Spatio-temporal Model-checking for Collective Adaptive Systems in QUANTICOL

Quanticol project (2013-2017): work in progress

A Quantitative Approach to Management and Design of Collective and Adaptive Behaviours

Vincenzo Ciancia, Diego Latella, Michele Loreti, *Mieke Massink*
CNR-ISTI, Pisa, University of Florence/IMT Lucca

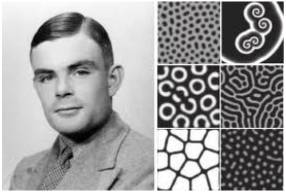
Thanks also to: Gina Belmonte, Rytis Paškauskas and Andrea Vandin

DeCPS, 17-06-2016, Pisa

Collective Adaptive Systems

www.quanticol.eu

Examples of decentralised collective adaptive behaviour in nature:



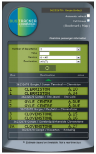
Characteristics of CAS

quanticol
www.quanticol.eu

- Coordination based on (local) decentralised interaction
- Large scale, heterogeneous agents, competing goals, open
- Capacity to smoothly adapt to changing circumstances
- Spatially inhomogeneous distribution influences global patterns
- Multiple scales in time and space, systems of systems
- Decentralised and centralised control

Designing CAS for a smart society

The development of our methodology will focus on the provisioning challenges of smart urban transport and smart grid.



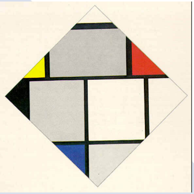
The objective is to develop an innovative formal design framework that is scalable and addresses spatial aspects

Spatial Modelling and Reasoning

Physical Sciences

Ordinary/ Partial Differential Equations

Pure Mathematics

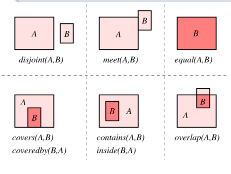


Topology
Modal Logics

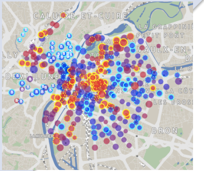
Decidability
Satisfiability

SPACE

Region Connection Calculus

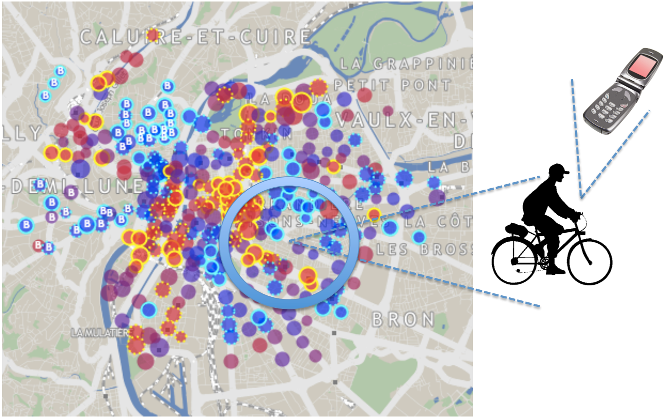


Artificial Intelligence



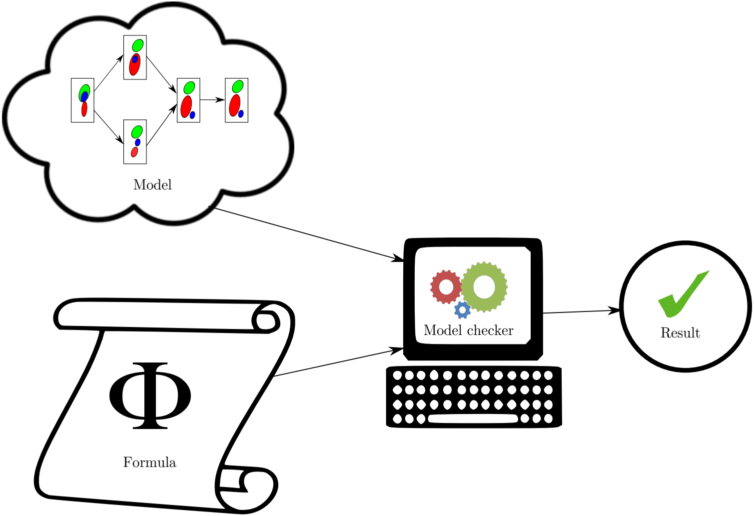
Model checking

Collective Adaptive Systems



Continuous space, discrete regular grid, graph of stations, street map

Spatio-temporal model checking



Modal Logic of Space

[Tarski, 1938, Tarski&McKinsey, 1944]

