다항최적화의 이론과 해법

서울대학교·산업공학과

홍성필, 박명주

2011 하계방학 최적화 공개 특강

8월 16 ∼ 18일

차례

- SDP 기초
- 대수 기초
- 다항최적화문제의 계층적 완화 방법의 원리
- 모멘트 수열과 행렬을 이용한 계층적 완화 방법
- 계층적 완화 방법의 수렴성
- 계층적 완화 방법의 성능(계산오차)

SDP 기초

차례

- SDP의 정의 ✓
  - SDP의 정의 ✓
  - SDP의 원-쌍대 문제 ✓

- 뿔 선형계획(cone LP)
  - 뿔 선형계획 ✓
  - 원-쌍대 뿔 선형계획 ✓
  - 2차뿔계획문제(SOCP)

- SDP의 다항시간성
  - 타원해법을 통한 분리문제와 최적화문제의 동등성
  - SDP의 다항성 ✓

- SDP의 응용 : 최대절단면문제 ✓

SDP의 정의

$$\begin{array}{ll} \inf & c^T x \\ \text{s.t.} & x_1 A_1 + x_2 A_2 + \cdots + x_m A_m \succeq B. \end{array} \tag{1}$$

- inf는 최소극한값을 취한다는 의미로 min의 일반화
- 모든 A_i, $B \in \mathbb{S}^n := n \times n$ 실수 대칭 행렬 집합.

▪ $A \in \mathbb{S}^n$가, 모든 벡터 $y \in \mathbb{R}^n$에 대해 $y^T A y \geqslant 0$을 만족하면, A를 PSD(positive semidefinite)라고 부르며, $A \succeq 0$ 으로 표기
- $A \succeq B$는 $A - B$가 PSD라는 의미. $\succeq$는 대칭행렬집합 위의 부분순서가 되며, *뢰브너(Löbner) 순서*라고 한다.

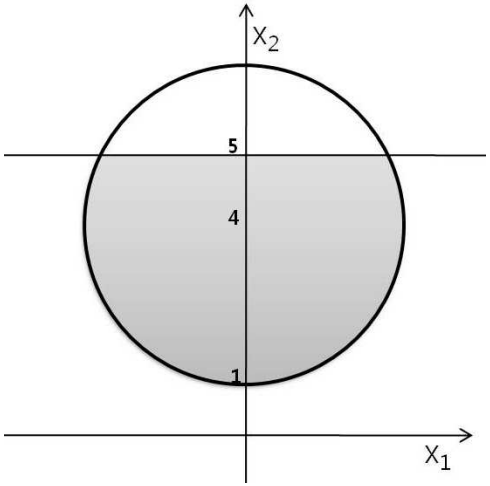
▪ **SDP 해집합** : 모든 $y \in \mathbb{R}^n$에 대해 $y^T(x_1 A_1 + x_2 A_2 + \cdots + x_m A_m - B)y \geqslant 0$을 만족하는 $x \in \mathbb{R}^m$ 집합의 교집합이기 때문에 닫힌 볼록집합이다.

- $x_1A_1 + x_2A_2 + \cdots + x_mA_m \succeq B$를 선형행렬부등식(LMI)이라고 부른다.

- 선형계획 부등호 제약식의 일반화. 선형계획의 해집합이 유한 개의 반공간(halfspace)의 교집합, 즉, 다면체라는 것에 비해, SDP 해집합은 무수한 반공간의 교집합이어서 곡면을 포함할 수 있다.

$$x_1 \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} + x_2 \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix} \succeq \begin{bmatrix} -3 & 4 & 0 \\ 4 & -3 & 0 \\ 0 & 0 & -5 \end{bmatrix}$$

$$\Leftrightarrow \; x_1^2 + (x_2 - 4)^2 \leqslant 9, \; x_2 \leqslant 5.$$



▪ 목적함수의 최소극한값(infimum)은 존재하여도 그 값을 갖는 해가 존재하지 않는 경우가 존재한다 :

$$\begin{array}{ll} \inf & x_1 \\ \text{s.t} & x_1 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} + x_2 \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \succeq 0. \end{array} \tag{2}$$

- 위 LMI 제약식은 다음의 부등식으로 주어진다 : $x_1 \geqslant 0,\ x_2 \geqslant 0,\ x_1 x_2 \geqslant 1.$
- 이때, x_1은 0값에 무한히 접근할 수 있지만 0보다는 항상 커야한다.

- 즉, SDP (2)의 <u>최적목적함수값은 0이지만 그 해는 존재하지 않는다</u>. (The infimum is not attained.)

▪ SDP를 다음과 같이 행렬을 변수로 하는 형태로 표현할 수 있다 :

$$\begin{array}{ll} \sup & B \cdot Y \\ \text{s.t.} & A_i \cdot Y = c_i, \quad i = 1, \cdots, m \\ & Y \succeq 0 \end{array} \tag{3}$$

- 변수 Y, 행렬 A_i, $B \in \mathbb{S}^n$,
- 연산 '$\cdot$'은 행렬의 내적, 즉 같은 위치의 원소들을 곱하여 모두 더한 값을 의미한다.

▪ 문제 (1)과 (3)은 형태는 다르지만, 본질적으로 같은 문제 : 한 문제를 다른 문제의 형태로 쉽게 변환할 수 있다. ((1)을 (3)으로 변환하기 위해서는 $x = x^+ - x^-,\ x^+ \geqslant 0,\ x^- \geqslant 0$, 로 치환, $Y := x_1^+ A_1 + \cdots + x_m^+ A_m - x_1^- A_1 - \cdots - x_m^- A_m - B,\ Y \succeq 0$ 으로 변환, 각 원소에 대한 행렬등식을 대각행렬의 내적으로 표현.)

SDP $\stackrel{?}{\in}$ NP

▪ 결정문제 '주어진 SDP가 가능해를 가지는가?'는 NP에 속하는가?

- NP란, 참일 때, 이를 효율적으로 확인할 수 있는 'certificate'이 존재하는 결정문제의 집합. 예를 들어, LP $\in$ NP인 이유는 가능해를 'certificate'으로 사용할 수 있기 때문.

- SDP에는 비선형성이 존재하기 때문에 가능해가 무리수일 수 있다.

$$\textbf{예: } \{(x_1, x_2) \mid x_1^2 + x_2^2 \leqslant 2, x_1^2 \geqslant 2\} = \{(\sqrt{2}, 0)\}.$$

- SDP가 유리수 가능해를 가진다 하더라도 그 입력크기가 문제의 입력크기의 지수함수가 될 수 있다. 따라서 가능해를 'certificate'으로 사용할 수 없음.

▪ 아직 NP에 속하는지 증명되지 않았음. 하지만, 뒤에 보겠지만, 절대오차 ϵ에 대해 ϵ-최적화가 다항시간에 가능.

SDP의 원-쌍대 문제

- 다음 문제를 원문제(Primal SDP, PSDP)로 부르자 :

$$\begin{array}{ll} \inf & c^T x \\ \text{s.t} & x_1 A_1 + x_2 A_2 + \cdots + x_m A_m \succeq B. \end{array}$$

- 이에 대하여 쌍대문제(Dual SDP, DSDP)를 다음과 같이 정의한다 :

$$\begin{array}{ll} \sup & B \cdot Y \\ \text{s.t} & A_i \cdot Y = c_i, \quad i = 1, \cdots, m \\ & Y \succeq 0 \end{array}$$

- 선형계획에 버금가는 쌍대성이 존재: 약쌍대성이 성립하고, 추가적인 조건이 성립하면 강쌍대성도 성립한다.

정리 1. *(약쌍대정리) x와 Y를 SDP의 원-쌍대 가능해 쌍이라고 하자. 그러면 $c^T x \geqslant B \cdot Y$가 성립한다.*

증명

$$
\begin{aligned}
& c^T x - B \cdot Y \\
= & x_1 A_1 \cdot Y + x_2 A_2 \cdot Y + \cdots + x_m A_m \cdot Y - B \cdot Y \\
= & (x_1 A_1 + x_2 A_2 + \cdots + x_m A_m - B) \cdot Y \geqslant 0
\end{aligned}
$$

x와 Y가 가능해이므로, 마지막 식은 한 쌍의 PSD 행렬의 내적. 그러나 두 *PSD행렬의 내적은 항상 0보다 같거나 크다*는 성질에 의해, 마지막 부등호 성립한다. □

▪ 어떤 조건이 성립하면 (PSDP)와 (DSDP)의 강쌍대성을 증명할 수 있다. 이는 분리초평면 정리로부터 유도한 파아카스 정리 사용하는 선형계획의 강쌍대성 증명과 유사.

분리초평면정리(Separation Hyperplane Theorem) $\Longrightarrow$
파아카스정리(Farkas Lemma) $\Longleftrightarrow$ 강쌍대성(Strong Duality)

정리 2. *(분리초평면정리) C를 $\mathbb{R}^n$의 닫힌 볼록 집합이라고 하자. 만약 z가 C에 속하지 않는 벡터라면, z와 C를 분리하는 초평면이 존재한다. 즉, C에 속한 모든 w에 대해 $w^T x \leqslant \beta$이고 동시에 $z^T x > \beta$인, 벡터 x와 실수 β가 존재한다.*

증명: 생략. □

정리 3. *(선형시스템의 파아카스정리)* $A \in \mathbb{R}^{m\times n}, c \in \mathbb{R}^n$*일 때,* $A^T y = c$*가 비음해* $y \geqslant 0$*을 가질 필요충분조건은* $Ax \geqslant 0$*을 만족하는 모든* x*에 대하여* $c^T x \geqslant 0$*이 성립하는 것이다.*

증명: $A^T y = c$가 비음해 $y \geqslant 0$를 가지지 않는다고 하자. 이는 c가 $C := \{A^T y : y \geqslant 0\}$에 속하지 않는다는 것과 동치이다. 따라서 분리초평면정리에 의하여 어떤 x와 β가 존재하여 모든 $y \geqslant 0$ 대하여 $(A^T y)^T x = y^T Ax \geqslant \beta$이고 동시에 $c^T x < \beta$이다. 그런데 C는 뿔(cone)이다. 즉, 모든 비음수의 곱에 대해 닫힌 집합이다. 따라서 β는 0으로 놓을 수 있다.

모든 $y \geqslant 0$에 대하여 $y^T Ax \geqslant 0$이 성립한다는 것은 $Ax \geqslant 0$과 동치이다. 따라서 $A^T y = c$가 비음해 $y \geqslant 0$를 가지지 않으면, $Ax \geqslant 0$와 $c^T x < 0$을 만족하는 어떤 x가 존재한다. 그리고 그 역도 성립함을 알 수 있다.

이는 바로 선형계획의 파아카스정리(의 대우)이다. □

- 파아카스 정리와 강쌍대정리의 동치관계를 직관적으로 살펴 보자. 예를 들어, 강쌍대정리가 파아카스 정리 중 충분조건 부분을 의미하는 것을 살펴보자.

선형계획문제 $\min\{c^T x | Ax \geqslant b\}$와 그 쌍대문제 $\max\{b^T y | A^T y = c, y \geqslant 0\}$을 생각하자. 파아카스 정리의 뒤의 조건에서 $Ax \geqslant 0$을 만족하는 x를 *제차해(homogeneous solution)*라고 부르는데, 원문제 가능해 집합의 하나의 (무한) 반직선에 해당한다. 따라서 만약 목적함수를 무한히 감소시킬 수 있다면, 반드시 목적함수 감소 방향 $-c$와 예각을 이루는 반직선 방향이 존재한다. 즉, $c^T x < 0$을 만족하는 제차해 x가 존재한다. 그러므로 파아카스 정리의 뒤의 조건은, 원문제가 가능한 경우, 유한한 최적해를 갖는다는 것을 의미한다. 이는, 쌍대정리에 의하여 쌍대문제가 가능해를 가진다는 의미이며, 파아카스 정리의 앞의 조건에 해당한다.

