Teoría de Juegos en contextos de seguridad

Pamela Alejandra Bustamante Faúndez[1]

[1]Pontificia Universidad Católica de Chile

14 Agosto 2020

About me

- Estudiante de Doctorado en Ciencias de la Ingeniería, Pontificia Universidad Católica de Chile
- Magíster en Ingeniería Industrial, Universidad del Bío-Bío, Chile
- Ingeniería Civil Industrial, Universidad del Bío-Bío, Chile

PONTIFICIA
UNIVERSIDAD
CATÓLICA
DE CHILE

UNIVERSIDAD DEL BÍO-BÍO

- www.pamelabustamante.com
- https://github.com/pambus
- pebustamante@uc.cl

About me

- Lenguajes de programación preferidos
  - Python
  - Julia (`https://introajulia.org/`)
  - C++
- Presentación de hoy
  - `https://github.com/pambus/or_gametheory`

Índice 1

1. Investigación de Operaciones
   - Definición
   - Aplicaciones
2. Teoría de Juegos
   - Juegos de Stackelberg
   - Juegos de Seguridad de Stackelberg
   - Juegos de Seguridad de Stackelberg

Investigación de Operaciones

Enfoque científico en la toma de decisiones que busca el mejor diseño y operación de un sistema, generalmente en condiciones que requireren la asignación de recursos escasos (Winston, 2005).

Ejemplo 1: Mochila

Tenemos n artículos y una mochila de capacidad C. Cada artículo i tiene una determinada utilidad u_i y peso v_i. Queremos elegir qué artículos llevar en la mochila, maximizando la utilidad obtenida y sin sobrepasar la capacidad de la mochila.

Vamos a definir un modelo de optimización para solucionar este problema.

Partes de un modelo LP

- Las **variables de decisión** que pretendemos determinar.
- El **objetivo** (la meta) que necesitamos optimizar (maximizar o minimizar).
- Las **restricciones** que la solución debe satisfacer.

Modelo Ejemplo 2: Mochila

Variables

$$x_i = \begin{cases} 1 & \text{Si el artículo i se coloca en la mochila} \\ 0 & \text{En otro caso} \end{cases} \quad \forall i \in [0, ..., n]$$

Modelo

Función Objetivo

$$\max \sum_i u_i x_i$$

s.a

Restricciones

$$\sum_i v_i x_i \leq C \qquad \forall i \in [0, ..., n]$$

$$x_i \in [0, 1] \qquad \forall i \in [0, ..., n]$$

Maneras de obtener solución exacta

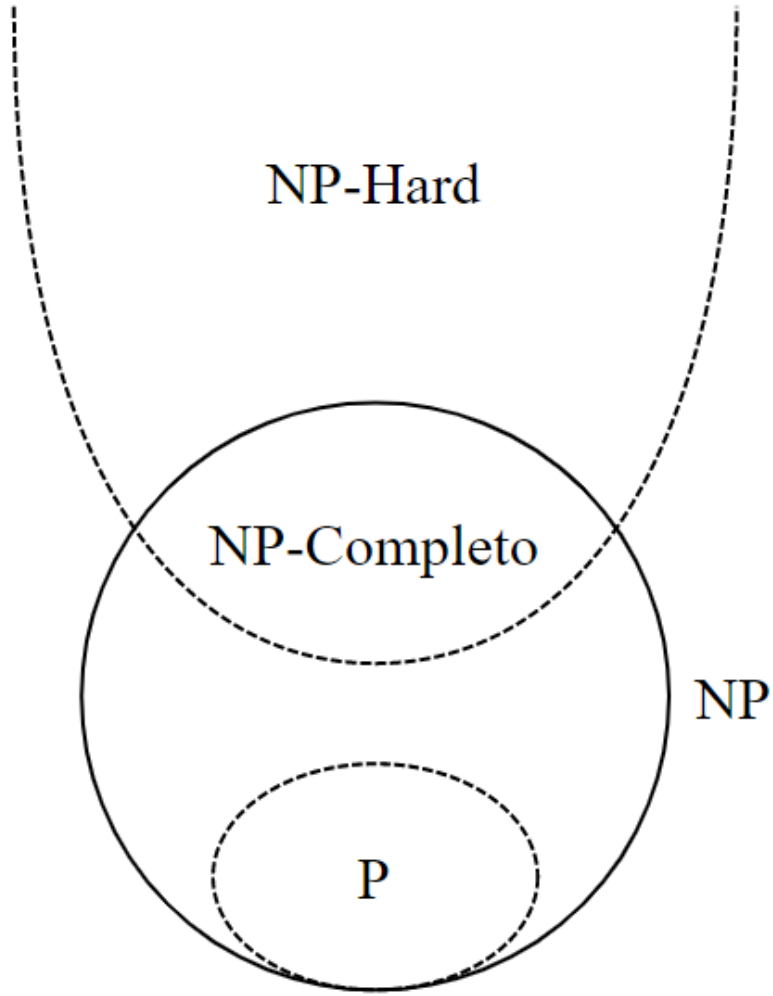
- **Manual**
  - Visual
  - Simplex
- **Solvers de LP**
  - SCIP
  - Cplex
  - Gurobi

