Almost perfect sequences from relative difference set

김강산, 송홍엽

Channel Coding Lab.

Yonsei University

{gs.kim, hysong}@yonsei.ac.kr

Motivation

- Perfect sequence는 여러 통신 시스템에 적용할 수 있는 이론적으로 최적의 수열임.
- 2진 수열은 4보다 긴 길이에서 알려진 수열이 없음, 여기서 Wolfman(1992 IT), Luke(1995 IEEE Trans. Aerospace)이 Almost perfect sequence라는 개념을 도입하여 이진 Almost perfect sequence를 연구함.
- Krengel(2010, SETA), Nogami(2016, IEICE)등이 Almost perfect sequence를 다상수열로 확장시키는 연구를 진행함.
- Kim(2020, ISITA)는 Relative Difference Set과 Almost perfect sequence의 관계를 규명하는 연구를 진행함.
- 본 논문에서는 RDS로부터 Almost perfect sequence 집합을 생성하기 위한 방법 및 조건을 제시한다.

Almost perfect sequence

- Perfect sequence: 수열 $\boldsymbol{s}$는 0이 아닌τ 에 대하여 $C_{\boldsymbol{s}}(\tau) = 0$ 이면 Perfect sequence이다.

- 강한 의미의 Almost perfect sequence정의: 수열 $\boldsymbol{s}$는 오직 두개의 τ를 제외하고 $C_{\boldsymbol{s}}(\tau) = 0$이면 거의 Almost perfect sequence이다.

- 보편적 의미의 Almost perfect sequence 정의: 수열 $\boldsymbol{s}$는 적은 개수의 τ를 제외하고 $C_{\boldsymbol{s}}(\tau) = 0$이면 거의 완벽수열이다.

Almost perfect sequence

정의 1 (Almost perfect sequence).

M<<L에 대하여
주기 L인 두수열 $\boldsymbol{r}$, $\boldsymbol{s}$를 고려하자. $\boldsymbol{r}$이 다음을 만족시키면 *(M,L)-APS* 이라고 한다.

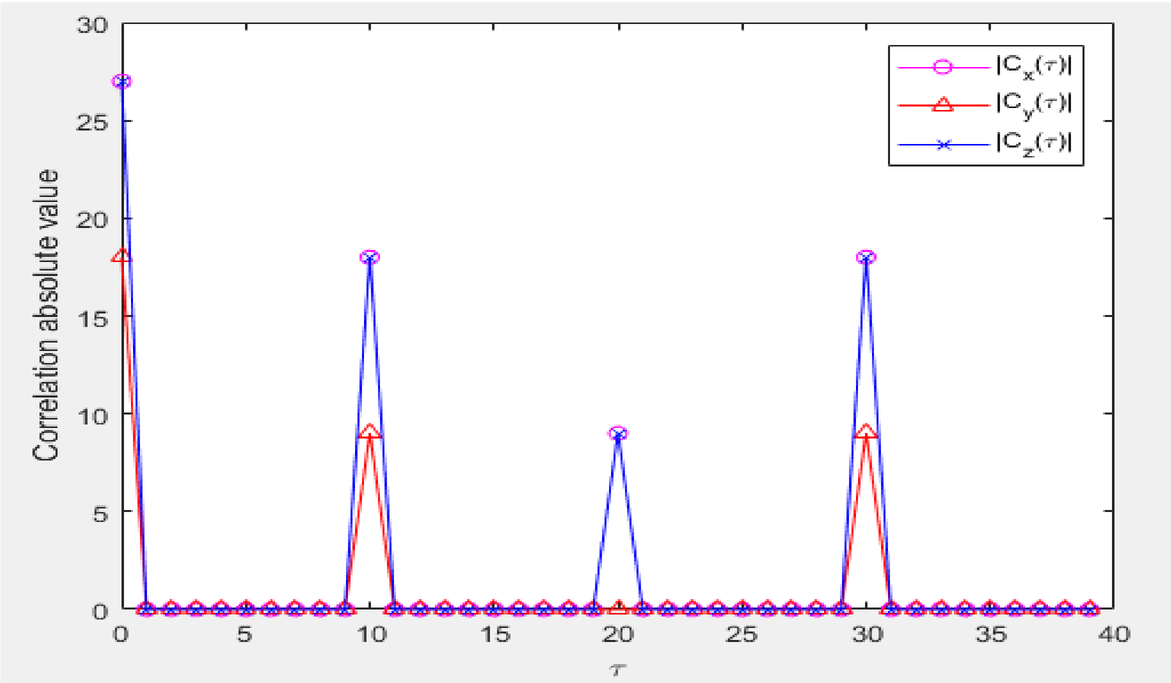
$$\left|\{0 \le \tau < \mathrm{L} \,|\, \mathrm{C}_{\boldsymbol{r},\boldsymbol{r}}(\tau) \neq 0\}\right| \le \mathrm{M}$$

두수열 $\boldsymbol{r}$, $\boldsymbol{s}$ 가 각각 *(M, L)*-거의완벽수열일 때, 다음을 만족시키면 수열 쌍 **(**$\boldsymbol{r}$, $\boldsymbol{s}$**)** 는 ***(M,L)*-APS 쌍** 이라고 한다.

