TRUTHFUL MECHANISMS FOR GENERALIZED UTILITARIAN PROBLEMS

G. MELIDEO,[1] P.P.,[2] G. PROIETTI,[1,3]
R. WATTENHOFER,[4] P. WIDMAYER[4]

[1] UNIVERSITÀ DI L'AQUILA
[2] UNIVERSITÀ DI SALERNO
[3] CNR
[4] ETH ZÜRICH

INTERNET

- NO CENTRAL AUTHORITY
- SELF-INTERESTED COMPONENTS
  - DIFFERENT GOALS
  - NOT ALTRUISTIC
  - MAY NOT FOLLOW THE "PROTOCOL"

PRIVATE COMPANIES
AUTONOMOUS SYSTEMS
PROVIDERS
UNIVERSITIES
⋮

INTERNET

- NO CENTRAL AUTHORITY

- SELF-INTERESTED COMPONENTS
  - DIFFERENT GOALS
  - NOT ALTRUISTIC
  - MAY NOT FOLLOW THE "PROTOCOL"

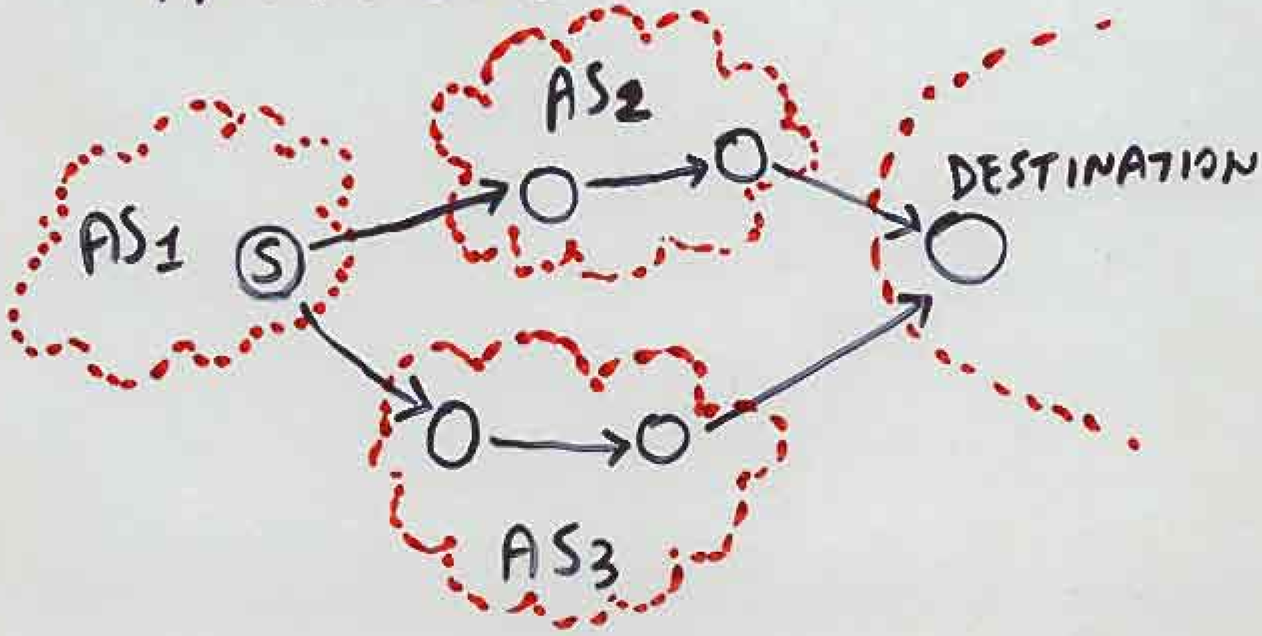
$\Updownarrow$

SELFISH AGENTS

INTERNET ROUTING

AUTONOMOUS SYSTEMS

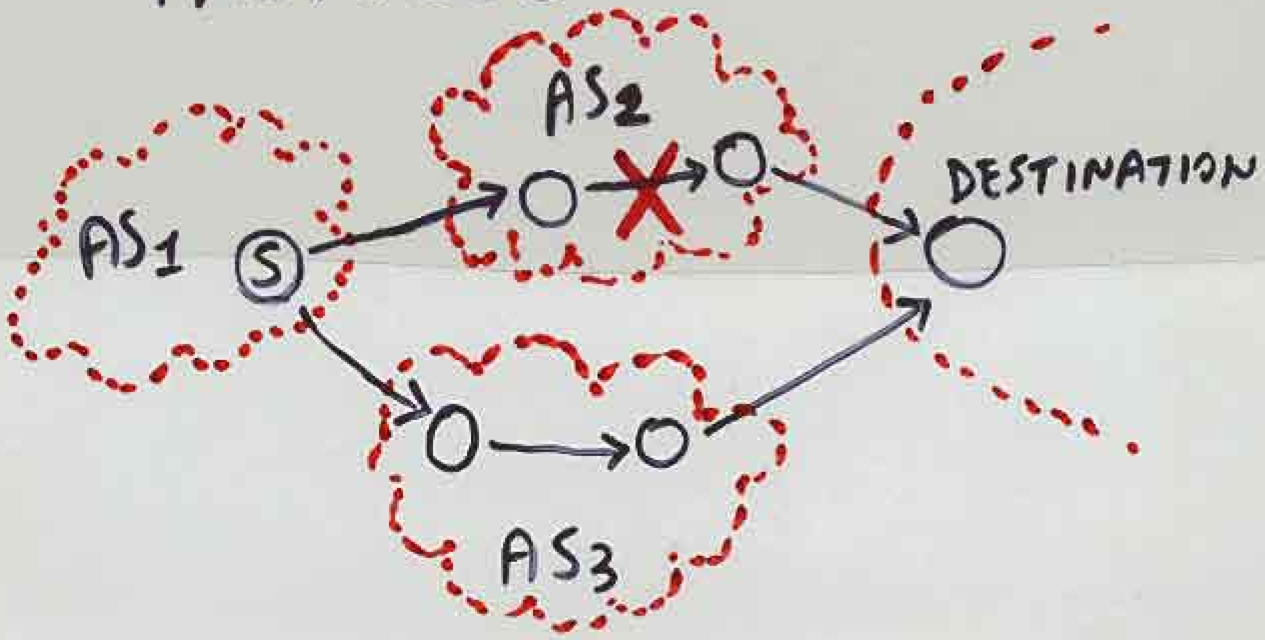
- OWN PHYSICAL RESOURCES (ROUTERS, SUBNETS,..)
- EXCHANGE INFORMATION
- IMPLEMENT ROUTING PROTOCOL



