# 1 Různé

## 1.1 Notation

Let $\mathrm{Form}_X$ be the set of all prepositional formulas over the set of variables $X$; $V_X$ be the set of all valuations of variables $X$. Formulas $\varphi_0, \varphi_1 \in \mathrm{Form}_X$ are (semantically) equivalent, written $\varphi_0 \equiv \varphi_1$, if $v(\varphi_0) = v(\varphi_1)$ for all $v \in V_X$. For a formula $\varphi \in \mathrm{Form}_X$, let $\tau_X(\varphi) = |\{v \in V_X \mid v(\varphi) = 1\}|$ be the number of valuations by which $\varphi$ is satisfied. We often omit the index $X$ if it is clear from the context.

For any unary predicate $P$, $\#i \in A.P(i) = |\{i \in A \mid P(i)\}|$. We often omit the "$\in A$" part and write only $\#i.P(i)$ if the range of $i$ is clear from the context.

Let $\mathrm{Perm}_X$ be the set of all permutations of $X$.

## 1.2 Fake-coin problem

There is a lot of variants of a logic puzzle with coins and a pair of scales balance. Here we present the most interesting ones and their generalization, which we study in the sequel.

In all the problems, you can use the scales only to weight coins. You can put as many coins at the sides as you like as long as the number is the same. All information you get is that both sides weight equally or which side is heavier (i.e., there are 3 possible results).

The weight of a *fake* coin is always different than the weight of a authentic one but it is not know whether it is heavier or ligther.

**Problem 1 (The twelve coin problem).** *You are given 12 coins, exactly one of which is fake. Determine the unique coin and its weight relavite to others. You can use the balance at most 3 times.*

**Problem 2 (The thirteen coin problem).** *You are given 13 coins, exactly one of which is fake. You have one more coin at your disposal which is guaranteed to be authentic. Determine the unique fake coin and its weight relavite to others.*

**Problem 3 (General fake coin problem).** *You are given n coins, f of them are fake (some of them may be lighter, some of them heavier). You have another m authentic coins at your disposal. In as less weightings as possible, determine which coins are fake.*

## 1.3 Mastermind

*Mastermind* is a classic 2-player board game invented by Mordecai Meirowitz in 1970[wiki]. The principle of the game is the same as of *Bulls and Cows*, it just uses colors instead of letters.

# 2 Code-breaking Games

Motivace: Ve hře chci najít přiřazení proměnných. Hru tedy reprezentuju jako mnozinu promennych, a jakousi mnozinu experimentu. Po provedeni experimentu dostanu formuli v danych promennych, o ktere vim, ze je splnena v hledane valuaci. Tato formule reprezentuje castecnou informaci, kterou jsem experimentem ziskal. Kazdy experiment muze dopadnout vice zpusoby, pro kazdy mam tedy mnozinu moznych formuli, ktere mi da.
Pro kompaktni zapis reprezentuju experiment jako dvojici (typ experimentu, parametrizace), kde parametrizace je retezec nad danou abecedou. Pro kazdy typ experimentu pak mam mnozinu parametrizovanych formuli. This whole idea is formalized below.

---

**Definition 4.** A *code-breaking game* is a septuple $\mathcal{G} = (X, \varphi_0, T, \Sigma, E, F, \Phi)$, where

- $X$ is a finite set of propositional variables,
- $\varphi_0 \in \text{Form}_X$ is a satisfiable prepositional formula,
- $T$ is a finite set of types of experiments,
- $\Sigma$ is a finite alphabet,
- $E \subseteq T \times \Sigma^\star$ is an *experiment* relation, and
- $F$ is a finite collection of functions of type $\Sigma \to X$,
- $\Phi : T \to 2^{\text{PForm}_{X,F,\Sigma}}$ is an *outcome function* such that $\Phi(t)$ is finite for any $t \in T$. Definition of PForm follows (Definition 5).

