TPI – 13
Kody liniowe, poprawianie błędów

Zadania domowe, przygotowujące do kartkówki

ZOT jest nieobowiązkowy; zainteresowani oddają na ćwiczeniach jego pisemne rozwiązanie.

We wszystkich zadaniach Q oznacza ciało skończone. Można bez dowodu korzystać z faktu, że Q^n (ze standardowymi operacjami na wektorach) jest przestrzenią liniową nad Q. Można też korzystać z faktu, że moc ciała skończonego jest potęgą liczby pierwszej.

A1. Podaj przykład kodu $C \subseteq \mathbb{F}_3^5$ (wypisując wszystkie jego słowa), który

(a) jest linowym kodem wymiaru 2.
(b) jest liniowy i ma dokładnie 9 słów.
(c) jest kodem $[5, 2]$, o rozstępie 2.

A2.

(a) Ile elementów ma kod binarny długości 10, wymiaru 3?
(b) Ile elementów ma kod długości n, wymiaru k, nad ciałem Q, jeżeli $|Q| = q$?
(c) Ile elementów może liczyć ciało Q, jeżeli pewien kod liniowy nad tym ciałem składa się z 49 słów? Podaj wszystkie możliwości.
(d) Jaki może być wymiar kodu liniowego składającego się z 16 słów? Podaj wszystkie możliwości.

A3. Wypisz wszystkie słowa kodu liniowego nad ciałem $\mathbb{F}_3$, o poniższej macierzy generującej.

$$\text{(a)} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 2 & 1 & 1 & 1 \end{bmatrix} \quad \text{(b)} \begin{bmatrix} 1 & 2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 \end{bmatrix}.$$

A4. Dany jest kod C składający się ze słów: $(0, 1, 0, 1)$, $(1, 0, 1, 1)$, $(0, 0, 0, 0)$, $(1, 1, 1, 0)$.

(a) Czy C jest kodem liniowym, gdy rozpatrujemy go nad ciałem $\mathbb{F}_2$?
(b) Czy jest liniowy gdy rozpatrujemy go jako kod nad ciałem $\mathbb{F}_5$?

Jeśli odpowiedź na którekolwiek z tych pytań jest twierdząca, znajdź przykładową macierz generującą tego kodu.

A5. Macierz generująca kodu C nad ciałem $\mathbb{F}_5$ ma postać $G = \begin{bmatrix} 1 & 0 & 4 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$.

(a) Jaki jest wymiar kodu C?
(b) Ile słów należy do kodu C?
(c) Znajdź przykładową macierz parzystości dla kodu C.
(d) Korzystając z macierzy parzystości, sprawdź, które ze słów $(1, 2, 1, 2), (3, 3, 3, 3), (1, 2, 3, 4)$ należą do tego kodu. Przedstaw każde z (podanych) słów należących do C jako kombinację liniową wierszy macierzy G.

A6. Macierz parzystości kodu C nad ciałem $\mathbb{F}_5$ ma postać $H = \begin{bmatrix} 2 & 3 & 4 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{bmatrix}$.

(a) Sprawdź, które ze słów $(4, 1, 3, 3, 3), (1, 1, 2, 2, 2), (1, 2, 3, 1, 2)$ należą do kodu C.
(b) Dla każdego z powyższych słów, które do C nie należą, znajdź wszystkie najbliższe mu słowa kodu C.
(c) Jaki jest wymiar kodu C? Ile słów ma kod?
(d) Znajdź przykładową macierz generującą dla kodu C.

A7. Macierz parzystości kodu C binarnego ma postać

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

(a) Znajdź przynajmniej jedno słowo kodu najbliższe słowu $y = (0, 1, 0, 1)$.
(b) Znajdź przynajmniej jedno słowo kodu najbliższe słowu $z = (1, 1, 1, 0)$.

A8. Wygeneruj macierz parzystości dla kodu Hamminga nad ciałem $\mathbb{F}_5$.

