Lecture #4

- Conspiracy in the Take-Grant Protection Model
- *de facto* rules (information flow)
- Knowing in a combined graph

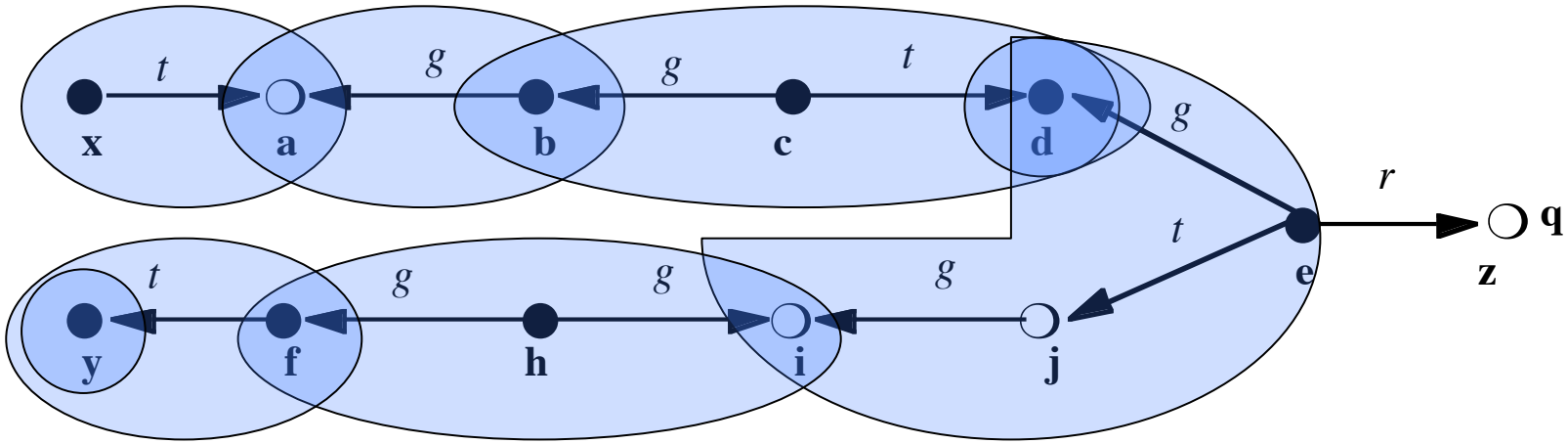
Conspiracy

- Minimum number of actors to generate a witness for *can•share*(α, **x**, **y**, G_0)
  - Actor is defined as **x** such that **x** initiates ϱ_i
- Access set describes the "reach" of a subject
- Deletion set is set of vertices that cannot be involved in a transfer of rights
- Build *conspiracy graph* to capture how rights flow, and derive actors from it

Access Set

- *Access set A(***y***) with focus* **y**: set of vertices:
  - { **y** }
  - { **x** | **y** initially spans to **x** }
  - { **x** | **y** terminally spans to **x** }
- Idea is that focus can give rights to, or acquire rights from, a vertex in this set

Example



- $A(\mathbf{x}) = \{ \mathbf{x}, \mathbf{a} \}$
- $A(\mathbf{b}) = \{ \mathbf{b}, \mathbf{a} \}$
- $A(\mathbf{c}) = \{ \mathbf{c}, \mathbf{b}, \mathbf{d} \}$
- $A(\mathbf{d}) = \{ \mathbf{d} \}$
- $A(\mathbf{e}) = \{ \mathbf{e}, \mathbf{d}, \mathbf{i}, \mathbf{j} \}$
- $A(\mathbf{h}) = \{ \mathbf{h}, \mathbf{f}, \mathbf{i} \}$
- $A(\mathbf{f}) = \{ \mathbf{f}, \mathbf{y} \}$
- $A(\mathbf{y}) = \{ \mathbf{y} \}$

tg-sink

- $\mathbf{x_0}$, only incoming *t* edge
- $\mathbf{x_i}$, two incoming incident edges, both labeled *t* or both labeled *g*
- $\mathbf{x_n}$, only incoming *g* edge