▪ 선형계획의 경우, 아무런 부가적인 조건의 가정이 없이, 분리초평면정리로부터, 강쌍대정리와 동치인 파아카스 정리를 얻을 수 있다. 이는 $C = \{A^T y : y \geqslant 0\}$가 다면체를 선형변환하여 얻은 집합이어서 분리초평면정리의 가정인 볼록성과 닫힘성을 만족하기 때문이다.

▪ SDP의 경우, 선형계획의 경우와 같이 해당 집합의 닫힘성을 항상 보장할 수 없기 때문에 부가적인 조건이 필요하다.

기본정리 1. *(슬레이터 조건) (PSDP) 제약식의 제차방정식이 내부해를 가진다고 하자. 즉, $\sum_{i=1}^m x_i A_i \succ 0$를 만족하는 x가 존재한다고 하자. 그러면 $C = \{(A_1 \cdot Y, A_2 \cdot Y, \cdots, A_m \cdot Y) : Y \succeq 0\}$는 닫힌 집합이 된다.*

증명: 생략. □

정리 4. *(SDP의 파아카스 정리) 기본정리 1의 가정이 성립하여* $C = \{(A_1 \cdot Y, A_2 \cdot Y, \cdots, A_m \cdot Y) : Y \succeq 0\}$*가 닫힌 집합이라고 하자. 그러면 (DSDP)의 제약식,* $A_i \cdot Y = c_i, i = 1, \cdots, m$*,* $Y \succeq 0$*의 가능해가 존재할 필요충분조건은* $\sum_{i=1}^{m} x_i A_i \succeq 0$*를 만족하는 모든* x*에 대하여* $c^T x \geqslant 0$*이 성립하는 것이다.*

증명 ($\Leftarrow$) 대우를 증명, $A_i \cdot Y = c_i, i = 1, \cdots, m$를 만족하는 $Y \succeq 0$가 존재하지 않는다고 하자. 이는 $c \notin C := \{(A_1 \cdot Y, A_2 \cdot Y, \cdots, A_m \cdot Y) : Y \succeq 0\}$을 의미.

가정에 의해, C는 닫힌 볼록집합이므로 c와 C를 분리하는 초평면이 존재한다 : 어떤 $x \in \mathbb{R}^m$가 존재하여 모든 $Y \succeq 0$에 대하여, $x^T(A_1 \cdot Y, A_2 \cdot Y, \cdot, A_m \cdot Y) = (\sum_{i=1}^{m} x_i A_i) \cdot Y \geqslant 0$이며 $c^T x < 0$이 성립. 이때, *어떤 행렬이 모든 PSD 행렬과의 내적이 비음이면 그 행렬은 PSD*이기 때문에, 어떤 $x \in \mathbb{R}^m$가 존재하여 $\sum_{i=1}^{m} x_i A_i \succeq 0$이며 $c^T x < 0$이 성립.

증명 (계속) ($\Rightarrow$) 어떤 x가 $\sum_{i=1}^{m} x_i A_i \succeq 0$를 만족한다고 하자 : 전제에 의하여 $A_i \cdot Y = c_i, i = 1, \cdots, m$를 만족하는 $Y \succeq 0$가 존재. 따라서 $c^T x = x_1 A_1 \cdot Y + \cdots + x_m A_m \cdot Y = (\sum_{i=1}^{m} x_i A_i) \cdot Y$. 또한 $\sum_{i=1}^{m} x_i A_i \succeq 0$와 $Y \succeq 0$이므로, 두 PSD 행렬의 내적은 항상 비음이라는 성질에 의하여 $c^T x \geqslant 0$. $\square$

SDP의 파아카스정리가 성립하면 그러면 이와 동치로서 다음의 강쌍대성이 성립한다:

정리 5. *(강쌍대정리 [Alizadeh,1995]) 앞의 슬레이터 조건이 성립한다고 하자. (PSDP)의 최소극한값을 p^*, (DSDP)의 최대극한값을 d^*라고 하면, 두 값은 일치한다 : $p^* = d^*$. 단, $\inf\ \emptyset = +\infty, \sup\ \emptyset = -\infty$라고 표기한다.*

증명 우선 슬레이터 조건은 원문제(PSDP)가 가능해를 갖는다는 것을 의미함. 따라서 $p^* = +\infty$인 경우는 배제되고 유한하거나, $-\infty$인 경우가 남는다.

$p^* = -\infty$인 경우. 이 경우, 약쌍대정리에 의해 쌍대문제인 (DSDP)가 가능해를 가질 수 없음. 이는 $d^* = -\infty$이며 따라서 정리는 참임. 역으로,

$d^* = -\infty$인 경우, 즉, 쌍대문제가 불가능일 때는 앞의 SDP의 파아카스 정리에 의하여 $\sum_{i=1}^{m} x_i A_i \succeq 0$를 만족하며 $c^T x < 0$인 어떤 x가 존재. 이는 원문제의 목적함수값을 무한히 감소시킬 수 있다는 의미이며, $p^* = -\infty$이 되고 정리가 성립.

p^*와 d^* 모두 유한한 경우. 약쌍대정리에 의하여, $p^* \geqslant d^*$. 이때, $p^* > d^*$라고 가정해보자. 이는 다음의 시스템이 불가능이라는 것을 의미 :

$$\begin{aligned} B \cdot Y &= p^* \\ A_i \cdot Y &= c_i, \quad i = 1, \cdots, m \\ Y &\succeq 0 \end{aligned}$$

여기에 파아카스정리를 적용하면, 어떤 실수 x_0와 벡터 $x = (x_1, \cdots, x_m)$가 존재하여, 다음을 만족한다 :

$$\begin{aligned} x_0 B + \textstyle\sum_{i=1}^{m} x_i A_i &\succeq 0 \\ p^* x_0 + c^T x &< 0 \end{aligned}$$

경우 1 : $x_0 = 0$. 앞에서와 같이 쌍대문제가 불가능이 되어 d^*가 유한하다는 가정에 맞지 않는다.

경우 2 :$x_0 > 0$. $y = (1/x_0)x$로 치환하여 $\sum_{i=1}^m y_i A_i \succeq -B,\ c^T y < -p^*$를 얻게 됨. 따라서 $c^T y < -p^* - \epsilon$인 어떤 $\epsilon > 0$을 잡을 수 있음.
한편 p^*가 원문제의 최소극한값이므로 $\sum_{i=1}^m z_i A_i \succeq B$이며 $c^T z < p^* + \epsilon$인 가능해 z가 존재한다. 따라서 $\sum_{i=1}^m (y_i + z_i) A_i \succeq 0,\ c^T(y+z) < 0$이 성립하여, 쌍대문제의 불가능성을 의미하게 되어 모순.

경우 3 : $x_0 < 0$. $y = (-1/x_0)x$로 치환하면, $\sum_{i=1}^m y_i A_i \succeq B,\ c^T y < p^*$를 얻게 됨. 이는 p^*가 원문제의 최소극한값이라는 것에 모순.

따라서 모든 경우에 모순이 생기며, 이것은 $p^* > d^*$의 전제가 거짓이라는 것을 의미. 따라서 $p^* \leqslant d^*$ 이며, 약쌍대정리, $p^* \geqslant d^*$와 결합하면 $p^* = d^*$이다.
□

▪ SDP도 선형계획과 마찬가지로 상보여유조건을 얻을 수 있다 :

$X = \sum_{i=1}^{m} x_i A_i - B$로 표기하면 $c^T x - B \cdot Y = X \cdot Y$. 따라서 한 쌍의 원-쌍대 가능해가 최적해일 필요충분조건은 $X \cdot Y = 0$이다. 이때 두 개의 PSD 행렬의 '내적이 0일 필요충분조건은 두 행렬 곱이 0'이기 때문에 다음과 같은 결과를 얻을 수 있다.

따름정리 1. *한 쌍의 원-쌍대 가능해가 최적해일 필요충분조건은 $XY = 0$이다.*

▪ 다음의 예를 통해 슬레이터 조건을 만족하지 않는 경우, 원-쌍대간격(duality gap)이 나타날 수 있음을 확인할 수 있다 :

$$\begin{array}{lll} & \inf & x_1 \\ \text{s.t} & x_1 \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} + x_2 \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & x_1 & 0 \\ x_1 & x_2 & 0 \\ 0 & 0 & x_1+1 \end{bmatrix} \succeq 0. \end{array}$$

$$\begin{array}{lll} & \sup & -y_{33} \\ \text{s.t} & y_{12}+y_{21}+y_{33}=1 \\ & y_{22}=0 \\ & Y \succeq 0. \end{array}$$

$$\underline{p^* = 0 > -1 = d^*}$$

뿔 선형계획(cone LP, conic programs)

▪ $A \in \mathbb{R}^{m\times n}$, $b \in \mathbb{R}^m$, 그리고 $K \subseteq \mathbb{R}^n$를 내부점을 가진 닫힌 볼록 뿔(closed convex cone)이라고 하자. 뿔 위에서 정의되는 선형시스템은 다음과 같이 정의한다 :

$$Ax = b,\ x \in K. \tag{4}$$

- 시스템 (4)는 선형시스템뿐만 아니라 SDP의 제약식을 포함한다.

$$a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 = b,\ x \in \text{ PSD 뿔}, \mathbb{S}^n_+.$$

$$\Leftrightarrow \begin{bmatrix} a_1 & \frac{a_2+a_3}{2} \\ \frac{a_2+a_3}{2} & a_4 \end{bmatrix} \cdot \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} = b, \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \succeq 0.$$

쌍대 뿔 (dual cone)

▪ 집합 K의 쌍대뿔(dual cone)을 다음과 같이 정의한다 :

$$K^* = \left\{ x \in \mathbb{R}^n \mid x^T y \geqslant 0,\ \forall y \in K \right\}.$$

- 이렇게 정의한 K^*는 K의 성질과 관계 없이 항상 닫힌 볼록 뿔.

- K가 내부점을 가지면 K^*는 뾰족뿔(pointed cone). 즉, $K^* \bigcap (-K^*) = \{0\}$.

정리 6. *(뿔 선형시스템의 파아카스 정리)* $A \in \mathbb{R}^{m\times n}, b \in \mathbb{R}^m$ 이고, $K(\subseteq \mathbb{R}^n)$, $A(K) = \{Ax \mid x \in K\}$가 모두 닫힌 볼록 뾰족뿔이라고 하자. 그러면 $Ax = b,\ x \in K$를 만족하는 $x \in \mathbb{R}^n$가 존재할 필요충분조건은 $A^T y \in K^*$를 만족하는 모든 y가 $b^T y \geqslant 0$를 만족하는 것이다.

증명 필요조건을 증명하자. $Ax = b,\ x \in K$를 만족하는 $x \in \mathbb{R}^n$가 존재한다고 하자. 그러면 $y \in \mathbb{R}^m$가 $A^T y \in K^*$를 만족하면 $b^T y = x^T(A^T y) \geqslant 0$이 성립.

역의 대우를 증명하기 위해, $Ax = b,\ x \in K$를 만족하는 $x \in \mathbb{R}^n$가 존재하지 않는다고 하자. 즉, $b \notin A(K)$ 이라고 하자. 가정에 의해 $A(K)$가 닫힌 볼록 뾰족뿔이기 때문에, 분리초평면정리에 의해서 다음과 같은 $y \in \mathbb{R}^m$ 가 존재한다 :

$$b^T y < 0,\ z^T y \geqslant 0,\ \forall z \in A(K).$$
$$\Rightarrow b^T y < 0,\ (Ax)^T y = x^T(A^T y) \geqslant 0,\ \forall x \in K.$$

따라서 $A^T y \in K^*$가 성립하여 증명이 끝난다. □

원-쌍대 뿔 선형계획

▪ K가 $\mathbb{R}^n$에서의 닫힌 볼록 뾰족 뿔라고 할 때 다음과 같은 뿔에서 정의되는 선형계획 문제와 그 쌍대문제를 고려한다.

$$\begin{array}{ll} \min & c^T x \\ \text{s.t.} & Ax = b, \\ & x \in K. \end{array} \qquad \begin{array}{ll} \max & b^T y \\ \text{s.t.} & A^T y + s = c, \\ & s \in K^*. \end{array}$$

- 뿔 K에 대해 $y - x \in K$를 $x \leqslant_K y$로 표기하면, 쌍대문제는 다음과 같이 다시 쓸 수 있다.

$$\begin{array}{ll} \max & b^T y \\ \text{s.t.} & A^T y \leqslant_{K^*} c. \end{array}$$

▪ 뿔 선형계획문제는 K가 모든 볼록 뿔을 포함하므로, 매우 광범위한 문제를 포함함 : 원리적으로는 모든 볼록계획문제가 이 형태로 변환가능하다.

