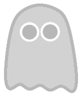
Quantum Hoare Logic
... and Ghosts

Dominique Unruh

RWTH Aachen, University of Tartu

Overview

- What are Hoare logics?
- What are quantum Hoare logics?
- What about ghosts??? 

Chapter I

Hoare Logic

Hoare Logic

Relates precondition
and postcondition of a program

$$\{x = 1\} \;\; x := x + 1 \;\; \{x = 2\}$$

"If memory initially satisfies $x = 1$,
then memory afterwards satisfies $x = 2$"

Why Hoare Logic?

- Describe what a program does
- Reason about programs
- More abstractly:
  Understand processes with effects?

Specification of programs

$\{set(x) = x_0\}$ **quicksort** $\{set(x) = x_0 \wedge x\ sorted\}$

What about these?
How are they defined?

Easier: just predicates about values of variables

Example reasoning

$$\{\boldsymbol{x} = \boldsymbol{x_0} \wedge \ \boldsymbol{y} = \boldsymbol{y_0}\}$$

$$x \leftarrow x + y$$

$$\{\boldsymbol{x} = \boldsymbol{x_0} + \boldsymbol{y_0} \wedge \ \boldsymbol{y} = \boldsymbol{y_0}\}$$

$$y \leftarrow x - y$$

$$\{\boldsymbol{x} = \boldsymbol{x_0} + \boldsymbol{y_0} \wedge \ \boldsymbol{y} = \boldsymbol{x_0}\}$$

$$x \leftarrow x - y$$

$$\{\boldsymbol{x} = \boldsymbol{y_0} \wedge \boldsymbol{y} = \boldsymbol{x_0}\}$$

$$\{\boldsymbol{x} = \boldsymbol{x_0} \ \wedge \ \boldsymbol{y} = \boldsymbol{y_0}\}$$

$$x \leftarrow x + y$$

$$y \leftarrow x - y$$

$$x \leftarrow x - y$$

$$\{\boldsymbol{x} = \boldsymbol{y_0} \ \wedge \ \boldsymbol{y} = \boldsymbol{x_0}\}$$

Rules

$$\frac{\{A\}c\{B\} \qquad \{B\}d\{C\}}{\{A\}c;d\{C\}} \qquad \frac{A \Rightarrow B\{e/x\}}{\{A\}x \leftarrow e\{B\}} \qquad \ldots$$

- Either **axiomatic**
  (rules define semantics of the language)
- Or **proven sound**
  (given a semantics of the language)

Chapter II

Quantum Hoare Logic

Quantum mechanics

Classical world

State of a system: $(123, 383, 633)$

Set

Quantum world

State of a system: $|123, 383, 633\rangle$

But also: $\frac{1}{\sqrt{2}}|123, 383, 633\rangle + \frac{1}{\sqrt{2}}|932, 503, 321\rangle$

Hilbert space

Quantum programs

- Have a memory that is quantum (with superpositions)
- Can do quantum operations (what physics tells us is allowed)
- E.g., speed-up due to “parallelism”
- Also just interesting from a logical point of view

Quantum programs (semantically)

- Take a quantum state ψ
- Return a new quantum state ψ'

- A function from a Hilbert space to itself
  - (Usually “unitary”, or “contractive”)

- Example:
  flipx takes $|x, y, z\rangle$ to $|\neg x, y, z\rangle$

Quantum Hoare Logic

{precondition} program {postcondition}

What is this?

- Should describe the content of the memory
- Classically: a predicate
- Quantum: a subspace!

Example

$$\overset{X=|0\rangle}{\{span\{|0,y,z\rangle\}\}}\ \textbf{\textit{flipx}}\ \overset{X=|1\rangle}{\{span\{|1,y,z\rangle\}\}}$$

- Explicitly writing subspaces: Horrible
- Need nice syntax
- von Neumann / Birkhoff:
  - Operations like ∧ and ∨ and "complement"
  - Similar, but not the same as a Boolean algebra

