TDS - Solution

I- 1. Let $x \in \{0,1\}^{2n}$ with the promise that either x is balanced or x is constant.

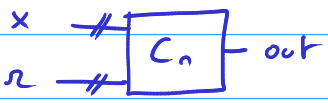
- Best exact algorithm in $O(n)$
- Algorithm correct w.p. $\geq 1-(1/2)^m$ in time $O(m)$
  $\Rightarrow \geq 2/3$ in time $O(1)$

2. Every polynomial algorithm can be simulated by a polynomial circuit of gates $\{\wedge, \vee, \neg\}$, (Cook's Theorem)
Take $F \in P$ and M a T.M. realising F.

On input n :

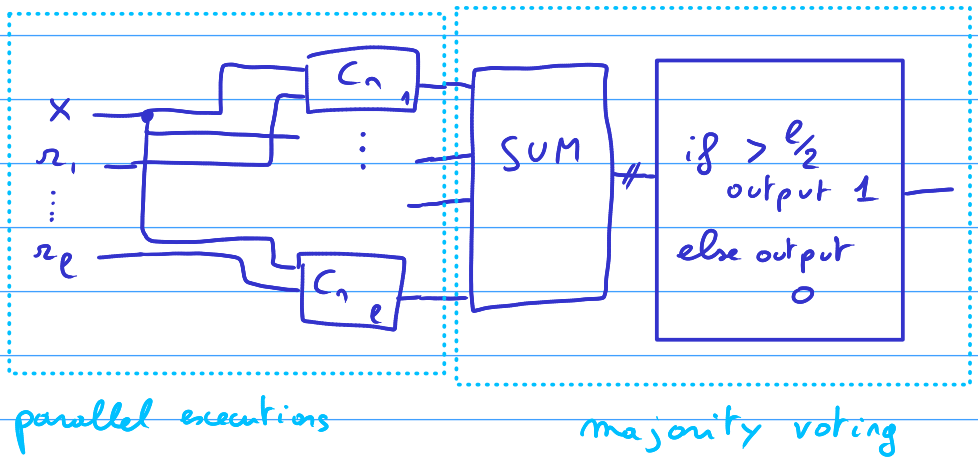
1. Simulate M on input of size n, let C_n be the circuit representing the boolean formulae.
2. Return C_n (without random coins)

3. Clearly, $BPP' \subseteq BPP$
Let $F \in BPP$, let $n \in \mathbb{N}$, let C_n realising F w.p. $\geq 2/3$



Circuit:

$C_{n,\ell}$



This circuit is of polynomial size

Now, let $x \in \{0,1\}^*$.

Let X_i be the random variable:

$X_i = 1$ iif $C_{n,i}(x) = F(x)$

We have $\mathbb{P}(X_i = 1) \geq 2/3$, $\gamma = 2/3 \cdot \ell$

Let $Z = \sum_{i=1}^{\ell} X_i$ The probability for $C_{n\ell}$ to fail is

$$\mathbb{P}(Z < \ell/2) \leq \mathbb{P}(Z \leq \tfrac{3}{4}\cdot\gamma)$$
$$\leq \mathbb{P}(|Z-\gamma| > \tfrac{1}{4}\cdot\gamma)$$
$$\text{Chernoff} \leq 2\exp\left(-\tfrac{1}{16\cdot 3}\cdot\tfrac{2}{3}\cdot\ell\right) = 2\exp\left(-\tfrac{\ell}{72}\right)$$

Now we want to take ℓ such that

$$2\exp\left(-\tfrac{\ell}{72}\right) = \exp(-n^c)$$
$$\Leftrightarrow \ell = 72[n^c + \ln(2)] \rightarrow \text{polynomial, OK}$$

