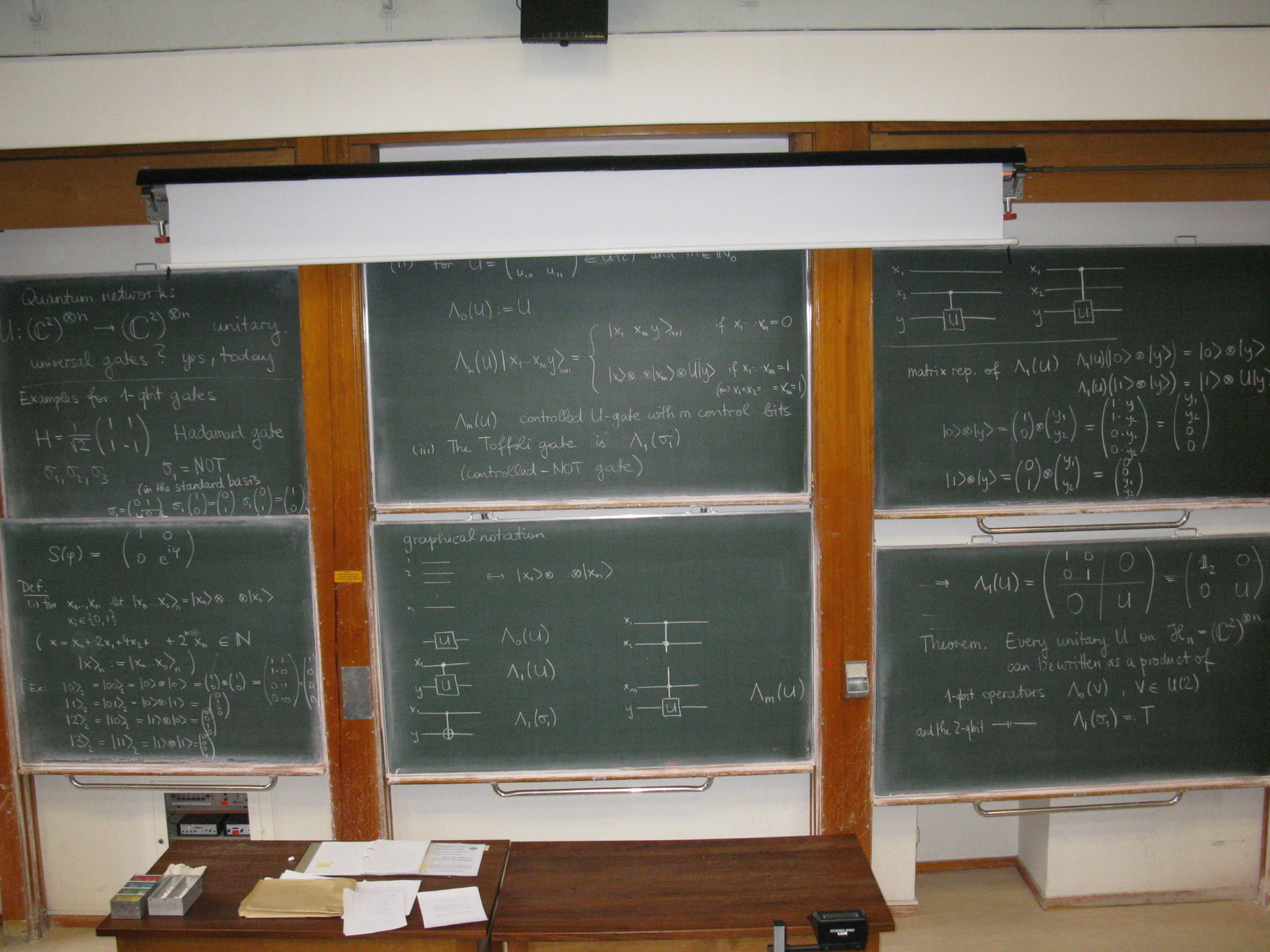
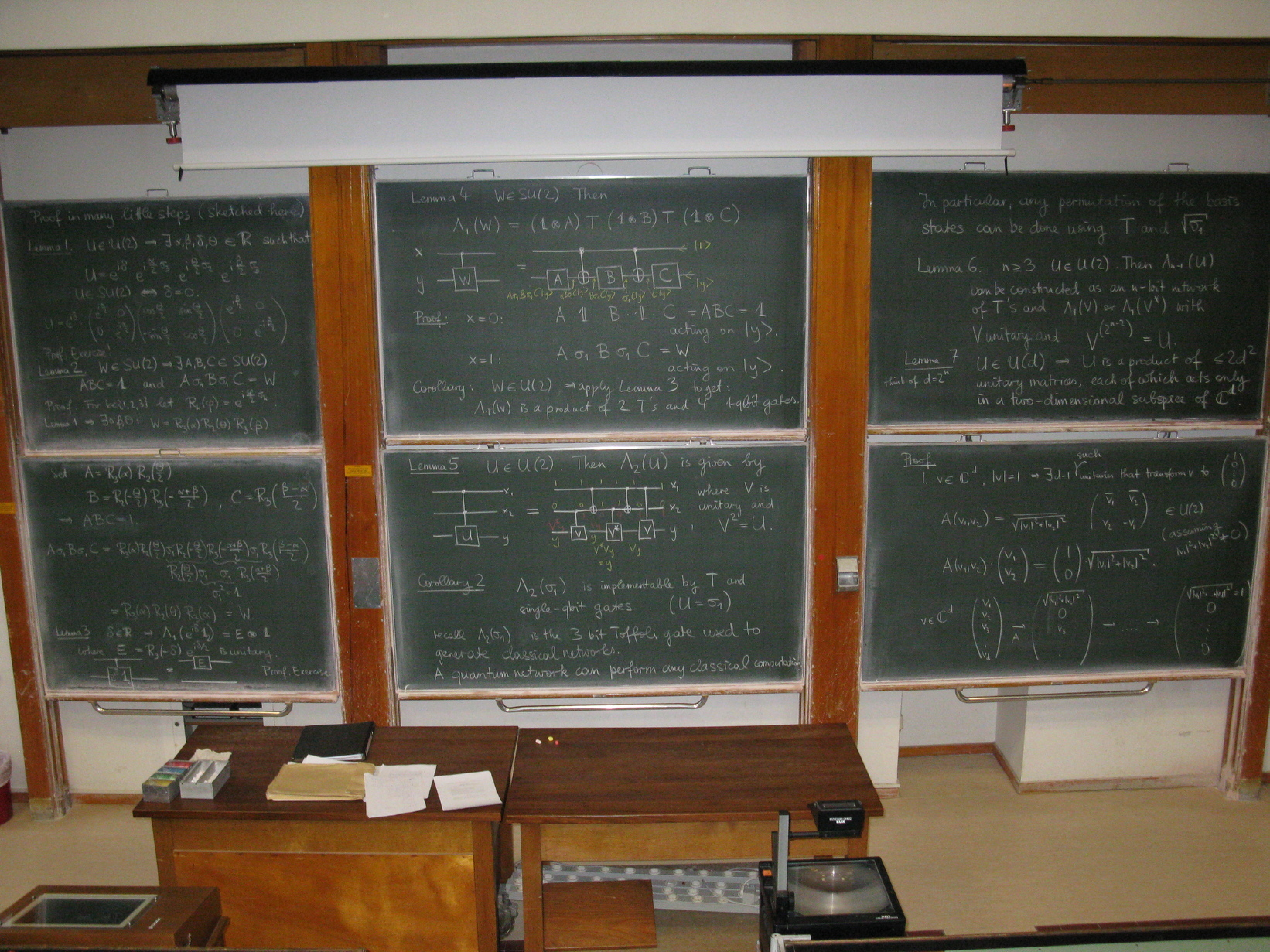


Quantum network:
$U: (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes n}$ unitary
universal gates? yes, today
Examples for 1-qbit gates
$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ Hadamard gate
$\sigma_1, \sigma_2, \sigma_3$ σ_1 = NOT
(in the standard basis)
$S(\varphi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$
Def.
(i) for $x_0, \dots, x_n$ let $|x_n \dots x_0\rangle_n = |x_n\rangle \otimes \dots \otimes |x_0\rangle$
$x_i \in \{0,1\}$
$(x = x_0 + 2x_1 + 4x_2 + \dots + 2^n x_n \in \mathbb{N}$
$|x\rangle_n := |x_n \dots x_0\rangle_n)$
Ex: $|0\rangle_2 = |00\rangle_2 = |0\rangle \otimes |0\rangle$
$|1\rangle_2 = |01\rangle_2 = |0\rangle \otimes |1\rangle$
$|2\rangle_2 = |10\rangle_2 = |1\rangle \otimes |0\rangle$
$|3\rangle_2 = |11\rangle_2 = |1\rangle \otimes |1\rangle$
$\Lambda_0(U) := U$
$\Lambda_m(U)|x_1 \dots x_m y\rangle_{m+1} = |x_1 \dots x_m y\rangle_{m+1}$ if $x_1 \cdots x_m = 0$; $|x_1\rangle \otimes \dots \otimes |x_m\rangle \otimes U|y\rangle$ if $x_1 \cdots x_m = 1$ $(\Leftrightarrow x_1 = x_2 = \dots = x_m = 1)$
$\Lambda_m(U)$ controlled U-gate with m control bits
