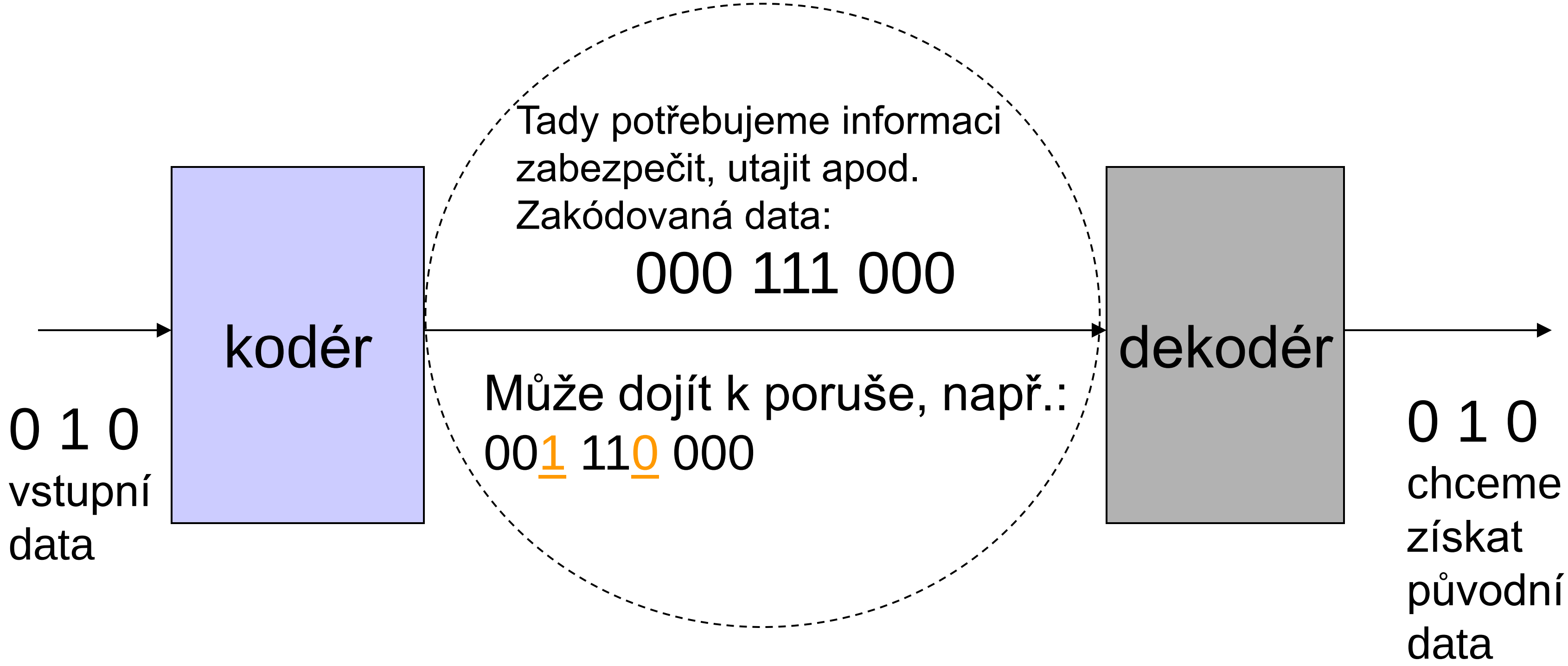
Kódy pro detekci a opravu chyb

INP 2019

FIT VUT v Brně

Princip kódování



- Předpokládejme kódovací předpis, např.:

  $0 \rightarrow 000$, $1 \rightarrow 111$
- Uvedené kódování může být použito pro přenos dat buď mezi jednotkami nebo celými systémy (například počítači).
- Zabezpečení informace je založeno na vhodném využití redundance.

Základní kódy pro detekci a opravu chyb

- Parita
- Ztrojení
- Hammingův kód (7,4)
- Rozšířený Hammingův kód

- Pozn. Pokročilé kódy (např. CRC) nejsou probírány v INP.