$$\Phi ::= p \mid \top \mid \bot \mid \neg\Phi \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \Box\Phi \mid \Diamond\Phi$$

A topological space (X, O)

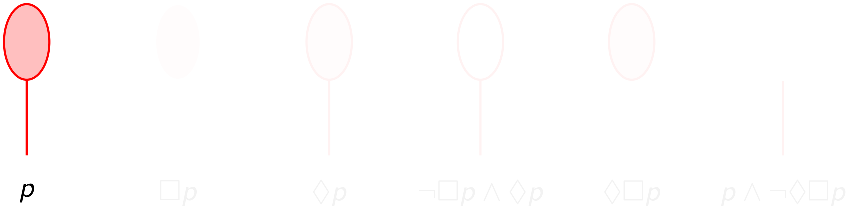
- X a set of points
- O the set of open sets of X

A *model* $\mathcal{M} = ((X, O), \mathcal{V})$

- (X, O) a topological space
- $\mathcal{V} : P \to \mathcal{P}(X)$ a valuation function

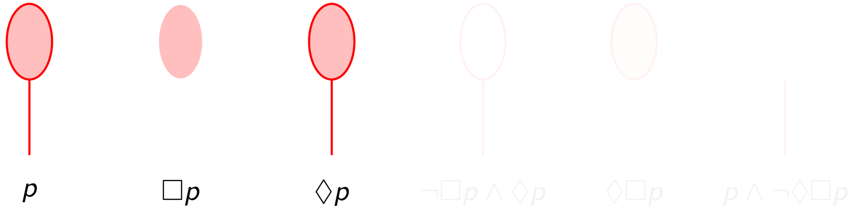
$\mathcal{V}$ assigns to each atomic proposition the set of points that satisfy it.

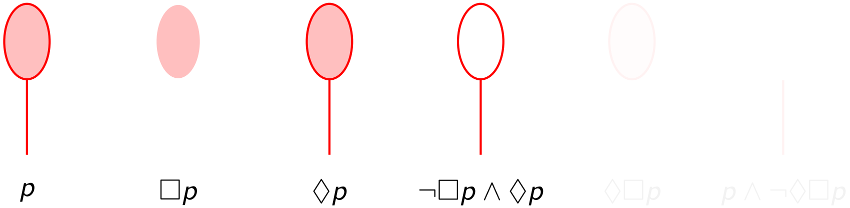
$$\begin{array}{lcl}
\mathcal{M}, x \models \top & \iff & \mathit{true} \\
\mathcal{M}, x \models p & \iff & x \in \mathcal{V}(p) \\
\mathcal{M}, x \models \neg\phi & \iff & \texttt{not}\ \mathcal{M}, x \models \phi \\
\mathcal{M}, x \models \phi \wedge \psi & \iff & \mathcal{M}, x \models \phi\ \texttt{and}\ \mathcal{M}, x \models \psi \\
\mathcal{M}, x \models \Box\phi & \iff & \exists o \in O.(x \in o\ \texttt{and}\ \forall y \in o.\mathcal{M}, y \models \phi) \\
\mathcal{M}, x \models \Diamond\phi & \iff & \forall o \in O.(x \in o\ \texttt{implies}\ \exists y \in o.\mathcal{M}, y \models \phi)
\end{array}$$



