

ECS 235B Module 12

Stealing in the Take-Grant Model

can•steal Predicate

Definition:

- $\text{can}\bullet\text{steal}(r, \mathbf{x}, \mathbf{y}, G_0)$ if, and only if, there is no edge from \mathbf{x} to \mathbf{y} labeled r in G_0 , and there exists a sequence of protection graphs G_0, G_1, \dots, G_n for which the following hold simultaneously:
 - a) There is an edge from \mathbf{x} to \mathbf{y} labeled r in G_n
 - b) There is a sequence of rule applications ρ_1, \dots, ρ_n such that $G_{i-1} \vdash G_i$ using ρ_i
 - c) For all vertices \mathbf{v} and \mathbf{w} in G_{i-1} , $1 \leq i < n$, if there is an edge from \mathbf{v} to \mathbf{y} labeled r , then ρ_i is **not** of the form “ \mathbf{v} grants (r to \mathbf{y}) to \mathbf{w} ”

can•steal Theorem

- $\text{can}\bullet\text{steal}(\alpha, \mathbf{x}, \mathbf{y}, G_0)$ if, and only if, the following hold simultaneously:
 - a) There is no edge from \mathbf{x} to \mathbf{y} labeled α in G_0
 - b) There exists a subject \mathbf{x}' such that $\mathbf{x}' = \mathbf{x}$ or \mathbf{x}' initially spans to \mathbf{x}
 - c) There exists a vertex \mathbf{s} with an edge labeled α to \mathbf{y} in G_0
 - d) $\text{can}\bullet\text{share}(t, \mathbf{x}', \mathbf{s}, G_0)$ holds

Outline of Proof

\Rightarrow : Assume conditions hold

- **x** subject
 - **x** gets t rights to **s**, then takes α to **y** from **s**
- **x** object
 - $can\bullet share(t, \mathbf{x}', \mathbf{s}, G_0)$ holds
 - If \mathbf{x}' has no α edge to **y** in G_0 , \mathbf{x}' takes (α to **y**) from **s** and grants it to **x**
 - If \mathbf{x}' has α edge to **y** in G_0 , \mathbf{x}' creates surrogate \mathbf{x}'' , gives it (t to **s**) and (g to \mathbf{x}''); then \mathbf{x}'' takes (α to **y**) and grants it to **x**

Outline of Proof

\Leftarrow : Assume $can\bullet steal(\alpha, \mathbf{x}, \mathbf{y}, G_0)$ holds

- First two conditions immediate from definition of $can\bullet steal$, $can\bullet share$
- Third condition immediate from theorem of conditions for $can\bullet share$
- Fourth condition: ρ minimal length sequence of rule applications deriving G_n from G_0 ; i smallest index such that $G_{i-1} \vdash G_i$ by rule ρ_i and adding α from some \mathbf{p} to \mathbf{y} in G_i
 - What is ρ_i ?

