Diagonalization and the Pigeonhole Principle

Friday Four Square!
Today at 4:15PM, Outside Gates

Announcements

- Problem Set 2 due right now.
- Problem Set 3 out:
  - **Checkpoint** due on Monday, January 28.
  - **Remainder** due on Friday, February 1.
  - Play around with relations, functions, and cardinalities!
- Unnamed Problem Set 1 found; did you forget to put your name on it?

Recap from Last Time

Functions

- A **function** f is a mapping such that every value in A is associated with a single value in B.
- If f is a function from A to B, we call A the **domain** of f andl B the **codomain** of f.
- We denote that f is a function from A to B by writing

$$\boldsymbol{f : A \to B}$$

Injective Functions

- A function $f : A \to B$ is called **injective** (or **one-to-one**) if each element of the codomain has at most one element of the domain associated with it.
  - A function with this property is called an **injection**.
- Formally, $f : A \to B$ is an injection iff

$$\textbf{For any } x_0, x_1 \in A\textbf{:}$$
$$\textbf{if } f(x_0) = f(x_1)\textbf{, then } x_0 = x_1$$

- An intuition: injective functions label the objects from A using names from B.

Surjective Functions

- A function $f : A \to B$ is called **surjective** (or **onto**) if each element of the codomain has at least one element of the domain associated with it.
  - A function with this property is called a **surjection**.
- Formally, $f : A \to B$ is a surjection iff

$$\textbf{For every } b \in B\textbf{, there exists at least one } a \in A \textbf{ such that } f(a) = b.$$

- An intuition: surjective functions cover every element of B with at least one element of A.

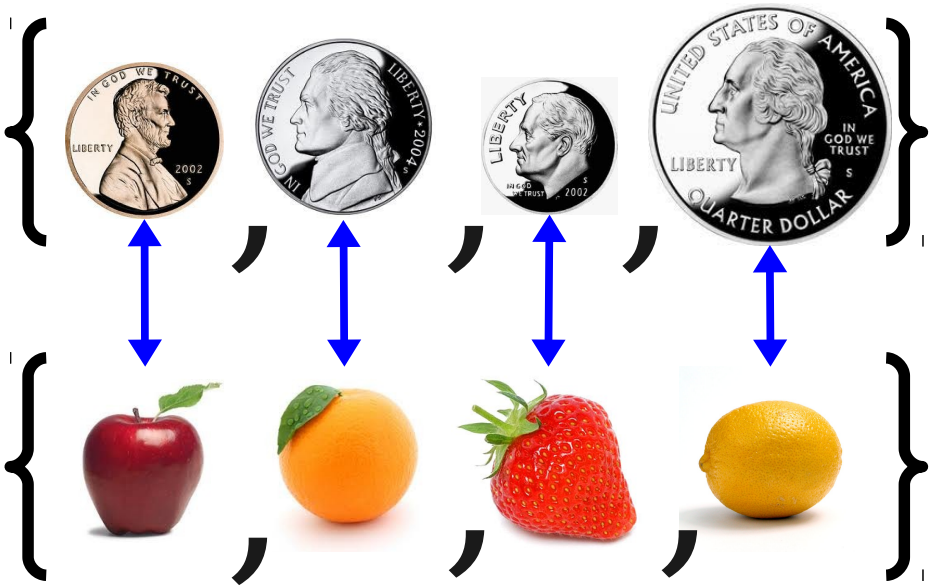
Bijections

- A function that associates each element of the codomain with a unique element of the domain is called **bijective**.
  - Such a function is a **bijection**.
- Formally, a bijection is a function that is both **injective** and **surjective**.
- A bijection is a one-to-one correspondence between two sets.

Equal Cardinalities

- The relationships between set cardinalities are defined in terms of functions between those sets.
- $|S| = |T|$ is defined using bijections.

