A. Proof of Lemma 3

In this section, we show that conditions 1-3 holds with high probability and prove Lemma 3. To prove the lemma we first prove three auxiliary lemmas; each of these three Lemma will lead to one of the three conditions in Lemma 3. These three lemmas characterizes the statistical properties of the collection of good batches B_G. We state and prove these lemmas in the next subsection.

A.1. Statistical Properties of the Good Batches

Recall that, for a good batch $b \in B_G$ and subset $S \subseteq [k]$, $\mathbf{1}_S(X_i^b)$, for $i \in [n]$, are i.i.d. indicator random variables and $\bar{\mu}_b(S)$ is the mean of these n indicator variables. Since the indicator random variables are sub-gaussian, namely $\mathbf{1}_S(X_i^b) \sim \text{subG}(p(S), 1/4)$, the mean $\bar{\mu}_b(S)$ satisfies $\bar{\mu}_b(S) \sim \text{subG}(p(S), 1/4n)$. subG(.) is used to denote a sub-gaussian distribution. This observation plays the key role in the proof of all three auxiliary lemmas in this section.

The first lemma among these three lemmas show that for any fixed subset $S \subseteq [k]$, $\bar{\mu}_b(S)$ for most of the good batches is close to $p(S)$. This lemma is used to show Condition 1.

Lemma 10. *For any $\epsilon \in (0, 1/4]$ and $|B_G| \geq 12k/\epsilon$, $\forall\, S \subseteq [k]$, with probability $\geq 1 - e^{-k}$,*

$$\left|\left\{b \in B_G : |\bar{\mu}_b(S) - p(S)| \geq \sqrt{\frac{\ln(1/\epsilon)}{n}}\right\}\right| \leq \epsilon |B_G|.$$

Proof. From Hoeffding's inequality, for $b \in B_G$ and $S \subseteq [k]$,

$$\Pr\left[|\bar{\mu}_b(S) - p(S)| \geq \sqrt{\frac{\ln(1/\epsilon)}{n}}\right] \leq 2e^{-2\ln(1/\epsilon)} \leq 2\epsilon^2 \leq \epsilon/2.$$

Let $\mathbf{1}_b(S)$ be the indicator random variable that takes the value 1 iff $|\bar{\mu}_b(S) - p(S)| \geq \sqrt{\ln(1/\epsilon)/n}$. Therefore, for $b \in B_G$, $E[\mathbf{1}_b(S)] \leq \epsilon/2$. Using the Chernoff bound,

$$\Pr[\sum_{b \in B_G} \mathbf{1}_b(S) \geq \epsilon |B_G|] \leq e^{-\frac{1}{3}\cdot\frac{\epsilon}{2}|B_G|} \leq e^{-2k}.$$

Taking the union bound over all 2^k subsets S completes the proof. ∎

The next lemma show that even upon removal of any small fraction of good batches from B_G, the empirical mean and the variance of the remaining sub-collection of batches approximate the distribution mean and the variance well enough.

Lemma 11. *For any $\epsilon \in (0, 1/4]$, and $|B_G| \geq \frac{k}{\epsilon^2 \ln(e/\epsilon)}$. Then $\forall\, S \subseteq [k]$ and $\forall\, B'_G \subseteq B_G$ of size $|B'_G| \geq (1-\epsilon)|B_G|$, with probability $\geq 1 - 6e^{-k}$,*

$$\left|\bar{p}_{B'_G}(S) - p(S)\right| \leq 3\epsilon\sqrt{\frac{\ln(e/\epsilon)}{n}} \tag{2}$$

and

$$\left|\frac{1}{|B'_G|}\sum_{b \in B'_G}(\bar{\mu}_b(S) - p(S))^2 - V(p(S))\right| \leq 32\frac{\epsilon \ln(e/\epsilon)}{n}. \tag{3}$$

Proof. From Hoeffding's inequality,

$$\begin{aligned}\Pr\left[|B_G||\bar{p}_{B_G}(S) - p(S)| \geq |B_G|\epsilon\sqrt{\frac{\ln(e/\epsilon)}{n}}\right] &= \Pr\left[\left|\sum_{b \in B_G}(\bar{\mu}_b(S) - p(S))\right| \geq |B_G|\epsilon\sqrt{\frac{\ln(e/\epsilon)}{n}}\right] \\ &\leq 2e^{-\frac{|B_G|\epsilon^2}{2/(4n)}\cdot\frac{\ln(e/\epsilon)}{n}} = 2e^{-2|B_G|\epsilon^2\ln(e/\epsilon)} \leq 2e^{-2k}.\end{aligned} \tag{4}$$

Similarly, for a fix sub-collection $U_G \subseteq B_G$ of size $1 \le |U_G| \le \epsilon|B_G|$,

$$\Pr\Big[|U_G| \cdot |\bar{p}_{U_G}(S) - p(S)| \ge \epsilon|B_G|\sqrt{\frac{\ln(e/\epsilon)}{n}}\Big] = \Pr\Big[\Big|\sum_{b\in U_G}(\bar{\mu}_b(S) - p(S))\Big| \ge \epsilon|B_G|\sqrt{\frac{\ln(e/\epsilon)}{n}}\Big]$$
$$\le 2e^{-2\ln(e/\epsilon)\frac{(\epsilon|B_G|)^2}{|U_G|}} \le 2e^{-2\epsilon|B_G|\ln(e/\epsilon)},$$