Conceptos de Investigación de Operaciones

- Solución factible: Solución que cumple con todas las restricciones.
- Solución óptima: Mejor solución factible.

Complejidad Computacional

El problema de la mochila es NP-Completo.



Heurísticas

Una forma de resolver problemas que ocupa métodos prácticos que no garantizan un resultado óptimo o perfecto.

Índice 2

1. Investigación de Operaciones
   - Definición
   - Aplicaciones

2. Teoría de Juegos
   - Juegos de Stackelberg
   - Juegos de Seguridad de Stackelberg
   - Juegos de Seguridad de Stackelberg

Teoría de juegos

Teoría de juegos estudia a través de modelos matemáticos la competencia y cooperación entre agentes racionales

Teoría de juegos: Nash vs Stackelberg

- Nash: los jugadores actúan de manera simultánea.
- Stackelberg: los jugadores actúan de manera secuencial

Stackelberg Games

Un juego de Stackelberg (Stackelberg Game, o SG) modela una interacción sencuencial y competitiva entre dos agentes.

Stackelberg Security Games, Aplicaciones

Stackelberg Security Games

Definición: Two-player general-sum game

Un primer jugador (Lider o Defensor) lleva a cabo una estrategia mixta para localizar un conjunto de recursos que le permiten defender un conjunto de objetivos. El segundo jugador (seguidor o atacante) observa la estrategia y elige un objetivo para atacar.

Stackelberg Security Games

Ejemplo

Atacante/Seguidor:
Criminales

n=5
(targets/objetivos)

A

B

C

D

E

Líder/Defensor:
Institución de Carabineros

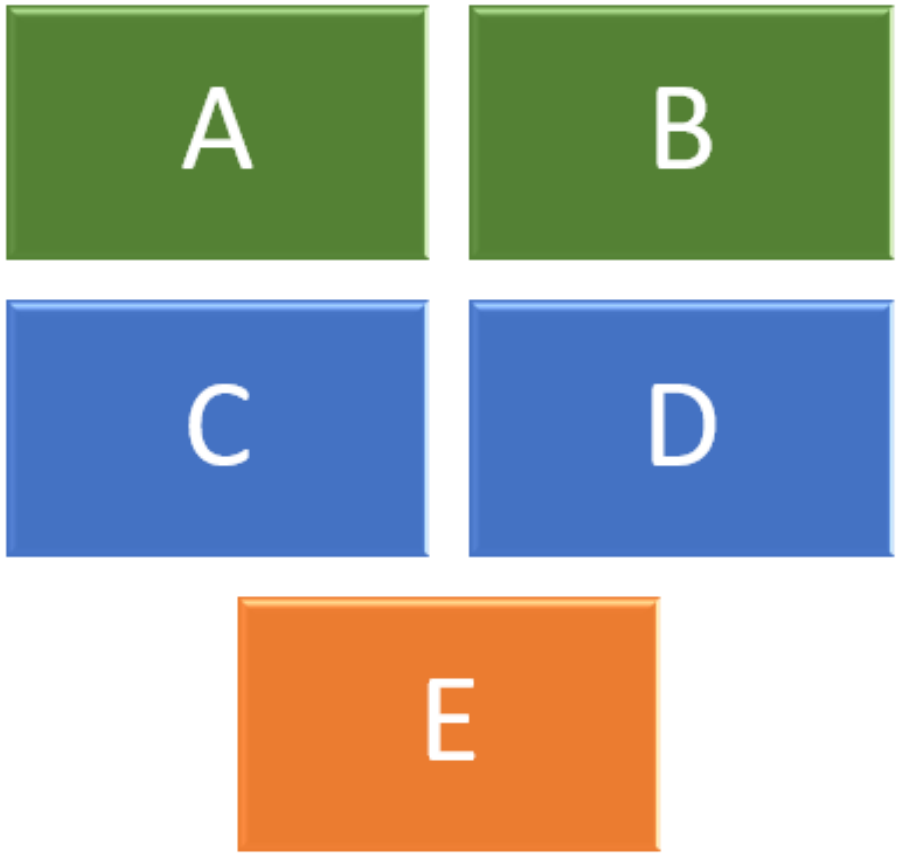
m=2
(recursos)

