Universality of quantum circuit

Ryuhei Mori

Tokyo Institute of Technology

Universality of a quantum circuit

Theorem (Universality of finite gate set)

For any unitary matrix $U \in L(\mathbb{C}^{2^n})$ and $\epsilon > 0$, there is a quantum circuit with H, T, CNOT gates computing $\widetilde{U}$ satisfying $D(U, \widetilde{U}) < \epsilon$.

Proof.

1. Any unitary matrix can be decomposed to a product of two-level unitary matrices. Done
2. Any two-level unitary matrix can be decomposed to a product of controlled-unitary gates. Done
3. Any controlled-untary gate can be decomposed to a product of CNOT and arbitrary single-qubit gates.
4. Any single-qubit gate can be approximated by H and T.

□

Special unitary group

- $\mathrm{U}(n) :=$ the set of $n \times n$ unitary matrices.

- $\mathrm{SU}(n) :=$
  the set of $n \times n$ unitary matrices U with $\det(U) = 1$.

- $\mathrm{U}(n)$ and $\mathrm{SU}(n)$ are groups.

- For $U \in \mathrm{U}(n)$, there exists $V \in \mathrm{SU}(n)$ and $\theta \in \mathbb{R}$ such that $U = \mathrm{e}^{i\theta} V$.

- For $U \in \mathrm{SU}(n)$ and $V \in \mathrm{U}(n)$, $VUV^\dagger \in \mathrm{SU}(n)$.

- For $V \in \mathrm{U}(n)$ and $W \in \mathrm{U}(n)$, $VWV^\dagger W^\dagger \in \mathrm{SU}(n)$
  (group commutator).

Controlled-unitary

Theorem

Any controlled-unitary gate can be decomposed to a product of CNOT and arbitrary single-qubit gates.

Proof.

1. Controlled-U(2) with single controlled qubit.
2. Controlled-SU(2) with n controlled qubits.
3. Controlled-U(2) with n controlled qubits.

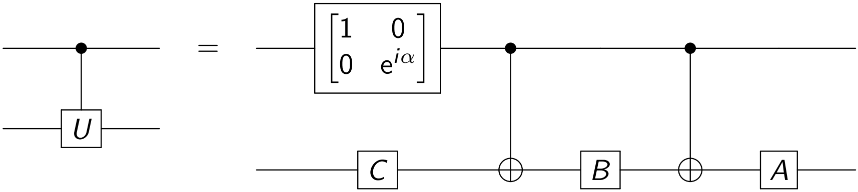
$\square$

Decomposition of single qubit unitary

Lemma

Any single qubit unitary $U \in \mathrm{U}(2)$, there is single qubit unitary matrices A, B, C such that $ABC = I$ and $\mathrm{e}^{i\alpha} AXBXC = U$.

From this lemma,



Decomposition of single qubit unitary

Lemma

Any single qubit unitary $U \in \mathrm{U}(2)$, there is single qubit unitary matrices A, B, C and $\alpha \in \mathbb{R}$ such that $ABC = I$ and $\mathrm{e}^{i\alpha} AXBXC = U$.

Proof.

For any $U \in \mathrm{U}(2)$, there exists $\alpha \in [0, 2\pi)$ and $V \in \mathrm{SU}(2)$ such that $U = e^{i\alpha} V$.

For $R_Z(\theta) = \begin{bmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{bmatrix}$, $XR_Z(\theta)XR_Z(-\theta) = R_Z(-2\theta)$.

For any $V \in \mathrm{SU}(2)$, there exists $\theta \in [0, 2\pi)$ and $P \in \mathrm{SU}(2)$ such that

$$V = PR_Z(-2\theta)P^\dagger = PXR_Z(\theta)XR_Z(-\theta)P^\dagger.$$

$A = P$, $B = R_Z(\theta)$, $C = R_Z(-\theta)P^\dagger$ satisfy the conditions. □

Controlled-unitary

Theorem

Any controlled-unitary gate can be decomposed to a product of CNOT and arbitrary single-qubit gates.

