8 Proofs

Proposition 1. *Let $\hat{\mu}$ be defined as in Eq.(3). If Eq.(4) is satisfied for some $\zeta \in (0,1)$ and $c > 0$, then*

$$\Pr\left[|\hat{\mu} - \mathbb{E}[Y]| > r + \frac{Z_{(m-k)} - Z_{(1+k)}}{2}\right] \leq \zeta. \quad (5)$$

Proof of Proposition 1. Whenever $\mathbb{E}[Z] \leq Z_{(m-k)} + r$ and $\mathbb{E}[Z] \geq Z_{(1+k)} - r$, we have

$$\begin{aligned}|\hat{\mu} - \mathbb{E}[Y]| &= \left|\mathbb{E}[Z] - \frac{Z_{(m-k)} + Z_{(1+k)}}{2}\right| \\ &= \max\left(\mathbb{E}[Z] - \frac{Z_{(m-k)} + Z_{(1+k)}}{2}, \right. \\ &\qquad \left. \frac{Z_{(m-k)} + Z_{(1+k)}}{2} - \mathbb{E}[Z]\right) \\ &\leq \max\left(Z_{(m-k)} + r - \frac{Z_{(m-k)} + Z_{(1+k)}}{2}, \right. \\ &\qquad \left. \frac{Z_{(m-k)} + Z_{(1+k)}}{2} - Z_{(1+k)} + r\right) \\ &= \frac{Z_{(m-k)} - Z_{(1+k)}}{2} + r\end{aligned}$$

In other words, we cannot have

$$|\hat{\mu} - \mathbb{E}[Y]| > \frac{Z_{(m-k)} - Z_{(1+k)}}{2} + r$$

unless either $\mathbb{E}[Z] > Z_{(m-k)} + r$ or $\mathbb{E}[Z] < Z_{(1+k)} - r$ is true, which implies that

$$\begin{aligned}&\Pr\left[|\hat{\mu} - \mathbb{E}[Y]| > r + \frac{Z_{(m-k)} - Z_{(1+k)}}{2}\right] \\ &\leq \Pr[\mathbb{E}[Z] > Z_{(m-k)} + r \text{ or } \mathbb{E}[Z] < Z_{(1+k)} - r] \\ &\leq \Pr[\mathbb{E}[Z] > Z_{(m-k)} + r] + \Pr[\mathbb{E}[Z] < Z_{(1+k)} - r] \\ &\leq \zeta\end{aligned}$$

□

Theorem 1. *Let $Z_{(1)}, \ldots, Z_{(m)}$ denote the order statistics of m independent samples of a random variable Z. If Z is s-resilient, $\forall \zeta \in (0,1), T \in \mathbb{N}$ and $0 \leq k < m/2$, then letting r be the output of Algorithm 1, we have*

$$\Pr\left[Z_{(m-k)} \leq \mathbb{E}[Z] - r\right] \leq \zeta \quad (6)$$

$$\Pr\left[Z_{(1+k)} \geq \mathbb{E}[Z] + r\right] \leq \zeta \quad (7)$$

If Z is s-resilient from above/below, then only Eq.(6)/Eq.(7) holds.

Proof of Theorem 1. Before proving Theorem 1, we first need a Lemma.

Lemma 2. *If Z is s-resilient from above, then $\forall \delta \in (0,1)$,*

$$\Pr\left[Z \leq \mathbb{E}[Z] - s(\delta)\frac{1-\delta}{\delta}\right] \leq \delta.$$

For some $r \in \mathbb{R}$, let B_r be the event $Z \leq \mathbb{E}[Z] - r$.

$$\begin{aligned}&\Pr\left[Z_{(m-k)} \leq \mathbb{E}[Z] - r\right] \\ &= \Pr\left[\sum_{j=0}^{m} \mathbb{I}(Z_j \notin B_r) \leq k\right] \\ &= \sum_{i=0}^{k} \binom{m}{i} \Pr[B_r]^{m-i}(1 - \Pr[B_r])^i \quad (8) \\ &\leq \left(\sum_{i=0}^{k} \binom{m}{i}(1 - \Pr[B_r])^i\right) \Pr[B_r]^{m-k} \\ &\leq \left(\sum_{i=0}^{k}(m(1 - \Pr[B_r]))^i\right) \\ &\leq (m(1 - \Pr[B_r]) + 1)^k \Pr[B_r]^{m-k}\end{aligned}$$