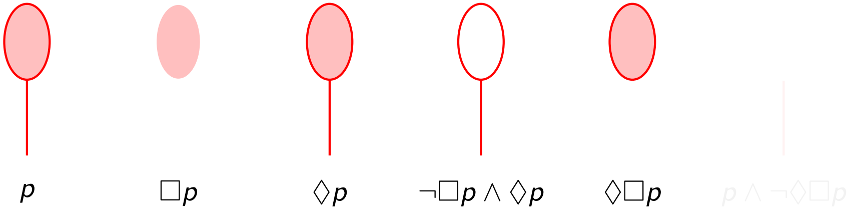
p
$\Box p$
$\Diamond p$
$\neg\Box p \wedge \Diamond p$
$\Diamond\Box p$
$p \wedge \neg\Diamond\Box p$

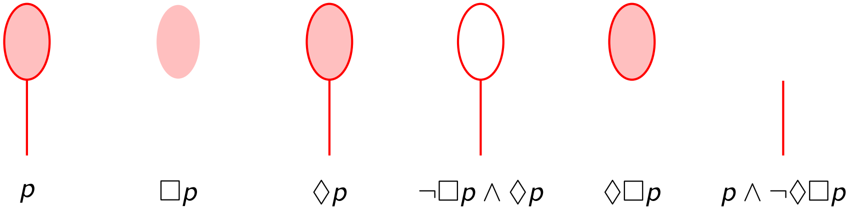
p $\Box p$ $\Diamond p$ $\neg\Box p \wedge \Diamond p$ $\Diamond\Box p$ $p \wedge \neg\Diamond\Box p$


p
□p
◊p
¬□p ∧ ◊p
◊□p
p ∧ ¬◊□p



p
□p
◊p
¬□p ∧ ◊p
◊□p
p ∧ ¬◊□p


p
□p
◊p
¬□p ∧ ◊p
◊□p
p ∧ ¬◊□p


p
$\Box p$
$\Diamond p$
$\neg\Box p \wedge \Diamond p$
$\Diamond\Box p$
$p \wedge \neg\Diamond\Box p$

Čech Spaces or Closure Spaces

A *closure space* is a pair $(X, \mathcal{C})$ with $\mathcal{C} : 2^X \to 2^X$ such that

for each $A, B \subseteq X$:

- $\mathcal{C}(\emptyset) = \emptyset$
- $\mathcal{C}(A \cup B) = \mathcal{C}(A) \cup \mathcal{C}(B)$
- $A \subseteq \mathcal{C}(A)$
- ~~$\mathcal{C}(\mathcal{C}(A)) = \mathcal{C}(A)$~~

Define:

- $\mathcal{I}(A) = \overline{\mathcal{C}(\overline{A})}$
- A is *open* iff $A = \mathcal{I}(A)$
- A is *closed* iff $A = \mathcal{C}(A)$
- A is a *neighbourhood* of $x \in X$ iff $x \in \mathcal{I}(A)$

Interior and closure are duals:

- $\mathcal{C}(A) = \overline{\mathcal{I}(\overline{A})}$

Theorem

$(X, \mathcal{C})$ is quasi-discrete iff there is $R \subseteq X \times X$ such that $\mathcal{C} = \mathcal{C}_R$

Čech Spaces or Closure Spaces

A *closure space* is a pair $(X, \mathcal{C})$ with $\mathcal{C} : 2^X \to 2^X$ such that

for each $A, B \subseteq X$:

- $\mathcal{C}(\emptyset) = \emptyset$
- $\mathcal{C}(A \cup B) = \mathcal{C}(A) \cup \mathcal{C}(B)$
- $A \subseteq \mathcal{C}(A)$
- ~~$\mathcal{C}(\mathcal{C}(A)) = \mathcal{C}(A)$~~

Define:

- $\mathcal{I}(A) = \overline{\mathcal{C}(\overline{A})}$
- A is *open* iff $A = \mathcal{I}(A)$
- A is *closed* iff $A = \mathcal{C}(A)$
- A is a *neighbourhood* of $x \in X$ iff $x \in \mathcal{I}(A)$