$|S| = |T|$ iff there is a bijection $f : S \to T$

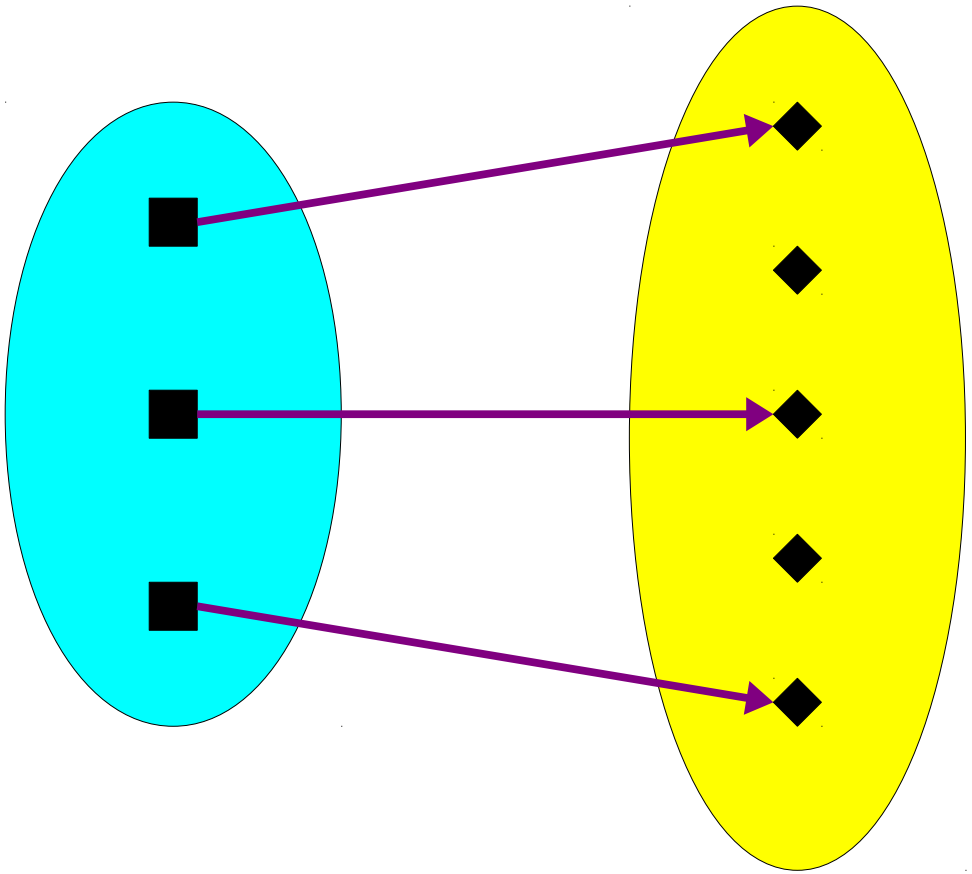


Differing Infinities

Ranking Cardinalities

- We define $|S| \leq |T|$ as follows:

$$|S| \leq |T| \text{ iff there is an injection } f : S \to T$$



Ranking Cardinalities

- We define $|S| \leq |T|$ as follows:

$$\mathbf{|S| \leq |T| \text{ iff there is an injection } f : S \to T}$$

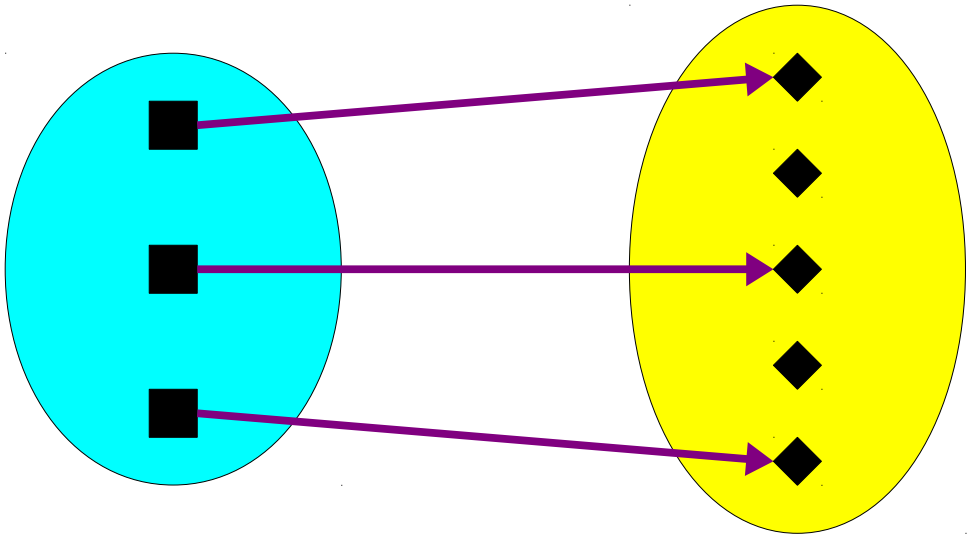
- The $\leq$ relation over set cardinalities is a total order. For any sets R, S, and T:
  - $|S| \leq |S|$. ***(reflexivity)***
  - If $|R| \leq |S|$ and $|S| \leq |T|$, then $|R| \leq |T|$. ***(transitivity)***
  - If $|S| \leq |T|$ and $|T| \leq |S|$, then $|S| = |T|$. ***(antisymmetry)***
  - Either $|S| \leq |T|$ or $|T| \leq |S|$. ***(totality)***
- These last two proofs are **extremely hard**.
  - The antisymmetry result is the **Cantor-Bernstein-Schroeder Theorem**; a fascinating read, but beyond the scope of this course.
  - Totality requires the **axiom of choice**. Take Math 161 for more details.

