Betrachte Variante 1 des Ein-Bit Zufallsgenerators

1. $|x\rangle \leftarrow |1\rangle$ (neu)
2. $|x\rangle \leftarrow H|x\rangle$
3. Messen von $|x\rangle$

Wir beobachten:

1. Schritt: Qubit wird in den Anfangszustand $|1\rangle$ versetzt

2. Schritt: Anwendung der Hadamard-Transformation liefert

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

3. Schritt: Messen des Qubits liefert

- mit Wahrscheinlichkeit $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$ den Zustand $|0\rangle$, bzw.
- mit Wahrscheinlichkeit $\frac{1}{2}$ den Zustand $|1\rangle$

Im Ergebnis ist kein Unterschied zum ursprünglichen Verfahren festzustellen.

Betrachte Variante 2 des Ein-Bit Zufallsgenerators

Für $\alpha, \beta \in \mathbb{C}$ mit $|\alpha|^2 + |\beta|^2 = 1$:

1. $|x\rangle \leftarrow \alpha|0\rangle + \beta|1\rangle$ (neu)
2. $|x\rangle \leftarrow H|x\rangle$
3. Messen von $|x\rangle$

Wir beobachten:

1. Schritt Qubit wird in einen zulässigen Zustand versetzt

2. Schritt Anwendung der Hadamard-Transformation ergibt

$$\begin{aligned} H|x\rangle &= \alpha H|0\rangle + \beta H|1\rangle \\ &= \alpha \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \beta \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle \end{aligned}$$

3. Schritt Messen liefert

- mit Wahrscheinlichkeit $\frac{|\alpha+\beta|^2}{2}$ den Zustand $|0\rangle$, bzw.
- mit Wahrscheinlichkeit $\frac{|\alpha-\beta|^2}{2}$ den Zustand $|1\rangle$.

Die Ergebnisse $|0\rangle$ und $|1\rangle$ in Schritt 3 sind i.A. nicht mehr gleichwahrscheinlich.

Wähle etwa $\alpha=\beta=\frac{1}{\sqrt{2}}$. Dann ist $|\alpha|^2+|\beta|^2=\frac{1}{2}+\frac{1}{2}=1$, aber

$$\left|\frac{\alpha+\beta}{\sqrt{2}}\right|^2=\left|\frac{\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}}{\sqrt{2}}\right|^2=1,$$

$$\left|\frac{\alpha-\beta}{\sqrt{2}}\right|^2=\left|\frac{\frac{1}{\sqrt{2}}-\frac{1}{\sqrt{2}}}{\sqrt{2}}\right|^2=0.$$

Übung Zeige: Aus $|\gamma_0|^2+|\gamma_1|^2=1$, $|\beta_0|^2+|\beta_1|^2=1$ für $|x_0\rangle=\gamma_0|0\rangle+\gamma_1|1\rangle$, $|x_1\rangle=\beta_0|0\rangle+\beta_1|1\rangle$ folgt $|\alpha_{00}|^2+|\alpha_{01}|^2+|\alpha_{10}|^2+|\alpha_{11}|^2=1$ für

$$R=|x_1\rangle|x_0\rangle$$
$$=\alpha_{00}|00\rangle+\alpha_{01}|01\rangle+\alpha_{10}|10\rangle+\alpha_{11}|11\rangle.$$

Es gilt

$$\begin{aligned}
1&=\left(|\beta_0|^2+|\beta_1|^2\right)\left(|\gamma_0|^2+|\gamma_1|^2\right)\\
&=|\beta_0|^2|\gamma_0|^2+|\beta_0|^2|\gamma_1|^2+|\beta_1|^2|\gamma_0|^2+|\beta_1|^2|\gamma_1|^2\\
&=|\beta_0\gamma_0|^2+|\beta_0\gamma_1|^2+|\beta_1\gamma_0|^2+|\beta_1\gamma_1|^2\\
&=|\alpha_{00}|^2+|\alpha_{01}|^2+|\alpha_{10}|^2+|\alpha_{11}|^2
\end{aligned}$$

$\alpha_{ij}:=\beta_i\gamma_j$

Übung Betrachte $R = |x_1\rangle|x_0\rangle$ mit
$|x_0\rangle = \frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$, $|x_1\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$
Bestimmen Sie die Amplituden $\alpha_0, \alpha_1, \alpha_2, \alpha_3$.

$$R = \left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)\left(\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle\right)$$
$$= \frac{1}{4}|00\rangle - \frac{\sqrt{3}}{4}|01\rangle + \frac{\sqrt{3}}{4}|10\rangle + \frac{3}{4}|11\rangle$$
$$= \frac{1}{4}|0\rangle - \frac{\sqrt{3}}{4}|1\rangle + \frac{\sqrt{3}}{4}|2\rangle + \frac{3}{4}|3\rangle$$

Also: $\alpha_0 = \frac{1}{4}$, $\alpha_1 = -\frac{\sqrt{3}}{4}$, $\alpha_2 = \frac{\sqrt{3}}{4}$, $\alpha_3 = \frac{3}{4}$

Übung Zeigen Sie, dass A_{CNOT} unitär ist.

$$A_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$
ist reell und symmetrisch, also gilt $\overline{A}_{CNOT} = A_{CNOT}$ und $A^T_{CNOT} = A_{CNOT}$.

D.h. $A^+_{CNOT} = A_{CNOT}$. Es genügt also zu zeigen, dass A_{CNOT} selbstinvers ist.

$$A^2_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = I_4$$

Zeige Permutationsmatrizen sind unitär

Erinnerung: Sei $\pi \in S_n$. Die zugehörige $(n \times n)$-Permutationsmatrix $P_\pi = (p_{ij})$ ist definiert durch

$$p_{ij} = \delta_{\pi(i),j} = \begin{cases} 1, \text{ falls } \pi(i) = j, \\ 0, \text{ sonst.} \end{cases}$$

Per Definition sind die Einträge von P_π Elemente aus $\{0, 1\} \subset \mathbb{Z}$, also gilt $\overline{P_\pi} = P_\pi$.

Transponieren liefert nun

$$P_\pi^T = (p_{ji}) = (\delta_{\pi(j),i}) \text{ mit } \delta_{\pi(j),i} = \begin{cases} 1, \text{ falls } \pi(j) = i \\ 0, \text{ sonst} \end{cases}$$

$$= P_{\pi^{-1}} = P_\pi^{-1}$$

wobei π^{-1} die zu π inverse Permutation bzgl. Komposition bezeichnet.

Mit $P_\pi^T = P_\pi^{-1}$ folgt $P_\pi^+ = (\overline{P_\pi})^T = P_\pi^T = P_\pi^{-1}$.

Permutationsmatrizen sind also unitär.