정리 7. *(뿔에서 정의되는 선형계획의 약쌍대정리)* x*와* (y, s)*가 각각 뿔에서 정의되는 선형계획의 원문제와 쌍대문제의 가능해라면* $b^T y \leqslant c^T x$ *가 성립한다.*

증명 $c^T x - b^T y = c^T x - (Ax)^T y = x^T(c - A^T y) = x^T s \geqslant 0$. 마지막 부등식은 K와 K^*의 뿔 쌍대성으로부터 성립. □

▪뿔 선형계획의 강쌍대정리는 선형계획이나 SDP의 경우와 같이 정리 6, 즉, 뿔 선형시스템의 파아카스 정리를 사용하여 증명할 수 있다. $A(K)$가 닫혔다고 가정하자. 이러한 충분조건의 예는 뒤에서 보겠다.

정리 8. *(뿔에서 정의되는 선형계획의 강쌍대정리)* $A(K)$*가 닫혔다고 가정한다. 만약* z_p*및* z_d*가 뿔에서 정의되는 선형계획의 원문제와 쌍대문제의 최적 목적함수값이고 이들이 유한하다면* $z_p = z_d$ *이다.*

증명 약쌍대정리로부터 $z_p \geqslant z_d$. 모순법을 사용하여 $z_p \leqslant z_d$임을 증명하자. 즉, $z_p > z_d$를 가정하자. 그러면 시스템 $c^T x = z_d,\ \ Ax = b,\ x \in K$는 해가 존재하지 않는다. 따라서 파아카스 정리에 의해 (y_0, y)가 존재하여 다음 시스템의 해가 된다.

$$A^T y + cy_0 \in K^*,\ b^T y + z_d y_0 < 0.$$

이때, y_0의 부호에 따라 다음의 세 가지 경우로 나눌 수 있다.

경우 1 : $y_0 = 0$. $A^T y \in K^*, b^T y < 0$. 파아카스 정리로부터 $Ax = b,\ x \in K$인 해가 존재하지 않기 때문에 z_p가 유한값을 갖는다는 것에 모순.

경우 2 : $y_0 > 0$. y_0로 나누면 $c - A^T\left(-\frac{y}{y_0}\right) \in K^*,\ z_d - b^T\left(-\frac{y}{y_0}\right) < 0$이다. 이는 $-\frac{y}{y_0}$가 목적함수 값이 z_d보다 더 큰 쌍대가능해라는 의미가 되므로, z_d의 정의에 모순.

경우 3 : $y_0 < 0$. $-y_0$로 나누면 다음과 같은 관계를 얻는다.

$$A^T\left(\frac{y}{y_0}\right) \leqslant_{K^*} -c,\ b^T\left(\frac{y}{y_0}\right) > -z_d.$$

$\epsilon > 0$을 충분히 작은 양수라고 하면, 다음의 관계가 성립한다.

$$A^T\left(\frac{y}{y_0}\right) \leqslant_{K^*} -c,\ b^T\left(\frac{y}{y_0}\right) > -z_d + \epsilon. \tag{5}$$

또한 z_d의 정의에 따라 다음과 같은 쌍대 가능해 $\bar{y}$가 존재한다.

$$A^T\bar{y} \leqslant_{K^*} c,\ b^T\bar{y} > z_d - \epsilon. \tag{6}$$

$w := \bar{y} + \left(\frac{y}{y_0}\right)$로 정의하면, (5)와 (6)에 의하여 w가 다음과 같은 성질을 갖는 것을 알 수 있다.

$$A^T w \leqslant_{K^*} 0,\ b^T w > 0.$$

이는 w가 쌍대문제에서 목적함수를 무한히 증가시키는 가능방향이 되는 것을 의미하며 역시 가정에 모순이다. □

▪ 정리에서 $A(K)$가 닫혔다는 가정은 파아카스 정리에서 요구되는 가정이므로 강쌍대정리에도 필요하다. $A(K)$가 닫히기 위한 충분조건에는 다음의 조건들이 있다 :

- **조건 1** $\exists x : x >_K 0,\ Ax = b$. 즉, $x \in \text{int } K, Ax = b$인 x가 존재한다.
- **조건 2** $\exists y : A^T y >_{K^*} 0$. 즉, $A^T y \in \text{int } K^*$인 y가 존재한다.
- **조건 3** $\{(y, s) | A^T y + s = c,\ s \geqslant_{K^*} 0\}$가 유계(bounded)이다.

▪ 조건 1은 원문제의 슬레이터류의 조건, 조건 2는 쌍대문제의 슬레이터류의 조건이고, 조건 3은 쌍대문제의 가능영역 제한 조건이다.

▪ 뿔 선형계획 문제의 쌍대 문제를 정의하는 규칙을 정리하면 다음과 같다.

inf		sup	
변수	$\geqslant_K 0$ $\leqslant_K 0$ 부호제약 없음	$\leqslant_{K^*} 0$ $\geqslant_{K^*} 0$ $=$	제약조건
제약조건	$\leqslant_K 0$ $\leqslant_K 0$ $=$	$\leqslant_{K^*} 0$ $\geqslant_{K^*} 0$ 부호제약 없음	변수

$$\begin{array}{lll} \min & c^T x & \\ \text{s.t.} & Ax = b, & \\ & x \in K. & \end{array} \quad \Longleftrightarrow \quad \begin{array}{lll} \max & b^T y & \\ \text{s.t.} & A^T y + s = c, & \\ & s \in K^*. & \end{array}$$

▪ 다음 문제들은 K가 모두 자기쌍대성(self-duality)을 갖고 있는 문제들이다 :

- 선형계획 : $\min\ \{c^T x : Ax = b,\ x \geqslant 0\}$.

- 2차뿔계획문제 (SOCP, Second Order Cone Programming) :

$$\inf\ \{c^T x : Ax = b,\ x \in K^{n_1} \times K^{n_2} \times \cdots \times K^{n_m}\}.$$

$$\text{단, } K^{n_i} = \left\{ \begin{bmatrix} w \\ z \end{bmatrix} \in \mathbb{R} \times \mathbb{R}^{n_i - 1} : \|z\|_2 \leqslant w \right\}.$$

- SDP : $\sup\ \{B \cdot X : A_i \cdot X = c_i\ i = 1, \ldots, m,\ X \succeq 0\}$.

▪ 선형계획문제 $\subseteq$ 2차뿔계획문제 $\subseteq$ SDP 이며, 모두 효율적인 해법이 존재함.

2차뿔계획문제(SOCP)

▪ SOCP는 다음과 같은 형태로도 표현할 수 있다. $x \in \mathbb{R}^n$인 결정변수, $A_i \in \mathbb{R}^{n_i \times n}$, $F \in \mathbb{R}^{p \times n}$일 때,

$$\begin{array}{ll} \sup & f^T x \\ \text{s.t} & \|A_i^T x + b_i\|_2 \leqslant c_i^T x + d_i, \quad i = 1, \ldots, m \\ & Fx = g. \end{array}$$

- 앞서 살펴본 형태와 위 형태는 서로 쌍대관계에 있음을 쌍대 규칙에 따른 변환을 통해 확인할 수 있다.

▪ 다음과 같은 제약식을 2차뿔 제약식이라 한다 : $\|A^T x + b\|_2 \leqslant c^T x + d$.

▪ **강건 선형계획문제** : 일반적인 선형계획문제의 불확실성 및 변동성을 가진 계수 c, A_i, b_i에 대한 선형 부등식을 고려하는 문제.

- c와 b_i는 고정된 값을 갖고 A_i이 다음 타원 안에서 변동하는 경우, $(P_i \in \mathbb{R}^{n\times n})$

$$A_{i\cdot} \in \mathcal{U}_i = \{\bar{A}_{i\cdot} + P_i y \mid \|y\|_2 \leqslant 1\},$$

강건 선형계획문제를 이루는 A_i의 모든 가능한 값을 만족시키는 최적화 모형은 다음과 같다 :

$$\begin{aligned} \inf \quad & c^T x \\ \text{s.t} \quad & A_i x \leqslant b_i \quad \forall A_i \in \mathcal{U}_i \quad i = 1, \ldots, m \end{aligned}$$

- 위 제약식을 다시 표현하면,

$$
\begin{aligned}
& A_i x \leqslant b_i \quad \forall A_i \in \{\bar{A}_i + P_i y \mid \|y\|_2 \leqslant 1\} \\
\Rightarrow \quad & \sup \{(\bar{A}_i + y^T P_i^T)x : \|y\|_2 \leqslant 1\} \leqslant b_i \\
\Rightarrow \quad & \bar{A}_i x + \sup \{y^T P_i^T x : \|y\|_2 \leqslant 1\} \leqslant b_i \\
\Rightarrow \quad & \bar{A}_i x + \|P_i^T x\|_2 \leqslant b_i
\end{aligned}
$$

▪ 위 식은 SOCP임을 알 수 있으며, 따라서 위에서 정의한 강건 선형계획문제는 다음과 같은 2차뿔계획문제이다.

$$
\begin{aligned}
\inf \quad & c^T x \\
\text{s.t} \quad & \bar{A}_i x + \|P_i x\|_2 \leqslant b_i \quad i = 1, \ldots, m
\end{aligned}
$$

▪ **확률 제약식을 가진 선형계획** : i 번째 제약식 계수 벡터 A_i가 평균이 $\bar{A}_i$이고, 공분산 Σ_i를 가진 독립적인 정규분포 확률변수 벡터라고 가정하자. 각각의 제약식 $A_i^T x \leqslant b_i$는 어떤 지정된 값, η 이상을 가지는 확률로 다음과 같이 나타낼 수 있다 :

$$\Pr\left(A_i x \leqslant b_i\right) \geqslant \eta.$$

이러한 확률 제약식을 2차뿔계획 문제로 표현할 수 있다.

- 분산 σ^2을 가진 $u = A_i^T x$를 다음과 같이 치환하고, 위 제약식을 다시 쓰면,

$$\Pr\left(\frac{u-\bar{u}}{\sigma} \leqslant \frac{b_i-\bar{u}}{\sigma}\right) \geqslant \eta.$$

- $(u-\bar{u})/\sigma$는 평균이 0, 분산인 1인 정규분포를 따르므로, 위 식의 확률은 $\Phi((b_i-\bar{u})/\sigma)$와 같이 표현할 수 있다. ($\Phi$는 표준정규분포의 누적분포함수)

- 따라서 앞선 확률 제약식은 다음과 같이 표현할 수 있다.

$$\frac{b_i - \bar{u}}{\sigma} \geqslant \Phi^{-1}(\eta),$$

- $\bar{u} = \bar{A}_i x$와 $\sigma = (x^T \Sigma_i x)^{1/2}$로부터 다음 식을 얻을 수 있다.

$$\bar{A}_i x + \Phi^{-1}(\eta) \|\Sigma_i^{1/2} x\|_2 \leqslant b_i.$$

▪ 위 식은 2차뿔 제약식이므로, 확률 제약식을 2차뿔 제약식으로 바꿀 수 있음을 확인하였다.

볼록집합 위에서의 선형최적화

▪ SDP는 다항시간에 풀 수 있을까? :

- SDP의 분리문제(separation problem)는 다항시간에 풀 수 있음.

- 분리문제와 최적화문제(optimization problem)는 동등함 (via 타원해법)

⇒ SDP는 다항시간에 풀 수 있음.

▪ 예를 들어 살펴보자 : 우선 볼록집합 위에서의 선형최적화를 정의해보자.

$$\begin{aligned} \min \quad & c^T x \\ \text{s.t} \quad & x \in K. \end{aligned}$$

- K는 닫힌 볼록집합.

