Introduction to Quantum Information Processing

CS 467 / CS 667
Phys 467 / Phys 767
C&O 481 / C&O 681

Lecture 10 (2005)

Richard Cleve
DC 3524
cleve@cs.uwaterloo.ca

Course web site at:
http://www.cs.uwaterloo.ca/~cleve/courses/cs467

Contents

- More state distinguishing problems
- Return to approximately universal gate sets
- Complexity classes
- Density matrix formalism

- More state distinguishing problems
- Return to approximately universal gate sets
- Complexity classes
- Density matrix formalism

More state distinguishing problems

Which of these states are distinguishable? Divide them into equivalence classes:

1. $|0\rangle + |1\rangle$

2. $-|0\rangle - |1\rangle$

3. $\begin{cases} |0\rangle \text{ with prob. } \frac{1}{2} \\ |1\rangle \text{ with prob. } \frac{1}{2} \end{cases}$

4. $\begin{cases} |0\rangle + |1\rangle & \text{with prob. } \frac{1}{2} \\ |0\rangle - |1\rangle & \text{with prob. } \frac{1}{2} \end{cases}$

5. $\begin{cases} |0\rangle & \text{with prob. } \frac{1}{2} \\ |0\rangle + |1\rangle & \text{with prob. } \frac{1}{2} \end{cases}$

6. $\begin{cases} |0\rangle & \text{with prob. } \frac{1}{4} \\ |1\rangle & \text{with prob. } \frac{1}{4} \\ |0\rangle + |1\rangle & \text{with prob. } \frac{1}{4} \\ |0\rangle - |1\rangle & \text{with prob. } \frac{1}{4} \end{cases}$

7. The first qubit of $|01\rangle - |10\rangle$

Answers later on ...

This is a probabilistic mixed state

- More state distinguishing problems
- Return to approximately universal gate sets
- Complexity classes
- Density matrix formalism

Universal gate sets

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

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

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)

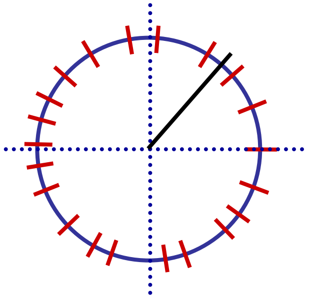
***Approximately* universal gate sets**

Answer 2: yes, for universality in an ***approximate*** sense

As an illustrative example, any rotation can be approximated within any precision by repeatedly applying

$$R = \begin{bmatrix} \cos(\sqrt{2}\pi) & -\sin(\sqrt{2}\pi) \\ \sin(\sqrt{2}\pi) & \cos(\sqrt{2}\pi) \end{bmatrix}$$

some number of times



In this sense, R is ***approximately universal*** for the set of all one-qubit rotations: any rotation S can be approximated within precision ε by applying R a suitable number of times

It turns out that $O((1/\varepsilon)^c)$ times suffices (for a constant c)

Approximately universal gate sets

In three or more dimensions, the rate of convergence with respect to ε can be exponentially faster

Theorem 2: the gates CNOT, H, and $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$ are ***approximately universal***, in that any unitary operation on k qubits can be simulated within precision ε by applying $O\left(4^k \log^c(1/\varepsilon)\right)$ of them (c is a constant)

[Solovay, 1996][Kitaev, 1997]

- More state distinguishing problems
- Return to approximately universal gate sets
- Complexity classes
- Density matrix formalism

