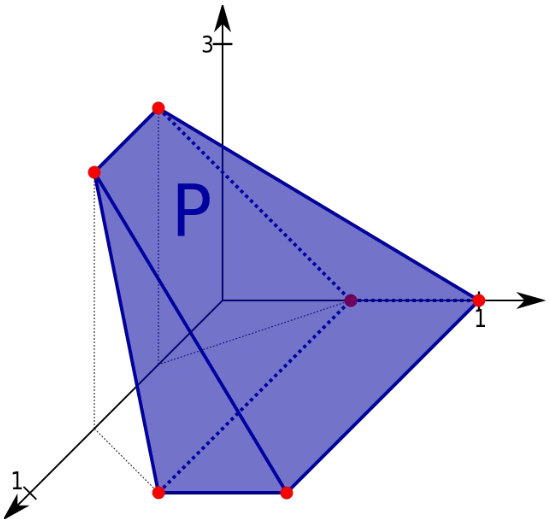
Byzantine Vector Consensus in Complete Graphs

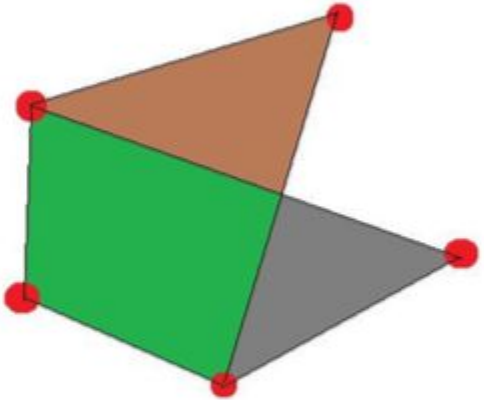
Nitin Vaidya
University of Illinois at Urbana-Champaign

Vijay Garg
University of Texas at Austin

Vector Consensus

In a lot of linear optimization problems, the feasible solutions lies inside a convex region.





Byzantine General Consensus

Works for one dimension

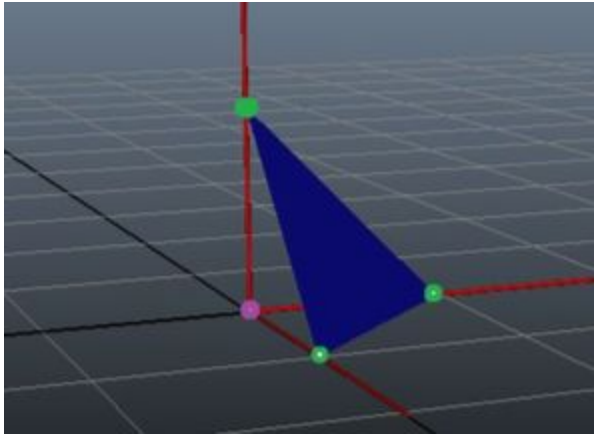
Agreement: non-faulty processes agree on the same value

