1 Monday, January 26

1.1 Rosen 1.7 — Introduction to Proofs

Reading: Rosen 1.7. LLM 1.3, 1.4, 1.5. Ducks 1.4.

Theorems that are meant for human consumption are almost always *informal proofs*, where we combine multiple rules of inference in a single step! Makes that proof about Knights and Knaves from the previous section much quicker! We can also sometimes not explicitly state all axioms or premises, expecting the reader to already accept those statements.

Definitions: *theorem* (*proposition*, *fact*, *result*), *proof*, *axioms* (*postulates*), *lemma*, *corollary*, *conjecture*.

Note: There is a difference between *axioms* and *definitions*. An *axiom* is a statement that is accepted as truth, such as "0 is a number." "If n is a number, then $n + 1$ is a number." (Trust me, these are important axioms.) However, a *definition* is a way to compact complicated propositions into a single word.

Def: An integer n is *odd* if it can be expressed as $n = 2k + 1$ for some integer k. An integer n is *even* if it can be expresses as $n = 2k$ for some integer k.

Remark: We will accept *for now* that every integer is either odd or even (and exactly one). To prove this fact requires using *induction*.

Note: A lot of our example propositions will be using language of real numbers and integers, including algebraic manipulations (such as addition, multiplication, powers, absolute value etc.) and comparisons (inequalities). In order to prove these statements, we will use all of your high-school level mathematics as previous knowledge. Thus, we can use these facts to our benefit.

Theorems are stated using natural language, not the symbolic form that we have been using.

1.1.1 Direct Proof

A *direct proof* of a statement "$p \to q$" is to assume that p is true, follow rules of inference, and conclude that q is true. This truly demonstrates "If p, then q."

Ex: Give a direct proof of the statement "If $m + n$ and $n + p$ are even, then $m + p$ is even."

Proof. Since $m + n$ is even, there exists an integer k such that $m + n = 2k$. Since $n + p$ is even, there exists an integer ℓ such that $n + p = 2\ell$. Therefore,

$$(m + p) = (m + n) + (n + p) - 2n = 2k + 2\ell - 2n = 2(k + \ell - n).$$

Since $k + \ell - n$ is an integer, $m + p$ is even. □

Ex: Give a direct proof of the statement "If n is even, then n^2 is even."

Ex: Give a direct proof of the statement "If n is odd, then n^2 is odd."

Def: An integer n is a *perfect square* if it can be expressed as $n = k^2$ for some integer k.

Ex: Give a direct proof of the statement "If n and m are perfect squares, then nm is a perfect square."

Ex: Give a direct proof of the statement "If $n = k^4$ for some integer k, then n is a perfect square."

1.1.2 Proof by Contrapositive

A *proof by contrapositive* (or *proof by contraposition*) of a statement "$p \to q$" is to assume that q is false, follow rules of inference, and conclude that p is false. This demonstrates "p only if q" or "$\neg q \to \neg p$."

Ex: Give a proof of the statement "If n is an integer and $5n - 4$ is odd, then n is odd."

Proof. We prove by contrapositive. Suppose that n is even, so there exists an integer k such that $n = 2k$. Then $5n - 4 = 5(2k) - 4 = 10k - 4 = 2(5k - 2)$. Therefore, $5n - 4$ is even. □

Ex: Give a proof of the statement "If $n = abc$, then $a \geq \sqrt[3]{n}$, $b \geq \sqrt[3]{n}$, or $c \geq \sqrt[3]{n}$."

Proof. We prove by contrapositive. Suppose that $a < \sqrt[3]{n}$, $b < \sqrt[3]{n}$, and $c < \sqrt[3]{n}$. (Note use of DeMorgan's Law here!) Then

$$abc < (\sqrt[3]{n})(\sqrt[3]{n})(\sqrt[3]{n}) = n.$$

Therefore, $abc \neq n$. □

Ex: Give a proof of the statement "If n is an integer and $3n + 2$ is odd, then n is odd."

1.1.3 Determine which proof type to use!

Def: A real number r is *rational* if there exists integers p, q ($q \neq 0$) such that $r = p/q$. Otherwise, r is *irrational.*

Ex: Prove that "If r and t are rational, then $r + t$ is rational."