---

**Definition 5.** A set of *parametrized formulas* $\text{PForm}_{X,F,\Sigma}$ is a set of all strings $\psi$ generated by the following grammar:

$$\psi ::= x \mid f(\$n) \mid \psi \circ \psi \mid \neg\psi,$$

where $x \in X$, $f \in F$, $n \in \mathbb{N}$, and $\circ \in \{\wedge, \vee, =>\}$. By $\psi(p)$ we denote application of a parametrization $p \in \Sigma^\star$ on a formula $\psi$, which is defined recursively on the stucture of $\psi$ in the following way:

$$(x)(p) = x,$$
$$(f(\$n))(p) = p[n],$$
$$(\psi_1 \circ \psi_2)(p) = \psi_1(p) \circ \psi_2(p),$$
$$(\neg\psi)(p) = \neg(\psi(p)).$$

For the sake of simplicity, let us write $\Phi(e) = \{\psi(p) \mid \psi \in \Phi(t)\}$ for any experiment $e = (t, p) \in E$.

A code-breaking game is *well-formed* if for all $(t, p) \in E$,

$$\forall v \in V_X : v(\varphi_0) = 1 \Rightarrow \exists \text{ exactly one } \psi \in \Phi(t) . v(\psi(p)) = 1$$

This guarantees that the result of every experiment is uniquely defined for any valuation. Note that this property is not easy to check. In sequel, we suppose a game to be well-fordmed, if not stated otherwise.

**Example 6 (Fake-coin problem).** Fake-coin problem with $n$ coins, one of which is fake, can be formalized as a code breaking game $\mathcal{F}_n = (X, \varphi_0, T, \Sigma, E, F, \Phi)$.

- $X = \{x_1, x_2, \ldots, x_n, y\}$,
  $\varphi_0 = \text{Exactly-1}(\{x_1, \ldots, x_n\})$.
  Intuitively, variable $x_i$ tells weather the coin $i$ is fake. Variable $y$ tells weather it is lighter or heavier. Formule $\varphi_0$ says that exactly one coin is fake.

- $T = \{w_2, w_4, \ldots, w_n\}$,
  $\Sigma = \{1, 2, \ldots, n\}$,
  $E = \bigcup_{1 \leq m \leq n/2}\{(w_{2m}, p) \mid p \in \{1, \ldots, n\}^{2m}, \forall x \in X.\#_x(p) \leq 1\}$.
  There are $n/2$ types of experiment – according to the number of coins we put on the weights. The alphabet contains natural numbers up to $n$ and possible parametrizations for $w_{2m}$ are strings of length $2m$ with no repetitions.

- $F = \{f_x\}$, where $f_x(i) = x_i$ for $1 \leq i \leq n$,
  $\Phi(w_m) =$
  $$\big\{ ((f_x(\$1) \vee \ldots \vee f_x(\$m)) \wedge \neg y) \vee ((f_x(\$m+1) \vee \ldots \vee f_x(\$2m)) \wedge y),$$
  $$((f_x(\$1) \vee \ldots \vee f_x(\$m)) \wedge y) \vee ((f_x(\$m+1) \vee \ldots \vee f_x(\$2m)) \wedge \neg y),$$
  $$\neg(f_x(\$1) \vee \ldots \vee f_x(\$2m)) \big\}.$$

  There are 3 possible outcomes of every experiment. First, the right side is heavier. This happens if the fake coin is lighter and it appears in the first half of the parametrization, or if it is heavier and it appears in the second half. Second, analogously, the left side is heavier. Third, the weights are balanced if the fake coin do not participate in the experiment.

**Example 7 (Fake-coin problem, alternative).** For demonstration purposes, here is another formalization of the same problem. $\mathcal{F}'_n = (X, \varphi_0, T, \Sigma, E, F, \Phi)$.

- $X = \{x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n\}$,
  $\varphi_0 = \text{Exactly-1}(\{x_1, \ldots, x_n, y_1, \ldots, y_n\})$.

