ETH zürich

Byzantine Agreement with Unknown Participants and Failures

Pankaj Khanchandani, Roger Wattenhofer
Distributed Computing Group (DISCO)
www.disco.ethz.ch

Byzantine Agreement

Required: Agreement, Termination, Validity

Byzantine Agreement

Required: Agreement, Termination, Validity

Assumption: Participants know *n* and *f*

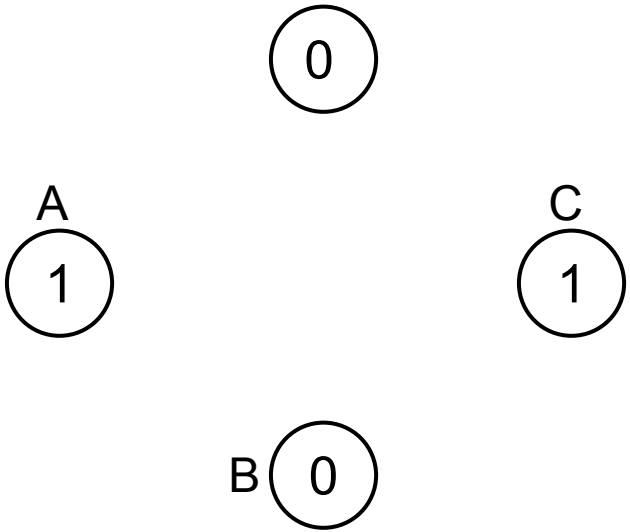
Byzantine Agreement

Required: Agreement, Termination, Validity

~~Assumption: Participants know *n* and *f*~~