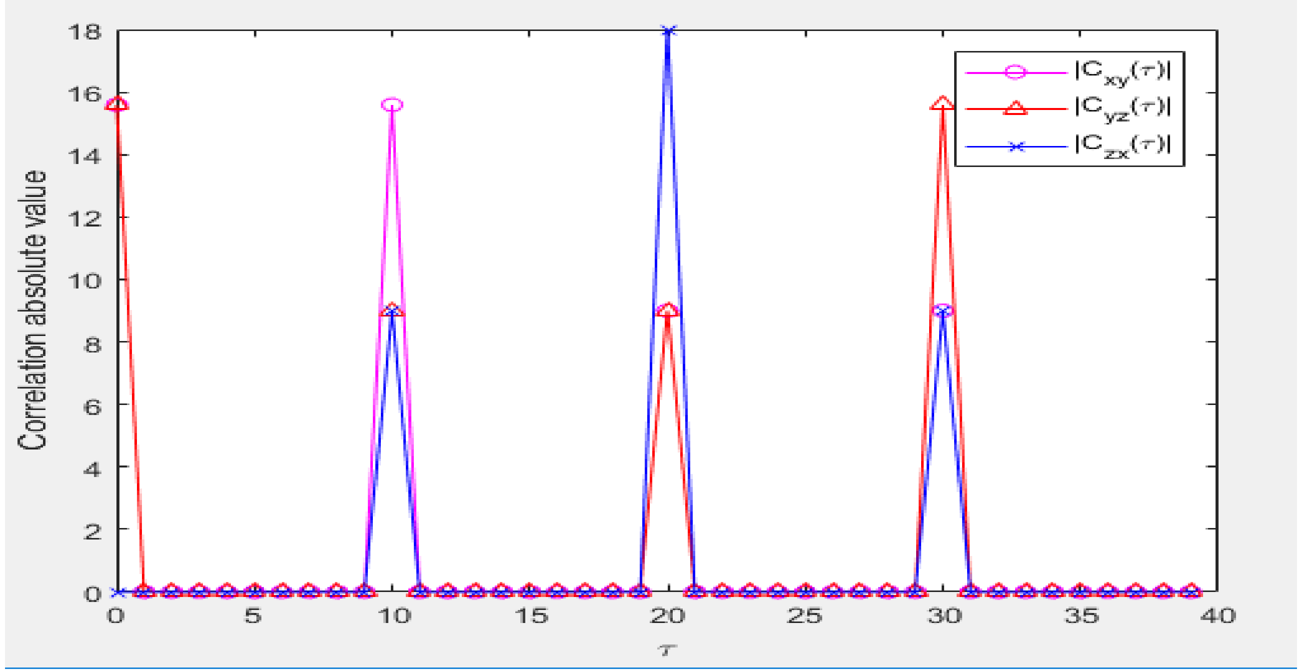
$$\left|\{0 \le \tau < \mathrm{L} \,|\, \mathrm{C}_{\boldsymbol{r},\boldsymbol{s}}(\tau) \neq 0\}\right| \le \mathrm{M}$$

수열 집합 S 에서 임의의수열쌍이 *(M,L)*-거의완벽수열쌍일 때, S를 거의 ***(M,L)*-APS 집합**이라고 한다.

RDS의 특성수열: Example



주기 40인 어떤 수열 $\mathbf{x}, \mathbf{y}, \mathbf{z}$의 자기상관 함수



주기 40인 어떤 수열 $\mathbf{x}, \mathbf{y}, \mathbf{z}$ 사이의 교차상관 함수

- ✓ 주기가 40인 세 수열 $\mathbf{x}, \mathbf{y}, \mathbf{z}$는 모두 $(4,40)$-APS이다.
- ✓ 세 수열쌍 $(\mathbf{x}, \mathbf{y})$, $(\mathbf{y}, \mathbf{z})$, $(\mathbf{x}, \mathbf{z})$는 모두 $(4,40)$-APS 쌍이다.
- ✓ 수열 집합 $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$는 $(4,40)$-APS 집합이다.

Relative difference set

정의 2(Relative difference sets)

4개의 양수 u, v, k, λ . $\mathbb{Z}_{\mathrm{uv}}$ 의 k개의 원소를 갖는 부분집합 $D = \{d_1, d_2, \ldots, d_k\}$이 다음을 만족시키면 (u, v, k, λ)–RDS라고 한다.

Ⅰ. $\{d_i - d_j \mid d_i \neq d_j, \text{ for } d_i, d_j \in D\} = \mathbb{Z}_{\mathrm{uv}} \setminus \mathrm{u}\mathbb{Z}_{\mathrm{uv}}$

Ⅱ. For any $d \in \mathbb{Z}_{\mathrm{uv}} \setminus \mathrm{u}\mathbb{Z}_{\mathrm{uv}}$, $|D \cap (d + D)| = \lambda$.

성질 1(RDS의 성질)

임의의 (u, v, k, λ)–RDS $D = \{d_1, d_2, \ldots, d_k\}$와 임의의 $c \in u\mathrm{Z}_{uv}$, $\mathrm{d} \in \mathrm{Z}_{uv} \setminus u\mathrm{Z}_{uv}$에 대하여 다음을 만족한다.