4

Variable $x_i$ tells that the coin $i$ is lighter, variable $y_i$ tells that the coin $i$ is heavier. Formule $\varphi_0$ says that exactly one coin is different.

- $T, \Sigma, E$ is defined as in Example 6.
- $F = \{f_x, f_y\}$, where $f_x(i) = x_i$ and $f_y(i) = y_i$ for $1 \leq i \leq n$,
$$\Phi(w_m) = \big\{ (f_x(\$1) \vee \ldots \vee f_x(\$m)) \vee (f_y(\$m+1) \vee \ldots \vee f_y(\$2m)),$$
$$(f_y(\$1) \vee \ldots \vee f_y(\$m)) \vee (f_x(\$m+1) \vee \ldots \vee f_x(\$2m)),$$
$$\neg(f_x(\$1) \vee \ldots \vee f_x(\$2m) \vee f_y(\$1) \vee \ldots \vee f_y(\$2m)) \big\}.$$

**Example 8 (Mastermind).** <span style="color:red">UPDATOVAT!</span> Mastermind puzzle with $n$ pegs and color set $C$ can be formalized as a code breaking game $\mathcal{M}_{n,C} = (X, \varphi_0, T, E, \Phi)$, where

- $X = \{x_{i,c} \mid 1 \leq i \leq n, c \in C\}$.
  Variable $x_{i,c}$ tells whether there is the color $c$ at position $i$. For simplicity, let us use the notation $X_c = \{x_{i,c} \mid 1 \leq i \leq n\}$.
- $\varphi_0 = \bigwedge \{\text{Exactly-1} \{x_{i,c} \mid c \in C\} \mid 1 \leq i \leq n\}$.
  This guarantees that there is exactly one color at each position.
- $T = \{t\}$.
  There is only one type of experiment – guessing a combination.
- $E = \{(t, p) \mid p = x_{1,c_1} x_{2,c_2} \ldots x_{n,c_n}\}$.
  Parametrization of $t$ can be any string of length $n$, $i$-th symbol of which belongs to $\{x_{i,c} \mid c \in C\}$.
- Inference function is defined by

$$\Phi(v, (t, p)) = \text{Exactly-b} \{p[i] \mid 1 \leq i \leq n\} \wedge$$
$$\text{Exactly-t} \bigcup \big\{$$
$$\{\text{AtLeast-k} \{x_{i,c} \mid 1 \leq i \leq n\} \mid 1 \leq k \leq \#i.(p[i] \in X_c)\}$$
$$\mid c \in C \big\}$$

where $b = \#i.(v(p[i]) = 1)$ captures the number of black pegs in the response for the experiment $(t, p)$ and $t = \sum_{c \in C} \min(\#i.(v(x_{i,c}) = 1), \#i.(p[i] \in X_c))$ is the total number of pegs (black + white).
<span style="color:red">Fakt to nejde nějak jednodušej?</span>

## 2.1 Strategies

**Definition 9.** A *strategy* is a function $\sigma : \text{Form}_X \to E$, determining the next experiment for given accumulated knowledge, such that

$$\varphi_0 \equiv \varphi_1 \Rightarrow \sigma(\varphi_0) = \sigma(\varphi_1).$$

A strategy $\sigma$ together with a valuation $v$ (satisfying $\varphi_0$) induce a *solving process*, which is an infinite sequence

$$\pi_{\sigma,v} = \varphi_0 \xrightarrow{e_1} \varphi_1 \xrightarrow{e_2} \varphi_2 \xrightarrow{e_3} \dots,$$

where $e_i = \sigma(\varphi_0 \wedge \varphi_1 \wedge \dots \wedge \varphi_{i-1})$ and $\varphi_i \in \Phi(e_i)$ and $v(\varphi_i) = 1$, for all $i \in \mathbb{N}$. Notice that due to the condition 2, there is always exactly one such $\psi_i$.

For the sake of simplicity, let us write $\varphi_{0..k}$ instead of $\varphi_0 \wedge \varphi_1 \wedge \dots \wedge \varphi_k$.