BA with Unknown *n* & *f*

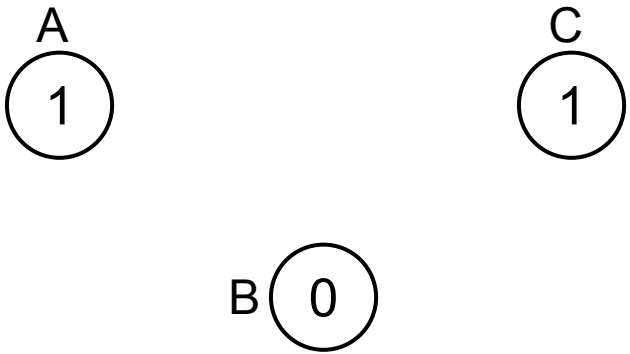
BA with Unknown *n* & *f*



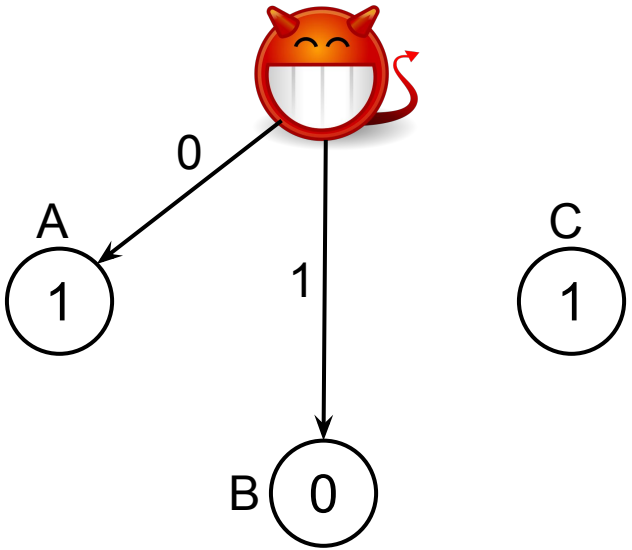
Synchronous

BA with Unknown *n* & *f*

Synchronous

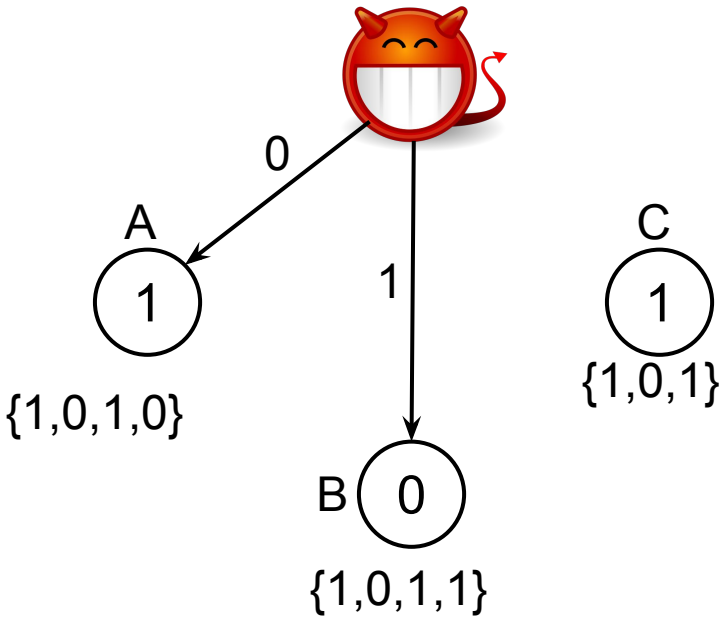


BA with Unknown *n* & *f*



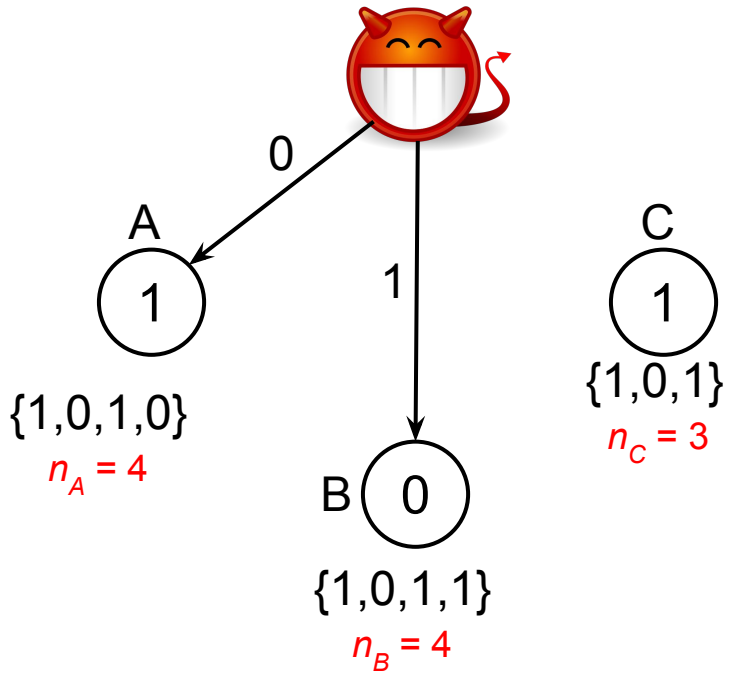
Synchronous
Broadcast

BA with Unknown *n* & *f*



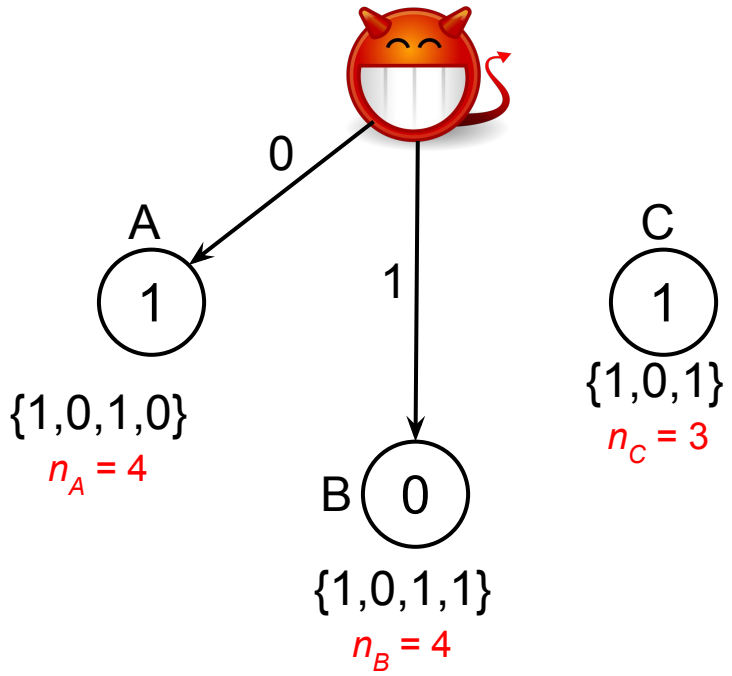
Synchronous
Broadcast

BA with Unknown n & f



Synchronous
Broadcast

