Answers to Homework Assignment #3

ANSWER TO QUESTION 1.
(a) For n a power of 2, the recurrence becomes:

$$S(n) = \begin{cases} C, & \text{if } n = 1 \\ 7 \cdot S\left(\frac{n}{2}\right) + D\left(\frac{n}{2}\right)^2, & \text{if } n > 1 \end{cases}$$

By repeated substitution to the definition of S we get:

$$\begin{aligned}
S(n) &= 7S\left(\frac{n}{2}\right) + D\left(\frac{n}{2}\right)^2 \\
&= 7\left(7S\left(\frac{n}{2^2}\right) + D\left(\frac{n}{2^2}\right)^2\right) + D\frac{1}{4}n^2 \\
&= 7^2 S\left(\frac{n}{2^2}\right) + D\frac{7}{4^2}n^2 + D\frac{1}{4}n^2 \\
&= 7^2\left(7S\left(\frac{n}{2^3}\right) + D\left(\frac{n}{2^3}\right)^2\right) + D\frac{7}{4^2}n^2 + D\frac{1}{4}n^2 \\
&= 7^3 S\left(\frac{n}{2^3}\right) + D\frac{7^2}{4^3}n^2 + D\frac{7}{4^2}n^2 + D\frac{1}{4}n^2 \\
&\cdots \\
&= 7^i S\left(\frac{n}{2^i}\right) + \frac{D}{4}\left(\left(\frac{7}{4}\right)^{i-1} + \left(\frac{7}{4}\right)^{i-2} + \cdots + \left(\frac{7}{4}\right)^2 + \left(\frac{7}{4}\right) + 1\right) n^2 \\
&= 7^i S\left(\frac{n}{2^i}\right) + D\left(\frac{7^i - 4^i}{3 \cdot 4^i}\right) n^2.
\end{aligned}$$

This informal derivation suggests that we should prove the following:

Claim. If n is a power of 2 then, for any i such that $0 \le i \le \log_2 n$,

$$S(n) = 7^i S\left(\frac{n}{2^i}\right) + D\left(\frac{7^i - 4^i}{3 \cdot 4^i}\right) n^2$$

PROOF. Let $P(i)$ be the following predicate:

$$P(i): \qquad S(n) = 7^i S\left(\frac{n}{2^i}\right) + D\left(\frac{7^i - 4^i}{3 \cdot 4^i}\right) n^2$$

We will prove that $P(i)$ is true for each integer i such that $0 \le i \le \log_2 n$, using induction.
BASIS: $i = 0$. We have,

$$\begin{aligned}
&7^0 S\left(\frac{n}{2^0}\right) + D\left(\frac{7^0 - 4^0}{3 \cdot 4^0}\right) n^2 \\
&= S(n) + D \cdot 0 \cdot n^2 \\
&= S(n)
\end{aligned}$$

INDUCTION STEP: Let j be an arbitrary integer such that $0 \leq j < \log_2 n$. Assume that $P(j)$ holds. We will prove that $P(j+1)$ holds as well. Since $j < \log_2 n$, it follows that $2^j < n$ and so $n/2^j > 1$. We have:

$$\begin{aligned}
S(n) &= 7^j S\left(\frac{n}{2^j}\right) + D\left(\frac{7^j - 4^j}{3 \cdot 4^j}\right) n^2 && \text{[by i.h.]} \\
&= 7^j \left(7S\left(\frac{n}{2^{j+1}}\right) + D\left(\frac{n}{2^{j+1}}\right)^2\right) + D\left(\frac{7^j - 4^j}{3 \cdot 4^j}\right) n^2 && \text{[by def. of } S \text{, since } n/2^j > 1] \\
&= 7^{j+1} S\left(\frac{n}{2^{j+1}}\right) + D\left(\frac{7^j}{4^{j+1}} + \frac{7^j - 4^j}{3 \cdot 4^j}\right) n^2 \\
&= 7^{j+1} S\left(\frac{n}{2^{j+1}}\right) + D\left(\frac{7^{j+1} - 4^{j+1}}{3 \cdot 4^{j+1}}\right) n^2
\end{aligned}$$

This concludes the proof of the claim.

