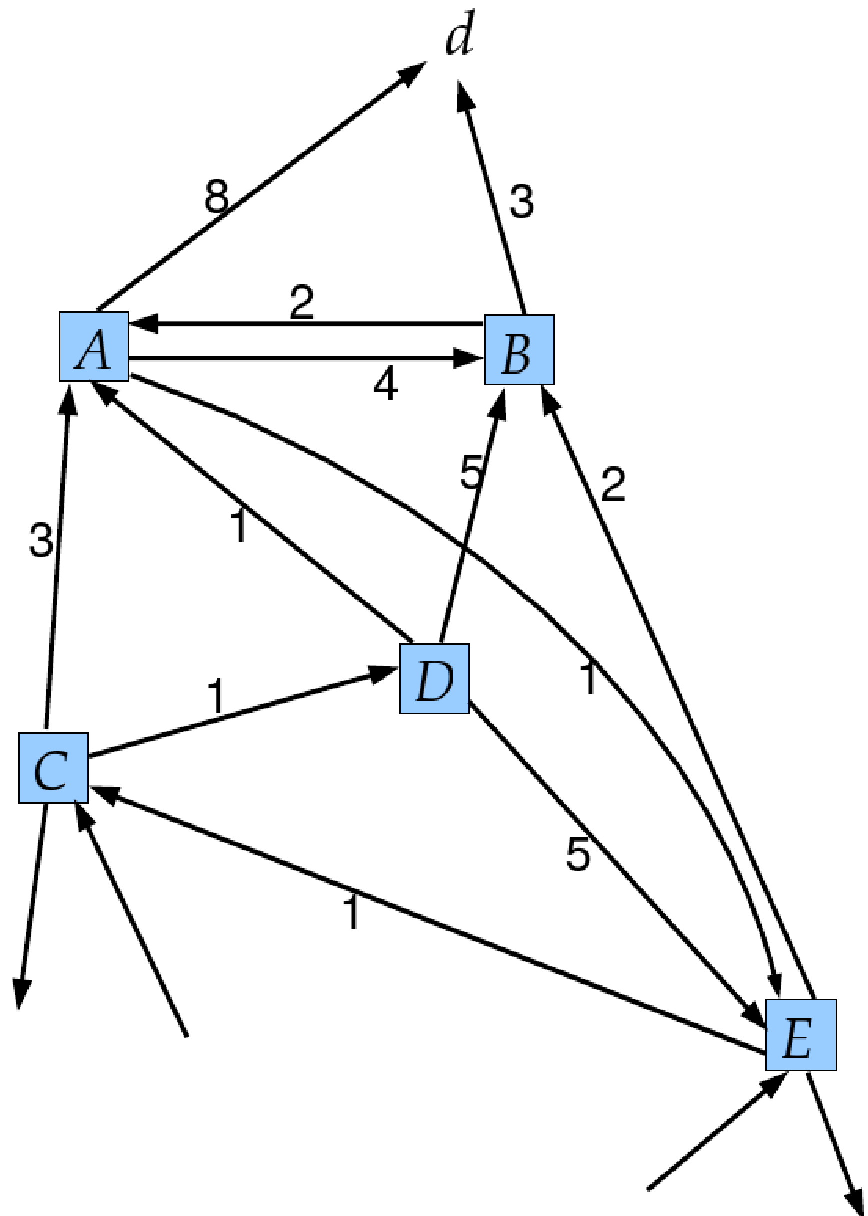


network topology

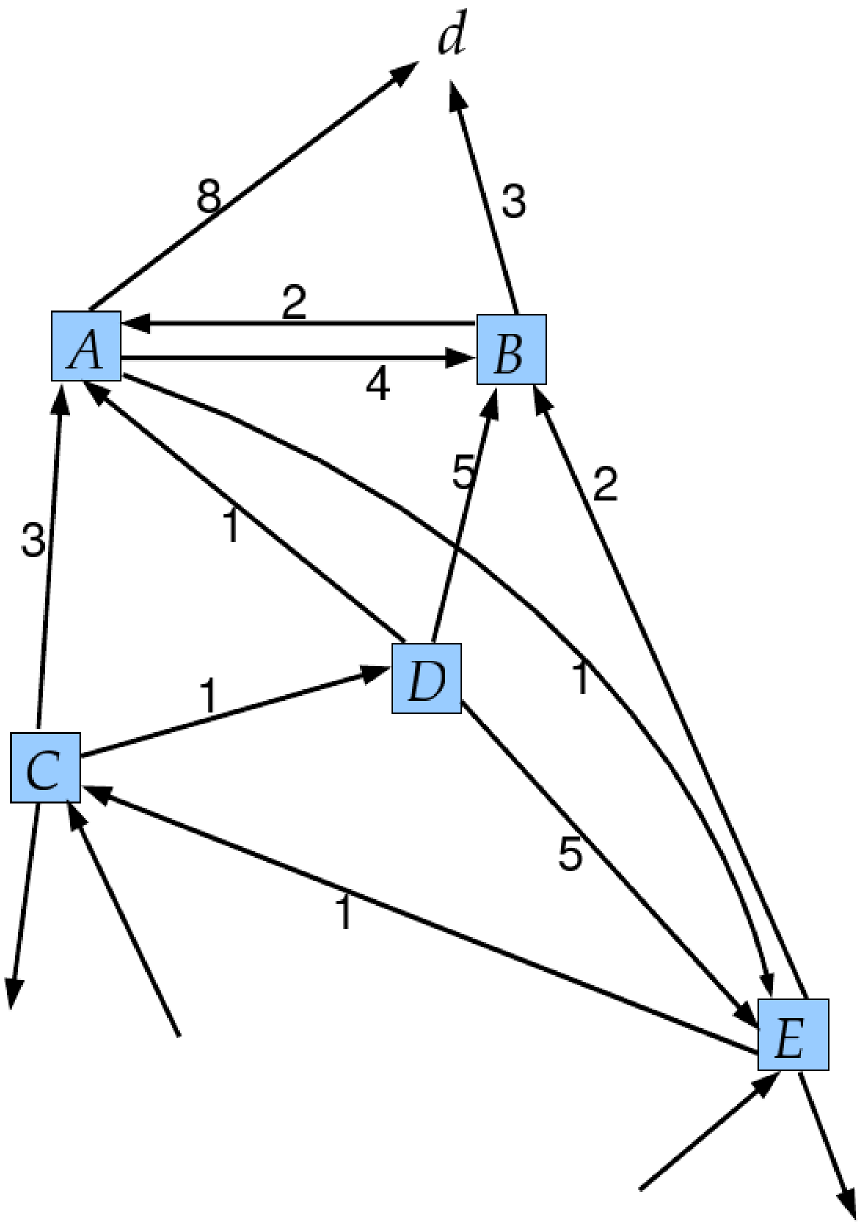


network topology

one additive measure on links

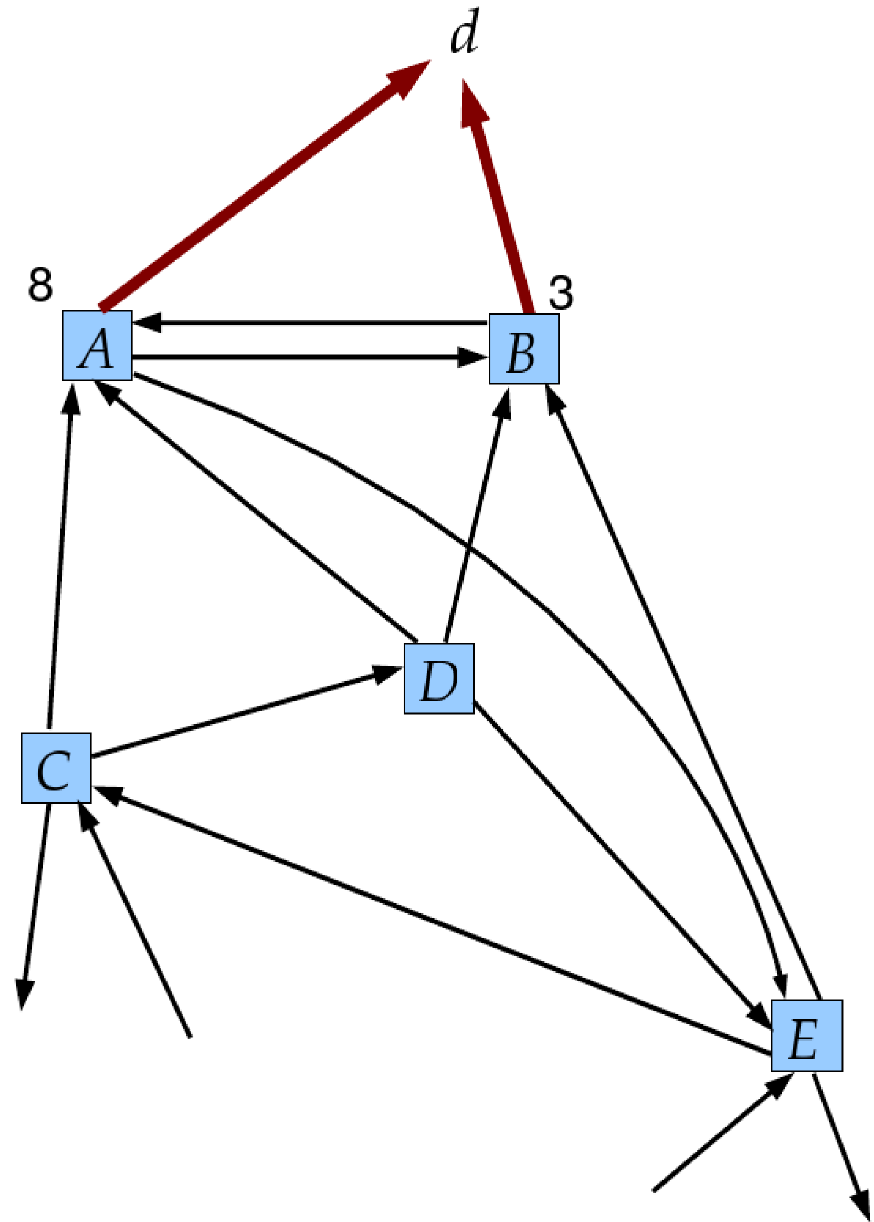


every node requests the "cheapest" path to *d*
every node communicates with its immediate peers only

