通信情報保護學會誌
第5卷 第2號, 1995. 6

Gröbner Bases와 응용

임 종 인*, 서 창 호*, 박 대 연**

요 약

본 논문에서는 다항식 환 $k[x_1, \cdots, x_n]$에서의 Gröbner bases 개념과 응용을 소개하고 있다. 특히, Gröbner bases를 이용한 binary cyclic code에 대한 효율적인 algebraic decoding method를 자세히 설명하고 있다.

1. 서 론

본 논문에서는 20여년간 computer algebra 분야에서 중요한 위치를 차지하여 왔으며 최근 수학, 전산학, 부호이론 등 여러 분야에서 광범위한 응용성이 발견되고 있는 Gröbner bases에 대해 소개하려한다. 1965년 B. Buchberger[Bu65]에 의해 정의되었고, 1985년 획기적으로 개선된 계산 알고리즘[Bu85]이 소개된 Gröbner bases는 이후 수학의 제분야 및 전산학의 symbolic 연산 및 대수적 연산분야에서 광범위한 응용이 발견되어 왔다[AdLou]. 특히 최근 X. Chen[Chen] 등에 의해서 Gröbner bases 이용한 binary cyclic code를 $t = \lfloor (d-1)/2 \rfloor$ error, d는 code의 실제 최소거리까지 정정할수있는 대수적 decoding method가 발견되어 더욱 우리의 관심을 끌고 있다.

Gröbner bases는 또한 integer programming 문제[CoTr]에도 성공적으로 적용될 수 있으므로, 일반적인 knapsack 암호시스템의 해독에도 이용될 수 있다. Gröbner bases의 수학 분야 특히, 대수 기하(algebraic geometry) 분야에서의 기여도는 무척 크다. 현재 Chen 등의 Gröbner bases를 이용한 decoding 의 방법을 algebraic geometric code에 적용하는 문제를 연구 중에 있으며 곧 결과가 나올 것으로 예상된다. 2절에서는 Gröbner bases 및 관련 결과들을 도입하려 한다. 3 절에서는 Gröbner bases의 응용으로서 binary cyclic code에 대한 Chen 등의 방법을 소개하려 한다.

본 연구는 1994년 교육부 기초과학 연구소 연구비에 의하여 지원받았음

* 고려대학교 자연과학대학 수학과
** 전주대학교 사범대학 수학교육학과

2. Gröbner bases

k를 체(field)라 하고 $k[x_1, \cdots, x_n]$를 k 위에서의 n 변수 다항식 환(polynomial ring)이라 하자. $X = x_1^{\beta_1} \cdots x_n^{\beta_n}$, β_i는 자연수,를 power product라 하면 $k[x_1, \cdots, x_n]$의 임의의 다항식 $f(x_1, \cdots, x_n)$은 $f = \sum_{finite} c_{\beta_1 \cdots \beta_n} x_1^{\beta_1} \cdots x_n^{\beta_n}$와 같이 유한개의 power product들의 합으로 표시될 수 있다.

▨ 정의 2-1 power product 들의 집합 위에서의 total order $\langle$가 다음의 2 조건을 만족할 때 우리는 term order라고 부른다. X, Y, Z가 power product라 할때

조건 1) $X \neq 1$이면 $1 \langle X$가 항상 성립한다.
조건 2) $X \langle Y$이면 $XZ \langle YZ$이다.

예 2-2) 사전식 순서(lexicographic order)는 term order 의 가장 중요한 예의 하나이다. 2변수 경우를 예로 들면 $x_1 \langle x_2$할 때

$$1 \langle x_1 \langle x_1^2 \langle x_1^3 \langle \cdots \langle x_2 \langle x_1x_2 \langle x_1^2x_2 \langle \cdots \langle x_2^2 \langle \cdots$$

이다. 우리는 앞으로 사전식 순서를 lex로 표시할 것이다.

term order $\langle$가 주어지면 우리는 $f \in k[x_1, \cdots, x_n]$에 대해서 leading power product $lp(f)$와 leading coefficient $lc(f)$를 자연스럽게 정의할 수 있다. $f = 2x_1^2x_2x_3 + 3x_1x_2^3 - 2x_3^2$의 경우 ($x_1 \langle x_2 \langle x_3$), $lp(f) = x_3^2$, $lc(f) = -2$가 됨을 쉽게 알 수 있다. 이 때 $-2x^2$을 leading term이라 하고 $lt(f) = -2x^2$으로 표시한다.

