Advanced Proof Systems - Problem Set 4

Yosef Goren

January 13, 2023

1 $IP \subseteq PSPACE$

1.1

Given a graph of *vertecies*, consider the following series of matrices:

$$M_k[i,j] := \begin{cases} 1 & \text{exists a path from } i \text{ to } j \text{ with length } \leq k \\ 0 & \text{otherwise} \end{cases}$$

Corollary: M_1 is the adjacency matrix of the graph.
Between any two matrices of size $n \times n$, define the following operation:

$$(A \otimes B)[i,j] := \bigvee_{x \in [n]} (A[i,x] \wedge B[x,j])$$

.

Lemma:

$$\forall k \in [n] : M_k \otimes M_k = M_{2k}$$

. Proof: Assume (by induction) for M_k [1]. Now, we need to prove for M_{2k}. Consider a path $l_{i,j}$ from i to j with length $\leq 2k$.
It can be decomposed into two paths of length $\leq k$; The first path from i to x ($l_{i,x}$) and the second path from x to j ($l_{x,j}$).
Hence $M_{2k}[i,j] \Rightarrow \exists x \in [n] : M_k[i,x] \wedge M_k[x,j] \Rightarrow (M_k \otimes M_k)[i,j]$.
Conversely, if $(M_k \otimes M_k)[i,j] = 1$, then there exists $x \in [n]$ such that $M_k[i,x] = 1$ and $M_k[x,j] = 1$, which means that there exists a path from i to x of length $\leq k$ and a path from x to j of length $\leq k$. So $(M_k \otimes M_k)[i,j] \Rightarrow M_{2k}[i,j]$.
Finally we have that $M_k \otimes M_k = M_{2k}$.

Algorithm: The algorithm which the circuit will follow is as follows:

1. Initialize M_1 to be the adjacency matrix of the graph.

[1] formally this would not prove for k values that are not a power of 2, but we actually do not make use of those sizes anyways since $\forall k \geq n, M_k = M_n$ and we only care about M_n.

2. For each $k \in [n]$:
   (a) Compute M_{2k} by applying the operation $\otimes$ on M_k and M_k.
   (b) If $k = 2^r$ for some $r \in [n]$, then set M_k to be M_{2^r}.

2 Batch Verification for P