BEZPEČNOSTNÍ KÓDY

PŘENÁŠENÁ A ULOŽENÁ DATA JSOU OVLIVŇOVÁNA ŠUMEM.

ŠUM SE MŮŽE PROJEVIT DVĚMA ZPŮSOBY:

1. ZÁMĚNA ZNAKU ZA JINÝ ZNAK
2. PORUŠENÍ SYNCHRONIZACE (ZTRÁTA ZNAKU BEZ NÁHRADY NEBO VYTVOŘENÍ „FALEŠNÉHO" ZNAKU.

ZPOČÁTKU BUDEME PŘEDPOKLÁDAT JEN CHYBY TYPU 1) (ZÁMĚNA ZNAKŮ).

BUDEME PRACOVAT S BLOKOVÝMI KÓDY (VŠECHNY ZNAČKY MAJÍ STEJNOU DÉLKU n).

JAK MŮŽE KÓD OBJEVOVAT A OPRAVOVAT CHYBY? DÍKY REDUNDANCI.

NĚKTERÉ ZNAKY KÓDOVÉ ZNAČKY NENESOU ŽÁDNOU INFORMACI, ALE SLOUŽÍ POUZE K ZABEZPEČENÍ (KONTROLE).

PŘÍKLAD „KÓDU" S VYSOKOU REDUNDANCÍ:

ČEŠTINA: VYSLANÉ SLOVO: OPAKOVÁNO
PŘIJATO: OPAKKVÁNO
LZE OPRAVIT JEDINÝM ZPŮSOBEM: OPAKOVÁNO
(JE TO JEDINÉ „KÓDOVÉ SLOVO", KTERÉ SE OD PŘIJATÉ KOMBINACE LIŠÍ V JEDINÉM PÍSMENU
(NEJBLIŽŠÍ SLOVO)

VYSLANÉ SLOVO: OPAKOVÁNO
PŘIJATO: OPAKOVÁNR
LZE OPRAVIT DVĚMA ZPŮSOBY: OPAKOVÁNO
OPAKOVÁNÍ
(NEJBLIŽŠÍ SLOVO NENÍ JEDNOZNAČNÉ)

V PŘÍPADĚ UMĚLÝCH KÓDŮ MŮŽEME VHODNOU KONSTRUKCÍ KÓDU VYTVOŘIT PODMÍNKY PRO ODHALENÍ, RESP. OPRAVENÍ CHYB SE ZADANOU NÁSOBNOSTÍ DOPLNĚNÍM KONTROLNÍCH (ZABEZPEČOVACÍCH) ZNAKŮ.

OBJEVOVÁNÍ CHYB

PŘEDPOKLÁDÁME BLOKOVÝ KÓD K NAD KONEČNOU ABECEDOU T.

$$T^m = \{A_1 A_2 \dots A_m \mid A_i \in T \quad \forall i = 1, 2, \dots, m\}$$

JE MNOŽINA VŠECH SLOV DÉLKY m NAD T

$K \subseteq T^m$ JE KÓD

PAK EXISTUJE DVOUBLOKOVÝ ROZKLAD MNOŽINY T^m NA

<u>KÓDOVÁ SLOVA</u> K

<u>NEKÓDOVÉ KOMBINACE</u> $T^m - K$

VYSÍLÁME KÓDOVÁ SLOVA
PŘIJÍMÁME (OBECNĚ) SLOVA Z T^m

PŘIJETÍ NEKÓDOVÉ KOMBINACE =>
=> OBJEVENÍ CHYBY
PŘIJETÍ KÓDOVÉHO SLOVA =>
=> BUĎ K CHYBĚ NEDOŠLO,
NEBO DOŠLO K TAKOVÉ CHYBĚ,
KTEROU JSME NEOBJEVILI.

NÁSOBNOST CHYBY

t-NÁSOBNÁ CHYBA ($t = 1, 2, 3, \ldots$) ZNAMENÁ, ŽE POČET CHYBNÝCH MÍST JE NEJVÝŠE t.

