THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

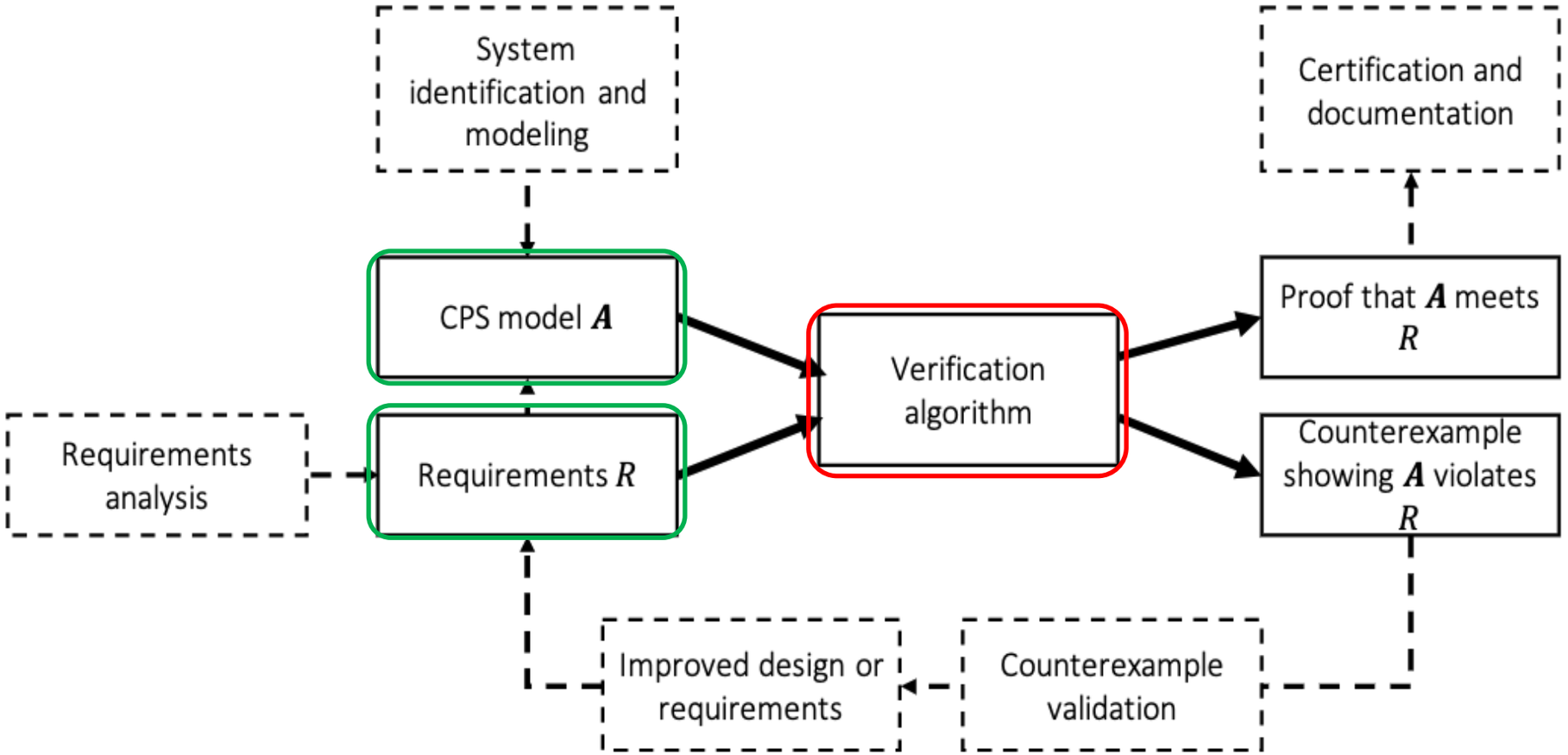
Verifying Cyber-Physical Systems

Chapter 9 – Reachability Analysis

Abenezer Taye

Feb 6, 2023

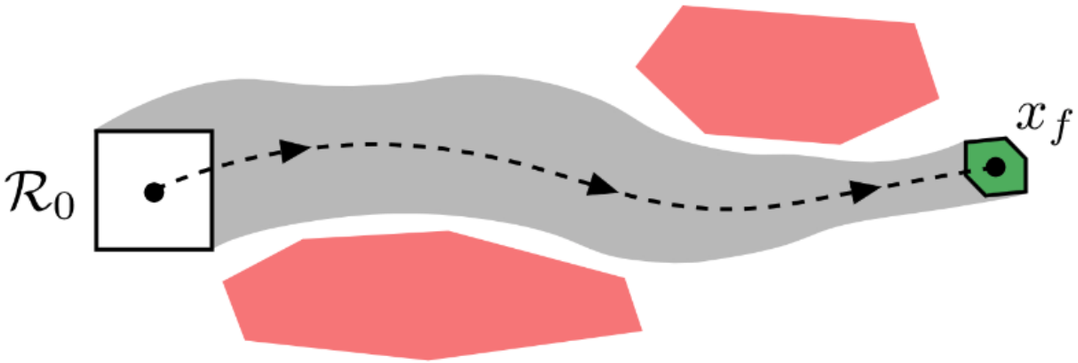
System Design Ecosystem



Introduction

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

- **Invariant verification problem / Safety verification problem:**
  - Deciding whether a given set of states x_f is reachable for system A
- Testing can partially answer such verification problem
  - Generate finite number of executions of A from R_0
  - Check whether these executions reach x_f



- If:
  - x_f represents an undesirable/bad behavior of the system → debug the system design.
  - Finite tests do not touch unsafe states ➔ can't say for sure the system is safe because A has infinite many executions.
- Alternative ➔ Reachability Analysis

Introduction

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

- Typical problem in reachability analysis → **State Space Explosion**
  - Dimension of the system
  - Time horizon
  - Degree of uncertainty in the model
