

Introduction to Quantum Information Processing

Lecture 18

Richard Cleve

Overview of Lecture 18

- Continuation of fingerprinting
- Hidden matching problem
- Restricted-equality nonlocality
- Universal sets of gates

continuation
of quantum
fingerprints

Quantum fingerprints

Question 1: how many orthogonal states in m qubits?

Answer: 2^m

Let ε be an arbitrarily small positive constant

Question 2: how many *almost orthogonal** states in m qubits?

(* where $|\langle \Psi_x | \Psi_y \rangle| \leq \varepsilon$)

Answer: 2^{2am} , for some constant $a > 0$

The states can be constructed via a suitable (classical) error-correcting code, which is a function $e: \{0,1\}^n \rightarrow \{0,1\}^{cn}$ where, for all $x \neq y$, $dcn \leq \Delta(e(x), e(y)) \leq (1-d)cn$ (c, d are constants)

Construction of *almost* orthogonal states

Set $|\psi_x\rangle = \frac{1}{\sqrt{cn}} \sum_{k=1}^{cn} (-1)^{e(x)_k} |k\rangle$ for each $x \in \{0,1\}^n$ ($\log(cn)$ qubits)

Then $\langle \psi_x | \psi_y \rangle = \frac{1}{cn} \sum_{k=1}^{cn} (-1)^{[e(x) \oplus e(y)]_k} |k\rangle = 1 - \frac{2\Delta(e(x), e(y))}{cn}$

Since $dcn \leq \Delta(e(x), e(y)) \leq (1-d)cn$, we have $|\langle \psi_x | \psi_y \rangle| \leq 1 - 2d$

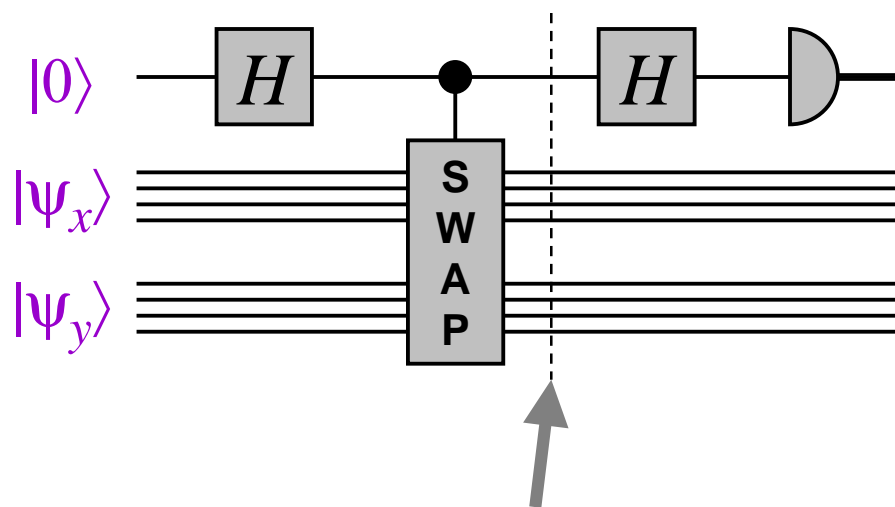
By duplicating each state, $|\psi_x\rangle \otimes |\psi_x\rangle \otimes \dots \otimes |\psi_x\rangle$, the pairwise inner products can be made arbitrarily small: $(1 - 2d)^r \leq \varepsilon$

Result: $m = r \log(cn)$ qubits storing $2^n = 2^{(1/c)2^{m/r}}$ different states

Quantum fingerprints

Let $|\psi_{000}\rangle, |\psi_{001}\rangle, \dots, |\psi_{111}\rangle$ be 2^n states on $O(\log n)$ qubits such that $|\langle \psi_x | \psi_y \rangle| \leq \epsilon$ for all $x \neq y$