PŘ: SLOVO: 1111

PRODUKTY DVOJNÁSOBNÉ CHYBY:
0110, 0011, 0111, 1110, ...

KÓD K OBJEVUJE 1-NÁSOBNÉ CHYBY, JESTLIŽE PŘI VYSLÁNÍ LIBOVOLNÉHO KÓDOVÉHO SLOVA A VZNIKU LIBOVOLNÉ 1-NÁSOBNÉ CHYBY JE PŘIJATÉ SLOVO VŽDY NEKÓDOVÉ.

PŘ: KÓD „DVA Z PĚTI"

„1"	11000	„6"	00101
„2"	10100	„7"	00011
„3"	10010	„8"	00110
„4"	10001	„9"	01100
„5"	01001	„0"	01010

BINÁRNÍ KÓD DÉLKY 5, $K \subseteq \{0,1\}^5$

KAŽDÉ KÓDOVÉ SLOVO OBSAHUJE PRÁVĚ DVĚ JEDNIČKY.

KÓD OBJEVUJE JEDNODUCHÉ CHYBY (PŘIJATÁ ZNAČKA PAK DÁ 1 NEBO 3 JEDNIČKY).

KÓD UŽ ALE NEOBJEVUJE DVOJITÉ CHYBY:

PŘÍKLAD KONKRÉTNÍ CHYBY VE DVOU PRVCÍCH:

ZNAČKA: $100\underline{1}\underline{0}$	PŘIJATO: $10001 \in K$
$1\underline{0}\underline{0}10$	$11110 \notin K$
$\underline{1}00\underline{1}0$	$00000 \notin K$

HAMMINGOVA VZDÁLENOST DVOU SLOV

$v = v_1 v_2 \dots v_n$

$w = w_1 w_2 \dots w_n$

$$d(v,w) = \operatorname{card}\{i \mid i=1,2,\dots,n,\ v_i \neq w_i\}$$

TJ. POČET ODLIŠNÝCH ZNAKŮ SLOV v A w.

MINIMÁLNÍ HAMMINGOVA VZDÁLENOST KÓDU

$$d_0(K) = \min d(v,w) \quad \forall v,w \in K \ \ v \neq w$$

TJ. MINIMÁLNÍ HAMMINGOVA VZDÁLENOST DVOU RŮZNÝCH KÓDOVÝCH SLOV.

HAMMINGOVA VZDÁLENOST JE METRIKOU NA MNOŽINĚ T^n, TJ. $\forall v,w,u \in T^n$ PLATÍ:

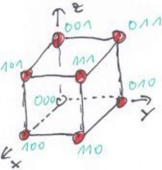
$$d(v,w) \geq 0 \;;\; d(v,w) = 0 \iff v = w$$

$$d(v,w) = d(w,v)$$

$$d(v,w) \leq d(v,u) + d(u,w)$$

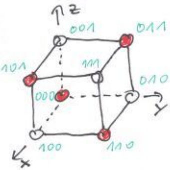
PŘ: BINÁRNÍ KÓDY DÉLKY $n = 3$

K_1



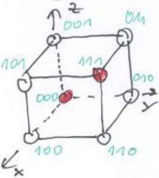
$d_0 = 1$

K_2



$d_0 = 2$

K_3



$d_0 = 3$

$K_1 = \{000, 001, 010, 011, 100, 101, 110, 111\}$

$d_0 = 1$, NEOBJEVÍ ŽÁDNOU CHYBU.

$K_2 = \{000, 011, 101, 110\}$

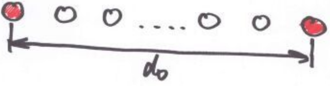
$d_0 = 2$, OBJEVÍ JEDNODUCHÉ CHYBY

$K_3 = \{000, 111\}$

$d_0 = 3$ OBJEVÍ DVOJITÉ CHYBY

SCHOPNOST OBJEVOVAT A-NÁSOBNÉ CHYBY SOUVISÍ S MINIMÁLNÍ HAMMINGOVOU VZDÁLENOSTÍ KÓDU.

