Przedmiot:	Matematyczne narzędzia komputerowe w zastosowaniach telekomunikacyjnych
Prowadzący:	Piotr Chołda piotr.cholda@agh.edu.pl
Kierunek:	Elektronika i Telekomunikacja
Specjalność:	Sieci i usługi
Semestr:	I sem. (letni) studiów magisterskich

Konspekt

Piotr Chołda

12 czerwca 2018

1 Zastosowania algebry liniowej w kodowaniu nadmiarowym i kryptografii

1.1 Algebra liniowe — przypomnienie i uzupełnienie

1. Struktura algebraiczna, binarne działania wewnętrzne, binarne działania zewnętrzne.
2. Grupa, łączność, element neutralny, element odwrotny.
3. Grupa przemienna/abelowa (*abelian/commutative group*).
4. Grupa skończona (*finite group*). Rząd grupy (*order*) $|G|$.
5. Przykładowe grupy: zbiór liczb całkowitych z dodawaniem, zbiór liczb wymiernych z mnożeniem, $\langle \mathbb{Z}_p, + \rangle$, $\langle \mathbb{Z}_p^*, \times \rangle$.
6. Element odwrotny w $\langle \mathbb{Z}_p, + \rangle$. Algorytm Euklidesa.
7. Algebra zbiorów jako przykład struktury algebraicznej innego typu niż grupa.
8. Pierścień (*ring*). Pierścień z jedynką. Pierścień przemienny.
9. Ciało (*field*). Ciało Galois $GF(q)$. Ciało $GF(2)$. Ciała rozszerzone $GF(p^m)$.
10. Liniowa przestrzeń wektorowa rozpięta nad ciałem (*linear vector space over field*), rozdzielność działań (*distribution*) i przemienność w przestrzeni wektorowej. Wektory, skalary. Kombinacja liniowa wektorów. Liniowa niezależność (*linear independence*) wektorów. Baza przestrzeni wektorowej (*basis for vector space*). Wymiar przestrzeni wektorowej (*dimension*). Liniowa podprzestrzeń wektorowa (*subspace*).
11. Rząd macierzy (*rank*). Iloczyn skalarny wektorów (*inner product*). Ortogonalność wektorów.
12. (Pod)przestrzeń dualna/dopełnienie ortogonalne (*dual space/orthogonal complement*).

1.2 Zastosowania: binarne kody liniowe, AES

1. Nadmiarowe kody kanałowe: detekcyjne i korekcyjne.
2. Kod blokowy, parametry (n, k), liczba pozycji nadmiarowych, kody systematyczne i niesystematyczne.
3. Odległość Hamminga i jej właściwości. *Minimalna odległość Hamminga* dla kodu $d_{\min}$.
4. Reguła największego prawdopodobieństwa przy dekodowaniu.
5. Właściwości korekcyjne i detekcyjne kodów a minimalna odległość Hamminga.
6. Binarny kod liniowy.
7. Podstawowe właściwości kodów liniowych.
8. Macierz generująca kodu liniowego, macierz testów parzystości kodu liniowego.
9. Dekodowanie na podstawie syndromu (*syndrome decoding*).
10. Przykłady kodów liniowych: kod z kontrolą parzystości, kod Hamminga.
11. Algorytm AES: zastosowanie ciała skończonego $GF\left(2^8\right)$.

1.3 Zadania

1. Czy 233 ma odwrotność modulo 2111?
2. Rozwiązać równość: $197x = 1259 \mod 2017$.
3. Znaleźć wartości całkowite takie że $65537x + 3511y = 1$.
4. Sprawdzić, że liczby 65537 i 3511 są względnie pierwsze.
5. Podać odwrotność $3511 \mod 65537$.
6. Czy jeśli wektory $\mathbf{x}$, $\mathbf{y}$ i $\mathbf{z}$, należące do binarnej przestrzeni wektorowej nad ciałem Galois $GF(2)$, są liniowo niezależne, to można to samo orzec o następujących trzech wektorach:
$$\mathbf{x}+\mathbf{y} \quad \mathbf{y}+\mathbf{z} \quad \mathbf{x}+\mathbf{z}?$$
7. Pokazać, że w liniowej przestrzeni wektorowej V rozpiętej nad ciałem Galois $GF(2)$, w której wektor ma długość c pozycji, maksymalna liczność zbioru wektorów, takiego że żadna para zawartych w nim wektorów nie jest liniowo zależna, wynosi:
$$2^c - 1.$$
8. Mamy dany konkretny ciąg kodowy binarnego kodu nadmiarowego (n, k). Obliczyć dla $0 \leq i \leq n$, ile istnieje ciągów, których odległość Hamminga od tego ciągu wynosi i. Pokazać, że ich suma po $i = 0, 1, \ldots, n$ jest równa liczbie wszystkich binarnych ciągów n-elementowych.

