Proof Techniques[1]

1 Basic Notation

The following is standard notation for proofs:

- $A \Rightarrow B$. A implies B.
- $A \Leftarrow B$. B implies A.
  Note that $A \Rightarrow B$ does not mean $B \Rightarrow A$. Example: If (A) a person eats two apples, she also (B) eats one apple. However, if (B) a person eats one apple, that does not imply that she also (A) eats two apples.
- $A \Leftrightarrow B$. A implies B and B implies A.
  Another way of saying this is that A holds if and only if (iff) B holds, or that A is equivalent to B.
- $\neg A$. Not A, or the negation of A.
  Example: If A is the event that $x \leq 10$, then $\neg A$ is the event that $x > 10$.

It is common to use mathematical symbols for words while writing proofs in order to write faster. The following are commonly used symbols:

$\forall$ For all, for any

$\exists$ There exists

$\in$ Is contained in, is an element of

$\ni$ Such that, contains as an element

$\subset$ Is a subset of

QED Latin for "quod erat demonstandum", or "which was to be proven". A common way to signal to the reader that you have successfully concluded your proof.

2 Proofs

We seek for ways to prove that $A \Rightarrow B$.

Remark 1 *When we want to prove a general statement then we need to prove it for the general case. When we want to disprove a statement it suffices to show an example where the statement fails.*

[1]Notes provided with gratitude to Maria Jose Boccardi.

2.1 Direct Proofs

2.1.1 Deductive Reasoning

A direct proof by deductive reasoning is a sequence of accepted axioms or theorems such that $A_0 \Rightarrow A_1 \Rightarrow A_2 \Rightarrow \cdots \Rightarrow A_{n-1} \Rightarrow A_n$, where $A = A_0$ and $B = A_n$. The difficulty is finding a sequence of theorems or axioms to fill the gaps.

Example: Prove the number three is an odd number.

Proof: A number q is odd if there exists an integer m such that $q = 2m + 1$. Let $m = 1$. Then $2m + 1 = 3$. Therefore three is an odd number. QED

2.1.2 Contrapositive

A contrapositive proof is just a direct proof of the negation. It makes use of the fact that the statement $A \Rightarrow B$ is equivalent to the statement $\neg B \Rightarrow \neg A$. For example, if (A) all people with driver's licenses are (B) at least 16 years old, then if you are not $(\neg B)$ 16 years old, then you do not $(\neg A)$ have a driver's license. So proving $A \Rightarrow B$ is really the same as proving $\neg B \Rightarrow \neg A$.

Example: Let x and y be two positive numbers. Prove that if $xy > 9$, then $x > 3$ or $y > 3$.

Proof: Suppose that both $x \leq 3$ and $y \leq 3$. Then $xy \leq 9$. QED (Here A: $xy > 9$, B: $x > 3$ or $y > 3$. In order to prove $A \Rightarrow B$ we proved $\neg B \Rightarrow \neg A$.)

2.2 Indirect Proofs

2.2.1 Contradiction

Suppose that we are trying to prove a proposition A, and we cannot prove it directly. However, we can show that all other alternatives to A are impossible. Then we have indirectly proved that A must be true. Therefore, the we can prove $A \Rightarrow B$ by first assuming that $A \not\Rightarrow B$ and finding a contradiction. In other words, we start off by assuming that A is true but B is not. If this leads to a contradiction, then either B was actually true all along, or A was actually false. But since we assume A is true, then it must be that B is true, and we have a proof by contradiction.

Example: Prove that $\sqrt{2}$ is an irrational number.

Proof: Suppose not. Then $\sqrt{2}$ is a rational number, so it can be expressed in the form $\frac{p}{q}$, where p and q are integers which are not both even. This implies that

$$2 = \frac{p^2}{q^2} \Rightarrow 2q^2 = p^2,$$

which implies that p^2 is even, which in turn implies that q^2 is not even. The fact that p^2 is even also implies that p is even, so there exists a integer m such that $2m = p$. This implies

$$4m^2 = p^2 = 2q^2 \Rightarrow q^2 = 2m^2,$$

which means that q is even, a contradiction. QED

2.2.2 Induction

Induction can only be used for propositions about integers or indexed by integers. Consider a list of statements indexed by the integers. Call the first statement $P(1)$, the second $P(2)$, and the nth statement $P(n)$. If we can prove the following two statements about the sequence, then every statement in the entire sequence must be true:

1. $P(1)$ is true.

