IST 4
Information and Logic
## IST 4: Planned Schedule - Spring 2015

<table>
<thead>
<tr>
<th>mon</th>
<th>tue</th>
<th>wed</th>
<th>thr</th>
<th>fri</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>$M_1$</td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>oh</td>
<td>$M_1$</td>
<td>oh</td>
</tr>
<tr>
<td>13</td>
<td>oh</td>
<td>1</td>
<td>2</td>
<td>$M_2$</td>
</tr>
<tr>
<td>20</td>
<td>oh</td>
<td>oh</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>oh</td>
<td>$M_2$</td>
<td>oh</td>
<td><strong>midterms</strong></td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>T</td>
<td>oh</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>oh</td>
<td>3</td>
<td>4</td>
<td>oh</td>
</tr>
<tr>
<td>18</td>
<td>oh</td>
<td>oh</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>25</td>
<td></td>
<td>oh</td>
<td></td>
<td>oh</td>
</tr>
<tr>
<td>1</td>
<td>oh</td>
<td>5</td>
<td></td>
<td>oh</td>
</tr>
</tbody>
</table>

- **T** = today
- **x = hw#x out**
- **x = hw#x due**
- **oh = office hours**
- **Mx = MQx out**
- **Mx = MQx due**
It is all about languages

10 + 10 = 20

$(x + 1) \cdot (x + 1) = x^2 + 2 \cdot x + 1$

10 + 10 = 100

$(x + 1) \cdot (x + 1) = 1$
Boolean Proofs: Axioms + Fun

- **A1. Identities:**
  \[ a + 0 = a \quad \text{and} \quad a \cdot 1 = a \]

- **A2. Complements:**
  \[ a + \bar{a} = 1 \quad \text{and} \quad a \cdot \bar{a} = 0 \]

- **A3. Commutativity:**
  \[ a + b = b + a \quad \text{and} \quad a \cdot b = b \cdot a \]

- **A4. Distributivity:**
  \[ a + (b \cdot c) = (a + b) \cdot (a + c) \quad \text{and} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c) \]

- **L1. Self Absorption:**
  \[ a + a = a \quad \text{and} \quad a \cdot a = a \]

- **L2. Simple Absorption:**
  \[ a + 1 = 1 \quad \text{and} \quad a \cdot 0 = 0 \]

- **T0. Duality:**
  Correctness is maintained when interchange + and \( \cdot \), as well as 0 and 1.

- **T1. Distinct Complement:**
  Every element has another element that is its unique complement.

- **T2. Absorption:**
  \[ a + ab = a \quad \text{and} \quad a \cdot (a + b) = a \]
**Proof Dependency**

- **T3. Associativity:**
  \[(a + b) + c = a + (b + c)\]
  \[(a \cdot b) \cdot c = a \cdot (b \cdot c)\]

- **T4. DeMorgan Laws:**
  \[\overline{(a + b)} = \overline{a} \cdot \overline{b}\]
  \[\overline{(a \cdot b)} = \overline{a} + \overline{b}\]

- **L1. Self Absorption:**
  \[a + a = a\] and \[a \cdot a = a\]

- **L2. Simple Absorption:**
  \[a + 1 = 1\] and \[a \cdot 0 = 0\]

- **T0. Duality:**
  Correctness is maintained when interchange + and \(\cdot\), as well as 0 and 1.

- **T1. Distinct Complement:**
  Every element has another element that is its unique complement.

- **T2. Absorption:**
  \[a + ab = a\] and \[a \cdot (a + b) = a\]
Core Idea in a Proof

- **T3. Associativity:**
  \[(a + b) + c = a + (b + c)\]
  \[(a \cdot b) \cdot c = a \cdot (b \cdot c)\]

- **T4. DeMorgan Laws:**
  \[\overline{a + b} = \bar{a} \cdot \bar{b}\]
  \[\overline{a \cdot b} = \bar{a} + \bar{b}\]

- **L1. Self Absorption:**
  \[a + a = a\]

- **L2. Simple Absorption:**
  \[a + 1 = 1\] and \[a \cdot 0 = 0\]

- **T0. Duality:**
  Correctness is maintained when interchange + and ·, as well as 0 and 1.

- **T1. Distinct Complement:**
  Every element has another element that is its unique complement.