Necessity

- Lower bound on number of conspirators
  - Rights can be transmitted to any vertex in the access set
  - Rights can be "passed along" through the overlap of access sets, *unless* common vertex cannot initiate rule (*tg*-sink)
  - If only common vertex is *tg*-sink, must aid in transfer

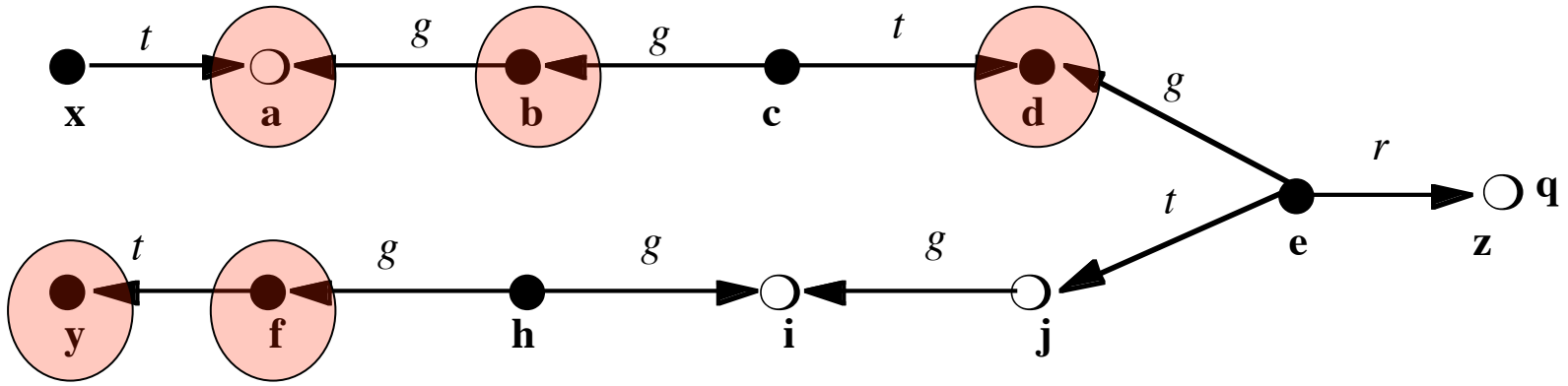
Necessity Theorem

- Let *can•share*(α, **p**, **q**, *G*) hold, and define G_0 to be *G*–{ **q** }. Let *k* be the number of access sets in a minimal cover of G_0, and let *l* be the number of *tg*-sinks. Then *k* + *l* initiators are necessary to witness *can•share*(α, **p**, **q**, *G*).

Deletion Set

- Deletion set $\delta(\mathbf{y}, \mathbf{y}')$: contains those vertices in $A(\mathbf{y}) \cap A(\mathbf{y}')$ such that:
  - **y** initially spans to **z** and $\mathbf{y}'$ terminally spans to **z**;
  - **y** terminally spans to **z** and $\mathbf{y}'$ initially spans to **z**;
  - **z** = **y**
  - **z** = $\mathbf{y}'$
- Idea is that rights can be transferred between **y** and $\mathbf{y}'$ if this set non-empty

Example



- $\delta(\mathbf{x}, \mathbf{b}) = \{ \mathbf{a} \}$
- $\delta(\mathbf{b}, \mathbf{c}) = \{ \mathbf{b} \}$
- $\delta(\mathbf{c}, \mathbf{d}) = \{ \mathbf{d} \}$
- $\delta(\mathbf{c}, \mathbf{e}) = \{ \mathbf{d} \}$
- $\delta(\mathbf{d}, \mathbf{e}) = \{ \mathbf{d} \}$
- $\delta(\mathbf{y}, \mathbf{f}) = \{ \mathbf{y} \}$
- $\delta(\mathbf{h}, \mathbf{f}) = \{ \mathbf{f} \}$
- $\delta(\mathbf{e}, \mathbf{h}) = \varnothing$