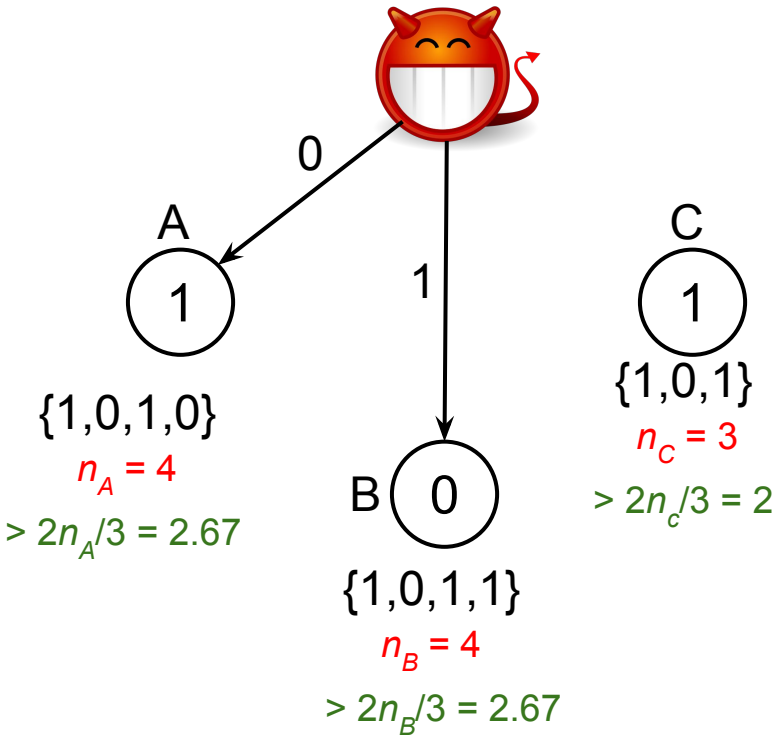
BA with Unknown *n* & *f*



Synchronous Broadcast

Is $n > 3f$ enough?

BA with Unknown *n* & *f*



Synchronous Broadcast
Is $n > 3f$ enough?

Equivalent Thresholds

$n - f \Rightarrow 2n_v/3$

$n - 2f \Rightarrow n_v/3$

n_v = number of nodes that v heard from

Agreement without Termination

In each round

Broadcast **m** if received $n_v/3$ copies of **m**.

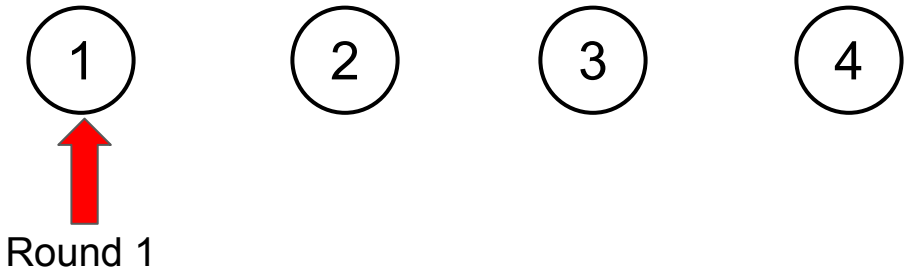
Accept **m** if received $2n_v/3$ copies of **m**.

