

1. (a) [3 points] How many functions are there from  $\{a, b, c\}$  to  $\{1, 2, 3, 4\}$ .

**Solution**  $4^3$ : there are four choices of output for each input in  $\{a, b, c\}$ .

- (b) [3 points] How many of these functions are one-to-one?

**Solution**  $4 \times 3 \times 2$ : there are 4 choices of output for  $a$ , once that has been chosen there are three choices of output for  $b$ , and once that's been chosen, 2 choices for  $c$ .

- (c) [2 points] How many of these functions are onto?

**Solution** 0: there are no functions with domain  $a, b, c$  that have range all of  $\{1, 2, 3, 4\}$ .

2. [10 points] Prove by induction that  $3^{2n-1} + 1 \equiv 0 \pmod{4}$  for all  $n \geq 1$ .

**Solution** Let  $P(n)$  be the statement  $3^{2n-1} + 1 \equiv 0 \pmod{4}$ .  $P(1)$  says that  $3 + 1 \equiv 0 \pmod{4}$ , which is clearly true. Suppose that  $P(n)$  holds; that is  $3^{2n-1} + 1 \equiv 0 \pmod{4}$ , or equivalently,  $3^{2n-1} \equiv -1 \pmod{4}$ . We want to show that  $P(n+1)$  holds.  $P(n+1)$  says that  $3^{2n+1} + 1 \equiv 0 \pmod{4}$ . Now  $3^{2n+1} = 9 \cdot 3^{2n-1}$ . By the induction hypothesis,  $3^{2n-1} \equiv -1 \pmod{4}$ . Note that  $9 \equiv 1 \pmod{4}$ . It follows that  $3^{2n+1} = 9 \times 3^{2n-1} \equiv 1 \times -1 \equiv -1 \pmod{4}$ . Thus,  $3^{2n+1} + 1 \equiv 0 \pmod{4}$ .

3. (a) [1 points] What are the units of  $\mathbb{Z}_{11}$ ?

**Solution** All non-zero elements are units, so the units are  $1, \dots, 10$ .

- (b) [1 points] What is  $\phi(11)$ ?

**Solution** 10, since there are 10 units.

- (c) [4 points] Use Euler's theorem to compute  $18^{1922} \pmod{11}$ .

**Solution**  $[18]_{11}^{[1922]_{10}} = [7]_{11}^{[2]_{10}} = [49]_{11} = [5]_{11}$ .

4. (a) [3 points] In how many ways can three computer scientists and two geologists be chosen from a group of seven computer scientists and six geologists to visit an oil rig? (There's no need to simplify your answer.)

**Solution** There are  $C(7, 3)$  ways of choosing three computer scientist and  $C(6, 2)$  ways of choosing the geologists, so there are  $C(7, 3) \times C(6, 2)$  ways of choosing the whole group.

- (b) [3 points] What is the probability that Alice (a computer scientist) and Bob (a geologist) will both be chosen, if each possible combination of three computer scientists and two geologists is equally likely?

**Solution** Once Alice and Bob are chosen, there are  $C(6, 2)$  of choosing the remaining two computer scientists and  $C(5, 1)$  way of choosing the remaining biologist. Thus, the probability is  $(C(6, 2) \times C(5, 1)) / (C(7, 3) \times C(6, 2)) = 5 / (7 \times 6 \times 5 / 3 \times 2) = 1/7$ .

5. [4 points] There are 52 people at a party, all between the ages of 1 and 100. Use the pigeonhole principle to prove that there are either two people of the same age, or two people whose ages are consecutive integers.

**Solution** Partition  $1 \dots 100$  into 50 intervals of length 2;  $\{1, 2\}, \{3, 4\}, \dots, \{99, 100\}$ . These are the “holes”. Thus, there are 50 holes. The pigeons are the people. A person goes into a hole if his age matches one of the two numbers. Since there are 52 pigeons and 50 holes, at least two pigeons are in the same hole. These two people have either the same age or their ages are consecutive integers.

6. Two fair dice are rolled. Suppose that you describe the outcomes using the sample space  $\{(i, j) : 1 \leq i \leq 6, 1 \leq j \leq 6\}$ , with each element being equally likely. Consider the following random variables:

$$X_1(i, j) = \begin{cases} 1 & \text{if } i = 6 \\ 0 & \text{otherwise,} \end{cases}$$

$$X_2(i, j) = \begin{cases} 1 & \text{if } j = 6 \\ 0 & \text{otherwise.} \end{cases}$$

- (a) [1 points] What does  $X_1$  represent (in English)? What does  $X_2$  represent?

