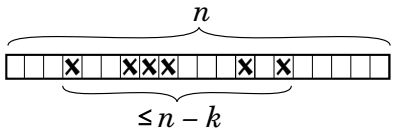
V prednáške sa budeme venovať špeciálnej metóde dekódovania cyklických kódov. Predpokladáme základné vedomosti o cyklických kódoch.

1 Error trapping dekódovanie

Error trapping dekódovanie („chytanie/lapanie“ chýb) je metóda dekódovania cyklických kódov. Vhodná je pri kódoch opravujúcich jednu, prípadne dve chyby a v situáciach, keď očakávame výskyt chýb na blízkych pozíciach v kódovom slove (tzv. burst chyby).

Počas celej prezenácie metódy budeme predpokladať, že K je cyklický (n, k) kód nad Z_2 opravujúci t chýb. Teda kódové slová v K majú dĺžku n a k informačných symbolov. Nech $g(x)$ je generujúci polynóm kódu K. Metóda funguje správne vtedy, ak je najviac t chýb rozmiestnených na najviac $n-k$ susedných pozíciach.



Nech $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ je polynóm nad Z_2. Označme $\mathrm{wt}(f(x)) = \sum_i a_i$ jeho váhu. Nech w je slovo s najviac t chybami. Potom platia nasledujúce tvrdenia.

Lema 1. *Ak je váha syndrómu slova w najviac t, tak chybový polynóm je rovný syndrómu.*

Dôkaz. Označme $s(x)$ syndróm a $e(x)$ príslušný chybový polynóm slova w. Potom platí:

$$s(x) = e(x) \bmod g(x).$$

Inak povedané, $e(x) = q(x)g(x) + s(x)$. Z predpokladu o počte chýb vo w vyplýva, že $\mathrm{wt}(e(x)) \leq t$. Navyše vieme, že $\mathrm{wt}(s(x)) \leq t$ (predpoklad lemy). Teda váha $e(x) - s(x)$ je najviac $2t$. Kód K opravuje t chýb, teda minimálna vzdialenosť ľubovoľných dvoch kódových slov je aspoň $2t + 1$. Keďže $e(x) - s(x)$ je kódové slovo (je to násobok generujúceho polynómu) s váhou najviac $2t$ a 0 je tiež kódové slovo, dostávame:

$$e(x) - s(x) = 0.$$

Odtiaľ bezprostredne vyplýva tvrdenie lemy. □

Lema 2. *Ak sú chyby na najviac $n-k$ susedných pozíciach, tak existuje cyklický posun w, ktorý má syndróm váhy najviac t.*

Dôkaz. Vezmime taký cyklický posun w, pre ktorý sú chyby „najviac vpravo“ (formálne, stupeň chybového polynómu pre príslušný cyklický posun je minimálny). Označme takýto posun w' a prislúchajúci chybový polynóm $e'(x)$. Podľa predpokladu lemy je $\deg(e'(x)) \leq n-k-1$, kde symbolom $\deg$ označujeme stupeň polynómu. Pre syndróm $s'(x)$ máme:

$$s'(x) = e'(x) \bmod g'(x).$$

Keďže $g(x)$ je generujúcim polynómom kódu K, $\deg(g(x)) = n - k$. Preto $s'(x) = e'(x)$. Po zohľadnení predpokladu o počte chýb vo w dostávame $\mathrm{wt}(s'(x)) \leq t$. □

Predchádzajúce dve lemy poskytujú teoretické zdôvodnenie pre error trapping dekódovanie cyklických kódov (samozrejme, pri splnení predpokladov o umiestnení chýb v dekódovanom slove w). Postupne skušame pre všetky rotácie w' slova w:

1. $s'(x) \leftarrow w'(x) \bmod g(x)$
2. ak $\mathrm{wt}(s'(x)) \leq t$ (podľa lemy 2):
   (a) oprav w': $w'(x) \leftarrow w'(x) + s'(x)$ (lema 1)
   (b) $w \leftarrow$ aplikuj „inverznú“ rotáciu na w'
   (c) koniec

Pod pojmom inverzná rotácia máme na mysli to, že ak sme w' dostali z w cyklickým posunom o p pozícií doľava, tak teraz opravené w' posunieme cyklicky o p pozícií doprava. Na konci dostaneme vo w opravené slovo.

Príklad. Uvažujme BCH kód $(15, 7)$ opravujúci 2 chyby, s generujúcim polynómom

$$g(x) = x^8 + x^7 + x^6 + x^4 + 1.$$

V tomto prípade bude error trapping metóda dekódovania úspešná pre tie dvojice chýb, ktoré sú od seba vzdialené (cyklicky) o najviac $15 - 7 = 8$ pozícií. A to sú všetky

Samozrejme, slová s jednou (alebo dokonca žiadnou) chybou dokáže error trapping dekódovať vždy.

Príklad. Uvažujme BCH kód $(15, 5)$ opravujúci 3 chyby, s generujúcim polynómom

$$g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

Vzdialenosť chýb musí byť v tomto prípade najviac $15 - 5 = 10$. Pre chyby váhy menšej ako 3 je podmienka triviálne splnená. Demonštrujme si príklad dokódovania na slove $w = 100000100010110$. Poznamenajme, že pri výpočtoch budeme polynómy reprezentovať ako vektory ich koeficientov (pre prehľadnejší zápis). Postupne rotujeme w doľava, počítame syndróm a hľadáme taký, ktorý má váhu najviac 3:

```
posun: 0                posun: 1
100000100010110         000001000101101
10100110111                  1000101101
  1001001100110
  10100110111
    11010111010
    10100110111
     1110001101

posun: 2                posun: 3
000010001011010         000100010110100
    10100110111             10100110111
      101101101               1011011010

posun: 4
001000101101000
  10100110111
    10110110100
    10100110111
       10000011
```

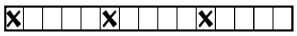
Váha syndrómu pre posun 4 je rovná 3. Takže môžeme opraviť slovo $w' = 001000101101000 \oplus 10000011 = 001000111101011$ a posunúť ho naspäť (o 4 pozície doprava). Teda opravené slovo w je:

$$101100100011110.$$

Urobme ešte skúšku správnosti, keď skúsime vydeliť toto slovo generujúcim polynómom (pre kódové slovo očakávame zvyšok 0):

```
101100100011110
10100110111
   101001101110
   10100110111
              0
```

V prípade BCH $(15, 5)$ kódu môže nastať práve päť rozmiestnení 3 chýb, keď tieto neležia v úseku dĺžky 10. Jedno rozmiestnenie je nakreslené na nasledujúcom obrázku, ostatné sú jeho cyklickými posunmi.



Pravdepodobnosť, že takáto situácia nastane pri náhodnej voľbe práve 3 chýb je $5/\binom{15}{3} \sim 0,011$.