2021년 2월
교육학석사(수학교육)학위논문

사영직선 위의 MDS 대수기하 부호

조선대학교 교육대학원

수학교육전공

박 성 화

사영직선 위의 MDS 대수기하 부호

MDS Algebraic Geometry Code on Projective Line

2021년 2월

조선대학교 교육대학원

수학교육전공

박 성 화

사영직선 위의 MDS 대수기하 부호

지도교수 이 관 규

이 논문을 교육학석사(수학교육)학위 청구논문으로 제출함.

2020년 10월

조선대학교 교육대학원

수학교육전공

박 성 화

박성화의 교육학 석사학위 논문을 인준함.

심사위원장　조선대학교 교수　오동렬　(인)

심사위원　조선대학교 교수　김광섭　(인)

심사위원　조선대학교 교수　이관규　(인)

2020년　12월

조선대학교 교육대학원

CONTENTS

ABSTRACT

MDS Algebraic Geometry Code on Projective Line

Park Seong-hwa
Advisor : Prof. Kwan Kyu Lee, Ph.D.
Major in Mathematics Education
Graduate School of Education, Chosun University

The algebraic geometry code was introduced in 1981 by V.D. Goppa. Goppa discovered the relationship between algebraic geometry and error correcting code and studied the composition of error correcting codes using the algebraic functional field. Algebraic geometry code have been important in code theory for a long time. The algebraic geometry code on algebraic straight line is called the rational algebraic geometry code, and the Reed-Solomon code is seen as the algebraic geometry code on an affine line. In this thesis, we look at the algebraic geometry code on a projective line and show that this code is the MDS code. Then, find the general matrix and dual code of this code and obtain the parity check matrix of the original code. It is shown that the dual code of this code is also MDS code.

제 1 장

소개

유한체 $\mathbb{F}$가 있고 X는 $\mathbb{F}$ 위의 부드러운 대수적 곡선이라 하자. 그리고 $\mathbb{F}(X)$는 X의 함수체(function field)이고 $P_1, \ldots, P_n$은 차수가 1인 X의 서로 다른 자리라고 하자. 인자 $D = P_1 + \cdots + P_n$이고 G는 D와 겹치는 자리가 없는 X의 인자(divisor)라고 할 때 선형공간

$$L(G) = \{f \in \mathbb{F}(X) \mid (f) + G \geq 0\}$$

이고 대수기하 부호(Algebraic Geometry Code)를

$$C_L(D, G) = \{(f(P_1), \ldots, f(P_n)) \mid f(x) \in L(G)\} \subseteq \mathbb{F}^n$$

로 정의한다. 대수기하 부호는 1981년에 V. D. Goppa에 의해 소개되었다. Goppa는 대수기하학과 오류 정정 부호 사이의 관계를 발견하고 대수적 함수체를 사용한 오류 정정 부호의 구성을 살펴 보았다. 이후로 대수기하 부호는 부호 이론에서 오랫동안 중요시 되어 왔다. 특히 X가 직선인 경우 X 위의 대수기하 부호를 유리 대수기하 부호(Rational Algebraic Geometry Code)라고 부른다.

2장에서는 부호 이론에 대한 주요 개념을 살펴보고 대수기하 부호의 정의를 소개한다. 리드솔로몬 부호는 대수기하 부호 이론에서 가장 유명한 부호로 볼 수 있다. 리드솔로몬 부호는 1960년에 Reed와 Solomon에 의해 연구되었다. 지금은 CD, DVD, QR code등에 응용되고 있다. 리드솔로몬 부호는 아핀 직선(affine line) 위의 대수기하 부호로 볼 수 있으며 3장 2절에서는 대수기하 부호 관점에서 리드솔로몬 부호를 소개한다.

마지막으로 3장 3절과 4절에서는 이 논문의 주 결과를 소개한다. 3장 3절에서는 사영 직선(projective line) 위의 대수기하 부호에 대해 살펴보고 사영 직선 위에서의 대수기하 부호를 정의한다. 그리고 이 부호가 MDS(Maximum Distance Separable) 선형부호임을 보이고 생성행렬(generator matrix)을 구한다. 이어서 3장 4절에서는 사영 직선 위의 대수기하 부호의 쌍대부호를 찾고 이 부호의 홀짝검사 행렬(parity check matrix)을 구체적으로 구하여 이 부호의 쌍대부호도 MDS 부호임을 보인다.

제 2 장

부호 이론

이 장에서는 [2]를 참고하여 부호 이론의 주요 개념을 살펴보고 여러가지 선형부호를 소개한다. 그 다음에는 대수기하 부호의 주요 용어를 정리한 후 대수기하 부호의 정의를 소개한다.

2.1 선형부호

체 $\mathbb{F}$는 임의의 소수 p와 양의 정수 n에 대하여 $q = p^n$이라고 할 때, 위수가 q인 유한체이다. n차원 벡터공간 $\mathbb{F}^n$을 생각하자.

정의 1. $\mathbb{F}^n$의 벡터 $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n)$가 있다고 하자. u_i와 v_i가 다른 i의 개수를 u와 v의 해밍거리(Hamming distance)라 하고 $d(u, v)$로 나타낸다. 즉

$$d(u, v) = |\{1 \leq i \leq n \mid u_i \neq v_i\}|$$

이다. 벡터 u의 성분중에서 0이 아닌 성분의 개수를 u의 무게(weight)라 하고

wt(u)로 나타낸다. 즉

$$\text{wt}(u) = |\{1 \le i \le n \mid u_i \neq 0\}|$$

이다. 그러므로 wt$(u) = d(u, 0)$이다.

예제 1. $\mathbb{F}_2{}^5$의 벡터

$$v = (0, 1, 1, 0, 1), \quad w = (1, 1, 0, 1, 1), \quad u = (1, 0, 0, 1, 1)$$

에서

$$d(v, w) = \text{wt}(v - w) = \text{wt}(1, 0, 1, 1, 0) = 3$$

$$d(v, u) = \text{wt}(u - v) = \text{wt}(1, 1, 1, 1, 0) = 4$$

이다.

거리 d가 주어진 벡터공간 $\mathbb{F}^n$을 해밍공간이라 한다.

정의 2. $\mathbb{F}$ 위의 벡터공간 $\mathbb{F}^n$의 부분공간 C를 길이가 n인 선형부호(binary linear code)라고 하고 C의 원소를 부호어(codeword)라고 한다. C의 차원을 k라고 하면 C는 $[n, k]$ 선형부호라고 한다.

정의 3. C가 $[n, k]$ 선형부호일 때

$$d(C) = \min\{d(u, v) \mid u, v \in C, u \neq v\}$$

를 C의 최소거리(minimum distance)라고 한다. C는 선형부호이므로

$$d(C) = \min\{\text{wt}(u) \mid u \in C, u \neq 0\}$$

이다. $[n, k]$ 선형부호 C의 최소거리가 d일때 C를 $[n, k, d]$ 선형부호라고 한다.

