SENSOR SELECTION FOR FINE-GRAINED BEHAVIOR VERIFICATION THAT RESPECTS PRIVACY

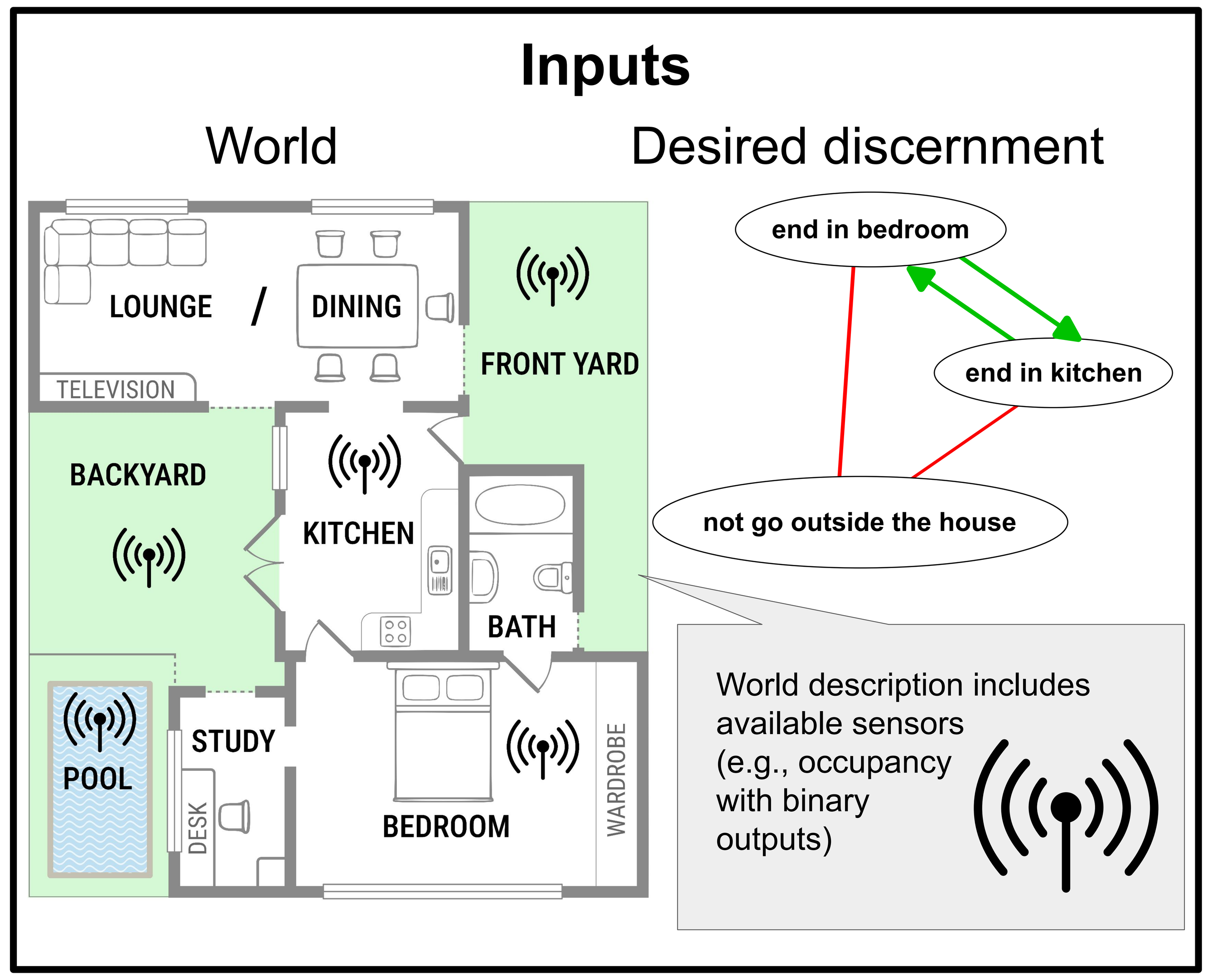
Rishi Phatak and Dylan A. Shell

Texas A&M University

COMPUTER SCIENCE & ENGINEERING
TEXAS A&M UNIVERSITY

What is a sensor selection?

- Given a claim made by an agent in an environment, how do we verify it?
- Place sensors throughout the environment
- Which sensors do we select ⇒ the sensor selection problem
- Rahmani et al.[1] showed that minimum sensor selection is **NP-Hard**



Modeling the problem

- A world graph is an edge-labelled, directed multigraph
- Each edge on the world graph has a label associated with it
- Any walk taken on the world graph leads to a so-called "signature" with the caveat that edges with empty labels don't produce a symbol
- Itinerary: A set of walks described by a DFA or regular expression

What about privacy?