Given $|\psi_x\rangle|\psi_y\rangle$, one can check if $x = y$ or $x \neq y$ as follows:



if $x = y$, $\Pr[\text{output} = 0] = 1$

if $x \neq y$, $\Pr[\text{output} = 0] = (1 + \epsilon^2)/2$

Intuition: $|0\rangle|\psi_x\rangle|\psi_y\rangle + |1\rangle|\psi_y\rangle|\psi_x\rangle$

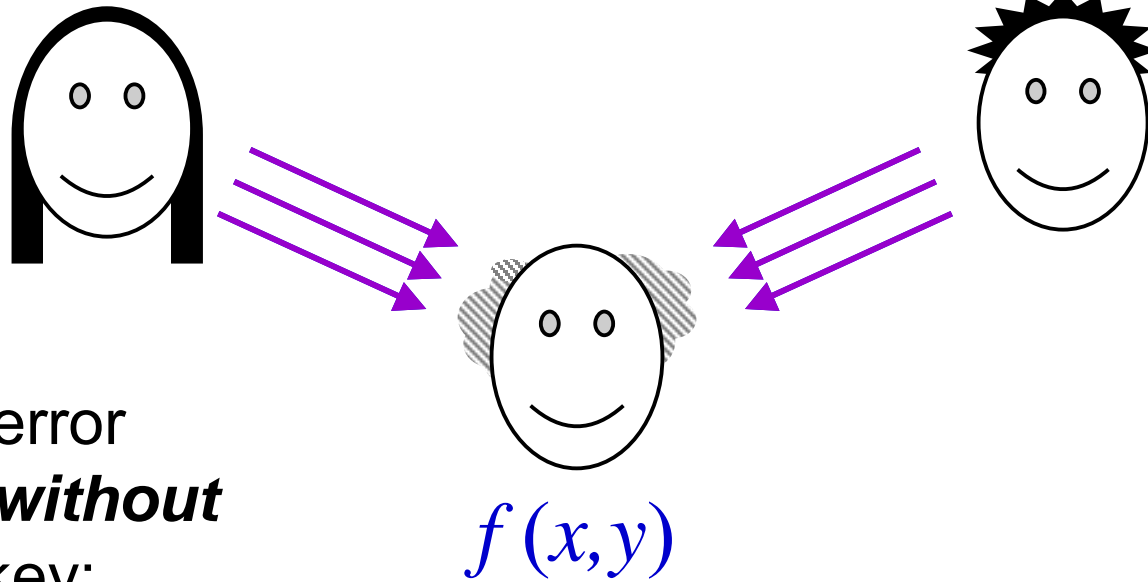
Note: error probability can be reduced to $((1 + \epsilon^2)/2)^r$

Equality revisited

in simultaneous message model

$x_1 x_2 \dots x_n$

$y_1 y_2 \dots y_n$



Bounded-error
protocols *without*
a shared key:

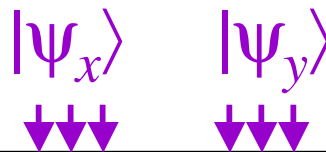
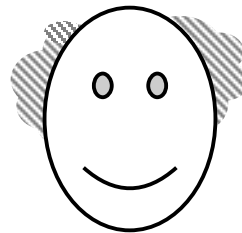
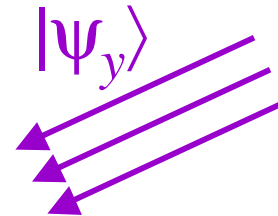
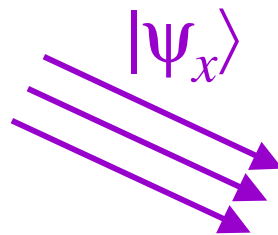
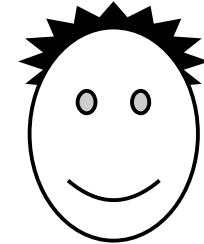
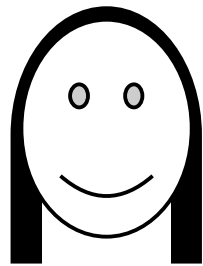
Classical: $\theta(n^{1/2})$

Quantum: $\theta(\log n)$

Quantum protocol for equality in simultaneous message model

$x_1 x_2 \dots x_n$

$y_1 y_2 \dots y_n$



Orthogonality
test



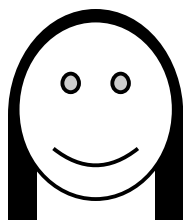
Recall that, **with** a shared key, the problem is easy classically ...

