2019년 2월
교육학석사(수학교육)학위논문

리드-뮬러 부호의 일반화된 해밍 무게

조선대학교 교육대학원

수학교육전공

오 유 정

리드-뮬러 부호의 일반화된 해밍 무게

Generalized Hamming weights of Reed-Muller codes

2019년 2월

조선대학교 교육대학원

수학교육전공

오 유 정

리드-뮬러 부호의 일반화된 해밍 무게

지도교수 이 관 규

이 논문을 교육학석사(수학교육)학위 청구논문으로 제출함.

2018년 10월

조선대학교 교육대학원

수학교육전공

오 유 정

오유정의 교육학 석사학위 논문을 인준함.

심사위원장　　조선대학교 교수　안 영 준 (인)

심사위원　　조선대학교 교수　오 동 렬 (인)

심사위원　　조선대학교 교수　이 관 규 (인)

2018년　12월

조선대학교 교육대학원

목 차

ABSTRACT

Generalized Hamming weights of Reed-Muller codes

Oh Yu Jeong
Advisor: Professor Kwankyu Lee
Major in Mathematics Education
Graduate School of Education, Chosun University

The Reed-Muller codes are one of the best known error correcting codes. The Reed-Muller codes are used to create secret sharing schemes. It is effective to use the generalized Hamming weights of the error correction codes to analyze the access structure of the secret sharing schemes. The generalized Hamming weights are a generalization of the minimum distance of the error correction codes. In this thesis, we obtain lower bounds of the generalized Hamming weights of Reed-Muller codes based on the theory of the Groebner basis. It turns out that the values we obtain are true generalized Hamming weights of the Reed-Muller codes. To obtain these result we first summarize the basic theory and concepts of Reed-Muller codes.

제 1 장

소개

리드-뮬러 부호는 가장 유명한 오류정정부호 중 하나이다. 최근에는 오류정정부호를 이용하여 비밀공유스킴을 만들며 오류정정부호의 일반화된 해밍무게를 알면 비밀공유스킴의 접근구조분석에 도움이 된다. Tapia-Recillas, Renteria, Lachaud와 Duursma는 [2],[5],[8] 에서 고전적 리드-뮬러 부호를 사영공간의 점들을 이용하여 일반화하였다. 특별히 토러스 부호, 아핀 리드-뮬러 부호, 사영 리드-뮬러 부호에 대해서는 일반화된 해밍무게 연구가 많이 이루어지고 있다. 따라서 이 논문에서는 그뢰브너 기저이론을 바탕으로 이 부호들의 일반화된 해밍무게를 구하고자 한다.

구체적으로 2장에서는 유한체 위에서 해밍거리와 해밍무게를 정의하고 오류정정부호의 일반화된 해밍무게를 정의한다. 이때 일반화된 해밍무게와 오류정정부호의 최소거리는 밀접한 관계가 있다. 사영공간의 점을 이용한 리드-뮬러 부호를 정의하고 리드-뮬러 부호 중 토러스 부호, 아핀 리드-뮬러 부호, 사영 리드-뮬러 부호에 대하여 알아보고 이들의 일반화된 해밍무게에 알려진 결과를 소개한다.

3장에서는 단항식들의 차수역사전식 순서에 대하여 선두항을 이용하여 이데알 I에 대한 $\Delta(I)$와 $\Sigma(I)$를 정의하고 $\Sigma(I)$을 사용하여 그뢰브너 기저를 정의한다. 그리고 사영공간의 부분집합 X가 정의하는 이데알과 리드-뮬러 부호와의 관계를 본다. 다음에 리드-뮬러 부호의 일반화된 해밍무게를 이데알의 그뢰브너 기저를 이용하여 하계를 구하는 방법을 소개하고 토러스 부호, 아핀 리드-뮬러 부호, 사영 리드-뮬러 부호 순으로 그뢰브너 기저이론을 이용하여 일반화된 해밍무게를 구하는 방법을 구체적으로 보인다. 여기에 싱글턴 상계를 이용하여 우리가 구한 일반화된 해밍무게 하계가 정확히 리드-뮬러 부호의 일반화된 해밍무게의 값이 됨을 확인한다.

제 2 장

기본개념

2.1 오류정정부호

$\mathbb{F}_q$는 q개의 원소를 갖는 유한체(finite field)를 나타내고 $\mathbb{F}_q^*$는 $\mathbb{F}_q$의 원소에서 0을 제외한 모든 원소를 나타낸다. 다음은 유한체 $\mathbb{F}_9$에 대하여 보고자한다.

예제 1. 체 $\mathbb{F}_3 = \{0, 1, 2\}$ 위에서 $p(x) = x^2 + x + 2$는 기약다항식이다.
$p(\alpha) = \alpha^2 + \alpha + 2 = 0$라고 하면 위수 9인 체 $\mathbb{F}_9$는

$$\begin{aligned}\mathbb{F}_9 &= \{a_0 + a_1\alpha \mid a_0, a_1 \in \mathbb{F}_3\} \\ &= \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}\end{aligned}$$

이다. 이때

$$\begin{aligned}\alpha^0 &= 1 & \alpha^4 &= 2 \\ \alpha^1 &= \alpha & \alpha^5 &= 2\alpha \\ \alpha^2 &= 2\alpha + 1 & \alpha^6 &= \alpha + 2 \\ \alpha^3 &= 2\alpha + 2 & \alpha^7 &= \alpha + 1\end{aligned}$$

이므로

$$\mathbb{F}_9 = \{0\} \cup \{\alpha^i \mid 0 \le i \le 7\} = \{0, \alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$$

이고

$$\mathbb{F}_9^* = \{\alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$$

이다.

이때 $\mathbb{F}_q^m = \{(a_1, \cdots, a_m) \mid a_i \in \mathbb{F}_q\}$이고 두 벡터 v_1, $v_2 \in \mathbb{F}_q^m$에 대하여

$$d(v_1, v_2) = |\{1 \le i \le m \mid a_i \neq b_i\}|$$

은 v_1과 v_2의 해밍 거리(Hamming distance)이고 벡터 $v \in \mathbb{F}_q^m$에 대하여

$$\mathrm{wt}(v) = |\{1 \le i \le m \mid a_i \neq 0\}|$$

은 v의 해밍 무게(Hamming weight)이다. 다음 예제를 보자.

예제 2. 체 $\mathbb{F}_2 = \{0,1\}$ 위에서 $p(x) = x^2 + x + 1$은 기약다항식이다. $p(\alpha) = \alpha^2 + \alpha + 1 = 0$라고 하면 $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$이고 $\mathbb{F}_4^3 = \{(a_1, a_2, a_3) \mid a_i \in \mathbb{F}_4\}$이다. $\mathbb{F}_4^3$의 두 벡터 $v_1 = (1,0,1), v_2 = (0,0,\alpha)$에 대하여 해밍 거리는 $d(v_1, v_2) = 2$ 이고 해밍 무게는 $\mathrm{wt}(v_1) = 2$, $\mathrm{wt}(v_2) = 1$ 이다.

$\mathbb{F}_q^n$의 부분공간 C에 대하여

$$\begin{aligned} d &= \min\{d(v_1, v_2) \mid v_1, v_2 \in C, v_1 \neq v_2\} \\ &= \min\{\mathrm{wt}(v) \mid v \in C, v \neq 0\} \end{aligned}$$

이고 C의 최소거리이다. 이때 차원이 k, 최소거리 d, 길이가 n이면 C를 $[n,k,d]$ 오류정정부호라고 한다.

Wei는 오류정정부호의 최소거리를 [10]에서 자연스럽게 일반화하였다. 이제 V가 C의 r차원$(1 \le r \le k)$ 부분공간일때

$$\mathrm{supp}(V) = \{i \mid v \in V, v_i \neq 0\}$$

로 정의한다. 오류정정부호 C의 r차원의 일반화된 해밍무게를 $1 \le r \le k$에 대해서

$$d_r(C) = \min\{|\mathrm{supp}(V)| \mid V \subset C, \quad \dim \mathbb{F}_q(V) = r\}$$

로 정의한다. 그러면 $d_1(C) = d$이다.

예제 3. $q = 7$, $d = 3$일 때

$$C = \mathrm{span}\{(1,1,1,1,1,1), (1,2,3,4,5,6), (1,4,2,2,4,1), (1,1,0,1,6,6)\}$$

에 대하여 C의 길이가 6이고 차원이 4이고 최소거리 3이다. 따라서 C는 $[6,4,3]$ 오류정정부호이다. 이제 $\mathbb{F}_7^6$의 2차원 부분공간

$$V = \mathrm{span}\{(0,3,1,1,3,0), (0,1,3,3,6,0)\}$$

에 대해서

$$\mathrm{supp}(V) = \{2,3,4,5\}$$

이고

$$|\mathrm{supp}(V)| = 4$$

이다. 사실은 $d_2(C) = 4$이다.

Wei [10]에 의하면

정리 1. $[n,k,d]$ 오류정정부호 C가 있을때 양수 k에 대하여

$$1 \le d_1(C) < d_2(C) < \cdots < d_k(C) \le n$$

이다. 또

$$d_r(C) \le n-k+r$$

이고 이것을 일반적인 싱글턴 상계(general Singleton bound)라고한다.

