CSE20-SP12 Midterm 2 ((May 15, 2012) Solution

1. Residual Number System:
1.1 State the Chinese remainder theorem. (5 points)

Given a residual number $(r_1, r_2 \ldots r_k)$ with moduli $(m_1, m_2 \ldots m_k)$, where all m_i are mutually prime. We set

$$M = m_1 \times m_2 \times \ldots m_k, M_i = M/m_i \textbf{ (1 point)}$$

and

- Find S_i such that $(M_i \times S_i)\%m_i = 1$, where S_i is an inverse of M_i in mod m_i. **(2 point)**
- The corresponding number $X = \sum_{i=1}^{k}(M_i S_i r_i))\%M$. **(2 point)**

1.2 Prove the Chinese remainder theorem. (10 points)

Let $A = \sum_{i=1}^{k}(M_i S_i r_i)$, we need to show that

- $A\%m_v = r_v$ **(2 point)**
- $x = A\%M$ is unique **(2 point)**

Proof for $A\%m_v = r_v$ is shown as below. **(3 point)**

$$\begin{aligned} A\%m_v &= [\sum_{i=1}^{k}(M_i S_i r_i)]\%m_v \\ &= [\sum_{i=1}^{k}(M_i S_i r_i)]\%m_v]\%m_v \\ &= (M_v S_v r_v)\%m_v \\ &= [(M_v S_v)\%m_v \times r_v\%m_v]\%m_v \\ &= r_v\%m_v \\ &= r_v \end{aligned} \tag{1}$$

Proof for $x = A\%M$ is unique is shown as below. **(3 point)**
By contradiction, suppose that there is another integer such that we have $0 \leq y < x < M$ and $y : (y_1, y_2 \ldots y_k)$, where $y_i = y\%m_i$, and

$$(r_1, r_2 \ldots r_k) = (y_1, y_2 \ldots y_k)$$

As a result, we have

$$(x-y) : (r_1 - y_1 \ldots r_k - y_k) = (0 \ldots 0)$$

Since

$$\forall i \in [1,k], (x-y) \bmod m_i \equiv 0$$

we have

$$\forall i \in [1,k], (x-y) = k_i m_i$$

Since $\forall i, j \in 1 \ldots k$, m_i and m_j are mutually prime, we have

$$(x-y) = k' \prod_{i=1}^{k}(m_i) = k'M$$

where k' is an integer. As $0 \leq y < x < M$ thus $0 \leq x - y < M$, we could only have $x - y = 0$ thus $x = y$, which contradicts.
As a result, $x = A\%M$ is unique.

2. Residual Number System: Show the operation of 21×18 in a residual number system with moduli $(m_1, m_2, m_3) = (7, 8, 9)$ (no need to convert the residual number back to integer). (10 points)

$$21 \rightarrow (21\%7, 21\%8, 21\%9) = (0, 5, 3) \textbf{ (3 point)}$$
$$18 \rightarrow (18\%7, 18\%8, 18\%9) = (4, 2, 0) \textbf{ (3 point)}$$
$$21 \times 18 = (0,5,3) \times (4,2,0) = ((0 \times 4)\%7, (5 \times 2)\%8, (3 \times 0)\%9) = (0,2,0) \textbf{ (4 point)}$$

3. Cryptography (RSA Protocol): In a RSA protocol, we have the public key (e, N), where $N = 5 \times 11$ and $e = 27$.
3.1 Derive the secret key (d, N). (10 points)

$$N = 5 \times 11 = p \times q \Rightarrow p = 5, q = 11 \textbf{ (1 point)}$$
$$f(N) = (p-q) \times (q-1) = 4 \times 10 = 40 \textbf{ (3 point)}$$
$$(ed) \bmod f(N) = (27d) \bmod (40) = 1 \textbf{ (3 point)}$$

We then find that $d = 3$ satisfies the above equation. Thus the secret key is $(d, N) = (3, 55)$. **(3 point)**

3.2 Suppose that the receiver obtains an encrypted message $P(M) = M^e\%N = 2$. Decrypt the message M. (5 points)

We have $P(M) = 2$ and $d = 3$, and $M = (P(M))^d\%N$ **(2 point)** so

$$M = 2^3\%55 = 8\%55 = 8 \textbf{ (3 point)}$$

4. Boolean Algebra: Show that Boolean algebra is valid for set operations (hint: state the definition of Boolean algebra and use Venn diagram to verify the four laws)? (10 points)

