ADVANCED INFORMATION, COMPUTATION, COMMUNICATION I

L06 – 20191004

ARJEN K. LENSTRA, I&C

If you find a typo in these lecture notes (or earlier ones), no matter how small, or if there is something that you do not understand, please send me an email message (at akl@epfl.ch).

Assuming familiarity with the regular and subdomain negation rules for quantifiers as proved last time, namely

$$\neg\forall x\ P(x) \equiv \exists x\ \neg P(x), \qquad \neg\exists x\ P(x) \equiv \forall x\ \neg P(x)$$

and

$$\neg\forall x \in S\ P(x) \equiv \exists x \in S\ \neg P(x), \qquad \neg\exists x \in S\ P(x) \equiv \forall x \in S\ \neg P(x),$$

(where $S \subseteq D$ and where D, as usual, denotes the domain of the propositional function P), we continued the discussion of logical statements and quantifiers. Remember that a statement or a negation of a statement concerning elements of a (sub)domain in general never expresses anything about elements not contained in that (sub)domain: for instance, from "$\forall x \in S\ P(x)$" it does not follow that for x not belonging to S the statement $P(x)$ is false.

The scope of quantification variables (used but barely mentioned in class). The variable used in a quantifier (the x in quantified statements such as $\forall x\ P(x)$ or $\exists x\ Q(x)$) exists only within the quantified statement where it is used: before or after the statement that variable x (as used in the quantified statement) does not exist: there it is called *free*. The *scope* of a variable is just a term used for the range, or places, where the variable has a meaning. For instance, in $\forall y\,[\forall x \in S\ P(x)] \wedge Q(y)$ the variable x that occurs between [and] exists in that meaning only between those same [and], so the part between [and] is the scope of the variable x and that same x cannot occur in any way in $Q(y)$ because that would be out of the scope of that x.

It is common to write things like $\big(\forall x\ P(x)\big) \wedge \big(\exists x\ Q(x)\big)$ where the variable x in the first (P) part has "nothing to do" with the variable x in the second (Q) part, because the scopes of the two variables do not overlap so that the same name can be used for them; it depends on the circumstances if it is confusing or not: though it is possibly true (depending on the domain), some do not find it elegant to write $\big(\exists x\ x + 1 = 0\big) \wedge \big(\exists x\ x - 1 = 0\big)$ because the two parts result in different values for x – each of which does not exist outside its scope and has nothing to do with the other. It would be downright ugly to write things like $\forall x\big((\forall x \in S\ P(x)) \wedge Q(x)\big)$, even though the inner x that ranges over $S \subseteq D$ can be argued to have nothing to do with the outer x that ranges over the entire domain D. Like in programming, there are no general rules to select variable names: use common sense and avoid misunderstandings. The same remark applies to the use of parentheses (do not overdo it, but better too many than not enough) and to the use of summation variables (as we will see later).

Unique existential quantification. To be able to derive a negation rule for the unique existential quantifier $\exists!$ we first have to express $\exists!$ in terms of the regular universal and existential quantifiers $\forall$ and $\exists$ (because for those two we know how negation works). After a few interesting suggestions we converged to

$$\exists x \, \big(\, P(x) \wedge \forall y \ (P(y) \to y = x) \, \big).^{1}$$

First of all, we need an x for which $P(x)$ is true. So put that first ("$\exists x \ P(x)$"), and call it x. Then start worrying about what other elements may do, if they exist: any y for which $P(y)$ is true must be equal to x, which is expressed by the second part (to the right of the "$\wedge$"). It is not always easy to find the right expression and it may be even harder to figure out why a proposed solution is correct or not. As usual it helps to follow different lines of reasoning that lead to the same solution. Practice helps. It also helps to check that it works for exceptional cases (such as an empty domain, or a domain containing just a single element).

