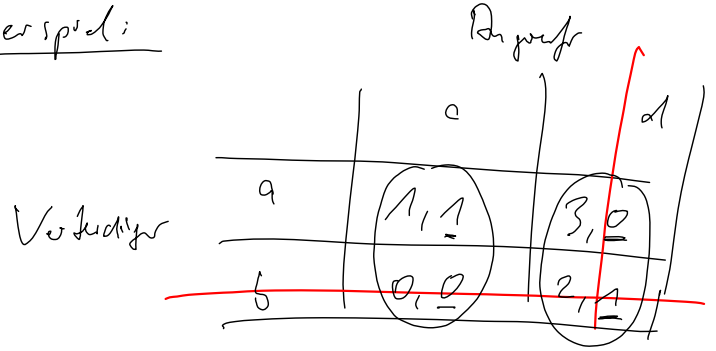
Fallstudie: Sicherheitsspiele

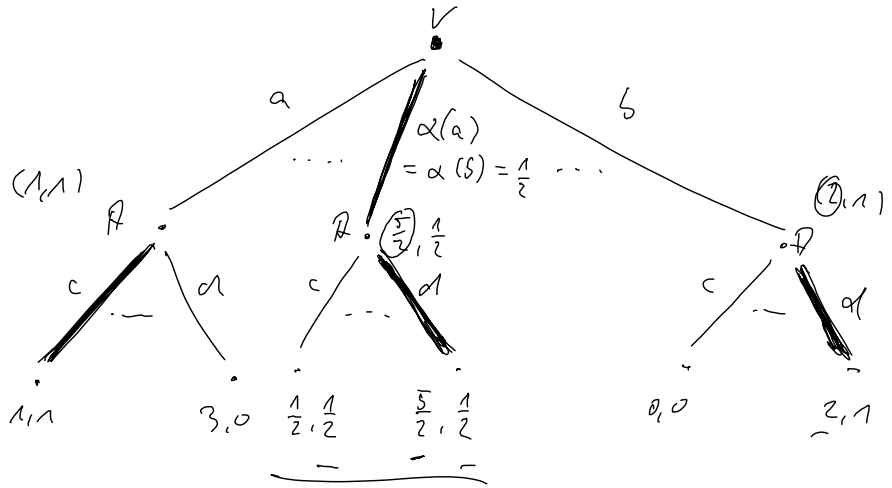
- Schützen Infrastrukturen durch patrouillierende Eskorten.
- wähle Wahrscheinlichkeitsverteilung über Routen, s.d. Schaden minimiert wird, gegeben Wahrscheinlichkeiten werden vom Angreifer beobachtet.

Unterscheide, ob Wahrsch. beobachtbar: strat. oder ext. Spiel.

Beispiel:



- Falls Wahrsch. nicht beobachtbar: strat. Spiel.
  ⇝ (a, c) ein reines NG
- Falls Wahrsch. beobachtbar ⇝ ext. Spiel



⇝ TPG (α, α)

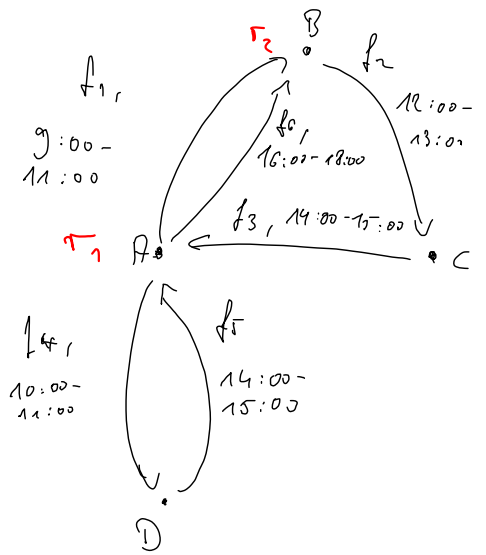
Wir zeigen: Unter beschränkten Ressourcen ist jedes starke Stackelberg-Gleichgewicht (Def. später, vgl. TPG) (SSG)
auch ein NG ⟶ Konzentration auf SSGs.