- Focus on specific classes of Hybrid Automata for which safety properties (invariants) can be verified completely automatically
  - Timed Automata
  - Rational time automata
  - Multi-rate automata

- ➢ Rectangular Initialized HA
- ➢ Rectangular HA
- ➢ Linear HA
- ➢ Nonlinear HA

Integral Timed Automata

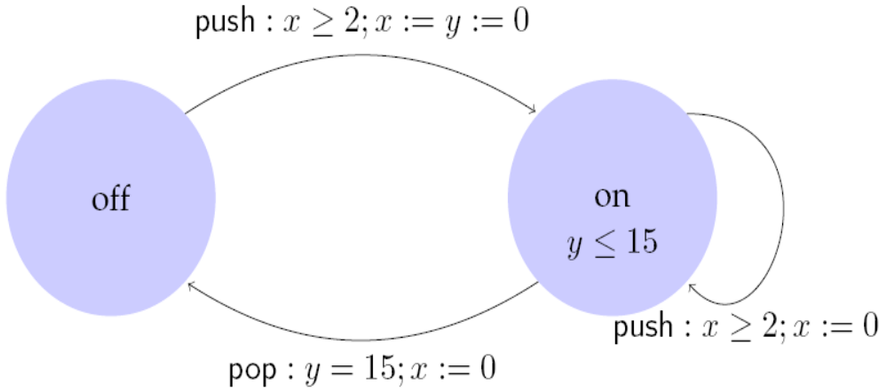
THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

- **Definition.** ***integral timed automaton*** is a HIOA $\mathcal{A} = \langle V, \Theta, A, \mathcal{D}, \mathcal{T} \rangle$ where
  - V = X ∪ $\{l\}$, where X is a set of n clocks and l is a discrete state variable of finite type L
  - A is a finite set
  - $\mathcal{D}$ is a set of transitions such that
    - The guards are described by clock constraings $\Phi(X)$
    - $\langle x, l \rangle - a \rightarrow \langle x', l' \rangle$ implies either $x' = x$ or $x = 0$
  - $\mathcal{T}$ set of clock trajectories for the clock variables in X

Example: Light Switch

Description

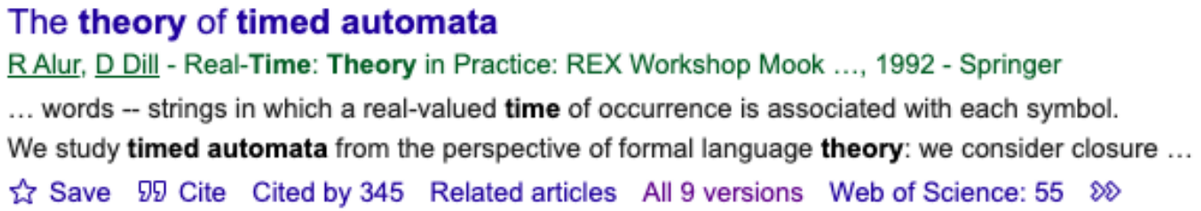
Switch can be turned on whenever at least 2 time units have elapsed since the last turn on. Switches off automatically 15 time units after the last on.



