Warm-up problem

Example: Prove the biconditional by proving both directions:

An integer n is even if and only if n - 1 is odd.

Warm-up problem

Example: Prove the biconditional by proving both directions:

An integer n is even if and only if n - 1 is odd.

Proof:

(⇒, direct) S’pose n is an even integer.

1. Then $n = 2a$, where a is some integer
2. Then $n - 1 = 2a - 1 = 2(a - 1) + 1$, which is odd
3. Thus, if n is even, then n - 1 is odd. ✔

(⇐, direct) S’pose n - 1 is an odd integer.

1. Then $n - 1 = 2a + 1$, where a is some integer
2. Then $n = 2a + 2 = 2(a + 1)$, which is even
3. Thus, if n - 1 is odd, then n is even. ✔

□

University of Colorado **Boulder**

CSCI 2824: Discrete Structures

Fall 2018 Tony Wong

Lecture 11: Proof Methods and Strategies

HW 4 (written) is posted

Announcements and reminders

- Homework 3 **due Today at 12 pm (noon)**
- **Midterm 1: 6:30-8 PM, Tuesday 2 October**
    - Rachel (001) in HUMN 1B50
    - Tony (002) in DUAN G1B30

What did we do last time?

- Direct proofs (aka “conditional proofs”)
- Contrapositive proofs
- Proofs by contradiction

Today:

We will learn about proof strategies and methods:

1. Proving existence of stuff
2. Proving uniqueness of stuff
3. *Exhaustive* proofs (with multiple cases)

Proof methods and strategies

Proof by Cases

Proof methods and strategies

Example: Suppose you want to prove $p \rightarrow q$ if p is some statement that is true for all CU undergraduates.

"If a *student studies*, then *they are cool*."

Proof methods and strategies

Example: Suppose you want to prove $p \rightarrow q$ if p is some statement that is true for all CU undergraduates.

"If a *student studies*, then *they are cool*."

Break up into smaller cases:

"If a ***Fr***_eshman studies_ **or** *a* ***So***_phomore studies_
or *a* ***Ju***_nior studies_ **or** *a* ***Se***_nior studies_, then *they are cool.*"

Which is: $(p(Fr) \vee p(So) \vee p(Ju) \vee p(Se)) \rightarrow q$

Proof methods and strategies

Example: Suppose you want to prove $p \to q$ if p is some statement that is true for all CU undergraduates.

"If a *student studies*, then *they are cool*."

Break up into smaller cases:

"If a ***Fr**eshman studies* **or** *a **So**phomore studies*
or *a **Ju**nior studies* **or** *a **Se**nior studies*, then *they are cool.*"

Which is: $(p(Fr) \lor p(So) \lor p(Ju) \lor p(Se)) \to q$

Can we break this up into smaller statements?

$$(p(Fr) \to q) \land (p(So) \to q) \land (p(Ju) \to q) \land (p(Se) \to q)$$

This is **proof by cases**

Proof methods and strategies

Example: Prove that if n is any integer not divisible by 5, then n^2 leaves a remainder of 1 or 4 when divided by 5.

How can we represent an integer that is **not** divisible by 5?

4 cases: remainder of 1: $n = 5k + \underline{1}$

remainder of 2 $n = 5k + \underline{2}$

remainder of 3 $n = 5k + 3$

remainder of 4 $n = 5k + 4$

Proof methods and strategies

Example: Prove that if n is any integer not divisible by 5, then n^2 leaves a remainder of 1 or 4 when divided by 5.

How can we represent an integer that is **not** divisible by 5?

- n leaves a remainder of 1: $n = 5a + 1$ (for some integer a)
- n leaves a remainder of 1: $n = 5a + 2$
- n leaves a remainder of 1: $n = 5a + 3$
- n leaves a remainder of 1: $n = 5a + 4$

So we check these 4 cases, and show that in each case that n^2 divided by 5 leaves a remainder of 1 or 4.

The benefit of using **proof by cases** here is that we have **more information** about each specific case (the four bullet points above) than we would have about just some general n.

