

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ  
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

---

# STROJOVÉ UČENÍ: ZÁKLADNÍ PŘEHLED A TERMINOLOGIE

**Autor textu:**  
**Ing. Petr Honzík, Ph.D.**

Květen 2014

Komplexní inovace studijních programů a zvyšování kvality výuky na FEKT VUT v Brně  
OP VK CZ.1.07/2.2.00/28.0193



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

# Témata probíraná v MSTU

- 1.: Úvod do STU. Základní dělení, paradigmatata.
- 2.: Základy statistiky. Charakteristiky, rozložení, testy.
- 3.: Modely: rozhodovací stromy.
- 4.: Modely: učení založené na instancích.
- 5.: Odhad přesnosti modelu: Křížová validace, bootstrap.
- 6.: Chybové funkce.
- 7.: Předzpracování dat.
- 8.: Modely: bayesovské klasifikátory.
- 9.: Modely: diskriminační analýza, lineární modely, SVM
- 10.: Optimalizace: GA, DE, AC
- 11.: Meta algoritmy: bagging, boosting, stacking.
- 12.: Učení bez učitele. Shluková analýza.
- 13.: Dolování dat, dobývání znalostí z databází

# Obsah přednášky

- jak zdárně absolvovat kurz MSTU
- motivační příklad
- definice SU, učení s učitelem a bez učitele
- rozdíl mezi SU (strojové učení) a UI (umělá inteligence), DM (dolování dat) a KDD (dobývání znalostí z databází)
- komponenty procesu učení s učitelem
- data podle typu
- vybraná terminologie
- teorémy SU (occamovo ostří, přeučení modelu)
- indukce vs. dedukce
- chyba bias vs. variance
- předpojatost modelu a schopnost generalizace

# Jak úspěšně absolvovat MSTU

- **studijní materiály** (informační systém), materiály v pdf + slidy (?, VIS)
- **! cvičení nahrazují konzultace !**
- **konzultace** domluvám předem emailem s konkrétním dotazem, přicházím nasáklý znalostmi
- **projekt** za max 20 bodů
  - datum zadání: do 3.11.2014
  - datum odevzdání: 8.12.2014
- **zápočet** = za odevzdání **projektu v termínu**
- písemná **zkouška** – 80 bodů (cca 40 bodů teorie, cca 40 bodů příklady)

# Projekt do MSTU

- **zadání:** přidělené nebo vlastní zadání (pak musí být schváleno), možnost propojení s diplomovou prací
- **komunikace:** hlavička emailu začíná „MSTU...“
- **do pondělí 3.11.2014** potvrzení zadání (zažádat emailem, potvrdím emailem – až poté je zadání oficiální)
- **do pondělí 8.12.2014** odevzdání projektu (osobně předat tištěnou dokumentaci, emailem pdf a případné přílohy)
- **práce v týmech:** možnost pracovat až ve třech
- **projekt (20b)** = dokumentace a program nebo schéma v RapidMineru ([rapid-i.com](http://rapid-i.com))
- **zápočet** se uděluje za **v termínu** odevzdaný projekt, bez zápočtu není možná účast na zkoušce
- zápočet **není podmíněn** minimálním **počtem bodů** za projekt

# Program RapidMiner

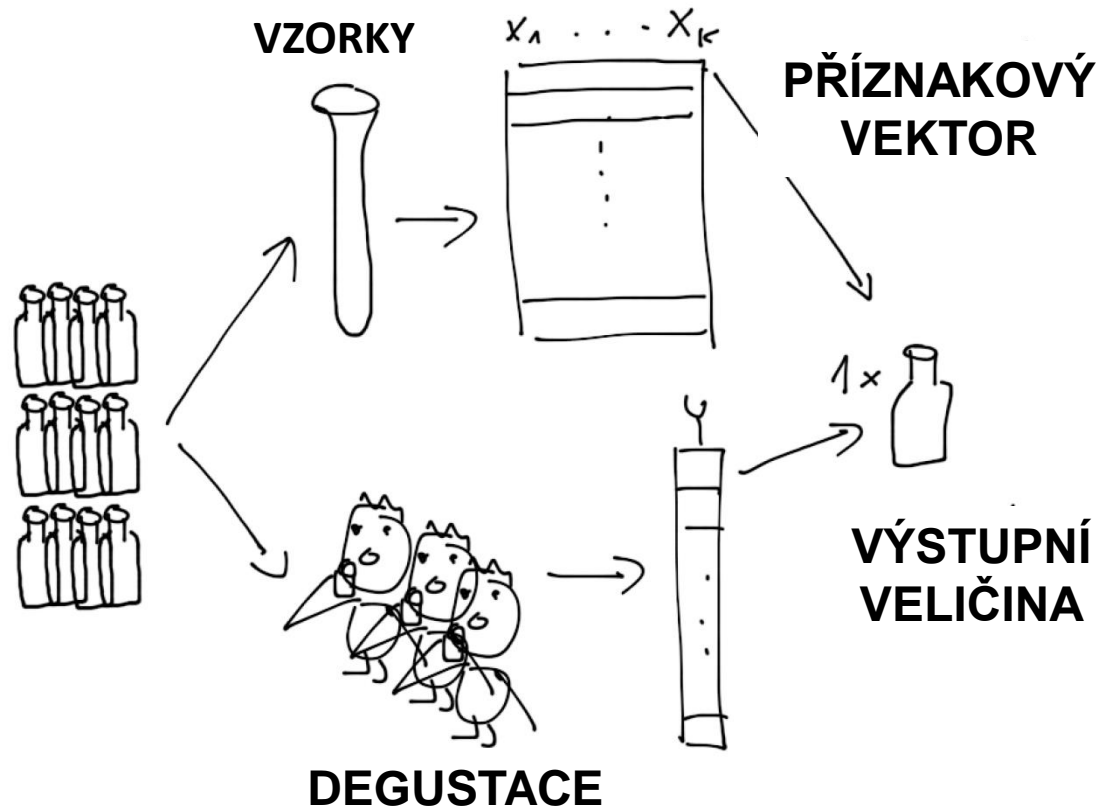
- K řešení projektu doporučuji použít program RapidMiner (rapidminer.com)
- Do verze 5.x community edition bez problémů
- Od verze 6.0 (2014) omezení u free verze ve velikosti RAM (1 GB) – což bylo i dříve, navíc ale podpora jen některých datových formátů (CSV a XLS) a zablokování přístupu k databázím (jen pro komerční verze)
- K řešení projektu doporučuji použít verzi **RapidMiner 5.3** (pokud nepoužijete Matlab nebo vlastní kód a knihovny jako OpenCV, AForge.NET nebo další...)

