Term Paper, Option 1

(1) What are proofs and their purposes

Proofs are the logical justification for a proposition to hold, built upon axioms and preceding/already proven theorems, with each individual line and reasoning holding true themselves. Proofs provide a rigorous and accessible means of evidence to which we can explore, share, and uncover the fundamental truths of logic and numbers. We may have an intuitive understanding that something is true, but a proof provides undeniable justification that conjecture indeed holds. And by writing proofs, we are able to share our findings with colleagues, preserve them for future mathematicians, and allow for the progress for more advanced mathematics by adding to the set of theorems that can be used in proofs. Therefore, proofs are the instrument and the building blocks in which we can explore the beauty of mathematical truth and allow us to uncover and definitely test such truths.

(2) The importance and limitations of proofs

Proofs reveal truth, and thus provide absolute consistently with statements proven to be true which is extremely useful. For example, for computer algorithms, and more specifically for building a computer CPU, if we were to build a component for a bit-wise logical "XOR" ($\oplus$) operation, assuming we have "AND" ($\wedge$) and "NOT" ($\sim$) components to work with, we can get an implementation like

$$x \oplus y \equiv \sim (\sim (\sim x \wedge y) \wedge \sim (x \wedge \sim y)).$$

But how do check if we implemented it correctly, one way is to take every combination of x and y and XORing them together and checking with our implantation with every length of bit strings e.i. "0001, 0010, 0011,..., 10010010101,..." or waiting until the machine breaks. The first is computationally impossible and the ladder is also not optimal either, we want to know if the logic is constant and correct, and thus a proof would be much more effective. To prove that our implementation is correct, we notice that bits are independent from each other when ANDed or NOTed together:

$$0110 \wedge 1001 = 0000$$

$$0 \wedge 1 = 0 \quad 1 \wedge 0 = 0 \quad 1 \wedge 0 = 0 \quad 0 \wedge 1 = 0$$

$$\sim 1011 = 0100$$

$$\sim 1 = 0 \quad \sim 0 = 1 \quad \sim 1 = 0 \quad \sim 1 = 0$$

Thus we can use a truth table with just single bits:

x	y	$\sim x$	$\sim y$	$\sim (\sim x \wedge y)$	$\sim (x \wedge \sim y)$	$\sim (\sim (\sim x \wedge y) \wedge \sim (x \wedge \sim y))$
1	1	0	0	1	1	0
1	0	0	1	1	0	1
0	1	1	0	0	1	1
0	0	1	1	1	1	0

x	y	$x \oplus y$
1	1	0
1	0	1
0	1	1
0	0	0

Therefore we have show that indeed our implementation of "XOR" is indeed logically equivalent to "XOR" for every combination of bits (1's or 0's) and so if we implemented this in our CPU have proved that this implementation works and there will be no errors or faults in our system. Here is the power and importance of proofs, we can assure logical consistently and correct implementations and thus saving time and potential, harmful mistakes.
Although proofs are extremely powerful, in many "real-world"/material applications there are many limitations. First proofs need to have a controlled and limited setting in which the physical world is not, for example if someone wanted to prove that the price of a stock will to up 0.02% the next day they might look at trends which are not proofs but observation, then you would have to predict/prove the behavior of all people who own said stock, and how their mood and thoughts are affected by the people around them, the food they ate, genetic factors, and maybe even a pebble that someone will step on that will anger them, etc. The point is that it is an inconceivable task to prove that the proposition "The stock 'X' will increase by 0.02% by tomorrow," holds due to the nature reality with so many inter-playing variables. A even better example may be the weather forecast, where the predictions are often wrong and can predict only into the immediate future, again as a consequence of a chaotic system with trillions of factors. Another limitation of proofs its the translation to the material world. We have proved that many CPU's are Turing Compete, meaning that any computational problem can be solved by said CPU, but doing so on these would take infinite memory and time, thus proof of something's feasibility does all for it to exist without the constants of current technology and understanding of physical laws.