Comparing Cardinalities

- Formally, we define < on cardinalities as

$$|S| < |T| \text{ iff } |S| \leq |T| \text{ and } |S| \neq |T|$$

- In other words:
  - There is an injection from S to T.
  - There is no bijection between S and T.



What is the relation between $|\mathbb{N}|$ and $|\mathbb{R}|$?

Theorem: $|\mathbb{N}| \leq |\mathbb{R}|$.

Proof: We exhibit an injection from $\mathbb{N}$ to $\mathbb{R}$. Let $f(n) = n$. Then $f : \mathbb{N} \to \mathbb{R}$, since every natural number is also a real number.

We further claim that f is an injection. To see this, suppose that for some $n_0, n_1 \in \mathbb{N}$ that $f(n_0) = f(n_1)$. We will prove that $n_0 = n_1$. To see this, note that

$$n_0 = f(n_0) = f(n_1) = n_1$$

Thus $n_0 = n_1$, as required, so f is an injection from $\mathbb{N}$ to $\mathbb{R}$. Thus $|\mathbb{N}| \leq |\mathbb{R}|$. ■

Key Question:

Does $|\mathbb{N}| = |\mathbb{R}|$?

Theorem: $|\mathbb{N}| \neq |\mathbb{R}|$

Our Goal

- We need to show the following:

There is no bijection $f : \mathbb{N} \to \mathbb{R}$

- This is a different style of proof from what we have seen before.
- To prove it, we will do the following:
  - Assume for the sake of contradiction that there is a bijection $f : \mathbb{N} \to \mathbb{R}$.
  - Derive a contradiction by showing that f cannot be surjective.
  - Conclude our assumption was wrong and that no bijection can possibly exist from $\mathbb{N}$ to $\mathbb{R}$.

The Intuition

- Suppose we have a function $f : \mathbb{N} \to \mathbb{R}$.
- We can then list off an infinite sequence of real numbers

$$r_0, r_1, r_2, r_3, r_4, \ldots$$

  by setting $r_i = f(i)$.
- We will show that we can always find a real number d such that

$$\textbf{For any } \boldsymbol{n} \in \mathbb{N}\textbf{: } \boldsymbol{r_n \neq d}\textbf{.}$$

Rewriting Our Constraints

- Our goal is to find some $d \in \mathbb{R}$ such that

$$\textbf{For any } n \in \mathbb{N}\textbf{: } r_n \neq d.$$

- In other words, we want to pick d such that

$$r_0 \neq d$$

$$r_1 \neq d$$

$$r_2 \neq d$$

$$r_3 \neq d$$

$$\ldots$$

The Critical Insight

- **Key Proof Idea:** Build the real number d out of infinitely many "pieces," with one piece for each r_i.
  - Choose the 0th piece such that $r_0 \neq d$.
  - Choose the 1st piece such that $r_1 \neq d$.
  - Choose the 2nd piece such that $r_2 \neq d$.
  - Choose the 3rd piece such that $r_3 \neq d$.
  - ...
- Building a "frankenreal" out of infinitely many pieces of other real numbers.

