Tutorial

Practical Theory or Theoretical Practice?

A Discussion on Models of Synchrony, Faults, and Sensors...

Xavier DÉFAGO

School of Information Science
Japan Advanced Institute of Science and Technology

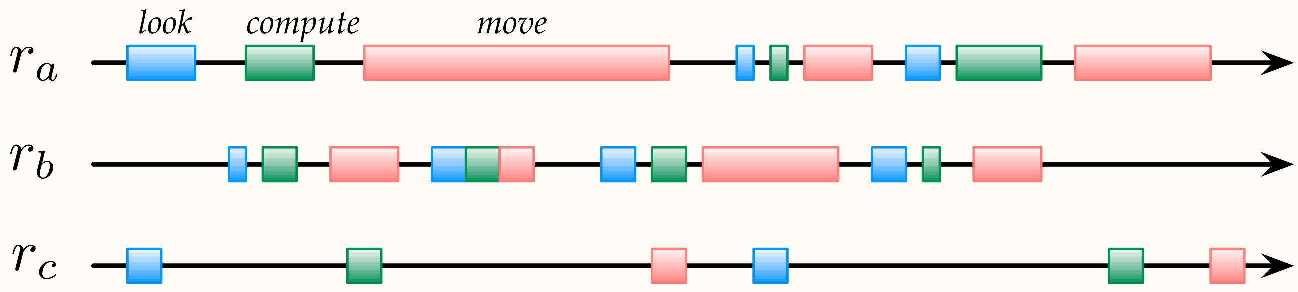
Structure / Outline

- **Tutorial part**
  - Models of Synchrony
  - Fault Models
  - Sensors / Agreement
- **Discussion part**
  - Theme: Theory vs. practice

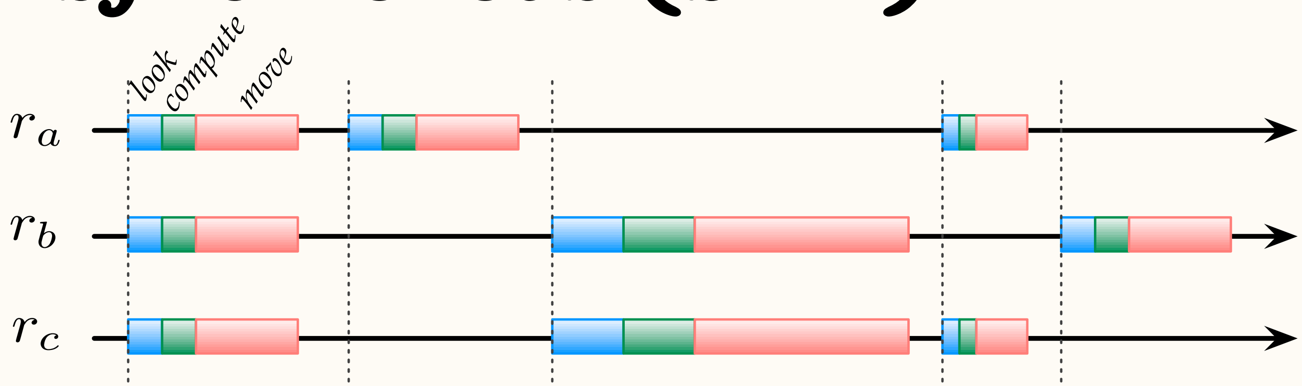
Models of Synchrony

Models of Synchrony

- Asynchronous (CORDA)



- Semi-synchronous (SYm)



- Fully Synchronous

Schedulers

- **Fair vs. Unfair**
  - **Fair**: Every robot active ∞-often.
  - **Unfair**: Some robot active ∞-often.
- **Centralized vs. Distributed**
  - **Centralized**: At most one robot activated
  - **Distributed**: Any subset of robots activated

[Défago, Gradinariu, Messika, Raipin-P. 2006] + exten.