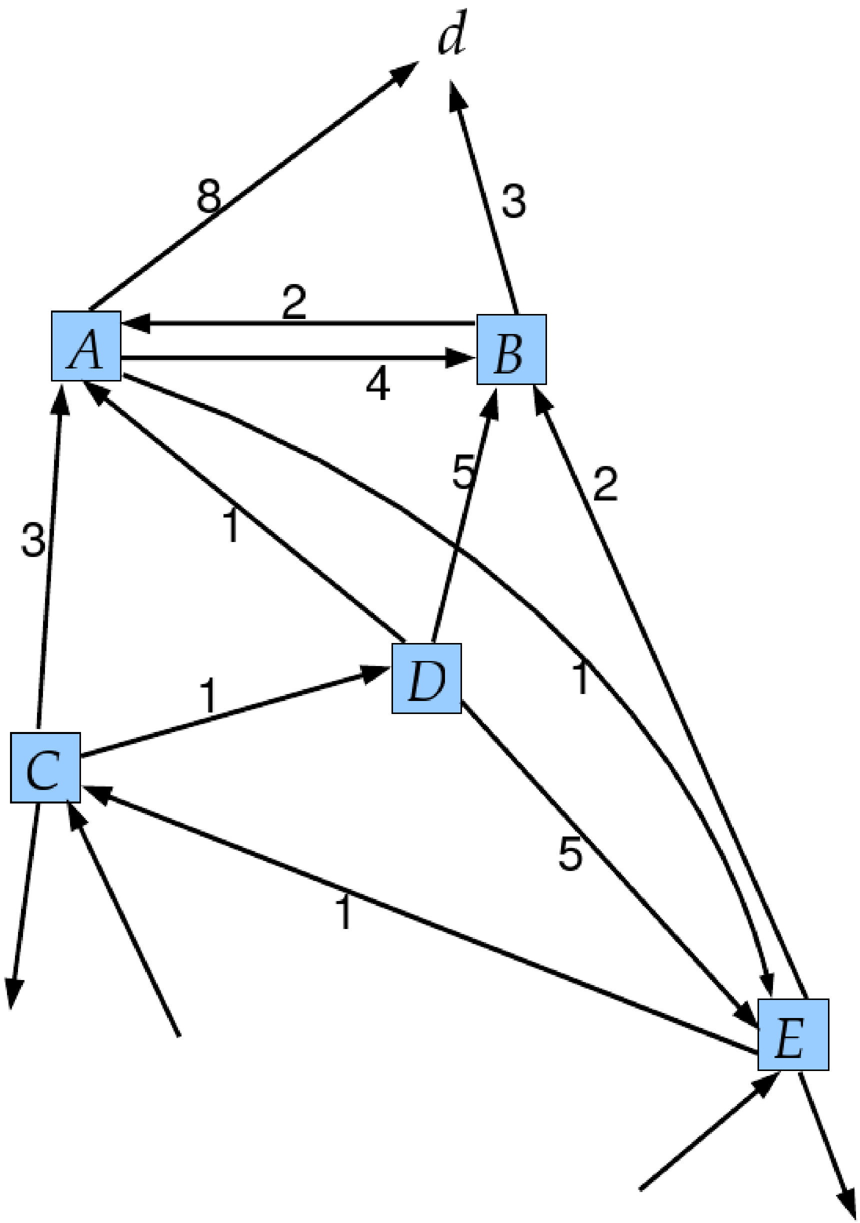


additive measure on links

at end of time = 1

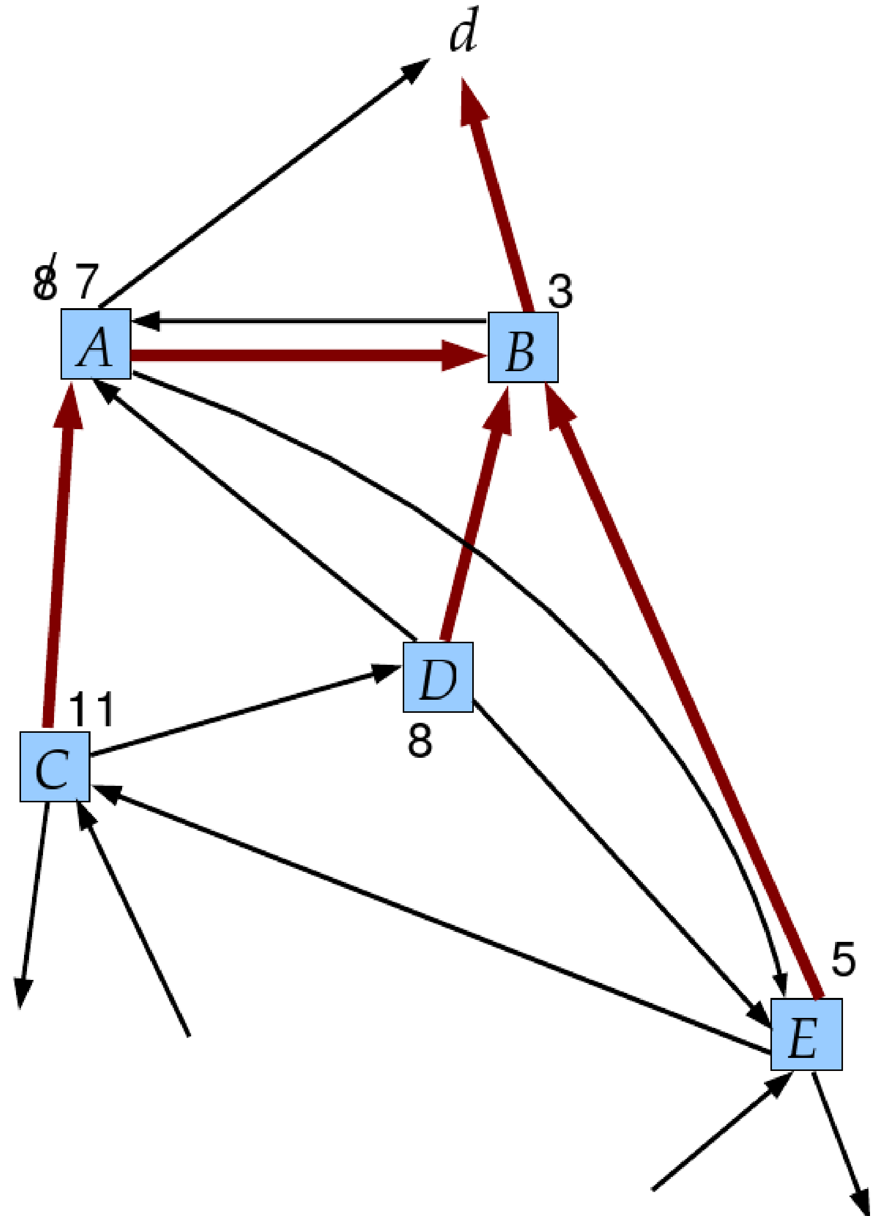


after ***d*** broadcasts to ***A*** and ***B***

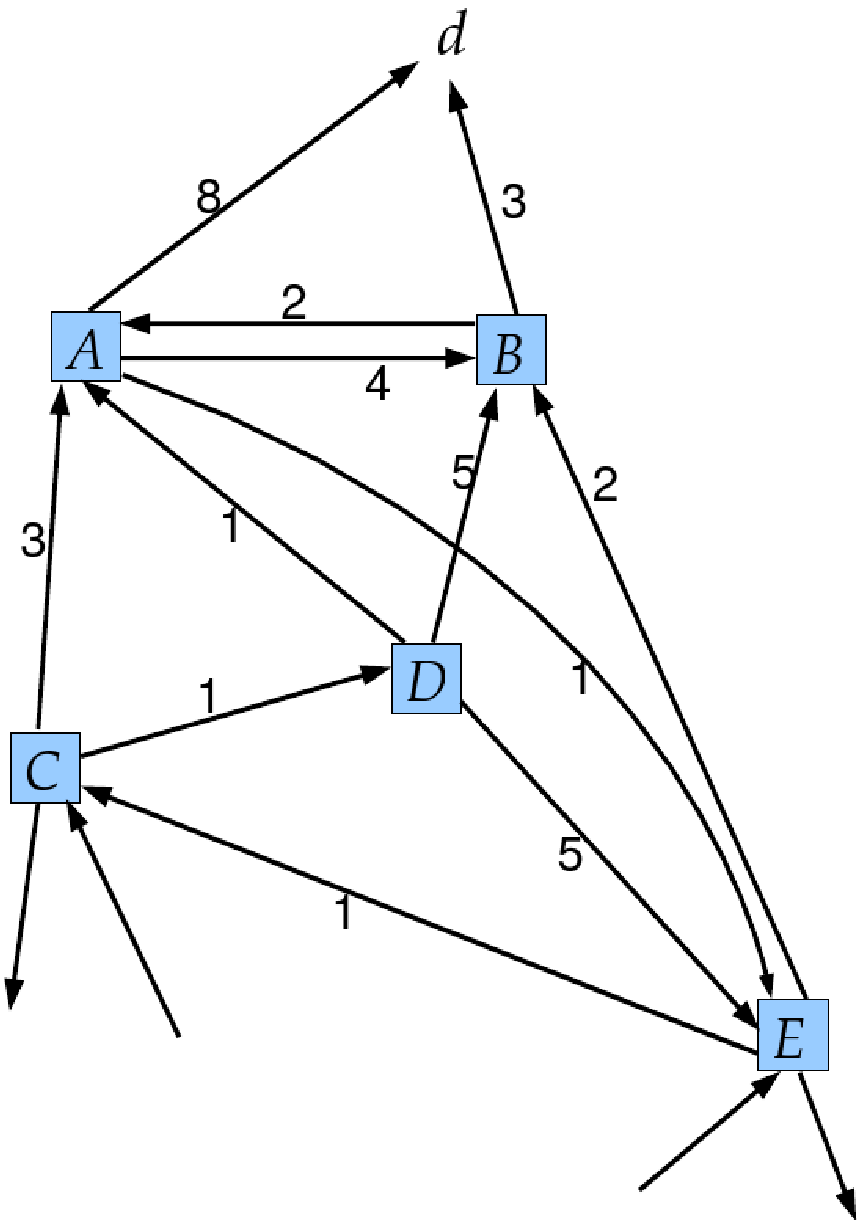


additive measure on links

at end of time = 2

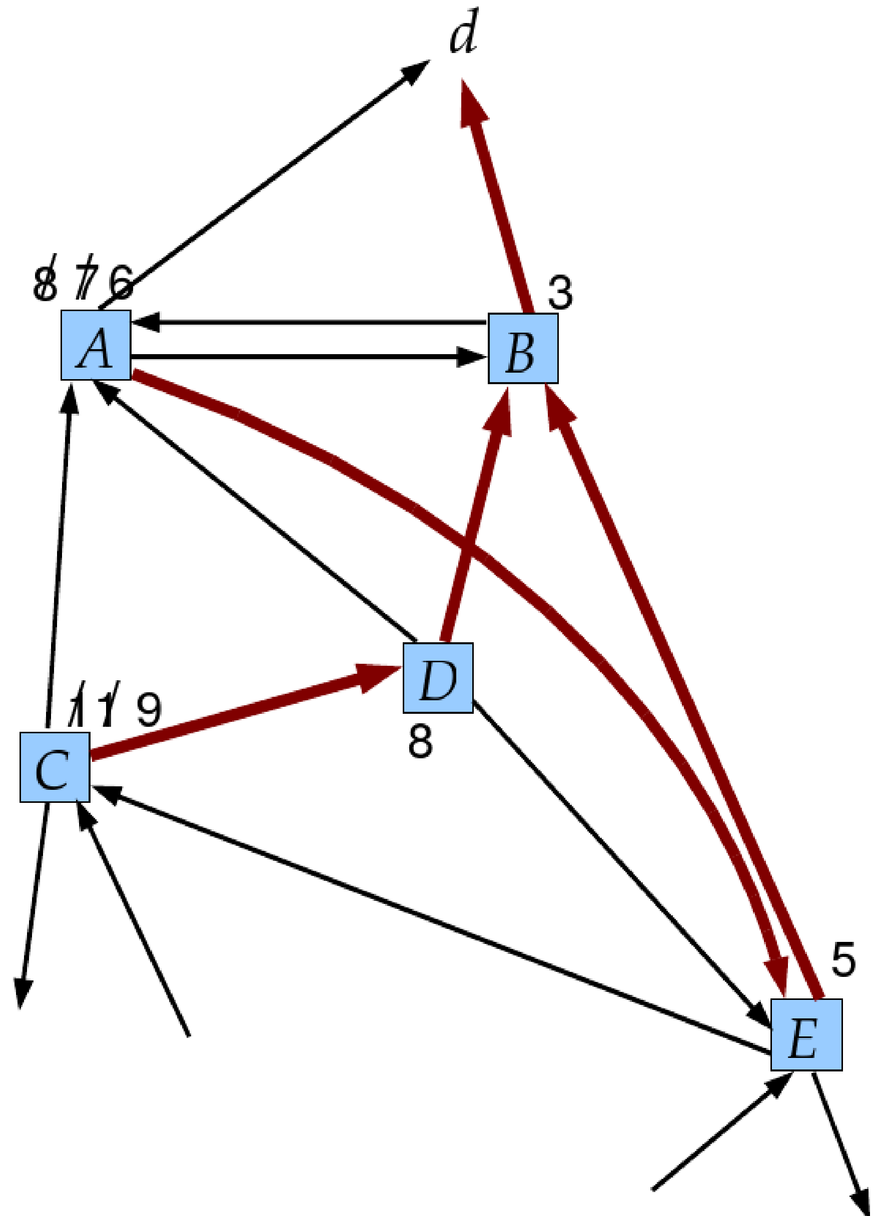


