CIS 160 - Fall 2012 (instructor Val Tannen)

Homeworks, with Solutions

HOMEWORK 1

Problem 1 (20pts)

(a) Let A, B, C, D be arbitrary sets. Prove that $(A \cap C) \cup (B \cap D) \subseteq (A \cup B) \cap (C \cup D)$.

Answer: Let $x \in (A \cap C) \cup (B \cap D)$ arbitrary.

Case 1 $x \in A \cap C$

$x \in A$ and $x \in C$

$x \in A \cup B$ and $x \in C \cup D$

$x \in (A \cup B) \cap (C \cup D)$

Case 2 $x \in B \cap D$

$x \in B$ and $x \in D$

$x \in A \cup B$ and $x \in C \cup D$

$x \in (A \cup B) \cap (C \cup D)$

In both cases $x \in (A \cup B) \cap (C \cup D)$.

(b) Let X, Y be nonempty sets and $f : X \to Y$ be a function with domain X and codomain Y. Recall that we denote by $f(D)$ the direct image through f of a subset $D \subseteq X$. Let $A, B \subseteq X$ be any two subsets of X. Prove that

1. $f(A \cap B) \subseteq f(A) \cap f(B)$

   Answer: Let $y \in f(A \cap B)$ arbitrary.

   Then there exists $x \in A \cap B$ s.t. $f(x) = y$.

   $x \in A$ and $x \in B$

   $f(x) \in f(A)$ and $f(x) \in f(B)$

   $y \in f(A)$ and $y \in f(B)$

   $y \in f(A) \cap f(B)$

2. $f(A) - f(B) \subseteq f(A - B)$

   Answer: Let $y \in f(A) - f(B)$ arbitrary.

   $y \in f(A)$ and $y \notin f(B)$

   Then there exists $x \in A$ s.t. $f(x) = y$.

   Because $f(x) \notin f(B)$ we cannot have $x \in B$ so $x \notin B$

   Then $x \in A - B$ so $f(x) \in f(A - B)$

   $y \in f(A - B)$

Problem 2 (20pts)

(a) Recall that a subset $A \subseteq X$ is *proper* if $A \neq X$. How many proper and nonempty subsets does a set with n elements have? (Give the answer and an explanation of how you figured it out. No proofs required.)

Answer: $2^n - 2$ for $n > 0$ and 0 for $n = 0$. Indeed, there are 2^n subsets of a set with n elements and out of these 2 are not proper: the empty susbset and the set itself. This gives $2^n - 2$. However, it is easy to forget that the question is asked for all possible n. And the explanation above needs to be amended for $n = 0$. In this case the set is empty, and there are no proper subsets. But note also that the two improper subsets are the same (empty) so the formula $2^n - 2$ is wrong! The best way to see that this case must be dealt with separately is to plug $n = 0$ into the formula $2^n - 2$ producing -1.

(b) Suppose that X has n elements and Y has $n + 2$ elements. How many injections $f : X \to Y$ are there? (Hint: use the Generalized Product Rule. Give the answer and an explanation of how you figured it out. No proofs required.)

Answer: $(n + 2)(n + 1) \cdots 3$. For an injection with domain X and codomain Y, distinct elements of X map to distinct elements of Y. Let's say that $X = \{a_1, a_2, \ldots, a_n\}$. There are $n + 2$ elements in Y to which we can map a_1, for each of these there are $n + 1$ left to map a_2, etc., until there are only 3 elements to map a_n. Using the Generalized Product Rule gives the answer. (Notice that this is the way we counted permutations in class. Indeed, there is a one-to-one correspondence (a bijection) between the set of injections from X to Y and the set of permutations of n elements out of $n + 2$.) *Alternative explanation.* Here is another way of counting the injections. For each injection first choose a set of two elements of Y to which *none* of the elements of X is mapped. This can be done in $\binom{n+2}{2}$ ways. For each of these we map distinct elements of X to distinct elements of the remaining n elements of Y. This can be done in $n!$ ways. So the answer is $\binom{n+2}{2}\, n!$. (Check that it equals the formula above).

(c) How many of the natural numbers between 100 and 1000 are either multiples of 3 or multiples of 7? (Give the answer and an explanation of how you figured it out. No proofs required.)

Answer: 385. The multiples of 3 between 100 and 1000 are 102, 105, …, 987, 990, 993, 996, 999. There are $(999 - 102)/3 + 1 = 300$ of them.

The multiples of 7 between 100 and 1000 are 105, 112, …, 987, 994. There are $(994-105)/7+1 = 128$ of them.

Now we might answer $300+128 = 428$. But it would be a mistake because we would have counted some numbers twice! Which ones? Those divisible by *both* 3 and 7 (see 105 and 987) in the lists above. These are exactly the number divisible by 21 and there are $(987 - 105)/21 + 1 = 43$. So, to account for counting them twice we calculate the answer as $300 + 128 - 43 = 385$.

(This kind of counting generalizes to the "principle of inclusion-exclusion" that we will learn about soon.)

Problem 3 (20pts)

Let X, Y be non-empty sets and $f : X \to Y$ be a function with domain X and codomain Y.

(a) Let $A, B \subseteq X$ be any two subsets of X. Prove that if f is an injection then $f(A \cap B) = f(A) \cap f(B)$.

Answer: By Problem 1(b)1 above we know that $f(A \cap B) \subseteq f(A) \cap f(B)$ for *any* function f. It remains to show that when f is actually an injection the other inclusion also holds: $f(A) \cap f(B) \subseteq f(A \cap B)$.

Let $y \in f(A) \cap f(B)$ arbitrary.

$y \in f(A)$ and $y \in f(B)$

Because $y \in f(A)$ there exists $x_1 \in A$ s.t. $f(x_1) = y$.

Because $y \in f(B)$ there exists $x_2 \in B$ s.t. $f(x_2) = y$.

Since $f(x_1) = y = f(x_2)$ and f is injective we have $x_1 = x_2$.

Therefore $x_1 \in B$, so $x_1 \in A \cap B$.

$f(x_1) \in f(A \cap B)$

$y \in f(A \cap B)$

(b) Prove that if for any $A, B \subseteq X$ we have $f(A \cap B) = f(A) \cap f(B)$ then f is an injection.

Answer: Assume that for any $A, B \subseteq X$ we have $f(A \cap B) = f(A) \cap f(B)$. We want to prove that f must be an injection. The key to this is to notice the *any*.

Let $x_1, x_2 \in X$ s.t. $f(x_1) = f(x_2)$. (And we want to show that $x_1 = x_2$.)

Choose $A = \{x_1\}$ and $B = \{x_2\}$. (Because of the "any" we can do this.)

Let $y = f(x_1) = f(x_2)$ so we have $f(A) = f(B) = \{y\}$ and therefore $f(A) \cap f(B) = \{y\}$.

From the assumption it follows that $f(A \cap B) = \{y\}$.

Then there exists $x \in A \cap B$ s.t. $f(x) = y$.

$x \in A$ therefore $x = x_1$.

$x \in B$ therefore $x = x_2$.

$x_1 = x_2$

(It is essential that the premise of the implication specifies "for any A, B". There are lots of possible A, B for which $f(A \cap B) = f(A) \cap f(B)$ holds (for example, when $A = B$) but f is not necessarily injective.)

HOMEWORK 2

Problem 1 (20pts)

(a) Give an example of finite sets X, Y and functions $f : X \to Y$ and $g : Y \to X$ such that

- $g \circ f$ is a bijection,
- $g \circ f$ is different from the identity function,
- f is not a surjection,
- g is not an injection, and
- X has exactly 2 elements.

You must justify why your $g \circ f$ is different from the identity function, why your f is not a surjection, and why your g is not an injection. No other proof is required.

Answer: Take $X = \{a, b\}$ and $Y = \{1, 2, 3\}$ and define

x	$f(x)$
a	2
b	1

y	$g(y)$
1	a
2	b
3	b

(The problem doesn't require proving this but it is easy to see that $g \circ f$ is a bjection by looking at its table:

x	$(g \circ f)(x)$
a	b
b	a

Now

(i) $g \circ f$ is different from the identity function because, for example, for the argument $a \in X$ we have $(g \circ f)(a) = g(f(a)) = g(2) = b \neq a = \mathsf{id}_X(a)$.

(ii) f is not a surjection because for $3 \in Y$ there is no $x \in X$ such that $f(x) = 3$.

(iii) g is not an injection because for $2, 3 \in Y$ we have $2 \neq 3$ but $f(2) = b = f(3)$.

(By the way, one can prove that if $g \circ f$ is a bijection then g is a surjection and f is an injection. However, as this problem shows neither has to be a bijection!)

(b) Given $f : X \to Y$ and $C \subseteq Y$ define

$$f^{-1}(C) = \{x \in X | f(x) \in C\}$$

(by the way, this is called the *inverse* image of C under f) Prove that for any $C, D \subseteq Y$ we have $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.

Answer: First we prove $f^{-1}(C \cap D) \subseteq f^{-1}(C) \cap f^{-1}(D)$.

Let $x \in f^{-1}(C \cap D)$
Then $f(x) \in (C \cap D)$
$f(x) \in C$ and $f(x) \in D$
$x \in f^{-1}(C)$
$x \in f^{-1}(D)$
$x \in f^{-1}(C) \cap f^{-1}(D)$.
Next we prove $f^{-1}(C) \cap f^{-1}(D) \subseteq f^{-1}(C \cap D)$.
Let $x \in f^{-1}(C) \cap f^{-1}(D)$
$x \in f^{-1}(C)$
$f(x) \in C$
$x \in f^{-1}(D)$
$f(x) \in D$
$f(x) \in C \cap D$
$x \in f^{-1}(C \cap D)$.