(iii) The Toffoli gate is $\Lambda_1(\sigma_1)$
(controlled-NOT gate)
graphical notation
$\leftrightarrow |x_1\rangle \otimes \dots \otimes |x_n\rangle$
$\Lambda_0(U)$
$\Lambda_1(U)$
$\Lambda_1(\sigma_1)$
$\Lambda_m(U)$
matrix rep. of $\Lambda_1(U)$
$\Lambda_1(U)(|0\rangle \otimes |y\rangle) = |0\rangle \otimes |y\rangle$
$\Lambda_1(U)(|1\rangle \otimes |y\rangle) = |1\rangle \otimes U|y\rangle$
$|0\rangle \otimes |y\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ 0 \\ 0 \end{pmatrix}$
$|1\rangle \otimes |y\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ y_1 \\ y_2 \end{pmatrix}$
$\Rightarrow \Lambda_1(U) = \begin{pmatrix} \mathbb{1}_2 & 0 \\ 0 & U \end{pmatrix}$
Theorem. Every unitary U on $\mathcal{H}_n = (\mathbb{C}^2)^{\otimes n}$ can be written as a product of
1-qbit operators $\Lambda_0(V)$, $V \in U(2)$
and the 2-qbit $\Lambda_1(\sigma_1) =: T$


Proof in many little steps (sketched here)
Lemma 1. $U \in U(2) \Rightarrow \exists \alpha, \beta, \delta, \theta \in \mathbb{R}$ such that
$U = e^{i\delta} e^{i\frac{\alpha}{2}\sigma_3} e^{i\frac{\theta}{2}\sigma_2} e^{i\frac{\beta}{2}\sigma_3}$
$U \in SU(2) \Leftrightarrow \delta = 0$.