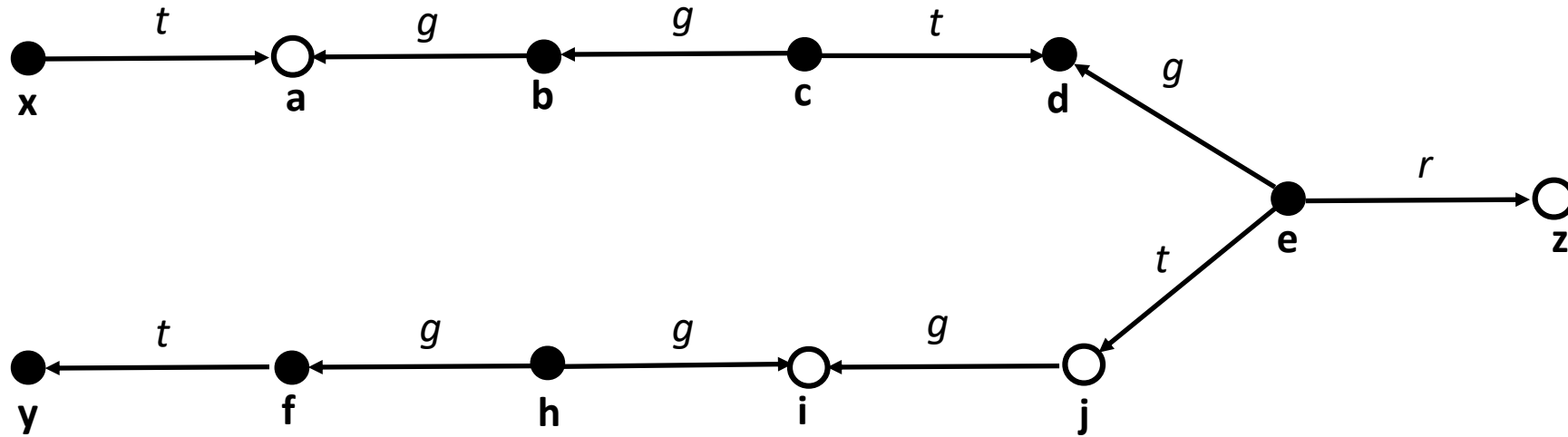
Outline of Proof

- Not remove or create rule
 - \mathbf{y} exists already
- Not grant rule
 - G_i first graph in which edge labeled α to \mathbf{y} is added, so by definition of *can•share*, cannot be grant
- take rule: so *can•share*($t, \mathbf{p}, \mathbf{s}, G_0$) holds
 - So is subject \mathbf{s}' such that $\mathbf{s}' = \mathbf{s}$ or terminally spans to \mathbf{s}
 - Sequence of islands with $\mathbf{x}' \in I_1$ and $\mathbf{s}' \in I_n$
- Derive witness to *can•share*($t, \mathbf{x}', \mathbf{s}, G_0$) that does not use “ \mathbf{s} grants (α to \mathbf{y}) to” anyone

Conspiracy

- Minimum number of actors to generate a witness for $can\bullet share(\alpha, \mathbf{x}, \mathbf{y}, G_0)$
- 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