(3) Different types of proofs and how to construct them (you should mention at least the following four kinds: direct proof, proof by mathematical induction, proof by contrapositive, and proof by contradiction.)
Assume we have the propositional statement, "if P then Q", i.e. $P \implies Q$, where "P" and "Q" are propositional statements themselves. Here are the different ways you would construct a proof to show that $P \implies Q$ holds.
Direct Proof: A direct proof, as the name suggests, is straightforward with no changes to our propositions, constructed by assuming that the given P holds and show that Q holds from that, thus proving that $P \implies Q$ holds.
Proof by Contrapositive To construct a proof by contrapositive we would take the contrapositive of the implication to get $\sim Q \implies \sim P$. Then to prove this contrapositive we should assume $\sim Q$ holds and show that $\sim P$ holds. Then we can say that the original implication, $P \implies Q$, holds since the contrapositive is logical equivalent the original implication.
Proof by Contradiction A proof by contradiction would be set up by negating what we want to prove and assume that holds. So our new, assumed implication would be $\sim (P \implies Q)$. Then P must be true and Q be false since that is the only way for $P \implies Q$ to be false and $\sim (P \implies Q)$ to hold true. Then from P being true and Q being false, we go through the steps until we any two contradictory statements to thus prove your original $P \implies Q$ to be true.
Proof by Mathematical Induction This type of proof does not necessarily prove the same form of propositions as the ones above. A proof by mathematical induction is used to prove a proposition with some relation to the natural numbers, e.x. $P(n) \equiv n^2 + 1 \geq 2n \; \forall n \in \mathbb{N}$. To prove our $P(n)$ with mathematical induction, we would need to establish that the first

number in our bounds of n holds, in this case 1. So we have to prove that $P(1)$ holds which would be our case case. Then we have our inductive hypothesis which assumes that $P(k)$ holds for some arbitrary number k within the bounds of n . Now we need to complete our inductive step and show that $P(k) \implies P(k+1)$ holds true. Finally, if all these steps are complete, we can say that $P(n)$ holds for all n in your bounds of $\mathbb{N}$ by the Principle of Mathematical Induction. An intuitive understanding of this is that of domino's falling, if the first one falls (base case), assuming any domino falls (our inductive hypothesis), and if some domino fell then it hits the next one and the next falls (inductive step), then all the domino's fall, since we hit the first one, which hits the second, then the third, etc.

HW 02, Problem 4

Prove

$$1^3 + 2^3 + ... + n^3 = (1 + 2 + ... + n)^2$$

for all n $\in \mathbb{N}$.

Proof. Let $P(n)$ be "$1^3 + 2^3 + ... + n^3 = (1 + 2 + ... + n)^2$" for some $n \in \mathbb{N}$
Base Case: When $n = 1$. So, the left hand side of $P(1)$ is $1^3 = 1$ and the right hand side is $(1)^2 = 1$, thus the left hand side and right hand side are equal so $P(1)$ holds and the base case holds.
Inductive Hypothesis: Suppose $P(k)$ hold for arbitrary $k \in \mathbb{N}$.
Inductive Step: From our inductive hypothesis we know that

$$1^3 + 2^3 + ... + k^3 = (1 + 2 + ... + k)^2 \qquad (\heartsuit)$$

holds. We also know that

$$(k+1)^3 = (k^2 + 2k + 1)(k + 1)$$

$$= k^3 + 2k^2 + k + k^2 + 2k + 1$$

by distributing. Now we can distribute out a k to get

$$k(k^2 + 2k + 1) + k^2 + 2k + 1.$$

Then by factoring again we get

$$k(k+1)^2 + (k+1)^2.$$

We can distribute a $k + 1$ from the left term and it multiply by $1 = 2/2$ to get

$$2 \cdot \frac{k(k+1)}{2} \cdot (k+1) + (k+1)^2.$$

Now we can use $\dfrac{k(k+1)}{2} = 1+2+...+k$, which was proven in class, as a substitution above to get