예제 2. $\mathbb{F}_2{}^6$의 부분공간

$$C = \{000000, 011011, 110110, 001110, 101101, 010101, 111000, 100011\}$$

$$= \langle 100011, 011011, 001110 \rangle$$

는 $[6,3]$ 선형부호이다. 그리고 C에 속하는 000000을 제외한 부호어의 무게는 각각 4, 4, 3, 4, 3, 3, 3이므로 $d(C) = 3$이다. 그러므로 C는 $[6,3,3]$ 선형부호이다.

정의 4. C는 $[n,k]$ 선형부호이고 k개의 행이 벡터공간 C의 기저인 $k \times n$ 행렬 G를 C의 생성행렬(generator matrix)이라고 한다.

$\mathbb{F}^n$의 벡터 $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n)$에 대해서 u와 v의 내적을

$$\langle u, v \rangle = u_1 v_1 + \cdots + u_n v_n$$

으로 나타낸다.

정의 5. $C \subseteq \mathbb{F}^n$이고

$$C^{\perp} = \{v \in \mathbb{F}^n \mid \text{모든 } u \in C,\ \langle u, v \rangle = 0\}$$

은 $\mathbb{F}^n$의 부분공간이다. $C^{\perp}$를 C의 쌍대부호(dual code)라고 한다.

정의 6. $C^{\perp}$의 생성행렬 H를 C의 홀짝검사 행렬(paritycheck matrix)라고 한다. $[n,k]$ 선형부호 C의 홀짝검사 행렬 H는 계급수가 $n-k$인 $(n-k) \times n$ 행렬이다.

2.1.1 MDS 부호

정리 1. $[n,k,d]$ 선형부호 C는

$$d + k \leq n + 1$$

를 만족한다.

증명. $\mathbb{F}^n$의 부분공간 $E = \{u = (u_1, \ldots, u_n) \mid u_i = 0, \text{모든 } i \geq d\}$라고 하자. 모든 $u \in E$는 $\mathrm{wt}(u) \leq d-1$이고 C의 최소거리가 d이므로 $C \cap E = \{0\}$이다. E의 차원은 $d-1$이므로

$$k + (d-1) = \dim C + \dim E = \dim(C+E) + \dim(C \cap E) = \dim(C+E) \leq n$$

이다. 따라서 $k + d - 1 \leq n$이므로 $d + k \leq n + 1$이다.

위 부등식을 싱글톤 상계(Singleton bound)라고 한다. 만약 $[n, k, d]$ 선형부호 C에 대해

$$d + k = n + 1$$

이 성립하면 C를 MDS(Maximum Distance Separable) 부호라고 한다.

2.1.2 리드솔로몬 부호

유한체 $\mathbb{F}$의 서로 다른 원소를 $\alpha_1, \alpha_2, \ldots, \alpha_n$이라고 하자. 그리고 집합

$$\mathbb{F}[x]_n = \{f \in \mathbb{F}[x] \mid \deg f(x) < n\}$$

라고 하자. 선형사상 $\mathrm{ev} : \mathbb{F}[x]_n \to \mathbb{F}^n$를

$$f \mapsto (f(\alpha_1), \ldots, f(\alpha_n))$$

으로 정의한다. 사상 ev는 $\mathbb{F}[x]_n$과 $\mathbb{F}^n$ 사이의 동형사상이다. 정수 $1 \leq k \leq n$에 대해서 리드솔로몬 부호(Reed-Solomon code)를

$$\mathrm{RS}(\alpha, k) = \{\mathrm{ev}(f) \mid \deg f(x) < k\} = \mathrm{ev}(\mathbb{F}[x]_k)$$

으로 정의한다. $\mathrm{RS}(\alpha,k)$는 $\mathbb{F}$ 위에서 $[n,k]$ 선형부호이고 $0 \neq c = \mathrm{ev}(f) \in \mathrm{RS}(\alpha,k)$의 무게는

$$\begin{aligned}\mathrm{wt}(c) &= n - |\{1 \le i \le n \mid f(\alpha_i) = 0\}| \\ &\ge n - \deg f \ge n - (k-1)\end{aligned}$$

이므로 $\mathrm{RS}(\alpha,k)$의 최소거리 d는 $d \ge n-k+1$를 만족한다. 한편 싱글톤 상계에 의하여 $d \le n-k+1$이 성립하므로 $d = n-k+1$이다. 따라서 $\mathrm{RS}(\alpha,k)$는 $\mathbb{F}$ 위에서 $[n,k]$ MDS 선형부호이다.

$\mathbb{F}[x]_k$의 기저는 $\{1, x, \ldots, x^{k-1}\}$이므로 $\mathrm{RS}(\alpha,k)$의 생성행렬은

$$G = \begin{pmatrix} \mathrm{ev}(1) \\ \mathrm{ev}(x) \\ \vdots \\ \mathrm{ev}(x^{k-1}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_1 & \ldots & \alpha_n \\ {\alpha_1}^2 & {\alpha_2}^2 & \ldots & {\alpha_n}^2 \\ \vdots & \vdots & \ddots & \vdots \\ {\alpha_1}^{k-1} & {\alpha_2}^{k-1} & \ldots & {\alpha_n}^{k-1} \end{pmatrix}$$

이다.

2.2 대수기하 부호

대수기하 부호를 정의하기 전에 주요 용어를 살펴보자. 유한체 $\mathbb{F}$가 있고 X는 기약 대수적 곡선이다. $\mathbb{F}(X)$는 X의 함수체(function field)이고 $P_1, \ldots, P_n$은 차수가 1인 X의 서로 다른 자리이다. 인자(divisor) $D = P_1 + \cdots + P_n$이고 G는 D와 겹치는 자리가 없는 다른 인자이다.

영이 아닌 함수 $f \in \mathbb{F}(X)$에 대해서 함수 f가 자리 P에서 중복도 n인 영(zero)을 가지면 $v_P(f) = n$이라고 한다. 그리고 중복도 n인 극(pole)을 가지면 $v_P(f) = -n$

이다. 그러면 f의 인자는

$$\sum_{P} v_P(f)P$$

으로 정의한다. 즉 f의 영과 극을 중복도를 포함해서 합으로 나타낸 것이다. 또 f의 영인자는

$$(f)_0 = \sum_{f\text{의영}P} v_P(f)P$$

이고 f의 극인자는

$$(f)_\infty = \sum_{f\text{의극}P} (-v_P(f))P$$

이다. 그러므로 f의 인자는

$$(f) = (f)_0 - (f)_\infty$$

이다. 영이 아닌 함수 $f, g \in \mathbb{F}(X)$에 대해서 $(fg) = (f) + (g)$이다.

예제 3. X를 대수적 직선이라고 하자. α가 $\mathbb{F}$의 원소일 때 P_α를 함수 $x - \alpha$의 영이라고 하자. 함수

$$f = \frac{x}{(x-1)^2} \in \mathbb{F}(X)$$

의 인자는 인자의 성질에 의해

$$(f) = (x) - 2(x-1)$$

이고 x는 P_0에서 영을 갖고 P_∞에서 극을 갖으므로 $(x)_0 = P_0$, $(x)_\infty = P_\infty$이다. 그러면

$$(x) = (x)_0 - (x)_\infty = P_0 - P_\infty$$

이다. 또 $x-1$은 P_1에서 0을 갖고 P_∞에서 극을 갖으므로 $(x-1)_0 = P_1$, $(x-1)_\infty = P_\infty$ 이다. 그러면

$$(x-1) = (x-1)_0 - (x-1)_\infty = P_1 - P_\infty$$

이다. 따라서 f의 인자는

$$(f) = (x) - 2(x-1) = P_0 - P_\infty - 2(P_1 - P_\infty) = P_0 - 2P_1 + P_\infty$$

이다.

