EQUIVALENCES (can be used in either direction, and it is legal to make substitutions even in part of an expression)

E_1: $\sim\sim p \Leftrightarrow p$ (Epp uses $\equiv$ for $\Leftrightarrow$)

E_2: $p \wedge q \Leftrightarrow q \wedge p$

E_3: $p \vee q \Leftrightarrow q \vee p$

E_4: $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$

E_5: $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$

E_6: $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$

E_7: $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$

E_8: $\sim(p \wedge q) \Leftrightarrow \sim p \vee \sim q$

E_9: $\sim(p \vee q) \Leftrightarrow \sim p \wedge \sim q$

E_{10}: $p \vee p \Leftrightarrow p$

E_{11}: $p \wedge p \Leftrightarrow p$

E_{12}: $r \vee (p \wedge \sim p) \Leftrightarrow r$ $[r \vee \mathbf{c} \Leftrightarrow r]$

E_{13}: $r \wedge (p \vee \sim p) \Leftrightarrow r$ $[r \wedge \mathbf{t} \Leftrightarrow r]$

E_{14}: $r \vee (p \vee \sim p) \Leftrightarrow \mathbf{t}$ $[r \vee \mathbf{t} \Leftrightarrow \mathbf{t}]$

E_{15}: $r \wedge (p \wedge \sim p) \Leftrightarrow \mathbf{c}$ $[r \wedge \mathbf{c} \Leftrightarrow \mathbf{c}]$

E_{16}: $p \rightarrow q \Leftrightarrow \sim p \vee q$

E_{17}: $\sim(p \rightarrow q) \Leftrightarrow p \wedge \sim q$

E_{18}: $p \rightarrow q \Leftrightarrow \sim q \rightarrow \sim p$

E_{19}: $p \rightarrow (q \rightarrow r) \Leftrightarrow (p \wedge q) \rightarrow r$

E_{20}: $\sim(p \leftrightarrow q) \Leftrightarrow p \leftrightarrow \sim q$

E_{21}: $p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$

E_{22}: $p \leftrightarrow q \Leftrightarrow (p \wedge q) \vee (\sim p \wedge \sim q)$

RULES FOR FORMAL PROOFS

RULE P: Any premise (a given hypothesis) can be used as a line in your proof.

RULE T: The righthand side of an implication (I_1-I_{16}) can become a line in your proof as long as each of the hypotheses on the left have occurred earlier in your proof. Either side of an equivalence (E_1-E_{32}) can likewise be inferred from the other side; furthermore, it's legal to use an E-rule substitution on just part of an expression.

RULE CP: If your conclusion (or subgoal) is of the form $A \rightarrow B$, then you may assume A as an additional hypothesis, and your new goal is to merely prove B.

There are many ways to prove any theorem. Try Sample Proof #1 yourself (see the next column) but instead put H_3 on line 4, and look for yet another opportunity to use Rule I_{13} . Then try Sample Proof #2 without using CP (use E_{16}).

IMPLICATIONS (if ALL the hypotheses are known to be true, then the conclusion follows; but you CANNOT make substitutions for only a part of an earlier line)

I_1: $p \wedge q \Rightarrow p$

I_2: $p \wedge q \Rightarrow q$

I_3: $p \Rightarrow p \vee q$

I_4: $q \Rightarrow p \vee q$

I_5: $\sim p \Rightarrow p \rightarrow q$

I_6: $q \Rightarrow p \rightarrow q$

I_7: $\sim(p \rightarrow q) \Rightarrow p$

I_8: $\sim(p \rightarrow q) \Rightarrow \sim q$

I_9: $p\ ,\ q \Rightarrow p \wedge q$

I_{10}: $p \vee q\ ,\ \sim p \Rightarrow q$

I_{11}: $p\ ,\ p \rightarrow q \Rightarrow q$

I_{12}: $\sim q\ ,\ p \rightarrow q \Rightarrow \sim p$

I_{13}: $p \rightarrow q\ ,\ q \rightarrow r \Rightarrow p \rightarrow r$

I_{14}: $p \rightarrow r\ ,\ q \rightarrow r\ ,\ p \vee q \Rightarrow r$

SAMPLE Formal Proof #1:

Derive the conclusion $R \vee S$ from the following four premises:

H_1: $(C \vee D) \rightarrow \sim H$

H_2: $\sim H \rightarrow (A \wedge \sim B)$

H_3: $(A \wedge \sim B) \rightarrow (R \vee S)$

H_4: $C \vee D$

Proof:

1. $(C \vee D) \rightarrow \sim H$ P (premise, Rule P)
2. $\sim H \rightarrow (A \wedge \sim B)$ P
3. $(C \vee D) \rightarrow (A \wedge \sim B)$ I_{13} 1,2 (Rule T)
4. $(C \vee D)$ P
5. $A \wedge \sim B$ I_{11} 4,3
6. $(A \wedge \sim B) \rightarrow (R \vee S)$ P
7. $R \vee S$ I_{11} 5,6

SAMPLE Formal Proof #2 (Rule CP):

Derive the conclusion $R \rightarrow S$ from the premises H_1: $(\sim R \vee M)$ and H_2: $M \rightarrow S$

1. R Assumed Premise
2. $\sim R \vee M$ P
3. $\sim\sim R$ E_1 on 1
4. M I_{10} on 3,2
5. $M \rightarrow S$ P
6. S I_{11} on 4,5
7. $R \rightarrow S$ CP on 1,6

The CP "trick" works because showing
$(\sim R \vee M) \wedge (M \rightarrow S) \Rightarrow (R \rightarrow S)$
is logically equivalent to showing
$((\sim R \vee M) \wedge (M \rightarrow S) \wedge R) \Rightarrow S$

We will mostly practice working with symbols, but of course this is not very useful unless it can be applied to solve real-world problems ("word problems"). Here is an example:

SAMPLE #3 (word problem): If A works hard, then either B or C will have fun. If B has fun, then A will not work hard. If D has fun, then C will not.

From these three given facts, we can deduce that: If A works hard, then D will not have fun.

To turn this word problem into symbols (so we don't have big long sentences in every step), let us define:

a: A works hard
b: B has fun
c: C has fun
d: D has fun

Our hypotheses are then shortened to:

H_1: $a \to (b \vee c)$
H_2: $b \to \sim a$
H_3: $d \to \sim c$

Our conclusion (goal) is $a \to \sim d$.

Try to prove this formally; note that since the conclusion is an "if-then", this is an opportunity to use rule CP. Rule CP (when applicable) tends to make proofs easier, since you get an extra hypothesis to work with "for free".

An **indirect proof**, or proof by contradiction, also gives you an extra hypothesis, and is a method that can always be used (so if you get stuck doing a proof the "regular" way, you can always shift gears and finish it off as a proof by contradiction). The idea is to argue that if all the hypotheses are true, there is no way for the conclusion to fail to be true as well. That is, our "trick" will be to assume the negation of the conclusion as an additional hypothesis, and then show that this leads to a contradiction. Any contradiction you can find will do; that is, anything of the form $m \wedge \sim m$ completes the proof. For example, $(h \to n) \wedge \sim (h \to n)$ would work.

SAMPLE #4 (proof by contradiction): Show that the conclusion $\sim(p \wedge q)$ follows from the hypothesis $\sim q \wedge \sim p$. We have one hypothesis to work with, but we can gain another one by using an indirect proof. Note that the premise on line 1 is the negation of the conclusion.

1. $\sim\sim(p \wedge q)$	P (Assumed Premise)
2. $\sim q \wedge \sim p$	P
3. $(p \wedge q)$	E_1 on 1
4. p	I_1 on 3
5. $\sim p$	I_2 on 2
6. $p \wedge \sim p$	I_9 on 4 and 5

We have our contradiction, and this completes the proof. Note that as soon as we wrote down the new assumed premise, our goal *changed*; we are no longer trying to get the conclusion on a line by itself, we are instead seeking a (any!) contradiction.

You can cook up instances where the set of hypotheses themselves lead to a contradiction, irrespective of what the conclusion of the theorem is. Such a set of premises are said to be **inconsistent**; in every universe, no matter what truth values you assign to the variables, there is no way for all the premises to be true at the same time. Theorems with inconsistent hypotheses are uninteresting, because those theorems will never apply to any situation in any universe, ever.

SAMPLE #5 (inconsistent hypotheses).

H_1: If Jack misses many classes, he fails.
H_2: If Jack fails, then he is uneducated.
H_3: If Jack reads a lot of books, then he is not uneducated.
H_4: Jack misses many classes, and reads a lot of books.

