CS 70 Discrete Mathematics and Probability Theory
Spring 2020 **DIS 5A**

1 Secret Sharing Practice

Consider the following secret sharing schemes and solve for asked variables.

(a) Suppose there is a bag of candy locked with a passcode between 0 and an integer n. Create a scheme for 5 trick-or-treaters such that they can only open the bag of candy if 3 of them agree to open it.

(b) Create a scheme for the following situation: There are 4 cats and 3 dogs in the neighborhood, and you want them to only be able to get the treats if the majority of the animals of each type are hungry. The treats are locked by a passcode between 0 and an integer n.

(c) Let p be a degree 3 polynomial modulo 7, and $p(1) = 2, p(2) = 1, p(3) = 5, p(4) = 5$. Find p.

Solution:

(a) Solutions vary. The polynomial should be degree 2 and each trick-or-treater should be given the polynomial evaluated at one point.

(b) The guiding principle in this solution is that a polynomial of degree d, is uniquely determined by $d+1$ points. Let there be three polynomials, one for cats c, one for dogs d, and one joint one j that has the secret that actually unlocks the treats. c will be degree 2 since you need 3 cats to agree to get the 3 points to uniquely determine it. and d with be degree 1 since you need 2 dogs to agree to get the 2 points to uniquely determine it. The j will be degree 1 and $c(0)$ will be $j(1)$, and the $d(0)$ will be $j(2)$. This way you need both the point from the dogs and the point from the cats to uniquely determine j and otherwise you will be unable to determine the $j(0)$. This is also why we make $j(0)$ our secret.

(c) We use Lagrange interpolation to construct the unique quadratic polynomial $P(x)$ such that

$p(1) = 2, p(2) = 1, p(3) = 5, p(4) = 5$:

$$\begin{aligned}
\Delta_1(x) &= \frac{(x-2)(x-3)(x-4)}{(1-2)(1-3)(1-4)} = \frac{(x-2)(x-3)(x-4)}{-6} \equiv (x-2)(x-3)(x-4) \pmod{7} \\
\Delta_2(x) &= \frac{(x-1)(x-3)(x-4)}{(2-1)(2-3)(2-4)} = \frac{(x-1)(x-3)(x-4)}{2} \equiv 4(x-1)(x-3)(x-4) \pmod{7} \\
\Delta_3(x) &= \frac{(x-1)(x-2)(x-4)}{(3-1)(3-2)(3-4)} = \frac{(x-1)(x-2)(x-4)}{-2} \equiv 3(x-1)(x-2)(x-4) \pmod{7} \\
\Delta_4(x) &= \frac{(x-1)(x-2)(x-3)}{(4-1)(4-2)(4-3)} = \frac{(x-1)(x-2)(x-4)}{6} \equiv 6(x-1)(x-2)(x-4) \pmod{7} \\
P(x) &= 2\Delta_1(x) + 1\Delta_2(x) + 5\Delta_3(x) + 5\Delta_4(x) \\
&\equiv 2x^3 + x^2 + 3x + 3 \pmod{7}
\end{aligned}$$

2 Secret Sharing

Suppose the Oral Exam questions are created by 2 TAs and 3 Readers. The answers are all encrypted, and we know that:

- Both TAs should be able to access the answers
- All 3 Readers can also access the answers
- One TA and one Reader should also be able to do the same

Design a Secret Sharing scheme to make this work.

Solution:

Use a degree 2 polynomial and requires at least 3 shares to recover the polynomial. Generate a total of 7 shares, give each Reader a share, and each TA 2 shares. Then, all possible combinations will have at least 3 shares to recover the answer key.

Basically, the point of this problem is to assign different weight to different class of people. If we give one share to everyone, then 2 Readers can also recover the secret and the scheme is broken.

3 Secret Veto

In the usual secret-sharing scenario we consider (for instance) a secret vault at the United Nations, which we want to design with the property that any k representatives can pool their information and open it, but any smaller number has no hope of doing so. Assume that the solution in the notes has been implemented, so that the key is some number s, and each member has been assigned a number $f(i) \mod q$ for some degree $k-1$ polynomial f with coefficients in $\mathrm{GF}(q)$ and satisfying $f(0) = s$.

(a) A group of $k+\ell$ representatives get together to discuss opening the vault. What will happen if ℓ representatives are opposed to opening the vault and, instead of revealing their true numbers, secretly reveal some *different* numbers from $\mathrm{GF}(q)$? Will the group be able to open the vault? If so, how long will it take?

(b) Repeat part (a) in the event that only $\ell/2$ of the ℓ representatives in opposition reveal different numbers than they were assigned—assume that ℓ is even.

Solution:

(a) In this situation, the polynomial interpolating the $k+\ell$ points will be some polynomial $\tilde{f}$, differant then f, but with the property that $\tilde{f}(i) = f(i)$, for any representative i who gave the correct number. In fact, we claim that $\tilde{f}$ must have degree striclty larger than that of f. This is because Lagrange interpolation produces the *unique* polynomial of lowest degree passing through a given set of points: if f and $\tilde{f}$ had the same degree, they would have to be the same, since both pass through the k points $(i, f(i))$ of the representatives who answered truthfully.

In other words, when group sees that the polynomial has degree strictly larger than $k-1$, they will know that someone has given faulty information, but not who did so. By trying all possible subsets of k of the $k+\ell$ representatives, it would be possible to both recover the key and discover which members were engaging in the subterfuge. However, there are exponentially many such subsets in ℓ.

(b) If only $\ell/2$ representatives give incorrect information, the resulting polynomial will be of degree at most $k+\ell/2-1$. This time, however, the group can use the Berlekamp-Welch algorithm to efficiently figure out who was responsible and what the true polynomial is! Recall that in the Berlekam-Welch setting you receive a list $f(1), f(2), \ldots, f(k+\ell)$, of which up to $\ell/2$ entries may have been corrupted; the algorithm allows you to recover the locations of the errors and the true polynomial f. This setting is functionally the same: the group has access to $k+\ell$ evaluations of a polynomial, and they know that $k+\ell/2$ of them are correct. The only difference is that the polynomial is not evaluated at the points $1, 2, \ldots, k+\ell$, but rather at $k+\ell$ arbitrary points among the numbers $1, \ldots, n$.