유한체 이론 및 응용 (Take-Home Final Exam)

본대학원 전기전자공학과

기간: 6월 25일(월) 오전 10:00 - 6월 26일(화) 오전 10:00

총 5 pages. 총점: 7문항 x 100점 = 700점.

Open book, open note, open every materials, except for discussions with others

담당교수: 송홍엽 hysong@yonsei.ac.kr

답안지로는 반드시 A4용지를 사용하시오.

Staple once at the top-left corner.

PROMISE: (답안지 첫 페이지에 아래를 옮겨 적고 서명하시오)

> **본 시험의 답안을 작성함에 있어서 동료 수강생뿐만 아니라 어느 누구와도 상의하지 않고 스스로 혼자서 해결하였으며, 이 점이 사실이 아닌 것으로 밝혀질 경우, F학점을 포함한 어떤 penalty도 감수하겠습니다.   서명:___________________**

문제 해설

#1. Berlekamp's Algorithm of factoring polynomials

#2. Classification of cyclic projective equivalence of solutions to linear recursive equation over GF(q)

#3. Existence/Construction of (v, k, λ) cyclic difference sets

#4. finite projective planes and cyclic difference sets

#5. Proof that the cycle-and-add property implies m-sequence.

#6. Calculation of cross-correlations of pair of m-sequences

#7. Search project for balanced binary sequences of length 31 [programming]

#1. Factor the following polynomials using Berlekamp's algorithm:

a. $x^{12}+x^{11}+x^{10}+x^9+x^7+x^2+1$ over GF(2) = { 0, 1 }

b. $x^{12}+x^{11}+x^{10}+x^9+x^7+x^2+1$ over GF(4) = $\{0,1,\omega,\omega^2\}$ with $\omega^2=\omega+1$

c. $x^7-x^5-x^4-x^3-x^2-x-1$ over GF(3) = { 0, 1, -1 }

#2. Given that the following polynomials are irreducible over the given fields, find n, N, d, e, N_1, and the set of N_1 sequences of length d which represent all possible solutions to the recursion with characteristic polynomial $f(x)$ over $GF(q)$ up to cyclic projective equivalence.

a. $f(x) = x^3+x^2+x+2,\quad q=3$

b. $f(x) = x^5+2x^3+x^2+2x+2,\quad q=3$

c. $f(x) = x^2+3x+1,\quad q=7$

d. $f(x) = x^6+x^5+x^4+x^2+1,\quad q=2$

#3. For each of the following parameters of (v, k, λ), **either** (a) find a cyclic difference set with these parameters, and verify that it represents every non-zero residue mode v as differences exactly λ times, **or** (b) prove that such a cyclic difference set does not exist. In each case, assume that every prime divisor of $k-\lambda$ is a multiplier.

a. (15, 7, 3)　　b. (21, 5, 1)　　c. (27, 13, 6)　　d. (13, 4, 1)

e. (37, 9, 2)　　f. (29, 8, 2)　　g. (43, 7, 1)　　h. (19, 9, 4)

#4. Answer the following:

a. A finite projective plane of order n을 정의하고 각각의 parameter에 대해 정확히 설명하시오.

b. Fix $n=3$, and list the 13 lines and points of the finite projective plane of order 3.

c. Explain the relation with the plane in part b and the cyclic difference set with parameter ($v=13$, $k=4$, $\lambda=1$) [that you found in part d of #3.]

#5. Prove the following statement:

We are given a binary sequence $\{s(t)\}$ of period 31. For any $\tau \neq 0$ (mod 31), the sequence satisfies the condition that there exists a unique constant $\sigma(\tau)$ that depends on τ such that

$$s(t)+s(t+\tau)=s(t+\sigma(\tau)) \text{ for all } t.$$

Then $\{s(t)\}$ must be an m-sequence of period 31.

[Hint: try to find (or argue that there exists) a linear recursive relation among terms of $\{s(t)\}$.]

#6. Answer the series of questions regarding the cross-correlation of pair of m-sequences of period 31. [You may use your computer to solve the problem.]

a. Use x^5+x^2+1 as a characteristic polynomial to draw a 5-stage LFSR, and find an output sequence of period 31 with initial condition 00001.

b. Denote the above as $s(t)$ for $t=0,1,2,\dots,30$. Write down all possible decimations of $s(t)$. That is, define $s_d(t) = s(dt)$ for each d from 2 to 30, and write them down term-by-term. Note that $s(t)=s_1(t)$.

c. Determine those sequences from part c that are distinct with each others up to cyclic shifts. For this, let A be the set of those d's such that if $d_1 \neq d_2$ and both belong to A then the sequences $s_{d_1}(t)$ and $s_{d_2}(t)$ are not the same sequence up to cyclic equivalence. Determine the set A.

d. For every pair of integers (d_1, d_2) with $d_1 < d_2$ and both belong to A, calculate the periodic unnormalized cross-correlation $\phi_{d_1,d_2}(\tau)$ of $s_{d_1}(t)$ and $s_{d_2}(t)$ for all $\tau = 0, 1, \ldots, 30$, and make a table of the following type:

pair	number of distinct values of $\phi_{d_1,d_2}(\tau)$	distribution		
(d_1, d_2)	5(*)	−1(**)	7(***)	………(****)
		(#**)	(#***)	(#****)
⋮ (##)				

(*) – this is the number of distinct values that $\phi_{d_1,d_2}(\tau)$ takes on for $0 \le \tau \le 30$.

(**) and (***) and (****) – These are the values in the increasing order in absolute value.

(#) – You put the number of times that the value, for example −1 in (**), occurred in $\phi_{d_1,d_2}(\tau)$ for $0 \le \tau \le 30$.

(##) and (****) – use any more rows or columns as necessary.

For example, if $\phi_{1,3}(\tau)$ has values

−1, −1, −1, 7, 5, 5, 5, −3, −3, −1, 5, 1, 1, 1, 1, (period 15, for example)

then the table looks like the following:

pair	number of distinct values of $\phi_{d_1,d_2}(\tau)$	distribution				
(1,3)	5	-1	1	-3	5	7
		4	4	2	4	1

Note that, for example,

$$\phi_{1,3}(\tau) = \sum_{i=0}^{N-1} (-1)^{s_1(i) + s_3(i+\tau)}$$

where N is the period, and $s(i) \in \{0,1\}$.

#7. [Programming]

Let U be the set of all the balanced binary sequences of period 31. That is, in each sequence, the number of 0's is 16 and the number of 1's is 15. The size of U is *31_choose_15* which is 300540195.

Define various subsets of U as follows:

R=those that have the same run-distribution property as m-sequences;
S=those that have the same span-n property as m-sequences;
H=those that have the same autocorrelation property as m-sequences;
M=those that have the property that $s(t) = s(2t)$ for all t; and finally,
P=those that **are** m-sequences.

a. Write a program to search for those belong to the subset $A = R \cap M - P$. The output must list up all the sequences belonging to the subset A **up to cyclic equivalence**. That is, the output must list up all the cyclically distinct sequences that belong to A.

b. Repeat part a with the subset $R \cap H - P$.

c. Repeat part a with the subset $S \cap M - P$.

d. Repeat part a with the subset $S \cap H - P$.

※ Submit a diskette containing all your source programs in C (or C++) and executable files with comments (4 programs). Submit a printed list containing the result for parts a, b, c, and d. Some subset could be empty and in this case your program should write it so.

Have a GREAT Summer Vacation !