- **T2. Absorption:**
  \[a + ab = a\] and \[a \cdot (a + b) = a\]

- **A1. Identities:**
  \[a + 0 = a\] and \[a \cdot 1 = a\]

- **A2. Complements:**
  \[a + \bar{a} = 1\] and \[a \cdot \bar{a} = 0\]

- **A3. Commutativity:**
  \[a + b = b + a\] and \[a \cdot b = b \cdot a\]

- **A4. Distributivity:**
  \[a + (b \cdot c) = (a + b) \cdot (a + c)\] and \[a \cdot (b + c) = (a \cdot b) + (a \cdot c)\]
• L1. Self Absorption:
  \[ a + a = a \quad \text{and} \quad a \cdot a = a \]

• L2. Simple Absorption:
  \[ a + 1 = 1 \quad \text{and} \quad a \cdot 0 = 0 \]

\[ (a \mid a) \cdot (a \mid \bar{a}) \]

= \[ (a + a) \cdot 1 \]

= \[ a + a \]  \quad \text{A1}

\[ = a + (a \cdot \bar{a}) \]  \quad \text{A2}

\[ = a + 0 = a \]  \quad \text{A1}

• A1. Identities:
  \[ a + 0 = a \quad \text{and} \quad a \cdot 1 = a \]

• A2. Complements:
  \[ a + \bar{a} = 1 \quad \text{and} \quad a \cdot \bar{a} = 0 \]

• A3. Commutativity:
  \[ a + b = b + a \quad \text{and} \quad a \cdot b = b \cdot a \]

• A4. Distributivity:
  \[ a + (b \cdot c) = (a + b) \cdot (a + c) \quad \text{and} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c) \]
Core Idea in a Proof

- **T3. Associativity:**
  \[(a + b) + c = a + (b + c)
  \]
  \[(a \cdot b) \cdot c = a \cdot (b \cdot c)
  \]

- **T4. DeMorgan Laws:**
  \[
  \overline{a + b} = \overline{a} \cdot \overline{b}
  \]
  \[
  \overline{a \cdot b} = \overline{a} + \overline{b}
  \]

- **L1. Self Absorption:**
  \[a + a = a \quad \text{and} \quad a \cdot a = a\]

- **L2. Simple:**
  \[a + 1 = 1 \quad \text{and} \quad a \cdot 0 = 0\]

- **A1-A4**

- **T0. Duality:**
  Correctness is maintained when interchange + and \(\cdot\), as well as 0 and 1.

- **T1. Distinct Complement:**
  Every element has another element that is its unique complement.

- **T2. Absorption:**
  \[a + ab = a \quad \text{and} \quad a \cdot (a + b) = a\]

- **A1. Identities:**
  \[a + 0 = a \quad \text{and} \quad a \cdot 1 = a\]

- **A2. Complements:**
  \[a + \overline{a} = 1 \quad \text{and} \quad a \cdot \overline{a} = 0\]

- **A3. Commutativity:**
  \[a + b = b + a \quad \text{and} \quad a \cdot b = b \cdot a\]

- **A4. Distributivity:**
  \[a + (b \cdot c) = (a + b) \cdot (a + c) \quad \text{and} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c)\]

\[(a + 1) \cdot (a + \overline{a})\]
• L1. Self Absorption:
  \[ a + a = a \quad \text{and} \quad a \cdot a = a \]

• L2. Simple Absorption:
  \[ a + 1 = 1 \quad \text{and} \quad a \cdot 0 = 0 \]

\[
(a + 1) \cdot (a + \overline{a}) = (a + 1) \cdot 1
\]
\[
= a + 1 \quad \text{[A1]}
\]
\[
= a + (1 \cdot \overline{a}) \quad \text{[A3 A1]}
\]
\[
= a + \overline{a} = 1 \quad \text{[A2]}
\]

• A1. Identities:
  \[ a + 0 = a \quad \text{and} \quad a \cdot 1 = a \]

• A2. Complements:
  \[ a + \overline{a} = 1 \quad \text{and} \quad a \cdot \overline{a} = 0 \]

• A3. Commutativity:
  \[ a + b = b + a \quad \text{and} \quad a \cdot b = b \cdot a \]

• A4. Distributivity:
  \[ a + (b \cdot c) = (a + b) \cdot (a + c) \quad \text{and} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c) \]
Boolean Algebra

Boolean is not Binary...
Two-valued Boolean Algebra

Boolean Algebra: set of elements $B=\{0,1\}$, two binary operations OR and AND

<table>
<thead>
<tr>
<th>$xy$</th>
<th>$\text{OR}(x,y)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>0</td>
</tr>
<tr>
<td>01</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
</tr>
</tbody>
</table>

0 iff both $x$ and $y$ are 0

<table>
<thead>
<tr>
<th>$xy$</th>
<th>$\text{AND}(x,y)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>0</td>
</tr>
<tr>
<td>01</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
</tr>
</tbody>
</table>

1 iff both $x$ and $y$ are 1

We proved it is a Boolean algebra
Four-valued Boolean Algebra:
set of elements $\{??\}$
two binary operations $??$ and $??$

Two-valued Boolean Algebra:
set of elements $B=\{0,1\}$,
two binary operations OR and AND
\textbf{0-1 vectors:} \\
\textbf{Elements:} \\
\begin{tabular}{cccc}
(00) & (10) & (01) & (11) \\
\end{tabular}

\textbf{operations?}
Elements are: (00), (11), (10), (01)

<table>
<thead>
<tr>
<th>+</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>00</td>
<td>01</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>01</td>
<td>01</td>
<td>01</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>11</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>11</td>
</tr>
</tbody>
</table>
Elements are: (00), (11), (10), (01)

