Matematyka Dyskretna — Lista zadań 4

M. Michalski, 21.04.2021

1. Dany jest binarny kod blokowy typu (n, k). Jaka powinna być minimalna odległość między jego słowami kodowymi, aby kod ten

a) wykrywał przekłamania na 1, 2 lub 3 bitach
b) korygował przekłamania na 1, 2 lub 3 bitach

2. Zdolność detekcyjna kodu wynosi 3. Jaka musi być minimalna odległość jego słów kodowych i jaka jest zdolność korekcyjna tego kodu? Odpowiedz na to samo pytanie dla zdolności detekcyjnej 4 i 5.

3. Zdolność korekcyjna kodu wynosi 1. Jaka musi być minimalna odległość jego słów kodowych i jaka jest zdolność detekcyjna tego kodu? Odpowiedz na to samo pytanie dla zdolności korekcyjnej 2 i 3. (W każdym przypadku możliwe są 2 odpowiedzi).

4. Korekta t przekłamanych bitów w binarnym kodzie blokowym typu (n, k) jest możliwa, jeśli n spełnia nierówność

$$2^{n-k} \;\geq\; \sum_{p=0}^{t} \binom{n}{p}.$$

Jak duże musi być n, aby przy przesyłaniu $k = 4$ użytkowych bitów możliwa była korekta $t = 1, 2$ lub odpowiednio 3 bitów? Znajdź podobne oszacowania dla n, gdy $k = 6$.

5. Przesyłamy 32-bitowe słowa kodowe przez zaszumione łącze. Ile bitów użytkowych można zakodować w tych słowach jeśli przewidujemy korektę a) jednego, b) dwóch przekłamanych bitów?

6. Wypisz wszystkie słowa kodowe liniowego kodu cyklicznego nad $\mathbb{Z}_2$ generowanego przez

$$\text{a) } \boldsymbol{x} = [1, 1, 0, 0]\,, \qquad \text{b) } \boldsymbol{x} = [1, 0, 0, 1, 1]\,.$$

Jakie są wymiary przestrzeni słów kodowych w każdym z tych przypadków? Jakie są mininalne odległości między słowami kodowymi w tych przestrzeniach? Jakie są ich zdolności detekcyjne i korekcyjne?

7. Tak jak w poprzednim zadaniu, lecz tym razem rozpatrujemy przestrzenie kodów nad $\mathbb{Z}_3$ generowane przez a) $[1, 2, 0]$, b) $[1, 1, 0, 2]$.

8. Zbuduj macierz kodową $\boldsymbol{C}$ i macierz syndromu $\boldsymbol{S}$ dla binarnego kodu blokowego (7,4), w którym bity użytkowe stoją na pozycjach $1-4$, natomiast pozycje $5-7$ to bity parzystości:

$$b_5 = b_2 + b_3 + b_4, \qquad b_6 = b_1 + b_3 + b_4, \qquad b_7 = b_1 + b_2 + b_4\,.$$

9. Dla kodu z poprzedniego zadania oblicz sygnalizowane wartości syndromu, gdy przekłamaniu ulegnie a) pojedynczy bit $b_1 - b_7$, b) dwa bity jednocześnie, np. b_3 i b_5 oraz b_1 i b_7, c) trzy bity jednocześnie, np. b_1, b_2 i b_3 oraz b_1, b_4 i b_7.

10. Rozwiąż powtórnie zadania 8 i 9 korzystając innej z macierzy syndromu

$$\boldsymbol{S} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Należy najpierw przekonać się, że istotnie jest to macierz syndromu dla macierzy $\boldsymbol{C}$ uzyskanej w zad. 8. Zwróć uwagę, że wartości syndromu wskazują teraz bezpośrednio numer pojedynczego przekłamanego bitu.

11. Utożsamiamy przestrzeń liniową $\mathbb{F}_2^n$ z pierścieniem ilorazowym wielomianów $\mathbb{K} = \mathbb{F}_2[X]/(X^n - 1)$ przez odwzorowanie

$$[b_0, b_1, \ldots, b_{n-2}, b_{n-1}] \qquad \leftrightarrows \qquad p(X) \;=\; b_0 \;+\; b_1 X \;+\; \cdots \;+\; b_{n-2} X^{n-2} \;+\; b_{n-1} X^{n-1}\,.$$

Wówczas różne podprzestrzenie kodów cyklicznych w $\mathbb{F}_2^n$ odpowiadają ideałom wyznaczonym przez podzielniki $g(X)$ wielomianu $X^n - 1$:

$$V_g \;=\; \big\{\, g(X)\cdot p(X) \pmod{X^N - 1} \;:\quad p(X) \in \mathbb{F}_2[X] \,\big\}\,.$$

Dalej, jeśli $s(X)\cdot g(X) = X^N - 1$ (to znaczy, gdy $s(X) = (X^N - 1)/g(X)$), wielomian $s(X)$ pełni rolę syndromu dla tego kodu, bowiem dla dowolnego słowa kodowego $u(X) \in V_g$ mamy

$$s(X)\cdot u(X) \;=\; s(X)\cdot g(X)\cdot p(X) \;=\; (X^N - 1)\cdot p(X) \;=\; 0 \pmod{X^N - 1}\,.$$

Jeśli jednak zamiast tego $u(X) \notin V_g$, to jest $u(X) \neq g(X)\cdot p(X)$ dla jakiegokolwiek $p(X)$, wówczas $s(X)\cdot u(X) \neq 0 \pmod{X^n - 1}$. Dla następujących wielomianów $g(X) \in \mathbb{F}_p[X]$ oraz liczby n należy sprawdzić, że istotnie $g(X)$ jest podzielnikiem $X^n - 1$, a następnie wyznaczyć przestrzeń słów kodowych V_g oraz macierze kodującą $\boldsymbol{C}$ rozmiaru $n \times (n-k)$ i syndromu $\boldsymbol{S}$ rozmiaru $k \times n$, gdzie k jest stopniem wielomianu $g(X)$.

(a) $g(X) = X^2 + 1$, $n = 4$, nad $\mathbb{F}_2$

(b) $g(X) = X^2 + 1$, $n = 4$, nad $\mathbb{F}_3$

(c) $g(X) = X^2 + 4X + 3$, $n = 4$, nad $\mathbb{F}_5$

(d) $g(X) = X^2 + X + 1$, $n = 6$, nad $\mathbb{F}_2$

(e) $g(X) = X^2 + 1$, $n = 6$, nad $\mathbb{F}_2$

(f) $g(X) = X^3 + X + 1$, $n = 7$, nad $\mathbb{F}_2$