Proof.

1. Controlled-U(2) with single controlled qubit. Done
2. Controlled-SU(2) with n controlled qubits.
3. Controlled-U(2) with n controlled qubits.

$\square$

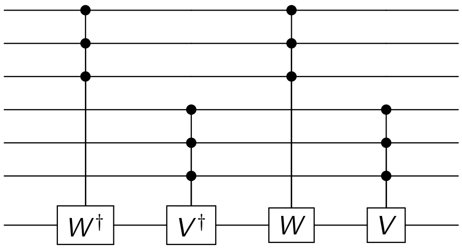
Group commutator and controlled-unitary

Theorem

For any $U \in SU(2)$, controlled-U gate with n controlled qubits can be realized by $O(n^2)$ CNOT and arbitrary single-qubit gates without ancillas (working qubits).

Proof.

Induction on n. For the group commutator decomposition $U = VWV^\dagger W^\dagger$ using $V = PiXP^\dagger$, $W = PR_Z(\theta)P^\dagger \in SU(2)$ for some $\theta \in [0, 2\pi)$ and $P \in SU(2)$.



$S_n = 4S_{n/2} = 4^{\log n} S_1 = O(n^2)$. $\square$

Controlled-unitary

Theorem

Any controlled-unitary gate can be decomposed to a product of CNOT and arbitrary single-qubit gates.

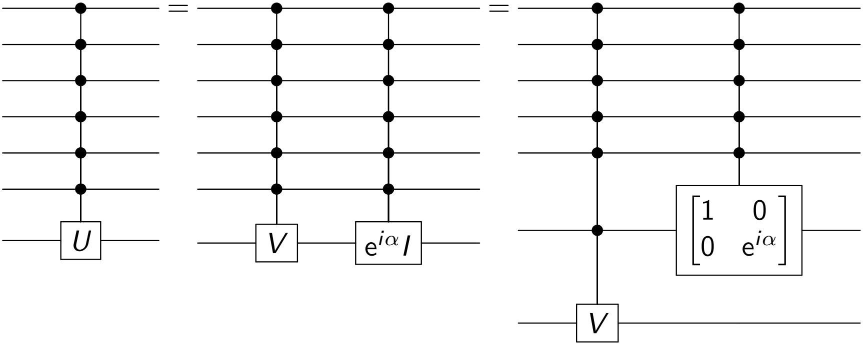
Proof.

1. Controlled-U(2) with single controlled qubit. Done
2. Controlled-SU(2) with n controlled qubits. Done
3. Controlled-U(2) with n controlled qubits.

□

Controlled-$U(2)$ with n controlled qubits

For any $U \in \mathrm{U}(2)$, there exists $V \in \mathrm{SU}(2)$ and $\alpha \in \mathbb{R}$ such that $U = \mathrm{e}^{i\alpha} V$.



$A_n = S_n + A_{n-1} = O(n^3)$

Controlled-unitary

Theorem

Any controlled-unitary gate can be decomposed to a product of CNOT and arbitrary single-qubit gates.

Proof.

1. Controlled-U(2) with single controlled qubit. Done
2. Controlled-SU(2) with n controlled qubits. Done
3. Controlled-U(2) with n controlled qubits. Done

□

Universality of a quantum circuit

Theorem (Universality of finite gate set)

For any unitary matrix $U \in L(\mathbb{C}^{2^n})$ *and* $\epsilon > 0$*, there is a quantum circuit with* H, T, CNOT *gates computing* $\widetilde{U}$ *satisfying* $D(U, \widetilde{U}) < \epsilon$.

Proof.

1. Any unitary matrix can be decomposed to a product of two-level unitary matrices. Done
2. Any two-level unitary matrix can be decomposed to a product of controlled-unitary gates. Done
3. Any controlled-untary gate can be decomposed to a product of CNOT and arbitrary single-qubit gates. Done
4. Any single-qubit gate can be approximated by H and T.