Alternative proof in the style of "chain of iffs, see tetxbook.
$x \in f^{-1}(C) \cap f^{-1}(D)$
iff $x \in f^{-1}(C)$ and $x \in f^{-1}(D)$
iff $f(x) \in C$ and $f(x) \in D$
iff $f(x) \in C \cap D$
iff $x \in f^{-1}(C \cap D)$.

(c) Let X, Y be non-empty finite sets and let $f : X \to Y$ be a k-to-one function ($k \geq 1$). (We already know that this means that f is, in particular, a surjection.) Prove by contradiction that if f is a bijection then k must be 1.

Answer: Assume that f is a bijection.

Suppose (hoping fervently to reach eventually a contradiction :) that $k \neq 1$, that is, $k \geq 2$.

Now, Y is nonempty so it has at least one element, say, $b \in Y$.

Because f is k-to-one, exactly k elements of X are mapped by f to b.

Because $k \geq 2$ there exist at least two *distinct* elements among those mapped to b by f.

Therefore, $\exists x_1, x_2 \in X$ s.t. $x_1 \neq x_2$ and $f(x_1) = b = f(x_2)$.

That means that f is not injective, and this contradicts the assumption that f is a bijection. (Yey.)

Problem 2 (20pts)

(a) How many sequences of bits of length 100 have as many 0's as 1's? (Give the answer and an explanation of how you figured it out. No proofs required.)

Answer: $\binom{100}{50}$.

Indeed it's the same as counting sequences of bits of length 100 with 50 1's. Which is the same as counting the number of ways of choosing 50 positions in the sequence in which to put 1's out of a total of 100 positions. Which is the same as the number of subsets of size 50 of a set of 100 elements, i.e., combinations of 50 out of 100.

(b) What is the coefficient of x^{20} in $(x + \frac{1}{x})^{100}$? (Give the answer and an explanation of how you figured it out. No proofs required.)

Answer: $\binom{100}{40}$.

Indeed, using the Binomial Theorem

$$(x + \frac{1}{x})^{100} = \sum_{k=0}^{100} \binom{100}{k} x^{100-k} (\frac{1}{x})^k = \sum_{k=0}^{100} \binom{100}{k} x^{100-2k}$$

Now $100 - 2k = 20$ implies $k = 40$.

(c) What is the number of ways to color the objects $a_1, a_2, \ldots, a_n$ $(n \geq 3)$ using 3 colors if every color must be used at least once? (Give the answer and an explanation of how you figured it out. No proofs required.)

Answer: $3^n - 3 \cdot 2^n + 3$.

The number of ways to color those objects with 3 colors is (by the Product Rule) $3 \times 3 \times \cdots \times 3 = 3^n$.

But wait. Among these ways we also counted the ones that use just two or just one color. We have to count *these* special ways and subtract.

Let's say the colors are red, green and blue. By the product rule again there are 2^n ways to color with just red and green, 2^n with just green and blue, and again 2^n with just blue and red. So it looks like the answer is $3^n - 2^n - 2^n - 2^n$.

But wait (again!). In the second step we counted the ways to color with just one color *twice.* For example we counted coloring with just red when we counted red or green and again when we counted blue and red. There is exactly one way to color with just red, and the same for green and blue.

So the number of ways to color with just two or just one color is $2^n + 2^n + 2^n - 1 - 1 - 1 = 3 \cdot 2^n - 3$. Hence the answer.

(Sanity check: let's if the answer makes sense when $n = 3$. When we have only 3 objects using all colors means that the number of ways to color is the same as the number of permutations of the three colors, $3! = 6$. And indeed $3^3 - 3 \cdot 2^3 + 3 = 6$.)

HOMEWORK 3

Problem 1 (20pts)

(a) How many ways are there to place m distinguishable objects into n distinguishable bins? Each object must be placed in some bin but some bins may remain empty. There is no limit on how many objects can be placed in each bin. (Give the answer and an explanation of how you figured it out. No proofs required).

Answer: There are n^m ways of putting m distinguishable objects into n distinguishable bins. There are n bins the first object can go into. Next, there are n bins the second object can go into, as multiple objects can go in the same bin.. This continues until all the objects have been assigned. By the Product Rule the total number of ways of putting the objects into the bins is then $n * n * n * ... * n = n^m$. The is the same as the number of functions from a domain of size m to a domain of size n, which, if you recall, we counted in the same way.

(b) Assume $m \leq n$. How many ways are there to place m distinguishable objects into n distinguishable bins such that each bin can contain at most on object? Each object must be placed in some bin. (Give the answer and an explanation of how you figured it out. No proofs required).

Answer: (first version) We do this in two phases. First we choose the bins we want to place in (this handles the distinguishable bins). There are $\binom{n}{m}$ ways of doing this. Each bin amongst this selection must contain exactly one object. There are $m!$ ways of placing these objects into the bins (this handles the distinguishable objects). By the Generalized Product Rule we multiply to get the answer:

$$\binom{n}{m} m!$$

Answer: (second version) We use the Generalized Product Rule from the beginning. For the first object there are n bins we can place it in. Once we place the first object we have only $n-1$ bins to choose from for the second object. Then we have $n-2$ for the third, etc. The answer is

$$n(n-1)\cdots(n-m+1)$$

This equals the number obtained in the first version and further equals the number of permutations of m out of n, which we counted in class (where we also counted in two ways).

(c) How many ways are there to place m indistinguishable objects into n distinguishable bins? Each object must be placed in some bin but some bins may remain empty. There is no limit on how many objects can be placed in each bin. (Give the answer and an explanation of how you figured it out. No proofs required).

Answer: (This is a generalization of the 12 donuts of 5 flavors problem in the textbook that we also did in class.) We arrange the objects m in a row. Since the objects are indistinguishable it does not matter how we do this. Now, dividing them in n bins is equivalent to placing $n-1$ separators between them: the objects between the beginning of the row and the first separator in the first bin, between the first and second separator in the second bin, etc. Two separators may be adjacent to each other; this would correspond to leaving a bin empty. The number of ways of doing this is counted by considering the set of positions of this decorated row (objects + separators). There are $m+n-1$ positions and each way corresponds to choosing $n-1$ out of them to put separators in (or, equivalently, choosing m of the positions to objects in). Hence the answer is

$$\binom{m+n-1}{n-1}$$

Problem 2 (20pts)

Function composition can be generalized to *binary relation composition* with the following definition. If $R \subseteq X \times Y \text{and} S \subseteq Y \times Z$ are binary relations define $S \circ R \subseteq X \times Z$ as follows

$$S \circ R = \{(x,z) \in X \times Z | \; \exists y \in Y \text{s.t.} (x,y) \in R \text{ and } (y,z) \in S\}$$

(a) Prove that this composition is *associative*, i.e., prove that $\forall R \subseteq X \times Y, S \subseteq Y \times Z, T \subseteq Z \times U$ we have $T \circ (S \circ R) = (T \circ S) \circ R$.

Answer: We want to prove that $T \circ (S \circ R) = (T \circ S) \circ R$. These two relations have the same domain, X, and the same codomain, Z, so we only have to show that they have the same graph. The graphs are sets (of pairs) so we show their equality as usual, by showing inclusions both ways.

First we prove

$$T \circ (S \circ R) \subseteq (T \circ S) \circ R$$

Let $(x,u) \in T \circ (S \circ R)$, arbitrary.
$\exists z \in Z$ s.t. $(x,z) \in S \circ R$ and $(z,u) \in T$
$\exists y \in Y$ s.t. $(x,y) \in R$ and $(y,z) \in S$
$(y,z) \in S$ and $(z,u) \in T$ imply that $(y,u) \in T \circ S$ (by definition of relation composition)
Then $(x,y) \in R$ and $(y,u) \in T \circ S$ imply that $(x,u) \in (T \circ S) \circ R$.
Next we prove

$$(T \circ S) \circ R \subseteq T \circ (S \circ R)$$

Let $(x,u) \in (T \circ S) \circ R$, arbitrary.
$\exists y \in Y$ s.t. $(x,y) \in R$ and $(y,u) \in T \circ S$
$\exists z \in Z$ s.t. $(y,z) \in S$ and $(z,u) \in T$

$(x, y) \in R$ and $(y, z) \in S$ imply that $(x, z) \in S \circ R$
Then $(x, z) \in S \circ R$ and $(z, u) \in T$ imply that $(x, u) \in T \circ (S \circ R)$.
Hence, $T \circ (S \circ R) = (T \circ S) \circ R$ and $\circ$ is associative.

(b) For any set X define the binary relation $\Delta_X \subseteq X \times X$ by

$$\Delta_X = (x, x)|x \in X$$

Prove that $\forall R \subseteq X \times Y \ R \circ \Delta_X = R$
(Clearly the other direction is similar. In algebra we say that the Δ's are *identities* with respect to the operation of composition).

