Quiz 9 Solutions

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.

   False. A degree d polynomial is uniquely defined by $d+1$ points. Thus, for each fewer point we require, there is another p set of points we can choose. There are only p^2 unique polynomials of degree d that 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 $d < p-1$.

   True. Let us rewrite y as $y = x - e$. This means $y(0) = -e$ and that $p(-(-e)) = p(e) = 0$. In short e is a root of p.

   We see that $y(x) = \frac{p(x)}{q(x)}$, so $y(x)q(x) = p(x)$ where $y(x) = x - e$, so $(x-e)q(x) = p(x)$ where e is a root of p. This means that $q(x)$ is composed exactly of the d-1 other roots of $p(x)$.

   Thus, the problem can be reduced to "In $GF(p)$, can two polynomials of degree d and d-1, respectively, share d-1 roots, where $d < p-1$?" This is most definitely True.

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.)

   False. These are the coordinates for x^2, which definitely exists in $GF(8)$. Be careful to not confuse "all polynomials that Lagrange Interpolation can output" with "all polynomials". At some point in lagrange interpolation, there will be a 2 in the denominator, and since $2^{-1} \pmod 8$ does not exist, the algorithm will fail.