<table>
<thead>
<tr>
<th>+</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>00</td>
<td>01</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>01</td>
<td>01</td>
<td>01</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>11</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>11</td>
</tr>
</tbody>
</table>
Elements are: (00), (11), (10), (01)

<table>
<thead>
<tr>
<th></th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>01</td>
<td>00</td>
<td>01</td>
<td>00</td>
<td>01</td>
</tr>
<tr>
<td>10</td>
<td>00</td>
<td>00</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>11</td>
<td>00</td>
<td>01</td>
<td>10</td>
<td>11</td>
</tr>
</tbody>
</table>
Elements are: (00), (11), (10), (01)

<table>
<thead>
<tr>
<th></th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>01</td>
<td>00</td>
<td>01</td>
<td>00</td>
<td>01</td>
</tr>
<tr>
<td>10</td>
<td>00</td>
<td>00</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>11</td>
<td>00</td>
<td>01</td>
<td>10</td>
<td>11</td>
</tr>
</tbody>
</table>
Is it a Boolean algebra?

Elements:
- (00)
- (10)
- (01)
- (11)
- 0
- 1

Operations:
- Bitwise OR
- Bitwise AND
- Bitwise Complement

A1. Identities:
\[ a + 0 = a \quad \text{and} \quad a \cdot 1 = a \]

A2. Complements:
\[ a + \bar{a} = 1 \quad \text{and} \quad a \cdot \bar{a} = 0 \]

A3. Commutativity:
\[ a + b = b + a \quad \text{and} \quad a \cdot b = b \cdot a \]

A4. Distributivity:
\[ a + (b \cdot c) = (a + b) \cdot (a + c) \quad \text{and} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c) \]
### A1. Identities:

\[
a + 0 = a \quad \text{and} \quad a \cdot 1 = a
\]
• A2. Complements:
\[ a + \overline{a} = 1 \quad \text{and} \quad a \cdot \overline{a} = 0 \]
- **A3. Commutativity:**
  \[ a + b = b + a \quad \text{and} \quad a \cdot b = b \cdot a \]
### +

<table>
<thead>
<tr>
<th></th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>00</td>
<td>01</td>
<td>10</td>
<td>11</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>01</td>
<td>01</td>
<td>01</td>
<td>11</td>
<td>11</td>
<td>01</td>
<td>00</td>
<td>01</td>
<td>00</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>11</td>
<td>10</td>
<td>11</td>
<td>10</td>
<td>00</td>
<td>00</td>
<td>10</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>00</td>
<td>01</td>
<td>10</td>
</tr>
</tbody>
</table>

- **A4. Distributivity:**

\[ a + (b \cdot c) = (a + b) \cdot (a + c) \quad \text{and} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c) \]

*We can prove it!*
Is it a Boolean algebra? For any finite size vector?

Elements: 0-1 vectors

Operations:
- Bitwise OR
- Bitwise AND
- Bitwise Complement

A1. Identities:
    \[ a + 0 = a \quad \text{and} \quad a \cdot 1 = a \]

A2. Complements:
    \[ a + \bar{a} = 1 \quad \text{and} \quad a \cdot \bar{a} = 0 \]

A3. Commutativity:
    \[ a + b = b + a \quad \text{and} \quad a \cdot b = b \cdot a \]

A4. Distributivity:
    \[ a + (b \cdot c) = (a + b) \cdot (a + c) \quad \text{and} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c) \]
**Is it a Boolean algebra?**

**For any finite size vector?**

**0-1 vectors Boolean algebra**

**Elements:**

<table>
<thead>
<tr>
<th>(000)</th>
<th>(001)</th>
<th>(010)</th>
<th>(011)</th>
<th>(100)</th>
<th>(101)</th>
<th>(110)</th>
<th>(111)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

**n=3**

**Operations:**

- Bitwise OR
- Bitwise AND
- Bitwise Complement

**True for a two-valued Boolean algebra n=1**

**True for any Boolean algebra with 0-1 vectors and bitwise OR and AND**

**Arbitrary finite n**
Boolean Algebra

Two-value? Or not?
• A1. Identities:
  \[ a + 0 = a \quad \text{and} \quad a \cdot 1 = a \]

• A2. Complements:
  \[ a + \bar{a} = 1 \quad \text{and} \quad a \cdot \bar{a} = 0 \]

• A3. Commutativity:
  \[ a + b = b + a \quad \text{and} \quad a \cdot b = b \cdot a \]

• A4. Distributivity:
  \[ a + (b \cdot c) = (a + b) \cdot (a + c) \quad \text{and} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c) \]

**Prove or Disprove**

\[ a + b = 1 \]

At least one of the following is true:

\[ a = 1 \]

\[ b = 1 \]
A1. Identities:
\[ a + 0 = a \quad \text{and} \quad a \cdot 1 = a \]

A2. Complements:
\[ a + \bar{a} = 1 \quad \text{and} \quad a \cdot \bar{a} = 0 \]

A3. Commutativity:
\[ a + b = b + a \quad \text{and} \quad a \cdot b = b \cdot a \]

A4. Distributivity:
\[ a + (b \cdot c) = (a + b) \cdot (a + c) \quad \text{and} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c) \]

<table>
<thead>
<tr>
<th>xy</th>
<th>OR(x,y)</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>0</td>
</tr>
<tr>
<td>01</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
</tr>
</tbody>
</table>

Prove or Disprove

\[ a + b = 1 \]

At least one of the following is true:

\[ a = 1 \]

\[ b = 1 \]

Is it true for 0-1 vectors Boolean algebras?