Proof methods and strategies

Example: Prove that if n is any integer not divisible by 5, then n^2 leaves a remainder of 1 or 4 when divided by 5. $\rightarrow$ $5\underbrace{\text{integer}} + \underbrace{\text{remainder}} = n^2$

Proof (by cases):

Case 1: S'pose $n/5$ leaves a remainder of 1: $n = 5a + 1$ (for some integer a)

$$n^2 = (5a+1)^2 = \underbrace{25a^2 + 10a} + 1$$
$$= 5(5a^2 + 2a) + \underbrace{1}$$

remainder = 1 ✓

Case 2: $n = 5a + 2$

$$n^2 = (5a+2)^2 = 25a^2 + 20a + 4$$
$$= 5(5a^2 + 4a) + \underbrace{4}$$

remainder = 4 ✓

Proof methods and strategies

Example: Prove that if n is any integer not divisible by 5, then n^2 leaves a remainder of 1 or 4 when divided by 5.

Proof (by cases):

<u>Case 1:</u> S'pose $n/5$ leaves a remainder of 1: $n = 5a + 1$ (for some integer a)

$\Rightarrow n^2 = (5a + 1)^2 = 25a^2 + 10a + 1 = 5(5a^2 + 2a) + 1$

$\Rightarrow n^2/5$ leaves a remainder of 1 ✔

<u>Case 2:</u> $n = 5a + 2$

$\Rightarrow n^2 = (5a + 2)^2 = 25a^2 + 20a + 4 = 5(5a^2 + 4a) + 4$

$\Rightarrow n^2/5$ leaves a remainder of 4 ✔

Proof methods and strategies

Example: Prove that if n is any integer not divisible by 5, then n^2 leaves a remainder of 1 or 4 when divided by 5.

Proof (by cases):

Case 3: $n = 5a + 3$

$n^2 = (5a+3)^2 = 25a^2 + 30a + 9$

$= 25a^2 + 30a + 5 + 4$

$= 5(5a^2 + 6a + 1) + \boxed{4}$

Case 4: $n = 5a + 4$ FYOG

For all 4 cases, if n is not divis. by 5, then n^2 has a remainder of 1 or 4 when divided by 5. ☒

Proof methods and strategies

Example: Let's open the hood on the logic here.

Proof by cases logic: We're using the fact (which we still need to show) that

$$\underbrace{(p_1 \lor p_2 \lor p_3 \lor p_4)}_{\text{cover all } p} \to q \;\equiv\; (p_1 \to q) \land (p_2 \to q) \land (p_3 \to q) \land (p_4 \to q)$$

want to distribute the $\to$ through

but need $\land$ or $\lor$ for distr.

So let's prove this logical equivalence.

$$(p_1 \lor p_2 \lor p_3 \lor p_4) \to q \equiv \neg(p_1 \lor p_2 \lor p_3 \lor p_4) \lor q \qquad \text{RBI}$$

$$\equiv (\neg p_1 \land \neg p_2 \land \neg p_3 \land \neg p_4) \lor q \qquad \text{De Morgan's}$$

$$\equiv (\neg p_1 \lor q) \land (\neg p_2 \lor q) \land \ldots \qquad \text{Distribution}$$

$$\equiv (p_1 \to q) \land (p_2 \to q) \land \ldots \qquad \text{RBI}$$

Proof methods and strategies

Example: Let’s open the hood on the logic here.

Proof by cases logic: We’re using the fact (which we still need to show) that

$$\underbrace{(p_1 \lor p_2 \lor p_3 \lor p_4)}_{\text{cover all } p} \rightarrow q \;\equiv\; (p_1 \rightarrow q) \land (p_2 \rightarrow q) \land (p_3 \rightarrow q) \land (p_4 \rightarrow q)$$

So let’s prove this logical equivalence.

$$\begin{aligned}
(p_1 \lor p_2 \lor p_3 \lor p_4) \rightarrow q &\equiv \neg(p_1 \lor p_2 \lor p_3 \lor p_4) \lor q && \text{(RBI)} \\
&\equiv (\neg p_1 \land \neg p_2 \land \neg p_3 \land \neg p_4) \lor q && \text{(De Morgan)} \\
&\equiv (\neg p_1 \lor q) \land (\neg p_2 \lor q) \land (\neg p_3 \lor q) \land (\neg p_4 \lor q) && \text{(distribution)} \\
&\equiv (p_1 \rightarrow q) \land (p_2 \rightarrow q) \land (\neg p_3 \rightarrow q) \land (\neg p_4 \rightarrow q) && \text{(RBI)}
\end{aligned}$$

$\square$

Proof methods and strategies

FYOG: Use a proof by cases to show that for real numbers x and y,
$\max(x, y) + \min(x, y) = x + y$.