2.2 리드-뮬러 부호

$\mathbb{F}_q$ 위의 m차원 사영공간(projective space)을

$$\mathbb{P}^m_{\mathbb{F}_q} = \{(a_0 : a_1 : \cdots : a_m) \mid (a_0, a_1, \ldots, a_m) \neq 0, \quad a_0, a_1, \ldots, a_m \in \mathbb{F}_q\}$$

로 정의한다. 사영공간 $\mathbb{P}^m_{\mathbb{F}_q}$의 원소는 0이 아닌 $\mathbb{F}_q$의 원소λ에 대하여
$(a_0 : \cdots : a_m) = (\lambda a_0 : \cdots : \lambda a_m)$이다. 그러므로

$$|\mathbb{P}^m_{\mathbb{F}_q}| = \frac{q^{m+1}-1}{q-1}$$

이다. 다음 예제에서 사영공간 $\mathbb{P}^2_{\mathbb{F}_4}$에 대하여 보고자한다.

예제 4. 기약다항식 $\alpha^2+\alpha+1=0$에 대하여 체 $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$이다. 이때

$$\begin{aligned}\mathbb{P}^2_{\mathbb{F}_4} &= \{(a_0 : a_1 : a_2) \mid (a_0 : a_1 : a_2) \neq 0, a_0, a_1, a_2 \in \mathbb{F}_4\} \\ &= \{(1:0:0), (0:1:0), (0:0:1), \ldots, (1:\alpha:\alpha^2)\}\end{aligned}$$

이고

$$|\mathbb{P}^2_{\mathbb{F}_4}| = \frac{4^3-1}{4-1} = 21$$

이다. 이때 사영공간 $\mathbb{P}^2_{\mathbb{F}_4}$의 원소 $(1:1:1)$는 $(\alpha:\alpha:\alpha)$와 같다.

다변수 다항식 환 S

$$\begin{aligned}S &= \mathbb{F}_q[x_0, x_1, \ldots, x_m] \\ &= S_0 \oplus S_1 \oplus \cdots\end{aligned}$$

는 $\mathbb{F}_q$ 위의 벡터공간이다. 차수가 d인 동차다항식의 집합

$$S_d = \text{span}\{{x_0}^{n_0} {x_1}^{n_1} \cdots {x_m}^{n_m} \mid n_0 + n_1 + \ldots + n_m = d\}$$

에 대해서

$$\dim S_d = \binom{d+m}{m}$$

이다. 단항식 $f = x_0^{n_0} \cdots x_m^{n_m}$에 대해서 $\deg(f) = n_0 + n_1 + \ldots + n_m$이다. 다음 예제를 보자.

예제 5. $m=2,\ d=3$인경우

$$\begin{aligned} S_3 &= \text{span}\{{x_0}^{n_0}{x_1}^{n_1}{x_2}^{n_2} \mid n_0+n_1+n_2=3\} \\ &= \{{x_0}^3, {x_1}^3, {x_2}^3, {x_0}^2x_1, {x_0}^2x_2, x_0{x_1}^2, x_0{x_2}^2, {x_1}^2x_2, x_1{x_2}^2, x_0x_1x_2\} \end{aligned}$$

이고

$$\dim S_3 = \binom{5}{2} = 10$$

이다.

사영공간 $\mathbb{P}^m_{\mathbb{F}_q}$의 부분집합 $X=\{P_1, P_2, \ldots, P_n\}$이고 $d \geq 0$ 이라고 하자. 이제 $f_{d,i} \in S_d,\ 1 \leq i \leq n$에 대하여 각각 i에 대해 $f_{d,i}(P_i) \neq 0$을 선택한다. 구체적으로 $P_i=(x_0 : x_1 : \cdots : x_m)$가 있을때 $x_0=0, \cdots, x_{j-1}=0, x_j \neq 0$이면$f_{d,i}=x_j^d$ 으로 선택할 수 있다. S_d의 원소 다항식 f에 대하여

$$\text{ev}(f) = (\frac{f}{f_{d,1}}(P_1), \frac{f}{f_{d,2}}(P_2), \ldots, \frac{f}{f_{d,n}}(P_n)) \in \mathbb{F}_q^n$$

로 정의한다. 다음 예제를 통하여 $\text{ev}(f)$를 직접 구하여 보고자한다.

예제 6. $\mathbb{F}_9=\mathbb{F}_3(\alpha),\ \alpha^2+\alpha+2=0$을 생각하자. 이때 X에서 첫번째 자리가 1인 8개의 점을

$$[1:1:1], [1:1:2], [1:1:\alpha], [1:1:\alpha+1], [1:1:\alpha+2],$$

$$[1:1:2\alpha], [1:1:2\alpha+1], [1:1:2\alpha+2]$$

으로 선택한다. 이제 $d=3,\ f_{3,i}={x_0}^3$ 이고 $f=x_0x_1x_2$ 이면

$$\frac{f}{f_{3,1}}(P_1)=\frac{f(1,1,1)}{f_{3,1}(1,1,1)}=1$$
$$\frac{f}{f_{3,2}}(P_2)=\frac{f(1,1,2)}{f_{3,2}(1,1,2)}=2$$
$$\frac{f}{f_{3,3}}(P_3)=\frac{f(1,1,\alpha)}{f_{3,3}(1,1,\alpha)}=\alpha$$
$$\frac{f}{f_{3,4}}(P_4)=\frac{f(1,1,\alpha+1)}{f_{3,4}(1,1,\alpha+1)}=\alpha+1$$
$$\frac{f}{f_{3,5}}(P_5)=\frac{f(1,1,\alpha+2)}{f_{3,5}(1,1,\alpha+2)}=\alpha+2$$
$$\frac{f}{f_{3,6}}(P_6)=\frac{f(1,1,2\alpha)}{f_{3,6}(1,1,2\alpha)}=2\alpha$$
$$\frac{f}{f_{3,7}}(P_7)=\frac{f(1,1,2\alpha+1)}{f_{3,7}(1,1,2\alpha+1)}=2\alpha+1$$
$$\frac{f}{f_{3,8}}(P_8)=\frac{f(1,1,2\alpha+2)}{f_{3,8}(1,1,2\alpha+2)}=2\alpha+2$$

이므로

$$\mathrm{ev}(f)=(1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2)\in\mathbb{F}_9^8$$

이다.

이제 $\mathrm{ev}:S_d\longrightarrow\mathbb{F}_q^n$이 $\mathbb{F}_q$위의 선형사상이므로

$$C_X(d)=\{\mathrm{ev}(f):f\in S_d\}$$

는 $\mathbb{F}_q^n$의 부분공간이고 $C_X(d)$를 X위의 리드-뮬러(Reed-Muller)부호라고 한다.

2.3 특별한 리드-뮬러 부호

리드-뮬러 부호에는 여러가지 부호가 있다. 이때 대표적인 부호로 토러스 부호, 아핀 리드-뮬러 부호, 사영 리드-뮬러 부호가 있다. 이때 토러스는

$$\mathbb{T}_q^m=\{(a_0:a_1:\cdots:a_m)\mid a_i\in\mathbb{F}_q^*,\quad 0\le i\le m\}$$

이고 $X=\mathbb{T}_q^m$일 때 정의되는 리드-뮬러 부호를 토러스 부호라고 한다. Pinto, Saemiento, Villarreal [9]에 의하면 $m=1$인 경우 $C_{\mathbb{T}_q^1}$의 길이는 $q-1$이고 차원은 $d+1$이고 $d_r(C_{\mathbb{T}_q^1})=q-d+r-2$이다.

예제 7. $q=4$일때 $\mathbb{T}_4^1=\{(1:1),(1:\alpha),(1:\alpha^2)\}$이다. 따라서 $(C_{\mathbb{T}_4^1})$의 길이는 3이고 차원은 $d+1$이고 $d_r(C_{\mathbb{T}_4^1})=2-d+r$이다.

그리고 아핀공간은

$$\mathbb{A}_q^m=\{(1:a_1:\cdots:a_m)\mid a_i\in\mathbb{F}_q^*,\quad 1\le i\le m\}$$

이고 $X=\mathbb{A}_q^m$일 때 아핀 리드-뮬러 부호라고 한다. Pellikaan, Henijnen [4]에 의하면 $m=1$인 경우 $C_{\mathbb{A}_q^1}$의 길이는 q이고 차원은 $d+1$이고 $d_r(C_{\mathbb{A}_q^1})=q-d+r-1$이다.

예제 8. $q=4$일때 $\mathbb{A}_4^1=\{(1:0),(1:1),(1:\alpha),(1:\alpha^2)\}$이다. 따라서 $(C_{\mathbb{A}_4^1})$의 길이는 4이고 차원은 $d+1$이고 $d_r(C_{\mathbb{A}_4^1})=3-d+r$이다.

마지막으로 사영공간은

$$\mathbb{P}_q^m=\{(a_0:a_1:\cdots:a_m)\mid(a_0,a_1,\ldots,a_m)\neq 0,\quad a_i\in\mathbb{F}_q,\quad 0\le i\le m\}$$

이고 $X=\mathbb{P}_q^m$일 때 사영 리드-뮬러 부호라고 한다. Lachaud [6]에 의하면 $m=1$인 경우 $C_{\mathbb{P}_q^1}$의 길이는 $q+1$이고 차원은 $d+1$이고 $d_r(C_{\mathbb{P}_q^1})=q-d+r$이다.

예제 9. $q=4$일때 $\mathbb{P}_4^1=\{(0:1),(1:0),(1:1),(1:\alpha),(1:\alpha^2)\}$이다. 따라서 $(C_{\mathbb{P}_4^m})$의 길이는 5이고 차원은 $d+1$이고 $d_r(C_{\mathbb{P}_4^1})=4-d+r$이다.