# Obsah přednášky

- jak zdárně absolvovat kurz MSTU
- **motivační příklad**
- definice SU, učení s učitelem a bez učitele
- rozdíl mezi SU (strojové učení) a UI (umělá inteligence), DM (dolování dat) a KDD (dobývání znalostí z databází)
- komponenty procesu učení s učitelem
- data podle typu
- vybraná terminologie
- teorémy SU (occamovo ostří, přeučení modelu)
- indukce vs. dedukce
- chyba bias vs. variance
- předpojatost modelu a schopnost generalizace

# Příklad: KVALITA VÍNA

Vyrábíte vlastní víno a rádi byste věděli, jak by si stálo při degustaci. Jak na to? (*ideový příklad*)





# O čem je tedy strojové učení?

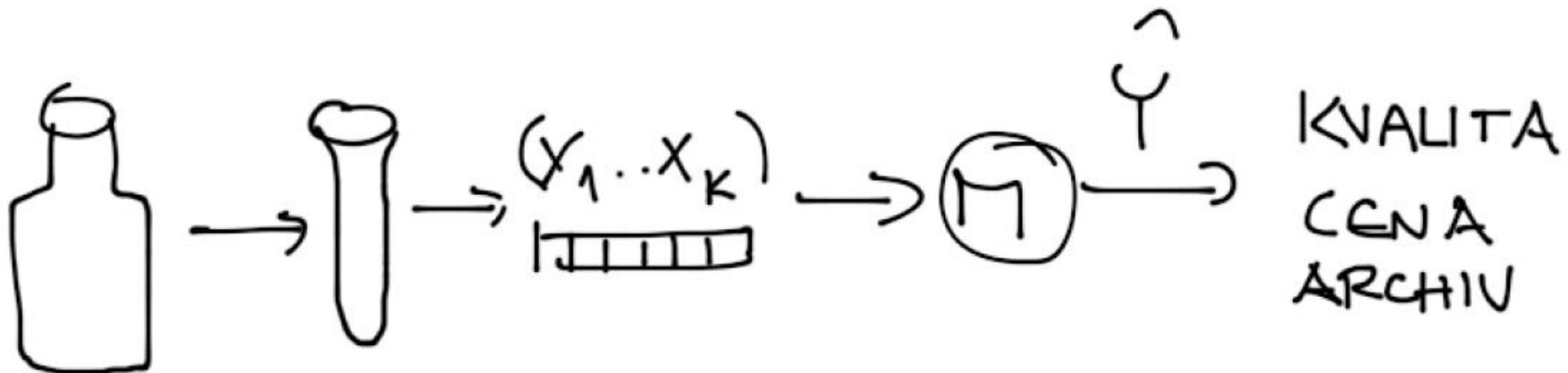
- **Nejtypičtější úlohy** jsou z oblasti **učení s učitelem** (supervised learning).
- Jsou dány:
  - **vstupní veličiny** (příznaky)  $\mathbf{X}$
  - **výstupní veličina**  $\mathbf{y}$  (nebo  $\mathbf{g}$ ).

Cílem je **vytvořit model**  $M$ , který co nejlépe postihne závislost výstupní veličiny  $\mathbf{y}$  ( $\mathbf{g}$ ) na vstupech (příznacích)  $\mathbf{X}$ , tedy  $\hat{\mathbf{y}} = M(\mathbf{X})$
- $\hat{\mathbf{y}}$  ( $\hat{\mathbf{g}}$ ) značí **výstup modelu**
- Snahou je model  $M$  nastavit tak, aby pro nová data ideálně  $\hat{\mathbf{y}} = \mathbf{y}$  ( $\hat{\mathbf{g}} = \mathbf{g}$ )

# Takže cílem SU je vytvořit model?

Velmi často. Celé je to poněkud složitější, ale u většiny **úloh s učitelem** je výsledkem **model** a **odhad jeho přesnosti**.

A na co je to dobré u vína? Pokud model máte, můžete odhadnout, jak je vaše víno kvalitní, nasadit tu „správnou“ cenu na trhu, zamyslet se nad úpravou procesu výroby nebo zcela v rozporu se zákonem nad úpravou vína již hotového... A to vše lze automatizovat (nakonec jsme ústav automatizace...).