INTERNET ROUTING

AUTONOMOUS SYSTEMS

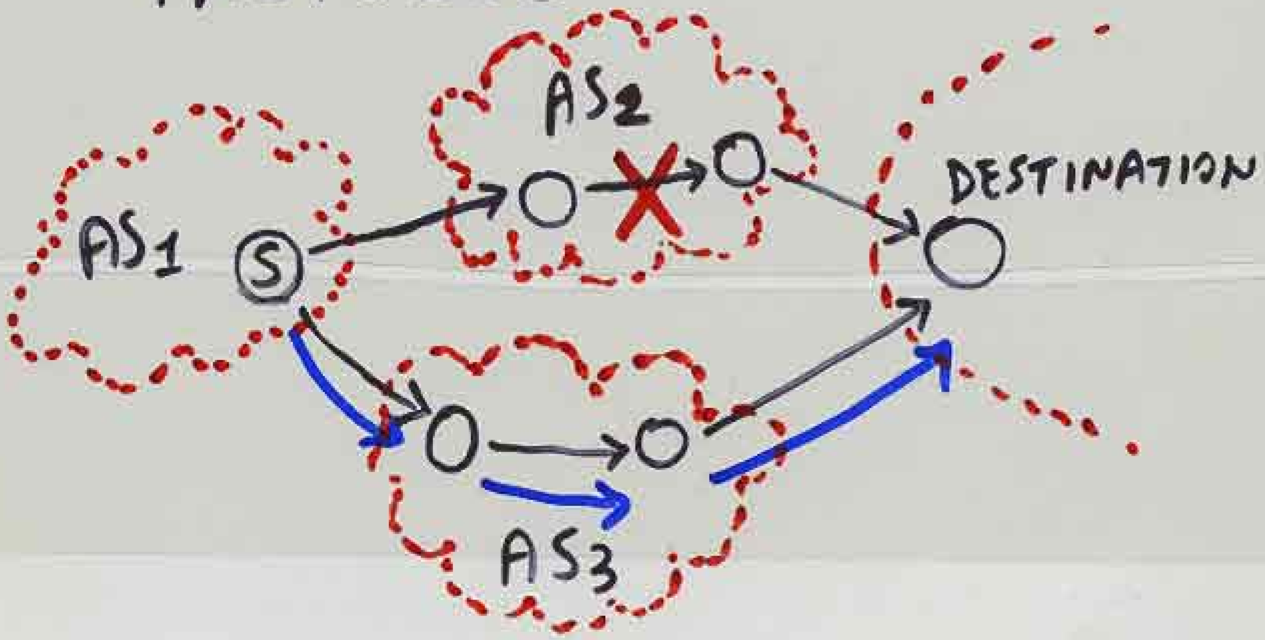
- OWN PHYSICAL RESOURCES (ROUTERS, SUBNETS,..)
- EXCHANGE INFORMATION
- IMPLEMENT ROUTING PROTOCOL



INTERNET ROUTING

AUTONOMOUS SYSTEMS

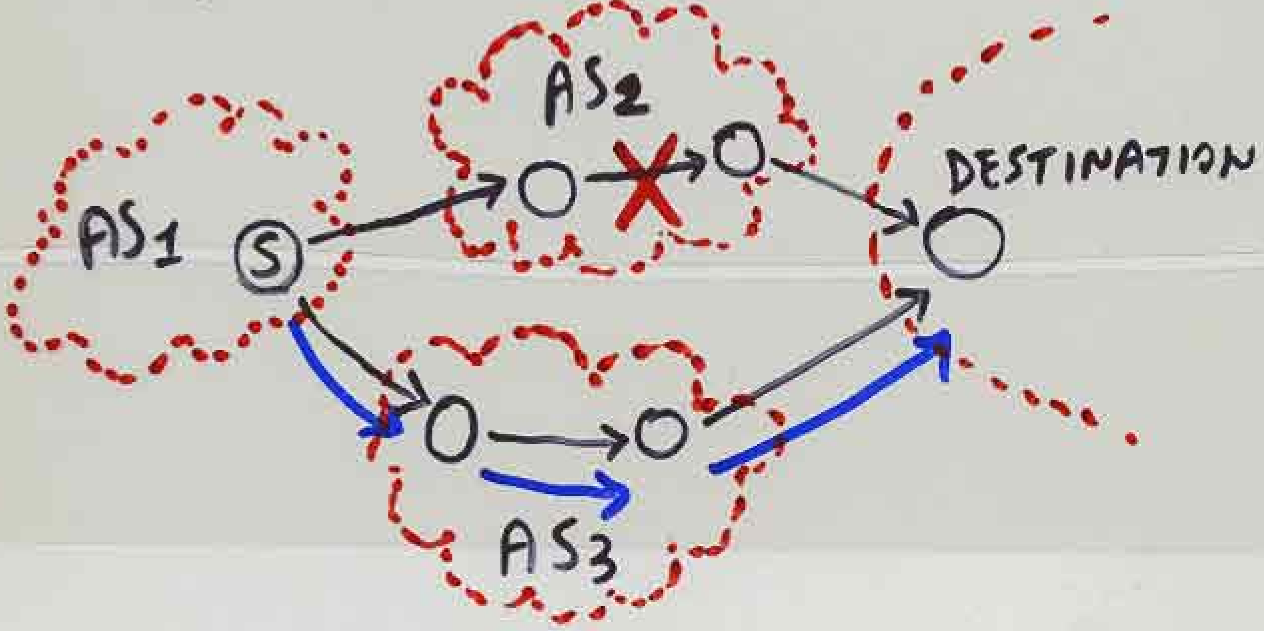
- OWN PHYSICAL RESOURCES (ROUTERS, SUBNETS,..)
- EXCHANGE INFORMATION
- IMPLEMENT ROUTING PROTOCOL



INTERNET ROUTING

AUTONOMOUS SYSTEMS

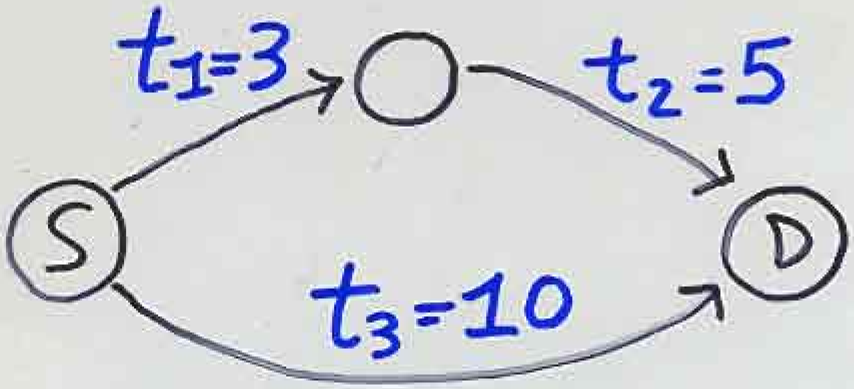
- OWN PHYSICAL RESOURCES (ROUTERS, SUBNETS,..)
- EXCHANGE INFORMATION
- IMPLEMENT ROUTING PROTOCOL



