

Formal Methods for Probabilistic Systems

Annabelle McIver
Carroll Morgan

- Source-level program logic
- Meta-theorems for loops
- Examples
- Relational operational model
- Almost-certain termination
- Mu-calculus, temporal logic and games

British *EPSRC* (Oxford),
then Australian *ARC*
(Macquarie/UNSW),
1994-continuing.

Annabelle McIver
Carroll Morgan
Jeff Sanders
Karen Seidel

`web.comlab.ox.ac.uk/
oucl/
research/
areas/
probs/`



Abstraction, refinement and proof for probabilistic systems

Annabelle McIver
Carroll Morgan

- Source-level program logic
 - Introduction to probabilistic-program logic
 - Systematic presentation via structural induction
 - Layout of calculations in practice
 - Random variables and expected values
 - The impact of demonic choice

Abstraction, refinement and proof for probabilistic systems

Annabelle McIver
Carroll Morgan

- Source-level program logic
- Meta-theorems for loops
 - Introduction and example
 - Review of rules for standard loops
 - Rules for probabilistic loops
 - Analysis of an example
 - Probability-one termination
 - The Zero-One Law



Abstraction, refinement and proof for probabilistic systems

Annabelle McIver
Carroll Morgan

- Source-level program logic
- Meta-theorems for loops
- Examples
 - Probabilistic amplification
 - Uniform selection

Abstraction, refinement and proof for probabilistic systems

Annabelle McIver
Carroll Morgan

- Source-level program logic
- Meta-theorems for loops
- Examples
- Relational operational model
 - Standard, deterministic, terminating *functions*
 - Standard, deterministic, non-terminating *functions with \perp*
 - Standard, demonic, non-terminating *relations with \perp*
 - Standard powerdomains *closure*
 - Probabilistic powerdomains *sub-distributions*
 - Demonic, probabilistic powerdomains *sets of...*
 - Examples *program geometry*

Abstraction, refinement and proof for probabilistic systems

Annabelle McIver
Carroll Morgan

- Source-level program logic
- Meta-theorems for loops
- Examples
- Relational operational model
- Almost-certain termination
 - “Herman’s Graph”
 - Probabilistic variant rule
 - Termination of Herman’s Graph
 - Herman’s Ring
 - Termination of Herman’s Ring
 - Expected time to stability;
comparison with model-checking (*PRISM*)

