Discussion 4B Recap

Tyler Zhu

February 28, 2020

1 Polynomials

- There are two ways to uniquely determine a degree d polynomial:
  - using $d+1$ coefficients
  - using $d+1$ points
- A nonzero degree d polynomial has at most d roots
- Working over GF(p) (the Galois Field of size p) is equivalent to working over mod p (i.e. all coefficients and variables are interpreted this way).
- Polynomial Division Algorithm: given polynomials $p(x), q(x)$, we can write $p(x) = q(x)h(x) + r(x)$, where $\deg r < \deg q$ (compare to integer division algorithm).
- # of polynomials of degree $\leq d$ over GF(p) passing through $d+1-k$ points is p^k

2 Secret Sharing

- We want to share a secret that needs consensus of at least k people to reveal.
- Scheme is to create a degree $k-1$ polynomial with $P(0) =$ secret and give everyone a different pair $(i, P(i))$
- One variation is if we need different amount of types of people to agree (a secretary general and 55 people or just 164 people). Simply give different people more shares, i.e. weighting scheme.
- Another variation is if different committees need to agree to reveal the secret. Create polynomials for each committee and distribute shares to their members. Only when all members agree will their committee secret be revealed; need all committee secretes to reveal the overall secrets.
- Can't use the first scheme in the second case as different people in different committees can then collude.