True for two-valued Boolean algebra
Is it true for 0-1 vectors Boolean algebras?

NO
Boolean algebra

it is 0-1...
The 0-1 Theorem

0-1 Theorem:
An identity is true for any 0-1 vectors Boolean algebra if and only if it is true for a two valued (0-1) Boolean algebra.

Proof: The easy direction
Assume an identity true for any 0-1 vectors Boolean algebra

True for 0-1 Boolean algebra
The 0-1 Theorem

**0-1 Theorem:**

An identity is true for any 0-1 vectors Boolean algebra if and only if it is true for a two valued (0-1) Boolean algebra.

**Proof:**

The non-obvious direction

Assume an identity true for a 0-1 Boolean algebra

Need to prove true for any 0-1 vectors Boolean algebra
Absorption Theorem

Theorem 2: \[ a + a \cdot b = a \]

Proof: The identity is true for 0-1 Boolean algebra

\[
\begin{align*}
0 + 0 \times 0 &= 0 \\
0 + 0 \times 1 &= 0 \\
1 + 1 \times 0 &= 1 \\
1 + 1 \times 1 &= 1
\end{align*}
\]

Need to prove it for any Boolean algebra
Example: 0-1 Theorem

By contradiction

Assume true for all 0-1 assignments and not true for some other assignment

Theorem 2: \[ a + a \cdot b = a \]

Proof (for 0-1 vectors):

If an identity is not true in general; then there is an assignment of elements that violates the equality

Hence, there must be a position in the binary vector that is violated

There exists a 0-1 assignment to the identity that violates the equality, CONTRADICTION!!
Recap: The 0-1 Theorem

An identity is true for any 0-1 vectors Boolean algebra if and only if it is true for a two valued (0-1) Boolean algebra.

Proof: The easy direction

- Assume an identity true for any 0-1 vectors Boolean algebra
- 0-1 is a special case: True for 0-1 Boolean algebra

The non-obvious direction

- Assume an identity true for a 0-1 Boolean algebra
- Need to prove true for any 0-1 vectors Boolean algebra
- Assume there exists a general 'identity violating' assignment
- Show that there is a 0-1 'identity violating' assignment

CONTRADICTION!!
Claim: Assume 0-1 Boolean algebra

If \( a + b = 1 \)

Then \( a = 1 \) or \( b = 1 \)

Proof:

<table>
<thead>
<tr>
<th>xy</th>
<th>OR(x,y)</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>0</td>
</tr>
<tr>
<td>01</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
</tr>
</tbody>
</table>
The 0-1 Theorem: True Only for identities!!

If \( a + b = 1 \)

Then \( a = 1 \) or \( b = 1 \)

<table>
<thead>
<tr>
<th></th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>00</td>
<td>01</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>00</td>
<td>00</td>
<td>01</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>01</td>
<td>01</td>
<td>01</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>11</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>11</td>
</tr>
</tbody>
</table>
Examples of Boolean Algebras

- 0-1 vectors
- Arithmetic Boolean algebras
- Algebra of subsets
  union / intersection
Boolean algebra
Boolean integers
Greatest Common Divisor

297 = \(3 \times 3 \times 3 \times 11\)

405 = \(3 \times 3 \times 3 \times 3 \times 5\)

884 = \(2 \times 2 \times 13 \times 17\)

612 = \(2 \times 2 \times 3 \times 3 \times 17\)

27 = \(3 \times 3 \times 3\)

884 = \(2 \times 2 \times 13 \times 17\)

68 = \(2 \times 2 \times 17\)

Application: Simplifying fractions
Least Common Multiple

297 = 3\times3\times3\times11

405 = 3\times3\times3\times3\times5

884 = 2\times2\times13\times17

612 = 2\times2\times3\times3\times17

4455 = 3\times3\times3\times3\times5\times11

884 = 2\times2\times13\times17

7956 = 2\times2\times3\times3\times13\times17

Application: Adding fractions
Greatest Common Divisor

Least Common Multiple

gcd(297, 405) = 27
lcm(297, 405) = 4455

27 \times 4455 = 120,285
297 \times 405 = 120,285

gcd(a, b) \times lcm(a, b) = a \times b
Arithmetic Boolean Algebra

The set of elements: \( \{1,2,3,6\} \)

The operations: \( \text{lcm} \) and \( \text{gcd} \)

- \( 1 \) is Boolean 0
- \( 6 \) is Boolean 1

\( \text{lcm} = \) lowest common multiple
\( \text{gcd} = \) greatest common divisor
The set of elements: \( \{1, 2, 3, 6\} \)

The operations: \(\text{lcm} \) and \(\text{gcd}\)

1 is Boolean 0

6 is Boolean 1

What is the complement?

