Byzantine Generals Problem

Graham Swain

October 15th, 2022
Math 479

A. All loyal generals decide upon the same plan of action.
B. A small number of traitors cannot cause the loyal generals to adopt a bad plan.

- Condition A is met by having the generals use the same method of decision making.

- Condition A is met by having the generals use the same method of decision making.
- Condition B is met by having the generals use a robust decision making method.

1. Every loyal general must obtain the same information $v_1, \ldots, v_n$.

1. Every loyal general must obtain the same information $v_1, \ldots, v_n$.
2. If the i^{th} general is loyal, then the value that they sends must be used by every loyal general as the value of v_i.

1. Every loyal general must obtain the same information $v_1, \ldots, v_n$.
2. If the i^{th} general is loyal, then the value that they sends must be used by every loyal general as the value of v_i.

1. Every loyal general must obtain the same information $v_1, ..., v_n$.
2. If the i^{th} general is loyal, then the value that they sends must be used by every loyal general as the value of v_i.

Condition 1 can be rewritten as:

1′. For every i, any two loyal generals use the same value of v_i.

To help ensure that Condition A and Condition B are met, we need to meet two other conditions:

To help ensure that Condition A and Condition B are met, we need to meet two other conditions:

IC1. All loyal lieutenants obey the same order.

To help ensure that Condition A and Condition B are met, we need to meet two other conditions:

IC1. All loyal lieutenants obey the same order.

IC2. If the commander is loyal, then every loyal lieutenant obeys the order they sends.

- Loyal generals cannot take a value v_i at face value.

- Loyal generals cannot take a value v_i at face value.
- Condition $1'$ and Condition 2 are both contingent on a single v_i sent by the i^{th} general.

Byzantine Generals Problem

Byzantine Generals Problem

A commanding general must send an order to their $n-1$ lieutenants such that:

Byzantine Generals Problem

A commanding general must send an order to their $n-1$ lieutenants such that:

IC1. All loyal lieutenants obey the same order.

Byzantine Generals Problem

A commanding general must send an order to their $n-1$ lieutenants such that:

IC1. All loyal lieutenants obey the same order.

IC2. If the commander is loyal, then every loyal lieutenant obeys the order they sends.

References

[1] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem", ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, 1982, 382-401.