Fallstudie: Sicherheitsspiele

- Schütze Infrastruktur durch patrouillierende Einheiten.
- wähle W'keitsverteilung über Routen, s.d. Schaden minimiert wird, gegeben W'keiten werden vom Angreifer beobachtet.

Unterschied, ob W'keiten beobachtbar: strat. oder ext. Spiel.

Beispiel:

Angreifer

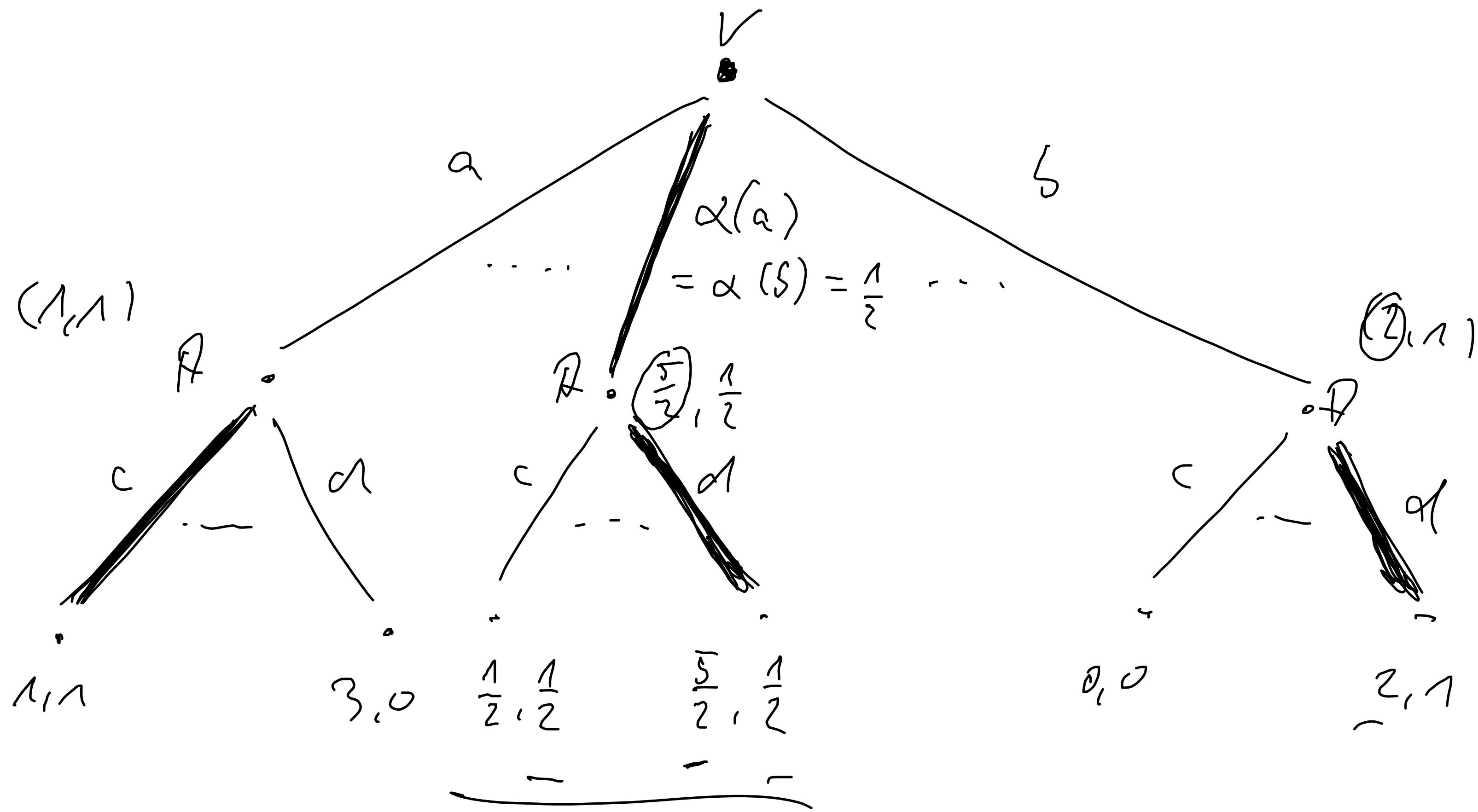
Verteidiger

	c	d
a	1, 1	3, 0
b	0, 0	2, 1

- Falls U'kcten nicht beobachtet: strat. Spiel.