Ⅰ. $\{d_i - d_j \mid d_i \neq c + d_j, \text{ for } d_i \in c + D,\ d_j \in D\} = \mathbb{Z}_{\mathrm{uv}} \setminus \mathrm{u}\mathbb{Z}_{\mathrm{uv}}$

Ⅱ. $|(c + D) \cap (d + D)| = \lambda$.

Ⅲ. If $c = 0$, then $|(c + D) \cap D| = 0$

Ⅳ. $(u - 1)v\lambda = k(k - 1)$

Relative Difference Set Example

- D={17, 31, 32, 39, 44, 48, 50, 73, 76} is a $(u=10, v=8, k=9, \lambda=1)$-RDS

D

	17	31	32	39	44	48	50	73	76
17	0	14	15	22	27	31	33	56	59
31	66	0	1	8	13	17	19	42	45
32	65	79	0	7	12	16	18	41	44
39	58	72	73	0	5	9	11	34	37
44	53	67	68	75	0	4	6	29	32
48	49	63	64	71	76	0	2	25	28
50	47	61	62	69	74	78	0	23	26
73	24	38	39	46	51	55	57	0	3
76	21	35	36	43	48	52	54	77	0

D

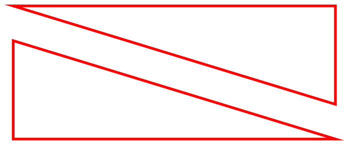
$$\mathbb{Z}_{80} \backslash 10\mathbb{Z}_{80}$$

Relative Difference Set Example

- D={17, 31, 32, 39, 44, 48, 50, 73, 76} is a $(u=10, v=8, k=9, \ \lambda=1)$-RDS

	17	31	32	39	44	48	50	73	76
17	0	14	15	22	27	31	33	56	59
31	66	0	1	8	13	17	19	42	45
32	65	79	0	7	12	16	18	41	44
39	58	72	73	0	5	9	11	34	37
44	53	67	68	75	0	4	6	29	32
48	49	63	64	71	76	0	2	25	28
50	47	61	62	69	74	78	0	23	26
73	24	38	39	46	51	55	57	0	3
76	21	35	36	43	48	52	54	77	0

Counting in two ways



①: # of possible $(d_i - d_j)$ × # of solution of $(d_i - d_j = d)$

$=|\mathbb{Z}_{80} \backslash 10\mathbb{Z}_{80}| \times \lambda = (u-1)v\lambda = 72$

②: # of coordinates except for the diagonal

$= k(k-1) = 72$

Relative Difference Set Example: Ⅱ

- D={17, 31, 32, 39, 44, 48, 50, 73, 76} is a $(u = 10, v = 8, k = 9,\ \lambda = 1)$-RDS

$\overbrace{\qquad\qquad}^{10 + D}$

D	27	41	42	49	54	58	60	3	6
17	10	24	25	32	37	41	43	66	69
31	76	10	11	18	23	27	29	52	55
32	75	9	10	17	22	26	28	51	54
39	68	2	3	10	15	19	21	44	47
44	63	77	78	5	10	14	16	39	42
48	59	73	74	1	6	10	12	35	38
50	57	71	72	79	4	8	10	33	36
73	34	48	49	56	61	65	67	10	13
76	31	45	46	53	58	62	64	7	10

$$\mathbb{Z}_{80} \backslash 10\mathbb{Z}_{80}$$

Relative Difference Set Example: Ⅱ

- D={17, 31, 32, 39, 44, 48, 50, 73, 76} is a $(u = 10, v = 8, k = 9,\ \ \lambda = 1)$-RDS

$20 + D$

D \ $20+D$	37	51	52	59	64	68	70	13	16
17	20	34	35	42	47	51	53	76	79
31	6	20	21	28	33	37	39	62	65
32	5	19	20	27	32	36	38	61	64
39	78	12	13	20	25	29	31	54	57
44	73	7	8	15	20	24	26	49	52
48	69	3	4	11	16	20	22	45	48
50	67	1	2	9	14	18	20	43	46
73	44	58	59	66	71	75	77	20	23
76	41	55	56	63	68	72	74	17	20

$$\mathbb{Z}_{80} \setminus 10\mathbb{Z}_{80}$$

Relative Difference Set Example: Ⅱ

- D={17, 31, 32, 39, 44, 48, 50, 73, 76} is a $(u = 10, v = 8, k = 9, \lambda = 1)$-RDS

