# Harold's Proofs Cheat Sheet

4 November 2021

## Definitions

| Term | Example | Definition |
|---|---|---|
| **Proof** | *The sum of two even integers is always even. …* | Exhaustive deductive reasoning which establishes logical certainty for *all* cases. |
| **Theorem** | $a^2 + b^2 = c^2$ *for a right-angled triangle* | A non-self-evident statement that has been proven to be true, either on the basis of generally accepted statements such as axioms or on the basis of previously established statements such as other theorems. |
| **Axioms** | *"Nothing can both be and not be at the same time and in the same respect"* | An axiom, postulate or assumption is a statement that is taken to be true, to serve as a premise or starting point for further reasoning and arguments. |
| **Conjecture** | *When n is a prime number; n + 2 is always prime.* | A conclusion or a proposition which is suspected to be true due to preliminary supporting evidence, but for which no proof or disproof has yet been found. |
| **Hypothesis** | *Drinking sugary drinks daily leads to being overweight* | A proposed explanation for a phenomenon.<br>Antecedent.<br>P is the assumption in a (possibly counterfactual) "What If?" question. |
| **Statement** | **Let** <insert hypothesis>. **If** <insert hypothesis>, **then** <insert conclusion>. | |
| **Antecedent** | $P \rightarrow Q$, *P is the antecedent* | Assumptions or premises of a conditional statement. |
| **Consequent** | $P \rightarrow Q$, *Q is the consequent* | Conclusions of a conditional statement. |
| **Free Variable** | $y \in \{x \mid x2 < 9\}$, *y is a free variable* | • Letters that stand for objects that the statement says something about.<br>• They stand for some particular but unspecified elements of the universe of discourse.<br>• x is free to stand for anything. |
| **Bound (Dummy) Variable** | $y \in \{x \mid x2 < 9\}$, *x is a bound variable* | • Letters that are used as a convenience to help express an idea and should not be thought of as standing for any particular object.<br>• A bound variable can always be replaced by a new variable without changing the meaning of the statement. |
| **Instance** | $x = 4$ | • An assignment of particular values to free variables. |
| **Tautologies** | $P \vee \neg P$ | Formulas that are always true. |
| **Contradictions** | $P \wedge \neg P$ | Formulas that are always false. |

## Proof Language Template

| Action | Example Proof Statement |
|---|---|
| **Suppose** | Suppose ____, and suppose ____.<br>Assume ____,<br>If ____,<br>By hypothesis, ____.<br>*We will prove the contrapositive.* |
| **Assumptions** | Let x be an arbitrary element of ____.<br>Let x be an arbitrary real number, and suppose <equation>. |
| **Clarification** | This means that ____ and ____.<br>Then the definition of ____ tells us that ____.<br>Substituting this into the equation <equation > , we get <equations>, so <equation>.<br>Via algebraic manipulations, ____ and therefore ____. |
| **Since** | Since ____ and ____, by the definition of ____, ____.<br>Since ____, it follows that ____, and since ____ are ____, we must have ____.<br>Then since ____, ____, so ____. |
| **Contradiction** | *But this contradicts the fact that ____.* |
| **Thus** | Thus, if ____ then ____.<br>Therefore, ____.<br>We can show that ____.<br>Then <equation>. |
| **Conclusion** | Since x was an arbitrary element of ____, we can conclude that <logic>, so <set>.<br>But x was an arbitrary element of ____, so this shows that ____, as required.<br>Therefore, we have proved that ____.<br>Therefore, by the definition of ____ again, we have shown that ____.<br>... and thus it is proved.<br>Thus, if <equation> and <equation> then <equation>.<br><br>*Thus, it cannot be the case that ___ is an element of ____ but not ____, so ____.*<br>*Since the assumption that ____ has led to a contradiction, there must be ____.* |
| ∴ | Conclusion.<br>Is generally used before a logical consequence, such as the conclusion of a proof. |
| □, ☐, ■, ■, Q.E.D. | Indicates the end of a proof. This abbreviation stands for "*quod erat demonstrandum*", which is Latin for "*that which was to be demonstrated*". |

