Quiz 8 Solutions

written by Alvin Wan . alvinwan.com/cs70

Monday, October 3, 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 Polynomials

1. **True** or **False** We can construct two equal polynomials, where one has k non-zero coefficients b_i and the other has k distinct roots e_i (i.e.,$\Pi c_i(x - e_i) = b_{k-1}x^{k-1} \cdots b_1 x + b_0$)

   Solution: False.

   A polynomial with k coefficients has degree $k-1$. A polynomial with k roots has degree k. It is impossible for a polynomial of degree k to equal a polynomial of degree $k-1$.

2. **True** or **False** For some prime p, we know a polynomial of degree $p+1$ is not unique by Fermat's Little Theorem in $GF(p)$. Is a polynomial of degree p unique in $GF(p)$? $p-1$? (Remember that, for this course, $GF(p)$ just means all polynomials are taken p).

   Solution: No. Yes.

   We can only apply the variant of Fermat's Little Theorem where $x^p \equiv x(\mod p)$. This version of FLT applies because p is prime. However, we cannot apply $x^{p-1} \equiv x(\mod p)$ since x could be 0.

3. From a group, at least b members must come together to unlock the secret. All members carry the same amount of unique information and $b-1$ members are not sufficient. If only $b-a$ members come together, how many possible polynomials would they need to try? How many possible secrets? Assume this is in $GF(p)$ for some prime p. (Consider the case where $a = 0$, then $a = b$)

   Solution: p^a, p

   The first two sentences simply mean that each member carries 1 point, for a polynomial uniquely identified by b points. This means that when $b-a$ members gather, the group is a points shy of uniquely constructing the polynomial. For each point, we have p possibilities, making p^a total combinations of points we could pick to construct a polynomial.

   By convention in secret sharing, we pick $p(0) = b_0$ to be our secret. For b_0 we have only p possible values.