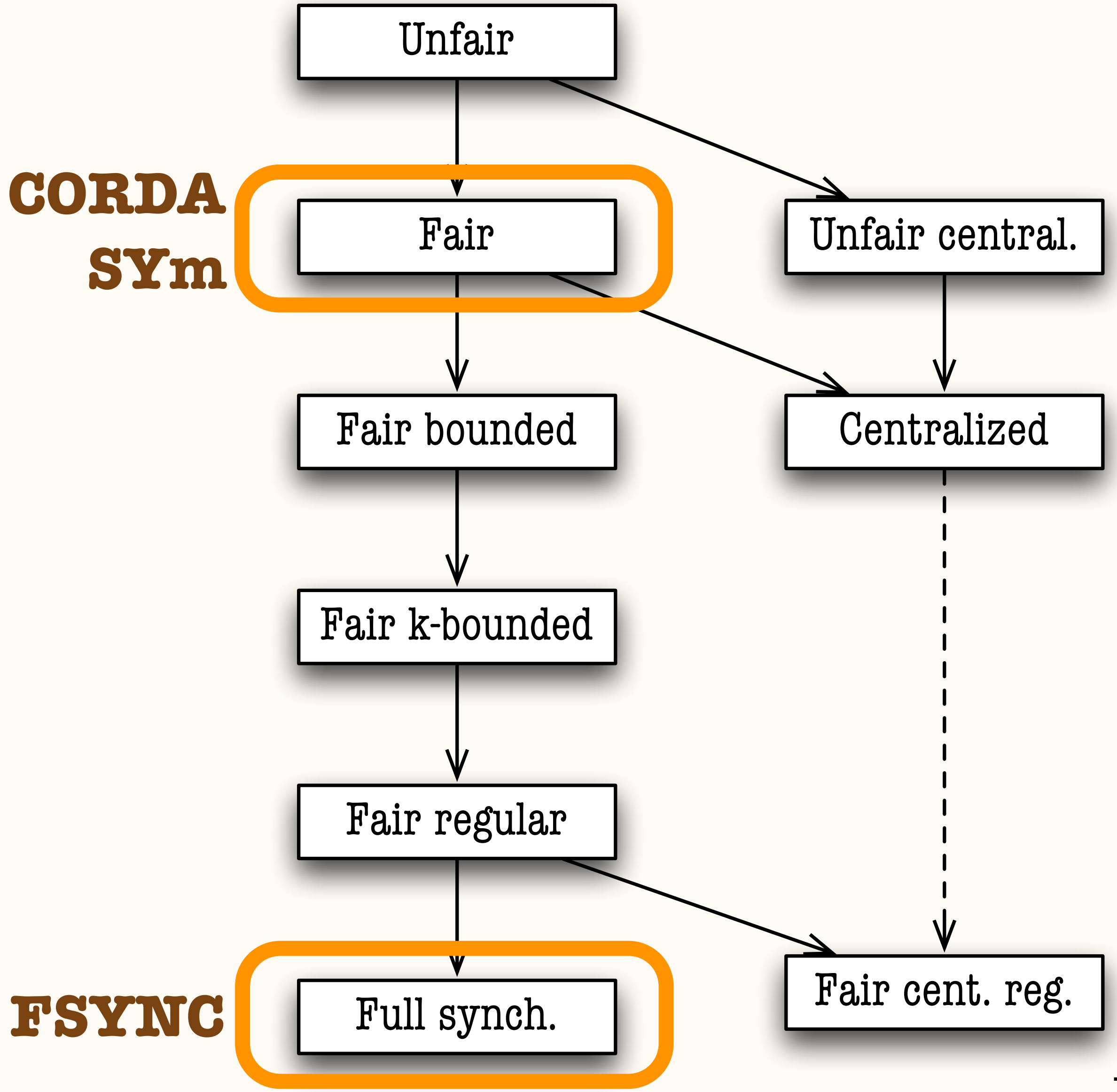
...

Schedulers

- **Bounded vs. Unbounded**
  - **k-Bounded**: $\forall r_a \forall r_b$ r_a active at most k times between any two consecutive activations of r_b
  - **Bounded**: $\exists$k s.t., system is k-bounded (k is unknown)
  - **Unbounded**: No bounds
  - **Bounded Regular**: Special case; means 1-Bounded.

