1 Pokus zavést hry formálně

Definition 1. *A* code-breaking game *is a triple* $\mathcal{G} = (C, E, (\rho_c)_{c \in C})$*, where* C *is a finite set of possible codes,* E *is a finite set of possible experiments and* $\rho_c : E \to 2^C$ *is the result function for code* $c \in C$ *such that* $c \in \rho_c(e)$ *for every* $e \in E$*.*

Definition 2. *A* history *is a sequence* π *of elements from* $\Delta = (E \times 2^C)$*. Let* $\pi[i]$ *and* $\pi[j..k]$ *denote the* i*-th element of* π *and the subsequence from the* j*-th to the* k*-th element, respectively. Furher, if* $\pi[i] = (e, D)$*, let* $\pi[i]^e = e$ *and* $\pi[i]^\rho = D$ *denote the projections.*
Let $\pi \in \Delta^n$ *be a history and let* $m = |\bigcap_{i=1}^{n} \pi[i]^\rho|$*. We call a history* finished *if* $m = 1$ *and* invalid *if* $m = 0$*.*

Definition 3. *Strategy is a function* $\sigma : \Delta^* \to E$ *giving the next experiment based on the history of the game. On a code* $c \in C$*, a strategy* σ *generates a history* $\pi(\sigma, c) \in \Delta^\omega$ *defined by*

$$\forall i > 1\ .\ \pi^{\sigma,c}[i+1] = \Big(\underline{\sigma(\pi^{\sigma,c}[1..i])}, \rho_c(\underline{\sigma(\pi^{\sigma,c}[1..i])})\Big).$$

Definition 4. *Number of steps* $\lambda^{\sigma,c}$ *of a strategy* σ *on a code* c *is the least number* k *such that* $\pi^{\sigma,c}[1..k]$ *is finished. Let*

$$\lambda^\sigma_{max} = \max\{\lambda^{\sigma,c} \mid c \in C\}$$

is the worst-case number of steps of strategy σ*. Given a probability distribution on codes, let* $\lambda^\sigma_{exp} = E(\lambda^{\sigma,c})$ *be the expected number of steps of strategy* σ*.*

Bibliography