We define *length* of the solving process, denoted $|\pi_{\sigma,v}|$ (despite the infinite length of the sequence), as the smallest $k \in \mathbb{N}_0$ such that $\tau_X(\varphi_{0..k}) = 1$. This corresponds to the point where we can uniquely determine the valuation used in the process (i.e. we can determine the secret code). Note that it always holds $\tau(\varphi_{0..k}) > 0$ because $v(\varphi_i) = 1$ for all $i \in \mathbb{N}_0$.

The following lemma is a straightforward consequence of the memory-less nature of the games. It says that once a strategy gives us an experiment that yields no new information, we will never get any new information (using the strategy).

**Lemma 10.** *If $\tau(\varphi_{0..k}) = \tau(\varphi_{0..k+1})$ for some $k \in \mathbb{N}$, then $\tau(\varphi_{0..k}) = \tau(\varphi_{0..k+l})$ for any $l \in \mathbb{N}$.*

*Proof.* If $\varphi_{0..k+1} = \varphi_{0..k} \wedge \varphi_{k+1}$ is satisfied by valuation $v$, so must be $\varphi_{0..k}$. Since $\tau(\varphi_{0..k}) = \tau(\varphi_{0..k+1})$, the sets of valuations satisfying $\varphi_{0..k}$ and $\varphi_{0..k+1}$ must be exactly the same and the formulas are thus equivalent. This implies $\sigma(\varphi_{0..k}) = \sigma(\varphi_{0..k+1})$ and thus also $\varphi_{k+2} = \varphi_{k+1}$. By induction, $\varphi_{k+l} = \varphi_{k+1}$ and $\varphi_{0..k+l} \equiv \varphi_{0..k}$ for any $l \in \mathbb{N}$. ∎

The *worst-case number of experiments* $\lambda^\sigma$ of a strategy $\sigma$ is the maximal length of the solving process $\pi_{\sigma,v}$ over all valuations $v$ by which $\varphi_0$ is satisfied, i.e. $\lambda^\sigma = \max_{v \in V_X, v(\varphi_0)=1} |\pi_{\sigma,v}|$. We say that a strategy $\sigma$ *solves the game* if $\lambda^\sigma$ is finite. The game is *solvable* if there exists a strategy that solves the game.

Není to jednoduchý, ale je to zajímavý? Given a code-breaking game $\mathcal{G}$, decide whether $\mathcal{G}$ is solvable.

**Definition 11.** A strategy $\sigma$ is *optimal* if $\lambda^\sigma \leq \lambda^{\sigma'}$ for any strategy $\sigma'$.

**Definition 12.** Let $f : \text{Form}_X \to \mathbb{Z}$. A strategy $\sigma$ is *$f$-greedy* if for every $\varphi \in \text{Form}_X$ and $e' \in E$,

$$\max_{\psi \in \Phi(\sigma(\varphi)), SAT(\varphi \wedge \psi)} f(\varphi \wedge \psi) \leq \max_{\psi \in \Phi(e), SAT(\varphi \wedge \psi)} f(\varphi \wedge \psi).$$

In words, a greedy strategy minimizes the value of $f$ on the formula in the next step.

We say $\sigma$ is *greedy* if it is $\tau_X$-greedy.

**Problem 13.** *Given a code-breaking game $\mathcal{G}$, decide whether all greedy strategies are optimal. Hypothesis: It is the case for Fake-coin problem (?). It is not the case for Mastermind[ref].*

**Definition 14.** An experiment $e_1$ is in relation $\sim_\varphi$ with an experiment $e_2$ if and only if there exists a permutation $\pi \in \text{Perm}_X$ such that $\{\varphi \wedge \psi \mid \psi \in \Phi(e_1)\} \equiv \{(\varphi \wedge \psi)^\pi \mid \psi \in \Phi(e_2)\}$.

Meaning?

# Bibliography