Abstraction, refinement and proof for probabilistic systems

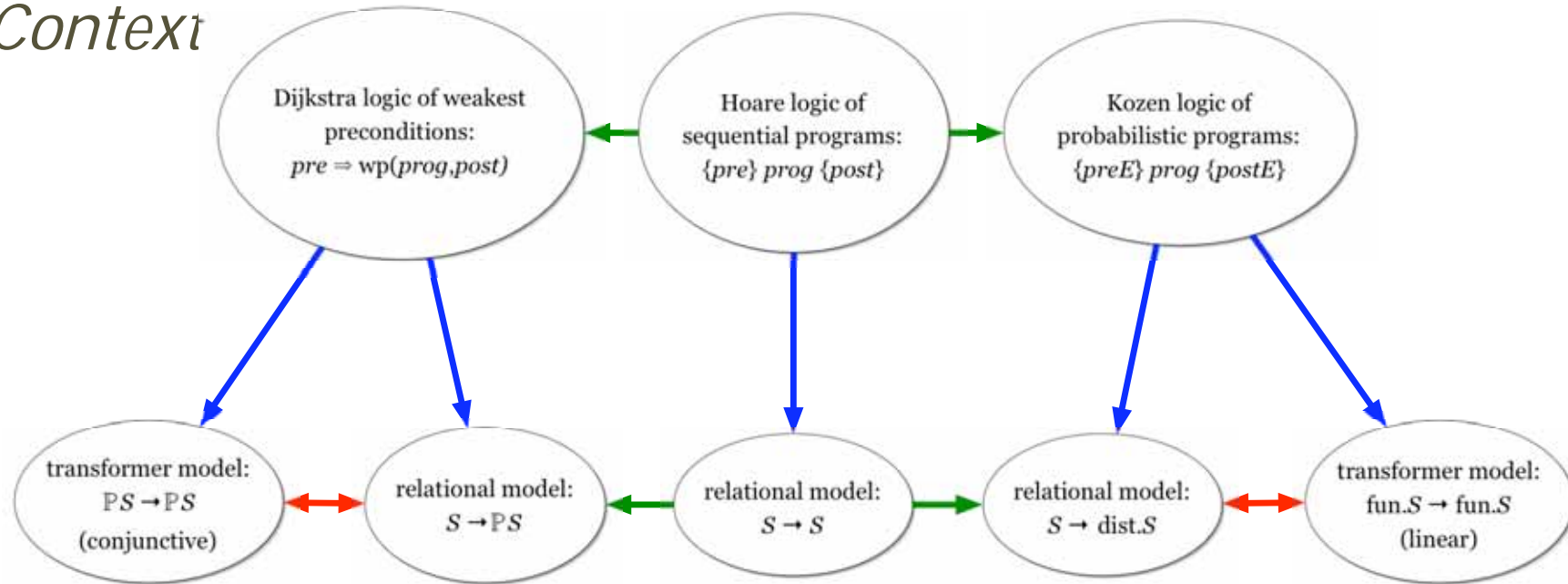
Annabelle McIver
Carroll Morgan

- Source-level program logic
- Meta-theorems for loops
- Examples
- Relational operational model
- Almost-certain termination
- Mu-calculus, temporal logic and games
 - Two-player probabilistic games, and their value
 - The $qM\mu$ and its game interpretation
 - *Minimax* and *maximin* for games
 - The denotational interpretation of $qM\mu$
 - *Theorem*: the equivalence of games and denotations
 - Example: solution via *Mathematica* and *PRISM*

add non-determinism

add probability

Context



Is modelled by...

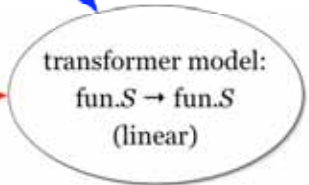
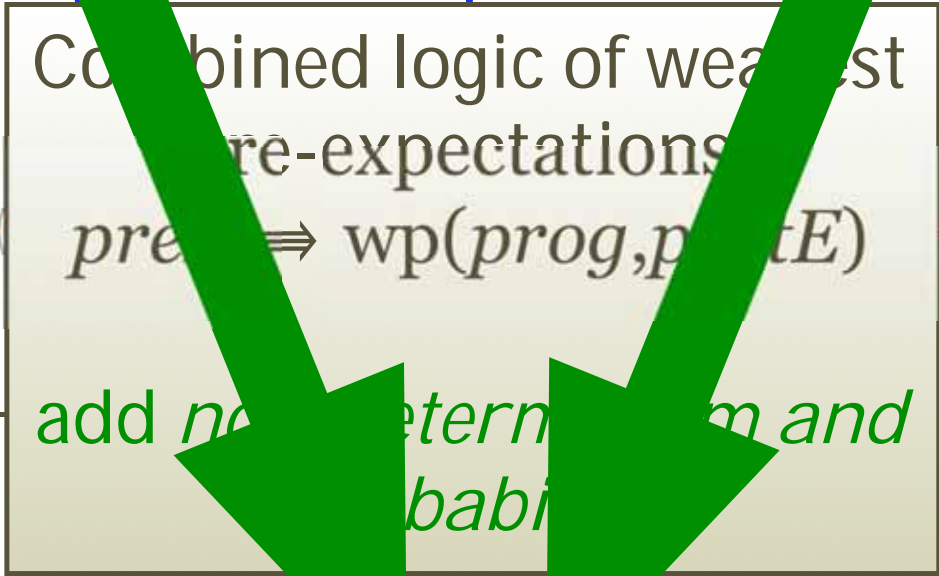
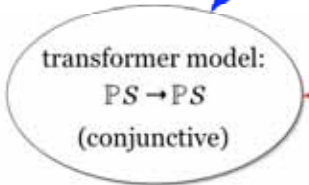
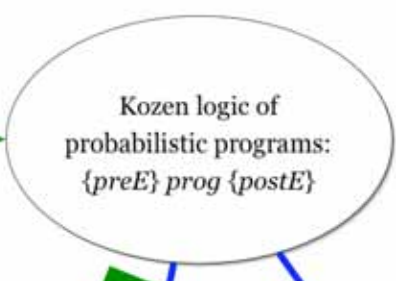
Generalises to...

Has a Galois connection between...