Boolean Algebra Definition.
A set of elements B with the following two operations. **(2 point)**

- $+(OR, \cup, \vee)$
- $*(AND, \cap, \wedge)$

It satisfies the following 4 laws for every $a, b, c \in B$. **(4 point)**

- P1. Commutative Laws:

$$a + b = b + a; a * b = b * a \textbf{ (1 point)}$$

- P2. Distributive Laws:

$$a + (b * c) = (a + b) * (a + c) \textbf{ (0.5 point)}$$
$$a * (b + c) = (a * b) + (a * c) \textbf{ (0.5 point)}$$

- P3. Identity Elements: Set B has two distinct elements denoted as 0 and 1, such that

$$a+0=a; a*1=a \textbf{ (1 point)}$$

- P4. Complement Laws:

$$a+a'=1; a*a'=0 \textbf{ (1 point)}$$

Set operations using Venn's diagrams. **(4 point)**

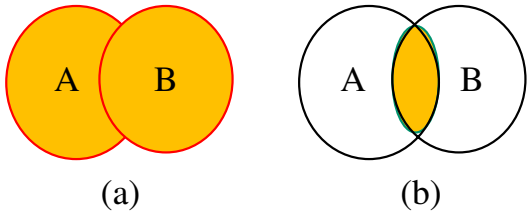

Figure 1: Commutative laws in Venn diagram.

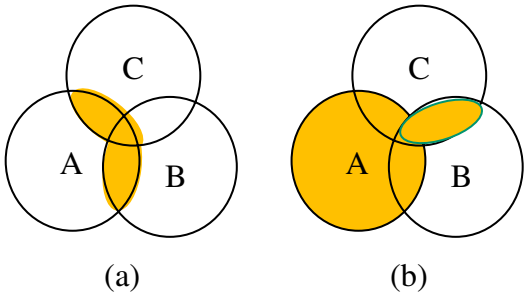

Figure 2: Distributive laws in Venn diagram.

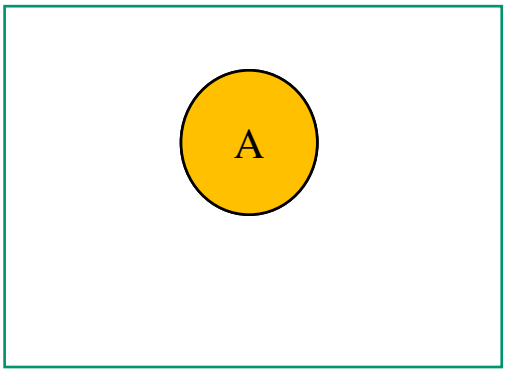

Figure 3: Identity elements in Venn diagram.

- P1. Commutative Laws:
  $A \cup B = B \cup A$ as illustrate in Figure 1(a) **(0.5 point)**
  $A \cap B = B \cap A$ as illustrate in Figure 1(b) **(0.5 point)**

- P2. Distributive Laws:
  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ as illustrate in Figure 2(a) **(0.5 point)**
  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ s illustrate in Figure 2(b) **(0.5 point)**

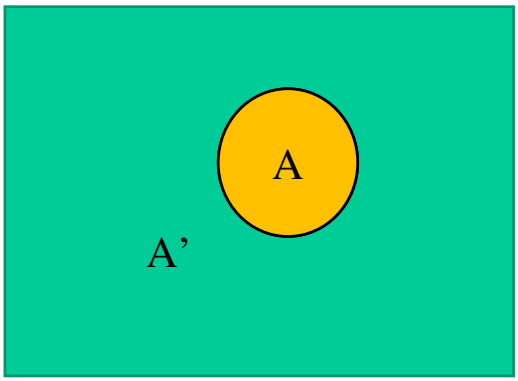

Figure 4: Complement laws in Venn diagram.

- P3. Identity Elements:
  $0 = \{\}, 1 =$ universe of the set.
  We have $A \cup 0 = A$ and $A \cap 1 = A$, as illustrate in Figure 3. **(1 point)**

- P3. Complement Laws:
  $A \cup A' = 1, A \cap A' = 0$ as illustrate in Figure 4. **(1 point)**

5. Boolean Algebra: Prove the associative theorem, i.e. $a + (b + c) = (a + b) + c$ for every a, b, c elements in Boolean algebra B. (15 points)

Denote $x = a + (b + c)$ and $y = (a + b) + c$, our proof comprises the following two steps.