- A1. Identities:
  \(a + 0 = a\) and \(a \cdot 1 = a\)

- A2. Complements:
  \(a + \bar{a} = 1\) and \(a \cdot \bar{a} = 0\)

- A3. Commutativity:
  \(a + b = b + a\) and \(a \cdot b = b \cdot a\)

- A4. Distributivity:
  \(a + (b \cdot c) = (a + b) \cdot (a + c)\) and \(a \cdot (b + c) = (a \cdot b) + (a \cdot c)\)

\[
\bar{a} = \frac{6}{a}
\]

\[a + \bar{a} = \text{lcm}(a, \bar{a}) = 6\]

\[a \cdot \bar{a} = \text{gcd}(a, \bar{a}) = 1\]

\(lcm(1, 6) = 6\)

\(gcd(1, 6) = 1\)

\(lcm(2, 3) = 6\)

\(gcd(2, 3) = 1\)
The set of elements: \{1,2,3,6\}

The operations: \text{lcm} and \text{gcd}

1 is Boolean 0  
6 is Boolean 1

\textbf{Elements:}

Set of all the divisors of an integer \( n \)

For which \( n \) does it work?
The set of elements: \{1, 2, 4, 8\}

The operations: \text{lcm} and \text{gcd}

1 is Boolean 0
8 is Boolean 1

\[ a + \bar{a} = \text{lcm}(a, \bar{a}) = 8 \]
\[ a \cdot \bar{a} = \text{gcd}(a, \bar{a}) = 1 \]

- A1. Identities:
  \[ a + 0 = a \quad \text{and} \quad a \cdot 1 = a \]
- A2. Complements:
  \[ a + \bar{a} = 1 \quad \text{and} \quad a \cdot \bar{a} = 0 \]
- A3. Commutativity:
  \[ a + b = b + a \quad \text{and} \quad a \cdot b = b \cdot a \]
- A4. Distributivity:
  \[ a + (b \cdot c) = (a + b) \cdot (a + c) \quad \text{and} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c) \]

\[ \text{lcm}(1, 8) = 8 \]
\[ \text{gcd}(1, 8) = 1 \]
\[ \text{lcm}(2, 4) = 4 \]
\[ \text{gcd}(2, 4) = 2 \]
The set of elements: \{1,2,3,6\}
The operations: \text{lcm} and \text{gcd}

1 is Boolean 0
6 is Boolean 1

Elements:
Set of all the divisors of an integer \( n \)
For which \( n \) does it work?
Prime factors appear at most once in \( n \)
Boolean Integers

\[2 \times 3 \times 5 = 30\]
\[2 \times 3 \times 7 = 42\]

Every prime in the prime factorization is a power of one (\textit{square-free integer})

Elements:

The set of divisors of a Boolean integer
\[\{1, 2, 3, 5, 6, 10, 15, 30\}\]

The operations: \textit{lcm} and \textit{gcd}

The 0 and 1 elements: 1 and 30
Is Bunitskiy Algebra a Boolean Algebra?

Yes

6 = 3 × 2
3 = 3
2 = 2
1 = 1

LCM

GCD

Bitwise OR

Bitwise AND
Is Bunitskiy Algebra a Boolean Algebra?

| 30 = 5×3×2 | 111 |
| 15 = 5×3  | 110 |
| 10 = 5×2  | 101 |
| 6 = 3×2   | 011 |
| 5 = 5     | 100 |
| 3 = 3     | 010 |
| 2 = 2     | 001 |
| 1 = 1     | 000 |

LCM

GCD

Bitwise OR

Bitwise AND

YES
Bunitskiy algebra is **isomorphic** to the algebra of 0-1 vectors, it is a Boolean algebra!

syntax the same - different semantics
Boolean algebra

subsets of a set
Algebra of Subsets

$S$ is the set of all points

**Elements:** all possible subsets of a set $S$

+ is union of sets: $\cup$
+ is intersection of sets

How many elements? $2^{|S|}$
Example: \[ S = \{ a, b \} \]

**Operations: union and intersection**

**Elements:** \[ \emptyset \quad \{ a, b \} \quad \{ a \} \quad \{ b \} \]

**Complement:**

\[ \{ a, b \} = \emptyset \]
\[ \overline{\emptyset} = \{ a, b \} \]
\[ \{ a \} = \{ b \} \]
\[ \overline{\{ b \}} = \{ a \} \]
## Algebra of Subsets