□

Approximation of a single-qubit gate is sufficient

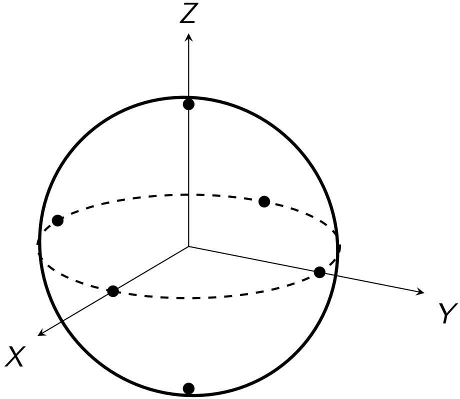
Theorem

For any $U \in U(2)$ and $\epsilon > 0$, there exists a single-qubit quantum circuit V consisting of H and T gates such that $D(U, V) \leq \epsilon$.

This theorem shows the universality of the gate set with CNOT. Assume $D(U_i, V_i) \leq \epsilon$ for $i = 1, \ldots, m$.

$$
\begin{aligned}
&D(U_m U_{m-1} \cdots U_1, V_m V_{m-1} \cdots V_1) \\
&\leq \sum_{i=1}^{m} D\left(U_m \cdots U_i V_{i-1} \cdots V_1, U_m \cdots U_{i+1} V_i \cdots V_1\right) \quad \text{(triangle inequality)} \\
&= \sum_{i=1}^{m} D\left(U_i, V_i\right) \quad \text{(unitary invariance)} \\
&\leq m\epsilon.
\end{aligned}
$$

Non-universality of X, Y, Z, H, S



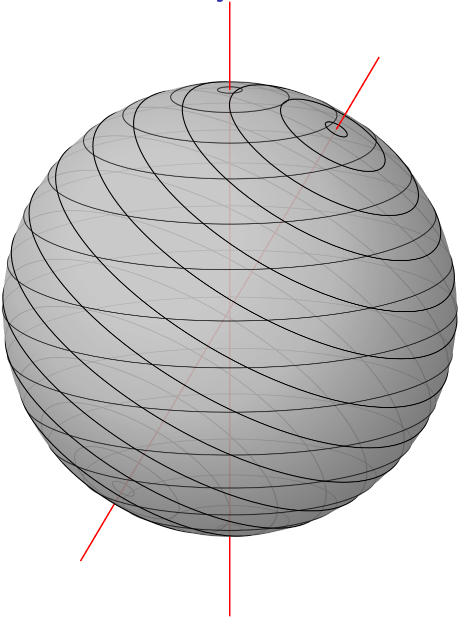
Universality of H, T

$T \cong R_Z(\pi/4)$. $HTH \cong R_X(\pi/4)$.

$$
\begin{aligned}
R_Z(\pi/4)R_X(\pi/4) &= \left[\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}Z\right]\left[\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}X\right] \\
&= \cos^2\frac{\pi}{8}I - i\sin\frac{\pi}{8}\left[\cos\frac{\pi}{8}(X+Z) + \sin\frac{\pi}{8}Y\right] \\
&=: \cos\frac{\eta}{2}I - i\sin\frac{\eta}{2}\left(n_x X + n_Y Y + n_Z Z\right) \\
&= R_{\hat{n}}(\eta)
\end{aligned}
$$

where η satisfying $\cos(\eta/2) = \cos^2(\pi/8)$ and $\hat{n}$ is a unit vector along with $(\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8})$. Here, η is an irrational multiple of π. $HR_{\hat{n}}(\eta)H = R_{\hat{m}}(\eta)$ where $\hat{m}$ is a unit vector along with $(\cos\frac{\pi}{8}, -\sin\frac{\pi}{8}, \cos\frac{\pi}{8})$.

Universality of two rotations 1/2



Universality of two rotations 2/2

Theorem

For any $U \in \mathrm{SU}(2)$, there exists $n \in \mathbb{Z}_{\geq 0}$ and $\alpha_1, \dots, \alpha_n \in (0, 2\pi)$ such that $R_{\hat{n}}(\alpha_1) R_{\hat{m}}(\alpha_2) R_{\hat{n}}(\alpha_3) \cdots R_{\hat{n}}(\alpha_n)$ is equal to U or $-U$.