where the last inequality used $|U_G| \le \epsilon|B_G|$. Next, the number of sub-collections (non-empty) of B_G with size $\le \epsilon|B_G|$ is bounded by

$$\sum_{j=1}^{\lfloor\epsilon|B_G|\rfloor}\binom{|B_G|}{j} \le \epsilon|B_G|\binom{|B_G|}{\lfloor\epsilon|B_G|\rfloor} \le \epsilon|B_G|\Big(\frac{e|B_G|}{\epsilon|B_G|}\Big)^{\epsilon|B_G|} \le e^{\epsilon|B_G|\ln(e/\epsilon)+\ln(\epsilon|B_G|)} < e^{\frac{3}{2}\epsilon|B_G|\ln(e/\epsilon)}, \tag{5}$$

where last of the above inequality used $\ln(\epsilon|B_G|) < \epsilon|B_G|/2$ and $\ln(e/\epsilon) \ge 1$. Then, using the union bound, $\forall\, U_G \subseteq B_G$ such that $|U_G| \le \epsilon|B_G|$, we get

$$\Pr\Big[|U_G| \cdot |\bar{p}_{U_G}(S) - p(S)| \ge \epsilon|B_G|\sqrt{\frac{\ln(e/\epsilon)}{n}}\Big] \le 2e^{-\frac{1}{2}\epsilon|B_G|\ln(e/\epsilon)} < 2e^{-\frac{k}{2\epsilon}} < 2e^{-2k}. \tag{6}$$

For any sub-collection $B'_G \subseteq B_G$ with $|B'_G| \ge (1-\epsilon)|B_G|$,

$$\Big|\sum_{b\in B'_G}(\bar{\mu}_b(S) - p(S))\Big| = \Big|\sum_{b\in B_G}(\bar{\mu}_b(S) - p(S)) - \sum_{b\in B_G/B'_G}(\bar{\mu}_b(S) - p(S))\Big|$$
$$\le \Big|\sum_{b\in B_G}(\bar{\mu}_b(S) - p(S))\Big| + \Big|\sum_{b\in B_G/B'_G}(\bar{\mu}_b(S) - p(S))\Big|$$
$$\le |B_G| \times |\bar{p}_{B_G}(S) - p(S)| + \max_{U_G:|U_G|\le\epsilon|B_G|}|U_G| \times |\bar{p}_{U_G}(S) - p(S)|$$
$$\le 2\epsilon|B_G|\sqrt{\frac{\ln(e/\epsilon)}{n}},$$

with probability $\ge 1 - 2e^{-2k} - 2e^{-2k} \ge 1 - 4e^{-2k}$. Then

$$|\bar{p}_{B'_G}(S) - p(S)| = \frac{1}{|B'_G|}\Big|\sum_{b\in B'_G}(\bar{\mu}_b(S) - p(S))\Big| \le 2\frac{\epsilon|B_G|}{|B'_G|}\sqrt{\frac{\ln(e/\epsilon)}{n}}$$
$$\le \frac{2\epsilon}{(1-\epsilon)}\sqrt{\frac{\ln(e/\epsilon)}{n}} < 3\epsilon\sqrt{\frac{\ln(e/\epsilon)}{n}},$$

with probability $\ge 1 - 4e^{-2k}$. The last step used $\epsilon \le 1/4$. Since there are 2^k different choices for $S \subseteq [k]$, from the union bound we get,

$$\Pr\Big[\bigcup_{S\subseteq[k]}\Big\{|\bar{p}_{B'_G}(S) - p(S)| > 4\epsilon\sqrt{\frac{\ln(e/\epsilon)}{n}}\Big\}\Big] \le 4e^{-2k} \times 2^k = 4e^{-k}.$$

This completes the proof of (2).

Let $Y_b = (\bar{\mu}_b(S) - p(S))^2 - \mathrm{V}(p(S))$. For $b \in B_G$, $\bar{\mu}_b(S) - p(S) \sim \mathrm{subG}(1/4n)$, therefore

$$(\bar{\mu}_b(S) - p(S))^2 - E(\bar{\mu}_b(S) - p(S))^2 = Y_b \sim \mathrm{subE}(\frac{16}{4n}) = \mathrm{subE}(\frac{4}{n}).$$

Here subE is sub exponential distribution (Philippe, 2015). Then Bernstein's inequality gives:

$$\Pr[\Big|\sum_{b\in B_G} Y_b\Big| \ge 8|B_G|\frac{\epsilon}{n}\ln(e/\epsilon)] \le 2e^{-\frac{|B_G|}{2}\left(\frac{8\epsilon\ln(e/\epsilon)/n}{4/n}\right)^2} = 2e^{-2|B_G|\epsilon^2\ln^2(e/\epsilon)} \le 2e^{-2k}.$$

Next, for a fix sub-collection $U_G \subseteq B_G$ of size $1 \leq |U_G| \leq \epsilon |B_G|$,

$$\Pr\Big[\Big|\sum_{b\in U_G} Y_b\Big| \geq 16\epsilon|B_G|\frac{\ln(e/\epsilon)}{n}\Big] \leq 2e^{-\frac{16\epsilon|B_G|\frac{\ln(e/\epsilon)}{n}}{2\times 4/n}} \leq 2e^{-2\epsilon|B_G|\ln(e/\epsilon)}.$$

Then following the same steps as in the proof of (2) one can complete the proof of (3). ■

To state the next lemma, we make use of the following definition. For a subset $S \subseteq [k]$, let

$$B_G^d(S,\epsilon) \triangleq \big\{b \in B_G : |\bar{\mu}_b(S) - p(S)| \geq 2\sqrt{\frac{\ln(6e/\epsilon)}{n}})\big\}$$

be the sub-collection of batches for which empirical probabilities $\bar{\mu}_b(S)$ are far from $p(S)$ for a given set S.