Now we will show that the algorithm chooses v_i, $i = 0, \ldots, T$ such that

$$(m(1 - v_i) + 1)^k v_i^{m-k} \leq \zeta \quad (9)$$

To show this we first show that $v_{i+1} \geq v_i$, $\forall i = 0, \ldots, T-1$. This is obviously true for $i = 0$ because $0 \leq v_0 \leq 1$ so

$$\begin{aligned}v_0 &= \left(\frac{\zeta}{(m+1)^k}\right)^{\frac{1}{m-k}} \\ &\leq \left(\frac{\zeta}{(m(1-v_0)+1)^k}\right)^{\frac{1}{m-k}} = v_1\end{aligned}$$

and we can proceed to use induction and conclude

$$\begin{aligned}v_i &= \left(\frac{\zeta}{(m(1-v_{i-1})+1)^k}\right)^{\frac{1}{m-k}} \\ &\leq \left(\frac{\zeta}{(m(1-v_i)+1)^k}\right)^{\frac{1}{m-k}} = v_{i+1}\end{aligned}$$

Now we use induction to show that Eq.(9) is true. First at iteration 0 this is true because

$$(m(1 - v_0) + 1)^k v_0^{m-k} \leq (m+1)^k v_0^{m-k}$$

which is less than ζ as long as

$$v_0 \leq \left(\frac{\zeta}{(m+1)^k}\right)^{\frac{1}{m-k}}$$

Suppose Eq.(9) is true at iteration i, then at iteration $i+1$ it is still true. Denote the values as v_i and v_{i+1}. Because we choose v_{i+1} such that

$$(m(1 - v_i) + 1)^k v_{i+1}^{m-k} = \zeta$$

Observe that $v_{i+1} \geq v_i$ it must be true that

$$(m(1 - v_{i+1}) + 1)^k v_{i+1}^{m-k} \leq \zeta$$

After we have established Eq.(9) we can apply Lemma 2 to achieve $\Pr[B_r] \leq v$ it suffices to have

$$r \geq s(v)\left(v^{-1} - 1\right)$$

What remains is to prove Lemma 2

Proof of Lemma 2. Let B_r be the event $Z \leq \mathbb{E}[Z] - r$ for any $r \geq 0$. Suppose it is true that $\Pr[B_r] = \delta_r$ for some $\delta_r \in (0, 1)$, we have

$$\begin{aligned}\mathbb{E}[Z] &= \mathbb{E}[Z|B_r]\Pr[B_r] + \mathbb{E}[Z|\bar{B}_r](1 - \Pr[B_r]) \\ &\leq (\mathbb{E}[Z] - r)\delta_r + (\mathbb{E}[Z] + s(\delta_r))(1 - \delta_r)\end{aligned}$$

which implies that

$$r \leq s(\delta_r)\frac{1 - \delta_r}{\delta_r}$$

which implies

$$\Pr\left[Z \leq \mathbb{E}[Z] - s(\delta)\frac{1 - \delta}{\delta}\right] \leq \delta$$

□

□

Corollary 1. *If Z is $b_1(1-\epsilon)^a + b_2$ resilient for any constants $a \in [-1, 0]$ and $b_1, b_2 \in \mathbb{R}^+$, then there exists $\lambda > 0$ such that for sufficiently large m*

$$\Pr\left[\mathbb{E}[Z] \leq Z_{(1+k)} - \lambda\frac{\log\frac{1}{\zeta} + k\log m}{m^{1+a}}\right] \leq \zeta$$
$$\Pr\left[\mathbb{E}[Z] \geq Z_{(m-k)} + \lambda\frac{\log\frac{1}{\zeta} + k\log m}{m^{1+a}}\right] \leq \zeta.$$