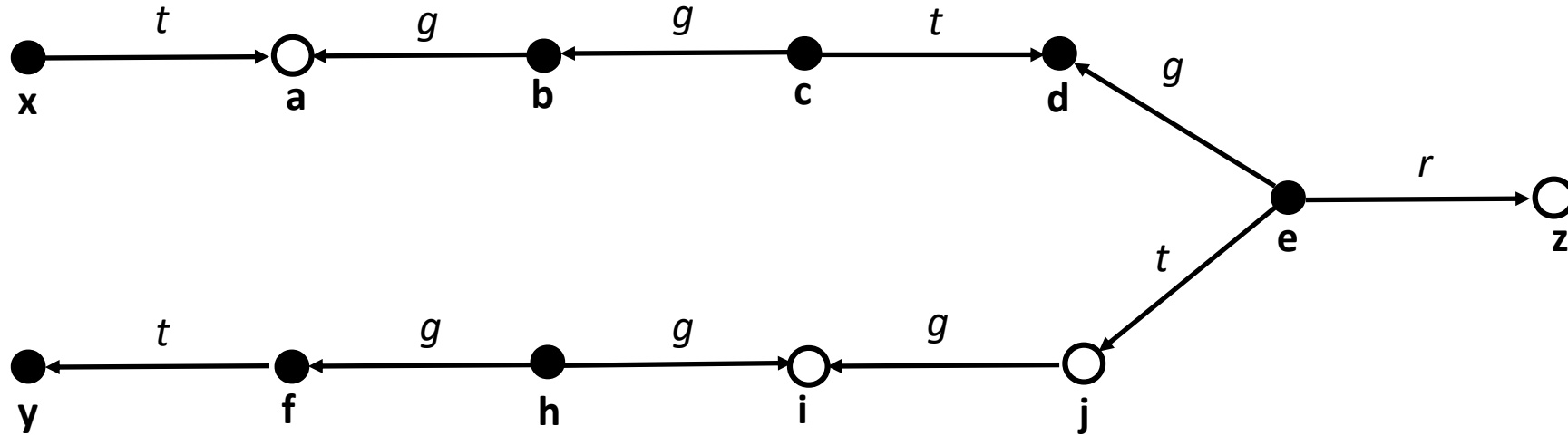
Example



Access Set

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

Example

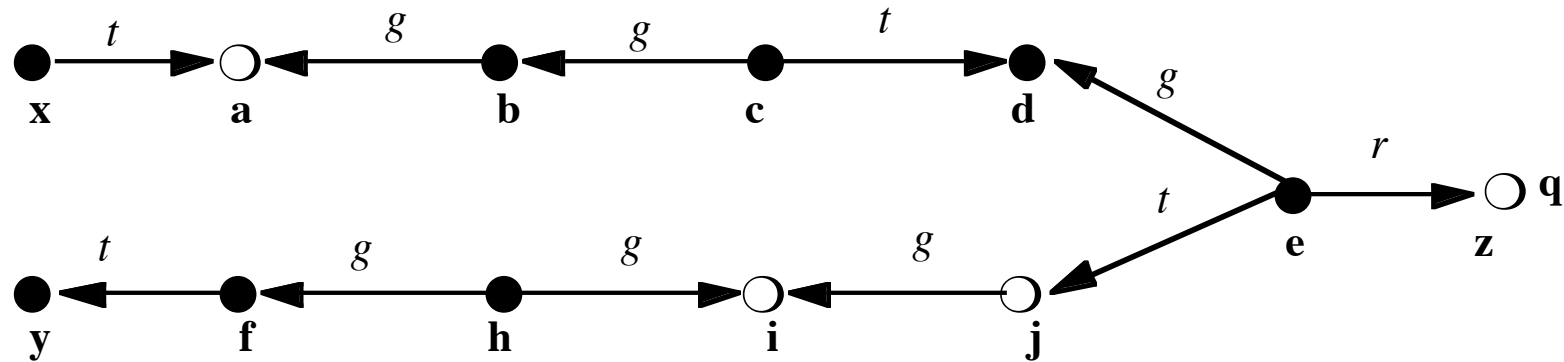


- $A(\mathbf{x}) = \{ \mathbf{x}, \mathbf{a} \}$
- $A(\mathbf{b}) = \{ \mathbf{b}, \mathbf{a} \}$
- $A(\mathbf{c}) = \{ \mathbf{c}, \mathbf{b}, \mathbf{d} \}$
- $A(\mathbf{d}) = \{ \mathbf{d} \}$
- $A(\mathbf{e}) = \{ \mathbf{e}, \mathbf{d}, \mathbf{i}, \mathbf{j} \}$
- $A(\mathbf{y}) = \{ \mathbf{y}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

