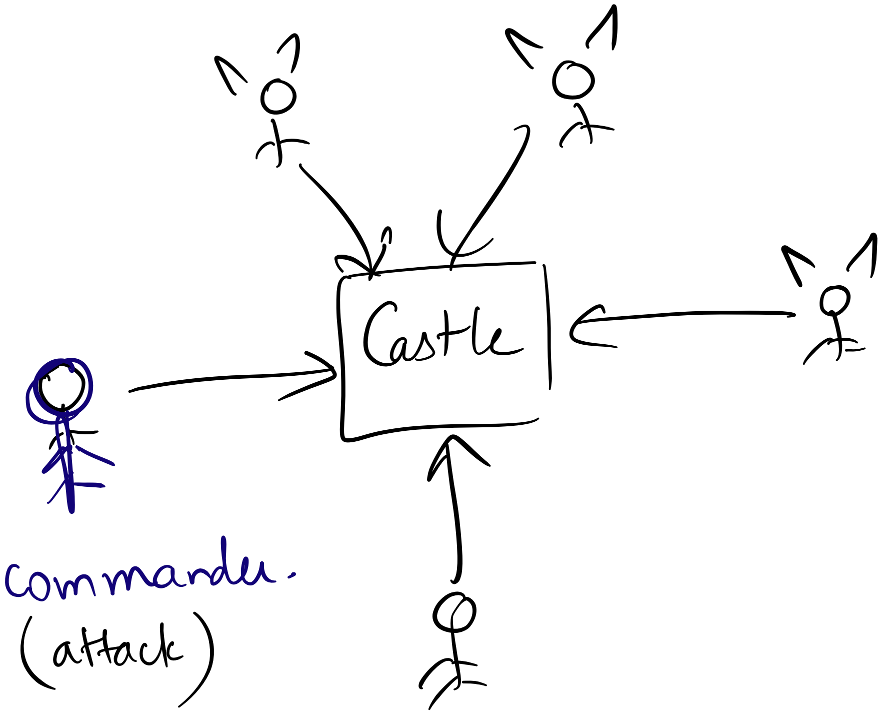
Byzantine Broadcast:

n parties, t corrupt/malicious/Byzantine.



Agreement: No two honest generals take different actions.

Termination: Every honest general eventually either attacks or retreats.

Validity: If commander is honest, then honest parties output commander's order.

Dolev-Strong Protocol: (1983)

Intuition:

txn

command

- If some honest party receives a value, share it with all honest parties.
- Eventually, one honest party learns x

$\Downarrow$

all honest parties learn x.

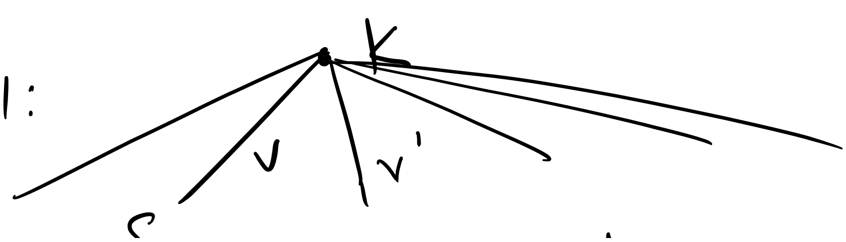
Round 1: Commander (sender) sends value v to all parties.

Round 2: If I receive a value from the commander, then I ~~sh~~ send it to all parties.

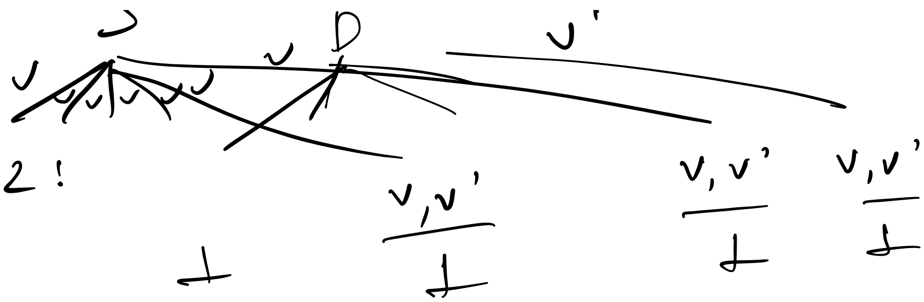
Commit: If I receive exactly one value v, then output v.

output $\perp$.

Round 1:



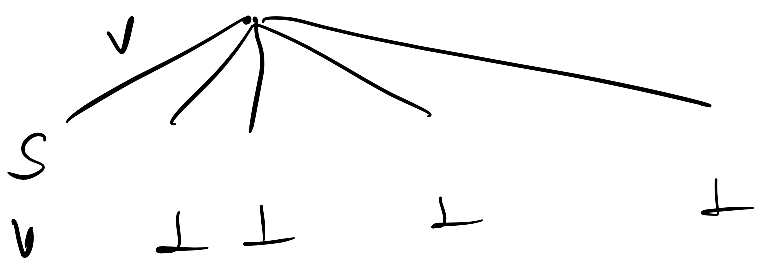
Round 2 !



Attack 2 :

Round 1 : .K

Round 2 :



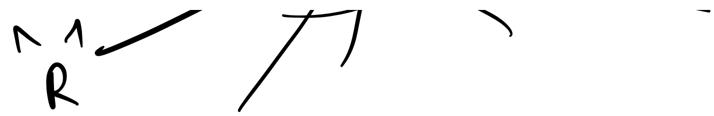
Solution:

Round 2 : Do not consider commander's value.