2. If $P(k)$ is true, then $P(k+1)$ is true.

Induction works because by 1., $P(1)$ is true. By 2., $P(2)$ is true since $P(1)$ is true. Then $P(3)$ is true by 2. again, and so is $P(4)$ and $P(5)$ and $P(6)$, until we show that all the P's are true. Notice that the number of propositions need not be finite.

Example: Prove that the sum of the first n natural numbers is $\frac{1}{2}n(n+1)$.

Proof: Let $n = 1$. Then $\frac{1}{2}\cdot 1(1+1) = \sum_{j=1}^{1} j = 1$. Now let $n = k$, and assume that $\sum_{j=1}^{k} j = \frac{1}{2}k(k+1)$. We add $k+1$ to both sides to get

$$\sum_{j=1}^{k+1} j = \frac{1}{2}k(k+1) + k + 1 = \left(\frac{1}{2}k + 1\right)(k+1) = \frac{1}{2}(k+1)((k+1)+1).$$

QED

3 Examples

3.1 Existence of a utility function

Theorem 2 (Theorem 1 in Lecture Notes 1) *For any finite set X and complete choice correspondence $C : 2^X/\varnothing \to 2^X/\varnothing$, there exists a complete preference relation $\succeq$ that rationalizes that choice correspondence if and only if C satisfies property α and β.*

Proof. The first thing to do is note that this proof must come in two parts, as we are making two claims: this comes from the fact that the statement is "if and only if', so we have to show (i) that α and β imply that we can find a rationalizing preference relation and (ii) any rationalizable choice function satisfies α and β. We will start with the former, as this is the more tricky bit (in fact, we have already argued informally for the latter.) ■

Proof (axioms imply representation). We will break the proof down into the following steps

1. **Generate a candidate binary relation.** Our claim is that, if the choice correspondence satisfies α and β, then it is rationalizable by some complete preference relation. The first stage of the proof is to describe such a relation, which we will then show does the necessary job. We will define the relationship using choices from two objects by saying that $x \trianglerighteq y$ if and only if $x \in C(\{x, y\})$, so x is 'weakly preferred' to y (according to our candidate preference relation) if it is chosen from the set containing x and y only. We will stretch this definition somewhat by saying that $x \trianglerighteq x$, as x is definitionally chosen from the set $\{x\}$.

2. **Show that $\trianglerighteq$ is a complete preference relation.** So we have defined a binary relation. Great. However, our theorem demands that choices be rationalized by a complete preference relation - i.e. a complete, transitive, reflexive binary relation. We next need to show that $\trianglerighteq$ has these

properties. Reflexivity is easy - in fact we defined $\trianglerighteq$ explicitly so that it is reflexive. Completeness is also relatively straightforward. By definition, $C(\{x,y\})$ is either $\{x\}$, $\{y\}$ or $\{x,y\}$. Thus, by the construction of $\trianglerighteq$ either $x \trianglerighteq y$, $y \trianglerighteq x$ or both. Finally, we need to show transitivity, which we will do by contradiction. Imagine there exists $x,y,z \in X$ such that $x \trianglerighteq y \trianglerighteq z$ but not $x \trianglerighteq z$. This implies

$$\begin{aligned} x &\in C(\{x,y\}) \\ y &\in C(\{y,z\}) \\ x &\notin C(\{x,z\}) \end{aligned}$$

This in turn implies that $z \in C(\{x,z\})$. We can now show that we must have a violation of either property α or property β. Consider the set $\{x,y,z\}$. If $x \in C(\{x,y,z\})$, then the fact that $x \notin C(\{x,z\})$ is a direct violation of property α. If $y \in C(\{x,y,z\})$, then by property α, $y \in C(\{x,y\}) = \{x,y\}$. Property β then implies that $x \in C(\{x,y,z\})$, which we have already shown leads to a violation of α. If $z \in C(\{x,y,z\})$, then by α $z \in C(\{y,z\}) = \{y,z\}$, and so by β $y \in C(\{x,y,z\})$. Again, we have already shown that this leads to a violation. However, as $C(\{x,y,z\})$ is nonempty, one of these cases must occur, and so a failure of transitivity implies a failure of either α or β.