정의 7. 인자 $A = \sum_P a_P P,\ B = \sum_P b_P P$일 때 모든 P에서 $a_P \geq b_P$이면 $A \geq B$로 표현한다.

정의 8. X의 인자 G에 대해서

$$L(G) = \{f \in \mathbb{F}(X) \mid (f) + G \geq 0\}$$

는 $\mathbb{F}$ 위의 선형공간이다. $L(G)$를 리만 로흐 공간(Riemann-Roch space)이라고 한다.

예제 4. $G = 2P_\infty$이면 $f(x) = x(x-1)$라고 했을 때

$$(f) = P_0 + P_1 - 2P_\infty$$

이므로

$$(f) + G = P_0 + P_1 - 2P_\infty + 2P_\infty = P_0 + P_1 \geq 0$$

이다. 따라서 $f \in L(G)$이다.

정의 9. 인자 $D = P_1 + \cdots + P_n$와 G로 결정되는 대수기하 부호를

$$C_L(D, G) = \{(f(P_1), \ldots, f(P_n)) \mid f \in L(G)\} \subseteq \mathbb{F}^n$$

으로 정의한다.

이제 선형사상 $\mathrm{ev}_D : L(G) \to \mathbb{F}^n$를

$$\mathrm{ev}_D(f) = (f(P_1), \ldots, f(P_n)) \in \mathbb{F}^n$$

라고 하자. 그러면 $C_L(D,G) = \mathrm{ev}_D(L(G))$이다. 인자 D, G를 적절하게 결정하면 리드솔로몬 부호는 직선 위의 대수기하 부호로 볼 수 있다. 이는 3장에서 좀 더 자세히 다루도록 한다.

제 3 장

사영직선 위의 MDS 대수기하 부호

이 장에서는 대수적 곡선 X가 직선인 경우 X 위의 대수기하 부호를 살펴본다. 직선은 가장 간단한 대수적 곡선으로서 사영 직선(projective line)과 아핀 직선(affine line)이 있다. 3장 2절에서는 아핀 직선 위의 대수기하 부호로서 리드솔로몬 부호를 소개하고 3장 3절과 4절에서는 사영 직선 위의 대수기하 부호와 그 쌍대부호를 소개한다.

3.1 대수적 직선

이제 $\mathbb{F}$ 위의 사영 직선을 $\mathbb{P}^1_{\mathbb{F}}$로 표기하자. $\mathbb{P}^1_{\mathbb{F}}$을 원으로 표현하고 아핀 직선을 직선으로 표현하면 $\mathbb{P}^1_{\mathbb{F}}$ 위의 점은 한 점을 제외하고 아핀 직선 위의 점과 대응한다. 아핀 직선 위의 점과 대응하지 않는 $\mathbb{P}^1_{\mathbb{F}}$ 위의 점을 무한원점(point at infinity) P_∞로

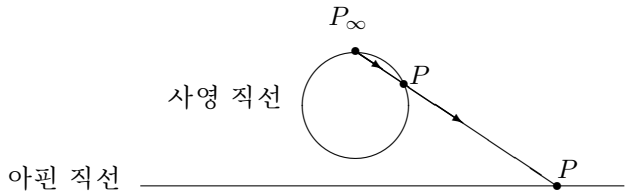

그림 3.1: 직선

나타낸다. 또 직선 위의 차수가 1인 점을 유리점이라고 하고 아핀 직선 위의 차수가 1인 점은 $\mathbb{F}$의 원소와 대응한다.

대수적 곡선 X의 함수체 $\mathbb{F}(X)$의 값매김 환(valuation ring) O란 아래의 조건

(i) $\mathbb{F} \subsetneq O \subsetneq \mathbb{F}(X)$

(ii) 모든 $f \in \mathbb{F}(X)$ 에 대해서 $f \in O$ 이거나 $\frac{1}{f} \in O$ 이다.

을 만족하는 $\mathbb{F}(X)$의 부분환을 말한다.

$\mathbb{P}^1_{\mathbb{F}}$의 함수체는 유리식체 $\mathbb{F}(x)$이다. $\mathbb{P}^1_{\mathbb{F}}$ 위의 모든 점들은 $\mathbb{F}(x)$의 값매김 환과 대응한다. $\mathbb{P}^1_{\mathbb{F}}$ 위의 점이 기약다항식 $p(x)$의 영이면 이 점은 값매김 환

$$O_{p(x)} = \{\frac{h(x)}{g(x)} \mid h(x), g(x) \in \mathbb{F}[x],\ \ p(x) \nmid g(x)\}$$

와 대응하고 이 환의 극대 이데알은

$$P_{p(x)} = \{\frac{h(x)}{g(x)} \mid h(x), g(x) \in \mathbb{F}[x],\ \ p(x) \mid h(x),\ \ p(x) \nmid g(x)\}$$

이다. 아핀 직선 위의 점 $\alpha \in \mathbb{F}$에 대해서 $p(x) = x - \alpha$의 영을 P_α로 표기한다.

한편 $\mathbb{P}^1_{\mathbb{F}}$의 유리점 P_∞는 함수 x의 극이다. 이 점은 값매김 환

$$O_\infty = \{\frac{h(x)}{g(x)} \mid h(x), g(x) \in \mathbb{F}[x],\ \ \deg h(x) \leq \deg g(x)\}$$

와 대응하고 이 환의 극대 이데알은

$$P_\infty = \{\frac{h(x)}{g(x)} \mid h(x), g(x) \in \mathbb{F}[x],\ \ p(x) \mid h(x),\ \ \deg h(x) < \deg g(x)\}$$

이다. 그러면

$$O_{p(x)}/P_{p(x)} \cong \mathbb{F}[x]/(p(x)), \quad O_\infty/P_\infty \cong \mathbb{F}$$

이고 특히 $p(x) = x - \alpha$일 때 $O_{x-\alpha}/P_{x-\alpha} \cong \mathbb{F}[x]/(x-\alpha) \cong \mathbb{F}$이다. 함수$f \in \mathbb{F}(x)$에 대해서 f의 P에서의 값 $f(P)$를

$$f(P) = f + P \in O/P$$

로 정의한다.

정리 2. $f \in \mathbb{F}(x)$일 때 $f(P_\alpha) = f(\alpha)$이다.

증명. $p(x) = x - \alpha$인 경우 $P_\alpha = P_{x-\alpha}$이다. $O_{x-\alpha}/P_{x-\alpha} \cong \mathbb{F}[x]/(x-\alpha)$이므로

$$f + P_\alpha = f + P_{x-\alpha} = f(x - \alpha + \alpha) + (x - \alpha) = f(\alpha) + (x - \alpha)$$

이므로 $f(P_\alpha) = f(\alpha)$이다.

