CS3102 Theory of Computation
Solutions to Problem Set 1
Department of Computer Science, University of Virginia

Gabriel Robins

Please start solving these problems immediately, and work in study groups. Please prove all your answers; informal arguments are acceptable, but please make them precise / detailed / convincing enough so that they can be easily made rigorous. To review notation and definitions, please read the "Basic Concepts" summary posted on the class Web site, and also read the first chapter from the Sipser textbook.

"Begin at the beginning," said the King very gravely,
"and go on till you come to the end; then stop."

1. True or false:

a. $\emptyset \subseteq \emptyset$

Solution: True; the empty set is a subset of **any** set.

b. $\emptyset \subset \emptyset$

Solution: False; the empty set has no **proper** subsets.

c. $\emptyset \in \emptyset$

Solution: False; the empty set has no elements in it.

d. $\{1,2\} \in 2^{\{1,2\}}$

Solution: True, since $2^{\{1,2\}} = \{\emptyset,\{1\},\{2\},\{1,2\}\}$. Generally, $S \in 2^S$ always holds.

e. $\{1,2\} \subseteq 2^{\{1,2\}}$

Solution: False, since neither 1 nor 2 is a member of $\{\emptyset,\{1\},\{2\},\{1,2\}\}$ (although $\{1\}$ and $\{2\}$ are: watch your types!).

f. $\{x,y\} \in \{\{x,y\}\}$

Solution: True.

2. Write the following set explicitly: $2^{\{1, 2\}} \times \{v,w\}$

Solution: $2^{\{1, 2\}} \times \{v,w\} = \{Ø,\{1\},\{2\},\{1,2\}\} \times \{v,w\}$
$= \{(Ø,v),(\{1\},v),(\{2\},v),(\{1,2\},v),(Ø,w),(\{1\},w),(\{2\},w),(\{1,2\},w)\}$

3. Show that for an arbitrary finite set S, 2^S and $\{0,1\}^{|S|}$ have the same number of elements.

Solution: Any subset T of a finite set S may be uniquely represented by a string of |S| bits, encoding which elements of S are present and which are missing in the subset T. Conversely, any string of n bits uniquely encodes a distinct subset of an n-element set. Thus a set of n elements has exactly 2^n distinct subsets.

4. Which of the following sets are closed under the specified operations:

a) $\{x \mid x \text{ is an odd integer}\}$, multiplication

Solution: Closed, since the product of two integers is always an integer.

b) $\{y \mid y=2n, \text{ n some integer}\}$, subtraction

Solution: Closed, since the difference of two even integers is always an even integer.

c) $\{2m+1 \mid \text{m some integer}\}$, division

Solution: Not closed, since the quotient of two odd integers is usually not an odd integer.

d) $\{z \mid z=a+bi \text{ where a and b are real and } i=\sqrt{-1}\}$, exponentiation

Solution: Closed, since for two complex numbers x and y, x^y is always a complex number.

5. Is the transitive closure of a symmetric closure of a binary relation necessarily reflexive? (Assume that every element of the "universe" set participates in at lease one relation pair.)

Solution: In general, for any pair (x,y) in such a relation, closure under symmetry implies (y,x) is also in the relation, and closure under transitivity then implies that (x,x) must be in the relation as well. Thus, such a relation must necessarily be reflexive. The only exceptions to this are relations where some elements of the domain are not involved in any tuple of the defined relation (but defining the domain of a relation to implicitly be equal to the union of all elements involved in any tuple eliminates such exceptions, and makes the original statement true in general).

6. True or false: a countable union of countable sets is countable.

Solution: Use dovetailing to arrange a list of all the elements in all the sets. The elements (i,j) on such a list may, for example, be sorted by the magnitude of the sum i+j where (i,j) corresponds to the i^{th} element of the j^{th} set.