Proof.

Let $|\psi\rangle$ and $|\psi^\perp\rangle$ be the eigenvectors of $R_{\hat{n}}(\theta)$.

Let $|\varphi\rangle := U|\psi\rangle$, $|\varphi^\perp\rangle := U|\psi^\perp\rangle$.

There exists $n \in \mathbb{Z}_{\geq 0}$ and $\theta_0, \theta_1, \alpha_1, \dots, \alpha_n \in (0, 2\pi)$ such that

$$\begin{aligned}
|\varphi\rangle &= e^{i\theta_0} R_{\hat{n}}(\alpha_1) R_{\hat{m}}(\alpha_2) R_{\hat{n}}(\alpha_3) \cdots R_{\hat{m}}(\alpha_{n-1}) |\psi\rangle \\
&= e^{i(\theta_0 + \frac{\alpha_n}{2})} R_{\hat{n}}(\alpha_1) R_{\hat{m}}(\alpha_2) R_{\hat{n}}(\alpha_3) \cdots R_{\hat{m}}(\alpha_{n-1}) R_{\hat{n}}(\alpha_n) |\psi\rangle \\
|\varphi^\perp\rangle &= e^{i\theta_1} R_{\hat{n}}(\alpha_1) R_{\hat{m}}(\alpha_2) R_{\hat{n}}(\alpha_3) \cdots R_{\hat{m}}(\alpha_{n-1}) |\psi^\perp\rangle \\
&= e^{i(\theta_1 - \frac{\alpha_n}{2})} R_{\hat{n}}(\alpha_1) R_{\hat{m}}(\alpha_2) R_{\hat{n}}(\alpha_3) \cdots R_{\hat{m}}(\alpha_{n-1}) R_{\hat{n}}(\alpha_n) |\psi^\perp\rangle .
\end{aligned}$$

By choosing $\alpha_n = \theta_1 - \theta_0$, then $\theta_0 + \frac{\alpha_n}{2} = \theta_1 - \frac{\alpha_n}{2}$. Hence, $R_{\hat{n}}(\alpha_1) \cdots R_{\hat{n}}(\alpha_n)$ maps $|\psi\rangle \mapsto e^{i\theta}|\varphi\rangle$, $|\psi^\perp\rangle \mapsto e^{i\theta}|\varphi^\perp\rangle$, implying $R_{\hat{n}}(\alpha_1) \cdots R_{\hat{n}}(\alpha_n) = e^{i\theta} U$. Since $U \in \mathrm{SU}(2)$, θ must be 0 or π. $\square$

Universality of a quantum circuit

Theorem (Universality of finite gate set)

For any unitary matrix $U \in L(\mathbb{C}^{2^n})$ and $\epsilon > 0$, there is a quantum circuit with H, T, CNOT gates computing $\widetilde{U}$ satisfying $D(U, \widetilde{U}) < \epsilon$.

Proof.

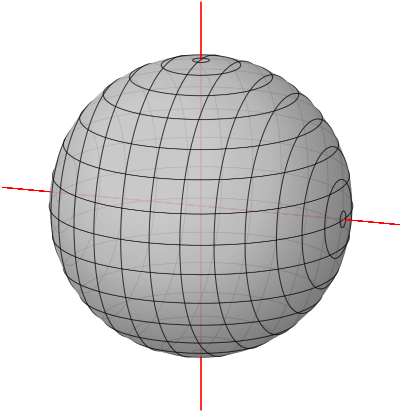
1. Any unitary matrix can be decomposed to a product of two-level unitary matrices. Done
2. Any two-level unitary matrix can be decomposed to a product of controlled-unitary gates. Done
3. Any controlled-untary gate can be decomposed to a product of CNOT and arbitrary single-qubit gates. Done
4. Any single-qubit gate can be approximated by H and T. Done

$\square$

Corollary

For any $U \in \mathrm{U}(2)$, *there exists* $\alpha, \beta, \gamma, \delta \in [0, 2\pi)$ *such that* $U = e^{i\alpha} R_Z(\beta) R_Y(\gamma) R_Z(\delta)$.