# Definice (strojového) učení

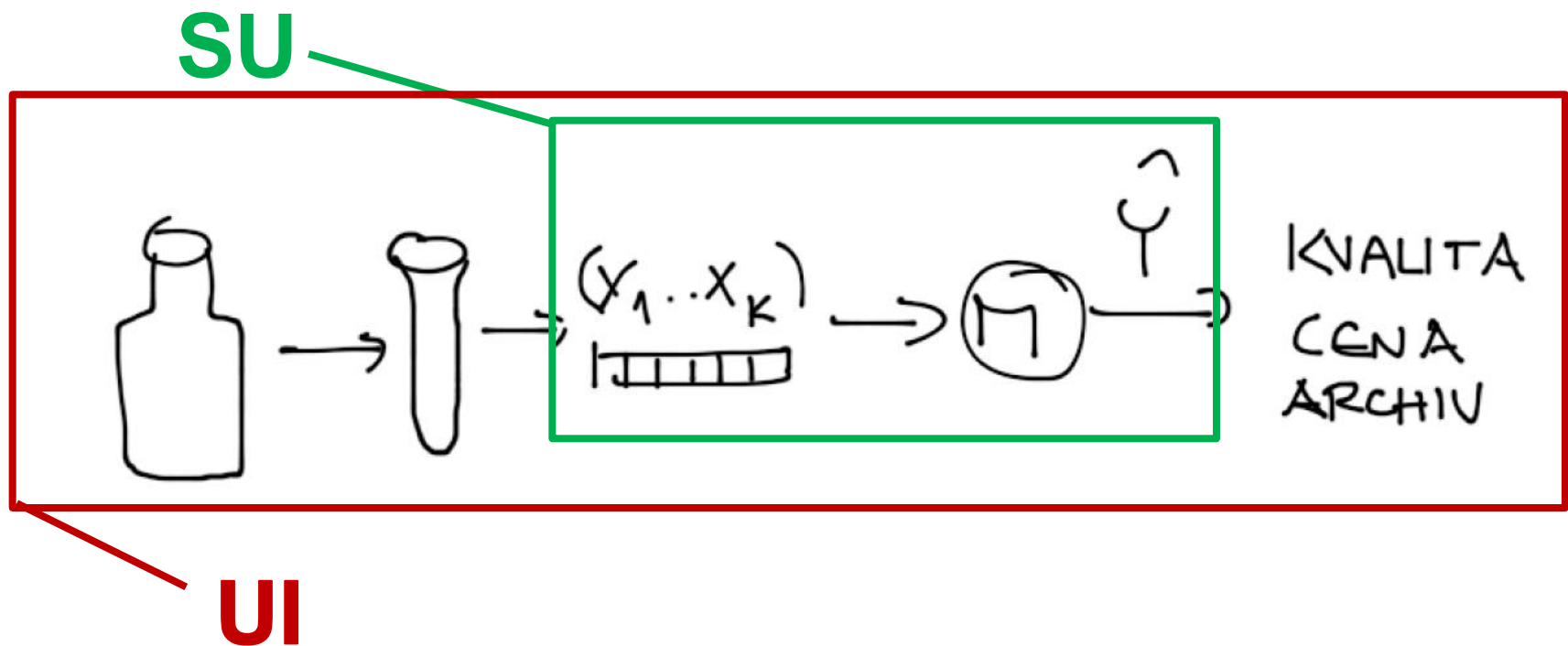
- **učení** je schopnost **zlepšování výkonnosti** (=přesnost modelu) tím, jak vzrůstá **znalost** (=nastavení parametrů modelu) na základě **zkušenosti** (=data)
- **strojové učení** je nauka o nástrojích (algoritmech, programech), které umožňují učení umělých objektů (artefaktů)
- **program** se učí pomocí **zkušenosti E** vzhledem k nějaké třídě úloh **T** a míře **výkonnosti P**, pokud se jeho výkonnost pro dané úlohy v **T** měřená pomocí **P** zlepšuje použitím **E**
- memorování není učení – nezahrnuje proces indukce.

