

Due on December 1
In class, at the beginning of the lecture

The work you submit must be your own. You may discuss problems with each other; however, you should prepare written solutions alone. In particular, you should not leave with any written notes from such discussions. The style and clarity of your answers will be an important factor in the grade.

For part (a), the correspondence is obvious: the r in the “randomized” definition corresponds to a branch in the “non-deterministic” definition.

For part (b), let $m = m(|x|) = \text{poly}(|x|)$ be the circuit size of a polytime algorithm $A(x, \cdot)$ (recall that in general, an algorithm that runs in time t can be simulated with a circuit of size $O(t^2)$).

Consider the algorithm $A'(x, z) := A(x, G_m(z))$, and note

$$\Pr_{z \in \{0,1\}^{O(\log(m))}} [A'(x, r) \text{ is correct}] \geq \frac{3}{4} - \frac{1}{8} = \frac{5}{8}$$

because suppose that there is an x_0 such that $A(x_0, G_m(z))$ and $A(x_0, z)$ differ on a fraction of inputs greater than $\frac{1}{8}$ (where $z \in \{0,1\}^{O(\log(m_0))}$ and $r \in \{0,1\}^{m_0}$, $m_0 = m(|x_0|)$). Then $A(x_0, \cdot)$ gives rise to a circuit $D_{A(x_0, \cdot)}$ of size $\leq m_0$ separating the random from the pseudorandom strings, contradicting the assumption.

Next, we derandomize A' as follows: on input x , we run it on all strings $r \in \{0,1\}^{O(\log(|x|))}$ and accept the majority of outcomes. Note that the running time is $2^{O(\log(|x|))}$ times m times the running time of G squared, all together a polynomial.

For part (c), as this is an “open ended” question, see the paper by Impagliazzo and Wigderson, **P = BPP unless E has subexponential circuits**, 29th Symposium on Theory of Computing, 1997.