Algebra Abstrakcyjna i Kodowanie
Lista zadań

Jacek Cichoń, WPPT PWr,
Wrocław 2016/17

1 Grupy

Zadanie 1 — Pokaż, że jeśli grupy G i H są abelowe, to grupa $G \times H$ też jest abelowa.

Zadanie 2 — Niech X będzie niepustym zbiorem. Niech $\triangle$ oznacza różnicę symetryczną zbiorów.

1. Pokaż, że $(P(X), \triangle)$ jest grupą abelową.
2. Załóżmy, że X jest skończony. Niech $n = |X|$. Pokaż, że grupa $(P(X), \triangle)$ jest izomorficzna z grupą $\underbrace{C_2 \times \cdots \times C_2}_{n}$.

Zadanie 3 — Wyznacz podgrupę grupy G generowaną przez zbiór X:

1. $X = \{4, 10, -18\}$, $G = (\mathbb{Z}, +)$
2. $X = \{\sqrt{2}, \sqrt{3}\}$, $G = (\mathbb{R}, +)$
3. $X = \{2, \sqrt{3}\}$, $G = (\mathbb{R}, +)$
4. $X = \{i\}$, $G = (\mathbb{C} \setminus \{0\}, \cdot)$

Zadanie 4 — Pokaż, że grupa symetrii S_3 nie jest cykliczna.

Zadanie 5 — Pokaż, że grupy $C_5 \times C_5$ oraz C_{25} nie są izomorficzne.

Zadanie 6 — Załóżmy, że H jest podgrupą grupy G oraz, że $|G/H| = 2$. Pokaż, że H jest normalną podgrupą grupy G.

Zadanie 7 — Niech $G = (\mathbb{R}^2, +)$ oraz $H = \{(x, 0) : x \in \mathbb{R}\}$.

1. Pokaż, że H jest normalną podgrupą grupy G.
2. Znajdź homomorfizm $f : G \to \mathbb{R}$ taki, że $ker(f) = H$.
3. Wyznacz G/H.

Zadanie 8 — Narysuj diagramy Cayley'a grup $C_3 \times C_5$, $\mathbb{Z} \times C_3$, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{D}_{10}$

Zadanie 9 — Niech τ oznacza obrót o 90^o w grupie $\mathbb{D}_8$ zaś α odbicie. Pokaż, że $\{e, \tau^2, \alpha\tau, \alpha\tau^3\}$ jest podgrupą grupy $\mathbb{D}_8$.

Zadanie 10 — Centrum grupy G nazywamy zbiór $Z(G) = \{x \in G : (\forall g \in G)(xg = gx)\}$. Pokaż, że centrum grupy jest podgrupą grupy G.

Zadanie 11 — Wyznacz warstwy następujących podgrup H w gripie G:

1. $H = \{0, 3\}$, $G = C_6$
2. $H = \{Id, (2, 3)\}$, $G = S_3$
3. $H = \mathbb{R} \times \{0\}$, $G = (\mathbb{R}^2, +)$
4. $H = \{(x, x) : x \in \mathbb{R}\}$, $G = (\mathbb{R}^2, +)$
5. $H = \{1, i, -1, -i\}$, $G = (\{z \in \mathbb{C} : |z| = 1\}, \cdot)$
6. $H = \{0, \alpha\}$, $G = \mathbb{D}_8$

Zadanie 12 — **(Twierdzenie Cayley'a)** Niech $(G, \cdot)$ będzie grupą. Niech $Sym(G)$ oznacza grupę wszystkich bijekcji ze zbioru G w zbiór G z działaniem określonym jako złożenie bijekcji. Dla każdego $a \in G$ definiujemy funkcję $f_a : G \to G$ wzorem $f_a(x) = a \cdot x$. (Uwaga: tu był błąd; było $f_a(x) = x \cdot a$)

1. Pokaż, że $f_a \in Sym(G)$
2. Pokaż, że jeśli $f_a = f_b$ to $a = b$
3. Pokaż, że funkcja $\phi : G \to Sym(G)$ zadana wzorem $\phi(a) = f_a$ jest monomorfizmem $\phi : (G, \cdot) \to Sym(G)$.

Zadanie 13 — Pokaż, że każda podgrupa H grupy $(\mathbb{Z}, +)$ jest postaci $a\mathbb{Z} = \{ak : k \in \mathbb{Z}\}$ dla pewnej liczby naturalnej a.