<u>OBECNĚ</u>:



KÓD OBJEVUJE A-NÁSOBNÉ CHYBY $\forall A \; A < d_0$.

PŘ: KÓD CELKOVÉ KONTROLY PARITY

(K BINÁRNÍMU SLOVU PŘIDÁ DE JEDEN KONTROLNÍ ZNAK TAK, ABY CELKOVÝ POČET JEDNIČEK BYL SUDÝ).

PRO DÉLKU $n = 4$ (VČETNĚ PARITNÍHO PRVKU):

$$K = \{0000, 1100, 1010, 1001, 0111, 0101, 0011, 1111\}$$

ZŘEJMĚ $d_0 = 2$, ODJEVÍ JEDNODUCHÉ CHYBY.

PŘ: OPAKOVACÍ KÓD

$$K = \{\underbrace{aaa\ldots a}_{n\times} \mid \forall a \in T\}$$

ZŘEJMĚ $d_0 = n$, ODJEVÍ $n-1$ NÁSOBNÉ CHYBY.

OPRAVOVÁNÍ CHYB

ZA URČITÝCH PŘEDPOKLADŮ LZE CHYBY NEJEN OBJEVOVAT, ALE I OPRAVOVAT.

POUŽIJEME PŘEDPOKLAD STATISTICKY NEZÁVISLÝCH CHYB:

TO, ZDA SE V i-TÉM PRVKU OBJEVÍ CHYBA, NEZÁVISÍ NA TOM, ZDA SE OBJEVÍ CHYBA V JINÝCH PRVCÍCH.

p .... CHYBOVOST (P-ST VÝSKYTU CHYBY V JEDNOM KONKRÉTNÍM ZNAKU.

PAK PLATÍ:

P-ST BEZCHYBNÉHO PŘENOSU n-ZNAKOVÉ ZNAČKY: $p_0 = (1-p)^n$

P-ST CHYBY V JEDNOM KONKRÉTNÍM ZNAKU

$$p \cdot (1-p)^{n-1}$$

P-ST JEDNODUCHÉ CHYBY VE ZNAČCE

$$p_1 = n \cdot p \cdot (1-p)^{n-1}$$

OBECNĚ $p_i = \binom{n}{i} p^i (1-p)^{n-i}$

PRO KONKRÉTNÍ p LZE SPOČÍTAT :

n=8 chybovost 1,00E-02

i	p-st chyby
0	0,922744694
1	0,074565228
2	0,002636144
3	5,32554E-05
4	6,72417E-07
5	5,43367E-09
6	2,74428E-11
7	7,92E-14
8	1E-16
Σ	1

n=8 chybovost 1,00E-04

i	p-st chyby
0	0,99920028
1	0,00079944
2	2,79832E-07
3	5,5972E-11
4	6,9972E-15
5	5,59832E-19
6	2,79944E-23
7	7,9992E-28
8	1E-32
Σ	1

n=8 chybovost 1,00E-06

i	p-st chyby
0	0,999992
1	7,99994E-06
2	2,79998E-11
3	5,59997E-17
4	6,99997E-23
5	5,59998E-29
6	2,79999E-35
7	7,99999E-42
8	1E-48
Σ	1

n=8 chybovost 1,00E-08

i	p-st chyby
0	0,99999992
1	8E-08
2	2,8E-15
3	5,6E-23
4	7E-31
5	5,6E-39
6	2,8E-47
7	8E-56
8	1E-64
Σ	1

PŘEDVEDENÉ VÝPOČTY ILUSTRUJÍ OPRAVITELNOST OPRAVOVÁNÍ CHYB NA PRINCIPU HLEDÁNÍ „NEJBLIŽŠÍ" KÓDOVÉ ZNAČKY VE SMYSLU HAMMINGOVY VZDÁLENOSTI.