1. We first prove $ax = ay$ and $a'x = a'y$.
2. Based on 1) we then prove $x = y$.

We first prove that $ax = ay$ as below.

$$\begin{aligned}
ax &= a(a + (b + c)) && (distributive) \\
&= aa + a(b + c) && (idempotence) \\
&= a + a(b + c) && (absorption) \\
&= a && \textbf{(3 points)} \\
ay &= a((a + b) + c) && (distributive) \\
&= a(a + b) + ac && (distributive) \\
&= (aa + ab) + ac && (idempotence) \\
&= (a + ab) + ac && (absorption) \\
&= a + ac && (absorption) \\
&= a && \textbf{(3 points)}
\end{aligned} \tag{2}$$

So we have $ax = ay = a$.
Similarly, we prove $a'x = a'y$ as below.

$$
\begin{aligned}
a'x &= a'(a+(b+c)) && (distributive)\\
&= a'a+a'(b+c) && (complement)\\
&= 0+a'(b+c) && (identity)\\
&= a'(b+c) && \textbf{(3 points)}\\
a'y &= a'((a+b)+c) && (distributive)\\
&= a'(a+b)+a'c && (theorem8)\\
&= a'b+a'c && (distributive)\\
&= a'(b+c) && \textbf{(3 points)}
\end{aligned}
\tag{3}
$$

So we have $a'x = a'y = a'(b+c)$.
As we have

$$x = 1*x = (a+a')x = ax+a'x = ay+a'y = (a+a')y = 1*y = y$$

thus $x = a+(b+c) = (a+b)+c = y$. **(3 points)**

If you provide some ideas,
but fail to prove the whole theorem,
you can get 1 to 3 points.

6. Boolean Algebra: Transform Boolean function, $E(a,b,c) = ac+bc+a'b$, into a minimal number of literals. (10 points)

Solution 1:

$$
\begin{aligned}
E(a,b,c) &= ac+bc+a'b && (identity)\\
&= ac+1*bc+a'b && (complement)\\
&= ac+(a+a')bc+a'b && (distributive)\\
&= ac+abc+a'bc+a'b && (associative)\\
&= (ac+acb)+(a'bc+a'b) && (absorption)\\
&= ac+a'b
\end{aligned}
\tag{4}
$$

Solution 2:

$$
\begin{aligned}
E(a,b,c) &= ac+bc+a'b && (identity)\\
&= ac+0+bc+a'b && (complement)\\
&= ac+aa'+bc+ba' && (distributive)\\
&= a(a'+c)+b(a'+c) && (distributive)\\
&= (a+b)(a'+c)
\end{aligned}
\tag{5}
$$

Each step of reduction gets 2 points.
If you get correct solution but fail to provide
postulates or theorems, you can get 9 points.
If you fail to minimize the number of literals,
but have correct reduction and indication of
postulates and theorems being used at each step,
you can get 1 to 4 points.

7. Boolean Algebra: Reduce the following to an expression of a minimal number of literals: $E(a,b,c) = ac'+b'c+a'b'c'+a'bc$. (hint number of literals ≤ 5) (15 points)

Solution 1:

$$
\begin{aligned}
E(a,b,c) &= ac' + b'c + a'b'c' + a'bc && (commutative) \\
&= ac' + a'b'c' + b'c + a'bc && (associative) \\
&= (ac' + a'b'c') + (b'c + a'bc) && (distributive) \\
&= (a + a'b')c' + (b' + a'b)c && (theorem 8) \\
&= (a + b')c' + (b' + a')c && (distributive) \\
&= ac' + b'c' + b'c + a'c && (associative) \\
&= ac' + (b'c' + b'c) + a'c && (distributive) \\
&= ac' + b'(c' + c) + a'c && (complement) \\
&= ac' + b' * 1 + a'c && (identity) \\
&= ac' + a'c + b'
\end{aligned}
\tag{6}
$$

Each step of reduction gets 1 to 2 points.
If you make wrong reduction at intermediate steps,
you can get up to 12 points.
If you get correct solution but fail to provide
postulates or theorems, you can get 13 points.
If you fail to minimize the number of literals,
but have correct reduction and indication of
postulates and theorems being used at each step,
you can get 1 to 6 points.