**Solution**  $X_1$  is the random variable “the first die lands 6”.  $X_2$  is “the second die lands 6”.

- (b) [1 points] Let  $X = X_1 + X_2$ . What does  $X$  represent (in English)?

**Solution**  $X$  is “the number of dice that land 6, if the two dice are rolled”.

- (c) [2 points] We claim that  $X_1$  and  $X_2$  are independent. What would you have to check to confirm that?

**Solution** You have to check that  $\Pr(X_1 = i \cap X_2 = j) = \Pr(X_1 = i) \times \Pr(X_2 = j)$  for all values of  $i$  and  $j$  with  $1 \leq i \leq 6$  and  $1 \leq j \leq 6$ ,

- (d) [3 points] What is  $E(X)$ ?

**Solution**  $E(X) = E(X_1) + E(X_2) = 1/6 + 1/6 = 1/3$ , since  $E(X_i) = 1/6$ , since  $X_i = 1$  with probability  $1/6$  and  $X_i = 0$  with probability  $5/6$ .

7. [5 points] A simplified form of Bayes’s rule is given by the following expression:

$$\Pr(A|B) = \frac{\Pr(B|A) \Pr(A)}{\Pr(B)}$$

Prove this identity.

**Solution** By definition,  $\Pr(A|B) = \Pr(A \cap B) / \Pr(B)$ . Thus  $\Pr(A \cap B) = \Pr(B) \Pr(A|B)$ . Similarly,  $\Pr(B \cap A) = \Pr(A) \Pr(B|A)$ . Thus  $\Pr(A) \Pr(B|A) = \Pr(B) \Pr(A|B)$ . Dividing both sides by  $\Pr(A)$  gives the formula.

8. (This is a variant of a problem due to Lewis Carroll, who wrote “Alice in Wonderland”.) A bag has a white ball in it. A second ball is put into the bag, which is white with probability  $2/3$  and black with probability  $1/3$  (so with probability  $2/3$ , there are two white balls in the bag and with probability  $1/3$  there is a white ball and a black ball). Now a ball is chosen from the bag at random.

- (a) [2 points] Carefully describe a sample space for this problem.

**Solution** The sample space consists of two balls in the bag and the ball that is chosen. Let  $W$  be the white ball that was originally in the bag, let  $W'$  be the second white ball, and let  $B$  be the black ball. Thus, the sample space has four elements:

- $(WW', W)$  (ball  $W'$  is put in the bag,  $W$  is chosen)

- $(WW', W')$  (ball  $W'$  is put in the bag,  $W$  is chosen)
- $(WB, W)$
- $(WB, B)$

(It's OK to omit the  $W$  that is in the bag all along.)

(b) [2 points] What is the probability of each element of this sample space.

**Solution** The first two elements in the space above ( $(WW', W)$  and  $(WW', W')$ ), where the white ball  $W'$  is put in, each have probability  $1/3$ ; the second two elements each have probability  $1/6$ .

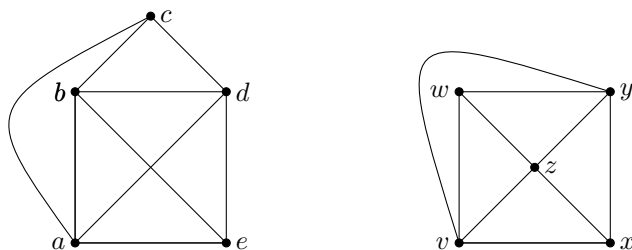
(c) [3 points] If the ball chosen is white, what is the probability that the second ball is white?

**Solution** The ball chosen is white in the first three elements of the sample space. The second ball is white in the first two. Thus, the conditional probability is  $(\frac{1}{3} + \frac{1}{3}) / (\frac{1}{3} + \frac{1}{3} + \frac{1}{6}) = \frac{4}{5}$ .

9. [3 points] If an undirected graph has chromatic number 2, is it bipartite? Why or why not?

**Solution** An undirected graph  $G = (V, E)$  with chromatic number 2 is bipartite. If it has chromatic number 2, each vertex can be associated with one of two colors, say blue and yellow, such that all the edges go between blue vertices and yellow vertices. Let  $V_1$  consist of the blue vertices and let  $V_2$  consist of the yellow vertices.  $V_1$  and  $V_2$  is a partition of  $V$ , and all edge in  $E$  go from a vertex in  $V_1$  to a vertex in  $V_2$ , so  $G$  is bipartite.