Answer: We want to show $R \circ \Delta_X \subseteq R$ and $R \subseteq R \circ \Delta_X$.
Let $(x, y) \in R \circ \Delta_X$ arbitrary.
$\Rightarrow \exists x' \in X$ such that $(x, x') \in \Delta_X$ and $(x', y) \in R$.
But because of the definition of $\Delta_X, x = x'$.
Thus, $(x, y) \in R \circ \Delta_X \Rightarrow \exists x'$ such that $(x, x) \in \Delta_X$ and $(x, y) \in R$.
$\Rightarrow \forall\ (x, y) \in R \circ \Delta_X, (x, y) \in R$.
So we have shown $R \circ \Delta_X \subseteq R$. Now we want to show $R \subseteq R \circ \Delta_X$.
Let $(x, y) \in R$ arbitrary.
Then $x \in X$.
By the definition of Δ_X we have $(x, x) \in \Delta_X$.
Thus, $\exists x' \in X$ such that $(x, x') \in \Delta_X$ and $(x', y) \in R$, namely x' is x itself. Therefore $(x, y) \in R \circ \Delta_X$!
Thus, $R \subseteq R \circ \Delta_X$ as needed.

(c) Show that composition of binary relations whose domain and codomain are the same is in general *not commutative.* That is, give two relations $R, S \subseteq X \times X$ such that $S \circ R \neq R \circ S$ (a *counterexample*)

Answer: Review the definitions:
$S \circ R = \{(x_1, x_3) \in X \times X \quad | \quad \exists x_2 \in X \text{ s.t. } (x_1, x_2) \in R \text{ and } (x_2, x_3) \in S\}$,
$R \circ S = \{(x_1, x_3) \in X \times X \quad | \quad \exists x_2 \in X \text{ s.t. } (x_1, x_2) \in S \text{ and } (x_2, x_3) \in R\}$
Now take $X = \mathbb{R}$ and define
$R = \{(x_1, x_2) \in X \times X \quad | \quad x_2 = x_1^2\}$ and
$S = \{(x_1, x_2) \in X \times X \quad | \quad x_2 = x_1 + 2\}$.
Now $x_2 = x_1 + 2$ and $x_3 = x_2^2 \iff x_3 = (x_1 + 2)^2\}$
while $x_2 = x_1^2$ and $x_3 = x_2 + 2 \iff x_3 = x_1^2 + 2\}$

Therefore,
$R \circ S = \{(x_1, x_3) \in X \times X \quad | \quad \exists x_2 \in X \text{ s.t. } x_3 = (x_1 + 2)^2\}$
$S \circ R = \{(x_1, x_3) \in X \times X \quad | \quad \exists x_2 \in X \text{ s.t. } x_3 = x_1^2 + 2\}$

Since there exist $x_1 \in \mathbb{R}$ such that $x_1^2 + 2 \neq (x_1 + 2)^2$, the compositions $S \circ R$ and $R \circ S$ are two different relations entirely. Composition of relations is in general *not commutative.*

(d) Show with a counterexample that the inverse of a relation is not an inverse in the sense used in algebra, that is give a relation $R \subseteq X \times X$ such that $R^{-1} \circ R \neq \Delta_X$.

Answer: Assume that $X = \{x_1, x_2\}$ and consider the relation R with domain X and codomain X and graph $\{(x_1, x_2), (x_2, x_2)\}$.
By definition of inverse relations, the domain of R^{-1} is X, the codomain is also X and the graph is $\{(x_2, x_1), (x_2, x_2)\}$.
By definition of composition of relations $R^{-1} \circ R = \{(x_1, x_1), (x_1, x_2), (x_2, x_1), (x_2, x_2)\}$.
So, $R^{-1} \circ R \neq \Delta_X$ because $\Delta_X = \{(x_1, x_1), (x_2, x_2)\}$.

Problem 3 (20pts)

Recall the definition of direct image of a subset A of the domain X under a binary relation $R \subseteq X \times Y$:

$$R(A) = \{y \in Y | \exists x \in As.t.(x, y) \in R\}$$

Recall that $pow(X) = \{A | A \subseteq X\}$. Now consider the function $d_R : pow(X) \to pow(Y)$ such that $\forall A \in pow(X)\ d_R(A) = R(A)$.

(a) Let $R \subseteq X \times Y$ and $S \subseteq Y \times Z$ be binary relations. Prove that $d_{S \circ R} = d_S \circ d_R$. (For the definition of $S \circ R$ see problem 2).

Answer: We have to show that the function $d_{S \circ R}$ is equal to the function $d_S \circ d_R$. For two functions to be equal they must have the same domain and codomain and must map the same argument to the same value (we can also say: on any input, the output is the same).
Both these functions have domain $pow(X)$ and codomain $pow(Z)$.
Now consider an arbitrary argument $M \in pow(X)$. We need to show that $(d_S \circ d_R)(M) = d_{S \circ R}(M)$ which is the equality of two sets, in fact two subsets of Z.
First we show $d_{S \circ R}(M) \subseteq (d_S \circ d_R)(M)$.
Consider $z \in d_{S \circ R}(M)$, arbitrary.
Since $d_{S \circ R}(M) = (S \circ R)(M)$, by definition of direct image through a relation $\exists x \in M$ s.t. $(x, y) \in S \circ R$.
By definition of $S \circ R$, $\exists y \in Y$ s.t. $(x, y) \in R$ and $(y, z) \in S$.

$y \in R(M)$ therefore $y \in d_R(M)$ (by definition of d_R).

$z \in S(d_R(M))$ therefore $z \in d_S(d_R(M)$

Next we show $d_S \circ d_R(M) \subseteq d_{S \circ R}(M)$

Let $z \in (d_S \circ d_R)(M)$, arbitrary.

$z \in d_S(d_R(M))$ therefore $z \in S(d_R(M)$.

$\exists y \in d_R(M)$ (therefore $y \in R(M)$) s.t. $(y, z) \in S$.

$\exists x \in M$ s.t. $(x, y) \in R$

$(x, z) \in S \circ R$

$z \in (S \circ R)(M)$ therefore $z \in d_{S \circ R}(M)$

So, as we've shown each is contained in the other, the two sets are equal!

(b) Prove that $d_{\Delta_X} = id_{pow(X)}$. (Recall that id_U is the identity function with domain U and codomain U, that is $\forall U \; id_U(x) = x$).

Answer: The question asks us again to prove that two functions are equal. The domains and codomains are the same, namely $pow(X)$.

Now we have to prove that for any $A \in pow(X)$ we have $d_{\Delta_X}(A) = id_{pow(X)}(A)$, that is, $\Delta_X(A) = A$. This is the equality of two sets and we proceed as usual.

Let $x \in \Delta_X(A)$, arbitrary.

Then, there exists $x' \in A$ s.t. $(x', x) \in \Delta_X$.

But $(x', x) \in \Delta_X$ implies $x' = x$ (by definition of the graph of Δ_X).

Therefore $x \in A$.

Now let $x \in A$, arbitrary.

Since $x \in X$ we have $(x, x) \in \Delta_X$

Therefore $x \in \Delta_X(A)$.

We have shown both $\Delta_X(A) \subseteq A$ and $A \subseteq \Delta_X(A)$ therefore these sets are equal.

(c) Show with counterexamples that, in general, d_R is neither an injective function nor a surjective function.

Answer: We can take X, Y to be any nonempty sets (think about what happens when they are empty!) but let's say $X = \mathbb{N}$ and $Y = \mathbb{R}$. Take R to be the relation with domain $\mathbb{N}$, codomain $\mathbb{R}$ and whose graph is *empty* (no pairs).

Then, for any $A \in pow(\mathbb{N})$ we have $d_R(A) = \emptyset$. This function is not injective because, for example, $\emptyset \neq \{37\}$ but $d_R(\emptyset) = d_R(\{37\})$. This function is not surjective because, for example, there is no $A \subseteq \mathbb{N}$ such that $d_R(A) = \{2.71, 3.14\}$.

(d) Explain how part (c) above should imply that for binary relations $R \subseteq X \times X$, in general, it is not the case that the functions d_R and $d_{R^{-1}}$ are inverse to each other. (You may need to adjust the counterexamples in part (c) for this to work properly).

Answer: If a function is not injective, then that function cannot have an inverse. In problem 3c) we demonstrated that d_R need not be injective or surjective. Hence, we must give a example of a relation $R \subseteq X \times X$ such that d_R is not a injection.
Example:
Let X $= \{1, 2, 3\}$ and $R = \{(x, 3)|x \in X\}$
Let $d_R(A) = \{3\}\forall A \subseteq X$
For this example, R is not injective, since $d_R(\{1, 2\}) = d_R(\{2, 3\})$, but $\{1, 3\} \neq \{2, 3\}$.
Hence, we have shown that not all binary relations $R \subseteq X \times X$ allow d_R and $d_{R^{-1}}$ to be injective. In these cases, d_R and $d_{R^{-1}}$ are not inverses.
Note that if the counterexample in 3c) was not from a set X to itself, then it is not a valid counterexample for this problem.

Problem 4 (20pts)

(a) What is the minimum number of people that need to be in a group to ensure that at least 4 people were born in the same month of the year and on the same day of the week? Explain how you applied the pigeonhole principle to get your answer (you need to identify the pigeons, the pigeonholes and the function that assigns pigeons to the pigeonholes).

Answer: The set of pigeons is a set of people. The set of pigeonholes is the set of pairs (my, dw) where my are possible months of the year (e.g., February) and there are 12 of these, while dw are the possible days of the week (e.g., Tuesday) and there are 7 of these. The function that maps pigeons to pigeonholes is the function that maps a person to the pair of her/his birth month of the year and his/her day of the week. In this problem we need the Generalized Pigeonhole Principle because we want at least one pigeonhole used by 4 pigeons or more. The size of the set of pigeoholes is $12 \cdot 7 = 84$. To have the same pigeonhole used by $4 = 3 + 1$ pigeons or more, we need the set of pigeons to have size *strictly* bigger than $3 \cdot 84 = 252$. That is, we need a minimum of $252 + 1 = 253$ people.

