Homework 30

Joe Baker, Brett Schreiber, Brian Knotten

April 3, 2018

55

Let $f \in BQP$ and let M be a quantum turing machine that accepts f. Next construct a new quantum turing machine from M called M' which works the same as M except it takes in a quantum register m' of size $m+1$ where M took in a quantum register of size m. Additionally the final qubit of the new register must be 0 if and only if all amplitudes of the first m qubits correspond to the real-part of their amplitudes in the original M and 1 if and only if all amplitudes of the first m qubits correspond to the imaginary-part of their amplitudes in the original M. Then apply elementary quantum operations $F_1, ..., F_T$ on m'. Finally measure the register and let Y denote the obtained value.

57

Let L be a language that has a PCP-verifier using r coins and q adaptive queries and let V be the PCP-verifier with $\{x_1, x_2, ..., x_q\}$ as the q adaptive queries. We can construct a PCP-verifier V' with 2^q non-adaptive queries by having V' read all possible 2^q bits that can be read by V.

58

Let π^n be the proof string where the ith bit contains a polynomial $g(x)$ which is supposedly the permanent of the matrix encoded as i with the 1st row and the xth column removed. The verifier composes i as A and queries for the ith bit of π^n. Then the verifier calculates $\Sigma_{c=1}^{n-1} a_c g(c)$ where a_c is the cth value of the first row of A and checks to make sure that the sum equals k. If it does not, reject. Then, do this for the second row of A on the advice tape π^{n-1} and again compare the result to k. Continue this for all rows in A.

To deal with the multiple proof $\pi^1 ... \pi^n$, just concatenate all the proof strings into one, and have the verifier consider this offset in the query. The verifier does not use the result of each query in order to specify the next query, since the queries are determined only by the input.