토러스 부호, 아핀 리드-뮬러 부호, 사영 리드-뮬러 부호의 일반화된 해밍무게에 대하여 각 저자들은 서로 다른 방법을 이용하여 결과를 얻었다. 다음 장에서 우리는 그뢰브너 기저이론을 이용하여 동일한 방법으로 각 리드-뮬러 부호에 대하여 일반화된 해밍무게의 하계를 구하려고한다. 또 하계가 정확한 값이 됨을 보인다.

제 3 장

연구결과

3.1 그뢰브너 기저와 정리

두 단항식 $x^d = {x_0}^{d_0}{x_1}^{d_1}\cdots{x_m}^{d_m}$와 $x^e = {x_0}^{e_0}{x_1}^{e_1}\cdots{x_m}^{e_m}$에 대해서

$$\deg(x^d) = d_0 + d_1 + \ldots + d_m, \quad \deg(x^e) = e_0 + e_1 + \ldots + e_m$$

이다. 이때

$$x^d > x^e \Leftrightarrow \deg(x^d) > \deg(x^e) \quad \text{이거나}$$
$$\deg(x^d) = \deg(x^e) \quad \text{이면} \quad d_m = e_m, \cdots, d_{i+1} = e_{i+1}, \quad d_i < e_i$$

를 단항식들의 차수역사전식(degrevlex) 순서로 정의한다. 그리고 다항식 $f \in \mathbb{F}[x_0, x_1, \ldots, x_m]$에 대하여 다항식 f를 이루는 여러 단항식 중 가장 큰 단항식은 선두항(leading term)이고 기호는 $\mathrm{lt}(f)$이다. 다음 예제를 보자.

예제 10. 다음 다항식

$$f = {x_0}^3{x_2}^2 + {x_1}^3{x_2}^2 + {x_0}^3x_1x_2, \quad f \in \mathbb{F}[x_0, x_1, x_2]$$

를 차수역사전식 순서에 의해 나타내면 f의 단항식들의 순서는

$${x_0}^3x_1x_2 > {x_0}^3{x_2}^2 > {x_1}^3{x_2}^2$$

이다. 따라서 f의 선두항은

$$\mathrm{lt}(f) = {x_0}^3x_1x_2$$

이다.

이제 다항식의 선두항을 이용하여 이데알 I에 대한 $\Delta(I)$과 $\Sigma(I)$를 정의할 수 있다.

$$\Sigma(I) = \{\mathrm{lt}(f) \mid f \in I\}$$

이고

$$\Delta(I) = \Sigma(S) \backslash \Sigma(I)$$

이다. 이제 $f_1, f_2, \cdots, f_r \in I$에 대하여 $\Sigma(I) = \langle \mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_r) \rangle$이면 $\{f_1, f_2, \ldots, f_r\}$을 I의 그뢰브너 기저(groebner basis)라고 한다. 그뢰브너 기저에 대한 자세한 내용은 David [1]를 참고한다. 다음 예제를 통하여 $\Delta(I)$집합과 $\Sigma(I)$집합을 찾아보고자 한다.

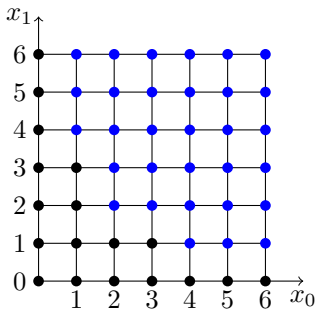
예제 11. 이데알

$$I = \langle x_0^4 x_1 + x_0^2 x_1, x_0 x_1^4, x_0^2 x_1^2 \rangle$$

이고 $f_1 = x_0^4 x_1 + x_0^2 x_1$, $f_2 = x_0 x_1^4$, $f_3 = x_0^2 x_1^2 \in \mathbb{F}[x_0, x_1]$에 대하여 f_1를 차수역사전식 순서에 따라 나타내면 $x_0^4 x_1 > x_0^2 x_1$이다. 따라서 선두항은

$$\mathrm{lt}(f_1) = x_0^4 x_1, \quad \mathrm{lt}(f_2) = x_0 x_1^4, \quad \mathrm{lt}(f_3) = x_0^2 x_1^2$$

이고 I의 그뢰브너 기저는 $\{x_0^4 x_1 + x_0^2 x_1, x_0 x_1^4, x_0^2 x_1^2\}$ 이다. 그러므로 아래 그림과 같이 $\Sigma(I)$는 파란점들의 집합을 나타내고 $\Delta(I)$은 검은점들의 집합을 나타낸다.



X를 $\mathbb{P}^m_{\mathbb{F}_q}$의 부분집합이라 하자. S의 동차이데알(homogeneous ideal)

$$I_X = \langle f \in S_d \mid f(P) = 0, P \in X \rangle \in S$$

을 X의 이데알이라고 한다. 여기서 $\mathrm{ev} : S_d \longrightarrow \mathbb{F}_q^n$으로 가는 선형사상이므로

$$\begin{aligned} \ker(\mathrm{ev}) &= \langle f \in S_d : \mathrm{ev}(f) = 0, d \geq 0 \rangle \\ &= I_X \cap S_d \end{aligned}$$

이다. 그러면

$$C_X(d) \cong (S/I_X)_d = S_d/I_{X,d} \quad (I_{X,d} = I_X \cap S_d)$$

성립한다. David [1]에 의하면

$$\dim(C_X(d)) = \dim(S_d/I_{X,d}) = |\Delta_d(I)| = k$$

이다. 그리고 $|\Delta_d(I)|$는 계속 증가하다가 충분히 커지고 나면 일정한 값이 된다. 이때 일정한 값이 되는 수 중 가장 작은 d의 값을 ν라고한다. 이관규 [7]에 의하면

정리 2. $C_X(d)$의 부분공간 V에 대하여 V의 기저벡터가 $\mathrm{ev}(g_1), \mathrm{ev}(g_2), \cdots, \mathrm{ev}(g_r)$일 때

$$\mathrm{wt}(V) = |\mathrm{supp}(V)| \geq |\bigcup_{i=1}^{r} \{\rho \in \Delta_\nu(I) : \rho \mathrm{lt}(g_i) \in \Delta_{\nu+d}(I)\}|$$

이다.

이제 $\mu_1, \mu_2, \ldots, \mu_r \in \Delta_d(I)$이면

$$D(\mu_1, \mu_2, \ldots, \mu_r) = \bigcup_{i=1}^{r} \{\rho \in \Delta_\nu(I) : \rho\mu_i \in \Delta_{\nu+d}(I)\}$$

를 D집합이라고 하고

$$\delta_r = \min\{|D(\mu_1, \mu_2, \ldots, \mu_r)| : \mu_1 > \mu_2 > \cdots > \mu_r \in \Delta_d(I)\}$$

로 정의한다. 정리2에 의하면 $d_r \geq \delta_r$이다.

3.2 토러스 부호

사영공간 $\mathbb{P}_q^m$의 부분집합

$$\mathbb{T}_q^m = \{(a_0 : a_1 : \cdots : a_m) \mid a_i \in \mathbb{F}_q^*, \quad 0 \leq i \leq m\}$$

를 토러스라고 한다. Renteria [3]에 의하면

정리 3. 토러스 $\mathbb{T}_q^m$의 이데알은

$$I_{\mathbb{T}_q^m} = \langle x_i^{q-1} - x_m^{q-1} : 0 \leq i < m \rangle$$

이고 이데알 $I_{\mathbb{T}_q^m}$의 그뢰브너 기저는

$$\{x_i^{q-1} - x_m^{q-1} : 0 \leq i < m\}$$

이다.

예제 12. $m = 1$이고 $q = 9$라 하자. 이때 $I_{\mathbb{T}_9^1}$의 그뢰브너 기저는 $\{x_0^8 - x_1^8\}$이고 $I = I_{\mathbb{T}_9^1} = \langle x_0^8 - x_1^8 \rangle$이므로 그림3.1과 같이 $\Sigma(I)$와 $\Delta(I)$를 찾을 수 있다.

정리 4. 오류정정부호 $C = C_{\mathbb{T}_q^1}(d)$의 길이는 $n = q - 1$이고 $0 \leq d \leq q - 2$에 대하여 차원은 $k = d + 1$이다. 그리고

$$d_r(C) = q - d + r - 2, \quad 1 \leq r \leq k$$

이다.