Hint: You could use the cases: (1) $x \geq y$ and (2) $x < y$.

Note that you need one to be "or equal to" and the other to be strict inequality, otherwise there might be overlap between the two cases!

Proof methods and strategies

Example: Suppose you have two water jugs: one holds 5 gallons and the other holds 3 gallons. Assume you have an endless supply of water. Prove that an algorithm exists that allows you to measure out exactly 4 gallons of water just by transferring water between the two jugs (or pouring it down the drain, if that helps).

Think about it for a while!

Try to come up with an algorithm that will work.

Proof methods and strategies

Example: Suppose you have two water jugs: one holds 5 gallons and the other holds 3 gallons. Assume you have an endless supply of water. Prove that an algorithm exists that allows you to measure out exactly 4 gallons of water just by transferring water between the two jugs (or pouring it down the drain, if that helps).

Proof:

1. Pour 5G into the 5G jug.
2. Pour 3G. from the 5G jug into the 3G jug (leaving 2G in the 5G jug).
3. Pour the 3G in the 3G jug down the drain.
4. Pour the 2G from the 5G jug into the 3G jug.
5. Pour 5G into the 5G jug.
6. Pour 1G from the 5G jug into the 3G jug.

At this point, the 3G jug is full and **5G jug has 4G in it.**□

Proof methods and strategies

Example: Suppose you have two water jugs: one holds 5 gallons and the other holds 3 gallons. Assume you have an endless supply of water. Prove that an algorithm exists that allows you to measure out exactly 4 gallons of water just by transferring water between the two jugs (or pouring it down the drain, if that helps).

Proof:

1. Pour 5G into the 5G jug.
2. Pour 3G. from the 5G jug into the 3G jug (leaving 2G in the 5G jug).
3. Pour the 3G in the 3G jug down the drain.
4. Pour the 2G from the 5G jug into the 3G jug.
5. Pour 5G into the 5G jug.
6. Pour 1G from the 5G jug into the 3G jug.

At this point, the 3G jug is full and **5G jug has 4G in it.** □

Proved the **existence** of a solution to the problem by explicitly **constructing** it. Called a **proof by construction**.

Existence and uniqueness

Example: Show that if *n* is an odd integer, then there $\boxed{\textbf{exists}}$ a $\boxed{\textbf{unique}}$ integer *k* such that *n* is the sum of *k* - 2 and *k* + 3.

Existence and uniqueness

Example: Show that if *n* is an odd integer, then there **exists** a **unique** integer *k* such that *n* is the sum of *k* - 2 and *k* + 3.

This one is asking for two things:

1. Show that such an integer *k* exists.
2. Show that there is only one such *k* that does this.

Existence and uniqueness

Example: Show that if n is an odd integer, then there **exists** a **unique** integer k such that n is the sum of k - 2 and k + 3.

This one is asking for two things:

1. Show that such an integer k exists.
2. Show that there is only one such k that does this.

We typically tackle these **existence and uniqueness** proofs in two steps:

1) show existence by construction (i.e., actually find it).
2) show uniqueness by supposing that there are two such k, but then we do math and find out that they must be equal to each other

Existence and uniqueness

Example: Show that if n is an odd integer, then there **exists** a **unique** integer k such that n is the sum of k - 2 and k + 3.

Proof of existence:

- *Show* that such a k exists directly using our old friend, Algebra:

$n = k-2 + k+3 = 2k+1$ s'pose n is an odd integer

$\Rightarrow \frac{n-1}{2} = k$, which is an integer, b/c n is odd so n-1 is even

Existence and uniqueness

Example: Show that if n is an odd integer, then there **exists** a **unique** integer k such that n is the sum of k - 2 and k + 3.

Proof of existence:

- *Show* that such a k exists directly using our old friend, Algebra:
- S'pose n is an odd integer

  ⇒ $n = 2a + 1$, for some integer a

  ⇒ $n = 2a + 1 = (k - 2) + (k + 3) = 2k + 1$

  ⇒ $k = a$

  ⇒ so to find our k for any given odd $n = 2a + 1$, **take k = (n-1)/2** ✔

Existence and uniqueness

Example: Show that if n is an odd integer, then there **exists** a **unique** integer k such that n is the sum of k - 2 and k + 3.

