The story so far: Interactive proof systems (IP) were introduced as a formal model to investigate issues in cryptography and as a natural extension to NP, the class of problems solvable in nondeterministic polynomial time. The vision was that in an interactive proof system between Prover and Verifier would interact in such way that the Prover could convince the Verifier with high probability of a true fact, but could only convince a Verifier with very low probability of a false fact. In this model, the Prover is all-powerful and the Verifier is limited to run in polynomial time. The Verifier has the additional ability to flip an unbiased coin.[1]

---

1. Boolean functions into multilinear polynomials. A *multilinear polynomial* is a multivariate polynomial where each variable has degree 1. For example, $f(x,y,z) = 3xyz - 5xz + 3$ is a multilinear polynomial on 3 variables, but $g(x,y) = x^2y + 3$ is not multilinear.

   - Let ϕ be an n-variable 3-CNF formula; denote the Boolean variable vector as $x = (x_1, \ldots, x_n)$. Let $C = (x_i \vee x_j \vee x_k)$ be a single clause of ϕ.

     Come up with a multilinear polynomial $\widetilde{f_C}$ such that

     $$\widetilde{f_C}(x) = \begin{cases} 1 & \text{if } x \text{ satisfies } C \\ 0 & \text{if } x \text{ does not satisfies } C \end{cases}$$

     for all $x \in \{0,1\}^n$. The value of $\widetilde{f_C}(x)$ can be arbitrary if x is not Boolean.

   You just created a **multilinear extension** of C. Now that you possess the necessary technical tools, ponder about the following fact:

   Lemma 1 (Multilinear Extension Lemma). *Any Boolean function $f : \{0,1\}^* \to \{0,1\}$ has a unique multilinear extension $\widetilde{f}$.*

   We will not prove this fact, but do try to wrap your head around its statement.

2. ***An interactive protocol for counting triangles.*** Let G be a graph with n vertices and let A be its adjacency matrix.

   (a) Represent adjacency matrix A as a Boolean function f_A on $2\log n$-bit Boolean vectors.

   (b) Use the multilinear extension lemma to represent A^2 as a multilinear polynomial in $4\log_2 n$ variables.

   (c) Let Δ be the number of triangles (3-cliques) in G. Show that

   $$\Delta = \frac{1}{6}\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} A_{ij}A_{jk}A_{ki}.$$

   (d) Express Δ as a multivariate polynomial in $6\log_2 n$ variables.

   (e) Design an IP protocol for a polynomially-bounded verifier to verify Δ.

[1] Condon, Anne, and Richard Ladner. "Interactive proof systems with polynomially bounded strategies." Journal of Computer and System Sciences 50.3 (1995): 506-518. This is a pretty interesting article to peruse.