A Technical Results

A.1 Proof of Lemma 1

Using the definition of $Z$ and $h_x$, we have

$$1 - \text{err}(h_x) = \Pr_{(r,s),b \sim D}(b = h_x(r,s)) = \Pr(s = P(x)) \Pr(b = h_x(r,s) | s = P(x)) + \Pr(s \neq P(x)) \Pr(b = h_x(r,s) | s \neq P(x)) = \Pr(s = P(x)) \star 1 + \Pr(s \neq P(x)) \star \frac{1}{2} = \frac{1}{2}(Pr(s = P(x)) + 1).$$

Rearranging, we get the result.

A.2 Proof of Lemma 2

Let $p_k$ denote the probability that after drawing $r_1, \ldots, r_k$, i.i.d., an independently drawn $r_{k+1}$ is not spanned by $r_1, \ldots, r_k$. Also, let $B_k$ be a Bernoulli random variable with parameter $p_k$. Whenever $B_k = 1$, the dimensionality of the subspace spanned by the vectors we drew so far increases by 1. Since we are in an $n$-dimensional space, we must have $B_1 + \ldots + B_{m'} \leq n$ with probability 1. In particular, we have

$$n \geq \mathbb{E}[B_1 + \ldots + B_{m'}] = p_1 + \ldots + p_{m'}.$$

Also, for any $k \leq m'$, by the assumption that the vectors are drawn i.i.d., we have

$$p'_m = \Pr(r_{m'+1} \notin \text{span}(r_1, \ldots, r_m)) \leq \Pr(r_{m'+1} \notin \text{span}(r_1, \ldots, r_k)) = \Pr(r_{k+1} \notin \text{span}(r_1, \ldots, r_k)) = p_k.$$

Combining the two inequalities, it follows that $m'p_{m'} \leq n$, so $p_{m'} \leq n/m'$ as required.