Exercise 1 (10 points). Prove the Johnson Bound: If $C$ is a code of minimum distance $1/2 - \epsilon$ and $\delta > 10\sqrt{\epsilon}$ then for every string $h$ there are at most $10/\delta^2$ distinct codewords in $C$ of distance at most $1/2 - \delta$ to $h$. (Hint: think of codewords as vectors in $\{\pm 1\}^n$. Also the proof is in the book, but I prefer if you first try to prove it yourself.)

Exercise 2 (20 points). Do Exercise 19.16 ($Q(x, P(x)) \equiv 0$ iff $P(x) - y$ divides $Q(x, y)$)

Exercise 3 (40 points). Using the local list decoder for Reed Muller stated in Theorem 19.26, and the Goldreich-Levin Theorem (that you proved in Homework 4), complete the proof of the optimal worst-case to average-case reduction: show that there is a way to transform every function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ in $2^{O(n)}$ time into a function $\tilde{f} : \{0, 1\}^{O(n)} \rightarrow \{0, 1\}$ such that if there exists a circuit $\tilde{C}$ of size $S$ such that $\Pr_x[\tilde{C}(x) = \tilde{f}(x)] \geq 1/2 + 1/S$ then there exists a circuit $C$ of size $S^{O(1)}$ that computes $f$ on every input in $\{0, 1\}^n$.

Exercise 4 (20 points). Do Exercise 20.8 (easy case of IW98)

Exercise 5 (30 points). Do Exercise 20.10 (converse to $\text{NEXP} \subseteq \text{P/poly} \implies \text{NEXP} = \text{MA}$)

Exercise 6 (Open question, as far as I know - better than any points :)). Find a simpler proof (maybe without using pseudorandom generators?) for the statement that if $\text{NEXP} \subseteq \text{P/poly}$ then $\text{NEXP} = \text{EXP}$.