AGH UNIVERSITY OF SCIENCE AND TECHNOLOGY

Nazwa modułu zajęć: Kody Blokowe

Rok akademicki: 2019/2020 Kod: AMAT-2-022-MN-s Punkty ECTS: 4

Wydział: Matematyki Stosowanej

Kierunek: Matematyka Specjalność: Matematyka w naukach technicznych i przyrodniczych

Poziom studiów: Studia II stopnia Forma studiów: Stacjonarne

Język wykładowy: Polski Profil: Ogólnoakademicki (A) Semestr: 0

Strona www: http://www.wms.agh.edu.pl/~skupien/student.htm

Prowadzący moduł: prof. zw. dr hab. Skupień Zdzisław (skupien@agh.edu.pl)

Treści programowe zapewniające uzyskanie efektów uczenia się dla modułu zajęć

Zastosowanie algebry w problemach związanych z kodowaniem, szyfrowaniem, gromadzeniem i przesyłaniem informacji.

Opis efektów uczenia się dla modułu zajęć

Kod MEU	Student, który zaliczył moduł zajęć zna i rozumie/potrafi/jest gotów do	Powiązania z KEU	Sposób weryfikacji i oceny efektów uczenia się osiągniętych przez studenta w ramach poszczególnych form zajęć i dla całego modułu zajęć
Wiedza: zna i rozumie			
M_W001	Zna głębiej elementy algebry	MAT2A_W04	Egzamin
Umiejętności: potrafi			
M_U001	Umie stosować metody algebraiczne	MAT2A_U10	Egzamin
M_U002	Umie stosować algebrę liniową	MAT2A_U13	Egzamin
M_U003	Dostrzega obecność struktur algebraicznych w różnych zagadnieniach		Egzamin

Liczba godzin zajęć w ramach poszczególnych form zajęć

Suma	Forma zajęć dydaktycznych										
	Wykład	Ćwiczenia audytoryjne	Ćwiczenia laboratoryjne	Ćwiczenia projektowe	Konwersatorium	Zajęcia seminaryjne	Zajęcia praktyczne	Zajęcia terenowe	Zajęcia warsztatowe	Prace kontrolne i przejściowe	Lektorat
30	30	0	0	0	0	0	0	0	0	0	0

Matryca kierunkowych efektów uczenia się w odniesieniu do form zajęć i sposobu zaliczenia, które pozwalają na ich uzyskanie

Kod MEU	Student, który zaliczył moduł zajęć zna i rozumie/potrafi/jest gotów do	Forma zajęć dydaktycznych										
		Wykład	Ćwiczenia audytoryjne	Ćwiczenia laboratoryjne	Ćwiczenia projektowe	Konwersatorium	Zajęcia seminaryjne	Zajęcia praktyczne	Zajęcia terenowe	Zajęcia warsztatowe	Prace kontrolne i przejściowe	Lektorat
Wiedza: zna i rozumie												
M_W001	Zna głębiej elementy algebry	+	-	-	-	-	-	-	-	-	-	-
Umiejętności: potrafi												
M_U001	Umie stosować metody algebraiczne	+	-	-	-	-	-	-	-	-	-	-
M_U002	Umie stosować algebrę liniową	+	-	-	-	-	-	-	-	-	-	-
M_U003	Dostrzega obecność struktur algebraicznych w różnych zagadnieniach	+	-	-	-	-	-	-	-	-	-	-

Nakład pracy studenta (bilans punktów ECTS)

Forma aktywności studenta	Obciążenie studenta
Udział w zajęciach dydaktycznych/praktyka	30 godz
Samodzielne studiowanie tematyki zajęć	63 godz
Egzamin lub kolokwium zaliczeniowe	2 godz
Dodatkowe godziny kontaktowe	5 godz
Sumaryczne obciążenie pracą studenta	100 godz
Punkty ECTS za moduł	4 ECTS

Pozostałe informacje

Szczegółowe treści kształcenia w ramach poszczególnych form zajęć (szczegółowy program wykładów i pozostałych zajęć)

Wykład

Gromadzenie i przesyłanie informacji.

1. Kodowanie kontra szyfrowanie. Gromadzenie i przesyłanie informacji. System PESEL. Kod blokowy. Alfabet. Słowa informacyjne, słowa kodowe, błąd addytywny, słowo otrzymane. Kod powtarzający, kod parzysty. Długość kodu: n. Moc (liczność) kodu. Wymiar k kodu liniowego. Kod binarny. Założenia o kanale przesyłowym, błędy losowe. Niezawodność kanału. Binarny kanał symetryczny. Schemat transmisji z kodowaniem i dekodowaniem. Metryka Hamminga. Waga słowa. Dystans kodu. Sprawność R kodu blokowego. Kontrola parzystości i jej efektywność. Dekodowanie wg największego prawdopodobieństwa (MLD). Dekodowanie pełne lub nie. Twierdzenia o wykrywaniu lub korygowaniu błędów.

2. Ciała Galois. Ciała reszt. Wielomiany nierozkładalne, ciała wielomianów. Przykłady rozszerzania ciał skończonych. Funkcja μ Möbiusa i zliczanie wielomianów nierozkładalnych.

