Homework 30

Austin Frownfelter Matthew Bialecki

April 4, 2018

1 Problem 55

We were not able to come up with a proper solution for this problem. Here is our intuition:

Effectively, since the complex number is not necessary for the computational power, we should turn it into a real number to get the same result. Since the magnitude of the amplitude squared is the probability, we can turn a complex amplitude into a real 'amplitude' which gives the same probability.

Where we got stuck with this approach is determining whether the new real amplitude should be positive or negative, since the magnitude of a complex number is $\pm\sqrt{a^2 + b^2}$.

2 Problem 57

Arthur makes r coin flips, and sends q adaptive queries to the book. In other words, Arthur makes a query, then makes another query based on the result he received from the first query. He repeats this q times.

Now, assume Arthur is nonadaptive. He must send all queries at the beginning, which means he does not know what the result of each query is before coming up with the next. Thus, he must make all possible queries which can follow the previous. In every case, there are 2 possible queries based on the previous (based on the next coin flip). Thus, for q queries, there are 2^q possible queries based on the r coin flips. Therefore, Arthur must make all 2^q queries if he is nonadaptive.

3 Problem 58

PCP(poly(n),poly(n)) allows for n^k random bits and n^k queries.

For a given pair (A,k), a verifier can perform a PCP protocol to probabilistically determine whether perm(A) = k. Since perm(A) is the sum of n! terms, this is not deterministically provable in a polynomial number of steps (or at least it is not known whether it is possible as such.) However, with a PCP protocol,

a verifier can have completeness of 1 and soundness error $\leq \frac{1}{3}$ (or exponentially small). The protocol would be as follows:

The verifier uses random bits to decide what to ask the book. It will choose the first element of a random symmetric group in the matrix. The book responds with the submatrix which would make up the remainder of the symmetric group along with the value of the permanent for that group. The verifier will then continue recursively for a random path, and assume the given permanent from the other paths are correct, and accept if the book is right (the resulting permanent is k), and reject if it is wrong.