# Dva základní typy problémů

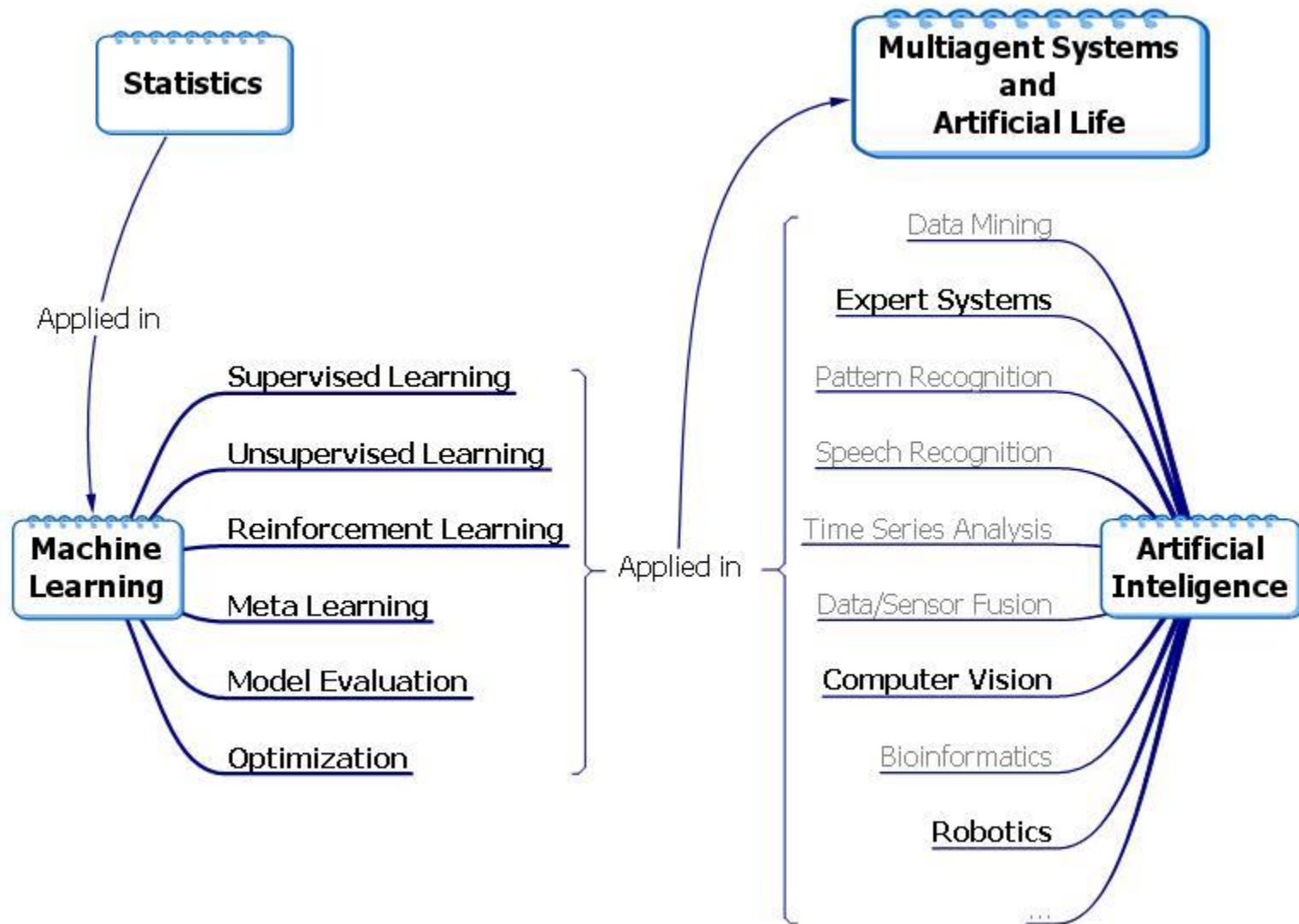
- **učení s učitelem**
  - je známa výstupní veličina  $y$  ( $g$ )
  - predikce (regrese, klasifikace)
- **učení bez učitele**
  - není známa výstupní veličina, pouze vstupní  $X$
  - hledání shluků (hypotetických tříd) či souvislostí v datech

# Rozdíl mezi umělou inteligencí a strojovým učením

Strojové učení nabízí matematický aparát a algoritmy, které jsou používány na řešení v úloh umělé inteligence.



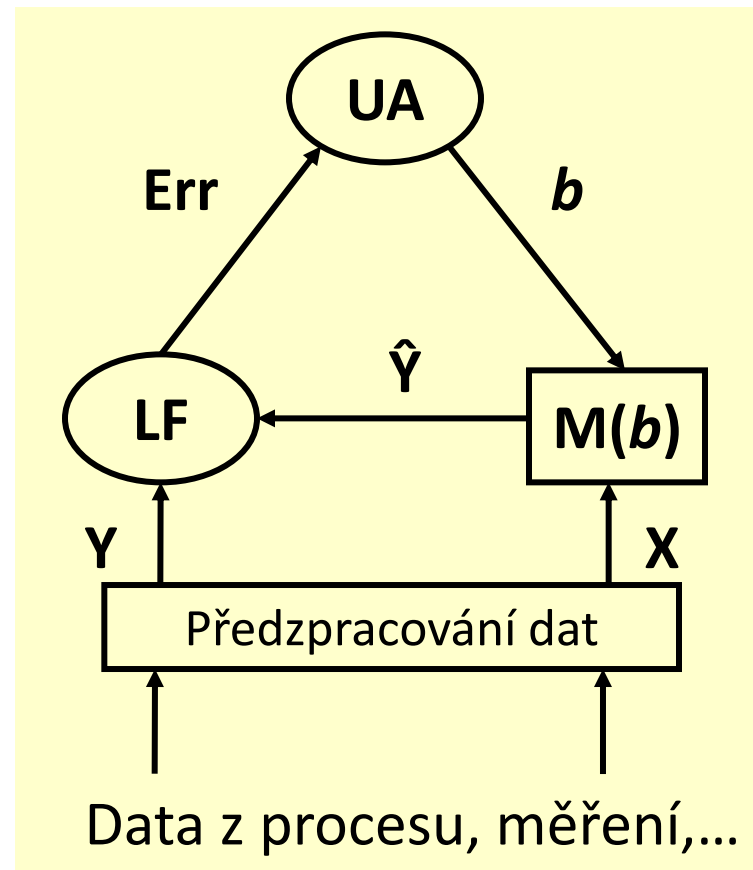
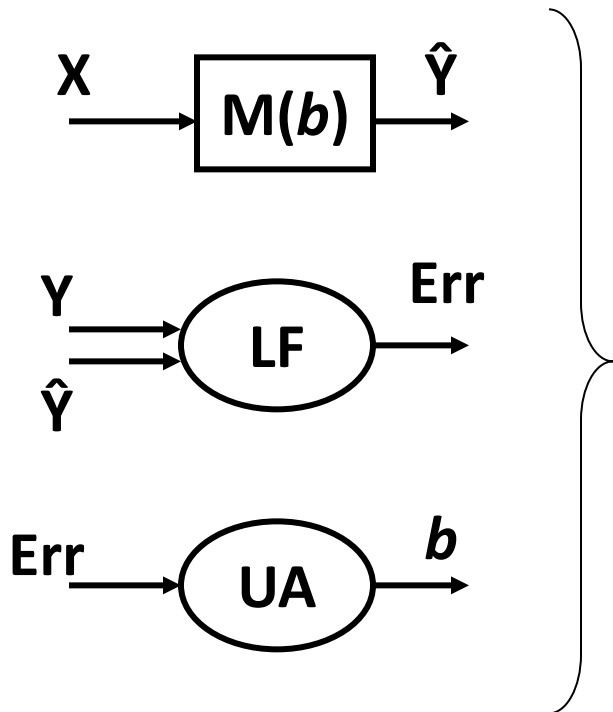
# Strojové učení vs. Umělá inteligence