7. True or false: if T is countable, then the set $\{S \mid S \subseteq T, S \text{ finite}\}$ is also countable.

Solution: If T is countable, then the set $\{S \mid T \subseteq S, S \text{ finite}\}$ is indeed countable; note that it is not sufficient to simply list the finite subsets of T by increasing size, because there may be an infinite number of them for a particular size (even for size 1, e.g., all the singleton (one-element) subsets in T), and so our list will not be exhaustive. On the other hand, since S is constrained to be finite, a finite description would suffice to completely describe such an S: in the worst case, simple list all the indices in T of the elements of S using some unique code (e.g., encode each $S=\{T_{i_1}, T_{i_2}, ..., T_{i_k}\}$ as the string $\$i_1\$i_2\$...\$i_k\$$). Now sort all of these strings by lexicographic order (size first, and then within size by dictionary order), to give us a one-to-one correspondence between $\{S \mid T \subseteq S, S \text{ finite}\}$ and the naturals. Note that if the restriction "finite" on S is lifted, our original definition (which now boils down to $\{S \mid T \subseteq S\}$), is simply that of the powerset of S, which has cardinality always bigger than S itself.

8. Give a simple bijection for each one of the following pairs of sets:

a) the integers, and the odd integers.

Solution: $h(x) = 2x+1$

b) the integers, and the positive integers.

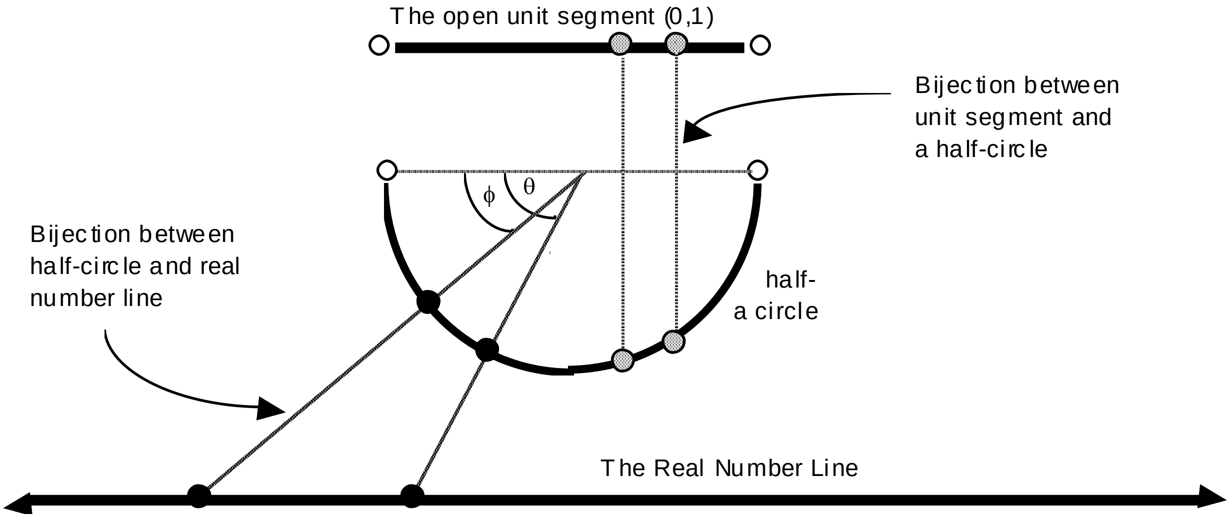
Solution: $g(x) = 2x+1$ if x is a non-negative integer
$g(x) = -2x$ if x is a negative integer

c) the naturals, and the rationals crossed with the integers.

Solution: Represent each element of $\mathbf{Q}\times\mathbf{Z}$ as $(\frac{a}{b},c)$, where $a,b,c \in \mathbf{Z}$, $b\neq0$, and sort these elements by increasing order of $|a|+|b|+|c|$. Now simply number the elements in this sorted list using the natural numbers, and this is the bijection we seek. Note: this was an implicit use of dovetailing.