▨ 정의 2-3 $f, g, h \in k[x_1, \cdots, x_n]$, $g \neq 0$, 가 주어졌을 때 f의 term X에 대해서 $lp(g) \mid X$이고, $h = f - \frac{X}{lt(g)} \cdot g$의 꼴로 표시될 때, $f \xrightarrow{g} h$로 표시하고 f는 g를 법으로 하여 h로 reduced되었다고 한다.

정의를 확장하면 $f_1, \cdots, f_s$가 다항식들이라하고, $F = \{f_1, \cdots, f_s\}$라 할때, $f \xrightarrow{F} h$의 의미는 적당한 $f_{i_1}, \cdots, f_{i_t} \in F$에 대해서 $f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \to \cdots \to h_{t-1} \xrightarrow{f_{i_t}} h$가 되는 것을 의미한다.

예 2-4) $f_1 = x_2x_1 - x_2$, $f_2 = x_2^2 - x_1$, $F = \{f_1, f_2\}$라 하자. lex 순서를 생각하면 $lp(f_1) = x_2x_1$, $lp(f_2) = x_2^2$이다. $f = x_2^2x_1$이라 하면 $x_2^2x_1 \xrightarrow{f_1} x_2^2 \xrightarrow{f_2} x_1$ 즉 $f = x_2 \cdot f_1 + 1 \cdot f_2 + x_1$의 꼴로 표시된다.

f가 $F = \{f_1, \cdots, f_s\}$에 의해서 $f \xrightarrow{F} r$로 되고, $r = 0$이거나 r을 더 이상 F를 법으로 하여 reduce할 수 없을때 r을 F에 대한 f의 나머지라 부른다.(remainder of f w. r. t. F) 위의 예에서는 x_1이 나머지가 된다. 이 때 적당한 quotient $u_1, \cdots, u_s \in k[x_1, \cdots, x_n]$가 존재하여

$$f = u_1f_1 + \cdots + u_sf_s + r$$

의 꼴로 표시됨은 명백하다.

일변수의 경우와 달리 다변수의 경우에는 나머지의 유일성이 보장되지 않는다. 즉 reduction 과정에서 f_i들을 택하는 순서에 따라 r이 달라질 수 있다.

▨ 정의 2-5 $I \subset k[x_1, \cdots, x_n]$가 non-zero ideal이라 할 때, $G = \{g_1, \cdots, g_t\} \subset I$, $g_i \neq 0$가 조건 $f \in I$ iff $f \xrightarrow{G} 0$을 만족할 때, 우리는 G를 ideal I의 Gröbner basis라고 부른다.

$G = \{g_1, \cdots, g_t\}$가 ideal I의 Gröbner basis라면 $I = \langle g_1, \cdots, g_t \rangle$ 즉 I의 모든 원소가 $g_1, \cdots, g_t$의 일차 결합꼴로 표시됨은 명백하다. 모든 non-zero ideal이 Gröbner basis를 가진다는 사실은 증명되어 있으며 임의의 다항식 f를 G에 의해서 reduction하였을 때 나머지는 유일하다. 즉 임의의 다항식은 유일한 나머지 r에 대해서 $f = u_1g_1 + \cdots + u_tg_t + r$의 꼴로 표시될 수 있다. Ideal $I = \langle f_1, \cdots, f_s \rangle$가 주어졌을 때, $I = \langle g_1, \cdots, g_t \rangle$가 되는 I의 Gröbner basis $G = \{g_1, \cdots, g_t\}$는 Buchberger algorithm[Bu85]으로 구할 수 있다.

예 2-7) $f_1 = x_1^2 + x_2^2 + 1$, $f_2 = x_1^2 + 2x_1x_2 + x_1$가 주어 졌다고 하자. lex ordering 하에서 ideal $I = \langle f_1, f_2 \rangle \subset Z_5[x_1, x_2]$에 대한 Gröbner basis를 계산하면 $G = \{x_1^2 + x_2^2 + 1, x_1x_2 + 3x_1 + 2x_1^2 + 2x_2, x_2^5 + 2x_2^4 + 4x_2^2 + 2x_2 + 2\}$가 된다.