Letting $i = \log_2 n$ in the claim we obtain our exact formula for $S(n)$, when n is a power of 2:

$$\begin{aligned}
S(n) &= 7^{\log_2 n} S(1) + D\left(\frac{7^{\log_2 n} - 4^{\log_2 n}}{3 \cdot 4^{\log_2 n}}\right) n^2 \\
&= C n^{\log_2 7} + D\left(\frac{n^{\log_2 7} - n^2}{3 \cdot n^2}\right) n^2 \\
&= C n^{\log_2 7} + \frac{D}{3}(n^{\log_2 7} - n^2) \\
&= \left(C + \frac{D}{3}\right) n^{\log_2 7} - \frac{D}{3} n^2
\end{aligned}$$

(b) Since $\log_2 7 > 2$, the above exact expression for $S(n)$ when n is a power of 2 implies that $S(2^k) \in \Theta\big((2^k)^{\log_2 7}\big)$. We will prove below that $S(n)$ is nondecreasing. Finally, $(2n)^{\log_2 7} = 7n^{\log_2 7} \in \Theta(n^{\log_2 7})$. From these three facts and Theorem 3.8 we conclude that $S(n) \in \Theta(n^{\log_2 7})$.

To prove that $S(n)$ is nondecreasing, it suffices to prove that the following predicate $P(n)$ holds for all positive integers n.

$$P(n): \qquad \text{for every integer } m \text{ such that } 1 \leq m \leq n,\ S(m) \leq S(n)$$

We use complete induction. Let k be an arbitrary positive integer. Assume that $P(j)$ holds for all integers j such that $1 \leq j < k$. We will prove that $P(k)$ also holds.

CASE 1. $1 \leq k \leq 2$. $P(1)$ is trivially true. From the definition of S we have: $S(1) = C$ and $S(2) = 7S(1) + D = 7C + D$. Assuming that $C, D \geq 0$ (an assumption that was incorrectly omitted from the statement of the problem!) we have that $S(1) \leq S(2)$, and so $P(2)$ holds.

CASE 2. $k > 2$. Note that in this case $k - 1 > 1$, $\lceil (k-1)/2 \rceil > 0$, and $\lceil k/2 \rceil < k$ (the last inequality is true because an easy proof by cases shows that, for any $n > 1$, $\lceil n/2 \rceil < n$). By induction hypothesis and transitivity of $\leq$, it suffices to prove that $S(k-1) \leq S(k)$. We have:

$$\begin{aligned}
S(k-1) &= 7S\big(\lceil (k-1)/2 \rceil\big) + D\lceil (k-1)/2 \rceil^2 && \text{[by def. of } S \text{, since } k-1 > 1] \\
&\leq 7S(\lceil k/2 \rceil) + D\lceil k/2 \rceil^2 && \text{[by i.h., since } 0 < \lceil (k-1)/2 \rceil \leq \lceil k/2 \rceil < k] \\
&= S(k)
\end{aligned}$$

ANSWER TO QUESTION 2. Let F_i, where $0 \le i \le 3$, be the bit in position i of the sum $x+y$, and let c_i, where $0 \le i \le 2$, be the carry out of position i. According to the algorithm for binary addition (see page 102 of the notes) we have:

$$\begin{aligned}
F_0 &= x_0 \oplus y_0 \\
c_0 &= x_0 \wedge y_0 \\
F_1 &= x_0 \oplus y_0 \oplus c_0 \\
&= x_0 \oplus y_0 \oplus (x_0 \wedge y_0) \\
c_1 &= (x_1 \wedge y_1) \vee \big(c_0 \wedge (x_1 \vee y_1)\big) \\
&= (x_1 \wedge y_1) \vee \big(x_0 \wedge y_0 \wedge (x_1 \vee y_1)\big) \\
F_2 &= x_1 \oplus y_1 \oplus c_1 \\
&= x_1 \oplus y_1 \oplus \Big((x_1 \wedge y_1) \vee \big(x_0 \wedge y_0 \wedge (x_1 \vee y_1)\big)\Big) \\
c_2 = F_3 &= (x_2 \wedge y_2) \vee \big(c_1 \wedge (x_2 \vee y_2)\big) \\
&= (x_2 \wedge y_2) \vee \bigg(\Big((x_1 \wedge y_1) \vee \big(x_0 \wedge y_0 \wedge (x_1 \vee y_1)\big)\Big) \wedge (x_2 \vee y_2)\bigg)
\end{aligned}$$

ANSWER TO QUESTION 3.

(a)

	$(x \leftrightarrow \neg y) \rightarrow \neg(x \rightarrow y)$	
LEQV	$\neg(x \leftrightarrow \neg y) \vee \neg(\neg x \vee y)$	[$\rightarrow$-law, twice]
LEQV	$\neg\big((x \wedge \neg y) \vee (\neg x \wedge y)\big) \vee (x \wedge \neg y)$	[$\leftrightarrow$-law, double neg., DeMorgan]
LEQV	$\big(\neg(x \wedge \neg y) \wedge \neg(\neg x \wedge y)\big) \vee (x \wedge \neg y)$	[DeMorgan]
LEQV	$\big((\neg x \vee y) \wedge (x \vee \neg y)\big) \vee (x \wedge \neg y)$	[DeMorgan and double neg., twice]
LEQV	$\big((\neg x \wedge x) \vee (\neg x \wedge \neg y) \vee (y \wedge x) \vee (y \wedge \neg y)\big) \vee (x \wedge \neg y)$	[distributivity]
LEQV	$(\neg x \wedge \neg y) \vee (x \wedge y) \vee (x \wedge \neg y)$	[identity (twice), commut., assoc.]
LEQV	$(\neg x \wedge \neg y) \vee \big(x \wedge (y \vee \neg y)\big)$	[distributivity]
LEQV	$(\neg x \wedge \neg y) \vee x$	[identity]
LEQV	$(\neg x \vee x) \wedge (\neg y \vee x)$	[distributivity]
LEQV	$\neg y \vee x$	[identity]
LEQV	$y \rightarrow x$	[$\rightarrow$-law]

(b) This logical equivalence is valid as the following derivation shows.

	$(x \rightarrow y) \wedge (x \rightarrow z)$	
LEQV	$(\neg x \vee y) \wedge (\neg x \vee z)$	[$\rightarrow$-law, twice]
LEQV	$\neg x \vee (y \wedge z)$	[distributivity]
LEQV	$x \rightarrow (y \wedge z)$	[$\rightarrow$-law]

(c) This logical equivalence does not hold. Consider the truth assignment τ that makes y true and makes x and z false. (That is, $\tau(y) = 1$ and $\tau(x) = \tau(z) = 0$.) This truth assignment falsifies $y \rightarrow x$ and so it falsifies the conjunction $(y \to x) \wedge (z \to x)$. On the other hand this truth assignment falsifies $(y \wedge z)$ and so it satisfies the conditional $(y \wedge z) \to x$. Since there is a truth assignment that falsifies $(y \to x) \wedge (z \to x)$ and satisfies $(y \wedge z) \to x$, these two formulas are not logically equivalent.

ANSWER TO QUESTION 4. Let $S(n)$ be the following predicate:

$$S(n): \quad \text{for } \textit{any } n \text{ propositional formulas } P_1, \dots, P_n,$$
$$P_1 \to (P_2 \to (\cdots \to (P_{n-1} \to P_n) \cdots)) \ \text{LEQV} \ (P_1 \wedge P_2 \wedge \cdots \wedge P_{n-1}) \to P_n$$

We prove that $S(n)$ holds for all integers $n \geq 2$ by induction.

Basis: $n = 2$. $S(2)$ asserts that for any two propositional formulas P_1 and P_2, $P_1 \to P_2$ LEQV $P_1 \to P_2$, which is trivially true, so $S(2)$ holds.