# Dolování dat a dobývání znalostí z databází

- **Strojové učení je jako matematika** – nabízí efektivní aparát na řešení různých problémů, žádným konkrétním se však nezabývá.
- **KDD** (dobývání znalostí z databází) i **DM** (dolování dat) jsou procesy, jejichž **cílem je získání nové znalosti** či informace z rozsáhlé databáze (*v literatuře uváděné definice jsou takřka identické, více v samostatné přednášce věnované této problematice*).
- **KDD provozuje ten, kdo vlastní data a problém** a bude profitovat z řešení, tedy z nalezené znalosti (v obchodu, provozu, ...).
- **DM provozuje ten, kdo má know-how ve strojovém učení;** dostane vybraná historická data a úloha pro něj končí předáním nové znalosti.
- Někdy KDD a DM dělá ta samá osoba/tým/pracoviště, potom rozdíl mezi oběma termíny mohou splývat v jedno a to samé.

# Proces modelování s učitelem



*VIS: ? nakreslete schéma „procesu modelování s učitelem“*



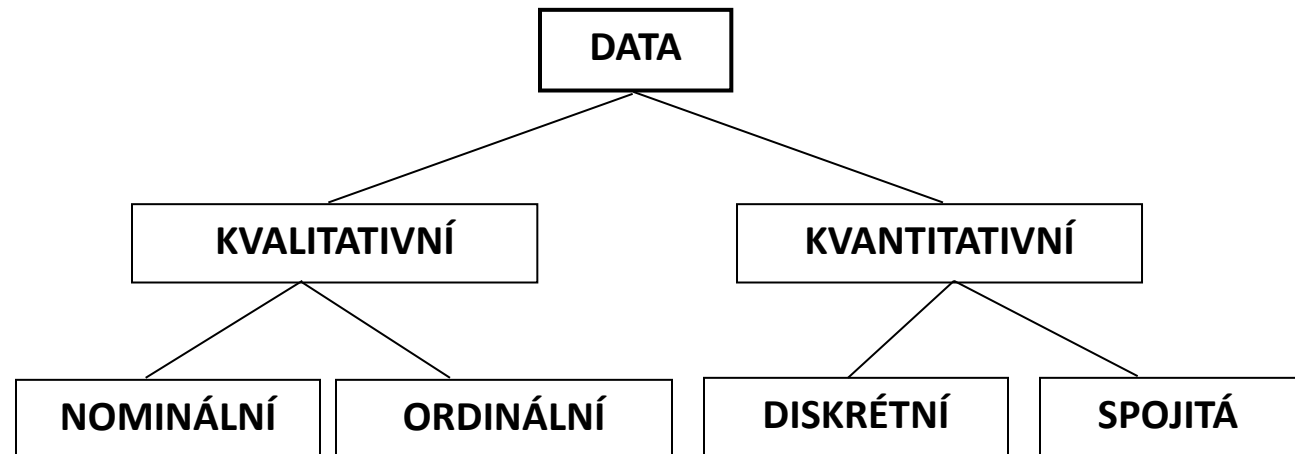
# Komponenty procesu „modelování“

- 1) **data  $X, Y, \hat{Y}$**  (*kvantitativní, kvalitativní*)
- 2) **předzpracování** (*ouliers, chybějící data, relevantní atributy, rozšíření příznakového prostoru*)
- 3) **model  $M$**  (*NS, rozhod. stromy, regresní modely*)  
mající parametry  $b$
- 4) **chybové funkce  $LF$**  (*MNČ, ML, entropie*) vracející chybu predikce  $Err$
- 5) **učicí algoritmy  $UA$**  (*optimalizační algoritmy; (ne)lineární prog., kvadratické, parametrické,..*)
- 6) **testy** (*cross-validation, bootstrap*)
- 7) **meta algoritmy** (*boosting, bagging, stacking*)

*VIS: ? vyjmenujte komponenty používané v procesu modelování*

# DATA – základní dělení, značení

- kvantitativní
  - spojitá
  - diskrétní
- kvalitativní
  - nominální
  - ordinální



- $X$  – vstupní proměnná, nezávislá veličina, prediktor, vysvětlující proměnná
- $y$  – kvantitativní výstupní veličina, závislá veličina, cílový atribut, vysvětlovaná proměnná
- $G$  – kvalitativní výstupní veličina
- $\hat{Y}$  – predikovaná kvantitativní veličina
- $\hat{G}$  – predikovaná kvalitativní veličina

*VIS? uveďte dělení a vysvětlete rozdíl mezi daty kvantitativními a kvalitativními*