after *A* broadcasts to *B*,*C*,*D*
and *B* broadcasts to *A*,*D*,*E*



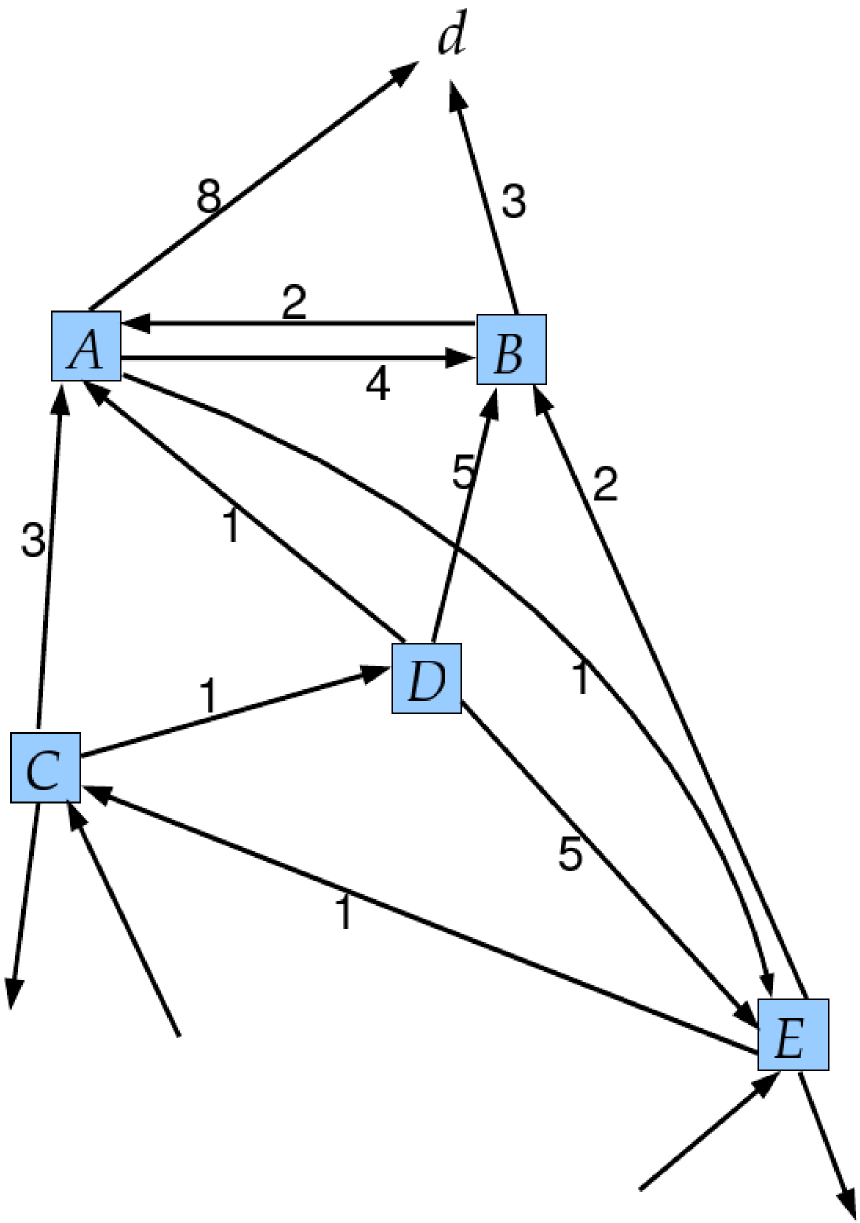
additive measure on links

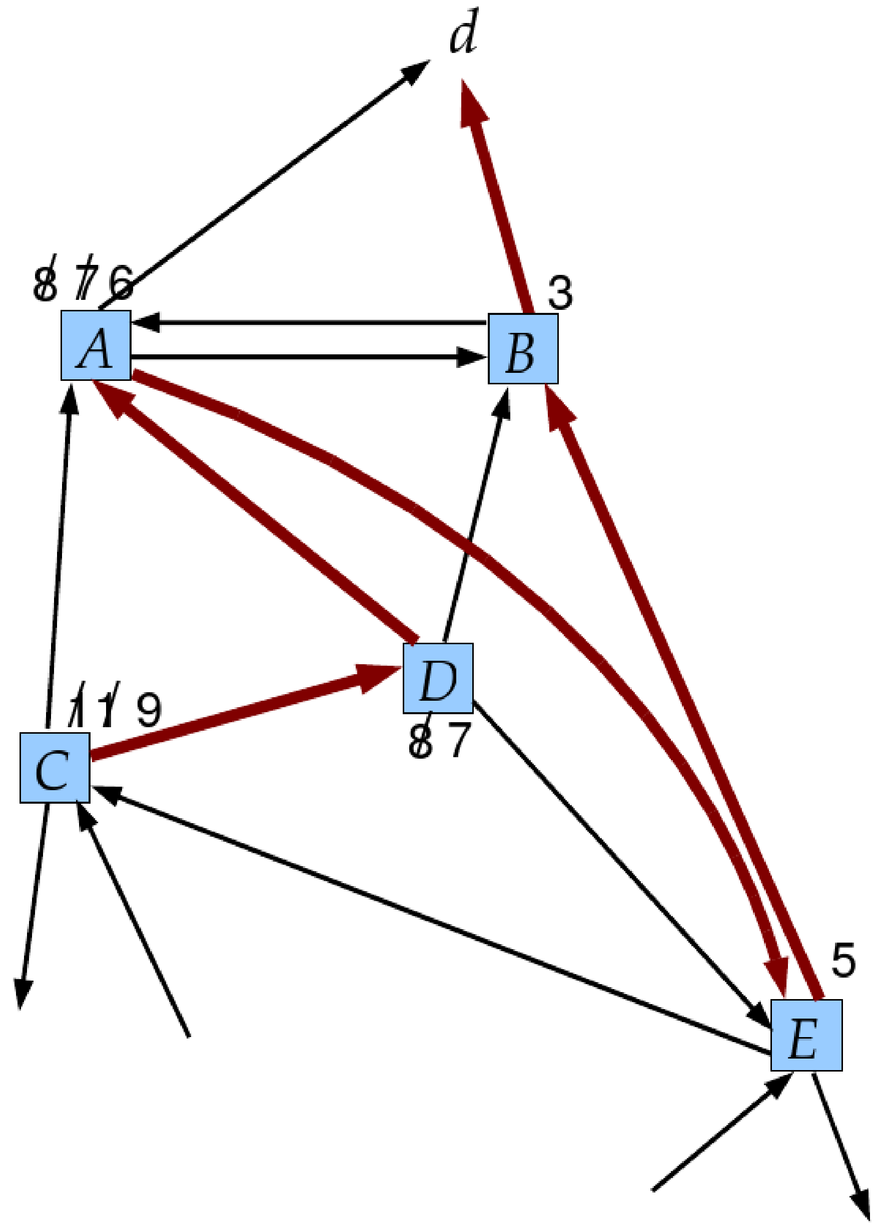
at end of time = 3



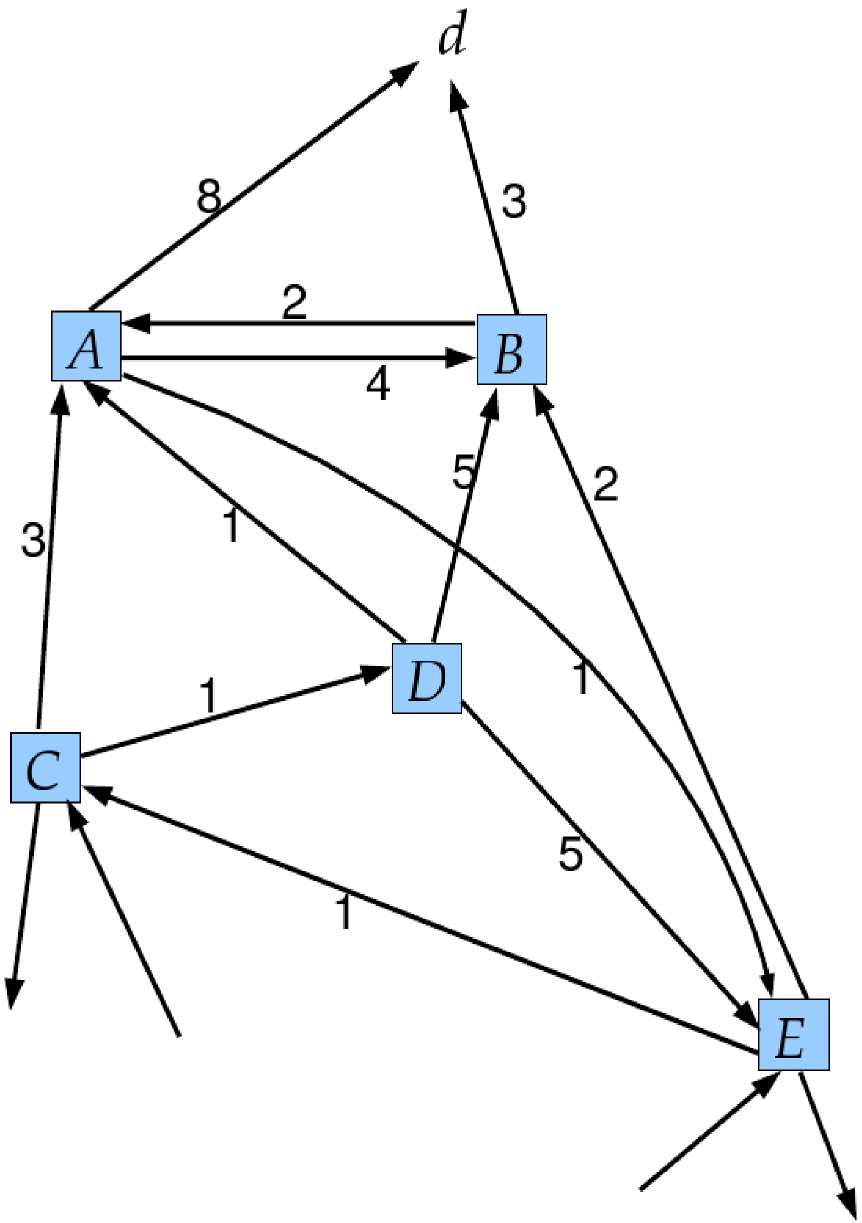
after *C* broadcasts to *E*,...
D* broadcasts to *C
***E* broadcasts to *A*,*D*,...**