3. Generowanie kodu liniowego. Ortogonalność słów. Kod dualny. Baza i macierz generująca. Liczba baz kodu liniowego. Elementarne przekształcenia wierszowe i algorytmy znajdowania bazy (macierzy generującej) kodu i/lub kodu dualnego. Macierz kontroli parzystości. Przykłady rachunkowe. Kodowanie za pomocą macierzy generującej. Kod liniowy systematyczny. Kody równoważne. Macierz kontroli parzystości determinuje dystans kodu liniowego.

4. Kod Hamminga binarny [n,k,d] z parametrami n = 2^r – 1 dla r > 2, k = n – r, d = 3. Kody sympleks. Ograniczenie Hamminga (ograniczenie dla upakowania kul). Kody doskonałe. Kody trywialne. Ograniczenie Singletona. Kody MDS. Ograniczenie Gilberta-Varshamova (Warszamowa). Ograniczenie Plotkina.

5. Warstwy kodu (translacje). Słownik kodu. Objaw (syndrom) warstwy. Dekodowanie: standardowa tablica dekodująca (SDA). Przykład: SDA dla kodu Hamminga.

6. Wydłużanie kodu. Kod Golaya jako przedziurawienie wydłużonego kodu Golaya. Samodualność.

7. Kody liniowe cykliczne. Wielomian generujący, jego charakteryzacja. Algorytm

Euklidesa. Liczba kodów cyklicznych danej długości. Macierz kontroli parzystości kodu cyklicznego i wielomian generujący jego kod dualny.

8. Wielomiany idempotentne, Funkcja φ Eulera. Faktoryzacja dwumianu binarnego 1 + x^n, znajdowanie wszystkich kodów cyklicznych długości n. Element pierwotny ciała jako generator grupy multiplikatywnej tego ciała. Wielomian pierwotny stopnia m. Ciało Galois z mnożeniem modulo wielomian pierwotny. Ciało słów. Zliczanie wielomianów pierwotnych.

9. Wielomian minimalny elementu ciała. Kody BCH (Bose—Ray-Chaudhuri—Hocquenghem), w szczególności pierwotne i w wąskim sensie. Dystans projektowany i ograniczenie BCH. Kod Hamminga jako kod cykliczny BCH. Kody Reeda-Solomona.

10. Kody Hadamarda. Z_4 –liniowe wersje nieliniowych kodów Kerdocka i Preparata'y. Entropia i twierdzenia Shannona.

Metody i techniki kształcenia:

Wykład: Treści prezentowane na wykładzie są przekazywane w formie prezentacji multimedialnej w połączeniu z klasycznym wykładem tablicowym wzbogaconymi o pokazy odnoszące się do prezentowanych zagadnień.

Warunki i sposób zaliczenia poszczególnych form zajęć, w tym zasady zaliczeń poprawkowych, a także warunki dopuszczenia do egzaminu:

Nie określono

Zasady udziału w poszczególnych zajęciach, ze wskazaniem, czy obecność studenta na zajęciach jest obowiązkowa:

Wykład:
– Obecność obowiązkowa: Nie
– Zasady udziału w zajęciach: Studenci uczestniczą w zajęciach poznając kolejne treści nauczania zgodnie z syllabusem przedmiotu. Studenci winni na bieżąco zadawać pytania i wyjaśniać wątpliwości. Rejestracja audiowizualna wykładu wymaga zgody prowadzącego.

Sposób obliczania oceny końcowej

1. Ocenę końcową **OK** wyznacza się na podstawie **OKZal** , oceny uzyskaną z kolokwium zaliczeniowego,
2. Ocena końcowa **OK.** jest obliczana według algorytmu:
Jeżeli **OKZal** ≥ 4.75, to **OK** = 5.0 (bdb),
jeżeli 4.75 > **OKZal** ≥ 4.25, to **OK** = 4.5 (db),
jeżeli 4.25 > **OKZal** ≥ 3.75, to **OK** = 4.0 (db),
jeżeli 3.75 > **OKZal** ≥ 3.25, to **OK** = 3.5 (dst),
jeżeli 3.25 > **OKZal** ≥ 3.00, to **OK** = 3.0 (dst).

Sposób i tryb wyrównywania zaległości powstałych wskutek nieobecności studenta na zajęciach:

Nie określono

Wymagania wstępne i dodatkowe, z uwzględnieniem sekwencyjności modułów

Nie podano wymagań wstępnych lub dodatkowych.

Zalecana literatura i pomoce naukowe

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.

Publikacje naukowe osób prowadzących zajęcia związane z tematyką modułu

1. Skupień, Zdzisław; Majorization and the minimum number of dominating sets; Discrete Appl. Math. 165, 295-302 (2014).

2. Skupień, Zdzisław; Sums of powered characteristic roots count distance-independent circular sets; Discuss. Math., Graph Theory 33, No. 1, 217-229 (2013).

3. Fortuna, Artur; Skupień, Zdzisław; Universal third parts of any complete 2-graph and none of DK 5; Opusc. Math. 33, No. 4, 685-696 (2013).

4. Euler, Reinhardt; Oleksik, Paweł; Skupień, Zdzisław;
Counting maximal distance-independent sets in grid graphs;
Discuss. Math., Graph Theory 33, No. 3, 531-557 (2013).

5. Meszka, Mariusz; Skupień, Zdzisław; Decompositions of a complete multidigraph into almost arbitrary paths; Discuss. Math., Graph Theory 32, No. 2, 357-372 (2012).

Informacje dodatkowe

Brak