최적 상관특성을 갖는 주파수 도약패턴 집합의 설계

Constructions for Frequency Hopping Patterns Having An Optimum Hamming Correlation

은유창, 김정헌, 송홍엽

연세대학교 전자공학과 컴퓨터응용 연구실

처음 페이지로 이동

<발 표 순 서>

- **FHMA(Frequency Hopping Multiple Access)**

  주파수 도약패턴 설계를 위한 수학적 모델

  주파수 도약패턴 설계 방법

  - 곱셈표 이용방법

  - 원시근 이용방법

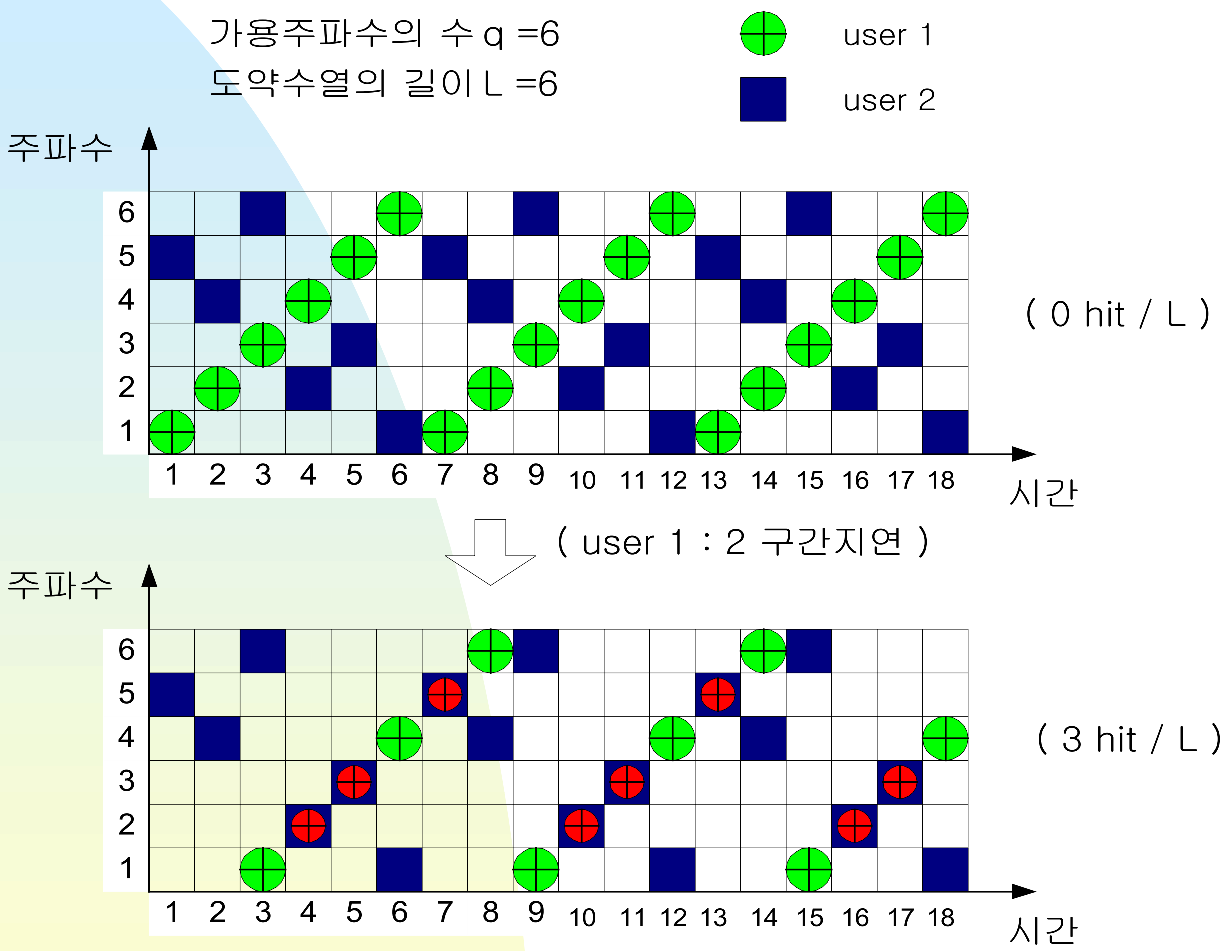
  - M-sequence를 이용하는 방법

  - RS 부호를 이용하는 방법

  - (n,k) 수열 이용하는 방법

  결론

< Frequency Hopping Multiple Access>



- 도약수열의 심볼이 반송 주파수에 해당
- 일정 시간마다 반송주파수를 바꿔 가며 사용
- 패턴(도약수열)간 간섭을 최소화하는 것이 목표
- 최대 해밍거리 부호