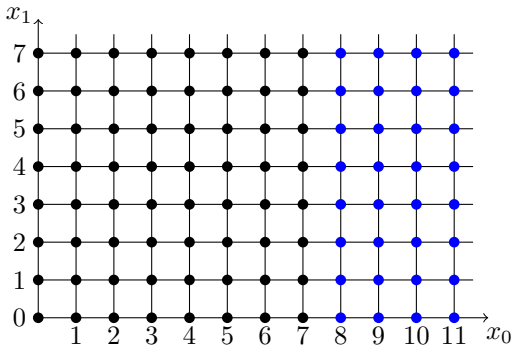
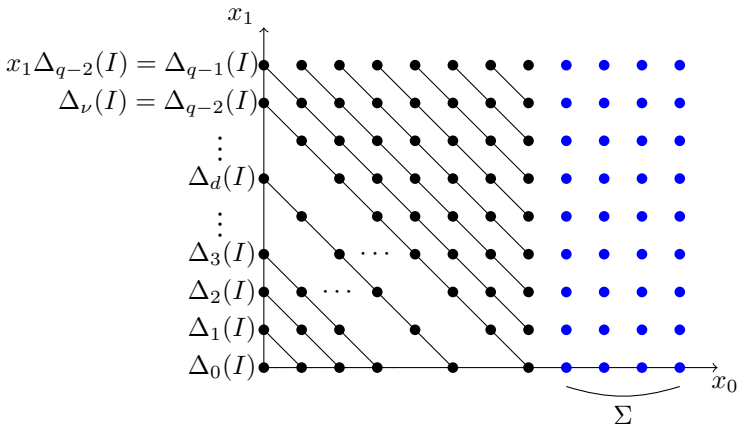


그림 3.1: 검은점의 집합은 $\Delta(I)$ 파란점의 집합은 $\Sigma(I)$

증명. 정리3으로부터 $m = 1$이면 $I = I_{\mathbb{T}_q^1} = \langle x_0^{q-1} - x_1^{q-1} \rangle$이고 그뢰브너 기저는 $\{x_0^{q-1} - x_1^{q-1}\}$이다. 따라서 $\Sigma(I) = \{x_0^{q-1+i}x_1^j \mid i, j \geq 0\}$이고 $\Delta_d(I) = \Sigma(S_d) \backslash \Sigma(I)$이므로

$$\begin{aligned}
\Delta_0(I) &= \{1\} \\
\Delta_1(I) &= \{x_0, x_1\} \\
\Delta_2(I) &= \{x_0^2, x_0x_1, x_1^2\} \\
&\vdots \\
\Delta_{q-2}(I) &= \{x_0^{q-2}, x_0^{q-3}x_1, \cdots, x_1^{q-2}\} \\
\Delta_{q-1}(I) &= x_1\Delta_{q-2}(I)
\end{aligned}$$

이다. 아래의 그림을 참고하면 이해하기 쉽다.



그리고 0보다 큰 s에 대하여 $\Delta_{q-2+s}(I) = x_1^s\Delta_{q-2}(I)$이고 $\nu = q-2$이다. 그러므로

$$\Delta_\nu(I) = \{x_0^{q-2}, x_0^{q-3}x_1, \cdots, x_0x_1^{q-3}, x_1^{q-2}\}$$

이다. 그리고

$$\Delta_d(I) = \{x_0^d, x_0^{d-1}x_1, \cdots, x_0x_1^{d-1}, x_1^d\}$$

이고

$$\Delta_{\nu+d}(I) = x_1^d\Delta_\nu(I) = \{x_0^{q-2}x_1^d, x_0^{q-3}x_1^{d+1}, \cdots, x_0x_1^{d+q-3}, x_1^{d+q-2}\}$$

이다.

일반적으로 $\Delta_d(I)$의 원소를 $\mu = x_0^{d-i}x_1^i,\ 0 \le i \le d$라고 하면

$$\mu\Delta_\nu(I) = \{x_0^{q+d-i-2}x_1^i, x_0^{q+d-i-3}x_1^{i+1}, \cdots, x_0^{d-i}x_1^{q+i-2}\}$$

이고 $\mu\Delta_\nu(I) \cap \Delta_{\nu+d}(I) = \{x_0^{q-2}x_1^d, \cdots, x_0^{d-i+1}x_1^{q+i-3}, x_0^{d-i}x_1^{q+i-2}\}$이다. 따라서

$$|\mu\Delta_\nu(I) \cap \Delta_{\nu+d}(I)| = q - d + i - 1$$

이다. 이때 D집합은

$$\begin{aligned} D(\mu) &= \{\rho \in \Delta_\nu(I) : \mu\rho \in \Delta_{\nu+d}(I)\} \\ &= \{x_0^{q-d+i-2}x_1^{d-i}, x_0^{q-d+i-3}x_1^{d-i+1}, \cdots, x_1^{q-2}\} \end{aligned}$$

이므로

$$|D(\mu)| = q - d + i - 1$$

이다.

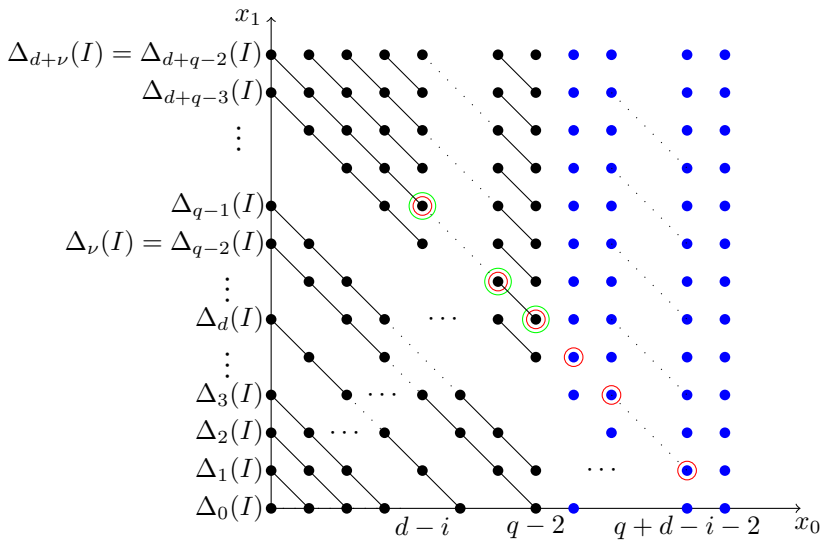


그림 3.2: 빨간원은 $\mu\Delta_\nu$, 초록원은 $\mu\Delta_\nu \cap \Delta_{\nu+d}$

다음 과정을 더 쉽게 이해하기 위하여 $i=0$일 때와 $i=1$일 때를 보고자한다. 위의 결과에 따라 $i=0$이면 $\mu = x_0^d$이고

$$\begin{aligned} D(\mu) &= \{\rho \in \Delta_\nu(I) : \rho\mu \in \Delta_{\nu+d}(I)\} \\ &= \{x_0^{q-d-2}x_1^d, x_0^{q-d-3}x_1^{d+1}, \cdots, x_1^{q-2}\} \end{aligned}$$

이다. 그 다음 $i=1$이면 $\mu = x_0^{d-1}x_1$이고

$$\begin{aligned} D(\mu) &= \{\rho \in \Delta_\nu(I) : \mu\rho \in \Delta_{\nu+d}(I)\} \\ &= \{x_0^{q-d-1}x_1^{d-1}, x_0^{q-d-2}x_1^d, \cdots, x_1^{q-2}\} \end{aligned}$$

이다. 이와 같이 차수역사전식 순서에 따라 $x_0^d > x_0^{d-1}x_1$이고 $D(x_0^d) \subset D(x_0^{d-1}x_1)$임을 알았다. 아래의 그림3.3을 참고하면 이해하기 쉽다.

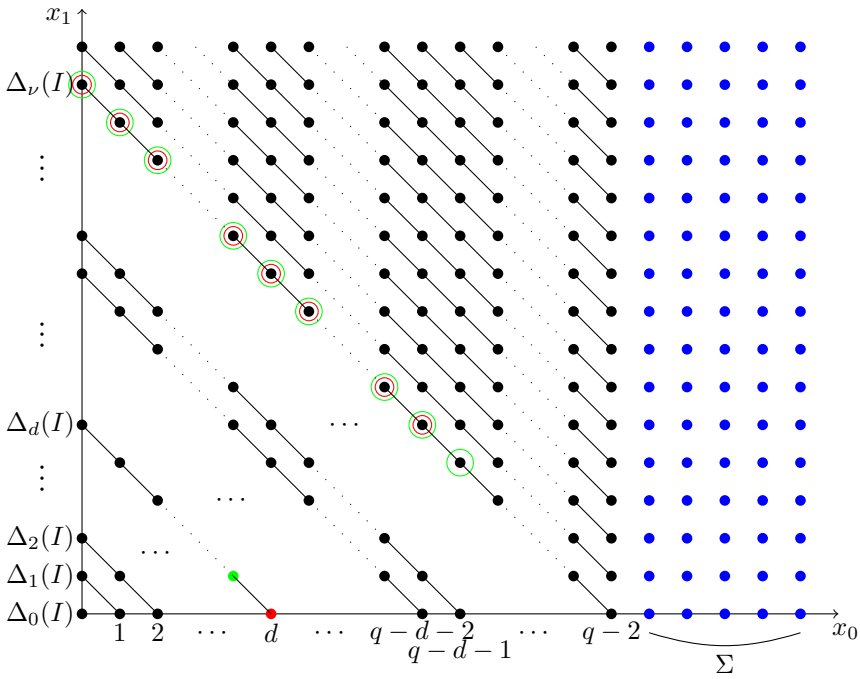


그림 3.3: 빨간점은 x_0^d, 빨간원은 $D(x_0^d)$, 초록점은 $x_0^{q-1}x_1$, 초록원은 $D(x_0^{q-1}x_1)$

따라서 $\Delta_d(I)$의 원소들을 차수역사전식 순서에 따라 원소를 나열하면

$$x_0^d > x_0^{d-1}x_1 > \cdots > x_1^d$$

이고 큰 단항식을 선택할수록 D집합들의 관계는

$$D(x_0^d) \subset D(x_0^{d-1}x_1) \subset \cdots \subset D(x_1^d)$$

이다. 이제 $1 \le r \le k$라고 하자. $\mu_1 > \mu_2 > \cdots > \mu_r$, $\mu_i \in \Delta_d(I)$에 대하여

$$D(\mu_1) \subset D(\mu_2) \subset \cdots \subset D(\mu_r)$$

이므로

$$D(\mu_1, \mu_2, \ldots, \mu_r) = D(\mu_1) \cup D(\mu_2) \cup \cdots \cup D(\mu_r) = D(\mu_r)$$

이다. 따라서

$$\begin{aligned}\delta_r &= \min\{|D(\mu_1, \mu_2, \ldots, \mu_r)| : \mu_1 > \mu_2 > \cdots > \mu_r \in \Delta_d(I)\} \\ &= |\{x_0^{q-d+r-3}x_1^{d-r+1}, x_0^{q-d+r-4}x_1^{d-r+2}\}| \\ &= q-d+r-2\end{aligned}$$

이다.