$$2 \cdot (1 + 2 + ... + k) \cdot (k+1) + (k+1)^2.$$

Thus we have shown that

$$(k+1)^3 = 2 \cdot (1+2+...+k) \cdot (k+1) + (k+1)^2. \qquad (\clubsuit)$$

Now we can combine ($\heartsuit$) and ($\clubsuit$) with addition to get

$$1^3 + 2^3 + ... + k^3 + (k+1)^3 = (1+2+...+k)^2 + 2 \cdot (1+2+...+k) \cdot (k+1) + (k+1)^2.$$

Now from the binomial theorem we know that $a^2 + 2 \cdot a \cdot b + b^2 = (a+b)^2$, now lets use this on the right hand side of the equation above with $a = 1+2+...+k$ and $b = k+1$ to get

$$1^3 + 2^3 + ... + k^3 + (k+1)^3 = (1+2+...+k+k+1)^2.$$

Thus we have proved that $P(k+1)$ holds and thus we have finished our inductive step. Therefore, by the Principle of Mathematical Induction, $P(n)$ holds for all $n \in \mathbb{N}$. ■

HW 05, Problem 1

Let A be a bounded nonempty subset of $\mathbb{R}$, $\beta \in \mathbb{R}$ and $\beta < 0$. Let $\beta A = \{\beta a : a \in A\}$. Prove that

$$sup(\beta A) = \beta inf(A).$$

Let A be a bounded nonempty subset of $\mathbb{R}$, $\beta \in \mathbb{R}$ and $\beta < 0$. Let $\beta A = \{\beta a : a \in A\}$. Prove that

$$sup(\beta A) = \beta inf(A).$$

Do not use Proposition 1.2.6.

Proof. We know $inf(A)$ exists since A is bounded and non-empty, which also means the set βA is non-empty. Now, for all $y \in \beta A$, $\exists x \in A$, such that $y = \beta x$. Then since $inf(A)$ is a lower bound of A and x is in A, we get

$$x \geq inf(A).$$

Since we are given that $\beta < 0$, when we multiply by β to the inequality, the sign flips sides, giving us

$$\beta x \leq \beta inf(A).$$

Then we can replace the right hand side with $y = \beta x$ which gives us

$$y \leq \beta inf(A).$$

Thus we can say that for all $y \in \beta A$, $y \leq \beta inf(A)$ and thus by the definition of upper bound, $\beta inf(A)$ is an upper bound of βA. Then, since $sup(\beta A)$ is the least upper bound of βA, and $\beta inf(A)$ is an upper bound of βA we can say that

$$sup(\beta A) \leq \beta inf(A). \qquad \text{Inequality 1}$$

Now for all $x \in A$, $\beta x \in \beta A$ by the definition of set βA. Since $\beta x \in \beta A$ and $sup(\beta A)$ is an upper bound of βA, we can say that

$$\beta x \leq sup(\beta A).$$

We also know that $\frac{1}{\beta} < 0$ since $\beta < 0$, and thus when we multiply the inequality by $\frac{1}{\beta}$ we flip the direction of the inequality sign, giving us

$$\frac{1}{\beta}\beta x \geq \frac{1}{\beta} sup(\beta A).$$

Now by the existence of a multiplicative inverse and then by identity property of multiplication we can simplify the $\frac{1}{\beta}\beta$ on the left hand side to get

$$x \geq \frac{1}{\beta} sup(\beta A).$$

Thus, for all $x \in A$, $x \geq \frac{1}{\beta} sup(\beta A)$ and by the definition of lower bound, $\frac{1}{\beta} sup(\beta A)$ is a lower bound of A. Now since $inf(A)$ is the greatest lower bound of A and $\frac{1}{\beta} sup(\beta A)$ is a lower bound of A, it means that

$$\frac{1}{\beta} sup(\beta A) \leq inf(A)$$

Then since $\beta < 0$, when we multiply the inequality by β we flip the direction of the inequity to get

$$\beta \frac{1}{\beta} sup(\beta A) \geq \beta inf(A)$$

Now by the existence of a multiplicative and then by identity property of multiplication we can simplify the left hand side $\beta \frac{1}{\beta} sup(\beta A)$ to get

$$sup(\beta A) \geq \beta inf(A) \qquad \text{Inequality 2}$$

Then when we combine Inequality 1 with Inequality 2 it must hold that $sup(\beta A) = \beta inf(A)$. ■