▪ **예 1**, 선형계획문제
- $x \in \mathbb{R}^n$이고 K가 m개의 반공간(halfspace), ${a_i}^T x \geqslant b_i \ (i = 1, \cdots, m)$으로 주어진 경우.

▪ **예 2**, 최대안정집합문제(stable set problem)
- 연결된 무향그래프 $G = (V, E)$가 주어졌을 때, 다음의 시스템을 만족하는 $x \in \mathbb{R}^{|V|}$의 집합, 유한다면체(polytope) P를 정의하자 :

$$x_u + x_v \leqslant 1, \forall (u, v) \in E$$

$$x_v \geqslant 0, \forall v \in V$$

x가 만일 P에 속하는 $0-1$ 벡터라면, $x_v = 1$을 만족하는 노드마디 v의 집합은, 그 안의 어떤 두개의 노드마디도 서로 이웃하지(adjacent) 않는다. 즉, G의 *안정집합(stable set)*이 된다. P의 $0-1$ 벡터들을 모두 포함하는 가장 작은 볼록집합을 K라고 하고, $c = [-1, -1, \cdots, -1]^T \in \mathbb{R}^{|V|}$로 정의하자. 그러면 이 문제는 최대안정집합문제가 된다.

▪ **예 3**, 최소비용 완전짝짓기문제(minimum cost perfect matching problem)

- 연결된 무향 그래프 $G = (V, E)$에서, 어떤 두 개의 호도 같은 노드마디를 공유하지 않는, 호들의 집합을 *짝짓기(matching)*라고 한다. 어떤 짝짓기가 모든 노드를 포함하면, 이를 *완전짝짓기(perfect matching)*이라고 한다. 각 호 e에 비용 $c_e \in E$가 주어졌을 때, 비용의 합이 최소가 되는 짝짓기를 구하는 문제를 *최소비용 완전짝짓기문제*라고 한다.

에드몬즈(Edmonds)는 완전짝짓기의 특성벡터 $x \in \mathbb{R}^{|E|}$들을 포함하는 최소 볼록다면체, K를 다음과 같은 선형 시스템으로 나타낼 수 있음을 증명 :

$$\sum_{e \in \delta(v)} x_e = 1, \forall v \in V,$$

$$\sum_{e \in \delta(S)} x_e \geqslant 1, \forall\ |S|\text{가 홀수인 } S \subseteq V,$$

$$x_e \geqslant 0, \forall e \in E.$$

이때, $\delta(S)$는 집합 S에 한 쪽 노드만이 포함되는 호의 집합을 의미. 따라서 이 문제는 최소비용 완전짝짓기문제가 된다.

▪ 예 4, SDP

- K가, 주어진 $A_i \in \mathbb{R}^{n\times n}$이 대칭행렬들에 대해, $x_1A_1 + x_2A_2 + \cdots + x_mA_m - B$가 PSD가 되도록 하는, $x \in \mathbb{R}^m$의 집합으로 정의되는 경우.

- 예 1, 선형계획은 다항시간 안에 풀 수 있음.

- 예 2, 최대안정집합문제는 NP-hard. 원리적으로는 K가 유한다면체이기 때문에 반공간들의 교집합으로 표시하면 선형계획문제가 된다. 하지만 그 개수가 지수적으로 많을 뿐 아니라 이를 효과적으로 다룰 수 있는 방법이없다.

- 예 3, 최소비용 완전짝짓기문제도 K를 표시하기 위해 필요한 반공간의 개수는 지수적으로 많다. 하지만 이 문제는 다항시간 안에 풀 수 있음.

- 예 4, SDP의 가능해 집합은 셀 수 없이 많은 반공간들의 교집합으로 주어지지만, 몇가지 부차적인 조건이 있다면 다항시간에 풀 수 있음.

$\longrightarrow$ 다항시간 내에 풀 수 있는 세 개의 예 1, 3, 4의 공통적인 특징은
K의 분리문제를 다항시간에 풀 수 있다는 것!

분리문제와 최적화문제

정의 1. (최적화문제) 임의의 유리수 벡터 $c \in \mathbb{Q}^n$에 대해, 다음을 만족하는 y를 구한다 : $c^T y \leqslant c^T x,\ \forall x \in K$.

정의 2. (분리문제) 임의의 유리수 벡터 $y \in \mathbb{Q}^n$가 주어졌을 때, y가 K에 속함을 보이거나, 그렇지 않은 경우, Y를 K로부터 분리하는 분리초평면을 구한다. 즉, 다음을 만족하는 c를 구한다 : $\|c\| \geqslant 1$이며 $c^T y < c^T x,\ \forall x \in K$.

- 앞의 분리초평면 정리에서의 정의 보다 더 약화된 것임을 알 수 있다.

- 1981년 그뢰첼, 로바즈, 슈라이버는 어떤 볼록집합의 분리문제를 다항시간에 풀 수 있는 경우, 그 위의 선형 최적화문제를 다항시간에 풀 수 있음을 증명하였음. $\Longrightarrow$ SDP도 분리문제를 다항시간에 풀 수 있기 때문에 최적화 역시 다항시간에 풀 수 있음.

"분리문제 = 최적화문제"

▪ 분리문제와 최적화문제의 동등함은 타원해법으로부터 비롯된다.

- 타원해법의 적용을 위해서는 매 반복 단계마다, 현재 해 x와 볼록집합 K사이의 분리문제만 해결하면 된다.

- 예를 들어, 선형계획법의 경우, 현재해가 가능하지 않을 때, 모든 제약식을 다 고려할 필요없이, 현재 해를 K로부터 분리하는 **분리초평면을 구하면**, 새로운 타원을 생성하여 다음 반복단계로 넘어 갈 수 있기 때문이다.

> 가능해 영역 K에 대한 분리문제를 다항시간에 풀 수 있다면,
> K를 정의하는 제약식들을 모두 명시적으로 알지 못해도
> 다항시간 안에 최적해를 구할 수 있다.

▪ 선형계획문제에 대한 두가지 타원 해법

1 쌍대정리를 이용하여 가능성 문제로 전환한 다음, 가능해를 찾도록 타원해법을 사용하는 방식.

2 목적함수를 함께 고려하여, 매 반복단계에서, i. 현재해가 가능해가 아닐 때는 현재해와 가능해집합을 분리하는 분리초평면을 사용하고, ii. 현재해가 가능해일 때는 목적함수가 현재해의 목적함수값과 같은 점들로 정의된 초평면을 사용하여, **목적함수가 감소하는 쪽으로 탐색 가능해 집합을 줄여 나가며** 최적화문제를 직접 푸는 방식.

▪ 쌍대정리를 이용할 수 없는 일반적인 선형최적화문제의 경우 2 방식을 사용할 수 있다.

▪ 타원해법 (스케치)

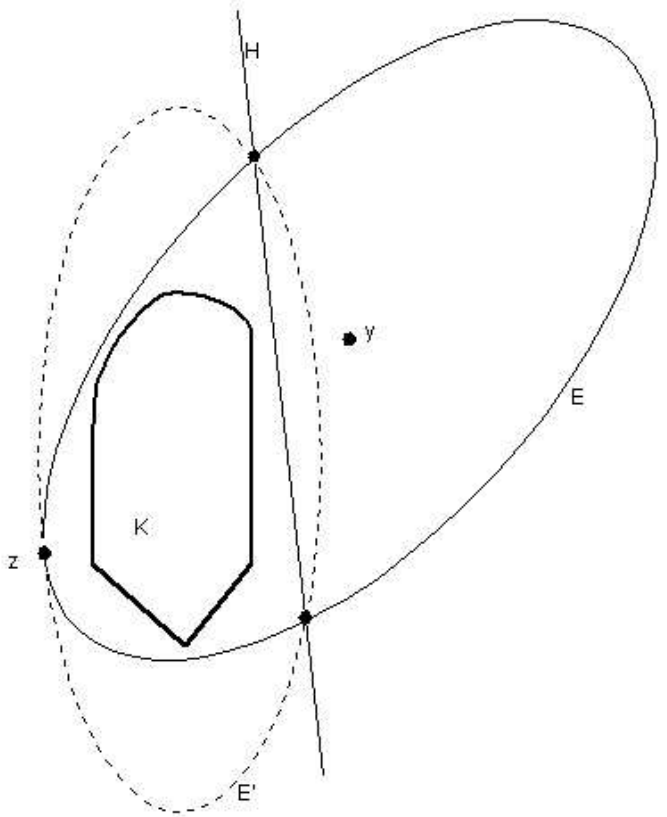
- 논의의 간편성을 위하여 무리수 때문에 발생하는 오차가 없으며, 분리문제도 풀 수 있다고 가정하고 타원해법의 한 반복단계를 설명한다 :

단계 0. 초기해를 $x_0 = a_0$, 초기타원을 $E_0 = B(x_0, R)$로 놓는다. 일반적으로 k번째 반복단계를 시작할 때, 다음과 같은 타원 E_k가 주어진다 : $k-1$번째 반복단계까지 구해진 어떤 가능해보다 목적함수 값이 같거나 작은 해들의 집합을 K_k라고 할 때, E_k는 K_k를 포함한다. E_k의 중심을 x_k라고 하자. k번째 반복단계는 다음과 같이 진행된다.

단계 1. $E = E_k$, 그리고 $y = x_k$라고 하자. 주어진 분리문제 알고리듬을 사용하여, y와 K의 분리문제를 푼다.

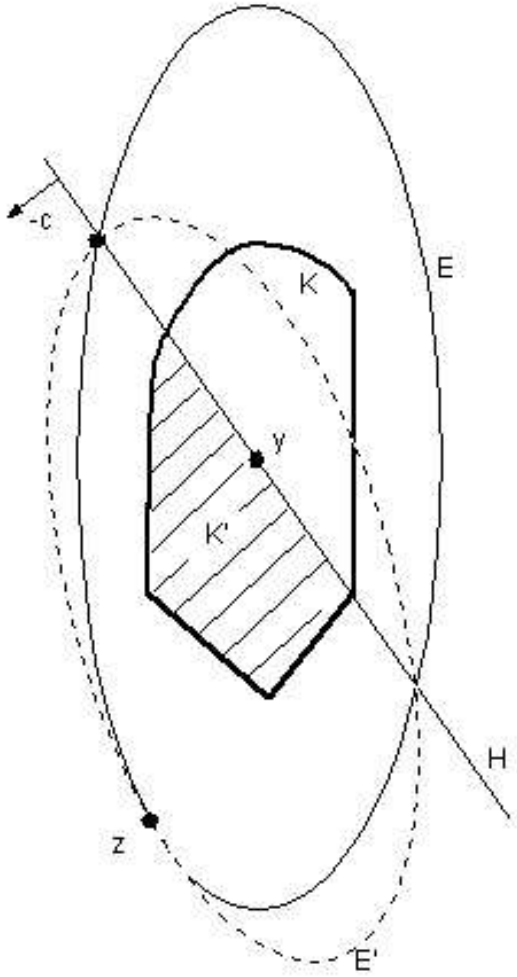
단계 2-1. y가 K에 속하지 않는 경우

이 경우, 분리문제 알고리듬으로부터 y를 K로부터 분리하는 초평면 H도 함께 주어질 것이다. 이 때, H와 평행한 분리초평면이 E와 접하는 점 z에서 E와 접하며, $E \cap H$에서 E와 교차하는 최소타원 E'를 구할 수 있다. (이 때, K에 대한 직접적인 정보가 필요 없음에 주목하자.) $E_{k+1} \longleftarrow E'$로 하고 k번째 반복단계가 끝난다.



단계 2-2. y가 K에 속하는 경우

이 경우에는 $c^T x = c^T y$로 정의되는 초평면을 H로 정의하고 첫째 경우와 동일한 방법으로 새로운 타원 E'을 구하여 E_{k+1}으로 놓는다.



SDP의 분리문제 : SDP의 최적화 문제의 다항시간성

▪ $\bar{x}$가 유리수일 때, SDP 분리문제를 다항시간에 풀 수 있음을 보이자.