The proposed solution is logically equivalent (using the contrapositive of $P(y) \to y = x$) to

$$\exists! x \ P(x) \equiv \exists x \, \big(\, P(x) \wedge \forall y \ y \neq x \to \neg P(y) \, \big)$$

and also to the nicely concise formulation (using our carefully derived universal subdomain quantification)

$$\exists x \ P(x) \wedge \forall y \neq x \ \neg P(y).$$

Negation of unique existential quantification. Negation of the second alternative above immediately leads to (using standard manipulations)

$$\neg \exists! x \ P(x) \equiv \forall x \ \big((\neg P(x)) \vee \exists y \ y \neq x \wedge P(y) \big)$$

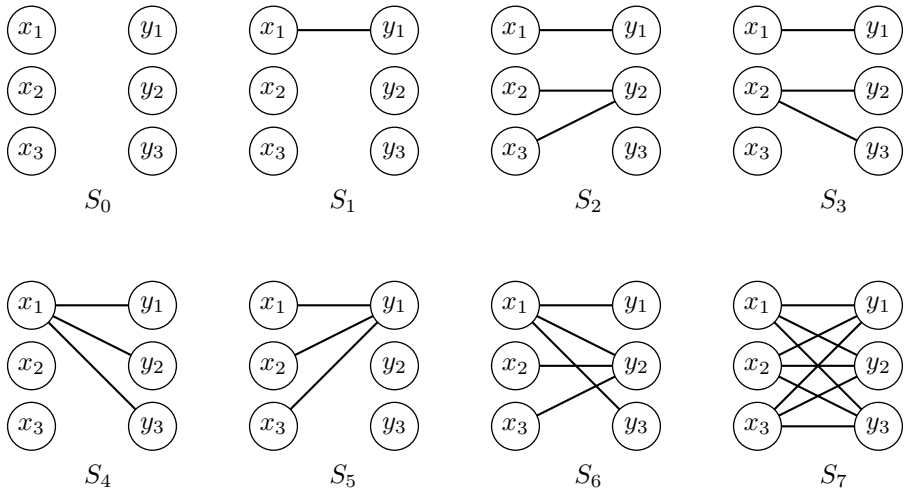
which is logically equivalent to the concise formulation (which can also be derived directly from the third formulation above)

$$\forall x \ \big(P(x) \to \exists y \neq x \ P(y) \big).$$

We had a closer look at the first formulation to make sure that it makes sense as the negation of a unique existence: if there is not a unique element with a certain property, then there is either no element at all with the property, or there are at least two distinct elements with the property. If $P(x)$ is false for all x, then $(\neg P(x)) \vee \exists y \ y \neq x \wedge P(y)$ is true for all x because $\neg P(x)$ is true for all x, so that is all right. Now assume that there is an x, say $\bar{x}$, for which $P(\bar{x})$ is true and thus $\neg P(\bar{x})$ is false, then to make $(\neg P(\bar{x})) \vee \exists y \ y \neq \bar{x} \wedge P(y)$ true (which it must be, because $(\neg P(x)) \vee \exists y \ y \neq x \wedge P(y)$ is true for all x), the $\big(\exists y \ y \neq \bar{x} \wedge P(y)\big)$-part must be true, implying that indeed there must be some y different from $\bar{x}$, for which $P(y)$ is true as well.

[1] Without parentheses, thus "$\exists x \ P(x) \wedge \forall y \ (P(y) \to y = x)$", it may not be clear what is meant: the correct "$\exists x \, \big(\, P(x) \wedge \forall y \ (P(y) \to y = x) \, \big)$" or the incorrect (because implying a scope-error) "$\big(\exists x \ P(x)\big) \wedge \big(\forall y \ (P(y) \to y = x) \, \big)$"; usage of parentheses may not be strictly required but is advisable to avoid incorrect interpretation.

Nesting order. To show the effect of different nesting orders of different quantifiers, let X be a set $\{x_1, x_2, x_3\}$ of three vertices, let Y be another set $\{y_1, y_2, y_3\}$ of three vertices, and let $S_i(x, y)$ for $0 \leq i < 8$ be the eight distinct propositional functions from $X \times Y$ to $\{0, 1\}$ where $S_i(x, y)$ is true if and only if there is an edge between x and y as pictured:



S	$\exists x \exists y\, S(x,y)$	$\exists x \forall y\, S(x,y)$		$\forall y \exists x\, S(x,y)$	$\exists y \forall x\, S(x,y)$		$\forall x \exists y\, S(x,y)$	$\forall x \forall y\, S(x,y)$
S_0	false	false		false	false		false	false
S_1	true	false		false	false		false	false
S_2	true	false		false	false	$\not\leftarrow$	true	false
S_3	true	false	$\not\leftarrow$	true	false		false	false
S_4	true	true	$\rightarrow$	true	false		false	false
S_5	true	false		false	true	$\rightarrow$	true	false
S_6	true	true	$\rightarrow$	true	true	$\rightarrow$	true	false
S_7	true	true	$\rightarrow$	true	true	$\rightarrow$	true	true

The table lists which of $\exists x \exists y\, S_i(x, y)$, $\exists x \forall y\, S_i(x, y)$, $\forall y \exists x\, S_i(x, y)$, $\exists y \forall x\, S_i(x, y)$, $\forall x \exists y\, S_i(x, y)$ and $\forall x \forall y\, S_i(x, y)$ hold for S_i for $0 \leq i < 8$. Note that for any propositional function $S(x, y)$ (and not just for the S_i's considered here) it is the case that the statement

$$\exists x \forall y \;\; S(x, y) \;\; \rightarrow \;\; \forall y \exists x \;\; S(x, y)$$

is a tautology and, equivalently, that the statement

$$\exists y \forall x \;\; S(x, y) \;\; \rightarrow \;\; \forall x \exists y \;\; S(x, y)$$

is a tautology. These are the two $\rightarrow$'s in the table. The converse of those two implications are not tautologies, as proved by the two $\not\leftarrow$'s in the table.

For the rest, note that the final column implies all others (i.e., $\forall x \forall y\, S(x, y)$ implies all five combinations of universal and existential quantifiers listed, including the non-listed ones $\forall y \forall x\, S(x, y)$ and $\exists y \exists x\, S(x, y)$) and there are no other implications among any other two columns.

It follows that, in general, the nesting order of distinct quantifiers matters and that switching distinct quantifiers around will change the meaning of the expression. Switching around directly consecutive identical quantifiers, however, does not change the meaning: "$\forall x \forall y \ldots$" is equivalent to "$\forall y \forall x \ldots$" (assuming the "$\ldots$"-parts are the same) and may be written as "$\forall x, y \ldots$". Similarly, "$\exists x \exists y \ldots$" is equivalent to "$\exists y \exists x \ldots$" (again assuming the "$\ldots$"-parts are the same) and may be written as "$\exists x, y \ldots$".

Rules of inference for quantifiers. See Table 2 in Section 1.6 of the book for these rules. Note that it is assumed that the domain is not empty.

Universal instantiation: from $\forall x\ P(x)$, it follows that $P(c)$ is true for arbitrary c in the domain: thus, a c may be chosen that already has a meaning in the context before the universal instantiation was applied. This is written in the following manner (with "$\therefore$" pronounced as "therefore"):

$$\frac{\forall x\ P(x)}{\therefore\ P(c)}$$

Universal generalization: if $P(c)$ is true for arbitrary c in the domain, it follows that $\forall x\ P(x)$:

$$\frac{P(c) \text{ for arbitrary } c}{\therefore\ \forall x\ P(x)}$$

Existential instantiation: from $\exists x\ P(x)$, it follows that $P(c)$ is true for some c in the domain — but this is a c that is at this point newly introduced in the context, and that, in general, cannot be chosen as an element that already has a meaning in the context before the existential instantiation was applied:

$$\frac{\exists x\ P(x)}{\therefore\ P(c) \text{ for some element } c}$$

Existential generalization: if $P(c)$ is true for some particular c in the domain, it follows that $\exists x\ P(x)$:

$$\frac{P(c) \text{ for some element } c}{\therefore\ \exists x\ P(x)}$$

Rules of inference application example. Suppose that the following two statements are known to be true:

(1) There is someone here who likes C,
(2) Everyone who likes C is a fan of Dennis Ritchie,

where the domain is the set of people. For most it will not be hard to conclude that there is someone here who is a fan of Dennis Ritchie. But how do we "formally" derive this conclusion? That is what rules of inference are about. This application of rules of inference may not be truly convincing, but the same methodology can also be applied in circumstances where it may not be so simple for humans to derive the correct conclusion. Furthermore, rules of inference have the advantage that the line of reasoning can be "mechanically" verified.