Scheduler

- **Classes**
  - Unfair
  - Unfair centralized
  - Fair
  - Fair centralized
  - Bounded
  - k-bounded
  - Regular
  - Centralized regular
  - Fully synchronized



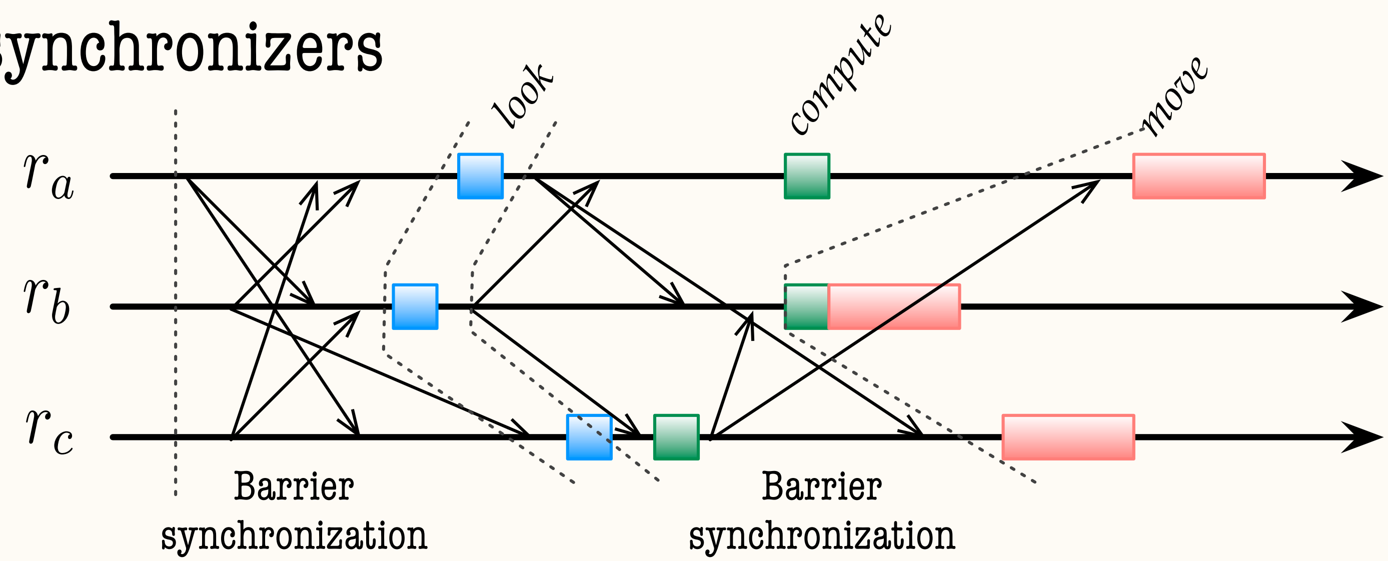
Viewpoint: Implicit Comm.