- SDP의 분리문제 ('ϵ-분리문제')를 다항시간에 풀 수 있음을, 구체적인 예를 통하여 보이는 것으로 증명을 대신한다 :

예 1. SDP 제약식,

$$A(x) = x_1 \begin{bmatrix} 1 & -2 \\ -2 & 1 \end{bmatrix} + x_2 \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} -2 & 1 \\ 1 & 0 \end{bmatrix}$$
$$= \begin{bmatrix} x_1 + x_2 - 2 & -2x_1 + x_2 + 1 \\ -2x_1 + x_2 + 1 & x_1 + x_2 \end{bmatrix} \succeq 0$$

을 고려하자. 주어진 벡터, $\bar{x} = [3, 1]^T$과 $K = \{x : A(x) \succeq 0\}$로 정의된 분리문제를 풀어보자 : $\bar{x} \in K$인지, 즉, $A(\bar{x}) \succeq 0$인지를 밝히거나, 아니면 $c^T\bar{x} < c^Tx, \forall x \in K$인 c를 구한다.

- '대칭 가우스소거법'을 사용하면, 이 문제를 동시에 해결할 수 있다. $A(\bar{x}) \succeq 0$일 필요충분조건은, 행렬 $A(\bar{x})$에 가우스소거법을 적용할 때, 피봇 원소들이 모두 비음인 것이다. 그러면 행렬 $A(\bar{x})$는 다음과 같이 소거된다.

$$A(\bar{x}) \;=\; \begin{bmatrix} 2 & -4 \\ -4 & 4 \end{bmatrix} \longrightarrow \begin{bmatrix} 2 & -4 \\ 0 & -4 \end{bmatrix} \longrightarrow \begin{bmatrix} 2 & 0 \\ 0 & -4 \end{bmatrix}.$$

- 따라서 $\bar{x}$는 K에 속하지 않음을 알 수 있다. 그리고 위에 적용한 소거는 다음과 같이 기본행연산(elementary row operation)과 기본열연산에 대응되는 행렬을 $A(\bar{x})$의 좌우에 곱한 것과 같은 의미이다.

$$\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 2 & -4 \\ -4 & 4 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & -4 \end{bmatrix}.$$

따라서 다음의 관계가 성립한다.

$$\begin{bmatrix}0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 2 & 1\end{bmatrix}\begin{bmatrix}2 & -4\\ -4 & 4\end{bmatrix}\begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = -4$$

이것은 다음의 식이 K의 원소들에는 만족되지만, $\bar{x}$에는 만족되지 않는다는 의미이며, 따라서 분리초평면을 정의하게 되는 것이다.

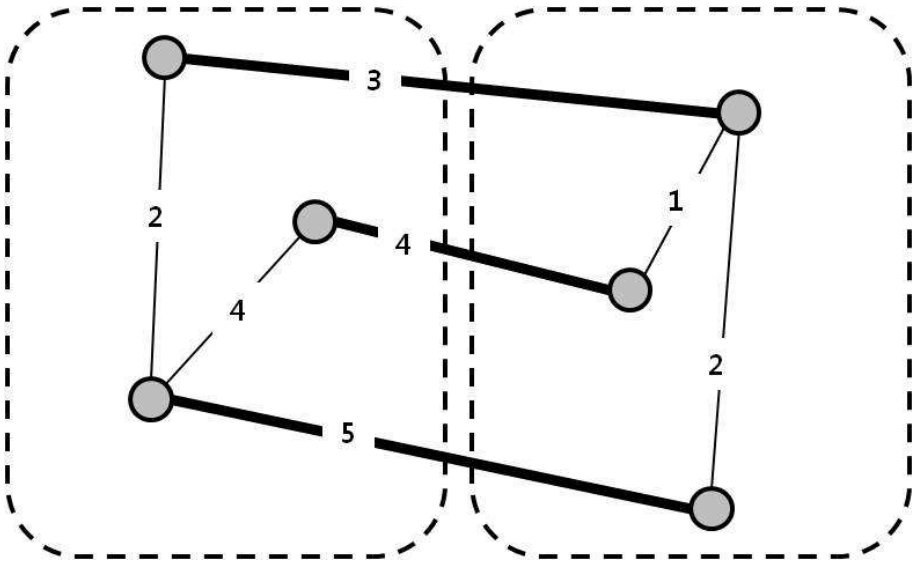
$$\begin{bmatrix}0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 2 & 1\end{bmatrix}\begin{bmatrix}x_1+x_2-2 & -2x_1+x_2+1\\ -2x_1+x_2+1 & x_1+x_2\end{bmatrix}\begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix}$$
$$= -3x_1+9x_2-4 \geqslant 0. \quad \square$$

SDP 응용 : 최대절단면문제

- Goemans와 Williamson의 최대절단면문제 근사해법연구는, 다른 접근법으로 달성할 수 있는 최대절단면문제의 최대 가능 근사값을, SDP를 사용하면 획기적으로 개선할 수 있다는 것을 보인 최초의 연구이다.

최대절단면문제

주어진 그래프 $G = (V, E)$, 호의 가중치를 $w_{ij}, (i, j) \in E$에 대해, 노드 마디집합을 양분했을 때 두 노드집합에 걸치는 호(edge)들의 집합을 *절단면(cut)*이라 한다. 최대절단면문제는 호의 가중치의 합이 최대가 되는 절단면을 구하는 문제.



▪ 최대절단면문제가 $0-1$ 2차함수계획법과 같은 문제임은 잘 알려진 사실이다. $V = V_1 \dot{\cup} V_2$로 양분할 때, $i \in V_1$이면 $x_i = -1$, $i \in V_2$이면 $x_i = 1$로 $x \in \mathbb{R}^{|V|}$를 정의하자. 이때, 최대절단면문제는 다음의 $-1, +1$ 2차함수계획법 문제와 같다 :

$$\begin{aligned} \max \quad & \tfrac{1}{2}\sum_{i<j} w_{ij}(1 - x_i x_j) \\ \text{s.t} \quad & x_i \in \{-1,\ 1\}\ \forall i \in V. \end{aligned}$$

▪ 근사해법의 첫번째 단계로, $-1, +1$ 2차함수계획법을 '벡터계획법'문제로 완화한다 :

- 각 1차 변수 x_j를 n-차원 단위 벡터, v_j로 대체하여 다음과 같은 문제를 정의한다. (S_n : n차원 구면)

$$\begin{aligned} \max \quad & \tfrac{1}{2}\sum_{i<j} w_{ij}(1 - \boldsymbol{v}_i^T \boldsymbol{v}_j) \\ \text{s.t} \quad & \boldsymbol{v}_i \in S_n \ \forall i \in V. \end{aligned}$$

- 최대절단면문제의 임의의 가능해 $\bar{x_j}$ $j \in V$가 주어졌을 때, $\bar{v_j} = (\bar{x_j}, 0, \cdots, 0)$ $j \in V$은 위 문제의 가능해가 되며, 두 해의 목적함수 값은 같음을 알 수 있다. 따라서 위 문제의 최적목적함수 값은 최대절단면문제의 상한이 됨을 알 수 있다.

$\Longrightarrow$ 이런 의미에서 위 문제는 최대절단면문제의 완화문제(relaxation)이다.

▪ 이 벡터계획문제는 효율적으로 풀 수 있는가?

- 다음과 같은 행렬들의 곱을 생각하자.

$$\begin{bmatrix} - - \boldsymbol{v}_1^T - - \\ - - \boldsymbol{v}_2^T - - \\ \vdots \\ - - \boldsymbol{v}_n^T - - \end{bmatrix} \begin{bmatrix} | & | & & | \\ \boldsymbol{v}_1 & \boldsymbol{v}_2 & \cdots & \boldsymbol{v}_n \\ | & | & & | \end{bmatrix} = \begin{bmatrix} \boldsymbol{v}_1^T\boldsymbol{v}_1 & \boldsymbol{v}_1^T\boldsymbol{v}_2 & \boldsymbol{v}_1^T\boldsymbol{v}_3 & \cdots & \boldsymbol{v}_1^T\boldsymbol{v}_n \\ \boldsymbol{v}_2^T\boldsymbol{v}_1 & \boldsymbol{v}_2^T\boldsymbol{v}_2 & \boldsymbol{v}_2^T\boldsymbol{v}_3 & \cdots & \boldsymbol{v}_2^T\boldsymbol{v}_n \\ \vdots & & & & \vdots \\ \boldsymbol{v}_n^T\boldsymbol{v}_1 & \boldsymbol{v}_n^T\ v_2 & \boldsymbol{v}_n^T\boldsymbol{v}_3 & \cdots & \boldsymbol{v}_n^T\boldsymbol{v}_n \end{bmatrix}.$$

- 이 때, $y_{ij} \equiv \boldsymbol{v}_i^T\boldsymbol{v}_j (= \boldsymbol{v}_i \cdot \boldsymbol{v}_j)$로 정의하면 얻어진 행렬,

$$Y \equiv \begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1n} \\ y_{21} & y_{22} & \cdots & y_{2n} \\ \vdots & & \ddots & \vdots \\ y_{n1} & y_{n2} & \cdots & y_{nn} \end{bmatrix}$$

은 PSD행렬이 된다.

- 따라서 위 벡터계획문제는 다음과 같은 SDP가 된다.

$$\begin{aligned} \max \quad & \tfrac{1}{2}\textstyle\sum_{i,j} w_{ij}(1-y_{ij}) \\ \text{s.t.} \quad & y_{ii} = 1 \ \forall i = 1, \cdots, n \\ & Y = (y_{ij}) \succeq 0. \end{aligned}$$

- PSD 행렬은 정방행렬의 곱으로 표시될 수 있으므로 , $Y = W^T W$로 쓸 수 있고, W의 각 행으로 정의된 벡터들은 벡터계획문제의 해가 된다.

- 이것은 벡터계획문제를 다항시간에 풀 수 있다는 의미이다.

- 이 완화 문제의 최적해는 원 문제의 근사 해를 구하는데 사용될 수 있는가?
- 다음과 같은 확률 알고리듬(randomized algorithm)을 생각해보자.

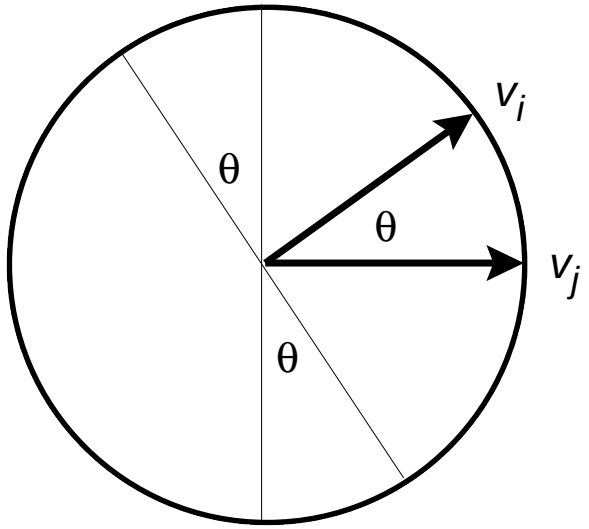
1. 최적해, $\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_n$를 구한다.
2. 단위 구면 S_n으로부터 균일한 확률로 벡터, $\boldsymbol{r}$을 무작위로 선택한다.
3. $\boldsymbol{r}$과 수직이고 원점을 지나는 초평면으로 $\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_n$를 두 그룹으로 나누고, 이에 따라 노드들을 양분하여 G의 절단면을 생성한다. 즉, 만약 $\boldsymbol{r}^T\boldsymbol{v}_i \geqslant 0$이면, $x_i \leftarrow 1$로 놓고, 그렇지 않으면, $x_i \leftarrow -1$로 놓는다.

