CSC B36 Additional Notes

what you should know about proofs

⋆ Introduction

These notes summarize what students should know about proofs.
For use in examples, we define a function $f : \mathbb{R} \to \mathbb{R}$ by

$$f(x) = x^2 - 10x + 27.$$

⋆ What is a proof?

A proof is a convincing argument. The meaning of "convincing" depends on the intended audience of the proof. When writing a proof of a statement S, we should always start with something that is known, then give a sequence of logical arguments leading to the conclusion that S is true. Each step, where appropriate, should be justified.

Example 1:

We prove the statement: $f(7) = 7 - 1$.

$$\begin{aligned} f(7) &= (7)^2 - 10(7) + 27 && \text{[definition of } f\text{]} \\ &= 49 - 70 + 27 && \text{[basic arithmetic]} \\ &= 6 && \text{[basic arithmetic]} \\ &= 7 - 1 && \text{[basic arithmetic]} \end{aligned}$$

Therefore $f(7) = 7 - 1$. □

⋆ Direct Proofs

A direct proof of a statement S is a proof whose structure reflects the structure of S. The simplest statement is one that can be expressed logically without quantifier or logic symbols (e.g., $\forall$, $\exists$, $\wedge$, $\vee$, $\neg$, $\rightarrow$, etc). These are called atomic statements. Example 1 shows a direct proof of an atomic statement. For statements with quantifier and/or logic symbols, the structure of a direct proof depends on the outermost such symbol. We now consider some common direct proofs.

◦ Direct Proof of a Conjunction

Let S be a statement of the form $P \wedge Q$ ("P AND Q"), where P and Q are statements. Then a direct proof of S consists of two "smaller" proofs, namely a proof of P and a proof of Q. The smaller proofs need not be direct proofs.

Structure of a direct proof of $P \wedge Q$:

[proof of P]
Hence P.

[proof of Q]
Hence Q.

Therefore $P \wedge Q$. □

Example 2:

We prove the statement: $(f(2) = 11) \wedge (f(9) < f(10))$.

$f(2) = (2)^2 - 10(2) + 27$ [definition of f]
$= 4 - 20 + 27$ [basic arithmetic]
$= 11$ [basic arithmetic]

Hence $f(2) = 11$.

$f(9) = (9)^2 - 10(9) + 27$ [definition of f]
$= 9(9 - 10) + 27$ [basic algebra]
$< 10(10 - 10) + 27$ [replace 9 by 10, which is larger]
$= 10^2 - 10(10) + 27$ [basic algebra]
$= f(10)$ [definition of f]

Hence $f(9) < f(10)$.

Therefore $(f(2) = 11) \wedge (f(9) < f(10))$. □

◦ **Direct Proof of an Implication**

Let S be a statement of the form $P \to Q$ ("IF P THEN Q", or "P IMPLIES Q"), where P and Q are statements. Then a direct proof of S starts by assuming P, then proves Q under that assumption. The proof of Q need not be a direct proof.

Structure of a direct proof of $P \to Q$:

Assume P.
[proof of Q under assumption of P]
Hence Q.

Therefore $P \to Q$. □

Example 3:

We prove the statement: $(f(9) > 864) \to (f(10) > 864)$.

Suppose $f(9) > 864$.
Then $f(10) > f(9)$ [proved in example 2]
> 864 [our assumption]
Hence $f(10) > 864$.

Therefore $(f(9) > 864) \to (f(10) > 864)$. □

Note: If S is a statement of the form $P \leftrightarrow Q$ ("P IF AND ONLY IF Q"), then a direct proof of S consists of two smaller proofs, namely a proof of $P \to Q$ and a proof of $Q \to P$. This is because $P \leftrightarrow Q$ is logically the same as $(P \to Q) \wedge (Q \to P)$, and we are simply treating S as the conjunction of two statements. The smaller proofs need not be direct proofs.

Aside: Here are some interesting questions to ponder.

1. Is it true that $f(10) > 864$?
2. Is it true that $(f(9) > 864) \to (f(10) > 864)$?
3. Is the proof in example 3 correct?

◦ **Direct Proof of a Universally Quantified Statement**

Let S be a statement of the form $\forall x \in D$, $P(x)$, where D is some domain and P is some predicate on D (i.e., a statement about an element in D). Then a direct proof of S starts by letting x be an *arbitrary* element of D, then proves $P(x)$. The proof of $P(x)$ need not be a direct proof.

Structure of a direct proof of $\forall x \in D,\ P(x)$:

Let $x \in D$ be arbitrary.
[proof of $P(x)$]
Hence $P(x)$.