❑ Context

- Synchronization by communication
- No faults, reliable communication

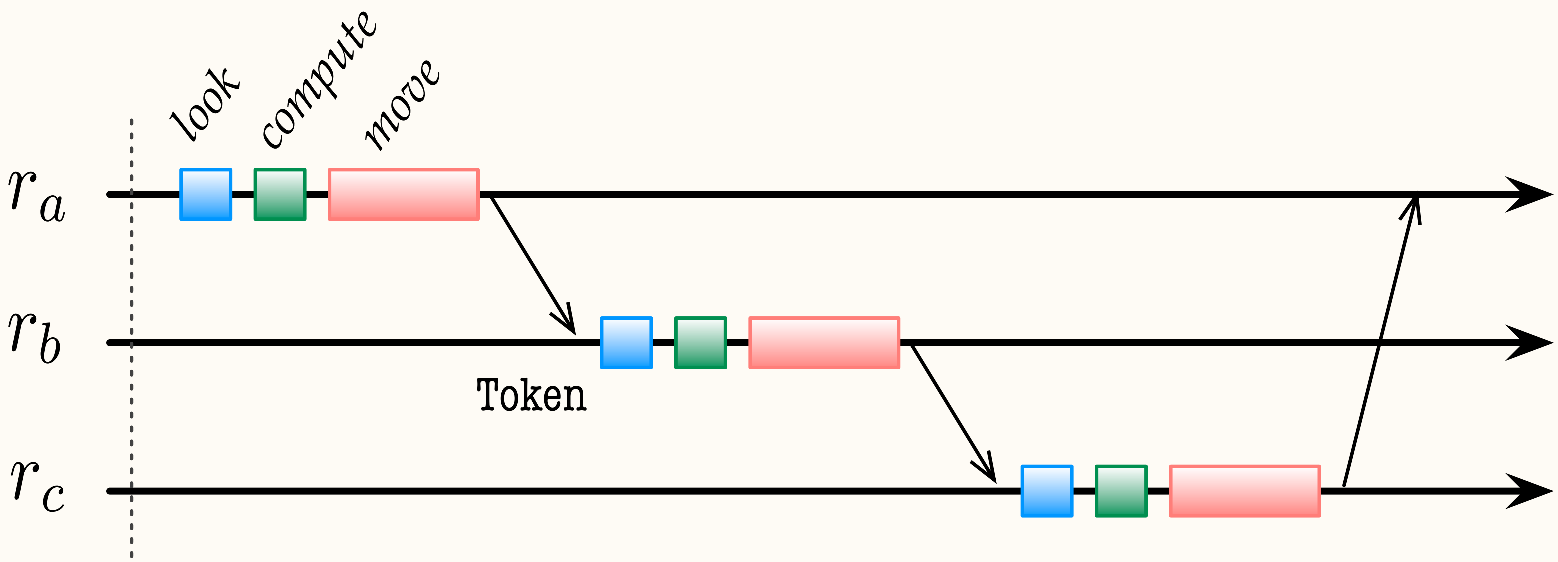
❑ Idea

- Analogy to "round synchronous model"
- Relate to synchronizers



Viewpoint: Implicit Comm.

- ❑ **Centralized regular scheduler**



Fault Models

Fault Models

- **Crash Faults**
  - A faulty robot stops executing any action.
- **Omission Faults**
  - A faulty robot "omits" executing some actions
- **Byzantine Faults**
  - A faulty robot behaves arbitrarily (potentially maliciously).

Crash Faults

- **"Is a crashed robot recognized as a robot?"**
- **Case 1: No**
  - Illustrations:
    - crashed robot blown into pieces!
    - crashed robot stops sending positioning beacons
  - Countermeasure:
    - oblivious algorithms (trivial)

JAIST
JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY 1990

Crash Faults

- **"Is a crashed robot recognized as a robot?"**
- **Case 2: Yes**
  - Illustrations:
    - out-of-battery
  - Countermeasure:
    - failure detection
    - randomization
    - ...

Byzantine Faults

- **“Adversary stronger than model?”**
- **Case 1: No**
  - Byzantine robot must abide by scheduler rules
  - Adversary can chose schedule
- **Case 2: Yes**
  - Byzantine robot can override schedule limits
  - Scheduler rules must apply to correct robots

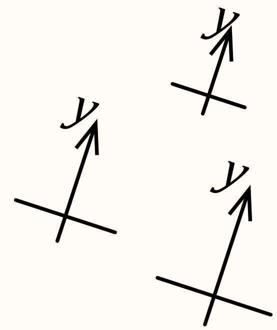
NB: Also raised by Andrzej Pelc yesterday

Sensors

Compasses

❑ Compass

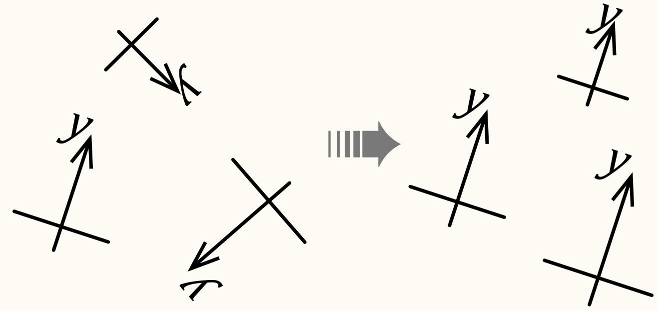
- ❍ Agreement on one common direction (North)



❑ Unreliable compasses

- ❍ Many classes

❑ Eventual compasses



- ❍ Vary in time (fluctuate)
- ❍ **Eventually**: all compasses agree permanently

  [Souissi, Défago, Yamashita 2006/2009]

JAIST
JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY 1990

Compasses

- **Bounded errors**
  - Fixed direction / fluctuate
  - Bounded errors

    [Katayama, Inuzuka, Wada 2006]