9. Is there a bijection between $\{x \mid x \in \mathbf{R}, 0 \leq x \leq 1\}$ and $\mathbf{R}$?

Solution: Yes; there exists a number of possible bijections between the open unit interval $(0,1)=\{x \mid x\in\mathbf{R}, 0<x<1\}$ and $\mathbf{R}$; here we pictorially present one possible bijection (constructed via the intermediate curve of a half-circle):


The open unit segment (0,1)
Bijection between unit segment and a half-circle
φ
θ
Bijection between half-circle and real number line
half-a circle
The Real Number Line

But the interval $[0,1] = \{x \mid x\in\mathbf{R}, 0\leq x\leq 1\}$ is **closed** (i.e., containing its endpoints 0 and 1), so now the question is "to what points on the real line do we map the end points 0 and 1 of the unit interval?" One possible answer is to look at one countable subset of our bijection relation: $\{(\frac{1}{2}, x_1), (\frac{1}{4}, x_2), (\frac{1}{8}, x_3), (\frac{1}{16}, x_4), \ldots, (\frac{1}{2k}, x_k), \ldots\}$ where the first components are points in the unit interval, and the second components are the corresponding points on the real number line. Now we simply modify our original bijection by replacing this entire family of pairs by the following new family: $\{(\frac{1}{2}, 0), (\frac{1}{4}, 1), (\frac{1}{8}, x_1), (\frac{1}{16}, x_2), (\frac{1}{32}, x_3)\ldots, (\frac{1}{2k+2}, x_k), \ldots\}$; we have simply pushed every point in this family two places down to accommodate our two endpoints (remember the story of the hotel with the infinite number of rooms!). Now the two problematic endpoints 0 and 1 **are** included, and we are left with a perfect bijection between the **closed** unit interval and the real numbers.

"Why," said the Dodo, "the best way to explain it is to do it."

10. Generalize $|2^S| > |S|$ to arbitrary sets (not necessarily countable ones).

Solution: Assume towards contradiction that some bijection actually exists between S and 2^S, and call it f: $S \rightarrow 2^S$. Now form the set $S' = \{x \mid x \in S,\ x \notin f(x)\}$, and since we have a bijection between S and 2^S, and $S' \in 2^S$, there must exist some $x' \in S$ such that $f(x')=S'$. We can't have $x' \in S'$ (since by the definition of S' we know that then x' **may not** be included in S'), **but** on the other hand we can't have $x' \notin S'$ either (since then by definition we **must** have included x' in S'), a logical contradiction. It follows that a set and its powerset can never have the same cardinality. This proof is due to Georg Cantor in the late nineteenth century; note how it generalizes the diagonalization argument (which was used to show that $|\mathbf{N}|<|\mathbf{R}|$) to arbitrarily large sets.

11. What is the cardinality of each of the following sets ?

a. The set of all polynomials with rational coefficients.

Solution: The set of all polynomials with rational coefficients is countable (and hence of cardinality $\aleph_0$): simply sort all such polynomials $\frac{a_k}{b_k} X^k + \frac{a_{k-1}}{b_{k-1}} X^{k-1} + ... + \frac{a_1}{b_1} X + \frac{a_0}{b_0}$ where $a_i, b_i \in \mathbf{Z}$ is sorted by increasing order of $(\sum|a_i|) + (\sum|b_i|) + |k|$, and then number the items on this list with consecutive integers beginning with 1 on up. Clearly every polynomial appears somewhere on our list, and so this scheme describes a bijection between natural numbers and the polynomials with rational coefficients.

b. The set of all functions mapping reals to reals.

