Quiz 9 Solutions

written by Alvin Wan . alvinwan.com/cs70

Wednesday, October 5, 2016

This quiz does not count towards your grade. It exists to simply gauge your understanding. Treat this as though it were a portion of your midterm or final exam.

1 Error Correction

1. There are n students in a room. Of the students in the room, approximately $k << n$ will mis-remember the information given to them. Given a secret m, construct a scheme to recover the secret.

   Solution: Construct a polynomial of degree $p-1$, called $P(x)$ such that $P(0) = m$. Assign each student 1 point. Then, any group of $p + 2k$ students can recover the secret; as to recover from at most k errors, we need $p + 2k$ students to gather.

2 Countability

1. **True** or **False**: $\mathbb{N}$ has the same cardinality as the set of all positive numbers divisible by 10. (Extra: Prove this if it's true, or provide a counterexample if otherwise.)

   Solution: True.

   We construct a bijection from $\mathbb{N}$, to B, the set of all numbers divisible by 10. Let the bijection be $f(a) = a * 10$. This is injective as no two multiples of 10 could map to the same a. It is additionally surjective, as all positive multiples of 10 are of the form $10k$, where $k \in \mathbb{N}$.

2. Prove that the set of all polynomials (finite-degree and infinite-degree) is uncountably infinite. Let the coefficients be drawn from the set of all integers.

   Solution: Consider just $x = 10$ for all polynomials $p(x)$. For all possible polynomials with coefficients a_i (considering $x = 10$), we're actually constructing base-10 numbers. Negate all degrees, so that the base-10 number is now between (0, 1). Assume for contradiction that the set of all polynomials is countable. This means all real numbers between (0, 1) are countable. Contradiction.

   Note that this only works because we included infinite-degree polynomials, which are required to represent irrationals such as $\sqrt{2}$. With that said, "infinite-degree polynomials" are Taylor series.

3. Prove that the set of all unique polynomials in GF(p), for some prime p, is countable. Let the coefficients be drawn from the set of all integers.

   Solution: In mod p, we have exactly p^p possible polynomials. Since this is finite, we can arbitrarily number the polynomials for some ordering. Thus, the set of all unique polynomials in **GF**(p) is enumerable, or likewise, countable.