(b) Show how to use the Pigeonhole Principle (you need to identify the pigeons, the pigeonholes and the function that assigns pigeons to the pigeonholes) to prove that there exist two natural numbers $m, n \geq 1$ such that $37^m - 37^n$ is divisible by 10.

Answer: First observe that an integer is divisible by 10 iff its least significant digit (the digit in the "ones" position) is 0. Therefore $37^m - 37^n$ is divisible by 10 iff 37^m and 37^n have the *same* least significant digit. Therefore we have to show that that there exist two natural numbers $m, n \geq 1$ such that 37^m and 37^n have the same least significant digit.

In fact, we can show more: in any set of 11 natural numbers there exist two of them, distinct, call them m and n, such that 37^m and 37^n have the same least significant digit. This follows immediately from the Pigeonhole Principle if we take the set of pigeons to be the set of 11 numbers considered, the pigeonholes to be the digits $0, 1, \ldots, 9$ (there are 10 of them and $11 > 10$) and the function that maps pigeons to pigeonholes as the function that maps p to the least significant digit of 37^p.

(c) Show how to use the principle of inclusion exclusion to count how many of the numbers between 100 and 1000 are divisible by 3 or 7 or 11.

Answer: Let's denote as A_3 the set of all numbers between $100 - 1000$ that are divisible by 3, as A_7 the set of numbers between $100 - 1000$ that are divisible by 7 and by A_{11} the set of numbers between $100 - 1000$ that are divisible by 11. We need to compute $|A_3 \cup A_7 \cup A_{11}|$. We can observe that those three sets are not disjoint because there are numbers between $100 - 1000$ that are divisible by two or all of $3, 7, 11$. For example 231 is divisible by all of them. Thus, we need to use the inclusion-exclusion rule to find the size of their union.

Let's compute the union of the first pair of two of those sets.

$S_1 = |A_3 \cup A_7| = |A_3| + |A_7| - |A_3 \cap A_7|$

By the same rule and if we use the above,

$$\begin{aligned}
|A_3 \cup A_7 \cup A_{11}| &= |(A_3 \cup A_7) \cup A_{11}| && (1)\\
&= |S_1 \cup A_{11}| && (2)\\
&= |S_1| + |A_{11}| - |S_1 \cap A_{11}| && (3)\\
&= |A_3 \cup A_7| + |A_{11}| - |(A_3 \cup A_7) \cap A_{11}| && (4)\\
&= |A_3| + |A_7| - |A_3 \cap A_7| + |A_{11}| - |(A_3 \cup A_7) \cap A_{11}| && (5)
\end{aligned}$$

And from the distributive law of sets, we get,

$$|S_1 \cup A_{11}| = |A_3| + |A_7||A_3| + |A_7| - |A_3 \cap A_7| + |A_{11}| - |(A_3 \cap A_{11}) \cup (A_7 \cap A_{11})| \qquad (6)$$

Now, if we denote as $S_2 = A_3 \cap A_{11}$ and $S_3 = A_7 \cap A_{11}$ then, by the inclusion-exclusion rule again, we have,

$$\begin{aligned}
|(A_3 \cap A_{11}) \cup (A_7 \cap A_{11})| &= |S_2 \cup S_3| && (7)\\
&= |S_2| + |S_3| - |S_2 \cap S_3| && (8)\\
&= |A_3 \cap A_{11}| + |A_7 \cap A_{11}| - |A_3 \cap A_{11} \cap A_7 \cap A_{11}| && (9)\\
&= |A_3 \cap A_{11}| + |A_7 \cap A_{11}| - |A_3 \cap A_7 \cap A_{11}| && (10)
\end{aligned}$$

So, if we combine all the above, we get:

$|A_3 \cup A_7 \cup A_{11}| = |A_3| + |A_7| + |A_{11}| - |A_3 \cap A_7| - |A_3 \cap A_{11}| - |A_7 \cap A_{11}| + |A_3 \cap A_7 \cap A_{11}|$

Now we know that the numbers that belong to $A_3 \cap A_7$ are the numbers that are divisible by both 3 and 7. Thus, they are divisible by 21 because for all $x \in (A_3 \cap A_7)$ it must hold that $x = 3 \times 7 \times k = 21 \times k$, k is a natural number. The sane holds for $A_3 \cap A_{11}$, A_7, A_{11} and $A_3 \cap A_7 \cap A_{11}$.

So we need to find $|A_3|$, $|A_7|$, $|A_{11}|$, $|A_3 \cap A_7| = |A_{21}|$, $|A_3 \cap A_{11}| = |A_{33}|$, $|A_7 \cap A_{11}| = |A_{77}|$ and $|A_7, A_{11}$ and $A_3 \cap A_7 \cap A_{11}| = |A_{231}|$, and apply the above equation.

HOMEWORK 4

Problem 1 (20pts)

(a) Prove by induction that for any real number $q \neq 1$ and any $n \in \mathbb{N}$ we have

$$\sum_{i=0}^{n} q^i = \frac{q^{n+1} - 1}{q - 1}$$

(this is the sum of a *geometric progression*).

Answer: We will prove that $\sum_{i=0}^{n} q^i = \frac{q^{n+1}-1}{q-1}$ by induction.

- (BASE CASE) For $n = 0$, we have $\sum_{i=0}^{0} q^i = q^0 = 1$ and $\frac{q^{0+1}-1}{q-1} = \frac{q^1-1}{q-1} = \frac{q-1}{q-1} = 1$.
- (INDUCTION STEP) Let $k \in \mathbb{N}$. Assume that the equation holds for $n = k$ (INDUCTION HYPOTHESIS). We will show that it follows that the same equation holds for $n = k + 1$. We write explicitely the induction hypothesis: $\sum_{i=0}^{k} q^i = \frac{q^{k+1}-1}{q-1}$.
For $n = k + 1$, we can write $\sum_{i=0}^{k+1} q^i$ as $(\sum_{i=0}^{k} q^i) + q^{k+1}$. From the induction hypothesis we get that the above is equal to $\frac{q^{k+1}-1}{q-1} + q^{k+1}$ and now, we can easily compute that, $\frac{q^{k+1}-1}{q-1} + q^{k+1} = \frac{q^{k+1}-1}{q-1} + \frac{q^{k+1}(q-1)}{q-1} = \frac{q^{k+1}-1}{q-1} + \frac{q^{k+2}-q^{k+1}}{q-1} = \frac{q^{k+2}-1}{q-1}$. Therefore $\sum_{i=0}^{k+1} q^i = \frac{q^{k+2}-1}{q-1}$, which is what we wanted to show.

(b) Prove by induction that the number of subsets of a set with n elements is 2^n.

Answer: Recall that the set of all subsets of S is also called the powerset of S, notation pow(S).

So we restate what we have to prove: for any $n \in \mathbb{N}$, for any set S such that $|S| = n$ we have $|\text{pow}(S)| = 2^n$.

(BASE CASE) $n = 0$. Any set with 0 elements is empty. $\text{pow}(\emptyset) = \{\emptyset\}$ so it has 1 element. Since $1 = 2^0$ the base case is verified.

(INDUCTION STEP) Let $k \in \mathbb{N}$. Assume that for any set S such that $|S| = k$ we have $|\text{pow}(S)| = 2^k$ (INDUCTION HYPOTHESIS).

Now we want to show that from the induction hypothesis it follows that for any set S' such that $|S'| = k+1$ we have $|\text{pow}(S')| = 2^{k+1}$. (The induction hypothesis says "for any S..." while this statement that we want to prove says "for any S'...". The choice of a different notation, S' instead of S is just for clarity we could have used S again but the exact name of variables in a universal or existential quantification only matters *inside* the quantification; outside the name has no special meaning.)

Let S' be a set with $k+1$ elements. Let the name of one of these elements be a. We decompose $\text{pow}(S')$ into two disjoint sets: the set A whose elements are the subsets of S' that contain a and the set B whose elements are the subsets of S' that do *not* contain a. By the Sum Rule $|\text{pow}(S')| = |A| + |B|$.

Define $S = S' - \{a\}$. The elements of B are exactly the subsets of S, that is, $B = \text{pow}(S)$. Now S has k elements therefore we can apply the induction hypothesis to obtain $|B| = 2^k$.

Next we argue that $|A| = |B|$, i.e., there are exactly as many subsets of S' that contain a as there are subsets that do not contain a. (Remember this! It may prove useful in another context.) We show this by establishing a bijection between B and A. This function $f : B \to A$ is defined as follows: for each element R of B, that is, each subset of $R \subseteq S$, define $f(R) = R \cup \{a\}$. In keeping with our practice of not proving in detail that the functions used in the Bijection Rule are actually bijections, we can skip these details (but it would be useful for you to think why f is an injection and why it is a surjection). Therefore $|A| = |B| = 2^k$.

Finally $|\text{pow}(S')| = |A| + |B| = 2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$.

(By the way, in the induction step k could well be 0. It is instructive to check how the reasoning in this case particularizes.)

(c) Prove by induction that any sequence of bits of length at least 2 that starts with a 0 and ends with a 1 must have somewhere a 0 followed immediately by a 1.

Answer: So we need to prove that for any natural number $n \geq 2$, any sequence of bits of length n that starts with a 0 and ends with a 1 must have somewhere a 0 followed immediately by a 1.

Step 1 - Base Case Show true for $n = 2$:

A sequence of length 2 that starts with a 0 and ends with a 1 must equal 01 and therefore it contains a 0 immediately followed by a 1.