FALSE LINK STATUS

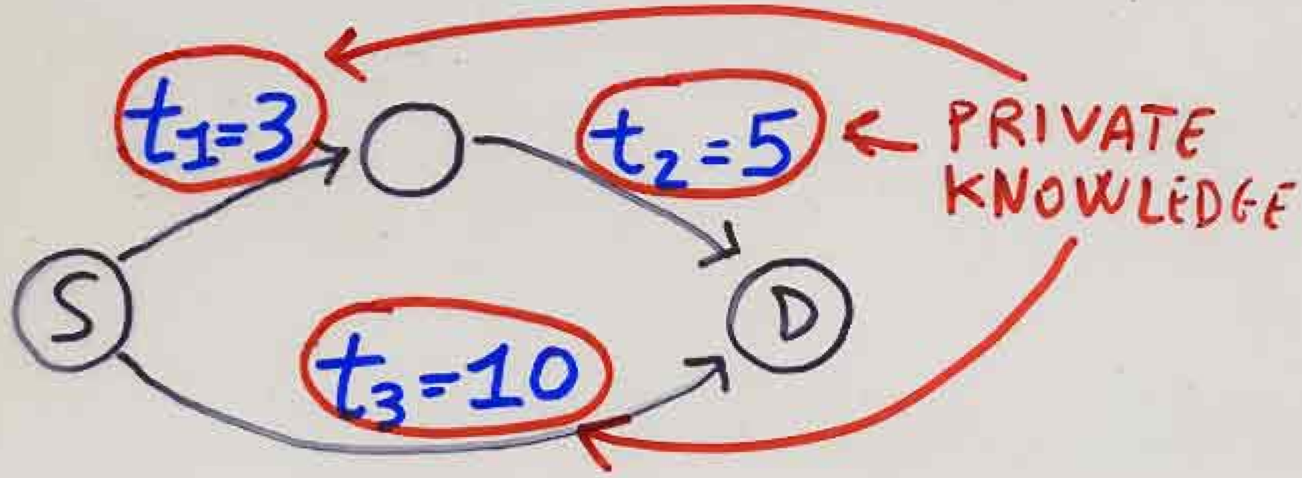
⇓

REDIRECT THE TRAFFIC



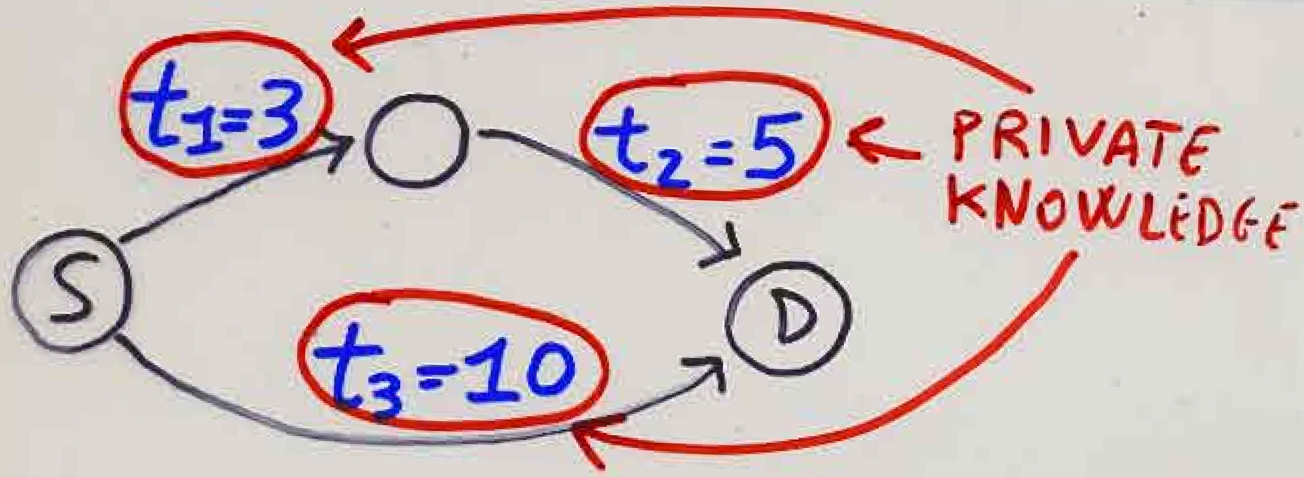
t_i = TIME TO PROCESS 1 PACKET OVER LINK i