Stackelberg Security Games

Ejemplo

Atacante/Seguidor:
Criminales

n=5
(targets/objetivos)



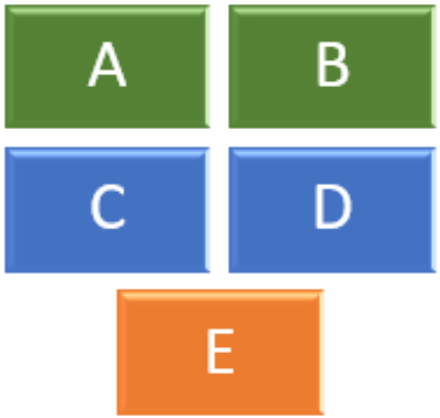
Líder/Defensor:
Institución de Carabineros

m=2
(recursos)

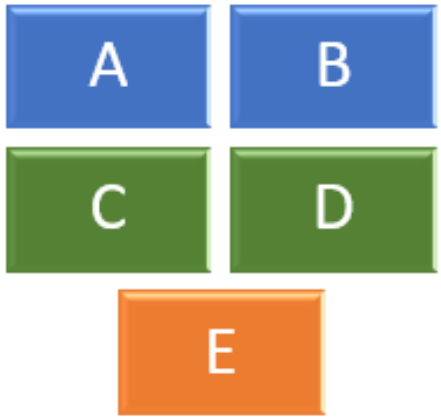
Stackelberg Security Games

Ejemplo

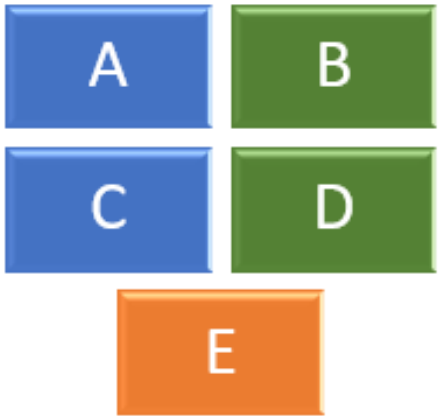
Estrategia pura 1



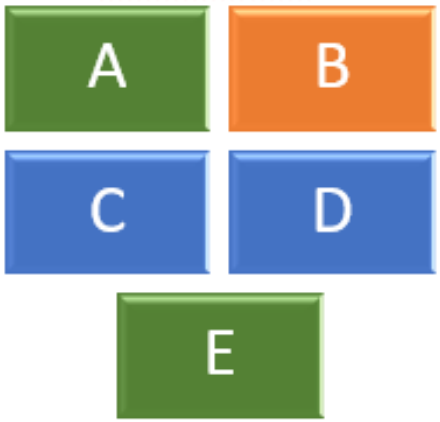
Estrategia pura 2



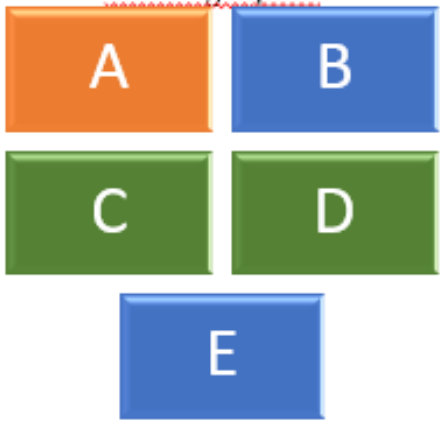
Estrategia pura 3



Estrategia pura 4



Estrategia pura 5



Stackelberg Security Games

Posible schedules de recurso 1 (verde)

- AB
- CD
- BD
- AE

Posible schedules de recurso 2 (azul)

- AB
- CD
- AC
- BE

Schedule de un recurso

Conjunto de objetivos que pueden ser protegidos por ese recurso, en una estrategia.

En este caso, recursos son heterogeneos

Aleatorización

La localización de los recursos no debe ser predecible, pues esto podría ser aprovechado por un atacante. Es por ello que el defensor usa estrategias mixtas.