We can use the following definitions to shorten these statements:

m: Jack misses many classes
f: Jack fails.
r: Jack reads a lot of books.
u: Jack is uneducated.

The hypotheses then become:

H_1: $m \to f$ H_2: $f \to u$
H_3: $r \to \sim u$ H_4: $m \wedge r$

Try deriving a contradiction from these.

EXERCISES jc-A

1. Formally prove that the conclusion (on the right) follows from the list of [comma-separated] hypotheses (to the left of "$\Rightarrow$").

(a) $\sim(a\wedge \sim b),\ \sim b\vee d,\ \sim d \Rightarrow \sim a$

(b) $\sim j \rightarrow (m\vee n),\ h\rightarrow \sim j,\ h \Rightarrow m\vee n$

(c) $g\rightarrow h, h \rightarrow\sim i, i, g\vee (j\wedge s) \Rightarrow (s\wedge j)$

(d) $p\rightarrow q, (\sim q\vee r)\wedge\sim r, \sim(\sim p\wedge s) \Rightarrow \sim s$

(e) $(k\wedge m)\rightarrow n, \sim n\vee s, \sim s \Rightarrow \sim k \vee \sim m$

(f) $(a\rightarrow b)\wedge(a\rightarrow e), \sim(b\wedge e), d\vee a \Rightarrow d$

(g) $b\wedge c,\ (b\leftrightarrow c)\rightarrow(h\vee g) \Rightarrow (g\vee h)$

(h) $(p\rightarrow q)\rightarrow r,\ p\wedge n,\ q\wedge \mathbf{t} \Rightarrow r$

2. Derive the following, using Rule CP.

(a) $\sim a\vee b,\ \sim b\vee d,\ d\rightarrow e \Rightarrow a\rightarrow e$

(b) $j,\ j\rightarrow(k\rightarrow(m\wedge n)) \Rightarrow k\rightarrow n$

(c) $g\rightarrow h \Rightarrow g\rightarrow(g\wedge h)$

(d) $(u\vee v)\rightarrow w \Rightarrow (u\wedge v)\rightarrow w$

(e) $p\rightarrow(q\rightarrow r), q\rightarrow(r\rightarrow s) \Rightarrow p\rightarrow(q\rightarrow s)$

For (e), a subgoal will be $(q\rightarrow s)$, which means you can use CP a second time, and get yet another "extra" premise (q).

3. Show that the following sets of premises are inconsistent.

(a) $p\rightarrow q,\ p\rightarrow r,\ q\rightarrow \sim r,\ p$

(b) $a\rightarrow(b\rightarrow c),\ d\rightarrow(b\wedge\sim c),\ a\wedge d$

Hence, prove that

$p\rightarrow q,\ p\rightarrow r,\ q\rightarrow \sim r,\ p \Rightarrow m$, and that

$a\rightarrow(b\rightarrow c),\ d\rightarrow(b\wedge\sim c),\ a\wedge d \Rightarrow h\vee g$

4. Prove via the indirect method.

(a) $r\rightarrow\sim q,\ r\vee s,\ s\rightarrow\sim q,\ p\rightarrow q \Rightarrow \sim p$

(b)j,$\sim(a\rightarrow i)\rightarrow\sim(j\vee e), (i\rightarrow a)\vee\sim j \Rightarrow a\leftrightarrow i$

(c) $s\rightarrow\sim q,\ \sim r\leftrightarrow q,\ s\vee r,\ \sim r\Rightarrow p$

For (c), p not being mentioned in the hypotheses is a clue that the premises themselves are inconsistent.

Predicate Calculus Rules

RULE US (Universal Specification):

$(\forall y)P(y) \ \Rightarrow P(k)$

That is, if you know every object in the universe has property P, then it is OK to say that some particular object has property P. With US (unlike the ES rule below), you can choose *any* letter you like, even letters that "have been used before".

RULE ES (Existential Specification):

Given a statement such as $(\exists z)B(z)$, you can give the object with this property a name, such as $B(d)$. That is, you can "remove" the "$\exists$" *as long as you choose a new name for the object* (d in this example) *for which you have no other information.* [This is easy: just pick a "new" letter.]

RULE EG (Existential Generalization):

$A(m) \ \Rightarrow (\exists x)A(x)$

That is, if you know some particular concrete object m has property A, you can always be "more vague" and say merely that some object has property A.