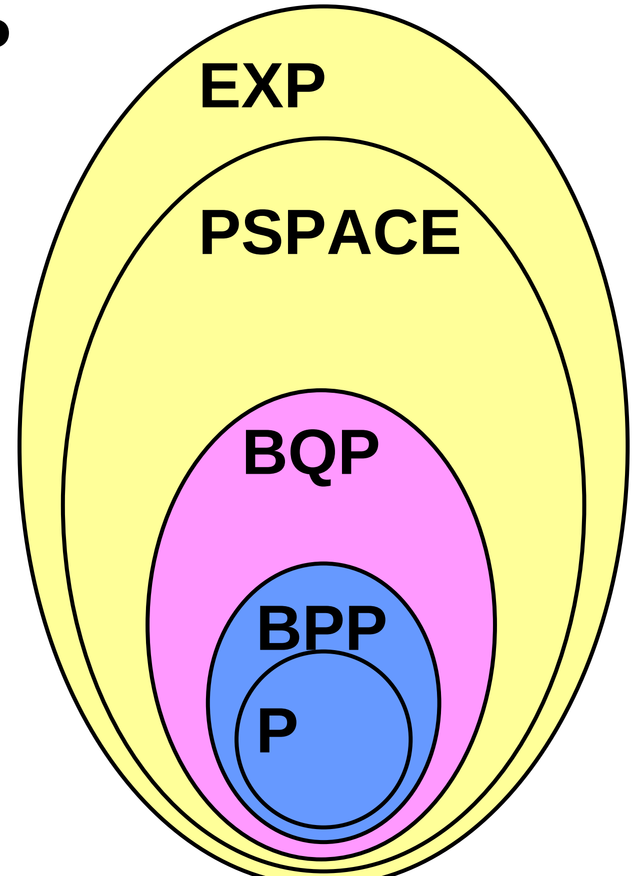
Complexity classes

Recall:

- **P (polynomial time):** problems solved by $O(n^c)$-size classical circuits (decision problems and uniform circuit families)
- **BPP (bounded error probabilistic polynomial time):** problems solved by $O(n^c)$-size ***probabilistic*** circuits that err with probability $\leq$ ¼
- **BQP (bounded error quantum polynomial time):** problems solved by $O(n^c)$-size ***quantum*** circuits that err with probability $\leq$ ¼
- **PSPACE (polynomial space):** problems solved by algorithms that use $O(n^c)$ memory.

Summary of previous containments

P $\subseteq$ **BPP** $\subseteq$ **BQP** $\subseteq$ **PSPACE** $\subseteq$ **EXP**



We now consider further structure between **P** and **PSPACE**

Technically, we will restrict our attention to ***languages*** (i.e. $\{0,1\}$-valued problems)

Many problems of interest can be cast in terms of languages

For example, we could define

FACTORING $= \{(x,y) : \exists\, 2 \le z \le y$, such that z divides $x\}$

NP

Define **NP (non-deterministic polynomial time)** as the class of languages whose ***positive*** instances have "witnesses" that can be verified in polynomial time

Example: Let **3-CNF-SAT** be the language consisting of all **3-CNF** formulas that are satisfiable

3-CNF formula:

$$f(x_1,\ldots,x_n) = (x_1 \vee \bar{x}_3 \vee x_4) \wedge (\bar{x}_2 \vee x_3 \vee \bar{x}_5) \wedge \cdots \wedge (\bar{x}_1 \vee x_5 \vee \bar{x}_n)$$

$f(x_1,\ldots,x_n)$ is ***satisfiable*** iff there exists $b_1,\ldots,b_n \in \{0,1\}$ such that $f(b_1,\ldots,b_n) = 1$

No sub-exponential-time algorithm is known for **3-CNF-SAT**

But poly-time verifiable witnesses exist (namely, $b_1, \ldots, b_n$)