Zadanie 14 — Wyznacz warstwy następujących podgrup H grupy G:

1. $H = \{0, 5\}$, $G = C_{10}$
2. $H = \{e, \tau\}$, $G = \mathbb{D}_{10}$
3. $H = \{-1, 1\}$, $G = (R \setminus \{0\}, \cdot)$

Zadanie 15 — Niech G będzie grupą abelową. Niech $a, b \in G$ będą takie, że $ord(a) = 5$ oraz $ord(b) = 2$. Pokaż, że

$$\langle \{a, b\} \rangle = \{e, a, a^2, a^3, a^4, b, ba, ba^2, ba^3, ba^4\} \ .$$

Zadanie 16 — Niech $G = \langle g \rangle$ będzie n elementową grupą cykliczną o generatorze g.

1. Pokaż, że $\langle g^k \rangle = \langle g^{nwd(k,n)} \rangle$ dla każdego $k \geq 1$.
2. Wywnioskuj z tego, że jeśli $d|m$ to w grupie cyklicznej m-elementowej istnieje dokładnie jedna podgrupa mocy d.

Zadanie 17 — Wyznacz wszystkie podgrupy grupy C_8.

Zadanie 18 — Niech p, q będą różnymi liczbami pierwszymi. Wyznacz wszystkie podgrupy grup C_p, C_{pq} oraz C_{p^2q}.

Zadanie 19 — Pokaż, że $\left\{ \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} : k \in \mathbb{Z} \right\}$ jest cykliczną podgrupą grupy $GL(2, \mathbb{R})$.

2 Elementy Teorii Liczb

Zadanie 20 — Oblicz $2^{2017} \mod 11$, $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \mod 7$.

Zadanie 21 — Niech p będzie liczbą pierwszą. Pokaż, że dla dowolnych liczb całkowitych a, b mamy $(a + b)^p \equiv a^p + b^p \mod p$.

Zadanie 22 — Oblicz $\phi(2500)$, $\phi(81000)$ znajdując rozkład argumentów na czynniki pierwsze.

Zadanie 23 — Pokaż, że $\phi(n)$ jest liczbą parzystą dle $n > 2$.

Zadanie 24 — Wyznacz wszystkie takie liczby n, że $\phi(n) = 4$ oraz $\phi(n) = 6$.

Zadanie 25 — Pokaż, że nie istnieje n takie, że $\phi(n) = 14$.

Zadanie 26 — Wyznacz wszystkie takie liczby n, że $\phi(n)|n$.

Zadanie 27 — Niech p, q będą dwoma różnymi liczbami pierwszymi. Niech a będzie liczbą, która nie jest podzielna przez p ani przez q. Pokaż, że

$$a^{(p-1)(q-1)} \equiv 1 \mod pq$$

Zadanie 28 — Znajdź takie $x \in \{0, \ldots, 99\}$, że $x \equiv 6 \mod 25$ oraz $x \equiv 7 \mod 4$.

Zadanie 29 — Skorzystaj z Chińskiego twierdzenia o resztach do znalezienia rozwiązania równania $x^3 - x + 1 \equiv 0 \mod 35$.

Zadanie 30 — **(Twierdzenie Wilsona)** Niech p będzie liczbą pierwszą. Dla $x \in \mathbb{Z}_p^*$ określamy $f(x) = x^{-1}$.

1. Zauważ, że $f \circ f = Id_G$ oraz znajdź punkty stałe odwzorowania f.
2. Oblicz w grupie $\mathbb{Z}_p^*$ iloczyn $1 \cdot 2 \cdots (p-1)$ grupując elementy x, y takie, że $y = f(x)$
3. Wywnioskuj z tego Twierdzenie Wilsona: jeśli p jest liczbą pierwszą, to $(p-1)! \equiv -1 \mod p$.

Zadanie 31 — Niech g będzie takim elementem pewnej grupy, że $ord(g) = 20$. Wyznacz liczby $ord(g^2)$, $ord(g^5)$, $ord(g^8)$, $ord(g^3)$.

Zadanie 32 — Wyznacz wszystkie generatory grup Z_5^*, Z_7^*, Z_{11}^*.

Zadanie 33 — Sprawdź, że liczba 1000003 jest pierwsza.

1. Wyznacz najmniejszy generator grupy $Z_{1000003}^*$. Wskazówka: Napisz w dowolnym języku programowania odpowiednią procedurę. Zastosuj algorytm szybkiego potegowania modulo n.
2. Zaimplementuj protokół Diffie-Helmana oparty na znalezionym generatorze.