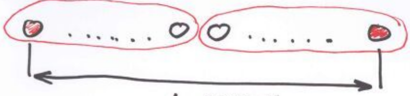
POKUD LZE „NEJBLIŽŠÍ" ZNAČKU URČIT JEDNOZNAČNĚ, LZE PŘIJATOU NEKÓDOVOU ZNAČKU OPRAVIT NA NALEZENOU NEJBLIŽŠÍ KÓDOVOU ZNAČKU.

POKUD JE „NEJBLIŽŠÍCH" ZNAČEK NĚKOLIK, NELZE PŘIJATOU NEKÓDOVOU ZNAČKU OPRAVIT.

KÓD K OPRAVUJE t-NÁSOBNÉ CHYBY, JESTLIŽE PŘI VYSLÁNÍ LIBOVOLNÉHO KÓDOVÉHO SLOVA $v \in K$ A PŘI LIBOVOLNÉ t-NÁSOBNÉ CHYBĚ MÁ PŘIJATÉ SLOVO $w \in T^n$ VZDÁLENOST $d(v,w)$ MENŠÍ, NEŽ VZDÁLENOST OD LIBOVOLNÉHO JINÉHO KÓDOVÉHO SLOVA.

$$d(v,w) < d(x,w) \quad \forall x \in K \quad x \neq v$$

OBECNĚ:



d_0 LICHÉ

KÓD OPRAVUJE λ-NÁSOBNÉ CHYBY

$$\forall \lambda \quad \lambda < d_0/2$$

d_0 SUDÉ

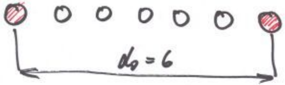
KÓD OPRAVUJE λ-NÁSOBNÉ CHYBY

$$\forall \lambda \quad \lambda < d_0/2$$

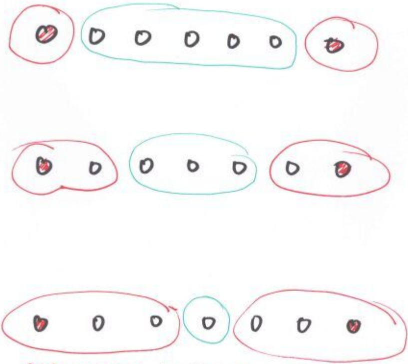
NEKÓDOVÁ KOMBINACE, KTEROU NELZE JEDNOZNAČNĚ OPRAVIT (STEJNÁ HAMMINGOVA VZDÁLENOST OD VÍCE KÓDOVÝCH ZNAČEK)

PŘÍJEMCE MŮŽE PŘI OBJEVOVÁNÍ/OPRAVOVÁNÍ CHYB VOLIT RŮZNÉ STRATEGIE.

PŘ:



RŮZNÉ STRATEGIE:



OPRAVUJE NEOPRAVUJE OPRAVUJE

DEKÓDOVÁNÍ: $\delta : T^m \to K$

„NEDĚLENÁ PŘIJATÁ KÓDOVÁ SLOVA"

$$\begin{cases} \delta(v_1 v_2 \dots v_n) = v_1 v_2 \dots v_n \\ \forall\, v_1 v_2 \dots v_n \in K \end{cases}$$

POKUD JE δ ÚPLNÁ (TOTÁLNÍ) FUNKCE, JEDNÁ SE O ÚPLNÉ DEKÓDOVÁNÍ.

POKUD JE δ JEN PARCIÁLNÍ FUNKCE, HOVOŘÍME O ČÁSTEČNÉM DEKÓDOVÁNÍ.

DEKÓDOVACÍ FUNKCE δ JEDNOZNAČNĚ DEFINUJE ROZKLAD MNOŽINY T^m

$\{K_1, K_2, \dots, K_{|K|}, K_{CH}\}$ KDE K_i JE MNOŽINA VŠECH SLOV Z T^m, KTERÉ OPRAVUJEME NA KÓDOVOU ZNAČKU v_i (VČETNĚ TÉTO ZNAČKY).