3. Gröbner bases의 응용

서론에서 언급한 바와 같이 Gröbner bases는 Buchberger[Bu65]에 의해 소개된 이후 여러 분야에서 응용이 개발되어 왔으며, 1985년 개선된 실용적인 Buchberger 알고리즘이 발표된 이후 computational mathematics 분야에서 응용폭을 넓혀왔다. 특히 algebraic geometry에서의 응용은 물론 확대체 원소의 최소 다항식(minimal polynomial)구하는 문제, graph의 coloring 문제, integer programming 문제 등에 응용되고 있으며 최근에는 Chen[Chen] 등에 의하여 Gröbner bases를 이용한 binary cyclic code의 효율적인 algebraic decoding method가 개발되었다. 이들의 방법은 algebraic geometric code의 decoding에도 적용될 수 있을 것으로 생각되며, 현재 연구중에 있다. 또한 integer programming 문제의 해법은 knapsack에 적용성이 있을 것이다.

본 절에서는 Gröbner bases의 응용으로서 Chen의 binary cyclic code에 대해 decoding 방법을 소개하려 한다.

$K = GF(2^m)$을 다항식 $x^n + 1$의 분해체(splitting field)라 하자. 그러면 원시 단위 n 승근(primitive n-th root of unity)라 불리는 원소 $\alpha \in K$가 존재하여, $x^n + 1 = \prod_{i=0}^{n-1} (x + \alpha^i)$이 된다.

예를 들어, $x^{31} + 1$의 분해체는 $GF(2^5)$이 된다. C를 K 위에서의 (n, k, d) binary cyclic code라 하자. 그러면 최대 $t = \lfloor (d-1)/2 \rfloor$개의 오류정정(error - correcting)이 가능하고, $C = \{c(x) | c(\alpha^i) = 0, \forall i \in Q\}$의 형태로 표시할 수 있다. 여기에서 Q는 code C의 complete-defining set이고 $c(x)$는 $GF(2)[x]/(x^n - 1)$의 다항식이다. 이때 code C의 생성다항식(generator polynomial) $g(x)$는 차수 $n - k$를 가지며, $\{\alpha^i | i \in Q\}$에 속하는 원소들의 최소다항식의 LCM 이 된다. $Q_r = \{r \cdot 2^j | j = 0, 1, \cdots, n_r-1\}$, n_r은 $r \cdot 2^{n_r} = r \pmod n$이 성립하는 최소 자연수이고 r은 Q_r의 최소수, 이라하면 Q는 Q_r들의 합집합으로 표시되며 이때 r들의 모임을 C의 base라 하고 R로 표시한다.

예 3-1) (31, 16, 7) binary quadratic residue code의 defining set $Q = Q_1 \cup Q_5 \cup Q_7 \{1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28\}$이고 $R = \{1, 5, 7\}$이다.

codeword $c(x) = \alpha(x) \cdot g(x)$가 noisy channel을 통하여 전송되어 수신된 codeword가 $r(x) = c(x) + e(x)$라 하자. 여기에서 $e(x)$는 error pattern vector의 다항식이다. 그러면, syndromes s_i는 $s_i = e(\alpha^i)$이고, $c(\alpha^i) = 0$이므로 $s_i = e(\alpha^i) = r(\alpha^i)$가 된다.

$$F_1 = \{\sum_{j=1}^{v_b} x_j^i + s_i | i \in R\},$$

$$F_2 = \{x_j^{n+1} + x_j | 1 \le j \le v_b\},$$

$$F = F_1 \cup F_2$$

라하자. 여기에서 v_b는 $0 < v_b \le t$인 정수이고 R은 base set이다.

예 3-2) 예3-1의 경우 송신 codeword가 all-zero codeword라 하고, 두개의 error가 발생하여 수신 codeword가 $r(x) = x^3 + x^5$이라 하자. 그러면 syndromes는 $s_1 = \alpha^8$, $s_5 = \alpha^{19}$, $s_7 = \alpha^3$이 된다. 이때

$F = \{x_2 + x_1 + \alpha^8, x_2^5 + x_1^5 + \alpha^{19}, x_2^7 + x_1^7 + \alpha^3, x_1^{32} + x_1, x_2^{32} + x_2\}$

가 된다.