Therefore $\forall x \in D,\ P(x)$. □

Example 4:

We prove the statement: $\forall x \in \mathbb{R},\ f(x) \geq 2$.

Let $x \in \mathbb{R}$ be arbitrary (i.e., let x be an arbitrary real number).

Then $f(x)$	$= x^2 - 10x + 27$	[definition of f]
	$= x^2 - 10x + 25 - 25 + 27$	[add and subtract 25]
	$= (x-5)^2 + 2$	[$x^2 - 10x + 25 = (x-5)^2$, $-25 + 27 = 2$]
	≥ 2	[$(x-5)^2 \geq 0$]

Hence $f(x) \geq 2$.

Therefore $\forall x \in \mathbb{R},\ f(x) \geq 2$. □

◦ Direct Proof of an Existentially Quantified Statement

Let S be a statement of the form $\exists x \in D,\ P(x)$, where D is some domain and P is some predicate on D (i.e., a statement about an element in D). Then a direct proof of S starts by letting x be some *specific* element of D, then proves $P(x)$. The proof of $P(x)$ need not be a direct proof.

Structure of a direct proof of $\exists x \in D,\ P(x)$:

Let $x \in D$ be _____ (*here we give some specific value for x*).
[proof that $x \in D$ — often this is quite obvious]
Then $x \in D$.

[proof of $P(x)$]
Hence $P(x)$.

Therefore $\exists x \in D,\ P(x)$. □

Example 5:

We prove the statement: $\exists x \in \mathbb{R},\ f(x) = 2$.

Let $x = 5$.
Then $x \in \mathbb{R}$. (too obvious to merit justification)

Also, $f(x)$	$= f(5)$	[$x = 5$]
	$= (5)^2 - 10(5) + 27$	[definition of f]
	$= 25 - 50 + 27$	[basic arithmetic]
	$= 2$	[basic arithmetic]

Hence $f(x) = 2$.

Since $5 \in \mathbb{R}$ and $f(5) = 2$, therefore $\exists x \in \mathbb{R},\ f(x) = 2$. □

⋆ Indirect Proofs

Here are two ways to view an indirect proof of a statement S.

- It is a proof which is not a direct proof (i.e., its proof structure does not reflect that of S).
- It is a direct proof of a statement which is logically equivalent to S.

We now consider some common indirect proofs.

◦ Proof by Contradiction

A contradiction arises when some statement P is shown to be both true and false. I.e., both P and $\neg P$ ("NOT P", the negation of P) are shown to be true. To prove a statement S by contradiction, we start by assuming that S is false (or that $\neg S$ is true), then argue for a contradiction. In effect, we give a direct proof of the statement $\neg S \to$ FALSE, which is logically equivalent to S.

Structure of a proof of S by contradiction:

Assume S is false.
[derive some contradictory statements P and $\neg P$ under assumption of $\neg S$]
Hence P and $\neg P$ (a contradiction).

Therefore S. □

Example 6:

We prove by contradiction the statement: $f(10) > 10$.

By way of contradiction, suppose $f(10) \leq 10$.

Then $f(10) \leq 18$	$[10 < 18]$.	**(*)**
Also, $f(10) > f(9)$	[proved in example 2]	
$= (9)^2 - 10(9) + 27$	[definition of f]	
$= 81 - 90 + 27$	[basic arithmetic]	
$= 18$	[basic arithmetic].	**(**)**

Hence $(f(10) \leq 18)$ and $(f(10) > 18)$ [by (*) and (**)], which is a contradiction.

Therefore $f(10) > 10$. □

◦ Proof of an Implication by Proving its Contrapositive

We can prove a statement of the form $P \to Q$ by giving a direct proof of its contrapositive, $\neg Q \to \neg P$, which is logically equivalent to $P \to Q$.

Structure of a proof of $P \to Q$ by a proof of its contrapositive:

Assume Q is false (or $\neg Q$ is true).
[under assumption of $\neg Q$, prove P is false (or $\neg P$ is true)]
Hence $\neg P$.

Therefore $\neg Q \to \neg P$, or equivalently, $P \to Q$. □

Example 7:

We prove, by proving the contrapositive, the statement: $(f(9) > 864) \to (f(10) > 864)$.
(This is the same statement as in example 3.)

By way of contraposition, suppose $f(10) \leq 864$.

Then $864 \geq f(10)$	[our assumption]
$> f(9)$	[proved in example 2]

Hence $f(9) \leq 864$.