## Proof Methods

| Method | Definition |
|---|---|
| **Direct** | The conclusion is established by logically combining the axioms, definitions, and earlier theorems. |
| **Induction** | A single "base case" is proved, and an "induction rule" is proved that establishes that any arbitrary case implies the next case. |
| **Contrapositive** | Infers the statement $P \rightarrow Q$ by establishing the logically equivalent contrapositive statement: $\neg Q \rightarrow \neg P$. |
| **Contradiction** | If some statement is assumed true, and a logical contradiction occurs, then the statement must be false. |
| **Construction** | The construction of a concrete example with a property to show that something having that property exists. AKA proof by example. |
| **Exhaustion** | The conclusion is established by dividing it into a finite number of cases and proving each one separately. |

## Direct Proof Strategies: General

| Strategy | Form | Description |
|---|---|---|
| **Write Out the Definitions** | *Logical form of statement* | In many cases the logical form of a statement can be discovered by writing out the meaning or definition of some mathematical word or symbol that occurs in the statement. |
| **Mathematical Truths** | | • Definitions<br>• Theorems<br>• Axioms<br>• Computations |
| **Next Steps** | | When analyzing the logical forms of givens and goals in order to figure out a proof, it is usually best to do only as much of the analysis as is needed to determine the <u>next step</u> of the proof. Going further with the logical analysis usually just introduces unnecessary complication, without providing any benefit. |
| **False Starts** | | When trying to write a proof you may make a few false starts before finding the right way to proceed.<br><br>"*We tried both methods, and the second worked.*" |
| **Nested Logic** | | This means that whenever you use one of these strategies you can write a sentence or two at the beginning or end of the proof and then forget about the original problem and work instead on the new problem, which will usually be easier.<br><br><u>Form:</u><br>Suppose $\neg R$.<br>Suppose $P$.<br>Since $P$ and $P \rightarrow (Q \rightarrow R)$, it follows that $Q \rightarrow R$.<br>[Proof of $\neg Q$ goes here.]<br>Therefore $P \rightarrow \neg Q$.<br>Therefore $\neg R \rightarrow (P \rightarrow \neg Q)$. |
| **Reuse** | | Once you have shown that a statement is true, you can use it later in the proof exactly as if it were a hypothesis. |
| **Counterexample** | **goal** of the form $P$, try to show $\neg P$ | If you find a counterexample to a theorem, then you can be sure that the theorem is incorrect. |
| **Variables** | $x_0, A_0$ | Variables must always be introduced <u>before</u> they are used. |

 

| | | |
|---|---|---|
| **Concise Write-up** | | A proof should contain only the reasoning needed to justify the conclusion of the proof, **not** an explanation of how you thought of that reasoning.<br><br>Although we have used the symbols of <u>logic</u> freely in the scratch work, we have not used them in the final write-up of the proof.<br><br>Stick to ordinary English.<br>Replace → with 'then' or 'therefore'.<br><br>Use of set notation is acceptable.<br><br>The efficiency of exposition is one of the most attractive features of proofs, but it also often makes them difficult to read. |

## Proof Strategy: Transforming ($P \rightarrow Q$)

| Strategy | Form | Description |
|---|---|---|
| **Transforming** | | Transform the problem into one that is equivalent but easier to solve.<br><br>Revise your givens and goal in some way. |
| To prove a **goal** | $P \rightarrow Q$ | Assume P is true and then prove $Q$.<br><br>If the form is $P \rightarrow Q$, then you can transform the problem by adding $P$ to your list of hypotheses (givens) and changing your conclusion (goal) from $P \rightarrow Q$ to $Q$. |
| To prove a **goal** | $P \rightarrow Q$ | Assume $P$ is true and then prove $Q$.<br><br><u>Form:</u><br>Suppose $P$.<br>[Proof of $Q$ goes here.]<br>Therefore $P \rightarrow Q$. |
| To prove a **goal** | $P \rightarrow Q$ | Prove the contrapositive. Assume that Q is false and prove that P is false.<br><br><u>Form:</u><br>Suppose $Q$ is false.<br>[Proof of $\neg P$ goes here.]<br>Therefore $P \rightarrow Q$. |

## Proof Strategy: Inference Rules ($P \rightarrow Q$)

| Strategy | Form | Description |
|---|---|---|
| **Inference Rules** | | |
| To use a **given** | $\neg P$ | If possible, reexpress this given in some other form. |
| To use a **given** | $P \rightarrow Q$ | if you know that both $P$ and $P \rightarrow Q$ are true, you can conclude that $Q$ must also be true. (***modus ponens***) |
| To use a **given** | $P \rightarrow Q$ | if you know that $P \rightarrow Q$ is true and $Q$ is false, you can conclude that $P$ must also be false. (***modus tollens***) aka Contrapositive. |

