Question 1 [10 points]: In class we learned about Boolean circuits, in which the circuit wires carry Boolean values. In an arithmetic circuit, the wires carry values from some finite field, and the basis (i.e. the gate values) contains \{+,-,\times\}, where the operations are over that field.

- Show that if there is a family of Boolean circuits over basis \(B_0 = \{\land, \lor, \neg\}\) and size \(T(n)\), then there is a family of arithmetic circuits with wire values in \(\mathbb{GF}(2)\) and size \(c \cdot T(n)\), where \(c\) is some constant.

- Show that if there is a family of arithmetic circuits with wire values in \(\mathbb{GF}(2)\) and size \(T(n)\), then there is a family of Boolean circuits over basis \(B_0\) and size \(d \cdot T(n)\), for some constant \(d\).

- What’s the best bound you can give on \(c\) and \(d\)?

(Note, you can assume that circuits have some input wires that carry fixed values.)

Question 2 [10 points]: Prove that the following two definitions of \(\mathcal{RP}\) are equivalent:

\(L \in \mathcal{RP}\) if there exists a ppt machine \(M\) such that:

\[\begin{align*}
  x \in L &\implies \Pr[M(x) = 1] \geq 1/8 \\
  x \notin L &\implies \Pr[M(x) = 0] = 1.
\end{align*}\]

\(L \in \mathcal{RP}\) if there exists a ppt machine \(M\) such that:

\[\begin{align*}
  x \in L &\implies \Pr[M(x) = 1] \geq 1 - 2^{-q(|x|)} \\
  x \notin L &\implies \Pr[M(x) = 0] = 1.
\end{align*}\]

where \(q(\cdot)\) is some fixed polynomial.

Question 3 [10 points]: Prove that \(\mathcal{ZPP} = \mathcal{RP} \cap \text{co}\mathcal{RP}\).

(This should be done in 3 steps: 1) prove that \(\mathcal{ZPP} \subseteq \mathcal{RP}\), 2) prove that \(\mathcal{ZPP} \subseteq \text{co}\mathcal{RP}\), and 3) prove that \(\mathcal{RP} \cap \text{co}\mathcal{RP} \subseteq \mathcal{ZPP}\).)

Question 4 [5 points]: Suppose you roll a 6-sided die 96 times. Use the Chernoff bound to give an upper bound on the probability that more than 40 rolls result in a value less than 3.