Step 2 - Inductive step Let $n \geq 2$ arbitrary. Assume true for n (INDUCTION HYPOTHESIS) , prove true for $n+1$.

Consider any sequence s of $n+1$ bits that starts with a 0 and ends with a 1. Since $n \geq 2$ this sequence has at least length 3 so the n's bit is neither the first nor the last bit. We have two cases.

Case 1: the n's bit of s is a 0. Then the last two bits are 01 and s has a 0 followed immediately by a 1.

Case 2: the n's bit of s is a 1. Then the sequence consisting of the first n bits of s is a sequence of length n that begins with a 0 and ends with a 1. By induction hypothesis this sequence has somewhere a 0 followed immediately by a 1 and therefore so does s.

Problem 2 (20pts)

(a) Let $f : \mathbb{N} \to \mathbb{N}$ be a function such that $f(0) = 1$ and $\forall m \in \mathbb{N}\ f(m+1) = 2f(m)$. Prove by induction that for any $n \in \mathbb{N}$ we have $f(n) = 2^n$.

Answer: First we must prove the Base Case which is $n = 0$. $f(0) = 2^0 = 1$, and therefore the base case is true.

Next we must prove the Induction Step. Let n be an arbitrary natural number. Assume the Induction Hypothesis which states that the equation is true for n. Now we want to prove $f(n+1) = 2^{n+1}$. We use the property $f(m+1) = 2f(m)$ that holds for any natural number m. Hence

$$\begin{aligned} f(n+1) &= 2 \cdot f(n) \\ &= 2 \cdot (2^n) \\ &= 2^{n+1} \end{aligned}$$

(b) Let $f : \mathbb{N} \to \mathbb{N}$ be a function such that $\forall m \in \mathbb{N}\ f(m+1) - f(m) \leq 7$. Prove by induction that for any $n \in \mathbb{N}$ we have $|f(n) - f(0)| \leq 7n$.

Answer: To prove by induction, we prove a base case and an inductive step.
Base case: n=0
$|f(n) - f(0)| = |f(0) - f(0)| = 0 = 7n$, so
$|f(n) - f(0)| \leq 7n$ for the base case.

Inductive step: Let n be arbitrary. Assume that $|f(n) - f(0)| \leq 7n$ and prove it for $n + 1$:
$|f(n+1) - f(0)| = |f(n+1) - f(n) + f(n) - f(0)| \leq |f(n+1) - f(n)| + |f(n) - f(0)|$
(did you know that for any $a, b \in \mathbb{R}$ $|a + b| \leq |a| + |b|$?)
$|f(n+1) - f(n)| + |f(n) - f(0)| \leq 7 + 7n$ (by f's property and by induction hypothesis, respectively)

Therefore, $|f(n+1) - f(0)| \leq 7 + 7n = 7(n+1)$

Since we have shown that the base case holds and that
$|f(n) - f(0)| \leq 7n \Rightarrow |f(n+1) - f(0)| \leq 7(n+1)$,
we have shown the statement to be true for all $n \in \mathbb{N}$

(c) Let $f : \mathbb{N} \to \mathbb{N}$ be a function such that $f(0) = 0$, $f(1) = 2$, and $\forall m \in \mathbb{N}\ m \geq 2 \Rightarrow f(m) = 4(f(m-1) - f(m-2))$. Prove by strong induction that for any $n \in \mathbb{N}$ we have $f(n) = n2^n$.

Answer: Given

$f(0) = 0$

$f(1) = 2$

$f(m) = 4(f(m-1) - f(m-2))$

To prove that: $f(n) = n2^n$

- Base Case: $f(0) = 0$ and $f(1) = 2$
- Let $n \geq 1$ arbitrary. Induction Hypothesis: $f(k) = k2^k$ for all natural numbers $k \leq n$
  To show that: $f(n+1) = (n+1)2^{n+1}$

$$\begin{aligned}
f(n+1) &= 4(f(n) - f(n-1)) && (11)\\
&= 4(n2^n - (n-1)2^{n-1}) \text{ Using Induction hypothesis} && (12)\\
&= n2^{n+2} - (n-1)2^{n+1} && (13)\\
&= (2n - (n-1))2^{n+1} && (14)\\
&= (n+1)2^{n+1} && (15)
\end{aligned}$$

Problem 3 (20pts)

(a) Recall the definition of the Fibonnaci numbers:

$$F_0 = 0 \qquad F_1 = 1 \qquad F_{n+2} = F_{n+1} + F_n$$

Prove by strong induction that for all $n \in \mathbb{N}$ we have

$$F_n + 2F_{n+1} = F_{n+4} - F_{n+2}$$

Answer: $F_n + 2 \cdot F_{n+1} = F_{n+4} - F_{n+2}$ Proof by strong induction!
Base case: $n = 0$
$F_0 + 2 \cdot F_{0+1} = 0 + 2 \cdot 1 = 2.$
$F_{0+4} - F_{0+2} = 3 - 1 = 2.$
Base case: $n = 1$
$F_1 + 2 \cdot F_{1+1} = 1 + 2 = 3.$
$F_{1+4} - F_{1+2} = 5 - 2 = 3.$
Induction Step: Let $n \geq 1$ arbitrary. Assume true for all $k \leq n$, prove true for $n+1$
$F_{n+1} + 2 \cdot F_{n+2} = (F_{n-1} + F_n) + 2 \cdot (F_n + F_{n+1})$
$= (F_{n-1} + 2 \cdot F_n) + (F_n + 2 \cdot F_{n+1})$
$= (F_{n+3} - F_{n+1}) + (F_{n+4} - F_{n_2})$ by (strong) induction hypothesis

$= (F_{n+3} + F_{n+4}) - (F_{n+1} + F_{n+2})$
$= F_{n+5} - F_{n+3}$

(b) Prove by induction that the number of permutations of k out of n elements ($k \leq n$) is $\frac{n!}{(n-k)!}$.

Answer: It is important to take into consideration the order of the quantifiers in this statement so let's write it carefully:

$\forall n \in \mathbb{N}$, $\forall k \in \mathbb{N}$ such that $k \leq n$ the number of permutations of k out of n elements is $n!/(n-k)!$.

We show two proofs, the first one by induction on k the second one by induction on n.

First Proof

Let n be an arbitrary natural number. (For the rest of this proof n is "fixed".)

Now we prove by induction on k that for any natural number k, if $k \leq n$ then the number of permutations of k out of n elements is $n!/(n-k)!$.

(In preparation for the proof we worry about the case $k > n$. Well, in that case the statement becomes "false implies something" and it is trivially true!)

Base Case: $k = 0$

The number of permutations of 0 out of n elements is 1, as there is only 1 way to pick the empty sequence of elements. $n!/(n-0)! = n!/n! = 1$, so we're good!

Induction step: assume true for k, prove true for $k+1$.

Assume $k+1 \leq n$. Every permutation of $k+1$ out of n elements consist of a sequence of k distinct elements followed by one last element distinct from the first k ones. By induction hypothesis there are $n!/(n-k)!$ sequences of k distinct elements (i.e., permutations) out of the n. For each of these we have $n-k$ ways of picking the last element that completes the permutation of $k+1$ elements. (Notice that the assumption $k+1 \leq n$ is essential because it implies $n-k > 0$ therefore there are elements to pick the last one from!) Overall we get

$$\frac{n!}{(n-k)!}\,(n-k) = \frac{n!}{(n-k-1)!} = \frac{n!}{(n-(k+1))!}$$

permutations of $k+1$ out of n which completes the induction step.

Second Proof

We prove by induction on n that $\forall n \in \mathbb{N}$, $\forall k \in \mathbb{N}$ such that $k \leq n$ the number of permutations of k out of n elements is $n!/(n-k)!$.

(BASE CASE) $n = 0$

We need to show that $\forall k \in \mathbb{N}$ such that $k \leq 0$ the number of permutations of k out of 0 elements is $0!/(0-k)!$. Since $k \leq 0$ we have $k = 0$. There is exactly one permutation of 0 elements out of 0 elements and $0!/(0-0)! = 1/1 = 1$.

(INDUCTION STEP) Since k is busy, we use m. Let $m \in \mathbb{N}$ arbitrary.

Let's formulate the induction hypothesis carefully.

(INDUCTION HYPOTHESIS) $\forall k \in \mathbb{N}$ such that $k \leq m$ the number of permutations of k out of m elements is $m!/(m-k)!$.

Assuming the induction hypothesis we wish to prove

$\forall k \in \mathbb{N}$ such that $k \leq m+1$ the number of permutations of k out of $m+1$ elements is $(m+1)!/(m+1-k)!$.

Let $k \leq m+1$ arbitrary and consider $m+1$ elements.

Let's name a one of these elements. We can divide the permutations of k out of $m+1$ elements into two sets the ones that contain a and the ones that do not contain a and we count the size of each of these two sets.

For the permutations that contain a, there are k positions in which a can occur. Taking a out of the permutation we are left with a permutation of $k-1$ elements out of m. Now $k \leq m+1$ implies $k-1 \leq m$ so we can use the induction hypothesis to count these: $m!/(m-(k-1))!$. (Essential here was that induction hypothesis k was universally quantified because we used it for $k-1$.) So the number of permutations that contain a is $(m!/(m-(k-1))!) \cdot k$.

For the ones that do not contain a we have two cases.

Case 1: $k \leq m$. Then these are permutations of k out of m and we can apply the induction hypothesis to count them: $m!/(m-k)!$.