정리 3. $f = \frac{h(x)}{g(x)} \in \mathbb{F}(x)$이고 $\deg h(x) \leq \deg g(x)$일 때

$$f(P_\infty) = \lim_{x\to\infty} \frac{h(x)}{g(x)}$$

이다.

증명. $\deg h(x) = t$, $\deg g(x) = r$이라고 하자. $f = \frac{h(x)}{g(x)}$의 분모 분자를 x^r로 나누면

$$\begin{aligned}\frac{h(x)/x^r}{g(x)/x^r} &= \frac{(b_t x^t + b_{t-1}x^{t-1} + \cdots + b_0)/x^r}{(a_r x^r + a_{r-1}x^{r-1} + \cdots + a_0)/x^r} \\ &= \left(\frac{b_t}{x^{r-t}} + \cdots + \frac{b_0}{x^r}\right)\left(\frac{1}{a_r + a_{r-1}/x + \cdots + a_0/x^r}\right)\end{aligned}$$

이고 $a_{r-1}/x + \cdots + a_0/x^r \in P_\infty$이므로

$$f + P_\infty = \frac{1}{a_r}\left(\frac{b_t}{x^{r-t}} + \cdots + \frac{b_0}{x^r}\right) + P_\infty$$

이다. 그러면

$$f + P_\infty = \frac{b_r}{a_r} + P_\infty \quad (t = r)$$

$$f + P_\infty = 0 + P_\infty \quad (t < r)$$

이므로 $t = r$이면 $f(P_\infty) = b_r/a_r$이고 $t < r$이면 $f(P_\infty) = 0$이다. 따라서 $f(P_\infty)$의 값은 로피탈 정리로 볼 수 있으므로 $f(P_\infty) = \lim_{x\to\infty} \frac{h(x)}{g(x)}$이다.

3.2 아핀직선 위의 RS 선형부호

이 절에서는 특별히 리드솔로몬 부호가 아핀 직선 위의 대수기하 부호로 볼 수 있음을 보인다. 일반적으로 [2]의 정리2.3.5에서 리드솔로몬의 일반화는 직선 위의 대수기하 부호라고 알려져 있다. 다음정리를 살펴보자.

보조정리 1. 인자 G를 $(k-1)P_\infty$라 하자. 그러면

$$L((k-1)P_\infty) = \{f \in \mathbb{F}(x) \mid \deg f(x) \le k-1\}$$

이다.

증명. 서로소인 두 다항식 $h(x)$와 $g(x)$가 있고 선형 공간

$$L((k-1)P_\infty) = \{f = \frac{h(x)}{g(x)} \in \mathbb{F}(x) \mid (f) + (k-1)P_\infty \ge 0\}$$

에서 만약 $g(x)$가 상수다항식이 아니면

$$(f) + (k-1)P_\infty = (h)_0 - (h)_\infty - (g)_0 + (g)_\infty + (k-1)P_\infty$$

는 $-(g)_0 < 0$이므로 $(h)_0 - (g)_0 \ge 0$를 만족하지 않는다. 따라서 $(f) + (k-1)P_\infty \ge 0$을 만족하지 않는다.

한편 $g(x)$가 상수다항식이면 $f(x)=h(x)$이고 $\deg h(x)=t$라고 할 때

$$(f)+(k-1)P_\infty=(h)_0-(h)_\infty+(k-1)P_\infty=(h)_0-tP_\infty+(k-1)P_\infty\geq 0$$

이려면 $(h)_0\geq 0$이므로 $-tP_\infty+(k-1)P_\infty=(-t+k-1)P_\infty\geq 0$이면 된다. 따라서 $t\leq k-1$이므로 $f(x)=h(x)$는 $\deg h(x)\leq k-1$인 다항식이다.

정리 4. 인자 $D=P_1+\cdots+P_q$라고 하자. 그러면 리드솔로몬 부호는

$$C_L(D,(k-1)P_\infty)=\{(f(\alpha_1),\ldots,f(\alpha_q))\mid \deg f(x)\leq k-1\}$$

와 일치한다.

증명. 대수기하부호의 정의와 보조정리1과 정리2에 의해

$$\begin{aligned}C_L(D,(k-1)P_\infty)&=\{(f(P_1),\ldots,f(P_q))\mid f\in L((k-1)P_\infty)\}\\&=\{(f(\alpha_1),\ldots,f(\alpha_q))\mid \deg f(x)\leq k-1\}\\&=\mathrm{RS}(\alpha,k)\end{aligned}$$

이다.

3.3 사영직선 위의 MDS 대수기하 부호

이 절에서는 사영 직선 위의 대수기하 부호를 소개하고 이 부호의 최소거리와 차원을 구하여 MDS 부호임을 보인다. 먼저 사영 직선 위의 대수기하 부호를 살펴보기 전에 필요한 보조정리를 살펴보자.

보조정리 2. Q는 기약다항식 $r(x)$의 영이다. 인자 G를 $\deg r(x)=r\leq q$의 영이라고 하자. 즉 $G=Q$ 이다. 그러면

$$L(Q)=\{f=\frac{h(x)}{r(x)}\in\mathbb{F}(x)\mid \deg h(x)\leq r\}$$

이다.

증명. 서로소인 두 다항식 $h(x)$와 $g(x)$가 있고 선형 공간

$$L(Q) = \{f = \frac{h(x)}{g(x)} \in \mathbb{F}(x) \mid (f) + Q \geq 0\}$$

에서

$$(f) + Q = (h) - (g) + Q = (h)_0 - (h)_\infty - (g)_0 + (g)_\infty + Q \geq 0$$

이려면 $-(h)_\infty + (g)_\infty \geq 0$이면 되므로 $\deg g(x) \geq \deg h(x)$이다.

한편 $(h)_0 - (g)_0 + Q \geq 0$이려면 $h(x)$와 $g(x)$가 서로소인 다항식이므로 $(g)_0$가 Q를 포함하면 된다. 그런데 $r(x)$는 기약다항식이므로 $g(x) = r(x)$이고

$$\deg h(x) = t \leq \deg g(x) = \deg r(x) = r$$

이므로 $f = h(x)/g(x) = h(x)/r(x)$이고 $\deg h(x) \leq r$이다.

정리 5. 인자 $D = P_1 + P_2 + \cdots + P_q + P_\infty$라고 하자. 사영 직선 위의 대수기하 부호는

$$C_L(D, Q) = \{\left(\frac{h(\alpha_1)}{r(\alpha_1)}, \frac{h(\alpha_2)}{r(\alpha_2)}, \ldots, \frac{h(\alpha_q)}{r(\alpha_q)}, \lim_{x\to\infty} \frac{h(x)}{r(x)}\right) \mid \deg h(x) \leq r\}$$

이다.