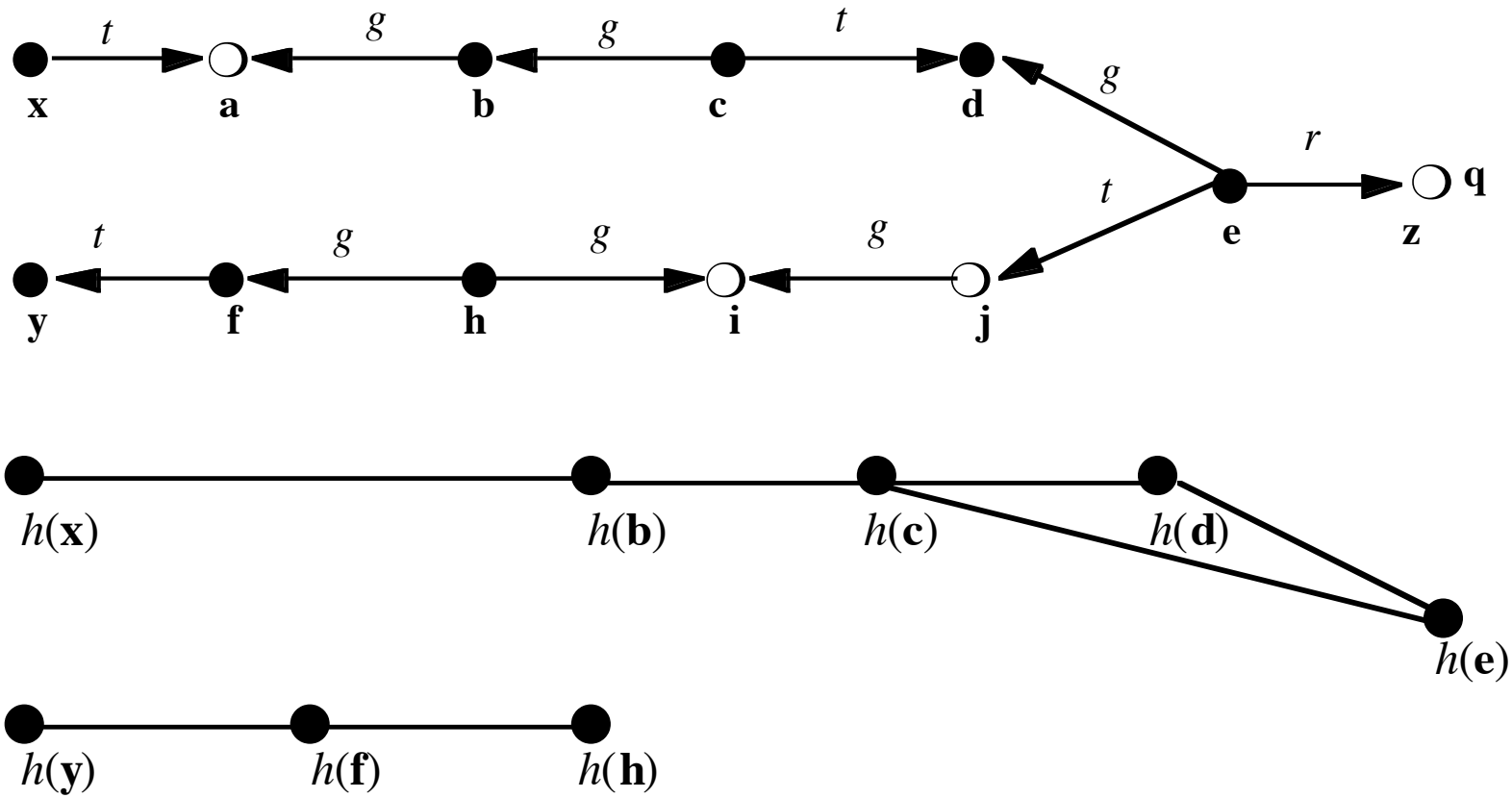
Sufficiency

- Consider $A(\mathbf{x}_i) \cap A(\mathbf{x}_{i+1}) = \{ \mathbf{y} \}$
  - If edges incoming to **y** are *both t* or *both g*, **y** must act
  - If edges incoming to **y** are *t* and *g*, it's a bridge and **y** need not act
- So, in first case, need one additional operation initiated by **y**
- Note: **y** is a *tg*-sink in these cases

Conspiracy Graph

- Abstracted graph H from G_0:
  - Each subject $\mathbf{x} \in G_0$ corresponds to a vertex $h(\mathbf{x}) \in H$
  - If $\delta(\mathbf{x}, \mathbf{y}) \neq \varnothing$, there is an edge between $h(\mathbf{x})$ and $h(\mathbf{y})$ in H
- Idea is that if $h(\mathbf{x})$, $h(\mathbf{y})$ are connected in H, then rights can be transferred between **x** and **y** in G_0

Example



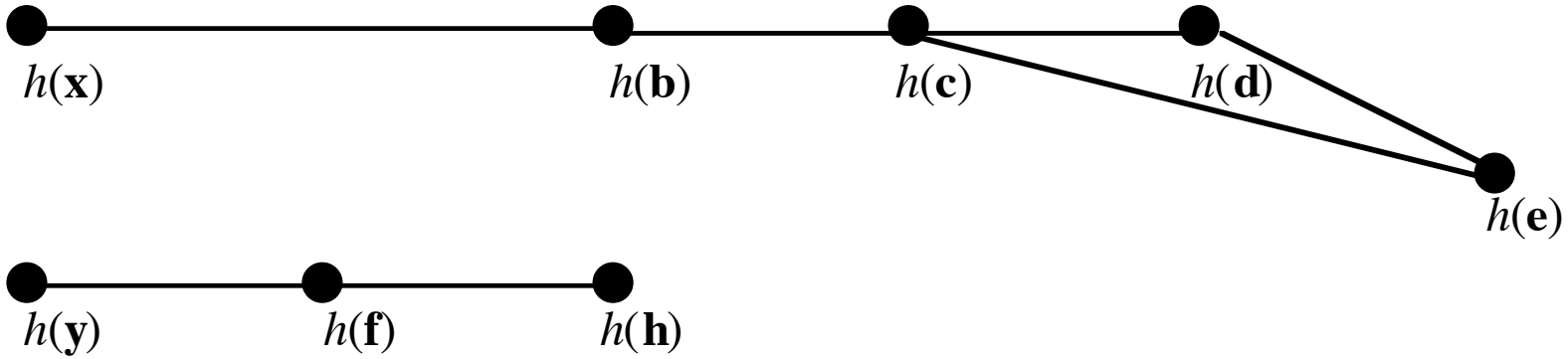
Sharing

- $I(\mathbf{x})$: $h(\mathbf{x})$, all vertices $h(\mathbf{y})$ such that **y** initially spans to **x**
- $T(\mathbf{x})$: $h(\mathbf{x})$, all vertices $h(\mathbf{y})$ such that **y** terminally spans to **x**
- Theorem: *can*•*share*(α, **x**, **y**, G_0) iff there exists a path from some $h(\mathbf{p})$ in $I(\mathbf{x})$ to some $h(\mathbf{q})$ in $T(\mathbf{y})$
  - Idea: path exists if access sets overlap and rights can be transferred between endpoints
  - Note *tg*-sinks correspond to singleton access sets with foci that must act (idea of deletion sets)

Counting Conspirators

- Theorem: if there are l vertices on shortest path between $h(\mathbf{p})$, $h(\mathbf{q})$ in above theorem, l conspirators necessary and sufficient to witness
  - Follows immediately from previous two theorems, definitions