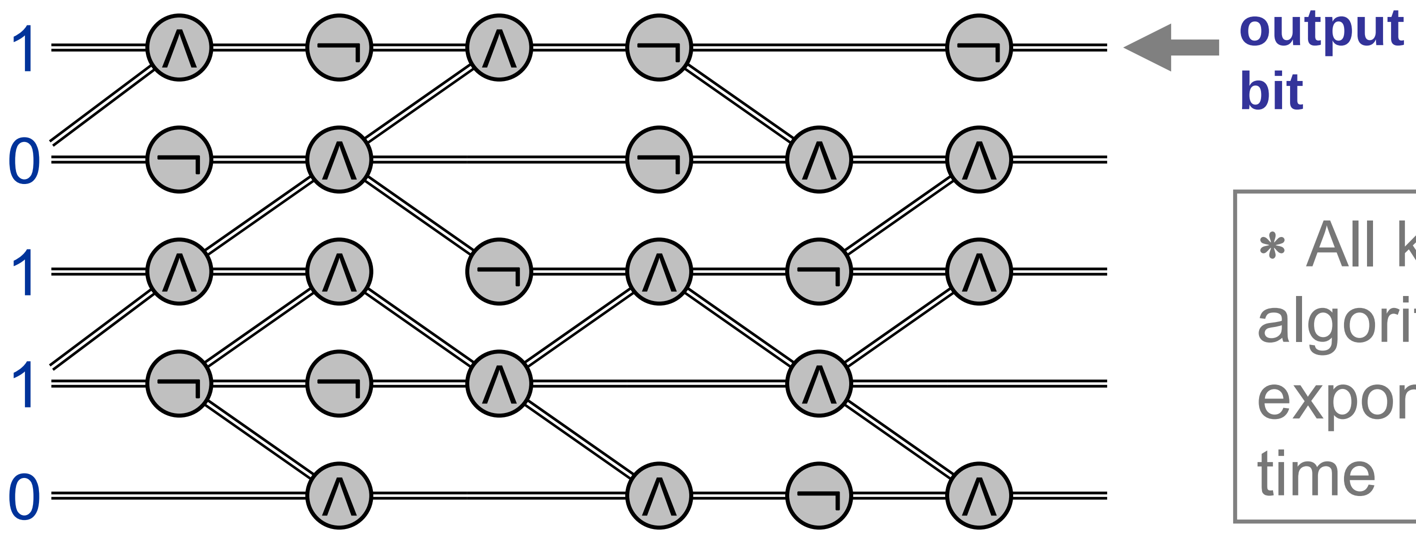
Other "logic" problems in NP

- ***k*-DNF-SAT**:

$$f(x_1,\ldots,x_n) = (x_1 \wedge \overline{x}_3 \wedge x_4) \vee (\overline{x}_2 \wedge x_3 \wedge \overline{x}_5) \vee \cdots \vee (\overline{x}_1 \wedge x_5 \wedge \overline{x}_n)$$

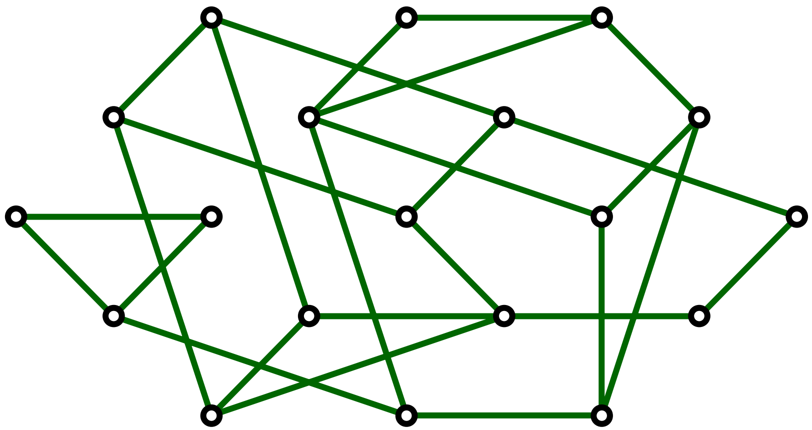
∗ But, unlike with *k*-**CNF-SAT**, this one is known to be in **P**

- **CIRCUIT-SAT**:



∗ All known algorithms exponential-time

"Graph theory" problems in NP



- k-**COLOR**: does G have a k-***coloring***?
- k-**CLIQUE**: does G have a ***clique*** of size k?
- **HAM-PATH**: does G have a ***Hamiltonian path***?
- **EUL-PATH**: does G have an ***Eulerian path***?

"Arithmetic" problems in NP

- **FACTORING** = $\{(x, y) : \exists\, 2 \leq z \leq y$, such that z divides $x\}$

