Matematyka dyskretna

Wykład 7: Kody korygujące błędy

Gniewomir Sarbicki

Błędy transmisji i kodowanie nadmiarowe

Zakładamy, że przy pewnym małym prawdopodobieństwie ϵ przy transmisji bit zmienia wartość. Kanał jest bez pamięci, czyli zmiany wartości kolejnych bitów są od siebie niezależne. Podobnie, przy przechowywaniu informacji na nośniku może zajść z małym prawdopodobieństwem zamiana wartości bitu.

Możemy dowolnie zmniejszyć prawdopodobieństwo błędu w przekazie informacji przez **kodowanie nadmiarpwe** - do kodowania informacji używamy tylko podzbioru możliwych sekwencji znaków z alfabetu (bitów).

Przykład: Słowo *nadmiarpwe* bez problemu odczytujemy jako *nadmiarowe*

Przykład

Przykład: Kodujemy 0 jako 000 a 1 jako 111.

Trójkę dekodujemy jako 0 gdy ma więcej zer i jako 1 gdy ma więcej jedynek.

Przeskoczenie jednego bitu wygeneruje sekwencje $001, 010, 100, 110, 101, 011$, które bez trudu możemy poprawić. Błąd popełnimy dopiero, gdy przynajmniej dwa bity z trzech zmienią wartość.

Prawdopodobieństwo błędu zmniejszyło się z $\epsilon(3 - 3\epsilon + \epsilon^2) \approx 3\epsilon$ do $\epsilon^2(3 - 2\epsilon) \approx 3\epsilon^2$.

Kodowanie przez powtarzanie

Definicja: (Odległość Hamminga)

Odległością Hamminga dwóch elementów w $\mathbb{F}_q^n$ nazywamy funkcję:

$$d(x,y) = \#\{i : x_i \neq y_i\}$$

Fakt:

Funkcja $d : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{N}$ jest **metryką**, tzn. spełnia trzy warunki:

- $\forall x, y \; d(x,y) \geqslant 0 \wedge (d(x,y) = 0 \iff x = y)$
- $\forall x, y \; d(x,y) = d(y,x)$ - symetryczność
- $d(x,y) + d(y,z) = d(x,z)$ - nierówność trójkąta

Dowód: Ćwiczenie

Definicja: (Kula domknięta)

Kulą domkniętą (w metryce Hamminga) o promieniu r i środku w x_0 nazywamy zbiór:

$$B(C,r) = \{x : d(x,x_0) \leqslant r\}$$

Definicja: (Kod)

Kodem długości n nad $\mathbb{F}_q$ nazywamy zbiór $C \subset \mathbb{F}_q^n$ (zbiór słów kodowych).

Definicja: (Dekodowanie)

Dekodowanie słowa $s \in \mathbb{F}_q^n$ polega na znalezieniu najbliższego słowa kodowego

Definicja: (minimalna odległość kodu)

minimalna odległość kodu to odległość pomiędzy najbliższymi słowami kodowymi:

$$d_{min}(C) = \min\{d(x, y) : x, y \in C\}$$

Definicja: (Wykrywanie i korekcja)

- Mówimy, że kod $C \subset \mathbb{F}_q^n$ **wykrywa** t błędów, jeżeli odległość Hamminga dowolnych dwóch słów kodowych jest większa od t.
- Mówimy, że kod $C \subset \mathbb{F}_q^n$ **koryguje** r błędów, jeżeli dla każdego słowa $y \in \mathbb{F}_q^n$ istnieje co najwyżej jedno słowo kodowe $x \in C$ takie że $d(x, y) \leqslant r$.

Twierdzenie:

Kod o minimalnej długości d wykrywa $d - 1$ błędów i koryguje $\lfloor (d-1)/2 \rfloor$ błędów

Dowód: Ćwiczenie

Jak zbudować kod o danej mocy $\#C$ i maksymalnej odległości minimalnej?

Twierdzenie: (Ograniczenie Hamminga)

Jeżeli kod $C \subset \mathbb{F}_q^n$ koryguje r błędów, to

$$\#C\left(1+(q-1)\binom{n}{1}+\cdots+(q-1)^r\binom{n}{r}\right) \leqslant q^n$$

Dowód: Wyrażenie w nawiasie to ilość elementów w kuli o promieniu r

Fakt: (ograniczenie Singletona)

Dla kodu $C \subset \mathbb{F}_q^n$ o min. odległości d zachodzi $\#C \leqslant q^{n-d+1}$

Definicja:

Kody dla których zachodzi równość nazywamy MDS (*Maximum Distance Separable*)

Definicja: (kod liniowy i wymiar kodu)

- Jeżeli $C \subset \mathbb{F}_q^n$ jest podprzestrzenią liniową przestrzeni $\mathbb{F}_q^n$, to kod C nazywamy **kodem liniowym**.
- Wymiar podprzestrzeni C nazywamy **wymiarem kodu**.

Definicja: (macierz kontroli parzystości)

Macierz H_C rzędu $n-k$ spełniająca warunek:
$\forall x \in C \quad H \cdot x = 0$
nazywamy **macierzą kontroli parzystości** kodu C o wymiarze k.

Definicja: (macierz generująca)

Macierzą generującą kodu C o wymiarze k nazywamy dowolną macierz G rzędu k spełniającą warunek $H_C \cdot G^T = 0$

Wiersze macierzy G tworzą bazę przestrzeni C, a wiersze macierzy H bazę jej dopełnienia ortogonalnego.

Przykład: Niech $G = [I_k, A]$. Wtedy $H = [-A^T, I_{n-k}]$. Kod taki nazywamy *kodem systematycznym*.

Dekodowanie kodu liniowego

$w = Hy$ nazywamy **syndromem** słowa y.

