Ex1: DET and low-depth arithmetic and boolean circuits

1. Prove the Schwartz-Zippel lemma.

   If $p : \mathbb{F}^m \to \mathbb{F}$ is a non-zero polynomial of total degree d over a field $\mathbb{F}$ and $\Lambda \subseteq \mathbb{F}$, then $\Pr_{a_1,\ldots,a_m \in \Lambda}[p(a_1,\ldots,a_m) = 0] \leq \frac{d}{|\Lambda|}$.

2. Shortly outline the proof of each of the following:

   (a) Addition of two integers represented in binary is in AC^0 ?

   (b) Addition of n integers (n-bit each) is in NC^1 ?

   (c) Multiplication of two integers in NC^1 ?

   (d) Multiplication of two boolean matrices is in AC^0 ?

3. Prove that $\mathsf{NC}^k \subseteq \mathsf{SPACE}(O(\lg^k n))$. Note the cost of pointers.

4. Prove that $\mathsf{NL} \subseteq \mathsf{AC}^1$. If you use a reduction, carefully note the resources it takes.

5. (Ben-Or) Denote $e_d(x_1,\ldots,x_n) = \sum_{S\subseteq[n],|S|=d} \Pi_{j\in S} x_j$, $1 \leq d \leq n$. We are going to construct a depth three, polynomial size arithmetic formula for e_d over $\mathbb{C}$ (with addition and multiplication gates of unbounded fan-in). For that:

   - Define $p(t) = p_{x_1,\ldots,x_n}(t) = \Pi_{i=1}^{n}(t + x_i)$. p is a degree n polynomial $p(t) = \sum_{i=0}^{n} a_i t^i$. what are the a_i as functions of $x_1,\ldots,x_n$?
   - Build the required circuit.

     Hint: first evaluate p on n points that you choose, then deduce the coefficients of p from the evaluations.
   - Is the family of circuits that you build uniform?

6. Show that matrix inversion of *lower triangular* matrix is in SAC^1.

   SAC^1: uniform polynomial-size boolean circuits with $O(\log n)$ depth over: unbounded fan-in $\vee$, bounded fan-in $\wedge$ and $\neg$ at input level only.

7. Show that computing the characteristic polynomial of an arbitrary matrix is in SAC^1.

8. Show that checking the rank of an arbitrary matrix and inverting an invertible matrix are both in SAC^1.