<u>GOAL</u>: PICK THE CHEAPEST PATH FROM S TO D



t_i = TIME TO PROCESS 1 PACKET OVER LINK i

<u>GOAL</u>: PICK THE CHEAPEST PATH FROM S TO D

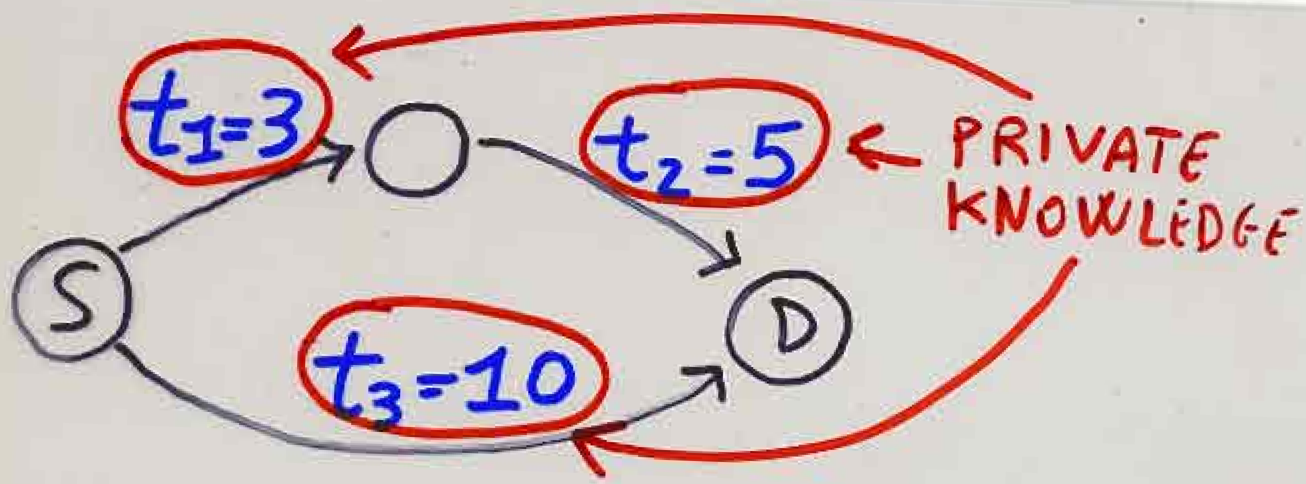


t_i = TIME TO PROCESS 1 PACKET OVER LINK i

$\Downarrow$

COST FOR AGENT i

<u>GOAL</u>: PICK THE CHEAPEST PATH FROM S TO D



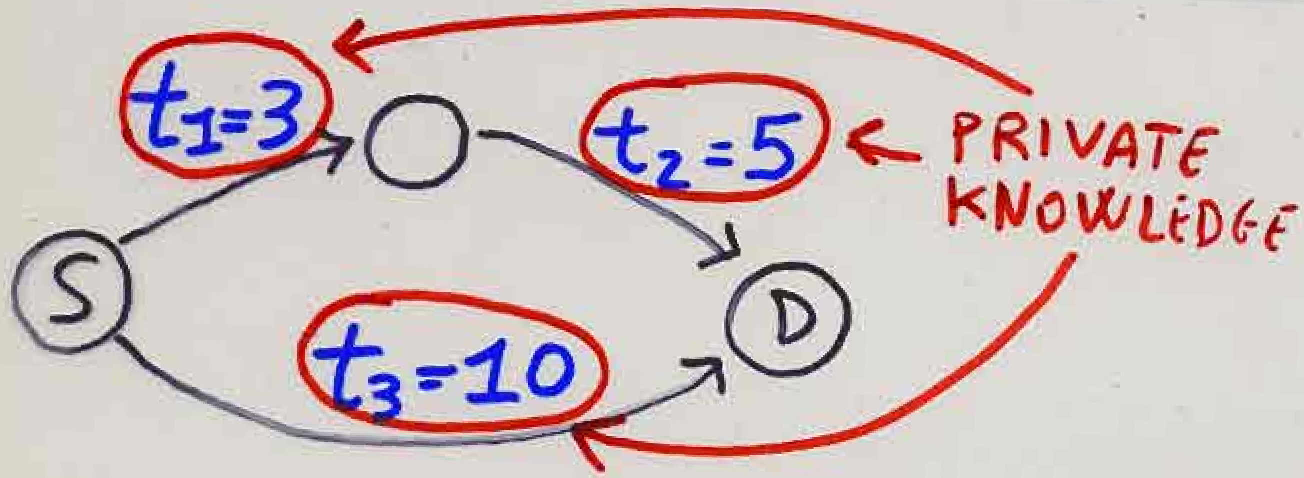
t_i = TIME TO PROCESS 1 PACKET OVER LINK i

$\Downarrow$

COST FOR AGENT i

GOAL: PICK THE CHEAPEST PATH FROM S TO D

AGENTS CAN CHEAT: REPORT $r_i \neq t_i$



t_i = TIME TO PROCESS 1 PACKET OVER LINK i

$\Downarrow$

COST FOR AGENT i

GOAL: PICK THE CHEAPEST PATH FROM S TO D

AGENTS CAN CHEAT: REPORT $r_i \neq t_i$

GIVE INCENTIVES!

PROBLEMS INVOLVING SELFISH AGENTS

INPUT: $I = (\pi, t)$

PUBLIC

PRIVATE

$t_1, \dots, t_m$

$AG_1 \quad AG_m$

MEASURE: SOLUTION X

$m(X, t)$

DEPENDS ON PRIVATE INPUT

GOAL: OPTIMIZE $m(X, t)$
(MAXIMIZE)

PROBLEMS INVOLVING SELFISH AGENTS

INPUT: $I = (\pi, t)$

PUBLIC PRIVATE

$t_1, \dots, t_m$

AG_1 AG_m

MEASURE: SOLUTION X

$m(X, t)$

DEPENDS ON PRIVATE INPUT

GOAL: OPTIMIZE $m(X, t)$
(MAXIMIZE)

WE NEED $t_1, \dots, t_m$!

MECHANISM DESIGN

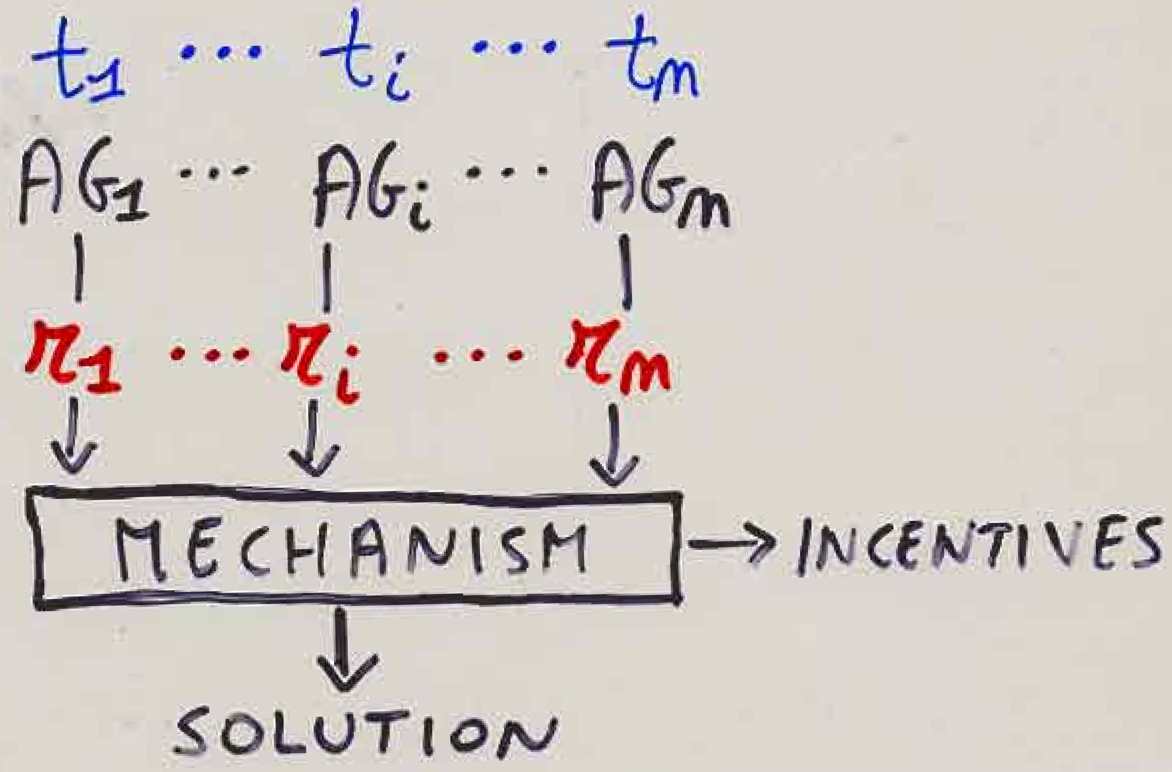
MECHANISM:

ALGORITHM + INCENTIVES
(e.g. PAYMENTS)

MECHANISM DESIGN

MECHANISM:

ALGORITHM + INCENTIVES
(e.g. PAYMENTS)



MECHANISM DESIGN

MECHANISM:

ALGORITHM + INCENTIVES
(e.g. PAYMENTS)