Termination when *n* & *f* are known

Electing a correct leader (king)

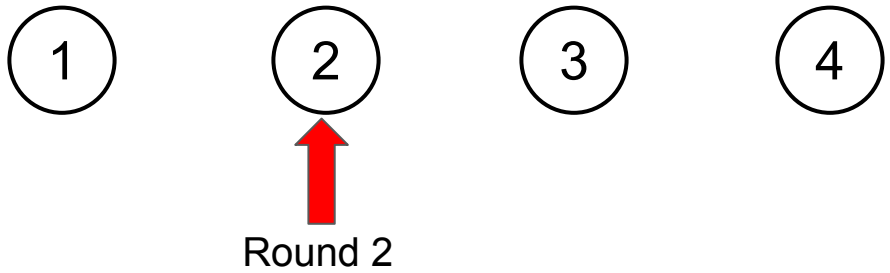
Termination when *n* & *f* are known

Electing a correct leader (king)



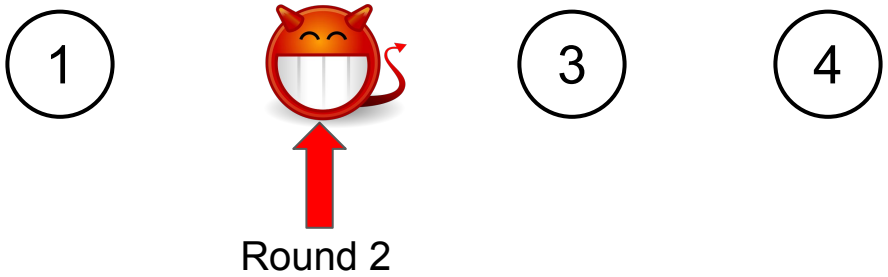
Termination when *n* & *f* are known

Electing a correct leader (king)



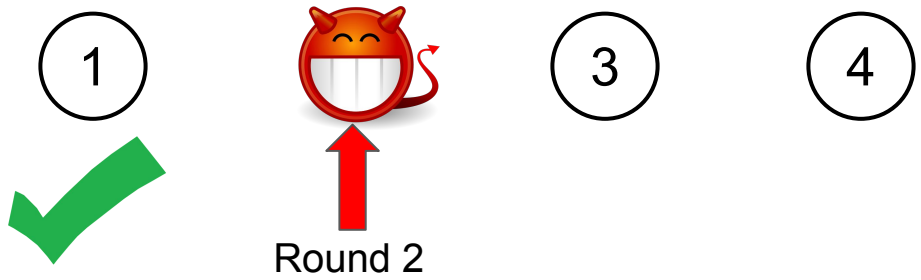
Termination when *n* & *f* are known

Electing a correct leader (king)



Termination when *n* & *f* are known

Electing a correct leader (king)



Termination when *n* & *f* are **not** known

Electing a correct leader (king)

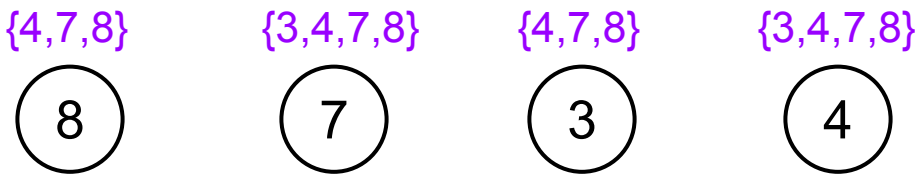
Termination when *n* & *f* are **not** known

Electing a correct leader (king)