$30 + D$

D

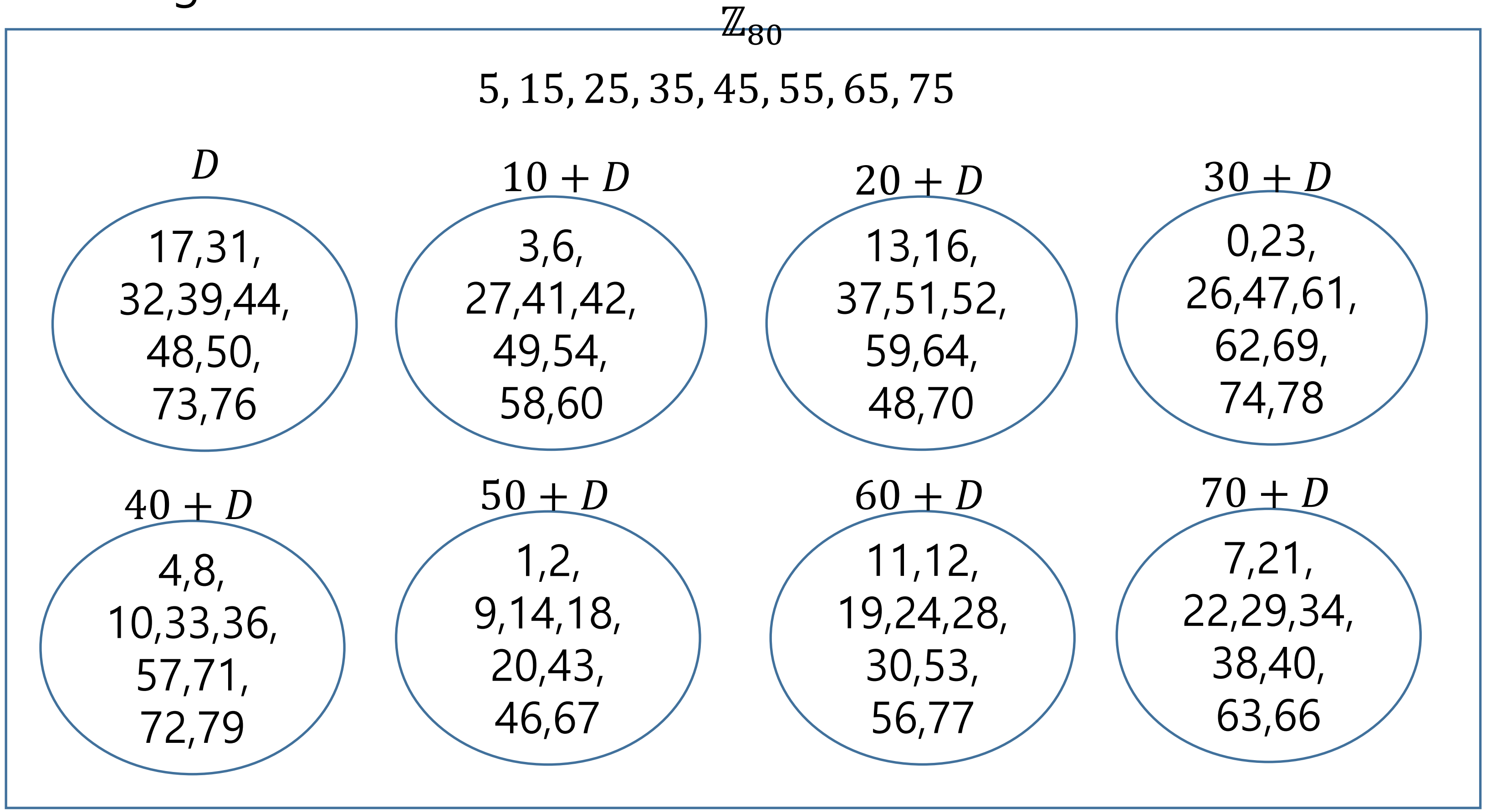
	47	61	62	69	74	78	0	23	26
17	30	44	45	52	57	61	63	6	9
31	16	30	31	38	43	47	49	72	75
32	15	29	30	37	42	46	48	71	74
39	8	22	23	30	35	39	41	64	67
44	3	17	18	25	30	34	36	59	62
48	79	13	14	21	26	30	32	55	58
50	77	11	12	19	24	28	30	53	56
73	54	68	69	76	1	5	7	30	33
76	51	65	66	73	78	2	4	27	30

$\mathbb{Z}_{80} \backslash 10\mathbb{Z}_{80}$

Relative Difference Set Example:

- D={17, 31, 32, 39, 44, 48, 50, 73, 76} is a $(u = 10, v = 8, k = 9,\ \lambda = 1)$-RDS

Bendiagram



RDS의 특성수열

정의 3(RDS 특성수열)

(u, v, k, λ) -RDS인 D, v -tuple의 복소 벡터 $\underline{a} = (a_0, a_1, \dots, a_{v-1})$, 상수 c에 대하여 주기 uv인 ($\underline{a}$, c, D)의 특성 수열 $\boldsymbol{x}$ 는 다음과 같이 정의된다.

$$x_t = \begin{cases} a_l & \text{If } t \in lu + D, \text{ for } l = 0,1,\dots,v-1 \\ c & \text{otherwise} \end{cases}$$

RDS의 특성수열: Example

$H=\{t \in \mathbb{Z}_{80} | \mathrm{Tr}_1^2(\alpha^t) = 1\}=\{17, 31, 32, 39, 44, 48, 50, 73, 76\}$ 는 (10,8,9,1)-RDS

$D=\{t (\mathrm{mod}\ 40) | t \in H\}=\{4, 8, 10, 17, 31, 32, 33, 36, 39\}$ 는 (10,4,9,2)-RDS, $D+10=\{1, 2, 3, 6, 9, 14, 18, 20, 27\}$

$D+20=\{11, 12, 13, 16, 19, 24, 28, 30, 37\}$, $D+30=\{0, 7, 21, 22, 23, 26, 29, 34, 38\}$

주기 40인 수열 $\boldsymbol{s}^{(k)}$ $\left((\mathrm{j}^{\mathrm{k}}, \mathrm{j}^{2\mathrm{k}}, \mathrm{j}^{3\mathrm{k}}, \mathrm{j}^{4\mathrm{k}}), c_k, \mathrm{D}\right)$의 특성 수열로 정의하자.