$t_1 \cdots t_i \cdots t_m$ ← PRIVATE

$AG_1 \cdots AG_i \cdots AG_m$

$r = (r_1 \cdots r_i \cdots r_m)$ REPORTED INFOS

$\boxed{\text{MECHANISM}} \rightarrow$ INCENTIVES

$\downarrow$

SOLUTION

MECHANISM DESIGN

MECHANISM:

ALGORITHM + INCENTIVES
(e.g. PAYMENTS)

$$
\begin{tikzcd}
 & M=(A,P) \arrow[dl] \arrow[dr] & \\
X=A(r) \arrow[dr] & & P_1(r),\dots,P_i(r),\dots,P_m(r) \arrow[dl] \\
\underline{AG_i}: & \mu_i(X, P_i(r), t_i) &
\end{tikzcd}
$$

X AND $P_i(r)$ DEPEND ON

$r = (r_1, \dots, r_i, \dots, r_m)$

MECHANISM DESIGN

MECHANISM:

ALGORITHM + INCENTIVES
(e.g. PAYMENTS)

$$M=(A,P)$$

$$X=A(r) \qquad P_1(r),\dots,P_i(r),\dots,P_m(r)$$

$\underline{AG_i}$:

$$\underbrace{u_i(X, P_i(r), t_i)}_{\text{AG}_i \text{ WANTS TO MAXIMIZE THIS}}$$

X AND $P_i(r)$ DEPEND ON

$$r=(r_1,\dots,\underline{r_i},\dots,r_m)$$

MECHANISM DESIGN

MECHANISM:

ALGORITHM + INCENTIVES
(e.g. PAYMENTS)

$$M=(A,P)$$

$$X=A(r) \qquad P_1(r),\dots,P_i(r),\dots,P_m(r)$$

$\underline{AG_i}$:

$$\mu_i(X, P_i(r), t_i)$$

CAN LIE ($r_i \neq t_i$)

X AND $P_i(r)$ DEPEND ON

$$r=(r_1,\dots,\underline{r_i},\dots,r_m)$$

MAIN ISSUES

WHICH PROBLEMS CAN BE SOLVED?

- $M=(A,P)$ IS TRUTHFUL
- $A(t)$ IS OPTIMAL SOLUTION

GENERAL TECHNIQUES?

ANSWER:

UTILITARIAN PROBLEMS

CAN BE SOLVED WITH

VCG MECHANISMS

[VICREY'61, CLARKE'71, GROVES'73]

THE ONLY WAY (IN SOME CASES)

[GREEN-LAFFONT'77]

MECHANISM $M = (A, P)$ IS **TRUTHFUL** IF

$$t_i \longleftarrow AG_i \longrightarrow \pi_i$$

MECHANISM $M=(A,P)$ IS **TRUTHFUL** IF

$$AG_i$$

$$r_1,\dots,r_{i-1},t_i,r_{i+1},\dots,r_m \qquad\qquad r_1,\dots,r_{i-1},r_i,r_{i+1},\dots,r_m$$

MECHANISM $M = (A, P)$ IS **TRUTHFUL** IF

AG_i

$$A(r_1, \ldots, r_{i-1}, t_i, r_{i+1}, \ldots, r_m) \qquad A(r_1, \ldots, r_{i-1}, r_i, r_{i+1}, \ldots, r_m)$$

$$P_i(\quad " \qquad\qquad " \quad) \qquad P_i(\quad " \quad " \quad " \quad)$$

$$\Downarrow \qquad\qquad\qquad \Downarrow$$

$$u_i(t_i, r_{-i}) \geq u_i(r_i, r_{-i})$$

MECHANISM $M = (A, P)$ IS **TRUTHFUL** IF

$$\forall i, \forall r_{-i} = (r_1, \ldots, r_{i-1}, r_{i+1}, \ldots, r_m), \forall r_i$$

AG_i

$$\begin{matrix} A(r_1, \ldots, r_{i-1}, t_i, r_{i+1}, \ldots, r_m) \\ P_i(\quad " \qquad\qquad " \quad) \\ \Downarrow \\ u_i(t_i, r_{-i}) \end{matrix} \quad \geq \quad \begin{matrix} A(r_1, \ldots, r_{i-1}, r_i, r_{i+1}, \ldots, r_m) \\ P_i(\quad " \qquad " \qquad " \quad) \\ \Downarrow \\ u_i(r_i, r_{-i}) \end{matrix}$$

MECHANISM $M=(A,P)$ IS **TRUTHFUL** IF

$$\forall i,\ \forall r_{-i}=(r_1,\dots,r_{i-1},r_{i+1},\dots,r_m),\ \forall r_i$$

AG_i

$$\begin{array}{ccc} A(r_1,\dots,r_{i-1},t_i,r_{i+1},\dots,r_m) & & A(r_1,\dots,r_{i-1},r_i,r_{i+1},\dots,r_m) \\ P_i(\quad '' \qquad\qquad '' \quad) & & P_i(\quad '' \quad '' \quad '' \quad) \\ \Downarrow & & \Downarrow \\ u_i(t_i,r_{-i}) & \geq & u_i(r_i,r_{-i}) \end{array}$$

NONE HAS AN INCENTIVE TO LIE, EVER!!

UTILITARIAN PROBLEMS

UTILITIES:

$$\mu_i(P_i, X, t_i)$$

$$\|$$

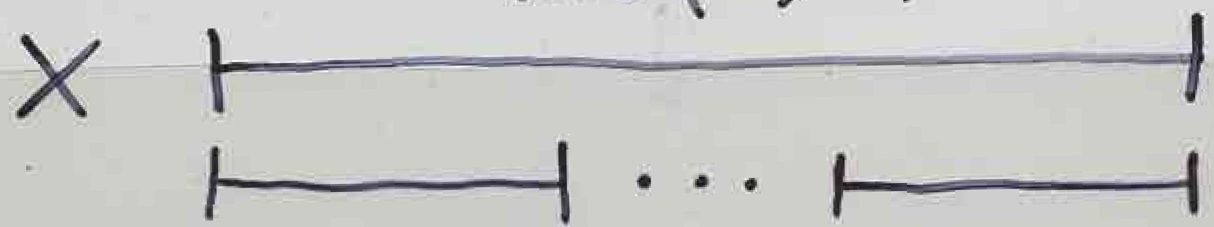
$$VAL_i(X, t_i) + P_i$$

$\Uparrow$ HOW MUCH AG_i "LIKES" SOLUTION X

$\Uparrow$ MONEY RECEVED

MEASURE:

$$m(X, t)$$



$$VAL_1(X, t_1) + \cdots + VAL_m(X, t_m)$$

SOLUTIONS: $SOL(I) = SOL(\pi)$

$\uparrow$ PUBLIC

UTILITARIAN PROBLEMS

UTILITIES:

$$\mu_i(P_i, X, t_i)$$

$$\parallel$$

TOO RESTRICTIVE

$$VAL_i(X, t_i) + P_i$$

HOW MUCH AG_i "LIKES" SOLUTION X

MONEY RECEVED

TOO RESTRICTIVE

MEASURE:

$$m(X, t)$$

X

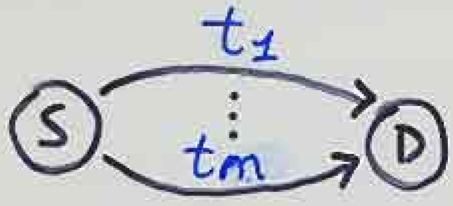
$$VAL_1(X, t_1) + \cdots + VAL_m(X, t_m)$$

