KODY KORYGUJĄCE BŁĘDY

1. MOTYWACJE

A) OGRANICZENIA NOŚNIKA POWODUJĄ, ŻE CZASAMI ILOŚĆ BŁĘDÓW JEST DUŻA,

B) CZASAMI NIE MOŻEMY SOBIE POZWOLIĆ NA RETRANSMISJĘ (KOMUNIKACJA JEDNOSTRONNA),

C) CZASAMI NOŚNIK MOŻE ULEGAĆ DEGRADACJI WRAZ Z CZASEM,

D) PRZYKŁADY:

- DYSKI KOMPAKTOWE,
- KOMUNIKACJA Z SONDAMI KOSMICZNYMI.

2. PODSTAWOWE DEFINICJE

- $(n, k, d)_q$ – KOD TO PODZBIÓR $C \in \Sigma^n$
  - n – DŁUGOŚĆ BLOKU/PAKIETU DANYCH
  - $k = \log_q |C|$ – ILOŚĆ INFORMACJI UMIESZCZONA W ZAKODOWANYM PAKIECIE
  - d – MINIMALNA ODLEGŁOŚĆ MIĘDZY KODAMI C
  - $q = |\Sigma|$ – ROZMIAR ALFABETU

- ODLEGŁOŚĆ HAMMINGA MIĘDZY $\vec{x}(x_1, \ldots, x_n)$ A $\vec{y}(y_1, \ldots, y_n)$ TO LICZBA POZYCJI, NA KTÓRYCH $\vec{x}$ RÓŻNI SIĘ OD $\vec{y}$. OZN. $\Delta(\vec{x}, \vec{y})$

- MINIMALNA ODLEGŁOŚĆ MIĘDZY KODAMI C

$$\Delta(C) = \min_{\vec{x} \neq \vec{y} \in C} \Delta(\vec{x}, \vec{y})$$

- KODY LINIOWE $[n,k,d]_q$: GDY C PODPRZESTRZEŃ LINIOWA $GF(q)^n$ (CIAŁA SKOŃCZONEGO O CHAR. q PODNIESIONEGO DO n-TEJ POTĘGI)

3. PRZYKŁADY

A) IDENTYCZNOŚĆ DAJE $[n,n,1]_q$ KOD

B) $[n,n-1,2]_q$ KOD DOSTAJEMY PRZEZ

$$(x_1,\dots,x_{n-1}) \longmapsto (x_1,\dots,x_{n-1},\sum_{i=1}^{n-1} x_i)$$

C) KODY REEDA-SOLOMONA ($[n,k,n-k+1]_q$ KODY)

- USTALAMY n RÓŻNYCH ELEMENTÓW $GF(q)$: $a_1,\dots,a_n$
- DLA DANEGO KOMUNIKATU $m=(m_0,\dots,m_{k-1})$ TWORZYMY WIELOMIAN

$$m(x)=\sum_{i=0}^{k-1} m_i x^i$$

(KTÓRY MOŻNA TRAKTOWAĆ JAK WEKTOR O k WSPÓŁRZĘDNYCH)

- KODUJEMY:

$$(m_0,\dots,m_{k-1}) \longmapsto (m(a_1),\dots,m(a_n))$$

- IDEOLOGIA: PRZY ODTWARZANIU m WYBIERAMY WIELOMIAN STOPNIA $k-1$ NAJBLIŻSZY WIELOMIANOWI STOPNIA $n-1$, JAKI OTRZYMALIŚMY (UWAGA: TO JEST NP-ZUPEŁNE)
- WYDAJNOŚĆ: ISTNIEJĄ ALGORYTMY OBLICZAJĄCE POWYŻSZE W CZASIE $O_q(k^3)$ (A NAWET $O_q(k^{2,3\dots})$ — W GRANICACH ZNANYCH OGR. NA MNOŻENIE MACIERZY), PRZY ZAŁOŻENIU, ŻE UZYSKALIŚMY BEZBŁĘDNĄ ODPOWIEDŹ.

D) KODY REEDA - MÜLLERA

IDEA: UŻYJMY WIELOMIANÓW WIELU ZMIENNYCH

ZYSK: NIE MUSIMY ZAKŁADAĆ, ŻE $q \geq n$

DLACZEGO: l RÓŻNYCH ZMIENNYCH POZWALA NA KODOWANIE l RÓŻNYCH WSPÓŁRZĘDNYCH O ROZMIARACH q KAŻDA.