이때 C의 길이는 $n = |\mathbb{T}_q^1| = q-1$이고 차원은 $k = |\Delta_d(I)| = d+1$이다. 정리1에 의하면 $1 \le r \le k$ 에 대하여

$$\begin{aligned}d_r &\le n-k+r \\ &= (q-1)-(d+1)+r \\ &= q-d+r-2 \\ &= \delta_r\end{aligned}$$

이다. 즉 $d_r \le \delta_r$이고 정리2에 의하면 $d_r \ge \delta_r$이므로

$$d_r = \delta_r = q-d+r-2$$

이고 이 값이 정확한 값이 된다.

예제 13. $m=1$이고 $q=9$라 하자. 그러면 $n=8$, $k=d+1$이다. 이때 정리4를 이용하여 $C_{\mathbb{T}_9^1}(d)$의 일반화된 해밍무게를 표 3.1에서 구하여 보였다.

	n	k	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8
$d=1$	8	2	7	8						
$d=2$	8	3	6	7	8					
$d=3$	8	4	5	6	7	8				
$d=4$	8	5	4	5	6	7	8			
$d=5$	8	6	3	4	5	6	7	8		
$d=6$	8	7	2	3	4	5	6	7	8	
$d=7$	8	8	1	2	3	4	5	6	7	8

표 3.1: $C_{\mathbb{T}_9^1}(d)$의 일반화된 해밍무게

3.3 아핀 리드-뮬러 부호

아핀공간은 $\mathbb{A}_q^m \approx \mathbb{F}_q^m$이다. Renteria [8]에 의하면

정리 5. 아핀공간 $\mathbb{A}_q^m$의 이데알은

$$I_{\mathbb{A}_q^m} = \langle x_i^q - x_i x_m^{q-1} : 0 \le i < m \rangle$$

이고 이데알 $I_{\mathbb{A}_q^m}$의 그뢰브너 기저는

$$\{x_i^q - x_i x_m^{q-1} : 0 \le i < m\}$$

이다.

예제 14. $m = 1$이고 $q = 9$라 하자. 이때 $I_{\mathbb{A}_9^1}$의 그뢰브너 기저는 $\{x_0^9 - x_0 x_1^8\}$이고 $I = I_{\mathbb{A}_9^1} = \langle x_0^9 - x_0 x_1^8 \rangle$이므로 그림3.4와 같이 $\Sigma(I)$와 $\Delta(I)$를 찾을 수 있다.

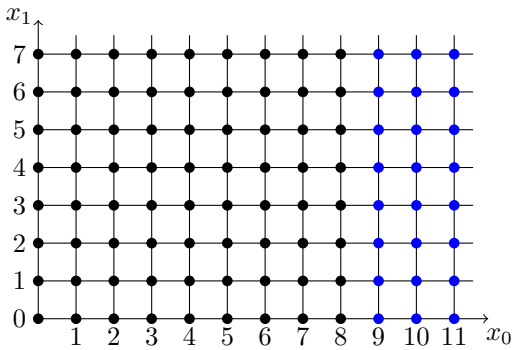


그림 3.4: 검은점의 집합은 $\Delta(I)$, 파란점의 집합은 $\Sigma(I)$

정리 6. 오류정정부호 $C = C_{\mathbb{A}_q^1}(d)$의 길이는 $n = q$이고 $0 \le d \le q-1$에 대하여 차원은 $k = d+1$이다. 그리고

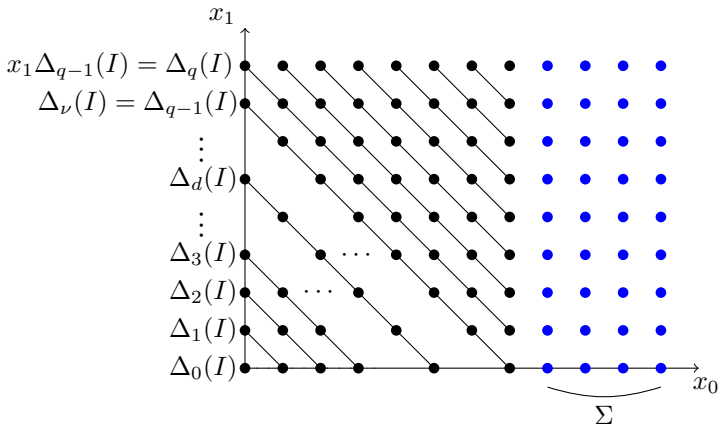
$$d_r(C) = q - d + r - 1, \quad 1 \le r \le k$$

이다.

증명. 정리5로부터 $m = 1$이면 $I = I_{\mathbb{A}_q^1} = \langle x_0^q - x_0 x_1^{q-1} \rangle$ 이고 그뢰브너 기저는 $\{x_0^q - x_0 x_1^{q-1}\}$이다. 따라서 $\Sigma(I) = \{x_0^{q+i} x_1^j \mid i, j \ge 0\}$이고 $\Delta_d(I) = \Sigma(S_d) \backslash \Sigma(I)$이므로

$$\begin{aligned}\Delta_0(I) &= \{1\}\\ \Delta_1(I) &= \{x_0, x_1\}\\ \Delta_2(I) &= \{x_0^2, x_0x_1, x_1^2\}\\ &\vdots\\ \Delta_{q-1}(I) &= \{x_0^{q-1}, x_0^{q-2}x_1, \cdots, x_1^{q-1}\}\\ \Delta_q(I) &= x_1\Delta_{q-1}(I)\end{aligned}$$

이다. 아래의 그림을 참고하면 이해하기 쉽다.



그리고 0보다 큰 s에 대하여 $\Delta_{q-1+s}(I) = x_1^s\Delta_{q-1}(I)$이고 $\nu = q-1$이다. 그러므로

$$\Delta_\nu(I) = \{x_0^{q-1}, x_0^{q-2}x_1, \cdots, x_0x_1^{q-2}, x_1^{q-1}\}$$

이다. 그리고

$$\Delta_d(I) = \{x_0^d, x_0^{d-1}x_1, \cdots, x_0x_1^{d-1}, x_1^d\}$$

이고

$$\Delta_{\nu+d}(I) = \{x_0^{q-1}x_1^d, x_0^{q-2}x_1^{d+1}, \cdots, x_0x_1^{d+q-2}, x_1^{d+q-1}\}$$

이다.

일반적으로 $\Delta_d(I)$의 원소를 $\mu = x_0^{d-i}x_1^i,\ 0 \le i \le d$라고 하면

$$\mu\Delta_\nu(I) = \{x_0^{q+d-i-1}x_1^i, x_0^{q+d-i-2}x_1^{i+1}, \cdots, x_0^{d-i}x_1^{q+i-1}\}$$

이고 $\mu\Delta_\nu(I) \cap \Delta_{\nu+d}(I) = \{x_0^{q-1}x_1^d, \cdots, x_0^{d-i+1}x_1^{q+i-2}, x_0^{d-i}x_1^{q+i-1}\}$이다. 따라서

$$|\mu\Delta_\nu(I) \cap \Delta_{\nu+d}(I)| = q - d + i$$

이다. 이때 D집합은

$$\begin{aligned} D(\mu) &= \{\rho \in \Delta_\nu(I) : \mu\rho \in \Delta_{\nu+d}(I)\} \\ &= \{x_0^{q-d+i-1}x_1^{d-i}, x_0^{q-d+i-2}x_1^{d-i+1}, \cdots, x_1^{q-1}\} \end{aligned}$$

이므로

$$|D(\mu)| = q - d + i$$

이다.