SOLUTIONS: $SOL(I) = SOL(\pi)$

PUBLIC

NON-UTILITARIAN CASES

EX1: MOST RELIABLE LINK



$$t_i = \Pr[\text{LINK } i \text{ DOES NOT FAIL}]$$

INCENTIVE: PAY P_i IF LINK i SUCCEDED

UTILITY: $\mu_i(X, P_i, t_i) = P_i \cdot \underbrace{t_i}_{\mathrm{VAL}_i(X, t_i)}$

EX2: TASK SCHEDULING

X = JOB ALLOCATION

$\mathrm{VAL}_i(X, t_i)$ = FINISH TIME OF MACHINE i

$$m(X, t) = \mathrm{MAX}\left(\mathrm{VAL}_1(X, t_1), \ldots, \mathrm{VAL}_m(X, t_m)\right)$$

OUR CONTRIBUTION

① EXTEND THE VCG IDEA TO A <u>WIDER CLASS</u> OF PROBLEMS:

CONSISTENT PROBLEMS (EXTEND UTILITARIAN) $\longleftarrow$ TRUTHFUL VCGC MECHANISMS (EXTEND VCG)

② UNIQUENESS

$C^{VCGC}_{ONLY} \longleftarrow$ ONLY VCGC WORK

③ LIMITS

$C^{VCGC}_{NONE} \longleftarrow$ VCGC DO NOT WORK

$C_{NONE} \longleftarrow$ NO TRUTHFUL MECHANISM

④ APPLICATIONS

NON-UTILITARIAN PROBLEMS

(BASIC CS PROBLEMS)

INTUITION

OUR GOAL	AG_i'S GOAL
$m(X,t)$	$\mu_i(X,P_i,t_i)$

POSSIBLE "=" IF $m(\cdot)$ AND $\mu_i(\cdot)$ HAVE A COMMON "ROOT"

$$
\begin{tikzcd}
 & \oplus \arrow[dl] \arrow[dr] & \\
\mu_i(X,P_i,t_i) & & m(X,t) \\
\mathrm{VAL}_i(X,\lambda)\in P_i & & \mathrm{VAL}_1(X,\lambda_1)\oplus\cdots\oplus\mathrm{VAL}_m(X,\lambda_m)
\end{tikzcd}
$$

INTUITION

OUR GOAL | AG$_i$'S GOAL

$$m(X,t) = \mu_i(X, P_i, t_i)$$

AG$_i$ IS WILLING TO HELP US

(MAXIMIZE $m(X,t)$) ☺

INTUITION

OUR GOAL AG$_i$'S GOAL

$$m(X,t) \;=\; \mathcal{U}_i(X, P_i, t_i)$$

AG$_i$ IS WILLING TO HELP US
(MAXIMIZE $m(X,t)$) ☺

POSSIBLE "=" IF $m(\cdot)$ AND $\mathcal{U}_i(\cdot)$
HAVE A COMMON "ROOT"

INTUITION

OUR GOAL — AG$_i$'S GOAL

$$m(X,t) \quad = \quad \mu_i(X,P_i,t_i)$$

AG$_i$ IS WILLING TO HELP US
(MAXIMIZE $m(X,t)$)

POSSIBLE "=" IF $m(\cdot)$ AND $\mu_i(\cdot)$
HAVE A COMMON "ROOT"

$$\oplus$$

$$\mu_i(X,P_i,t_i) = VAL_i(X,t_i) \oplus P_i \qquad m(X,t) = VAL_1(X,t_1) \oplus \cdots \oplus VAL_m(X,t_m)$$

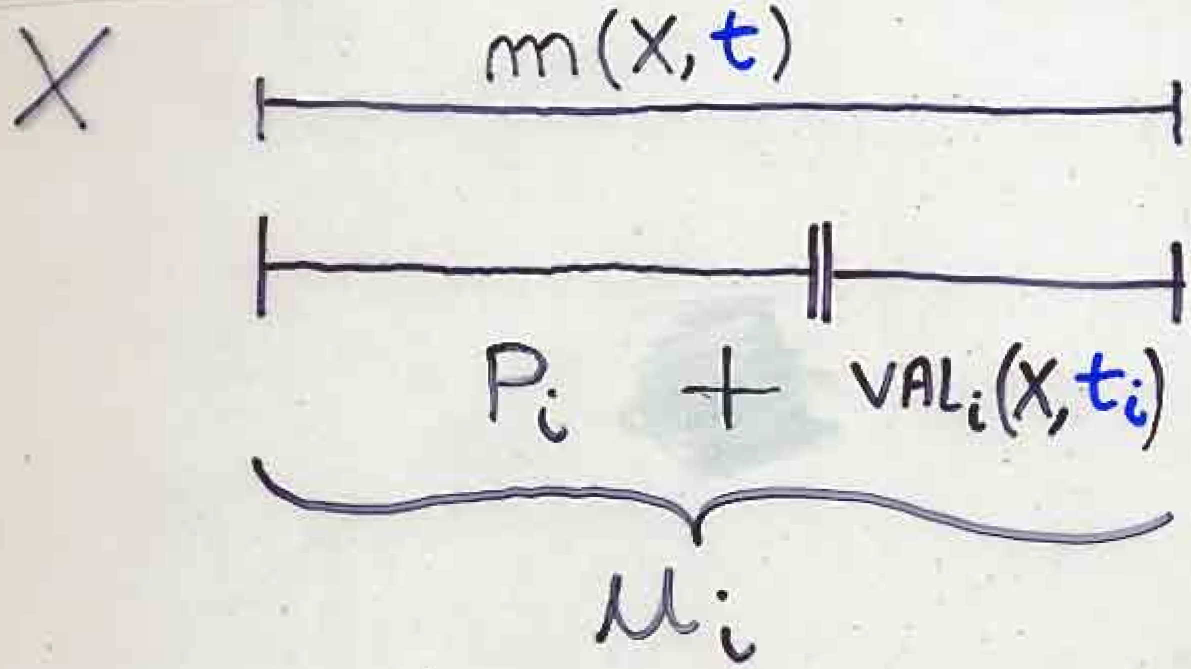
VCG PAYMENTS

KNOW ALL BUT ONE (t_i)

