22. Give formal proofs of the following two statements, which were discussed in class without full formal proofs.

- Every pseudorandom generator is a one-way function. In your proof, make the statement precise, using appropriate $\epsilon(n)$'s and $s(n)$'s. [1 points]

- If a function is ($\epsilon(n), s(n)$)-pseudorandom (according to Yao’s definition), then it is ($\epsilon(n), s(n)$)-unpredictable (according to the Blum–Micali definition). [1 points]

23. Suppose $x \in \{0, 1\}^n$ is an unknown $n$-bit string. A helper reveals to us the bits $x \odot r_i$ (for $1 \leq i \leq n$) where the strings $r_1, \ldots, r_n \in_R \{0, 1\}^n$ are chosen uniformly at random, and independently. Describe a deterministic algorithm that successfully reconstructs $x$ from this information, with probability at least $1/4$. Note: $x$ is fixed, and the probability is only over the choice of $r_i$s. [2 points]

Hint: Linear algebra over the finite field $\mathbb{F}_2$ works much the same as linear algebra over the reals.

24. We say that a language $L \subseteq \{0, 1\}^*$ is in the class $\text{IP}_{\alpha, \beta}$ if there is a polynomial-time verifier $V$ that uses a random string $r$ and has the following properties, where $P$ is an arbitrarily powerful prover that interacts with $V$:

$$x \notin L \implies \forall P : \Pr_r[V \ast P(x, r) = 1] \leq \alpha,$$

$$x \in L \implies \exists P : \Pr_r[V \ast P(x, r) = 1] \geq \beta.$$

(In case I switched the meaning of $\alpha$ and $\beta$ when writing on the board in class, please use only the above definition for this problem.)

We defined $\text{IP} = \text{IP}_{\frac{1}{2}, \frac{2}{3}}$ and remarked that the choice of the constants isn’t terribly important, as can be proven by suitable repetition and Chernoff bound analysis. We also remarked that $\beta$ can be made equal to 1 (perfect completeness), though not by simple repetition. Finally, we remarked that $\alpha$ cannot be made zero (perfect soundness) in general, because that would weaken the underlying class to plain old $\text{NP}$.

Justify this last remark. Specifically, prove that $\text{IP}_{0, \frac{2}{3}} = \text{NP}$. [2 points]