The last lemma of the section upper bounds the total squared deviation of empirical probabilities $\bar{\mu}_b(S)$ from $p(S)$ for batches in sub-collection $B_G^d(S,\epsilon)$. It helps in upper bounding the corruption for good batches and show that Condition 3 holds with high probability.

Lemma 12. *For any $0 < \epsilon < 1/2$, and $|B_G| \geq \frac{120k}{\epsilon\ln(e/\epsilon)}$. Then $\forall\, S \subseteq [k]$, with probability $\geq 1 - 2e^{-k}$,*

$$|B_G^d(S,\epsilon)| \leq \frac{\epsilon}{40}|B_G|, \tag{7}$$

and

$$\sum_{b\in B_G^d(S,\epsilon)} (\bar{\mu}_b(S) - p(S))^2 < \frac{\epsilon}{2}|B_G|\frac{\ln(e/\epsilon)}{n}. \tag{8}$$

Proof. The proof of the first part is the same as (with different constants) Lemma 10 and we skip it to avoid repetition.

To prove the second part we bound the total squared deviation of any subset of size $\leq \frac{\epsilon}{40}|B_G|$.

Let $Y_b = (\bar{\mu}_b(S) - p(S))^2 - \mathrm{V}(p(S))$. Similar to the previous lemma, for a fix sub-collection $U_G \subseteq B_G$ of size $1 \leq |U_G| \leq \frac{\epsilon}{40}|B_G|$, Bernstein's inequality gives:

$$\Pr\Big[\Big|\sum_{b\in U_G} Y_b\Big| \geq 8\frac{\epsilon}{20}|B_G|\frac{\ln(e/\epsilon)}{n}\Big] \leq 2e^{-\frac{8\epsilon|B_G|\frac{\ln(e/\epsilon)}{n}}{20\times 2\times 4/n}} \leq 2e^{-\frac{\epsilon}{20}|B_G|\ln(e/\epsilon)}.$$

From (5), there are $e^{\frac{3}{80}\epsilon|B_G|\ln(e/\epsilon)}$ many sub-collections of size $\leq \frac{\epsilon}{40}|B_G|$. Then taking the union bound for all sub-collections of this size and all subsets $S \subseteq [k]$ we get,

$$\Big|\sum_{b\in U_G}\Big((\bar{\mu}_b(S) - p(S))^2 - \mathrm{V}(p(S))\Big)\Big| \leq \frac{2\epsilon}{5}|B_G|\frac{\ln(e/\epsilon)}{n},$$

for all U_G of size $\leq \frac{\epsilon}{40}|B_G|$. Then using the fact that $\mathrm{V}(.)$ is upper bounded by $\frac{1}{4n}$, and therefore $|U_G|\mathrm{V}(p(S)) \leq \frac{\epsilon}{4\times 40}|B_G|$, completes the proof. ■

A.2. Completing the proof of Lemma 3

We first show condition 1 holds with high probability.

It is easy to verify that $|p(S) - \mathrm{med}(\bar{\mu}(S))| \geq \sqrt{\ln 6/n}$, only if the sub-collection $T = \{b : |p(S) - \bar{\mu}_b(S)| \geq \sqrt{\ln 6/n}\}$ has at-least $0.5m$ batches. But

$$|T| = |T\cap B_G| + |T\cap B_A| \overset{(a)}{<} |B_G|/6 + |B_A| = \frac{m}{6} + \frac{5}{6}|B_A| \overset{(b)}{\leq} \frac{m}{6} + \frac{2m}{6} = 0.5m,$$

where inequality (a) follows from Lemma 10 by choosing $\epsilon = 1/6$ and (b) follows since $|B_A| \le \beta m \le 0.4m$.

Using $\epsilon = \beta/6$ in Lemma 11 gives Condition 2.

Finally, we show the last condition. To show it we use $\epsilon = \beta$ in Lemma 12. From Condition 1, note that for $b \in B_G \setminus B_G^d(S,\beta)$

$$|\bar{\mu}_b(S) - \text{med}(\bar{\mu}(S))| \le |\bar{\mu}_b(S) - p(S)| + |p(S) - \text{med}(\bar{\mu}(S))| \le 2\sqrt{\frac{\ln(6e/\beta)}{n}} + \sqrt{\frac{\ln 6}{n}} \le 3\sqrt{\frac{\ln(6e/\beta)}{n}},$$

Then, for $b \in B_G \setminus B_G^d(S,\beta)$, from the definition of corruption score it follows that $\psi_b(S) = 0$. Next set of inequalities complete the proof of condition 3.

