Proofs from axioms

David Gerard

2017-09-12

Learning Objectives

- Proving probability results from axioms

Recall: The Axioms of Probability

A **probability** on a sample space S (and a set $\mathcal{A}$ of events) is a function which assigns each event A (in $\mathcal{A}$) a value in $[0,1]$ and satisfies the following rules:

- **Axiom 1:** All probabilities are nonnegative:

$$P(A) \geq 0 \qquad \text{for all events } A.$$

- **Axiom 2:** The probability of the whole sample space is 1:

$$P(S) = 1.$$

- **Axiom 3 (Addition Rule):** If two events A and B are disjoint (have no outcomes in common) then

$$P(A \cup B) = P(A) + P(B),$$

The Complement Rule

The axioms are the fundamental building blocks of probability.
Any other probability relationships can be derived from the axioms.

Show that $P(A^c) = 1 - P(A)$

This proof asks us to confirm an equation
mathematical expression A = mathematical expression B

General form of a proof:

- First, write down any existing definitions or previously proven facts you can think of that are related to any formulas/symbols appearing in expressions A and B
- Start the proof with the left side (expression A) or with the most complex of the two expressions.
- Use algebra and established statistical facts to re-write this right-side expression until it equals the left-side

The Complement Rule

The axioms are the fundamental building blocks of probability.
Any other probability relationships can be derived from the axioms.

[Some knowledge of sets will be needed too.]

Show that $P(A^c) = 1 - P(A)$

The Complement Rule

The axioms are the fundamental building blocks of probability.
Any other probability relationships can be derived from the axioms.

[Some knowledge of sets will be needed too.]

Show that $P(A^c) = 1 - P(A)$

- A & A^c are disjoint (mutually exclusive, don't overlap).
  So, $P(A \cup A^c) = P(A) + P(A^c)$ (Axiom 3).

The Complement Rule

The axioms are the fundamental building blocks of probability.
Any other probability relationships can be derived from the axioms.

[Some knowledge of sets will be needed too.]

Show that $P(A^c) = 1 - P(A)$

- A & A^c are disjoint (mutually exclusive, don't overlap).
  So, $P(A \cup A^c) = P(A) + P(A^c)$ (Axiom 3).
- Also, $A \cup A^c = S$.
  So, $P(A \cup A^c) = P(S) = 1$ (Axiom 2).

The Complement Rule

The axioms are the fundamental building blocks of probability.
Any other probability relationships can be derived from the axioms.

[Some knowledge of sets will be needed too.]

Show that $P(A^c) = 1 - P(A)$

- A & A^c are disjoint (mutually exclusive, don't overlap).
  So, $P(A \cup A^c) = P(A) + P(A^c)$ (Axiom 3).
- Also, $A \cup A^c = S$.
  So, $P(A \cup A^c) = P(S) = 1$ (Axiom 2).
- Therefore, $P(A) + P(A^c) = 1$.

The Complement Rule

The axioms are the fundamental building blocks of probability.
Any other probability relationships can be derived from the axioms.

[Some knowledge of sets will be needed too.]

Show that $P(A^c) = 1 - P(A)$

- A & A^c are disjoint (mutually exclusive, don't overlap).
  So, $P(A \cup A^c) = P(A) + P(A^c)$ (Axiom 3).
- Also, $A \cup A^c = S$.
  So, $P(A \cup A^c) = P(S) = 1$ (Axiom 2).
- Therefore, $P(A) + P(A^c) = 1$.
- That is, $P(A^c) = 1 - P(A)$.

The Complement Rule

The axioms are the fundamental building blocks of probability.
Any other probability relationships can be derived from the axioms.

[Some knowledge of sets will be needed too.]

Show that $P(A^c) = 1 - P(A)$

- A & A^c are disjoint (mutually exclusive, don't overlap).
  So, $P(A \cup A^c) = P(A) + P(A^c)$ (Axiom 3).
- Also, $A \cup A^c = S$.
  So, $P(A \cup A^c) = P(S) = 1$ (Axiom 2).
- Therefore, $P(A) + P(A^c) = 1$.
- That is, $P(A^c) = 1 - P(A)$.

We only needed 1st step of proof algorithm this time - gather info.

Isn't $0 \leq P(A) \leq 1$? ...but Axiom 1 is just $P(A) \geq 0$.

The axioms are the fundamental building blocks of probability.

Any other probability relationships can be derived from the axioms.

Let's prove that $P(A) \leq 1$.

Isn't $0 \leq P(A) \leq 1$? ...but Axiom 1 is just $P(A) \geq 0$.

The axioms are the fundamental building blocks of probability.

Any other probability relationships can be derived from the axioms.