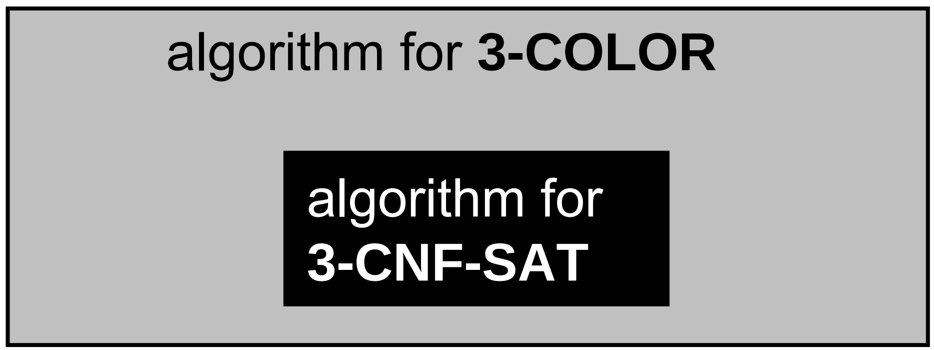
- **SUBSET-SUM**: given integers $x_1, x_2, \ldots, x_n, y$, do there exist $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, n\}$ such that $x_{i_1} + x_{i_2} + \ldots + x_{i_k} = y$?

- **INTEGER-LINEAR-PROGRAMMING**: linear programming where one seeks an ***integer-valued*** solution (its existence)

P vs. NP

All of the aforementioned problems have the property that they ***reduce*** to **3-CNF-SAT**, in the sense that a polynomial-time algorithm for **3-CNF-SAT** can be converted into a poly-time algorithm for the problem

Example:



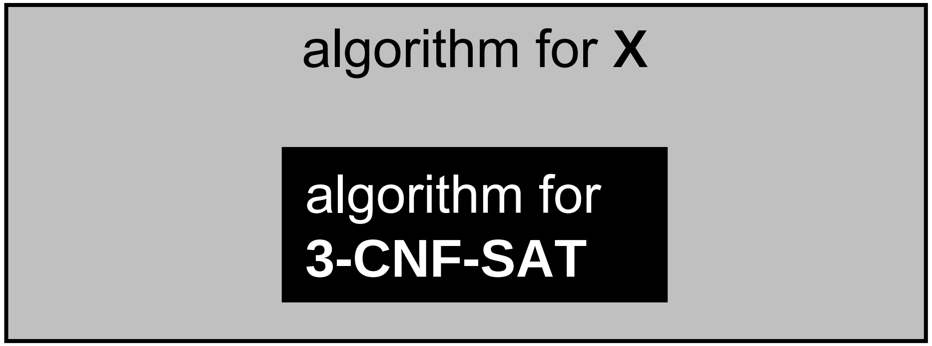
If a polynomial-time algorithm is discovered for **3-CNF-SAT** then a polynomial-time algorithm for **3-COLOR** easily follows

In fact, this holds for ***any*** problem **X** $\in$ **NP**, hence **3-CNF-SAT** is ***NP-hard*** ...

P vs. NP

All of the aforementioned problems have the property that they ***reduce*** to **3-CNF-SAT**, in the sense that a polynomial-time algorithm for **3-CNF-SAT** can be converted into a poly-time algorithm for the problem

Example:



If a polynomial-time algorithm is discovered for **3-CNF-SAT** then a polynomial-time algorithm for **3-COLOR** easily follows

In fact, this holds for ***any*** problem **X** $\in$ **NP**, hence **3-CNF-SAT** is ***NP-hard*** ... Also **NP-hard: CIRCUIT-SAT**, k-**COLOR**, ...