IDs not consecutive

Termination when *n* & *f* are **not** known

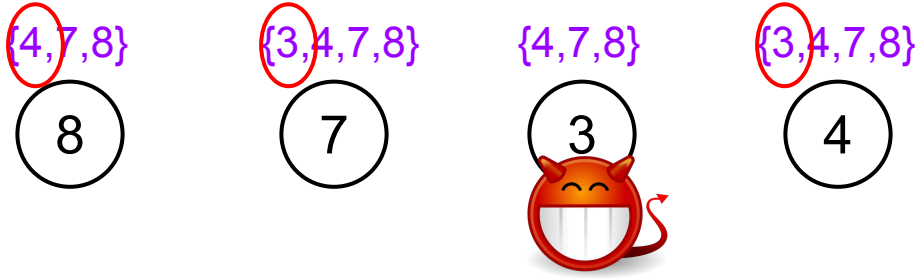
Electing a correct leader (king)



IDs not consecutive

Termination when *n* & *f* are **not** known

Electing a correct leader (king)

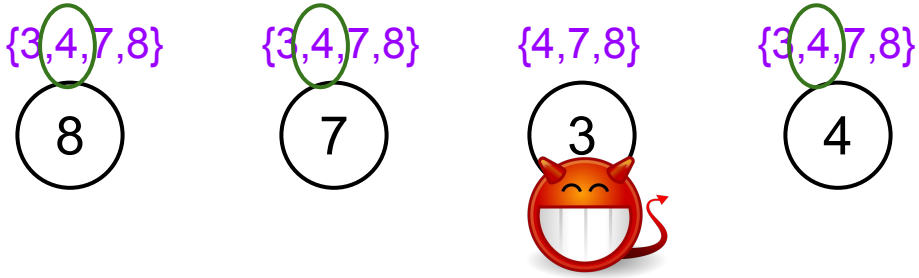


IDs not consecutive

Round 1: select smallest ID as leader

Termination when *n* & *f* are **not** known

Electing a correct leader (king)

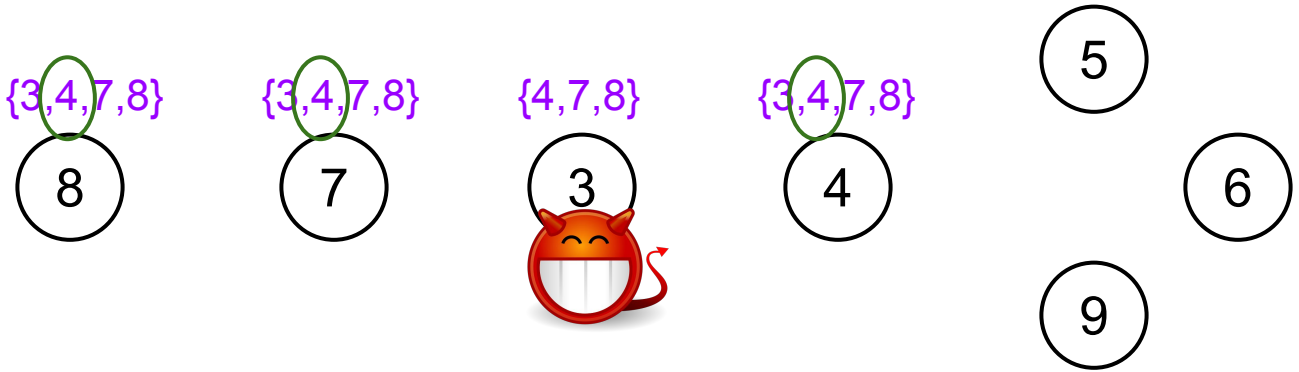


IDs not consecutive

Round 2: select 2nd smallest ID as leader

Termination when *n* & *f* are **not** known

Electing a correct leader (king)