# DATA – další dělení

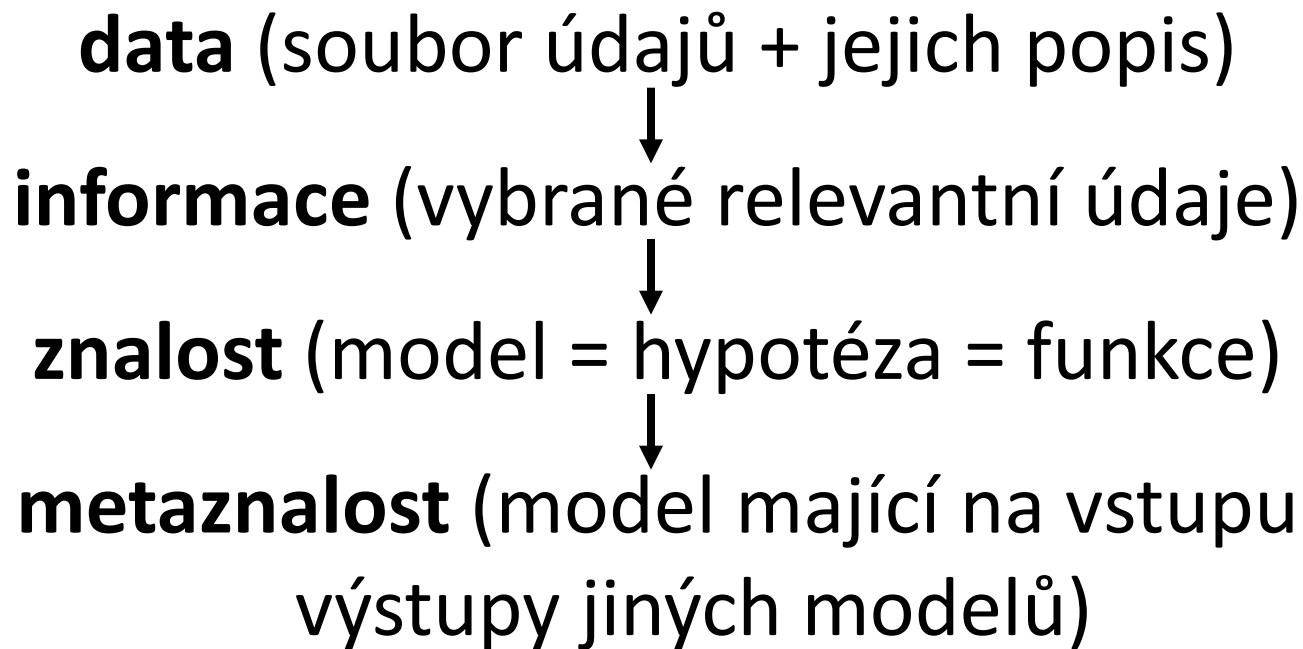
- specifické typy
  - text, datum, dichotomická/binární, ...
- data: čistá / zašuměná
- data: konzistentní / nekonzistentní
- doména (atributy): otevřená / uzavřená
- vzory: pozitivní / pozitivní i negativní

*? co je to otevřená/uzavřená doména*

# Data, Informace, Znalost, Moudrost...

- **Data**
  - diskrétní prvky
  - jednoduchá neorganizovaná fakta, obrázky, ...
- **Informace**
  - vzájemně propojená **data**
  - strukturovaná **data** s přidáním kontextu významnosti
  - **data a pravidla** na ně aplikovaná
  - **data s významem**
  - **popis CO**
- **Znalost**
  - organizovaná **informace**
  - **schopnost** použít informace k dosažení cíle
  - smysluplně využitá **informace**
  - **popis JAK**
- **Moudrost**
  - aplikovaná **znalost**
  - **schopnost** výběru smysluplných cílů
  - **zdůvodnění PROČ**
- **Data – cokoliv co ukládáte**
  - čísla, obrázky, dokumenty, videa
  - svá data umíte interpretovat (víte, co znamenají)
  - statistické údaje o libovolné veličině
  - libovolný vzor (pattern) v datech
- **Informace – relevantní data**
  - informace jsou data, která jsou užitečná v kontextu řešeného problému
  - přínosný (relevantní) vzor, statistický údaj
- **Znalost – funkce**
  - má vstupy (informace) a na jejich základě vrací smysluplný výstup (taky informace)
  - znalost tvoří struktura + parametry vztahů mezi veličinami vstupními a výstupními (informacemi)
- **Moudrost**
  - to je zpravidla lepší nechat na zákazníka

# DATA v SU – od dat k metaznalosti



*? vypište a vysvětlete význam úrovní od šumu po metaznalosti*

# MODEL

- **model** (též **znalost**, **funkce**, **hypotéza**) je z pohledu SU matematicko-logická reprezentace zařízení nebo procesů, do jejíž struktury a parametrů jsou uloženy znalosti získané z analyzovaných dat
- **regresní modely** (výstup – kvantitativní data)
- **klasifikátory** (výstup – kvalitativní data)
- regresní klasifikátory

*? vysvětlete rozdíl mezi regresním modelem a klasifikátorem*

# CHYBOVÁ FUNKCE

- smyslem chybové funkce je kvantifikovat míru odchytky výstupu modelu ( $\hat{Y}$  nebo  $\hat{G}$ ) oproti požadované hodnotě ( $Y$  nebo  $G$ )
- metoda nejmenších čtverců (MNČ)
- maximální věrohodnost (ML)
- nákladová matice (cost matrix)
- regularizace – penalizace za složitost modelu, zabraňuje přeučení

? co je smyslem chybové funkce

# UČICÍ (OPTIMALIZAČNÍ) ALGORITMY

- smyslem učicích algoritmů je měnit parametry modelu tak, aby minimalizovaly hodnotu chybové funkce
- prakticky se jedná o **prohledávání** prostoru možných řešení
- některé metody:
  - analytická/heuristická řešení
  - gradientní metody
  - simplexová metoda
  - genetické algoritmy
  - mravenčí kolonie, žíhání, ...