K_{CH} ... MNOŽINA VŠECH NEKÓDOVÝCH ZNAČEK, KTERÉ V DANÉ DEKÓDOVACÍ STRATEGII NEOPRAVUJE.

PŘÍKLAD (POKRAČOVÁNÍ „KÓDŮ NAVLÉKANÝCH NA n-ROZMĚRNOU KRYCHLI")

a) VYUŽÍVÁME-LI VŠECH 8 KOMBINACÍ, NEMÁ KÓD ŽÁDNÉ ZABEZPEČOVACÍ VLASTNOSTI, NEMÁ SMYSL.

b) $K = \{000, 011, 101, 110\}$

VZDÁLENOST LIBOVOLNÝCH KÓDOVÝCH ZNAČEK JE 2 => CHYBY NELZE OPRAVOVAT.

DEKÓDOVÁNÍ:

w	$\delta(w)$
000	000
001	×
010	×
011	011
100	×
101	101
110	110
111	×

ROZKLAD

$K_1 = \{000\}$

$K_2 = \{011\}$

$K_3 = \{101\}$

$K_4 = \{110\}$

$K_{CH} = \{001, 010, 100, 111\}$

c) w $\delta(w)$ ROZKLAD

w	$\delta(w)$
000	000
001	000
010	000
011	111
100	000
101	111
110	111
111	111

$K_{CH} = \emptyset$

$K_1 = \{000, 001, 010, 100\}$

$K_2 = \{011, 101, 110, 111\}$

PŘ: DEKÓDOVÁNÍ OPAKOVACÍHO BINÁRNÍHO KÓDU

$K = \{000000, 111111\}$

$\delta : \{0,1\}^6 \to \{000000, 111111\}$

MAJORITNÍ PRINCIP:

$\delta(w_1 w_2 \dots w_6) =$
- 000000 JSOU-LI VE ZNAČCE ALESPOŇ 4 NULY
- 111111 JSOU-LI VE ZNAČCE ALESPOŇ 4 JEDNIČKY

ČÁSTEČNÉ DEKÓDOVÁNÍ

INFORMAČNÍ A KONTROLNÍ ZNAKY

V NĚKTERÝCH KÓDU LZE ZNAKY VE ZNAČKÁCH ROZDĚLIT NA INFORMAČNÍ A KONTROLNÍ (ZABEZPEČOVACÍ).

INFORMAČNÍ ZNAKY LZE LIBOVOLNĚ VOLIT.
KONTROLNÍ ZNAKY JSOU PLNĚ URČENY VOLBOU INFORMAČNÍCH ZNAKŮ.

PŘ: KÓD CELKOVÉ KONTROLY PARITY DÉLKY 6

5 INFORMAČNÍCH

1 KONTROLNÍ

PŘÍKLAD ZNAČKY: $\underbrace{11001}_{\text{VOLITELNÉ}}\underline{1}$ SPOČÍTAT

LZE-LI Z n ZNAKŮ ZNAČKY k INFORMAČNÍCH ZNAKŮ VOLIT, MUSÍ EXISTOVAT PŘEDPIS, KTERÝ BUDE DEFINOVAT JAK SE K INFORMAČNÍ ČÁSTI ZJISTÍ KÓDOVÁ ZNAČKA – KÓDOVÁNÍ INFORMAČNÍ ČÁSTI

$$\varphi : T^k \to K$$

PŘESNĚJI:

$K \subseteq T^m$ JE BLOKOVÝ KÓD DÉLKY m. JESTLIŽE EXISTUJE PROSTÉ ZOBRAZENÍ $\varphi: T^k \to K$, ŘEKNEME, ŽE KÓD K MÁ k INFORMAČNÍCH ZNAKŮ A $m-k$ KONTROLNÍCH ZNAKŮ. ZOBRAZENÍ φ SE NAZÝVÁ KÓDOVÁNÍ INFORMAČNÍCH ZNAKŮ.