4. ZASTOSOWANIE: CIRC

CROSS-INTERLEAVED REED-SOLOMON CODING

- KODY REEDA-SOLOMONA KORYGUJĄ DO $\frac{n-k}{2}$ BŁĘDÓW
- NP.: KOD RS $[255, 223, \bullet]$. DLA BAJTÓW KORYGUJE DO 16×8 BŁĘDÓW BITOWYCH
- CIRC
  1. NAJPIERW BIERZEMY 24 ÓSMIOBITOWE SŁOWA
  2. KODUJEMY JE RS(28, 24) – KOREKCJA 2 SYMBOLI
  3. ROZPRASZAMY WYNIK POŚRÓD 108 RAMEK
  4. KODUJEMY WYNIK RS(28, 32) – KOREKCJA 2 SYMBOLI
  5. ROZPRASZAMY WYNIK POŚRÓD 108 RAMEK
- 108 RAMEK KORYGUJE 4 36 BŁĘDÓW; PRZY ROZPRASZANIU 13 625 RAMEK MOŻNA POPRAWIĆ
- RS(28, 24) – KODOWANIE POZIOMU C2 KORYGUJE BŁĘDY NAGRANIA I FIZYCZNEGO STANU DYSKU
- RS(32, 28) – KODOWANIE POZIOMU C1 KORYGUJE BŁĘDY Z ODCISKÓW PALCÓW I ZARYSOWAŃ

5. OGRANICZENIA NA KODY

- PODSTAWOWE OGRANICZENIE TEORIOINFORMACYJNE NA $(n, k, d)_q$ KODY:

$$q^k \cdot \mathrm{Vol}_q\left(\left\lfloor \frac{d-1}{2} \right\rfloor, n\right) \leq q^n$$

q^k – LICZBA KUL; Vol_q – ODLEGŁOŚĆ KULI; $\left\lfloor \frac{d-1}{2} \right\rfloor$ – PROMIEŃ KULI; n – WYMIAR KULI; q^n – ROZMIAR PRZESTRZENI ZAPISÓW Σ^n

- OGRANICZENIE SINGLETONA (SINGLETON TO NAZWISKO) DLA $(n, k, d)_q$ KODÓW ZACHODZI

$$d \leq n - k + 1$$

- OGRANICZENIE PLOTKINA

1) JEŚLI $(n, k, d)_2$ KOD SPEŁNIA $d \geq \frac{n}{2}$, TO

$$k \leq \log_2 2n$$

2) KAŻDY $(n, k, d)_2$ KOD SPEŁNIA

$$k \leq n - 2d + \log_2(4d)$$

- OGRANICZENIE GILBERTA – WARSHAMOWA

$$\underset{0<\delta<\frac{1}{2}}{\forall} \; \underset{\varepsilon>0}{\forall} \; \underset{N}{\exists} \; \underset{n>N}{\forall}$$

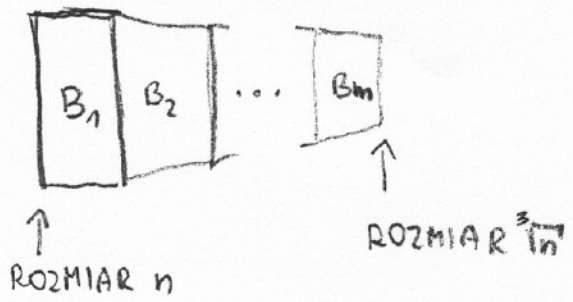
ISTNIEJE $[n, n(1-H(\delta)-\varepsilon), \delta n]_q$ KOD

$$(H(\delta) = -(\delta \log_2 \delta + (1-\delta)\log_2(\delta)))$$

6. KODY LINIOWO DEKODOWALNE

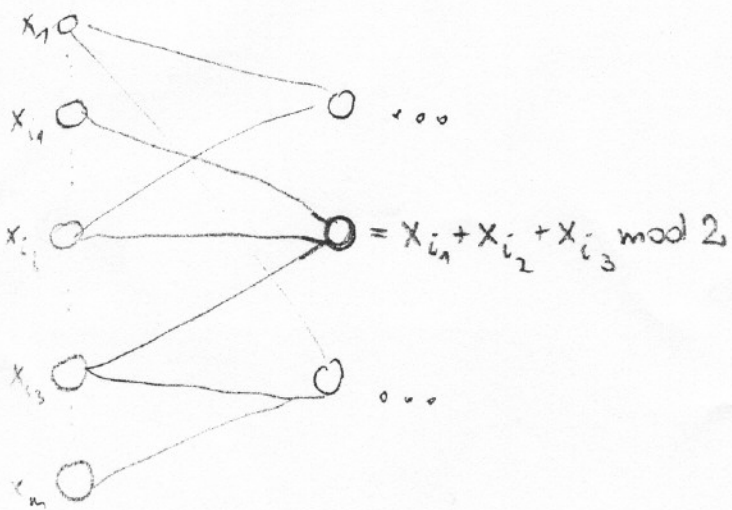
A) GŁÓWNA IDEA

ŁĄCZYMY ZE SOBĄ BLOKI:



KAŻDY BLOK B_i DLA $i=1,\dots,m$ TO GRAF DWUDZIELNY (L_i, R_i, E_i)

PODSTAWOWA IDEA ZWIĄZANA Z B_i:



KODOWANIE:

1. DLA KOLEJNYCH BLOKÓW $B_1, \dots, B_m$ WYPROWADŹ Z WARTOŚCI W WIERZCHOŁKACH L_i WARTOŚCI W WIERZCHOŁKACH R_i PRZEZ DODAWANIE mod 2
2. DLA R_m ZASTOSUJ TRADYCYJNĄ TECHNIKĘ NP.: KODOWANIE REEDA-SOLOMONA

ODKODOWYWANIE: Z PRAWA NA LEWO; DOPÓKI ISTNIEJE X_L TRZEBA WIĘCEJ NIESPEŁNIONYCH PRAWYCH WĘZŁÓW NIŻ SPEŁNIONYCH, ODWRÓĆ WARTOŚĆ TAKIEGO X_L.

B) GŁÓWNY PROBLEM

JAKĄ STRUKTURĘ POWINNY MIEĆ BLOKI B_i?

C) BLOKI DETERMINISTYCZNE

DEF 1.

GRAF DWUDZIELNY $B=(L,R,E)$ JEST (d_L,d_R)-OGRANICZONY, JEŚLI WIERZCHOŁKI W L MAJĄ STOPIEŃ OGRANICZONY PRZEZ d_L, ZAŚ WIERZCHOŁKI W R MAJĄ STOPIEŃ OGRANICZONY PRZEZ d_R.

GRAF J.W. JEST (d_L,d_R)-REGULARNY, JEŚLI WIERZCHOŁKI W L MAJĄ STOPIEŃ DOKŁADNIE d_L, ZAŚ WIERZCHOŁKI W R MAJĄ STOPIEŃ DOKŁADNIE d_R.

DEF 2.

GRAF $B=(L,R,E)$ JEST (α,δ) EKSPANDEREM JEŚLI DLA WSZYSTKICH $S\subseteq L$ $(|L|=n)$, TAKICH ŻE $|S|<\delta n$ ZACHODZI $|\partial(S)|\geq\alpha|S|$, GDZIE $\partial(S)=\{r\in R \mid \exists s\in S,\ (s,r)\in E\}$.

TWIERDZENIE:

JEŚLI $G=(L,R,E)$ JEST (d_L,d_R) OGRANICZONY ORAZ (α,δ) EKSPANDEREM, TO KODY UZYSKANE Z G PRZEZ KONKATENACJĘ WARTOŚCI BITÓW Z L I R MAJĄ ODLEGŁOŚĆ $\frac{2\alpha\delta}{d_L}$ O ILE $2\alpha>d_L$.

UWAGA: (d_L,d_R) OGRANICZONY EKSPANDER MA $\alpha\leq d_L$

TWIERDZENIE

JEŚLI $G=(L,R,E)$ JEST (d_L,d_R) OGRANICZONY ORAZ (α,δ) EKSPANDEREM ORAZ $\alpha>\frac{3}{4}d_L$ TO KOD KORYGUJE DO $\left(\frac{2\alpha-d_L}{d_L}\cdot\delta\right)n$ BŁĘDÓW W CZASIE LINIOWYM.

ZŁE WIEŚCI: NIE MA JAWNYCH KONSTRUKCJI (d_L, d_R) OGRANICZONYCH EKSPANDERÓW DLA $\alpha > \frac{3}{4} d_L$

DOBRE WIEŚCI: LOSOWE (d_L, d_R) REGULARNE GRAFY MAJĄ Z DUŻYM PRAWDOPODOBIEŃSTWEM $\alpha > \frac{3}{4} d_L$

DLA GRAFÓW LOSOWYCH MOŻNA OKREŚLIĆ WEKTORY

$$(\lambda_1, \ldots, \lambda_{d_L}) \qquad (\rho_1, \ldots, \rho_{d_R})$$

λ_i – PRAWDOPODOBIEŃSTWO, ŻE WIERZCHOŁEK PO LEWEJ MA STOPIEŃ i

ρ_i – PRAWDOPODOBIEŃSTWO, ŻE WIERZCHOŁEK PO PRAWEJ MA STOPIEŃ i

OPTYMALNE ROZKŁADY: $\lambda_i \propto \frac{1}{i^2}$

$\rho_i \propto \frac{\alpha^i}{i!}$