- Information collected could be considered private, or sensitive
- Specify many itineraries with 2 types of constraints:
  - Positive: 2 itineraries, each of which must not be confused with the other
  - Negative: 2 itineraries, one of which must appear identical to the other
- Constraints taken together form the desired discernment (DD) graph
  - Positive constraints – **undirected** edges
  - Negative constraints – **directed** edges

Decision Problem: Minimal sensor selection to accommodate a discernment designation in itineraries (MSSADDI)

Input: A world graph G, a discernment designation D, and a natural number k ∈ N.
Output: A satisfying sensor selection M ⊆ S for D on G with |M| ≤ k, or 'INFEASIBLE' if none exist.

Satisfying Sensor Selections

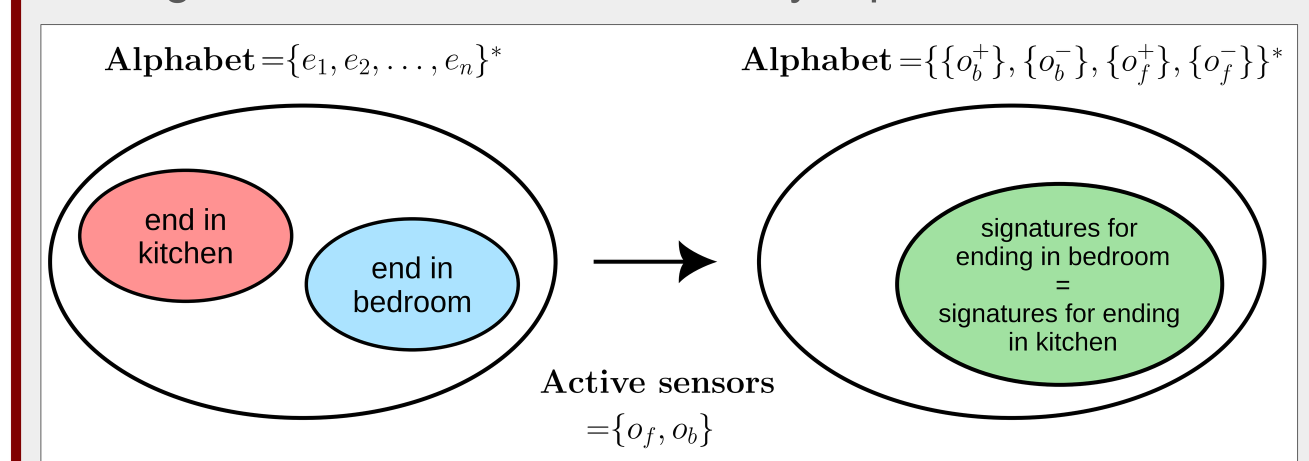
- For each (undirected) pair of itineraries in discrimination ⇒ no walks should have the same signature
- For each (directed) pair of itineraries in conflation ⇒ for each walk from the first itinerary there must be a walk in the second itinerary having the same signature

Observations

- Adding privacy may increase the number of sensors required to satisfy all constraints
- Merely minimizing selected sensor on discrimination requirements does not guarantee specific privacy