증명. 대수기하 부호의 정의와 보조정리2와 정리3에 의해

$$\begin{aligned} C_L(D, Q) &= \{(f(P_1), \ldots, f(P_q), f(P_\infty)) \mid f \in L(Q)\} \\ &= \{\left(\frac{h(\alpha_1)}{r(\alpha_1)}, \frac{h(\alpha_2)}{r(\alpha_2)}, \ldots, \frac{h(\alpha_q)}{r(\alpha_q)}, \lim_{x\to\infty} \frac{h(x)}{r(x)}\right) \mid \deg h(x) \leq r\} \end{aligned}$$

이다.

예제 5. 원시다항식 $x^2 - x - 1 = 0$을 만족하는 원시원소 $\beta \in {\mathbb{F}_3}^2$에 대해서 $\alpha_1 = 0$, $\alpha_i = \beta^{i-1} (2 \leq i \leq 9)$라고 하자. $r_1(x) = x^4 - x^3 - x + \beta$는 ${\mathbb{F}_3}^2$ 위의 기약다항식이고

인자 Q_1를 $r_1(x)$의 영이라고 하자. $h(x) = x^2$이면

$$\begin{aligned} c &= \left(\frac{h(\alpha_1)}{r_1(\alpha_1)}, \frac{h(\alpha_2)}{r_1(\alpha_2)}, \ldots, \frac{h(\alpha_9)}{r_1(\alpha_9)}, \lim_{x\to\infty} \frac{h(x)}{r_1(x)} \right) \in C_L(D, Q_1) \\ &= (0, 1, \beta+1, 2, \beta+2, \beta, \beta+1, 2\beta, \beta, 0) \\ &= (0, \beta^8, \beta^2, \beta^4, \beta^7, \beta, \beta^2, \beta^5, \beta, 0) \end{aligned}$$

이다. 또 $h(x) = x^4$이면

$$\begin{aligned} c &= \left(\frac{h(\alpha_1)}{r_1(\alpha_1)}, \frac{h(\alpha_2)}{r_1(\alpha_2)}, \ldots, \frac{h(\alpha_9)}{r_1(\alpha_9)}, \lim_{x\to\infty} \frac{h(x)}{r_1(x)} \right) \in C_L(D, Q_1) \\ &= (0, \beta+1, 2\beta+2, \beta+1, \beta+2, 2\beta+1, 2\beta+2, 2\beta+1, \beta, 1) \\ &= (0, \beta^2, \beta^6, \beta^2, \beta^7, \beta^3, \beta^6, \beta^3, \beta, 1) \end{aligned}$$

이다.

정리 6. $\dim C_L(D, Q) = r + 1$ 이다.

증명. $a_0, a_1, \ldots, a_r \in \mathbb{F}$에 대해서 선형결합

$$a_0 \frac{1}{r(x)} + a_1 \frac{x}{r(x)} + \cdots + a_r \frac{x^r}{r(x)} = 0 \iff a_0 + a_1 x + \cdots + a_r x^r = 0$$

이다. 그런데 $1, x, \ldots, x^r$은 선형독립이므로

$$\{ \frac{1}{r(x)}, \frac{x}{r(x)}, \ldots, \frac{x^r}{r(x)} \}$$

은 $L(Q)$의 기저이다. 따라서 $\dim L(Q) = r + 1$이다.

한편 $f \in \mathrm{Ker}(\mathrm{ev}_D)$ 이면

$$\mathrm{ev}_D(f) = (\frac{h(\alpha_1)}{r(\alpha_1)}, \frac{h(\alpha_2)}{r(\alpha_2)}, \ldots, \frac{h(\alpha_q)}{r(\alpha_q)}, \lim_{x\to\infty} \frac{h(x)}{r(x)}) = (0, \ldots 0)$$

이다. 즉

$$h(\alpha_1) = 0, \ldots, h(\alpha_q) = 0, \quad \lim_{x\to\infty} \frac{h(x)}{r(x)} = 0$$

이므로 $h(x)$는 차수가 r보다 작은 다항식이고 $h(x)$는 q개의 근을 갖는데 $r \leq q$이므로 $h(x)$는 영다항식이다. 따라서 $\dim(\mathrm{Ker}(\mathrm{ev}_D)) = 0$이고

$$\dim(\mathrm{Im}(\mathrm{ev}_D)) + \dim(\mathrm{Ker}(\mathrm{ev}_D)) = \dim L(Q) = r + 1$$

이므로 $\dim(\mathrm{Im}(\mathrm{ev}_D)) = r + 1$이다. 그러므로 $\dim C_L(D, Q) = r + 1$이다.

정리 7. 사영 직선 위의 $C_L(D, Q)$의 생성행렬은

$$G = \begin{pmatrix} \frac{1}{r(\alpha_1)} & \frac{1}{r(\alpha_2)} & \cdots & \frac{1}{r(\alpha_q)} & 0 \\ \frac{\alpha_1}{r(\alpha_1)} & \frac{\alpha_2}{r(\alpha_2)} & \cdots & \frac{\alpha_q}{r(\alpha_q)} & 0 \\ \frac{{\alpha_1}^2}{r(\alpha_1)} & \frac{{\alpha_2}^2}{r(\alpha_2)} & \cdots & \frac{{\alpha_q}^2}{r(\alpha_q)} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{{\alpha_1}^r}{r(\alpha_1)} & \frac{{\alpha_2}^r}{r(\alpha_2)} & \cdots & \frac{{\alpha_q}^r}{r(\alpha_q)} & 1 \end{pmatrix} \tag{1}$$

이다.

증명. 정리6의 증명에서

$$\{\frac{1}{r(x)}, \frac{x}{r(x)}, \ldots, \frac{x^r}{r(x)}\}$$

는 $L(Q)$의 기저이고 $\dim L(Q) = r+1 = \dim C_L(D, Q)$이므로 ev_D는 동형사상이다. 따라서 $C_L(D, Q)$의 기저는 $\{\mathrm{ev}_D(\frac{1}{r(x)}), \mathrm{ev}_D(\frac{x}{r(x)}), \ldots, \mathrm{ev}_D(\frac{x^r}{r(x)})\}$이다.

정리 8. $C_L(D, Q)$의 최소거리 d는 $q - r + 1$이다.

증명. $C = C_L(D, Q)$는 선형부호이므로

$$c = \left(\frac{h(\alpha_1)}{r(\alpha_1)}, \ldots, \frac{h(\alpha_q)}{r(\alpha_q)}, \lim_{x\to\infty} \frac{h(x)}{r(x)}\right)$$

를 C의 임의의 부호어라고 했을 때 C의 최소거리는 $\mathrm{wt}(c)$의 최솟값과 같다.

$\deg h(x) = r$이면

$$\lim_{x\to\infty} \frac{h(x)}{r(x)} \neq 0$$

이고 c는 마지막 성분을 제외한 q개의 성분 중에 최대 r개의 0을 가진다. 그러면 $q-r$개 이상이 0이 아니고 마지막 성분도 0이 아니므로 wt(c)는 $q-r+1$ 이상이다.

