Sequential Nondeterminism

Stefan Muller, based on material by Jim Sasaki

CS 536: Science of Programming, Spring 2022
Lecture 19

1 What and Why?

1.1 What?

- Up until now, our programs have been *deterministic*: they behave exactly one way at runtime.
- We may not know which way when we run the program, e.g.:

  $$\mathsf{if}\ (x < \overline{0})\ \mathsf{then}\ \{z := \overline{0}\}\ \mathsf{else}\ \{z := \overline{1}\}$$

  We don't know what x is when we write/analyze/annotate/compile/etc. the program, but at runtime x has a definite value, so this program will have a definite behavior.
- This is why, until now, $M(s, \sigma)$ has been a set containing exactly one state.
- *Nondeterminism* is when a program may have different, unpredictable behaviors at runtime.
- A major source of nondeterminism in programs is *concurrency*, where multiple threads run at the same time and the computer schedules them nondeterministically. We'll study this in coming lectures.
- Today, we'll look at nondeterminism in *sequential* (not parallel or concurrent) programs.

1.2 Why?

- Sequential programs generally aren't *actually* nondeterministic, which is why nondeterminism hasn't really come up until now.
- However, nondeterminism is useful for modeling anything that we can't reason about when we're writing, analyzing or compiling a program:
  - Randomness[1]
  - User input
  - Undefined behavior
- It's also useful when writing a program when we don't want to have to worry about overlapping cases. Consider these two programs to calculate the max of x and y:

  $$\mathsf{if}\ (x \geq y)\ \mathsf{then}\ \{m := x\}\ \mathsf{else}\ \{m := y\}$$
  $$\mathsf{if}\ (y \geq x)\ \mathsf{then}\ \{m := y\}\ \mathsf{else}\ \{m := x\}$$

[1] You may think that randomness should be the very definition of nondeterministic behavior, but most randomness used in programming (e.g. pseudorandom number generators or PRNGs) is in fact deterministic if one considers as inputs to the program anything from the environment that might be used to seed a PRNG, like the time or `/dev/rand`.

They're basically the same, but differ when $x = y$: the first program will choose x and the second will choose y. This isn't real nondeterminism: the result is of course the same either way, but it's possible we might prefer one choice over the other for efficiency or other reasons, and we might want to delay that choice, or even let the compiler choose the most efficient version.

- A nondeterministic version of the if statement would let us choose nondeterministically between $m := x$ and $m := y$ in this case.

2 Syntax and Informal Semantics

2.1 Nondeterministic Branch

We'll add a nondeterministic branching statement:

$$s ::= \ldots \mid \mathsf{branch}\ \{e_1 \to s_1 \,\square \cdots \square\, e_n \to s_n\}$$

It consists of multiple statements $s_1, \ldots, s_n$, each *guarded* by a Boolean expression $e_1, \ldots, e_n$. That $\square$ symbol between the branches isn't a missing font in your PDF reader or printer, it's actually the symbol we'll use (if you do have a missing font in your PDF reader or printer and you're seeing squares in other places, you may start getting very confused, unfortunately...) Each e_i tells us whether it's OK to run s_i (if e_i is true, it's OK). This is like a `switch` statement in C/Java or a pattern match in some higher-level languages, but with a key difference: it's nondeterministic, while most of those language constructs are deterministic.

Informally:

- If none of the e_i are true, abort with a runtime error.
- Otherwise, if multiple guards are true, run one of the corresponding statements nondeterministically (in the special case that exactly one is true, that one will be run deterministically).

Example: We can write our max program from above as

$$\mathsf{branch}\ \{x \geq y \to m := x \,\square\, y \geq x \to m := y\}$$

if $x = y$, either branch can run. In this case, since both set m to the same value, we don't care which. In general, the branches might do different things.