Proof.



Solovay–Kitaev theorem

Theorem

Assume $\{U_1, \dots, U_k\}$ *generates a dense subset of* $\mathrm{SU}(2)$*. Then, any* $U \in \mathrm{SU}(2)$ *can be approxmiated with error* ϵ *by* $[\log(1/\epsilon)]^c$ *multiplications of* $\{U_1, \dots, U_k\}$ *for some constant* c*.*

Assignments

1. Show a quantum circuit for controlled-$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$ gate with two controlled qubits using the CNOT gates and arbitrary single-qubit gates.

2. [Advanced] Show a quantum circuit for controlled-$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ gate with two controlled qubits using six CNOT gates and seven T and $T^\dagger$ gates.

Special unitary group and group commutator

Theorem

For any $U \in \mathrm{SU}(2)$, there exist $V, W \in \mathrm{SU}(2)$ such that $U = VWV^\dagger W^\dagger$ for some V, W satisfying $D(I, V) < c_{\mathrm{GC}}\sqrt{D(I, U)}$ and $D(I, W) < c_{\mathrm{GC}}\sqrt{D(I, U)}$ for some constant $c_{\mathrm{GC}} > 1/\sqrt{2}$.

Proof.

$$
\begin{aligned}
&R_Z(\theta)R_X(\theta)R_Z(\theta)^\dagger R_X(\theta)^\dagger = R_Z(\theta)R_X(\theta)R_Z(-\theta)R_X(-\theta) \\
&= R_Z(\theta)R_X(\theta)R_Z(-\theta)R_X(-\theta) \\
&= \left[\cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z\right]\left[\cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X\right]\left[\cos\frac{\theta}{2}I + i\sin\frac{\theta}{2}Z\right]\left[\cos\frac{\theta}{2}I + i\sin\frac{\theta}{2}X\right] \\
&= \left[\cos^4\frac{\theta}{2} + 2\cos^2\frac{\theta}{2}\sin^2\frac{\theta}{2} - \sin^4\frac{\theta}{2}\right]I + \cdots \\
&= \left[1 - 2\sin^4\frac{\theta}{2}\right]I + \cdots = R_{\hat{n}_\theta}(\varphi)
\end{aligned}
$$

$\cos\frac{\varphi}{2} = 1 - 2\sin^4\frac{\theta}{2}$. For some $S \in \mathrm{U}(2)$ and $\varphi \in \mathbb{R}$, $U = SR_{\hat{n}_\theta}(\varphi)S^\dagger$. For $V := SR_Z(\theta)S^\dagger$ and $W := SR_X(\theta)S^\dagger$, $U = VWV^\dagger W^\dagger$. □

Rotation matrix and distance

$$D(I, R_{\widehat{n}}(\theta)) = \left|\sin\frac{\theta}{2}\right|$$

For $U \in \mathrm{SU}(2)$, $V, W \in \mathrm{SU}(2)$ satisfying $U = VWV^\dagger W^\dagger$ in the construction

$$D(I, U) = \left|\sin\frac{\varphi}{2}\right| = \sqrt{1 - \cos^2\frac{\varphi}{2}} \approx 2\sin^2\frac{\theta}{2} = 2D(I, V)^2$$

With some constant $c_{\mathrm{GC}} > 1/\sqrt{2}$, $D(I - V) \leq c_{\mathrm{GC}}\sqrt{D(I, U)}$.

