Byzantine Processes in a Topological Perspective

Zohir Bouzid Petr Kuznetsov
Télécom ParisTech, France

MMDC13 - Bremen

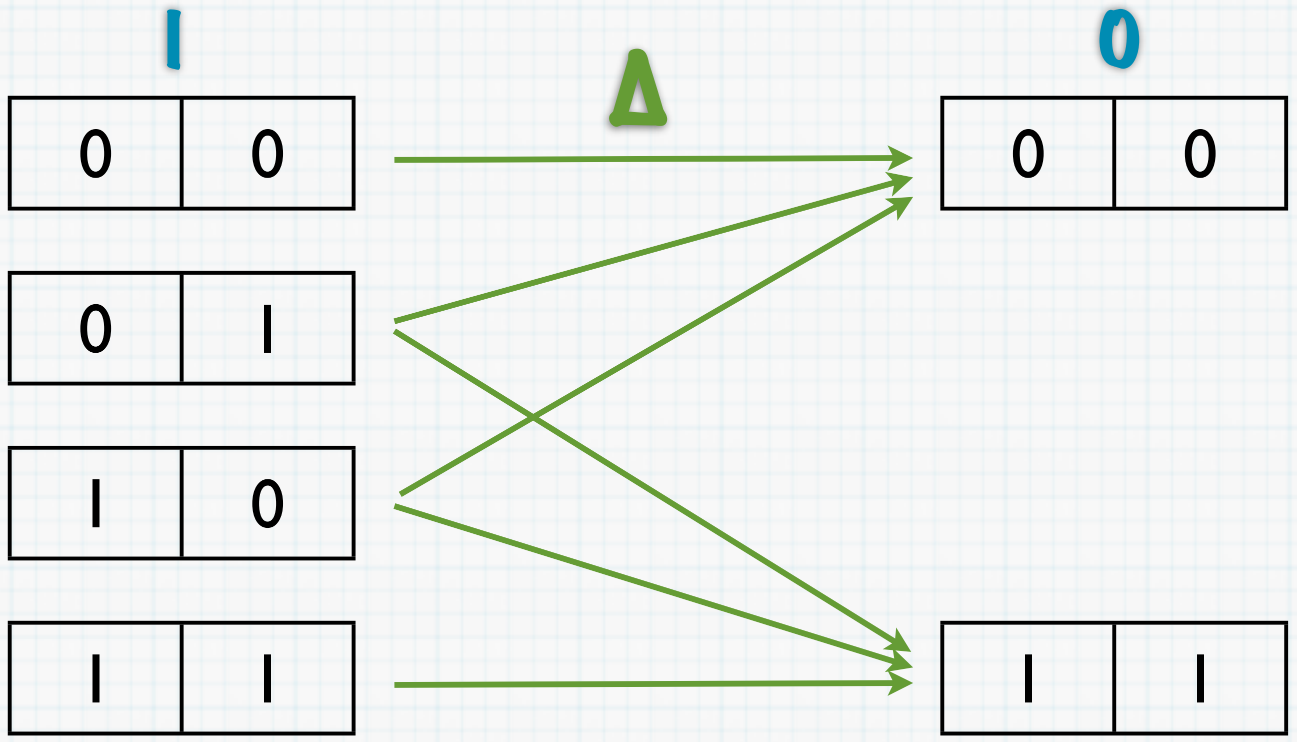
Tasks

I: a set of input vectors

O: a set of onput vectors

Δ: Given V∈I, **Δ(V)** is the set of allowable output vectors for V.

Tasks



dim(I): maximal number of distinct values in a single vector of I.

Model

Message passing with f Byzantines with $n > 3f$
(or 1WMR Shared memory with $n > 2f$)

What can be computed asynchronously in this model ?

Byzantine

Definition of a task ?

- Input of a Byzantine ? its output ?
- Δ ?

Byzantine resilience ?

Byzantine Tasks

Mendes-Herlihy-Tasson

Message passing, $n > 3f$
"strong" resilience

A task is solvable
Only If
$n-f > f * (\dim(I))$

K-Weak Agreement

Input:

a value V_i

$V = \cup V_i$

→

Output:

a set S_i

K-Agreement :

$|\cup S_i| \leq K$

Weak Validity:

For every i,

$|S_i \cap V| \geq 1$

4-Weak Agreement

Input:

1	3	2	6	3	9

Output:

{1,5}	{3}	{3,8}	{1,8}	{1,5,8}	{3}

S= {1, 3, 5, 8}

K-Weak Agreement

Message passing, n > 3f

K-WA solvable

IFF

K > 2f

(2f+1)-WA

Algorithm

1: RB-SEND (V_i)

2: WAIT until (n-f) values are received (in S)

3: CHOOSE the (f+1) maximal values $x \in S$

Properties

At most (2f+1) values are output, f among them may be byzantine.

(f+1)-WA

Mendes-Herlihy-Tasson

(f+1)-WA solvable
IFF
n-f > f * (dim(I))

Results

Message passing, n > 3f

	K-WA	Conditions
Mendes-Tasson-Herlihy	$K \geq f+1$	n-f > f * (dim(I))
Bouzid-Kuznetsov	$K \geq 2f+1$	-

(f+X)-WA

Message passing, n > 3f

	K-WA	Conditions
Mendes-Herlihy-Tasson	$K \geq f+1$ $(X=1)$	$n > f * (dim(I)+2)$
Bouzid-Kuznetsov	$K \geq 2f+1$ $(X=f+1)$	-

Problem

Message passing, $n > 3f$

Under what conditions
$(f+X)$-WA is solvable
f-resiliently ?

Notation

S : a multiset

$1_S(v)$: MULTIPLICITY of v in S

S^* : SET of values in S

Example

S = {1, 1, 1, 2, 5, 6, 6}

$1_S(6)$ = 2

S^* = {1, 2, 5, 6}

Notation

Let $V \in I$ (an input vector),

$M_f(V)$ = min { $|W^*|$: ($W \subseteq V$) and ($|W| = f+1$) }

Examples:

$M_3($

1	2	7	5	9	7	8	3

$)=3$

$M_3($

1	2	6	5	9	7	8	3

$)=4$

$M_2($

1	2	1	2	3	1	3	4

$)=1$

Notation

$\Omega_f(I)$ = max ($M_f(V)$: $V \in I$, $|V|=n-f$)

Examples:

MENDES-HERLIHY-TASSON : $\Omega_f(I) = 1$

BOUZID-KUZNETSOV : $\Omega_f(I) = f+1$

$(f+\Omega_f(I))$-WA

Algorithm

1: RB-SEND (V_i)

2: put received values in S

3: WAIT until
$|S| \geq (n-f)$ and $M_f(S) \leq \Omega_f(I)$

4: CHOOSE the $M_f(S)$ maximal values $x \in S$
Lexical order $(1_S(x), x)$

At most $(\Omega_f(I) + f)$ values are output.

Results

Message passing, $n > 3f$

	K-WA	Conditions
Mendes-Tasson-Herlihy	$K \geq f+1$	$n-f > f * (dim(I))$
Bouzid-Kuznetsov	$K \geq 2f+1$	-
	$K \geq f+X$	$X \geq \Omega_f(I)$

Ongoing Work

Topological characterisation
of (f, Υ)-resilient solvable tasks ($\Upsilon \leq f$)