In this case the total number of permutations of k out of $m+1$ is

$$\frac{m!}{(m-(k-1))!} \cdot k + \frac{m!}{(m-k)!} = \frac{m!}{(m-k)!} \cdot \left(\frac{k}{m-k+1} + 1\right) = \frac{m!}{(m-k)!} \cdot \frac{m+1}{m-k+1} = \frac{(m+1)!}{(m+1-k)!}$$

which proves the induction step in this case.

Case 2: $k = m+1$. All the permutations contain a so the total count is obtained by setting $k = m+1$ in $(m!/(m-(k-1))!) \cdot k$. We obtain

$$\frac{m!}{(m-(m+1-1))!} \cdot (m+1) = (m+1)! = \frac{(m+1)!}{(m+1-(m+1))!}$$

so this proves the induction step in this case too.

HOMEWORK 5

Problem 1 (20pts) Alice is playing "Solitaire Dice". The game uses two regular and fair dice, that is, each die has 6 faces marked 1,2,3,4,5,6, each face comes up with the same probability and each die is thrown independently of the other. The outcome of the game is an integer between 1 and 6 which is determined as follows:

- Alice throws the first die. If it shows an even number then the game stops and that number is the outcome.

- If the first die shows an odd number then Alice throws the second die and whatever number the second die shows is the outcome of the game.

(a) We consider the probability space in which the sample space consists of the outcomes of the game. Using the four step method (draw the diagram please!) determine the probability of each of the outcomes of the game: 1,2,3,4,5, or 6.

Answer: Here is the tree diagram for 3+6=9 outcomes of how the game *proceeds*. Warning, these are *not* the outcomes of the game!

```
                   1st die                  2nd die


___________1/6_______ 2 (1/6)
 \                                 ____1/6____ 1 (1/2*1/6=1/12)
  \________1/6_______ 4 (1/6)     /____1/6____ 2 (1/2*1/6=1/12)
   \                             /_____1/6____ 3 (1/2*1/6=1/12)
    \______1/6_______ 6 (1/6)   /______1/6____ 4 (1/2*1/6=1/12)
     \                         /_______1/6____ 5 (1/2*1/6=1/12)
      \____1/2_______ odd ____/________1/6____ 6 (1/2*1/6=1/12)
```

The outcomes of the game are 1-6 and some of them correspond to *two* possible ways in which the game proceeds. So here is the sample space of the game, outcomes and probabilities:

Outcome	Probability
1	$1/12$
2	$1/6 + 1/12 = 1/4$
3	$1/12$
4	$1/6 + 1/12 = 1/4$
5	$1/12$
6	$1/6 + 1/12 = 1/4$

(b) What is the probability that the outcome of the game is even?

Answer: The event "the outcome of the game is even" is $U = \{2, 4, 6\}$. $\Pr[U] = 1/4 + 1/4 + 1/4 = 3/4$.

(c) Show that the probability that the outcome is between 2.5 and 4.5 is 1/3.

Answer: The event the outcome is between 2.5 and 4.5 is is $V = \{3, 4\}$. $\Pr[V] = 1/12 + 1/4 = 1/3$.

(d) Give an example of two independent events $E \perp F$ in this probability space. The events must be non-trivial, that is, neither one can be empty or equal to the whole sample space!)

Answer: Take $E = \{2, 4\}$ and $F = \{4, 6\}$. Then $\Pr[E] = 1/4 + 1/4 = 1/2$. $\Pr[F]$ is also 1/2 and $\Pr[E \cap F] = \Pr[\{4\}] = 1/4$. Since

$$\Pr[E] \cdot \Pr[F] = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} = \Pr[E \cap F]$$

it follows that $E \perp F$.

(e) We would like to assess events such as "Alice's first throw came up even". Explain why this is not possible in the probability space in which the sample space consists of the outcomes of the game.

Answer: It is not possible because there is no event in our probability space, i.e., no set of *game* outcomes that corresponds exactly to the "Alice's first throw came up even". For example, we know from the analysis of the game that if the outcome is 1,3, or 5 then Alice's first throw must have come up odd so these outcomes would not correspond to the desired event. But the other outcomes, namely the event $\{2, 4, 6\}$ does not correspond exactly to Alice's first throw coming up even because it also includes cases when first throw was odd (but the second one was even).

Note. The event "Alice's first throw came up even" can be represented in a different probability space, the one corresponding to the tree diagram we started with in part (a). In that probability space (which has 3+6=9 outcomes) the event has probability $1/6 + 1/6 + 1/6 = 1/2$. Such a space is discussed in Problem 2 below, but for simpler game involving just coins, not dice.

Problem 2 (20pts) Bob is playing "Solitaire Coin Toss". The game uses two fair coins and let's denote their heads/tails by H_1/T_1 and H_2/T_2. The game has three possible outcomes: H_1, T_1H_2, T_1T_2 obtained as follows

- Bob tosses the first coin. If it comes up heads then the game stops with the outcome H_1.
- If the first coin comes up tails then Bob tosses the second coin. If the second coin comes up heads then the outcome of the game is T_1H_2, otherwise it is T_1T_2.

(a) We consider the probability space in which the sample space consists of the outcomes of the game. Using the four step method (draw the diagram please!) determine the probability of each of the three outcomes of the game.

Answer:

```
________1/2_______ H1 (1/2)
 \
  \_____1/2_______ T1 ________1/2____ T1H2 (1/2*1/2=1/4)
                          \
                           \__1/2____ T1T2 (1/2*1/2=1/4)
```

(b) Which outcomes are elements of the event "if the first coin comes up tails then the second coin comes up tails"? Compute the probability of this event.

Answer: The event is $I = \{H_1, T_1T_2\}$. The outcome H_1 is part of this event because "false implies anything" is true. When the first coin comes up heads then the event "if the first coin comes up tails then the second coin comes up tails" happens! $\Pr[I] = 1/2 + 1/4 = 3/4$

(c) Consider the events $E = \{T_1H_2, T_1T_2\}$ and $F = \{T_1T_2\}$. Compute $\Pr[F|E]$.

(**Note.** This conditional probability can be read as the probability that the second coin comes up tails given that we know that the first one came up tails. Yet, the probability you have computed in (a) is different from the conditional probability you computed here. Think about this :)

Answer:

$$\Pr[F|E] = \frac{\Pr[F \cap E]}{\Pr[E]} = \frac{\Pr[\{T_1T_2\}]}{\Pr[\{T_1H_2, T_1T_2\}]} = \frac{1/4}{\Pr[1/4 + 1/4]} = \frac{1}{2}$$

(d) Bayes' Rule is the following equality:

$$\Pr[A|B] = \frac{\Pr[B|A] \cdot \Pr[A]}{\Pr[B]}$$

Mathematically it is a trivial consequence of the definition of conditional probability. But it is interesting conceptually if the events considered can be understood as occuring one after the other, B after A. Then you can think of B as an observation and A as a potential "cause" of whatever is observed. $\Pr[A|B]$ then measures the degree of confidence in stating that A actually happened, given that we have observed B.

Assume the notation of part (c) above. Using Bayes Rule compute $\Pr[E|F]$. You should have expected this answer. Explain why.

Answer:

$$\Pr[E|F] = \frac{\Pr[F|E] \cdot \Pr[E]}{\Pr[F]} = \frac{1/2 \cdot (1/4 + 1/4)}{1/4} = 1$$

We have seen in part (c) that $\Pr[F|E]$ can be thought of as the probability that the second coin comes up tails given that we know that the first one came up tails. Correspondingly, $\Pr[E|F]$ can be thought of as the probability that the first coin must have come up tails given that we observe that the second one comes up tails. In Bob's game there wouldn't even be a second coin toss unless the first coin came up tails. So if we observe the second coing being tossed at all (and this is implied by the observation that it came up tails) then it is *sure* that the first coin came up tails. (BTW, we would get the same result if E were the event that the second coin toss comes up heads.)

HOMEWORK 6

Problem 1 (25pts) Consider the set PP of pairs of natural numbers recursively defined as follows.

base case $(0, 0) \in$ PP

constructor 1 If $(m, n) \in$ PP then $(m + 1, n) \in$ PP.

constructor 2 If $(m, n) \in$ PP then $(m, n + 1) \in$ PP.

(a) Prove by ordinary induction on m that $\forall m \in \mathbb{N}\ (m, 0) \in \mathrm{PP}$.

Answer:

(BASE CASE) $m = 0$. $(0, 0) \in \mathrm{PP}$ by the base case of the recursive definition of PP.

(INDUCTION STEP) Let $k \in \mathbb{N}$ arbitrary. Assume (INDUCTION HYPOTHESIS) that $(k, 0) \in \mathrm{PP}$. Then $(k + 1, 0) \in \mathrm{PP}$ by constructor 1 of the recursive definition of PP.

(b) Fix an arbitrary $m \in \mathbb{N}$. Prove by ordinary induction on n that $\forall n \in \mathbb{N}\ (m, n) \in \mathrm{PP}$. Explain clearly where in your proof you use the result that you proved in part (a).

(By the way, this proves what we intuitively expect: PP contains *all* the pairs of natural numbers, $\mathrm{PP} = \mathbb{N} \times \mathbb{N}$. But is this a good way of working with $\mathbb{N} \times \mathbb{N}$? Not really, see below!)

Answer: Recall that we have fixed an arbitrary $m \in \mathbb{N}$.

(BASE CASE) $n = 0$. $(m, 0) \in \mathrm{PP}$ because that's exactly what we have proved in part (a).

(INDUCTION STEP) Let $k \in \mathbb{N}$ arbitrary. Assume (INDUCTION HYPOTHESIS) that $(m, k) \in \mathrm{PP}$. Then $(m, k + 1) \in \mathrm{PP}$ by constructor 2 of the recursive definition of PP.

