The exclusive "or"

One more logical connective, of great importance in computer science, is XOR, denoted by $\veebar$ in Grimaldi's book:

p	q	$p \veebar q$
0	0	0
0	1	1
1	0	1
1	1	0

Thus $p \veebar q$ says that either p or q is true, but not both:

$$p \veebar q \iff (p \vee q) \wedge \neg(p \wedge q). \tag{25}$$

Two interesting observations about XOR are:

- XOR is the *negation* of IFF (compare their truth tables!):

$$p \veebar q \iff \neg(p \longleftrightarrow q). \tag{26}$$

- XOR is the *dual* of IFF, as we'll see next.

The duality principle

Summarizing from Grimaldi p. 60: Any logic law (stating the tautological equivalence of two statements) that involves only $\vee$ and $\wedge$ (and possibly T_0 and F_0) has a partner in which $\vee$ and $\wedge$ are interchanged (and T_0 and F_0 are interchanged). For example, $p \vee \neg p \iff T_0$ is dual to $p \wedge \neg p \iff F_0$.

In dualizing a statement, note carefully:

- If a statement s contains $\rightarrow$, $\longleftrightarrow$, or $\veebar$, those connectives can be reexpressed in terms of $\vee$ and $\wedge$, and then its dual s^{d} is defined by the prescription above.
- p is not interchanged with $\neg p$ (even though T_0 is interchanged with F_0).
- The $\iff$ in the logical law is not replaced by $\veebar$ (although $\veebar$ is the dual of $\longleftrightarrow$). The reason for this is that $s_1 \iff s_2$ is equivalent to $(s_1 \longleftrightarrow s_2) \iff T_0$, and the dual of the latter is ${s_1}^{\mathrm{d}} \veebar {s_2}^{\mathrm{d}} \iff F_0$, not ${s_1}^{\mathrm{d}} \veebar {s_2}^{\mathrm{d}} \iff T_0$.

A **sketch of the proof of the duality principle** can be extracted from Sec. 15.4 of Grimaldi: All the logic laws follow from a list of 8 laws, which is (collectively) symmetric under the interchange of $\wedge$ with $\vee$ and T_0 with F_0 . (A certain amount of notational translation is necessary to relate Sec. 15.4 to Chapter 2.)

Now let's see why XOR is dual to IFF. The first step is to get rid of all connectives except $\vee$ and $\wedge$: $p \longleftrightarrow q$ is equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$, which in turn should be rewritten as

$$(\neg p \vee q) \wedge (\neg q \vee p). \tag{27}$$

The dual of this statement is

$$(\neg p \wedge q) \vee (\neg q \wedge p). \tag{28}$$

Common sense indicates that (28) means the same thing as $p \veebar q$. The equivalence can be formally demonstrated by applying the distributive law and some other logic laws (in particular, "Inverse" and "Identity" from Grimaldi p. 59):

$$\begin{aligned}
(28) \iff & [\neg p \vee (\neg q \wedge p)] \wedge [q \vee (\neg q \wedge p)] \\
\iff & (\neg p \vee \neg q) \wedge (\neg p \vee p) \wedge (q \vee \neg q) \wedge (q \vee p) \\
\iff & (\neg p \vee \neg q) \wedge T_0 \wedge T_0 \wedge (p \vee q) \\
\iff & (p \vee q) \wedge (\neg p \vee \neg q) \\
\iff & (p \vee q) \wedge \neg(p \wedge q),
\end{aligned}$$

and this is $p \veebar q$, according to (25). The dual of (25) is (after simplification by a De Morgan law)

$$p \longleftrightarrow q \iff (p \wedge q) \vee (\neg p \wedge \neg q), \tag{29}$$

which, not surprisingly, is equivalent to (27) via an argument like the one we just went through, using the other two inverse and identity laws.

The duality principle extends to formulas containing quantifiers; $\forall$ gets interchanged with $\exists$. This principle can be seen at work in Table 2.22, p. 98 of Grimaldi.

The substitution rules

More useful than duality in everyday reasoning are the two *substitution rules* stated on Grimaldi p. 61 and paraphrased here:

1. In a *tautology*, if we replace *every* occurrence of a *primitive* statement p by a certain statement s (not necessarily primitive), then the result is still a tautology.

2. Suppose that $s_1 \iff s_2$. In any *compound statement* (not necessarily a tautology) involving s_1 (which is not necessarily primitive) as a component, if we replace *one or more* (not necessarily all) occurrences of s_1 by s_2, we do not change the truth value of the statement.