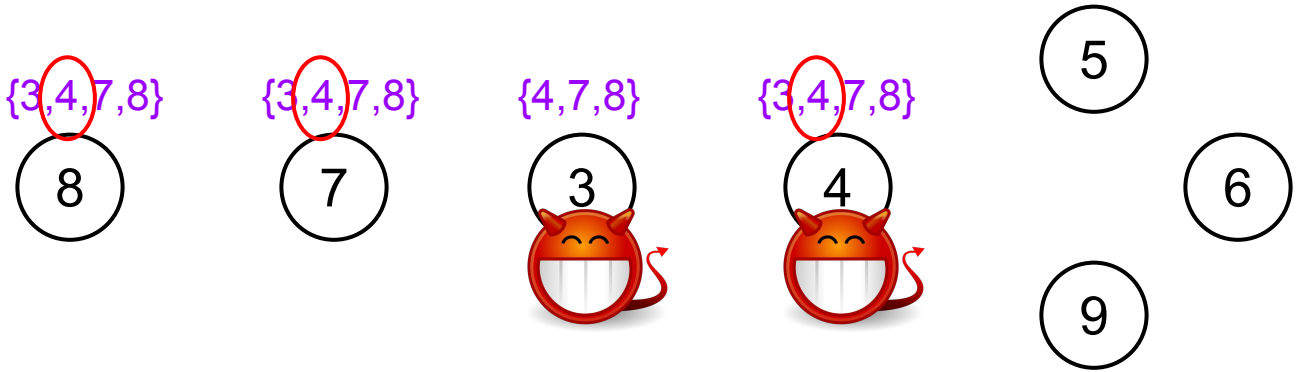


IDs not consecutive

Round 2: select 2nd smallest ID as leader

Termination when *n* & *f* are **not** known

Electing a correct leader (king)

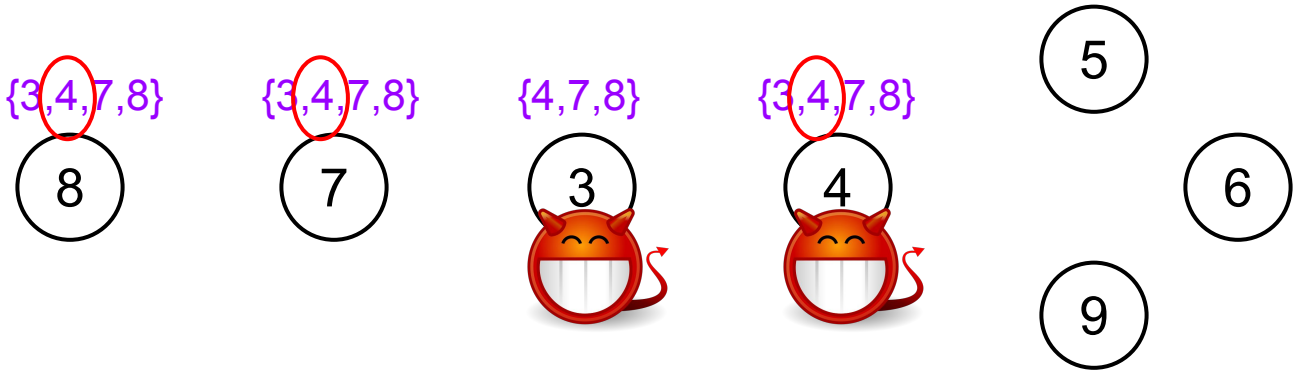


IDs not consecutive

Round 2: select 2nd smallest ID as leader

Termination when *n* & *f* are **not** known

Electing a correct leader (king)



IDs not consecutive

Round *i*: select i^{th} smallest ID as leader

Summary

Optimal resiliency of BA $n > 3f$ even w/o knowledge of n & f

Summary

Optimal resiliency of BA $n > 3f$ even w/o knowledge of n & f
Asynchrony makes it impossible

Summary

Optimal resiliency of BA $n > 3f$ even w/o knowledge of n & f
Asynchrony makes it impossible
Semi-synchrony ? Dynamics ?