Building our “Frankenreal”

- Goal: build “frankenreal” d out of infinitely many pieces, one for each r_i.
- One idea: Define d via its decimal representation.
- Choose the digits of d as follows:
  - The 0th digit of d is not the same as the 0th digit of r_0.
  - The 1st digit of d is not the same as the 1st digit of r_1.
  - The 2nd digit of d is not the same as the 2nd digit of r_2.
  - …
- So $d \neq r_i$ for any $i \in \mathbb{N}$.

Building our “Frankenreal”

- If r is a real number, define $r[n]$ as follows:
  - $r[0]$ is the integer part of r.
  - $r[n]$ is the nth decimal digit of r, if $n > 0$.
- Examples:
  - $\pi[0] = 3$ $\quad$ $(-e)[0] = -2$ $\quad$ $5[0] = 5$
  - $\pi[1] = 1$ $\quad$ $(-e)[1] = 7$ $\quad$ $5[1] = 0$
  - $\pi[2] = 4$ $\quad$ $(-e)[2] = 1$ $\quad$ $5[2] = 0$
  - $\pi[3] = 1$ $\quad$ $(-e)[3] = 8$ $\quad$ $5[3] = 0$

Building our "Frankenreal"

- We can now build our frankenreal d.
- Define $d[n]$ as follows:

$$d[n] = \begin{cases} 1 & \text{if } r_n[n] = 0 \\ 0 & \text{otherwise} \end{cases}$$

- Now, $d \neq r_i$ for any $i \in \mathbb{N}$:
  - If $r_i[i] = 0$, then $d[i] = 1$, so $r_i \neq d$.
  - If $r_i[i] \neq 0$, then $d[i] = 0$, so $r_i \neq d$.

0	⟷	8.	6	7	5	3	0	...
1	⟷	3.	1	4	1	5	9	...
2	⟷	0.	1	2	3	5	8	...
3	⟷	-1.	0	0	0	0	0	...
4	⟷	2.	7	1	8	2	8	...
5	⟷	1.	6	1	8	0	3	...
...	⟷	...	...	...	...	...	...	...

	d_0	d_1	d_2	d_3	d_4	d_5	...
0	8.	6	7	5	3	0	...
1	3.	1	4	1	5	9	...
2	0.	1	2	3	5	8	...
3	-1.	0	0	0	0	0	...
4	2.	7	1	8	2	8	...
5	1.	6	1	8	0	3	...
...	...	...	...	...	...	...	...

	d_0	d_1	d_2	d_3	d_4	d_5	...
0	8.	6	7	5	3	0	...
1	3.	1	4	1	5	9	...
2	0.	1	2	3	5	8	...
3	-1.	0	0	0	0	0	...
4	2.	7	1	8	2	8	...
5	1.	6	1	8	0	3	...
...	...	...	...	...	...	...	...

	d_0	d_1	d_2	d_3	d_4	d_5	...
0	8.	6	7	5	3	0	...
1	3.	1	4	1	5	9	...
2	0.	1	2	3	5	8	...
3	-1.	0	0	0	0	0	...
4	2.	7	1	8	2	8	...
5	1.	6	1	8	0	3	...
...	...	...	...	...	...	...	...

8.	1	2	0	2	3	...

	d_0	d_1	d_2	d_3	d_4	d_5	...
0	8.	6	7	5	3	0	...
1	3.	1	4	1	5	9	...
2	0.	1	2	3	5	8	...
3	-1.	0	0	0	0	0	...
4	2.	7	1	8	2	8	...
5	1.	6	1	8	0	3	...
...	...	...	...	...	...	...	...

0.	0	0	1	0	0	...

Set all nonzero values to 0 and all 0s to 1.

Theorem: $|\mathbb{N}| \neq |\mathbb{R}|$.

Proof: By contradiction; suppose that $|\mathbb{N}| = |\mathbb{R}|$. Then there exists a bijection $f : \mathbb{N} \to \mathbb{R}$.

We introduce some new notation. For a real number r, let $r[0]$ be the integer part of r, and let $r[n]$ for $n \in \mathbb{N}$, $n > 0$, be the nth digit in the decimal representation of r. Now, define the real number d as follows:

$$d[n] = \begin{cases} 1 & \text{if } f(n)[n] = 0 \\ 0 & \text{otherwise} \end{cases}$$

Since $d \in \mathbb{R}$, there must be some $n \in \mathbb{N}$ such that $f(n) = d$. So consider $f(n)[n]$ and $d[n]$. We consider two cases:

Case 1: $f(n)[n] = 0$. Then by construction $d[n] = 1$, so $f(n) \neq d$.