ZOT 8. Statek kosmiczny TEPEI dostaje wiadomości z Ziemi w postaci bloków po 16 bitów, które możemy wyobrazić sobie jako tabele binarne 4×4. Wiadomość odebrana zawsze różni się od nadanej, bo odbiornik na TEPEI jest zepsuty: zmienia dokładnie trzy bity (w trzech różnych miejscach) w każdym bloku wiadomości, w dodatku robi to za każdym razem losowo. Załoga statku na szczęście o tym wie. Wie też, że wszystkie 16-bitowe bloki są wysyłane z Ziemi w kodzie zwanym dwuwymiarową kontrolą parzystości: mają parzystą liczbę jedynek w każdym wierszu i parzystą liczbę jedynek w każdej kolumnie.
Pewnego razu załoga odebrała blok bitów ukazany na pierwszym rysunku. Nie mając pewności, jaką wiadomość wysłała Ziemia, załoga poprosiła o powtórne przesłanie tej samej wiadomości. Za drugim razem otrzymali blok bitów przedstawiony na drugim rysunku.

1	0	1	0
0	0	1	1
1	1	0	1
0	0	0	0

1	0	1	1
0	0	1	1
1	1	0	0
0	1	0	1

Czy na podstawie wszystkich tych danych załoga TEPEI może jednoznacznie odtworzyć wiadomość?

Zadania na ćwiczenia

Zad.1. (*Zadanie, z którego można w przyszłości korzystać, nawet jeśli nie zrobimy go na ćwiczeniach.*) Wykaż, że rozstęp kodu liniowego jest równy najmniejszej liczbie niezerowych współrzędnych występujących w niezerowych słowach kodu.

Zad.2. Rozważmy język składający się ze słów dwuliterowych alfabetu $\mathbb{F}_3$. Do kodowania informacji w tym języku zastosowano kod C, w którym każdy znak powtarzamy 5 razy (tzn. 12 kodujemy jako 1111122222).

(a) Czy istnieje macierz generująca tego kodu w postaci normalnej?
(b) Czy istnieje macierz parzystości tego kodu?
(c) Popraw błędy w słowie 1212121220.

Zad.3. Kod C nad ciałem $\mathbb{F}_7$ składa się ze wszystkich słów $x_1x_2x_3x_4x_5$ spełniających warunki:

$$x_1 + x_2 + x_3 + x_4 + x_5 = 0 \quad \text{i} \quad x_1 + x_3 + x_5 = 0\,.$$

(a) Ile słów należy do kodu C?
(b) Znajdź przykładową macierz generującą G kodu C w postaci normalnej (o ile istnieje).
(c) Znajdź przykładową macierz parzystości tego kodu.

Zad.4. Kod ternarny $C \subseteq \mathbb{F}_3^8$ ma podaną poniżej macierz parzystości H.

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 2 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 2 & 0 & 1 & 0 & 0 \end{bmatrix}$$

(a) Sprawdź, że słowo $y = (0,0,1,1,1,1,0,0)$ nie należy do kodu.
(b) Czy istnieje słowo z o wadze 1, dla którego $Hz = Hy$?
(c) Czy można zmienić jedną współrzędną słowa y tak, aby otrzymany wektor był słowem kodu?
(d) Popraw błedy w y, to znaczy znajdź przynajmniej jedno słowo kodu najbliższe y. Czy istnieje ich więcej niż jedno?

Zad.5.

(a) Skonstruuj kod Hamminga dla $q = 7$ i $n = 8$.
(b) Dla tak skonstruowanego kodu, popraw błędy w słowie (1,0,0,3,1,6,0,0) (oczywiście, jeśli nie należy on do kodu).
(c) Czy istnieje słowo różniące się od każdego słowa powyższego kodu na co najmniej trzech współrzędnych?

Zad.6. (rezerwowe) Wybrane podpunkty z zadania B9.

Zadania do samodzielnego rozwiązania później

B1. W komunikacji z niektórymi sondami kosmicznymi stosowano następujące kodowanie korekcyjne: każdy bit źródłowej wiadomości przesyłany był pięciokrotnie, np. dla wiadomości 1011 wysyłane były cztery paczki: 11111 00000 11111 11111. Podczas transmisji możliwe były błędy: prawdopodobieństwo zmiany bitu wynosiło 0,05 dla każdego bitu. Podczas odczytu za poprawny bit wiadomości uznawało się ten, który w paczce bitów pojawiał się częściej. Na przykład paczka 10110 traktowana była jako bit 1, a paczka 10000 jako bit 0. Oblicz prawdopodobieństwo poprawnego odczytania wiadomości, która w wersji źródłowej składała się z 8 bitów. Jakie byłoby prawdopodobieństwo poprawnego odczytu, gdyby nie stosowano kodowania korekcyjnego, tzn. gdyby wysłano tylko 8 bitów wiadomości? Odpowiedzi podaj z dokładnością do 0,01.