Induction Step: Let $k \geq 2$ be an arbitrary integer. Suppose that $S(k)$ holds. We will prove that so does $S(k+1)$. Let $P_1, P_2, \dots, P_{k+1}$ be any $k+1$ propositional formulas. By induction hypothesis, the following is true about the k propositional formulas $P_2, \dots, P_{k+1}$:

$$P_2 \to (\cdots \to (P_k \to P_{k+1})) \quad \text{LEQV} \quad (P_2 \wedge \cdots \wedge P_k) \to P_{k+1}$$

Therefore, we have:

$$\begin{array}{lll}
 & P_1 \to (P_2 \to (\cdots \to (P_k \to P_{k+1}) \cdots)) & \\
\text{LEQV} & P_1 \to ((P_2 \wedge \cdots \wedge P_k) \to P_{k+1}) & [\text{by i.h.}] \\
\text{LEQV} & \neg P_1 \vee (\neg(P_2 \wedge \cdots \wedge P_k) \vee P_{k+1}) & [\to\text{-law, applied twice}] \\
\text{LEQV} & (\neg P_1 \vee \neg(P_2 \wedge \cdots \wedge P_k)) \vee P_{k+1} & [\text{associativity of } \vee] \\
\text{LEQV} & \neg(P_1 \wedge (P_2 \wedge \cdots \wedge P_k)) \vee P_{k+1} & [\text{DeMorgan's law}] \\
\text{LEQV} & \neg(P_1 \wedge P_2 \wedge \cdots \wedge P_k) \vee P_{k+1} & [\text{associativity of } \wedge] \\
\text{LEQV} & (P_1 \wedge P_2 \wedge \cdots \wedge P_k) \to P_{k+1} & [\to\text{-law}]
\end{array}$$

as wanted.

ANSWER TO QUESTION 5.

(a) These formulas can be written directly from inspection. For DNF we write one minterm for each line in the truth table for which Parity(x, y, z) has value 1. The result is

$$(\neg x \wedge \neg y \wedge z) \vee (\neg x \wedge y \wedge \neg z) \vee (x \wedge \neg y \wedge \neg z) \vee (x \wedge y \wedge z) \ .$$

For CNF we write one maxterm for each line in the truth table for which Parity(x, y, z) has value 0. The result is

$$(x \vee y \vee z) \wedge (x \vee \neg y \vee \neg z) \wedge (\neg x \vee y \vee \neg z) \wedge (\neg x \vee \neg y \vee z) \ .$$

(b) The following logical equivalences can be proved in a variety of ways (including truth tables):

$$\begin{array}{rcll}
\neg P & \text{LEQV} & (P \downarrow P) & [\text{E1}] \\
(P \vee Q) & \text{LEQV} & \big((P \downarrow Q) \downarrow (P \downarrow Q)\big) & [\text{E2}] \\
\neg(P \vee Q \vee R) & \text{LEQV} & \big((P \downarrow Q) \downarrow (P \downarrow Q)\big) \downarrow R & [\text{E3}]
\end{array}$$

Using E1 and E3, we can convert each minterm of the DNF formula into an equivalent formula that uses only $\downarrow$:

$$
\begin{array}{lll}
 & (\neg x \wedge \neg y \wedge z) & \\
\text{LEQV} & \neg(x \vee y \vee \neg z) & \text{[DeMorgan and associativity]} \\
\text{LEQV} & \big((x \downarrow y) \downarrow (x \downarrow y)\big) \downarrow \neg z & \text{[E3]} \\
\text{LEQV} & \underbrace{\big((x \downarrow y) \downarrow (x \downarrow y)\big) \downarrow (z \downarrow z)}_{T_1} & \text{[E1]}
\end{array}
$$