2.2 Nondeterminism vs. Randomness

In this class, we'll treat "nondeterministic" as meaning something closer to "unpredictable" than "random". Consider the following program:

$$\mathit{flip} \triangleq \mathsf{branch}\ \{T \to x := \overline{0} \,\square\, T \to x := \overline{1}\}$$

Both guards always hold, so flip will always set x to 0 or 1 nondeterministically. As the name suggests, this models a coin flip, but it doesn't necessarily *act* like a coin flip:

- With a real coin flip, you expect a 50-50 chance of getting 0 or 1, but since flip is nondeterministic, its behavior is completely unpredictable.
- A thousand calls of flip might give us anything: all 0's, all 1's, some pattern, random 500 heads and 500 tails, etc.

Nondeterminism shouldn't affect correctness. We'll use nondeterminism when we don't want to worry about how choices are made. Maybe when we write the final version of the program, we'll replace *flip* with a call to a random number generator, or a prompt for user input. The point is we want to make sure the rest of our program is correct whether the coin comes up heads or tails.

This also applies in our max example above. If we were actually writing a max function, we'd probably go back and replace the nondeterministic code with deterministic code that makes one of the choices, but

it's good to know that the correctness of the program won't change when we make that choice. Or maybe our language actually has a nondeterministic branching operator and the compiler will actually make the most efficient choice when multiple guards are true: in this case, we may want to leave it nondeterministic, but we definitely want to know that the correctness of the program doesn't depend on the compiler's choice (which may change in a future version of the compiler)!

This also exposes the difference between nondeterminism and randomness: in the *max* function, the compiler will almost certainly choose a branch deterministically (rather than randomly), but this choice is part of the *compiler*, not the *program*, and we don't want to reason about the whole compiler when we're proving our program correct.

Undefined behavior in languages is another good example of this. For example, in C, accessing an out-of-bounds array index is "undefined." The compiler is free to do anything it wants, including return a random number. Now, for any given compiler, what it does is deterministic, generally whatever lets the compiler generate the fastest code (probably return whatever's in memory next to the array, or segfault). But if we wanted our program to be correct in the face of undefined behavior, we'd treat this as nondeterminism because it's *unpredictable* (to us).

2.3 Havoc

Extending the *flip* example, we might want code that sets x to *anything*, like so:

$$\mathsf{branch}\ \{\cdots \square\, T \to x := \overline{-1} \square\, T \to x := \overline{0} \square\, T \to x := \overline{1} \square \ldots\}$$

Of course, we can't write such a program in a finite amount of space[2]. Instead, we'll explicitly make it a statement:

$$s ::= \ldots \mid \mathsf{havoc}\ x$$

$\mathsf{havoc}\ x$ assigns any integer nondeterministically to x (as above, we can think of this as a call to a random number generator, taking user input, or any sort of unpredictable behavior; the point is it's some process we can't or don't want to reason about).

2.4 Nondeterministic Loop

We'll also add a nondeterministic while loop:

$$s ::= \ldots \mid \mathsf{while}\ \{e_1 \to s_1 \square \cdots \square\, e_n \to s_n\}$$

Informal semantics:

- At the top of the loop, check for any true guards.
- If no guard is true, the loop terminates.
- If exactly one guard is true, execute its corresponding statement and jump to the top of the loop.
- If more than one guard is true, select one of the corresponding guarded statements and execute it. (The choice is nondeterministic.) Once we finish the guarded statement, jump to the top of the loop.

3 Small-step semantics

Nondeterminism is fairly simple to express in small-step semantics. We'll just have a rule for each possibility. When you step, you can apply *any rule* whose premise holds. This means that now, there may be multiple σ' and s' such that $\langle s, \sigma\rangle \to \langle s', \sigma'\rangle$, but the steps will look the same as before.

If any guard fails or all are false, nondeterministic branching fails. Otherwise, we can step to any statement guarded by a true guard.

