Byzantine Generals Problem
The Situation

GW (0)

NG (1)

ML (2)

BA (3)

The Enemy

Have to decide: Attack or Retreat
The Situation

GW (0)

NG (1)

ML (2)

BA (3)

The Enemy

Have to decide: Attack or Retreat

Can reliably send messages to each other
The Situation

Have to decide: Attack or Retreat
Can reliably send messages to each other
Must reach consensus

The Enemy
Trace: 4 Armies

- Make a choice
- Send your choice to every other general.
- Build vector of choices.
- Choose the majority vote (tie = retreat)
There May Be A *Traitor!*

George Washington (0)

Nathanael Greene (1)

Marquis de Lafayette (2)

Benedict Arnold (3)

The Enemy
Trace: 3 Loyalists + 1 Traitor

G0 wants to RETREAT
G1 wants to ATTACK
G2 wants to ATTACK
G3 is a TRAITOR!

<table>
<thead>
<tr>
<th>G0 plan</th>
<th>3</th>
<th>2</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>R</td>
</tr>
<tr>
<td>G1 plan</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>R</td>
</tr>
<tr>
<td>G2 plan</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>R</td>
</tr>
</tbody>
</table>

Loyal generals send consistent messages
Trace: 3 Loyalists + 1 Traitor

G0 wants to RETREAT
G1 wants to ATTACK
G2 wants to ATTACK
G3 is a TRAITOR!

G0 plan

3 2 1 0
R A A R

G1 plan

3 2 1 0
A A A R

G2 plan

3 2 1 0
A A A R

Traitors can send any message
Trace: 3 Loyalists + 1 Traitor

G0 wants to RETREAT
G1 wants to ATTACK
G2 wants to ATTACK
G3 is a TRAITOR!

G0 plan   3 2 1 0
          R A A R

G1 plan   3 2 1 0
          A A A R

G2 plan   3 2 1 0
          A A A R

G0 says RETREAT
G1 says ATTACK
G2 says ATTACK

Traitors can defeat consensus among loyalists.
Trace: 3 Loyalists + 1 Traitor

G0 wants to RETREAT
G1 wants to ATTACK
G2 wants to ATTACK
G3 is a TRAITOR!

G0 plan  
3 2 1 0  
R A A R

G1 plan  
3 2 1 0  
A A A R

G2 plan  
3 2 1 0  
A A A R

G0 says RETREAT  
G1 says ATTACK  
G2 says ATTACK

Traitors can defeat consensus among loyalists.  
A BYZANTINE FAILURE
Two Phase Approach

• Send out your choice as before.

• Build the vector of your choice and what your colleagues told you as before.

• Send the choice vector to each colleague.

• Create a choice table:
  – Rows: choice vectors for each general.
  – Cols: choices received from that general.

• Take majority from each column as the corresponding general’s “real” choice.

• Action = majority across this vector of choices.
Trace: 3 Loyalists + 1 Traitor - Attack

G0 wants to RETREAT
G1 wants to ATTACK
G2 wants to ATTACK
G3 is a TRAITOR!

G0 plan   3 2 1 0
R A A R

G1 plan   3 2 1 0
A A A R

G2 plan   3 2 1 0
A A A R

G0 says ATTACK
G1 says ATTACK
G2 says ATTACK
Trace: 3 Loyalists + 1 Traitor - Attack

<table>
<thead>
<tr>
<th>General</th>
<th>Plan</th>
<th>All Plans</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>G0</strong></td>
<td>3 2 1 0</td>
<td>G0 R A A R</td>
</tr>
<tr>
<td></td>
<td>R A A R</td>
<td>G1 A A A R</td>
</tr>
<tr>
<td><strong>G1</strong></td>
<td>3 2 1 0</td>
<td>G0 R A A R</td>
</tr>
<tr>
<td></td>
<td>A A A R</td>
<td>G1 A A A R</td>
</tr>
<tr>
<td><strong>G2</strong></td>
<td>3 2 1 0</td>
<td>G0 R A A R</td>
</tr>
<tr>
<td></td>
<td>A A A R</td>
<td>G1 A A A R</td>
</tr>
<tr>
<td><strong>G3</strong></td>
<td>R R R R</td>
<td>G0 R A A R</td>
</tr>
<tr>
<td></td>
<td>R R R R</td>
<td>G1 A A A A</td>
</tr>
<tr>
<td></td>
<td>R R R R</td>
<td>G2 A A A A</td>
</tr>
<tr>
<td></td>
<td>R R R R</td>
<td>G3 A A A A</td>
</tr>
</tbody>
</table>

Every general knows his own choice. Ignore what others say he chose.
Trace: 3 Loyalists + 1 Traitor - Attack