Proof of uniqueness:

S'pose that there are two integers k & m. such that

$n = k-2 + k+3$ & $n = m-2 + m+3$

our job is to show that k & m must be =

$\Rightarrow n = k-2+k+3 = m-2+m+3$

$\Rightarrow 2k+1 = 2m+1$

$\Rightarrow 2k = 2m$

$\Rightarrow k = m$

∴ ~~any~~ the solution must be unique ∎

Existence and uniqueness

Example: Show that if n is an odd integer, then there **exists** a **unique** integer k such that n is the sum of k - 2 and k + 3.

Proof of uniqueness:

- S'pose two such numbers exist, k and m. That is:

  $n = (k - 2) + (k + 3)$ and $n = (m - 2) + (m + 3)$

  $\Rightarrow n = (k - 2) + (k + 3) = (m - 2) + (m + 3)$

  $\Rightarrow 2k + 1 = 2m + 1$

  $\Rightarrow k = m$

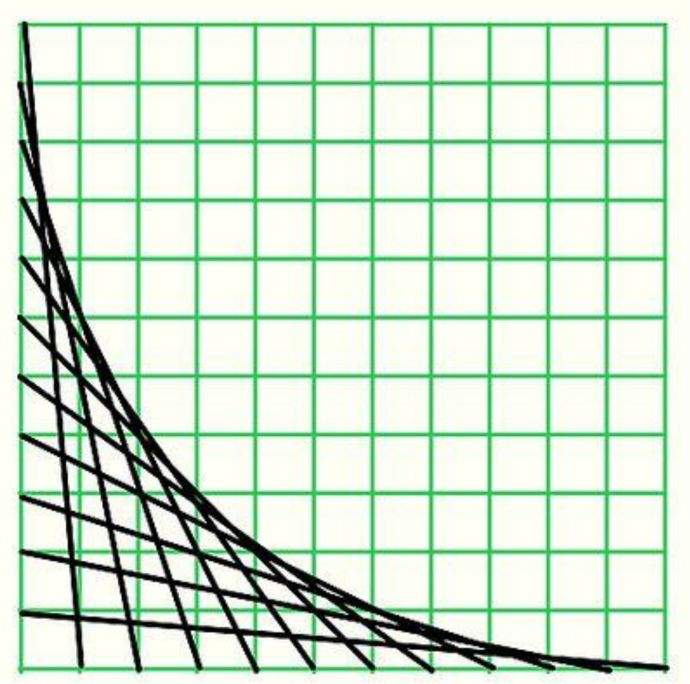
  Since any numbers that satisfy this problem are necessarily the same, the solution is **unique**. ✔

□

Existence and uniqueness

FYOG: Show that if *a, b* and *c* are real numbers with $a \neq 0$, then there **exists** a **unique** solution x to the equation $ax + b = c$.

Note: This is the statement that non-horizontal lines pass through each y coordinate exactly once.



Conditional proof (specific kind of direct proof)

HERE

x

Example: S'pose that anyone who is mad is evil. Let the domain be all people. Prove that all mad scientists are evil.

$M(x)$ $E(x)$ $S(x)$

$\forall x\,(M(x) \rightarrow E(x))$ premise

$\forall x\,((M(x) \wedge S(x)) \rightarrow E(x))$ conclusion

Conditional proof

Example: S'pose that anyone who is mad is evil. Let the domain be all people. Prove that all mad scientists are evil.

Proof:
Let $S(x)$ denote "x is a scientist"
Let $M(x)$ denote "x is mad"
Let $E(x)$ denote "x is evil"

Conditional proof

(3): If the person is Mad & a Scientist... then they must be evil (5)

Example: S'pose that anyone who is mad is evil. Let the domain be all people. Prove that all mad scientists are evil.