# Přesnost modelu

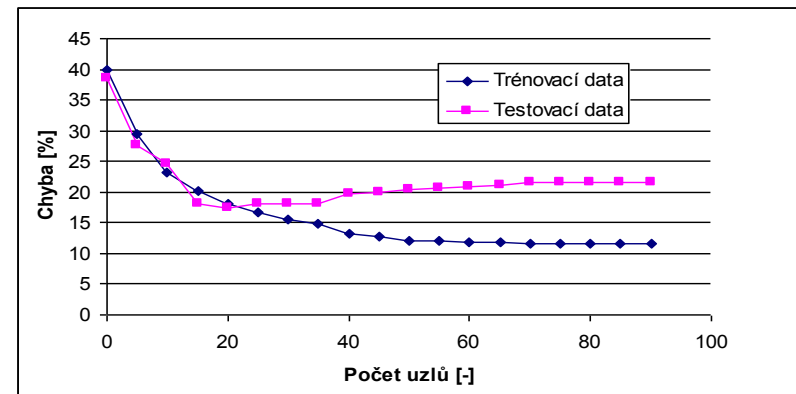
- přesnost modelu lze pouze **odhadnout**
- rozdělení dat
  - trénovací
  - (verifikační)
  - testovací
- metody odhadu chyby
  - cross-validation
  - bootstrap

# Meta–algoritmy

- též **meta-learning** nebo **ensemble methods**
- meta-learning tvoří algoritmy, které umožňují predikovat na základě rozhodnutí více modelů
- vstupem do meta-modelu je  $\hat{Y}$ , nikoliv  $X$
- metody
  - bagging
  - boosting
  - stacking

# Teorémy SU

- **occamovo ostří:** nejjednodušší z více stejně přesných řešení je správné. Analýza oprávněnosti generalizace přesahující naměřená data.
- **přeučení modelu:** přesné naučení modelu na trénovací data vedoucí k naučení šumu nebo neexistujících souvislostí; projeví se velkou chybou na testovacích datech
- **kapacita funkce:** (Vapnik-Chervonenkis)



*VIS: Vysvětli pojmy: occamovo ostří, přeučení modelu*

## Některé další pojmy

- **indukce** – přechod od konkrétního k obecnému (od dat ke znalostem); algoritmy SU jsou induktivního charakteru, platné vždy jen s určitou pravděpodobností; (důsledek – důvod)
- **dedukce** – přechod od obecného ke konkrétnímu (od znalostí k datům, novým řešením), platné s jistotou (pokud jsou předpoklady pravdivé); (důvod - důsledek)

Základní ideu učení s učitelem lze nalézt např. v tomto úryvku (*Sir Arthur Conan Doyle: Poslední poklona Sherlocka Holmese, povídka Vila Vistárie*):

"Domníváte se, milý Watsoně, že lidský důmysl dokáže najít **VYSVĚTLENÍ**, které by zahrnovalo **OBĚ** tyto **SKUTEČNOSTI**? Jestliže by pak takové vysvětlení nevyklučovalo ani onen **TAJUPLNÝ LÍSTEK**, tak prazvláštně stylizovaný, stálo by za to, přijmout jej jako **DOČASNOU HYPOTÉZU**. Kdyby se **VŠECHNY NOVÉ SKUTEČNOSTI**, jež se dozvíme, **HODILY DO JEJÍHO SCHÉMATU**, možná že by se postupně ta hypotéza změnila v **ODHALENOU PRAVDU**."

- **heuristika** – *iterační stochastický postup, nová iterace ovlivněna zkušeností z předešlých iterací.*

# Bias a Variance

- **bias** (*předpojatost*)
  - **odchylka konceptu modelu** od skutečných vazeb (závislostí) v datech
  - systematická chyba
  - jak přesně odpovídá model skutečnosti
  - existuje i při nekonečném množství dat
- **variance**
  - chyba naučení dílčího modelu z konečné množiny dat
  - odchylka od bias způsobená **nedostatkem dat**, nebo nevhodným výběrem z dat (není „ideální“)
- **chyba modelu = bias+variance** (rozbor označován ang. termínem *bias-variance decomposition*)

*VIS: vysvětli rozdíl mezi chybou bias a variance*

# Generalizace

- jedním ze základních požadavků na model je jeho generalizace = zobecnění, obecně platný popis vazeb mezi vstupy a výstupy získaný z dat
- rozlišujeme tři typy generalizace hypotéz (modelů)
  - jiná sudá čísla než 2 nejsou prvočísla **správná generalizace**
  - přirozená čísla končící na 1 jsou prvočísla **neoprávněná generalizace**
  - žádné prvočíslu není větší než 100 **podceněná generalizace**

# Metoda prostoru hypotéz (verzí)

- metoda pracuje průběžně se dvěma hypotézami (modely) pomocí **specializace** a **generalizace**
- **oba modely popisují** všechny **pozitivní** prvky a **vylučují** všechny **negativní** prvky
- **první model**
  - co **nejspecifičtější**
  - s přibývajícími **pozitivními** prvky dochází k jeho **generalizaci**
- **druhý model**
  - co **nejobecnější**
  - s přibývajícími **negativními** dochází k jeho **specializaci**

