Quiz 9

written by Alvin Wan . alvinwan.com/cs70

Tuesday, February 23, 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. "Intuition Practice" might be tricky; watch out for subtleties. "Proofs" will be challenging to start; develop an arsenal of *approaches* to starting a problem.

1 Intuition Practice

1. In $GF(p)$, p^3 unique polynomials of degree d can share $d-1$ points.
2. In $GF(p)$, $p(x)$ of degree d and $q(x)$ of degree d-1 such that a degree 1 polynomial $y(x) = \frac{p(x)}{q(x)}$ satisfies $p(-y(0)) = 0$, where $d < p-1$.
3. No polynomial with the coordinates $(-1, 1), (0, 0), (2, 4)$ exist in $GF(8)$. (Hint: See what lagrange interpolation does. Remember what I said about the space of algorithm outputs.)