Paritní kód

Nejjednodušší kód **detekující** jednu chybu (SED – Single Error Detection) dostaneme doplněním paritního bitu, např. na *sudou* paritu.

0110 1010 0

1000 0000 1

1111 1111 0

. . .

Popsané uspořádání se nazývá **paritní kód**. Kombinace se zvolenou sudou (tedy správnou) paritou se označují jako **kódové**, kombinace s chybnou (lichou) paritou jako **nekódové**. Kontrola správnosti dat se zjišťuje *kontrolou parity*.

Hammingova vzdálenost

Hammingova vzdálenost je definovaná jako nejmenší počet bitů, v nichž se dvojice kódových kombinací liší, zjištěný pro všechny možné dvojice.

Příklad sudého paritního kódu:

x_2	x_1	x_0	p
0	*0*	*0*	*0*
0	*0*	*1*	*1*
0	*1*	*0*	*1*
0	*1*	*1*	*0*
1	*0*	*0*	*1*
1	*0*	*1*	*0*
1	*1*	*0*	*0*
1	*1*	*1*	*1*

Minimální vzdálenost, zjištěná u každé dvojice kódových slov, je **Hammingova vzdálenost kódu** d_H.

U paritního kódu je to $d_H = 2$.

Ztrojení (kód typu SEC - Single-Error Correction)

Ztrojením jednoho bitu dostaneme dvě kódové kombinace, a to 000, 111, a 6 nekódových kombinací.

kódové kombinace	**nekódové kombinace**
0 0 0	0 0 1
1 1 1	0 1 0
	0 1 1
	1 0 0
	1 0 1
	1 1 0

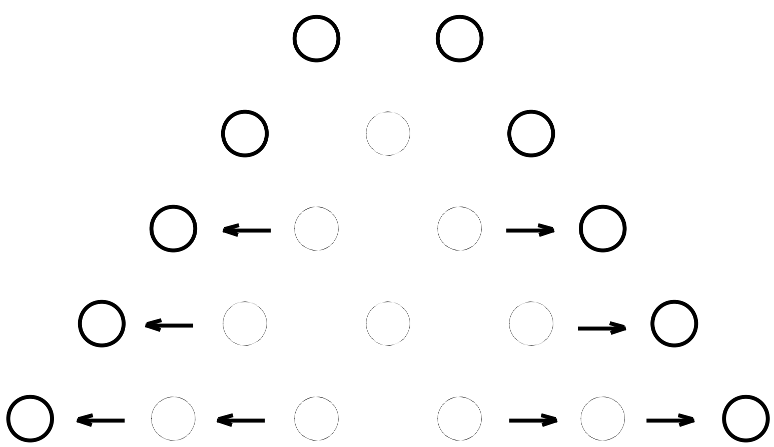
Za **předpokladu jediné chyby** (jednobitové) je možno určit, ze které kódové kombinace daná nekódová kombinace vznikla. Dostali jsme tak kód **opravující** jednoduché chyby (Single-Error Correction - SEC). Jeho Hammingova vzdálenost je 3.

Hammingova vzdálenost a schopnost kódu detekovat/opravovat chyby

Pro opravu *x*-násobné chyby musí být Hammingova vzdálenost

$$d_H \geq 2x + 1.$$

Ilustrace principu: Kroužky nakreslené plnou čarou představují kódové kombinace, tečkované kroužky znamenají nekódové kombinace. Mezi sousedními kroužky v jednom řádku je Hammingova vzdálenost rovna jedné. Je zřejmé, že pro kód s Hammingovou vzdáleností d_H = 2 nemůžeme rozhodnout, ze které kódové kombinace vzniklo vlivem jednobitové chyby nekódové slovo, a nedokážeme tedy chybu opravit. Opravu jednobitové chyby můžeme provést až u kódu se vzdáleností d_H = 3.