<table>
<thead>
<tr>
<th>General</th>
<th>Plan</th>
<th>All Plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>G0</td>
<td>RETREAT</td>
<td>3 2 1 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>R A A R</td>
</tr>
<tr>
<td>G1</td>
<td>ATTACK</td>
<td>3 2 1 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A A A R</td>
</tr>
<tr>
<td>G2</td>
<td>ATTACK</td>
<td>3 2 1 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A A A R</td>
</tr>
<tr>
<td>G3</td>
<td>TRAITOR!</td>
<td>3 2 1 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- - R R R -</td>
</tr>
</tbody>
</table>

Every general knows what every other general said his choice was, so ignore the duplicate.
Trace: 3 Loyalists + 1 Traitor - Attack

G0 wants to RETREAT
G1 wants to ATTACK
G2 wants to ATTACK
G3 is a TRAITOR!

G0 plan   3 2 1 0
R A A R

G1 plan   3 2 1 0
A A A R

G2 plan   3 2 1 0
A A A R

G0 says ATTACK
G1 says ATTACK
G2 says ATTACK

G0 all plans   3 2 1 0
G0 R A A R
G1 A A --
G2 A A A R
T3 -- R R --

G1 all plans   3 2 1 0
G0 R A --
G1 A A A R
G2 A A R
T3 -- A --

G2 all plans   3 2 1 0
G0 R -- A
G1 A -- R
G2 A A A R
T3 -- A A

Every general records the column consensi
Trace: 3 Loyalists + 1 Traitor - Attack

<table>
<thead>
<tr>
<th>Player</th>
<th>Plan</th>
<th>All Plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>G0</td>
<td>3 2 1 0</td>
<td>G0 R A A R</td>
</tr>
<tr>
<td></td>
<td>R A A R</td>
<td>G1 A A A R</td>
</tr>
<tr>
<td></td>
<td>G1 A A A R</td>
<td>G2 A A A R</td>
</tr>
<tr>
<td></td>
<td>G2 A A A R</td>
<td>T3 R R R</td>
</tr>
<tr>
<td></td>
<td>T3 R R R</td>
<td>= A</td>
</tr>
<tr>
<td>G1</td>
<td>3 2 1 0</td>
<td>G0 R A A R</td>
</tr>
<tr>
<td></td>
<td>A A A R</td>
<td>G1 A A A R</td>
</tr>
<tr>
<td></td>
<td>G1 A A A R</td>
<td>G2 A A A R</td>
</tr>
<tr>
<td></td>
<td>G2 A A A R</td>
<td>T3 A A A</td>
</tr>
<tr>
<td></td>
<td>T3 A A A</td>
<td>= A</td>
</tr>
<tr>
<td>G2</td>
<td>3 2 1 0</td>
<td>G0 R A A R</td>
</tr>
<tr>
<td></td>
<td>A A A R</td>
<td>G1 A A A R</td>
</tr>
<tr>
<td></td>
<td>G1 A A A R</td>
<td>G2 A A A R</td>
</tr>
<tr>
<td></td>
<td>G2 A A A R</td>
<td>T3 A A A</td>
</tr>
<tr>
<td></td>
<td>T3 A A A</td>
<td>= A</td>
</tr>
</tbody>
</table>

Choice is the consensus of the consensi
Trace: 3 Loyalists + 1 Traitor - Retreat

G0 wants to ATTACK
G1 wants to RETREAT
G2 wants to RETREAT
G3 is a TRAITOR!

G0 plan

G1 plan

G2 plan

G0 says RETREAT
G1 says RETREAT
G2 says RETREAT

G0 all plans

G1 all plans

G2 all plans

R R R A = R

R R R A = R

R R R A = R
Trace: 2 Loyalists + 1 Traitor — No Consensus

G0 wants to ATTACK
G1 wants to ATTACK
G2 is a TRAITOR!

G0 plan  2 1 0
         A A A

G1 plan  2 1 0
         R A A

G0 says ATTACK
G1 says RETREAT

G0 all plans  2 1 0
             G0 A A A
             G1 R - -
             G2 - A -

G1 all plans  2 1 0
             G0 A - -
             G1 R A A
             G2 - - R

R A A = A
R A R = R
Trace: 2 Loyalists + 1 Traitor – No Consensus

G0 wants to ATTACK
G1 wants to ATTACK
G2 is a TRAITOR!

G0 plan 2 1 0
A A A

G1 plan 2 1 0
R A A

G0 all plans 2 1 0
G0 A A A
G1 R --
G2 -- A --

G1 all plans 2 1 0
G0 A --
G1 R A A
G2 -- R

R A A = A

R A R = R

To guarantee consensus can be reached when there are t traitors, we need 
2t+1 loyal generals or a total of 3t+1 generals.

1 traitor requires 4 generals
2 traitors requires 7 generals
3 traitors requires 10 generals