Grimaldi offers no proof of these rules; they are taken to be self-evident principles of reasoning. They may become more self-evident if we contemplate some analogous principles for reasoning with algebraic expressions:

1. In an *identity*, such as

   $$x^2 - y^2 = (x+y)(x-y),$$

   if we replace *every* occurrence of a *variable* by a certain number or expression, the result is a valid identity. The substituted expression may depend on other variables in the formula. In the example, if we replace x by y^3, we get

   $$y^6 - y^2 = (y^3+y)(y^3-y),$$

which is always true. (However, if we made the replacement in the left side only, we would get

$$y^6 - y^2 = (y^3 + y)(x - y),$$

which is not a valid identity.)

2. In any *formula or expression*, such as $y = (7!)^x + 7!$, if we replace *one or more* occurrences of something by something else *known to be equal* to it, then the value of the expression does not change. Example: $y = 5040^x + 7!$.

Deduction: General comments

In this course our treatment of the rules of deduction (Grimaldi Secs. 2.3 and 2.5) will of necessity be more superficial than our treatment of the conceptual/symbolic/linguistic aspects of logic.

Let's start by asking ourselves why we should be interested in formal deductions at all. The importance of logical formalism depends on context to some extent.

Why do mathematicians care about proofs? There are two different reasons:

1. To be sure that the theorems are true.
2. To understand how the theorems fit into a logical framework. Does a certain theorem follow from the axioms? Would it also follow from different axioms? For example, the proof of the identity

   $$(A + B)^2 = A^2 + 2AB + B^2$$

   uses the commutative law for multiplication. Therefore, it will not hold for objects such as matrices whose multiplication is noncommutative.

The second context requires closer attention to the logical details of the proof; in a sense, it is the proof itself that is the object of study, not just the mathematical objects that the theorems describe.

More to the point for most students in this course: Why do computer professionals care about logical deductions? Remarks parallel to the foregoing ones can be made.

1. To recognize whether arguments are valid (and to be able to construct valid arguments).
2. To design circuits, switch arrays, or computer programs that *implement* logic.

Again, the second context requires closer attention to formal details. In it we are not satisfied with a pragmatic assurance that a conclusion is correct; we need to analyze the device to guarantee that it will perform correctly for all possible inputs in all situations.

Unfortunately, because of the very fundamental nature of logic, detailed discussions of it sometimes appear to belabor the obvious. Then one suddenly discovers that something subtle and important is hidden inside. In the time available this semester, you will be doing well to find time to study Grimaldi's Chapter 2 thoroughly. But if you find this subject either confusing or intriguing, you will be well advised to go back later and read an elementary book entirely devoted to logic, such as

- W. V. Quine, *Methods of Logic*, revised edition, Holt Rinehart and Winston, 1964.
- C. Allen and M. Hand, *Logic Primer.* 2nd edition, MIT Press, 2001.

Rules of deduction (inference)

Grimaldi p. 79 gives a page-long table of rules of inference that may seem to be named by the Principle of Obfuscatory Polysyllabification. For us it is not necessary to memorize this table. It's more important to hit the high points:

Modus Ponens ("putting" or "pushing")**:** If we know $p \rightarrow q$ and p, then we can conclude q. This, of course, follows from the basic meaning of " → ".

Syllogism: If $p \rightarrow q$ and $q \rightarrow r$, then $p \rightarrow r$. (If we also know p, then we can now conclude r. This conclusion could also be reached by two steps of modus ponens. Thus there is some freedom of choice in constructing a multistep deduction.) Reasoning by syllogism is a special case of the following:

Conditionalization: If q can be proved from the *hypothesis* (assumption) p, then $p \rightarrow q$ is a theorem. (Grimaldi does not state this principle explicitly, but it frequently appears in the examples and exercises, often as an application of "syllogism" or "disjunctive syllogism". He usually avoids it by writing, e.g.,

$$\begin{array}{r} p \\ \underline{q} \\ \therefore r \end{array}$$

instead of $p \wedge q \rightarrow r$ as the conclusion of a deduction. See also the discussion of "stars" below.)

Modus Tollens ("taking" or "pulling back") **and Proof by Contradiction:** If we know $p \rightarrow q$ and $\neg q$, then we can conclude $\neg p$. A special case of this pulling back on an implication is the case where q is a logical contradiction (F_0) rather than merely factually false. (Grimaldi says that modus tollens and contradiction are essentially different; I disagree.)

