

Some exercises

Mark Ryan

April 16, 2012

These exercises are designed to let you demonstrate your mathematical and computational thinking abilities. Each section is around some theme, and starts with some easier questions and ends with some open-ended issues.

1 Probabilities

Some systems (such as banks) don't ask users for a full password, but only for some parts of it. For example, you may have a 10-character password with your bank, and when you login the bank asks you for three randomly chosen characters, such as the third, fourth and eighth. The idea is that if an attacker overhears this conversation, he does not learn your full password. However, the more such conversations he overhears, the more of your password he may discover.

1. System A uses 4-digit personal secret numbers (i.e., 0000–9999), and on each login attempt it randomly chooses two of the numbers and asks the user to cite them.
 - (a) Suppose the attacker has not made any observations yet, and tries to log into Alice's account by guessing the two digits requested. What is the probability that his guess of the two digits is correct?
 - (b) Suppose the attacker has made one observation of the credentials Alice used to successfully log into her account, and now he tries to log in by himself and is faced with a fresh request of two digits. Assume that he enters the requested digit if he knows it, and otherwise makes a random guess. What is the probability that he can enter them correctly?

- (c) Suppose Bob has made two observations of the correct credentials. What is the probability that he now knows all four digits of Alice's PIN?
2. System B uses a 20-character password, and the system asks for three randomly chosen characters each time the user authenticates. How many sessions must an attacker observe in order to have a 50% chance or more of having obtained the full password? (This is quite complicated.)
 3. Can you set out the problem of Part 2 (system B) as a Markov Chain, and show how to solve it in that setting?

2 Predicate Logic

1. Use the predicates

$$\begin{aligned}
 A(x, y) &: x \text{ admires } y \\
 B(x, y) &: x \text{ attended } y \\
 W(x, y) &: x \text{ is the wife of } y \\
 P(x) &: x \text{ is a professor} \\
 S(x) &: x \text{ is a student} \\
 L(x) &: x \text{ is a lecture}
 \end{aligned}$$

and the nullary function symbols (constants)

$$\begin{aligned}
 m &: \text{ Mary} \\
 j &: \text{ John}
 \end{aligned}$$

to translate the following into predicate logic:

- (a) Mary admires every professor.
- (b) Some professor admires Mary.
- (c) Mary admires herself.
- (d) No student attended every lecture.
- (e) No lecture was attended by any student.
- (f) If John has a wife, he admires her.

2. Prove the following arguments in predicate logic. (You can use any proof method, such as natural deduction, or a system of axioms. Please briefly explain your proof method.)

$$(a) \quad \forall x P(a, x, x), \forall x \forall y \forall z (P(x, y, z) \rightarrow P(f(x), y, f(z))) \\ \vdash \exists z P(f(a), z, f(f(a)))$$

$$(b) \quad \forall x \forall y \forall z (S(x, y) \wedge S(y, z) \rightarrow S(x, z)), \forall x \neg S(x, x) \\ \vdash \forall x \forall y (S(x, y) \rightarrow \neg S(y, x))$$

3. Let ϕ be the formula $\forall x \forall y \exists z (R(x, y) \rightarrow R(y, z))$, where R is a predicate symbol of two arguments.

(a) Consider a model \mathcal{M} with the individuals $\{a, b, c, d\}$ in which R is interpreted as $\{(b, c), (b, b), (b, a)\}$. Do we have $\mathcal{M} \models \phi$? Justify your answer, whatever it is.

(b) Consider a model \mathcal{M}' with the individuals $\{a, b, c\}$ and in which R is interpreted as $\{(b, c), (a, b), (c, b)\}$. Do we have $\mathcal{M}' \models \phi$? Justify your answer, whatever it is.

4. For each of the formulas of predicate logic below, either find a model which does not satisfy it, or prove it is valid:

$$(a) \quad (\forall x \forall y (S(x, y) \rightarrow S(y, x))) \rightarrow (\forall x \neg S(x, x))$$

$$(b) \quad \exists y ((\forall x P(x)) \rightarrow P(y))$$

$$(c) \quad (\forall x (P(x) \rightarrow \exists y Q(y))) \rightarrow (\forall x \exists y (P(x) \rightarrow Q(y)))$$

$$(d) \quad (\forall x \exists y (P(x) \rightarrow Q(y))) \rightarrow (\forall x (P(x) \rightarrow \exists y Q(y)))$$

$$(e) \quad \forall x \forall y (S(x, y) \rightarrow (\exists z (S(x, z) \wedge S(z, y))))$$

5. Part 2 of this exercise was about proof systems, and parts 3 and 4 are about models. Define formally two notions of entailment, one using proof systems (typically written \vdash) and the other using models (typically written \models). What is the relationship between them?

3 Programming

1. **Coins.** You work in a casino as a programmer. You have access to the following API:

```
bool coinflip();
```

It is simply a wrapper around a physical device that randomly produces 0 or 1, each with probability 0.5.

- (a) The manager asks you to create a function

```
int three_face_die();
```

that produces a random number in $\{0, 1, 2\}$ with uniform probability. Of course you can use `coinflip`. How many calls to `coinflip` does your program make?

- (b) The physical device that `coinflip` uses just broke down. Now `coinflip` produces 0 with probability p and 1 with probability $1 - p$, but you don't know what p is. You can assume $0 < p < 1$. Write a function

```
bool fair_coinflip();
```

that works like `coinflip` used to work. Your function has to be correct for all $0 < p < 1$. Stated otherwise, how can you create a non-biased coin from a biased one as subroutine (and without knowing the bias p).

2. **Linked list.** You are given a pointer to the head of a linked list. We want to determine whether the linked list is circular or not. Note that if the list is circular, the last node in the list does not necessarily point to the first node; it can point to any other node.
- (a) Write a function that does this in time $O(n^2)$, where n is the number of nodes.
- (b) Write a function that does this in time $O(n)$. Hint: use two pointers.

4 Searching

1. You start with a box containing zero or more red marbles, zero or more green marbles and zero or more blue marbles, as well as an unlimited supply of red, green and blue marbles outside the box. One move

consists of choosing two different colours, removing two marbles - one of each of your two chosen colours - from the box, and adding a marble of the third colour to the box from your supply. For what starting conditions can you get exactly one marble in the box by performing zero or more moves?

2. A group of adults and children want to cross a river, by boat. The boat will hold one adult or up to two children. How can they all cross? What must be true for the problem to be soluble at all?
3. Suppose you are given (1) a natural number N ; (2) a set of natural numbers $S = \{n_1, n_2, \dots\}$; (3) a set of arithmetic operators, say $+, *, -, /$ (with the usual meaning of addition, multiplication, subtraction, division). Your job is to construct an arithmetic expression R built from the given operators and using each of the numbers in S exactly once, with $R = N$.
 - (a) Explain in general how you could solve that problem.
 - (b) Solve the specific instance: $N = 24$, $S = \{1, 3, 4, 6\}$.

Acknowledgments

I have created these exercises using ideas from the following people (many thanks): Roderick Bloem, Ștefan Ciobâcă, Jean-Sébastien Coron, Hagen Voelzer, Guilin Wang.