Context

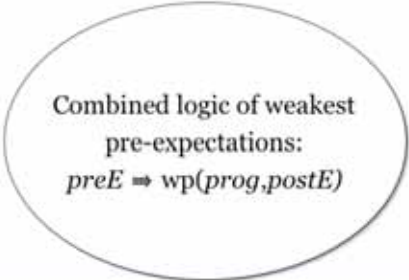
add non-determinism

add probability



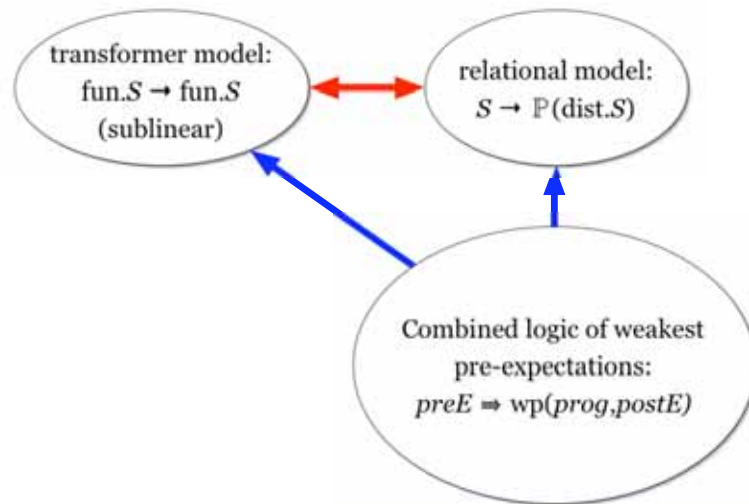
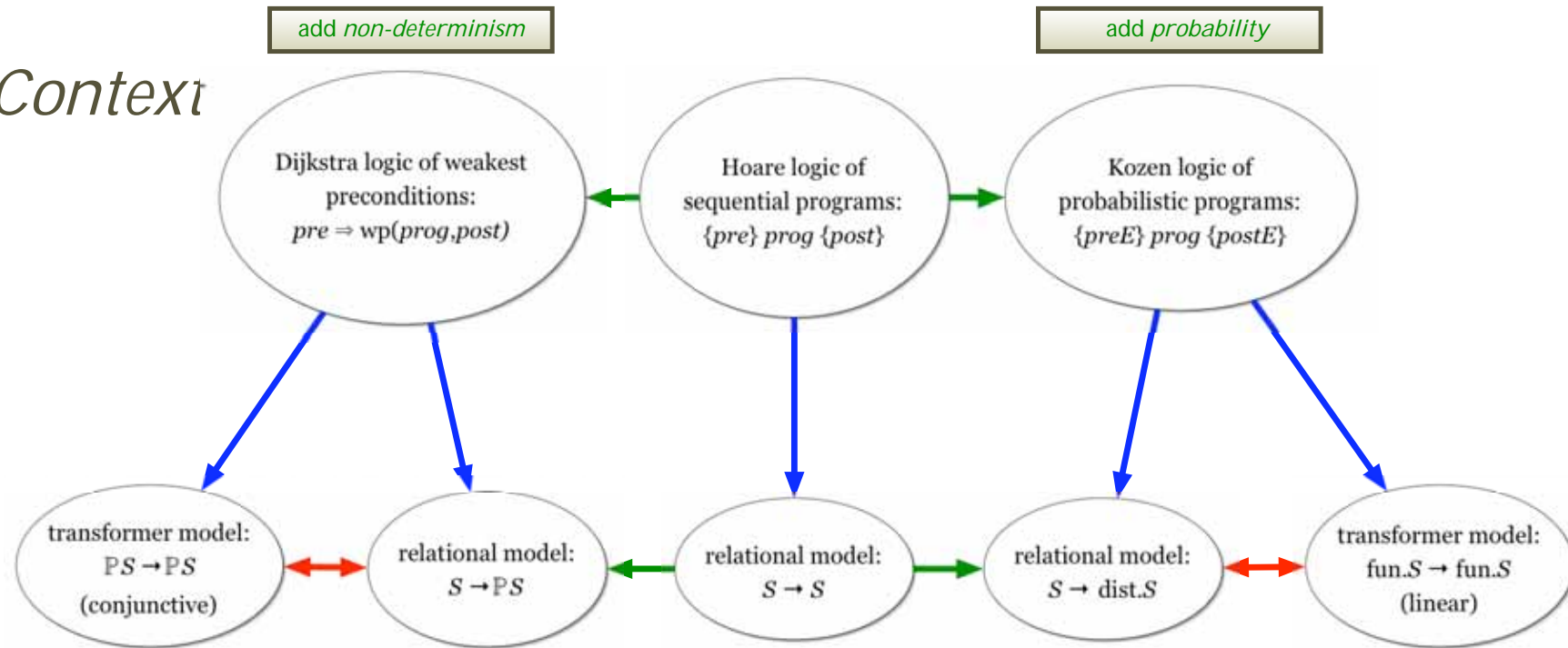
add non-determinism and probability

is modelled by...
Generalises to...
Has a Galois connection between...



add non-determinism and probability

Context



add non-determinism and probability

Is modelled by...
 Generalises to...
 Has a Galois connection between...