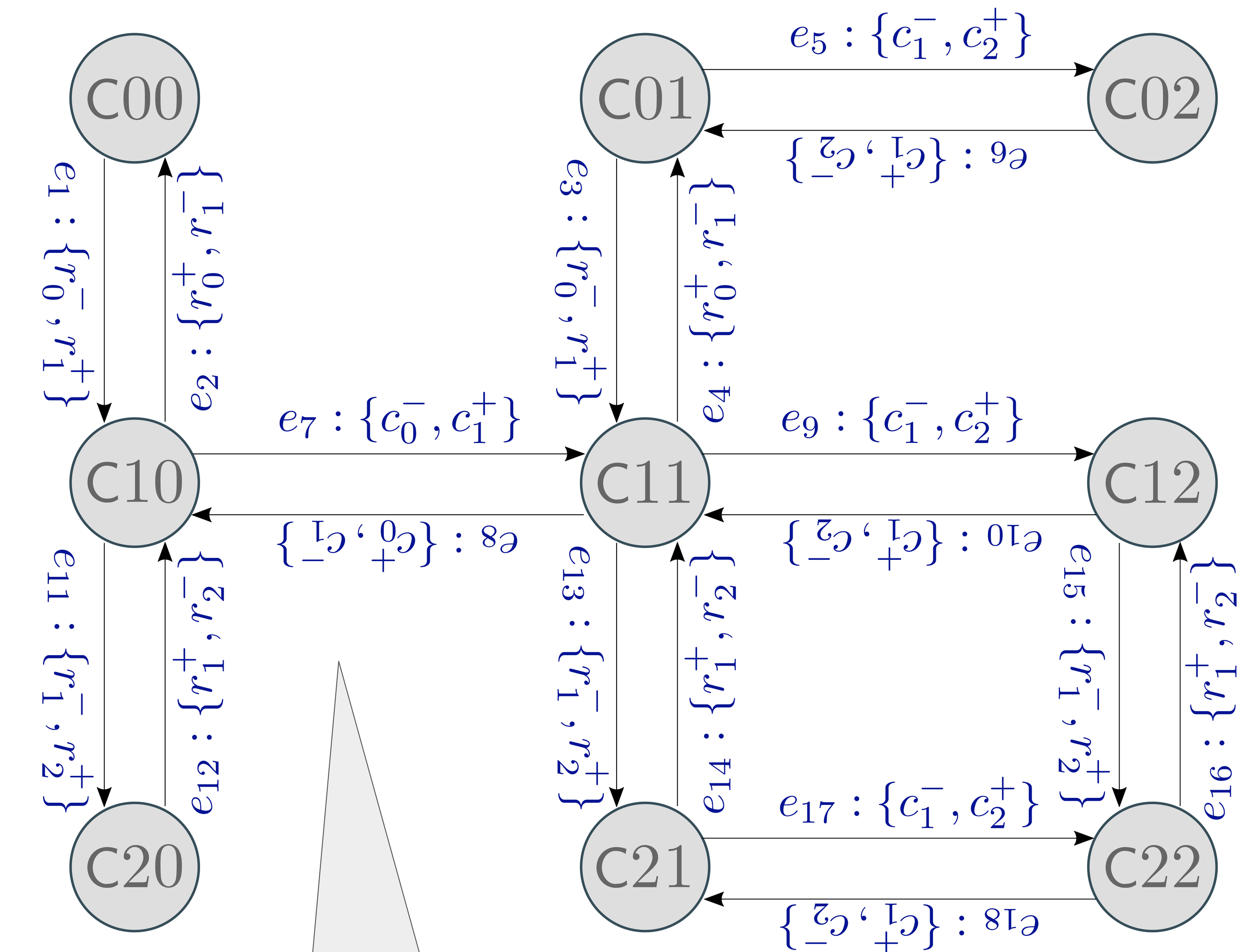
Hardness results

- With privacy (negative) constraints added, it is **PSPACE-Hard** to solve for the minimum sensor selection.
- Why? The following provides some intuition:
  - Signature automata replace the alphabet in the itinerary DFA's (i.e. the edges) with their respective labels which turns them into NFA's! Why?
    - 2 edges from the same node may have the same label
    - Some edges may have the empty symbol (no sensors)
  - Conflation constraints involve language inclusion checks on these signature automate ⇒ known to be **PSPACE-Complete**
- The example shows how conflation constraints map:
  - Each Venn diagram shows regular languages over the specified alphabets
  - Note that there are no common strings (walks) for itineraries ending in the kitchen and bedroom
  - Mapped over the active sensors, the set of their signatures turn out to be exactly equal

