evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

PSK2-5

Název školy:	Vyšší odborná škola a Střední průmyslová škola, Božetěchova 3
Autor:	Ing. Marek Nožka
Anotace:	Detekce a korekce chyb -- kanálové kódování
Vzdělávací oblast:	Informační a komunikační technologie
Předmět:	Počítačové sítě a komunikační technika (PSK)
Tematická oblast:	Vrstvy protokolu TCP/IP
Výsledky vzdělávání:	Žák objasňuje princip detekce a korekce chyb
Klíčová slova:	otisk, hash, detekce a korekce chyb
Druh učebního materiálu:	Online vzdělávací materiál
Typ vzdělávání:	Střední vzdělávání, 3. ročník, technické lyceum
Ověřeno:	VOŠ a SPŠE Olomouc; Třída: 3L
Zdroj:	Vlastní poznámky, Wikipedia, Wikimedia Commons

Kanálové kódování

Pojem kanálové kódování je odvozen z toho, že toto kódování přizpůsobuje zprávu pro daný přenosový kanál. Jeho úkolem je zabezpečit data proti cybám. K~přenášeným datům se přidají další data, která zprávu zabezpečují. *Zvětšuje se tedy redundance.*

Chyby

Při přenosu dat jakoukoli přenosovou trasou dochází **vždy** k chybám. Ty je nutné detekovat nebo opravit.

- ojedinělé chyby
- shluky chyb
- každá přenosová trasa vykazuje jinou *chybovost* a je zdrojem jiného druhu chyb

Chybovost je podíl špatně a správně přenesených bitů:

- optické vlákno: chybovost 10^{-9}
- rádiový přenos: chybovost 10^{-2} až 10^{-3}

$\Rightarrow$ volba *zabezpečovacího kódu*

- detekční kódy
- samoopravitelné kódy

Elementární detekční kódy

Detekční kódy slouží k detekci chyb. Pokud je chyba detekována, přijímací strana chybu pouze detekuje (a musí si od vysílací strany vyžádat opakování zprávy).

Paritní kód

Paritní kód je nejjednodušším detekčním kódem. Značka má $(n-1)$ míst informačních a jedno místo zabezpečující. K přenášeným datům doplníme vždy jeden bit tak, aby počet jedniček byl sudý (sudá parita) nebo lichý (lichá parita).

Příklad sudé parity

Poslední bit je vždy paritní.

```
10011011  1
00110111  1
01101001  0
00011000  0
```

Chybu nelze detekovat pokud \tecky{5} % dojde k dvěma chýbám najednou

Kódy K z N

Kódy K z N mají n-místné značky a v~každé je právě k~jedniček. Kontrola spočívá ve spočítání jedniček. U těchto kódů nelze oddělit data a zabezpečení.

Platná data	Chybná data
0 0 1 1	0 0 0 0
0 1 0 1	0 0 0 1
0 1 1 0	0 0 1 0
1 0 0 1	0 1 0 0
1 0 1 0	0 1 1 1
1 1 0 0	1 0 0 0
	1 0 1 1
	1 1 0 1
	1 1 1 0
	1 1 1 1

Hašovací funkce

Hašovací funkce nebo jen Hash je *reprodukovatelná (opakovatelná) metoda*

pro převod vstupních dat do (relativně) malého čísla, které vytváří jejich otisk -- můžeme ho označit jako charakteristiku dat.

Výsledný otisk se označuje také jako výtah, miniatura, **fingerprint** či **hash**. Funkce může sloužit ke kontrole integrity (neporušenosti) dat, k rychlému porovnání dvojice zpráv, indexování, vyhledávání apod. Je důležitou součástí kryptografických systémů pro elektronický podpis.

Jestliže mají dvě zprávy stejný hash je velká pravděpodobnost, že se shodují.

Nejznámější hashovací funkce jsou MD5, CRC nebo SHA.

Hašovací algoritmy jsou bezpečné pokud je velmi obtížné (tj. se současnými prostředky prakticky nemožné):

1. najít zprávu, která odpovídá svému otisku
2. najít dvě rozdílné zprávy, které mají stejný otisk

Například následující zpráva:...

```
Alenko!

Oběd máš v lednici. Vrátím se až večer.

    Máma
```

`--> stáhnout

... má tento MD5 otisk:

```
b99ed1417ff6469b94a605b9c789c161
```

a tento SHA1 otisk:

```
834bfc7d8ced0c10963dd8ef9123020bd441f450
```

Pokud změním zprávu, změní se i otisky. Všimněte si, že různě dlouhé zprávy mají vždy stejně dlouhé otisky.

```
Alenko!

Oběd máš v lednici. Vrátím se až večer.

--
Ahoj
   Tvoje Máma
```

`--> stáhnout

MD5:

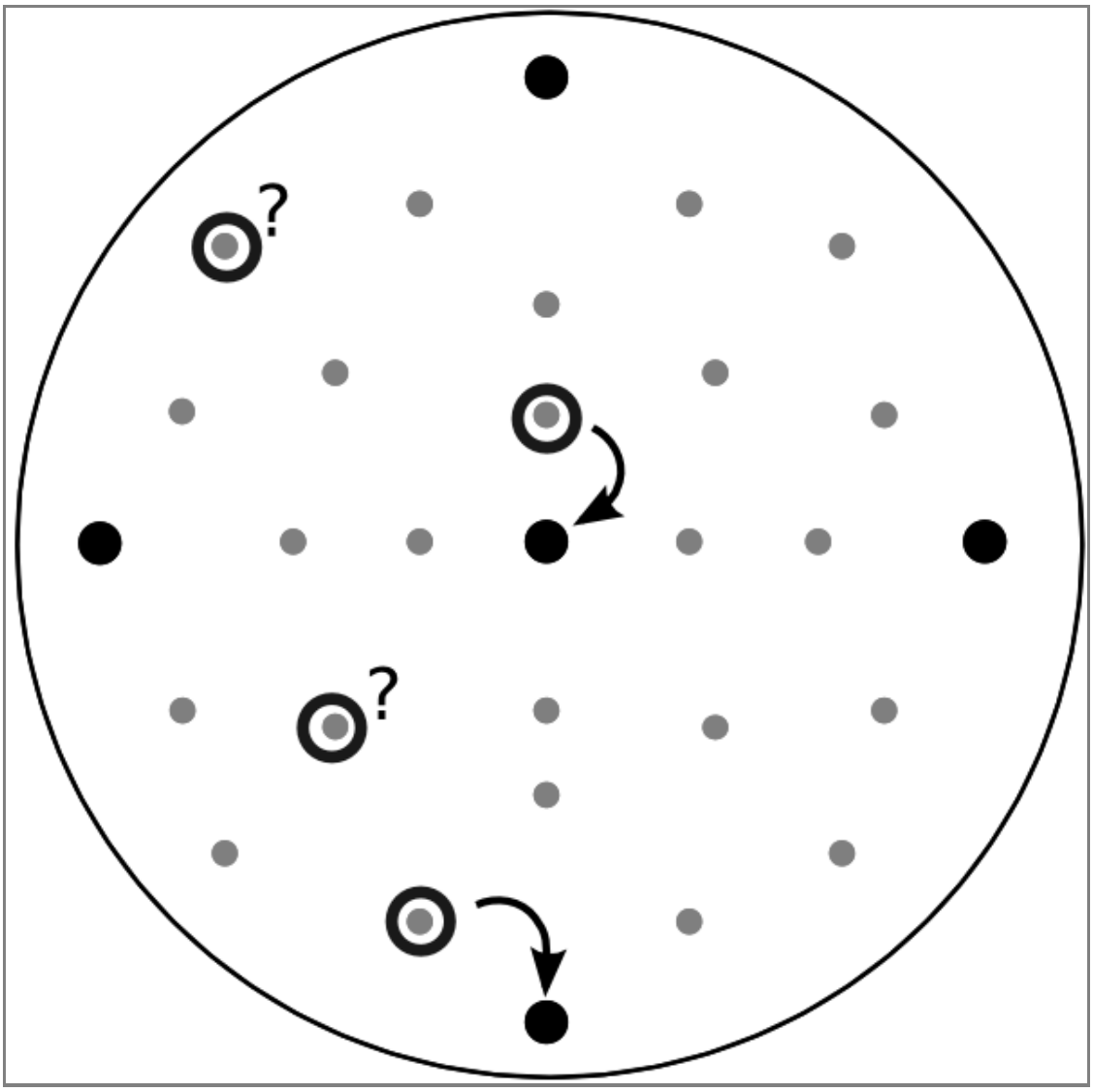
```
b35d7d1cc5874b6440f1eb0cca312314
```

SHA1:

```
7badc8f34d34ef422b833071dc7529595d958e19
```

Kódy pro detekci a opravu chyb

Některé přenosové linky vykazují tak velkou chybovost, že bychom si s pouhým detekčním kódem nevystačili. Pravděpodobnost výskytu chyby je tak velká, že téměř nepřeneseme jedinou značku bez chyby. Proto se používají kódy, které umí chybu nejen detekovat, ale do určitého množství chyb i opravit.



Na obrázku je schematické znázornění detekce a opravy chyb. Tečky představují množinu možných stavů. Černé tečky stavy povolené jsou , šedé tečky jsou stavy zakázané -- tedy chyby. U některých chybových stavů lze určit, který platný stav je mu nejblíže. U některých to ale nelze, a je možné pouze konstatovat, že došlo k chybě.

Blokové lineární kódy

- data jsou kódována a dekódována po blocích
- kód se vytváří na základě tzv. *vytvářecí matice* a na přijímací

straně jsou přijímaná data kontrolována pomocí * kontrolní matice*
- pomocí kontrolní matice lze chyby v přenesených datech detekovat a do určitého počtu chyb i opravit

Blokové cyklické kódy

- pracují podobně jako lineární kódy, ale používají *vytvářecí a kontrolní mnohočleny*
- nejznámější z těchto kódů je CRC

Konvoluční kódy

- jsou vybaveny pamětí
- kódování kódovaného úseku není určeno jen tímto úsekem, ale také předcházejícím průběhem zprávy