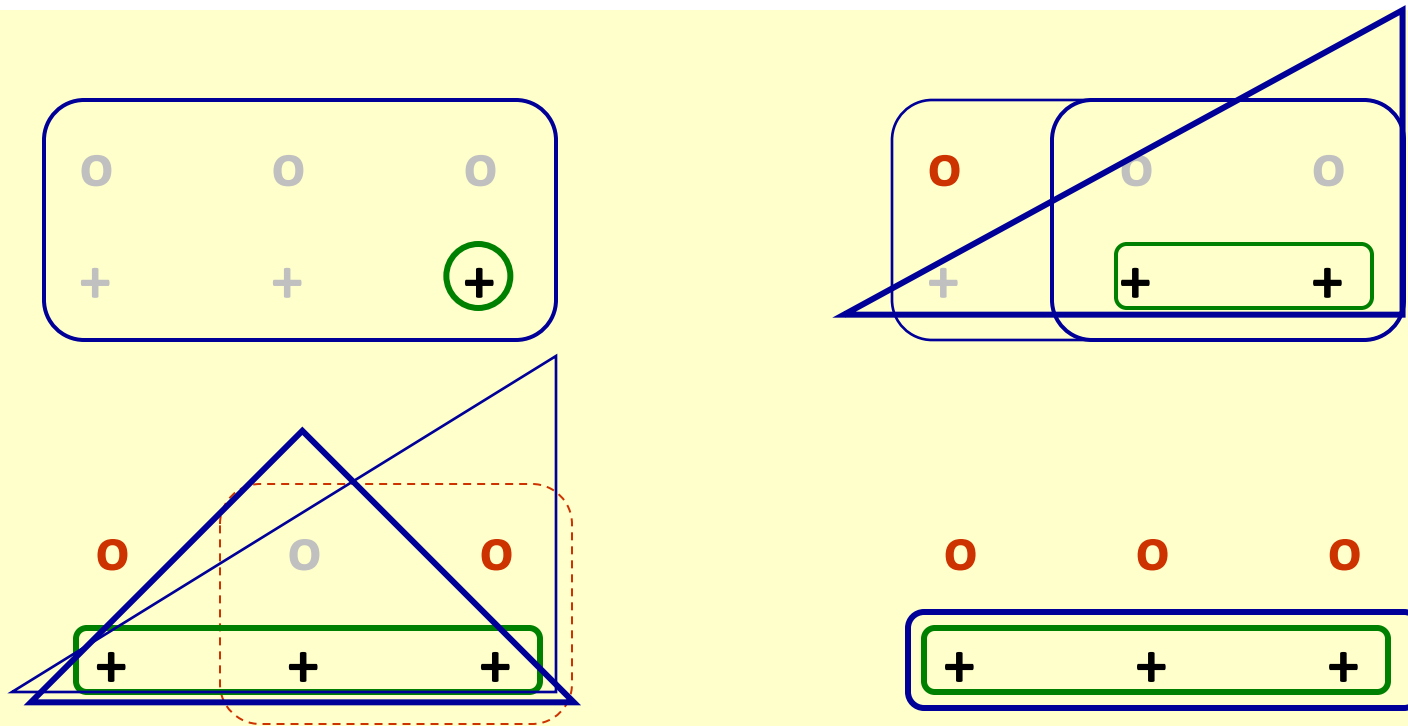
# Metoda prostoru verzí – tvorba hypotézy

- na počátku 2 modely, zcela speciální a obecný
- každý nový model je specializací (generalizací) modelu obecného (speciálního)
- úprava vždy minimální možnou změnou
- žádný nový speciální (obecný) model není generalizací (specializací) jiného specifického (obecného) modelu
- záporný příklad – úprava specializací (obecného)
- kladný příklad – generalizace (speciálního)
- vyškrtni nevyhovující specifické modely



# Příklad 1 – princip induktivního učení

- **pozitivní případ** – minimálně generalizuj
- **negativní případ** – minimálně specializuj



## Příklad 2 – indukativní učení

Lékař léčí pacienta, který občas trpí diarrheou. Intuitivně předpokládá, že tyto souvisejí s místem stravování pacienta. Následující tabulka zahrnuje informace, které byly získány od pacienta.

Restaurace	Jídlo	Den	Cena	Diarrhea
U Pepy	snídaně	pátek	levné	ano
Padovec	oběd	pátek	drahé	ne
U Pepy	oběd	sobota	levné	ano
Nádražní	snídaně	neděle	levné	ne
U Pepy	snídaně	neděle	drahé	ne

## Příklad 2 – význam předpojatosti

- označme  $X$  množinu všech **úplných instancí** (hodnoty všech atributů jsou definovány). Pak **mohutnost**  $X = |X| = 3 \cdot 2 \cdot 3 \cdot 2 = 36$
- **konceptem** je v binární klasifikaci rozuměna hypotéza (soubor hypotéz) určující prvky jedné třídy (všechna  $x \in X$  jedné třídy)
- počet **všech možných konceptů** = počet podmnožin  $X =$  mohutnost potenční množiny  $P(X) = 2^{|X|} = 2^{36} \approx \mathbf{10^{10}}$
- při použití uvedené metody **lze zapsat jen  $4 \cdot 3 \cdot 4 \cdot 3 = 144$  konceptů**; metoda je předpojatá, má schopnost generalizace
- u metody umožňující popis každého konceptu hrozí riziko přeučení (tzv. unbiased learner, např. rozhodovací strom bez prořezávání)
- **bez předpojatosti by nedošlo k žádné generalizaci**, byla by uložena pouze trénovací data