Control State Reachability Problem

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

- Given an ITA $\mathcal{A}$, check if a particular (discrete) control state is reachable from the initial states
- This problem is decidable [Alur Dill]



- Key idea:
  - Construct a finite automaton **B** that is a time-abstract bisimilar to the ITA **B**(behaves identically with respect to control state reachability)
  - That is, Finite Automaton **B** behaves identically to ITA **A** w.r.t. control state reachability, but does not preserve timing information.
  - Check reachability of FSM **B** using graph search techniques

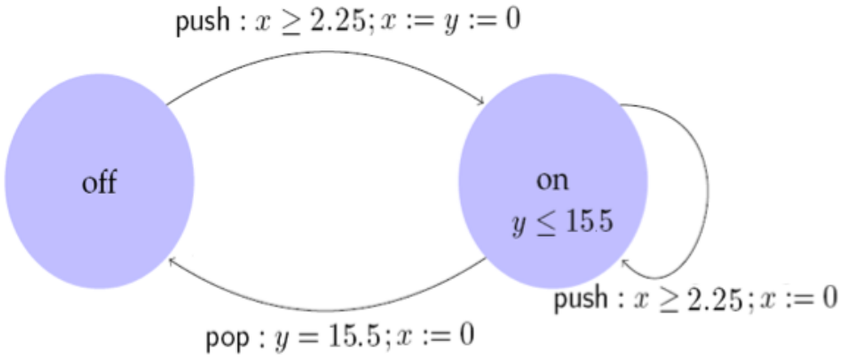
Rational Timed Automata

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

- **Definition.** A ***rational timed automaton*** is a HA $\mathcal{A} = \langle V, \Theta, A, \mathcal{D}, \mathcal{T} \rangle$ where
  - V = X ∪ $\{loc\}$, where X is a set of n clocks and l is a discrete state variable of finite type Ł
  - A is a finite set
  - $\mathcal{D}$ is a set of transitions such that
    - The guards are described by **rational** clock constraings $\Phi(X)$
    - $\langle x, l \rangle - a \rightarrow \langle x', l' \rangle$ implies either $x' = x$ or $x = 0$
  - $\mathcal{T}$ set of clock trajectories for the clock variables in X

Example: Light Switch

Description
Switch can be turned on whenever at least 2.25 time units have elapsed since the last turn off or on. Switches off automatically 15.5 time units after the last on.



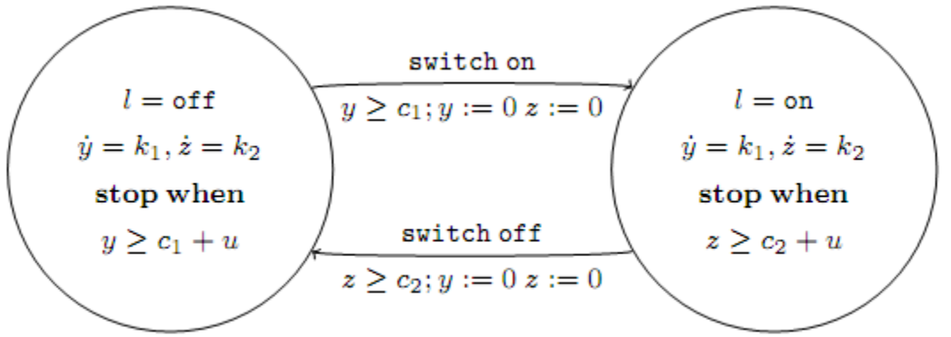
Multi-Rate Automaton

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

- **Definition.** A **multi-rate automaton** is $\mathcal{A} = \langle V, Q, \Theta, A, \mathcal{D}, \mathcal{T} \rangle$ where
  - V = X ∪ $\{loc\}$, where X is a set of n **continuous variables** and loc is a discrete state variable of finite type Ł
  - A is a finite set of actions
  - $\mathcal{D}$ is a set of transitions such that
    - The guards are described by **rational** clock constraings $\Phi(X)$
    - $\langle x, l \rangle - a \rightarrow \langle x', l' \rangle$ implies either $x' = c \; or \; x' = x$
  - $\mathcal{T}$ set of trajectories such that