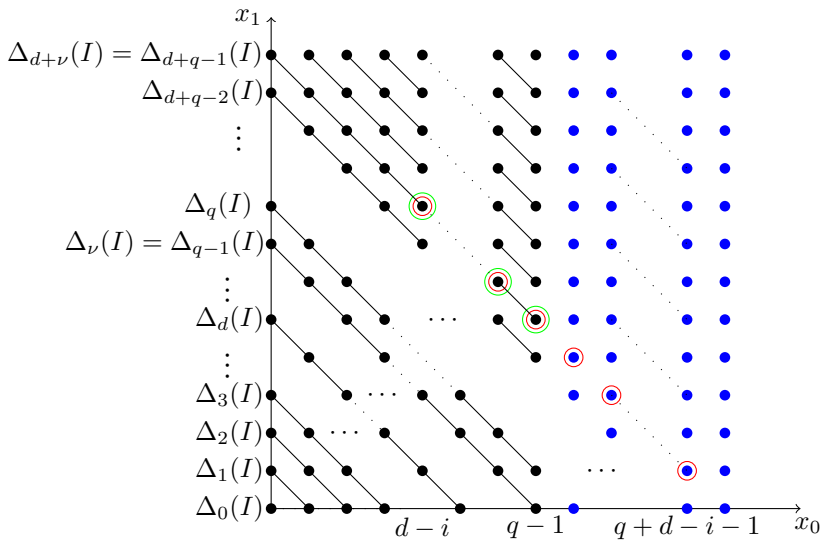


그림 3.5: 빨간원은 $\mu\Delta_\nu$, 초록원은 $\mu\Delta_\nu \cap \Delta_{\nu+d}$

다음 과정을 더 쉽게 이해하기 위하여 $i=0$일 때와 $i=1$일 때를 보고자 한다. 위의 결과에 따라 $i=0$이면 $\mu = x_0^d$이고

$$\begin{aligned} D(\mu) &= \{\rho \in \Delta_\nu(I) : \rho\mu \in \Delta_{\nu+d}(I)\} \\ &= \{x_0^{q-d-1}x_1^d, x_0^{q-d-2}x_1^{d+1}, \cdots, x_1^{q-1}\} \end{aligned}$$

이다. 그 다음 $i=1$이면 $\mu = x_0^{d-1}x_1$이고

$$\begin{aligned} D(\mu) &= \{\rho \in \Delta_\nu(I) : \rho\mu \in \Delta_{\nu+d}(I)\} \\ &= \{x_0^{q-d}x_1^{d-1}, x_0^{q-d-1}x_1^d, \cdots, x_1^{q-1}\} \end{aligned}$$

이다. 이와 같이 차수역사전식 순서에 따라 $x_0^d > x_0^{d-1}x_1$이고 $D(x_0^d) \subset D(x_0^{d-1}x_1)$임을 알았다. 아래의 그림3.6을 참고하면 이해하기 쉽다.

따라서 $\Delta_d(I)$의 원소들을 차수역사전식 순서에 따라 원소를 나열하면

$$x_0^d > x_0^{d-1}x_1 > \cdots > x_1^d$$

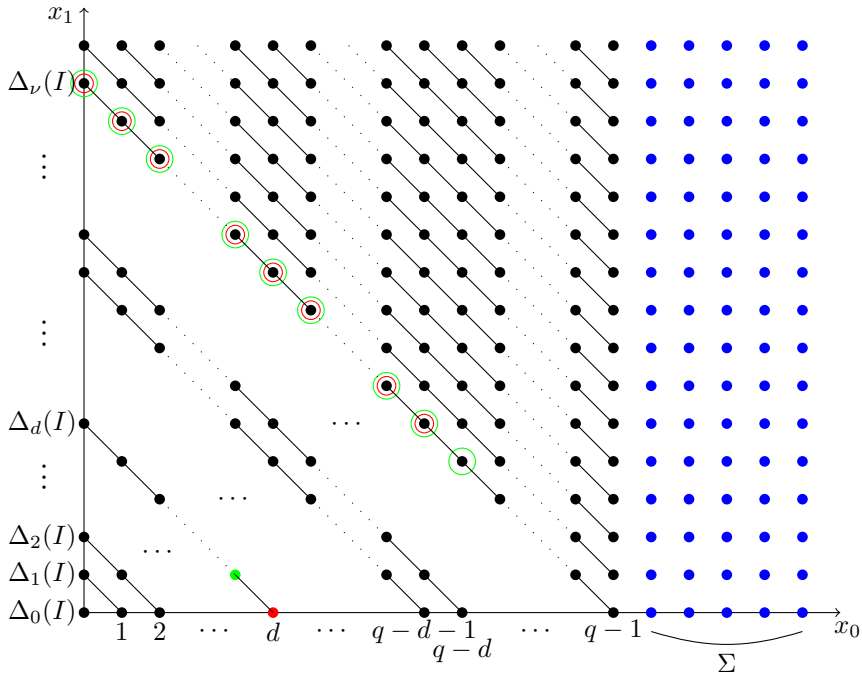


그림 3.6: 빨간점은 x_0^d, 빨간원은 $D(x_0^d)$, 초록점은 $x_0^{d-1}x_1$, 초록원은 $D(x_0^{d-1}x_1)$

이고 큰 단항식을 선택할수록 D집합들의 관계는

$$D(x_0^d) \subset D(x_0^{d-1}x_1) \subset \cdots \subset D(x_1^d)$$

이다. 이제 $1 \le r \le k$라고 하자. $\mu_1 > \mu_2 > \cdots > \mu_r$, $\mu_i \in \Delta_d(I)$에 대하여

$$D(\mu_1) \subset D(\mu_2) \subset \cdots \subset D(\mu_r)$$

이므로

$$D(\mu_1, \mu_2, \ldots, \mu_r) = D(\mu_1) \cup D(\mu_2) \cup \cdots \cup D(\mu_r) = D(\mu_r)$$

이다. 따라서

$$\begin{aligned} \delta_r &= \min\{|D(\mu_1, \mu_2, \ldots, \mu_r)| : \mu_1 > \mu_2 > \cdots > \mu_r \in \Delta_d(I)\} \\ &= |\{x_0^{q-d+r-2}x_1^{d-r+1}, x_0^{q-d+r-3}x_1^{d-r+2}, \cdots, x_1^{q-1}\}| \\ &= q-d+r-1 \end{aligned}$$

이다.

이때 C의 길이는 $n = |\mathbb{A}_q^1| = q$이고 차원은 $k = |\Delta_d(I)| = d+1$이다. 정리1에

의하면$1 \leq r \leq k$ 에 대하여

$$\begin{aligned} d_r(C) &\leq n-k+r \\ &= (q)-(d+1)+r \\ &= q-d+r-1 \\ &= \delta_r \end{aligned}$$

이다. 즉 $d_r \leq \delta_r$이고 정리2에 의하면 $d_r \geq \delta_r$이므로

$$d_r = \delta_r = q-d+r-1$$

이고 이 값이 정확한 값이 된다.

예제 15. $m=1$이고 $q=9$라 하자. 그러면 $n=9,\ k=d+1$이다. 이때 정리6을 이용하여 $C_{\mathbb{A}_9^1}(d)$의 일반화된 해밍무게를 표 3.2에서 구하여 보였다..

	n	k	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8	d_9
$d=1$	9	2	8	9							
$d=2$	9	3	7	8	9						
$d=3$	9	4	6	7	8	9					
$d=4$	9	5	5	6	7	8	9				
$d=5$	9	6	4	5	6	7	8	9			
$d=6$	9	7	3	4	5	6	7	8	9		
$d=7$	9	8	2	3	4	5	6	7	8	9	
$d=8$	9	9	1	2	3	4	5	6	7	8	9

표 3.2: $C_{\mathbb{A}_9^1}(d)$의 일반화된 해밍무게

3.4 사영 리드-뮬러 부호

사영공간은 $\mathbb{P}_q^m$이다. Renteria [8]에 의하면

정리 7. 사영공간 $\mathbb{P}_q^m$의 이데알은

$$I_{\mathbb{P}_q^m} = \langle x_i^q x_j - x_i x_m^q : 0 \leq i < j \leq m \rangle$$

이고 $I_{\mathbb{P}_q^m}$의 그뢰브너 기저는

$$\{x_i^q x_j - x_i x_m^q : 0 \leq i < j \leq m\}$$

이다.

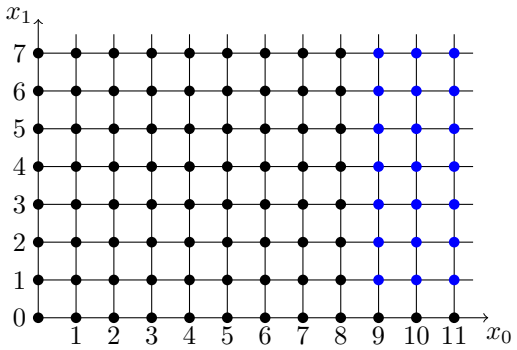


그림 3.7: 검은점의 집합은 $\Delta(I_{\mathbb{P}^1_9})$, 파란점의 집합은 $\Sigma(I_{\mathbb{P}^1_9})$

예제 16. $m=1$이고 $q=9$라 하자. 이때 $I_{\mathbb{P}^1_9}$의 그뢰브너 기저는 $\{x_0^9x_1 - x_0x_1^9\}$이고 $I = I_{\mathbb{P}^1_9} = \langle x_0^9x_1 - x_0x_1^9\rangle$이므로 그림3.7과 같이 $\Sigma(I)$와 $\Delta(I)$를 찾을 수 있다.

정리 8. 오류정정부호 $C = C_{\mathbb{P}^1_q}(d)$의 길이는 $n = q+1$ 이고 $0 \le d \le q$에 대하여 차원은 $k = d+1$이다. 그리고

$$d_r(C) = q - d + r, \quad 1 \le r \le k$$

이다.