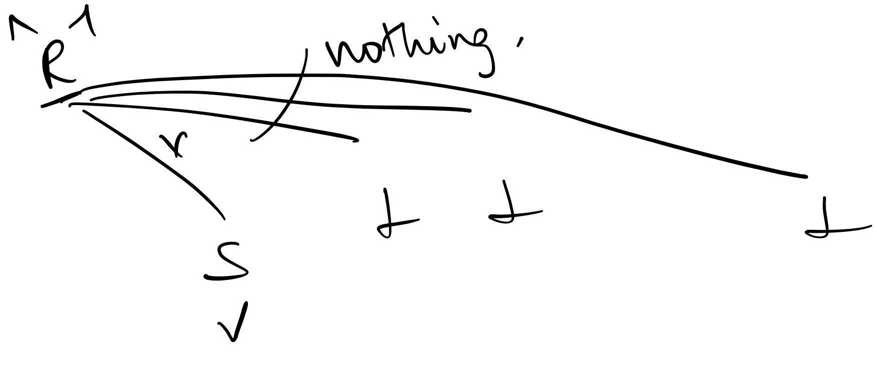
If ≤ 1 Byzantine :

≥ 2 Byzantine parties.

Round 1 :



Round 2:



We can tolerate Byzantine faults.

Signature chains: $P_1, P_2 \ldots P_n$.

$$\langle\langle \underbrace{\langle v, 1\rangle_{P_1}}_{m}, 2\rangle_{R}, 3\rangle_{S}.$$

What is a valid signature chain:

- in round i, the signature chain received should be length i.
- the signers in this chain should be distinct/
- signature should be valid.

Distinct signature chains: "value" should be distinct

Protocol:

$\cancel{\langle v', 1\rangle_{P_1}}$

Round 1: Sender P sends $\langle v, 1\rangle_P$ to all

Round 1: Sender S sends $\langle v \rangle_{S}$ to all other parties.

Rounds $\underbrace{2, \dots, t+1}_{i}$: If a party receives a valid signature chain in round $(i-1)$ and it has not broadcasted ≥ 2 signature chains, then it appends to the chain & broadcasts.

Commit: if a party receives exactly 1 valid signature chain with value v, output v
output $\perp$.

Agreement:

Termination: easy.

Validity:

Proof:

Agreement: If an honest party h receives value v, all honest parties receive it.

Rounds $1 \dots t$: h will send it to everyone.

$t+1$: the chain has length $t+1$
$\exists$ some honest party h' in this chain; h' would have sent it to everyone.

n, t Byzantine $t \le n-2$.

Latency: $\underline{t+1}$ rounds k rounds. $O(n^2 k)$

communication complexity: ~~$t \times n$~~ $\underline{2n^2}$ $\boxed{2n^2 t.}$ $\underline{O(n^2 t)}$

- ≤ 2 messages.
- n^2 ~~ea.~~ all-~~to~~-all.
- $\le t$ message size.

1. Are $O(t)$ rounds necessary?
2. Is $O(n^2 t)$ communication necessary?

Dolev-Reischuk. $O(t^2)$ lower bound:

Any (deterministic) BB protocol needs at least $\frac{t^2}{4}$ messages.

To prove: If a protocol fewer $\le (t/2)^2$ messages, $\exists$ one honest party who does not receive any message.

If $\le \left(\frac{t}{2}\right)^2$ messages are sent, consider any set V of size t parties. If each party in V

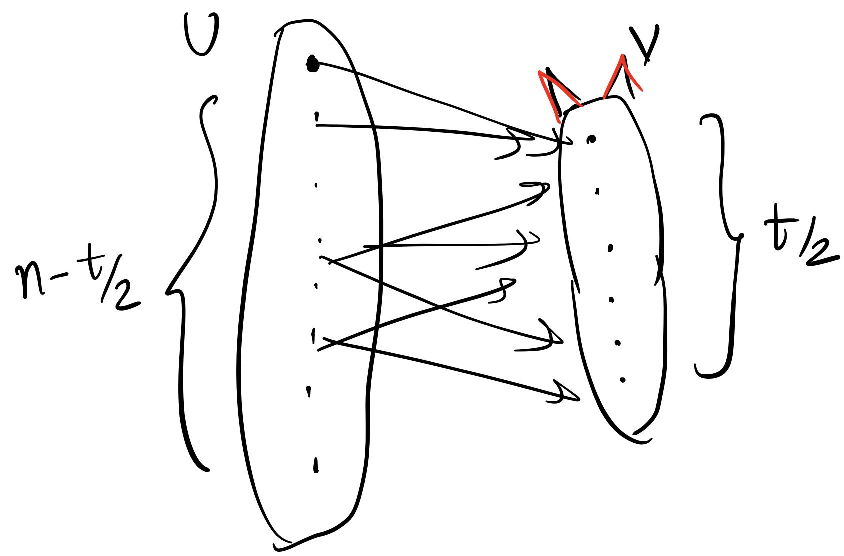
receives $\geq \frac{t}{2}$ msgs, then $\geq \left(\frac{t}{2}\right)^2$ msgs.

$\exists$ at least one party in V that receives $\leq t/2$ msgs.

$\Uparrow$

$\leq \lceil t/2 \rceil$ different parties.

<u>World 1</u>: Designated sender is honest:
Sender sends 0;



Byzantine parties in V behave honestly except:
(i) they ignore the first $t/2$ messages sent to them.

(ii) they do not send any messages to each other

Honest parties should output 0.