Proof of Corollary 1. Denote $\epsilon = \left(\frac{\zeta}{(m+1)^k}\right)^{\frac{1}{m-k}}$. We know that

$$\lim_{m\to\infty} \log\epsilon = \frac{1}{m-k}\left(\log\zeta - k\log(m+1)\right) = 0$$

which implies $\lim_{m\to\infty}\epsilon = 1$, so $\forall a < 0$ there must exist a M such that $\forall m \geq M$, $(1-\epsilon)^a + b \leq 2(1-\epsilon)^a$, and $\epsilon > 1/2$

$$r \leq 2(1-\epsilon)^a(\epsilon^{-1} - 1) = \frac{2(1-\epsilon)^{1+a}}{\epsilon} \leq 4(1-\epsilon)^{1+a}$$

Observe that $\epsilon < 1$ so $1 - \epsilon < -\log\epsilon$ so we have (for sufficiently large m)

$$\begin{aligned} r &\leq 4(-\log\epsilon)^{1+a} \\ &= 4\left(-\frac{1}{m-k}\log\zeta + \frac{k}{m-k}\log(m+1)\right)^{1+a} \\ &\leq \frac{5}{m^{1+a}}\left(\log\frac{1}{\zeta} + k\log m\right)^{1+a} \\ &\leq \frac{5}{m^{1+a}}\left(\log\frac{1}{\zeta} + k\log m\right)\end{aligned}$$

Now we only need the special case of $a = 0$, where

$$r \leq (1+b)(\epsilon^{-1} - 1) \leq 2(1+b)(1-\epsilon)$$

and the proof will follow as before. □

Lemma 1. *The following random variables are resilient:*

1. ***Bounded:*** *If $\mathcal{Z} \subseteq [a, b]$, then Z is $(b - \mathbb{E}[Z])$-resilient from above and $(\mathbb{E}[Z] - a)$-resilient from below. It is $(b-a)$-resilient.*
2. ***Bounded Moments:*** *If $\mathbb{E}\left[|Z - \mathbb{E}[Z]|^l\right] \leq \sigma^l$ for some $l > 1$, then Z is s-resilient for $s(\epsilon) = \frac{\sigma}{(1-\epsilon)^{1/l}}$.*
3. ***Sub-Gaussian:*** *If $Z - \mathbb{E}[Z]$ is σ^2 sub-Gaussian, then Z is s-resilient for $s(\epsilon) = \sqrt{2\sigma\log\frac{1}{1-\epsilon}} + \sqrt{2\pi}\sigma$.*

Proof of Lemma 1. Part 1 is trivial to prove. Part 2 is proved in Steinhardt (2018), Example 2.7. Part 3 is proven here.

Let F denote the CDF of Z. For convenience, let $\bar{\epsilon} = 1 - \epsilon$, $\tau = F^{-1}(\bar{\epsilon})$, and without loss of generality assume $\mathbb{E}[Z] = 0$. We first consider lower bounds on $\mathbb{E}[Z \mid Z \in B]$ where B is any subset of $\mathcal{Z}$ such that $\Pr[Z \in B] \geq \bar{\epsilon}$. It is easy to see that for any such B we have

$$\mathbb{E}[Z \mid Z \leq \tau] \leq \mathbb{E}[Z \mid Z \in B]$$

so we only have to provide a lower bound for $\mathbb{E}[Z \mid Z \leq \tau]$. Without loss of generality we can also assume $\tau \leq 0$ because suppose $\tau > 0$ then consider an alternative random variable $\tilde{Z}$ defined by $\tilde{Z} = \max(Z, 0)$. Then $\tilde{Z}$ is σ^2 sub-Gaussian, and

$$\mathbb{E}[Z \mid Z \leq \tau] \geq \mathbb{E}[\tilde{Z} \mid \tilde{Z} \leq \tau]$$

Then we can provide a lower bound for $\mathbb{E}[\tilde{Z} \mid \tilde{Z} \leq \tau]$

