Sundry

[Sarah Golden sgolden26@berkeley.edu]

1) Error Correcting Codes

a) fraction a of lost packets (where $0 < a < 1$)

expect $n \times a$ to be lost

$n + k$ packets

message : n

expect $N \cdot a$ to be lost

packets sent : $N = n + x$

packets that can be lost : $x = N \cdot a$

$$x = (n + x) \cdot a$$
$$x = an + ax$$
$$x - ax = an$$
$$x(1 - a) = an$$
$$x = \frac{an}{1-a} \rightarrow \boxed{n + \frac{na}{1-a}}$$

b) $n + 2(k)$

$$x = 2 \times N \times a$$
$$x = 2(x + n) \times a$$
$$x = (2x + 2n)a$$
$$x = 2xa + 2na$$
$$x - 2xa = 2na$$
$$x(1 - 2a) = 2na$$
$$x = \frac{2na}{1-2a} \rightarrow \boxed{n + 2\left(\frac{2na}{1-2a}\right)}$$

2) Alice and Bob

a) $Q(x) = P(x)E(x)$

$$\left.\begin{aligned} P(x) &= m_1x^2 + m_2x + m_3 \\ E(x) &= (x - e_1) \\ Q(x) &= a_3x^3 + a_2x^2 + a_1x + a_0 \end{aligned}\right\} \pmod 7$$

$P(0)$:

$a_0 = 1(0 + b_0)$

$a_0 = b_0 \pmod 7$

$a_0 - b_0 = 0 \pmod 7 \rightarrow a_0 + 6b_0 = 0$

$P(1)$:

$a_3 + a_2 + a_1 + a_0 = 3(1 + b_0)$

$a_3 + a_2 + a_1 + a_0 = 3 + 3b_0$

$a_3 + a_2 + a_1 + a_0 - 3b_0 = 3 \pmod 7 \rightarrow a_3 + a_2 + a_1 + a_0 + 4b_0 = 3$

$P(2)$:

$8a_3 + 4a_2 + 2a_1 + a_0 = 0 \pmod 7 \rightarrow a_3 + 4a_2 + 2a_1 + a_0 = 0$

$P(3)$:

$27a_3 + 9a_2 + 3a_1 + a_0 = 1(3 + b_0)$

$27a_3 + 9a_2 + 3a_1 + a_0 = 3 + 3b_0$

$27a_3 + 9a_2 + 3a_1 + a_0 - 3b_0 = 3 \pmod 7 \rightarrow 6a_3 + 2a_2 + 3a_1 + a_0 + 4b_0 = 3$

$P(4)$:

$64a_3 + 16a_2 + 4a_1 + a_0 = 0 \pmod 7 \longrightarrow a_3 + 2a_2 + 4a_1 + a_0 = 0$

$a_3 = 1$

$a_2 = 3$

$a_1 = 3$ $\quad \Rightarrow E(x) = x + 2 = x - 5$

$\boxed{e_1 = 5}$

$a_0 = 2$

$b_0 = 2$

$$P(x) = \frac{Q(x)}{E(x)} = \frac{x^3 + 3x^2 + 3x + 2}{x - 5}$$

$P(x) = x^2 + 8x + 43 \pmod 7$

$P(x) = x^2 + x + 1 \pmod 7$

$P(5) = 5^2 + 5 + 1$

$\boxed{= 31}$

original x-value of packet

b) $p(x) = a_1 x + a_0 \pmod{13}$

Alice sends:

$p(0) = 5$
$p(1) = 7$
$p(2) = 9$
$p(3) = -2 = 11$
$p(4) = 0$

Bob gets:

$p(0) = 5$
$p(1) = 7$
$p(2) = x$
$p(3) = 5$
$p(4) = 0$

Eve changes 2 packets

$a_1 = \frac{7-5}{1-0} = 2$

$p(x) = 2x + 5 \pmod{13}$

$p(2) = 5 \rightarrow$ then $p(0) = 5$, $p(2) = 5$ and $p(3) = 5$
so we get $y = 5$