	d_H
	1
SED	2
SEC	3
SEC - DED	4
DEC	5

Hammingův kód (n, k)

- n – délka kódového slova (v bitech)
- k – počet informačních bitů
- m – počet kontrolních bitů
- $n = 2^m - 1$
- $n = m + k$
- Př. HK(7, 4), HK(15, 11), …

- Nejznámější SEC je HK(7, 4)

Hammingův kód (7,4) – kódování

	2^6	2^5	2^4	2^3	2^2	2^1	2^0
i =	7	6	5	4	3	2	1
	I_7	I_6	I_5	C_4	I_3	C_2	C_1
	X		X		X		X
	X	X			X	X	
	X	X	X	X			

generující matice

$$C_1 = I_3 \otimes I_5 \otimes I_7$$
$$C_2 = I_3 \otimes I_6 \otimes I_7$$
$$C_4 = I_5 \otimes I_6 \otimes I_7$$

generující rovnice
(⊗ znamená XOR)

Podle hodnoty zavedeného indexu *i* se rozhodne o funkci příslušného bitu: je-li *i* mocnina dvojky, je bit kontrolní (C), v ostatních případech je bit informační (I). Rozmístění symbolů **X** v generující matici je popsáno generujícími rovnicemi. Je tak definován způsob doplňování hodnot kontrolních bitů, tedy jistým způsobem vypočítávaných paritních bitů.

Tvar kódové značky: $I_7I_6I_5C_4I_3C_2C_1$

Hammingův kód (7,4) - dekódování

“Přičteme-li” operací XOR k oběma stranám generujících rovnic pořadě C_1, C_2, C_4, dostaneme tzv. **kontrolní rovnice**

$$C_1 \oplus I_3 \oplus I_5 \oplus I_7 = 0 = S_1$$
$$C_2 \oplus I_3 \oplus I_6 \oplus I_7 = 0 = S_2$$
$$C_4 \oplus I_5 \oplus I_6 \oplus I_7 = 0 = S_4$$

Pokud dosadíme do kontrolních rovnic kódová (správná) slova, dostaneme **nuly**. Pro nekódová slova, která vzniknou jednobitovou chybou z kódových slov, vyjdou výpočtem kontrolních rovnic nenulové hodnoty S_4, S_2, S_1, zvané **syndrom chyby**. Syndrom jednoduché chyby udává binárně hodnotu indexu bitu s chybou. Chybu pak můžeme opravit změnou hodnoty takto zjištěného bitu na hodnotu opačnou.

Pro dvojnásobnou chybu však mechanizmus selhává a syndrom chyby udává nesprávnou polohu chyby. Je to způsobeno tím, že takto definovaný kód je SEC, nikoli však DED. Proto je často vhodné doplnit definici kódu tak, aby kód získal vlastnost DED, získáme rozšířený Hammingův kód.

Rozšířený Hammingův kód (SEC, DED)

I_7	I_6	I_5	C_4	I_3	C_2	C_1	C_0
x		x		x		x	
x	x			x	x		
x	x	x	x				
x	x	x	x	x	x	x	x

Do kódu je doplněn **kontrolní bit** C_0 (běžný paritní bit), popsaný generující rovnicí

$$C_0 = C_1 \oplus C_2 \oplus I_3 \oplus C_4 \oplus I_5 \oplus I_6 \oplus I_7$$

Kontrolní rovnice má tvar:

$$S_0 = C_0 \oplus C_1 \oplus C_2 \oplus I_3 \oplus C_4 \oplus I_5 \oplus I_6 \oplus I_7$$

Rozšířený Hammingův kód
$d_H = 4$
čtyři informační bity, čtyři kontrolní bity.

Linearita kódu:
součet (pomocí xor) dvou kódových slov vytvoří opět platné kódové slovo.