(k =1,2,3, $c_0 = 0, c_1 = 1, c_2 = j$)

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$s^{(1)}$ (t)	+1	-1	-1	-1	+j	0	-1	+1	+j	-1	+j	-j	-j	-j	-1	0	-j	+j	-1	-j
$s^{(2)}$ (t)	+1	+1	+1	+1	-1	+1	+1	+1	-1	+1	-1	-1	-1	-1	+1	+1	-1	-1	+1	-1
$s^{(3)}$ (t)	+1	-1	-1	-1	-j	+j	-1	+1	-j	-1	-j	+j	+j	+j	-1	+j	+j	-j	-1	+j

t	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
$s^{(1)}$ (t)	-1	+1	+1	+1	-j	0	+1	-1	-j	+1	-j	+j	+j	+j	+1	0	+j	-j	+1	+j
$s^{(2)}$ (t)	+1	+1	+1	+1	-1	+1	+1	+1	-1	+1	-1	-1	-1	-1	+1	+1	-1	-1	+1	-1
$s^{(3)}$ (t)	-1	+1	+1	+1	+j	+j	+1	-1	+j	+1	+j	-j	-j	-j	+1	+j	-j	+j	+1	-j

RDS의 특성수열

정리 1 거의완벽 RDS 특성수열의 상관값

(u,v,k,λ) -RDS인 D, v -tuple의 복소 벡터 $\underline{a}=(a_0,a_1,\dots,a_{v-1})$, $\underline{b}=(b_0,b_1,\dots,b_{v-1})$에 대하여 주기 uv인 $(\underline{a},\ c_x,\ D)$의 특성 수열 $\boldsymbol{x}$ 와 주기 uv인 $(\underline{b},\ c_y,\ D)$의 특성 수열 $\boldsymbol{y}$의 교차상관 $C_{\boldsymbol{x},\boldsymbol{y}}(\tau)$는 $l=0,1,\dots,v-1$에 대하여 $\tau=lu$ 일 경우

$$k\underline{a}\cdot\overline{T^l(\underline{b})}+(uv-vk)c_x\overline{c_y}$$

로 계산되고 $\tau\in Z_{uv}\backslash uZ_{uv}$일 경우

$$\lambda\left(\sum_{i=0}^{v-1}a_i\right)\left(\sum_{i=0}^{v-1}\overline{b_i}\right)+(k-v\lambda)\left\{\left(\sum_{i=0}^{v-1}a_i\right)\overline{c_y}+\left(\sum_{i=0}^{v-1}\overline{b_i}\right)c_x\right\}+(uv+v^2\lambda-2vk)c_x\overline{c_y}$$

로 계산된다.

RDS의 특성수열

(u, v, k, λ) -RDS인 D, v -tuple의 복소 벡터 $\underline{a} = (a_0, a_1, \ldots, a_{v-1})$, $\underline{b} = (b_0, b_1, \ldots, b_{v-1})$에 대하여 주기 uv인 ($\underline{a}$, $\mathrm{c_x}$, D)의 특성 수열 $\boldsymbol{x}$ 와 주기 uv인 ($\underline{b}$, $\mathrm{c_y}$, D)의 특성 수열 $\boldsymbol{y}$에 대하여

따름 정리 1

$\sum_{i=0}^{v-1} a_i = 0$, $c_x = 0$ 이면 $\boldsymbol{x}$는 (v, uv)-APS이다.

따름 정리 2

$\sum_{i=0}^{v-1} a_i = 0$, $\sum_{i=0}^{v-1} b_i = 0$, $c_x = 0, c_y = 0$ 이면 $(\boldsymbol{x}, \boldsymbol{y})$는 (v, uv)-APS 쌍이다.