Proof by Cases: If $p \rightarrow r$ and $q \rightarrow r$, then $(p \vee q) \rightarrow r$. So, if we can prove that *either* p or q is true (depending upon circumstances), then we can conclude r. (Example: Let r be "$n(n-1)$ is even", p be "n is even" and q be "n is odd". The conclusion (r) is correct in both cases, but for different reasons, so two separate proofs are needed, and the principle of proof by cases combines them at the end.)

The other rules, when needed, can be reconstructed by common sense from the meaning of the logical connectives.

Generalization and specification; Flags and stars

In Sec. 2.5 Grimaldi states some rules for reasoning with universal quantifiers, which we'll paraphrase tersely here.

Rule of Universal Specification: $\forall x\, p(x) \ \Rightarrow\ p(c)$ (for an arbitrary c in the universe of discourse). This, of course, is the very meaning of the universal quantifier.

Rule of Universal Generalization: If $p(c)$ can be proved for an *arbitrary* c belonging to the universe, then $\forall x\, p(x)$ is true.

On p. 122, in Exercise 10, the author states the corresponding rules for existential quantifiers:

Rule of Existential Specification: If $\exists x\, p(x)$ is true, then $p(c)$ is true for some c. (This is merely a matter of giving a name to the object whose existence is asserted, for convenience in the argument to follow.)

Rule of Existential Generalization: $p(c) \ \Rightarrow\ \exists x\, p(x)$. Again, this appears to follow from the meaning of the existential quantifier.

Here is a correct example of these four rules at work:

Theorem: $\exists y\, \forall x\, p(x,y) \ \rightarrow\ \forall x\, \exists y\, p(x,y)$

Proof:

(1) $\exists y\, \forall x\, p(x,y)$ (hypothesis)

(2) Let c be such a y: $\forall x\, p(x,c)$ (existential specification)

(3) Let d be arbitrary: $p(d,c)$ (universal specification)

(4) $\exists y\, p(d,y)$ (existential generalization)

(5) Since d was arbitrary, $\forall x\, \exists y\, p(x,y)$ (universal generalization)

(6) Therefore, $\exists y\, \forall x\, p(x,y) \ \rightarrow\ \forall x\, \exists y\, p(x,y)$ (because we've shown that (1) implies (5) (conditionalization))

But, then, what is wrong with this?

Bad Theorem: $\forall x\, \exists y\, p(x,y) \ \rightarrow\ \exists y\, \forall x\, p(x,y)$

Bad Proof:

(1) $\forall x\, \exists y\, p(x,y)$ (hypothesis)

(2) Let d be arbitrary: $\exists y\, p(d,y)$ (universal specification)

(3) Let c be such a y: $p(d,c)$ (existential specification)

(4) $\forall x\, p(x,c)$ (universal generalization) **(ERROR)**

(5) $\exists y\, \forall x\, p(x,y)$ (existential generalization)

(6) Therefore, $\forall x\, \exists y\, p(x,y) \ \rightarrow\ \exists y\, \forall x\, p(x,y)$ (conditionalization)

It is easy to see that this "theorem" is false. Let $p(x, y)$ be $x < y$. Then the hypothesis is true, because, given x, y could be $x + 1$. However, the conclusion is false, because, whatever y is, one can find an x that is larger, say $x = y+1$. Close examination of the bad argument, employing a bit of common sense about the reasons for the alleged correctness of each step, reveals that the fallacy occurs at step (4). That step would be valid if (3), with a *fixed* c, had been proved for an arbitrary d; but in fact the c in (3) depends on d, and there is no reason to believe that there is a single c that works for all x.

The dangerous laws are existential specification (because the free variable, or "constant", thereby introduced does not represent an arbitrary object) and universal generalization (because one must be sure that the free variable thereby eliminated is truly arbitrary). Their special status is reflected in the fact that we needed to state them by English sentences, not totally symbolic " $\Rightarrow$ " statements like the other two laws. In the book cited above, Quine states rules for using these laws correctly:

- Whenever existential specification or universal generalization is employed, the free variable in the unquantified line must occupy precisely the same places as the quantified variable in the quantified line. (For example, from $\exists y\, q(x, y)$ it is *not valid* to conclude $q(x, x)$. In contrast, there is nothing wrong with going from $\forall y\, q(x, y)$ to $q(x, x)$, or from there to $\exists y\, q(y, x)$.) This restriction is similar to the one in the "first substitution rule", previously discussed.

