Mathematical Foundations of Computer Science

# Ten Powerful Ideas

*and applications*

| QUIZ 2 Solutions | Bruce Maggs | March 16, 1998 |
| --- | --- | --- |

**NAME :**

**ANDREW ID :**

**SECTION : A B C D**

**INSTRUCTIONS.** For the first 7 problems you do not need to give any reason or justification for your answers. For the remaining problems you must give complete explanations. WRITE CLEARLY. WRITE YOUR NAME AND ANDREW ID ABOVE AND CIRCLE YOUR SECTION.

**Repeat After Me.**

This part is to test your ability to study material that has been pre-digested and labeled as useful or likely to appear on exams. If you do not do well on this section, your study habits could use adjustment.

**1.** [5 points]
How many ways are there of seating $n$ people around a circular table? (Two seatings are considered the same if one is simply a circular shift of the other.)

$(n-1)!$

**2.** [5 points]
True or false: for all sets $A$ and $B$, if $A \subset B$ and $A \neq B$, then $|A| \neq |B|$.

False, e.g. the even numbers have the same cardinality as all integers.

**3.** [5 points]
True or false: the rational numbers are countable.

True.

**4.** [5 points]
Give a formula for $|A \cup B \cup C|$ in terms of the intersections of $A$, $B$, and $C$, where $A$, $B$, and $C$ are finite sets.

$|A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$.

5. [5 points]
How many functions are there from the integers in the range $[1 \ldots k]$ to the boolean values $\{0, 1\}$?

$2^k$.

6. [5 points]
True or false: the problem of 2-coloring a graph is NP-complete.

Most likely false. 2-coloring a graph is in P, and it is widely believed that P is not equal to NP.

**Reading Solutions.**

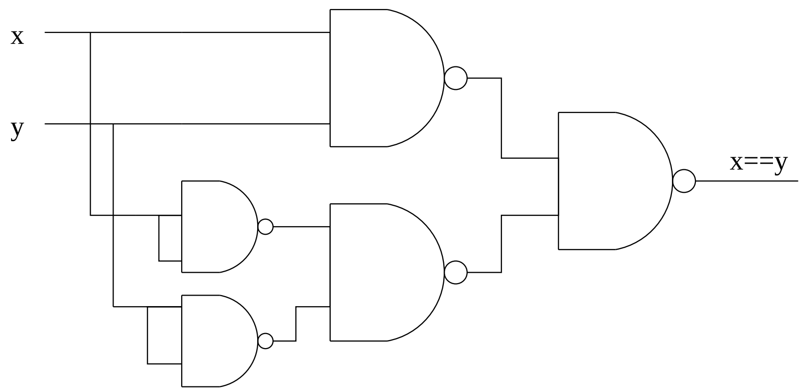
This section tests your understanding of the homework assignments, including your ability to read the homework solutions that we hand out.

7. [5 points]
How many different poker hands are flushes?

$4 * C(13, 5) - 4 * 9$. The second term is for straight flushes.

8. [10 points]
Using only NAND gates, draw a circuit that computes the EQUALS function, described in the truth table below. (You may use your NAND gate to design other kinds of gates and then use these gates.)

| $x$ | $y$ | $x == y$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |



**Basic Techniques.**

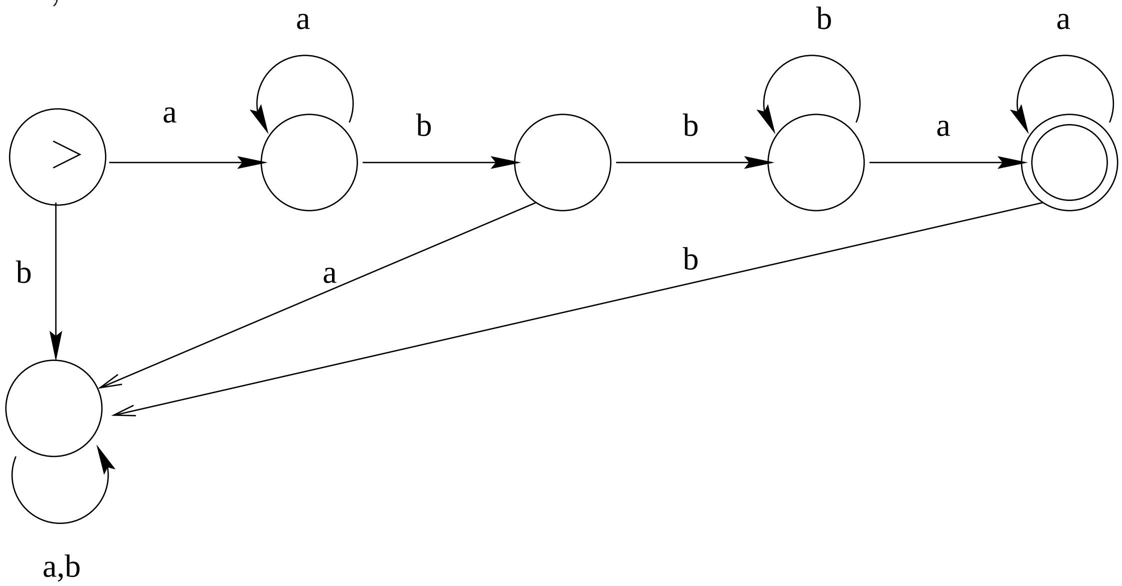
**This part will test your ability to apply techniques for which I have given explicit recipes. If you do not do well on this section, your study habits could use adjustment.**