$$\begin{aligned}
\psi(B_G) &= \sum_{b\in B_G} \psi_b(S) = \sum_{b\in B_G\setminus B_G^d(S,\beta)} \psi_b(S) + \sum_{b\in B_G^d(S,\beta)} \psi_b(S) \\
&= \sum_{b\in B_G^d(S,\beta)} \psi_b(S) \\
&\overset{(a)}{\le} \sum_{b\in B_G^d(S,\beta)} (\bar{\mu}_b(S) - \text{med}(\bar{\mu}(S)))^2 \\
&= \sum_{b\in B_G^d(S,\beta)} (\bar{\mu}_b(S) - p(S) + p(S) - \text{med}(\bar{\mu}(S)))^2 \\
&\overset{(b)}{\le} \sum_{b\in B_G^d(S,\beta)} (\bar{\mu}_b(S) - p(S))^2 + \sum_{b\in B_G^d(S,\beta)} (\text{med}(\bar{\mu}(S)) - p(S))^2 \\
&+ 2\sqrt{\left(\sum_{b\in B_G^d(S,\beta)} (\bar{\mu}_b(S) - p(S))^2\right)\left(\sum_{b\in B_G^d(S,\beta)} (\text{med}(\bar{\mu}(S)) - p(S))^2\right)} \\
&\overset{(c)}{\le} \frac{\beta}{2}|B_G|\frac{\ln(e/\beta)}{n} + \frac{\beta}{40}|B_G|\frac{\ln 6}{n} + \sqrt{\frac{\beta}{2}|B_G|\frac{\ln(e/\beta)}{n} \times \frac{\beta}{40}|B_G|\frac{\ln 6}{n}} < \beta|B_G|\frac{\ln(e/\beta)}{n},
\end{aligned}$$

here (a) follows from the definition of the corruption score, (b) uses Cauchy-Schwarz inequality and (c) follows from Lemma 12 and Condition 1.

B. Proof of the other Lemmas

We first prove an auxiliary Lemma that will be useful in other proofs. For a given sub-collection B' and subset S, the next lemma bounds the total squared distance of $\bar{\mu}_b(S)$ from $p(S)$ over the adversarial batches $b \in B' \cap B_A$ in terms of corruption score $\psi(B', S)$.

Lemma 13. *Suppose the conditions 1 and 3 holds. For subset S, let $\psi(B', S) = t \cdot \kappa_G$, for some $t \ge 0$, then*

$$(t - 3 - 2\sqrt{t})\kappa_G \le \sum_{b\in B'\cap B_A} (\bar{\mu}_b(S) - p(S))^2 \le (t + 17 + 2\sqrt{t})\kappa_G.$$

Proof. For the purpose of this proof, let $B'_G = B' \cap B_G$ and $B'_A = B' \cap B_A$. Then

$$\sum_{b\in B'_A} (\bar{\mu}_b(S) - p(S))^2 = \sum_{b\in B'_A:\psi_b(S)>0} (\bar{\mu}_b(S) - p(S))^2 + \sum_{b\in B'_A:\psi_b(S)=0} (\bar{\mu}_b(S) - p(S))^2 \tag{9}$$

From the definition of corruption score, for batch $b \in B'$, with zero corruption score $\psi_b(S)$, we have $|\bar{\mu}_b(S) - \text{med}(\bar{\mu}(S))| \le 3\sqrt{\frac{\ln(6e/\beta)}{n}}$. Then using Condition 1 and the triangle inequality, for such batches with zero corruption score, we get

$$|\bar{\mu}_b(S) - p(S)| \le \sqrt{\ln(6)/n} + 3\sqrt{\frac{\ln(6e/\beta)}{n}} < 4\sqrt{\frac{\ln(6e/\beta)}{n}}. \tag{10}$$

Next,

$$\begin{aligned}
&\sum_{b\in B'_A:\psi_b(S)>0}(\bar{\mu}_b(S)-p(S))^2\\
&=\sum_{b\in B'_A:\psi_b(S)>0}(\bar{\mu}_b(S)-\text{med}(\bar{\mu}(S))+\text{med}(\bar{\mu}(S))-p(S))^2\\
&\overset{(a)}{\le}\sum_{b\in B'_A:\psi_b(S)>0}(\bar{\mu}_b(S)-\text{med}(\bar{\mu}(S)))^2+\sum_{b\in B'_A:\psi_b(S)>0}(\text{med}(\bar{\mu}(S))-p(S))^2\\
&+2\sqrt{\left(\sum_{b\in B'_A:\psi_b(S)>0}(\bar{\mu}_b(S)-\text{med}(\bar{\mu}(S)))^2\right)\left(\sum_{b\in B'_A:\psi_b(S)>0}(\text{med}(\bar{\mu}(S))-p(S))^2\right)}\\
&\overset{(b)}{\le}\sum_{b\in B'_A}\psi_b(S)+\sum_{b\in B'_A}\frac{\ln 6}{n}+2\sqrt{\left(\sum_{b\in B'_A}\psi_b(S)\right)\left(\sum_{b\in B'_A}\frac{\ln 6}{n}\right)}\\
&\overset{(c)}{\le}\psi(B'_A,S)+\kappa_G+2\sqrt{\psi(B'_A,S)\cdot\kappa_G},
\end{aligned}\tag{11}$$

here (a) uses Cauchy-Schwarz inequality, (b) follows from the definition of corruption score and Condition 1, and (c) uses $|B'_A|\le\beta m$ and $(\beta m\ln 6)/n\le\kappa_G$.