## Proof Strategy: Negations ($\neg P$)

| Strategy | Form | Description |
|---|---|---|
| **Negations** | *Positive Stateme nts* | Usually it's easier to prove a positive statement than a negative statement, so it is often helpful to reexpress a goal of the form $\neg P$ before proving it. |
| To prove a **goal** | $\neg P$ | If possible, reexpress the goal as a positive statement, in some other form and then use one of the proof strategies for this other goal form. |
| To prove a **goal** | $\neg P$ | Assume $P$ is true and try to reach a **contradiction**. Once you have reached a contradiction, you can conclude that $P$ must be false.<br><br>Form:<br>Suppose $P$ is true.<br>[Proof of contradiction goes here.]<br>Thus, $P$ is false. |
| To use a **given** | $\neg P$ | If you're doing a proof by **contradiction**, try making $P$ your goal. If you can prove $P$, then the proof will be complete, because $P$ contradicts the given $\neg P$.<br><br>Form:<br>[Proof of $P$ goes here.]<br>Since we already know $\neg P$, this is a contradiction.<br><br>Usually it's best to try the other strategies first if any of them apply; but if you're stuck, you can try proof by contradiction in any proof. |
| To prove a **goal** | $x \in B$ | The goal $x \in B$ contains no logical connectives, so none of the techniques we have studied so far apply.<br><br>Try reexpressing as a positive statement.<br>Lacking anything else to do, we try proof by **contradiction**. |

## Proof Strategy: Quantifiers (∀*x*, ∃*x*)

| Strategy | Form | Description |
|---|---|---|
| **Quantifiers** | | |
| To prove a **goal** | ∀*x P(x)* | Introduce a new variable x to stand for an arbitrary object, then prove *P(x)*.<br><br>**Goal** changes from ∀*x P(x)* to *P(x)*.<br><br>Form:<br>Let *x* be arbitrary.<br>[Proof of *P(x)* goes here.]<br>Since *x* was arbitrary, we can conclude that ∀*x P(x)*. |
| To prove a **goal** | ∃*x P(x)* | Try to find a value of a new variable *x* for which you think *P(x)* will be true. Then start your proof with "Let *x* = (the value you decided on)" and proceed to prove *P(x)* for this value of *x*.<br><br>**Goal** changes from ∃*x P(x)* to *P(x)* after you add a new **given** of *x* = (the value you decided on).<br><br>Form:<br>Let *x* = (the value you decided on).<br>[Proof of *P(x)* goes here.]<br>Thus, ∃*x P(x)*. |
| To use a **given** | ∀*x P(x)* | You can plug in any value, say *a*, for *x* and use this given to conclude that *P(a)* is true. (*universal instantiation*) |
| To use a **given** | ∃*x P(x)* | If a given starts with ∃A, we should use it immediately.<br><br>Introduce a new variable $x_0$ into the proof to stand for an object for which $P(x_0)$ is true. This means that you can now assume that $P(x_0)$ is true. (*existential instantiation*) |

## Proof Strategy: Existence and Uniqueness ($\exists x$, $\exists! x$)

| Strategy | Form | Description |
|---|---|---|
| **Existence & Uniqueness** | | |
| To prove a **goal** | $\exists! x\ P(x)$ | Prove $\exists x\ P(x)$ and $\forall y\ \forall z\ ((P(y) \wedge P(z)) \rightarrow y = z)$. The first of these goals shows that there exists an x such that P(x) is true, and the second shows that it is unique. The two parts of the proof are therefore sometimes labeled **existence and uniqueness.** Each part is proven using strategies discussed earlier.<br><br><u>Form:</u><br>Existence: [Proof of $\exists x P(x)$ goes here.]<br>Uniqueness: [Proof of $\forall y \forall z((P(y) \wedge P(z)) \rightarrow y = z)$ goes here.] |
| To prove a **goal** | $\exists! x\ P(x)$ | Prove $\exists x\ (P(x) \wedge \forall y\ (P(y) \rightarrow y = x))$, using strategies. |
| To use a **given** | $\exists! x\ P(x)$ | Treat this as two given statements,<br>$\exists x\ P(x)$ and $\forall y\ \forall z\ ((P(y) \wedge P(z)) \rightarrow y = z)$.<br>To use the first statement you should probably choose a name, say $x_0$, to stand for some object such that $P(x_0)$ is true.<br>The second tells you that if you ever come across two objects $y$ and $z$ such that $P(y)$ and $P(z)$ are both true, you can conclude that $y = z$. |