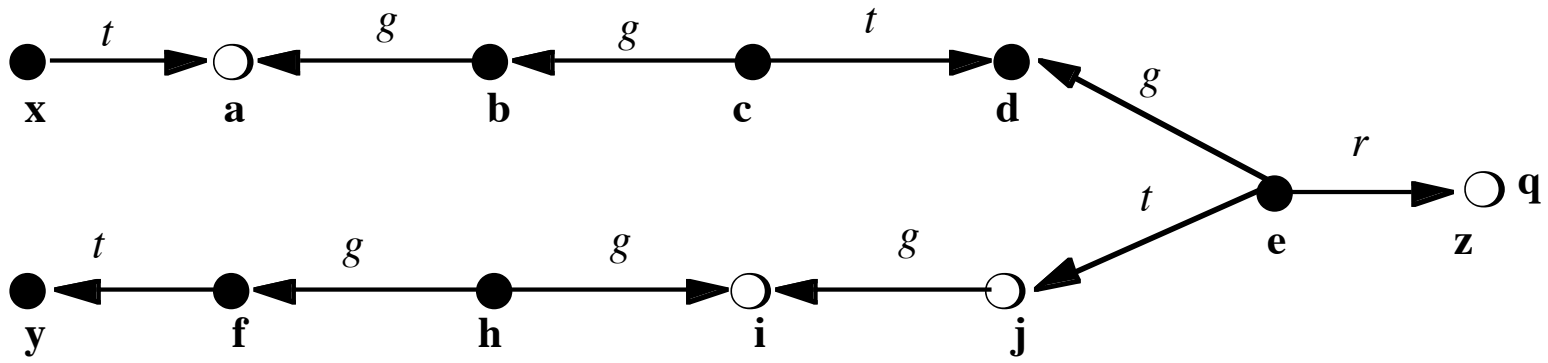
Example: Conspirators



- $I(\mathbf{x}) = \{ h(\mathbf{x}) \}, T(\mathbf{z}) = \{ h(\mathbf{e}) \}$
- Path between $h(\mathbf{x})$, $h(\mathbf{e})$ so $can\text{•}share(r, \mathbf{x}, \mathbf{z}, G_0)$
- Shortest path between $h(\mathbf{x})$, $h(\mathbf{e})$ has 4 vertices

$\Rightarrow$ Conspirators are **e**, **c**, **b**, **x**

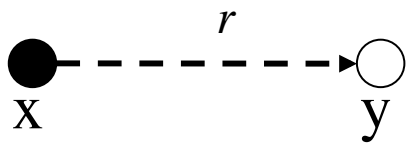
Example: Witness



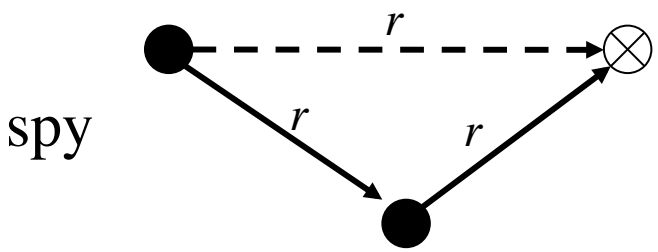
- **e** grants (*r* to **z**) to **d**
- **c** takes (*r* to **z**) from **d**
- **c** grants (*r* to **z**) to **b**
- **b** grants (*r* to **z**) to **a**
- **x** takes (*r* to **z**) from **a**