Case 2: $f(n)[n] \neq 0$. Then by construction $d[n] = 0$, so $f(n) \neq d$.

In either case, $f(n) \neq d$. This contradicts the fact that $f(n) = d$. We have reached a contradiction, so our assumption must have been wrong. Thus $|\mathbb{N}| \neq |\mathbb{R}|$. ■

Diagonalization

- The proof we just worked through is called a **proof by diagonalization** and is a powerful proof technique.
- Suppose you want to show $|A| \neq |B|$:
  - Assume for contradiction that $f : A \to B$ is surjective. We'll find $d \in B$ such that $f(a) \neq d$ for any $a \in A$.
  - To do this, construct d out of "pieces," one piece taken from each $a \in A$.
  - Construct d such that the ath "piece" of d disagrees with the ath "piece" of $f(a)$.
  - Conclude that $f(a) \neq d$ for any $a \in A$.
  - Reach a contradiction, so no surjection exists from A to B.

An Interesting Historical Aside

- The diagonalization proof that $|\mathbb{N}| \neq |\mathbb{R}|$ was Cantor's original diagonal argument; he proved Cantor's theorem later on.
- However, this was ***not*** the first proof that $|\mathbb{N}| \neq |\mathbb{R}|$. Cantor had a different proof of this result based on infinite sequences.
- Come talk to me after class if you want to see the original proof; it's absolutely brilliant!

Cantor's Theorem Revisited

Cantor's Theorem

- **Cantor's Theorem** states that

  For every set S, $|S| < |\wp(S)|$

- This is how we concluded that there are more problems to solve than programs to solve them.
- We informally sketched a proof of this in the first lecture.
- Let's now formally prove Cantor's Theorem.

Lemma: For any set S, $|S| \leq |\wp(S)|$.

Proof: Consider any set S. We show that there is an injection $f : S \to \wp(S)$. Define $f(x) = \{x\}$.

To see that $f(x)$ is a legal function from S to $\wp(S)$, consider any $x \in S$. Then $\{x\} \subseteq S$, so $\{x\} \in \wp(S)$. This means that $f(x) \in \wp(S)$, so f is a valid function from S to $\wp(S)$.

To see that f is injective, consider any x_0 and x_1 such that $f(x_0) = f(x_1)$. We prove that $x_0 = x_1$. To see this, note that if $f(x_0) = f(x_1)$, then $\{x_0\} = \{x_1\}$. Since two sets are equal iff their elements are equal, this means that $x_0 = x_1$ as required. Thus f is an injection from S to $\wp(S)$, so $|S| \leq |\wp(S)|$. ■

The Key Step

- We now need to show that

$$\textbf{For any set } S\textbf{, } |S| \neq |\wp(S)|$$

- By definition, $|S| = |\wp(S)|$ iff there exists a bijection $f : S \to \wp(S)$.
- This means that

$$|S| \neq |\wp(S)| \textbf{ iff there is no bijection } f : S \to \wp(S)$$

- Prove this by contradiction:
  - Assume that there is a bijection $f : S \to \wp(S)$.
  - Derive a contradiction by showing that f is not a bijection.

The Diagonal Argument

- Suppose that we have a function $f : S \to \wp(S)$.
- We want to find a "frankenset" $D \in \wp(S)$ such that for any $x \in S$, $f(x) \neq D$.
- Idea: Use a diagonalization argument.
  - Build D from many "pieces," one "piece" for each $x \in S$.
  - Choose those pieces such that the xth "piece" of $f(x)$ disagrees with the xth "piece" of D.
- Hard part: What will our "pieces" be?

