Homework 26

Austin Frownfelter Matthew Bialecki

March 26, 2018

1 Problem 46

1.1 Part a

Merlin knows a Hamiltonian cycle C in the public graph G, and must prove to Arthur that he knows it/it exists. Merlin sends a representation of the graph G to Arthur. Arthur responds with a random coin flip. On tails, Merlin shares the permutation with Arthur, who then checks whether it is consistent with the original graph G. On heads, Merlin computes the permutation on the private Hamiltonian cycle C, and shares the representation of the permutation on just the cycle C. Arthur then checks whether this is a Hamiltonian cycle, and whether it is consistent with the permuted graph G.

1.2 Part b

A computational zero knowledge proof is a relaxation of a perfect zero knowledge proof, where a verifier cannot learn any private information from an interaction in reasonable (polynomial) time. That is, a verifier is unable to learn any information under its polynomial time bounds, however with more time the verifier may be able to learn something (by random sampling or other.) In addition, an interactive proof is zero knowledge (computational or perfect) if it has completeness $\geq \frac{2}{3}$ and soundness error $< \frac{1}{3}$

1.3 Part c

This protocol is computationally zero knowledge because the verifier is unable to calculate the Hamiltonian cycle C. In the tails case, it only learns the given permutation of G of this round. In the heads case, it learns a Hamiltonian cycle C', but does not know what the edges in C' correspond to in graph G. This is because of the computational bound of the verifier.

2 Problem 47

Universality:

Not: Set $C = I_1 = 1$, then O_2 will equal $\neg I_2$

And: Set $I_2 = 0$, then O_2 will equal $C \wedge I_1$

Or: Use the Not/And gates and DeMorgan's law: $a \vee b = \neg(\neg a \wedge \neg b)$

Reversibility:

Toffoli gates yield the original inputs except in the case where the first two bits are 1. In this case, the Toffoli gate on the result yields the original input (an identity).

3 Problem 48

3.1 Part a

Compute the H_1 operation, then the not, then the H_1 operation on the original state to yield: $a|H> + (-b)|V>$

3.2 Part b

(This is assuming Horizontal input)

Probability of horizontal output = a^2, since the superposition collapses to the horizontal input.

3.3 Part c

(This is assuming Vertical input)

Probability of vertical output = b^2, since the superposition collapses to the vertical input.