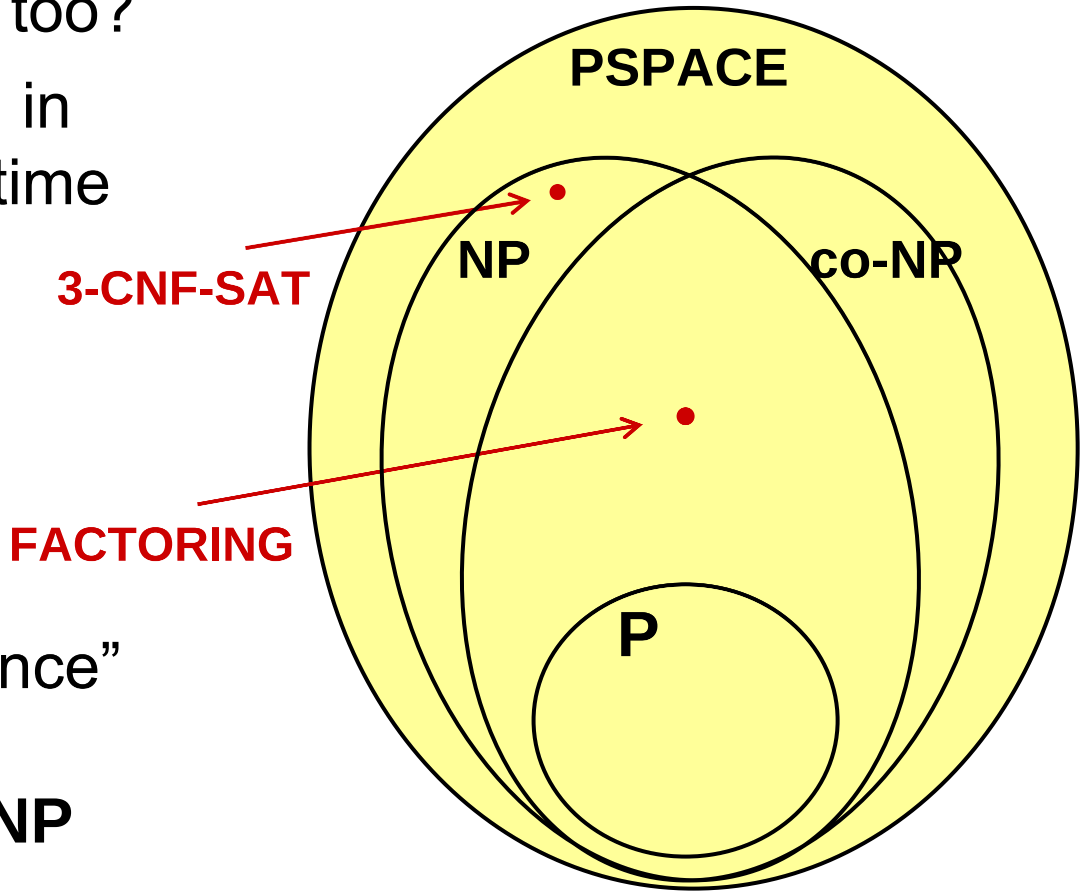
FACTORING vs. NP

Is **FACTORING NP**-hard too?

If so, then ***every*** problem in **NP** is solvable by a poly-time quantum algorithm!

But **FACTORING** has not been shown to be **NP**-hard

Moreover, there is "evidence" that it is not **NP**-hard: **FACTORING** $\in$ **NP**$\cap$**co-NP**



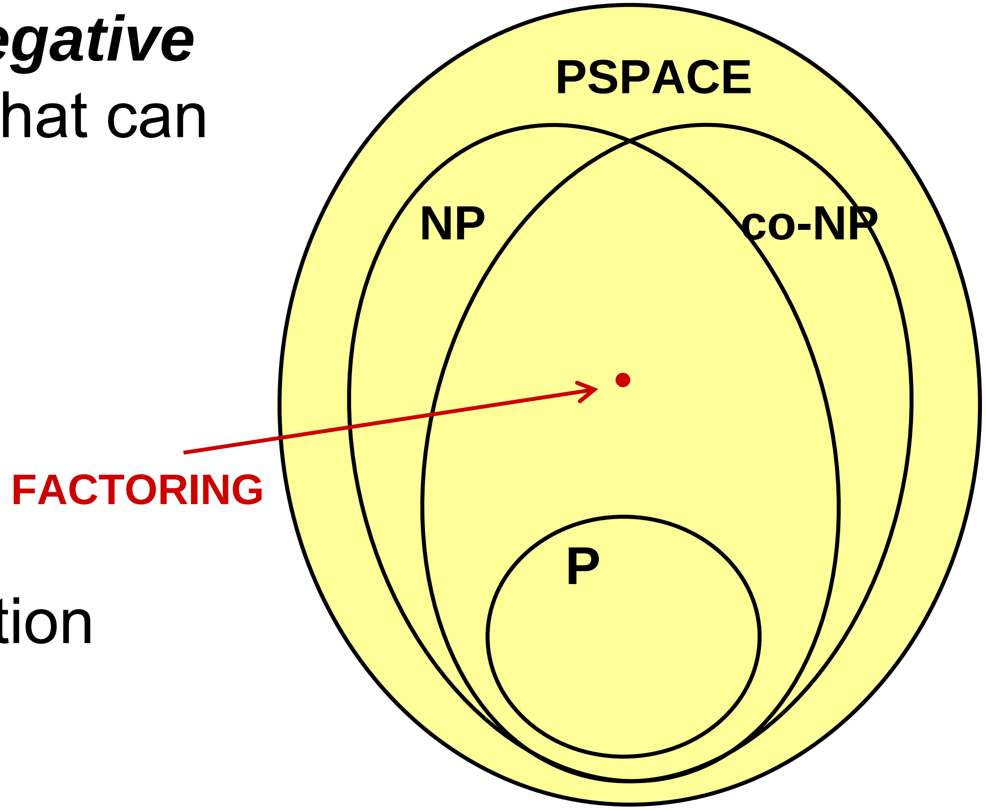
If **FACTORING** is **NP**-hard then **NP** = **co-NP**