Non-triviality

Termination

$n \geq 3f+1$

Naive Solution: BGA on each dimension



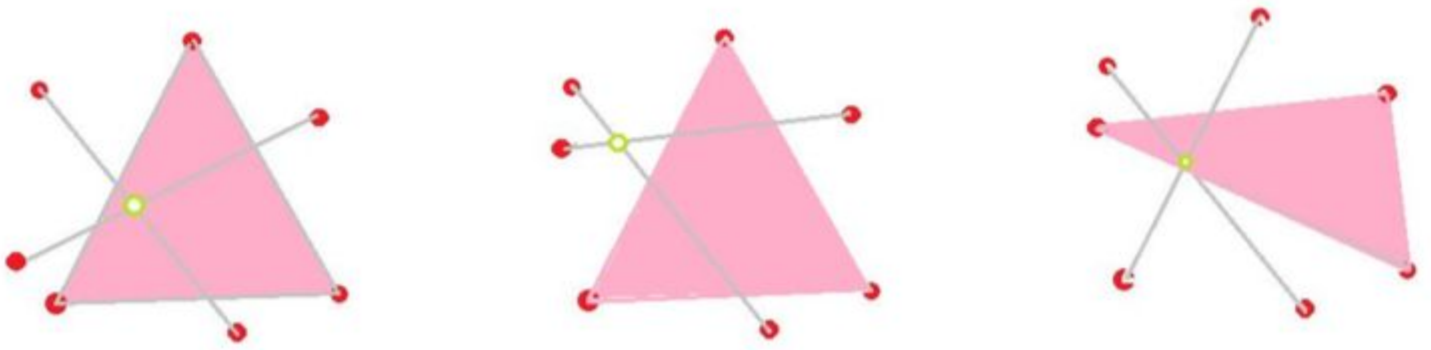
Tverberg’s Theorem

We have n points, each has d-dimensions

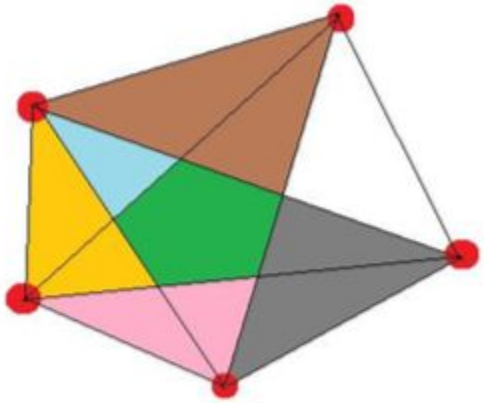
How to divide the points so that each partition intersects with other partitions on at least one point.

In particular, $n \geq (d+1)f+1$, there’s a set of $f+1$ partitions such that all the convex hulls intersects.

$n \geq (d+1)f+1$ for $n = 7$, $d = 2$, $f = 2$



Tverberg's partition exists for any |n - f| subset:



n = 5, f = 1, d = 2

All non-faulty processes can use a predetermined algorithm to find a location in this region. For example, use linear programming to locate an optimal point inside this region.

Summary

The problem of Byzantine vector consensus(BVC) requires agreement on a d-dimensional vector that is in the convex hull of the d-dimensional input vectors of the non-faulty processes. This paper states the following:

- In synchronous systems, $n \geq \max(3f+1, (d+1)f+1)$ is necessary and sufficient for achieving exact Byzantine vector consensus.

- In asynchronous systems, exact consensus is impossible in presence of faulty processes. $n \geq (d+2)f+1$ is necessary and sufficient to achieve approximate Byzantine vector consensus.

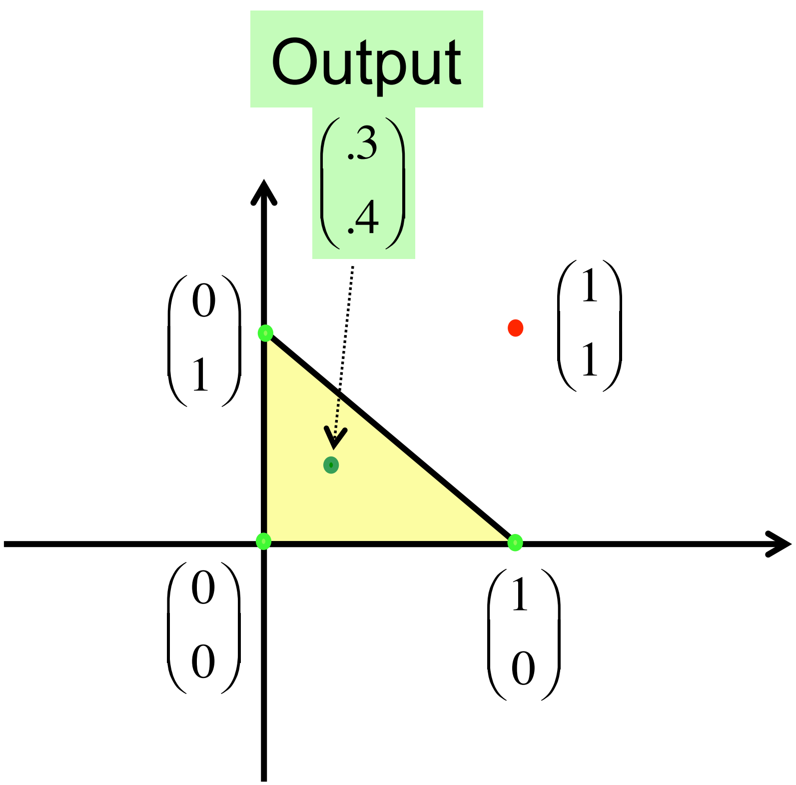
Exact Vector Consensus

- Agreement: *The decision vector at all the non-faulty processes must be identical.*

- Validity: The decision vector at each non-faulty process must be in the convex hull of the input vectors of all non-faulty processes.