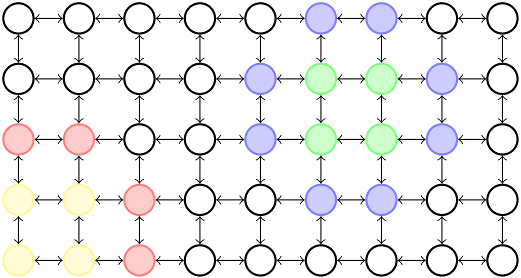
Interior and closure are duals:

- $\mathcal{C}(A) = \overline{\mathcal{I}(\overline{A})}$

Theorem

$(X, \mathcal{C})$ is quasi-discrete iff there is $R \subseteq X \times X$ such that $\mathcal{C} = \mathcal{C}_R$

Inspired by topological logic and (quasi discrete) Closure Spaces



All red and yellow points satisfy $\mathcal{N}\, yellow$

One yellow point satisfies $\mathcal{I}\, yellow$

No points satisfy $\mathcal{I}\, green$

Green points satisfy $green\, \mathcal{S}\, blue$

Yellow points satisfy $yellow\, \mathcal{S}\, red$

SLCS syntax

$$\begin{array}{lcll} \Phi & ::= & p & [\textsc{Atomic proposition}] \\ & \mid & \top & [\textsc{True}] \\ & \mid & \neg\Phi & [\textsc{Not}] \\ & \mid & \Phi \wedge \Phi & [\textsc{And}] \\ & \mid & \mathcal{N}\Phi & [\textsc{Near}] \\ & \mid & \Phi\,\mathcal{S}\,\Phi & [\textsc{Surrounded}] \end{array}$$

Semantics of SLCS

quanticol
www.quanticol.eu

Satisfaction $\mathcal{M}, x \models \phi$ of formula ϕ at point x in quasi-discrete closure model $\mathcal{M} = ((X, \mathcal{C}), \mathcal{V})$ is defined, by induction on terms, as follows:

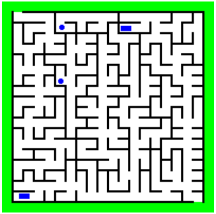
$$
\begin{array}{lclcl}
\mathcal{M}, x & \models & p & \iff & x \in \mathcal{V}(p) \\
\mathcal{M}, x & \models & \top & \iff & \mathit{true} \\
\mathcal{M}, x & \models & \neg\phi & \iff & \texttt{not}\, \mathcal{M}, x \models \phi \\
\mathcal{M}, x & \models & \phi \wedge \psi & \iff & \mathcal{M}, x \models \phi \;\texttt{and}\; \mathcal{M}, x \models \psi \\
\mathcal{M}, x & \models & \mathcal{N}\phi & \iff & x \in \mathcal{C}(\{y \in X | \mathcal{M}, y \models \phi\}) \\
\mathcal{M}, x & \models & \phi\, \mathcal{S}\, \psi & \iff & \exists A \subseteq X. x \in A \wedge \forall y \in A. \mathcal{M}, y \models \phi \wedge \\
 & & & & \quad \forall z \in \mathcal{B}^{+}(A). \mathcal{M}, z \models \psi
\end{array}
$$

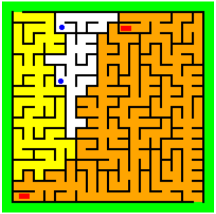
Prototype model-checker available on github:
www.github.com/vincenzoml/topochecker

Spatial Logics for Closure Spaces

$$\phi\,\mathcal{R}\psi \triangleq \neg((\neg\psi)\,\mathcal{S}(\neg\phi)) \qquad \text{(reachability)}$$
$$\phi\,\mathcal{T}\,\psi \triangleq \phi \wedge ((\phi \vee \psi)\,\mathcal{R}\psi) \qquad \text{(from-to)}$$