RDS의 특성수열: Example

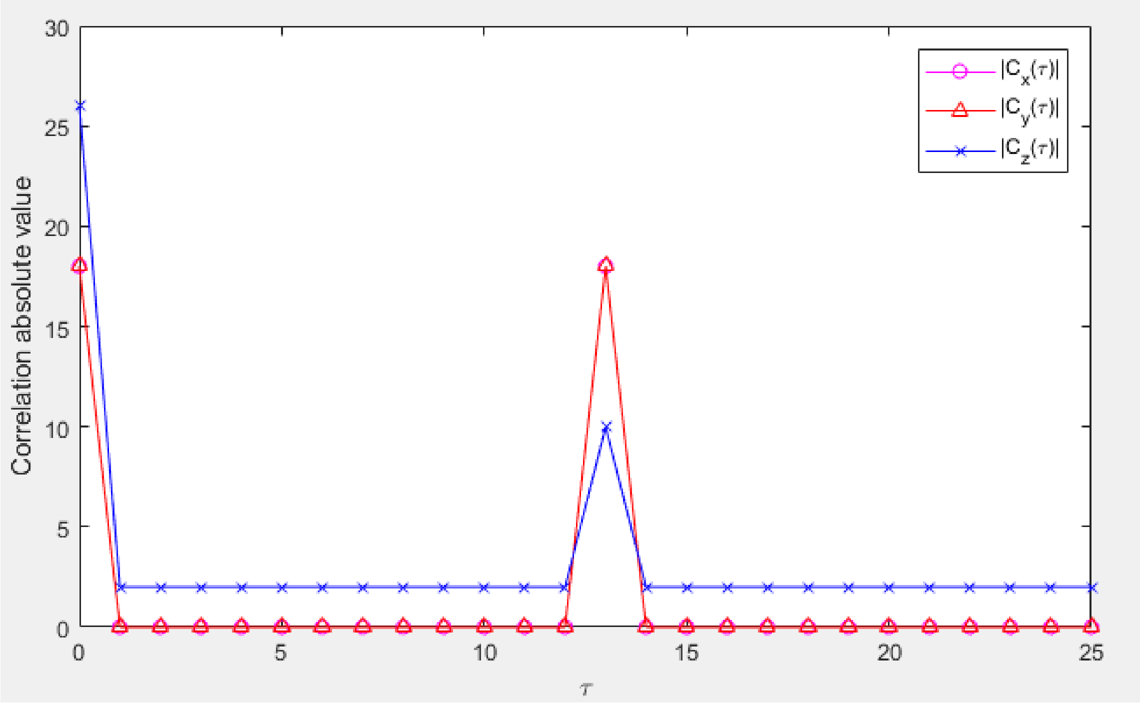
$D=\{t \in \mathbb{Z}_{26} | Tr_1^3(\alpha^t) = 1\}=\{1,2,3,6,7,9,11,18,21\}$ 는 (13,2,9,3)-RDS, $D+13=\{5,8,14,15,16,19,20,22,24\}$

주기 20인 수열 $\boldsymbol{x}$ 는$((-1,+1), 0, D)$의 특성 수열, 주기 20인 수열$\boldsymbol{y}$는 $((-j,+j), 0, D)$의 특성수열, 주기 20인 수열 $\boldsymbol{z}$는 $((-j,+j), 1, D)$의 특성수열로 정의하자.

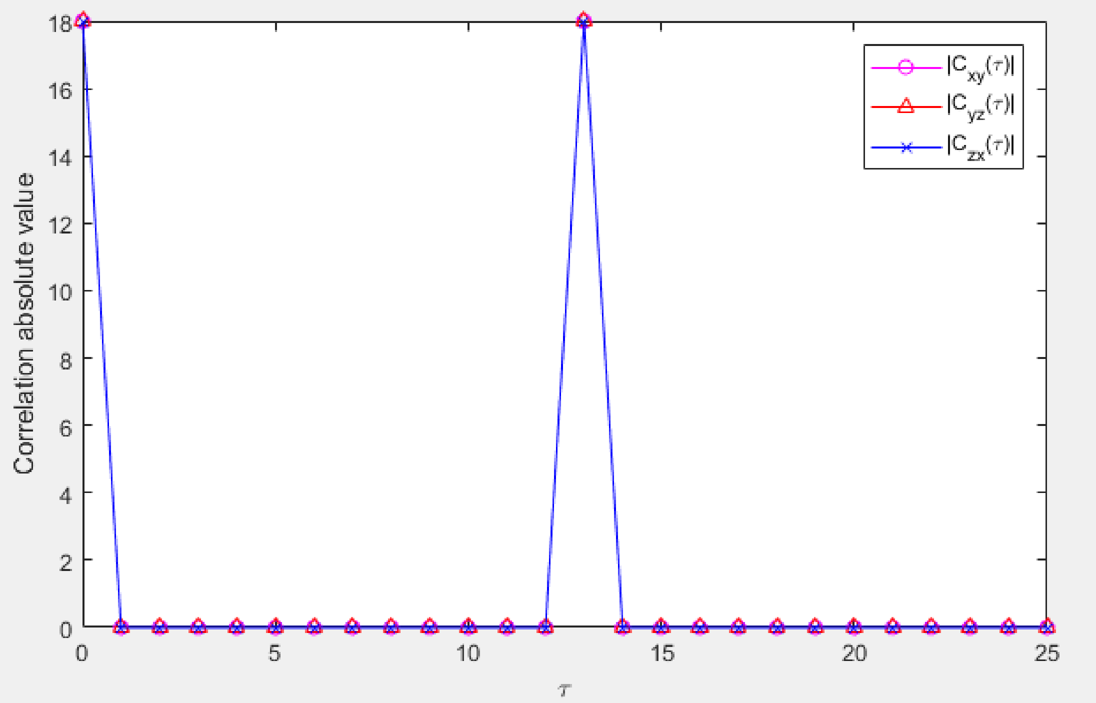
t	0	1	2	3	4	5	6	7	8	9	10	11	12
x(t)	0	-1	-1	-1	0	+1	-1	-1	+1	-1	0	-1	0
y(t)	0	$-j$	$-j$	$-j$	0	$+j$	$-j$	$-j$	$+j$	$-j$	0	$-j$	0
z(t)	+1	$-j$	$-j$	$-j$	+1	$+j$	$-j$	$-j$	$+j$	$-j$	+1	$-j$	+1

t	13	14	15	16	17	18	19	20	21	22	23	24	25
x(t)	0	+1	+1	+1	0	-1	+1	+1	-1	+1	0	+1	0
y(t)	0	$+j$	$+j$	$+j$	0	$-j$	$+j$	$+j$	$-j$	$+j$	0	$+j$	0
z(t)	+1	$+j$	$+j$	$+j$	+1	$-j$	$+j$	$+j$	$-j$	$+j$	+1	$+j$	+1

RDS의 특성수열: Example



(13,2,9,3)-RDS D의 특성 수열 $\boldsymbol{x}$, $\boldsymbol{y}, \boldsymbol{z}$의 자기상관 함수



(13,2,9,3)-RDS D의 특성 수열 $\boldsymbol{x}$, $\boldsymbol{y}, \boldsymbol{z}$의 서로간의 교차상관 함수

- ✓ 수열 집합($\boldsymbol{x}$, $\boldsymbol{y}$) 는 (2,26)-APS 쌍이다.
- ✓ 수열 $\boldsymbol{z}$는 APS가 아니다.