Ex: Prove that "If r is irrational and t is rational, then $r + t$ is irrational."

Ex: Prove that "If r is rational, then r^n is rational for every integer n."

Ex: Prove that "If n^2 is odd, then n is odd."

Ex: Prove that "If n^3 is odd, then n is odd."

1.1.4 Proof by Contradiction

A *proof by contradiction* of a statement "p" is to assume that p is false, follow rules of inference, and conclude that $q \wedge \neg q$ is true for some proposition q. Since $q \wedge \neg q$ is false, this is nonsense! Thus, it could not be possible for p to be false, and hence p is true.

Caveat: I want to point out something: If you assume $\neg p$, then make a direct proof of p, you can conclude that $p \wedge \neg p$, giving a contradiction. *This will not be accepted as a proof by contradiction, because it contains a direct proof.*

A *proof by contradiction* of a statement "$p \to q$" is to assume $p \wedge \neg q$, follow rules of inference, and conclude that $a \wedge \neg a$ is true for some proposition a. Since $a \wedge \neg a$ is false, this is nonsense! Thus, it could not be possible for $p \wedge \neg q$ to be true, and hence $p \to q$ is true.

Ex: Prove that "$\sqrt{2}$ is irrational."

Proof. Suppose (for the sake of contradiction) that $\sqrt{2}$ is rational. Let p and q be integers such that $\sqrt{2} = \frac{p}{q}$. We can also select p and q in *lowest terms* such that p and q have no common positive factors (other than 1). It follows that

$$2 = \sqrt{2}^2 = \frac{p^2}{q^2}.$$

Therefore $2q^2 = p^2$. Hence p^2 is even. Therefore (by previous result) p is even. Let k be an integer such that $p = 2k$. Thus, $2q^2 = p^2 = 4k^2$ and hence $q^2 = 2k^2$, so q^2 is even. Therefore q is even, and $q = 2\ell$ for some integer ℓ. Thus, 2 divides both p and q, contradicting the fact that p and q have no common factors. Our assumption that $\sqrt{2}$ is rational is false. □

Ex: Prove that "$\sqrt{3}$ is irrational." "$\sqrt{5}$ is irrational." or "$\sqrt{7}$ is irrational."

Ex: Prove that "$\sqrt{6}$ is irrational." "$\sqrt{8}$ is irrational." or "$\sqrt{10}$ is irrational."

Some of the statements above can be proven using the following lemma:

Lemma: If rt is rational for nonzero real numbers r and t, then either r and t are both rational, or r and t are both irrational

Proof. . Suppose (for the sake of contradiction) that rt is rational and exactly one of r and t is irrational. *Without loss of generality*, let r be rational and t be irrational. Thus, there exist integers p and q such that $r = p/q$; since r is nonzero, $p \neq 0$. There also exist integer n and m such that $rt = n/m$. Then $rt = t\frac{p}{q} = \frac{n}{m}$. By taking the equation $t\frac{p}{q} = \frac{n}{m}$ and multiplying both sides by $\frac{q}{p}$, we see that $t = \frac{nq}{mp}$ and hence t is rational. Thus, t is rational and irrational, a contradiction! Therefore, our assumption that rt is rational and exactly one of r and t is irrational is incorrect. Therefore, either r and t are both rational or r and t are both irrational. □

1.1.5 Proof Mistakes!

For the next two fallacies, assume "If p/q is even, then p is even." is true (it is).

Fallacy of affirming the conclusion: If $p \to q$ and q, then p. This does not always follow!

Ex: If p/q is even, then p is even. 30 is even, so $\frac{30}{10} = 3$ is even.

"Proof:" For every integer p, $p^2 \geq 0$. Therefore, $p \geq 0$.

Fallacy of denying the hypothesis: If $p \to q$ and $\neg p$, then $\neg q$. This does not always follow!

Ex: If p/q is even, then p is even. $\frac{12}{4} = 3$ is odd, so 12 is odd.

Begging the question or **Circular reasoning**: While trying to prove "$p \to q$," you use q to find a conclusion, which is then used to show q is true.

Ex: Every integer n is even or odd.