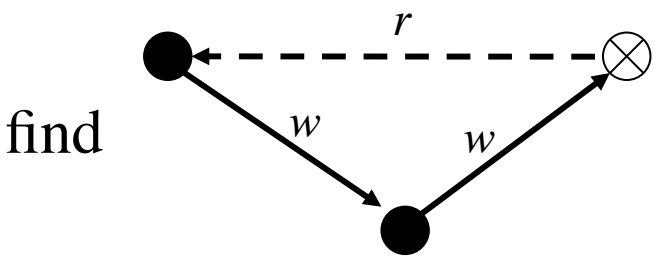
de facto Rules

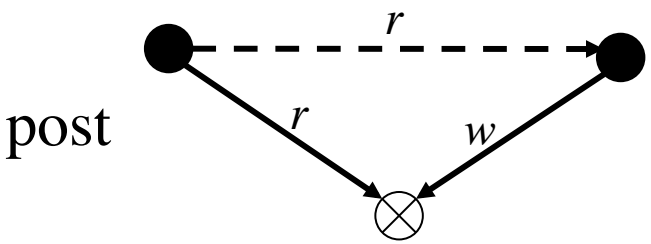
- These deal with information flow
- Not graph rewriting rules
  - Add no edges
  - Instead, represent flows by "implicit" edges, shown as:

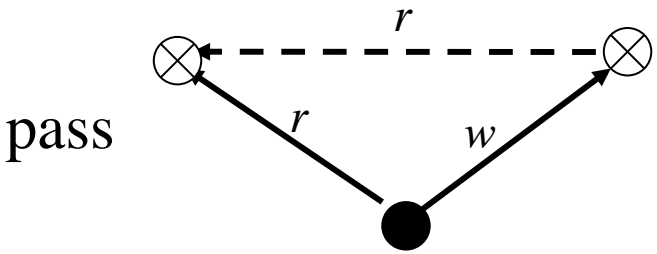


Rules

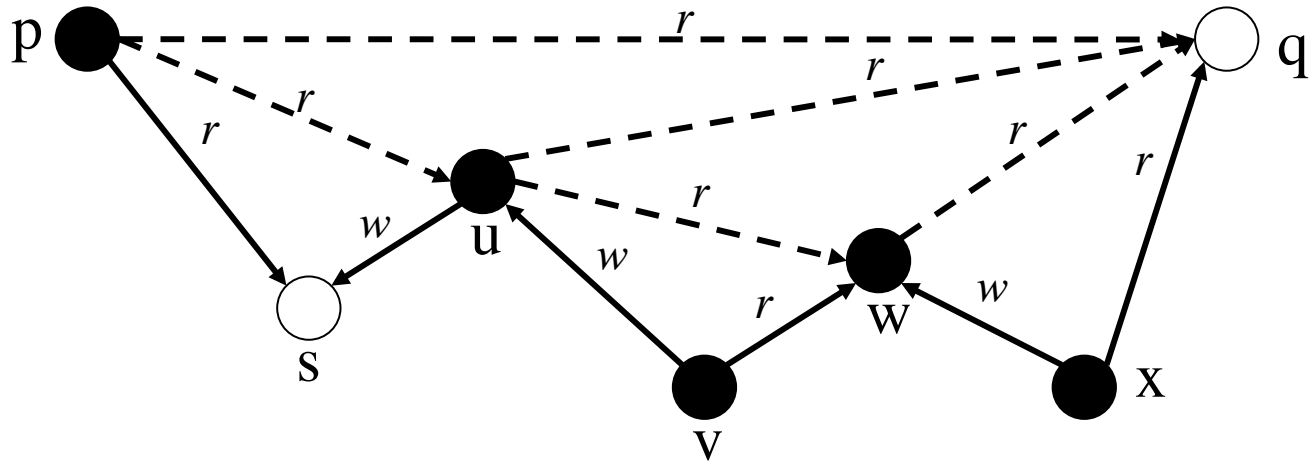








Example



u posts through **s** to **p**
v passes from **w** to **u**
w spies through **x** to **q**