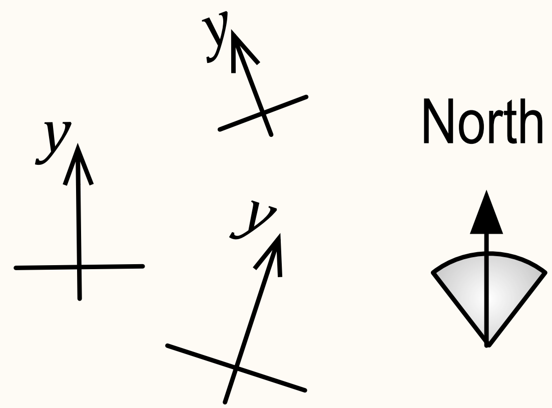
    [Souissi, Défago, Yamashita 2006]

    [Katayama, Tomida, Imazu, Inuzuka, Wada 2007]

    [Yamashita, Souissi, Défago 2007]

    [Izumi, Katayama, Inuzuka, Wada 2007]

    [Inuzuka, Tomida, Izumi, Katayama, Wada 2008



Discussion

JAIST
JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY 1990

Formation vs. Convergence

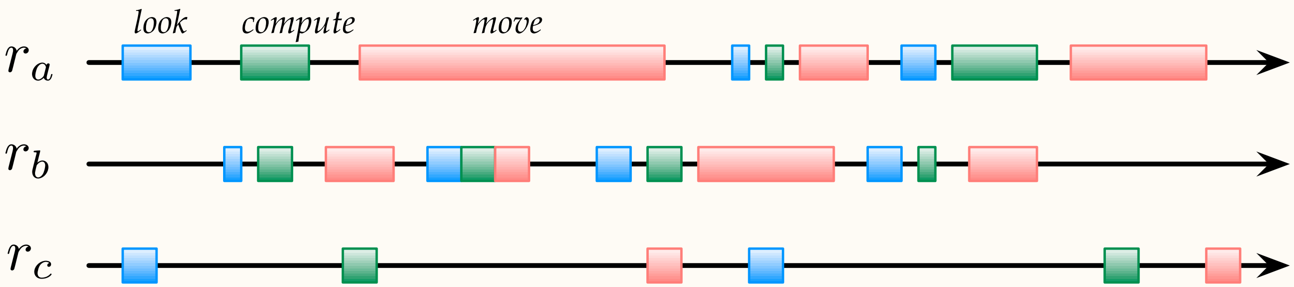
- **Formation**
  - Pattern obtained after finite number of steps by a deterministic algorithm.
- **Convergence**
  - Monotonic progress toward pattern
  - Pattern obtained asymptotically

Sensing & Actuation

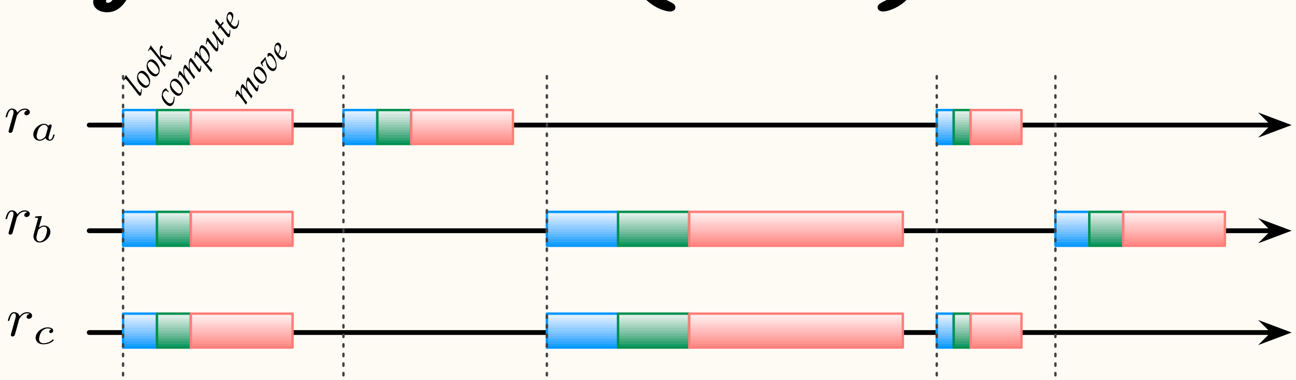
- **Proximity sensors**
  - Finite precision; Limited accuracy
  - Types: IR, sonar, visual, laser
- **Motors**
  - Finite precision; Limited accuracy
  - Types (e.g, wheeled): DC motor, stepper motor
- **Outcome**
  - Movement nearly discrete
  - Convergence **implies** formation

Models of Synchrony

- Asynchronous (CORDA)



- Semi-synchronous (SYm)



- Fully Synchronous

JAIST JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY 1990

Question?