Any digital image can be treated as a (quasi discrete) closure space





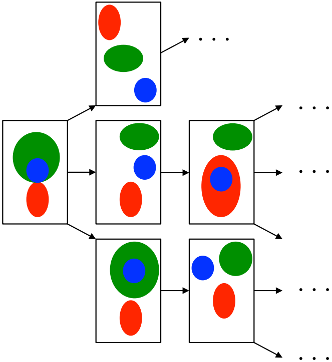
```
toExit = [white] T [green] {●, ●}
fromStartToExit = toExit & ([white] T [blue]) {●}
startCanExit = [blue] T fromStartToExit {●}
```

Further Derived Operators

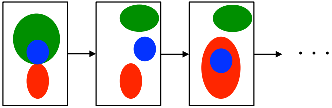
$$\begin{array}{rcll} \mathcal{G}\phi & \triangleq & \phi\,\mathcal{S}\,\bot & \text{(everywhere)} \\ \mathcal{F}\phi & \triangleq & \neg\mathcal{G}(\neg\phi) & \text{(somewhere)} \end{array}$$

"Snapshot" model:

Branching time:



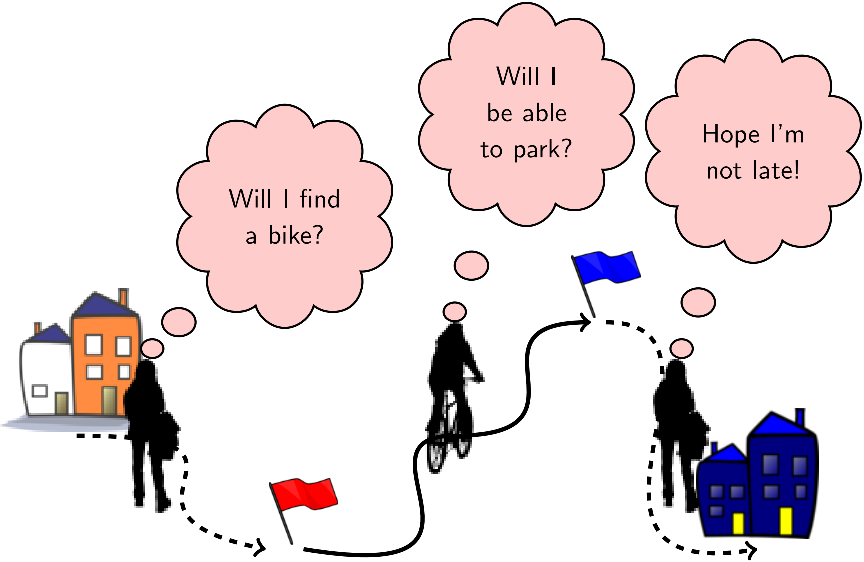
Path:



STLCS syntax

$$
\begin{array}{lcll}
\Phi & ::= & \top & [\textsc{True}] \\
 & \mid & p & [\textsc{Atomic predicate}] \\
 & \mid & \neg\Phi & [\textsc{Not}] \\
 & \mid & \Phi \vee \Phi & [\textsc{Or}] \\
 & \mid & \Phi \wedge \Phi & [\textsc{And}] \\
 & \mid & \mathcal{N}\,\Phi & [\textsc{Near}] \\
 & \mid & \Phi\mathcal{S}\Phi & [\textsc{Surrounded}] \\
 & \mid & \mathtt{A}\,\varphi & [\textsc{All Futures}] \\
 & \mid & \mathtt{E}\,\varphi & [\textsc{Some Future}] \\
 & & & \\
\varphi & ::= & \mathcal{X}\,\Phi & [\textsc{Next}] \\
 & \mid & \mathtt{F}\,\Phi & [\textsc{Eventually}] \\
 & \mid & \mathtt{G}\,\Phi & [\textsc{Globally}] \\
 & \mid & \Phi\;\mathcal{U}\;\Phi & [\textsc{Until}]
\end{array}
$$