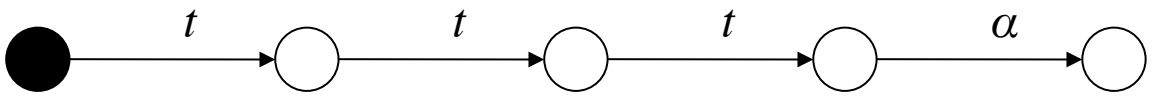
u spies through **w** to **q**
p spies through **u** to **q**

can•know

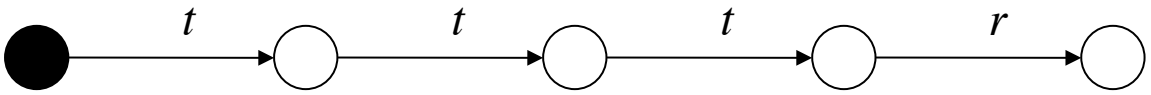
Definition:

- *can•know*(**x**, **y**, G_0) if, and only if, there is a sequence of protection graphs $G_0, \ldots, G_n$ such that $G_0 \vdash^* G_n$ using *de jure* or *de facto* rules and in G_n there is an edge from **x** to **y** labeled *r*.

Combined Transfers



terminal span

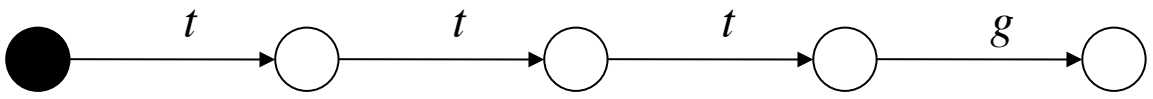


rw-terminal span

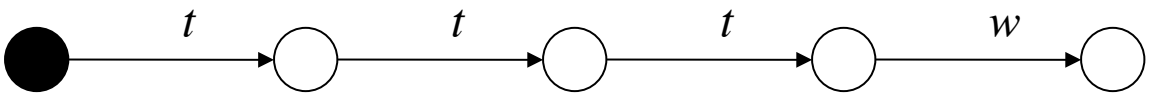
The subject can acquire α rights over the last object

The subject can acquire *r* rights over the last object

Combined Transfers



initial span

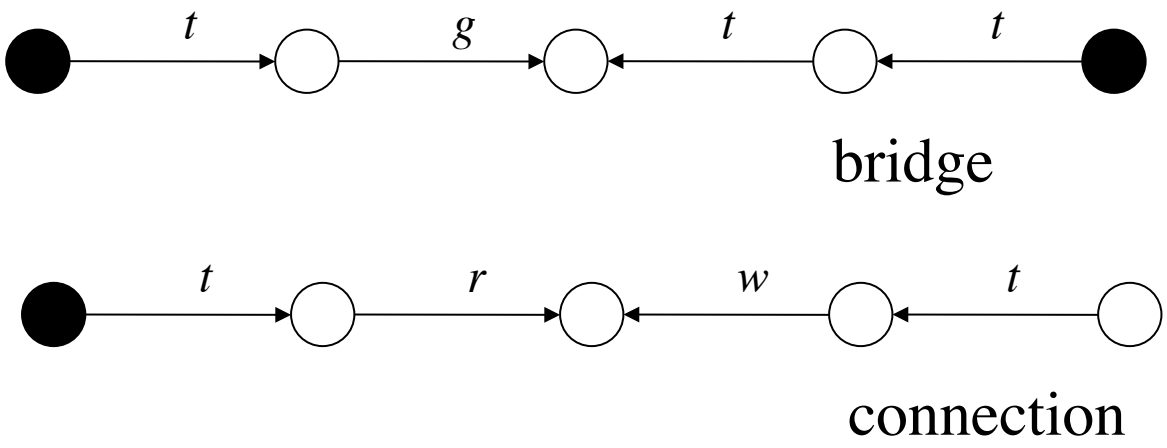


rw-initial span

The subject can acquire *g* rights over the last object

The subject can acquire *w* rights over the last object

Combined Transfers



Just as rights can be transferred over a bridge, information can flow over a connection