I_7	I_6	I_5	C_4	I_3	C_2	C_1	C_0
x		x		x		x	
x	x			x	x		
x	x	x	x				
x	x	x	x	x	x	x	x
0	0	0	0	0	0	0	0
0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1
0	0	1	1	1	1	0	0
0	1	0	1	0	1	0	1
0	1	0	1	1	0	1	0
0	1	1	0	0	1	1	0
0	1	1	0	1	0	0	1
1	0	0	1	0	1	1	0
1	0	0	1	1	0	0	1
1	0	1	0	0	1	0	1
1	0	1	0	1	0	1	0
1	1	0	0	0	0	1	1
1	1	0	0	1	1	0	0
1	1	1	1	0	0	0	0
1	1	1	1	1	1	1	1

Rozšířený Hammingův kód - syndrom

Definujeme **syndrom chyby**

$S = S_1 \vee S_2 \vee S_4$ (tj. OR)

Pomocí hodnot S, S_0 dostaneme klasifikaci chyb:

S	S_0	význam
0	0	bez chyby
0	1	neopravitelná chyba, např. porucha hlídače kódu
1	0	neopravitelná 2-, 4- atd. násobná chyba
1	1	opravitelná chyba

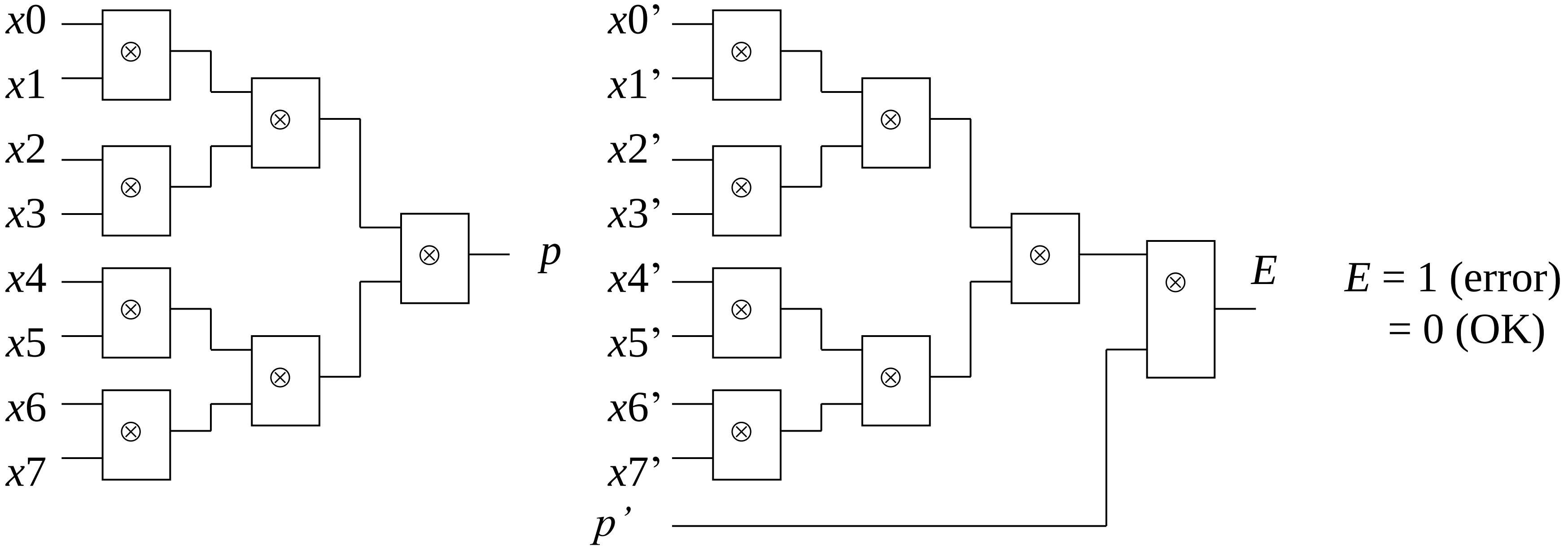
Základní typ *jednoduché chyby* se projeví nenulovým syndromem a chybou parity. V takovém případě se provede oprava.