HW 05, Problem 7

For each $n \in \mathbb{N}$, let $I_n = (-\infty, -n]$. Show that $\bigcap_{n=1}^{\infty} I_n = \emptyset$.

Proof. We will prove this through contradiction.
Suppose that that $\bigcap_{n=1}^{\infty} I_n$ is not empty. Thus by the definition of $\bigcap_{n=1}^{\infty} I_n$ there exists a x in I_n for all n in $\mathbb{N}$, and by the definition of $I_n = (-\infty, -n]$, there exists an x in $\mathbb{R}$ such that

$$x \leq -n \qquad \text{for all n in } \mathbb{N}$$

Then we multiply both sides by -1 which flips the sign of the inequality and gives us

$$-x \geq n \qquad \text{for all n in } \mathbb{N}$$

We know that $-x$ is in $\mathbb{R}$ since x is in $\mathbb{R}$. So there exists a $-x$ in $\mathbb{R}$ for all $n \in N$ such that $-x \geq n$, this is a clear contradiction to the Archimedean Property which states that for all t in $\mathbb{R}$ there exists an n_t in $\mathbb{N}$ such that $n_t > t$. Thus since $-x$ is in $\mathbb{R}$, there is a contraction with $-x \geq n$ for all n in $\mathbb{N}$, and there exists an n_t in $\mathbb{N}$ such that $n_t > -x$. Therefore it must hold that $\bigcap_{n=1}^{\infty} I_n = \emptyset$. ■

HW 10, Problem 7

Suppose that $a_n \geq 0$ for every $n \in \mathbb{N}$. Prove that, if $\sum_{n=1}^{\infty} a_n^2$ is a divergent series, then $\sum_{n=1}^{\infty} a_n$ is also a divergent series.

Proof. Lets do a proof by contrapositive, so let us assume that $\sum_{n=1}^{\infty} a_n$ is convergent and show that $\sum_{n=1}^{\infty} a_n^2$ is a convergent series. Since we know that $\sum_{n=1}^{\infty} a_n$ is convergent, then by the n-th term test, $\lim_{n\to\infty} a_n = 0$ and thus $\{a_n\}$ is a convergent sequence. Now, by Theorem 24, since $\{a_n\}$ is a convergent sequence, $\{a_n\}$ is bounded. Thus there exists a $u \in \mathbb{R}$ such that $a_n \leq u$ for all $n \in \mathbb{N}$, combing this with our given $a_n \geq 0$ for every $n \in \mathbb{N}$, we get

$$0 \leq a_n \leq u.$$

We multiply all sides by a_n to get

$$0 \leq a_n^2 \leq u \cdot a_n. \qquad (\spadesuit)$$

Now, we know from the linearity of series that since $\sum_{n=1}^{\infty} a_n$ is convergent, $\sum_{n=1}^{\infty} u \cdot a_n$ is also convergent. Now by the comparison test with $(\spadesuit)$, we get that $\sum_{n=1}^{\infty} a_n^2$ is a convergent series. Therefore, by our proof by contrapositive, it holds that if $\sum_{n=1}^{\infty} a_n^2$ is a divergent series, then $\sum_{n=1}^{\infty} a_n$ is a divergent series. ■

All of my knowledge on subjects in this paper has come from my understanding of previous and current classes at the University of Pittsburgh.
CS 0441 with Dr. Garrison
CS 0449 with with Dr. Olivera
MATH 0413 with Dr. Yibiao Pan