Zadanie 34 — **(RSA)** Oto szyfrogram pewnego tekstu:

```
03f824fd:033c7a71:050a6706:050a6706:03ffab5e:03f824fd:0189a78d:
005bca7d:00734305:04046ca6:017698b6:005bca7d:03f824fd:03d10ac0:
003622e4:011c1c7e:030cf03c:011c1c7e:03d10ac0:01b60e5d:03f824fd:
00734305:007a18e6:03ffab5e:00734305:0179f797:037906bb:050a6706:
007a18e6:015d897d:03f824fd:037906bb:03f824fd:0451f198:059ff1e0:
03d10ac0:02e6b154:037906bb:03f824fd:00734305:003622e4:011c1c7e:
0414fa45:03f824fd:00a6891a:042edbee
```

Tekst został zakodowany Twoim kluczem publicznym. Wiadomo, że kodowano oddzielnie wszystkie litery (najpierw przekształcono je na kody UTF-8, potem otrzymane liczby podniesiono do pewnej potęgi modulo 101080891 i otrzymane liczby zapisano w układzie szesnastkowym i połączono je w jeden łańcuch, oddzielając poszczególne podłańcuchy dwukropkiem. Twoim kluczem prywatnym jest para $(2062465, 101080891)$.

1. Odkoduj ten tekst.
2. Znajdź faktoryzację liczby 101080891.
3. Jaki jest Twój klucz publiczny?

Zadanie 35 — Załóżmy, że $(G, \cdot)$ i $(H, \star)$ są takimi skończonymi grupami, że $ndw(|G|, |H|) = 1$. Pokaż, że jedynym homomorfizmem z $(G, \cdot)$ do $(H, \star)$ jest homomorfizm trywialny (czyli taki, że $h(x) = e_2$ dla dowolnego $x \in G$, i gdzie e_2 oznacza element neutralny grupy $(H, \star)$.)

Zadanie 36 — Niech $\mathcal{G} = (G, \cdot)$ będzie grupą. Niech $Aut(\mathcal{G})$ oznacza rodzinę wszystkich izomorfizmów między $\mathcal{G}$ i $\mathcal{G}$.

1. Pokaż, że $Aut(\mathcal{G})$ jest grupą, gdy działanie określimy jako złożenie funkcji
2. Wyznacz $Aut((\mathbb{Z}, +))$.
3. Pokaż, że jeśli $f \in Aut(C_n)$, to istnieje k takie, że $nwd(n, k) = 1$ oraz $f(x) = kx \mod n$ dla każdego $x \in C_n$. Wywnioskuj z tego, że $|Aut(C_n)| = \phi(n)$.
4. Załóżmy, że $(G, \cdot)$ i $(H, \star)$ są takimi skończonymi grupami, że $ndw(|G|, |H|) = 1$. Pokaż, że grupy $Aut(G \times H)$ oraz $Aut(G) \times Aut(H)$ są izomorficzne.
5. Wykorzystaj poprzedni punkt do pokazania, że jeśli $nwd(n, m) = 1$ to $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$.

3 Pierścienie

Zadanie 37 — Niech

$$\mathcal{R} = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{R} \right\} .$$

1. Pokaż, że $\mathcal{R}$ jest podpierścieniem pierścienia $M_{2\times 2}(\mathbb{R})$
2. Pokaż, że funkcja
$$f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) = a + b \cdot i$$
jest izomorfizmem $\mathcal{R}$ z ciałem liczb zespolonych.

Zadanie 38 — Niech $R = \mathbb{R}[x]$ oraz $a \in \mathbb{R}$. Określmy $\theta_a(w) = w(a)$.
1. Pokaż, że $\theta_a : R \to \mathbb{R}$ jest homomorfizmem pieścieni
2. Wyznacz $ker(\theta_a)$ oraz $img(\theta_a)$.
3. Wyznacz pierścień $\mathbb{R}[x]/ker(\theta_a)$.

Zadanie 39 — Załóżmy, że I_1, I_2 są ideałami (przemiennego) pierścienia R. Niech
$$I_1 + I_2 = \{a + b : a \in I_1 \wedge b \in I_2\}$$
1. Pokaż, że $I_1 + I_2$ jest ideałem.
2. Pojaż, że $I_1 + I_2$ jest najmniejszym ideałem zawierającym $I_1 \cup I_2$.
3. Czy suma $I_1 \cup I_2$ musi być ideałem ideałem?