[2]Technically, if we only consider, e.g., 64-bit integers, we could, but please don't try.

$$\frac{\exists i \in [1,n].\sigma(e_i) = \bot_e}{\langle \mathsf{branch}\ \{e_1 \to s_1 \,\square\, \cdots \,\square\, e_n \to s_n\}, \sigma\rangle \to \langle \mathsf{skip}, \bot_e\rangle} \qquad \frac{\sigma(e_1) = \cdots = \sigma(e_n) = F}{\langle \mathsf{branch}\ \{e_1 \to s_1 \,\square\, \cdots \,\square\, e_n \to s_n\}, \sigma\rangle \to \langle \mathsf{skip}, \bot_e\rangle}$$

$$\frac{\sigma(e_i) = T}{\langle \mathsf{branch}\ \{e_1 \to s_1 \,\square\, \cdots \,\square\, e_n \to s_n\}, \sigma\rangle \to \langle s_i, \sigma\rangle}$$

The rule for havoc just picks a number and updates the state. There's only one rule, but we can choose any value for n, hence the nondeterminism.

$$\frac{n \in \mathbb{Z}}{\langle \mathsf{havoc}\ x, \sigma\rangle \to \langle \mathsf{skip}, \sigma[x \mapsto n]\rangle}$$

The rules for the nondeterministic loop are pretty similar to the nondeterministic branch; unfortunately, we can't just use the same trick of stepping a "while" to an "if" because the nondeterministic loop has a different behavior if all the guards are false.

$$\frac{\exists i \in [1,n].\sigma(e_i) = \bot_e}{\langle \mathsf{while}\ \{e_1 \to s_1 \,\square\, \cdots \,\square\, e_n \to s_n\}, \sigma\rangle \to \langle \mathsf{skip}, \bot_e\rangle} \qquad \frac{\sigma(e_1) = \cdots = \sigma(e_n) = F}{\langle \mathsf{while}\ \{e_1 \to s_1 \,\square\, \cdots \,\square\, e_n \to s_n\}, \sigma\rangle \to \langle \mathsf{skip}, \sigma\rangle}$$

$$\frac{\sigma(e_i) = T}{\langle \mathsf{while}\ \{e_1 \to s_1 \,\square\, \cdots \,\square\, e_n \to s_n\}, \sigma\rangle \to \langle s_i; \mathsf{while}\ \{e_1 \to s_1 \,\square\, \cdots \,\square\, e_n \to s_n\}, \sigma\rangle}$$

3.1 Example

Flip. There are two ways we could step the *flip* program:

$$\begin{array}{lll} & \langle \mathsf{branch}\ \{T \to x := \overline{0} \,\square\, T \to x := \overline{1}\}, \{\}\rangle & \\ \to & \langle x := \overline{0}, \{\}\rangle & \sigma(T) = T \\ \to & \langle \mathsf{skip}, \{x = 0\}\rangle & \end{array}$$

or:

$$\begin{array}{lll} & \langle \mathsf{branch}\ \{T \to x := \overline{0} \,\square\, T \to x := \overline{1}\}, \{\}\rangle & \\ \to & \langle x := \overline{1}, \{\}\rangle & \sigma(T) = T \\ \to & \langle \mathsf{skip}, \{x = 1\}\rangle & \end{array}$$

Infinite "Random" (Nondeterministic) Walk Let $W = \mathsf{while}\ \{T \to x := x + \overline{1} \,\square\, T \to x := x - \overline{1}\}$. This loop continues infinitely, incrementing or decrementing x on each iteration.

$$\begin{array}{rl} & \langle W, \{x = 0\}\rangle \\ \to & \langle x := x + \overline{1}; W, \\ \rangle \to^2 & \langle W, \{x = 1\}\rangle \\ \to & \langle x := x + \overline{1}; W, \\ \rangle \to^2 & \langle W, \{x = 2\}\rangle \\ \to & \langle x := x - \overline{1}; W, \\ \rangle \to^2 & \langle W, \{x = 1\}\rangle \\ & \cdots \end{array}$$

4 Big-Step Semantics

- Recall that $M(s, \sigma)$ is the set of states, which we'll sometimes denote Σ, that you can get to from running s in state σ.
- For deterministic programs, there is only one such state, so $M(s, \sigma) = \{\sigma'\}$ iff $\langle s, \sigma\rangle \to^* \langle \mathsf{skip}, \sigma'\rangle$.
- Nondeterministic programs may (or may not) have multiple final states.