at end of time = 4

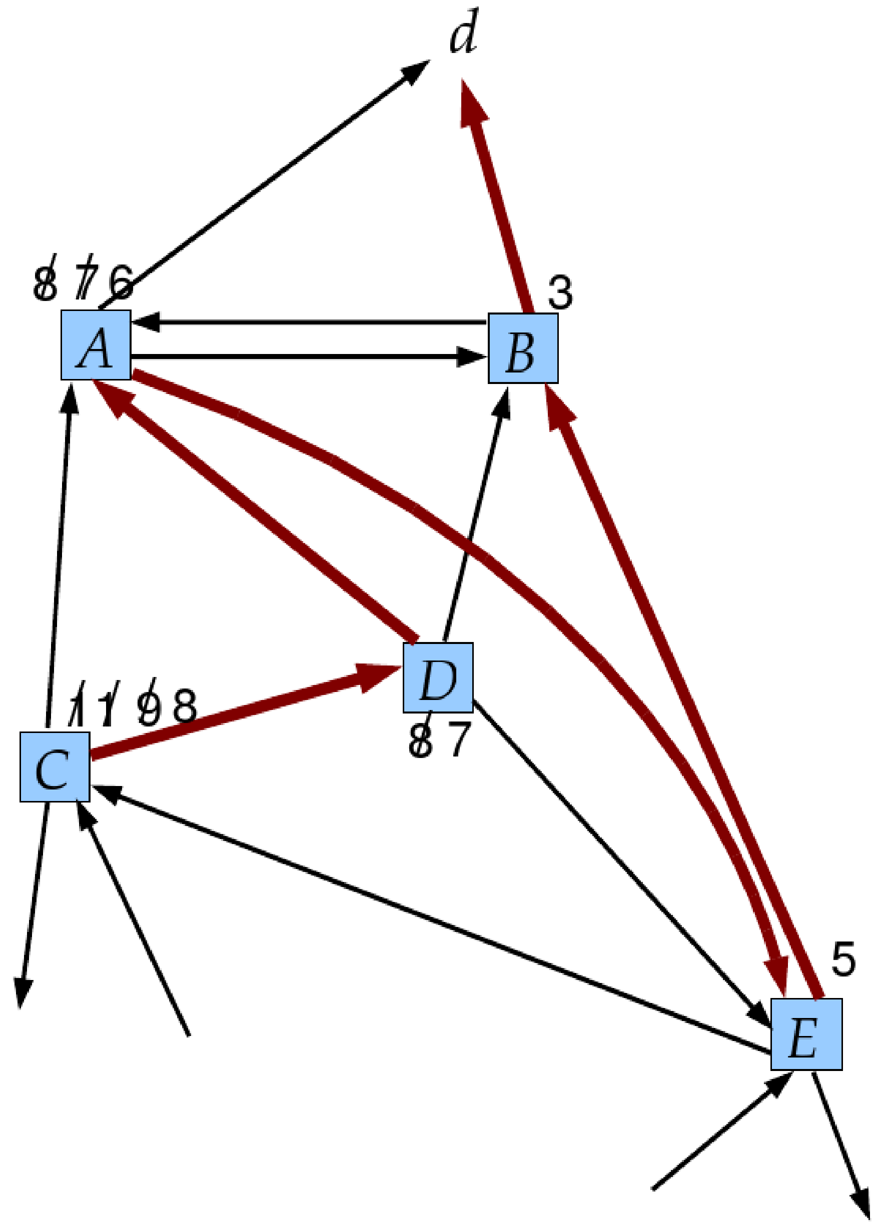




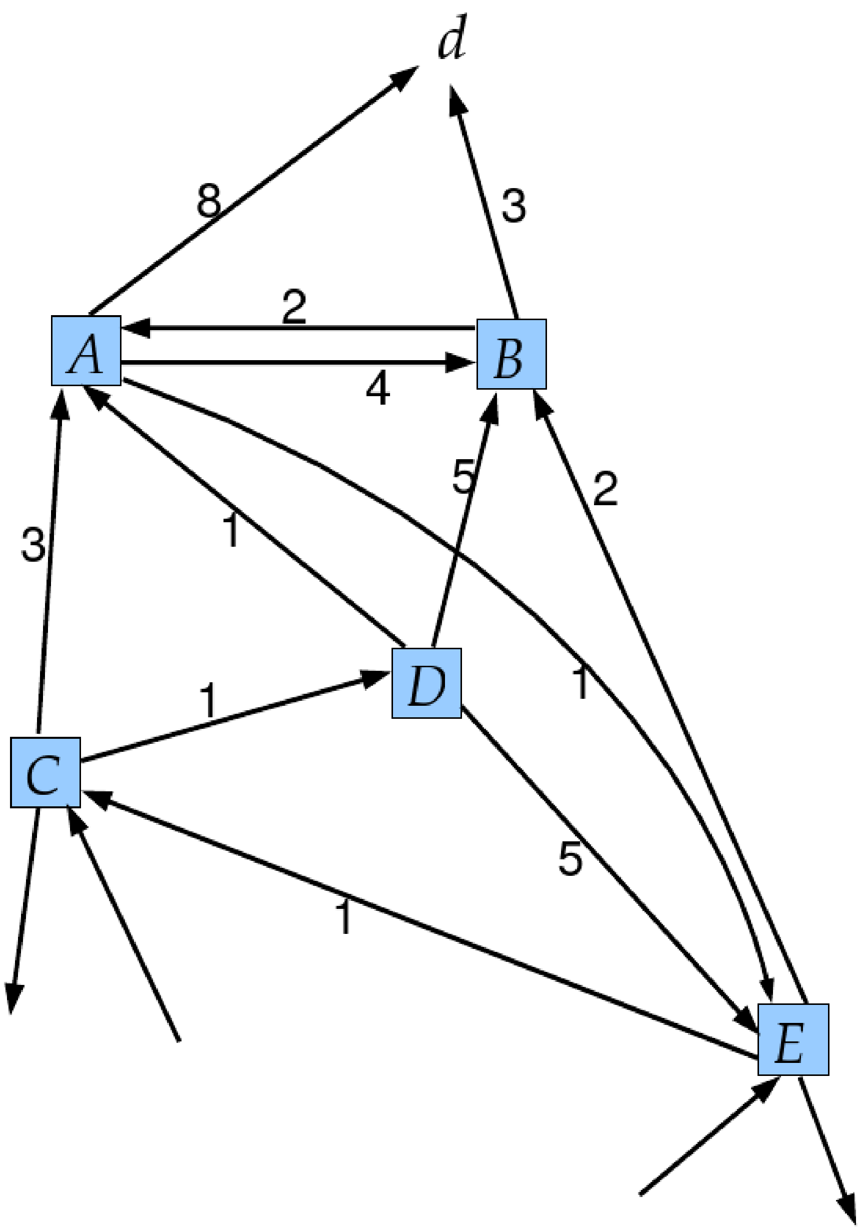
additive measure on links



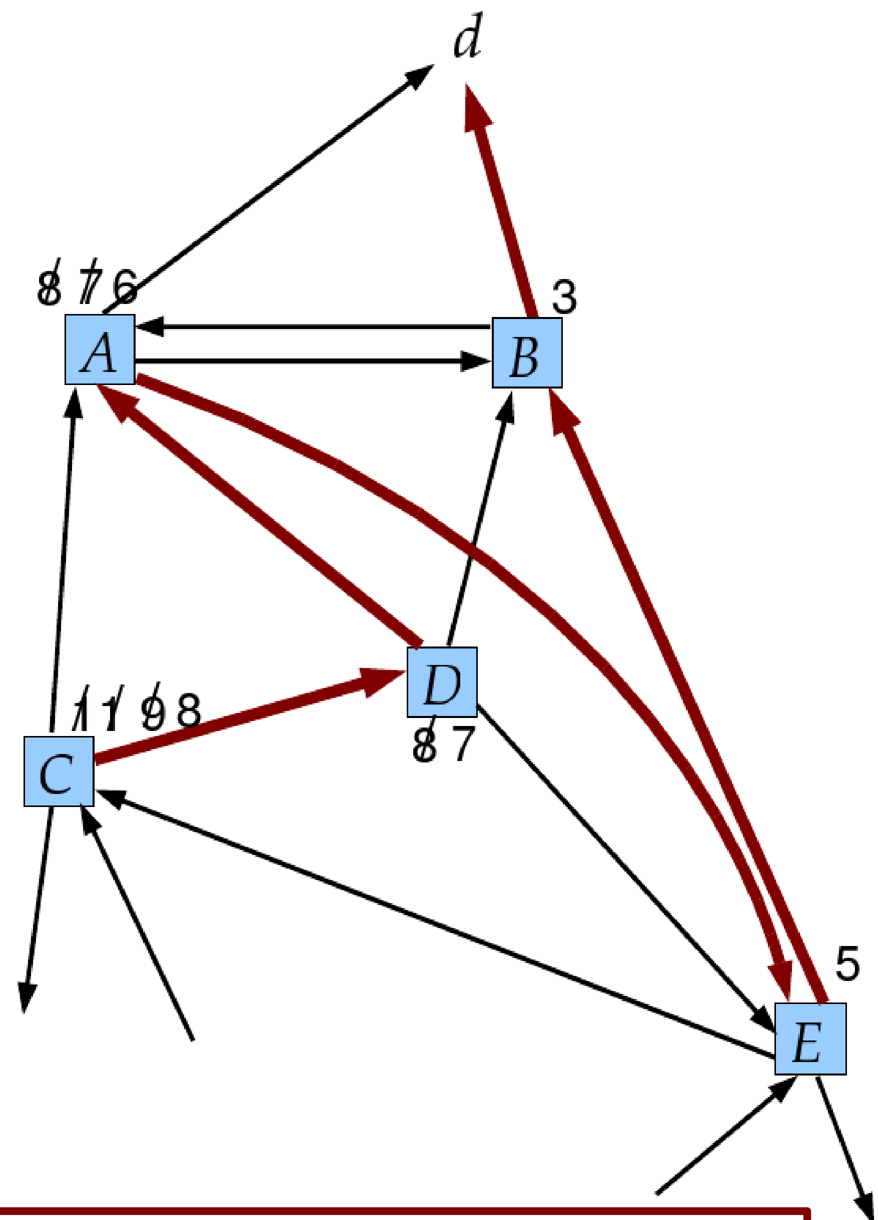
at end of time = 5



additive measure on links



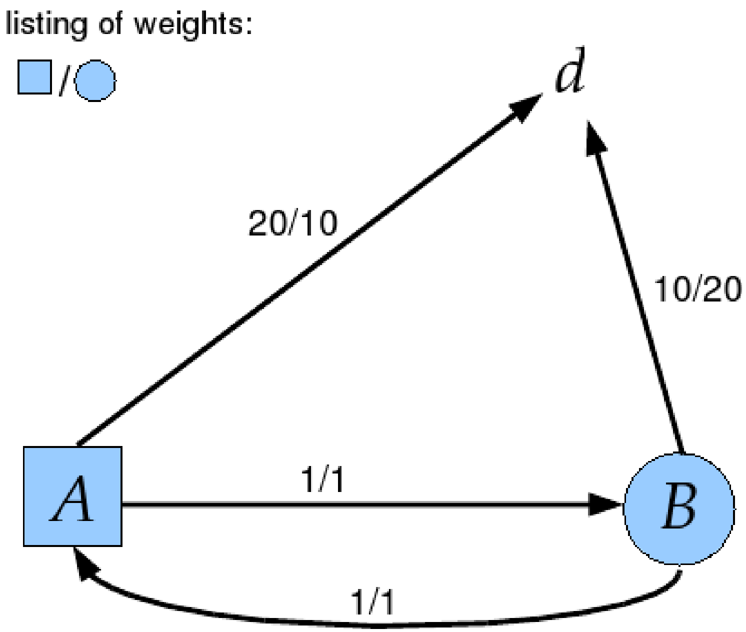
at end of time = 5



FACT.

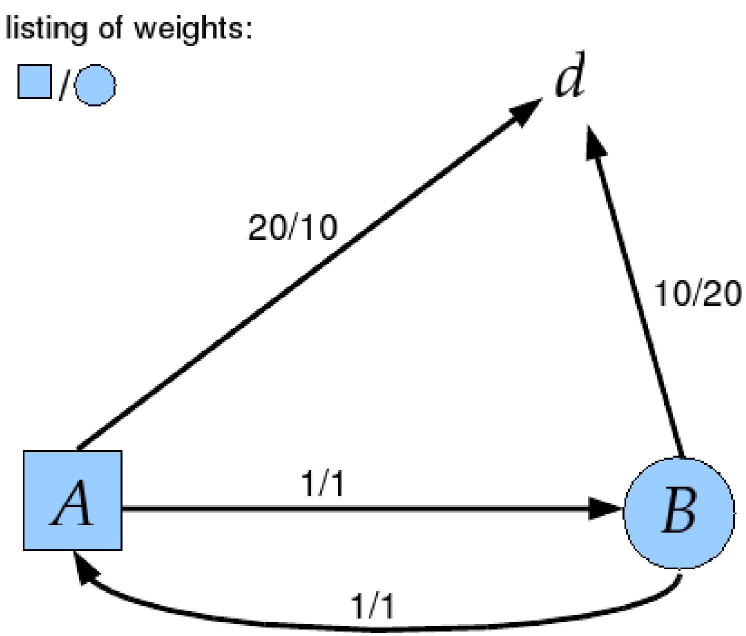
1. **Each node finds a stable path to *d*.**
2. **If the network is finite, a MST rooted at *d* is constructed.**