X

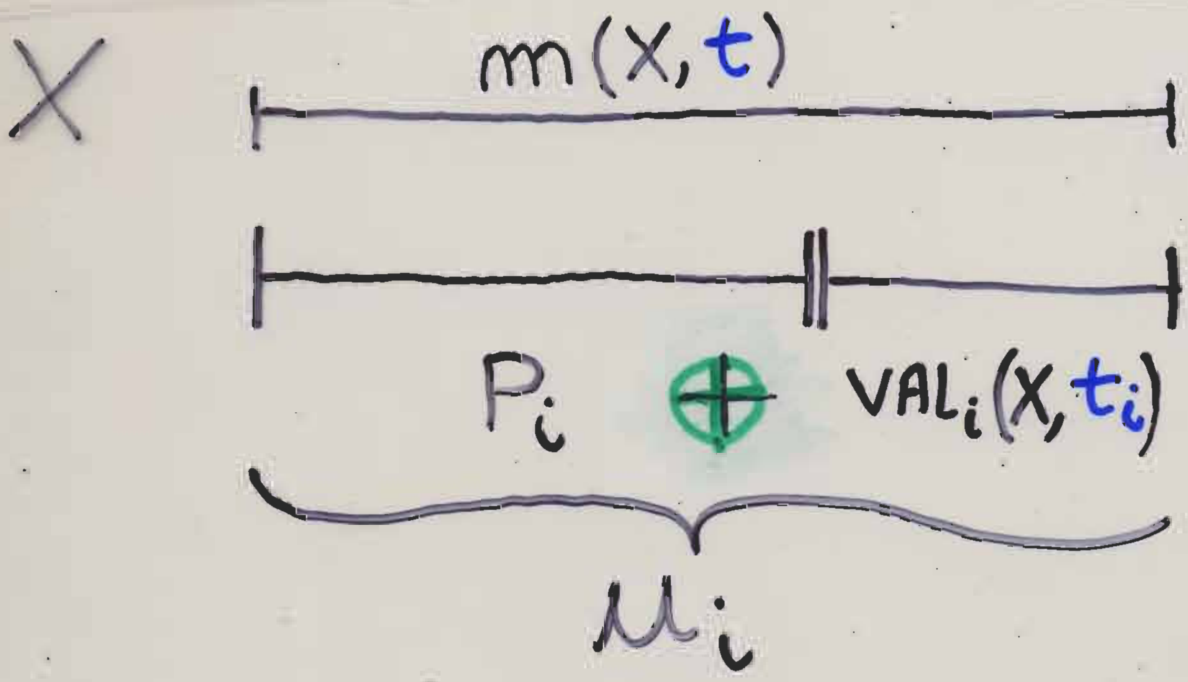
VCG PAYMENTS

KNOW ALL BUT ONE (t_i)



VCG PAYMENTS

KNOW ALL BUT ONE (t_i)



VCG PAYMENTS

KNOW ALL BUT ONE (t_i)

X $\qquad m(X,t)$

$$\underbrace{P_i \oplus VAL_i(X,t_i)}_{\mu_i}$$

$$P_i = \bigoplus_{j \neq i} VAL_j(X, \pi_j)$$

$$\Downarrow$$

$$\mu_i = m(X, (\pi_1, \dots, \pi_{i-1}, t_i, \pi_{i+1}, \dots, \pi_m))$$

VCG PAYMENTS

X

$$m(X,t)$$

$$\underbrace{P_i \oplus \mathrm{VAL}_i(X,t_i)}_{\mu_i}$$

$$P_i = \bigoplus_{j \neq i} \mathrm{VAL}_j(X,\pi_j)$$

$$\Downarrow ? \qquad (\text{'}+\text{' ok})$$

$$\mu_i = m(X,(\pi_1,\ldots,\pi_{i-1},t_i,\pi_{i+1},\ldots,\pi_n))$$

TRUTHFULNESS:

$$\begin{tikzcd}[column sep=small]
 & AG_i \arrow[dl] \arrow[dr] & \\
t_i \arrow[d, Rightarrow] & & r_i \arrow[d, Rightarrow] \\
\mu_i & & \mu_i'
\end{tikzcd}$$

$$\mu_i = m(X, (r_1, \dots, t_i, \dots, r_m)) \qquad \mu_i' = m(X', (r_1, \dots, t_i, \dots, r_m))$$

TRUTHFULNESS:

$$
\begin{tikzcd}
 & AG_i \arrow[dl] \arrow[dr] & \\
t_i \arrow[d, Rightarrow] & & r_i \arrow[d, Rightarrow] \\
\mu_i \arrow[d, equal] & & \mu_i' \arrow[d, equal] \\
m(X,(r_1,\dots,t_i,\dots,r_m)) & \geq & m(X',(r_1,\dots,t_i,\dots,r_m)) \\
\underbrace{A^*(r_1,\dots,t_i,\dots,r_m)}_{\text{OPT FOR } r_1,\dots,t_i,\dots,r_m} \arrow[u] & & A^*(r_1,\dots,r_i,\dots,r_m) \arrow[u]
\end{tikzcd}
$$

$$\mathcal{U}_i(X, P_i, t_i) \overset{?}{\Longrightarrow} m(X, \cdot)$$

DICOMPOSE $m(X, \pi)$ [PAYMENTS]

$$VAL_1(X, \pi_1) \oplus \cdots \oplus VAL_i(X, \pi_i) \oplus \cdots \oplus VAL_m(X, \pi_m)$$

RIASSEMBLE $m(X, \cdot)$ [UTILITY]

$$\mathcal{U}_i(X, P_i, t_i) = P_i \oplus VAL_i(X, t_i) =$$

$$(A \oplus B) \oplus VAL_i(X, t_i)$$

$$\mu_i(X,P_i,t_i) \overset{?}{\Longrightarrow} m(X,\cdot)$$

DICOMPOSE $m(X,\pi)$ [PAYMENTS]

$$VAL_1(X,\pi_1) \oplus \cdots \oplus VAL_i(X,\pi_i) \oplus \cdots \oplus VAL_m(X,\pi_m)$$

$$\mu_i(X, P_i, t_i) \xrightarrow{?} m(X, \cdot)$$

DICOMPOSE $\quad m(X, \pi) \quad$ [PAYMENTS]

$$\underbrace{VAL_1(X,\pi_1) \oplus \cdots \oplus}_{A} VAL_i(X, t_i) \underbrace{\oplus \cdots \oplus VAL_m(X, \pi_m)}_{B}$$

$$P_i = A \oplus B$$

$$u_i(X,P_i,t_i) \overset{?}{\Longrightarrow} m(X,\cdot)$$

DICOMPOSE $m(X,\pi)$ [PAYMENTS]

$$\underbrace{VAL_1(X,\pi_1)\oplus\cdots\oplus}_{A} VAL_i\cancel{(X,\pi_i)} \underbrace{\oplus\cdots\oplus VAL_m(X,\pi_m)}_{B}$$

$$P_i = A \oplus B$$

RIASSEMBLE $m(X,\cdot)$ [UTILITY]

