Homework 7
Due: 10:00am, Tuesday October 31

---

1. **(Subset sum.)** Consider the following task: The input is a function $f : 2^{[n]} \to \mathbb{N}$, given explicitly as a table of length $N = 2^n$. (Here $2^{[n]}$ denotes the set of all subsets of $[n] = \{1, 2, \dots, n\}$.) You may assume that each integer $f(S)$ is expressible with $O(n)$ bits. The goal is to output (also in table format) the function $g : 2^{[n]} \to \mathbb{N}$ defined by
$$g(T) = \sum_{S \subseteq T} f(S).$$
Give an algorithm for solving this problem in $N \cdot \mathrm{polylog}(N)$ time (i.e., in $2^n \cdot \mathrm{poly}(n)$ time). You may work in the random-access Turing Machine model (which means you can basically give a "normal" algorithmic description without really worrying about how the data is laid out on TM tapes). Hint: induction/recursion on n.

2. **(Computing a univariate polynomial.)** Let f be any univariate polynomial in X of degree n with complex coefficients. Show that f can be computed by an algebraic circuit that uses at most $2\sqrt{n}$ multiplications, no divisions, and with additions and multiplications by complex scalars being free of charge.

   (Remarks: It's possible to improve this to $\sqrt{2n} + \log_2 n + O(1)$; the proof is tricky, but elementary. On the other side, it is known that "almost all" degree-n polynomials need at least $\sqrt{n} - 1$ multiplications to compute, and Strassen showed that the following specific polynomial requires at least $(1 - o(1))\sqrt{n}$ multiplications: $f(X) = 2^{2^n} X + 2^{2^{2n}} X^2 + 2^{2^{3n}} X^3 + \cdots + 2^{2^{n^2}} X^n$.)

3. **(Why determinants are everywhere.)** In this problem you may take for granted the following properties of the determinant: multiplicativity ($\det(AB) = \det(A)\det(B)$); if A' is formed from A by multiplying some row by scalar c, then $\det(A') = c\det(A)$; if A' is formed from A by swapping two rows, then $\det(A') = -\det(A)$; and, cofactor expansion.

   For this problem, an algebraic formula F over indeterminates $X_1, \dots, X_n$ and coefficient field K means an algebraic circuit which is a binary tree, with the internal nodes being labeled $\times$ or $+$, and the leaves labeled either with an indeterminate or a scalar from K. The *size* of F is the number of leaves. The goal of this problem is to show the following:

   Claim: Any F of size L is expressible by the determinant of a $(3L-1) \times (3L-1)$ matrix A whose entries are either scalars or scalar-times-indeterminates.[1] Furthermore, the matrix A has the following special form:
$$A = \begin{bmatrix} * & * & * & \cdots & * & * \\ 1 & * & * & \cdots & * & * \\ 0 & 1 & * & \cdots & * & * \\ 0 & 0 & 1 & \ddots & * & * \\ \vdots & \vdots & \ddots & \ddots & * & * \\ 0 & 0 & 0 & \cdots & 1 & * \end{bmatrix}.$$

[1] Remark: it is known that this can be improved to $(L+3) \times (L+3)$, one can have just scalars *or* indeterminates, and that one can also replace "determinant" by "permanent".

(That is: arbitrary on and above the main diagonal; all 1's on the diagonal below the main one; and, all 0's below that.)

(a) Prove that for block matrices

$$Z = \left[\begin{array}{c|c} P & 0 \\ \hline Q & R \end{array}\right]$$

it holds that $\det(Z) = \det(P)\det(R)$. Hint: factorize Z using the matrices

$$\left[\begin{array}{c|c} P & 0 \\ \hline Q & I \end{array}\right], \quad \left[\begin{array}{c|c} I & 0 \\ \hline 0 & R \end{array}\right],$$

where I is the identity matrix.

(b) Show that the Claim is true for formulas of size 1 (i.e., single-leaf formulas).

(c) Show that if $F = \det(A)$ and $G = \det(B)$ where A, B are $m \times m$ and $n \times n$ matrices of the special form (respectively), then $F \times G$ is expressible as $\det(C)$ for an $(m+n) \times (m+n)$ matrix of the special form.

(d) Show that if $F = \det(A)$ and $G = \det(B)$ where A, B are $m \times m$ and $n \times n$ matrices of the special form (respectively), then $F + G$ is expressible as $\det(C)$ for an $(m+n+1) \times (m+n+1)$ matrix of the special form. Hint: consider the block matrix

$$C = \left[\begin{array}{c|c|c} 0 & 0 \;\; 0 \;\; \cdots \;\; 0 \;\; 1 & 0 \;\; 0 \;\; \cdots \;\; 0 \;\; 1 \\ \hline 1 & & \\ 0 & & \\ \vdots & A & 0 \\ 0 & & \\ 0 & & \\ \hline 1 & & \\ 0 & & \\ \vdots & 0 & B \\ 0 & & \\ 0 & & \end{array}\right].$$

Show that it works, and that it can be fixed up to the special form with a "swap" or two...

(e) Complete the proof of the Claim.