10. [3 points] Are the two graphs below isomorphic? If you think that they are isomorphic, give the bijection  $f$  between the graphs that demonstrates the isomorphism. If you think that they are not isomorphic, explain why.



**Solution** The graphs are isomorphic. Both graphs have two nodes of degree 3 ( $c$  and  $e$  on the left;  $w$  and  $x$  on the right) with the remaining three nodes having degree 4. Any function  $f$  that maps degree-3 nodes to degree-3 nodes and maps degree-4 nodes to degree-4 nodes is an isomorphism (e.g.,  $f(a) = v$ ,  $f(b) = w$ ,  $f(c) = w$ ,  $f(d) = z$ , and  $f(e) = x$ ).

11. [3 points] What is the clique number of the graph above on the left? (Explain your answer.)

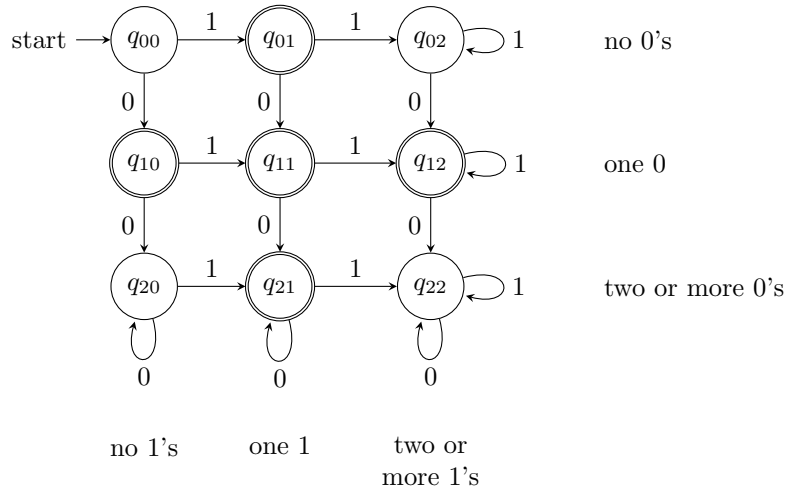
**Solution** The clique number is 4: clearly  $a, b, c$ , and  $e$  is a completely connected graph, so the clique number is at least 4. But it can't be 5, since the whole graph is not completely connected.

12. [6 points] Define the relation  $\sim$  on  $N \times N$  by taking  $(m, n) \sim (k, l)$  if  $m + l = n + k$ . Show that  $\sim$  is an equivalence relation.

**Solution** The relation is clearly reflexive:  $(m, m) \sim (m, m)$  since  $m + m = m + m$ . It is symmetric, since if  $(m, n) \sim (k, l)$ , then  $m + l = n + k$ , which is exactly what is needed to have  $(k, l) \sim (m, n)$ . Finally, it is transitive, since if  $(k, l) \sim (m, n)$  and  $(m, n) \sim (r, s)$ , then  $k + n = m + l$  and  $m + s = n + r$ . Adding the left-hand sides and the right-hand sides, we get that  $k + m + n + s = m + l + n + r$ . Subtracting  $m + n$  from both sides, it follows that  $k + s = l + r$ . Thus  $(k, l) \sim (r, s)$ , so  $\sim$  is transitive. Since  $\sim$  is reflexive, symmetric, and transitive, it is an equivalence relation.

13. [5 points] Build a deterministic finite automaton that recognizes the set of strings of 0's and 1's, that only contain a single 0 (and any number of 1's). Describe the set of strings that lead to each state.

**Solution** [TODO — this needs updating]



14. [10 points] Given a string  $x$ , we can define the “character doubling” of  $x$  to be  $x$  with every character doubled: for example  $cd(abc) = aabbcc$ . Formally,  $cd(\epsilon) = \epsilon$ , and  $cd(xa) = cd(x)aa$ . We can then define the “character doubling” of a language  $L$  to be the set of all strings formed by doubling the characters of strings in  $L$ ; formally  $cd(L) = \{cd(x) \mid x \in L\}$ .