Let's prove that $P(A) \leq 1$.

- By the complement rule, $1 - P(A) = P(A^c)$

Isn't $0 \leq P(A) \leq 1$? ...but Axiom 1 is just $P(A) \geq 0$.

The axioms are the fundamental building blocks of probability.

Any other probability relationships can be derived from the axioms.

Let's prove that $P(A) \leq 1$.

- By the complement rule, $1 - P(A) = P(A^c)$
- and $P(A^c) \geq 0$ (Axiom 1).

Isn't $0 \leq P(A) \leq 1$? ...but Axiom 1 is just $P(A) \geq 0$.

The axioms are the fundamental building blocks of probability.

Any other probability relationships can be derived from the axioms.

Let's prove that $P(A) \leq 1$.

- By the complement rule, $1 - P(A) = P(A^c)$
- and $P(A^c) \geq 0$ (Axiom 1).
- So, $1 - P(A) \geq 0 \implies 1 \geq P(A)$.

Some more probability facts

We can also prove ...

- The Law of Total Probability = Partition Rule

$$P(A) = P(A \cap B) + P(A \cap B^c)$$
$$\text{or}\;\; P(A) = P(A \cap B) + P(\text{``}A - B\text{''})$$

- The Inclusion-Exclusion Formula

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

- Probability for subsets If $A \subseteq B$, then $P(A) \leq P(B)$

  Let's try to prove the last one.

Proving a Conditional Statement

If $A \subseteq B$, then $P(A) \leq P(B)$

This proof asks us to confirm a conditional statement:
If statement A is true, then statement B must also be true
(the opposite direction might not hold)

General form of a proof:

- First, review existing definitions or previously proven facts related to statements A and B
- Start the proof by stating that statement A is true
- Use algebra and established statistical facts to write a series of "then" statements that logically follow from statement A; eventually leading logically to statement B

Proving a Conditional Statement

The axioms are the fundamental building blocks of probability.
Any other probability relationships can be derived from the axioms.

[Some knowledge of sets will be needed too.]

Show that if $A \subseteq B$, then $P(A) \leq P(B)$

Suppose $A \subseteq B$.

Proving a Conditional Statement

The axioms are the fundamental building blocks of probability.
Any other probability relationships can be derived from the axioms.

[Some knowledge of sets will be needed too.]

Show that if $A \subseteq B$, then $P(A) \leq P(B)$

Suppose $A \subseteq B$.

- Then, $A \cap B = A$

Proving a Conditional Statement

The axioms are the fundamental building blocks of probability.
Any other probability relationships can be derived from the axioms.

[Some knowledge of sets will be needed too.]

Show that if $A \subseteq B$, then $P(A) \leq P(B)$

Suppose $A \subseteq B$.

- Then, $A \cap B = A$
- Always true: $P(A \cap B) + P(A^c \cap B) = P(B)$
  (law of total probability)

Proving a Conditional Statement

The axioms are the fundamental building blocks of probability.
Any other probability relationships can be derived from the axioms.

[Some knowledge of sets will be needed too.]

Show that if $A \subseteq B$, then $P(A) \leq P(B)$

Suppose $A \subseteq B$.

- Then, $A \cap B = A$
- Always true: $P(A \cap B) + P(A^c \cap B) = P(B)$ (law of total probability)
- So, $P(A) + P(A^c \cap B) = P(B)$

Proving a Conditional Statement

The axioms are the fundamental building blocks of probability.
Any other probability relationships can be derived from the axioms.

[Some knowledge of sets will be needed too.]

Show that if $A \subseteq B$, then $P(A) \leq P(B)$

Suppose $A \subseteq B$.

- Then, $A \cap B = A$
- Always true: $P(A \cap B) + P(A^c \cap B) = P(B)$
  (law of total probability)
- So, $P(A) + P(A^c \cap B) = P(B)$
- and $P(A) \leq P(A) + P(A^c \cap B)$
  since $P(A^c \cap B) \geq 0$ (Axiom 1)

Proving a Conditional Statement

The axioms are the fundamental building blocks of probability.
Any other probability relationships can be derived from the axioms.

[Some knowledge of sets will be needed too.]

Show that if $A \subseteq B$, then $P(A) \leq P(B)$

Suppose $A \subseteq B$.

- Then, $A \cap B = A$
- Always true: $P(A \cap B) + P(A^c \cap B) = P(B)$
  (law of total probability)
- So, $P(A) + P(A^c \cap B) = P(B)$
- and $P(A) \leq P(A) + P(A^c \cap B)$
  since $P(A^c \cap B) \geq 0$ (Axiom 1)
- Putting everything together... $P(A) \leq P(B)$