RULE UG (Universal Generalization):

If you have proved $D(j)$, you can *sometimes* conclude $(\forall w)D(w)$. To decide if this is a "legal" use of UG, you must review your proof, and determine if you can repeat the proof for any object (rather than just the object j). If you can, then this rule applies.

These 4 rules work like implications: you are *not* allowed to use them on just a part of an expression. You can only "remove" a $\forall$ or $\exists$ if it modifies the *entire* expression. Ditto if you want to insert a $\forall$ or $\exists$.

SAMPLE #6 (Predicate Calculus).

Consider the theorem: "Socrates is a human, and all humans are mortal. Therefore, Socrates is mortal." With s representing Socrates, $M()$ representing the predicate "is mortal", and $H()$ representing the predicate "is a human", we can show: $H(s), (\forall x)(H(x)\rightarrow M(x)) \Rightarrow M(s)$

1. $(\forall x)(H(x)\rightarrow M(x))$ P
2. $H(s)$ P
3. $H(s)\rightarrow M(s)$ US on 1
4. $M(s)$ I_{11} on 2 and 3

Note that we could prove other conclusions from these inferences, such as:

5. $(\exists y)(M(y))$ EG on 4

That is, we could infer that "someone in this universe is mortal". Note that it would **not** be legal to conclude that all objects are mortal, e.g.,

X. $(\forall y)(M(y))$ *invalid!* UG on 4

...because our inferences depended upon a fact about s, which is a fact that might not be true of other objects. (Trying to conclude that Zeus was mortal, for example, would *not* follow from our hypotheses.)

In a formula such as $(\forall y)M(y)$, y is a dummy variable (placeholder), helping us express the concept "All objects are mortal." $(\forall z)M(z)$ or $(\forall x)M(x)$ make equivalent observations about our universe (just as $f(z) = 2z$ describes the same function as $f(y) = 2y$ in algebra).

more IMPLICATIONS

I_{15}:$(\forall x)A(x)\vee(\forall y)B(y)\Rightarrow(\forall z)(A(z)\vee B(z))$

I_{16}:$(\exists x)(A(x)\wedge B(x))\Rightarrow(\exists v)A(v)\wedge(\exists y)B(y)$

more EQUIVALENCES

E_{23}:$(\exists x)A(x)\vee(\exists y)B(y)\Leftrightarrow(\exists z)(A(z)\vee B(z))$

E_{24}:$(\forall x)(A(x)\wedge B(x))\Leftrightarrow(\forall v)A(v)\wedge(\forall y)B(y)$

E_{25}:$\sim(\forall x)(A(x)) \Leftrightarrow (\exists v)(\sim A(v))$

E_{26}:$\sim(\exists x)(A(x)) \Leftrightarrow (\forall v)(\sim A(v))$

E_{27}:$(\forall x)(C\vee B(x)) \Leftrightarrow C\vee(\forall y)B(y)$

E_{28}:$(\exists x)(C\wedge B(x)) \Leftrightarrow C\wedge(\exists y)B(y)$

E_{29}:$(\forall x)(A(x)) \rightarrow D \Leftrightarrow (\exists v)(A(v) \rightarrow D)$

E_{30}:$(\exists x)(A(x)) \rightarrow D \Leftrightarrow (\forall v)(A(v) \rightarrow D)$

E_{31}:$B \rightarrow (\forall x)A(x) \Leftrightarrow (\forall y)(B \rightarrow A(y))$

E_{32}:$B \rightarrow (\exists x)A(x) \Leftrightarrow (\exists y)(B \rightarrow A(y))$

Note the duality: interchanging $\forall$ with $\exists$ and $\wedge$ with $\vee$ (and $\Rightarrow$ with $\Leftarrow$) turns the odd-numbered formulas into the even-numbered formulas.

SAMPLE PROOF #7

Given premises $(\exists z)(\ I(z)\ \wedge \sim J(z)\ )$ and $(\exists x)(F(x)\wedge S(x)) \rightarrow (\forall y)(I(y)\rightarrow J(y))$, prove that $(\forall v)(F(v) \rightarrow \sim S(v))$.