정리 9. *위의 해법은 최대절단면문제의* 0.878*-근사해법이 된다.*

증명: 근사해법으로 얻어진 목적함수 값 $w(S)$의 기대값은 다음과 같이 주어진다.

$$\begin{aligned} E\left[w(S)\right] &= \sum_{i<j} w_{ij} \mathsf{Pr}\left[\boldsymbol{v}_i\text{와 } \boldsymbol{v}_j\text{가 } \boldsymbol{r}\text{과 수직인 초평면으로 나누어진다.}\right] \\ &= \sum_{i<j} w_{ij} \mathsf{Pr}\left[\mathsf{sgn}(\boldsymbol{r}^T\boldsymbol{v}_i) \neq \mathsf{sgn}(\boldsymbol{r}^T\boldsymbol{v}_j)\right] \end{aligned}$$

- 그러나 $\mathsf{sgn}(\boldsymbol{r}^T\boldsymbol{v}_i) \neq \mathsf{sgn}(\boldsymbol{r}^T\boldsymbol{v}_j)$일 필요충분조건은, $\boldsymbol{r}$을 $\boldsymbol{v}_i$와 $\boldsymbol{v}_j$로 생성되는 평면에 투영했을 때, 한 벡터와는 예각을 다른 벡터와는 둔각을 이루는 것이다.



- 이는 원주율 π 중에, $\boldsymbol{v}_i$와 $\boldsymbol{v}_j$의 사잇각의 두 배에 해당하는 부분에 $\boldsymbol{r}$이 투영될 확률과 같다. 따라서

$$\Pr[\boldsymbol{v}_i\text{와 }\boldsymbol{v}_j\text{가 }\boldsymbol{r}\text{과 수직인 초평면으로 나누어진다.}] = \frac{1}{\pi}\arccos(\boldsymbol{v}_i^T\boldsymbol{v}_j).$$

- 그러므로,

$$\begin{aligned} E[w(S)] &= \sum_{i<j} w_{ij}\frac{1}{\pi}\arccos(\boldsymbol{v}_i^T\boldsymbol{v}_j) \\ &\geqslant 0.878\cdot\frac{1}{2}\sum_{i<j} w_{ij}(1-\boldsymbol{v}_i^T\boldsymbol{v}_j) \quad \geqslant \ 0.878\times OPT.\ \square \end{aligned}$$

$*$ 첫 부등식은 다음과 같은 사실때문에 성립한다 :

$$\frac{1}{\pi}\arccos x \geqslant 0.878\cdot\frac{1}{2}(1-x) \ \ \forall\ -1<x<1.$$

참고 문헌

[1] F. Alizadeh, *Interior point methods in semidefinite programming with applications to combinatorial optimizations*, SIAM J. Optimization, 5(1):13-51, 1995.

[2] J. Edmonds, *Maximum matching and a polyhedron with 0-1 vertices*, J. Res. Nat. Bureau of Standards, 69B:125-130, 1965.

[3] M. X. Goemans and D. P. Williamson, *0.878-approximation algorithms for max-cut and max-2sat*, In proceedings of the 26th Annual ACM Symposium on the Theory of Computing, 422-433, 1994.

[4] M. X. Goemans and D. P. Williamson, *Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming*, Journal of ACM, 42:1115-1145, 1995.

[5] M. Grötschel, L. Lovász, and A. Schrijver, *The ellipsoid method and its consequences in combinatorial optimization*, Combinatorica, 1(2):169-197, 1981.

대수 기초

차례

- 다항식
- 아이디얼과 다양체
- 항순서와 나누기 알고리듬
- Gröbner 기저
- Quotient algebra $\mathbb{R}[x]/\boldsymbol{I}$

다항식(Polynomials)

- 단항(monomials): 미지수 $x_1, \ldots, x_n$의 거듭제곱, $x_1^{\alpha_1} \cdots x_n^{\alpha_n} (=: x^\alpha)$.
- 항(terms): 단항 x^α에 0이 아닌 실수 p_α를 곱한 것, $p_\alpha x^\alpha$.
- 다항식(polynomials): 유한 개의 항을 더한 식, $p(x) = \sum_\alpha p_\alpha x^\alpha$.
- $\mathbb{R}[x_1, \ldots, x_n]$ 또는 $\mathbb{R}[x]$: 미지수가 n개이고 계수가 실수인 다항식의 집합.
- 단항 x^α의 차수: $|\alpha| := \sum_{i=1}^n \alpha_i$.
- 항 $p_\alpha x^\alpha$의 차수: x^α의 차수.
- 다항식 $p(x)$의 차수: $p(x)$의 항의 차수 중에서 가장 큰 값, $\deg(p)$.

- $\mathbb{R}[x]_t$: 차수가 t 이하인 실수 다항식의 집합.

- 단항 x^α의 종류는 지수벡터 α에 의해 결정. 차수가 t 이하인 단항의 집합은 다음 집합 $\mathbb{N}^n_t$과 동치.

$$\mathbb{N}^n_t := \{\alpha \in \mathbb{N}^n | \sum_{i=1}^{n} \alpha_i \leqslant t\}$$

참고 1. $|\mathbb{N}^n_t| = \binom{n+t}{t}$임이 알려져 있음.

다항식의 해 구하기

원문제 해집합 유지 **변형된 문제**

$$\begin{array}{c} h_1(x) = 0 \\ \vdots \\ h_m(x) = 0 \end{array} \quad \Rightarrow \quad \begin{array}{c} h_1'(x) = 0 \\ \vdots \\ h_l'(x) = 0 \end{array}$$

예 2. 가우스 소거법

원문제 **변형된 문제**

$$\begin{array}{rcrcrcr} 2x_1 & + & x_2 & + & x_3 & = & 5 \\ 4x_1 & - & 6x_2 & & & = & -2 \\ -2x_1 & + & 7x_2 & + & 2x_3 & = & 9 \end{array} \quad \Rightarrow \quad \begin{array}{rcrcrcr} 2x_1 & + & x_2 & + & x_3 & = & 5 \\ & - & 8x_2 & - & 2x_3 & = & -12 \\ & & & & x_3 & = & 2 \end{array}$$

다항식의 아이디얼(Ideal)과 다양체(Variety)

아이디얼(ideal) I: 임의의 환(ring) R의 부분집합으로

i) 덧셈에 대해 닫혀 있고,

ii) $\forall f \in \boldsymbol{I}$와 $\forall h \in R$에 대해 $fh \in \boldsymbol{I}$.

다항식 $h_1, \ldots, h_m \in \mathbb{R}[x]$에 의해 생성된 아이디얼을 $\langle h_1, \ldots, h_m \rangle$로 표기.

$$\langle h_1, \ldots, h_m \rangle := \{\sum_{j=1}^{m} u_j(x) h_j(x) | u_1(x), \ldots, u_m(x) \in \mathbb{R}[x]\}.$$

이때 $\boldsymbol{I} = \langle h_1, \ldots, h_m \rangle$가 $\mathbb{R}[x]$에 속한 아이디얼인 것은 쉽게 확인할 수 있다. 그리고 $\{h_1, \ldots, h_m\}$을 아이디얼 $\boldsymbol{I}$의 기저(basis)라 부른다.

$A \subseteq \mathbb{R}[x]$에 대해, 다음을 각각 A의 복소수 다양체, 실수 다양체라 부르자.

$$V_{\mathbb{C}}(A) := \{x \in \mathbb{C}^n | f(x) = 0,\ \forall f \in A\}, \quad V_{\mathbb{R}}(A) = V_{\mathbb{C}}(A) \cap \mathbb{R}^n.$$

그러면 $V_{\mathbb{C}}(\{h_1, \ldots, h_m\}) = V_{\mathbb{C}}(\langle h_1, \ldots, h_m \rangle)$. 그래서 $\langle h_1, \ldots, h_m \rangle$의 기저 중 해를 구하기 쉬운 형태를 찾아야 한다.

예 3. $\boldsymbol{I} = \langle x^6 - 1, x^4 - 1 \rangle$인 경우 $\boldsymbol{I} = \langle x^2 - 1 \rangle$이므로 $V_{\mathbb{C}}(\boldsymbol{I}) = \{-1, 1\}$.

성질 1. *$\boldsymbol{I}$가 미지수가 1개인 실수 다항식의 아이디얼이면 $\boldsymbol{I} = \langle f \rangle$.*

증명: f를 $\boldsymbol{I}$에 속한 다항식 중 차수가 최소인 다항식이라 하자. 그러면 $\boldsymbol{I} \supseteq \langle f \rangle$는 자명.
이제 $\boldsymbol{I}$에 속한 임의의 다항식 g가 $g = qf$임을 보이자. g를 f로 나눈 결과를 $g = qf + r$라 하자. 이때 $r \neq 0$이면 $\deg(r) < \deg(f)$이다. 그런데 $\boldsymbol{I}$가 아이디얼이므로 $r = g - qf \in \boldsymbol{I}$이다. 이것은 f의 정의에 모순. □

정의 3. 미지수가 1개인 실수 다항식 f와 g의 $\mathrm{GCD}(f,g)$ 다항식:

- $\mathrm{GCD}(f,g)$는 f와 g를 나눈다.
- p가 f와 g를 나누면 p는 $\mathrm{GCD}(f,g)$를 나눈다.

성질 2. *미지수가 1개인 실수 다항식 f와 g에 대해 $\langle f,g\rangle = \langle \mathrm{GCD}(f,g)\rangle$.*

증명: 성질 1에 의해 $\langle f,g\rangle = \langle h\rangle$인 다항식 h가 존재한다. $h = \mathrm{GCD}(f,g)$임을 보이자. 일단 $f,g \in \langle h\rangle$이므로 h는 f와 g를 나눈다. p가 f와 g를 나눈다고 하자. 즉, $f = Ap$, $g = Bp$라 하자. $h \in \langle f,g\rangle$이므로 $h = Cf + Dg$로 쓸 수 있다.

$$h = Cf + Dg = (AC + BD)p$$

이므로 p는 h를 나눈다. 그래서 $h = \mathrm{GCD}(f,g)$이다. □

힐버트(Hilbert)의 결과들

(힐버트 기저 정리) $\mathbb{R}[x]$는 다음 두 가지를 만족한다.

(i) $\boldsymbol{I}$가 $\mathbb{R}[x]$의 아이디얼이면 $\boldsymbol{I}$를 생성하는 다항식 $h_1, \ldots, h_m \in \mathbb{R}[x]$이 존재한다. 즉, $\boldsymbol{I} = \langle h_1, \ldots, h_m \rangle$이다.

(ii) $\boldsymbol{I}_1 \subseteq \boldsymbol{I}_2 \subseteq \cdots \subseteq \boldsymbol{I}_n \subseteq \cdots$가 $R[x]$에 속한 아이디얼의 오름사슬(ascending chain)이면 $\boldsymbol{I}_N = \boldsymbol{I}_{N+1} = \boldsymbol{I}_{N+2} = \cdots$를 만족시키는 N이 존재한다.

(힐버트의 weak Nullstellensatz) $\boldsymbol{I} \subseteq \mathbb{R}[x]$에 대하여

$$\boldsymbol{I} = \mathbb{R}[x] \;\Leftrightarrow\; 1 \in \boldsymbol{I} \;\Leftrightarrow\; V_{\mathbb{C}}(\boldsymbol{I}) = \emptyset.$$

주어진 $V \subseteq \mathbb{C}^n$에 대하여 다음을 V의 소멸(vanishing) 아이디얼이라 한다.

$$\boldsymbol{I}(V) := \{f \in \mathbb{R}[x] | f(v) = 0, \forall v \in V\}$$

그리고 다음을 $\boldsymbol{I}$의 래디칼(radical)이라 하고,

$$\sqrt{\boldsymbol{I}} := \{f(x) \in \mathbb{R}[x] | f(x)^k \in \boldsymbol{I}, \exists k \in \mathbb{N}_+\}$$

$\boldsymbol{I}(V), \sqrt{\boldsymbol{I}}$는 $\mathbb{R}[x]$에서 아이디얼이 됨을 쉽게 보일 수 있다. 그리고 주어진 $\boldsymbol{I} \subseteq \mathbb{R}[x]$에 대하여 $\boldsymbol{I} \subseteq \sqrt{\boldsymbol{I}} \subseteq \boldsymbol{I}(V_{\mathbb{C}}(\boldsymbol{I}))$이 성립한다.

(힐버트의 strong Nullstellensatz) $\sqrt{\boldsymbol{I}} = \boldsymbol{I}(V_{\mathbb{C}}(\boldsymbol{I}))$.

$\boldsymbol{I} = \sqrt{\boldsymbol{I}}$이면 $\boldsymbol{I}$를 래디칼이라 부른다.