Deletion Set

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

Example



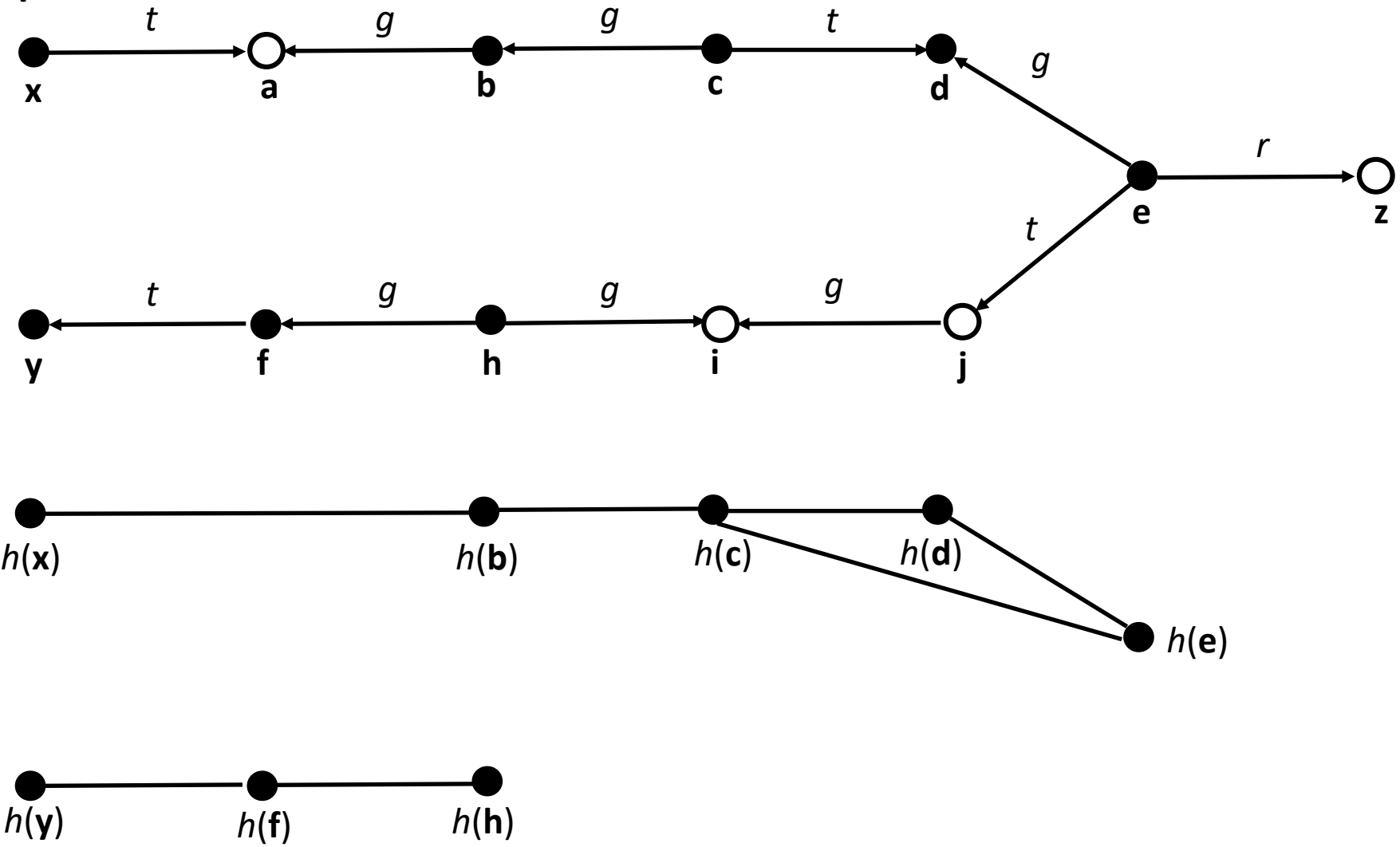
- $\delta(\mathbf{x}, \mathbf{b}) = \{ \mathbf{a} \}$
- $\delta(\mathbf{b}, \mathbf{c}) = \{ \mathbf{b} \}$
- $\delta(\mathbf{c}, \mathbf{d}) = \{ \mathbf{d} \}$
- $\delta(\mathbf{c}, \mathbf{e}) = \{ \mathbf{d} \}$

- $\delta(\mathbf{d}, \mathbf{e}) = \{ \mathbf{d} \}$
- $\delta(\mathbf{y}, \mathbf{f}) = \{ \mathbf{y} \}$
- $\delta(\mathbf{h}, \mathbf{f}) = \{ \mathbf{f} \}$

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 $\delta(\mathbf{x}, \mathbf{y}) \neq \emptyset$, 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 \mathbf{x} and \mathbf{y} in G_0

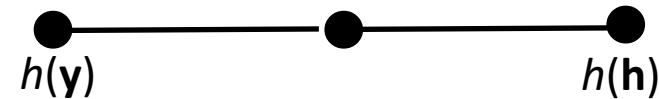
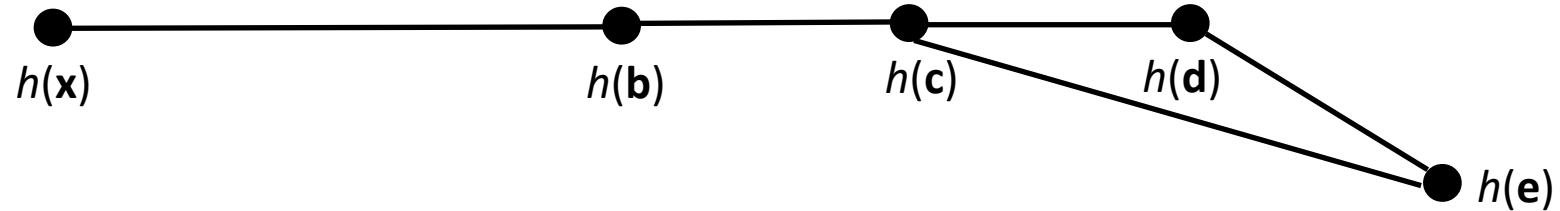
Example



