Homework5 For Machine Learning

Vergil/Zijun Li李子骏

1. **In the game of Nim, consider a single pile with 14 chips. What is the Nimber of this position? Is this a P-position or an N-position?**

   The Nimber of a single pile with 14 chips is 14. as Nimber of a position with a single pile of k chips, N(Pk) = k
   And it is a N-position(normal play)

2. **Consider the sum of two games. Game 1 and game 2 are in positions with Nimber 4 and 6 respectively. What is the Nimber of the combined game? Is this a P-position or an N-position?**

   Nim = Nim(Game1) $\oplus$ Nim(Game2) = 0100 $\oplus$ 0110 = 0010
   It is a N-position

3. **Consider the MPC protocol for computing averages which we saw in the class. Suppose that the first and third student are colluding. Show that they can compute the age of the second student**

   What they have:
   A: A, X+R
   B: B, X+A+R
   C: C, X+A+B+R
   If A and B are colluding, B = (X+A+B+R) - (X+A+R). They could compute the age of the second student

4. **Consider the ZK proof for graph 3-coloring. What if the prover doesn't permute the colors in every iteration? That is, the prover permutes the colors once in the beginning and then sticks to that permutation for all iterations. Will the protocol still be zero-knowledge?**

   No, it is not zero-knowledge, the verifier may have chance to gather enough information to infer the prover's specific coloring scheme