4: No, because it would necessitate an exponential number of gates

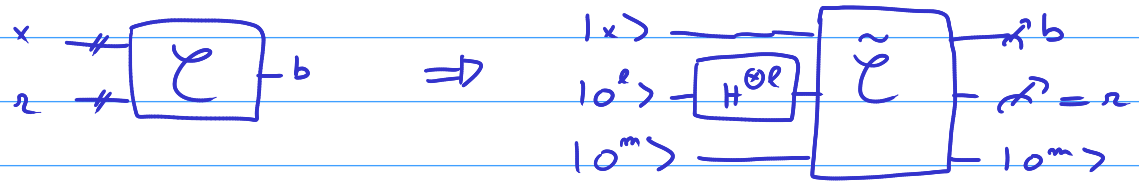
5: Let $\mathcal{L}$ be the language of word of the form $1^{\text{bin}(n)}$ where bin(n) is the representation of a Turing machine that halt on input $\emptyset$.

$\mathcal{L}$ is non-decidable, but the indecidability is "hidden" in the size of the input.

$$C_n = \begin{cases} \text{if } 1^n \in \mathcal{L}, & \text{the circuit } AND_n \\ \text{else} & \text{the circuit that output 0} \end{cases}$$

II 1. Every classical circuit can be simulated by quantum:

Take $\mathcal{C}$ a classical randomized circuit.



2. a) $|\psi\rangle = \sum_{i=0}^{2^n-1} a_i |i\rangle$ $\Rightarrow$ array of size 2^n

a_i floating point numbers (/ complex)

Each gate either multiply a_i by 1 (no precision needed)

Or divide by $\frac{1}{\sqrt{2}}$ $\Rightarrow$ We need to add $O(1)$ bit at most.

Overall: $O(\ell \cdot 2^n)$ bits needed.

b) Need to compute $G \cdot |\psi\rangle$ for any Gate:

done in time $O(2^n)$.

Complexity in time $O(\ell^2 \cdot 2^n)$

mem $O(\ell \cdot 2^n)$

3. a) Let M be a Turing machine using a polynomial space of size $\leq p(n)$, which finish on every input.

We are going to prove that M runs in EXP time.

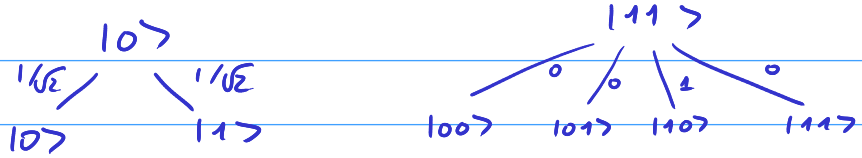
Let s be the number of internal states of M.

The number of possible states during the computation of M on an input $x \in \{0,1\}^n$ is:

$\leq \underbrace{2^{p(n)}}_{\text{state of the tape}} \cdot \underbrace{p(n)}_{\text{position of the head}} \cdot s$) internal state of M

As M does finish, it does not loop, and hence its running time on $x \in \{0,1\}^n$ is $\leq 2^{p(n)} \cdot p(n) \cdot s \leq EXP$ □

b) i)



(ii) $\langle j | g_p | i \rangle$

(iii) Easy with $O(\ell)$ bits of precision

(iv) By induction: $m = 1$ trivial

$$C = g_m \cdot C'$$

$$\langle y | C | x \rangle = \langle y | g_m \cdot C' | x \rangle = \langle y | g_m \cdot \sum_i |i\rangle\langle i| C' |x\rangle$$

$$= \sum_i \langle y | g_m | i \rangle \sum_{p : |x\rangle \xrightarrow{C'} |i\rangle} w(p)$$

$$= \sum_i \sum_{p' : |x\rangle \to |i\rangle \to |y\rangle} w(p')$$

$$= \sum_{p'} w(p')$$

(v) $\Rightarrow$ Computable in 2^{nm} comput° of the $w(p)$

$\Rightarrow O(m)$ bits of precision, $O(2^{nm} m)$ time

We can compute $\sum_{|y\rangle = |0 \cdots\rangle} |\text{weigh}(|x\rangle \to |y\rangle)|^2$ in poly-space