Bike-sharing trips from users' perspective

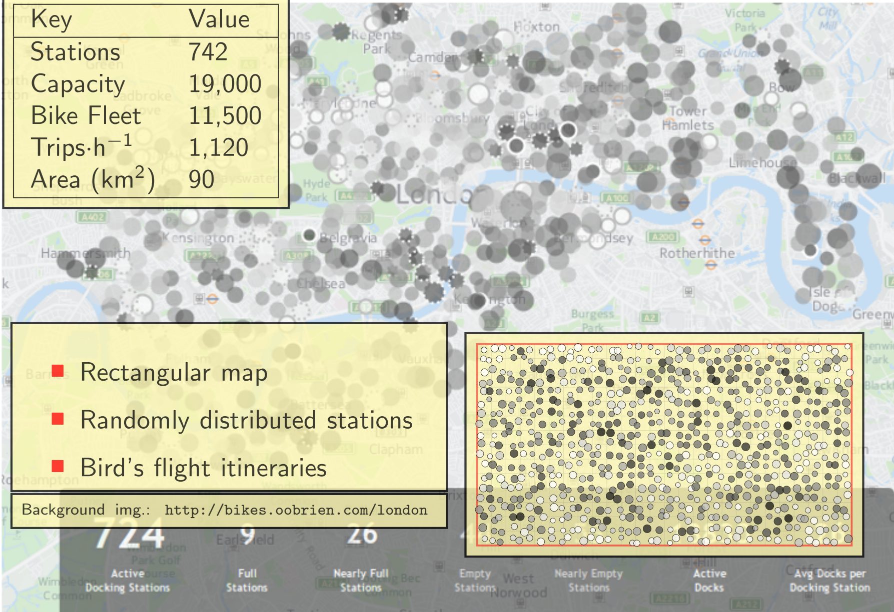


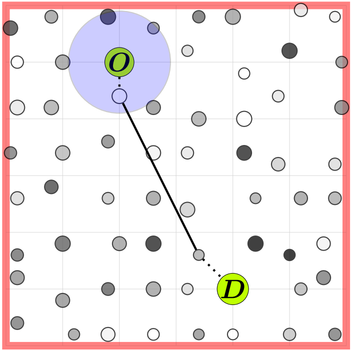
Bare-bones urban structure

Key	Value
Stations	742
Capacity	19,000
Bike Fleet	11,500
Trips·h^{-1}	1,120
Area (km^2)	90

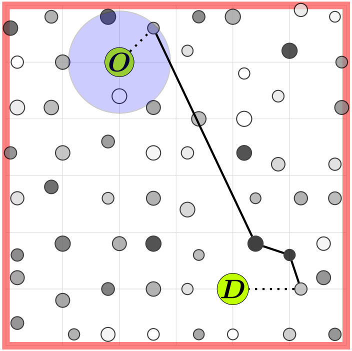
- Rectangular map
- Randomly distributed stations
- Bird's flight itineraries

Background img.: `http://bikes.oobrien.com/london`





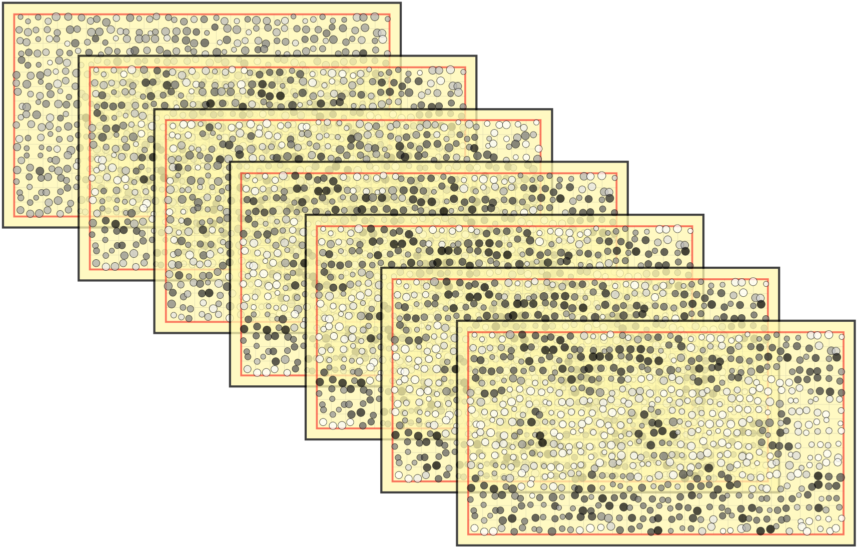
- Optimal path may not be available
- Empty station prevents hiring
  1. quit
  2. continue searching
- Full station prevents returning
  1. ~~quit~~
  2. continue searching
- Delays result from searching