A similar calculation as the above leads to the following

$$\sum_{b\in B'_A:\psi_b(S)>0}(\bar{\mu}_b(S)-p(S))^2\ge\psi(B'_A,S)-2\sqrt{\psi(B'_A,S)\cdot\kappa_G},\tag{12}$$

Next, we show the upper bound in the lemma. Combining equations (9), (10) and (11) gives

$$\begin{aligned}
\sum_{b\in B'_A}(\bar{\mu}_b(S)-p(S))^2&\le\psi(B'_A,S)+\kappa_G+2\sqrt{\psi(B'_A,S)\cdot\kappa_G}+\sum_{b\in B'_A:\psi_b(S)=0}4\sqrt{\frac{\ln(6e/\beta)}{n}}\\
&\le\psi(B',S)+\kappa_G+2\sqrt{\psi(B',S)\cdot\kappa_G}+16|B_A|\frac{\ln(6e/\beta)}{n}\\
&\le(t+17+2\sqrt{t})\kappa_G,
\end{aligned}$$

here the second last inequality used $B'_A\subseteq B'$ and $B'_A\subseteq B_A$. This completes the proof of the upper bound.

To prove the lower bound, we first note that

$$\begin{aligned}
\psi(B',S)&=\sum_{b\in B'}\psi_b(S)=\sum_{b\in B'_G}\psi_b(S)+\sum_{b\in B'_A}\psi_b(S)\\
&\le\sum_{b\in B_G}\psi_b(S)+\psi(B'_A,S)\\
&\le\psi(B_G)+\psi(B'_A,S)\le\frac{\beta m\ln(6e/\beta)}{n}+\sum_{b\in B'_A}\psi_b(S),
\end{aligned}$$

here the last inequality uses condition 3. The above equation implies that

$$\psi(B'_A,S)\ge\psi(B',S)-\beta m\frac{\ln(6e/\beta)}{n}=(t-1)\kappa_G.\tag{13}$$

By combining, equations (9) (12) and (13), we get the lower bound

$$\sum_{b\in B'_A}(\bar{\mu}_b(S)-p(S))^2\ge(t-1)\kappa_G-2\sqrt{|t-1|\kappa_G\cdot\kappa_G}=(t-1-2\sqrt{|t-1|})\kappa_G\ge(t-3-2\sqrt{t})\kappa_G.$$

■

B.1. Proof of Lemma 4

Proof. For the purpose of this proof, let $B'_G = B' \cap B_G$ and $B'_A = B' \cap B_A$. Note that $|B'| \geq |B'_G| \geq (1-\beta/6)B_G$. Fix subset $S \subseteq [k]$. Next,

$$\begin{aligned}
\bar{p}_{B'}(S) - p(S) &= \frac{1}{|B'|}\sum_{b\in B'} \bar{\mu}_b(S) - p(S) = \frac{1}{|B'|}\sum_{b\in B'} (\bar{\mu}_b(S) - p(S)) \\
&= \frac{1}{|B'|}\sum_{b\in B'_G} (\bar{\mu}_b(S) - p(S)) + \frac{1}{|B'|}\sum_{b\in B'_A} (\bar{\mu}_b(S) - p(S)) \\
&= \frac{|B'_G|}{|B'|}(\bar{p}_{B'_G}(S) - p(S)) + \frac{1}{|B'|}\sum_{b\in B'_A} (\bar{\mu}_b(S) - p(S))
\end{aligned}$$

Therefore,

$$\begin{aligned}
|\bar{p}_{B'}(S) - p(S)| &\leq \frac{|B'_G|}{|B'|}|\bar{p}_{B'_G}(S) - p(S)| + \frac{1}{|B'|}\sum_{b\in B'_A} |\bar{\mu}_b(S) - p(S)| \\
&\overset{(a)}{\leq} \frac{\beta}{2}\sqrt{\frac{\ln(6e/\beta)}{n}} + \frac{1}{|B'|}\sum_{b\in B'_A} |\bar{\mu}_b(S) - p(S)| \\
&\overset{(b)}{\leq} \frac{\beta}{2}\sqrt{\frac{\ln(6e/\beta)}{n}} + \frac{1}{|B'|}\sqrt{|B'_A|\sum_{b\in B'_A} (\bar{\mu}_b(S) - p(S))^2} \\
&\overset{(c)}{\leq} \frac{\beta}{2}\sqrt{\frac{\ln(6e/\beta)}{n}} + \frac{1}{|B'|}\sqrt{|B'_A|\cdot(t+17+2\sqrt{t})\kappa_G} \\
&\overset{(d)}{\leq} \frac{\beta}{2}\sqrt{\frac{\ln(6e/\beta)}{n}} + \frac{1}{|B'|}\sqrt{|B'_A|\cdot(t+17+2\sqrt{t})\frac{\beta m\ln(6e/\beta)}{n}} \\
&\leq \frac{\beta}{2}\sqrt{\frac{\ln(6e/\beta)}{n}} + \sqrt{\frac{|B'_A|\cdot m}{|B'|^2}\cdot(t+17+2\sqrt{t})\frac{\beta\ln(6e/\beta)}{n}},
\end{aligned} \tag{14}$$

here in (a) uses Condition 2 and $|B'_G| \leq |B'|$, inequality (b) follows from the Cauchy-Schwarz inequality, inequality (c) uses Lemma 13, and (d) uses the definition of κ_G. Let $|B'_A| = |B_A| - \mathrm{D}$, for some $\mathrm{D} \in [0, |B_A|]$. Also from Lemma note that

$$|B'_G| \geq (1-\beta/6)|B_G| = |B_G| - |B_G|\beta/6 = |B_G| - m\beta(1-\beta)/6.$$