Proof. Exercise!
Lemma 2. $W \in SU(2) \Rightarrow \exists A, B, C \in SU(2)$:
$ABC = \mathbb{1}$ and $A\sigma_1 B \sigma_1 C = W$
Proof. For $k \in \{1,2,3\}$ let $R_k(\varphi) = e^{i\frac{\varphi}{2}\sigma_k}$.
Lemma 1 $\Rightarrow \exists \alpha, \beta, \theta$: $W = R_3(\alpha) R_2(\theta) R_3(\beta)$
Set $A = R_3(\alpha) R_2(\frac{\theta}{2})$
$B = R_2(-\frac{\theta}{2}) R_3(-\frac{\alpha+\beta}{2})$, $C = R_3(\frac{\beta-\alpha}{2})$
$\Rightarrow ABC = 1$.
$\sigma_1^2 = \mathbb{1}$
$= R_3(\alpha) R_2(\theta) R_3(\alpha) = W$.
Lemma 3 $\delta \in \mathbb{R} \Rightarrow \Lambda_1(e^{i\delta}\mathbb{1}) = E \otimes \mathbb{1}$
where $E = R_3(-\delta) e^{i\delta/2}$ is unitary.
Proof. Exercise
Lemma 4 $W \in SU(2)$ Then
$\Lambda_1(W) = (\mathbb{1} \otimes A) T (\mathbb{1} \otimes B) T (\mathbb{1} \otimes C)$
Proof: $x = 0$: $A \mathbb{1} B \mathbb{1} C = ABC = \mathbb{1}$ acting on $|y\rangle$.
$x = 1$: $A \sigma_1 B \sigma_1 C = W$ acting on $|y\rangle$.
Corollary: $W \in U(2) \Rightarrow$ apply Lemma 3 to get:
$\Lambda_1(W)$ is a product of 2 T's and 4 1-qbit gates.
Lemma 5. $U \in U(2)$. Then $\Lambda_2(U)$ is given by
where V is unitary and $V^2 = U$.
Corollary 2 $\Lambda_2(\sigma_1)$ is implementable by T and single-qbit gates $(U = \sigma_1)$
recall $\Lambda_2(\sigma_1)$ is the 3 bit Toffoli gate used to generate classical networks.
A quantum network can perform any classical computation.
In particular, any permutation of the basis states can be done using T and $\sqrt{\sigma_1}$
Lemma 6. $n \geq 3$ $U \in U(2)$. Then $\Lambda_{n-1}(U)$ can be constructed as an n-bit network of T's and $\Lambda_1(V)$ or $\Lambda_1(V^*)$ with V unitary and $V^{(2^{n-2})} = U$.
Lemma 7 $U \in U(d) \Rightarrow U$ is a product of $\leq 2d^2$ unitary matrices, each of which acts only in a two-dimensional subspace of $\mathbb{C}^d$.
think of $d = 2^n$
Proof
1. $v \in \mathbb{C}^d$, $|v| = 1 \Rightarrow \exists d-1$ such unitaries that transform v to $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$
$A(v_1, v_2) = \frac{1}{\sqrt{|v_1|^2 + |v_2|^2}} \begin{pmatrix} \bar{v}_1 & \bar{v}_2 \\ v_2 & -v_1 \end{pmatrix} \in U(2)$
(assuming $|v_1|^2 + |v_2|^2 \neq 0$)
$A(v_1, v_2) \cdot \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \sqrt{|v_1|^2 + |v_2|^2}$.
$v \in \mathbb{C}^d$