Zadanie 40 — Niech $R = (\mathbb{Z}, +, \cdot)$,oraz $a, b \in \mathbb{Z}$.
1. Pokaż, że $(a, b) = (\text{nwd}(a, b))$.
2. Pokaż, że $(a) \cap (b) = (\text{nww}(a, b))$.

Zadanie 41 — Niech $\mathbb{Z}[i]$ oznacza pierścień liczb całkowitych Gaussa.
1. Wyznacz ideały (1), (i), (-1).
2. Wyznacz ideał $(1 + i)$.

Zadanie 42 — Niech R będzie przemiennym pierścieniem z jednością który ma tylko dwa ideały: $\{0\}$ i R. Pokaż, że R jest ciałem.

Zadanie 43 — Opisz wszystkie ideały pierścienia $\mathbb{Z}_n$.

Zadanie 44 — Pokaż, że $\mathbb{Z}[z]/(x) \simeq \mathbb{Z}$.

Zadanie 45 — Pokaż, że funkcja $f : \mathbb{R} \to \mathbb{R}[x]/(x^2 + 1)$ określona wzorem $f(a) = (x^2 + 1) + a$ jest zanurzeniem ciała $\mathbb{R}$ w ciało $\mathbb{R}[x]/(x^2 + 1)$ (czli, że jest różnowartościowym homomorfizmem).

Zadanie 46 — Zbadaj pierścień ilorazowy $\mathbb{R}[x]/(x^2 - 1)$. Zacznij od znalezienia dzielników zera w tym pierścieniu.

Zadanie 47 — Przez $R[x, y]$ rozumiemy pierścień wszystkich wielomianów dwóch zmiennych x i y o współczynnikach z pierścienia R.
1. Pokaż, że $R[x, y] \simeq (R[x])[y]$.
2. Pokaż, że w pierścieniu $\mathbb{R}[x, y]$ ideał (x, y) nie jest głównym ideałem.

Zadanie 48 — Rozważamy rodzinę $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{5}i : a, b \in \mathbb{Z}\}$
1. Pokaż, że $\mathbb{Z}[\sqrt{-5}]$ ze standardowym dodawaniem i mnożeniem z ciała $\mathbb{R}$ jest pierścieniem.
2. Niech $z = 2 + \sqrt{5}i$. Pokaż, że z jest elementem nierozkładalnym w $\mathbb{Z}[\sqrt{-5}]$.
3. Pokaż, że $z|3 \cdot 3$ oraz, że $\neg(z|3)$.
4. Wywnioskuj z tego, że z jest elementem nierozkładalnym, który nie jest elementem pierwszym.

Zadanie 49 — Znajdź takie liczby naturalne a i b, że $a^2 + b^2 = 2017$.

Zadanie 50 — Niech $\mathcal{R} = (R, +, \cdot)$ będzie pierścieniem ideałów głównych. Niech $a, b, d \in R$.

1. Pokaż, że d jest największym wspólnym dzielnikiem elementów a i b wtedy i tylko wtedy, gdy $(a,b) = (d)$
2. Zdefiniuje pojęcie najmniejszej wspólnej wielokrotności.
3. Pokaż, że przekrój dwóch ideałów w dowolnym pierścieniu jest ideałem.
4. Pokaż, że d jest najmniejszą wspólną wielokrotnością elementów a i b wtedy i tylko wtedy, gdy $(a) \cap (b) = (d)$

Zadanie 51 — Pokaż, że wielomian $w(x) = 1 + x + x^3$ jest wielomianem nierozkładalnym w pierścieniu $\mathbb{Z}_2[x]$. Niech $[v] = (w) + x$ dla $v \in \mathbb{Z}_2[x]$.

1. Wypisz wszystkie elementy ciała $GF_8 = \mathbb{Z}_2[x]/(w)$. Jaka jest moc tego ciała?
2. Niech C oznacza zbiór wielomianów stałych w pierścieniu $\mathbb{Z}_2[x]$. Pokaż, że $F = \{[a] : a \in C\}$ jest podciałem ciała GF_8 izomorficznych z ciałem $\mathbb{Z}_2$.
3. Sprawdź, że GF_8 jest przestrzenią liniową nad ciałem F. Jaki jest wymiar tej przestrzeni?
4. Niech $I = [x]$. Pokaż, że $w(I) = 0$. Wywnioskuj z tego, że w ciele GF_8 mamy $I^3 = 1 + I$.
5. Wyznacz tabliczki dodawania oraz mnożenia w GF_8.
6. Rozłóż wielomian w na czynniki liniowe w ciele GF_8.
7. Znajdź generator grupy multiplikatywnej $(GF_8)^*$ ciała GF_8.