9. Czy ciągi kodowe:

$$01101 \quad 11010 \quad 10111 \quad 11100$$

mogą wszystkie na raz być (niekoniecznie wszystkimi) ciągami kodowymi (niekoniecznie systematycznego) binarnego kodu liniowego $(5, 2)$?

10. Udowodnić, że jeśli kody $\mathcal{C}$ i $\mathcal{C}'$ są kodami liniowymi zawartymi w przestrzeni liniowej V rozpiętej nad binarnym ciałem Galois $GF(2)$, to wtedy kody:

$$\mathcal{C} + \mathcal{C}' = \{\mathbf{x} + \mathbf{x}' | \mathbf{x} \in \mathcal{C}, \mathbf{x}' \in \mathcal{C}'\}$$

oraz

$$\mathcal{C} \cap \mathcal{C}' = \{\mathbf{x} | \mathbf{x} \in \mathcal{C} \wedge \mathbf{x} \in \mathcal{C}'\}$$

również są kodami liniowymi. Czy kod:

$$\mathcal{C} \cup \mathcal{C}' = \{\mathbf{x} | \mathbf{x} \in \mathcal{C} \vee \mathbf{x} \in \mathcal{C}'\}$$

jest liniowy w każdej sytuacji? Jeśli nie, to jakie muszą być spełnione warunki, żeby był liniowy?

11. Kody $\mathcal{C}$ i $\mathcal{C}'$ są kodami liniowymi zawartymi w przestrzeni liniowej V rozpiętej nad binarnym ciałem Galois $GF(2)$ o macierzach generujących oraz kontroli parzystości odpowiednio $\mathbf{G}$, $\mathbf{H}$ i $\mathbf{G}'$, $\mathbf{H}'$. Podać macierz generującą kodu $\mathcal{C} + \mathcal{C}'$ oraz macierz kontroli parzystości kodu $\mathcal{C} \cap \mathcal{C}'$, gdzie:

$$\mathcal{C} + \mathcal{C}' = \{\mathbf{u} + \mathbf{u}' | \mathbf{u} \in \mathcal{C}, \mathbf{u}' \in \mathcal{C}'\},$$
$$\mathcal{C} \cap \mathcal{C}' = \{\mathbf{u} | \mathbf{u} \in \mathcal{C} \wedge \mathbf{u} \in \mathcal{C}'\}.$$

12. Pokazać, że jeśli binarny kod systematyczny $\mathcal{C}_i$ ma parametry (n, k_i) i odległość minimalną $d_{\min_i}$, to kod otrzymany w wyniku specjalnego złożenia poszczególnych słów kodowych (np. dla ciągów kodowych 00 i 11: $(00, 11) = 0011$):

$$\mathcal{C}_1 \bigstar \mathcal{C}_2 = \{(\mathbf{x}, \mathbf{x} + \mathbf{x}') | \mathbf{x} \in \mathcal{C}_1, \mathbf{x}' \in \mathcal{C}_2\}$$

ma parametry $(2n, k_1 + k_2)$ oraz odległość minimalną:

$$d_{\min_{\mathcal{C}_1 \bigstar \mathcal{C}_2}} = \min\{2d_{\min_1}, d_{\min_2}\}$$

Udowodnić, że jeśli kody $\mathcal{C}_i$ są liniowe, to kod $\mathcal{C}_1 \bigstar \mathcal{C}_2$ również jest liniowy.

13. Syndrom obliczany dla pewnego nadmiarowego kodu binarnego ma postać:

$$\mathbf{s} = \begin{bmatrix} y_1 + y_3 + y_5 & y_1 + y_2 + y_6 & y_3 + y_4 + y_6 \end{bmatrix}.$$

przy czym dekoder oblicza go na podstawie otrzymanego ciągu $\mathbf{y}$, gdzie y_i oznaczają wartości $\mathbf{y}$ na pozycjach i. Znaleźć parametry tego kodu (zakładając, że to najkrótszy możliwy kod) oraz określ jego właściwości korekcyjne i detekcyjne.

1.4 Do samodzielnego studiowania

Zagadnienia omówione w ramach tego wykładu są w dużym stopniu opisane w następujących pozycjach:

- Lynn Margaret Batten. *Public Key Cryptography.* John Wiley & Sons, Inc., Hoboken, NJ, 2013: rozdziały 2-4.
- Gareth A. Jones and J. Mary Jones. *Information and Coding Theory.* Springer-Verlag London Ltd., London, UK, 2000: rozdziały 5.1-5.2, 5.3-5.6, 6-7, dodatek C.
- Todd K. Moon. *Error Correction Coding.* John Wiley & Sons, Inc., Hoboken, NJ, 2005: rozdziały 1.8, 1.12.3-1.12.4, 2-3, 4.1-4.12, 5, dodatek 4.A.
- Alexander A. Stepanov and Daniel E. Rose. *From Mathematics to Generic Programming.* Addison-Wesley, Upper Saddle River, NJ, 2015: rozdziały 3.2-3.3, 5.2-5.6.