Quiz 8

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.,$\Pi c_i(x - e_i) = b_{k-1}x^{k-1} \cdots b_1 x + b_0$)

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).

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 $a = b$)