1 Useful versions of the Ahlswede-Winter Inequality

**Theorem 1** Let $Y$ be a random, symmetric, positive semi-definite $d \times d$ matrix such that $E[Y] = I$. Suppose $\|Y\| \leq R$ for some fixed scalar $R \geq 1$. Let $Y_1, \ldots, Y_k$ be independent copies of $Y$ (i.e., independently sampled matrices with the same distribution as $Y$). For any $\epsilon \in (0, 1)$, we have
\[
\Pr \left[ (1 - \epsilon)I \preceq \frac{1}{k} \sum_{i=1}^{k} Y_i \preceq (1 + \epsilon)I \right] \geq 1 - 2d \cdot \exp(-\epsilon^2 k / 4R).
\]
This event is equivalent to the sample average $\frac{1}{k} \sum_{i=1}^{k} Y_i$ having minimum eigenvalue at least $1 - \epsilon$ and maximum eigenvalue at most $1 + \epsilon$.

**Proof:** We apply the Ahlswede-Winter inequality with $X_i = (Y_i - E[Y_i]) / R$. Note that $E[X_i] = 0$, $\|X_i\| \leq 1$, and
\[
E[X_i^2] = \frac{1}{R^2} E[(Y_i - E[Y_i])^2] = \frac{1}{R^2} \left( E[Y_i^2] - 2E[Y_i]^2 + E[Y_i]^2 \right) \leq \frac{1}{R^2} E[Y_i^2] \quad \text{(since $E[Y_i]^2 \geq 0$)} \leq \frac{1}{R^2} E[\|Y_i\| \cdot Y_i] \leq \frac{R}{R^2} E[Y_i].
\]
Finally, since $0 \preceq E[Y_i] \preceq I$, we get
\[
\lambda_{\max}(E[X_i^2]) \leq 1 / R. \tag{1}
\]
Now we use Claim 15 from the Notes on Symmetric Matrices, together with the inequalities
\[
1 + x \leq e^x \quad \forall x \in \mathbb{R} \quad \text{and} \quad e^x \leq 1 + x + x^2 \quad \forall x \in [-1, 1].
\]
Since $\|X_i\| \leq 1$, for any $\lambda \in [0, 1]$, we have $e^{\lambda X_i} \preceq I + \lambda X_i + \lambda^2 X_i^2$, and so
\[
E[e^{\lambda X_i}] \preceq E[I + \lambda X_i + \lambda^2 X_i^2] \preceq I + \lambda^2 E[X_i^2] \preceq e^{\lambda^2 E[X_i^2]}.
\]
Thus by (1) we have
\[
\|E[e^{\lambda X_i}]\| \leq \|e^{\lambda^2 E[X_i^2]}\| \leq e^{\lambda^2 / R}.
\]
The same analysis also shows that $\|E[e^{-\lambda X_i}]\| \leq e^{\lambda^2 / R}$. Substituting these two bounds into the basic Ahlswede-Winter inequality from the previous lecture, we obtain
\[
\Pr \left[ \left\| \frac{1}{R} \sum_{i=1}^{k} (Y_i - E[Y_i]) \right\| > t \right] \leq 2d \cdot e^{-\lambda t} \prod_{i=1}^{k} e^{\lambda^2 / R} = 2d \cdot \exp(-\lambda t + k\lambda^2 / R).
\]
Substituting \( t = k\epsilon / R \) and \( \lambda = \epsilon / 2 \) we get

\[
\Pr \left[ \left\| \frac{1}{R} \sum_{i=1}^{k} Y_i - \frac{k}{R} \mathbb{E}[Y_i] \right\| > \frac{k\epsilon}{R} \right] \leq 2d \cdot \exp\left(-\frac{k\epsilon^2}{4R}\right). 
\]

Multiplying by \( R/k \) and using the fact that \( \mathbb{E}[Y_i] = I \), we have bounded the probability that any eigenvalue of the sample average matrix \( \sum_{i=1}^{k} Y_i / k \) is less than \( 1 - \epsilon \) or greater than \( 1 + \epsilon \).

**Corollary 2** Let \( Z \) be a random, symmetric, positive semi-definite \( d \times d \) matrix. Define \( U := \mathbb{E}[Z] \) and suppose \( Z \preceq R \cdot U \) for some scalar \( R \geq 1 \). Let \( Z_1, \ldots, Z_k \) be independent copies of \( Z \). For any \( \epsilon \in (0, 1) \), we have

\[
\Pr \left[ (1 - \epsilon) U \preceq \frac{1}{k} \sum_{i=1}^{k} Z_i \preceq (1 + \epsilon) U \right] \geq 1 - 2d \cdot \exp\left(-\frac{\epsilon^2}{4R}\right). 
\]

**Proof:** Let \( U^{+/2} := (U^+)^{1/2} \) denote the square root of the pseudoinverse of \( U \). Let \( \text{im}(U) \) denote the orthogonal projection on the image of \( U \). Define the random, positive semi-definite matrices

\[
Y := U^{+/2} \cdot Z \cdot U^{+/2} \quad \text{and} \quad Y_i := U^{+/2} \cdot Z_i \cdot U^{+/2}.
\]

Because \( Z_i \succeq 0 \) and \( U = \mathbb{E}[\sum_i Z_i] \), we have \( \text{im}(Z_i) \subseteq \text{im}(U) \). So Claim 16 in [Notes on Symmetric Matrices](#) implies

\[
(1 - \epsilon)U \preceq \frac{1}{k} \sum_{i=1}^{k} Z_i \preceq (1 + \epsilon)U \quad \iff \quad (1 - \epsilon)\text{im}(U) \preceq \frac{1}{k} \sum_{i=1}^{k} Y_i \preceq (1 + \epsilon)\text{im}(U).
\]

We would like to use Theorem 1 to obtain our desired bound. We just need to check that the hypotheses of the theorem are satisfied. By Fact 6 from the [Notes on Symmetric Matrices](#), we have

\[
Y = U^{+/2} \cdot Z \cdot U^{+/2} \preceq U^{+/2} \cdot (R \cdot U) \cdot U^{+/2} = R \cdot \text{im}(U),
\]

showing that \( \|Y\| \leq R \). Next,

\[
\mathbb{E}[Y] = U^{+/2} \cdot \mathbb{E}[Z] \cdot U^{+/2} = U^{+/2} \cdot U \cdot U^{+/2} = \text{im}(U).
\]

So the hypotheses of Theorem 1 are almost satisfied, with the small issue that \( \mathbb{E}[Y] \) is not actually the identity, but merely the identity on the image of \( U \). But, one may check that the proof of Theorem 1 still goes through as long as every eigenvalue of \( \mathbb{E}[Y] \) is either 0 or 1, i.e., \( \mathbb{E}[Y] \) is an orthogonal projection matrix. The details are left as an exercise. \( \square \)