< 주파수 도약패턴 설계를 위한 수학적 모델 >

- **q :** 가용주파수의 수 **(** 도약 수열의 심볼**)**
  L : 도약패턴**(**수열**)**의 길이**,**
  N : 도약수열의 수

- 가용주파수**q**에 대응하는 **q**개의 심볼 도약수열 ***X***와 ***Y***의 정의

$$X = (x(0), x(1), x(2)\cdots, x(L))$$

$$Y = (y(0), y(1), y(2)\cdots, y(L))$$

- ***X***와 ***Y***의 상호상관함수

$$H_{XY}(\tau) = \sum_{j=0}^{L-1} h[x(j), y(j+\tau)], \qquad 0 \le \tau \le L-1$$

$$h[x, y] = \begin{cases} 0, & if \quad x \ne y \\ 1, & if \quad x = y \end{cases}$$

- ***X***의 자기상관함수

$$H_X(\tau) = \sum_{j=0}^{L-1} h[x(j), x(j+\tau)], \qquad 0 \le \tau \le L-1$$

- 도약수열의 전체집합 ***S***에 속하는 수열 ***X***와 ***Y***에 대하여 다음을 정의하자.

$$H(X) = \max_{0<\tau\le L-1}\{H_X(\tau)\}$$

$$H(X,Y) = \max_{0\le\tau\le L-1}\{H_{XY}(\tau)\}$$

$$M(X,Y) = \max\{H(X), H(Y), H(X,Y)\}$$

- 어떤 수열 ***X*** 와 ***Y*** 가 ***S***속하는 모든 X'와 Y'에 대하여

$M(X,Y) \le M(X',Y') \quad \Leftrightarrow$ ***X*** 와 ***Y*** 는 최적 상관함수를 갖는다.

- ***S*** 의 부분 집합으로서 ***N*** 개의 수열을 포함하는 집합 ***F*** 를 정의하자.

집합 ***F***에 속하는 모든 수열쌍 ***X*** 와 ***Y*** 의 상관함수가 최적이다

$$\Rightarrow \quad M(X,Y) = M(X',Y') \quad \text{for all } X, Y, X', Y' \in F$$

- N개의 수열을 포함하는 집합 F에서 최대상관함수 값의 하한식

(Definition)

$$H_a(F) = \max_{X \in F} \{H(X)\}$$

$$H_c(F) = \max_{\substack{X,Y \in F \\ Y \neq X}} \{H(X,Y)\}$$

$$H_{\max}(F) = \max\{H_a(F),\ H_c(F)\}$$

$\Rightarrow$

(Bound)

$$H_{\max}(F) > \frac{L}{q} - \frac{1}{N}$$

$$H_{\max}(F) \geq \lceil \log_q(LN) \rceil - 1$$

연세대학교 전자공학과 컴퓨터 응용 연구실

< 주파수 도약패턴 설계 방법 >

곱셈표 이용방법

$$L = q \quad , \qquad q \text{ is a prime.}$$
$$N = q - 1$$
$$F = \{X_1, X_2, X_3, \cdots X_{q-1}\}$$
$$H_{\max}(F) = 1$$

$\Rightarrow$

$$1 \le i \le q - 1$$
$$0 \le t \le q - 1$$
$$X_i(t) = (it \mod q)$$

(예제)

$q = 7,\ L=7,\ N = 6$	t = 0 1 2 3 4 5 6
$X_1(t) = (t \mod 7)$	$X_1 =$ 0 1 2 3 4 5 6
$X_2(t) = (2t \mod 7)$	$X_2 =$ 0 2 4 6 1 3 5
$X_3(t) = (3t \mod 7)$	$X_3 =$ 0 3 6 2 5 1 4
$X_4(t) = (4t \mod 7)$	$X_4 =$ 0 4 1 5 2 6 3
$X_5(t) = (5t \mod 7)$	$X_5 =$ 0 5 3 1 6 4 2
$X_6(t) = (6t \mod 7)$	$X_6 =$ 0 6 5 4 3 2 1

원시근 이용방법

$L = q - 1, \quad q$ is a prime.