  $\rightsquigarrow$ (a, c) einziges NG

- Falls U'kcten beobachtet $\rightsquigarrow$ ext. Spiel



$\rightsquigarrow$ TPG (α, d)

Wir zeigen: Unter bestimmten Annahmen ist jedes Starke Stackelberg-Gleichgewicht (Def. später, vgl. TPGs) (SSG) auch ein NG $\longrightarrow$ Konzentration auf SSGs.

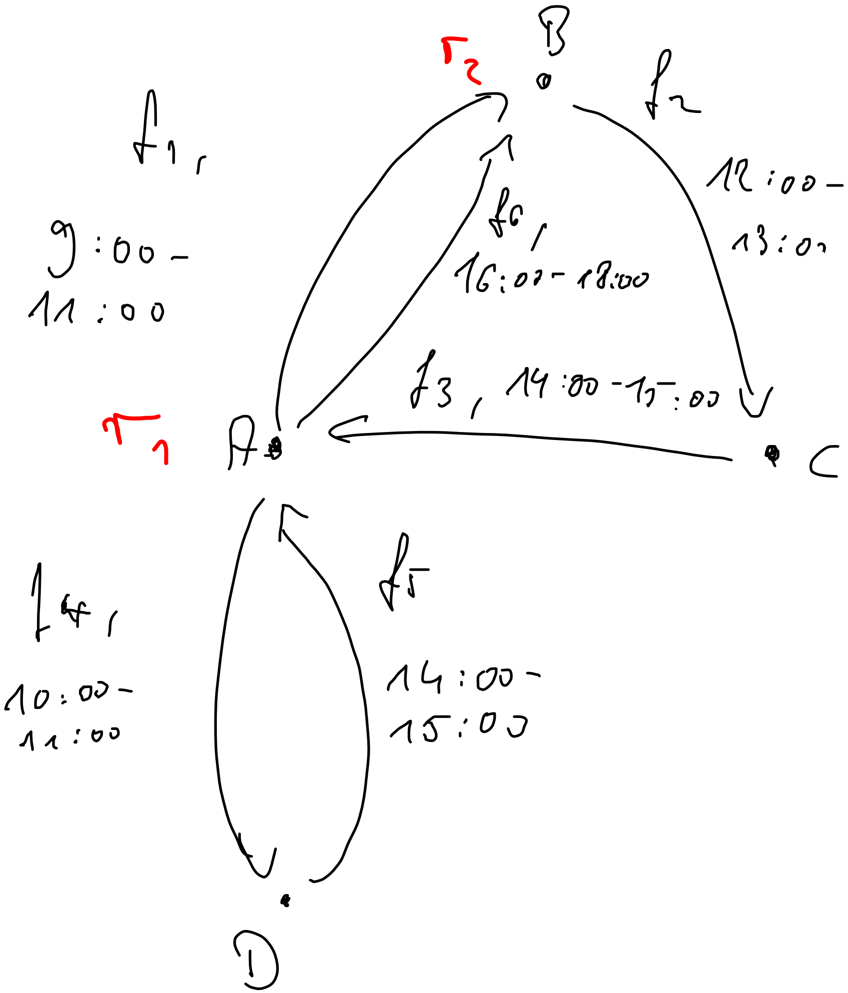
Def.: Ein Sicherheitsspiel ist ein Tupel

$\langle T, R, (S_i), U_d^c, U_d^u, U_a^c, U_a^u \rangle$, wobei:

- $T = \{t_1, \dots, t_n\}$ endl. Menge von Zielen,
- $R = \{r_1, \dots, r_k\}$ 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 Zielen, die von r_i „gleichzeitig" abgedeckt werden können.