Solution: The set F of all functions mapping reals to reals is certainly at least as big as $|\mathbf{R}|=\aleph_1$ simply by considering the subset of F consisting of the constant functions $\{f_r \mid f_r{:}\mathbf{R}\rightarrow\mathbf{R},\ r\in\mathbf{R},\ f_r(x)=r\}$. Moreover, we can see that F is also at least as big as the powerset of the reals, by considering the subset of F consisting of the class of boolean-valued "subset" selector functions over the reals: $F_S = \{f_S \mid f_S{:}\mathbf{R}\rightarrow\mathbf{R},\ S\subseteq\mathbf{R},\ f_S(x)=1 \text{ if } x\in S \text{ and } f_S(x)=0 \text{ if } x\notin S\}$. The cardinality of F_S is clearly $|2^{\mathbf{R}}| = \aleph_2$, and therefore since $F_S \subseteq F$ we have $|F| \geq \aleph_2$. Finally, we observe that functions from reals to reals are a special case of arbitrary 2-place relations on the reals, and that any such relation τ is an arbitrary subset of the real plane so $\tau \subseteq \mathbf{R}\times\mathbf{R}$. It follows that there exist exactly as many such relations as subsets of the plane, namely the number of such relations is $\left|2^{\mathbf{R}\times\mathbf{R}}\right|=2^{|\mathbf{R}\times\mathbf{R}|}=2^{|\mathbf{R}|}=\aleph_2$. Since a function is a special case of a relation (i.e., a relation with at most one element in the range for every element in the domain), it follows that the number of functions from reals to reals is also bounded from above by $\aleph_2$. Combining this result $|F| \leq \aleph_2$ with our previous $|F| \geq \aleph_2$ gives us the exact characterization we seek: $|F|= \aleph_2$.

c. The set of all possible Java programs.

Solution: The set of all possible Java programs is countable: simply list all such programs by increasing size (considering a program to be one long ASCII string), and within a particular size list them by lexicographic order. This scheme describes a bijection between natural numbers and Java programs.

d. The set of all finite strings over the alphabet $\{0,1,2\}$.

Solution: This is the language $\{0,1,2\}^*$, a countable set: simply sort by string size and then by lexicographic order within size, numbering the resulting list with consecutive natural numbers.

e. The set of all 5×5 matrices over the rationals.

Solution: This set of all 5×5 matrices over the rationals can be put into one-to-one correspondence with $\mathbf{Q}^{25}$or $\mathbf{Z}^{50}$which are both countable sets (by dovetailing)..

f. The set of all points in 3-dimensional Euclidean space.

Solution: The set of all points in 3-dimensional Euclidean space R^3 is isomorphic to any one of the following sets: $\mathbf{R}^2$, $\mathbf{R}=\mathbf{R}^1$, $\mathbf{R}^k$ for any positive integer k, $[0,1]=\{x|\ x\in\mathbf{R},\ 0\leq x\leq 1\}$, $[0,\varepsilon]$ for any real $\varepsilon>0$, etc, which are all of cardinality $|\mathbf{R}|=\aleph_1$. In particular, a simple bijection between $\mathbf{R}^3$ and $\mathbf{R}$ may be given as follows: each real number may be "decomposed" into a unique triple of real numbers by taking all the digits with position divisible by 3 (with respect to the decimal point) as the first number of the triple, all the digits with position divisible by 3 (mod 1) as the second number of the triple, and all the digits with position divisible by 3 (mod 2) as the third number of the triple; conversely, a triple of real numbers may be "fused" into a unique real number by reversing this process.

g. The set of all valid English words.

Solution: This is a large but **finite set** (see English Oxford Dictionary), whose cardinality is less than one million.

h. $\{\varnothing, \mathbf{N}, \mathbf{Q}, \mathbf{R}\}$

Solution: This is a **finite** set of cardinality four (although each of these elements is itself a set).

i. **N** × **Z** × **Q**

Solution: The cardinality of any finite cross-product of countable sets is countable, by a simple argument: take a countable class of countable sets S_1, S_2, S_3, ..., S_k, and form the cross product by left-association rule, such as $(((S_1 \times S_2) \times S_3) \times \ldots \times S_k)$. But we already know that the cross-product of two countable sets is countable, by dovetailing (like in the proof that **Q** is countable), so it follows that at any intermediate stage in the computation of our form above remains countable.