$N = q$

α is a primitive root of GF(q)

$F = \{X_0, X_1, X_2, \cdots X_{q-1}\}$

$H_{\max}(F) = 1$

$\Rightarrow$

$$0 \le i \le q - 1$$

$$1 \le t \le q - 1$$

$$X_i(t) = ((\alpha^t + i) \bmod q)$$

(예제)

$q=7, N=7, L=6, \alpha = 3$	t = 1 2 3 4 5 6
$X_0(t) = ((3^t+0) \bmod 7)$	$X_0 = 3\ 2\ 6\ 4\ 5\ 1$
$X_1(t) = ((3^t+1) \bmod 7)$	$X_1 = 4\ 3\ 0\ 5\ 6\ 2$
$X_2(t) = ((3^t+2) \bmod 7)$	$X_2 = 5\ 4\ 1\ 6\ 0\ 3$
$X_3(t) = ((3^t+3) \bmod 7)$	$X_3 = 6\ 5\ 2\ 0\ 1\ 4$
$X_4(t) = ((3^t+4) \bmod 7)$	$X_4 = 0\ 6\ 3\ 1\ 2\ 5$
$X_5(t) = ((3^t+5) \bmod 7)$	$X_5 = 1\ 0\ 4\ 2\ 3\ 6$
$X_6(t) = ((3^t+6) \bmod 7)$	$X_6 = 2\ 1\ 5\ 3\ 4\ 0$

M-sequence를 이용하는 방법

- 곱셈표 : $L = q$
  원시근 : $L = q - 1$

$\xrightarrow{}$ (**L 증가 가능**)

- M-sequence : $L = p^n - 1$
  (for all n , a prime p)

- For any k $(k \le n)$

심볼수	$q = p^k$	수열의 수	$N = q$
수열 길이	$L = p^n - 1$	최대 상관값	$H_{\max}(F) = p^{n-k}$

- 위 파라미터는 최적집합인가? **(Recall :** 최대 상관함수의 하한식**)**

$$H_{\max}(F) > \frac{L}{q} - \frac{1}{N}$$

$$= p^{n-k} - \frac{1}{p^k}$$

$\xrightarrow{}$ ($H_{\max}$는 정수)

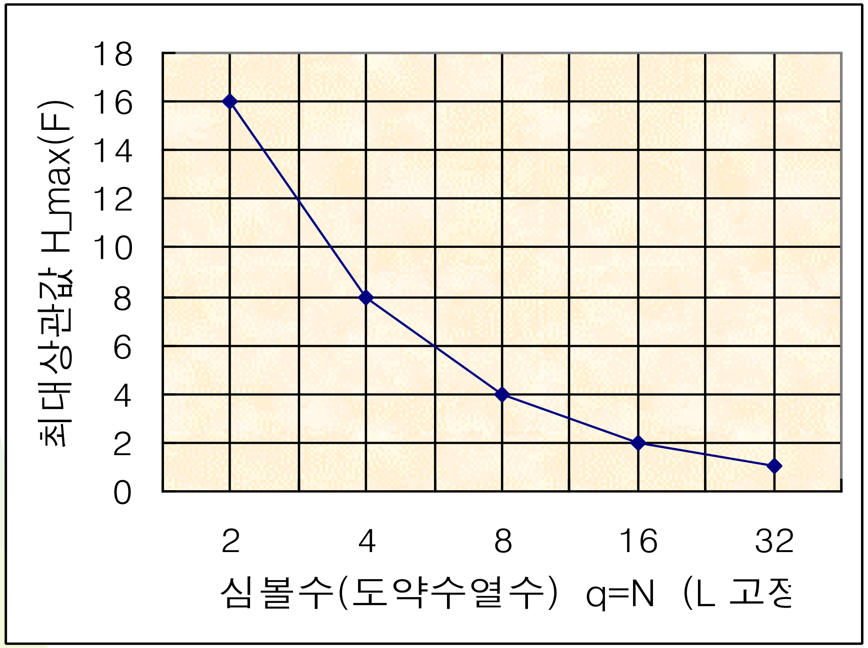
$$H_{\max}(F) \ge p^{n-k}$$

OK !