Similarly,

$$
\begin{array}{rcl}
(\neg x \wedge y \wedge \neg z) & \text{LEQV} & \underbrace{\big((x \downarrow z) \downarrow (x \downarrow z)\big) \downarrow (y \downarrow y)}_{T_2} \\
(x \wedge \neg y \wedge \neg z) & \text{LEQV} & \underbrace{\big((y \downarrow z) \downarrow (y \downarrow z)\big) \downarrow (x \downarrow x)}_{T_3} \\
(x \wedge y \wedge z) & \text{LEQV} & \underbrace{\Big(\big((x \downarrow x) \downarrow (y \downarrow y)\big) \downarrow \big((x \downarrow x) \downarrow (y \downarrow y)\big)\Big) \downarrow (z \downarrow z)}_{T_4}
\end{array}
$$

Thus, the DNF formula for Parity(x, y, z) is logically equivalent to $T_1 \vee T_2 \vee T_3 \vee T_4$, where T_1, T_2, T_3, T_4 are formulas that use only $\downarrow$. We have:

$$
\begin{array}{lll}
 & T_1 \vee T_2 \vee T_3 \vee T_4 & \\
\text{LEQV} & (T_1 \vee T_2) \vee (T_3 \vee T_4) & \text{[associativity of } \vee\text{]} \\
\text{LEQV} & \underbrace{\big((T_1 \downarrow T_2) \downarrow (T_1 \downarrow T_2)\big)}_{W_1} \vee \underbrace{\big((T_3 \downarrow T_4) \downarrow (T_3 \downarrow T_4)\big)}_{W_2} & \text{[E2]} \\
\text{LEQV} & (W_1 \downarrow W_2) \downarrow (W_1 \downarrow W_2) & \text{[E2]}
\end{array}
$$

W_1 and W_2 use only $\downarrow$ (because T_1, T_2, T_3 and T_4 do), and so the last expression is a formula that uses only $\downarrow$ and is logically equivalent to the DNF formula that represents Parity(x, y, z). For what it's worth, here is the formula written out in full: $(((((x \downarrow y) \downarrow (x \downarrow y)) \downarrow (z \downarrow z)) \downarrow (((x \downarrow z) \downarrow (x \downarrow z)) \downarrow (y \downarrow y))) \downarrow ((((x \downarrow y) \downarrow (x \downarrow y)) \downarrow (z \downarrow z)) \downarrow (((x \downarrow z) \downarrow (x \downarrow z)) \downarrow (y \downarrow y))) \downarrow ((((y \downarrow z) \downarrow (y \downarrow z)) \downarrow (x \downarrow x)) \downarrow ((((x \downarrow x) \downarrow (y \downarrow y)) \downarrow ((x \downarrow x) \downarrow (y \downarrow y))) \downarrow (z \downarrow z))) \downarrow ((((y \downarrow z) \downarrow (y \downarrow z)) \downarrow (x \downarrow x)) \downarrow ((((x \downarrow x) \downarrow (y \downarrow y)) \downarrow ((x \downarrow x) \downarrow (y \downarrow y))) \downarrow (z \downarrow z)))) \downarrow (((((x \downarrow y) \downarrow (x \downarrow y)) \downarrow (z \downarrow z)) \downarrow (((x \downarrow z) \downarrow (x \downarrow z)) \downarrow (y \downarrow y))) \downarrow ((((x \downarrow y) \downarrow (x \downarrow y)) \downarrow (z \downarrow z)) \downarrow (((x \downarrow z) \downarrow (x \downarrow z)) \downarrow (y \downarrow y))) \downarrow ((((y \downarrow z) \downarrow (y \downarrow z)) \downarrow (x \downarrow x)) \downarrow ((((x \downarrow x) \downarrow (y \downarrow y)) \downarrow ((x \downarrow x) \downarrow (y \downarrow y))) \downarrow (z \downarrow z))) \downarrow ((((y \downarrow z) \downarrow (y \downarrow z)) \downarrow (x \downarrow x)) \downarrow ((((x \downarrow x) \downarrow (y \downarrow y)) \downarrow ((x \downarrow x) \downarrow (y \downarrow y))) \downarrow (z \downarrow z))))$.