    for each variable $x \in X \; \exists k \; such \; that \; \tau \in \mathcal{T}, t \in \tau.dom$

    $$\tau(t).x = \tau(0).x + k\,t$$



Rectangular HA

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Definition. An **rectangular hybrid automaton (RHA)** is a HA $\mathcal{A} = \langle V, A, \mathcal{T}, \mathcal{D} \rangle$ where

- V = X ∪ $\{loc\}$, where X is a set of n **continuous variables** and loc is a discrete state variable of finite type L
- A is a finite set
- $\mathcal{T} = \cup_\ell \mathcal{T}_\ell$ set of trajectories for X
  - For each $\tau \in \mathcal{T}_\ell, x \in X$ either (i) $d(x) = k_\ell$ or (ii) $d(x) \in [k_{\ell 1}, k_{\ell 2}]$
  - Equivalently, (i) $\tau(t)[x = \tau(0)[x + k_\ell t$
    (ii) $\tau(0)[x + k_{\ell 1} t \leq \tau(t)[x \leq \tau(0)[x + k_{\ell 2} t$
- $\mathcal{D}$ is a set of transitions such that
  - Guards are described by **rational** clock constraings
  - $\langle x, l \rangle \rightarrow_a \langle x', l' \rangle$ implies $x' = x \; or x' \in [c_1, c_2]$
- Given an RHA, check if a particular location is reachable from the initial states?
- Is this problem decidable? No
  - **[Henz95]** Thomas Henzinger, Peter Kopke, Anuj Puri, and Pravin Varaiya. What's Decidable About Hybrid Automata?. Journal of Computer and System Sciences, pages 373–382. ACM Press, 1995.

Generalizes multi-rate automata by allowing nondeterministic trajectories and resets.

Initialized Rectangular HA

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Definition. ***An initialized rectangular hybrid automaton*** **(IRHA)** is a RHA $\mathcal{A}$ where

- V = X ∪ $\{loc\}$, where X is a set of n continuous variables and $\{loc\}$ is a discrete state variable of finite type Ł
- A is a finite set
- $\mathcal{T} = \cup_\ell \mathcal{T}_\ell$ set of trajectories for X
  - For each $\tau \in \mathcal{T}_\ell, x \in X$ either (i) $d(x) = k_\ell$ or (ii) $d(x) \in [k_{\ell 1}, k_{\ell 2}]$
  - Equivalently, (i) $\tau(t)\lceil x = \tau(0)\lceil x + k_\ell t$

    (ii) $\tau(0)\lceil x + k_{\ell 1} t \leq \tau(t)\lceil x \leq \tau(0)\lceil x + k_{\ell 2} t$
- $\mathcal{D}$ is a set of transitions such that
  - Guards are described by **rational** clock constraings
  - $\langle x, l\rangle \rightarrow_a \langle x', l'\rangle$ implies if dynamics changes from ℓ to ℓ' then $x' \in [c_1, c_2]$, otherwise $x' = x$

The continuous variables are forced to be initialized every time their dynamics changes

- For initialized Rectangular HA, control state reachability is decidable
  - Can we drop the initialization restriction?
    - No, problem becomes undecidable