■ (예제 1) $L = 2^5 - 1 = 31$ 일 때 $N = q = 2^k$, $H_{\max}(F) = 2^{n-k}$

심볼수 (도약수열수) **q**

vs 최대상관값 $H_{max}(F)$



➲ 심볼수가 커질수록 도약수열 개수가 따라서 증가하고, 최대 상관값이 작아진다.

연세대학교 전자공학과 컴퓨터 응용 연구실

처음 페이지로 이동

➲ 도약패턴 생성 방법

(Define)

- $X = (x(0), x(1), x(2), \ldots, x(L-1))$: **M-sequence over GF(*p*), *L* = *p*^{n} - 1**
- $F = \{Y_0, Y_1, Y_2, \cdots Y_{q-1}\}$: 최적집합, $N = q = p^k$
- $Y_v = (y_v(0), y_v(1), y_v(2), \ldots, y_v(j), \ldots, y_v(L-1))$: ***v*** **user**의 도약수열

☞어떤 **k** ($k \le n$) 에 대하여 $y_v(j)$ 를 다음과 같이 구할 수 있다.

(1) $$v = \sum_{i=0}^{k-1} v_i p^i$$

▸ p^k 진수를 p 진수로 나타냄

(2) $$y_v(j) = \sum_{i=0}^{k-1} (x(j+i) + v_i) p^i \quad (\bmod\ q)$$

▸ **X**벡터의 **j**번째 원소부터 **k**개를 **v**벡터와 **mod p**로 더한다.

▸ p 진수를 p^k 진수로 결합한다.

M-sequence를 이용한 도약패턴 생성 예제

P=3, k=2 < n=3 인 경우, $q = p^k = 9$, $L = p^n - 1 = 26$,

$N = q = 9$, $F = \{Y_0, Y_1, Y_2, \ldots, Y_7\}$ $H_{\max}(F) = p^{n-k} = 3$

$$X = 0\,0\,1\,1\,1\,0\,2\,1\,1\,2\,1\,0\,1\,0\,0\,2\,2\,2\,0\,1\,2\,2\,1\,2\,0\,2$$

$$Y_0 = 0\,3\,4\,4\,1\,6\,5\,4\,7\,5\,1\,3\,1\,0\,6\,8\,8\,2\,3\,7\,8\,5\,7\,2\,6\,2$$

$$Y_1 = 1\,4\,5\,5\,2\,7\,3\,5\,8\,3\,2\,4\,2\,1\,7\,6\,6\,0\,4\,8\,6\,3\,8\,0\,7\,0$$

$$\vdots$$

$$Y_4 = 4\;7\;8\;8\;5\;1\;6\;8\;2\;6\;5\;7\;5\;4\;1\;0\;0\;3\;7\;2\;0\;6\;2\;3\;1\;3$$

$$\vdots$$

$$Y_8 = 8\,2\,0\,0\,6\,5\,1\,0\,3\,1\,6\,2\,6\,8\,5\,4\,4\,7\,2\,3\,4\,1\,3\,7\,5\,7$$

If $Y_v = Y_4$, $v = 4 = 1\times 3^0 + 1\times 3^1 \longrightarrow v = (v_0, v_1) = (1,\ 1)$

$$y_4(0) = (x(0)+v_0)\times 3^0 + (x(1)+v_1)\times 3^1 \bmod 9 = 4$$

$$y_4(1) = (x(1)+v_0)\times 3^0 + (x(2)+v_1)\times 3^1 \bmod 9 = 7$$

$$y_4(2) = (x(2)+v_0)\times 3^0 + (x(3)+v_1)\times 3^1 \bmod 9 = 8$$

처음 페이지로 이동

• RS-code를 이용하는 방법

- α = GF(q)의 원시근 (단 $q = p^m$, p is a prime.) ($n = q$-1)

$$e_i = (\alpha^{i}, \alpha^{2i}, \alpha^{3i}, \cdots, \alpha^{ni}), \quad i = 0, 1, 2, \cdots, k$$

- E는 [n, k+1, n-k] Reed-Solomon 부호이다.

$$E = \{ \sum_{i=0}^{k} x_i e_i \mid x_i \in \mathrm{GF}(q) \}$$

- Definition
  - E' = 순회적으로 동등한 부호어의 대표들로 구성된 부호어 집합
  - E'' = E'에서 내부 주기가 있는 부호어를 모두 삭제하고 남는 부호어

    = 최적도약수열 집합

심볼수 (q) : q

수열 길이 (L) : $q - 1 = n$

수열의 수 (N) : $|E''|$

최대상관값 : $H_{\max}(F) = k$

- 집합 E'' 를 구성하기는 일반적으로 매우 복잡하다.