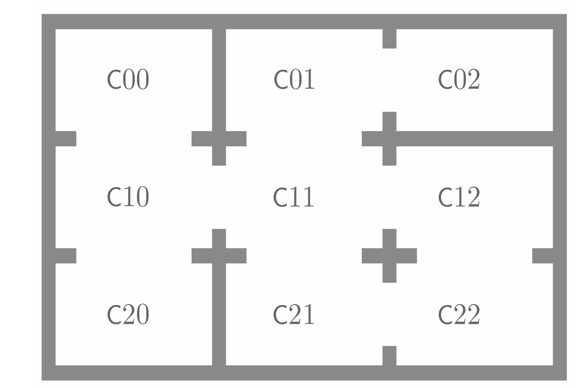


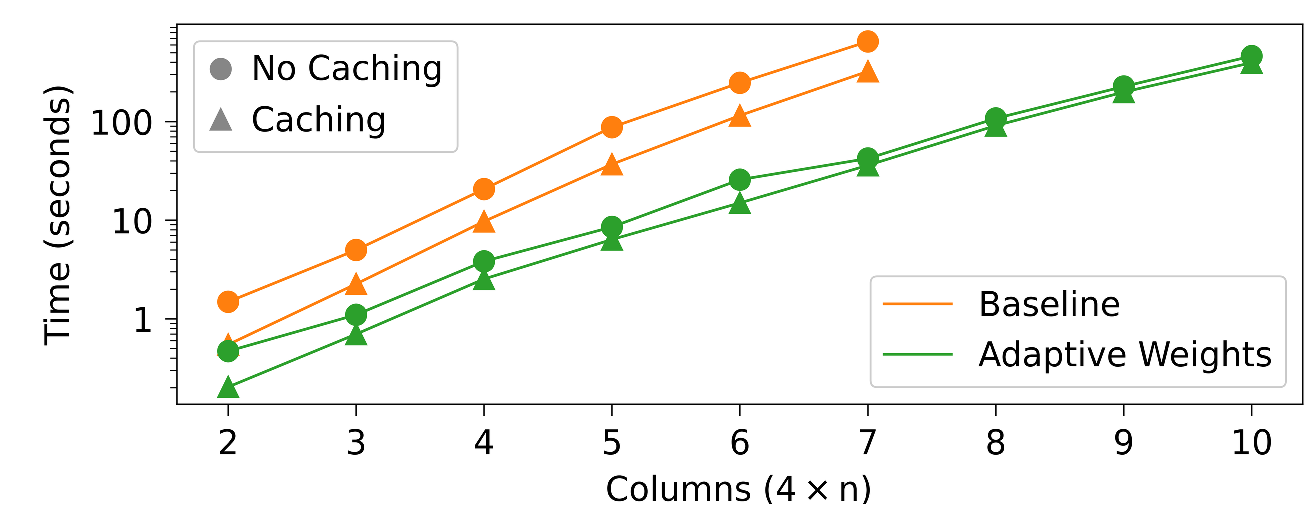
Implications for finding solutions

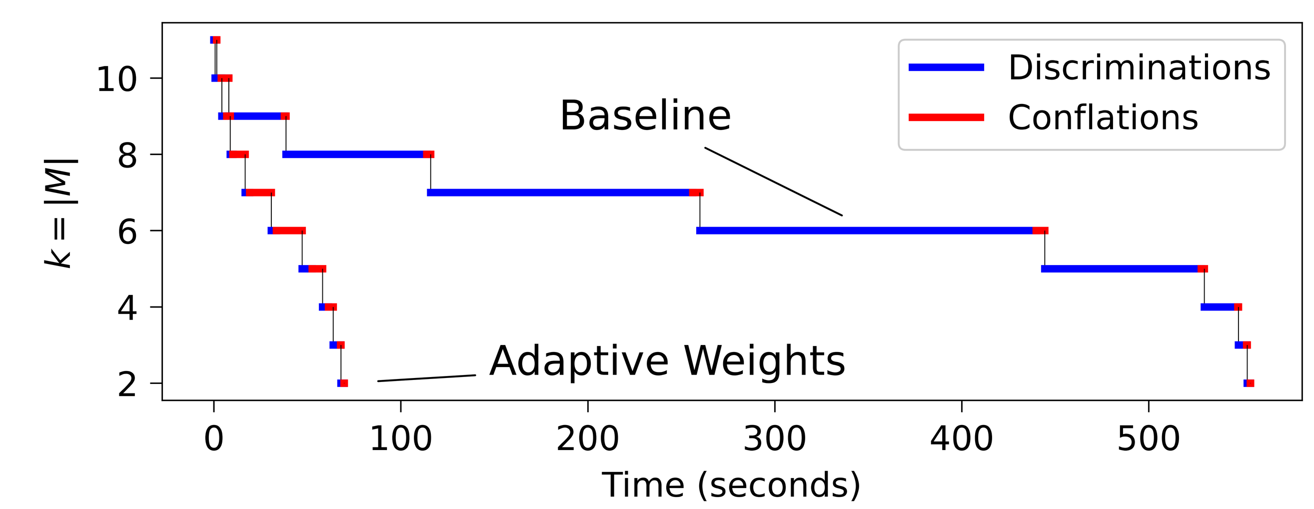
- Adding privacy constraints makes the sensor selection problem **significantly harder**!
- Thus, we understand that
  - Adding more discrimination requirements between itineraries is still NP-Hard
  - However, even one conflation requirement raises the complexity to PSPACE-Hard
- If P ≠ PSPACE, then our ability to solve large instances of this problem is impaired.



Notice how, starting from C00 and if only the row sensors are active, we cannot tell in which column an agent ends in







Optimizations

- On the complete enumeration of sensor sets, we can cache signature automata or apply adaptive weights on constraints
- Adaptive weights led to a 87% improvement in time.

[1] Hazhar Rahmani, Dylan A. Shell, and Jason M. O'Kane. Sensor selection for detecting deviations from a planned itinerary. In IEEE/RSJ International Conference on Intelligent Robots and Systems, pp. 6511–6518, Online, 2021.