"Proof:" Let n be an integer. If $n-1$ is even, then $n = 2k+1$ for some integer k and hence n is even. If $n-1$ is odd, then $n = (2k+1)+1$ for some integer k, and hence $n = 2(k+1)$ and n is even. Therefore, n is either even or odd.

(The "Proof" above assumes that the integer $n-1$ is even or odd, which is part of the conclusion. We will later show a proof method, called *induction*, that makes a similar argument valid.)

1.1.6 Suggested Homework

Rosen 1.7: 1–10, 15–18, 24–29, 33, 34–35.

2 Wednesday, January 28

2.1 Rosen 1.8 — Proof Methods and Strategy

Reading: Rosen 1.8. LLM 1.5, 1.6, 1.7, 1.8, 1.9.

2.1.1 Proof Strategies

Adapting Existing Proofs: You can use proofs you have seen before to prove new facts about similar statements. For instance, the proof that $\sqrt{2}$ is irrational can be used to prove that $\sqrt{p}$ is irrational for any prime number p.

Backward Reasoning: Sometimes it is difficult to see where to start when proving a mathematical statement. So instead, you can start with the statement you want to prove, perform operations to find an equivalent statement that you know is true, and then reverse the process.

Ex: For any two distinct positive real numbers x, y, $\frac{x+y}{2} > \sqrt{xy}$.

Start with $(x+y)/2 > \sqrt{xy}$, square both sides to find $(x+y)^2/4 > xy$, expand and subtract xy from both sides to find $(x^2+2xy+y^2)/4 - xy > 0$, multiply by 4 and combine like terms to find $x^2 - 2xy + y^2 > 0$, and then factor to see $(x-y)^2 > 0$. We know that $(x-y)^2 > 0$, as $x - y \neq 0$. We now reverse this discovery to make a proof:

Proof. Since x and y are distinct, $x - y \neq 0$. Therefore, $(x-y)^2 > 0$. By expanding the left-hand-side, we see that $x^2 - 2xy + y^2 > 0$. By adding $4xy$ to each side, we see that $x^2 + 2xy + y^2 > 4xy$. Observe that $x^2 + 2xy + y^2 = (x+y)^2$. Therefore, $(x+y)^2 > 4xy = (2\sqrt{xy})^2$. Since $x + y$ is positive and xy is positive, we can take square roots of both sides to find $x + y > 2\sqrt{xy}$ and by dividing by 2 we see $\frac{x+y}{2} > \sqrt{xy}$ as desired. □

2.1.2 Proof by Cases

Def: The proof method "*exhaustive proof*" means to evaluate all possibilities and determine that the statement is always true.

Def: An integer n is *composite* if there exist positive integers $p, q > 1$ such that $n = pq$. Otherwise, n is *prime*.

Thm: If n is a prime with $30 \leq n \leq 40$, then $n = 31$ or $n = 37$.

Proof. Before we consider our cases, note that if n is composite, then $n = pq$ for integers $p, q > 1$. Note that if $p \leq q$ then $p \leq \sqrt{n} \leq \sqrt{40} \approx 6.32$. Therefore, in order to test for n being prime or composite, we only need to determine if the numbers 2, 3, 4, 5, or 6 evenly divide n. (Note also that we do not need to test for 4 and 6 dividing n.)

Case $n = 30$: $30 = 3 \times 10$ so n is composite.

Case $n = 31$: 31 is odd, so 2 does not divide 31. $31/3 = 10 + \frac{1}{3}$, so 3 does not divide 31. $31/5 = 6 + \frac{1}{5}$, so 5 does not divide 31. Therefore, n is prime.

Case $n = 32$: $32 = 2 \times 16$ so n is composite.

Case $n = 33$: $33 = 3 \times 11$ so n is composite.

Case $n = 34$: $34 = 2 \times 17$ so n is composite.

Case $n = 35$: $35 = 5 \times 7$ so n is composite.

Case $n = 36$: $36 = 3 \times 12$ so n is composite.

Case $n = 37$: 37 is odd, so 2 does not divide 31. $37/3 = 12 + \frac{1}{3}$, so 3 does not divide 31. $37/5 = 7 + \frac{2}{5}$, so 5 does not divide 31. Therefore, n is prime.

Case $n = 38$: $38 = 2 \times 19$ so n is composite.

