Advanced Proof Systems - Problem Set 4

Yosef Goren

January 17, 2023

1 $IP \subseteq PSPACE$

1.1

Given a graph with n vertices, 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 $M_k \otimes M_k = M_{2k}$.

[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.

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

```
$k \leftarrow 1$
$M \leftarrow E$
while $k < n$ do
    $M \leftarrow M \otimes M$
    $k \leftarrow 2k$
end while
return $M[s,t]$.
```

Due to the lemma, at the end of each iteration - $M = M_k$, this means that when the loop ends, $M = M_n$. Thus $M[s,t]$ is the correct output.

Circuit: Here we assume the circuit recives E, s, t as input, we assume E is represented in the adjacency matrix form.
The $\otimes$ operation can be implemented with depth $O(log(n))$ using a binary tree of the big $\vee$ gate. Additionally $log(n)$ steps are required for $k := n$ - each step is a set of layers added to the circuit.
With $log(n)$ complexity we can implement a MUX gate to select s, t from M after the layer.
Hence the total depth of the circuit is $O(log(n)^2)$. The maximum width of the circuit is $O(n^2)$.

1.2

Let $L \in PSPACE$.
Hence exists a polynomial space nondeterministic turing machine M_L that decides it.
Consider the set of configurations possible for M_L. Since it's set of states is constant and the set of values for it's tape is exponentionally bounded by a polynome - the set of possible configurations for it is bounded exponentionally by a polynome.

Each such configuration can be represented as a vertex in the graph of all possible configurations. Moreover, each possible transition from one configuration to another can be represented as an edge in the graph. Denote this configuration graph as G.

Define the reduction f as $f(x) = (G, s, t)$ where s is the vertex corresponding to the initial configuration of M_L on the input x, and t is vertex corresponding to the accepting configuration [2].

[2] WLOG assume there is one accepting configuration, otherwise we can either construct a new turing machine that clears it's tape and then accepts, or add to the graph a new node (t) that is connected to all accepting configuration vertecies.

2 Batch Verification for P