Def.: Ein Scheduling-Spiel ist ein Tupel $(T, R, (S_i), U_d^c, U_d^u, U_a^c, U_a^u)$, wobei:

- $T = \{t_1, \dots, t_n\}$ endl. Menge von Tasks,
- $R = \{r_1, \dots, r_k\}$ endl. Menge von Ressourcen,
- $S_i \subseteq 2^T$ Menge der Schedules, die r_i abdecken kann. Ein Schedule $s \in S_i$ ist eine Menge von Tasks, die von r_i „gleichzeitig" abgedeckt werden können.

- $U_y^x(t_i)$ ist der Nutzen von Spieler $y \in \{\underline{a}ttacker, \underline{d}efender\}$, wenn Task t_i angegriffen wird und $x \in \{\underline{c}overed, \underline{u}ncovered\}$ ist.

Bsp.: Air Marshals Flip:



$T = \{f_1, f_2, f_3, f_4, f_5, f_6\}$

$R = \{r_1, r_2\}$

$S_1 = \{\{f_1, f_2, f_3\}, \{f_4, f_5\}\}$

$S_2 = \{\{f_2, f_3, f_6\}\}$

$U_y^x(t_i)$ in Bsp. ungleich 0.

Notation: $\Delta U_a(t_i) = U_a^u(t_i) - U_a^c(t_i)$

$\Delta U_d(t_i) = U_d^c(t_i) - U_d^u(t_i)$

Annahme: $\Delta U_a(t_i), \Delta U_d(t_i) > 0$.

Reine und gemischte Strategien:

reine Strat. des Angreifers: $A_a = T$

gem. Strat. —"— : $\Delta(A_a)$.

reine Strat. des Verteidigers: Zuordnung von Ressourcen zu Schedules, d.h. $\bar{s} = (s_1, \dots, s_K) \in \prod_{j=1}^{K} S_j$.

Ziel t_i ist abgedeckt in $\bar{s}$ gdw.
$t_i \in s_j$ für mindestens ein j, $1 \le j \le K$.

$\bar{s}$ induziert Abdeckungsvektor $\bar{d} = (d_1, \dots, d_n) \in \{0,1\}^n$
mit $d_i = 1$ gdw. t_i abgedeckt in $\bar{s}$.

Menge aller Abdeckungsvektoren, für die ein
$\bar{s} \in \prod_{j=1}^{K} S_j$ existiert, von dem sie induziert werden,
heißt $\mathcal{D} \subseteq \{0,1\}^n$

gemischte Strat. des Verteidigers: $\Delta(\mathcal{D})$.

Für $\alpha_d \in \Delta(\mathcal{D})$ sei die Abdeckungswahrsch. von Ziel t_i gegeben durch

$$c_i = \sum_{\bar{d} = (d_1, \dots, d_n) \in \mathcal{D}} d_i \cdot \alpha_d(\bar{d})$$

Notation: $cp(\alpha_d) := (c_1, \dots, c_n)$

Bsp.: $\bar{d}_1 = (1,1,0)$, $\bar{d}_2 = (0,1,1)$,
$\alpha_d(\bar{d}_1) = \alpha_d(\bar{d}_2) = \frac{1}{2}$.
Dann $(c_1, c_2, c_3) = (\frac{1}{2}, 1, \frac{1}{2})$.

Auszahlung: Sei $(\alpha_d, \alpha_a) \in \Delta(\mathcal{D}) \times \Delta(T)$
ein gem. Strategieprofil.
Erwarteter Nutzen von Spieler $y \in \{a, d\}$:

$$U_y(\alpha_d, \alpha_a) = \sum_{i=1}^{n} \alpha_a(t_i) \cdot \Big(c_i \cdot U_y^c(t_i) + (1 - c_i) \cdot U_y^u(t_i) \Big).$$

Def.: NE ist ein Strategieprofil, d.i. (α_d, α_a) ist NG gdw.
$U_d(\alpha_d, \alpha_a) \ge U_d(\alpha_d', \alpha_a)$ $\forall \alpha_d'$ und
$U_a(\alpha_d, \alpha_a) \ge U_a(\alpha_d, \alpha_a')$ $\forall \alpha_a'$.