Solovay–Kitaev algorithm

function $\textsc{Solovay–Kitaev}(U, n)$
  if $n = 0$ **then**
    return Basic approximation to U
  end if
  $U_{n-1} \leftarrow \textsc{Solovay–Kitaev}(U, n-1)$
  $V, W \leftarrow \textsc{GC–Decompose}(UU_{n-1}^{\dagger})$
  $V_{n-1} \leftarrow \textsc{Solovay–Kitaev}(V, n-1)$
  $W_{n-1} \leftarrow \textsc{Solovay–Kitaev}(W, n-1)$
  return $V_{n-1}W_{n-1}V_{n-1}^{\dagger}W_{n-1}^{\dagger}U_{n-1}$.
end function

function $\textsc{GC–Decompose}(\Delta)$
  return (V, W) satisfying $VWV^{\dagger}W^{\dagger} = \Delta$ and $D(I, V), D(I, W) \leq c_{\mathrm{GC}}\sqrt{D(I, \Delta)}$.
end function

Theorem

If $D(I,V)$, $D(I,W) \leq \delta$, $D(V,\widetilde{V})$, $D(W,\widetilde{W}) \leq \Delta$

$$D(VWV^\dagger W^\dagger, \widetilde{V}\widetilde{W}\widetilde{V}^\dagger\widetilde{W}^\dagger) \leq c_{\mathrm{B}}\Delta(\delta+\Delta).$$

From this (surprising) theorem for $\Delta = \epsilon_{n-1}$, $\delta = c_{\mathrm{GC}}\sqrt{\epsilon_{n-1}}$, for $c_{\mathrm{approx}} \approx c_B c_{\mathrm{GC}}$.

$$\ell_n \leq 5\ell_{n-1}$$
$$\epsilon_n \leq c_{\mathrm{approx}}\epsilon_{n-1}^{3/2}$$

Then,

$$\ell_n \leq 5^n \ell_0$$
$$c_{\mathrm{approx}}^2\epsilon_n \leq c_{\mathrm{approx}}^3\epsilon_{n-1}^{3/2} = (c_{\mathrm{approx}}^2\epsilon_{n-1})^{3/2}$$
$$\leq (c_{\mathrm{approx}}^2\epsilon_0)^{(3/2)^n}$$

If $\epsilon_0 < 1/c_{\mathrm{approx}}^2$, $\ell_n = O\left((\log(1/\epsilon))^{\frac{\log 5}{\log(3/2)}}\right)$.

Proof 1/3

Theorem

If $D(I,V),\ D(I,W) \le \delta,\ D(V,\widetilde{V}),\ D(W,\widetilde{W}) \le \Delta$

$$D(VWV^\dagger W^\dagger, \widetilde{V}\widetilde{W}\widetilde{V}^\dagger\widetilde{W}^\dagger) \le 8\Delta^2 + 8\Delta\delta + 4\Delta\delta^2 + 4\Delta^3 + \Delta^4.$$

Proof.

For $A, B \in \mathrm{SU}(2)$, $D(A,B) = \sqrt{1 - \mathrm{Tr}(A^\dagger B)^2/4}$.

$$\begin{aligned}\mathrm{Tr}\left(WVW^\dagger V^\dagger \widetilde{V}\widetilde{W}\widetilde{V}^\dagger\widetilde{W}^\dagger\right) &= \mathrm{Tr}\left(W^\dagger(V^\dagger\widetilde{V})\widetilde{W}\widetilde{V}^\dagger(\widetilde{W}^\dagger W)V\right)\\ &= \mathrm{Tr}\left(W^\dagger(V^\dagger\widetilde{V})W(W^\dagger\widetilde{W})(\widetilde{V}^\dagger V)V^\dagger(\widetilde{W}^\dagger W)V\right)\end{aligned}$$

Proof.

Let

$$V^\dagger \widetilde{V} = \cos\frac{\theta_V}{2} I - i\sin\frac{\theta_V}{2} A$$
$$W^\dagger \widetilde{W} = \cos\frac{\theta_W}{2} I - i\sin\frac{\theta_W}{2} B$$
$$V = \cos\frac{\tau_V}{2} I - i\sin\frac{\tau_V}{2} C$$
$$W = \cos\frac{\tau_W}{2} I - i\sin\frac{\tau_W}{2} D$$