<table>
<thead>
<tr>
<th>Union</th>
<th>$\emptyset$</th>
<th>${a}$</th>
<th>${b}$</th>
<th>${a, b}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\emptyset$</td>
<td>$\emptyset$</td>
<td>${a}$</td>
<td>${b}$</td>
<td>${a, b}$</td>
</tr>
<tr>
<td>${a}$</td>
<td>${a}$</td>
<td>${a}$</td>
<td>${a, b}$</td>
<td>${a, b}$</td>
</tr>
<tr>
<td>${b}$</td>
<td>${b}$</td>
<td>${a, b}$</td>
<td>${b}$</td>
<td>${a, b}$</td>
</tr>
<tr>
<td>${a, b}$</td>
<td>${a, b}$</td>
<td>${a, b}$</td>
<td>${a, b}$</td>
<td>${a, b}$</td>
</tr>
</tbody>
</table>
## Algebra of Subsets

### Intersection

<table>
<thead>
<tr>
<th></th>
<th>$\emptyset$</th>
<th>${a}$</th>
<th>${b}$</th>
<th>${a, b}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\emptyset$</td>
<td>$\emptyset$</td>
<td>$\emptyset$</td>
<td>$\emptyset$</td>
<td>$\emptyset$</td>
</tr>
<tr>
<td>${a}$</td>
<td>$\emptyset$</td>
<td>${a}$</td>
<td>$\emptyset$</td>
<td>${a}$</td>
</tr>
<tr>
<td>${b}$</td>
<td>$\emptyset$</td>
<td>$\emptyset$</td>
<td>${b}$</td>
<td>${b}$</td>
</tr>
<tr>
<td>${a, b}$</td>
<td>$\emptyset$</td>
<td>${a}$</td>
<td>${b}$</td>
<td>${a, b}$</td>
</tr>
</tbody>
</table>
Is the algebra of subsets a Boolean Algebra? YES

Corresponding 0-1 vectors:

\[ S = \{a, b\} \]

Elements:

\[
\begin{align*}
(00) & \leftrightarrow \emptyset \\
(11) & \leftrightarrow \{a, b\} \\
(10) & \leftrightarrow \{a\} \\
(01) & \leftrightarrow \{b\}
\end{align*}
\]

Algebra of subsets is isomorphic to the algebra of 0-1 vectors, it is a Boolean algebra!

syntax the same - different semantics
Elements are: (00), (11), (10), (01)

<table>
<thead>
<tr>
<th></th>
<th>∅</th>
<th>{a}</th>
<th>{b}</th>
<th>{a, b}</th>
</tr>
</thead>
<tbody>
<tr>
<td>∅</td>
<td>∅</td>
<td>{a}</td>
<td>{b}</td>
<td>{a, b}</td>
</tr>
<tr>
<td>{a}</td>
<td>{a}</td>
<td>{a}</td>
<td>{a, b}</td>
<td>{a, b}</td>
</tr>
<tr>
<td>{b}</td>
<td>{b}</td>
<td>{a, b}</td>
<td>{b}</td>
<td>{a, b}</td>
</tr>
<tr>
<td>{a, b}</td>
<td>{a, b}</td>
<td>{a, b}</td>
<td>{a, b}</td>
<td>{a, b}</td>
</tr>
</tbody>
</table>
**Union?**

**Bitwise OR**

Elements are: (00), (11), (10), (01)

<table>
<thead>
<tr>
<th></th>
<th>∪</th>
<th>∅</th>
<th>{a}</th>
<th>{b}</th>
<th>{a, b}</th>
</tr>
</thead>
<tbody>
<tr>
<td>∅</td>
<td></td>
<td>00</td>
<td>10</td>
<td>01</td>
<td>11</td>
</tr>
<tr>
<td>{a}</td>
<td></td>
<td>00</td>
<td>10</td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>{b}</td>
<td></td>
<td>01</td>
<td></td>
<td>01</td>
<td>11</td>
</tr>
<tr>
<td>{a, b}</td>
<td></td>
<td>11</td>
<td>11</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

![Bitwise OR Table]
Intersection?

Bitwise AND

Elements are: (00), (11), (10), (01)

<table>
<thead>
<tr>
<th></th>
<th>φ</th>
<th>{a}</th>
<th>{b}</th>
<th>{a, b}</th>
</tr>
</thead>
<tbody>
<tr>
<td>φ</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>00</td>
<td>00</td>
<td>10</td>
<td>01</td>
<td>11</td>
</tr>
<tr>
<td>{a}</td>
<td>10</td>
<td>00</td>
<td>00</td>
<td>10</td>
</tr>
<tr>
<td>10</td>
<td>00</td>
<td>00</td>
<td>10</td>
<td>00</td>
</tr>
<tr>
<td>{b}</td>
<td>01</td>
<td>00</td>
<td>01</td>
<td>01</td>
</tr>
<tr>
<td>01</td>
<td>00</td>
<td>00</td>
<td>01</td>
<td>01</td>
</tr>
<tr>
<td>{a, b}</td>
<td>11</td>
<td>00</td>
<td>10</td>
<td>11</td>
</tr>
</tbody>
</table>
Boolean algebra
an amazing theorem
Examples of Boolean Algebras

Size $2^k$

They are isomorphic!

