A Technical Results

A.1 Proof of Lemma 1

Using the definition of $\mathcal{Z}$ and $h_{\mathbf{x}}$, we have

$$
\begin{aligned}
&1 - \mathrm{err}(h_{\mathbf{x}}) = \Pr_{((\mathbf{r},\mathbf{s}),b)\sim\mathcal{D}}(b = h_{\mathbf{x}}(\mathbf{r},\mathbf{s})) \\
&= \Pr(\mathbf{s} = P(\mathbf{x}))\ \Pr(b = h_{\mathbf{x}}(\mathbf{r},\mathbf{s}) | \mathbf{s} = P(\mathbf{x})) + \\
&\quad \Pr(\mathbf{s} \neq P(\mathbf{x}))\ \Pr(b = h_{\mathbf{x}}(\mathbf{r},\mathbf{s}) | \mathbf{s} \neq P(\mathbf{x})) \\
&= \Pr(\mathbf{s} = P(\mathbf{x})) * 1 + \Pr(\mathbf{s} \neq P(x)) * \frac{1}{2} \\
&= \frac{1}{2}(Pr(\mathbf{s} = P(\mathbf{x})) + 1).
\end{aligned}
$$

Rearranging, we get the result.

A.2 Proof of Lemma 2

Let p_k denote the probability that after drawing $\mathbf{r}_1, \ldots, \mathbf{r}_k$, i.i.d., an independently drawn $\mathbf{r}_{k+1}$ is not spanned by $\mathbf{r}_1, \ldots, \mathbf{r}_k$. 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

$$
\begin{aligned}
p'_m &= \Pr(r_{m'+1} \notin \mathrm{span}(r_1, \ldots, r_{m'})) \\
&\leq \Pr(r_{m'+1} \notin \mathrm{span}(r_1, \ldots, r_k)) \\
&= \Pr(r_{k+1} \notin \mathrm{span}(r_1, \ldots, r_k)) \ = \ p_k.
\end{aligned}
$$

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