(c) Consider the function $f : \mathrm{PP} \to \mathbb{N}$ recursively defined by

base case $f((0, 0)) = 0$

constructor 1 $f((m + 1, n)) = f((m, n)) + n$

constructor 2 $f((m, n + 1)) = m + f((m, n))$

Prove by structural induction on (m, n) that $\forall (m, n) \in \mathrm{PP}\ f((m, n)) = m \cdot n$.

Answer:

base case $(m, n) = (0, 0)$. $f((0, 0)) = 0 = 0 \cdot 0$.

constructor 1 Let $(m, n) \in \mathrm{PP}$ arbitrary. Assume (INDUCTION HYPOTHESIS) that $f((m, n)) = m \cdot n$.
Now $f((m + 1, n)) = f((m, n)) + n = m \cdot n + n = (m + 1) \cdot n$.

constructor 2 Let $(m, n) \in \mathrm{PP}$ arbitrary. Assume (INDUCTION HYPOTHESIS) that $f((m, n)) = m \cdot n$.
Now $f((m, n + 1)) = m + f((m, n)) = m + m \cdot n = m \cdot (n + 1)$.

(d) In part (c) we have successfully defined a function recursively on PP. However, in general this doesn't work properly because the recursive definition of PP is *ambiguous*, i.e., the same elements of PP can be constructed in more than one way. Let's see why this can be bad. Consider

base case $g((0, 0)) = 1$

constructor 1 $g((m + 1, n)) = 2 \cdot g((m, n))$

constructor 2 $g((m, n + 1)) = g((m, n)) + 1$

Find an element (p, q) of PP that is constructed in two different ways such that if we compute $g((p, q))$ following one way we get a different result than the one obtained computing $g((p, q))$ the other way.

(Therefore, remember that when data is given by an ambiguous recursive definition, not every recursive definition of a function on it is correct.)

Answer: Take $(p, q) = (1, 1)$. This element of PP can constructed in two different ways: base case, constructor 1, constructor 2 and base case, constructor 2, constructor 1. This leads to two different results for $g((1, 1))$:
$g((1, 1)) = g((1, 0)) + 1 = 2 \cdot g((0, 0)) + 1 = 2 \cdot 1 + 1 = 3$
$g((1, 1)) = 2 \cdot g((0, 1)) = 2(g((0, 0)) + 1) = 2(1 + 1) = 4$

Problem 2 (25pts) Consider the set of strings Cond that is recursively defined as follows. The alphabet has 7 letters: $A = \{\ T, F,\ ?\ , :, !\ ,], [\ \}$.

base case 1 $T \in$ Cond.

base case 2 $F \in$ Cond.

constructor 1 If $e, f, g \in$ Cond then $[e\ ?\ f : g] \in$ Cond.

constructor 2 If $e \in$ Cond then $[!\ e] \in$ Cond.

Note. You probably guessed it: "T" represents true, "F" represent false, $e\ ?\ f : g$ is a syntax much loved by C hackers because it allows them to say "if e then f else g" with fewer keystrokes, and ! e represents negation. So one could say that these strings are nested logical-conditional expressions but without variables (adding variables can be done just as we did for arithmetic expressions in class but let's to keep things simpler here).

Consider also the function eval : Cond $\rightarrow \{T, F\}$ recursively defined as follows:

base case 1 $\text{eval}(T) = T$

base case 2 $\text{eval}(F) = F$.

constructor 1

$$\text{eval}([e\ ?\ f : g]) = \begin{cases} \text{eval}(f) & \text{if } \text{eval}(e) = T \\ \text{eval}(g) & \text{if } \text{eval}(e) = F \end{cases}$$

constructor 2

$$\text{eval}([!\ e]) = \begin{cases} F & \text{if } \text{eval}(e) = T \\ T & \text{if } \text{eval}(e) = F \end{cases}$$

(a) Define and : $\{T, F\} \times \{T, F\} \rightarrow \{T, F\}$ by $\text{and}(b_1, b_2) = \text{eval}([b_1\ ?\ b_2 : F])$. Using the definition of eval prove the following

$$\begin{aligned} \text{and}(T, T) &= T \\ \text{and}(T, F) &= F \\ \text{and}(F, T) &= F \\ \text{and}(F, F) &= F \end{aligned}$$

(Hint: this is *not* a proof by induction; reason by cases.)

Answer: "By cases" here means that the definition of $\text{eval}([b_1\ ?\ b_2 : F])$ is given by cases. One case is $\text{eval}([T\ ?\ b_2 : F]) = b_2$ and this gives us $\text{and}(T, T) = T$ and $\text{and}(T, F) = F$. The other case is $\text{eval}([F\ ?\ b_2 : F]) = F$ and this gives us $\text{and}(F, T) = F = \text{and}(F, F)$.

(b) Prove the following identities

$$\mathrm{eval}([!\ [!\ e]]) \;=\; \mathrm{eval}(e)$$

$$\mathrm{eval}([[!\ e]\ ?\ f : g]) = \begin{cases} \mathrm{eval}(g) & \text{if } \mathrm{eval}(e) = T \\ \mathrm{eval}(f) & \text{if } \mathrm{eval}(e) = F \end{cases}$$

(Hint: reason by cases.)

Answer: These are called "identities" because they must hold no matter what $e \in \mathrm{Cond}$ is (for the first one) and no matter what $e, f, g \in \mathrm{Cond}$ are (for the second one).

To prove the first one we have two cases.

Case 1: $\mathrm{eval}(e) = T$. Then $\mathrm{eval}([!\ e]) = F$ therefore $\mathrm{eval}([!\ [!\ e]]) = T = \mathrm{eval}(e)$.

Case 2: $\mathrm{eval}(e) = F$. Then $\mathrm{eval}([!\ e]) = T$ therefore $\mathrm{eval}([!\ [!\ e]]) = F = \mathrm{eval}(e)$.

To prove the second one we also have two cases.

Case 1: $\mathrm{eval}(e) = T$. Then $\mathrm{eval}([!\ e]) = F$ therefore $\mathrm{eval}([[!\ e]\ ?\ f : g]) = \mathrm{eval}(g)$.

Case 2: $\mathrm{eval}(e) = F$. Then $\mathrm{eval}([!\ e]) = T$ therefore $\mathrm{eval}([[!\ e]\ ?\ f : g]) = \mathrm{eval}(f)$.

(c) Consider moreover the function $\mathrm{sure} : \mathrm{Cond} \to \mathbb{R}$ recursively defined as follows:

base case 1 $\mathrm{sure}(T) = 1$

base case 2 $\mathrm{sure}(F) = 0$.

constructor 1

$$\mathrm{sure}([e\ ?\ f : g]) = \begin{cases} 1 & \text{if } \mathrm{sure}(f) = \mathrm{sure}(g) = 1 \\ 0 & \text{if } \mathrm{sure}(f) = \mathrm{sure}(g) = 0 \\ 1/2 & \text{otherwise} \end{cases}$$

constructor 2

$$\mathrm{sure}([!\ e]) = 1 - \mathrm{sure}(e)$$

Prove by structural induction on e that $\forall e \in \mathrm{Cond}\ \ (\mathrm{sure}(e) = 1 \Rightarrow \mathrm{eval}(e) = T)$ and $(\mathrm{sure}(e) = 0 \Rightarrow \mathrm{eval}(e) = F)$

Answer:

base case 1 $e = T$. Here $\mathrm{sure}(e) = 1$ and also $\mathrm{eval}(e) = T$ so the statement holds $(\mathrm{sure}(e) = 0 \Rightarrow \mathrm{eval}(e) = F)$ holds because false implies anything :).

base case 2 $e = F$. Here $\mathrm{sure}(F) = 0$ and $\mathrm{eval}(e) = F$ so it checks out also.

constructor 1 $e = [e'\ ?\ f : g]$ where $e', f, g \in \mathrm{Cond}$ are arbitrary. Assume (INDUCTION HYPOTHESIS) that

$$(\mathrm{sure}(e') = 1 \Rightarrow \mathrm{eval}(e') = T) \text{ and } (\mathrm{sure}(e') = 0 \Rightarrow \mathrm{eval}(e') = F)$$

$$(\mathrm{sure}(f) = 1 \Rightarrow \mathrm{eval}(f) = T) \text{ and } (\mathrm{sure}(f) = 0 \Rightarrow \mathrm{eval}(f) = F)$$

$$(\mathrm{sure}(g) = 1 \Rightarrow \mathrm{eval}(g) = T) \text{ and } (\mathrm{sure}(g) = 0 \Rightarrow \mathrm{eval}(g) = F)$$

(Out of these 6 implications only the last 4 will be needed but we want to see what the induction hypothesis look like in its full glory :)

Now we want to prove for $e = [e' \ ? \ f : g]$ that

$$(\text{sure}(e) = 1 \Rightarrow \text{eval}(e) = T) \text{ and } (\text{sure}(e) = 0 \Rightarrow \text{eval}(e) = F)$$