➲ $E'' \supseteq V$ 인 부분집합 ***V***를 쉽게 구성하는 방법

(1) **1**부터 ***k***까지 정수중에서 ***q*-1**과 서로 소인 정수의 수를 ***M***이라 하고
이들을 $i_1 = 1 < i_2 < i_3 \cdots < i_M$ 라 하자

(2) $b_1, b_2, b_3, \cdots, b_M$ 을 **GF(q)** 상에서 **0**이 아닌 임의의 **M**개의 원소라 하자.

(3)
$$V(1) = \{x \in E \mid x_1 = b_1\}$$
$$V(2) = \{x \in E \mid x_1 = 0,\ x_{i_2} = b_2\}$$
$$V(3) = \{x \in E \mid x_1 = x_{i_2} = 0,\ x_{i_3} = b_3\}$$
$$\vdots \quad \vdots \qquad\qquad \vdots$$
$$V(M) = \{x \in E \mid x_1 = x_{i_2} = \cdots = x_{i_{M-1}} = 0,\ x_{i_M} = b_M\}$$

(recall) $x = \sum_{i=0}^{k} x_i e_i$

$V = \bigcup_{i=1}^{M} V(i)$

연세대학교 전자공학과 컴퓨터 응용 연구실

- $|E''| \ge |V| = \dfrac{q^{k+1} - q^{k+1-M}}{q-1}$ ('='는 $1 \le k \le B(q)$ 일 때 성립)

  <u>여기서, $B(q)$ 는 q - 1 이 하나의 소수로만 나누어 지면 q-2 이고, q-1이 두개이상의 소수에 의해 나누어 지면 $B(q)$ 는 두 번째로 작은 소인수에서 1만큼 작은 값이다.</u>

- (예제 1)

  q 가 소수이면, k=1이고 $|E''| = |V| = q$ 이다.

  $V = V(1) = \{x \in E \mid x = x_0 e_0 + b_1 e_1\}$ $e_i = \{\alpha^i, \alpha^{2i}, \alpha^{3i}, \cdots, \alpha^{6i}\}$

  let $b_1 = 1, \quad \alpha = 3$

  $x = x_0(1,1,1,1,1,1) + (3,2,6,4,5,1) \Rightarrow x_{x_0}(t) = x_0 + \alpha^t$ => 원시근이용법

- (예제 2)

  $q = 7$이면, q - 1 $= 6 = 2 \cdot 3$ 이고, $B(q) = 2$ 이다.

  즉, k=1과 k=2에 대하여 $|E''| = |V|$ 를 만족한다.

아래에 k=2 에 대한 집합 E'를 보인다. 집합 E'는 아래에 보인 각각의 부호어의 모든 순회순열(Cyclic Permutation)로 이루어지고, 집합 E''는 아래부분의 49개 부호어들로 이루어진다.

Classes of period 1 :

(000000)	(111111)	(222222)	(333333)	(444444)	(555555)	(666666)

Classes of period 3 :

(241241)	(352352)	(463463)	(504504)	(615615)	(026026)	(130130)
(653653)	(064064)	(105105)	(216216)	(320320)	(431431)	(542542)

Classes of period 6 (Nonperiodic classes) :

E''

(326451)	(430562)	(541603)	(652014)	(063125)	(104236)	(215340)
(560622)	(601033)	(012144)	(123255)	(234366)	(345400)	(456511)
(031163)	(142240)	(253315)	(364426)	(405530)	(516641)	(620052)
(202334)	(313445)	(424556)	(535660)	(646001)	(050112)	(161223)
(443505)	(554616)	(665020)	(006131)	(110242)	(221353)	(332464)
(614046)	(025150)	(136261)	(240302)	(351413)	(462524)	(503635)
(155210)	(266321)	(300432)	(411543)	(522654)	(633065)	(044106)