RDS의 특성수열

(u, v, k, λ) -RDS인 D, v -tuple의 복소 벡터 $\underline{a} = (a_0, a_1, \dots, a_{v-1})$, $\underline{b} = (b_0, b_1, \dots, b_{v-1})$에 대하여 주기 uv인 ($\underline{a}$, $\mathrm{c_x}$, D)의 특성 수열 $\boldsymbol{x}$ 와 주기 uv인 ($\underline{b}$, $\mathrm{c_y}$, D)의 특성 수열 $\boldsymbol{y}$에 대하여

따름 정리 3

$\sum_{i=0}^{v-1} a_i = 0$, $\mathrm{k} = u - 1$ 이면 $\boldsymbol{x}$는 (v, uv)-APS이다.

따름 정리 4

$\sum_{i=0}^{v-1} a_i = 0$, $\sum_{i=0}^{v-1} b_i = 0$, $\mathrm{k} = u - 1$이면 $(\boldsymbol{x}, \boldsymbol{y})$는 (v, uv)-APS 쌍이다.

RDS의 특성수열: Example

$H=\{t \in \mathbb{Z}_{80} | \mathrm{Tr}_1^2(\alpha^t) = 1\}=\{17, 31, 32, 39, 44, 48, 50, 73, 76\}$ 는 (10,8,9,1)-RDS

$D=\{t(\mathrm{mod}\ 40) | t \in H\}=\{4, 8, 10, 17, 31, 32, 33, 36, 39\}$ 는 (10,4,9,2)-RDS, $D+10=\{1, 2, 3, 6, 9, 14, 18, 20, 27\}$

$D+20=\{11, 12, 13, 16, 19, 24, 28, 30, 37\}$, $D+30=\{0, 7, 21, 22, 23, 26, 29, 34, 38\}$

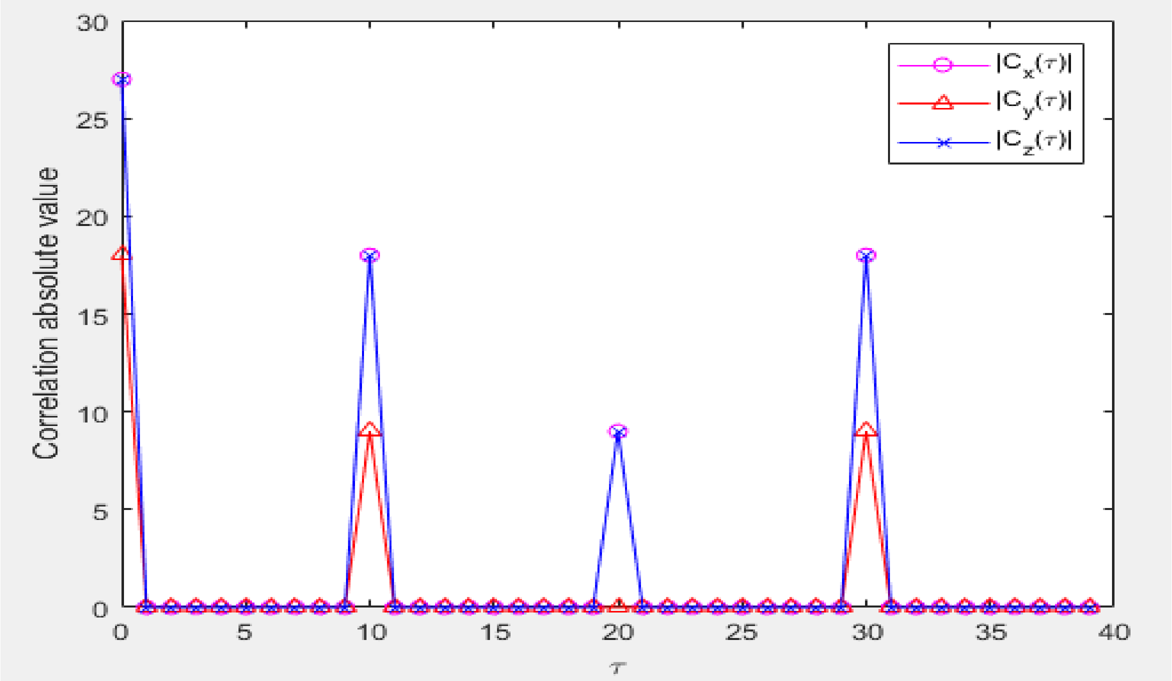
주기 40인 수열 $\boldsymbol{s}^{(k)}$ $\left((\mathrm{j}^{k}, \mathrm{j}^{2k}, \mathrm{j}^{3k}, \mathrm{j}^{4k}), c_k, \mathrm{D}\right)$의 특성 수열로 정의하자.