PŘÍKLADY:

OPAKOVACÍ KÓD DÉLKY 5 MÁ 1 INF. ZNAK A 4 KONTROLNÍ.

$$\varphi: T \to K \qquad \varphi(v) = vvvvv \quad \forall v \in T$$

PARITNÍ KÓD DÉLKY 4 MÁ 3 INF. ZNAKY A 1 ZNAK KONTROLNÍ

$$\varphi: T^3 \to K \qquad \varphi(v_1 v_2 v_3) = v_1 v_2 v_3 v_4$$

KDE $v_1 \oplus v_2 \oplus v_3 \oplus v_4 = 0$

$\forall\, v_1, v_2, v_3 \in T$

KÓD „2 Z 5" NEMÁ ODDĚLENÉ INFORMAČNÍ A KONTROLNÍ ZNAKY.

PROSTÉ ZOBRAZENÍ $\varphi : T^k \to K$ NEMŮŽE EXISTOVAT, PROTOŽE K MÁ 10 ZNAČEK A 10 NENÍ MOCNINOU 2.

TERMINOLOGICKÁ ZÁLUDNOST:

POJEM DEKÓDOVÁNÍ (VE SMYSLU „OPRAVA CHYBY") NENÍ INVERZNÍ POSTUP KE KÓDOVÁNÍ INFORMAČNÍCH ZNAKŮ.

JE TŘEBA ROZLIŠOVAT

$\varphi^{-1} : K \to T^k$ („VYKOPÁNÍ" INF. ZNAKŮ)

$\delta : T^n \to K$ (PŘÍPADNÁ OPRAVA PŘIJATÉ ZNAČKY)

CO SE DĚJE S PŘIJATOU ZNAČKOU w?

$$\varphi^{-1}(\delta(w))$$

OPRAVA CHYBY

„VYKOPÁNÍ" INFORMAČNÍCH ZNAKŮ.

JAK REALIZOVAT ?

KÓD MŮŽE BÝT (VČETNĚ DEKÓDOVACÍ STRATEGIE REPREZENTOVÁN TABULKAMI VYTVOŘENÝMI PODLE DEKÓDOVACÍHO ROZKLADU. KAŽDÉ KÓDOVÉ ZNAČCE v BUDE PŘIŘAZENA JEDNA TABULKA, V NÍŽ BUDOU VŠECHNY ZNAČKY Z T^n, KTERÉ BUDE PŘÍJEMCE NA v OPRAVOVAT. TABULKY BUDOU VYTVÁŘENY TAK, ŽE NA PRVNÍ POZICI BUDE KÓDOVÁ ZNAČKA v SAMA, NEKÓDOVÉ KOMBINACE DÁL BUDOU SEŘAZENY PODLE P-STI VÝSKYTU OD NEJVÝŠE PRAVDĚPODOBNÝCH PO NEJMÉNĚ PRAVDĚPODOBNÉ. TABULKY BUDOU PROHLEDÁVÁNY „CYKLICKY PROKLÁDANĚ", TJ. NEJDŘÍVE SE PŘIJATÁ ZNAČKA POROVNÁ SE VŠEMI KÓDOVÝMI ZNAČKAMI NA ČELECH TABULEK, PAK S NEKÓDOVÝMI ZNAČKAMI LIŠÍCÍMI SE V JEDNOM ZNAKU ATP.

NEVÝHODA TOHOTO PŘÍSTUPU: DOBA DEKÓDOVÁNÍ NENÍ KONSTANTNÍ, ZÁVISÍ NA PŘIJATÉ ZNAČCE.

SYSTEMATICKÉ KÓDOVÁNÍ JE TAKOVÉ, KDE JSOU INFORMAČNÍ ZNAKY VŽDY NA ZAČÁTKU ZNAČKY.