- Optimal path may not be available
- Empty station prevents hiring
  1. quit
  2. continue searching
- Full station prevents returning
  1. ~~quit~~
  2. continue searching
- Delays result from searching

model trace

quanticol
www.quanticol.eu



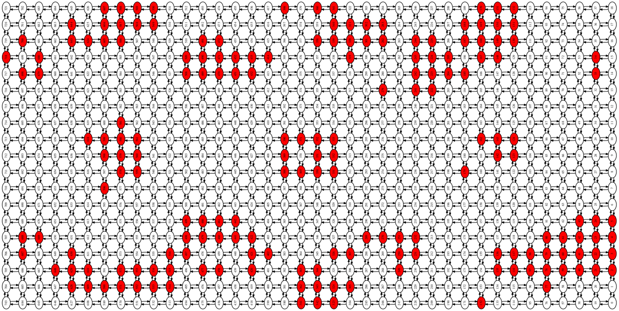
Example 1

Model checking specific rare events

quanticol
www.quanticol.eu

- Upon bumping on a full station, cycle to a nearby one or wait
- Rare event: User bumps to a full station, followed by bumping to a full station, followed by bumping to a full station,. . .
- Formula to express this event:

$$\texttt{unlucky3steps} = \texttt{full}\,\&\,(\texttt{N}\,(\texttt{A}\,\texttt{X}\,(\texttt{full}\,\&\,(\texttt{N}\,(\texttt{A}\,\texttt{X}\,(\texttt{full}\,\&\,\texttt{N}\,(\texttt{A}\,\texttt{X}\ \texttt{full})))))))$$



Example 2

Boundary and core of a cluster

- Define cluster: $\texttt{cluster} = \texttt{I}\,(\texttt{full})$
- Full is atomic $\Phi = \{\text{station is full}\}$: $\texttt{full} = [\texttt{vacant}{=}{=}0]$
- Interior of Φ: $\texttt{I}\,\Phi = !\,(\texttt{N}\,(!\,\Phi))$
- Standard implication: $\texttt{implies}(\texttt{f},\texttt{g}) = (!\,\texttt{f})\,|\,\texttt{g}$

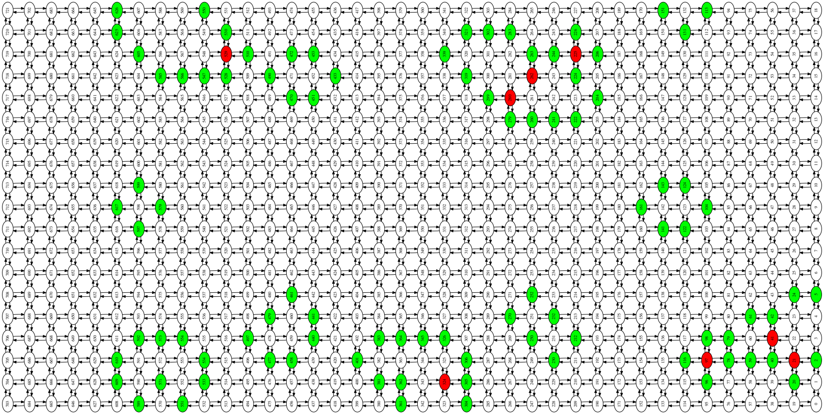
$$\texttt{boundaryCluster} = (!\,\texttt{E}\,\texttt{F}\,\texttt{cluster})\,\&\,(\texttt{N}\;\texttt{E}\,\texttt{F}\,\texttt{cluster})$$