$$\begin{array}{rcll} M(\mathsf{branch}\ \{e_1 \to s_1 \,\square \cdots \square\, e_n \to s_n\}, \sigma) & = & \{\bot_e\} & \sigma(e_i) = \bot_e \\ M(\mathsf{branch}\ \{e_1 \to s_1 \,\square \cdots \square\, e_n \to s_n\}, \sigma) & = & \{\bot_e\} & \forall i.\sigma(e_i) = F \\ M(\mathsf{branch}\ \{e_1 \to s_1 \,\square \cdots \square\, e_n \to s_n\}, \sigma) & = & \{\bigcup_{i\in[1,n],\sigma(e_i)=T} M(s_i, \sigma) & \\ M(\mathsf{havoc}\ x, \sigma) & = & \{\sigma[x \mapsto n] \mid n \in \mathbb{Z}\} & \end{array}$$

We won't formally define the big-step semantics for nondeterministic loops, but it involves the same technique we used for regular while loops.

Example: Flip.

$$\begin{array}{rl} & M(\mathsf{branch}\ \{T \to x := \overline{0} \,\square\, T \to x := \overline{1}\}, \{\}) \\ = & M(x := \overline{0}, \{\}) \cup M(x := \overline{1}, \{\}) \\ = & \{\{x = 0\}\} \cup \{\{x = 1\}\} \\ = & \{\{x = 0\}, \{x = 1\}\} \end{array}$$

Note: This is a set containing two states. DO NOT EVER write it as {x = 0, x = 1}, which is a single ill-formed state.

Examples: Nested nondeterminism.

$$\begin{array}{rl} & M(\mathsf{branch}\ \{T \to (\mathsf{branch}\ \{T \to x := \overline{0} \,\square\, T \to x := \overline{2}\}) \,\square\, T \to x := \overline{1}\}, \{\}) \\ = & M((\mathsf{branch}\ \{T \to x := \overline{0} \,\square\, T \to x := \overline{2}\}), \{\}) \cup M(x := \overline{1}, \{\}) \\ = & M(x := 0, \{\}) \cup M(x := 2, \{\}) \cup \{\{x = 1\}\} \\ = & \{x = 0\} \cup \{x = 2\} \cup \{x = 1\} \\ = & \{\{x = 0\}, \{x = 1\}, \{x = 2\}\} \end{array}$$

The set of states is a set, so the order doesn't matter.

Some observations:

- We still have that if $\langle s, \sigma\rangle \to^* \langle \mathsf{skip}, \sigma'\rangle$, then $\sigma' \in M(s, \sigma)$. But now there may be more than one σ' for which that's true.
- If $|M(s, \sigma)| > 1$, then s is nondeterministic.
- The converse isn't true: it's possible for a nondeterministic program to have only one final state:

$$\begin{array}{rl} & M(\mathsf{branch}\ \{x \geq y \to m := x \,\square\, y \geq x \to m := y\}, \{x = 3, y = 3\}) \\ = & M(m := x, \{x = 3, y = 3\}) \cup M(m := y, \{x = 3, y = 3\}) \\ = & \{x = 3, y = 3, m = 3\} \cup \{x = 3, y = 3, m = 3\} \\ = & \{\{x = 3, y = 3, m = 3\}\} \end{array}$$

- It's also possible for $|M(s, \sigma)|$ to vary based on σ: Let $s = \mathsf{branch}\ \{x \geq 0 \to x{:=}x{*}x \square x \leq 8 \to x{:=}{-}x\}$. We have:
  - $M(s, \{x = 0\}) = \{\{x = 0\}\}$
  - $M(s, \{x = 3\}) = \{\{x = 9\}, \{x = -3\}\}$
  - $M(s, \{x = 10\}) = \{\{x = 100\}\}$

- There's a difference between saying $M(s,\sigma) = \{\sigma'\}$ and saying $\sigma' \in M(s,\sigma')$. Both say that σ' can be a final state, but $M(s,\sigma) = \{\sigma'\}$ says it is the only final state and $\sigma' \in M(s,\sigma')$ leaves open the possibility that there are others.
- In particular, $M(s,\sigma) = \{\bot\}$ says that s always causes an error while $\bot \in M(s,\sigma)$ says that s *might* cause an error. It may also be the case that s could cause different kinds of errors: $M(s,\sigma) = \{\bot_d, \bot_e\}$.