- Termination: Each non-faulty process must terminate after a finite amount of time.

Inputs $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$



Traditional Consensus Problem

- Special case of vector consensus : $d = 1$

- Necessary & sufficient condition for complete graphs:

$$n \geq 3f + 1$$

in synchronous [Lamport,Shostak,Pease]

& asynchronous systems [Abraham,Amit,Dolev]

Synchronous Systems:
$n \geq \max(3, d+1)\, f + 1$ necessary

- $n \geq 3f + 1$ necessary due to Lamport, Shostak, Pease

Synchronous Systems: $n \geq \max(3, d+1)\, f + 1$ necessary

- $n \geq 3f + 1$ necessary due to Lamport, Shostak, Pease

- Proof of $n \geq (d+1)\, f + 1$ by contradiction …

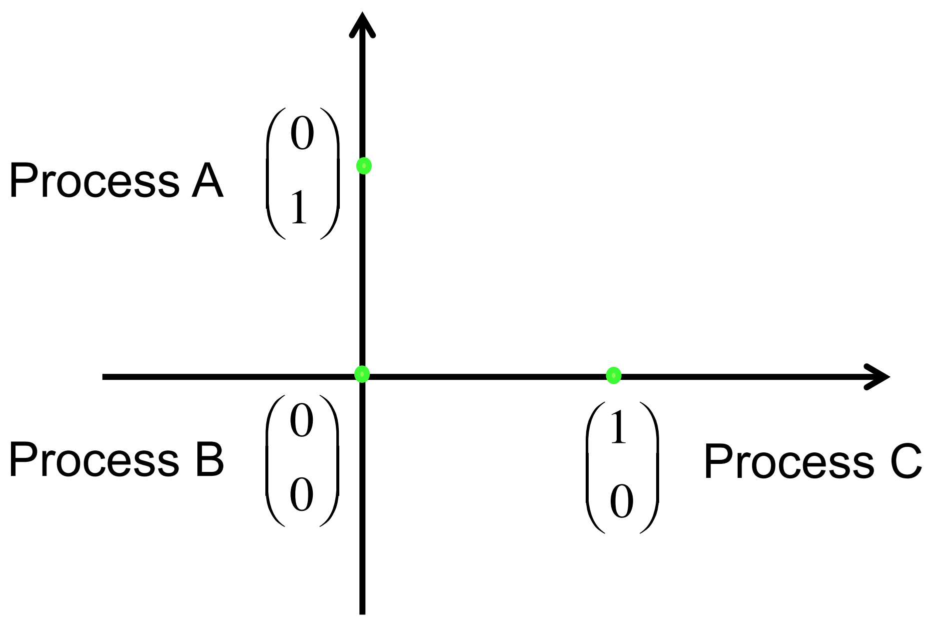
suppose that

$$f = 1$$

$$n \leq (d+1)$$

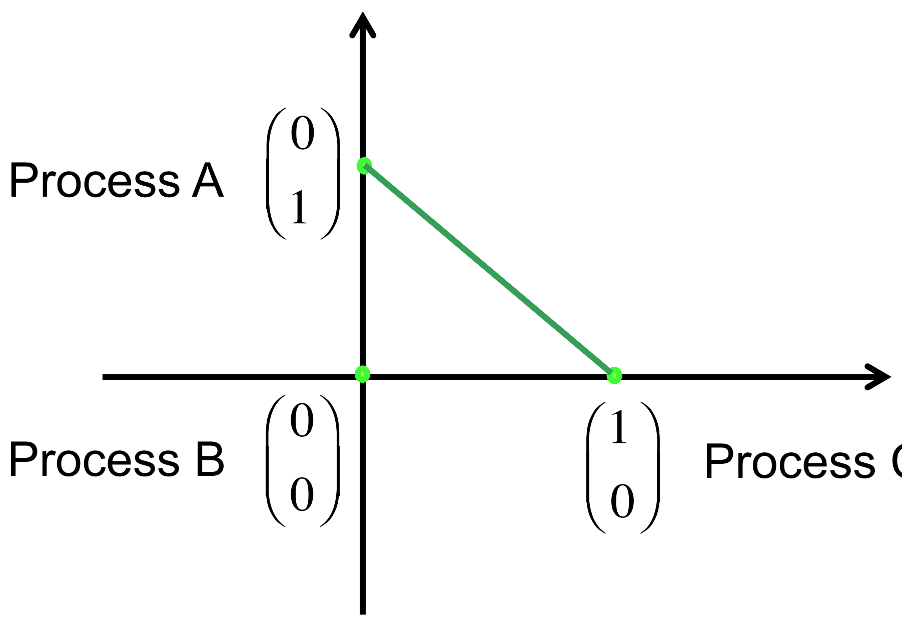
$n \leq d+1 = 3$ when $d = 2$

- Three processes, with inputs are shown below



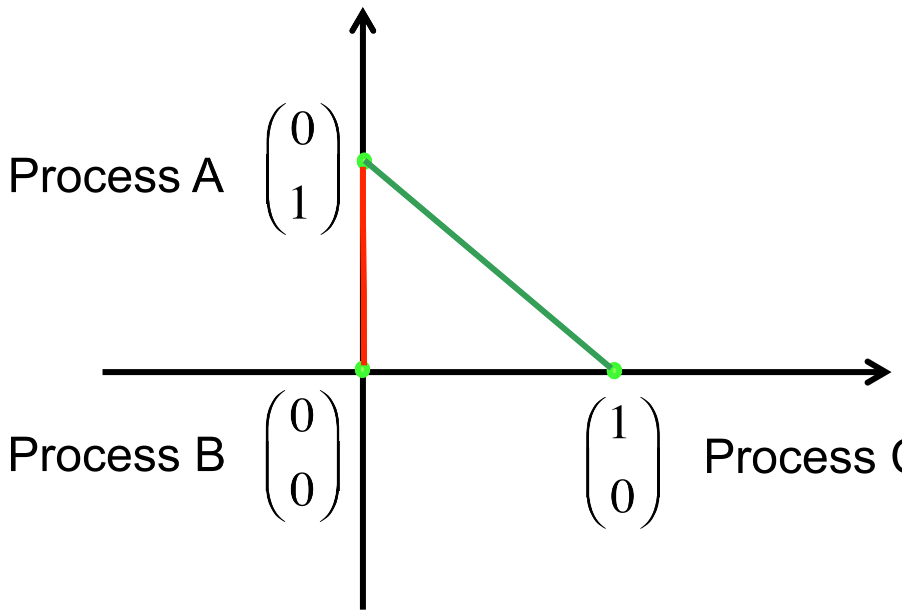
Process A's Viewpoint

- If B faulty : output on green segment (for validity)



Process A's Viewpoint

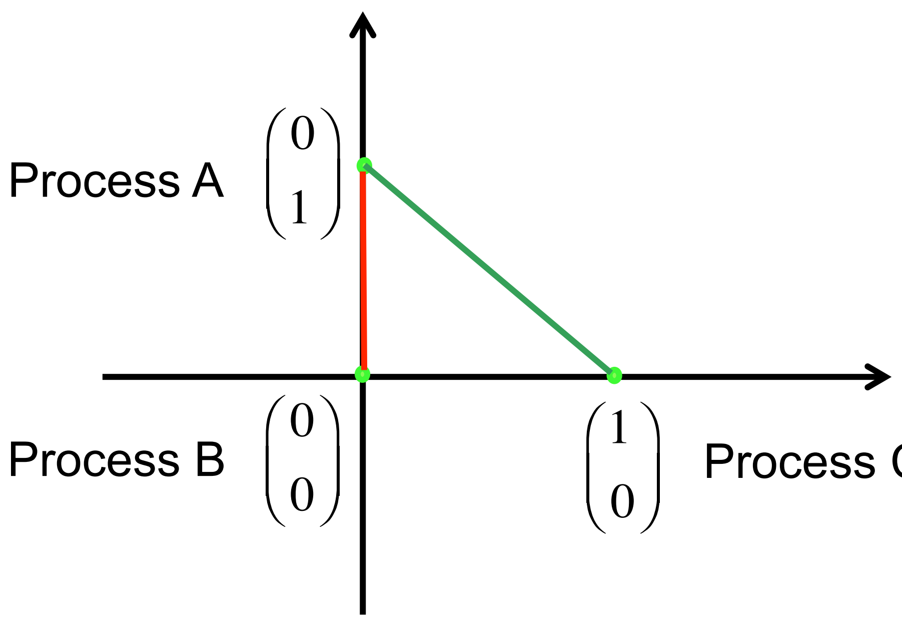
- If B faulty : output on green segment (for validity)
- If C faulty : output on red segment