3. **Show that $\trianglerighteq$ rationalizes C.** We now need to show that, for all sets, our DM chooses as if they are maximizing $\trianglerighteq$. In other words, for some arbitrary $A \in 2^X/\varnothing$ we need to show that $C(A) = \{x \in A | x \trianglerighteq y \; \forall \; y \in A\}$. As we are proving the equality of two sets, this in itself takes two stages:

   (a) $C(A) \subseteq \{x \in A | x \trianglerighteq y \; \forall \; y \in A\}$. Say $x \in C(A)$. Take any $y \in A$. We need to show that $x \trianglerighteq y$ - in other words that $x \in C(\{x,y\})$. However, this follows directly from property α. Thus, anything that is chosen from A must be 'weakly preferred' to everything else in A.

   (b) $C(A) \supseteq \{x \in A | x \trianglerighteq y \; \forall \; y \in A\}$. Say $x \trianglerighteq y \; \forall \; y \in A$. Then, $x \in C(\{x,y\})$ for all $y \in A$. Now $C(A)$ must be non-empty, so either $x \in C(A)$ (in which case we are done), or $y \in C(A)$ for $y \neq x$. By property α, this implies that $\{x,y\} = C(\{x,y\})$, and so by property β, $x \in C(A)$.

This shows that properties α and β are sufficient for rationalizability ■

Proof (representation implies axioms). Homework ■

3.2 Example

Prove whether or not the following making decision procedures result in choices that satisfy α and β.

The DM has two utility rankings u and v over X, and a threshold v^*. In any choice set, they identify a^* as the element that maximizes u and b^* as the element that maximizes v. If $v(a^*) \geqslant v^*$ then they choose a^*, otherwise they choose b^*. (Can you think up a story for this procedure?)

[(a)-α] Assume that $x \in B \subseteq A$, and $x \in C(A)$. **We want to show that:** $x \in C(B)$.

In this case this decision procedure **does not** satisfy this property.

Counterexample Let's consider $A = x, y, z$ and $B = x, y$ such that $u(z) > u(y) > u(x)$, $v(z) < v^* < v(y)$, and $v(x) > v(y)$. Then $C(A) = x$ but $C(B) = y$

.

[(b)-β] Let's assume that $x, y \in C(A)$, $A \subseteq B$ and $y \in C(B)$. **We want to show that:** $x \in C(B)$.

In this case this decision procedure **does not** satisfy this property.

Counterexample. Let $A \equiv \{x, y\}$ and $B \equiv \{x, y, z\}$, such that $u(x) = u(y) = 2, u(z) = 3$ and $v(x) = 2, v(y) = 4$ and $v(z) = 1$, with $v^* = 2$.

We have that:

$\{x, y\} = \arg max_{a \in A} u(a)$

$v(x) = 2 \geqslant v^* = 2$

$v(y) = 4 \geqslant v^* = 2$,

Therefore $x, y \in C(A)$. [1]

On the other hand we have that:

$z = \arg max_{a \in B} u(a)$,

but $v(z) = 1 < 2 = v^*$ and $y = \arg max_{b \in B} v(b)$

Therefore $y \in C(B)$. [2]

From [1] and [2] and the fact that as they were defined $A \subseteq B$, property β would tell us that $x \in C(B)$, but since by assumption $v(y) > v(x)$ we have that $x \notin C(B)$.

What this DM is doing is basically to valuate a set of objects in terms of two different criteria. In that way he/she ranks the alternatives according to these two different rankings, given by functions u and v. At first, this DM only cares about the ranking that results from function u, that is, his/her priority is to choose whatever is best given u. But, he/she also cares about v in the sense that he/she prefers to choose an alternative that is at least as good as (in utility terms given by v) v^*. If it is not the case, then he/she decides taking into account the ranking given by v.