Classe RP

Classe dei problemi decisionali *verificabili* in tempo polinomiale randomizzato.

- Π: problema decisionale
- x: istanza di input di Π
- y è un *certificato probabilistico* di x se:
  - y è di lunghezza al più polinomiale in $|x|$, e
  - y è estratto perfettamente a caso da un insieme associato a x.
- $A(x, y)$ è un algoritmo di verifica polinomiale se attesta in tempo polinomiale che x non possiede con certezza la proprietà, oppure che la possiede con probabilità $> 1/2$ (e.g. Miller-Rabin 3/4).

Congettura: $P \subset RP \subset NP$.