Given a DFA  $M = (Q, \Sigma, \delta, q_0, F)$ , we can construct a new DFA  $M_{cd}$  that recognizes  $cd(L(M))$  by adding a new state  $q'_{qa}$  to the middle of every transition from  $q$  on character  $a$ :



- (a) Formally describe the components  $(Q_{cd}, \Sigma_{cd}, \delta_{cd}, q_{0cd}, F_{cd})$  of  $M_{cd}$  in terms of the components of  $M$ . Be sure to describe  $\delta_{cd}$  on all inputs (you may need to add one or more additional states).

**Solution**  $Q_{cd} = Q \cup \{q'_{qa} \mid q \in Q, a \in A\} \cup \{X\}$

$\delta_{cd} : (q, a)q'_{qa}$ ;  $\delta_{cd} : (q'_{qa}, a)\delta(q, a)$ ;  $\delta_{cd} : (q'_{qa}, b)X$  if  $ab$ , and  $\delta_{cd} : (X, a)X$ .

The remaining components are unchanged:  $\Sigma_{cd} = \Sigma$ ,  $q_{0cd} = q_0$ , and  $F_{cd} = F$ .

- (b) Use structural induction on  $x$  to prove that for all  $x$ ,  $\widehat{\delta}(q_0, x) = \widehat{\delta}_{cd}(q_{0cd}, cd(x))$ .

**Solution** Let  $P(x)$  be the statement that  $\widehat{\delta}(q_0, x) = \widehat{\delta}_{cd}(q_{0cd}, cd(x))$ . I will prove  $x, P(x)$  by structural induction.

To show  $P(\epsilon)$ , note that  $\widehat{\delta}(q_0, \epsilon) = q_0$ . Moreover,  $cd(\epsilon) = \epsilon$ , so  $\widehat{\delta}_{cd}(q_{0cd}, cd(\epsilon)) = \widehat{\delta}_{cd}(q_{0cd}, \epsilon) = q_0 = \widehat{\delta}(q_0, \epsilon)$ , as required.

To show  $P(xa)$ , we assume the inductive hypothesis  $P(x)$ . we compute:

$$\begin{aligned}
 \widehat{\delta}_{cd}(q_0, cd(xa)) &= \widehat{\delta}_{cd}(q_0, cd(x)aa) && \text{by definition of } cd \\
 &= \delta_{cd}(\delta_{cd}(\widehat{\delta}_{cd}(q_0, cd(x)), a), a) && \text{by definition of } \widehat{\delta}_{cd} \\
 &= \delta_{cd}(\delta_{cd}(\widehat{\delta}(q_0, x), a), a) && \text{by definition of } \widehat{\delta}_{cd} \\
 &= \delta_{cd}(q_{(\widehat{\delta}(q_0, x))a}, a) && \text{by definition of } \delta_{cd} \\
 &= \delta(\widehat{\delta}(q_0, x), a) && \text{by definition of } \delta_{cd} \\
 &= \widehat{\delta}(q_0, xa) && \text{by definition of } \widehat{\delta}
 \end{aligned}$$

15. [10 points] We can also define the “string doubling” of  $x$  to be  $xx$ . For example,  $sd(abc) = abcabc$ . Show that the set of regular languages is not closed under string doubling. In other words, give a regular language  $L$  and prove that  $sd(L) = \{sd(x) \mid x \in L\}$  is not regular.

You can use any theorem proved in class to help prove this result.

**Solution** Let  $L = 0^*1$ . Clearly  $L$  is regular. Moreover,  $sd(L) = \{0^n10^n1 \mid n \in \mathbb{N}\}$ .

This language is not regular. To see this, assume for the sake of contradiction that it is. Then there exists some natural number  $m$  as in the pumping lemma. Let  $x = 0^m10^m1$ . Clearly  $x \in sd(L)$ , and  $|x| \geq m$ , so we can split  $x$  into  $u, v$ , and  $w$ , as in the pumping lemma. We know that  $|uv| \leq m$ , so  $v$  can only contain 0’s. Then  $x' = uv^2w$  contains more 0’s before the first 1 than after, and thus  $x' \notin sd(L)$ . But the pumping lemma says that  $x' \in sd(L)$ ; this is a contradiction, and thus  $sd(L)$  is not regular.

16. (a) [6 points] Build a proof tree showing that  $\vdash \neg(P \vee Q) \rightarrow \neg P$ . You may refer to the list of rules given at the end of the exam.