Process A's Viewpoint

- If B faulty : output on green segment (for validity)
- If C faulty : output on red segment

➔ Output must be on both segments = initial state



$d = 2$

- Validity forces each process to choose output = own input

➔ No agreement

➔ $n = (d+1)$ insufficient when $f = 1$

➔ By simulation, $(d+1)f$ insufficient

Proof generalizes to all d

Synchronous System

n $\geq$ max(3,d+1) f +1

1. Reliably broadcast input vector to all processes

[Lamport,Shostak,Pease]

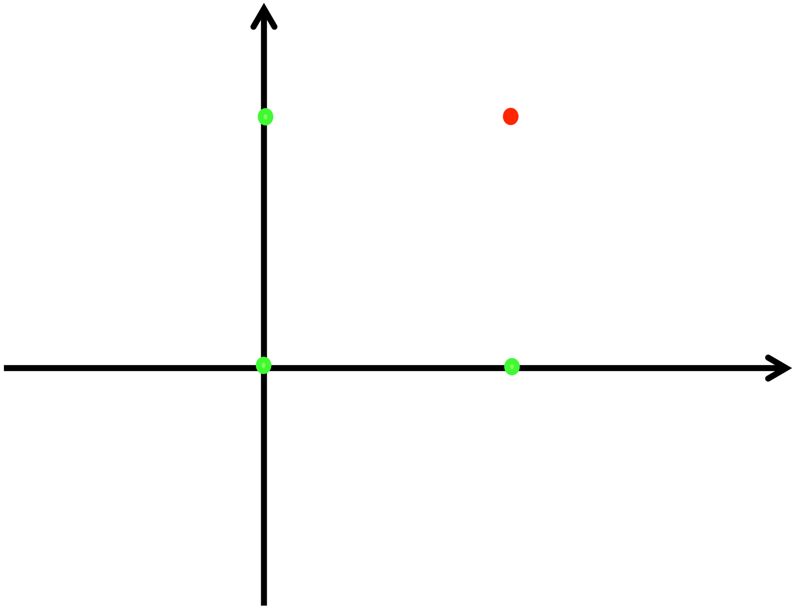
2. Receive multiset Y containing n vectors

3. Output = a deterministically chosen point in

$$\Gamma(Y) = \cap_{T \subseteq Y,\, |T|=|Y|-f}\ \mathrm{Hull}(T)$$

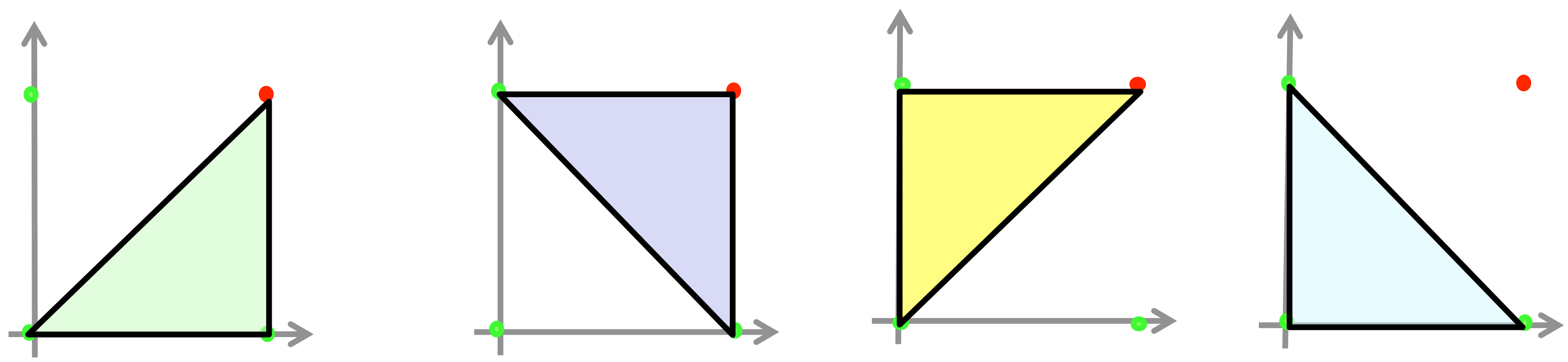
$d = 2, \quad f = 1, \quad n = 4$

- Y contains 4 points, one from faulty process



n-f = 3

- Y contains 4 points, one from faulty process
- Output in intersection of hulls of (n-f)-sets in Y