additive measure on links

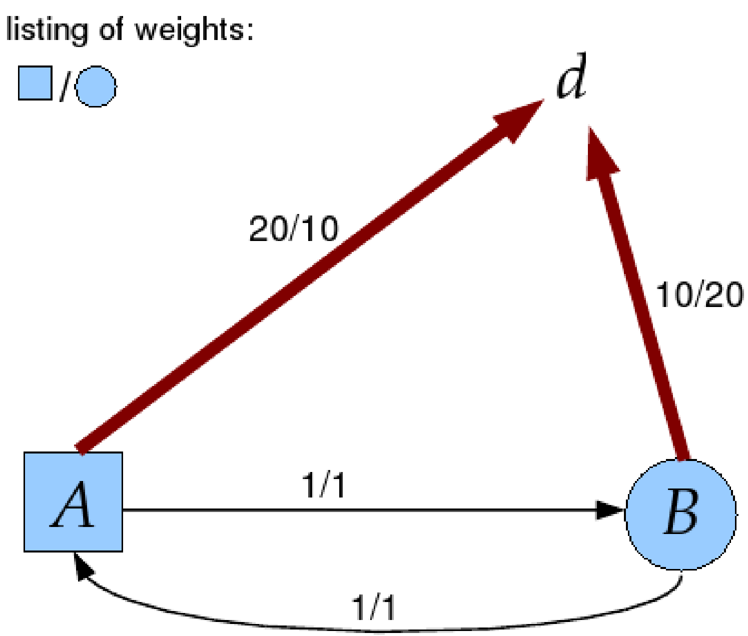


two additive measures on links

at end of time = 1

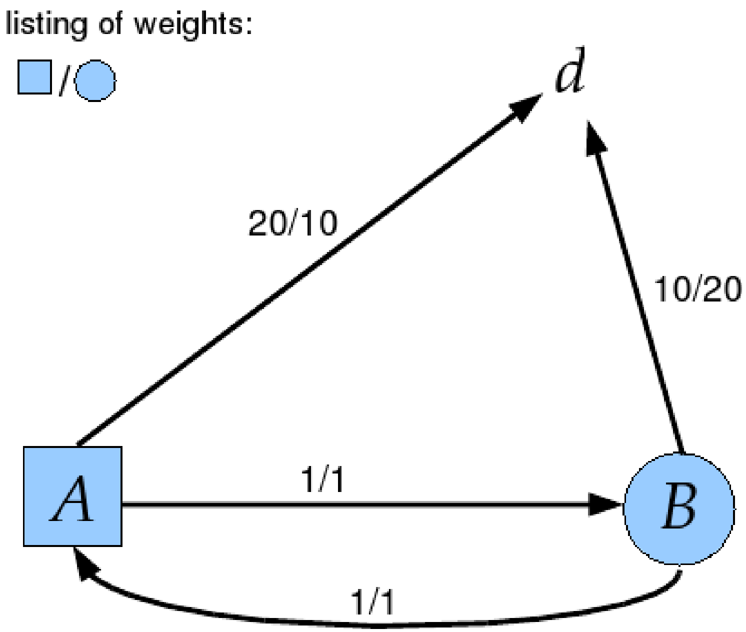


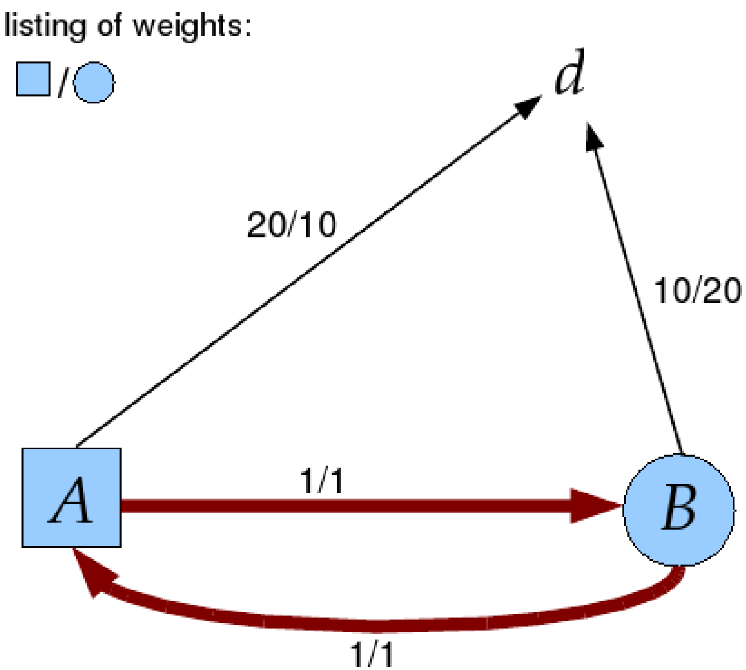
two additive measures on links



after *d* broadcasts to *A* and *B*

at end of time = 2

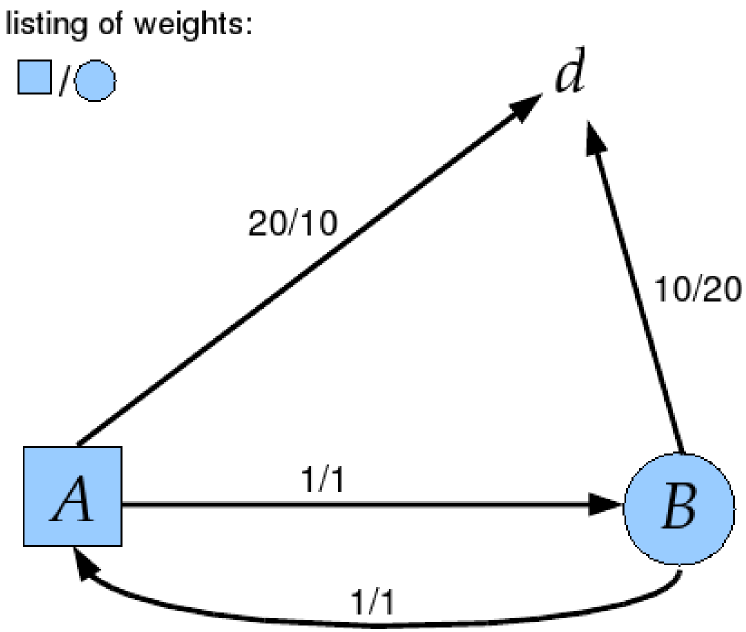


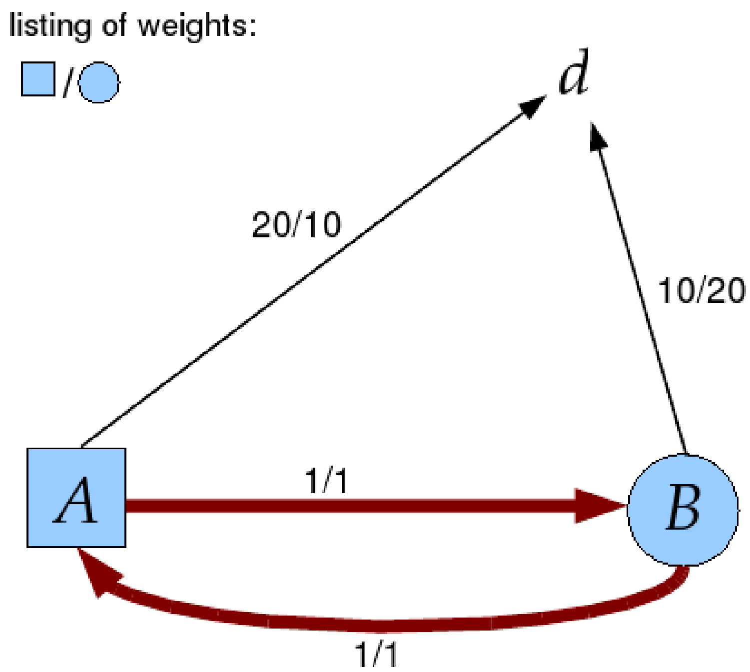


two additive measures on links

after *A* broadcasts to *B* and *B* broadcasts to *A*

