

1 Polynomial

Suppose we have a polynomial $P(x)$ of degree $n - 1$ over GF_q and we are given points $\{(a_1, P(a_1)), \dots, (a_n, P(a_n))\}$, Consider the following alternative algorithm for polynomial interpolation.

```

define interpolate([(a1, P(a1)), ..., (an, P(an))]) :
  if input is empty :
    return 1

  for i from 2 to n:
    bi ← -P(a1)/(ai - a1) mod q

  P'(x) ← interpolate([(a2, b2), ..., (an, bn)])

  return P'(x)(x - a1) + P(a1) mod q

```

Prove that the algorithm outputs the correct polynomial. (Hint: suppose $P(x)$ is the actual polynomial, then a_1 is a root of the polynomial $P(x) - P(a_1)$)

How many bit-operations does this algorithm perform to interpolate a polynomial of degree n ? Express your answers in big-O notation.

2 Erasure Channel Encoding

Consider the situation where we would like to send 2 packets $m_0 = 3, m_1 = 2$ over an unreliable erasure channel where up to 5 packets can be erased. What is the actual transmission you would send using the normal error-correction encoding method taught in lecture? (Assume both sides know we are working in mod 13).

3 Polynomial and Probability

A polynomial Q of degree at most 9 is picked uniformly at random among all polynomials of degree (at most) 9, modulo 13.

1. What is the sample space, and what is the probability of each sample point?
2. Let A be the event that $Q(1) = 5$ and $Q(2) = 7$. What is the probability of A ?
3. Let B be the event that $Q(3) = 5$ and $Q(4) = 7$. What is $P[B|A]$, the conditional probability of B given A ?
4. Are A and B independent events? Remember to justify your answer.

4 Counting Cards

A balanced bridge hand has four cards from some suit and three from each of the rest (a bridge hand consists of 13 cards). How many balanced bridge hands are there? Remember to explain how you derived your answer.

5 Arthropod Fashion

A milipede has 1000 pairs of feet and hence wears 1000 pairs of socks and 1000 pairs of shoes. Milipede George is not particularly fashionable and owns 1000 pairs of identical socks and 1000 pairs of identical shoes.

When George puts on a pair of socks, he always puts both socks of the matching pair on at the same time, and when George puts on a pair of shoes, he puts both shoes of the matching pair on at the same time also. On any specific foot, George has to always put on a pair of socks before he puts on a pair of shoes. How many ways can George put on socks and shoes on all of his feet?

6 Conditional Probability

The Cal Bears are playing Stanford in a 2-out-of-3 series, i.e. they play games until one team wins a total of two games. The probability that the Bears win the first game is $1/2$. For subsequent games, the probability of winning depends on the outcome of the preceding game; the team is energized by victory and demoralized by defeat. If the Bears win a game, then they have a $2/3$ chance of winning the next game. On the other hand, if the Bears lose, they have only a $1/3$ chance of winning the next game.

1. What is the probability that the Bears win the 2-out-of-3 series given that they win the first game?
2. What is the probability that the Bears won the first game, given that they won the series?

7 Political Randomness

Each state has 2 senators in the United States senate.

1. Suppose we randomly choose 10 senators to form a committee. What is the probability that no Californian senators are part of the committee?
2. Suppose we randomly choose 50 senators to form a committee. What is the probability that no two are from the same state?
3. Suppose we randomly choose 10 senators to form a committee and we know that there are no Californian senators in our committee, what is the probability that no two senators in our committee are from the same state?