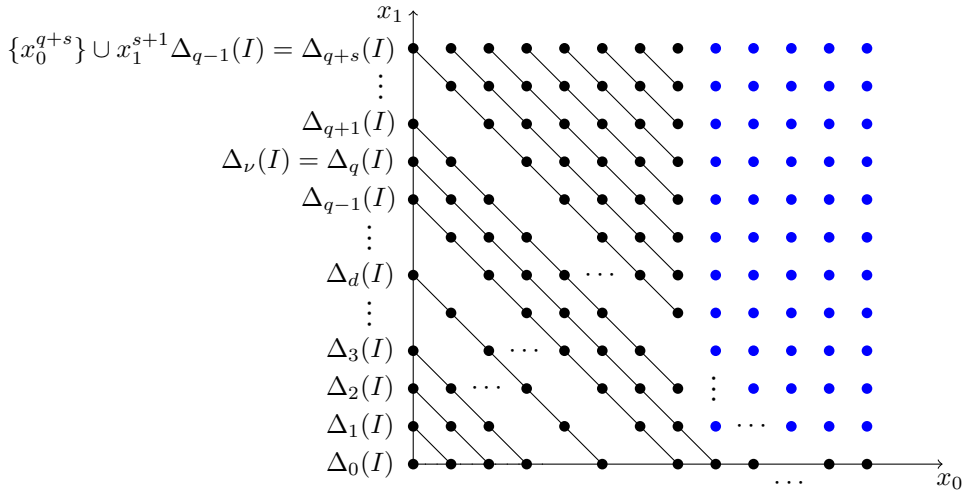
증명. 정리7로부터 $m=1$이면 $I = I_{\mathbb{P}^1_q} = \langle x_0^q x_1 - x_0 x_1^q\rangle$ 이고 그뢰브너 기저는 $\{x_0^q x_1 - x_0 x_1^q\}$이다. 따라서 $\Sigma(I) = \{x_0^{q+i}x_1^{1+j} \mid i,j \ge 0\}$이고 $\Delta_d(I) = \Sigma(S_d)\backslash\Sigma(I)$이므로

$$\begin{aligned}
\Delta_0(I) &= \{1\}\\
\Delta_1(I) &= \{x_0, x_1\}\\
\Delta_2(I) &= \{x_0^2, x_0x_1, x_1^2\}\\
&\vdots\\
\Delta_{q-1}(I) &= \{x_0^{q-1}, x_0^{q-2}x_1, \cdots, x_1^{q-1}\}\\
\Delta_q(I) &= \{x_0^q, x_0^{q-1}x_1, \cdots, x_1^q\}\\
\Delta_{q+1}(I) &= \{x_0^{q+1}\} \cup x_1^2\Delta_{q-1}(I)
\end{aligned}$$

이고 0보다 큰 s에 대하여

$$\Delta_{q+s}(I) = \{x_0^{q+s}\} \cup x_1^{s+1}\Delta_{q-1}(I)$$

이고 $\nu = q$이다. 아래의 그림을 참고하면 이해하기 쉽다.



그러므로

$$\Delta_\nu(I) = \{x_0^q, x_0^{q-1}x_1, \cdots, x_0x_1^{q-1}, x_1^q\}$$

이다. 그리고

$$\Delta_d(I) = \{x_0^d, x_0^{d-1}x_1, \cdots, x_0x_1^{d-1}, x_1^d\}$$

이고

$$\Delta_{\nu+d}(I) = \{x_0^{q+d}\} \cup \{x_0^{q-1}x_1^{d+1}, x_0^{q-2}x_1^{d+2}, \cdots, x_0x_1^{d+q-1}, x_1^{d+q}\}$$

이다.

사영 리드-뮬러 부호에서 D집합에 대하여 알아보기 위해서 두가지 경우로 나눈다.

CASE 1. $\Delta_d(I)$의 원소 $\mu = x_0^d$에 대하여

$$\mu\Delta_\nu(I) = \{x_0^{q+d}\} \cup \{x_0^{q+d-1}x_1, \cdots, x_0^dx_1^q\}$$

이다. 이때

$$\mu\Delta_\nu(I) \cap \Delta_{\nu+d}(I) = \{x_0^{q+d}\} \cup \{x_0^{q-1}x_1^{d+1}, x_0^{q-2}x_1^{d+2}, \cdots, x_0^{d+1}x_1^{q-1}, x_0^dx_1^q\}$$

이고

$$|\mu\Delta_\nu(I) \cap \Delta_{\nu+d}(I)| = q - d + 1$$

이다. 이때 D집합

$$\begin{aligned} D(\mu) &= \{\rho \in \Delta_\nu(I) : \mu\rho \in \Delta_{\nu+d}(I)\} \\ &= \{x_0^q\} \cup \{x_0^{q-d-1}x_1^{d+1}, x_0^{q-d-2}x_1^{d+2}, \cdots, x_1^q\} \end{aligned}$$

이고

$$|D(\mu)| = q - d + 1$$

이다.

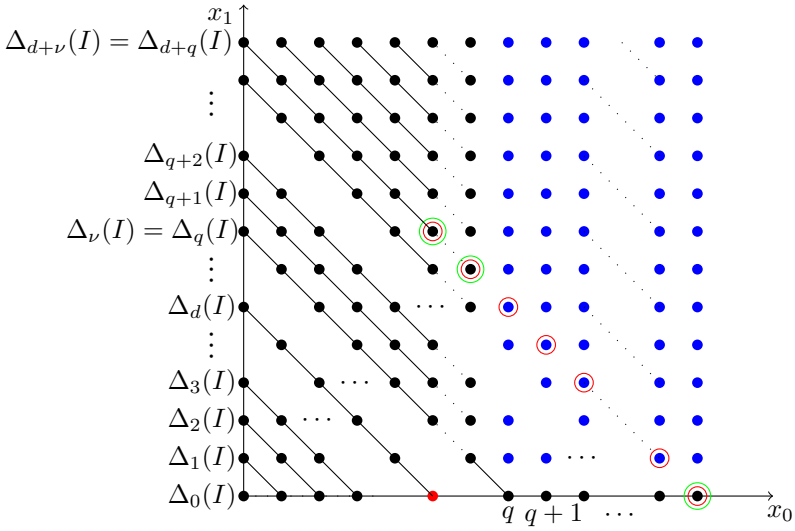


그림 3.8: 빨간점은 μ, 빨간원은 $\mu\Delta_\nu$, 초록원은 $\mu\Delta_\nu \cap \Delta_{\nu+d}$

CASE 2. $\mu = x_0^{d-i}x_1^i$, $1 \le i \le d$에 대하여

$$\mu\Delta_\nu(I) = \{x_0^{q+d-i}x_1^i, x_0^{q+d-i-1}x_1^{i+1}, \cdots, x_0^{d-i}x_1^{q+i}\}$$

이고

$$\mu\Delta_\nu(I) \cap \Delta_{\nu+d}(I) = \{x_0^{q-1}x_1^{d+1}, x_0^{q-2}x_1^{d+2}, \cdots, x_0^{d-i}x_1^{q+i}\}$$

이다. 따라서

$$|\mu\Delta_\nu(I) \cap \Delta_{\nu+d}(I)| = q - d + i$$

이다. 이때 D집합

$$\begin{aligned} D(\mu) &= \{\rho \in \Delta_\nu(I) : \mu\rho \in \Delta_{\nu+d}(I)\} \\ &= \{x_0^{q-d+i-1}x_1^{d-i+1}, x_0^{q-d+i-2}x_1^{d-i+2}, \cdots, x_1^q\} \end{aligned}$$

이다.

$$|D(\mu)| = q - d + i$$

이다.

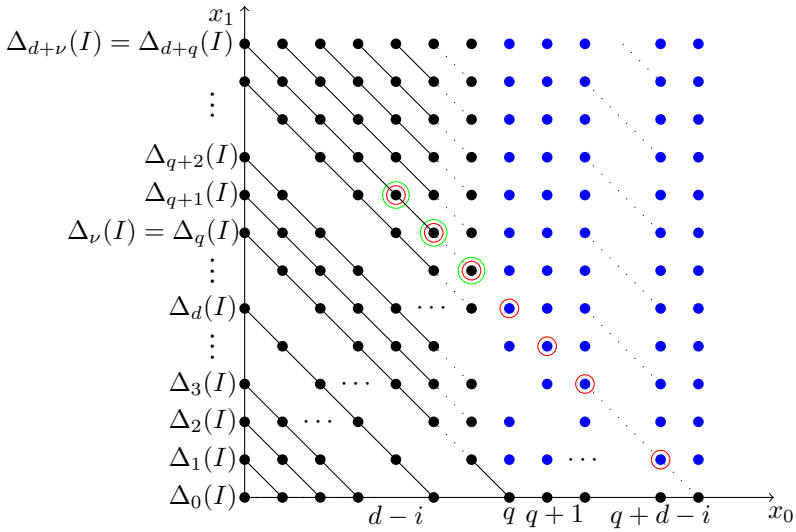


그림 3.9: 빨간원은 $\mu\Delta_\nu$, 초록원은 $\mu\Delta_\nu \cap \Delta_{\nu+d}$

다음 과정을 더 쉽게 이해하기 위하여 $i=1$일 때와 $i=2$일 때를 보고자 한다. 위의 결과에 따라 $i=1$이면 $\mu = x_0^{d-1}x_1$이고

$$\begin{aligned} D(\mu) &= \{\rho \in \Delta_\nu(I) : \rho\mu \in \Delta_{\nu+d}(I)\} \\ &= \{x_0^{q-d}x_1^d, x_0^{q-d-1}x_1^{d+1}, \cdots, x_1^q\} \end{aligned}$$

이다. 그 다음 $i=2$이면 $\mu = x_0^{d-2}x_1^2$이고

$$\begin{aligned} D(\mu) &= \{\rho \in \Delta_\nu(I) : \rho\mu \in \Delta_{\nu+d}(I)\} \\ &= \{x_0^{q-d+1}x_1^{d-1}, x_0^{q-d}x_1^d, \cdots, x_1^q\} \end{aligned}$$

이다. 이와 같이 역사전식 순서에 따른 $x_0^{d-1}x_1 > x_0^{d-2}x_1^2$이고 $D(x_0^{d-1}x_1) \subset D(x_0^{d-2}x_1^2)$임을 알았다. 아래의 그림3.10을 참고하면 이해하기 쉽다.