4 Elementy Teorii Kodowania

Zadanie 52 — Sprawdź, że odległość Hamminga, czyli funkcja $d_H : \Sigma^n \times \Sigma^n \to \mathbb{N}$ określona wzorem

$$d_H(x,y) = |\{i : x_i \neq y_i\}|$$

jest metryką na przestrzeni Σ^n.

Zadanie 53 — Ile błędów może wykryć oraz ile błędów może naprawić $(n, M, 8)_q$ - kod?

Zadanie 54 — Wyznacz parametry następujących kodów binarnych i sprawdź dla nich „Singleton Bound" oraz „Hamming Bound":

1. $C_1 = \{000, 011, 101, 110\}$
2. $C_2 = \{000, 001, 010, 011, 100, 101, 110, 111\}$
3. $C_3 = \{000, 011, 101, 110\}$
4. $C_4 = \{0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\}$

Zadanie 55 — Ustalmy liczby q, n i M.

1. Pokaż, że jeśli istnieje $(n, M, d)_q$ kod, to $1 \leq d \leq n$.
2. Zbuduj $(n, q^n, 1)_q$ kod.
3. Zbuduj $(n, q, n)_q$ kod.

Zadanie 56 — Niech C będzie $(n, M, d)_q$ kodem, gdzie $d \geq 2$. Zbuduj z kodu C kod o parametrach $(n-1, M, q-1)_q$.

Zadanie 57 — Niech C będzie binarnym (n, M, d) kodem. Załóżmy, że d jest liczbą nieparzystą. Dla $x = (x_1, \ldots, x_n) \in C$ określamy

$$\hat{x} = (x_1, \ldots, x_n, (x_1 + \ldots + x_n) \mod 2)$$

Uwaga: Konstrukcję tę nazywamy dodaniem bitu przystości.

1. Pokaż, że $\{\hat{x} : x \in C\}$ jest $(n+1, M, d+1)$ kodem. Wskazówka: Zauważ, że dla $\Sigma = \{0, 1\}$ mamy $d_H(x,y) = w(x) + w(y) - 2w(x \wedge y)$ gdzie $w(x) = d_H(x, \vec{0})$.
2. Dlaczego założyliśmy, że d jest liczbą nieparzystą ?

Zadanie 58 — Niech $A_q(n, d)$ oznacza największą liczbę naturalną M dla której istnieje q-arny (n, M, d) kod.

1. Skorzystaj z „Singleton bound” do pokazania, że dla dowolnej liczby $q \leq 2$ mamy $A_q(3,2) \leq q^2$.
2. Pokaż, że dla każdej liczby naturalnej $q \geq 2$ mamy $A_q(3,2) = q^2$. Wskazówka: Rozważ grupę C_q.

3. Na wykładzie przyglądaliśmy się kodowi

$$\mathcal{C}_2 = \begin{cases} 00000 \\ 01101 \\ 10110 \\ 11011 \end{cases}$$

   Pokaż,że jest to $(5,4,3)$-kod oraz, że $A_2(5,3) = 4$.
4. Oszacuj złożoność obliczeniową próby wyznaczenia liczby $A_q(n,d)$ metodą „brute force” (czyli przeglądania wszystkich możliwych kodów w zbiorze q^n

Zadanie 59 — Rozważmy przestrzeń dwuwymiarową V nad ciałem Z_3.

1. Ile jest prostych w przestrzeni V?
2. Ile jest punktów na każdej z tych prostych?
3. Ile jest prostych równoległych do danej prostej?
4. Zbuduj z punktów i kierunków w przestrzeni V przestrzeń rzutową $PG(2,3)$ (dwuwymiarową przestrzeń rzutową nad ciałem trójelementowym). Ile ma ona wierzchołków oraz ile ma linii?
5. Spróbuj znaleźć w miarę czytelną graficzną reprezentację $PG(2,3)$.

