Program wykładu:
KODY BLOKOWE

Wykład 30 godz.

1. Semestr letni
2. Cel przedmiotu:
   Opanowanie podstaw teorii kodowania i dekodowania
3. Warunek uczestnictwa: Zaliczenie przedmiotu Algebra liniowa
4. Forma zaliczenia przedmiotu
   Egzamin pisemny z oceną pozytywną, następnie ustny.
5. Zasada wystawiania oceny końcowej: Decyduje egzamin ustny

6. Streszczenie przedmiotu

Kody blokowe to zbiór matematycznych metod umożliwiających kontrolę poprawności danych informacyjnych przy ich gromadzeniu i przesyłaniu. Celem kodowania jest wykrywanie
oraz poprawianie błędów spowodowanych losowymi zakłóceniami.

7. Zawartość programowa:

1.Kodowanie kontra szyfrowanie. Przykłady kodów w matematyce: Pruefer i drzewa (1916), Hamilton i liczby zespolone (1837), Hamilton i kwaterniony (1843). System PESEL.
2. Gromadzenie i przesyłanie informacji. Alfabet, słowa informacyjne, słowa kodowe, ich długości *k* i *n.* Kod blokowy i jego długość *n*. Kod binarny. Metryka Hamminga, waga słowa. Schemat transmisji z kodowaniem i dekodowaniem. Założenia o kanale przesyłowym, addytywne błędy losowe. Niezawodność kanału. Binarny kanał symetryczny. Kod powtarzający, kod parzysty. Moc (liczność) kodu. Wymiar *k* kodu liniowego. Sprawność *R* kodu blokowego. Dystans kodu.
3.Kontrola parzystości i jej efektywność.
4. Dekodowanie wg największego prawdopodobieństwa (MLD). Dekodowanie pełne lub nie. Twierdzenia o wykrywaniu lub korygowaniu błędów. Ograniczenie Hamminga (ograniczenie dla upakowania kul) i ograniczenie Singletona. Kody doskonałe i kody MDS. Trywialne kody doskonałe.
5. Pierścienie skończone i ciała Galois. Ciała reszt. Kongruencje wielomianów. Wielomiany nierozkładalne, wielomian pierwotny stopnia *n*. Ciała wielomianów. Przykłady rozszerzania ciał skończonych poprzez przestrzenie liniowe.
6. Baza i macierz generująca kodu liniowego. Ortogonalność słów. Kod dualny. Macierz kontroli parzystości. Twierdzenie Kroneckera-Capellego. Elementarne przekształcenia wierszowe. Kodowanie za pomocą macierzy generującej. Kod liniowy systematyczny. Kody równoważne. Binarny kod Hamminga [n,k,d]. Macierz kontroli parzystości determinuje dystans kodu liniowego.
Kody sympleks. Sympleks w przestrzeni afinicznej.
7. Warstwy kodu (translacje). Słownik kodu. Objaw (syndrom) warstwy. Dekodowanie: standardowa tablica dekodująca (SDA). Przykład: SDA dla kodu Hamminga.
8. Nowe kody ze starych. Dystansowe kolorowania hiperkostki.
9. Kod Golaya jako przedziurawienie wydłużonego kodu Golaya. Samodualność.
10. Kody cykliczne i liniowe kody cykliczne. Wielomian generujący, jego charakteryzacja. Algorytm Euklidesa. Liczba kodów cyklicznych danej długości. Wielomiany nawzajem odwrotowe i dualność wśród liniowych kodów cyklicznych. Wielomiany idempotentne, Faktoryzacja dwumianu binarnego $1 + x^n$,
11. Elementy pierwotne w grupach. Funkcja φ Eulera. Element pierwotny ciała jako generator grupy multiplikatywnej tego ciała. Wielomian minimalny elementu. Ciało Galois z mnożeniem modulo wielomian pierwotny. Ciało słów. Zliczanie wielomianów pierwotnych. Funkcja μ Möbiusa i zliczanie wielomianów nierozkładalnych.
12. Kod Hamminga jako kod cykliczny BCH (Bose—Ray-Chaudhuri—Hocquenghem), Kody BCH. Dystans projektowany i ograniczenie BCH. Kody Reeda-Solomona.
13. Macierze Hadamarda i kody Hadamarda. Ograniczenia Plotkina.
14. Z_4–liniowe wersje nieliniowych kodów Kerdocka i Preparata'y.
15. Entropia i twierdzenia Shannona.

Literatura:

1. D.R. Hankerson et al. (7 co-authors), Coding Theory and Cryptography.
The Essentials, Marcel Dekker, 2nd ed., New York and Basel, 2000.
2. W.C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes,
Cambridge Univ. Press, 2003.
3. G.A. Jones, J.M. Jones, Information and Coding Theory,
Springer, 2002.
4. F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes,
North-Holland, 1977.
5. R.M. Roth, Introduction to Coding Theory,
Cambridge Univ. Press, 2006.

Modyfikacja: 23.VI. 2013, Z.S.