instead. Given the above setup we have

$$\begin{aligned}
&\bar\epsilon\,\mathbb{E}[Z|Z\le\tau]\\
&=\int_{x=-\infty}^{\tau} xF'(x)\,dx=\int_{x=-\infty}^{\tau}F'(x)\int_{y=x}^{0}(-1)\,dy\,dx\\
&=-\int_{x=-\infty}^{\tau}\int_{y=x}^{0}F'(x)\,dy\,dx\\
&=-\int_{x=-\infty}^{\tau}\int_{y=-\infty}^{0}\mathbb{I}(y>x)F'(x)\,dy\,dx\\
&=-\int_{y=-\infty}^{0}\int_{x=-\infty}^{\tau}\mathbb{I}(y>x)F'(x)\,dx\,dy\\
&=-\int_{y=\tau}^{0}\int_{x=-\infty}^{\tau}\mathbb{I}(y>x)F'(x)\,dx\,dy\\
&\qquad-\int_{y=-\infty}^{\tau}\int_{x=-\infty}^{\tau}\mathbb{I}(y>x)F'(x)\,dx\,dy\\
&=-\int_{y=\tau}^{0}\bar\epsilon\,dy-\int_{y=-\infty}^{\tau}\int_{x=-\infty}^{y}F'(x)\,dx\,dy\\
&=\bar\epsilon\tau-\int_{y=-\infty}^{\tau}F(y)\,dy\\
&=\bar\epsilon\tau-\int_{x=-\infty}^{\tau}F(x)\,dx
\end{aligned}$$

Let $\tilde F(x)=e^{-\frac{x^2}{2\sigma^2}}$. Since Z is σ^2 sub-Gaussian, by Chernoff bound we know that $\forall x<0$. $F(x)\le\tilde F(x)$, which also implies that whenever $F^{-1}(\bar\epsilon)<0$, $\tilde F^{-1}(\bar\epsilon)\le F^{-1}(\bar\epsilon)$, Then

$$\begin{aligned}
&\bar\epsilon\mathbb{E}[Z|Z\le F^{-1}(\bar\epsilon)]\\
&=\bar\epsilon F^{-1}(\bar\epsilon)-\int_{x=-\infty}^{F^{-1}(\bar\epsilon)}F(x)dx\\
&=\bar\epsilon F^{-1}(\bar\epsilon)-\int_{x=-\infty}^{\tilde F^{-1}(\bar\epsilon)}F(x)dx-\int_{x=\tilde F^{-1}(\bar\epsilon)}^{F^{-1}(\bar\epsilon)}F(x)dx\\
&\ge\bar\epsilon F^{-1}(\bar\epsilon)-\int_{x=-\infty}^{\tilde F^{-1}(\bar\epsilon)}\tilde F(x)dx-\int_{x=\tilde F^{-1}(\bar\epsilon)}^{F^{-1}(\bar\epsilon)}\bar\epsilon dx\\
&=\bar\epsilon\tilde F^{-1}(\bar\epsilon)-\int_{x=-\infty}^{\tilde F^{-1}(\bar\epsilon)}\tilde F(x)dx
\end{aligned}$$

Finally, denote $\phi_\sigma(x)$ as the PDF of $\mathcal{N}(0,\sigma^2)$ and Φ_σ be its CDF, we have

$$\begin{aligned}
\int_{x=-\infty}^{\tilde F^{-1}(\bar\epsilon)}\tilde F(x)dx&=\sqrt{2\pi}\sigma\int_{x=-\infty}^{\tilde F^{-1}(\bar\epsilon)}\phi_\sigma(x)dx\\
&=\sqrt{2\pi}\sigma\Phi_\sigma(\tilde F^{-1}(\bar\epsilon))\le\sqrt{2\pi}\sigma\bar\epsilon
\end{aligned}$$

Combining these results we get

$$\begin{aligned}
&\mathbb{E}[Z|Z\le F^{-1}(\bar\epsilon)]\\
&\ge\tilde F^{-1}(\bar\epsilon)-\sqrt{2\pi}\sigma=-\sqrt{2\sigma\log\frac{1}{\bar\epsilon}}-\sqrt{2\pi}\sigma
\end{aligned}$$

□

Corollary 2. *Let $Z_{(1)},\dots,Z_{(m)}$ denote the order statistics of m independent samples of a random variable Z. If Z is bounded in $[a,b]$, $\forall\zeta\in(0,1),T\in\mathbb{N}$ and $0\le k<m/2$, then letting v_T be computed as in Algorithm 1, we have*

$$\begin{aligned}
\Pr\left[\mathbb{E}[Z]\le a+v_T(Z_{(1+k)}-a)\right]\le\zeta\\
\Pr\left[\mathbb{E}[Z]\ge b-v_T(b-Z_{(m-k)})\right]\le\zeta.
\end{aligned}$$

