# MATH 224 FOUNDATIONS OF MATHEMATICS
# DR. MCLOUGHLIN'S CLASS
# METHODS OF PROOF HANDY DANDY GUIDE

**Direct Proof (1 simple):** To prove the conclusion C from a 'finite' set of premises {say $H_1, H_2, \ldots, H_k$ where $k \in \mathbb{N}$} simply begin with the premises and by deductive reasoning show that C is provable as a consequent of the set of premises (hypotheses) $H_1, H_2, \ldots, H_k$.

*PRACTICAL MEANING OF THE ABOVE:*
I want to prove ASSUMING the premises $H_1, H_2, \ldots, H_k$ that C follows from them; so, I assume $H_1, H_2, \ldots, H_k$ are true and prove that C follows from these premises.

**Direct Proof (1 compound):** To prove the implication $(A \Rightarrow B)$ from a 'finite' set of premises {say $H_1, H_2, \ldots, H_k$ where $k \in \mathbb{N}$} show that $(A \Rightarrow B)$ is provable as a consequent of the set of premises (hypotheses) $H_1, H_2, \ldots, H_k$.

*PRACTICAL MEANING OF THE ABOVE:*
I want to prove ASSUMING the premises $H_1, H_2, \ldots, H_k$ that $(A \Rightarrow B)$ follows from them; so, I assume $H_1, H_2, \ldots, H_k$ are true and prove that $(A \Rightarrow B)$ follows from these premises.

**Direct Proof (2):** To prove the implication $(A \Rightarrow B)$ from a 'finite' set of premises {say $H_1, H_2, \ldots, H_k$ where $k \in \mathbb{N}$} it is sufficient to include A in the set of premises {e.g.: $A, H_1, H_2, \ldots, H_k$ }and show that B is provable as a consequent of the augmented set of premises (hypotheses).

*PRACTICAL MEANING OF THE ABOVE:*
I want to prove ASSUMING the premises $H_1, H_2, \ldots, H_k$ that $(A \Rightarrow B)$ follows from them,
so, it is equivalent to:

Assume $A, H_1, H_2, \ldots, H_k$ are the premises and prove that (B) follows from these.
We say we assume the hypothesis of the conclusion (A).[1]

[1] Notice this is not the fallacy assuming the conclusion (which would be assuming $A \Rightarrow B$ is true) nor is it the fallacy of assuming the premise (where one of the hypotheses might be of the form $P \Rightarrow Q$ and you assume P is true).

**Direct Proof (3) [by contrapositive]**: To prove the implication $(A \Rightarrow B)$ from a 'finite' set of premises {say $H_1, H_2, \ldots, H_k$ where $k \in \mathbb{N}$}it is sufficient to include $\neg B$ in the set of premises {e.g.: $\neg B, H_1, H_2, \ldots, H_k$ }and show that $\neg A$ is provable as a consequent of the augmented set of premises (hypotheses).

*PRACTICAL MEANING OF THE ABOVE:*
I want to prove ASSUMING the premises $H_1, H_2, \ldots, H_k$ that $(A \Rightarrow B)$ follows from them, so, it is equivalent to: Assume $\neg B, H_1, H_2, \ldots, H_k$ are the premises and prove that $(\neg A)$ follows from these.

**Indirect Proof (2) [also called: method of elimination, method of cases, Holmsian[2], etc. ]**: To prove a question of magnitude from a set of premises {say $H_1, H_2, \ldots, H_k$ where $k \in \mathbb{N}$} we consider the possibilities say $\{C_1, C_2, \ldots, C_j$ where $j \in \mathbb{N}\}$ and show that all but one (not necessarily all but one in all cases, but for argument sake let us reduce to all but one) of the possibilities are false, then the one, call it $C_i$ where $i \in \{1, 2, \ldots, k\}$ is true.

*PRACTICAL MEANING OF THE ABOVE:*
I want to prove ASSUMING the premises $H_1, H_2, \ldots, H_k$ that one or more of the following holds: $C_1, C_2, \ldots, C_j$. Assume $H_1, H_2, \ldots, H_k$. Show that for the possibilities $C_1, C_2, \ldots, C_j$, we find $C_1, C_2, \ldots, C_{(i-1)}, C_i, \ldots, C_j$ <u>all</u> lead to contradictions of the form $\neg R \wedge R$ for some statement R; thus, $C_i$ must follow from the premises (it is the only one left- all others lead to $\neg R \wedge R$ which cannot be!).

**Contradiction[3] (Indirect Proof (1)) [also called reducto ad absurdum {reduce to the absurd}]**: To prove Q follows from a set of premises {say $H_1, H_2, \ldots, H_k$ where $k \in \mathbb{N}$} it is sufficient to consider $\neg Q$ as an additional premise {say $\neg Q, H_1, H_2, \ldots, H_k$ } and prove a statement of the form $\neg R \wedge R$ follows therefore the assumption of $\neg Q$ must be false which means $\neg(\neg Q)$ is true, so Q is true. .