**Solution**

$$\frac{\frac{\frac{\overline{\dots \vdash P} \text{ assum}}{\dots \vdash (P \vee Q)} \vee \text{intro} \quad \frac{\overline{\dots \vdash \neg(P \vee Q)} \text{ assum}}{\dots, P \vdash \neg P} \text{ absurd}}{\dots \vdash P \vee \neg P} \text{ excl mid} \quad \frac{\overline{\dots, \neg P \vdash \neg P} \text{ assum}}{\dots, P \vdash \neg P} \text{ absurd}}{\frac{\neg(P \vee Q) \vdash \neg P}{\vdash \neg(P \vee Q) \rightarrow \neg P} \rightarrow \text{intro}} \text{ Velim}$$

- (b) [5 points] Show, using truth tables, that  $\models \neg(P \vee Q) \rightarrow \neg P$ .

**Solution** Here is the truth table for  $\neg(P \vee Q) \rightarrow \neg P$ :

$P$	$Q$	$P \vee Q$	$\neg(P \vee Q)$	$\neg P$	$\neg(P \vee Q) \rightarrow \neg P$
T	T	T	F	F	T
T	F	T	F	F	T
F	T	T	F	T	T
F	F	F	T	T	T

As you can see, every row of the truth table is true.

17. [4 points] Translate the following expressions into first-order logic, making clear what the predicates you use stand for.

- (a) *Everyone is on someone's contact list.*  
 (b) *No one is on everyone's contact list.*

**Solution**

- (a) Taking  $C(x, y)$  to stand for “ $x$  is on  $y$ 's contact list”, then we get  $\forall x \exists y C(x, y)$ .  
 (b)  $\forall x \neg \forall y C(x, y)$  ( $\neg \exists x \forall y C(x, y)$  is also OK).

18. [4 points] *Which of the following formulas is true if the domain is the natural numbers, and which are true if the domain is the real numbers. (Explain your answer in each case.)*

- (a)  $\exists x \exists y (x < y \wedge \forall z (z \leq x \vee y \leq z))$   
 (b)  $\exists x \exists y (2x - y = 4 \wedge 2x + y = 6)$ .

**Solution**

- (a) This is true for the natural numbers: take  $x$  and  $y$  to be consecutive numbers such that  $x < y$  (e.g.,  $x = 3$  and  $y = 4$ ). Then every natural number  $z$  is either less than or equal to  $x$  or greater than or equal to  $y$ . It is false of the real numbers. For all real numbers  $x$  and  $y$  with  $x < y$ , there is a  $z$  (namely,  $z = (x + y)/2$ ) such that neither  $z \leq x$  nor  $y \leq z$  holds.  
 (b) The only solution to these equations is  $x = 2.5$  and  $y = 1$ . Thus, the formula is false for the natural numbers and true for the reals.

*Appendix: natural deduction proof rules*

$$\frac{}{\dots \vdash \varphi \vee \neg \varphi} \text{ (excl mid)} \quad \frac{}{\dots, \varphi \vdash \varphi} \text{ (assum)}$$

$$\frac{\dots \vdash \varphi \quad \dots \vdash \neg \varphi}{\dots \vdash \psi} \text{ (absurd)}$$

$$\frac{\dots \vdash \varphi \wedge \psi}{\dots \vdash \varphi} \text{ (\wedge elim)} \quad \frac{\dots \vdash \varphi \wedge \psi}{\dots \vdash \psi} \text{ (\wedge elim)} \quad \frac{\dots \vdash \varphi \quad \dots \vdash \psi}{\dots \vdash \varphi \wedge \psi} \text{ (\wedge intro)}$$

$$\frac{\dots \vdash \varphi_1 \vee \varphi_2 \quad \dots, \varphi_1 \vdash \psi \quad \dots, \varphi_2 \vdash \psi}{\dots \vdash \psi} \text{ (\vee elim)}$$

$$\frac{\dots \vdash \varphi}{\dots \vdash \varphi \vee \psi} \text{ (\vee intro)} \quad \frac{\dots \vdash \psi}{\dots \vdash \varphi \vee \psi} \text{ (\vee intro)}$$

$$\frac{\dots \vdash \varphi \quad \dots \vdash \varphi \rightarrow \psi}{\dots \vdash \psi} \text{ (\rightarrow elim)} \quad \frac{\dots, \varphi \vdash \psi}{\dots \vdash \varphi \rightarrow \psi} \text{ (\rightarrow intro)}$$