In order to apply the rules of inference, we first need to define a few propositional functions:

- $H(x)$: "x is here" (where "here" may be interpreted as "in this class");
- $U(x)$: "x likes C";
- $L(x)$: "x is a fan of Dennis Ritchie".

Our initial true statements can now be translated:

fact1: $\exists x\ (H(x) \wedge U(x))$.
fact2: $\forall x\ (U(x) \rightarrow L(x))$.

Note the usage of "$\wedge$" in **fact1** and of "$\rightarrow$" in **fact2** and convince yourself that these are the right logical operators in this context: "$\exists x\ (H(x) \rightarrow U(x))$" would also be true if the domain is empty: in that case there is no one, and in particular there is no one in this class, so it would not properly express that "there is someone here who likes C". Possibly more convincingly, if there even exists a single person

not in this class (i.e., for whom $H(x)$ is false), the statement "$\exists x\ (H(x) \to U(x))$" would be true. The statement $\forall x\ (U(x) \wedge L(x))$ would express that everyone likes C (strangely, this is not the case) and that everyone is a fan of Dennis Ritchie, which is (both intuitively and formally) not equivalent to our "everyone who likes C is a fan of Dennis Ritchie".

We are going to use quantified statements **fact1** and **fact2** along with the rules of inference, as defined in the book in section 1.6, to derive our conclusion "there is someone here who is a fan of Dennis Ritchie". Using the propositional functions, our desired conclusion "there is someone here who is a fan of Dennis Ritchie" can be translated into the quantified statement

conclusion: $\exists x\ (H(x) \wedge L(x))$

This may sound like a silly and useless exercise, but it will be seen that it can be done entirely by using the rules in the book, without having to think about, or get distracted by, C or Dennis Ritchie (distraction due to interpretation of the meaning or intended meaning of statements is one of many reasons why proofs may derail).

(1) From "$\exists x\ (H(x) \wedge U(x))$" in **fact1** we find that $H(c) \wedge U(c)$ is true for some c; here we use existential instantiation of the existential quantification "$\exists x\ (H(x) \wedge U(x))$": we know an x exists, so we take one and call it c. Note that c is "just" some person c that we did not know anything about before c was selected, and that all we know about c is that $H(c) \wedge U(c)$ is true.

(2) From the fact that $H(c) \wedge U(c)$ is true in (1) it follows that $U(c)$ is true; this is called "simplification".

(3) From the fact that $H(c) \wedge U(c)$ is true in (1) it also follows that $H(c)$ is true; "simplification" again.

(4) From "$\forall x\ (U(x) \to L(x))$" in **fact2** we find that $U(c) \to L(c)$ is true; we use universal instantiation of the universal quantification "$\forall x\ (U(x) \to L(x))$": we know it is true for all x, so in particular it is true for the c that we have (carefully) selected already.

> **Remark.** At this point it is important that the c that is selected (in the universal instantiation) has the desirable properties that were derived in steps (2) and (3). Doing this universal instantiation before the existential instantiation in step (1) would have derailed the proof: if we would first universally instantiate "$\forall x\ (U(x) \to L(x))$" and thus get some arbitrary z for which $U(z) \to L(z)$ is true, then we cannot later existentially instantiate "$\exists x\ (H(x) \wedge U(x))$" with that z: sure, an x exists, but why would it be equal to that particular z?

(5) Based on the fact that $U(c)$ is true from (2) and that $U(c) \to L(c)$ is true from (4) we use "modus ponens" to conclude that $L(c)$ is true.

(6) Based on the fact that $H(c)$ is true from (3) and that $L(c)$ is true from (5) we use "conjunction" to conclude that $H(c) \wedge L(c)$ is true.

(7) Finally, using that $H(c) \wedge L(c)$ is true from (6) we use existential generalization to reach the desired conclusion $\exists x\ (H(x) \wedge L(x))$.

Next class. Next time we will move to elementary proofs. Reread the final parts of Chapter 1 (until what was indicated before). Reading up on sets and power sets may be helpful too.