POLYNOMIALS, SECRET SHARING, ERASURE ERRORS, GENERAL ERRORS, SELF REFERENCE 4

COMPUTER SCIENCE MENTORS 70

October 3 to October 7, 2016

1 Polynomials

1.1 Introduction

1. There is a unique polynomial of degree $n-1$ such that $P(i) = m_i$ for each packet $m_1, \ldots, m_n$
2. To account for errors we send $c_1 = P(1), \ldots, c_{n+j} = P(n+j)$
3. If polynomial $P(x)$ has degree $n-1$ then we can uniquely reconstruct it from any n distinct points.
4. If a polynomial $P(x)$ has degree $n-1$ then it can be uniquely described by its n coefficients

1.2 Questions

1. Define the sequence of polynomials by $P_0(x) = x+12$, $P_1(x) = x^2-5x+5$ and $P_n(x) = xP_{n-2}(x) - P_{n-1}(x)$. (For instance, $P_2(x) = 17x - 5$ and $P_3(x) = x^3 - 5x^2 - 12x + 5$.)

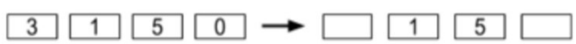
   (a) Show that $P_n(7) \equiv 0 \pmod{19}$ for every $n \in N$.

(b) Show that, for every prime q, if $P_{2013}(x) \not\equiv 0 \pmod{q}$, then $P_{2013}(x)$ has at most 2013 roots modulo q.

2 Erasure Errors

2.1 Introduction

We want to send n packets and we know that k packets could get lost.



How many more points does Alice need to send to account for k possible errors? __
What degree will the resulting polynomial be? __
How large should q be if Alice is sending n packets with k erasure errors, where each packet has b bits?

What would happen if Alice instead send $n+k-1$? Why will Bob be unable to recover the message?

2.2 Questions

1. Suppose $A = 1$, $B = 2$, $C = 3$, $D = 4$, and $E = 5$. Assume we want to send a message of length 3. Recover the lost part of the message, or explain why it can not be done.

   1. C_AA

   2. CE_ _

2. Suppose we want to send n packets, and we know $p = 20\%$ of the packets will be erased. How many extra packets should we send? What happens if p increases (say to 90%)?

3 Secret Sharing

3.1 Questions

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

   (a) Both TAs should be able to access the answers

   (b) All 3 Readers can also access the answers

   (c) One TA and one Reader should also be able to do the same

   Design a secret sharing scheme to make this work.

2. An officer stored an important letter in her safe. In case she is killed in battle, she decides to share the password with her troops. Everyone knows there are 3 spies among the troops, but no one knows who they are except for the three spies themselves.The 3 spies can coordinate with each other and they will either lie and make people not able to open the safe, or will open the safe themselves if they can. Therefore, the officer would like a scheme to share the password that satisfies the following conditions:

   1. When M of them get together, they are guaranteed to be able to open the safe even if they have spies among them.
   2. The 3 spies must not be able to open the safe all by themselves.

   Please help the officer to design a scheme to share her password. What is the scheme? What is the smallest M? Show your work and argue why your scheme works and any smaller M couldnt work.