- 0–1 (two valued) Boolean algebra
  OR / AND

- 0–1 vectors
  bitwise OR / bitwise AND

- Arithmetic Boolean algebras
  lcm / gcd

- Algebra of subsets
  union / intersection
An Amazing Theorem

**Representation Theorem (Stone 1936):**

Every *finite* Boolean algebra is isomorphic to a Boolean algebra of 0-1 vectors.

Algebra 1

- elements
- operations

---

Algebra 2

- elements
- operations
Representation Theorem (Stone 1936):

Every finite Boolean algebra is isomorphic to a Boolean algebra with elements being bit vectors of finite length with bitwise operations OR and AND.

Two Boolean algebras with $m$ elements are isomorphic.

Every Boolean algebra has $2^k$ elements.

Provides intuition beyond the axioms:

We can ‘naturally’ reason about results in Boolean algebra.
Marshall Stone
1903-1989

Marshall Stone

Proved in 1936
90AB = years After Boole
The Boolean Syntax invented in 1847 has a unique representative semantic!!

Marshall entered Harvard in 1919 intending to continue his studies at Harvard law school; fell in love with Mathematics, and the rest is history...

Harlan Fiske Stone
12th Chief Justice of the US
1941-1946

Marshall had a passion for travel. He began traveling when he was young and was on a trip to India when he died....
Proofs

creating
“simple and correct”
proofs
How to **create** "simple and correct" proofs?

Henri Poincaré 1854-1912

**Mathematical Creativity**

French mathematician
- Topology
- Chaos
- Relativity
- WooooooW.....
- ........
Henri Poincaré
1854-1912

What is Mathematical Creation?

“It does not consist in making new combinations with mathematical entities already known. Any one could do that...”

To create consists precisely in not making useless combinations and in making those which are useful and which are only a small minority. Invention is discernment, choice.

Invention is choice...
“For fifteen days I strove to prove that there could not be any functions like those I have since called Fuchsian functions. I was then very ignorant; every day I seated myself at my work table, stayed an hour or two, tried a great number of combinations and reached no results....”

“One evening, contrary to my custom, I drank black coffee and could not sleep. Ideas rose in crowds; I felt them collide until pairs interlocked, so to speak, making a stable combination.”

“...the next morning I had established the existence of a class of Fuchsian functions...”
Work... and relax...

“Often when one works at a hard question, nothing good is accomplished at the first attack.”

“Then one takes a rest, longer or shorter, and sits down anew to the work.”

“During the first half-hour, as before, nothing is found, and then all of a sudden the decisive idea presents itself to the mind.”
Conscious and unconscious

“It might be said that the conscious work has been more fruitful because it has been interrupted and the rest has given back to the mind its force and freshness.”

Rest vs unconscious work...

“But it is more probable that this rest has been filled out with unconscious work and that the result of this work has afterwards revealed itself...”
Homework #3
Due Tuesday, May 12, 2015, at 2:30 PM
Collaboration and discussions are not allowed on Problem 1 and Problem 2
and are allowed and encouraged on Problem 3

- A1. Identities:
  \( a + 0 = a \) and \( a \cdot 1 = a \)

- A2. Complements:
  \( a + \overline{a} = 1 \) and \( a \cdot \overline{a} = 0 \)

- A3. Commutativity:
  \( a + b = b + a \) and \( a \cdot b = b \cdot a \)

- A4. Distributivity:
  \( a + (b \cdot c) = (a + b) \cdot (a + c) \) and \( a \cdot (b + c) = (a \cdot b) + (a \cdot c) \)

- T0. Duality:
  Correctness is maintained when interchange + and \( \cdot \), as well as 0 and 1.

- T1. Distinct Complement:
  Every element has another element that is its unique complement.

- T2. Absorption:
  \( a + ab = a \) and \( a \cdot (a + b) = a \)

- T3. Associativity:
  \( (a + b) + c = a + (b + c) \)
  \( (a \cdot b) \cdot c = a \cdot (b \cdot c) \)

- T4. DeMorgan Laws:
  \( (a + b) = \overline{a} \cdot \overline{b} \)
  \( (a \cdot b) = \overline{a} + \overline{b} \)

- L1. Self Absorption:
  \( a + a = a \) and \( a \cdot a = a \)

- L2. Simple Absorption:
  \( a + 1 = 1 \) and \( a \cdot 0 = 0 \)
1. **Associativity Theorem** (*Collaboration is not allowed on this Problem*).