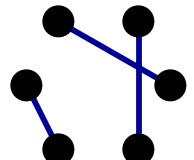
**... hidden
matching
problem**

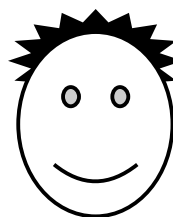
Hidden matching problem

For this problem, a quantum protocol is exponentially more efficient than any classical protocol—even with a shared key

Inputs: $x \in \{0,1\}^n$



$M =$  **matching** on $\{1, 2, \dots, n\}$

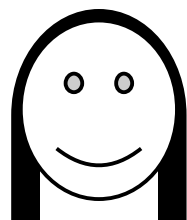


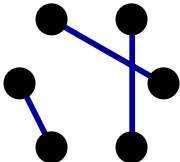
Output: $(i, j, x_i \oplus x_j)$, such that $(i, j) \in M$

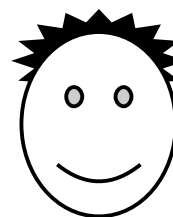
Only **one-way** communication (Alice to Bob) is permitted

The hidden matching problem

Inputs: $x \in \{0,1\}^n$



$M =$  *matching* on $\{1,2, \dots, n\}$



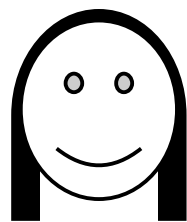
Output: $(i, j, x_i \oplus x_j)$, $(i, j) \in M$

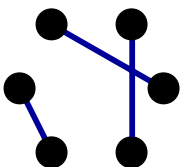
Classically, one-way communication is $\Omega(\sqrt{n})$, even with a shared classical key (the proof is omitted here)

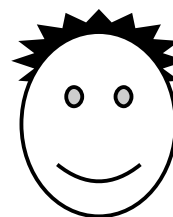
Rough intuition: Alice doesn't know which edges are in M , so she would have to send $\Omega(\sqrt{n})$ bits of the form $x_i \oplus x_j \dots$

The hidden matching problem

Inputs: $x \in \{0,1\}^n$



$M =$  *matching* on $\{1,2, \dots, n\}$



Output: $(i, j, x_i \oplus x_j)$, $(i, j) \in M$

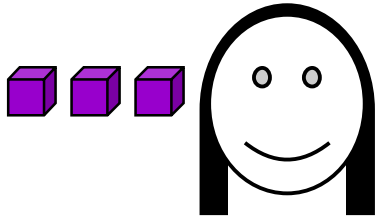
Quantum protocol: Alice sends $\frac{1}{\sqrt{n}} \sum_{k=1}^n (-1)^{x_k} |k\rangle$ ($\log n$ qubits)

Bob measures in $|i\rangle \pm |j\rangle$ basis, $(i, j) \in M$, and uses the outcome's relative phase to determine $x_i \oplus x_j$

nonlocality revisited

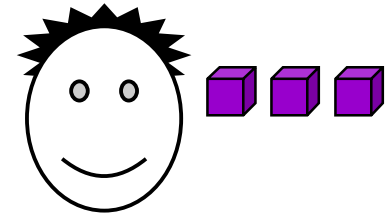
Restricted-equality nonlocality

inputs: x (n bits)



outputs: a ($\log n$ bits)

y (n bits)



b ($\log n$ bits)

Precondition: either $x = y$ or $\Delta(x,y) = n/2$

Required postcondition: $a = b$ iff $x = y$

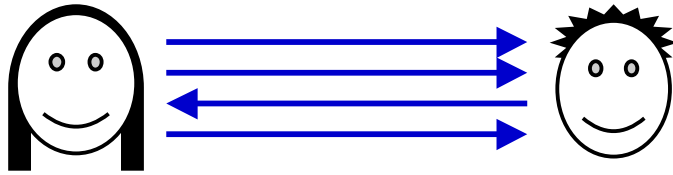
With classical resources, $\Omega(n)$ bits of communication needed **for an exact solution***