Read: which a point that is near a cluster *and* is not part of a cluster $\Rightarrow$ which is a boundary of a cluster!

$$\begin{aligned}\texttt{coreCluster} \;\; = {} & (\texttt{E}\,\texttt{F}\;\texttt{full})\,\&\\ & (\texttt{A}\,\texttt{G}\;\texttt{implies}(\texttt{full},\\ & \quad \texttt{A}\;\texttt{full}\;\texttt{U}\;\texttt{cluster}))\end{aligned}$$

Read: which is a point that will eventually become full *and*,
for every future state, whenever full, it will stay full until becoming part of a cluster.

Example 2
Boundary and core of a cluster

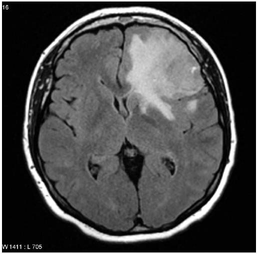


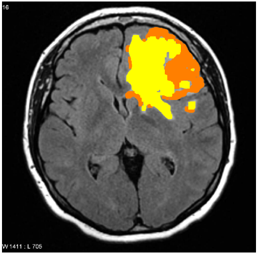
- A possible strategy: eliminate red points

Outlook and Related Work

- Additional spatial operators: e.g. bounded surround, propagation $\phi_1 \mathcal{P} \phi_2$
- Combination with Signal Temporal Logic: Spatial STL e.g. [Nenzi et al., VALUETOOLS14, RV15]
- Application in different domains: Medical Imaging

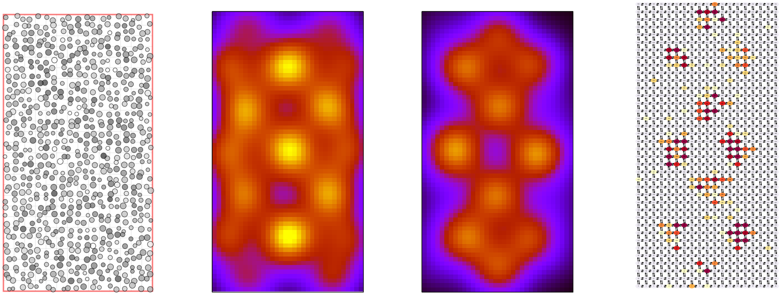
[Ciancia et al., FORECAST16, accepted] Case courtesy of Prof. Frank Gaillard, Radiopaedia.org, rID: 5292





Outlook and Related Work (2)

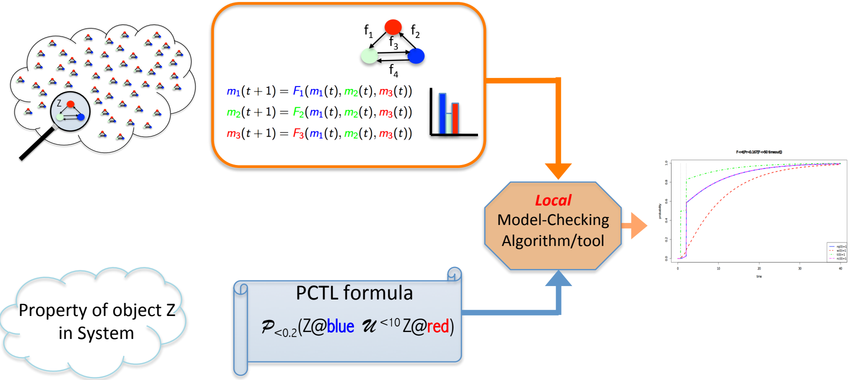
- Quantitative analysis: probability of satisfaction
  Spatial Statistical Model Checking:



stations | hiring density | returning density | prob. station gets full

[Ciancia et al., ISOLA16, accepted]

Mean Field Model-checking of large population DTMCs [Latella,Loreti,Massink, TGC13, SCP2015]



FlyFast on-the-fly mean field model checker at:
`http://j-sam.sourceforge.net/?page_id=21`

Thanks for your attention!