Reversible gates

- Landauer's Principle: Suppose a computer erases a single bit of information. The amount of energy dissipated into the environment is (the entropy of the environment increases by) *at least* $k_B T \ln 2$, where k_B is Boltzmann's constant and T is the temperature of the surrounding environment.

- Computers currently dissipate on the order of $500 k_B T \ln 2$ in energy for each elementary logical operation, so we are nowhere near the lower bound set by Landauer's Principle.

- Useful facts about XOR:

  $z \oplus z = 0$

  $z \oplus 0 = z$

  $z \oplus 1 = \text{NOT } z$

- AND, OR, NAND, NOR, XOR, and XNOR are not reversible.

- How to make XOR reversible? Add an extra output that just copies the x input:

x	y	x XOR y
0	0	0
0	1	1
1	0	1
1	1	0

x	y	x	x XOR y
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

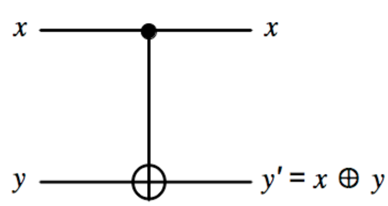
- Reversible XOR is called the *controlled-NOT* or CNOT gate. Inputs: x and y. Outputs: x (unchanged) and $y' = x \oplus y$. Input x acts as a control bit. When $x = 1$, y is negated, since $1 \oplus y = \text{NOT } y$. Otherwise y is unchanged, since $0 \oplus y = y$.

  $CNOT : |x, y\rangle \rightarrow |x, x \oplus y\rangle$

  Matrix representation:

  $$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

  Gate symbol:



- $CNOT \star CNOT = IDEN$

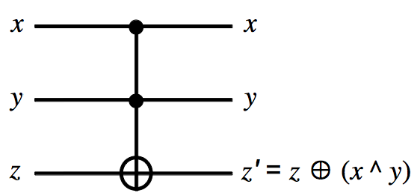
- If we apply $CNOT$ to an input vector V, we can undo the effect by applying another $CNOT$ operation:

  $CNOT \star CNOT \star V = IDEN \star V = V$

- **Toffoli gate**: controlled-controlled-NOT ($CCNOT$). Inputs: x, y, z. Outputs: x', y', z'. Inputs x and y act as control bits, which are just copied to the outputs x' and y'. When $x = 1$ and $y = 1$, z is negated, since $z \oplus 1 = \text{NOT } z$. Otherwise z is unchanged, since $z \oplus 0 = z$.

x	y	z	x' = x	y' = y	z' = z XOR (x AND y)
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

- Gate symbol:



- NOT from a Toffoli gate: set $x = 1$, $y = 1$ (just delete all rows from Toffoli truth table with $x = 0$ or $y = 0$):

x	y	z	x'	y'	z' = NOT z
1	1	0	1	1	1
1	1	1	1	1	0

- AND from a Toffoli gate: set $z = 0$ (just delete rows with $z = 1$ from Toffoli truth table):

x	y	z	x'	y'	z' = x AND y
0	0	0	0	0	0
0	1	0	0	1	0
1	0	0	1	0	0
1	1	0	1	1	1

- COPY from a Toffoli gate: set $x = 1$, $z = 0$ (just delete all rows from Toffoli truth table with $x = 0$ or $z = 1$). Input y gets copied to outputs y' and z':

x	y	z	x'	y'	z'
1	0	0	1	0	0
1	1	0	1	1	1

- **Fredkin gate**: controlled-SWAP

  $|0, y, z\rangle \to |0, y, z\rangle$

  $|1, y, z\rangle \to |1, z, y\rangle$

  When $x = 1$, the inputs y and z are swapped. Otherwise they are unchanged. Truth table:

x	y	z	x	y'	z'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

- AND from Fredkin: set $y = 0$ (delete all rows with $y = 1$). Output $y' = x$ AND z

x	y	z	x	y' = x AND z	z'
0	0	0	0	0	0
0	0	1	0	0	1
1	0	0	1	0	0
1	0	1	1	1	0

- NOT and COPY from Fredkin: set $y = 1$, $z = 0$. Output $y' =$ NOT x. Input x gets copied to outputs x and z':

x	y	z	x	y' = NOT x	z'
0	1	0	0	1	0
1	1	0	1	0	1

- Since we can make NOT and AND, we can make NAND, so we can make anything from Fredkin gates.