Therefore,

$$\begin{aligned}
\frac{|B'_A|\cdot m}{|B'|^2} = \frac{|B'_A|\cdot m}{(|B'_A| + |B'_G|)^2} &\leq \frac{(|B_A| - \mathrm{D})m}{(|B_A| - \mathrm{D} + |B_G| - m\beta(1-\beta)/6)^2} \\
&= \frac{(\beta m - \mathrm{D})m}{(m - \mathrm{D} - m\beta(1-\beta)/6)^2} \\
&\overset{(a)}{\leq} \frac{(\beta m - \mathrm{D})m}{(m - \mathrm{D} - 0.04m)^2} \\
&\overset{(b)}{\leq} \frac{\beta m^2}{(0.96m)^2} \leq \frac{\beta}{0.96^2},
\end{aligned}$$

here (a) follows since $\beta(1-\beta)$ takes maximum value at $\beta = 0.4$ in range $\beta \in (0, 0.4]$, and (b) follows since the expression is maximized at $\mathrm{D} = 0$.

Then combining above equation with (14) gives

$$|\bar{p}_{B'}(S) - p(S)| \leq \frac{\beta}{2}\sqrt{\frac{\ln(6e/\beta)}{n}} + \sqrt{(t+17+2\sqrt{t})\frac{\beta^2\ln(6e/\beta)}{0.96^2 n}}$$

$$\leq \Big(1/2 + \frac{1}{0.96}\sqrt{(t+17+2\sqrt{t})}\Big)\beta\sqrt{\frac{\ln(6e/\beta)}{n}} \tag{15}$$

$$\overset{(a)}{\leq} \Big(5+\sqrt{2.1t}\Big)\beta\sqrt{\frac{\ln(6e/\beta)}{n}}, \tag{16}$$

here inequality (a) uses the fact that $2t^{1/2} \leq t+1$ and $\sqrt{x^2+y^2} \leq |x|+|y|$. Finally, using the definition of L_1 distance between two distributions complete the proof of the Theorem. ■

B.2. Proof of Lemma 6

Proof. From the second statement in Lemma 5, each batch that gets removed is adversarial with probability ≥ 0.95. Batch deletion deletes more than $0.1\beta m$ good batches in total over all runs iff it samples $0.1\beta m$ good batches in first $0.1\beta m + |B_A|$ batches removed as otherwise all adversarial batches would have been exhausted already and Batch deletion algorithm would not remove batches any further. But the expected number of good batches sampled is $\leq 0.05(\times 0.1\beta m + |B_A|) \leq 0.005\beta m + 0.05\beta m < 0.06\beta m$.

Then using the Chernoff-bound, probability of sampling (removing) more than $0.1\beta m$ good batches in $0.1\beta m + |B_A|$ deletions is $\leq e^{-O(\beta m)} \leq e^{-O(k)}$. Hence, with high probability the algorithm deletes less than $0.1\beta m = 0.6\beta m/6 \leq |B_G|\beta/6$ batches. ■

B.3. Proof of Lemma 7

Proof. For the purpose of this proof, let $B'_G = B' \cap B_G$ and $B'_A = B' \cap B_A$. For batches b in a sub-collection B', the next equation relates the empirical variance of $\bar{\mu}_b(S)$ to sum of their squared deviation from $p(S)$.

$$\begin{aligned}
|B'|\overline{\mathrm{V}}_{B'}(S) &= \sum_{b\in B'}(\bar{\mu}_b(S) - \bar{p}_{B'}(S))^2 = \sum_{b\in B'}(\bar{\mu}_b(S) - p(S) - (\bar{p}_{B'}(S) - p(S)))^2 \\
&= \sum_{b\in B'}\Big((\bar{\mu}_b(S)-p(S))^2 + (\bar{p}_{B'}(S)-p(S))^2 - 2(\bar{p}_{B'}(S)-p(S))(\bar{\mu}_b(S)-p(S))\Big) \\
&= \sum_{b\in B'}(\bar{\mu}_b(S)-p(S))^2 + |B'|(\bar{p}_{B'}(S)-p(S))^2 - 2(\bar{p}_{B'}(S)-p(S))\sum_{b\in B'}(\bar{\mu}_b(S)-p(S)) \\
&= \sum_{b\in B'}(\bar{\mu}_b(S)-p(S))^2 + |B'|(\bar{p}_{B'}(S)-p(S))^2 - 2(\bar{p}_{B'}(S)-p(S))(|B'|\bar{p}_{B'}(S) - |B'|p(S)) \\
&= \sum_{b\in B'}(\bar{\mu}_b(S)-p(S))^2 - |B'|(\bar{p}_{B'}(S)-p(S))^2 \\
&= \sum_{b\in B'_A}(\bar{\mu}_b(S)-p(S))^2 + \sum_{b\in B'_G}(\bar{\mu}_b(S)-p(S))^2 - |B'|(p(S)-\bar{p}_{B'}(S))^2.
\end{aligned} \tag{17}$$

The next set of inequalities lead to the upper bound in the Lemma.