B2. Oto macierz generująca pewnego liniowego kodu binarnego:

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

Wyznacz przykładową macierzą parzystości tego kodu.

B3. Niech $C \subseteq \mathbb{F}_3^3$, $C = \{xxxyyy\colon x, y \in \mathbb{F}_3\}$.

(a) Wyznacz przykładową macierz generującą tego kodu.
(b) Wyznacz przykładową macierz parzystości tego kodu.
(c) Popraw błędy w słowie 022010.

B4. Macierz parzystości pewnego ternarnego kodu liniowego $C \subseteq \mathbb{F}_3^6$ ma postać

$$\begin{bmatrix} 2 & 2 & 1 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 & 1 & 1 \\ 2 & 0 & 2 & 1 & 0 & 1 \end{bmatrix}.$$

Znajdź słowo kodu będące najbliżej słowu $(1, 0, 1, 2, 1, 1)$.

B5. Macierz parzystości pewnego kodu liniowego $C \subseteq \mathbb{F}_5^8$ ma postać

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 4 \\ 0 & 1 & 0 & 1 & 1 & 0 & 3 & 1 \\ 0 & 0 & 1 & 2 & 0 & 2 & 0 & 0 \end{bmatrix}.$$

Znajdź przykładowe słowo kodu C będące najbliżej słowu $(0, 0, 2, 1, 1, 1, 0, 0)$.

B6. Kod liniowy $C \subseteq \mathbb{F}_3^7$ ma podaną obok macierz generującą.

(a) Jakiego wymiaru jest kod C?
(b) Ile słów ma kod C?
(c) Uzasadnij, nie wyznaczając macierzy parzystości, że (0,0,1,1,2,1,2) jest słowem kodu C.
(d) Wyznacz macierz parzystości H tego kodu.
(e) Korzystając z macierzy parzystości, sprawdź, czy (2,2,1,1,2,0,1) jest słowem kodu C.
(f) Jeśli $(2, 2, 1, 1, 2, 1, 2)$ jest słowem kodu, to zapisz go w postaci kombinacji liniowej wierszy macierzy G. W przeciwnym wypadku popraw błędy, to znaczy znajdź (przykładowe) najbliższe mu słowo kodu.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 2 & 1 \end{bmatrix}$$

B7. Sprawdź, czy dla każdego doskonałego liniowego kodu długości n, wymiaru k, o rozstępie 3, nad ciałem o q elementach zachodzi $n = \frac{q^{n-k}-1}{q-1}$.

B8.

(a) Skonstruuj binarny kod C Hamminga długości 7.
(b) Dla tak skonstruowanego tak kodu, znajdź słowo, które do niego nie należy. i popraw w tym słowie błędy.
(c) Sprawdź, czy do C należy $(0, 1, 1, 1, 0, 1, 1)$ i jeśli nie, to popraw w nim błędy.

B9. Oceń poprawność poniższych zdań. Odpowiedź należy poprzeć, jak zwykle, albo uzasadnieniem ogólnym, albo przykładem, albo kontrprzykładem. Poprawność przykładu/kontrprzykładu też należy uzasadnić. Uwaga: Jeżeli ciało (alfabet) nie zostało podane, to oznacza, że może być dowolne.

(a) Istnieje liniowy kod ternarny, złożony z 5 słów.
(b) Istnieje liniowy kod złożony z 15 słów.
(c) Jeżeli kod liniowy składa się z 13 słów, to jego wymiar wynosi 1.

(d) Jeżeli C jest ternarnym kodem liniowym i $(0,1,2),(0,2,1) \in C$, to C liczy przynajmniej 9 słów.

(e) Poniższa macierz H jest jest przykładową macierzą parzystości dla kodu binarnego o podanej macierzy generującej G.

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \qquad G = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

(f) Istnieje kod liniowy długości 3, złożony z 25 słów.

(g) Istnieje kod liniowy kod złożony z 32 słów, który ma rozstęp większy niż 5.

(h) Istnieje liniowy kod wymiaru 2, długości 4, o rozstępie 3, który **nie** jest doskonały w $\mathbb{F}_3^4$.

(i) Istnieje liniowy kod doskonały długości 7.

(j) Liniowy kod doskonały wymiaru 4, o długości 7 i o rozstępie 3.

(k) Kod Hamminga wymiaru 7, o słowach długości 10.

(l) Kod Hamminga o słowach długości 11.

(m) Kod Hamminga o długości 7.