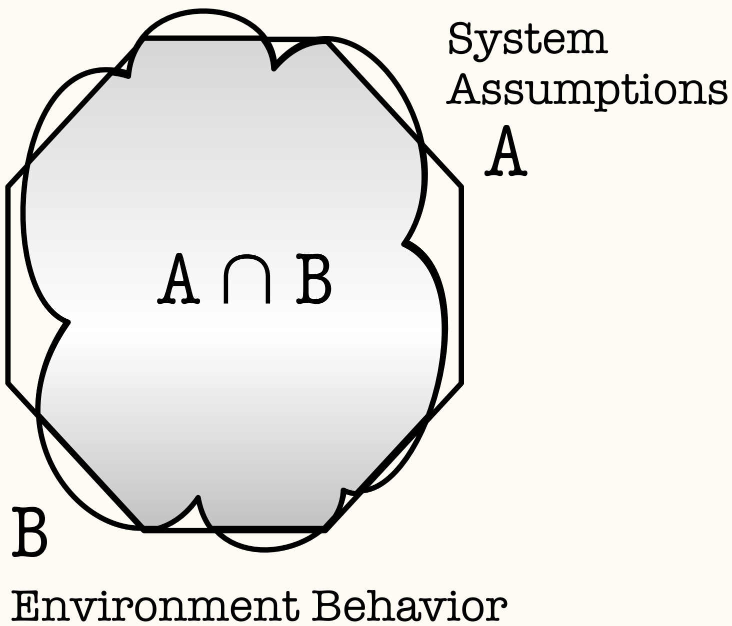
- **Practically speaking:**

  "Which model is most <u>relevant</u>?"

- **Answer: "It depends!"**

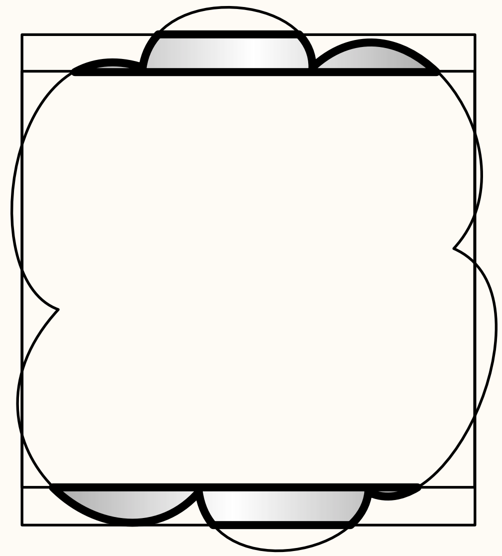
Assumption Coverage

- **System Assumptions (A)**
  - Algorithm proved correct
- **Environment Behavior (B)**
  - Actual behavior of the system
- **Coverage**
  - (A ∩ B) / B
- **Comment**
  - Choice of system model is essential



CORDA vs. SYm

- **Fundamentally**
  - SYm ⊂ CORDA ([Pre05] "The effect of synchronicity..." TCS)
- **So**
  - coverage(SYm) ≤ coverage(CORDA)
- **Why not strict inequality?**



Determ. vs. Probabilistic

- **Case 1**
  - deterministic algorithm
  - assumption coverage = 90%
- **Case 2**
  - probabilistic algorithm: P[correct ^ terminate] = 95%
  - assumption coverage = 95%
- **Which one is most dependable?**
  - Case 1 -> 10% undefined behavior
  - Case 2 -> 9.75% undefined behavior

Dumb, cheap robots...

- **Assumptions**
  - measure other robots positions with **infinite accuracy**?
- **Actual proximity sensors**
  - IR proximity sensors / sonar
  - Signal strength (RFID, WiFi)
  - Machine vision
  - Laser
- **Reality**
  - GPS / landmarks + communication is way cheaper!

JAIST
JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY
1990

Concluding Comments

- **Axiomatic approach**
  - Separates applicability from correctness issues
  - Models important to focus on fundamental problems / limits
  - Relation between problems
- **Dangers**
  - Ignoring practical considerations in model choices
  - Proving impossibility in weak models
  - Failing to quantify results [Paola's remark]
  - Considering problems only in isolation