$$\begin{aligned}
&\frac{1}{2}\mathrm{Tr}\left(W^\dagger(V^\dagger\widetilde{V})W(W^\dagger\widetilde{W})(\widetilde{V}^\dagger V)V^\dagger(\widetilde{W}^\dagger W)V\right)\\
&\geq \left(\cos^2\frac{\tau_V}{2}\cos^2\frac{\tau_W}{2}\right)\frac{1}{2}\mathrm{Tr}\left((V^\dagger\widetilde{V})(W^\dagger\widetilde{W})(\widetilde{V}^\dagger V)(\widetilde{W}^\dagger W)\right)\\
&+\left(\cos^2\frac{\theta_V}{2}\cos^2\frac{\theta_W}{2}\right)-\left(\cos^2\frac{\tau_V}{2}\cos^2\frac{\tau_W}{2}\right)\left(\cos^2\frac{\theta_V}{2}\cos^2\frac{\theta_W}{2}\right)\\
&-\left(\binom{4}{1}\delta+\binom{4}{2}\delta^2+\binom{4}{3}\delta^3+\binom{4}{4}\delta^4\right)\left(\binom{4}{1}\Delta+\binom{4}{2}\Delta^2+\binom{4}{3}\Delta^3+\binom{4}{4}\Delta^4\right)\\
&\geq \frac{1}{2}\mathrm{Tr}\left((V^\dagger\widetilde{V})(W^\dagger\widetilde{W})(\widetilde{V}^\dagger V)(\widetilde{W}^\dagger W)\right)-(1-(1-\delta^2)^2)(1-(1-\Delta^2)^2)\\
&-((1+\delta)^4-1)((1+\Delta)^4-1)
\end{aligned}$$

Proof 3/3

$$\frac{1}{2}\mathrm{Tr}\left(W^\dagger(V^\dagger\widetilde{V})W(W^\dagger\widetilde{W})(\widetilde{V}^\dagger V)V^\dagger(\widetilde{W}^\dagger W)V\right)$$
$$\geq \frac{1}{2}\mathrm{Tr}\left((V^\dagger\widetilde{V})(W^\dagger\widetilde{W})(\widetilde{V}^\dagger V)(\widetilde{W}^\dagger W)\right) - (1-(1-\delta^2)^2)(1-(1-\Delta^2)^2)$$
$$-((1+\delta)^4-1)((1+\Delta)^4-1)$$

$$\frac{1}{2}\mathrm{Tr}\left((V^\dagger\widetilde{V})(W^\dagger\widetilde{W})(\widetilde{V}^\dagger V)(\widetilde{W}^\dagger W)\right)$$
$$= \frac{1}{2}\mathrm{Tr}\Bigg(\left[\cos\frac{\theta_V}{2}I - i\sin\frac{\theta_V}{2}A\right]\left[\cos\frac{\theta_W}{2}I - i\sin\frac{\theta_W}{2}B\right]$$
$$\cdot\left[\cos\frac{\theta_V}{2}I + i\sin\frac{\theta_V}{2}A\right]\left[\cos\frac{\theta_W}{2}I + i\sin\frac{\theta_W}{2}B\right]\Bigg)$$
$$= \cos^2\frac{\theta_V}{2}\cos^2\frac{\theta_W}{2} + \sin^2\frac{\theta_V}{2}\cos^2\frac{\theta_W}{2} + \cos^2\frac{\theta_V}{2}\sin^2\frac{\theta_W}{2} + \sin^2\frac{\theta_V}{2}\sin^2\frac{\theta_W}{2}\frac{1}{2}\mathrm{Tr}(ABAB)$$
$$\geq \cos^2\frac{\theta_V}{2}\cos^2\frac{\theta_W}{2} + \sin^2\frac{\theta_V}{2}\cos^2\frac{\theta_W}{2} + \cos^2\frac{\theta_V}{2}\sin^2\frac{\theta_W}{2} - \sin^2\frac{\theta_V}{2}\sin^2\frac{\theta_W}{2}$$
$$= 1 - 2\sin^2\frac{\theta_V}{2}\sin^2\frac{\theta_W}{2} \geq 1 - 2\Delta^4$$