Interessant: Verteidiger legt sich zuerst auf eine gemischte Strategie fest, Angreifer beobachtet gem. Strategie (Gewichte) und wählt dann abhängig davon Antwort $\alpha_a = g(\alpha_d)$.
$g : \alpha_d \mapsto \alpha_a$ heißt Antwortfunktion.

Def.: Ein Paar (α_d, g) heißt starke Stackelberg-Gleichgewicht (SSG), wenn folgendes gilt:

1) $U_d(\alpha_d, g(\alpha_d)) \geq U_d(\alpha_d', g(\alpha_d'))$ f.a. α_d';

2) $U_a(\alpha_d, g(\alpha_d)) \geq U_a(\alpha_d, g'(\alpha_d))$ f.a. α_d und f.a. g'.

3) tie breaking:

$U_d(\alpha_d, g(\alpha_d)) \geq U_d(\alpha_d, f(\alpha_d))$ f.a. α_d und f.a. $f(\alpha_d)$, die beste Reaktion des Angreifers auf α_d sind.

Notation: Ω_{NE} sei die Menge aller gemischten Strategien des Verteidigers, die mindestens einem NG zugeordnet werden. Ω_{SSE} ..., ... mindest. einem SSG zugeordnet werden.

Satz: Für alle SSG (α_d, g) und alle NG (α_d', α_a) gilt $U_d(\alpha_d, g(\alpha_d)) \geq U_d(\alpha_d', \alpha_a)$. □

Gleichgewichte in Sicherheitsspielen

Bem.: In endlichen Zwei-Personen-Nullsummenspielen gilt NG = Minimax = Maximin = SSG.

Aber: Sicherheitsspiele i.A. keine Nullsummenspiele.

Fragen: 1) Zshg. SSG, NG, Minimax in Sicherheitsspielen?

2) Austauschbarkeit von NG-Strategien.

3) Eindeutigkeit von NG-/SSG-Strategien.

Äquivalenz von NGs und Minimax

Def.: Sei α_d eine gemischte Strategie des Verteidigers und sei $E(\alpha_d) = \max_{i=1,\dots,n} U_a(\alpha_d, t_i)$.

Ferner: $E^* := \min_{\alpha_d \in \Delta(\mathcal{O})} E(\alpha_d)$,

Die Menge aller Minimax-Strategien des Verteidigers ist dg. als $\Omega_M = \{\alpha_d \mid E(\alpha_d) = E^*\}$.

Def.: Sei α_a eine gemischte Strategie des Angreifers.

Def. die Funktion $f: \alpha_a \mapsto \overline{\alpha}_a$ durch

$$\overline{\alpha}_a(t_i) = \lambda \cdot \alpha_a(t_i) \cdot \frac{\Delta u_d(t_i)}{\Delta u_a(t_i)}, \text{ wobei } \lambda > 0$$

s.d. $\sum_{i=1}^{n} \overline{\alpha}_a(t_i) = 1$.

[f^{-1} analog: $\alpha_a(t_i) = \frac{1}{\lambda} \cdot \overline{\alpha}_a(t_i) \cdot \frac{\Delta u_a(t_i)}{\Delta u_d(t_i)}$]

Lemma 1: Sei $G = \langle T, R, (S_i), u_d^c, u_d^u, u_a^c, u_a^u \rangle$ ein Sicherheitsspiel und $\overline{G} = \langle T, R, (S_i), \overline{u}_d^c, \overline{u}_d^u, u_a^c, u_a^u \rangle$ mit

$\overline{u}_d^c = -u_a^c$ und $\overline{u}_d^u = -u_a^u$.

Dann ist $\langle \alpha_d, \alpha_a \rangle$ ein NG von G gdw. $\langle \alpha_d, f(\alpha_a) \rangle$ ein NG von $\overline{G}$ ist.

Beweis: Hausaufgabe.

Satz: In jedem Sicherheitsspiel gilt

$$\mathcal{U}_M = \mathcal{U}_{NE}$$