$I = I(F)$를 F에 의해서 생성된 $k[x_1, \cdots, x_{v_b}]$의 ideal이라 하고 lex ordeing 하에서 Buchberger 알고리즘을 적용하여, Gröbner basis G를 구한다. 이때 G에 속하는 다항식들의 leading coefficient를 전부 1로 바꾸고 G에 대하여 reduced된 형태로 바꾸어도 여전히 I에 대한 Gröbner basis이다. 이것을 G'이라 표시하자.

❖ **정리 3-3** $I \cap k[x_1]$은 $k[x_1]$의 ideal이므로 1개의 generator를 가진다. 즉 $I \cap k[x_1] = \langle g(x_1) \rangle$이 되는 $g(x_1)$이 존재한다. 그러면 $g(x_1) = G' \cap k[x_1]$이 성립한다.

❖ **정리 3-4** $v \le v_b \le t$이고 v개의 error가 발생하였을 때 정리 3-3에서 구한 $g(x_1)$은 다음을 만족한다

i) $g(x_1) = L(x_1)$ for $v = v_b$
ii) $g(x_1) = x_1 L(x_1)$ for $v = v_b - 1$
iii) $g(x_1) = x_1^{n+1} + x_1$ for $0 < v \le v_b - 2$.

여기에서 $L(x_1)$은 error-locator polynomial이다.

위의 정리 3-4에 의해서 error-location을 찾는 문제는 $g(x_1)$의 non-zero root를 구하는 문제로 귀착되었다. 이것은 예를 들면 Chien search[Chien]에 의해서 구할 수 있다.

위의 과정을 알고리즘화하면 다음과 같다.

■ 알고리즘

단계 1) $s_i = r(\alpha^i)$를 각 $i \in R$에 대해서 계산한다.

모든 $i \in R$에 대해서 $s_i = 0$이면 stop(error - free의 경우) 아니면 $v_b = 2$로 놓고 단계 2)를 수행한다.

단계 2) $v_b > t$이면 $v_b = v_b - 1$로 놓는다.

$F = \{\sum_{j=1}^{v_b} x_j^i + s_i | i \in R\} \cup \{x_j^{n+1} + x_j | i \le j \le v_b\}$라 하자.

단계 3) lex ordering 하에서 Buchberger 알고리즘을 적용하여 reduced Gröbner basis G'을 구한다. $1 \in G'$이면, $v_b = v_b + 2$라 하고 단계 2)로 간다. 아니면 단계 4)를 수행한다.

단계 4) $G' \cap k[x_1] = \{g(x_1)\}$을 구한다. $\deg(g(x_1)) > v_b$이면 stop 한다. 아닐 경우 단계 5)를 수행한다.

단계 5) Chien search에 의해서 $g(x_1) = 0$의 non-zero root를 찾아 error-location을 실행한다.

(주의)

i) $1 \in G'$이면 error - free의 경우이다.
ii) $\deg(g(x_1)) > t$의 경우 error 정정이 불가능하다.

예 3-5) $GF(2^5)$ $x^{31} + 1$의 분해체이다. 연산표는 [Mac, p 110]에서 발견할 수 있다.

예 3-2의 경우를 계속하면 2개의 error가 발생하였을 경우 $v_b = 2$로 하여 위의 알고리즘을 수행하면, $F = \{x_2 + x_1 + \alpha^8, x_2^5 + x_1^5 + \alpha^{19}, x_2^7 + x_1^7 + \alpha^3, x_1^{32} + x_1, x_2^{32} + x_2\}$가 되고, $g(x_1) = x_1^2 + \alpha^8 x_1 + \alpha^8$이 된다. $g(x_1) = 0$의 두 근은 α^3, α^5이 되므로 우리는 4번째와 6번째 위치에서 error가 발생하였음을 알 수 있다. 따라서 $r(x) = x^3 + x^5$이므로 $c(x) = 0$이다. 3개의 error가

발생하였을 경우 수신 codeword가 $r(x) = 1 + x^5 + x^{15}$이라 가정하자. 이때, syndromes $s_1 = \alpha^{16}$, $s_5 = \alpha^2$, $s_7 = \alpha^{15}$이 되고, $v_b = 3$이므로 $F = \{x_3 + x_2 + x_1 + \alpha^{16}, x_3^5 + x_2^5 + x_1^5 + \alpha^2, x_3^7 + x_2^7 + x_1^7 + \alpha^{15}, x_1^{32} - x_1, x_2^{32} + x_2, x_3^{32} + x_3\}$이고, $g(x_1) = x_1 + \alpha^{16}x_1^2 + \alpha^{28}x_1 + \alpha^{20}$을 얻게 된다. $g(x_1) = 0$로부터 α^0, α^5, α^{15}의 3근을 얻게 되고 우리는 1번째, 6번째, 16번째에서 error가 발생하였음을 알게 된다.