Zadanie 60 — **(”Konstrukcja Plotkina”)** Niech $(u|v)$ oznacza konkatenację ciągów u i v. Niech C_1 będzie binarnym (n, M_1, d_1) kodem oraz niech C_2 będzie binarnym (n, M_2, d_2) kodem. Rozważmy kod

$$C_3 = \{(u|u+v) : u \in C_1 \wedge v \in C_2\} \ .$$

(operacja + oznacza tutaj dodawanie w przestrzeni liniowej $\{0,1\}^n$ nad ciałem Z_2). Pokaż, że C_3 jest $(2n, M_1 \cdot M_2, d)$ kodem, gdzie $d = \min\{2d_1, d_2\}$.
Wskazówka: Pokaż najpierw, że $w(x) \leq w(y) + w(x+y)$ dla dowolnych $x, y \in \{0,1\}^n$, gdzie $w(x) = d_H(x, \vec{0})$.

Zadanie 61 — Znajdź $(4,8,2)$ oraz $(4,2,4)$ binarne kody. Zastosuj czterokrotnie konstrukcję z poprzedniego zadania do zbudowania $(32,64,16)$ kodu. Jest to tak zwany kod Reed’a-Mullera pierwszego rodzaju zastosowany do transmisji zdjęć Marsa przez sondy Mariner 6,7 i 9.

Zadanie 62 — Pokaż, że relacja podobieństwa kodów jest relacją równoważności na zbiorze q^n.

Zadanie 63 — Niech $H(x) = x \log_2 \frac{1}{x} + (1-x) \log_2 \frac{1}{1-x}$ dla $x \in (0,1)$, oraz $H(0) = H(1) = 0$ (entropia binarna).

1. Pokaż, że H jest funkcją ciągłą na $[0,1]$.
2. Wyznacz pochodną prawostronną funkcji H w punkcie 0.
3. Znajdź trzy pierwsze wyrazy rozwinięcia w szereg Taylora funkcji H w punkcie $\frac{1}{2}$.

Zadanie 64 — Niech $\lambda \in (0, \frac{1}{2})$. Skorzystaj ze wzoru Stirlinga do pokazania, że $\binom{n}{\lambda n} = 2^{n(H(\lambda) - \frac{1}{2}\log_2(n) + O(1))}$.

Zadanie 65 — Niech $E_n = \{x \in (\mathbb{Z}_2)^n : \sum_{i=1}^n x_i = 0\}$

1. Pokaż, że E_n jest kodem liniowym.
2. Pokaż, że $E_n = \{x \in (\mathbb{Z}_2)^n : x_n = \sum_{i=1}^{n-1} x_i\}$.
3. Wyznacz parametry tego kodu.
4. Wyznacz macierzy generującą tego kodu.
5. Wyznacz macierz kontroli parzystości dla tego kodu.

Zadanie 66 — Niech $G_{n,k} = [I_n|I_n|\ldots|I_n]$, gdzie macierz identycznościowa I_n jest powtórzona k razy. Niech $C_{n,k}$ będzie kodem liniowym o macierzy generatorów $G_{n,k}$.

1. Pokaż, że dla dowolnego $x \in F^n$ mamy $w(x \cdot G_{n,k}) = kw(x)$.

2. Wyznacz $\Delta(C_{n,k})$.
3. Wyznacz macierz kontroli parzystości.

Zadanie 67 — Niech C będzie $[n,k]$ kodem liniowym. Pokaż, że $(C^{\perp})^{\perp} = C$.

Zadanie 68 — Zastosuj binarny kod liniowy o macierzy kontroli parzystości

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

do odkodowanie otrzymanego wektora 1011.

Zadanie 69 — Niech $\mathcal{C}$ będzie binarnym $[6, M, d]$ kodem o macierzy generującej

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

1. Wyznacz macierz kontroli parzystości kodu $\mathcal{C}$
2. Wyznacz parametry M oraz d
3. Ile błędów może naprawić kod $\mathcal{C}$?
4. Czy to jest kod doskonały?
5. Załóżmy, że otrzymaliśmy wektor 011011. Czy wektor ten może być odkodowany przy założeniu, że podczas transmisji doszło do maksymalnie jednego błędu. Jeśli tak, to wskaż ten wektor.
6. Załóżmy, że otrzymaliśmy wektor 011010. Czy wektor ten może być odkodowany przy założeniu, że podczas transmisji doszło do maksymalnie jednego błędu. Jeśli tak, to wskaż ten wektor.

Zadanie 70 — Załóżmy, że $\mathcal{C}$ jest kodem blokowym długości n taki, że $\mathcal{C}^{\perp} = \mathcal{C}$. Pokaż, że n jest liczbą parzystą oraz, że $\mathcal{C}$ jest $[n, \frac{n}{2}]$ kodem.

c.d.n.
Powodzenia,
Jacek Cichoń