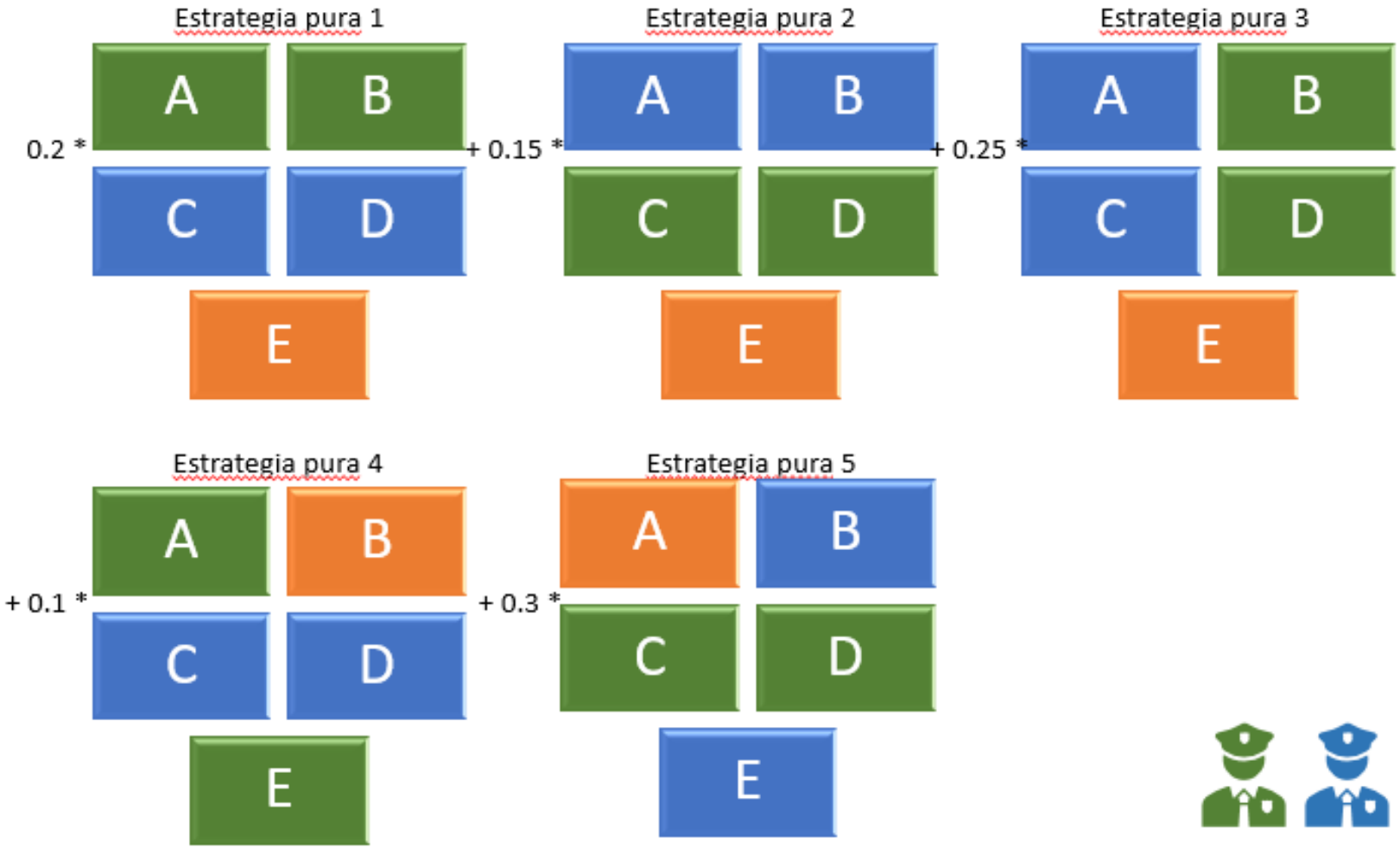
Estrategia pura

Sea $\epsilon \subseteq \{0,1\}^n$ el conjunto de estrategias puras. El tamaño de ϵ es grande, y generalmente exponencial con respecto al número de recursos de seguridad.