Therefore $(f(10) \leq 864) \to (f(9) \leq 864)$, or equivalently, $(f(9) > 864) \to (f(10) > 864)$. □

◦ **Proof by Cases**

Suppose we have n statements $C_1, \cdots, C_n$ and we know, or can prove, that $(C_1 \vee \cdots \vee C_n)$ is true. Then we can prove a statement S by giving n proofs, one each for $C_1 \to S$, $\cdots$, $C_n \to S$. Such a proof is called a proof by cases. By giving these n proofs, we prove (directly) that

$$(C_1 \to S) \wedge \cdots \wedge (C_n \to S),$$

which is logically equivalent to

$$(C_1 \vee \cdots \vee C_n) \to S,$$

which in turn is logically equivalent to S since $(C_1 \vee \cdots \vee C_n)$ is true.

Structure of a proof of S by cases:

[proof of $C_1 \to S$]
Hence $C_1 \to S$.

$\vdots$

[proof of $C_n \to S$]
Hence $C_n \to S$.

Since $(C_1 \vee \cdots \vee C_n)$ is true, therefore S. □

Example 8:

We prove by cases the statement "$987^2 \bmod 4 \neq 3$".

Consider the 4 values that $987 \bmod 4$ can take on, namely $0, 1, 2, 3$.

Suppose $987 \bmod 4 = 0$.

Then $987^2 \bmod 4$	$= 0^2 \bmod 4$	[by our assumption and modulo arithmetic]
	$= 0 \bmod 4$	[basic arithmetic]
	$\neq 3$	(too obvious to merit justification)

Hence $987^2 \bmod 4 \neq 3$.

Suppose $987 \bmod 4 = 1$.

Then $987^2 \bmod 4$	$= 1^2 \bmod 4$	[by our assumption and modulo arithmetic]
	$= 1 \bmod 4$	[basic arithmetic]
	$\neq 3$	(too obvious to merit justification)

Hence $987^2 \bmod 4 \neq 3$.

Suppose $987 \bmod 4 = 2$.

Then $987^2 \bmod 4$	$= 2^2 \bmod 4$	[by our assumption and modulo arithmetic]
	$= 4 \bmod 4$	[basic arithmetic]
	$= 0$	[modulo arithmetic]
	$\neq 3$	(too obvious to merit justification)

Hence $987^2 \bmod 4 \neq 3$.

Suppose $987 \bmod 4 = 3$.

Then $987^2 \bmod 4$	$= 3^2 \bmod 4$	[by our assumption and modulo arithmetic]
	$= 9 \bmod 4$	[basic arithmetic]
	$= 1$	[modulo arithmetic]
	$\neq 3$	(too obvious to merit justification)

Hence $987^2 \bmod 4 \neq 3$.

Since $987 \bmod 4$ must equal one of 0, 1, 2 or 3, therefore $987^2 \bmod 4 \neq 3$. □

⋆ Proof of a Disjunction

Let S be a statement of the form $P \vee Q$ ("P OR Q"), where P and Q are statements. Then a direct proof of S would simply consist of one "smaller" proof, namely either a proof of P or a proof of Q. However, in many cases a direct proof is not possible (can you see why?), so we turn to indirect proofs. We can prove $P \vee Q$ indirectly by providing a direct proof of one of these logically equivalent statements (both are implications).

(a) $\neg P \to Q$.

(b) $\neg Q \to P$.

We can also prove $P \vee Q$ by cases. Notice that if we choose our cases to be P and $\neg P$, then the first case, $P \to (P \vee Q)$, becomes trivial, and the second case, $\neg P \to (P \vee Q)$, is equivalent to implication (a) above.

Finally we can prove $P \vee Q$ by contradiction. Here we would assume that $P \vee Q$ is false (or that $\neg P \wedge \neg Q$ is true), then seek a contradiction. Notice how this proof is essentially the same as a direct proof of $\neg P \to Q$ if the proof of Q (under the assumption of $\neg P$) is by contradiction. Both proofs involve finding a contradiction on the assumption that both P and Q are false.

⋆ Important for this course!

In this course, you must begin indirect proofs by stating the type of proof you intend to use. Here are some examples for how you should introduce such proofs.

- For a Proof by Contradiction:
  By way of contradiction, suppose *[negation of what you want to prove]*.
- For a Proof by Contraposition:
  By way of contraposition, suppose *[negation of "then" part of implication you want to prove]*.
- For a Proof by Cases:
  We consider the cases *[description of your cases]*.