at end of time = 2



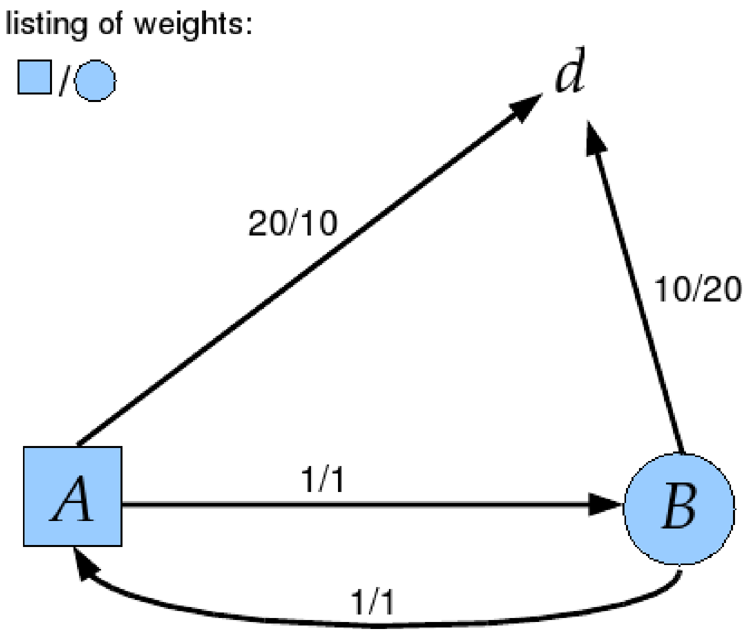


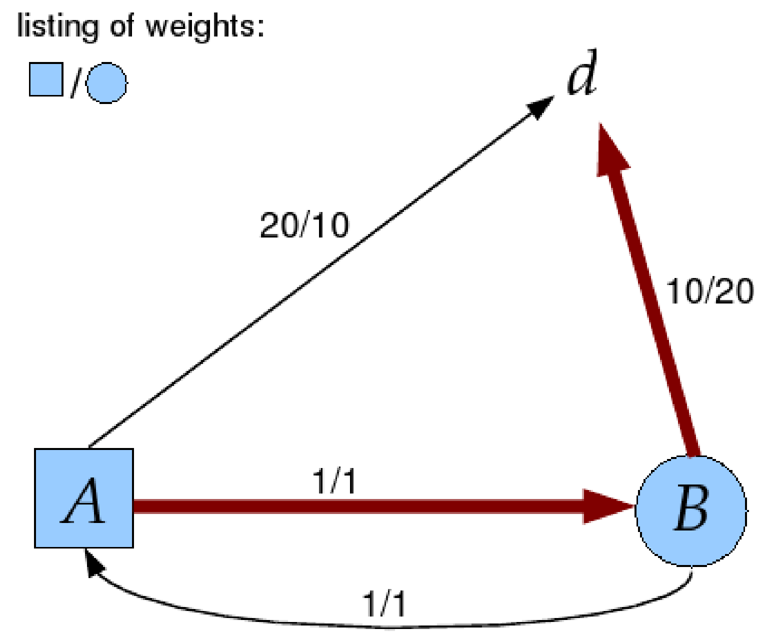
two additive measures on links

after *A* broadcasts to *B* and *B* broadcasts to *A*

FACT. No node (other than *d*) ever finds a stable path to *d*.

But there are stable configurations!

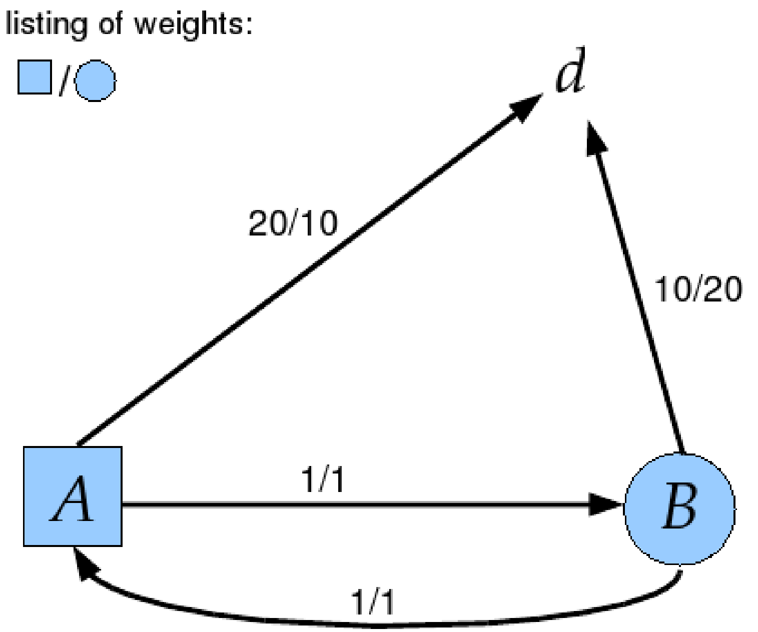


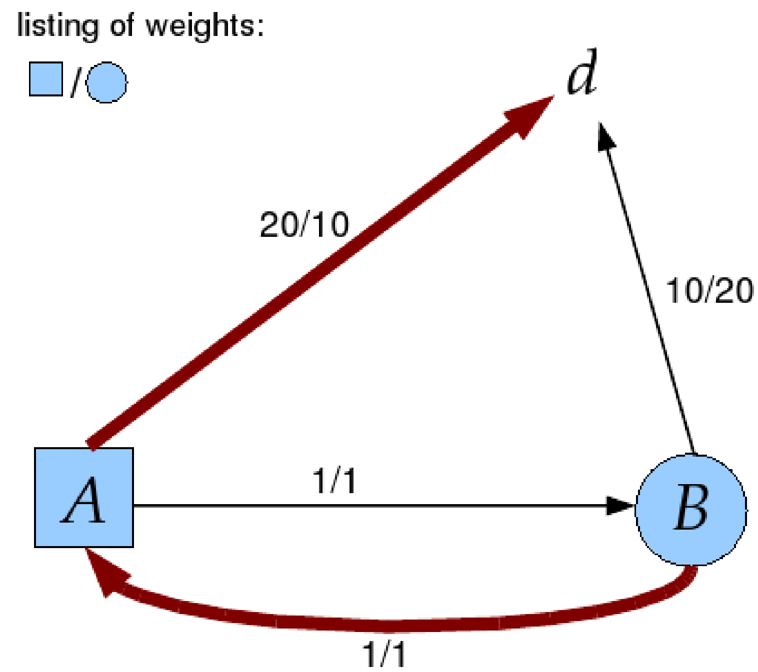


stable configuration 1

two additive measures on links

But there are stable configurations!