$$\begin{aligned}
&|B'|(\overline{\mathrm{V}}_{B'}(S) - \mathrm{V}(\bar{p}_{B'}(S))) \\
&\overset{(a)}{=} \sum_{b\in B'_A}(\bar{\mu}_b(S)-p(S))^2 + \sum_{b\in B'_G}(\bar{\mu}_b(S)-p(S))^2 - |B'|(p(S)-\bar{p}_{B'}(S))^2 - |B'|\mathrm{V}(\bar{p}_{B'}(S)) \\
&\overset{(b)}{\leq} (t+17+2\sqrt{t})\kappa_G + |B'_G|\mathrm{V}(p(S)) + |B'_G|\frac{6\beta\ln(\frac{6e}{\beta})}{n} - |B'|\mathrm{V}(\bar{p}_{B'}(S)) \\
&\overset{(c)}{\leq} (t+17+2\sqrt{t})\kappa_G + 6\beta m\frac{\ln(6e/\beta)}{n} + |B'|\mathrm{V}(p(S)) - |B'|\mathrm{V}(\bar{p}_{B'}(S)) \\
&\overset{(d)}{\leq} (t+23+2\sqrt{t})\kappa_G + m\frac{|p(S)-\bar{p}_{B'}(S)|}{n},
\end{aligned}$$

here inequality (a) follows from (17), (b) follows from Lemma 13 and condition 2, and (c) follows since $|B'_G| \leq |B'|$ and $\mathrm{V}(\cdot) \geq 0$, and inequality (d) uses (1) and $|B'| \leq m$. Next, from equation (16) we have,

$$|\bar{p}_{B'}(S) - p(S)| \leq (5+\sqrt{2.1t})\beta\sqrt{\frac{\ln(6e/\beta)}{n}}$$

$$= (5+\sqrt{2.1t})\beta\ln(6e/\beta)\sqrt{\frac{1}{n\ln(6e/\beta)}}$$
$$\leq (5+\sqrt{2.1t})\frac{n\kappa_G}{m}. \tag{18}$$

Combining the above two equations gives the upper bound in the lemma.

Next showing the lower bound,

$$\begin{aligned}
&|B'|(\overline{\mathrm{V}}_{B'}(S)-\mathrm{V}(\bar{p}_{B'}(S)))\\
&\overset{(a)}{=}\sum_{b\in B'_A}(\bar{\mu}_b(S)-p(S))^2+\sum_{b\in B'_G}(\bar{\mu}_b(S)-p(S))^2-|B'|(p(S)-\bar{p}_{B'}(S))^2-|B'|\mathrm{V}(\bar{p}_{B'}(S))\\
&\overset{(b)}{\geq}(t-3-2\sqrt{t})\kappa_G+|B'_G|\mathrm{V}(p(S))-|B'_G|\frac{6\beta\ln(\frac{6e}{\beta})}{n}-|B'|(p(S)-\bar{p}_{B'}(S))^2-|B'|\mathrm{V}(\bar{p}_{B'}(S))\\
&\geq(t-9-2\sqrt{t})\kappa_G+|B'_G|\mathrm{V}(p(S))-|B'|(p(S)-\bar{p}_{B'}(S))^2-|B'_G|\mathrm{V}(\bar{p}_{B'}(S))-|B'_A|\mathrm{V}(\bar{p}_{B'}(S))\\
&\geq(t-9-2\sqrt{t})\kappa_G-|B'_G|(\mathrm{V}(\bar{p}_{B'}(S))-\mathrm{V}(p(S)))-|B'|(p(S)-\bar{p}_{B'}(S))^2-|B'_A|\mathrm{V}(\bar{p}_{B'}(S))\\
&\overset{(c)}{\geq}(t-9-2\sqrt{t})\kappa_G-|B'_G|\frac{|p(S)-\bar{p}_{B'}(S)|}{n}-\frac{|B'_A|}{4n}-|B'|(p(S)-\bar{p}_{B'}(S))^2\\
&\geq(t-9-2\sqrt{t})\kappa_G-m\frac{|p(S)-\bar{p}_{B'}(S)|}{n}-\frac{\beta m}{4n}-m(p(S)-\bar{p}_{B'}(S))^2\\
&\overset{(d)}{\geq}(t-15-2\sqrt{t}-\sqrt{2.1t})\kappa_G-m(p(S)-\bar{p}_{B'}(S))^2,
\end{aligned}$$

here inequality (a) follows from (17), (b) follows from Lemma 13 and condition 2, (c) follows from (1) and $\mathrm{V}(\cdot)\leq\frac{1}{4n}$, and inequality (d) follows from (18).

Next, we bound the last tem in the above equation to complete the proof. From equation (15),

$$\begin{aligned}
(p(S)-\bar{p}_{B'}(S))^2&\leq\Big(1/2+\frac{1}{0.96}\sqrt{(t+17+2\sqrt{t})}\Big)^2\beta^2\frac{\ln(6e/\beta)}{n}\\
&\leq\Big(1/4+\frac{1}{0.96^2}(t+17+2\sqrt{t})+\frac{1}{0.96}\sqrt{(t+17+2\sqrt{t})}\Big)\beta\cdot\kappa_G\\
&\overset{(a)}{\leq}\Big(1/4+1.1(t+17+2\sqrt{t})+5+\sqrt{2.1t}\Big)\beta\cdot\kappa_G\\
&\leq\Big(24+1.1t+2.2\sqrt{t}+\sqrt{2.1t}\Big)\beta\cdot\kappa_G\\
&\overset{(b)}{\leq}0.4\Big(24+1.1t+2.2\sqrt{t}+\sqrt{2.1t}\Big)\kappa_G,
\end{aligned}$$

here inequality (a) uses the fact that $2t^{1/2}\leq t+1$ and $\sqrt{x^2+y^2}\leq|x|+|y|$ and inequality (b) uses $\beta\leq 0.4$. Combining above two equations give us the lower bound in the Lemma. ■

C. Proof of Theorem 9

First, we restate the statement of the main theorem.