With $(|00\rangle + |11\rangle)^{\otimes \log n}$ prior entanglement, no communication is needed at all*

[BCT '99] * Technical details similar to restricted equality of Lecture 17

Restricted-equality nonlocality

Bit communication:



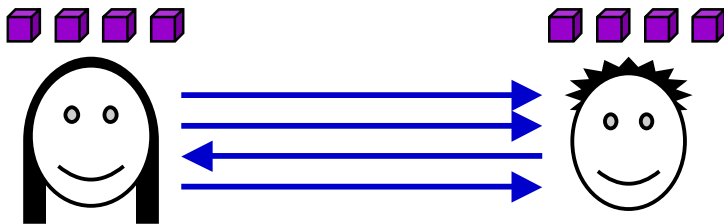
Cost: $\theta(n)$

Qubit communication:



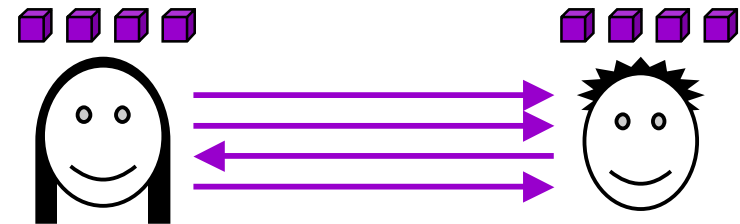
Cost: $\log n$

Bit communication
& prior entanglement:



Cost: zero

Qubit communication
& prior entanglement:



Cost: zero

Nonlocality and communication complexity conclusions

- Quantum information affects communication complexity in interesting ways
- There is a rich interplay between quantum communication complexity and:
 - quantum algorithms
 - quantum information theory
 - other notions of complexity theory ...

universality of two-qubit gates

A universal set of gates

Theorem: any unitary operation U acting on k qubits can be decomposed into $O(4^k)$ CNOT and one-qubit gates

(This was stated in Lecture 5 without a proof)

Proof sketch (for a slightly worse bound of $O(k^2 4^k)$) :

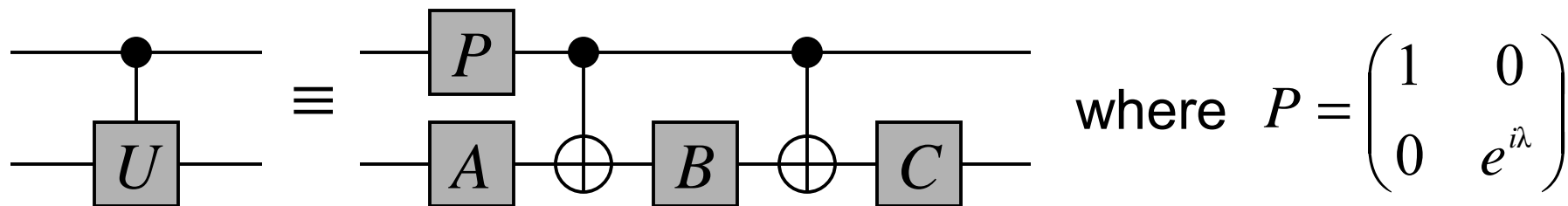
We first show how to simulate a controlled- U , for any one-qubit unitary U

Fact: for any one-qubit unitary U , there exist A, B, C , and λ , such that:

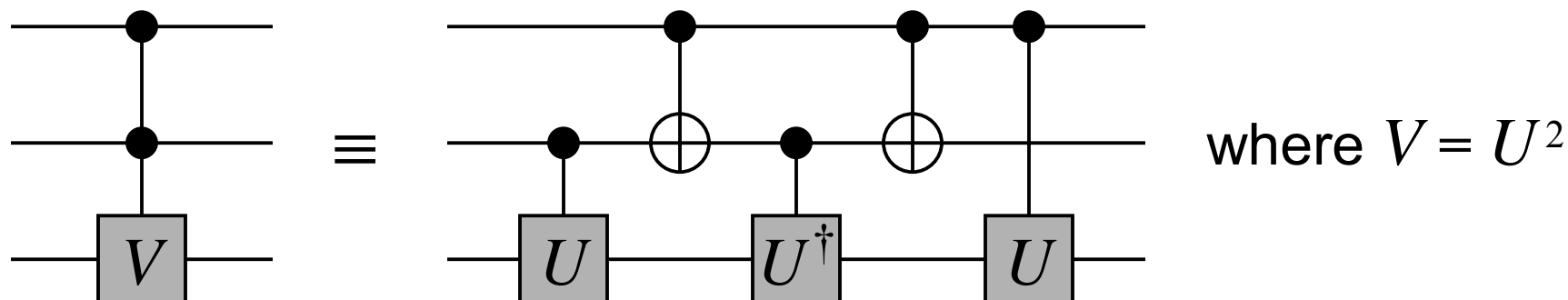
- $A B C = I$
- $e^{i\lambda} A X B X C = U$, where $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

A universal set of gates

The aforementioned fact implies



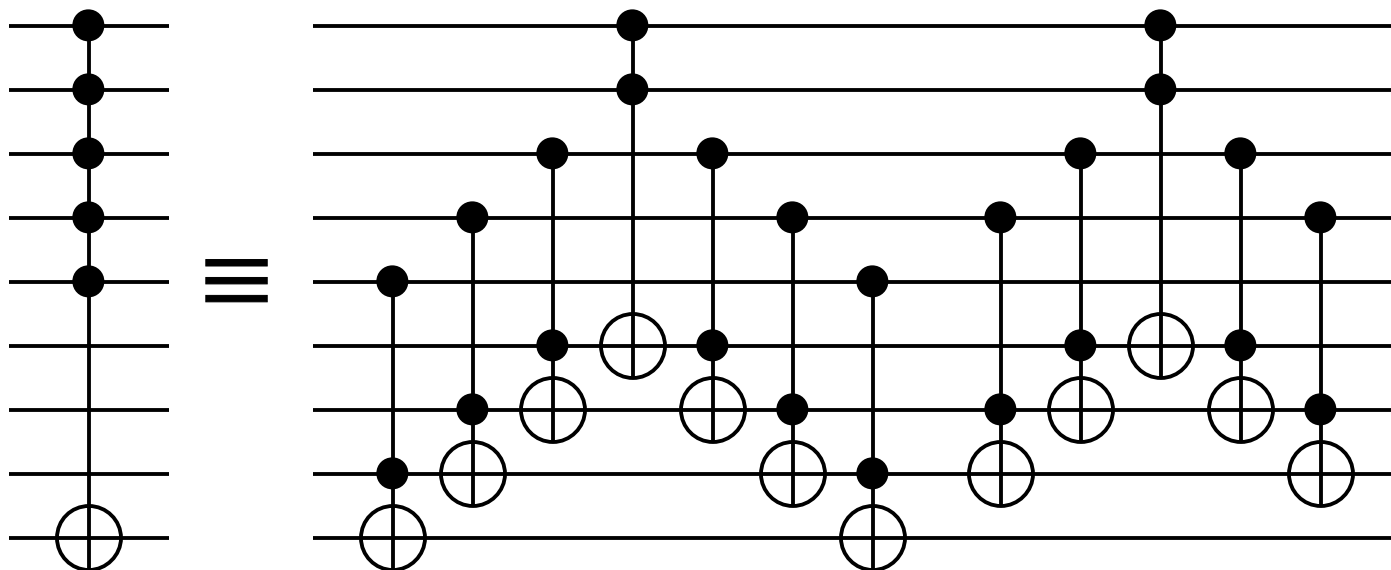
Using such controlled- U gates, one can simulate controlled-controlled- V gates, for any unitary V , as follows:



A universal set of gates

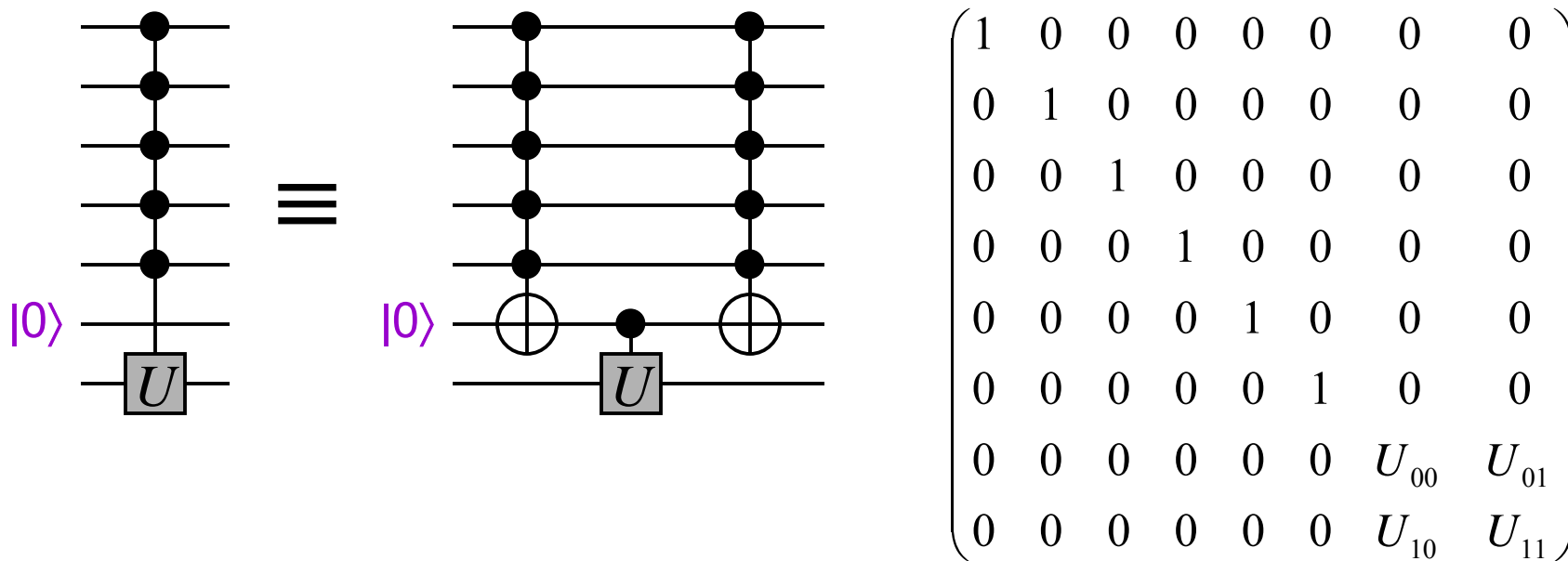
When $U = X$, this construction yields the 3-qubit *Toffoli gate*

From this gate, *generalized* Toffoli gates can be constructed:



A universal set of gates

From generalized Toffoli gates, **generalized controlled- U** gates (controlled-controlled- ... - U) can be constructed:



A universal set of gates

The approach essentially enables any k -qubit operation of the simple form

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & U_{00} & 0 & 0 & U_{01} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & U_{10} & 0 & 0 & U_{11} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

to be computed with $O(k^2)$ CNOT and one-qubit gates

Any $2^k \times 2^k$ unitary matrix can be decomposed into a product of $O(4^k)$ such simple matrices

A universal set of gates

This completes the proof sketch

Thus, the set of ***all*** one-qubit gates and the CNOT gate are ***universal*** in that they can simulate any other gate set

Question: is there a ***finite*** set of gates that is universal?

Answer 1: strictly speaking, ***no***, because this results in only countably many quantum circuits, whereas there are uncountably many unitary operations on k qubits (for any k)

THE END