Data Structures for Reachability Analysis

Common Data Structures for RA

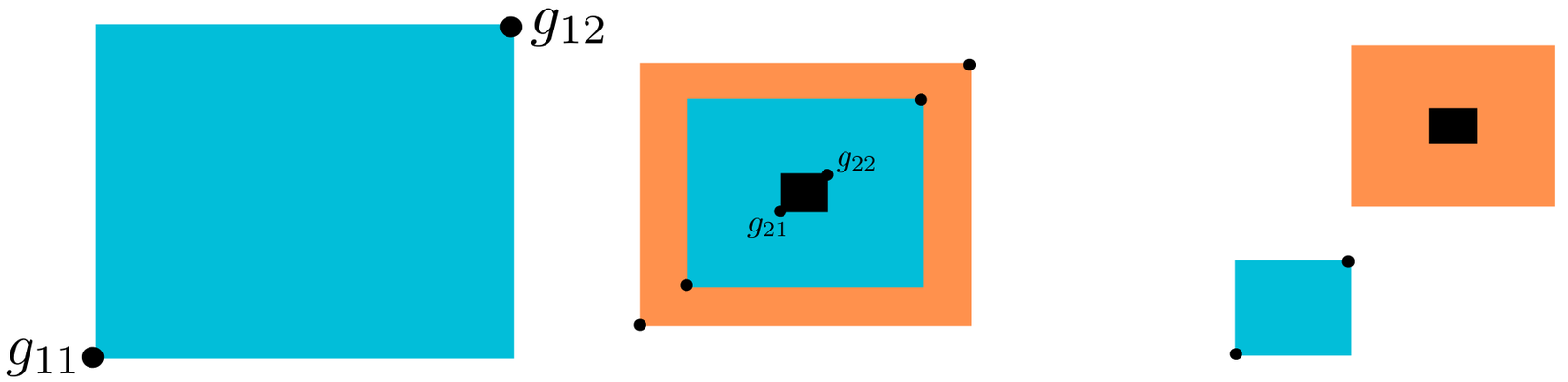
THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

- Hyperrectangles
- Polyhedra [Halbwachs et al. 1994]
- Zonotopes [Girard 2005]
- Ellipsoids [Kurzhanskiy 2001]
- Support functions [Guernic et al. 2009]
- Generalized star set [Duggirala and Viswanathan 2018]

Hyper-rectangles

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

- A hyperrectangle is the n-dimensional generalization of an interval [a,b].



$[[g_{11}, g_{12}]]$

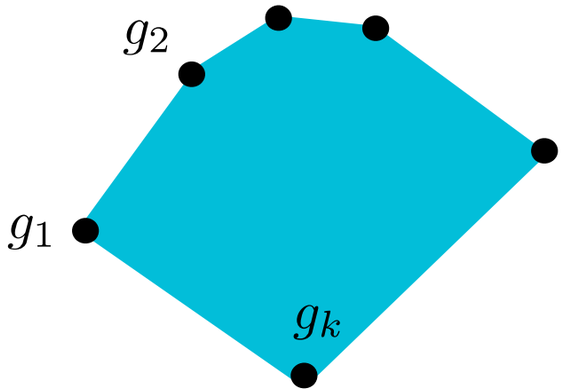
$[[g_{11}, g_{12}]] \oplus [[g_{21}, g_{22}]] = [[g_{11} + g_{12}, g_{21} + g_{22}]]$

$[[g_{11}, g_{12}]] \oplus [[t.g_1, t.g_2]]$

Polytopes

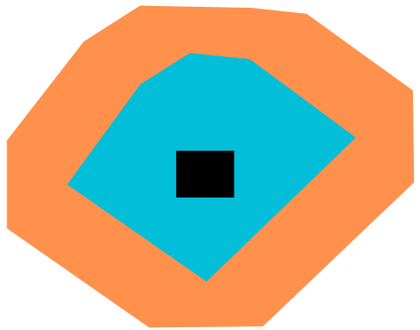
THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

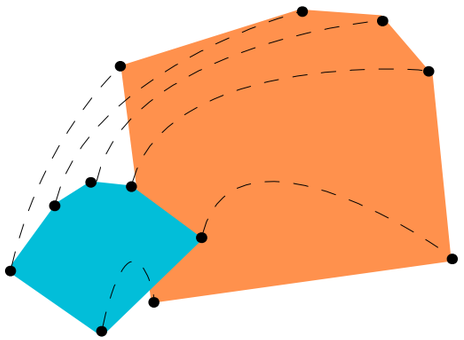
- Generalize hyperrectangles by representing sets as intersections of arbitrary – not necessarily orthogonal – half-spaces.



