ECS 235B Module 7
Take-Grant Model Rules

Take-Grant Protection Model

- A specific (not generic) system
  - Set of rules for state transitions
- Safety decidable, and in time linear with the size of the system
- Goal: find conditions under which rights can be transferred from one entity to another in the system

System

- ○ objects (files, …)
- ● subjects (users, processes, …)
- ⊗ don't care (either a subject or an object)

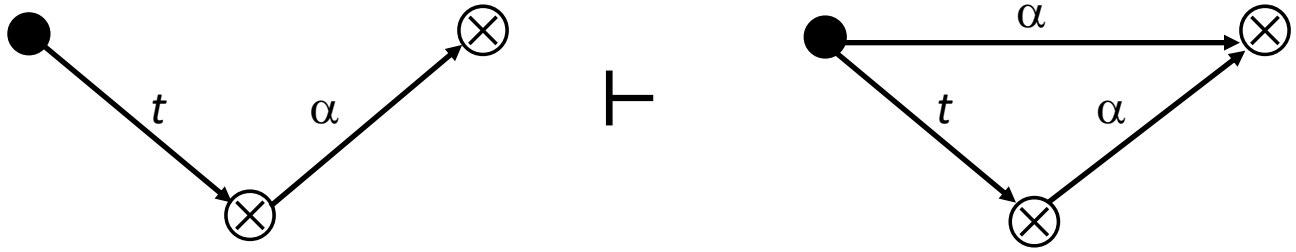
$G \vdash_x G'$ apply a rewriting rule x (witness) to G to get G'

$G \vdash^* G'$ apply a sequence of rewriting rules (witness) to G to get G'

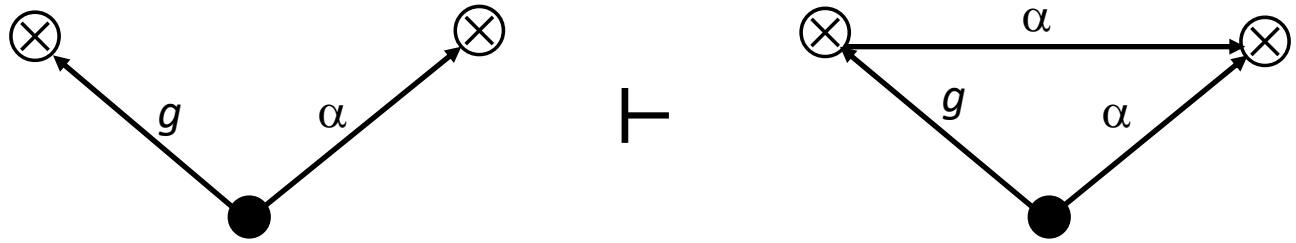
$R = \{ t, g, r, w, \ldots \}$ set of rights