$\deg h(x) < r$이면

$$\lim_{x\to\infty} \frac{h(x)}{r(x)} = 0$$

이고 c는 마지막 성분을 제외한 q개의 성분 중 최대 $r-1$개의 0을 가진다. 그러면 $q-(r-1)$개 이상은 0이 아니므로 wt(c)는 $q-(r-1)$ 이상이다. 따라서 $\deg h(x) \le r$일 때 wt(c)는 $q-r+1$ 이상이다. 따라서 C의 최소거리는 $q-r+1$ 이상이다.

한편 $h(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r)$이면 $h(x)$가 정확히 r개의 근을 갖게 되므로 c는 r개의 0을 갖는다. 그러면

$$\lim_{x\to\infty} \frac{h(x)}{r(x)} \neq 0$$

이므로 wt$(c) = q-r+1$이다. 그러므로 C의 최소거리는 $q-r+1$이다.

정리 9. 사영 직선 위의 대수기하 부호 $C_L(D,Q)$는 MDS 부호이다.

증명. 정리6과 정리8에 의해

$$d(C_L(D,Q)) + \dim C_L(D,Q) = (q-r+1) + (r+1) = (q+1)+1$$

이 성립하므로 MDS 부호이다.

예제 6. 예제5의 $C_L(D,Q_1)$의 생성행렬을 계산하면

$$G_1 = \begin{pmatrix} \beta^7 & \beta^6 & \beta^6 & \beta^6 & \beta^7 & \beta^7 & \beta^6 & \beta^7 & \beta & 0 \\ 0 & \beta^7 & \beta^8 & \beta & \beta^3 & \beta^4 & \beta^4 & \beta^6 & \beta & 0 \\ 0 & \beta^8 & \beta^2 & \beta^4 & \beta^7 & \beta & \beta^2 & \beta^5 & \beta & 0 \\ 0 & \beta & \beta^4 & \beta^7 & \beta^3 & \beta^6 & \beta^8 & \beta^4 & \beta & 0 \\ 0 & \beta^2 & \beta^6 & \beta^2 & \beta^7 & \beta^3 & \beta^6 & \beta^3 & \beta & 1 \end{pmatrix}$$

이다. 또 $C_L(D,Q_1)$은 부호의 길이가 $q+1=9+1$이고 차원은 $\deg r_1(x)+1=4+1$, 최소거리는 $q-\deg r_1(x)+1=9-4+1$이므로 $[10,5,6]$ MDS 부호이다.

예제 7. 원시다항식 $x^3+x+1=0$을 만족하는 원시원소 $\beta\in{\mathbb{F}_2}^3$에 대해서 $\alpha_1=0$, $\alpha_i=\beta^{i-1}(2\le i\le 8)$라고 하자. $r_2(x)=x^2+x+1$는 ${\mathbb{F}_2}^3$ 위의 기약다항식이고 인자 Q_2를 $r_2(x)$의 영이라고 하자. $C_L(D,Q_2)$의 생성행렬을 계산하면

$$G_2=\begin{pmatrix} 1 & \beta^2 & \beta^4 & \beta^2 & \beta & \beta & \beta^4 & 1 & 0\\ 0 & \beta^3 & \beta^6 & \beta^5 & \beta^5 & \beta^6 & \beta^3 & 1 & 0\\ 0 & \beta^4 & \beta & \beta & \beta^2 & \beta^4 & \beta^2 & 1 & 1 \end{pmatrix}$$

이다. 또 $C_L(D,Q_2)$는 부호의 길이가 $q+1=8+1$이고 차원은 $\deg r_2(x)+1=2+1$, 최소거리는 $q-\deg r_2(x)+1=8-2+1$이므로 $[9,3,7]$ MDS 부호이다.

3.4 $C_L(D,Q)$의 쌍대부호

이 절에서는 사영 직선 위의 MDS 대수기하 부호의 쌍대부호를 소개하고 이 부호의 차원과 생성행렬을 구하여 MDS 부호임을 보인다. 쌍대부호를 정의하기 전에 다음 정리를 살펴보자.

보조정리 3. 차수가 $q-1$인 기약다항식 $q(x)$가 있고 함수

$$s=\frac{x^q-x+1}{x^q-x+q(x)}$$

라고 하자. 그리고 인자 $A=(s)$, $B=(q)_0$라고 하자. 그러면

$$L(A+B-Q)=\{f=\frac{t(x)r(x)}{s\cdot q(x)}\in\mathbb{F}(x)\mid \deg t(x)\le q-r-1\}$$

이다.

증명.

$$L(A+B-Q)=\{f\in\mathbb{F}(x)\mid (f)+A+B-Q\geq 0\}$$

에서

$$(f)+A+B-Q=(f)+(s)+(q)_0-Q=(fs)+(q)_0-Q\geq 0$$

이려면 (fs)는 $Q=(r)_0$를 포함해야하므로 fs의 분자는 $t(x)r(x)$ $(t(x)\in\mathbb{F}[x])$이면 된다. 또 fs의 분모는 상수이거나 $q(x)$이면 된다. 그런데 fs의 분모가 상수이면 $fs=t(x)r(x)$이고

$$(fs)+(q)_0-Q=(t)+(r)+(q)_0-Q=(t)_0-(t)_\infty-(r)_\infty+(q)_0$$

이다. 그러면 $\deg t(x)=t$라고 할 때 $-(t)_\infty-(r)_\infty=-(t+r)P_\infty<0$이 되어 $(fs)+(q)_0-Q\geq 0$을 만족하지 않는다.

한편 fs의 분모가 $q(x)$이면 $fs=t(x)r(x)/q(x)$이고

$$(fs)+(q)_0-Q=(t)_0-(t)_\infty-(r)_\infty+(q)_\infty\geq 0$$

이려면 $-(t)_\infty-(r)_\infty+(q)_\infty=(-t-r+q-1)P_\infty\geq 0$이면 되므로 $t\leq q-r-1$이다. 따라서 $fs=t(x)r(x)/q(x)$이고 $\deg t(x)\leq q-r-1$이다.

정리 10. 인자 $D=P_1+P_2+\cdots+P_q+P_\infty$라고 하자. 사영 직선 위의 대수기하 부호는

$$C_L(D,A+B-Q)=\{(t(\alpha_1)r(\alpha_1),\ldots,t(\alpha_q)r(\alpha_q),\lim_{x\to\infty}\frac{t(x)r(x)}{s\cdot q(x)})\mid t\leq q-r-1\}$$

이다. 여기서 $t=\deg t(x)$이다.

증명. 대수기하 부호의 정의와 보조정리3과 정리3에 의해

$$C_L(D,A+B-Q)=\{(f(P_1),\ldots,f(P_q),f(P_\infty))\mid f\in L(A+B-Q)\}$$

$$=\{(t(\alpha_1)r(\alpha_1),\ldots,t(\alpha_q)r(\alpha_q),\lim_{x\to\infty}\frac{t(x)r(x)}{s\cdot q(x)})\mid \deg t(x)\leq q-r-1\}$$

이다.

정리 11. $\dim C_L(D, A+B-Q) = q-r$이다.