Case $n = 39$: $30 = 3 \times 13$ so n is composite.

Case $n = 40$: $40 = 2 \times 20$ so n is composite. □

Def: The proof method "*proof by case analysis*" can be more careful. By making choices for cases and subcases (and sub-sub-cases, etc.) we can decide we are already in a "dead end" and "turn around." Alternatively, we could partition the cases such that certain cases are handled more quickly.

Here is a shorter proof using a careful partition of cases.

Thm: If n is a prime with $30 \leq n \leq 40$, then $n = 31$ or $n = 37$.

Proof. Before we consider our cases, note that if n is composite, then $n = pq$ for integers $p, q > 1$. Note that if $p \leq q$ then $p \leq \sqrt{n} \leq \sqrt{40} \approx 6.32$. Therefore, in order to test for n being prime or composite, we only need to determine if the numbers 2, 3, 4, 5, or 6 evenly divide n. (Note also that we do not need to test for 4 and 6 dividing n.)

Case n is one of 30, 32, 34, 36, 38, or 40: These numbers are even, so they are composite.

Case n is one of 33 or 39: These numbers are divisible by 3, so they are composite.

Case $n = 35$: $35 = 5 \times 7$, so 35 is composite.

Case $n = 31$: 31 is odd, so 2 does not divide 31. $31/3 = 10 + \frac{1}{3}$, so 3 does not divide 31. $31/5 = 6 + \frac{1}{5}$, so 5 does not divide 31. Therefore, n is prime.

Case $n = 37$: 37 is odd, so 2 does not divide 31. $37/3 = 12 + \frac{1}{3}$, so 3 does not divide 31. $37/5 = 7 + \frac{2}{5}$, so 5 does not divide 31. Therefore, n is prime. □

Now, here is a more complicated example, where we want to consider cases and subcases (but some cases do not need subcases).

Ex: In the country of Togliristan (where Knights, Knaves, and Togglers live). Togglers will alternate between telling the truth and lying (no matter what other people say). You meet two people, A and B. They say, in order:

A : B is a Knave.
B : No, I am not.
A : B is a Knight.
B : Yes, I am.
A : B is a Toggler.
B : No, I am not.

Determine what types of people A and B are.

Solution: A is a Flopper and B is a Knight.

Proof. First, let us consider A's type.

Case 1: A is a Knight. If A is a Knight, then A will always tell the truth. However, A says conflicting statements "B is a Knave" and "B is a Knight." Therefore, A is not a Knight.

Case 2: A is a Knave. If A is a Knave, then A will always lie. However, A claims that B is each type of person that B could be, so the three statements "B is a Knave," "B is a Knight," and "B is a Toggler" cannot all be false. Therefore, A is not a Knave.

Case 3: A is a Toggler. We do not yet know if A starts by lying or telling the truth. Let us consider the type of B.

Case 3.a: B is a Knave. Then B's last claim of not being a Toggler is true, and B did not lie. Therefore, B is not a Knave.

Case 3.b: B is a Toggler. Then B's second and third statements are false, and B would not lie two times in a row. Therefore B is not a Toggler.

Case 3.c: B is a Knight. Then all three of B's statements are true, and B would never lie.

By considering all cases, A is a Toggler and B is a Knight. □

Note: There are many other ways to organize the case analysis above. Can you think of another way?

2.1.3 Existence Proof

Def: A statement of the form $\exists x P(x)$ is proven using an *existence proof.* That is: Demonstrate that there is some c such that $P(c)$ is true. This proof can be *constructive* or *nonconstructive.*

Constructive Example: Prove that $2^{99} + 1$ is a composite number.

(Another way to phrase this is $\exists p, q > 1(2^{99} + 1 = pq)$ where the universe is positive integers.)

Proof. Let $p = 2^{33} + 1$ and $q = 2^{66} - 2^{33} + 1$. Then,

$$pq = (2^{33} + 1)(2^{66} - 2^{33} + 1) = 2^{33} \cdot 2^{66} - 2^{33} \cdot 2^{33} + 2^{33} + 2^{66} - 2^{33} + 1 = 2^{99} + 1.$$ □

Nonconstructive Example: There exist two irrational numbers x and y such that x^y is rational.