**In order to show that two sets $R$ and $S$ have the same cardinality, it suffices to find a function $f : R \to S$ and then *prove* that $f$ is both one-to-one and onto. A function $f$ is one-to-one if for all $x$ and $y$ in $R$, if $f(x) = f(y)$ then $x = y$. A function is onto if for every $s \in S$, there exists an $r \in R$ such that $f(r) = s$.**

**9. [10 points]**
**Prove that the set of all even integers has the same cardinality as the set of all integers that are multiples of three.**

**The function $f(x) = 3/2x$ is a bijection from the evens to the multiples of three. It is one-to-one: $3/2x = 3/2y$ implies that $x = y$. It is onto because any multiple of 3, $3k$, is in the range as $f(2k)$. Futhermore, the range of $f$ is confined to multiples of $3$ when the domain is evens.**

**10. [10 points]**
**Draw a finite automaton that accepts the language of consisting of all strings of $a$'s and $b$'s that can be formed by starting with the name of the "easy listening" rock group $abba$ and replacing each $a$ with a non-empty string of $a$'s and each $b$ with a non-empty string of $b$'s. Examples of strings in the language include $abba$, $aaaabba$, and $aaabbbbaaa$.**



**A Moment's Thought!**

**This section tests your ability to think a little bit more insightfully. You must give complete explanations of your answers.**

**11. [15 points]**
**Ben Bitdiddle (our favorite misguided 15-299 student) has just made a remarkable discovery. He has designed an algorithm that can factor any number $n$ in time that is polynomial in $n$. In fact, his algorithm is so simple that he can explain it to anyone: First see if $2$ divides $n$, then see if $3$ divides $n$, then see if $4$ divides $n$, and so on. It takes at most $n-1$ divisions to find all of the factors of $n$. Knowing that the most powerful cryptographic systems rely on the difficulty of factoring, Ben is deeply concerned about the national security implications of his discovery. So he turns to another 15-299 student for advice. This student tells Ben that in one minute, with paper and pencil, a man can write out the digits of a base-10 number that all of the computers in the world working together for a full year in 1998 could not factor using Ben's algorithm. How can this be?**

**Ben's algorithm is not as fast as he thinks. On a prime input $p$, he must do $p-1$ divisions. Thus, if we write down a prime with, say, one hundred digits, (larger primes are known), it will be require at least $10^{100}$ divisions, which is a lot!**

**12. [20 points]**
**Prove that the set of complex numbers whose real and imaginary parts lie in the ranges $[0, 1]$ and $[0 \cdot i, 1 \cdot i]$ has the same cardinality as the set of real numbers in the range $[0, 1]$.**

**Too help you solve this problem, I will provide a useful lemma. It's proved on the last page of the quiz, in case you're curious about the proof.**

**Lemma:** *The set of real numbers in the range $[0, 1]$ can be placed in one-to-one and onto correspondence with the set of countably infinite sequences of base-10 digits.*

**Hint: Use this lemma to dovetail through the complex numbers.**

**That hint stinks! Way to go, Maggsnito. Each complex number consists of a real and an imaginary part, both of which can be represented by a real in the range $[0, 1]$. By the lemma, we know there is a bijective function from these two numbers to two infinite sequence of base-10 digits, say $[a_1, a_2, \ldots]$ and $[b_1, b_2, \ldots]$. We can define a bijection from pairs of infinite sequences to single infinite sequences by $f([a_1, a_2, \ldots], [b_1, b_2, \ldots]) = [a_1, b_1, a_2, b_2, \ldots]$. This is clearly one-to-one and onto. Furthermore, the set of infinite sequences has the same cardinality as reals in the range $[0, 1]$. Therefore, by transitivity of cardinality, we're done.**

**Lemma:** *The set of real numbers in the range $[0,1]$ can be placed in one-to-one and onto correspondence with the set of countably infinite sequences of base-10 digits.*

**Proof of Lemma: Any real number can be expressed as a countably infinite sequence of digits using its base-10 representation. For example, $1/3$ can be expressed as $0.3333\ldots$, $1/\sqrt{2}$ as $0.70710678\ldots$, and $1/2$ as $0.50000\ldots$. This observation would give us a one-to-one and onto correspondence between the reals and the sequences, except for one annoying detail: some real numbers have two representations! As an example, $1/2$ can also be expressed as $0.49999\ldots$. This detail makes the proof messy, so I'll take care of it for you.**

**A real number in $[0,1]$ has two countably infinite representations if and only if it has a finite representation. In the previous example, the finite representation of $1/2$ is 0.5. The real numbers with finite representations are all rational, and there are a countably infinite number of them. This means that the set of sequences of base-10 digits that "share" a real number with another sequence is also countably infinite.**

**To place the reals in the range $[0,1]$ into one-to-one and onto correspondence with the sequences, we will handle the rationals and the irrationals separately, as in Question 2 on Assignment 7. Each irrational number is placed into correspondence with its base-10 representation. This mapping is one-to-one and onto. The set of rationals is put into one-to-one and onto correspondence with the set of sequences of base-10 digits that represent one or two rational numbers – but now some sequences are in correspondence with rational numbers that they do not represent, and vice versa.** $\square$