	Step	Justification
1.	$\forall x\,(M(x) \rightarrow E(x))$	premise
2.	$M(c) \rightarrow E(c)$	univ. instantiation (1), c is an arbitrary element of the domain
3.	$M(c) \wedge S(c)$	assumption for conditional proof
4.	$M(c)$	simplification (3)
5.	$E(c)$	modus ponens (2,4)
6.	$[M(c) \wedge S(c)] \rightarrow E(c)$	by conditional proof (3-5)
7.	$\therefore\ \forall x\,[\,(M(x) \wedge S(x)) \rightarrow E(x)\,]$	universal generalization (6)

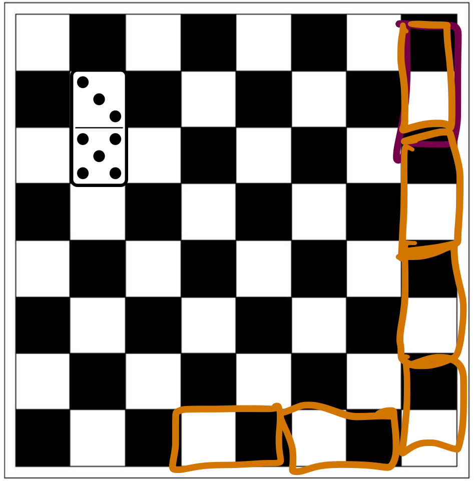
Conditional proof

Example: S’pose that anyone who is mad is evil. Let the domain be all people. Prove that all mad scientists are evil.

	Step	Justification
1.	$\forall x\,(M(x) \rightarrow E(x))$	premise
2.	$M(a) \rightarrow E(a)$	universal instantiation (1) (arb. *a*)
3.	$M(a) \land S(a)$	**assumption for conditional proof**
4.	$M(a)$	simplification (3)
5.	$E(a)$	modus ponens (2), (4)
6.	$[\,(M(a) \land S(a)) \rightarrow E(a)\,]$	**by conditional proof (3-5)**
7.	$\therefore\ \forall x\,[\,(M(x) \land S(x)) \rightarrow E(x)\,]$	universal generalization (6)

Disproving all things (or: looking for counterexamples)

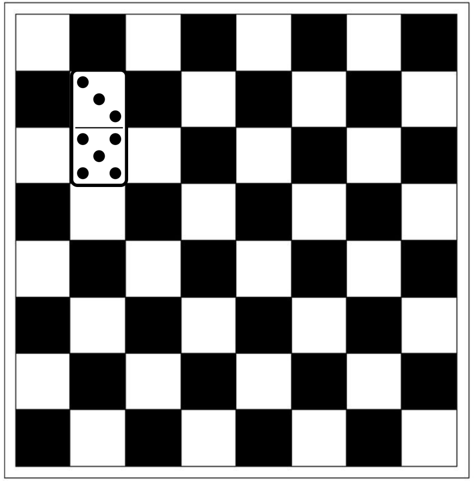
Example: Consider a standard 8x8 chessboard.



Can you completely cover the board in dominos that are the size of two squares?

Disproving all things (or: looking for counterexamples)

Example: Consider a standard 8x8 chessboard.

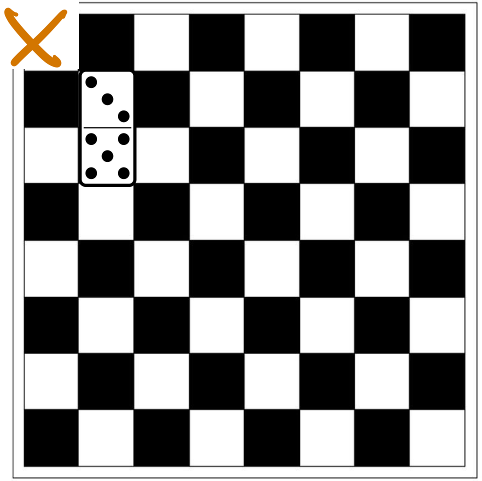


Can you completely cover the board in dominos that are the size of two squares?

⇒ **Yes.** There are **many** ways.

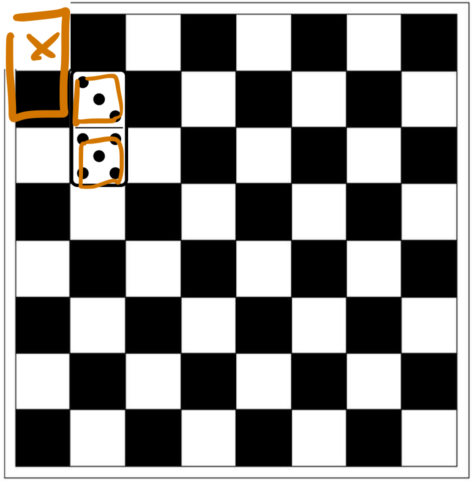
Disproving all things (or: looking for counterexamples)

Example: What about if we removed one of the corners?