$[[A, b]]$

$[[g_1, \ldots, g_k]]$

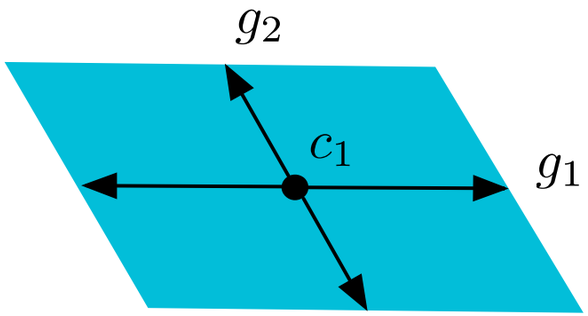




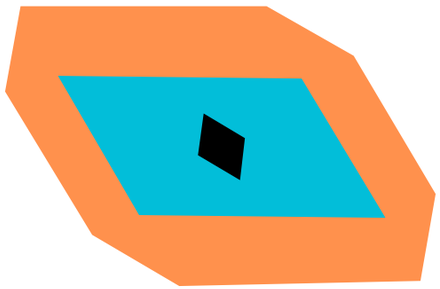
$[[\xi(g_1, t), \ldots, \xi(g_k, t)]]$

Zonotopes

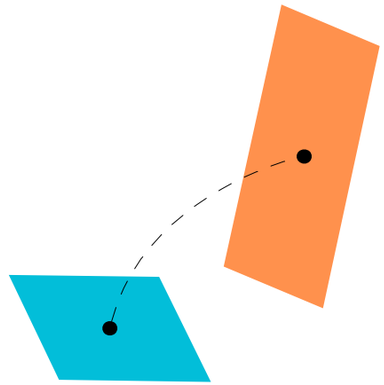
- A zonotope is specified by a center, and a collection of generator vectors.
- Each vector defines a line segment centered at the center.



$$[[c_1, \langle g_1, g_2 \rangle]]$$



$$[[c_1, \langle g_1, g_2 \rangle]] \oplus [[c_2, \langle g_1', g_2' \rangle]] = [[c_1 + c_2, \langle g_1, g_1', g_2, g_2' \rangle]]$$

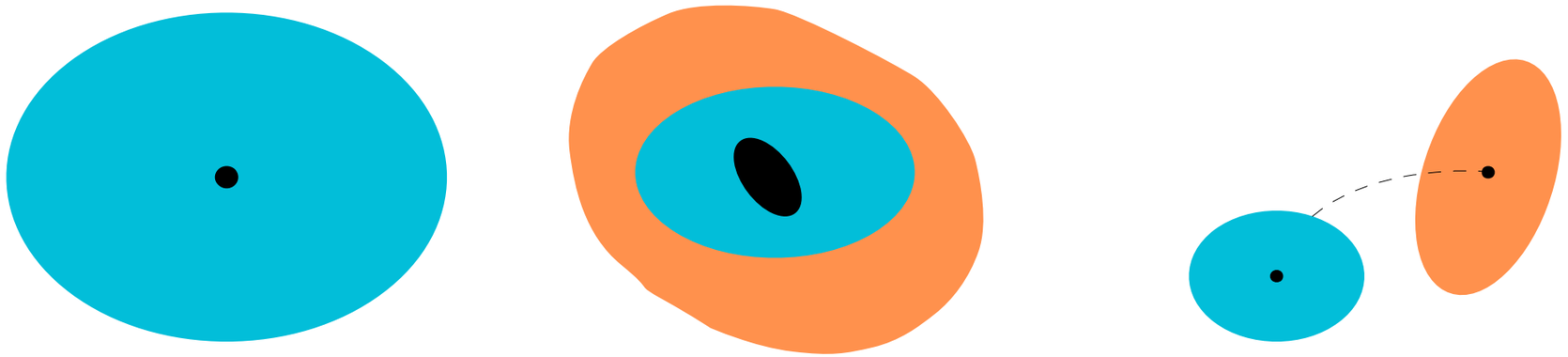


$$[[Ac_1, \langle Ag_1, Ag_2 \rangle]]$$

Ellipsoids

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

- Ellipsoids generalize spheres in R^n.
- It is defined by a center $c \in R^n$ and a shape matric $Q \in R^{nxn}$



$[[c_1, Q]]$ $[[c_1, Q_1]] \oplus [[c_2, Q_2]] \neq [[c_3, Q_3]]$ $[[Ac_1, AQA^T]]$

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Thank You!!!

Q&A