- At each step of existential specification or universal generalization, the new line in the deduction should be "flagged" by writing the pertinent free variable in the margin in brackets. (In the case of universal generalization, this free variable appears in the *previous* line, not the flagged line.)

- No variable may be flagged more than once in a deduction.

- A flagged variable must be alphabetically later than any [other] free variable in the line it flags.

Observing these restrictions prevents the ambiguous use of free variables that can yield false conclusions.

Quine uses another very helpful convention: Whenever a new hypothesis is introduced, a column of asterisks is begun in the proof, as a reminder that the starred lines *depend on the truth of that hypothesis*. The column of stars ends when one draws a conclusion (by use of the syllogism law, for instance) that no longer requires the hypothesis to be assumed. (This is called "discharging" the hypothesis.) This convention (similar to the indentations in modern computer programs) makes the structure of deductions clearer and prevents the error of forgetting an undischarged hypothesis.

Here is the correct proof from above, with all its flags and stars attached:

Properly Decorated Proof:

*(1) $\exists y\, \forall x\, p(x, y)$

*(2) Let c be such a y: $\forall x\, p(x, c)$ $[c]$

*(3) Let d be arbitrary: $p(d, c)$

*(4) $\exists y\, p(d,y)$

*(5) Since d was arbitrary, $\forall x\, \exists y\, p(x,y)$ $[d]$

(6) Therefore, $\exists y\, \forall x\, p(x,y) \;\rightarrow\; \forall x\, \exists y\, p(x,y)$

Convince yourself that there is no way to attach flags to lines (3) and (4) of the bad proof consistently with the rules. (Interchanging "c" and "d" won't help.)

The absorption and domination laws

Among the laws of logic listed on p. 59 of Grimaldi, probably the least obvious are the two absorption laws,

$$p \vee (p \wedge q) \iff p, \qquad p \wedge (p \vee q) \iff p.$$

That $p \vee (p \wedge q) \iff p \wedge (p \vee q)$ is an immediate consequence of the distributive and idempotent laws, but that both are equivalent to p requires a more complicated argument, which is left as an exercise for the reader in the proof of Theorem 15.3. (It could also be established by a truth table, of course, but the algebraic proof is more general, applying, for instance, to the set-theoretic absorption laws on p. 143.) The proof of the first absorption law runs

$$\begin{aligned} p \vee (p \wedge q) &\iff (p \wedge T_0) \vee (p \wedge q) \qquad \text{(identity)} \\ &\iff p \wedge (T_0 \vee q) \qquad \text{(distributive)} \\ &\iff p \wedge T_0 \qquad \text{(domination)} \\ &\iff p \qquad \text{(identity).} \end{aligned}$$

The other absorption law follows immediately (either by the foregoing remark that the two long expressions are equivalent, or by duality, or by a parallel (dual) argument to the one just given).

This proof obligates us to prove the domination law without using the absorption law. Here is one way:

$$\begin{aligned} p \vee T_0 &\iff (p \vee T_0) \wedge T_0 \qquad \text{(identity)} \\ &\iff (p \vee T_0) \wedge (p \vee \neg p) \qquad \text{(inverse)} \\ &\iff p \vee (T_0 \wedge \neg p) \qquad \text{(distributive)} \\ &\iff p \vee \neg p \qquad \text{(identity)} \\ &\iff T_0 \qquad \text{(inverse).} \end{aligned}$$

(Throughout this discussion we have used the commutative and substitution laws without comment.)

Logical vocabulary

Here are some terms to review. On a test, you will need a basic vocabulary both to understand the questions and to write something to explain or justify your answers.

universal quantifier
existential quantifier
counterexample
generalization
specification

conditional
biconditional
implication

contrapositive
converse
inverse

valid
tautology
contradiction
dual

distributive
De Morgan
idempotent

modus ponens
modus tollens
syllogism

More Exercises

1. Show in detail that the dual of (25) is (29).

2. Show in detail that (29) is equivalent to (27).

3. Show that the top two lines of Table 2.22 (p. 98 of Grimaldi) are dual to the bottom two.

4. Give counterexamples showing that $\Rightarrow$ cannot be strengthened to $\iff$ in the top and bottom lines of Table 2.22.

5. Choose one line of Table 2.22 and verify that it holds in a 3-element universe, using the equivalences
$$\begin{aligned} \forall x\, p(x) &\iff p(a) \wedge p(b) \wedge p(c), \\ \exists x\, p(x) &\iff p(a) \vee p(b) \vee p(c). \end{aligned}$$