Disproving all things (or: looking for counterexamples)

Example: What about if we removed one of the corners?

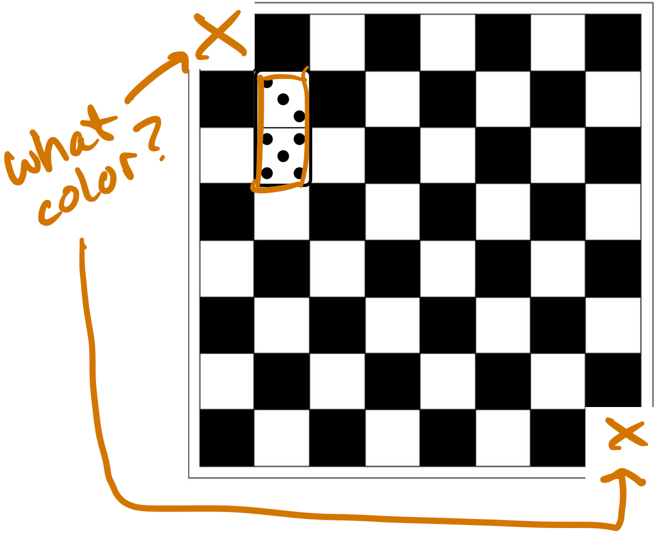


It might take a second, but you'll realize of course we can't!

- The domino tiles have 2 squares each, so we can only **tile** an even number of squares
- But with only 1 square removed, the chess board now has an *odd* number of squares

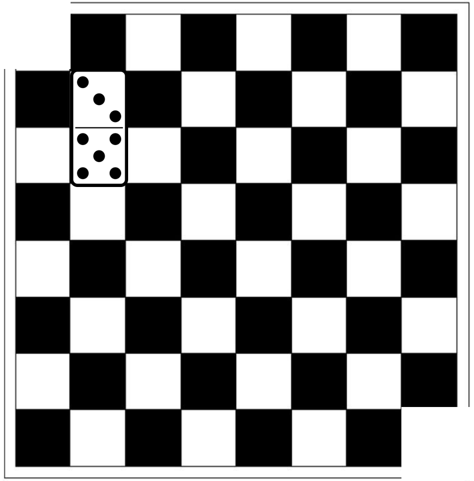
Disproving all things (or: looking for counterexamples)

Example: What about if we removed the opposite corner as well?



Disproving all things (or: looking for counterexamples)

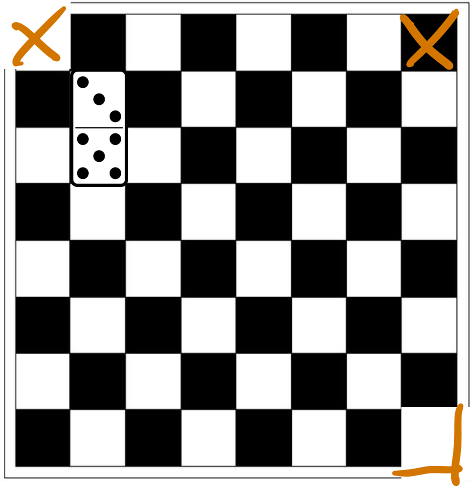
Example: What about if we removed the opposite corner as well?



This one is also tricky. Note that each domino must cover both a white and a black square.

Disproving all things (or: looking for counterexamples)

Example: What about if we removed the opposite corner as well?



prove it's possible to tile this: just need one example that works

This one is also tricky. Note that each domino must cover both a white and a black square.

Nope! Because we have fewer white squares than black ones now, and each domino must cover both a white and a black square.

Proof methods and strategies

Recap:

- We’ve seen now:
  - Proof by cases (exhaustive)
  - Proof by construction (existence) and the de facto method for proving uniqueness (s’pose two of them exist and show they must be the same thing)
- We’re going to keep coming back to proofs, so don’t purge it from your memory yet!

Next time:

- **Sets**
  - We have talked about “the set of all integers” for example… but what does that actually mean?
  - Could we make sets of arbitrary things? The set of all gray pants?

Bonus material!