Rules

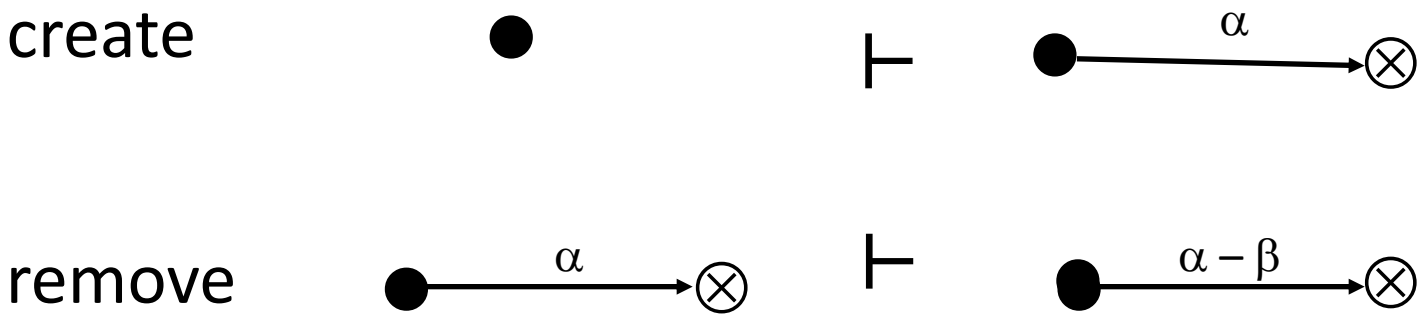
take



grant

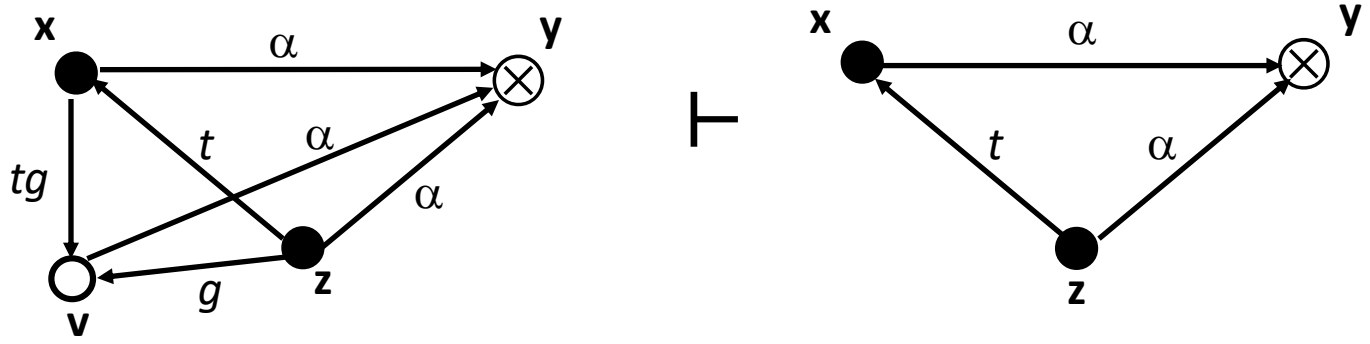


More Rules



These four rules are called the *de jure* rules

Symmetry



1. ***x*** creates (*tg* to new) ***v***
2. ***z*** takes (*g* to ***v***) from ***x***
3. ***z*** grants (α to ***y***) to ***v***
4. ***x*** takes (α to ***y***) from ***v***

Similar result for grant

Islands

- *tg*-path: path of distinct vertices connected by edges labeled *t* or *g*
  - Call them “tg-connected”
- island: maximal *tg*-connected subject-only subgraph
  - Any right one vertex has can be shared with any other vertex

Initial, Terminal Spans

- *initial span* from **x** to **y**
  - **x** subject
  - *tg*-path between **x**, **y** with word in $\{ \vec{t}^*\vec{g} \} \cup \{ \nu \}$
  - Means **x** can give rights it has to **y**
- *terminal span* from **x** to **y**
  - **x** subject
  - *tg*-path between **x**, **y** with word in $\{ \vec{t}^* \} \cup \{ \nu \}$
  - Means **x** can acquire any rights **y** has

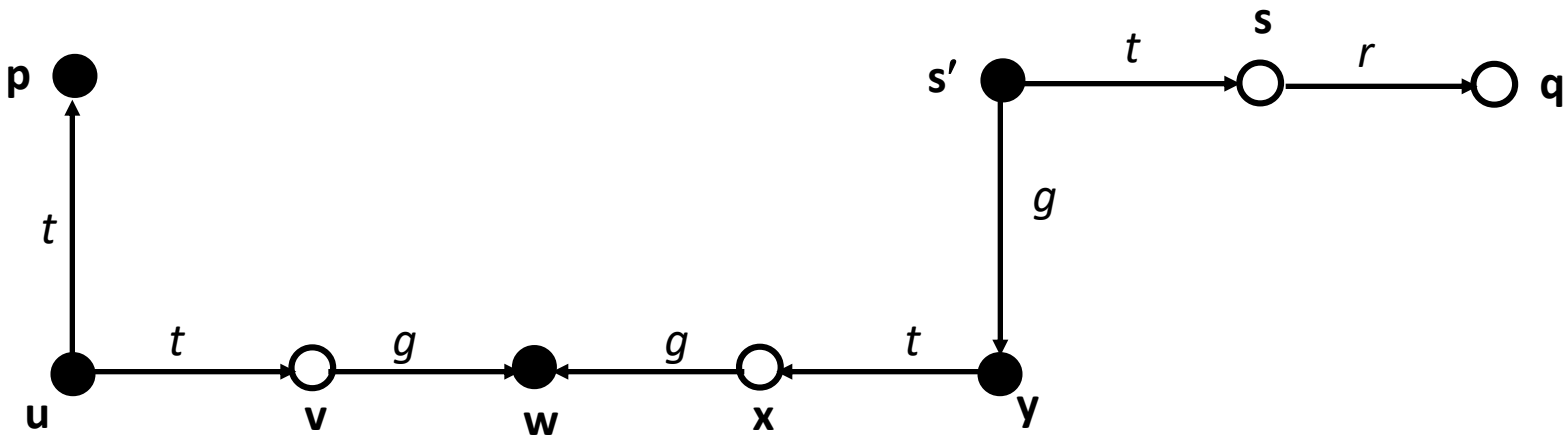
Bridges

- bridge: *tg*-path between subjects **x**, **y**, with associated word in

$$\{ \vec{t}^*, \vec{t}^*, \vec{t}^* \overleftarrow{g}\, \overleftarrow{t}^*, \vec{t}^* \vec{g}\, \overleftarrow{t}^* \}$$

  - Rights can be transferred between the two endpoints
  - It is *not* an island as intermediate vertices are objects

Example



- islands { **p**, **u** } { **w** } { **y**, **s′** }
- bridges **uvw**; wxy
- initial span **p** (associated word ν)
- terminal span **s′s** (associated word $\vec{t}$)