Results

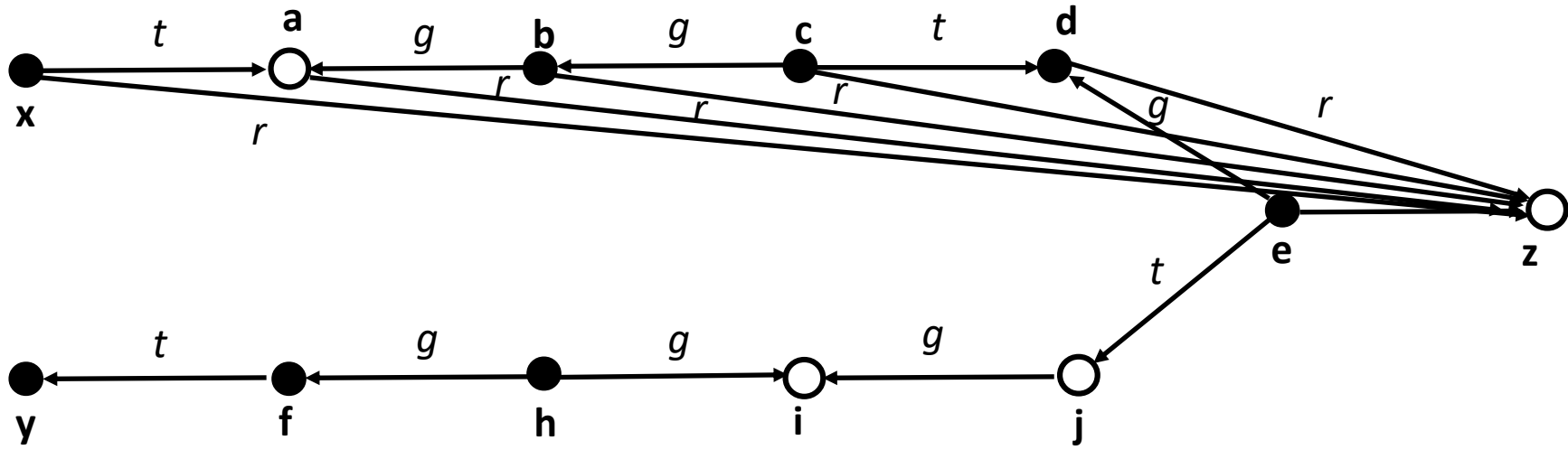
- $I(\mathbf{x})$: $h(\mathbf{x})$, all vertices $h(\mathbf{y})$ such that \mathbf{y} initially spans to \mathbf{x}
- $T(\mathbf{x})$: $h(\mathbf{x})$, all vertices $h(\mathbf{y})$ such that \mathbf{y} terminally spans to \mathbf{x}
- Theorem: $can_share(\alpha, \mathbf{x}, \mathbf{y}, G_0)$ iff there exists a path from some $h(\mathbf{p})$ in $I(\mathbf{x})$ to some $h(\mathbf{q})$ in $T(\mathbf{y})$
- Theorem: l vertices on shortest path between $h(\mathbf{p}), h(\mathbf{q})$ in above theorem; l conspirators necessary and sufficient to witness

Example: Conspirators



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

Example: Witness



- 1. **e** grants (*r* to **z**) to **d**
- 2. **c** takes (*r* to **z**) from **d**
- 3. **c** grants (*r* to **z**) to **b**
- 4. **b** grants (*r* to **z**) to **a**
- 5. **x** takes (*r* to **z**) from **a**

Quiz

In either 1 or 2 or both, can **y** steal α rights over **x**?

