- This worksheet is *optional*; ***no submissions required***, although we encourage to try it out and test your understanding.

---

1. ***Losing counts.*** Consider an incoming string w of length n. Every symbol in w has a *number* from 0 to k, signifying the *type*; and the plus-minus sign suggests whether to *add* or *subtract* from the count. For example, if the incoming string w is

   `+2-7-1+8+2-8-1+8+2+8-4-5-9+0-4+5+2-3-5-3+6-0+2+8-7+4-7-1-3+5+2`

   then the total count for $\langle$`0`$,\ldots,$`9`$\rangle$ is $\langle 0,-3,6,-3,-1,0,1,-3,3,-1\rangle$, respectively.

   For the machine model, you don't have general purpose memory but a single *counter*, that can store any number of length at most $O(\log n)$.[1] (Feel free to assume the constant C in the big-O notation is as big as you wish, but always strictly smaller than to the number of different types of symbols.)

   Design and analyze a randomized algorithm, so that after reading w in *one-single pass*, decide with high probability (that is, the error probability is less than $1/\mathrm{poly}\, n$) if the total counts for every type are *exactly zero*. In other words, the number of symbols of every type with a positive sign `+` is the same as the ones with negative sign `-`.

2. ***The simulator.*** The definition of zero-knowledge proof is confusing when we try to formalize the notion of no malicious verifier $\hat{V}$ can learn anything from the prover P, using a *simulator*. Formally speaking, an interactive proof (P, V) is ***zero-knowledge*** if

   - for every verifier $\hat{V}$ and every k-round interaction between P and $\hat{V}$, there exists a BPP maichine S (the ***simulator*** for P), such that for every $x \in L$, the record of interaction between $\hat{V}$ and with P on x is *indistinguishable* from running S standalone without access to P.

   The intuitive meaning of the simulator S is that for *every* malicious attempt from verifier $\hat{V}$ to extract extra information, $\hat{V}$ could have generated the "same" conversation record using the BPP machine S without talking to P, and thus $\hat{V}$ could not have learned anything new. Pay attention that $\hat{V}$ might not be using the prover P the same way as an honest verifier. (We also emphasize that S has access only to the input x, and the zero-knowledge is only required *when x is in L*.)

   (a) Recall the interactive proof protocol for distinguishing Coke from Pepsi. (What is input instance x and the underlying language L, so that the prover is trying to prove $x \in L$?) Is this a zero-knowledge protocol?

   (b) Now think back to the interactive proof protocol for *Where's Waldo?*. Construct a simulator S for P so that no matter what strategy the malicious verifier $\hat{V}$ chose, S can simulate the record of interaction between $\hat{V}$ and P. (Again remember that S does not have access to the location of Waldo, just the whole input picture x.)

[1] This is a typical model to assume for streaming big data.