Problem Set 1 — Solution

Problem 1

Part a

We show both directions of the equivalence. Let $A \in \mathsf{ZPP}$. Let M be a zero-error randomized algorithm that decides A whose running time is polynomial in expectation. Let T be a random variable that denotes the running time of M, so that on every input of length n, $\mathbb{E}[T] \leq f(n)$ for some polynomial $f(n)$.

We'll show that A has an algorithm M' with properties (i)–(iv) as stated in the question. Let M' be an algorithm that, on input x of length n, simulates M for at most $10 \cdot f(n)$ steps. If M halts, M' gives the same answer as M'. Otherwise, M answers "I don't know". Properties (i) and (ii) are clear from the definition of M'. Property (iii) holds since M is a zero-error randomized algorithm. Property (iv) follows from Markov's inequality: indeed, note that T is a non-negative random variable, so that

$$\Pr[M' \text{ answers "I don't know"}] = \Pr[T \geq 10\mathbb{E}[T]] \leq \frac{1}{10}.$$

In the other direction, suppose A has an algorithm M' with properties (i)–(iv) as stated in the question. Let $f(n)$ be a bound on the running time of M' for inputs of length n. We'll show a zero-error randomized algorithm M for A whose running time is polynomial in expectation. On input x of length n, M simply simulates the algorithm M'. If M' returns an answer, M' returns the same answer. Otherwise, if M' says "I don't know", M simulates M' again with fresh randomness, and so on until M returns an answer.

By the properties of M', M is a zero-error algorithm. The only thing left to show is that the running time of M is polynomial in expectation. Let p denote the probability that M' returns "I don't know". By assumption, $p \leq 1/3$. We make think of each run of M' as an experiment with success probability $1 - p$, success being that M' returns a yes or no answer (and not "I don't know"). We are repeating this experiment until the first success. This distribution is known as the geometric distribution (with parameter $1 - p$), and its expectation is $\frac{1}{1-p}$. Therefore, the running time of M is at most $\frac{1}{1-p} \cdot f(n)$, which is polynomial in n.

Alternatively, one can also directly calculate the expected running time. The probability that M performs k simulations of M' is $p^{k-1} \cdot (1 - p)$, since that would mean that the first $k - 1$ simulations returned "I don't know" and the k-th simulation returned an answer. Therefore, if we let T denote the running time of M, then for all k, $T = k \cdot f(n)$ with probability $p^{k-1} \cdot (1-p)$, which implies that

$$\mathbb{E}[T] = \sum_{k=1}^{\infty}(1-p)p^{k-1} \cdot k \cdot f(n) = (1-p) \cdot f(n) \cdot \left(\sum_{k=1}^{\infty} k \cdot p^{k-1}\right)$$
$$= (1-p) \cdot f(n) \cdot \frac{d}{dp}\left(\sum_{k=1}^{\infty} p^k\right) = (1-p) \cdot f(n) \cdot \frac{d}{dp}\left(\frac{1}{1-p}\right) = \frac{1}{1-p} f(n).$$

Part b

Recall that $\mathsf{BPP} = \mathsf{BPP}(1/3, 2/3)$. Let $A \in \mathsf{RP}$. Then there's an algorithm M such that if $x \notin A$, M accepts x with probability 0, and if $x \in A$, M accepts x with probability at least $1/2$. Consider an algorithm M' which runs A twice, each time with fresh and independent randomness, and accepts if one of the two runs accepted. If $x \notin A$, M' accepts x with probability 0. If $x \in A$, then the probability that both runs of M rejected is at most $\frac{1}{2} \cdot \frac{1}{2} = 1/4$, and thus M' accepts with probability at least $3/4$.
The proof that $\mathsf{coRP} \subseteq \mathsf{BPP}$ is analogous.