5 Hoare Triples, wp, sp (for loop-free nondeterministic programs)

For a nondeterministic branch, in each branch, we get the precondition that the branch's guard holds. We need all of the branches to guarantee the postcondition (as with if, we could have an alternate rule that lets s_i have postcondition q_i and then the postcondition for the whole nondeterministic branch is $q_1 \vee \cdots \vee q_n$, but this is more unwieldy with more branches.) Like with normal assignments, we have two rules for havoc, which you can see as a form of nondeterministic assignment. The backward rule requires that anything that is true of x in the postcondition needs to be true of *any* integer in the precondition. The forward rule replaces x with a new ghost variable x_0, representing the old value of x: this is the first half of what the normal forward assignment rule does. Instead of adding what we now know about x, it stops there, because we now know nothing about x! This is basically equivalent to forgetting anything we knew about x, except things that are true of any integer.

$$\frac{\vdash \{p \wedge e_i\}\ s_i\ \{q\}}{\vdash \{p\}\ \mathsf{branch}\ \{e_1 \to s_1 \,\square\, \cdots \,\square\, e_n \to s_n\}\ \{q\}}\ (\textsc{NDBranch})$$

$$\frac{}{\vdash \{\forall x_0 \in \mathbb{Z}.[x_0/x]q\}\ \mathsf{havoc}\ x\ \{q\}}\ (\textsc{NDHavoc-Backward}) \qquad \frac{x_0\ \mathsf{fresh}}{\vdash \{p\}\ \mathsf{havoc}\ x\ \{[x_0/x]p\}}\ (\textsc{NDHavoc-Forward})$$

It may seem like havoc x is equivalent to leaving x as an uninitialized variable (like a function argument), which we also know nothing about. In many cases, this is true, but we can also use havoc to forget things about x in the middle of a program, maybe in just one branch:

	$\{T\}$
$x := \overline{0};$	$\{x = 0\}$
if $(x < 0)$ {	$\{x = 0 \wedge x < 0\}$
havoc x	$\{x_0 = 0 \wedge x_0 < 0\} \Rightarrow \{F\} \Rightarrow \{x = 0\}$
} else {	$\{x = 0 \wedge x \geq 0\} \Rightarrow \{x = 0\}$
skip	$\{x = 0\}$
}	$\{x = 0\}$

The fact that we can prove a postcondition about x means that the branch with the havoc must never be reached!

The extensions to the algorithm for computing wlp are pretty straightforward.

$$\begin{aligned} wlp(\mathsf{branch}\ \{e_1 \to s_1 \,\square\, \cdots \,\square\, e_n \to s_n\}, q) &= (e_1 \to wlp(s_1, q)) \wedge \cdots \wedge (e_n \to wlp(s_n, q)) \\ wlp(\mathsf{havoc}\ x, q) &= \forall x_0.[x_0/x]q \end{aligned}$$

So are the extensions to the domain predicates. Note that in the predicate for nondeterministic branches, we need $(e_1 \vee \cdots \vee e_n)$ to prevent failure due to all guards being false.

$$\begin{aligned} D(\mathsf{branch}\ \{e_1 \to s_1 \,\square\, \cdots \,\square\, e_n \to s_n\}) &= D(e_1) \wedge \cdots \wedge D(e_n) \wedge (e_1 \vee \cdots \vee e_n) \wedge (e_1 \to D(s_1)) \wedge \ldots (e_n \to D(s_n)) \\ D(\mathsf{havoc}\ x) &= T \end{aligned}$$

And the strongest postcondition says that for a nondeterministic branch, we know one branch was taken but not which. The sp for havoc uses the forward rule.

$$\begin{aligned} sp(p, \mathsf{branch}\ \{e_1 \to s_1\} \,\square\, \cdots \,\square\, e_n \to s_n) &= sp(p \wedge e_1, s_1) \vee \cdots \vee sp(p \wedge e_n, s_n) \\ sp(p, \mathsf{havoc}\ x) &= [x_0/x]p \end{aligned}$$