Proof of Corollary 2. By Theorem 1 we have

$$\begin{aligned}
\zeta&\ge\Pr\left(Z_{(1+k)}\ge\mathbb{E}[Z]+(\mathbb{E}[Z]-a)(v_T^{-1}-1)\right)\\
&=\Pr\left(Z_{(1+k)}\ge v_T^{-1}\mathbb{E}[Z]-v_T^{-1}a+a\right)\\
&=\Pr\left(v_TZ_{(1+k)}\ge v_Ta-a+\mathbb{E}[Z]\right)\\
&=\Pr\left(\mathbb{E}[Z]\le a+v_T(Z_{(1+k)}-a)\right)
\end{aligned}$$

Similarly we can conclude

$$\zeta\ge\Pr\left(\mathbb{E}[Z]\ge b-v_T(b-Z_{(m-k)})\right)$$

□

Theorem 2. *Let $Z_{(1)},\dots,Z_{(m)}$ be independent samples of Z ordered such that $\|Z_{(1)}\|\le\dots\le\|Z_{(m)}\|$. If Z is s-resilient, then for any r output by Algorithm 1 and for any $\zeta\in(0,1)$, we have*

$$\Pr\left[\|Z_{(m-k)}\|\le\|\mathbb{E}[Z]\|-r\right]\le\zeta.$$

Proof of Theorem 2. Let

$$v^*=\operatorname*{arg\,sup}_{v,\|v\|_*=1}\langle v,\mathbb{E}[Z]\rangle$$

then $\|\mathbb{E}[Z]\|=\langle v^*,\mathbb{E}[Z]\rangle$. Let $\tilde Z_{(1)},\dots,\tilde Z_{(m)}$ be ranked such that

$$\langle v^*,\tilde Z_{(1)}\rangle\le\ldots\le\langle v^*,Z_{(m)}\rangle.$$

Denote the event $B\subset\mathcal{Z}$ as $\{Z,\langle v^*,Z\rangle\le\langle v^*,\mathbb{E}[Z]\rangle-r\}$ as before we have

$$\Pr\left[\langle v^*,\tilde Z_{(m-k)}\rangle\le\langle v^*,\mathbb{E}[Z]\rangle-r\right]\le(m+1)^k\Pr[B]^{m-k}$$

and we set the RHS $\le\zeta$. It suffices to have

$$\Pr[B]\le\left(\frac{\zeta}{(m+1)^k}\right)^{\frac{1}{m-k}}$$

Similar to Lemma 2, denote $\delta=\Pr[B]$

$$\begin{aligned}
&\langle v^*,\mathbb{E}[Z]\rangle=\mathbb{E}[\langle v^*,Z\rangle]\\
&=\mathbb{E}[\langle v^*,Z\rangle\mid B]\Pr[B]+\mathbb{E}[\langle v^*,Z\rangle\mid\bar B](1-\Pr[B])\\
&\le(\langle v^*,\mathbb{E}[Z]\rangle-r)\delta+(\langle v^*,\mathbb{E}[Z]\rangle+s(\delta))(1-\delta)
\end{aligned}$$

which implies that $\Pr[B] \leq \delta$ when $r \geq s(\delta)\frac{1-\delta}{\delta} = s(\delta)(\delta^{-1} - 1)$. When this is true we have

$$\Pr[\langle v^*, \tilde{Z}_{(m-k)} \rangle \leq \|\mathbb{E}[Z]\| - r] \leq \zeta$$

If we also rank $Z_{(1)}, \ldots, Z_{(m)}$ by

$$\|Z_{(1)}\| \leq \cdots \leq \|Z_{(m)}\|$$

we have $\forall i \geq m - k$

$$\langle v^*, \tilde{Z}_{(m-k)} \rangle \leq \langle v^*, \tilde{Z}_{(i)} \rangle \leq \|\tilde{Z}_{(i)}\|$$

so there are at least k samples $Z_{(i)}$ with norm at least $\langle v^*, \tilde{Z}_{(m-k)} \rangle$, and we can conclude that $\langle v^*, \tilde{Z}_{(m-k)} \rangle \leq \|Z_{(m-k)}\|$ which implies

$$\Pr[\|Z_{(m-k)}\| \leq \|\mathbb{E}[Z]\| - r] \leq \zeta$$

□