It is important to note that there is only a finite number of cross-product operations here (namely two); if there was a countably infinite number of cross-product operations, then this result would no longer hold. For example, if we cross the integers with themselves a countably infinite number of times, we get a set at least as large as the reals. That is, each element in our infinite cross-product is an infinite ordered tuple, or a point in infinite-dimensional Euclidean space (also called a Hilbert space, after the mathematician who invented it, David Hilbert). But such a tuple $(s_1, s_2, s_3, \ldots, s_k, \ldots)$ can uniquely represent an arbitrary real number $0.s_1s_2s_3\ldots s_k\ldots$

j. **R** - **Q**

Solution: In general, the cardinality of an uncountable set minus a countable one is still uncountable: if S = **R** - **Q** was countable, then so would be S ∪ **Q** = **R**, which we already know is not countable.

"And thick and fast they came at last, and more, and more, and more"

12. Show that n^4-$4n^2$ is divisible by 3 for all $n \geq 0$.

Solution: This can be done by induction. However, a simpler proof starts with the observation that n^4-$4n^2$ = $(n^2)(n+2)(n-2)$ and then noting that at least one of the factors n, n+2 or n-2 (or equivalently n, n-1 or n+1) must be divisible by 3.

13. How many distinct boolean functions on N variables are there? In other words, what is the value of $|\{f \mid f:\{0,1\}^N \rightarrow \{0,1\}\}|$?

Solution: An N-ary boolean function is defined at 2^n points in its domain, each of which can be mapped to one of two values. Thus the number of such distinct functions is 2^{2^n}.

14. How many distinct N-ary functions are there from finite set A to finite set B? Does this generalize the previous question?

Solution: An N-ary function from a finite set A to a finite set B is defined at $|A|^n$ points in its domain, each of which can be mapped to one of |B| values. Thus the number of such distinct functions is $|B|^{|A|^n}$.

15. Show that in any group of people, there are at least two people with the same number of acquaintances within the group. Assume that the "acquaintance" relation is symmetric but non-reflexive.

Solution: In a group of N people, each person knows between 0 and N-1 people. If for all K such that $0 \le K \le N-1$ there is a person in the group that knows K other people, then some person P must know all N-1 people, which means that all other N-1 people must know P. It follows that nobody in the group knows exactly 0 people, as required, which leaves only N-2 distinct choices for K. Since there are now only N-1 possibilities for the number of acquaintances for each of the N people, it follows by the pigeon-hole principle that two people must have the same number of acquaintances.

16. Show that in any group of six people, there are either 3 mutual strangers or 3 mutual acquaintances.

Solution: This is an easy result from an elegant branch of combinatorics called Ramsey Theory: consider the complete graph on 6 vertices (representing the people), where edges are colored either blue or red (representing the "strangers" or "acquaintances" relationship), respectively. Focus on a particular vertex V; by the pigeon-hole principle, at least 3 of the edges emanating from V are of the same color , which without loss of generality we can assume to be red. Call the vertices at the ends of these edges X, Y, and Z. If any of the edges (X,Y), (Y,Z), or (Z,X) is also red, then we have a red triangle, and the theorem is true. On the other hand, if all of these edges are blue, we have a blue triangle and the theorem is true again. This is another illustration of the power of the pigeon-hole principle: in general, if k objects are placed into j bins, at least one bin must contain $\lceil \frac{k}{j} \rceil$ objects; when k=j+1 this boils down to the weaker (but more common) version of the pigeon-hole principle.

17. A clique in a graph is a complete subgraph (i.e., all nodes are connected with edges). Show that every graph with N nodes contains a clique or the complement of a clique of size at least ½ $\log_2 N$.