(k =1,2,3, $c_0 = 0, c_1 = 1, c_2 = j$)

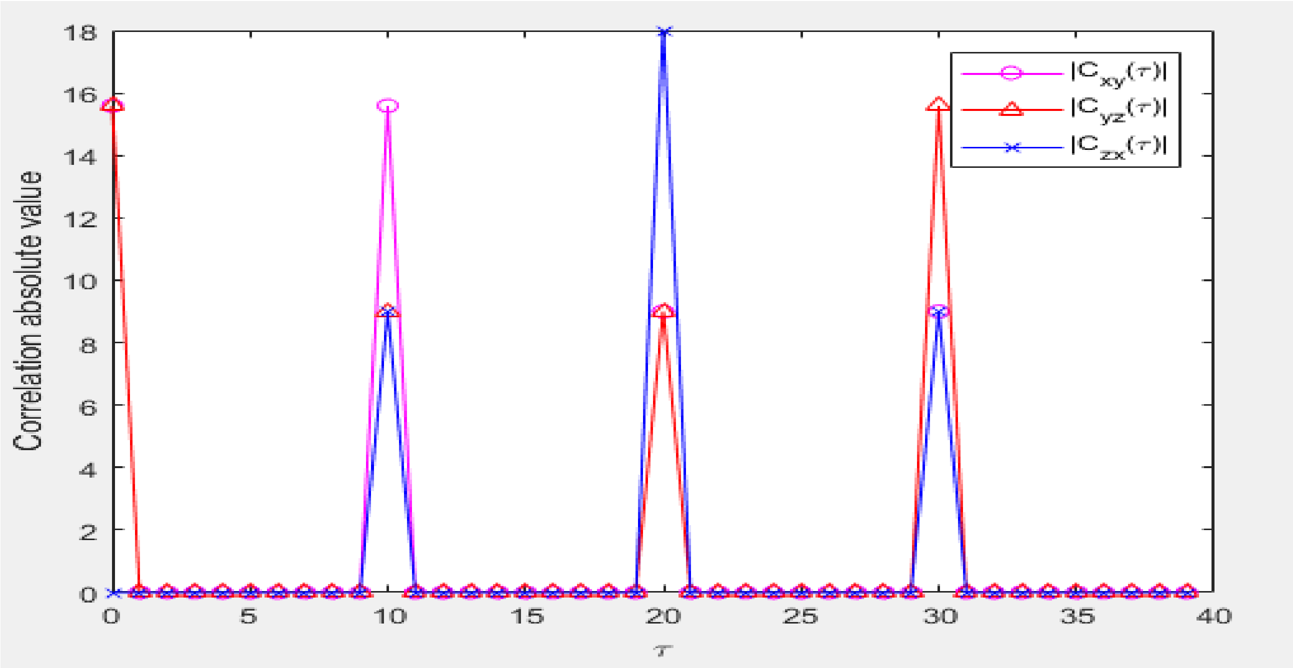
t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$s^{(1)}$ (t)	+1	-1	-1	-1	+j	0	-1	+1	+j	-1	+j	-j	-j	-j	-1	0	-j	+j	-1	-j
$s^{(2)}$ (t)	+1	+1	+1	+1	-1	+1	+1	+1	-1	+1	-1	-1	-1	-1	+1	+1	-1	-1	+1	-1
$s^{(3)}$ (t)	+1	-1	-1	-1	-j	+j	-1	+1	-j	-1	-j	+j	+j	+j	-1	+j	+j	-j	-1	+j

t	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
$s^{(1)}$ (t)	-1	+1	+1	+1	-j	0	+1	-1	-j	+1	-j	+j	+j	+j	+1	0	+j	-j	+1	+j
$s^{(2)}$ (t)	+1	+1	+1	+1	-1	+1	+1	+1	-1	+1	-1	-1	-1	-1	+1	+1	-1	-1	+1	-1
$s^{(3)}$ (t)	-1	+1	+1	+1	+j	+j	+1	-1	+j	+1	+j	-j	-j	-j	+1	+j	-j	+j	+1	-j

RDS의 특성수열: Example



(10,4,9,2)-RDS D의 특성 수열 $\boldsymbol{s}^{(1)}, \boldsymbol{s}^{(2)}, \boldsymbol{s}^{(3)}$의 자기상관 함수



(10,4,9,2)-RDS D의 특성 수열 $\boldsymbol{s}^{(1)}, \boldsymbol{s}^{(2)}, \boldsymbol{s}^{(3)}$의 서로간의 교차 상관 함수

✓ 수열 집합$\{\boldsymbol{s}^{(1)}, \boldsymbol{s}^{(2)}, \boldsymbol{s}^{(3)}\}$는 (4,40)-APS 집합이다.

결론

- 본 논문에서는 Relative difference set의 특성수열을 정의하고 그 특성수열들이 Almost perfect sequence 또는 Almost perfect sequence 쌍을 생성하기위한 조건들을 제시했다.

- 제시된 조건들로 부터 다양한 성질을 갖는 Almost perfect sequence 설계를 추후 연구로 진행할 수 있다.