## Proof Strategy: Biconditionals ($P \leftrightarrow Q$)

| Strategy | Form | Description |
|---|---|---|
| **Biconditionals** | $(P \rightarrow Q) \wedge (Q \rightarrow P)$ | Can use string of equivalences. $P$ iff $R$ iff $Q$. |
| To prove a **goal** | $P \leftrightarrow Q$ | Prove $P \rightarrow Q$ and $Q \rightarrow P$ separately.<br>Once proven, it can mean equivalence, or $P = Q$.<br><br><u>Form:</u><br>If A then B.<br>If B then A. |
| To use a **given** | $P \leftrightarrow Q$ | Treat this as two separate givens: $P \rightarrow Q$, and $Q \rightarrow P$. |

## Proof Strategy: Conjunctions (P $\wedge$ Q)

| Strategy | Form | Description |
|---|---|---|
| **Conjunctions** | | |
| To prove a **goal** | $P \wedge Q$ | Prove P and Q separately. In other words, treat this as two separate goals: P, and Q.<br><br><u>Form:</u><br>Let x be arbitrary.<br>Suppose $x \in A$.<br>[Proof of $x \in B$ goes here.]<br>[Proof of $x \in C$ goes here.]<br>Thus, $x \in B \wedge x \in C$, so …<br>Therefore …<br>Since x was arbitrary, … |
| To use a **given** | $P \wedge Q$ | Treat this as two separate givens: P, and Q. |

 

## Proof Strategy: Disjunctions ($P \vee Q$)

| Strategy | Form | Description |
|---|---|---|
| **Disjunctions** | | |
| To prove a **goal** | $P \vee Q$ | Break your proof into cases.<br>In each case, either prove $P$ or prove $Q$. |
| To prove a **goal** | $P \vee Q$ | If $P$ is true, then clearly the goal $P \vee Q$ is true, so you only need to worry about the case in which $P$ is false. You can complete the proof in this case by proving that $Q$ is true.<br><br><u>Scratch Work:</u><br>*Givens* *Goal*<br>$\neg P$ $Q$ |
| To use a **given** | $P \vee Q$ | Break your proof into cases.<br>For case 1, assume that $P$ is true and use this assumption to prove the goal.<br>For case 2, assume $Q$ is true and give another proof of the goal.<br><br><u>Form:</u><br>Suppose ____.<br>Let x be an arbitrary element of ____.<br>Then either x ∈ ____ or x ∈ ____.<br>We will consider these cases separately.<br>Case 1. x ∈ ____. Then since ____, x ∈ ____. Case 2. x ∈ ____. Then since ____, x ∈ ____.<br>Since we know that either x ∈ ____ or x ∈ ____, these cases cover all the possibilities, so we can conclude that x ∈ ____.<br>Since x was an arbitrary element of ____, <this means / we can conclude> that ____. |
| To use a **given** | $P \vee Q$ | If you are also given $\neg P$, or you can prove that $P$ is false, then you can use this given to conclude that $Q$ is true.<br><br>Similarly, if you are given $\neg Q$ or can prove that $Q$ is false, then you can conclude that $P$ is true. |

## Proof Strategy: Induction

| Strategy | Form | Description |
|---|---|---|
| **Induction** | Natural Numbers | |
| To prove a **goal** | $\forall n \in N\ P(n)$ | Mathematical Induction :<br>Used with natural numbers.<br><br>First prove P(0) (base case).<br>Then prove ∀n ∈ N (P(n) → P(n + 1)) (induction steps).<br><br>Form:<br>We use mathematical induction.<br><br>**Base case**: Setting n = 0, we get [Proof of P(0) goes here] as required.<br><br>**Induction step**: Let n be an arbitrary natural number and suppose that [P(n) formula]. Then [Proof of ∀n ∈ N (P(n) → P(n + 1)) goes here.]<br><br>Therefore [P(n + 1)], as required. |
| To prove a **goal** | $\forall n \in N\ [(\forall k < n\ P(k)) \rightarrow P(n)]$ | Strong induction :<br>Used with sets and recursive procedures.<br><br>Form:<br>Same Form as above.<br><br>Example : "finite and nonempty" means that it has n elements, for some n ∈ N, n ≥ 1.<br><br>... by the inductive hypothesis [P(k)] ... |