따라서 $\Delta_d(I)\backslash\{x_0^d\}$의 원소들을 차수역사전식 순서에 따라 원소를 나열하면

$$x_0^{d-1}x_1 > x_0^{d-2}x_1^2 > \cdots > x_1^d$$

이고 큰 단항식을 선택할수록 D집합들의 관계는

$$D(x_0^{d-1}x_1) \subset D(x_0^{d-2}x_1^2) \subset \cdots \subset D(x_1^d)$$

이다.

이제 $1 \le r \le k$라고 하자. $\mu_1 > \mu_2 > \cdots > \mu_r$, $\mu_i \in \Delta_d(I)$에 대하여

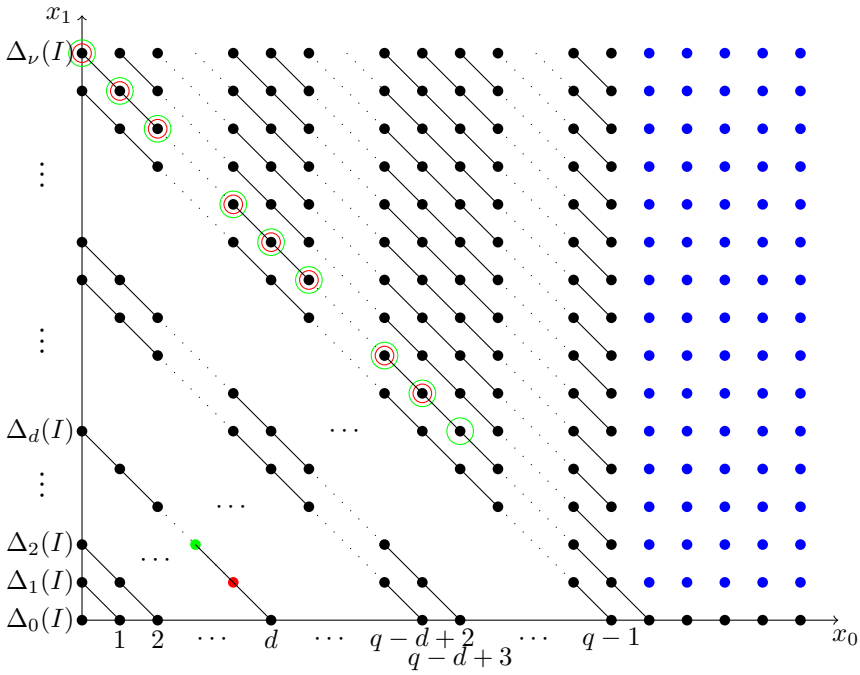


그림 3.10: 빨간점은 $x_0^{d-1}x_1$, 빨간원은 $D(x_0^{d-1}x_1)$, 초록점은 $x_0^{d-2}x_1^2$, 초록원은 $D(x_0^{d-2}x_1^2)$

CASE 1. $\mu_1 \neq x_0^d$인 경우

D집합들의 관계는

$$D(\mu_1) \subset D(\mu_2) \subset \cdots \subset D(\mu_r)$$

이므로

$$D(\mu_1, \mu_2, \ldots, \mu_r) = D(\mu_1) \cup D(\mu_2) \cup \cdots \cup D(\mu_r) = D(\mu_r)$$

이다.

CASE 2. $\mu_1 = x_0^d$인 경우

CASE 1에 의해

$$D(\mu_2) \subset \cdots \subset D(\mu_r)$$

이다. 그리고

$$\begin{aligned} D(\mu_1) &= \{\rho \in \Delta_\nu(I) : \mu\rho \in \Delta_{\nu+d}(I)\} \\ &= \{x_0^q\} \cup \{x_0^{q-d-1}x_1^{d+1}, x_0^{q-d-2}x_1^{d+2}, \cdots, x_1^q\} \subset \{\{x_0^q\} \cup D(\mu_2)\} \end{aligned}$$

이다. 이때 D집합

$$\begin{aligned} D(\mu_1, \mu_2, \ldots, \mu_r) &= D(\mu_1) \cup D(\mu_2) \cup \cdots \cup D(\mu_r) \\ &= \{x_0^q\} \cup D(\mu_r) \end{aligned}$$

이다.

따라서 $\mu_1 \neq x_0^d$인 경우는

$$\begin{aligned} &\min\{|D(\mu_1, \mu_2, \ldots, \mu_r)| : \mu_1 > \mu_2 > \cdots > \mu_r \in \Delta_d(I)\} \\ &= |\{x_0^{q-d+r-1}x_1^{d-r+1}, x_0^{q-d+r-2}x_1^{d-r+2}, \cdots, x_1^q\}| \\ &= q - d + r \end{aligned}$$

이고 $\mu_1 = x_0^d$인 경우는 $\mu_r = x_0^{d-r+1}x_1^{r-1}$일 때 최솟값을 갖는다. 따라서

$$\begin{aligned} &\min\{|D(\mu_1, \mu_2, \ldots, \mu_r)| : \mu_1 > \mu_2 > \cdots > \mu_r \in \Delta_d(I)\} \\ &= |\{x_0^q\} \cup \{x_0^{q-d+r-2}x_1^{d-r+2}, x_0^{q-d+i-3}x_1^{d-i+3}, \cdots, x_1^q\}| \\ &= q - d + r \end{aligned}$$

이다. 이와 같이 μ_r을 무엇으로 선택하든 같은 값을 나타낸다. 따라서

$$\begin{aligned} \delta_r &= \min\{|D(\mu_1, \mu_2, \ldots, \mu_r)| : \mu_1 > \mu_2 > \cdots > \mu_r \in \Delta_d(I)\} \\ &= q - d + r \end{aligned}$$

이다.

이때 C의 길이는 $n = |\mathbb{P}_q^1| = q + 1$이고 차원은 $k = |\Delta_d(I)| = d + 1$이다. 정리1에 의하면 $1 \leq r \leq k$ 에 대하여

$$\begin{aligned} d_r &\leq n - k + r \\ &= (q+1) - (d+1) + r \\ &= q - d + r \end{aligned}$$

이다. 즉 $d_r \leq \delta_r$이고 정리2에 의하면 $d_r \geq \delta_r$이므로

$$d_r = \delta_r = q - d + r$$

이고 이 값이 정확한 값이 된다.

예제 17. $m = 1$이고 $q = 9$라 하자. 그러면 $n = 10$, $k = d + 1$이다. 이때 정리8을 이용하여 $C_{\mathbb{P}_9^1}(d)$의 일반화된 해밍무게를 표 3.3에서 구하여 보였다.

	n	k	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8	d_9	d_{10}	d_{11}
$d=1$	10	2	9	10									
$d=2$	10	3	8	9	10								
$d=3$	10	4	7	8	9	10							
$d=4$	10	5	6	7	8	9	10						
$d=5$	10	6	5	6	7	8	9	10					
$d=6$	10	7	4	5	6	7	8	9	10				
$d=7$	10	8	3	4	5	6	7	8	9	10			
$d=8$	10	9	2	3	4	5	6	7	8	9	10		
$d=9$	10	10	1	2	3	4	5	6	7	8	9	10	
$d=10$	10	11	0	1	2	3	4	5	6	7	8	9	10

표 3.3: $C_{\mathbb{P}^1_9}(d)$의 일반화된 해밍무게

참고문헌

[1] David A. Cox, John Little, and Donal O'Shea. Ideals, varieties, and algorithms. Springer, pages 539–591, 2007.

[2] I. M. Duursma, C. Renteria, and H. Tapia-Recillas. Reed-Muller codes on complete intersections, Applicable Algebra in Engineering. Communication and Computing, 11(6):455–462, 2001.

[3] M. Gonzaelez-Sarabia, C. Renteriea, and M. H. de la Torre. Minimum distance and second generalized Hamming weight of two particular linear codes. Congressus Numerantium, pages 105–116, 2003.

[4] P. Henijnen and R. Pellikaan. Generalized Hamming weights of q-ray Reed-Muller codes. IEEE Trans. Inf. Theory, 44(1):181–196, 1998.

[5] G. Lachaud. Projective Reed-Muller codes. Coding Theory and Applications, pages 125–129, 1988.

[6] G. Lachaud. The parameters of projective Reed-Muller codes. Discrete Mathematics, 81(2):217–221, 1990.

[7] Kwankyu Lee. Bounds for generalized Hamming weights of Reed-Muller codes on varieties.

[8] C. Renteria and H. Tapia-Recillas. Reed-Muller codes: an ideal theory approach. Communications in algebra, 25(2):401–413, 1997.

[9] E. Sarmiento, R.H. Villarreal, and M.V. Pinto. The minimum distance of parameterized codes on projective tori. Applicable Algebra in Engineering, 22(4):249–264, 2011.

[10] V. K. Wei. Generalized Hamming weights for linear codes. IEEE Trans. Inf. Theory, 37(5):91, 1991.