Proof. Recall that $\sqrt{2}$ is irrational. If $\sqrt{2}^{\sqrt{2}}$ is rational, then let $x = y = \sqrt{2}$. Otherwise, consider $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^{2} = 2$. Then, let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. □

The proof above is nonconstructive because we do not know which pair $(\sqrt{2}, \sqrt{2})$ or $(\sqrt{2}^{\sqrt{2}}, \sqrt{2})$ satisfies the proposition $P(x, y) =$"x and y are irrational and x^y is rational." And in fact, *exactly one* of the two pairs works.

2.1.4 Uniqueness Proof

Sometimes, we want to claim there *exists a unique solution.* This has two parts:

1. There exists a y with the desired property.
2. If $x \neq y$, then x does not have the desired property.

2.1.5 Tiling Problems

A $m \times n$ *checkerboard* is a rectangle divided into mn squares, with m rows and n columns. The squares are colored black and white such that squares sharing an edge have opposite colors. The *standard checkerboard* is the 8×8 checkerboard.

A *domino* is a rectangular piece that fits perfectly over two squares of a checkerboard. A *domino tiling* is an arrangement of dominos on a checkerboard such that every square is covered by exactly one domino.

Thm: An $n \times n$ checkerboard has a domino tiling if and only if n is even.

(This can be demonstrated with an example. In the odd case, there are n^2 squares to cover, and n^2 is odd, but dominoes can only cover an even number of squared.)

Thm: An $n \times n$ checkerboard with the top-right square missing has a domino tiling if and only if n is odd.

(This can be demonstrated with an explicit tiling in the odd case. In the even case, $n^2 - 1$ is odd.)

Thm: Let n be even. An $n \times n$ checkerboard with the top-right square and bottom-left square missing has no domino tiling.

(In this case, $n^2 - 2$ is even, so using a parity argument will not work.)

Proof. In an $n \times n$ chessboard for even n, the top-right and bottom-left squares have the same color. When these are removed, there are two more squares of one color than the other. In a domino tiling, each domino covers exactly one square of each color. Therefore, no tiling covers more squares of one color than the other, and hence no tiling exists. □

Dominoes can be extended to other shapes. Such as *triominoes* (three squares) except there are two ways to make a triomino! First: a *straight triomino*. Second: a *right triomino*.

Thm: An $n \times n$ chessboard can be tiled with straight triominoes if and only if 3 divides n.

(Prove this!)

Thm: Let $n = 8$. An $n \times n$ chessboard with exactly one square removed can be tiled if and only if $t = 0$ or $t = 3$.

Proof. For $1 \leq i, j \leq n$, let the (i, j) position of the chessboard be the square in row i and column j (where $(1, 1)$ is the bottom-left square). Color the square in the (i, j) position with black if $i + j = 3k$, white if $i + j = 3k + 1$, and blue if $i + j = 3k + 2$ (observe that exactly one case holds for each (i, j)). If a triomino is placed on the chessboard and (i, j) is the square covered minimizing $i + j$, then the triomino covers the squares (i, j), $(i, j + 1)$, and $(i, j + 2)$ or the squares (i, j), $(i + 1, j)$, or $(i + 2, j)$. In each case, the triomino covers squares of all three colors. Thus, in a domino tiling, the triominoes cover the same number of squares of each color.

In our coloring of the 8×8 chessboard, there are 21 black squares, 22 white squares, and 20 blue squares. Even after removing ANY square we do not have equal numbers of each color square. Thus, no domino tiling exists. □

2.1.6 Suggested Homework

Rosen 1.8: 1–6, 7*, 8–11, 13–14, 17–22, 25*, 26*, 29–32, 34*, 38, 41–45, 47, 48*, 49.

3 Friday, January 30

3.1 Rosen 2.1 – Sets

Reading: Rosen 2.1. LLM 4.1. Ducks 2.1, 2.2.

3.2 Venn Diagrams

3.3 Subsets

3.4 Cartesian Products

3.5 Set Notation with Quantifiers

3.5.1 Suggested Homework

Rosen 2.1: 1,3–8,9–11, 14–17, 18–24, 25^*, 26–30, 35–37, 46^*, 47^*.