1. $(\exists z)(I(z) \wedge \sim J(z))$	P
2. $I(q) \wedge \sim J(q)$	ES on 1
3. $\sim(I(q) \rightarrow J(q))$	E_{17} on 2
4. $(\exists z)(\sim(I(z) \rightarrow J(z)))$	EG on 3
5. $\sim(\forall z)(I(z) \rightarrow J(z))$	E_{25} on 4
6. $(\exists x)(F(x)\wedge S(x))\rightarrow(\forall y)(I(y)\rightarrow J(y))$	P
7. $\sim(\exists x)(F(x)\wedge S(x))$	I_{12} on 6 and 5
8. $(\forall x) \sim (F(x)\wedge S(x))$	E_{26} on 7
9. $\sim(F(b) \wedge S(b))$	US on 8
10. $\sim F(b) \vee \sim S(b)$	E_9 on 9
11. $F(b) \rightarrow \sim S(b)$	E_{16} on 10
12. $(\forall v)(F(v) \rightarrow \sim S(v))$	UG on 11

Why does UG allow us to go from line 11 to line 12? Because we chose b as the name of the object when using US, but if we had instead chosen c on line 9, then line 11 would look like $F(c) \rightarrow \sim S(c)$, and so on for any letter we might have chosen. Thus, we can derive line 11 for every object.

The operators $\forall$ and $\exists$, as with other unary operators like $\sim$, modify "as little as possible". Parentheses are needed if you want them to apply to more than the very next symbol. In the next exercises, a common mistake is to mentally insert parentheses that are not really there!

EXERCISES jc-B

1. Formally prove that the conclusion (on the right) follows from the list of [comma-separated] hypotheses (to the left of "$\Rightarrow$").

a) $P(x) \wedge (\forall x)Q(x) \Rightarrow (\exists z)(P(z) \wedge Q(z))$

b)$(\forall x)(\sim J(x)\rightarrow K(x)), (\forall y)\sim K(y)\Rightarrow J(a)$

c)$\sim((\exists h)P(h)\wedge I(a))\Rightarrow(\exists z)P(z) \rightarrow\sim I(a)$

d) $(\forall q)(L(q)\vee S(q)), (\forall r)\sim L(r)\Rightarrow(\exists x)S(x)$

e) $(\forall q)(L(q)\vee S(q)), (\forall r)\sim L(r)\Rightarrow(\forall x)S(x)$

f)$\sim(\forall x)(P(x)\wedge Q(x)), (\forall x)P(x)\Rightarrow\sim(\forall x)Q(x)$

g)$(\forall x)(P(x)\rightarrow Q(x)), (\forall x)(Q(x)\rightarrow R(x)) \Rightarrow P(x)\rightarrow R(x)$

2. Look for a place to use CP on these:

a)$(\exists x)P(x)\rightarrow(\forall y)Q(y))\Rightarrow(\forall z)(P(z)\rightarrow Q(z))$

b)$(\forall x)(P(x)\rightarrow Q(x))\Rightarrow(\forall z)P(z)\rightarrow(\forall y)Q(y)$

c)$(\forall x)(P(x)\rightarrow Q(x)), (\forall x)(R(x)\rightarrow\sim Q(x))\Rightarrow (\forall m)(R(m)\rightarrow\sim P(m))$