PŘESNĚJI:

BLOKOVÝ KÓD $K \subseteq T^n$ SE NAZÝVÁ SYSTEMATICKÝ, JESTLIŽE EXISTUJE ČÍSLO $k < n$ TAKOVÉ, ŽE

$$\forall\ \underbrace{v_1 v_2 \dots v_k} \in T^k\ \exists\ \underbrace{v_1 v_2 \dots v_k}\, v_{k+1} \dots v_n \in K$$

VÝHODA SYSTEMATICKÉHO KÓDOVÁNÍ:

„VÝPOČET" KONTROLNÍCH PRVKŮ MŮŽE PROBÍHAT SOUČASNĚ S ODESÍLÁNÍM INFORMAČNÍ ČÁSTI DO SDĚLOVACÍHO KANÁLU.

JEDNODUCHÁ REALIZACE ZOBRAZENÍ φ^{-1} (ODŘÍZNUTÍ ZABEZPEČOVACÍCH PRVKŮ).

DŮLEŽITÉ TVRZENÍ: MINIMÁLNÍ VZDÁLENOST SYSTEMATICKÉHO KÓDU K SPLŇUJE PODMÍNKU

$$d_0(K) \leq n - k + 1$$

PROČ?

ZVOLÍME LIBOVOLNĚ $k-1$ PRVNÍCH ZNAKŮ JAKO $v_1 v_2 \dots v_{k-1}$.

OZNAČÍME K' MNOŽINU VŠECH ZNAČEK Z K, KTERÉ MAJÍ PREFIX $v_1 v_2 \dots v_{k-1}$.

PAK $d_0(K') \leq n - (k-1)$

(PO VYNECHÁNÍ $k-1$ PRVKŮ JE STEJNÝCH)

PROTOŽE $K' \subseteq K$, JE $d_0(K) \leq d_0(K')$

(PŘIDÁVÁNÍM DALŠÍCH ZNAČEK KE K' SE MINIMÁLNÍ VZDÁLENOST NEMŮŽE ZVĚTŠIT)

Z $d_0(K) \leq d_0(K') \leq n - (k-1)$

PŘÍMO PLYNE

$$d_0(K) \leq n - k + 1$$

ZÁVĚR: PŘI VÝBĚRU BEZPEČNOSTNÍHO KÓDU SE SNAŽÍME O TO, ABYCHOM BYLI SCHOPNI PŘENÁŠET VELKÝ POČET INFORMAČNÍCH ZNAKŮ (VELKÉ k), NA DRUHÉ STRANĚ CHCEME BÝT SCHOPNI OBJEVOVAT A OPRAVOVAT HODNĚ CHYB (VELKÉ d_0). TYTO POŽADAVKY JSOU V ROZPORU => JE NUTNÝ KOMPROMIS. DŮLEŽITÝ JE ZPŮSOB OPRAVY CHYB (JEDNODUCHÉ ALGORITMY, HW REALIZACE, PRÁCE V REÁLNÉM ČASE).

KRITÉRIUM EFEKTIVITY KÓDOVÁNÍ - INFORMAČNÍ POMĚR

$$R = k/n$$

DEKÓDOVÁNÍ PŘIJATÉ ZNAČKY JE VLASTNĚ ROZHODOVÁNÍ O TOM, ZDA JE (PŘIJATÁ) n-TICE PRVKEM ZADANÉ MNOŽINY n-TIC, KTERÉ PŘEDSTAVUJÍ KOMBINACE, OPRAVOVANÉ NA JEDNU KONKRÉTNÍ KÓDOVOU ZNAČKU.

ÚLOHY TYPU „JE x PRVKEM MNOŽINY M?" ALE UMÍME ZA URČITÝCH PŘEDPOKLADŮ ŘEŠIT EFEKTIVNĚJI, NEŽ POROVNÁVÁNÍM SE VŠEMI PRVKY MNOŽINY M.

PŘ. Z GEOMETRIE (MOTIVACE):

DÁNA ROVINA ρ PROCHÁZEJÍCÍ POČÁTKEM SOUŘADNÉ SOUSTAVY.

JE DÁN BOD $X = (x_1, x_2, x_3)$.

JAK ROZHODNEME, ZDA PLATÍ

$$X \overset{?}{\in} \rho$$