$p(2) = 6 \rightarrow$ then $p(1) = 7$, $p(2) = 6$ and $p(3) = 5$
we get $y = -x + 8$

$p(2) = 10 \rightarrow p(3) = 5$, $p(2) = 10$, $p(4) = 0$

for $x = 5, 6$ and 10, we have values of x Bob won't be able to determine Alice's message. For each of these x values, a new degree 1 polynomial is formed that leaves 2 points that don't lie on the line. Therefore, Bob might think those 2 points are the changed ones.

c) 6 packets, length $n = 6$

$n + 2k = 6$; $k = 1$
$n + 2(1) = 6$
$n = 4$

$\boxed{\text{length: } 10}$

Since there are 6 packets sent through channel X, and we know channel y will corrupt one packet, we use $n + 2k = 6$ (at most 6 packets) as the formula for general errors. plugging in $k = 1$ we solve for n, which gives us $n = 4$, and $4 + 6 =$ message of length 10.

3) Secret Sharing w/ Spies

- 3 spies
- N = 10

$\to n + 2k$
$\to n = 4 \quad k = 3$
$d = 3$

Since there are 3 spies, we account for 3 general errors, and we want to make sure it's recoverable. We construct a polynomial of degree $d = 3$, where k is the # of errors and n is the amount of points needed to recover.

We need $n + 2k$ for 10 pieces of info to distribute.

$$\left.\begin{array}{ll}
n_1: & P(1)\ P(2) \\
n_2: & P(2)\ P(3) \\
n_3 & P(3)\ P(4) \\
n_4: & P(4)\ P(5) \\
n_5: & P(5)\ P(6) \\
n_6: & P(6)\ P(7) \\
n_7: & P(7)\ P(8) \\
n_8: & P(8)\ P(9)
\end{array}\right\} \text{always recoverable,}$$

n_9: $P(9)$ $P(10)$

n_{10}: $P(10)$ $P(1)$

4) Counting, Counting and More Counting

a) n 1's and k 0's

$\hookrightarrow \binom{n+k}{n} = \binom{n+k}{k}$

b) 19 digit ternary bitstrings $\{0,1,2\}$; no 2 adj. digits are equal

$\hookrightarrow 3 \cdot 2^{18}$

c) 13 cards from 52

i) $\binom{52}{13}$

ii) $\binom{48}{13}$

iii) $\binom{48}{9}$

iv.) $\binom{13}{4} \cdot \binom{39}{9}$

↑ ways to choose 4 spades

↑ ways to choose rest of bridge hand

d) $\frac{104!}{2^{52}}$

e) $\binom{99}{49} + \binom{99}{48} + \ldots \binom{99}{0}$ or 2^{98}

f) ALABAMA

i) $\frac{7!}{4!}$

ii) $\frac{7!}{2!2!}$

h) $\binom{32}{8} \cdot \frac{1}{8!}$

i) $\binom{32}{8}$

g) i) $5!$ ii) $\binom{6}{2} \cdot 4!$

j) $n=6$, $k=2$

$\lfloor 0 \rfloor \lfloor 0 \rfloor \lfloor 0 \rfloor \lfloor 0 \rfloor \lfloor 0 \rfloor \lfloor 0 \rfloor$

$\hookrightarrow$ 2 possibilities left for 6 bins

$\binom{n+k-1}{k} \rightarrow \boxed{\binom{7}{2}}$

k) $n=20$, $k=10$

1) $\frac{19 \cdot 17 \cdot 15 \cdot \ldots 3 \cdot 1}{2^{10}}$

2) $\frac{20!}{2^{10}\, 10!}$

l) $\underbrace{x_0}_{1} + \underbrace{x_1 + \ldots + x_k}_{k} = n$

$1 + k$

$\binom{n+k}{k}$

m) $x_0 + x_1 = n$

$\hookrightarrow n-1$

n) $x_0 + x_1 + \ldots x_k = n$

$\binom{n-1}{k}$

5) Fermat's Wristband

a) n^p ; n color choices for the first bead, n colors for the second, etc. since we choose p beads, there are n^p possible choices.