증명. 선형결합

$$a_0\frac{r(x)}{s\cdot q(x)} + a_1\frac{xr(x)}{s\cdot q(x)} + \cdots + a_{q-r-1}\frac{x^{q-r-1}r(x)}{s\cdot q(x)} = 0$$

$$\iff a_0 + a_1x + \cdots + a_{q-r-1}x^{q-r-1} = 0$$

이다. 그런데 $1, x, \ldots, x^{q-r-1}$은 선형독립이므로

$$\{\frac{r(x)}{s\cdot q(x)}, \frac{xr(x)}{s\cdot q(x)}, \ldots, \frac{x^{q-r-1}r(x)}{s\cdot q(x)}\}$$

도 선형독립이다. 따라서 $L(A+B-Q)$의 기저이므로

$$\dim L(A+B-Q) = q-r$$

이다.

한편 $f \in \mathrm{Ker}(\mathrm{ev}_D)$ 이면

$$\mathrm{ev}_D(f) = (t(\alpha_1)r(\alpha_1), \ldots, t(\alpha_q)r(\alpha_q), \lim_{x\to\infty}\frac{t(x)r(x)}{s\cdot q(x)}) = (0, \ldots 0)$$

이다. $r(\alpha_i) \neq 0$이고 $s(\alpha_i) = q(\alpha_i) \neq 0$이므로

$$t(\alpha_1) = 0,\ \ldots,\ t(\alpha_q) = 0,\ \ \lim_{x\to\infty}\frac{t(x)r(x)}{q(x)} = 0$$

이다. 즉 $\deg t(x) < q-1-r$이고 $t(x)$는 q개의 근을 갖는데 $q-1-r \leq q$이므로 $t(x)$는 영다항식이다. 따라서 $\dim(\mathrm{Ker}(\mathrm{ev}_D)) = 0$이고

$$\dim(\mathrm{Im}(\mathrm{ev}_D)) + \dim(\mathrm{Ker}(\mathrm{ev}_D)) = \dim L(A+B-Q) = q-r$$

이므로 $\dim(\mathrm{Im}(\mathrm{ev}_D)) = q-r$이다. 그러므로 $\dim C_L(D, A+B-Q) = q-r$ 이다.

정리 12. $C_L(D, A+B-Q)$의 생성행렬은

$$H = \begin{pmatrix} r(\alpha_1) & \dots & r(\alpha_q) & 0 \\ \alpha_1 r(\alpha_1) & \dots & \alpha_q r(\alpha_q) & 0 \\ {\alpha_1}^2 r(\alpha_1) & \dots & {\alpha_q}^2 r(\alpha_q) & 0 \\ \vdots & \ddots & \vdots & \vdots \\ {\alpha_1}^{q-r-1} r(\alpha_1) & \dots & {\alpha_q}^{q-r-1} r(\alpha_q) & 1 \end{pmatrix} \tag{2}$$

이다.

증명. 정리11에 의하여 $\dim L(A+B-Q) = \dim C_L(D, A+B-Q) = q-r$이므로 ev_D는 동형사상이다. 따라서 $C_L(D, A+B-Q)$의 기저는

$$\{\mathrm{ev}(\frac{r(x)}{s \cdot q(x)}), \mathrm{ev}(\frac{xr(x)}{s \cdot q(x)}), \mathrm{ev}(\frac{x^{q-r-1}r(x)}{s \cdot q(x)})\}$$

이다.

위 생성행렬 H는 [1]의 5장의 $[q+1, k, q-k+2]$ MDS 부호의 홀짝검사 행렬을 구체적으로 구한것이다.

정리 13. $C_L(D, Q)$의 생성행렬을 G라고 하고 $C_L(D, A+B-Q)$의 생성행렬을 H라고 하자. 그러면 $G \cdot H^T = 0$이다.

증명. (1)에서 주어진 G의 각 행을 $u_0, u_1, \dots, u_r$이라고 하고 (2)에서 주어진 H의 각 행을 $v_0, v_1, \dots, v_{q-r-1}$이라고 하자. $\mathbb{F}$의 원시원소 β에 대해서 $\mathbb{F}$의 서로다른 q개의 원소 $\alpha = \{\alpha_1, \dots, \alpha_q\}$를 $\alpha_i = \beta^i (1 \le i \le q-1)$, $\alpha_q = 0$이라고 하자. 그리고 β는 원시원소이므로 $\beta^{q-1} = 1$이 성립한다.

(i) $0 \le i \le r-1$, $0 \le j \le q-r-2$일 때

$$u_i = (\frac{{\alpha_1}^i}{r(\alpha_1)}, \frac{{\alpha_2}^i}{r(\alpha_2)}, \dots, \frac{{\alpha_{q-1}}^i}{r(\alpha_{q-1})}, \frac{{\alpha_q}^i}{r(\alpha_q)}, 0),$$

$$v_j = ({\alpha_1}^j r(\alpha_1), {\alpha_2}^j r(\alpha_2), \dots, {\alpha_{q-1}}^j r(\alpha_{q-1}), {\alpha_q}^j r(\alpha_q), 0)$$

이다. 그러면

$$\begin{aligned} u_i \cdot v_j^T &= {\alpha_1}^{i+j} + {\alpha_2}^{i+j} + \cdots + {\alpha_{q-1}}^{i+j} + {\alpha_q}^{i+j} \\ &= (\beta^1)^{i+j} + (\beta^2)^{i+j} + \cdots + (\beta^{q-1})^{i+j} \\ &= (\beta^{i+j})^1 + (\beta^{i+j})^2 + \cdots + (\beta^{i+j})^{q-1} \\ &= \frac{\beta^{i+j}(1-(\beta^{i+j})^{q-1})}{1-(\beta^{i+j})} = \frac{\beta^{i+j}(1-(\beta^{q-1})^{i+j})}{1-(\beta^{i+j})} \end{aligned} \quad (*)$$

이다. $\beta^{q-1} = 1$이므로 ${u_i \cdot v_j}^T = 0$이다.

(ii) $i = r,\ \ 0 \le j \le q-r-2$일 때

$$u_i = (\frac{{\alpha_1}^i}{r(\alpha_1)}, \frac{{\alpha_2}^i}{r(\alpha_2)}, \ldots, \frac{{\alpha_{q-1}}^i}{r(\alpha_{q-1})}, \frac{{\alpha_q}^i}{r(\alpha_q)}, 1),$$

$$v_j = ({\alpha_1}^j r(\alpha_1), {\alpha_2}^j r(\alpha_2), \ldots, {\alpha_{q-1}}^j r(\alpha_{q-1}), {\alpha_q}^j r(\alpha_q), 0)$$

이다. 그러면

$${u_i \cdot v_j}^T = {\alpha_1}^{i+j} + {\alpha_2}^{i+j} + \cdots + {\alpha_{q-1}}^{i+j} + {\alpha_q}^{i+j}$$

는 (*)과 같으므로 ${u_i \cdot v_j}^T = 0$이다.