4개의 error가 발생하였을 경우 수신 codeword가 $r(x) = 1 + x + x^2 + x^3$이라면 syndromes는 $s_1 = \alpha^{23}$, $s_5 = \alpha^6$, $s_7 = \alpha^4$이 되고, $\deg(g(x_1)) = 9 > 3$이 된다.

4. 결 론

본 논문에서는 Gröbner bases를 소개하고 이의 응용으로서 Chen에 의해 발견된 binary cyclic code의 효율적인 algebaric decoding method를 소개하였다. 이 방법은 true minimum distance까지 오류정정이 가능하며, non-binary cyclic code나 algebaric geometric code에도 확장 가능성이 있다. 또한 본 논문에서는 소개하지 않았지만 Gröbner bases는 integer programming 문제나 graph-coloring 문제 등을 해결하는데 사용될 수 있다. 특히 integer programming 문제는 knapsack 문제를 비롯한 암호분야에서 중요한 문제중의 하나이므로, 앞으로 Gröbner bases의 암호분야에서 응용은 커질 것으로 예상된다.

참 고 문 헌

[AdLou] W. Adams, D. Loustaunau, An introduction to Gröbner bases, Graduate studies in Mathematics, vol. 3, AMS, 1994.

[Bu65] B. Buchberger, Ein algorithmus zum auffinden der basiselemente des restklassenringe nach einem null-dimensionalen polynomideal, Ph. D. Thesis, Inst. University of Innsbruck, Innsbruck, Austria, 1965.

[Bu85] B. Buchberger, Gröbner bases: An algorithmic method in polynomial ideal theory, N. K. Bose, Ed. Dordrecht: Reidel, 184-232, 1985.

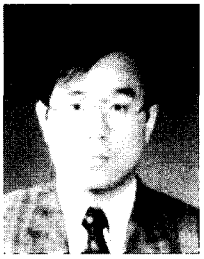
[Chen] X. Chen, I. S. Reed, T. Helleseth, T. K. Truong, Use of bases to decode binary cyclic codes up to the true minimum distance, IEEE Trans. Inform. Theory, vol. 40, 1654-1660, 1994.

[Chien] R. T. Chien, Cyclic decoding procedures for Bose-Chaudhuri-Hocquenghem codes, IEEE Trans. Inform. Theory, vol. IT-10, 357-363, 1964.

[CoTr] P. Conti, C. Traverso, Buchberger algorithm and integer programming, in Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes AAECC'9, Lecture Note in Comput. Sci., vol. 539, 130-139, 1991.

[Mac] F. J. MacWilliams, N. J. A.Sloane, The Theory of Error Correcting Codes, Amsterdam: North Holland, 1977.

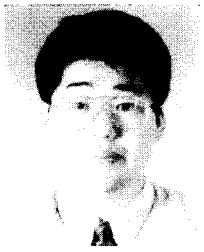
□ 著者紹介



임 종 인(정회원)

1980년 2월 고려대학교 수학과 학사
1982년 2월 고려대학교 대학원 수학과 석사
1986년 2월 고려대학교 대학원 수학과 이학박사
1986년 8월 - 현재 고려대학교 수학과 부교수

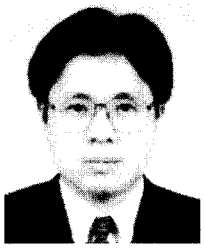
※ 주관심분야 : 응용 대수학 및 정수론, 암호론



서 창 호(학생회원)

1990년 2월 고려대학교 수학과 학사
1992년 8월 고려대학교 대학원 수학과 석사
1993년 - 현재 고려대학교 대학원 수학과 박사과정 수료

※ 주관심분야 : 응용 대수학 및 정수론, 암호론



박 대 연

1981년 2월 고려대학교 수학과 학사
1983년 2월 고려대학교 대학원 수학과 석사
1987년 2월 고려대학교 대학원 수학과 이학박사
1987년 3월 - 현재 전주대학교 수학교육학과 부교수

※ 주관심분야 : 이차 형식론 및 암호이론