FACTORING vs. co-NP

FACTORING $= \{(x, y) : \exists\, 2 \le z \le y,$ s.t. z divides $x\}$

co-NP: languages whose ***negative*** instances have "witnesses" that can be verified in poly-time

Question: what is a good witness for the negative instances?



Answer: the prime factorization $p_1, p_2, \ldots, p_m$ of x will work

Can verify primality and compare $p_1, p_2, \ldots, p_m$ with y, all in poly-time

- More state distinguishing problems
- Return to approximately universal gate sets
- Complexity classes
- Density matrix formalism

Density matrices (I)

Until now, we've represented quantum states as ***vectors*** (e.g. $|\psi\rangle$, and all such states are called ***pure states***)

An alternative way of representing quantum states is in terms of ***density matrices*** (a.k.a. ***density operators***)

The density matrix of a pure state $|\psi\rangle$ is the matrix $\rho = |\psi\rangle\langle\psi|$

Example: the density matrix of $\alpha|0\rangle + \beta|1\rangle$ is

$$\rho = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \begin{bmatrix} \alpha^* & \beta^* \end{bmatrix} = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix}$$

Density matrices (II)

How do quantum operations work using density matrices?

Effect of a unitary operation on a density matrix:

applying U to ρ yields $U\rho U^\dagger$

(this is because the modified state is $U|\psi\rangle\langle\psi|U^\dagger$)

Effect of a measurement on a density matrix:

measuring state ρ with respect to the basis $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_d\rangle$, yields the k^{th} outcome with probability $\langle\varphi_k|\rho|\varphi_k\rangle$

(this is because $\langle\varphi_k|\rho|\varphi_k\rangle = \langle\varphi_k|\psi\rangle\langle\psi|\varphi_k\rangle = |\langle\varphi_k|\psi\rangle|^2$)

—and the state collapses to $|\varphi_k\rangle\langle\varphi_k|$

Density matrices (III)

A probability distribution on pure states is called a ***mixed state***:

$\big((|\psi_1\rangle, p_1), (|\psi_2\rangle, p_2), \ldots, (|\psi_d\rangle, p_d) \big)$

The ***density matrix*** associated with such a mixed state is:

$$\rho = \sum_{k=1}^{d} p_k |\psi_k\rangle\langle\psi_k|$$

Example: the density matrix for $\big((|0\rangle, ½), (|1\rangle, ½) \big)$ is:

$$\frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Question: what is the density matrix of

$\big((|0\rangle + |1\rangle, ½), (|0\rangle - |1\rangle, ½) \big)$?

Density matrices (IV)

How do quantum operations work for these ***mixed*** states?

Effect of a unitary operation on a density matrix:

applying U to ρ ***still*** yields $U\rho U^{\dagger}$

This is because the modified state is:

$$\sum_{k=1}^{d} p_k U \left| \psi_k \right\rangle\!\left\langle \psi_k \right| U^t = U \left(\sum_{k=1}^{d} p_k \left| \psi_k \right\rangle\!\left\langle \psi_k \right| \right) U^t = U \rho U^t$$

Effect of a measurement on a density matrix:

measuring state ρ with respect to the basis $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_d\rangle$,
still yields the k^{th} outcome with probability $\langle\varphi_k|\rho|\varphi_k\rangle$

Why?

THE END