The Key Idea

- Key idea: Have the xth "piece" of D be whether or not D contains x.
- Want to construct D such that

  $f(x)$ contains x iff D does not contain x

- More formally, we want

$$x \in f(x) \quad \text{iff} \quad x \notin D$$

- Most formally:

$$D = \{ x \in S \mid x \notin f(x) \}$$

$$x_0 \longleftrightarrow \{ x_0, x_2, x_4, \ldots \}$$

$$x_1 \longleftrightarrow \{ x_0, x_3, x_4, \ldots \}$$

$$x_2 \longleftrightarrow \{ x_4, \ldots \}$$

$$x_3 \longleftrightarrow \{ x_1, x_4, \ldots \}$$

$$x_4 \longleftrightarrow \{ x_0, x_5, \ldots \}$$

$$x_5 \longleftrightarrow \{ x_0, x_1, x_2, x_3, x_4, x_5, \ldots \}$$

$$\ldots$$

	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	**Y**	**N**	**Y**	**N**	**Y**	**N**	…
x_1	**Y**	**N**	**N**	**Y**	**Y**	**N**	…
x_2	**N**	**N**	**N**	**N**	**Y**	**N**	…
x_3	**N**	**Y**	**N**	**N**	**Y**	**N**	…
x_4	**Y**	**N**	**N**	**N**	**N**	**Y**	…
x_5	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	…
…	…	…	…	…	…	…	…

	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	**Y**	**N**	**Y**	**N**	**Y**	**N**	…
x_1	**Y**	**N**	**N**	**Y**	**Y**	**N**	…
x_2	**N**	**N**	**N**	**N**	**Y**	**N**	…
x_3	**N**	**Y**	**N**	**N**	**Y**	**N**	…
x_4	**Y**	**N**	**N**	**N**	**N**	**Y**	…
x_5	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	…
…	…	…	…	…	…	…	…
	Y	**N**	**N**	**N**	**N**	**Y**	…

	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	**Y**	**N**	**Y**	**N**	**Y**	**N**	…
x_1	**Y**	**N**	**N**	**Y**	**Y**	**N**	…
x_2	**N**	**N**	**N**	**N**	**Y**	**N**	…
x_3	**N**	**Y**	**N**	**N**	**Y**	**N**	…
x_4	**Y**	**N**	**N**	**N**	**N**	**Y**	…
x_5	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	…
…	…	…	…	…	…	…	…

N	**Y**	**Y**	**Y**	**Y**	**N**	…

Flip all Y's to N's and vice-versa to get a new set

Lemma: For any set S, $|S| \neq |\wp(S)|$.

Proof: By contradiction; assume that there exists a set S such that $|S| = |\wp(S)|$. This means that there exists a bijection $f : S \to \wp(S)$. Consider the set $D = \{ x \in S \mid x \notin f(x) \}$. Note that $D \subseteq S$, since by construction every $x \in D$ satisfies $x \in S$.

Since f is a bijection, it is surjective, so there must be some $y \in S$ such that $f(y) = D$. Now, either $y \in f(y)$, or $y \notin f(y)$. We consider these cases separately:

Case 1: $y \in f(y)$. By our definition of D, this means that $y \notin D$. However, since $y \in f(y)$ and $f(y) = D$, we have $y \in D$. We have reached a contradiction.

Case 2: $y \notin f(y)$. By our definition of D, this means that $y \in D$. However, since $y \notin f(y)$ and $f(y) = D$, we have $y \notin D$. We have reached a contradiction.

In either case we reach a contradiction, so our assumption must have been wrong. Thus for every set S, we have that $|S| \neq |\wp(S)|$. ■

***Theorem* (Cantor's Theorem)**: For any set S, we have $|S| < |\wp(S)|$.

Proof: Consider any set S. By our first lemma, we have that $|S| \leq |\wp(S)|$. By our second lemma, we have that $|S| \neq |\wp(S)|$. Thus $|S| < |\wp(S)|$. ■

The Pigeonhole Principle

The **pigeonhole principle** is the following:

If m objects are placed into n bins, where $m > n$, then some bin contains at least two objects.

(We sketched a proof in Lecture #02)

Why This Matters

- The pigeonhole principle can be used to show results must be true because they are "too big to fail."
- Given a large enough number of objects with a bounded number of properties, eventually at least two of them will share a property.
- The applications are interesting, surprising, and thought-provoking.

Using the Pigeonhole Principle

- To use the pigeonhole principle:
  - Find the m objects to distribute.
  - Find the $n < m$ buckets into which to distribute them.
  - Conclude by the pigeonhole principle that there must be two objects in some bucket.
- The details of how to proceeds from there are specific to the particular proof you're doing.