Here you will complete the proof of the theorem that was presented in class. *Please justify every step in your proofs using the axioms, lemmas and theorems from class.* However, there is one exception, you cannot use the 0-1 Theorem we proved in class. The Associativity Theorem is stated as follows, for any three elements $a$, $b$ and $c$ in a Boolean algebra the following is true:

$$\quad (a + b) + c = a + (b + c)$$

and the dual statement:

$$\quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

The proof in class had 4 parts, however, we did not prove part (2). Prove the following statement (part (2) from class):

$$\bar{a} + (a \cdot (b \cdot c)) = \bar{a} + ((a \cdot b) \cdot c)$$

\[\text{Prove 1}\]

\[\begin{align*}
(a + a \cdot (b \cdot c)) \cdot (\bar{a} + a \cdot (b \cdot c)) &\equiv a \cdot (b \cdot c) \\
1 \quad \| \quad 2 \quad \| \quad 3 \\
(a + (a \cdot b) \cdot c) \cdot (\bar{a} + (a \cdot b) \cdot c) &= (a \cdot b) \cdot c \\
\text{multiply}
\end{align*}\]
2. **DeMorgan’s Theorem** *(Collaboration is not allowed on this Problem)*

Here you will complete the proof of the theorem that was presented in class. *Please justify every step in your proofs using the axioms, lemmas and theorems from class.* However, there is one exception, you *cannot use the 0-1 Theorem* we proved in class. DeMorgan’s Theorem is stated as follows, for any two elements \( a \) and \( b \) in a Boolean algebra the following is true:

\[
\overline{a \cdot b} = \overline{a} + \overline{b}
\]

and the dual statement:

\[
\overline{a + b} = \overline{a} \cdot \overline{b}
\]

The idea in the proof is to show that \( \overline{a + b} \) is the complement of \( a \cdot b \). Namely, by axiom **A2** we need to prove the following two statements:

(I) \( a \cdot b + \overline{a + b} = 1 \)

and

(II) \( a \cdot b \cdot (a + \overline{b}) = 0 \)
The idea in the proof is to show that \((\bar{a} + \bar{b})\) is the complement of \((a \cdot b)\). Namely, by axiom A2 we need to prove the following two statements:

(I) \((a \cdot b) + (\bar{a} + \bar{b}) = 1\)

and

(II) \((a \cdot b) \cdot (\bar{a} + \bar{b}) = 0\)

In class we proved statement (II) above. Here you will prove statement (I). In your proofs, you cannot use the Duality Theorem.

(a) Prove statement (I), please use the Associativity Theorem in your proof.

(b) Prove statement (I) without using the Associativity Theorem in your proof.

(c) Use DeMorgan’s Theorem and other axioms and theorems to find the complements of: (i) \((a \cdot \bar{b}) + (\bar{a} \cdot b)\), (ii) \((a + b + c + d)\), and (iii) \(a + (\bar{a} \cdot b \cdot c)\). Please justify every step in your derivations using the axioms, lemmas, and theorems from class.

For (c): Sum of products (no need to expand to DNF)
3. Syntax Boxes and the Binary Adder (*Collaboration is allowed on this Problem*)
In class we showed that the following syntax box \( m(a, b) \) is magical, namely, a composition of \( m \)-boxes (called a circuit) can compute an arbitrary \( n \)-input binary syntax box.

\[
\begin{array}{c|c|c}
    a & b & m \\
\hline
    0 & 0 & 1 \\
    0 & 1 & 1 \\
    1 & 0 & 1 \\
    1 & 1 & 0 \\
\end{array}
\]

\( m(a, b) = \)

(a) The *Parity* of two variables is defined by the following syntax box.

\[
\begin{array}{c|c|c}
    a & b & Parity \\
\hline
    0 & 0 & 0 \\
    0 & 1 & 1 \\
    1 & 0 & 1 \\
    1 & 1 & 0 \\
\end{array}
\]

\( Parity(a, b) = \)

You need to design a circuit of \( m \)-boxes to compute \( Parity(a, b) \). Your goal is to construct a circuit that consists of the smallest number of \( m \)-boxes possible. Please show your work and draw the circuit. An answer with 5 \( m \)-boxes or less will get full credit.
The binary adder has three inputs and two outputs. The outputs are the binary representation of the number of 1s in the inputs. Specifically, we showed in class that the first output (the sum) is $Parity(a, b, c)$ and the second output (the carry) is $Majority(a, b, c)$.

**majority**

<table>
<thead>
<tr>
<th>$a$</th>
<th>$b$</th>
<th>$c$</th>
<th>majority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

**parity**

<table>
<thead>
<tr>
<th>$a$</th>
<th>$b$</th>
<th>$c$</th>
<th>parity</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
(b) You need to design a circuit of $m$-boxes to compute $\text{Parity}(a, b, c)$. Your goal is to construct a circuit that consists of the smallest number of $m$-boxes possible. Please show your work and draw the circuit. An answer with 9 $m$-boxes or less will get full credit.

(c) You need to design a circuit of $m$-boxes to compute $\text{Majority}(a, b, c)$. Your goal is to construct a circuit that consists of the smallest number of $m$-boxes possible. Please show your work and draw the circuit. An answer with 8 $m$-boxes or less will get full credit.