*PRACTICAL MEANING OF THE ABOVE:*
I want to prove ASSUMING the premises $H_1, H_2, \ldots, H_k$ that (Q) follows from them,
so, it is equivalent to:
Assume $\neg Q, H_1, H_2, \ldots, H_k$ are the premises and prove that $(\neg R \wedge R)$ follows from these where $\neg R \wedge R$ can be any statement and its negation that follow (which is the contradiction - - because it is nonsensical to claim that R and not R can be true at the same time). With that being the case, then the addition of not Q to the hypotheses must have been in error! So, since all the hypotheses $H_1, H_2, \ldots, H_k$ were assumed true and $\neg Q, H_1, H_2, \ldots, H_k$ is false, then $\neg Q$ **is false**, ergo Q is true!

---

[2] I call this Holmsian from Sherlock Holmes (see the article I handed out) - - when all other possibilities are eliminated whatever remains, no matter how hard to believe, is the truth.

[3] My favourite method. Note: this does not imply it will be yours or that you should always attempt to prove a claim using this method. I am simply noting it is my favourite method for your edification.

**Adjoining Premises**: Any statement can be adjoined to the premises of a proof if it can be proved from the premises.

*PRACTICAL MEANING OF THE ABOVE:*

You are doing a proof and a result follows from the premises which is not the conclusion you are trying to derive. This can be added to the list of premises (e.g.: it becomes an additional premise) for the proof. **Warning:** *this does not mean you can assume anything and add it to the list of premises! It means only that which follows from the premises can be adjoined!*

**Adjunction**: If P is provable from the set of hypotheses $\{\text{say } H_1, H_2, \ldots, H_k \text{ where } k \in \mathbb{N}\}$ and Q is provable from the same set of hypotheses $H_1, H_2, \ldots, H_k$, then $[P \wedge Q]$ is provable from that set of hypotheses$\{\text{say } H_1, H_2, \ldots, H_k\}$.

*PRACTICAL MEANING OF THE ABOVE:*

You do a proof (any method) that P is provable from the set of hypotheses $H_1, H_2, \ldots, H_k$, later you do a proof Q is provable from the set of hypotheses $H_1, H_2, \ldots, H_k$
logic 'tells' us that $[P \wedge Q]$ is a result of $H_1, H_2, \ldots, H_k$

**Substitution**[4]: Suppose you have a set of hypotheses $\{\text{say } H_1, H_2, \ldots, H_k \text{ where } k \in \mathbb{N}\}$ and say $H_i$ (one of the hypotheses) is obtainable from another say, $H_p$, by substituting a statement R for any occurrence of a statement S in $H_i$. Then we can derive $H_p$ from $S \Leftrightarrow R$ and $H_i$.

*PRACTICAL MEANING OF THE ABOVE:*
You have a set of hypotheses $\{\text{say } H_1, H_2, \ldots, H_k\}$
You want to show a particular one of the hypotheses, say $H_p$, is derivable from another one of the premises, call it $H_i$ and the equivalence statement $S \Leftrightarrow R$. S can replace any occurrence of R or visa versa by substituting in any part of the proof.

[4] This method is hard to write out & explain, but I believe you will find it the easiest to do and through the doing will understand it better.

**Mathematical Induction**[5]: Suppose you are to prove a infinite sequence of statements: s(1), s(2), … where s(k) is the $k^{th}$ statement. The following is the definition of math induction:

(1) Prove s(j) is true for some j (usually j = 1, but this does not have to be the case)
(2) Prove the implication if p(m) is true for $m \geq j$, then p(m + 1) is true.

*PRACTICAL MEANING OF THE ABOVE:*

Suppose you are to prove a infinite sequence of statements: s(1), s(2), … where s(k) is the $k^{th}$ statement. You cannot just show a few and write dot, dot, dot. That is inducing that it will continue and there is not guarantee that such will occur! Therefore, you first prove the statement s(j) is true for some j (usually j = 1, but this does not have to be the case) *and then you must* second prove that assuming the statement s(m) is true for $m \geq j$, then it follows necessarily that the statement s(m + 1) is true.

*Comment*: I know this is redundant but recall this simply means that s (m + 1) is true based on the assumption s(m) is true. - - but follow it back to s(j) that was true, so s(j +1) is true, since s(j + 1) is true, s(j + 2) is true, and so forth. *Note*: this is <u>different</u> than showing independently that say, s(1), s(2), s(3), and s(4) is true and then hoping that s(5), s(6), etc. is true.).

**Cases**: To prove $[P \vee Q] \Rightarrow R$ it is necessary & sufficient to prove R follows from P and R follows from Q.

*PRACTICAL MEANING OF THE ABOVE:*

You do a proof (any method) that R follows logically from P, then later you do a proof (any method) R follows logically from Q, then logically $[P \vee Q] \Rightarrow R$

Comment: This can be generalised to $[P_1 \vee P_2 \vee ... \vee P_k] \Rightarrow R$ such that k is a natural number.

Last revised: 26 Jan. 2009

[5] This is the toughest method to really understand. Pay particular attention to the thought process that it reflects and note it is a deductive method to prove something that many people will just believe inductively, if you were to tell them, "and just follow that pattern on & on, ad nausea." .