3. Why are these invalid uses of US?

a) 1. $(\forall x)P(x) \quad \rightarrow \quad Q(x)$

. 2. $P(x) \quad \rightarrow \quad Q(x)$

b) 1. $(\forall x)P(x) \quad \rightarrow \quad Q(x)$

. 2. $P(b) \quad \rightarrow \quad Q(x)$

c) 1. $(\forall x)(P(x) \vee Q(x))$

. 2. $P(w) \vee Q(v)$

4. For each of the three scenarios in #3 above, build a universe where line 1 is true but line 2 is false.

5. Why are these invalid uses of EG?

a) 1. $P(x) \quad \rightarrow \quad Q(x)$

. 2. $(\exists x)P(x) \quad \rightarrow \quad Q(x)$

b) 1. $P(b) \rightarrow Q(a)$

. 2. $(\exists x)(P(x) \rightarrow Q(x))$

c) 1. $P(w) \vee Q(v)$

. 2. $(\forall v)(P(v) \vee Q(v))$

6. For the scenarios (a) and (c) in #5 above, build a universe where line 1 is true but line 2 is false.

7. Find the mistake in the following derivation:
7-1. $(\exists z)B(z)$ Premise
7-2. $(\exists z)F(z)$ Premise
7-3. $F(v)$ ES on 7-2
7-4. $B(v)$ ES on 7-1
Hint: Let $B(x)$ represent "x has a beard", and let $F(x)$ represent "x is female". In a typical classroom, most likely $(\exists x)B(x)$ and $(\exists x)F(x)$ are both valid premises. We could apply rule ES to either or both hypotheses. For example, we might conclude "Veronica is female" (as in 7-3). Somewhat like 7-4, we might also give a name to the person with a beard, e.g., "Jack has a beard", which would also be a valid conclusion. What would the flaw in the logic be if we were to instead conclude "Veronica has a beard" and claim that this was a valid use of ES (as was done in 7-4)?

8. Find the mistake in the following derivation:
8-1. $(\forall z)B(z)$ Premise
8-2. $(\exists z)F(z)$ Premise
8-3. $B(a)$ US on 8-1
8-4. $F(a)$ ES on 8-2
Hint: Let $B(x)$ represent "x is breathing", and let $F(x)$ represent "x is female". In a typical classroom, most likely $(\forall x)B(x)$ and $(\exists x)F(x)$ are both valid premises, and we could apply rule ES and US. For example, we might conclude "Arnold is breathing" (as in 8-3). However, we should NOT subsequently conclude "Arnold is female" (as in 8-4); this is another invalid use of ES (as in the previous problem, we must choose an "unused" variable name each time we invoke ES.
However, we can still conclude there is a student who has both properties B and F, if we structure the proof a bit differently:
8-3. $F(\text{Alison})$ ES on 8-2
8-4. $B(\text{Alison})$ US on 8-1
Since US applies to every student, there is no problem "reusing" a variable name with the US rule. In practice, just remember to apply ES before you apply US.

SAMPLE PROOF #8: "The difference of any two odd numbers is even." (formally!) First, we will rewrite this more precisely, so that we can better apply the tricks we have learned in the previous chapters:
$(\forall a)(\forall b)((a \text{ odd} \wedge b \text{ odd}) \to a{-}b \text{ is even})$
We will largely construct the proof "backwards", now that we know what the last line of the proof should look like. Since the outermost operator is that $(\forall a)$, it's a pretty sure bet that the line before it will look pretty much the same, but without the quantifier. That is, the next to last line will probably be something like:
$(\forall b)((n \text{ is odd} \wedge b \text{ is odd}) \to n{-}b \text{ is even})$
The dummy variable a was replaced by the specific object n here; it is legal to just use a instead of a different letter (n), but since they stand for different things (one is an actual number, and the other is just a placeholder to help us say "all things have this property"), it's better to use different symbols. Similarly, the line prior to that one will be
$(n \text{ is odd} \wedge m \text{ is odd}) \to n{-}m \text{ is even}$
...and we hope we can justify using UG twice to get to the desired conclusion.

This "third line from the bottom" is rather friendly; it is the sort of statement for which we can use CP. Now (finally!) we have a clue as to what the first line of our proof should be:
n is odd $\wedge$ m is odd Assumed Premise
(If we were writing this less formally and more conversationally, we would start by saying "Let n and m be arbitrary integers, and assume both of them are odd.")

Furthermore, since we are going to use CP, we have a much-simplified goal of:
$n{-}m$ is even CP on 1 and ?
Here's what we have constructed so far:
1. n is odd $\wedge$ m is odd Assumed P
2. ... ??? ???
$n{-}m$ is even ???
$(n \text{ odd} \wedge m \text{ odd}) \to n{-}m \text{ is even}$ CP 1,?
$(\forall b)((n \text{ odd} \wedge b \text{ odd}) \to n{-}b \text{ is even})$ UG
$(\forall a)(\forall b)((a \text{ odd} \wedge b \text{ odd}) \to a{-}b \text{ even})$ UG

Next, we have to "fill in the gaps," but we will have a better idea about where we are supposed to be headed if we work backward a little more. We look up what it means to say "$n-m$ is even" to discover: $(\exists k)(n-m = 2k)$

This informs us that once we get formulas for n and m, we need to do some algebra to put all the terms together and pull out a common factor of 2. Here's the full formal proof, using line 9 as a guide, and then working forward from step 1:

1. n is odd $\wedge$ m is odd Assumed Premise
2. n is odd I_1 on 1
3. m is odd I_2 on 1
4. $(\exists k)(n = 2k + 1)$ Def. of "odd" on 2
5. $(\exists k)(m = 2k + 1)$ Def. of "odd" on 3
6. $n = 2i + 1$ ES on 4
7. $m = 2j + 1$ ES on 5
8. $n-m = 2i+1-(2j+1)=2(i-j)$ alg. 6,7
9. $(\exists k)(n-m = 2k)$ EG on 8
10. $n-m$ is even Def. of "even" on 9
11. (n is odd $\wedge$ m is odd) $\rightarrow$ $n-m$ is even
. CP on 1,10
12. $(\forall b)((n$ odd $\wedge$ b odd$) \rightarrow n-b$ is even$)$
. UG on 11
13. $(\forall a)(\forall b)((a$ odd $\wedge$ b odd$) \rightarrow a-b$ even$)$
. UG on 12

I will allow you to go directly from line 11 to what I have on line 13 as long as you state the reason as "UG twice on 11."

In this proof, we restricted our universe to just the set of integers (not fractions, goats, colors, etc.), so when we said $(\exists k)$, it was understood that k must be an integer. We also relied on the underlying facts that adding, subtracting, or multiplying integers (e.g., $i - j$ or $2k$) always yields another integer. Note that the same cannot be said for division, so a proof that divides two integers and depends on the result being an integer would be flawed.

Sample Proof #9: $(\forall n \geq 0)(3|(2^{2n} - 1))$ This requires a proof by induction, and the very first step is **always** to be specific about what the proposition $P(n)$ is. In this case, we define $P(n) : 3|(2^{2n} - 1)$. Note that there is no "$\forall$" here; $P(n)$ is an assertion about one particular size [our goal is to prove it for all sizes, that is, to show $(\forall n)P(n)$, but $P(n)$ is for a single size].

Our basis step is $n = 0$. Why? Because our goal says $n \geq 0$, so we know we should be starting at 0. Remember that $P(n)$ is always a **statement**, and never a **number**. (It often involves some assertion about a number, which is either true or false; our goal is to show it evaluates to **true** every single time.) In this case, the assertion is that 3 divides some complicated expression. For $P(0)$, we must show $3|(2^{2\times 0} - 1)$, which works out to be $3|0$, which is true (since $0 = 3 \times 0$). So, $P(0)$ is true, and we've proved the basis step.

For the inductive step, we let m be arbitrary and assume that $P(m)$ is true; our new goal is to show that $P(m + 1)$ is also true. (We want m to be arbitrary, because later we have to assert that our line of reasoning works for all choices of m. That is, we want to use rule CP and then rule UG.)

Here is the full formal proof:

1. $0 = 3 \times 0$ arithmetic
2. $2^{2\times 0} - 1 = 3 \times 0$ arithmetic on 1
3. $(\exists k)(2^{2\times 0} - 1 = 3 \times k)$ EG on 2
4. $3 \mid (2^{2\times 0} - 1)$ Def. of "divides" on 3
5. $P(0)$ Def. of "P" on 4
6. $P(m)$ Assumed Premise
7. $3|(2^{2m} - 1)$ Def. of "P" on 6
8. $(\exists k)(2^{2m} - 1 = 3k)$ Def. of "|" on 7
9. $2^{2m} - 1 = 3q$ ES on 8
10. $2^{2(m+1)}-1 = 2^{2m}\times 2^2-1 = 2^{2m}\times 4 - 1 = 2^{2m} \times (3 + 1) - 1 = 2^{2m} \times 3 + 2^{2m} - 1 = 3 \times 2^{2m} + 3q = 3(2^{2m} + q)$ algebra on 9
11. $(\exists k)(2^{2(m+1)} - 1 = 3k)$ EG on 10
12. $3|(2^{2(m+1)} - 1)$ Def. of "|" on 11
13. $P(m + 1)$ Def. of "P" on 12
14. $P(m) \rightarrow P(m + 1)$ CP on 6,13
15. $(\forall i)(P(i) \rightarrow P(i + 1))$ UG on 14
16. $(\forall n \geq 0)(3|(2^{2n} - 1))$ P.o.M.I. 5,15

(e.g., Principle of Math Induction on 5,15)
Note that we wrote steps 1-5 "backward" from the way we reasoned it out; we must always begin with facts we know $[0 = 3\times 0]$ and proceed to our goal $[P(0)]$.

