State Updates and Satisfaction with Quantifiers

Stefan Muller, based on material by Jim Sasaki

CS 536: Science of Programming, Fall 2023
Lecture 3

1 Satisfaction with Quantifiers

Consider the following statement:

$$P \triangleq \forall x \in \mathbb{Z}. x \neq 0 \rightarrow x \leq x^2$$

- Is this statement a tautology? Remember that it's a tautology, written $\vDash P$, if $\sigma \vDash P$ for all well-formed, proper σ.
- What does that even mean here? What states are proper?
- Previously, a state was *proper* if it assigned values to all variables in P.
- So do we need σ to assign a value to x in order to evaluate the truth value of P?
  - Answer: No. We specifically *don't* want to commit to a particular value of x because the body of the statement ($x \neq 0 \rightarrow x \leq x^2$) needs to hold for all x.
- New definition: a proper state needs to assign a value to all *free* variables in P.

Bound and free variables A variable is *bound* by quantifiers, e.g. $\forall x.P$ and $\exists x.P$ both bind the variable x inside P so that if x appears in P, we know it's the x that corresponds to that quantifier. A variable is *free* if it's not bound. For example, in

$$(\forall x \in \mathbb{Z}. x \neq 0 \rightarrow \exists y. y^2 < x) \wedge (F \rightarrow T)$$

the variable x is bound in $x \neq 0 \rightarrow \exists y. y^2 < x$ (and free outside that) and y is bound in $y^2 < x$ (and free outside that).

We'll come back to the question of whether P is satisfied/a tautology later. First, we need to discuss how to introduce new variables into a state as they're bound.

2 State Updates

To check quantified predicates for satisfaction, we need to look at different states that are related to, but not identical to, our starting state. For example, in $\{y = 1\} \vDash \forall x \in \mathbb{Z}. x^2 + 1 \geq y - 1$, we need to know that $\{y = 1, x = \alpha\} \vDash x^2 + 1 \geq y - 1$ for *every* $\alpha \in \mathbb{Z}$ (here we've just barely restated the math into English). That is, we'd need

- $\{y = 1, x = -1\} \vDash x^2 + 1 \geq y - 1$
- $\{y = 1, x = 0\} \vDash x^2 + 1 \geq y - 1$
- $\{y = 1, x = 1\} \vDash x^2 + 1 \geq y - 1$

- $\{y = 1, x = 2\} \vDash x^2 + 1 \geq y - 1$
- And so on...

The case for $\{z = 4\} \vDash \exists x \in \mathbb{Z}.x \geq z$ is a little easier: we just need $\{z = 4, x = \alpha\} \vDash x \geq z$ for *some* particular integer α (we can just say $\alpha = 5$ and call it a day).

There is a complicating factor. If the quantified variable already appears in the state, then we need to replace its binding with one that gives the value we're interested in checking.

Example. We already know $\{z = 4\} \vDash \exists x \in \mathbb{Z}.x \geq z$ because $\{z = 4, x = 5\} \vDash x \geq z$. If we start with the state $\{z = 4, x = -15\}$, which already has a binding for x, we can still prove that $\exists x \in \mathbb{Z}.x \geq z$. Why? The x in the state is different than the one bound by the $\exists$.

This use of the same name for two different variables is called *shadowing* and gets confusing. Take the statement

$$\forall x \in \mathbb{Z}.(x \geq 0 \rightarrow \forall x \in \mathbb{Z}.x \geq 0 \vee x < 0)$$

The two xs are different (and indeed $\forall x \in \mathbb{Z}.x \geq 0 \vee x < 0$ is true regardless of the first part). Inside the second $\forall$, we don't care about (and can't even refer to) the "outer" x; x is bound here by the "inner" $\forall$. We could just as well give them different names:

$$\forall x_1 \in \mathbb{Z}.(x_1 \geq 0 \rightarrow \forall x_2 \in \mathbb{Z}.x_2 \geq 0 \vee x_2 < 0)$$

This process of renaming the variable introduced by a quantifier *and* all of the instances of that variable it binds is called *α-conversion* and it's generally always safe to do if you want to make things clearer.

State update. For any state σ, variable x and value α, the update of σ at x with a, which we write $\sigma[x \mapsto \alpha]$, is a state that is a copy of σ except that it binds x to α.

- If we let $\tau = \sigma[x \mapsto \alpha]$, then $\tau(x) = \alpha$ (regardless of whether $\sigma(x)$ was defined before) and $\tau(y) = \sigma(y)$ if $x \neq y$.
- Note that if $\sigma(x) = -15$ and $\tau = \sigma[x \mapsto 5]$, $\tau(x) = 5$ but $\sigma(x)$ is still -15; we're not actually *changing* x, we're making a copy of σ and updating x (or, if you prefer, we're adding a new binding of x to 5 in σ that shadows the old one; the definitions are equivalent).
- Because of the above, it's a little counterintuitive to call this operation *update*. I prefer something like *extend*, but that's just the way it is.
- We can also refer to the binding of variables in the updated state without giving it a name, e.g. $\{x = 5, y = 6\}[x \mapsto 7](x) = 7$.

Example. If $\sigma = \{x = 2, y = 6\}$, then $\sigma[x \mapsto 0] = \{x = 0, y = 6\}$.