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

Bsp.: Air Medals Flug:



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

$R = \{r_1, r_2\}$

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

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

$U_g^x(t_i)$ in Bsp. unspezifiziert.

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. ——〃——: $\Delta(A_a)$,

Kurze Schreibw. des Verfahrens: 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, $1 \leq j \leq K$.

$\bar{s}$ 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, heiße $\mathcal{D} \subseteq \{0,1\}^n$

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

Für $\alpha_d \in \Delta(\mathcal{D})$ sei die <u>Abdeckungs-wkeit</u> von Ziel t_i gegeben durch

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

<u>Notation:</u> $\varphi(\alpha_d) := (c_1, \dots, c_n)$

<u>Bsp.:</u> $\bar{d}_1 = (1,1,0)$, $\bar{d}_2 = (0,1,1)$,

$\alpha_d(\bar{d}_1) = \alpha_d(\bar{d}_2) = \frac{1}{2}$.

Dann $(c_1, c_2, c_3) = (\frac{1}{2}, 1, \frac{1}{2})$.

__Auszahlungen__: Sei $(\alpha_d, \alpha_a) \in \Delta(D) \times \Delta(T)$ 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.__: NG def. wie üblich, d.h. (α_d, α_a) ist NG gdw.

$$U_d(\alpha_d, \alpha_a) \geq U_d(\alpha_d', \alpha_a) \quad \forall \alpha_d' \quad \text{und}$$

$$U_a(\alpha_d, \alpha_a) \geq U_a(\alpha_d, \alpha_a') \quad \forall \alpha_a'.$$

__Interessanter__ Verteidiger legt sich zuerst auf eine gewählte Strategie fest, Angreifer beobachtet gew. Strategie (W'keiten) 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 <u>Starkes Stackelberg-Gleichgewicht</u> (SSG) gdw. folgendes gilt:

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

2) $U_a(\tilde{\alpha}_d, g(\tilde{\alpha}_d)) \geq U_a(\tilde{\alpha}_d, g'(\tilde{\alpha}_d))$ f.a. $\tilde{\alpha}_d$ und f.a. g'.

3) Tie-breaking:

$$U_d(\tilde{\alpha}_d, g(\tilde{\alpha}_d)) \geq U_d(\tilde{\alpha}_d, J(\tilde{\alpha}_d))$$ f.a. $\tilde{\alpha}_d$ und f.a. $J(\tilde{\alpha}_d)$, die beste Antworten des Angreifers auf $\tilde{\alpha}_d$ sind.

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

Satz: Für alle SSG $\langle \alpha_d, g \rangle$ und alle NG $\langle \alpha_d', \alpha_a \rangle$ gilt

$$U_d(\alpha_d, g(\alpha_d)) \geq U_d(\alpha_d', \alpha_a). \quad \square$$

Gleichgewichte in Sicherheitsspielen

Bem: In endlichen Zwei-Personen-Nullsummenspielen gilt $NG = \text{MinMax} = \text{MaxMin} = SSG$.

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:
$$E^* := \min_{\alpha_d \in \Delta(D)} E(\alpha_d).$$

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

Def.: Sei α_a eine gemischte Strategie des Angreifers.

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

$$\boxed{\overline{\alpha}_a(t_i) = \lambda \cdot \alpha_a(t_i) \cdot \frac{\Delta U_d(t_i)}{\Delta U_a(t_i)}}, \quad \text{wobei } \lambda > 0$$

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

[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 $\mathcal{G} = \langle T, R, (S_i), U_d^c, U_d^u, U_a^c, U_a^u \rangle$ ein Sicherheitsspiel und $\overline{\mathcal{G}} = \langle T, R, (S_i), \overline{U_d^c}, \overline{U_d^u}, U_a^c, U_a^u \rangle$ mit

$$\overline{U_d^c} = -U_a^c \quad \text{und} \quad \overline{U_d^u} = -U_a^u .$$

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

Beweis: Hausaufgabe.

Satz: Zu jedem Sicherheitsspiel gilt

$$\Omega_M = \Omega_{NE}$$