항순서(Term order)

단항순서(monomial order): 단항의 집합 $\mathbb{T}^n = \{x^\alpha | \alpha \in \mathbb{N}^n\}$에 대한 전순서(total order)로 다음의 두 조건을 만족하는 것이다.

(i) 1이 아닌 모든 단항 x^β는 $1 \prec x^\beta$이고,

(ii) $x^\alpha \prec x^\beta$이면 모든 $x^\gamma \in \mathbb{T}^n$에 대해 $x^{\alpha+\gamma} \prec x^{\beta+\gamma}$이다.

단항순서가 정의되면 항순서(term order)는 다음과 같이 정의된다: 영이 아닌 실수 a, b에 대해서 $x^\alpha \prec x^\beta$이면 $ax^\alpha \prec bx^\beta$이다.

임의의 $\alpha, \beta \in \mathbb{N}^n$에 대하여

- $x_1 \succ x_2 \succ \cdots \succ x_n$인 사전편찬식순서(lexicographic order):

$$x^\alpha \prec x^\beta \Leftrightarrow \alpha_i \neq \beta_i\text{인 좌표 중 가장 왼쪽의 좌표에서 } \alpha_i < \beta_i.$$

- $x_1 \succ x_2 \succ \cdots \succ x_n$인 차수사전편찬식순서(graded lexicographic order):

$$x^\alpha \prec x^\beta \Leftrightarrow \begin{cases} |\alpha| < |\beta| \text{ 이거나} \\ |\alpha| = |\beta|\text{일 때는 사전편찬식순서에 의해 } x^\alpha \prec x^\beta. \end{cases}$$

- $x_1 \succ x_2 \succ \cdots \succ x_n$인 차수역사전편찬식순서(graded reverse lexicographic order):

$$x^\alpha \prec x^\beta \Leftrightarrow \begin{cases} |\alpha| < |\beta| \text{ 이거나} \\ |\alpha| = |\beta|\text{일 때는 } \alpha_i \neq \beta_i\text{인 좌표 중} \\ \text{가장 오른쪽의 좌표에서 } \alpha_i > \beta_i. \end{cases}$$

$x_1 \succ x_2 \succ x_3$일 때 각 단항순서에 따라 $x_1^2x_2x_3$와 $x_1x_2^3$의 순서를 구해보자.

- 사전편찬식순서: $x_1^2x_2x_3 \succ x_1x_2^3$.
- 차수사전편찬식순서: $x_1^2x_2x_3 \succ x_1x_2^3$.
- 차수역사전편찬식순서: $x_1^2x_2x_3 \prec x_1x_2^3$.

차수사전편찬식순서와 차수역사전편찬식순서와 같이 차수가 큰 단항의 순서가 큰 단항순서를 total degree 단항순서라 부른다.

성질 3. *x^α가 x^β를 나누면, 즉 모든 $i = 1, \ldots, n$에 대해 $\alpha_i \leqslant \beta_i$이면 $\mathbb{T}^n$에서 정의된 임의의 단항순서에서 $x^\alpha \preceq x^\beta$이다.*

증명: 모든 $i = 1, \ldots, n$에 대해 $\gamma_i = \beta_i - \alpha_i$라 하자. 즉, $x^\beta = x^\alpha x^\gamma$. 단항순서의 첫 번째 조건에 의해 $x^\gamma \succeq 1$이고, 두 번째 조건에 의해 $x^\beta = x^\alpha x^\gamma \succeq x^\alpha$이다. □

정리 10. *$\mathbb{T}^n$에서 정의된 임의의 단항순서는 정렬순서(well-ordering)이다. 즉, $\mathbb{T}^n$의 모든 부분집합 A에 대해 최소원소 $x^\alpha \in A$가 항상 존재한다. 여기서 최소원소란 모든 $x^\beta \in A$에 대해 $x^\alpha \preceq x^\beta$를 만족하는 A의 원소이다.*

증명: 만약 주어진 단항순서가 정렬순서가 아니라고 하자. 그러면 다음을 만족시키는 $\mathbb{T}^n$의 부분집합 A가 존재한다: $i = 1, 2, \ldots$에 대해 $x^{\alpha^i} \in A$이고

$$x^{\alpha^1} \succ x^{\alpha^2} \succ x^{\alpha^3} \succ \cdots. \tag{7}$$

이것을 이용하여 다음의 오름사슬 아이디얼을 정의하자.

$$\langle x^{\alpha^1} \rangle \subseteq \langle x^{\alpha^1}, x^{\alpha^2} \rangle \subseteq \langle x^{\alpha^1}, x^{\alpha^2}, x^{\alpha^3} \rangle \subseteq \cdots. \tag{8}$$

그런데 $i = 1, 2, \ldots$에 대해 $\langle x^{\alpha^1}, \ldots, x^{\alpha^i} \rangle \neq \langle x^{\alpha^1}, \ldots, x^{\alpha^{i+1}} \rangle$이 성립한다. 만약 등식이 성립한다면

$$x^{\alpha^{i+1}} = \sum_{j=1}^{i} u_j x^{\alpha^j} \tag{9}$$

을 만족시키는 다항식 $u_j \in \mathbb{R}[x]$가 존재한다. 식 (9)의 우변의 각 항은 어떤 x^{α^j}에 의해 나뉜다. 그래서 $x^{\alpha^{i+1}}$도 우변의 항 중 하나이므로 어떤 x^{α^j}에 의해 나뉜다. 앞의 성질에 의해 $x^{\alpha^{i+1}} \succeq x^{\alpha^j}$이다. 이것은 식 (7)에 모순이다. 따라서 (8)은 오름사슬조건을 만족하지 않는다. 이것은 힐버트 기저 정리에 모순되므로 주어진 단항순서는 정렬순서이다. □

다항식 $f(x) = \sum_\alpha f_\alpha x^\alpha$에서 순서가 가장 큰 항을 선두항(leading term)이라 부르고 $\mathrm{lt}(f)$로 표기한다. 선두항의 계수를 $\mathrm{lc}(f)$, 선두단항을 $\mathrm{lp}(f)$로 표기한다. 즉, $\mathrm{lt}(f) = \mathrm{lc}(f)\mathrm{lp}(f)$. 그리고

$$\begin{aligned} f &= \mathrm{lt}(f) + \textstyle\sum_i X_i,\ X_i \prec \mathrm{lt}(f) \\ g &= \mathrm{lt}(g) + \textstyle\sum_j Y_j,\ Y_j \prec \mathrm{lt}(g) \\ fg &= \mathrm{lt}(f)\mathrm{lt}(g) + \mathrm{lt}(f)\textstyle\sum_j Y_j + \mathrm{lt}(g)\sum_i X_i + \sum_i X_i \sum_j Y_j \end{aligned}$$

그래서 $\mathrm{lt}(fg) = \mathrm{lt}(f)\mathrm{lt}(g)$, $\mathrm{lp}(fg) = \mathrm{lp}(f)\mathrm{lp}(g)$, $\mathrm{lc}(fg) = \mathrm{lc}(f)\mathrm{lc}(g)$가 성립.

나누기 알고리듬

이제 단항순서를 고정하자.

알고리듬 1. *나누기 알고리듬*
입력: *실수 다항식 f와 0이 아닌 실수 다항식 $h_1, \ldots, h_s$.*
출력: *다음이 성립하는 f의 분해 $f = \sum_{i=1}^{s} u_i h_i + r$:*

(i) $\mathrm{lt}(f) = \max(\max_{1 \leqslant i \leqslant s} \mathrm{lt}(u_i h_i), \mathrm{lt}(r))$ *이고,*

(ii) *r의 모든 항은 어떤* $\mathrm{lt}(h_i)$*에도 나누어지지 않는다.*

초기화: $u_1 = \cdots = u_s = 0, r = 0, g = f.$

주반복단계: $g \neq 0$*이면 다음을 반복;*

$\mathrm{lt}(h_i)$중 $\mathrm{lt}(g)$를 나눌 수 있는 i가 있으면 가장 작은 i를 고른 후 다음을 시행한다:

$$u_i := u_i + \frac{\mathrm{lt}(g)}{\mathrm{lt}(h_i)},\ g := g - \frac{\mathrm{lt}(g)}{\mathrm{lt}(h_i)} h_i.$$

그런 h_i가 없으면 다음을 시행한다:

$$r := r + \mathrm{lt}(g),\ g := g - \mathrm{lt}(g).$$

그래서 단항순서가 total degree 단항순서의 경우에는 $\deg(f) = \max(\max_{1 \leqslant i \leqslant s} \deg(u_i h_i), \deg(r))$가 성립한다.

나누기 알고리듬은 유한 번 안에 종료된다. 만약 그렇지 않다고 하자. 그리고 i번째 반복 단계의 g를 g^i라 하자. 그러면

$$\mathrm{lt}(g^1) \succ \mathrm{lt}(g^2) \succ \cdots \succ \mathrm{lt}(g^i) \succ \cdots$$

가 성립하여 고정한 단항순서가 정렬순서라는 것에 모순된다. 그리고 나머지

알고리듬의 출력이 (i), (ii)를 만족한다는 것은 쉽게 확인할 수 있다.

예 4. $x \succ y$인 차수사전편찬식순서를 사용하여 $f = x^2y + xy^2 + y^2$을 $h_1 = xy - 1, h_2 = y^2 - 1$로 나누어 보자.

초기화: $u_1 = u_2 = 0, r = 0, g = x^2y + xy^2 + y^2$.

첫 번째 반복단계: $\mathrm{lt}(h_1) = xy$가 $\mathrm{lt}(g) = x^2y$를 나눌 수 있으므로

$$u_1 = u_1 + \frac{x^2y}{xy} = x, \ g = g - \frac{x^2y}{xy}h_1 = xy^2 + y^2 + x.$$

두 번째 반복단계: $\mathrm{lt}(h_1) = xy$가 $\mathrm{lt}(g) = xy^2$을 나눌 수 있으므로

$$u_1 = u_1 + \frac{xy^2}{xy} = x + y, \ g = g - \frac{xy^2}{xy}h_1 = y^2 + x + y.$$

세 번째 반복단계: $\mathrm{lt}(h_2) = y^2$이 $\mathrm{lt}(g) = y^2$을 나눌 수 있으므로

$$u_2 = u_2 + \frac{y^2}{y^2} = 1,\ g = g - h_2 = x + y + 1.$$

네 번째 반복단계: $\mathrm{lt}(h_1) = xy$, $\mathrm{lt}(h_2) = y^2$ 모두 $\mathrm{lt}(g) = x$를 나눌 수 없으므로

$$r = r + \mathrm{lt}(g) = x,\ g = g - \mathrm{lt}(g) = y + 1.$$

다섯 번째 반복단계: $\mathrm{lt}(h_1) = xy$, $\mathrm{lt}(h_2) = y^2$ 모두 $\mathrm{lt}(g) = y$를 나눌 수 없으므로

$$r = r + \mathrm{lt}(g) = x + y,\ g = g - \mathrm{lt}(g) = 1.$$

여섯 번째 반복단계: $\mathrm{lt}(h_1) = xy$, $\mathrm{lt}(h_2) = y^2$ 모두 $\mathrm{lt}(g) = 1$를 나눌 수 없으므로

$$r = r + \mathrm{lt}(g) = x + y + 1,\ g = g - \mathrm{lt}(g) = 0.$$

반복단계 종료: $f = u_1h_1 + u_2h_2 + r = (x+y)h_1 + h_2 + x + y + 1.$

참고로 위 예에서 h_1과 h_2의 순서를 바꿔서 적용하면 $f = xh_1 + (x+1)h_2 + 2x + 1$이 되어 f를 h_1과 h_2로 나눈 나머지는 유일하지 않다.

Gröbner 기저

정의 4. 아이디얼 $\boldsymbol{I}$에 포함된 다항식의 집합 $G = \{g_1, \ldots, g_t\}$가 다음을 만족하면 $\boldsymbol{I}$의 Gröbner 기저라고 한다; $\boldsymbol{I}$에 속한 0이 아닌 다항식 f의 선두항 $\mathrm{lt}(f)$는 $\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t)$ 중 하나로 나누어진다.