b) $n^p - n$; there are n^p ways to arrange p beads w/ up to n colors. we want to consider the complement of using at least 2 colors, which is when you only use one color. since we have n colors, we have 1 possible invalid coloring sequence for each of the n colors, so we subtract n from n^p.

c) $\frac{n^p - n}{p}$; since we still have the constraint that p beads not have all the same color, we still use the expression $n^p - n$, and we divide by p (overcounting factor), since we can rotate each arrangement p ways w/equivalency.

d) Since $\frac{n^p - n}{p}$ is the number of ways to rotate p beads w/n colors, it must be an integer, so

$p \mid n^p - n$.

$$n^p - n \equiv 0 \pmod{p}$$
$$n^p \equiv n \pmod{p}$$
$$n^{p-1} \cdot n \equiv n \pmod{p}$$
$$n^{p-1} \equiv 1 \pmod{p}$$

same as $a^{p-1} \equiv 1 \pmod{p}$

$\therefore$ proven

6) Counting on Graphs + Symmetry

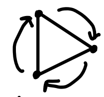
a) $\frac{6!}{24}$; there are 6! ways to color the faces of a cube, 6 colors for the first face, 5 colors for the second, etc. For each coloring, there are 4 ways to rotate the cube keeping the top & bottom face fixed. 4 * 6 faces = 24, divide 6! by the overcounting factor 24 to get the total # of ways.

b) $\frac{n!}{n}$; there are n! ways to color a bracelet w/ n colors, n for the first bead, n-1 for the second, n-2 for the third, etc. since we can rotate the bracelet n times to achieve equivalent pattern/colorings, we divide by n for the overcounting factor.

c) $\binom{n}{2}$ possible edges $\rightarrow$ $2^{\binom{n}{2}}$; there are n choose 2 possible edges for the graph, because we choose 2 vertices from n to form an edge. Then, we choose to include or not include that edge, so we get $2^{\binom{n}{2}}$.

d) # arrangements of vertices in cycle

$$\sum_{x=3}^{n} \binom{n}{x} \frac{(x-1)!}{2}$$

; the shortest cycle has 3 vertices, i.e.  therefore, we start from x = 3 and end at n. we choose x vertices from each of the n vertices for a cycle, where $3 \leq x \leq n$ then, there are (x-1)! ways to arrange x items in a cycle; we fix one vertex and permute the rest. we divide by overcounting factor of 2 because there are 2 ways to rotate a cycle, clockwise and counter-clockwise.

$64 = 8^2 = 2^3 = 2^6$

6 is 7-1

symmetry:

1 1 0 0 0 1 0

0 0 1 1 1 0 1

set A : 7 bit string w/ more 1's than 0

set B: 7 bit strings w/ more 0's than 1

so $|A| = |B|$

Total # 7-bit strings : 2^7

$|A| + |B| = 2^7$

$2 * |A| = 2^6$

↳ 2^3

swap

$\frac{0}{1}$ $\frac{1}{2}$ $\frac{0}{3}$

how many 3 digit bit strings are there?

2^3

how do we create overcounting duplicates?

1 _ 1 _ 1 1 _

$\binom{7}{3} + \binom{7}{2} + \binom{7}{1} + \binom{7}{0}$

multiply

↳ a · b ways to do

a + b

ABCDEF

'CE'1 + 'A'2 + 'B'3 + 'D'4 + 'F'5

g) $\binom{6}{5}$

1, 2, 3, 4, 5

bijection

$\frac{6!}{2}$

C _ _ _ _ E

$\frac{6!}{(6-4)!}$ →

C E _ _ _ _

$\binom{6}{2} \cdot 4!$

dependent both at same time

↑ choose C+E

n) 0 1 2 . . . k

n balls,

amt bins

k - amt balls

$\binom{n-k-1}{k}$

multiset -choose same set more than once

n = k+1

k = n-(k+1)

n-k-1

A : string w/ C to left of E

B: string w/ C to right of E

$(k+1)-(n-k-1)-1$

$n-k-1$

$\hookrightarrow$ $k+1-n+k+\cancel{k-1}$

$2k-n+1$