Theorem 14. *Suppose the conditions 1- 3 holds. Then Algorithm 2 runs in polynomial time and with probability* $\geq 1-O(e^{-k})$ *returns a sub-collection* $B'_f\subseteq B$ *such that* $|B'_f\cap B_G|\geq(1-\frac{\beta}{6})|B_G|$ *and for* $p^*=\bar{p}_{B'_f}$,

$$||p^*-p||_1\leq 100\beta\sqrt{\frac{\ln(6e/\beta)}{n}}.$$

Proof. Lemma 6 show that for the sub-collection B'_i at each iteration i, $|B'_i\cap B_G|\geq(1-\frac{\beta}{6})|B_G|$, hence, for sub-collection B'_f returned by the algorithm $|B'_f\cap B_G|\geq(1-\frac{\beta}{6})|B_G|$, with probability $\geq 1-O(e^{-k})$. This also implies that the total number of deleted batches are $<(1+1/6)\beta m$.

To complete the proof of the above Theorem, we state the following corollary, which is a direct consequence of Lemma 7.

Corollary 15. *Suppose the conditions 1- 3 holds. Then following hold for any $B' \subseteq B$ such that $|B' \cap B_G| \geq (1 - \frac{\beta}{6})|B_G|$.*

1. $|\overline{V}_{B'}(S) - V(\bar{p}_{B'}(S))| \geq 75\kappa_G$ *implies that* $\psi(B', S) \geq 25\kappa_G$.
2. $|\overline{V}_{B'}(S) - V(\bar{p}_{B'}(S))| \leq 150\kappa_G$ *implies that* $\psi(B', S) \leq 900\kappa_G$.

In each iteration of Algorithm 2, except the last, $Detection - Algorithm$ returns a subset for which the difference between two variance estimate is $\geq 75\kappa_G$. The first statement in the above corollary implies that corruption is high for this subset. Batch Deletion removes batches from the sub-collection to reduce the corruption for such subset. From Statement 3 of Lemma 5, in each iteration Batch Deletion removes $\geq 25\kappa_G - 20\kappa_G$ batches. Since the total batches removed are $< 7/6\beta m$, this implies that the algorithm runs for at-max $\frac{7\beta m}{6\times 5\kappa_G} < n$ iterations.

The algorithm terminates when $Detection - Algorithm$ returns a subset for which the difference between two variance estimate is $\leq 75\kappa_G$. Then Lemma 8 implies that the difference between two variance estimate is $\leq 150\kappa_G$ for all subsets. Then the above corollary shows that corruption for all subsets is $\leq 900\kappa_G$. Therefore, $\psi(B') \leq 900\kappa_G$. Then Lemma 4 bounds the L_1 distance. ■

D. Proof of Theorem 2

We restate the theorem and give a short proof.

Theorem 16. *For any given $\beta \leq 0.4$, n and k and m, Algorithm 2 runs in polynomial time, and its estimate p^* satisfies $||p^* - p||_1 \leq O(\max\{\beta\sqrt{\frac{\ln(1/\beta)}{n}}, \sqrt{\frac{k}{mn}}\})$ with probability $\geq 1 - O(e^{-k})$.*

Proof. First we prove the theorem for $m \geq \Omega(k)$. We further divide it into two case depending on number of batches, m.

1. When the number of batches $m \geq \Omega\Big(\frac{k}{\beta^2 \log(1/\beta)}\Big)$, then Theorem 1 implies the above result.
2. When the number of batches $m \leq \mathcal{O}(\frac{k}{\beta^2 \log(1/\beta)})$, then let β_* such that $m = \Theta\Big(\frac{k}{\beta_*^2 \log(1/\beta_*)}\Big)$. Clearly, $\beta_* \gg \beta$. From Theorem 1, the algorithm would achieve a distance $O\Big(\beta_*\sqrt{\frac{\log(1/\beta_*)}{n}}\Big) = O\Big(\sqrt{\frac{k}{nm}}\Big)$.

This proves the theorem for $m \geq \Omega(k)$.

For $m \leq \mathcal{O}(k)$, there are two possibilities depending on the total number of samples, mn.

1. When $mn \leq \mathcal{O}(k)$, one cannot learn the distribution, hence the L_1 error is $= \Omega(1)$, and the guarantees of the theorem trivially hold.
2. When $mn \geq \Omega(k)$, divide each of the m batches into $\Theta(k/m)$ smaller batches so that there are $m' = \Theta(k)$ batches of $n' = \Theta(mn/k)$ samples each. This operation preserves the fraction β of adversarial batches. Since we already proved the theorem for $m' > \Omega(k)$, applying this result for the updated batches yields the following bound:

$$\begin{aligned}
&\max\{\beta \cdot \sqrt{\frac{\log(1/\beta)}{n'}}, \sqrt{\frac{k}{m'n'}}\} \\
&= \max\{\beta \cdot \sqrt{\frac{k \cdot \log(1/\beta)}{mn}}, \sqrt{\frac{k}{mn}}\} \\
&= \sqrt{\frac{k}{mn}} \\
&\leq \max\{\beta \cdot \sqrt{\frac{\log(1/\beta)}{n}}, \sqrt{\frac{k}{mn}}\},
\end{aligned}$$

   where the second equality follows as $\beta < 1/2$ implies $\beta \cdot \sqrt{\log(1/\beta)} < 1$.

Thereby proving the theorem for the $m \leq \mathcal{O}(k)$ range. ■