Suppose sure(e) $= 1$ i.e., sure($[e' \ ? \ f : g]$) $= 1$. From the recursive definition of sure it follows that this can happen only when sure(f) $=$ sure(g) $= 1$. Now we have two cases:
Case 1: eval(e') $= T$. Then eval(e) $=$ eval(f). Since sure(f) $= 1$ it follows from the induction hypothesis that eval(f) $= T$ therefore eval(e) $= T$.
Case 2: Just like in case 1 but using the implication sure(g) $= 1 \Rightarrow$ eval(g) $= T$ from the induction hypothesis.
Therefore we have shown that sure(e) $= 1 \Rightarrow$ eval(e) $= T$.
Now suppose sure(e) $= 0$. Similarly to the above, reasoning with two cases and using the implications sure(f) $= 0 \Rightarrow$ eval(f) $= F$ and sure(g) $= 0 \Rightarrow$ eval(g) $= F$ from the induction hypothesis we conclude eval(e) $= F$.
Therefore sure(e) $= 0 \Rightarrow$ eval(e) $= F$ and this concludes the induction step for constructor 1.

constructor 2 $e = [!\ e']$ where $e' \in$ Cond is arbitrary. Assume (INDUCTION HYPOTHESIS) that

$$(\text{sure}(e') = 1 \Rightarrow \text{eval}(e') = T) \text{ and } (\text{sure}(e') = 0 \Rightarrow \text{eval}(e') = F)$$

Now we want to prove for $e = [!\ e']$ that

$$(\text{sure}(e) = 1 \Rightarrow \text{eval}(e) = T) \text{ and } (\text{sure}(e) = 0 \Rightarrow \text{eval}(e) = F)$$

Suppose sure(e) $= 1$. Since sure(e) $=$ sure($[!\ e']$) $= 1 -$ sure(e') it follows that sure(e') $= 0$. By induction hypothesis eval(e') $= F$ and therefore eval(e) $=$ eval($[!\ e']$) $= T$.
Suppose sure(e) $= 0$. Similar to above, then sure(e') $= 1$, by induction hypothesis eval(e') $= T$, and therefore eval(e) $= F$. This concludes the induction step for constructor 2.

HOMEWORK 7

Problem 1 (30pts) Let $G = (V, E)$ be a digraph. Recall that in our definition the edges of a digraph are pairs of vertices, that is, $E \subseteq V \times V$; we can also say that E is a binary relation with domain V and codomain V, or simply, E is a binary relation *on* V.

For this problem, we make the following definition: a binary relation R on V is said to be a *transitive closure of* E if

- R includes E, i.e., $E \subseteq R$,
- R is transitive, and

- if ρ is another binary relation on V that is transitive and includes E then $R \subseteq \rho$.

Consider the following recursive definition for a set PP of pairs of vertices (PP $\subseteq V \times V$; i.e., PP is a binary relation on V):

base case(s) For each $(u, v) \in E$ we have $(u, v) \in$ PP.

constructor If $(x, u) \in$ PP and $(u, v) \in$ PP then $(x, v) \in$ PP

(Observe that the definitions ensures that PP includes E and that PP is transitive. Below we will prove that PP is quite special among all the transitive binary relations that include E!)

(a) Show that this definition is ambiguous, that is, give an example of a digraph $G = (V, E)$ and of a pair $(u, v) \in$ PP that is constructed in two different ways by the recursive definition.

(This means that in general it is not a good idea to define functions recursively on PP. However, structural induction still works fine and we will use this below.)

Answer: Consider the digraph with $V = \{1, 2, 3\}$ and $E = \{(1, 2), (2, 3), (1, 3)\}$ The pair $(1, 3) \in$ PP is constructed in two different ways: one way is using just the base case; the other way is using the base case for $(1, 2)$ and $(2, 3)$ and then the constructor.

(b) Let ρ be a binary relation on V that is transitive and that includes E. Prove by structural induction on (u, v) that $\forall (u, v) \in$ PP we have $(u, v) \in \rho$.

(Observe that from this it follows that PP is a transitive closure of E.)

Answer:

base case(s) For each $(u, v) \in E$ we have $(u, v) \in \rho$ because ρ includes E.

constructor Let $(x, u) \in$ PP and $(u, v) \in$ PP, arbitrary. Assume (IND HYP) that $(x, u) \in \rho$ and $(u, v) \in \rho$. We want to show that this implies $(x, v) \in \rho$. This follows immediately from the fact that ρ is transitive.

(c) Consider the definition from the textbook:

$$\text{WW} = \{\ (u, v) \mid \text{there is a walk of length} \geq 1 \text{ from } u \text{ to } v\ \}$$

(BTW, in class I tried to simplify this by using "path" instead of "walk of length ≥ 1" but it doesn't work because in our textbook the definition of path excludes the case when the start and the end vertices are the same.)

We know from class that $E \subseteq$ WW and that WW is transitive.

Now let ρ be a binary relation on V that is transitive and that includes E. Prove by ordinary induction on n that $\forall n \in \mathbb{N}, n \geq 1, P(n)$ where

$P(n) =$ "for any walk of length n in G, if the walk starts at u and ends at v then $(u, v) \in \rho$"

(Observe that from this it follows that WW is a transitive closure of E.)

Answer:

BASE CASE $n = 1$. A walk of length 1 that starts at u and ends at v has the form $u - (u, v)\ v$ so $(u, v) \in E$. Since ρ includes E, $(u, v) \in \rho$.

INDUCTION STEP. Let n be an arbitrary natural number such that $n \geq 1$. Assume (IND HYP) that for any walk of length n in G, if the walk starts at u and ends at v then $(u, v) \in \rho$.

Now consider a walk of length $n+1$ and denote its start by x and end by y. This walk must have at least one edge so it must have the form $x - \cdots - z - (z, y) - y$ where $x - \cdots - z$ is a walk of length n and $(z, y) \in E$. By induction hypothesis $(x, z) \in \rho$. Because ρ includes E we have $(z, y) \in \rho$. From the transitivity of ρ it follows that $(x, y) \in \rho$.

(c) Let R_1 and R_2 be two binary relations on V such that both are transitive closures of E. Prove that $R_1 = R_2$.

(Therefore, we can talk about THE transitive closure of E since it is unique. The usual notation for the transitive closure of E is E^+. We also shown that it exists, in fact we showed it in two different ways: PP = WW = E^+.)

Answer: Because R_1 is the transitive closure of E and R_2 is a transitive relation that includes E we must have $R_1 \subseteq R_2$. Similarly, $R_2 \subseteq R_1$. Therefore $R_1 = R_2$.

(d) A binary relation R on V is said to be *symmetric* if $\forall u, v \in V \ (u, v) \in R \ \Rightarrow \ (v, u) \in R$. Prove that if E is symmetric then E^+ is symmetric. Prove it in two different ways:

1. Using $E^+ =$ WW.

   Answer: We could prove this by (ordinary) induction on the length of walks. However, here is a proof that is less "mechanistic" but still perfectly rigorous:
   Let $(u, v) \in$ WW arbitrary. Then there exists in G a walk of length ≥ 1 of the form:

   $$u \equiv x_0 - (x_0, x_1) - x_1 - (x_1, x_2) - x_2 - \cdots - x_{n-1} - (x_{n-1}, x_n) - x_n \equiv v$$

   Since $(x_{i-1}, x_i) \in E$ and E is symmetric we also have $(x_i, x_{i-1}) \in E$ for $i = 1, \ldots, n$. Therefore,

   $$v \equiv x_n - (x_n, x_{n-1}) - x_{n-1} - \cdots - x_1 - (x_1, x_0) - x_0 \equiv u$$

   is also a walk of length ≥ 1 in G so $(v, u) \in$ WW.
   (The moral of this little story: don't be affraid to use dot dot dot in mathematical proofs. They are not programs for computer consumption, proofs are for human consumption!)

2. Using $E^+ =$ PP, by structural induction.

   Answer: Assume that E is symmetric. We wish to prove by structural induction that $\forall (u, v) \in$ PP the pair (v, u) is also in PP.

   base case(s) For each $(u, v) \in E$ we have $(v, u) \in E$ because E is symmetric. Therefore $(v, u) \in$ PP.

   constructor Let $(x, u) \in$ PP and $(u, v) \in$ PP, arbitrary. Assume (IND HYP) that $(u, x) \in$ PP and $(v, u) \in$ PP. We want to show that this implies $(v, x) \in$ PP. This follows immediately from the fact that PP is transitive.

Problem 2 (20pts) Let $n \geq 2$ be a natural number. Consider the digraph $G = (V, E)$ where $V = \{0, 1, \ldots, n\}$ and $E = \{(0, 1), (1, 2), \ldots, (n-1, n), (n, 0)\} \cup \{(n, n-1), (n-1, n-2), \ldots, (1, 0), (0, n)\}$

(a) Draw this digraph.

Answer: Draw it as a necklace in which the beads are pairs of edges going in opposite directions. between the same two nodes. There are $n + 1$ beads.

(b) How many cycles of length $n+1$ does G have? (Give the answer and an explanation of how you figured it out. No proofs required.)

Answer: 2. One such cycle is going clockwise around the necklace using from each bead the edge that points in clockwise direction. The other cycle is similar but going counterclockwise.

(c) For any $0 \leq i < j \leq n$ give the number of paths in G from i to j. (Give the answer and an explanation of how you figured it out. No proofs required.)

Answer: 2(again). Again one going clockwise and the other one going counterclockwise.

(d) What is the minimum number of edges that you must remove from G to make it into a DAG? (Give the answer and an explanation of how you figured it out. No proofs required.)

Answer: $n+1$ Each bead is a cycle of length 2 that we need to break, so we need to remove one of the two edges of each bead. That's $n + 1$ edges. But will this suffice? Yes, if we also break the two big cycles of length $n + 1$ discussed in part (a). So among the $n + 1$ edges that we remove there needs to be at least one edge that goes in clockwise direction and at least one edge that goes in counterclockwise direction.