- $\sigma[x \mapsto 0](x) = 0$ (even though $\sigma(x) = 2$)
- $\sigma[x \mapsto 0](y) = \sigma(y) = 6$ (we didn't update y)
- $\sigma[x \mapsto 0] \vDash x^2 \leq 0$ (since $\sigma[x \mapsto 0](x) = 0$)

Multiple updates.

- We can update an updated state, e.g. $\sigma[x \mapsto 5][y \mapsto 6]$.
- We read the sequence of updates left to right. This doesn't matter in the above case, but, e.g. $\sigma[x \mapsto 5][x \mapsto 0](x) = 0$. The second update supersedes the first, like when x was already in σ and we do an update (which is, of course, exactly what's happening).

3 Back to Satisfaction with Quantifiers

- $\sigma \vDash \forall x \in \mathbb{Z}. x \neq 0 \to x \leq x^2$ if $\sigma[x \mapsto \alpha] \vDash x \neq 0 \to x \leq x^2$ for all $\alpha \in \mathbb{Z}$.
- This is true whether or not $x \in \sigma$ since the new x will shadow it.
- Similarly, for any set S, $\sigma \vDash \forall x \in S. x \neq 0 \to x \leq x^2$ if $\sigma[x \mapsto \alpha] \vDash x \neq 0 \to x \leq x^2$ for all $\alpha \in S$.
- So, to go back to the question of whether $\forall x \in \mathbb{Z}. x \neq 0 \to x \leq x^2$ is a tautology, this is the case if $\sigma[x \mapsto \alpha] \vDash x \neq 0 \to x \leq x^2$ for all well-formed, proper σ and all $\alpha \in \mathbb{Z}$ (remember that to be proper, σ doesn't need a value for x).
- In general, $\sigma \vDash \forall x \in S. P(x)$ if $\sigma[x \mapsto \alpha] \vDash P(x)$ for all $\alpha \in S$.
- $\sigma \vDash \exists x \in S. P(x)$ if there is *some* $\alpha \in S$ such that $\sigma[x \mapsto \alpha] \vDash P(x)$. We'll call this α a "witness".
- If there are many witnesses that work, you just need one.

Examples

1. Is $\{\} \vDash \forall x \in \mathbb{Z}. x \neq 0 \to x \leq x^2$
   Yes, because for any $\alpha \in \mathbb{Z}$, we have $\{x = \alpha\} \vDash x \neq 0 \to x \leq x^2$ (proving *that* is a separate question that uses the laws of math.)
2. Is $\forall x \in \mathbb{Z}. x \neq 0 \to x \leq x^2$ a tautology?
   Yes. The state $\{\}$ in the previous question wasn't used at all, so that holds for any state.
3. Is $\{\} \vDash \exists x \in \mathbb{Z}. x \neq 0 \wedge x \geq x^2$?
   Yes. We can use $x = 1$ as the witness (that's in fact the only one that works).
4. Is $\exists x \in \mathbb{Z}. x \neq 0 \wedge x \geq x^2$ a tautology?
   Yes. Again, we didn't use the state.
5. Is $\{y = 3\} \vDash \exists x. x^2 \leq y$?
   Yes, we can use $x = 0$ as the witness.
6. Is $\exists x. x^2 \leq y$ a tautology?
   No. If $\sigma(y) = -1$, then $\sigma \nvDash \exists x. x^2 \leq y$ because there's no $\alpha \in \mathbb{Z}$ such that $\sigma[x \mapsto \alpha] \vDash x^2 \leq y$.

- If our proposition is $x > 0 \to \exists y. y^2 < x$, then a proper state needs to have a value for x because x is free.
- How do we determine whether $\sigma \vDash x > 0 \to \exists y. y^2 < x$?
- If $\sigma(x) \leq 0$ then, the conditional is true because $F \to p$ is always true. So we just need to consider states where $\sigma(x) > 0$.
- So this is satisfied if for all σ such that $\sigma(x) > 0$, we have $\sigma[y \mapsto \alpha] \vDash y^2 < x$ for some $\alpha \in \mathbb{Z}$.
- Remember, we just need one such α. So we can pick $\alpha = 0$ and we're good.
- So $x > 0 \to \exists y. y^2 < x$ is a tautology because the it's true in all states.

Q: If p has no free variables or atomic propositions, can it be a contingency?
A: No. If it has no free variables, then the state doesn't matter and so the proposition is either true or false in all states.

- Consider $\sigma \vDash \forall x \in \mathbb{Z}. (x > y \to \exists z \in \mathbb{Z}. z \geq x + y^2)$.
- A well-formed proper state must have a value for y.

- $\forall x \in \mathbb{Z}. x > y \rightarrow \exists z \in \mathbb{Z}. z \geq x + y^2$ is a tautology if it's true for all y, a contingency if it's true for some y (and false for others) and a contradiction if it's not true for any y.
- So this is asking if for all $\alpha_1 \in \mathbb{Z}$ such that $\alpha_1 > \sigma(y)$, there exists some $\alpha_2 \in \mathbb{Z}$ such that $\sigma[x \mapsto \alpha_1][z \mapsto \alpha_2] \vDash z \geq x + y^2$.
- We're basically just peeling off quantifiers and converting them to words.
- (This is true/a tautology because no matter what α_1 and $\sigma(y)$ are, we can always pick a big enough α_2).