Inicjalizacja:

1. Dla każdego możliwego słowa wyznaczamy najbliższe słowo kodowe - generujemy słownik dekodujący
2. Rozbijamy słownik na mniejsze słowniki grupujące klucze o tym samym syndromie - tworzymy słownik przypisujący syndromowi jego słownik dekodujący

Dekodowanie:

Dla przychodzącego słowa znajdujemy syndrom i dekodujemy je przy pomocy odpowiadającego mu słownika dekodującego.

Definicja: (kod cykliczny)

Kod liniowy nazywamy cyklicznym, jeżeli dla każdego słowa kodowego $y = (a_0, \ldots, a_{n-1})$ słowo $y' = (a_{n-1}, a_0, \ldots, a_{n-2})$ jest również słowem kodowym.

Poprzez odwzorowanie $(a_0, \ldots, a_{n-1}) \to a_0 + a_1 X + \ldots a_{n-1} X^{n-1}$ można utożsamić przestrzeń liniową $\mathbb{F}_q^n$ z pierścieniem wielomianów $\mathbb{F}[X]/(X^n - 1)$. Mnożenie w pierścieniu przez X odpowiada przesunięciu cyklicznemu.

Fakt:

- $y(X) \in C \iff X \cdot y(X) \in C$
- $y(X) \in C \iff \forall r(X) \in \mathbb{F}[X]/(X^n - 1) \quad r(X) \cdot y(X) \in C$

Twierdzenie: (O istnieniu generatora)

Niech $C \subset \mathbb{F}[X]/(X^n - 1)$ będzie kodem cyklicznym wymiaru k. Istnieje dokładnie jeden wielomian $g \in \mathbb{F}[X]/(X^n - 1)$ o własnościach:

- $C = \{f \cdot g | f(X) \in \mathbb{F}[X]/(X^n - 1)\}$
- $\deg g = n - k$

Wielomian g dzieli wielomian $X^n - 1$. Wielomian ten nazywamy **generatorem kodu** C.

Dowód: Bez dowodu.

Wniosek: Tyle jest kodów cyklicznych nad $\mathbb{F}_q$ długości n i wymiaru k ile wielomian $X^n - 1$ nad ciałem $\mathbb{F}_q^n$ ma dzielników stopnia $n - k$.

Przykład: Sprawdźmy, że w pierścieniu $\mathbb{Z}_2[X]$ wielomian $x-1$ dzieli wielomian x^3-1.

Sprawdźmy, co jest wynikiem mnożenia wielomianów z $\mathbb{Z}_2[X]/(X^3-1)$ przez $x-1$:

000	$\rightarrow$	0	$\rightarrow$	0	$\rightarrow$	000
001	$\rightarrow$	1	$\rightarrow$	$x+1$	$\rightarrow$	011
010	$\rightarrow$	x	$\rightarrow$	x^2+x	$\rightarrow$	110
011	$\rightarrow$	$x+1$	$\rightarrow$	x^2+1	$\rightarrow$	101
100	$\rightarrow$	x^2	$\rightarrow$	x^2+1	$\rightarrow$	101
101	$\rightarrow$	x^2+1	$\rightarrow$	x^2+x	$\rightarrow$	110
110	$\rightarrow$	x^2+x	$\rightarrow$	$x+1$	$\rightarrow$	011
111	$\rightarrow$	x^2+x+1	$\rightarrow$	0	$\rightarrow$	000

Widzimy, że uzyskany kod jest kodem cyklicznym.
$\deg(x+1) = n-k = 3-2$. Wymiarem kodu jest 2. Rzeczywiście, $2^2 = 4$, tyle ile słów kodowych.

Ćwiczenie: Sprawdź że w $\mathbb{Z}_2[X]$ x^2+x+1 jest dzielnikiem x^3-1 i sprawdź jaki kod on generuje.

Twierdzenie: (macierz kontroli parzystości kodu cyklicznego)

Niech $g(X) = g_{n-k}X^{n-k} + g_{n-k-1}X^{n-k-1} + \dots g_1 X + g_0$ będzie generatorem kodu cyklicznego o wymiarze k.
Zdefiniujmy $h(X) = h_0 + h_1 X + \cdots + h_k X^k = (X^n - 1)/g(X)$.
Wówczas macierz

$$\begin{bmatrix} h_0 & h_1 & \cdots & h_k & 0 & \cdots & 0 \\ 0 & h_0 & h_1 & \cdots & h_k & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_k \end{bmatrix}$$

jest macierzą kontroli parzystości kodu C

Dowód: Ćwiczenie

Definicja: (kod RS)

Niech q - potęga liczby pierwszej i A - n-elementowy różnowartościowy ciąg elementów $\mathbb{F}_q$. Dla $k < n$ kod $\{f(A) : \deg f < k\} \subset \mathbb{F}_q^n$ nazywamy **kodem Reeda-Solomona**.

Twierdzenie: (własności kodu RS)

- Kod RS jest kodem wymiaru k
- Kod RS jest kodem MDS

Dowód: Każdy wielomian prowadzi do innego słowa kodowego $\implies \#C = q^k$

Dwa różne wielomiany stopnia $< k$ mogą mieć co najwyżej $k-1$ punktów wspólnych $\implies d_{min} \geqslant n-k+1$

Istnieją dwa wielomiany dla których punktów wspólnych jest dokładnie $k-1 \implies d_{min} \leqslant n-k+1$.

Minimalna odległość kodu wynosi zatem $n-k+1$

$q^{n-d_{min}+1} = q^k = \#C$, więc kod jest kodem MDS $\square$

Uwaga: Dla odpowiedniego wyboru ciągu A kod RS jest cykliczny.