Part c

We may use the definition of ZPP from part (a). Suppose $A \in \mathsf{ZPP}$. Let M be an algorithm for A with properties (i)–(iv) from part (a). Consider an algorithm M' which is identical to A except that if M says "I don't know", M' rejects. M' runs in polynomial time. If $x \notin A$, then M' accepts x with probability 0 (since x is either rejected by M, or, if M said "I don't know", M' rejects). If $x \in A$, then x can only be rejected if M said "I don't know", which happens with probability at most $1/3$. Thus, M' shows that $A \in \mathsf{RP}$. The proof that $A \in \mathsf{coRP}$ is identical, except that now we need to accept if M said "I don't know".
In the other direction, suppose $A \in \mathsf{RP} \cap \mathsf{coRP}$ and let M_1, M_2 be the two corresponding RP and coRP algorithms, respectively. We devise a new algorithm M with properties (i)–(iv) from part (a). On input x, M runs both M_1 and M_2. If M_1 accepted, M accept. If M_2 rejected, M rejects. Otherwise, M says "I don't know".
As we've seen in class we may assume that the error probability of both M_1 and M_2 is at most $1/3$.
If $x \in A$ then M_1 accepts with probability at least $2/3$ and M_2 never rejects. Thus, M either accepts, or, with probability at most $1/3$, says "I don't know".
Similarly, if $x \notin A$, then M_2 rejects with probability at least $2/3$ and M_1 never accepts. Thus, M either rejects, or, with probability at most $1/3$, says "I don't know".

Problem 2

The proof is by induction on n. For the base case, this is exactly the fact that a non-zero degree-d polynomial over a field $\mathbb{F}$ has at most d roots. For the induction step, write f as

$\sum_{i=0}^{d} x_n^d f_i(x_1,\ldots,x_{n-1})$ for some polynomials $f_0,\ldots,f_d$ on $n-1$ variables with $\deg(f_i) \le d-i$. Note that since $f \neq 0$, there exists at least one f_i which is non-zero. Let d_0 be the maximal i such that f_i is non-zero.
Consider now what happens when we pick $\alpha_1,\ldots,\alpha_{n-1},\alpha_n \in S$ uniformly at random and independently. Let E denote the event that $f_{d_0}(\alpha_1,\ldots,\alpha_{n-1}) = 0$. Since f_{d_0} is non-zero, the induction hypothesis now implies that $\Pr[E] \le \frac{d-d_0}{|S|}$. Further, if E does *not* happen,

$$P(x) = \sum_{i=0}^{d_0} f_i(\alpha_1,\ldots,\alpha_{n-1}) x_n^i$$

is a non-zero polynomial in x_n of degree d_0, and thus the probability of picking α_n such that $P(\alpha_n) = 0$ is at most $d_0/|S|$ by the base case of the induction.
Thus, we can compute

$$\begin{aligned}\Pr_{\alpha_1,\ldots,\alpha_n \in S}[f(\alpha_1,\ldots,\alpha_n) = 0] &= \Pr_{\alpha_1,\ldots,\alpha_n \in S}[f(\alpha_1,\ldots,\alpha_n) = 0 | E] \cdot \Pr[E] \\ &+ \Pr_{\alpha_1,\ldots,\alpha_n \in S}[f(\alpha_1,\ldots,\alpha_n) = 0 | \neg E] \cdot \Pr[\neg E] \\ &\le 1 \cdot \frac{d-d_0}{|S|} + \frac{d_0}{|S|} \cdot 1 = \frac{d}{|S|}.\end{aligned}$$

Problem 3

Part a

Let $x = (x_1,\ldots,x_n)$. By the assumption $\sum_{k=1}^{n} x_k^2 = 1$ thus there must be i such that $x_i^2 \ge 1/n$ and $|x_i| \ge \frac{1}{\sqrt{n}}$.