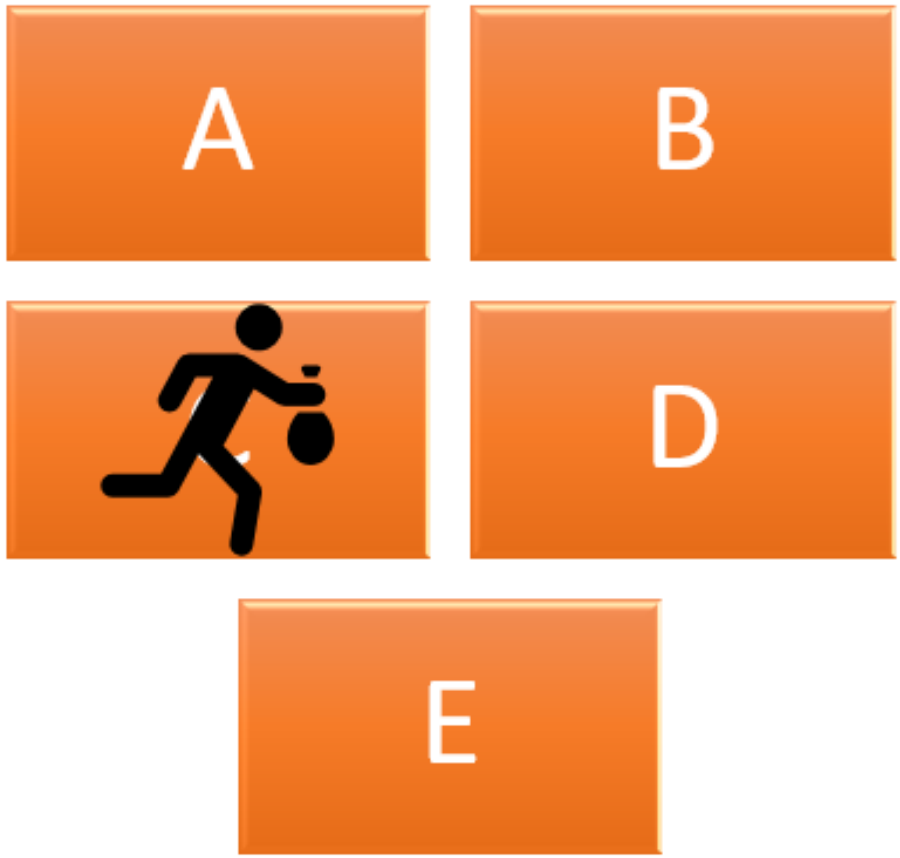
Estrategia mixta

Una estrategia mixta es una distribución p sobre los elementos en ϵ.

Ejemplo de estrategia mixta de defensor



Cont. Ejemplo de respuesta de atacante



Objetivo y concepto de solución

Nuestro objetivo es encontrar una estrategia mixta óptima (que maximice sus utilidades esperadas) para el líder, dado que el seguidor conoce esta estrategia mixta al escoger su estrategia (óptima).

Strong Stackelberg Equilibrium

El concepto de solución que se considera es el Strong Stackelberg Equilibrium, es decir, si el seguidor es indiferente entre varias estrategias óptimas, selecciona la mejor respuesta que favorezca al líder.

Obs: Recompensas

Matriz de recompensas depende solamente de si un objetivo esta protegido o no.

Formulación SG general

Conjuntos:
I= conjunto finito de estrategias puras del lider.
J= conjunto finito de estrategias puras del seguidor.

Parámetros:
R_{ij}= recompensa para el lider cuando toma la acción i y el seguidor la acción j.
C_{ij}= recompensa para el seguidor cuando el líder toma la acción i y el seguidor la acción j.

Variables:
$\boldsymbol{x} = (x_i)_{i \in I}$ tal que x_i es la probabilidad de que el lider elija la estrategia pura i.
$\boldsymbol{q} = (q_j)_{j \in J}$ tal que q_j es la probabilidad de que el seguidor elija la estrategia j.
U_L=utilidad esperada del líder. U_F=utilidad esperada del seguidor.

Formulación SG general

$$\max_{x,q,U_L,U_F} \quad U_L \tag{1}$$

$$U_L \leq \sum_{i \in I} R_{ij} x_i + M(1 - q_j), \ \forall j \in J \tag{2}$$

$$\boldsymbol{x}^T \mathbf{1} = 1, \ \boldsymbol{x} \geq 0 \tag{3}$$

$$0 \leq U_F - \sum_{i \in I} C_{ij} x_i \leq M(1 - q_j), \ \forall j \in J \tag{4}$$

$$\boldsymbol{q}^T \mathbf{1} = 1, \ \boldsymbol{q} \in \{0,1\}^{|J|} \tag{5}$$

$$U_L, U_F \in \mathbb{R} \tag{6}$$

Teoría de Juegos en contextos de seguridad

Pamela Alejandra Bustamante Faúndez[1]

[1]Pontificia Universidad Católica de Chile

14 Agosto 2020