A Surprising Application

Theorem: Suppose that every point in the real plane is colored either red or blue. Then for any distance $d > 0$, there are two points exactly distance d from one another that are the same color.

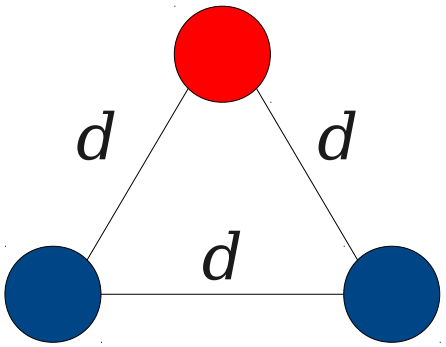
Thought: There are two colors here, so if we start picking points, we'll be dropping them into one of two buckets (red or blue).

How many points do we need to pick to guarantee that we get two of the same color?

A Surprising Application

Theorem: Suppose that every point in the real plane is colored either red or blue. Then for any distance $d > 0$, there are two points exactly distance d from one another that are the same color.

Any pair of these points is at distance d from one another. Since two must be the same color, there is a pair of points of the same color at distance d!



A Surprising Application

Theorem: Suppose that every point in the real plane is colored either red or blue. Then for any distance $d > 0$, there are two points exactly distance d from one another that are the same color.

Proof: Consider any equilateral triangle whose side lengths are d. Put this triangle anywhere in the plane. By the pigeonhole principle, because there are three vertices, two of the vertices must have the same color. These vertices are at distance d from each other, as required. ■

Theorem: For any natural number n, there is a nonzero multiple of n whose digits are all 0s and 1s.

Theorem: For any natural number n, there is a nonzero multiple of n whose digits are all 0s and 1s.

1
11
111
1111
11111
111111
1111111
11111111
111111111
1111111111

There are 10 objects here.

Theorem: For any natural number n, there is a nonzero multiple of n whose digits are all 0s and 1s.

	111111111	0
1111111111	1	1
	11	2
	111	3
	1111	4
	11111	5
	111111	6
	1111111	7
	11111111	8

Theorem: For any natural number n, there is a nonzero multiple of n whose digits are all 0s and 1s.

	111111111	0
1111111111	1	1
	11	2
	111	3
	1111	4
	11111	5
	111111	6
	1111111	7
	11111111	8

1111111111
- 1
1111111110

Proof Idea

- For any natural number $n \geq 2$ generate the numbers 1, 11, 111, ... until $n + 1$ numbers are generated.
- There are n possible remainders modulo n, so two of these numbers have the same remainder.
- Their difference is a multiple of n.
- Their difference consists of 1s and 0s.

Theorem: For any natural number n, there is a nonzero multiple of n whose digits are all 0s and 1s.

Proof: For any $k \in \mathbb{N}$ in the range $0 \le k \le n$, consider S_k defined as

$$S_k = \sum_{i=0}^{k} 10^i$$

Now, consider the remainders of the S_k's modulo n. Since there are $n + 1$ S_k's and n remainders modulo n, by the pigeonhole principle there must be at least two S_k's that leave the same remainder modulo n. Let two of these S_k's be S_x and S_y, with $x > y$, and let the remainder be r.

Since $S_x \equiv_n r$, there exists $q_x \in \mathbb{Z}$ such that $S_x = nq_x + r$. Similarly, since $S_y \equiv_n r$, there exists $q_y \in \mathbb{Z}$ such that $S_y = nq_y + r$. Then $S_x - S_y = (nq_x + r) - (nq_y + r) = nq_x - nq_y = n(q_x - q_y)$. Thus $S_x - S_y$ is a multiple of n. Moreover, we have that

$$n(q_x - q_y) = S_x - S_y = \sum_{i=0}^{x} 10^i - \sum_{i=0}^{y} 10^i = \sum_{i=y+1}^{x} 10^i$$

So $S_x - S_y$ is a sum of distinct powers of ten, so its digits are zeros and ones. Since $x > y$, we know that $x \ge y + 1$ and so the sum is nonzero. Therefore $S_x - S_y$ is a nonzero multiple of n consisting of 0s and 1s. ■

Next Time

- **Mathematical Logic**
  - How do we start formalizing our intuitions about mathematical truth?
  - How do we justify proofs by contradiction and contrapositive?