

We have computed μ_4 , i.e. the 4th moment of Z to be 2.999..., and that the difference $(\mu_4 - 3)$ is about $2.1 \cdot 10^{-14}$ for parameter 256. Let us now compute how many samples one would need to successfully distinguish $\text{mom}_{4,\mathbf{C}}(\mathbf{u})$ when $\mathbf{u} \in \pm\mathbf{C}$ and when $\mathbf{u} \notin \pm\mathbf{C}$. $\text{mom}_{4,\mathbf{C}}(\mathbf{u}) = \mathbb{E}[(\langle \mathbf{u}, \mathbf{C}\mathbf{x} \rangle^4)] = 3 + (\mu_4 - 3) \sum_{i=1}^n \langle \mathbf{u}, \mathbf{c}_i \rangle^4$. If $\mathbf{u} = \mathbf{c}_i$, the entire expression is $3 + (\mu_4 - 3) \cdot 1 = \mu_4$ because $\langle \mathbf{c}_i, \mathbf{c}_i \rangle = 1$ and $\langle \mathbf{c}_i, \mathbf{c}_j \rangle = 0$ for $i \neq j$. Otherwise, the sum $\sum_{i=1}^n \langle \mathbf{u}, \mathbf{c}_i \rangle^4 < 1$. Say one wants to distinguish $\text{mom}_{4,\mathbf{C}}(\mathbf{c}_i)$ and $\text{mom}_{4,\mathbf{C}}(\mathbf{u})$ for $\mathbf{u} \notin \pm\mathbf{C}$. Let $y = \langle \mathbf{u}, \mathbf{C}\mathbf{x} \rangle$ and assume y follows a standard normal distribution. Then we approximate the variance σ^2 and standard deviation σ for $\mathbb{E}[(\langle \mathbf{u}, \mathbf{C}\mathbf{x} \rangle^4)]$ as $\mathbb{E}[y^8] - \mathbb{E}[y^4]^2$. Then $\sigma^2 = 105 - 9 = 96$ and $\sigma = \sqrt{96} \approx 9.79796$.

Now, to estimate number of samples we use formula for confidence intervals and Central Limit Theorem, we have that

$$s \geq \left(\frac{Z_{\alpha/2} \cdot \sigma}{\text{err}} \right)^2$$

Now, we want err to be smaller than $2.1 \cdot 10^{-14}$ for parameter 256. If we set err to be 10^{-14} , and we want to determine a difference with, say, 75 % confidence, we get:

$$s \geq \left(\frac{0.68 \cdot 9.79796}{10^{-14}} \right)^2 = 443904000000000063778315961828$$

which is way beyond the limit of transcript size, which for parameter 256 is 2^{32} and for non-challenge parameters 512 and 1024 is 2^{64} .