(iii) $0 \le i \le r-1,\quad j = q-r-1$일 때

$$u_i = (\frac{{\alpha_1}^i}{r(\alpha_1)}, \frac{{\alpha_2}^i}{r(\alpha_2)}, \ldots, \frac{{\alpha_{q-1}}^i}{r(\alpha_{q-1})}, \frac{{\alpha_q}^i}{r(\alpha_q)}, 0),$$

$$v_j = ({\alpha_1}^j r(\alpha_1), {\alpha_2}^j r(\alpha_2), \ldots, {\alpha_{q-1}}^j r(\alpha_{q-1}), {\alpha_q}^j r(\alpha_q), 1)$$

이다. 그러면

$${u_i \cdot v_j}^T = {\alpha_1}^{i+j} + {\alpha_2}^{i+j} + \cdots + {\alpha_{q-1}}^{i+j} + {\alpha_q}^{i+j}$$

는 $(*)$과 같으므로 ${u_i \cdot v_j}^T = 0$이다.

(iv) $i = r,\quad i = q-r-1$일 때

$$u_i = (\frac{{\alpha_1}^r}{r(\alpha_1)}, \frac{{\alpha_2}^r}{r(\alpha_2)}, \ldots, \frac{{\alpha_{q-1}}^r}{r(\alpha_{q-1})}, \frac{{\alpha_q}^r}{r(\alpha_q)}, 1),$$

$$v_j = ({\alpha_1}^{q-r-1} r(\alpha_1), {\alpha_2}^{q-r-1} r(\alpha_2), \ldots, {\alpha_{q-1}}^{q-r-1} r(\alpha_{q-1}), {\alpha_q}^{q-r-1} r(\alpha_q), 1)$$

이다. 그러면

$$\begin{aligned} u_i \cdot {v_j}^T &= {\alpha_1}^{q-1} + {\alpha_2}^{q-1} + \cdots + {\alpha_{q-1}}^{q-1} + {\alpha_q}^{q-1} + 1 \\ &= (\beta^1)^{q-1} + (\beta^2)^{q-1} + \cdots + (\beta^{q-1})^{q-1} + 1 \\ &= (\beta^{q-1})^1 + (\beta^{q-1})^2 + \cdots + (\beta^{q-1})^{q-1} + 1 \end{aligned}$$

이다. $\beta^{q-1} = 1$이므로

$$= 1(q-1) + 1 = -1 + 1 = 0$$

이다. 따라서 모든 i, j에 대해서 $G \cdot H^T = 0$이다.

정리 14.

$$C_L(D, Q)^{\perp} = C_L(D, A + B - Q)$$

이다.

증명. 정리13에서 $G \cdot H^T = 0$이므로 $C_L(D, A+B-Q) \subset C_L(D, Q)^{\perp}$이다. 그리고 정리6과 정리11에 의해서

$$\dim C_L(D, Q) + \dim C_L(D, A + B - Q) = q + 1$$

이므로 $C_L(D, A + B - Q) = C_L(D, Q)^{\perp}$이다.

따라서 H는 $C_L(D, Q)$의 홀짝검사 행렬이다.

예제 8. 예제6의 $C_L(D, Q_1)$의 쌍대부호 $C_L(D, A + B - Q_1)$은 $[10, 5]$ 선형부호이고 $C_L(D, Q_1)$의 홀짝검사 행렬 H_1을 계산하면

$$H_1 = \begin{pmatrix} \beta & \beta^2 & \beta^2 & \beta^2 & \beta & \beta & \beta^2 & \beta & \beta^7 & 0 \\ 0 & \beta^3 & \beta^4 & \beta^5 & \beta^5 & \beta^6 & \beta^8 & \beta^8 & \beta^7 & 0 \\ 0 & \beta^4 & \beta^6 & \beta^8 & \beta & \beta^3 & \beta^6 & \beta^7 & \beta^7 & 0 \\ 0 & \beta^5 & \beta^8 & \beta^3 & \beta^5 & \beta^8 & \beta^4 & \beta^6 & \beta^7 & 0 \\ 0 & \beta^6 & \beta^2 & \beta^6 & \beta & \beta^5 & \beta^2 & \beta^5 & \beta^7 & 1 \end{pmatrix}$$

이다.

예제 9. 예제7의 $C_L(D, Q_2)$의 쌍대부호 $C_L(D, A+B-Q_2)$는 $[9, 6]$ 선형부호이고 $C_L(D, Q_2)$의 생성행렬 H_2를 계산하면

$$H_2 = \begin{pmatrix} 1 & \beta^5 & \beta^3 & \beta^5 & \beta^6 & \beta^6 & \beta^3 & 1 & 0 \\ 0 & \beta^6 & \beta^5 & \beta & \beta^3 & \beta^4 & \beta^2 & 1 & 0 \\ 0 & 1 & 1 & \beta^4 & 1 & \beta^2 & \beta & 1 & 0 \\ 0 & \beta & \beta^2 & 1 & \beta^4 & 1 & 1 & 1 & 0 \\ 0 & \beta^2 & \beta^4 & \beta^3 & \alpha & \beta^5 & \beta^6 & 1 & 0 \\ 0 & \beta^3 & \beta^6 & \beta^6 & \beta^5 & \beta^3 & \beta^5 & 1 & 1 \end{pmatrix}$$

이다.

정리 15. $C_L(D, A+B-Q)$는 MDS 부호이다.

증명. (2)에서 주어진 $C_L(D, A+B-Q)$의 생성행렬 H가 있다고 하자. $\deg z(x) = q-r-1$인 기약다항식이라고 할 때 정리8에 의해 $C_L(D, (z)_0)$의 최소거리는 $r+2$이다. 한편 $C_L(D, (z)_0)$의 생성행렬 G'은

$$G' = \begin{pmatrix} \frac{1}{z(\alpha_1)} & \frac{1}{z(\alpha_2)} & \cdots & \frac{1}{z(\alpha_q)} & 0 \\ \frac{\alpha_1}{z(\alpha_1)} & \frac{\alpha_2}{z(\alpha_2)} & \cdots & \frac{\alpha_q}{z(\alpha_q)} & 0 \\ \frac{{\alpha_1}^2}{z(\alpha_1)} & \frac{{\alpha_2}^2}{z(\alpha_2)} & \cdots & \frac{{\alpha_q}^2}{z(\alpha_q)} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{{\alpha_1}^{q-r-1}}{z(\alpha_1)} & \frac{{\alpha_2}^{q-r-1}}{z(\alpha_2)} & \cdots & \frac{{\alpha_q}^{q-r-1}}{z(\alpha_q)} & 1 \end{pmatrix}$$

이다. G'은 H의 $i(1 \le i \le q)$열에는 $\frac{r(\alpha_i)}{z(\alpha_i)}$를 곱하고 $q+1$열에는 1을 곱한것이므로 $C_L(D, (z)_0)$와 $C_L(D, A+B-Q)$는 부호로서 동형이다. 따라서 $C_L(D, A+B-Q)$의 최소거리와 차원의 합은 $(r+2)+(q-r) = (q+1)+1$이 성립하므로 MDS 부호이다.

참고문헌

[1] F. J. MacWilliams and N. J. A. Sloane. The Theory of Error-Correcting Codes. North Holland, 1983.

[2] Henning Stichtenoth. Algebraic Function Fields and Codes. Springer-Verlag, 2nd ed, 2009.