Proof of Validity

Output in $\Gamma(Y) = \cap_{T \subseteq Y,\, |T| = |Y| - f} \ \mathrm{Hull}(T)$

- Claim 1 : Intersection is non-empty
- Claim 2 : All points in intersection are in convex hull of fault-free inputs

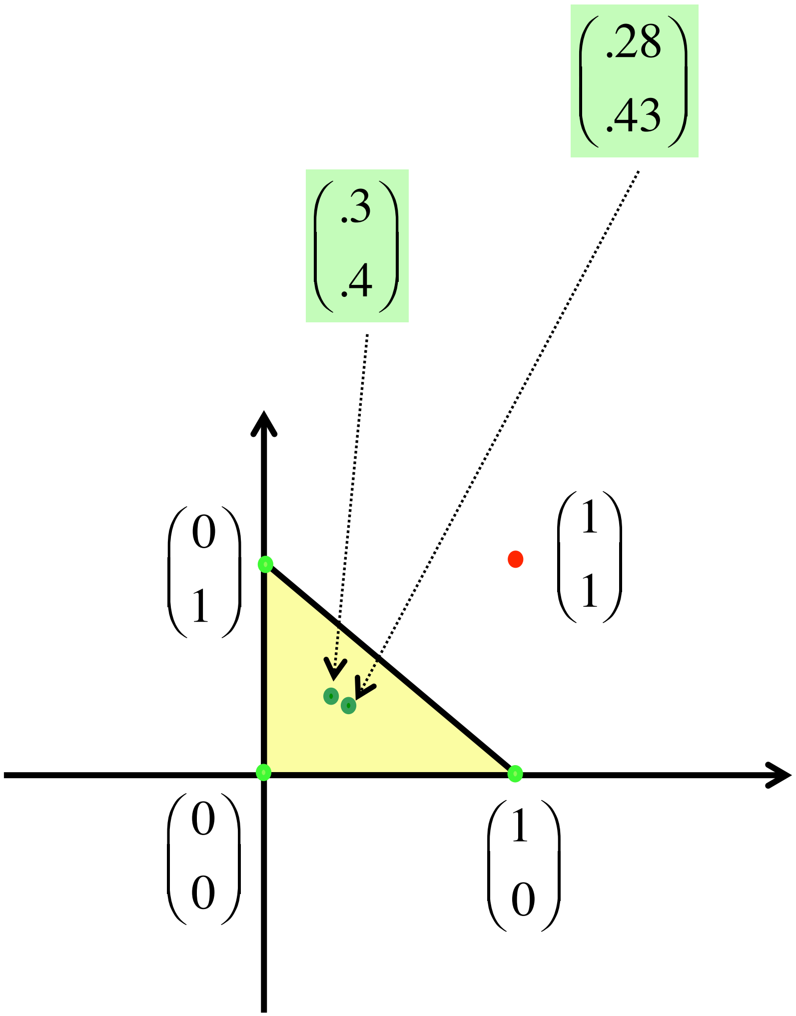
Approximate Vector Consensus

- ε-Agreement: Decision vectors at any two non-faulty processes must be within e of each other, where e > 0 is a pre-defined constant

- Validity: The decision vector at each non-faulty process must be in the convex hull of the input vectors of all non-faulty processes.

- Termination: Each non-faulty process must terminate after a finite amount of time.

$\varepsilon = 0.04$



Asynchronous BVC

Abraham, Amit and Dolev (AAD) proposed that the consensus can be approximated.

Each process i performs :

$V_i[t - 1]$,

state of at least n-f other processes,

Compute $V_i[t]$

V_i converges for all non-faulty processes.

approximate BVC work when $n-f \geq (d+1)f + 1$, or $n \geq (d+2)f + 1$