Stejně se však projeví i *trojnásobná chyba* a další chyby s *lichou násobností.*

Dvojitá chyba (a další *chyby se sudou násobností*) se projeví nenulovým syndromem a správnou paritou. Oprava není možná.

Zvláštním případem je hlášení s nulovým syndromem a chybnou paritou. Jde buďto o případ *vícenásobné chyby*, nebo o *poruchu hlídače parity*. V obou případech *se oprava chyby nedá provést*.

Generování a kontrola parity (8 bitů)

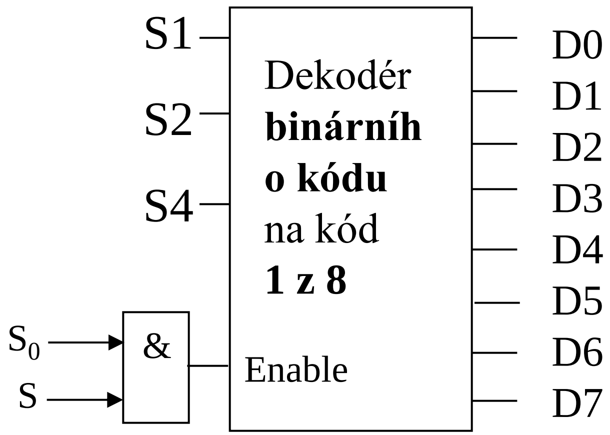


V kodéru: $p = x0 \otimes x1 \otimes x2 \otimes x3 \otimes x4 \otimes x5 \otimes x6 \otimes x7$

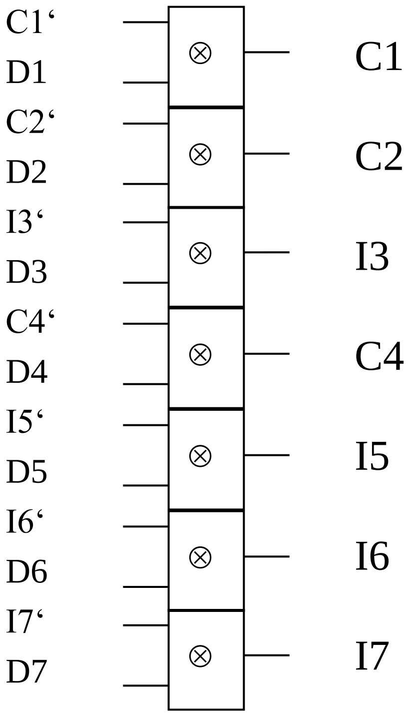
V dekodéru: $E = x0' \otimes x1' \otimes x2' \otimes x3' \otimes x4' \otimes x5' \otimes x6' \otimes x7' \otimes p'$

Pozn.: Apostrof označuje přijatý symbol, který v důsledku poruchy nemusí být stejný jako vyslaný symbol.

Oprava chyb pomocí syndromu Hammingova kódu v hardware



Dekodér syndromu



Korektor

Redundance kódu a CNC

- *Redundance kódu* R je procentuální vyjádření počtu *přidaných* (*kontrolních*) bitů C k původnímu počtu *informačních* (*datových*) bitů I

$$R = C / I$$

- Redundance 8-bitového kódu s přidaným paritním bitem je $R_{parity8} = 1/8 = 0{,}125 = 12{,}5\%$
- Redundance ztrojeného kódu je 200%.
- Dále se můžeme setkat s parametrem, označeným zkratkou *CNC* – *Code to Noncode ratio.* Je to poměr počtu kódových a nekódových slov, tedy kódových a nekódových binárních kombinací z celkového množství binárních kombinací dané délky.
- Pro paritní kód je poměr CNC 1:1, tedy 1, pro ztrojený kód je poměr CNC 2:6, tedy 0,33.
- **Otázka**: Jaká je hodnota redundance a CNC pro jednoduchý a rozšířený Hammingův kód s délkou n informačních bitů?