Part b

As shown in class, $\mathbf{1}$ is an eigenvector corresponding to the eigenvalue 1, and thus $\langle x, \mathbf{1} \rangle = 0$ which implies that $\sum_{k=1}^{n} x_k = 0$. Since $x_i \ge 1/\sqrt{n}$, for the sum to be zero there must be a different coordinate j such that $x_j \le 0$

Part c

Since G is connected, there's a path from vertex i to vertex j. We can also assume this is a simple path, whose length is at most n. Consider the sequence of vertices on the path

$$i = i_1, i_2, \ldots, i_t = j$$

where each adjacent pair is connected by an edge. Note that $|x_i - x_j| = |x_{i_1} - x_{i_t}| \ge \frac{1}{\sqrt{n}}$, and

$$\frac{1}{\sqrt{n}} \le |x_{i_1} - x_{i_t}| = \left| \sum_{k=1}^{t-1} (x_{i_k} - x_{i_{k+1}}) \right| \le \sum_{k=1}^{t-1} |x_{i_k} - x_{i_{k+1}}|.$$

Thus there must exist a pair (u, v) along this path such that $|x_u - x_n| \geq \frac{1}{n\sqrt{n}}$.

Part d

The equality $\lambda_2 = \lambda_2 \langle x, x \rangle$ follows from the assumption that $\|x\|_2 = 1$. The second equality follows from basic properties of the inner product, and the second from the fact that by assumption, λ_2 is an eigenvalue of the eigenvector x and thus $Bx = \lambda_2 x$. The fourth equality follows by definition of matrix product, and the fifth from the simple identity

$$x_k x_\ell = \frac{1}{2}(x_k^2 + x_\ell^2 - (x_k - x_\ell)^2).$$

The sixth equality is just an expansion of the sum, and the seventh uses again the fact that $\sum_k x_k^2 = 1$.
To conclude the upper bound on λ_2, first note that every summand in $\frac{1}{2}\sum_{k,\ell} B_{k,\ell} \cdot (x_k - x_\ell)^2$ is non-negative. Further, we know that there's at least one summand u, v for which $(x_u - x_v)^2 \geq \frac{1}{n^3}$. Since there's an edge u, v we know that $A_{u,v} \geq \frac{1}{d}$ (where A is the normalized adjacency matrix of G) and thus $B_{u,v} \geq \frac{1}{2d}$. This implies that the sum

$$\frac{1}{2}\sum_{k,\ell} B_{k,\ell} \cdot (x_k - x_\ell)^2$$

is at least $\frac{1}{4dn^3}$, completing the proof.

Problem 4

Let $a \in \{0,1\}^n$ and $b \in \{0,1\}^n$ denote the inputs of Alice and Bob, respectively. As in the hint, we interpret a and b as integers in the interval $[0, 2^n - 1]$ written in binary.
We devise the following protocol: Alice picks a random prime $p \in [1, n^{10}]$ and sends to Bob p and $a \bmod p$, both written in binary. Note that since $p \leq n^{10}$, the number of bits needed to encode p and $a \bmod p$ in binary is $O(\log n)$. Bob computes $b \bmod p$ and compares is to $a \bmod p$. If they are equal, Bob declares that the numbers are equal. Otherwise, Bob declares there are not equal.
Clearly, if $a = b$ then they are equal modulo p for every p and thus in this case Bob will always declare they are equal. Suppose $a \neq b$. Then $a \equiv b \bmod p$ if and only if p divides $a - b$. Suppose $a > b$ so that $a - b > 0$ (the other case is completely analogous by considering $b - a$). $a - b$ is an integer in $[1, 2^n - 1]$. The number of distinct prime divisors of every number of size less than N is at most $\log N$ (since every prime number is greater than or equal to 2), which in our case, is at most n. However, the total number of primes p of size at most n^{10} is, as shown in class $O\left(\frac{n^{10}}{\log n}\right)$ and in particular at least n^9 for large enough n. Thus, the probability that Bob picked a "bad" prime, that is, a prime p such that $a \equiv b \bmod p$ is at most $\frac{n}{n^9} = \frac{1}{n^8}$.