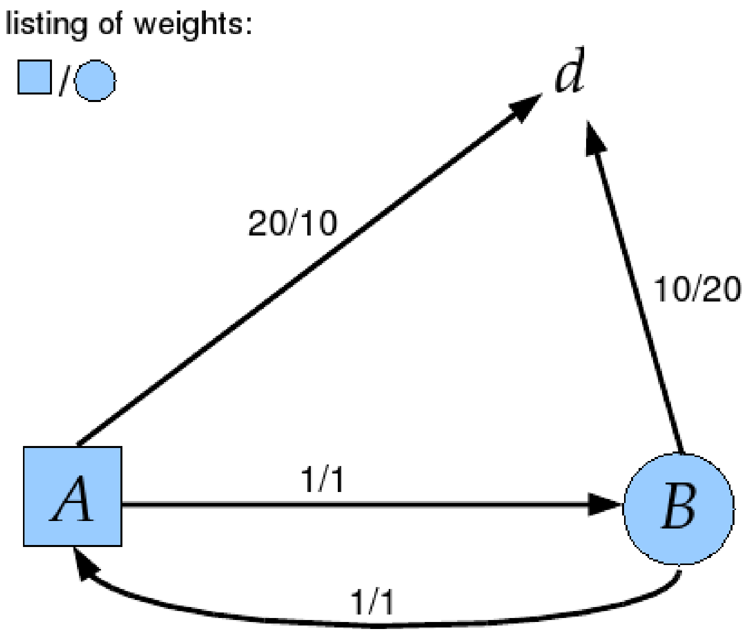


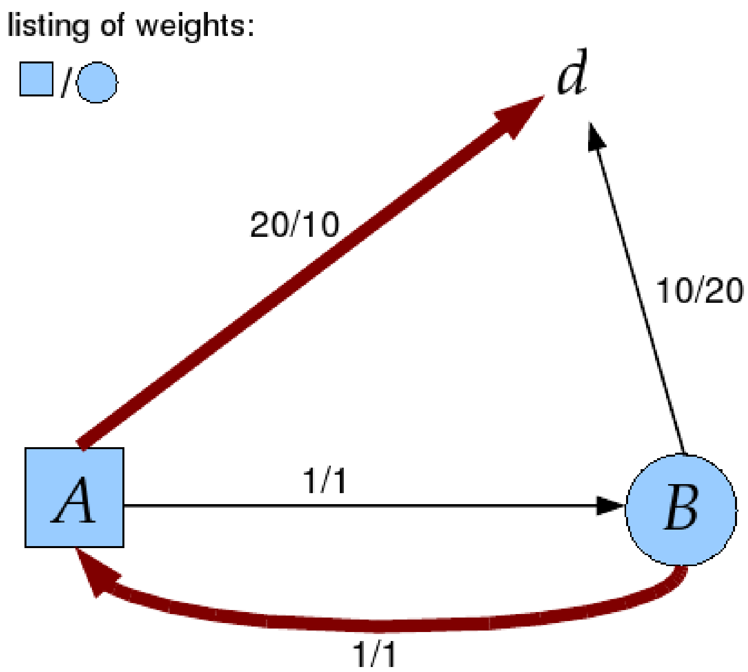


stable configuration 2

two additive measures on links

But there are stable configurations!



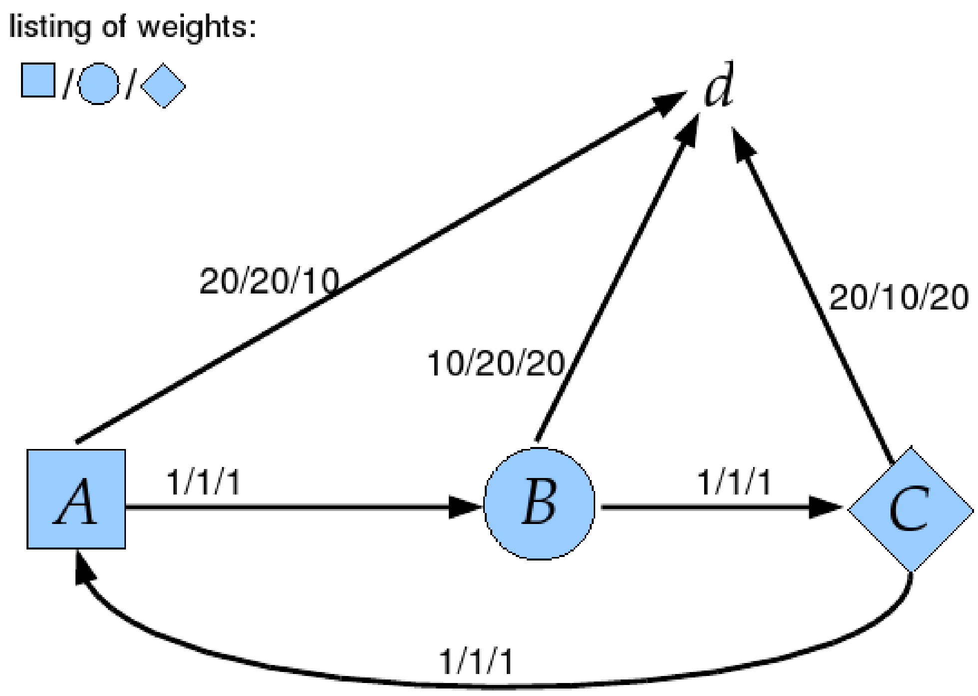


stable configuration 2

two additive measures on links

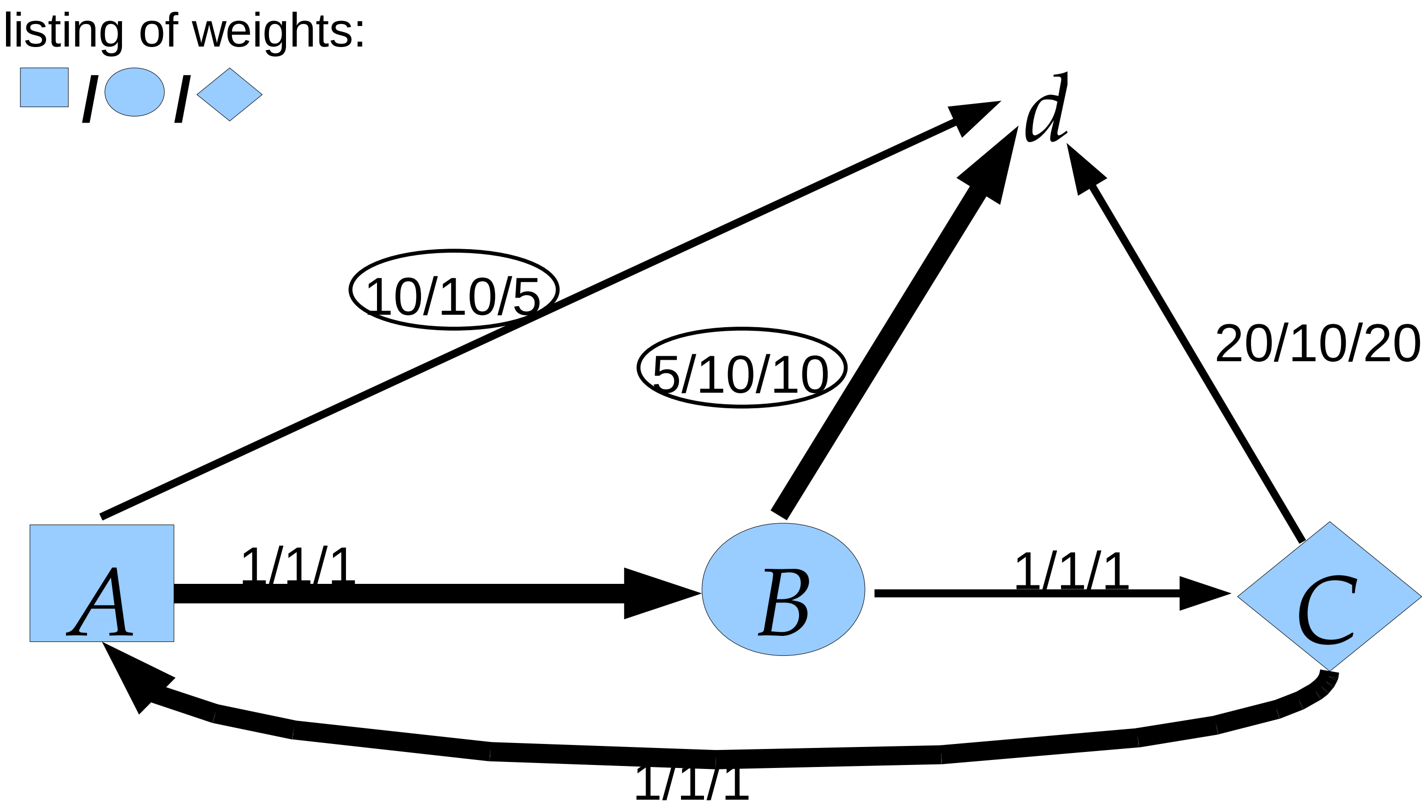
Is synchrony the culprit?
Perhaps there is an asynchronous procedure that will find stable paths ...

No! There are networks where no node (other than *d*) can find a stable path to *d* – regardless of the method used.