Here's a typical sample exam problem, covering many concepts. Define $P(n)$ by:

$$\prod_{i=1}^{n}\frac{i}{n}\le\sum_{i=1}^{n}\frac{i-1}{i+1}$$

We wouldn't try an inductive proof, since it is hardly ever true. Try, for example, calculating $P(2)$ [and if your "final answer" was a number, then reread the previous sentence, and remember that you are evaluating something that is an assertion].

SAMPLE PROOF #9 (set theory):
$(\forall A)(\forall B)(A\times(B\cup C)\subseteq(A\times B)\cup(A\times C))$
When dealing with cross products, there is a slight modification we need for the definition of subset: since a member of a cross product is an ordered pair, and we need to consider all combinations of first coordinates and second coordinates, we will need two $\forall$ quantifiers (see step 8 below).

1. $(u,w)\in F\times(G\cup H)$ Assumed Premise
2. $u\in F\wedge w\in(G\cup H)$ Def. of "$\times$" on 1
3. $u\in F\wedge(w\in G\vee w\in H)$ Def. of "$\cup$"
4. $(u\in F\wedge w\in G)\vee(u\in F\wedge w\in H)$ E_6
5. $((u,w)\in(F\times G))\vee((u,w)\in(F\times H))$ Def. of "$\times$" (twice) on 4
6. $(u,w)\in(F\times G)\cup(F\times H)$ Def. of "$\cup$" on 5
7. $(u,w)\in F\times(G\cup H)\to(u,w)\in(F\times G)\cup(F\times H)$ CP on 1,6
8. $(\forall x)(\forall y)((x,y)\in F\times(G\cup H)\to(x,y)\in(F\times G)\cup(F\times H))$ UG twice on 7
9. $(F\times(G\cup H)\subseteq(F\times G)\cup(F\times H))$
. Definition of "$\subseteq$" on 8
10. $(\forall A)(\forall B)(A\times(B\cup C)\subseteq(A\times B)\cup(A\times C))$ UG twice on 9

We use the symbol $\preceq$ to represent an arbitrary partial ordering: $\preceq$ might represent $\le$, or it could mean $\subseteq$, $\ge$, or $|$. Similarly, we use $\succeq$ as a shorthand for $\preceq^{-1}$ when we want to refer to the inverse of $\preceq$.

We can prove, for example, that any greatest element in a partial ordering must be a maximal element. That is,
$(\forall M)(M$ is greatest $\to M$ is maximal$)$

SAMPLE PROOF #10 (partial ordering): Here is an abbreviated formal proof:

1. M is greatest Assumed Premise
2. $M\preceq n$ Assumed Premise
3. $(\forall a)(a\preceq M)$ Def. of "greatest" on 1
4. $n\preceq M$ US on 3
5. $(n\preceq M)\wedge(M\preceq n)$ I_9 on 2,4
6. $n=M$ $\preceq$ is antisymmetric on 5
7. $M\preceq n\to n=M$ CP on 2,6
8. $(\forall n)(M\preceq n\to n=M)$ UG on 7
9. M is maximal Def. of "maximal" on 8
10. M is greatest$\to M$ is maximal CP 1,9
11. $(\forall M)(M$ is greatest $\to M$ is maximal$)$
. UG on 10

A truly formal proof should begin with the hypotheses that $\preceq$ is a partial ordering, use I_1 and I_2 to extract the fact that $\preceq$ is antisymmetric, use US twice to remove the quantifiers on the definition and put M and n in their place, and then use I_{11} to justify line 6. At this point in the course, I'm likely to allow you to skip that formalism and go directly from line 5 to line 6, with "antisymmetry" as the justification.

The partial ordering $\preceq$ is a bunch of ordered pairs over some underlying set A, so the actual definition of "greatest" is technically $(\forall a)((a\in A)\to(a\preceq M))$, but if we limit our universe to consist of only the elments in A, then we can get by with the simpler definition listed on line 3.

Note that the contrapositive statement,
$(\forall M)(M$ is maximal $\to M$ is greatest$)$
is **not** always true; you should be able to generate a very simple Haase diagram that illustrates the point (containing a maximal element, but no greatest element).