Solution: This is a generalization of the previous problem. First, color all the edges of the graph blue, and add all the missing edges and color those new edges red. Now we need to find a mono-chromatic (i.e., same-color) clique of size ½ $\log_2 N$. Select one node V_1 at random, and observe that by the pigeon-hole principle it must have adjacent edges of the same color to at least half of the remaining nodes; keep those nodes, but eliminate all the rest of the nodes (and their adjacent edges) from the graph, and color V_1 using the color of its adjacent edges. Now, iterate this process with the remaining (smaller) graph: pick another node V_2, find out which color dominates at least half of its adjacent nodes, color V_2 using that color, eliminate the remaining nodes, and keep iterating. After $\log_2 N$ iterations there will be no nodes left, and at that point we have colored $\log_2 N$ nodes along the way, one node per iteration. Note that by the pigeon-hole principle at least half of those nodes are of the same color, so the subgraph induced by those same-colored nodes is a clique of size ½ $\log_2 N$.

18. Show that the difference of an uncountable set and a countable set is uncountable.

Solution: This generalizes problem 11(j): for an arbitrary uncountable set U and an arbitrary countable set C, note that $U - C = U - U\cap C$. But $U\cap C$ is countable since $|U\cap C| \leq |C|$ and C is countable. We assume towards contradiction that $U - C = U - U\cap C$ is countable. Since the union of countable sets is countable, this implies that $(U - U\cap C) \cup (U\cap C) = U$ is countable as well, a contradiction.

19. Show that the intersection of two uncountable sets can be empty, finite, countably infinite, or uncountably infinite.

Solution: $[0,1] \cap [3,4] = \emptyset$, $[0,1] \cap [1,2] = \{1\}$, $(\mathbf{Q}\cup[0,1]) \cap(\mathbf{Q}\cup[1,2]) = \mathbf{Q}$, $\mathbf{R}\cap\mathbf{R}=\mathbf{R}$

20. For an arbitrary language L, prove or disprove each of the following:

a) $(L^*)^*=L^*$

Solution: $(L^*)^*=L^*$ is always true:

$L^* = L^0\cup L^1\cup L^2\cup L^3\cup...$

$(L^*)^* = (L^*)^0\cup(L^*)^1\cup(L^*)^2\cup(L^*)^3\cup... = \{\wedge\}\cup (L^*)\cup(L^*)^2\cup(L^*)^3\cup... = L^*$

b) $L^{+}=L^{*}-\{\text{^}\}$

<u>Solution</u>: $L^{+}=L^{*}-\{\text{^}\}$ is sometimes false. For a counter-example, let $L = \{\text{^}\}$, so $L^{+} = \{\text{^}\}$, but $L^{*}-\{\text{^}\} = \varnothing$. In fact, any language L containing the empty string ^ would constitute a counter-example, since L^{+} will contain ^ but $L^{*}-\{\text{^}\}$ will not.

"Is that all?" Alice timidly asked.

The Purpose of this Assignment

This assignment was designed to increase your familiarity with the basic concepts of and notation of discrete mathematics, including infinite sets. Don't be discouraged if you were not able to solve all of the problems, as some of them involved certain mathematical insights that you may not have encountered before. However, if you were not able to solve at least two-thirds of these problems, please spend considerable additional time reviewing this material. Go over the solutions above carefully, and try to understand why you missed some of them. Also work in groups with other students on solving homework problems – solving problems in teams is efficient, as well as a lot of fun. And of course, please solve lots of different problems (including other ones from our textbook as well as from other books) – there’s no substitute for lots of practice!

On Better Mastering the Material

One study method that I recommend is to put problems and concepts on index cards (and their solutions or definitions on the backs of the cards), and carry them in your pocket/purse; whenever you have a free moment (like when you wait for a bus, or stand in line at a store, etc.), pull a card out and try to solve a problem, reconstruct a proof, or recall a definition (a positive side-effect of this scheme is that you will tend to get less angry/impatient while waiting in these lines, because you will no longer be wasting your valuable time). If you get in this habit, you will find that you can solve these problems more and more quickly, and that you are becoming more fluent in the material. Please keep in mind that the basic definitions in this course are very important, since the material builds very heavily on top of previous material. Ideally, you should be able to recite (and explain) the basic definitions and proof techniques at any time and without hesitation. Most importantly, if you are not clear on something, please ask ASAP!

Alice thought "..No, it'll never do to ask:
perhaps I shall see it written up somewhere."