- (예제 3) $q = 7,\ k = 1,\ n = q - 1$

$$x_u = m\,\underline{e} + u\,\underline{1}$$

user index

message symbol $\in \mathrm{GF}(q)$

$$e = \{\alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^5\},\quad \alpha = 3$$

$$x = m\,(1,3,2,6,4,5) + u\,(1,1,1,1,1,1)$$

	m = 0	1	2	3	4	5	6
user 0	000000	132645	264513	326451	451326	513264	645132
user 1	111111	243056	305624	430562	562430	624305	056243
user 2	222222	354160	416035	541603	603541	035416	160354
user 3	333333	465201	520146	652014	014652	146520	201465
user 4	444444	506312	631250	063125	125063	250631	312506
user 5	555555	610423	042361	104236	236104	361042	423610
user 6	666666	021534	153402	215340	340215	402153	534021

E' E''

- (예제 4) $k = 2$

$$x_u = m\,\underline{e_1} + e_2 + u\,\underline{1} \longrightarrow \text{resynchronization is good}$$

처음 페이지로 이동

• **(n , k)-수열 이용법**

□ (n, k)-수열은 서로 다른 kn개의 심볼 $0, 1, 2, \ldots, kn-1$에 대한 순열(permutation) $a_1, a_2, a_3, \ldots, a_{kn}$ 이며 다음 조건을 만족한다.

n 과 k를 임의의 양의 정수라 할 때, 두 항 (a_i, a_j)에 대해서 a_i/n 과 a_j/n 의 정수부가 같으면 동등(comparable)하다고 하자.

(1) $a_1, a_2, a_3, \ldots, a_{kn}$ 은 $0, 1, 2, \ldots, kn-1$ 을 꼭 한 번씩 사용한다.

(2) $1 \le s < t < t+d \le kn$ 을 만족하는 모든 s, t, d 에 대해서 만일 (a_{s+d}, a_s) 와 (a_{t+d}, a_t) 가 동등한 두 개의 순서쌍인 경우 $a_{s+d} - a_s \neq a_{t+d} - a_t \pmod{n}$을 만족한다.

□ (n, k)-수열이 주어지면, 이로부터 길이가 $kn+1$ 이고 심볼 $q = kn+1$를 정확하게 한번씩 사용하는 최대상관값이 1인 n개의 도약 수열 집합을 쉽게 설계할 수 있다.

▫ (예제 2) (4, 2) 수열 이용

심볼수 (q) : $2 \bullet 4 + 1 = 9$ 수열의 수 (N): $n = 4$

수열 길이 (L) : $q = 9$ 최대상관값 $H_{\max}(F) = 1$

```
0   1   4   6   5   3   7   2
------------------------------
  1   *   2   3   *   *   *
    *   *   1   *   2   3
      *   *   *   1   *
        *   2   3   *
          3   *   *
            *   1
              2
```

(4, 2) -수열의 차삼각형

$X_0 =$	*	0	1	4	6	5	3	7	2
$X_1 =$	*	1	2	5	7	6	0	4	3
$X_2 =$	*	2	3	6	4	7	1	5	0
$X_3 =$	*	3	0	7	5	4	2	6	1

4, 5, 6, 7의 순환

0, 1, 2, 3 의 순환

새로운 심볼 첨가

4 개의 최적도약수열

결 론

- 최적집합을 최대상관함수의 하한식으로부터 규정할 수 있다.
- 최적집합을 구성하는 방법에는 곱셈표, 원시근, M- sequence, RS-code, (n, k)-수열 등을 이용하는 방법등이 있다.
- 곱셈표 및 원시근 이용법은 길이의 제약이 심한데 반하여, M-sequence는 그보다 길이를 늘일 수 있다. 또한 (n, k)-수열을 이용하면 (n, k)-수열의 길이 kn 보다 1만큼 긴 k개의 도약패턴을 구성할 수 있다.
- 향후, 최적도약패턴은 변조기법과 함께 고려되어야 하며 항재밍 및 LPI 능력을 가져야 한다. 즉 단순한 도약패턴은 지양해야 한다.

- 이라 하고, K+1개의 n-tuple 벡터를 GF(q) 위에서다음과 같이 정의하자.

$$\left|E''\right| = \left|V\right|$$

$$\left|E''\right| = \frac{1}{n}\sum_{d|n} \mu(d)\, q^{1+\lfloor k/d \rfloor}$$