8. Boolean Algebra: Given the logic circuit in the following figure.

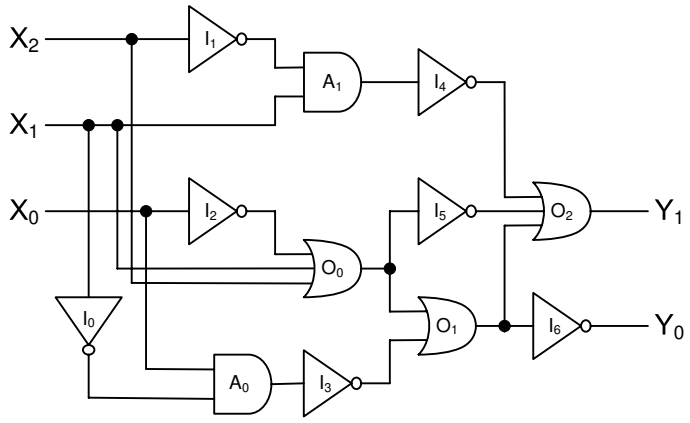

Figure 5: A 3-input 2-output logic circuit.

8.1 Express the Boolean function of the outputs. (5 points)

We index the outputs of each inverter, AND gate and OR gate by I_i, A_i and O_i, respectively.

$$
\begin{aligned}
I_0 &= X_1' \\
I_1 &= X_2' \\
I_2 &= X_0' \\
A_0 &= X_0X_1' \\
A_1 &= X_1X_2' \\
O_0 &= X_0' + X_1 + X_2 \\
I_3 &= (X_0X_1')' && (DeMorgan) \\
&= X_0' + X_1 \\
I_4 &= (X_1X_2')' && (DeMorgan) \\
&= (X_1' + X_2) \\
I_5 &= (X_0' + X_1 + X_2)' && (DeMorgan) \\
&= X_0X_1'X_2' \\
O_1 &= (X_0' + X_1) + X_0' + X_1 + X_2 \\
&= X_0' + X_1 + X_2 && (Idempotent) \\
O_2 &= (X_1' + X_2) + X_0X_1'X_2' + X_0' + X_1 + X_2 && (Associative) \\
&= (X_1 + X_1') + X_0' + X_2 + X_2 + X_0X_1'X_2' && (Complement) \\
&= 1 + X_0' + X_2 + X_2 + X_0X_1'X_2' && (Boundedness) \\
&= 1 \\
I_6 &= (X_0' + X_1 + X_2)' && (DeMorgan) \\
&= X_0X_1'X_2'
\end{aligned}
\tag{7}
$$

As a result, we have

$$
\begin{aligned}
Y_1(X_2, X_1, X_0) &= O_2 \\
&= (X_1X_2')' + (X_0' + X_1 + X_2)' + (X_0' + X_1 + X_2) + (X_0X_1')' && (DeMorgan) \\
&= (X_1' + X_2) + (X_0X_1'X_2') + (X_0' + X_1 + X_2) + (X_0' + X_1) && (Idempotent) \\
&= (X_1' + X_2) + (X_0X_1'X_2') + (X_0' + X_1 + X_2) && (Commutative) \\
&= (X_1' + X_1) + X_2 + (X_0X_1'X_2') + (X_0' + X_2) && (Complement) \\
&= 1 + X_2 + (X_0X_1'X_2') + (X_0' + X_2) && (Boundedness) \\
&= 1
\end{aligned}
\tag{8}
$$

$$
\begin{aligned}
Y_0(X_2, X_1, X_0) &= I_6 \\
&= ((X_0X_1')' + (X_0' + X_1 + X_2))' && (DeMorgan) \\
&= (X_0' + X_1 + X_2)' && (DeMorgan) \\
&= X_0X_1'X_2'
\end{aligned}
$$

Above expressions each 2 points, reductions each 0.5 points.

8.2 Write the truth table of the outputs. (5 points)

1 point for X_0 to X_2 columns, 2 points for Y_0 column and 2 points for Y_1 column.

Table 1: Truth table for the logic circuits.

id	X_2	X_1	X_0	Y_1	Y_0
0	0	0	0	1	0
1	0	0	1	1	1
2	0	1	0	1	0
3	0	1	1	1	0
4	1	0	0	1	0
5	1	0	1	1	0
6	1	1	0	1	0
7	1	1	1	1	0