Example II

$\{X = |0\rangle \wedge Y = |1\rangle\}$ ***flipx***

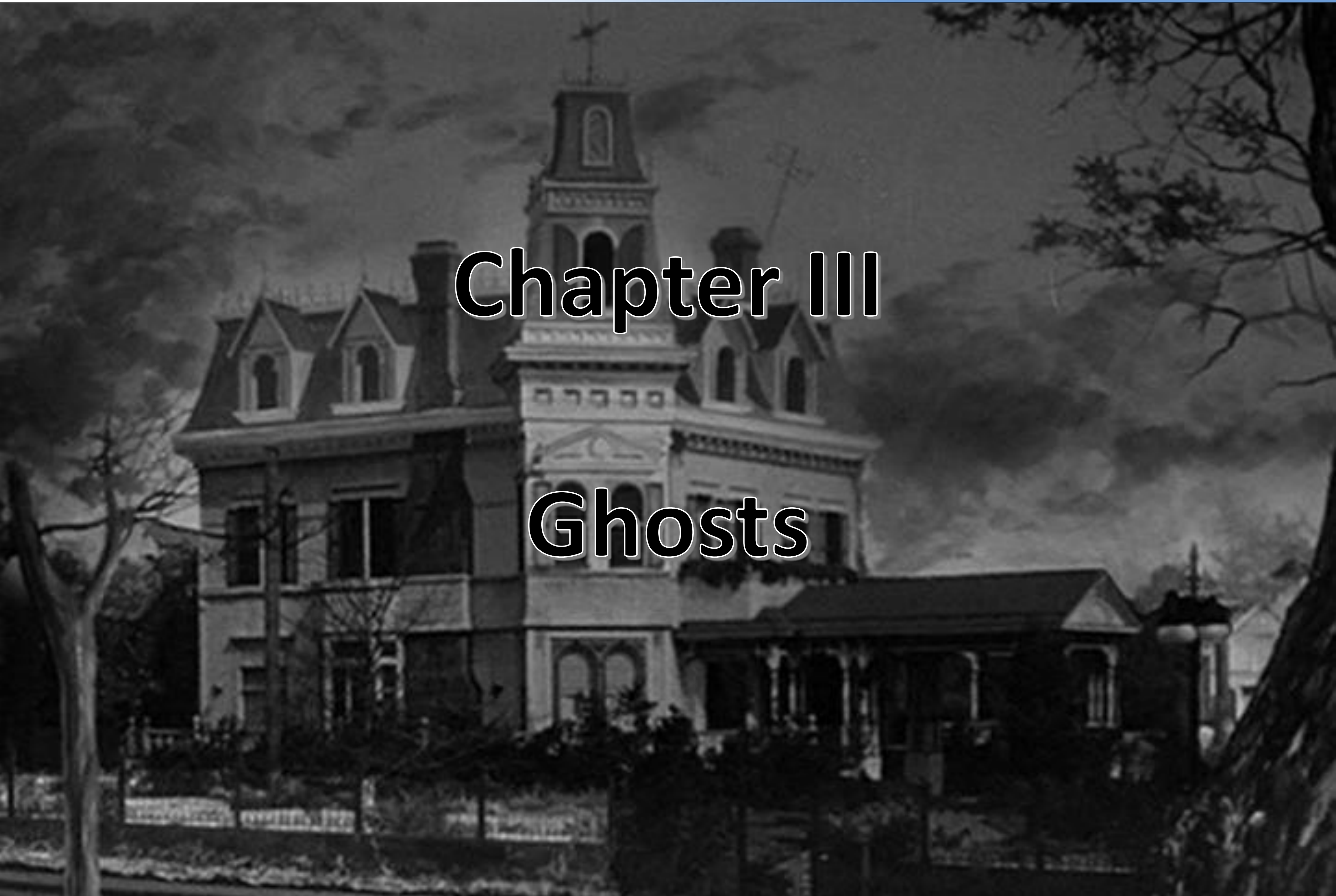
$\{X = |1\rangle \wedge Y = |1\rangle\}$ ***flipx***

$\{X = |0\rangle \wedge Y = |1\rangle\}$

- Powerful approach
- Bottom-up reasoning
- Predicates as subspaces:
  Natural mathematical structure

Chapter III

Ghosts



Limitations of subspaces

Trying to express: "x is classical"

$$x = |0\rangle \lor x = |1\rangle$$

Also contains $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. Not classical!

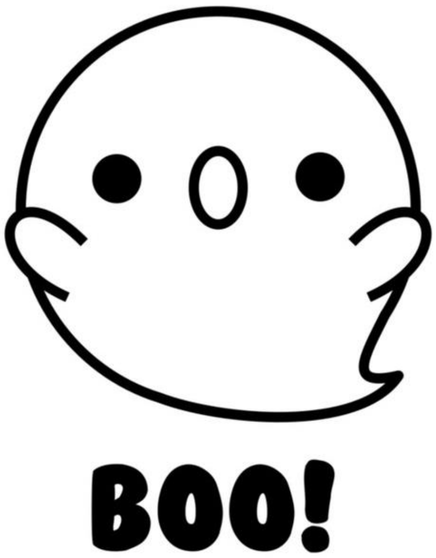
Trying to express: "x is uniformly random"

Impossible.

Trying to express: "x not entangled"

Impossible.

Ghost Variables



Hypothetical "existential" quantum variables

Solves the aforementioned problems

Leads to a richer QHL

Ghost Variables – classically

$$\{x = g^2\} \quad x \leftarrow 4x \quad \{x = g^2\}$$

Meaning: for some value of g, this is true

"If x is a square before,
x is a square afterwards."

$$\{\exists g.\, x = g^2\} \; x \leftarrow 4x \; \{\exists g.\, x = g^2\}$$

Ghost Variables – quantumly

$\{xg = |\Phi^+\rangle\}$ Hadamard $\{xg = |\Phi^+\rangle\}$

Meaning: for some value of g, this is true

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

- If $xg = |\Phi^+\rangle$, and g is removed, then x is uniformly distributed qubit

- Program memory satisfies $xg = |\Phi^+\rangle$

  $\Leftrightarrow$

  x is uniformly distributed qubit

Summary (so far)

Ghost variables: "Existential" quantum variables

- Cannot be simulated with ∃
- Can express:
  - Distribution of x (not just uniformity)
  - Classicality of x ("$x =_{cl} g$" for "unentangled" ghost)
  - Separability of x ("$x =_{qu} g$" for "unentangled" ghost)

Example

$\{\mathbf{true}\}$
$\quad x \leftarrow \mathbf{random}$
$\{x \text{ uniform}\}$

$\widehat{=}$

$\{\mathbf{true}\}$
$\quad xy \leftarrow |\Phi^+\rangle$
$\{xy = |\Phi^+\rangle\}$
$\quad y \leftarrow |0\rangle$
$\{xg = |\Phi^+\rangle\}$

Consequence: Classical sampling can be treated as a <u>derived</u> concept!

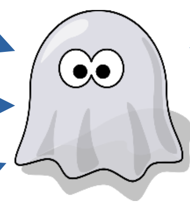
Ghost Variables → Minimalism

Built in

$x \leftarrow |0\rangle$

apply U

if/while



Derived

Sampling

Classical variables

$x \leftarrow$ expression

Measurement

+ rules for the above

Conclusion

Hoare logics:
Describe what a program does

Quantum Hoare logics:
Describe what a quantum program does

Ghosts:
Capture richer properties through hypothetical variables

Questions?