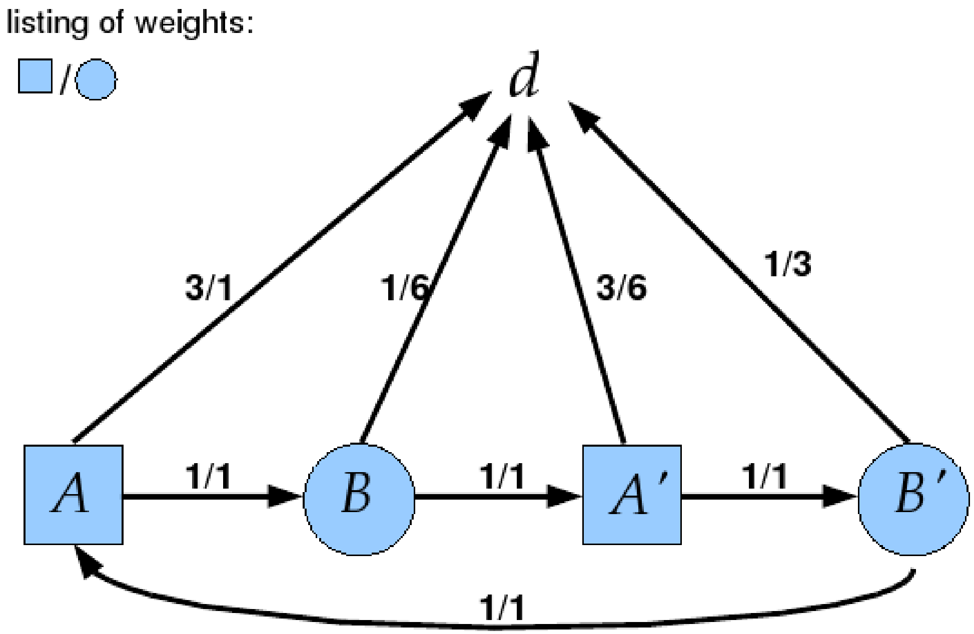


- **three additive measures on links**
- **inherently unstable network**

Same network topology, slightly adjusted measures.



- **three additive measures on links**
- **exactly one stable configuration**

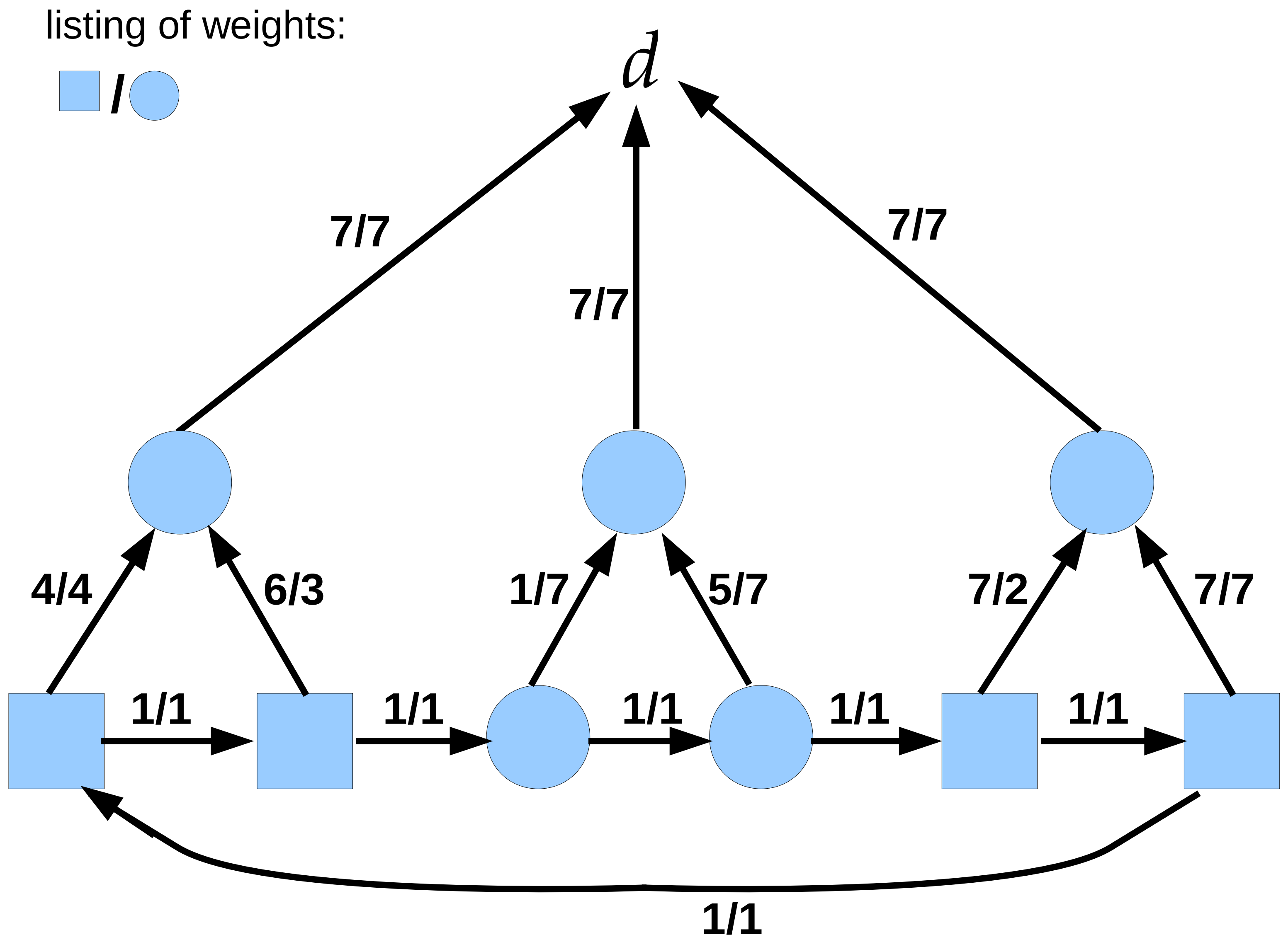


- **two additive measures on links**
- **inherently unstable network**

An instance of the Stable Paths Problem (SPP) is a network of Autonomous Systems (AS) each with a particular routing policies.

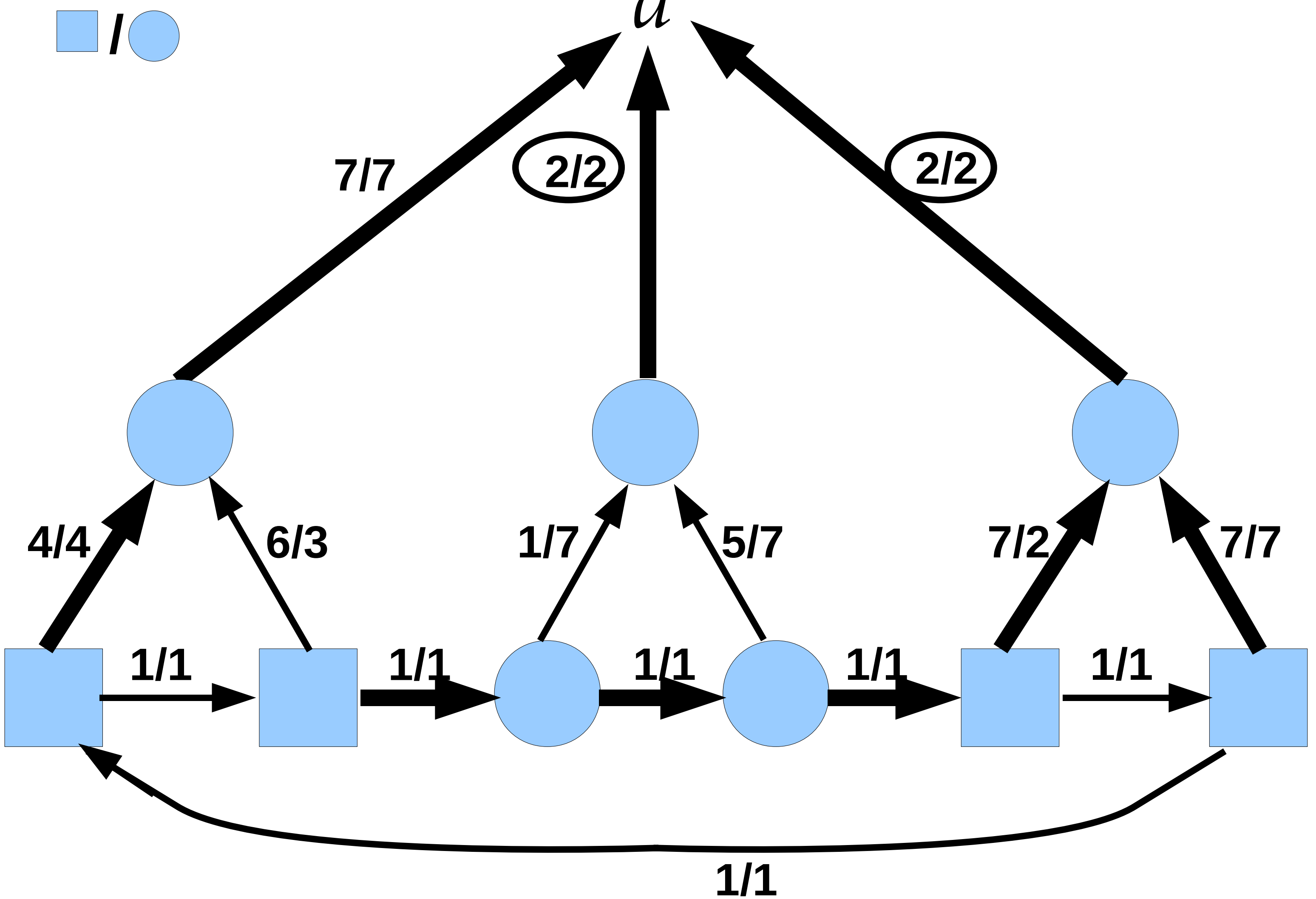
An instance of SPP is finite if the underlying network of AS's is finite.

THEOREM. It is an NP-complete question whether a finite instance of SPP, with at least two routing policies, has a stable configuration.



- **two additive measures on links**
- **inherently unstable network**

listing of weights:



- **two additive measures on links**
- **exactly one stable configuration**

References

1. *On the Stable Paths Problem and a Restricted Variant*
Kevin Donnelly and Assaf Kfoury
BU Tech Report, 5 February 2008

2. **Ibis**
lightweight logical framework and proof assistant
Andrei Lapets
http://safre.org/

Thank You!

Questions?