$$u_i(X,P_i,t_i) = P_i \oplus VAL_i(X,t_i) =$$
$$(A \oplus B) \oplus VAL_i(X,t_i)$$

$$\mu_i(X, P_i, t_i) \overset{?}{\Longrightarrow} m(X, \cdot)$$

DICOMPOSE $m(X, \pi)$ [PAYMENTS]

$$\underbrace{VAL_1(X, \pi_1) \oplus \cdots \oplus}_{A} \cancel{VAL_i(X, \pi_i)} \underbrace{\oplus \cdots \oplus VAL_m(X, \pi_m)}_{B}$$

$$P_i = A \oplus B$$

RIASSEMBLE $m(X, \cdot)$ [UTILITY]

$$\mu_i(X, P_i, t_i) = P_i \oplus VAL_i(X, t_i) =$$

$$(A \oplus B) \oplus VAL_i(X, t_i)$$

$$\parallel$$

$$A \oplus VAL_i(X, t_i) \oplus B$$

$$\mathcal{U}_i(X,P_i,t_i) \overset{?}{\Longrightarrow} m(X,\cdot)$$

DICOMPOSE $m(X,\tau)$ [PAYMENTS]

$$\underbrace{VAL_1(X,\tau_1)\oplus\cdots\oplus}_{A} VAL_i(X,\cancel{\tau_i}) \underbrace{\oplus\cdots\oplus VAL_m(X,\tau_m)}_{B}$$

$$P_i = A\oplus B$$

RIASSEMBLE $m(X,\cdot)$ [UTILITY]

$$\mathcal{U}_i(X,P_i,t_i) = P_i \oplus VAL_i(X,t_i) =$$

$$(A\oplus B)\oplus VAL_i(X,t_i)$$

$$\|$$

$$\underbrace{A\oplus VAL_i(X,t_i)\oplus B}_{m(X,(\tau_1,\dots,\tau_{i-1},t_i,\tau_{i+1},\dots,\tau_m))}$$

$$\mathcal{M}_i(X,P_i,t_i) \overset{?}{\Longrightarrow} m(X,\cdot)$$

DICOMPOSE $m(X,\pi)$ [PAYMENTS]

$$\underbrace{VAL_1(X,\pi_1)\oplus\cdots\oplus}_{A} VAL_i(\cancel{X,\pi_i}) \underbrace{\oplus\cdots\oplus VAL_m(X,\pi_m)}_{B}$$

$$P_i = A \oplus B$$

RIASSEMBLE $m(X,\cdot)$ [UTILITY]

$$\mathcal{M}_i(X,P_i,t_i) = P_i \oplus VAL_i(X,t_i) =$$

$$(A\oplus B)\oplus VAL_i(X,t_i)$$

$$\|$$

$$A \oplus VAL_i(X,t_i) \oplus B$$

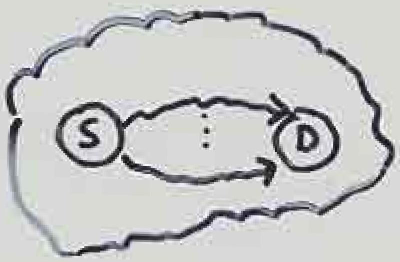
CONSISTENT PROBLEMS: "$\oplus$" ASSOCIATIVE, COMMUTATIVE

$$SOL(I) = SOL(\pi)$$

PUBLIC PART

MOST RELIABLE PATH

G =



$$\bigcirc \xrightarrow{t_i} \bigcirc$$

$$\Uparrow$$

$$\Pr[\text{LINK } i \text{ FAILS}]$$

<u>GOAL</u>: FIND MOST RELIABLE PATH FROM S TO D

MAXIMIZE $m(X, t)$

$$m(X,t) = \prod_{i \in X} t_i$$

UTILITY:

EXPECTED PAYMENT $P_i \cdot t_i$

PAYMENTS:

$$P_i = \Pr[X \text{ DOES NOT FAIL} \mid i \text{ DOES NOT FAIL}]$$

TASK SCHEDULING

m MACHINES, ℓ JOBS

ASSIGNMENT:

$$X : [\ell] \longrightarrow [m]$$

$$\Downarrow$$

$$\mathrm{VAL}_i(X, t_i) = -\begin{pmatrix}\text{FINISH TIME} \\ \text{OF MACHINE } i\end{pmatrix}$$

<u>GOAL</u>: MINIMIZE MAKESPAN

$$\max_i \{-\mathrm{VAL}_i(X, t_i)\}$$

CONSISTENT?

<u>YES</u>: "RENT THE MACHINES"

RENTING:

1) PAY α – FINISH TIME

2) NO MORE THAN P_i

$$\Downarrow$$

MONEY TO AG_i:

$$\text{MIN}\left\{\alpha + VAL_i(X, t_i), P_i\right\}$$

$$m(X, t) = \text{MIN}_i \left\{VAL_i(X, t_i)\right\}$$

CONSISTENT! ☺

__NOTE__: WITHOUT "RENTING" NO MECHANISM (EVEN FOR $m=2$)

[NISAN-RONEN'99]

RENTING:

1) PAY α - ~~FINISH~~ RELEASE TIME

2) NO MORE THAN P_i

$$\Downarrow$$

MONEY TO AG_i:

$$\text{MIN}\{\alpha + \text{VAL}_i(X, t_i), P_i\}$$

$$m(X, t) = \text{MIN}_i\{\text{VAL}_i(X, t_i)\}$$

CONSISTENT! ☺

<u>NOTE</u>: WITHOUT "RENTING" NO MECHANISM (EVEN FOR $m=2$)

[NISAN-RONEN'99]

OPEN QUESTIONS

SEMI-CONSISTENT PROBLEMS ?

$$\oplus \Downarrow m(X,t) = VAL_1(X,t_1) \oplus \cdots \oplus VAL_m(X,t_m)$$

$$\otimes \Downarrow \mu_i(X,P_i,t_i) = VAL_i(X,t_i) \otimes P_i$$

HOW MUCH COMPUTATIONAL ISSUES HELP ?

- TASK SCHEDULING
  (MAKE THE PROBLEM CONSISTENT)
- SELFISH KNAPSACK
  (WHICH INFORMATION ARE "CRITICAL")

INTUITION

OUR GOAL — AG$_i$'S GOAL

$$m(X,t) = \mathcal{M}_i(X,P_i,t_i)$$

AG$_i$ IS WILLING TO HELP US (MAXIMIZE $m(X,t)$)

POSSIBLE "=" IF $m(\cdot)$ AND $\mathcal{M}_i(\cdot)$ HAVE A COMMON "ROOT"

$$\oplus$$

$$\mathcal{M}_i(X,P_i,t_i) = VAL_i(X,t_i) \oplus P_i$$

$$m(X,t) = VAL_1(X,t_1) \oplus \cdots \oplus VAL_m(X,t_m)$$

IDENTICAL

MECH. DESIGN PART (FIND $P_i(\cdot)$)