예 5. $\boldsymbol{I} = \langle xy - 1, y^2 - 1\rangle$에 $x \succ y$인 차수사전편찬식순서를 적용한 경우 $\{xy - 1, y^2 - 1\}$은 $\boldsymbol{I}$의 Gröbner 기저가 아니다. 왜냐하면

$$x - y = y \cdot (xy - 1) - x \cdot (y^2 - 1) \in \boldsymbol{I}$$

인데 $\mathrm{lt}(x - y) = x$는 xy와 y^2으로 나누어지지 않는다.

예 6. $\{x - y, y^2 - 1\}$은 $\boldsymbol{I}$의 Gröbner 기저이다. 만약 $f \in \boldsymbol{I}$이고 $\mathrm{lt}(f)$가 x와 y^2으로 나누어지지 않는 0이 아닌 다항식 f가 존재한다고 하자. 그러면 f는 y의 1차 다항식($f = ay + b$). 그리고 f는 $V_{\mathbb{R}}(\boldsymbol{I}) = \{(1, 1), (-1, -1)\}$에서 0이어야 함. 즉, $f = 0$.

정의에서 모든 아이디얼 I에 Gröbner 기저 G가 존재한다는 것은 명확하지 않은데 이를 증명하자.

주어진 다항식의 집합 A의 선두항 아이디얼(leading term ideal)은 다음과 같다.

$$\mathrm{LT}(A) := \langle \mathrm{lt}(f) | f \in A \rangle.$$

정리 11. *$\boldsymbol{I}$를 $\mathbb{R}[x]$에 속한 아이디얼이라 하자. $\boldsymbol{I}$의 부분집합 $G = \{g_1, \ldots, g_t\}$에 대하여 다음 세 가지는 동치이다.*

1. *G는 $\boldsymbol{I}$의 Gröbner 기저이다.*

2. $f \in \boldsymbol{I} \Leftrightarrow f = \sum_{i=1}^{t} u_i g_i$ 이고 $\mathrm{lt}(f) = \max_{1 \leqslant i \leqslant t} \mathrm{lt}(u_i)\mathrm{lt}(g_i)$.

3. $\mathrm{LT}(\boldsymbol{I}) = \mathrm{LT}(G)$.

증명: 1. $\Rightarrow$ 2. $f \in \mathbb{R}[x]$라 하자. 그리고 f를 G로 나눈 결과가

$$f = \sum_{i=1}^{t} u_i g_i + r,\ \mathrm{lt}(f) = \max(\max_{1 \leqslant i \leqslant t} \mathrm{lt}(u_i g_i), \mathrm{lt}(r))$$

이라 하자. 그러면 $f - r \in I$이 성립하고 $f \in \boldsymbol{I}$와 $r \in \boldsymbol{I}$는 동치이다. 먼저 f가 G로 나누어지면 즉, $r = 0$이면 $r \in \boldsymbol{I}$이므로 $f \in \boldsymbol{I}$이다. 이제 $f \in \boldsymbol{I}$이면 $r = 0$을 보이자. 만약 $r \neq 0$이라 하자. $f \in \boldsymbol{I}$이므로 $r \in \boldsymbol{I}$이다. 그러면 1.에 의해 r의 선두항은 어떤 $\mathrm{lt}(g_i)$으로 나뉜다. 이것은 r이 f를 G로 나눈 나머지라는 데에 모순이다. 그래서 $r = 0$이다.
2. $\Rightarrow$ 3. G의 정의에 의해 $\mathrm{LT}(G) \subseteq \mathrm{LT}(I)$는 자명하자. 이제 역을 증명하자. $f \in \boldsymbol{I}$라 하자. 그러면 2.에 의해 $\mathrm{lt}(f) = \mathrm{lt}(u_i)\mathrm{lt}(g_i)$를 만족하는 i가 존재한다. 그래서 $\mathrm{lt}(f) \in \mathrm{LT}(G)$이다. 그런데 $\mathrm{lt}(f)$들이 $\mathrm{LT}(\boldsymbol{I})$를 생성하므로 $\mathrm{LT}(\boldsymbol{I}) \subseteq \mathrm{LT}(G)$이다.

3. $\Rightarrow$ 1. $f \in \boldsymbol{I}$라 하자. 그러면 $\mathrm{lt}(f) \in \mathrm{LT}(G)$이다. 그래서

$$\mathrm{lt}(f) = \sum_{i=1}^{t} u_i \mathrm{lt}(g_i), \tag{10}$$

를 만족시키는 $u_i \in \mathbb{R}[x]$가 존재한다. 식 (10)의 우변에 있는 모든 항들은 어떤 $\mathrm{lt}(g_i)$에 의해 나뉜다. 좌변에 있는 $\mathrm{lt}(f)$도 우변에 있는 항 중 하나이므로 어떤 $\mathrm{lt}(g_i)$에 의해 나뉜다. □

따름정리 2. *만약 $G = \{g_1, \ldots, g_t\}$가 아이디얼 $\boldsymbol{I}$의 Gröbner 기저이면 $\boldsymbol{I} = \langle G \rangle$이다.*

기본정리 2. *단항의 집합 $S \subsetneq \mathbb{R}[x]$에 대해 $\boldsymbol{I} = \langle S \rangle$라 하자. 그러면 $f \in \boldsymbol{I}$인 것과 f의 각 항이 S에 속한 단항으로 나뉜다는 것은 동치이다. 그리고 $\boldsymbol{I} = \langle S_0 \rangle$를 만족시키는 S의 유한 부분집합 S_0가 존재한다.*

증명: $f \in I$이면 $f = \sum_{i=1}^{l} u_i X_i$를 만족시키는 $u_i \in \mathbb{R}[x]$와 $X_i \in S$가 존재한다. 이 식의 우변의 임의의 항은 그 항을 나누는 어떤 X_i가 존재한다. 그런데 f의 모든 항은 우변에 있는 항 중 하나이므로 f의 모든 항도 역시 그러하다. 역으로 f의 모든 항에 대해 그 항을 나누는 어떤 $X_i \in S$가 존재한다고 하자. 그러면 f의 각 항은 $\boldsymbol{I} = \langle S \rangle$에 속하므로 $f \in \boldsymbol{I}$이다.
이제 마지막 문장을 증명하자. 힐버트 기저 정리에 의해 $\boldsymbol{I}$는 유한 생성된다. 즉, $\boldsymbol{I} = \langle h_1, \ldots, h_s \rangle$을 만족시키는 $h_i \in \mathbb{R}[x]$가 존재한다. $h_i \in \boldsymbol{I}$이므로 정리의 앞부분에 의해 h_i의 각 항에는 그 항을 나누는 단항을 S에서 고를 수 있다. h_i의 모든 항에 대해 대응되는 이 단항의 집합을 $S_i \subseteq S$라 하고 $S_0 = \cup_{i=1}^{s} S_i$라 하자. 그러면 $h_i \in \langle S_0 \rangle$이고 $\boldsymbol{I} \subseteq \langle S_0 \rangle$이다. 그리고 $S_0 \subseteq S$이므로 $\langle S_0 \rangle \subseteq \boldsymbol{I}$이다. 그래서 $\boldsymbol{I} = \langle S_0 \rangle$이다. □

따름정리 3. *$\mathbb{R}[x]$에 속한 아이디얼은 모두 Gröbner 기저를 갖는다.*

증명: $\boldsymbol{I}$가 $\mathbb{R}[x]$에 속한 아이디얼이라 하자. 기본정리에 의해 $\mathrm{LT}(\boldsymbol{I}) = \langle X_1, \ldots, X_m \rangle$를 만족시키는 단항의 유한집합 $\{X_1, \ldots, X_m\}$이 존재한다. $X_i \in \mathrm{LT}(\boldsymbol{I})$이므로 $X_i = \sum_{\nu}^{t_i} Y_\nu \mathrm{lt}(f_\nu)$를 만족하는 항 Y_ν와 $f_\nu \in \boldsymbol{I}$가 존재한다. 따라서 $X_i = Y_i \mathrm{lt}(f_i)$로 쓸 수 있다. $g_i = Y_i f_i$로 두면 $\mathrm{lt}(g_i) = X_i$이고 $g_i \in \boldsymbol{I}$이다. 따라서 $\mathrm{LT}(\boldsymbol{I}) = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle$이다. 정리 11의 3.에 의해 $G = \{g_1, \ldots, g_t\}$는 $\boldsymbol{I}$의 Gröbner 기저이다. □

정의 5. $\mathbb{R}[x]$의 부분집합 $G = \{g_1, \ldots, g_t\}$가 아이디얼 $\langle G \rangle$의 Gröbner 기저이면 간단하게 Gröbner 기저라고 부른다.

정리 12. *$G = \{g_1, \ldots, g_t\}$가 $\mathbb{R}[x]$에 속한 0이 아닌 다항식의 집합이라 하자. 그러면 G가 Gröbner 기저인 것과 임의의 $f \in \mathbb{R}[x]$를 G로 나눈 나머지가 유일한 것은 동치이다.*

증명: 생략.

$\{x - y, y^2 - 1\}$는 $\boldsymbol{I} := \langle x - y, y^2 - 1\rangle$의 Gröbner 기저이다. 그래서 $f = x^2y + xy^2 + y^2$을 $\{x - y, y^2 - 1\}$로 나누면 $x - y$와 $y^2 - 1$의 순서와 상관없이

$$\begin{aligned} f &= (xy + 2y^2) \cdot (x - y) + (2y + 1) \cdot (y^2 - 1) + 2y + 1 \\ &= (xy + 2) \cdot (x - y) + (2x + 1) \cdot (y^2 - 1) + 2y + 1 \end{aligned}$$

이 된다.

이제 Gröbner 기저를 구하는 방법인 Buchberger 알고리듬을 알아보자.

정의 6. 0이 아닌 $f, g \in \mathbb{R}[x]$에 대해 $L = \mathrm{lcm}(\mathrm{lp}(f), \mathrm{lp}(g))$라 하자. 이때 다항식

$$S(f,g) = \frac{L}{\mathrm{lt}(f)} f - \frac{L}{\mathrm{lt}(g)} g$$

을 f와 g의 S-다항식이라 한다.

예 7. 예 4의 $h_1 = xy - 1$과 $h_2 = y^2 - 1$의 S-다항식을 구해보면 $L = xy^2$이므로 $S(h_1, h_2) = \frac{xy^2}{xy}(xy-1) - \frac{xy^2}{y^2}(y^2-1) = x - y$이다.

정리 13. *(Buchberger). 0이 아닌 다항식의 집합 $G = \{g_1, \ldots, g_t\} \subset \mathbb{R}[x]$에 대해 다음이 성립한다: G는 Gröbner 기저이다. $\Leftrightarrow$ 모든 $i \neq j$에 대하여 $S(g_i, g_j)$를 G로 나눈 나머지는 0이다.*

증명: 생략.

알고리듬 2. ***Buchberger* 알고리듬**

입력: $F = \{f_1, \ldots, f_s\} \subseteq \mathbb{R}[x]$ s.t. $f_i \neq 0$ $(1 \leqslant i \leqslant s)$.

출력: 아이디얼 $\langle f_1, \ldots, f_s \rangle$의 Gröbner 기저 $G = \{g_1, \ldots, g_t\}$.

초기화: $G = F, \mathcal{G} = \{\{f_i, f_j\} | f_i \neq f_j \in G\}$

주반복단계: $\mathcal{G} = \emptyset$ 일때 까지 다음을 반복;

임의대로 $\{f, g\} \in \mathcal{G}$ 하나 고른다.

$\mathcal{G} := \mathcal{G} - \{\{f, g\}\}$

$S(f, g)$을 G로 나눈 나머지 h를 구한다; $S(f, g) \to_+^G h$.

만약 $h \neq 0$이면

$\mathcal{G} := \mathcal{G} \cup \{\{u, h\} | \forall u \in G\}$,

$G := G \cup \{h\}$.

Buchberger 알고리듬의 i번째 반복단계에서의 G를 G^i라 하자. Buchberger 알고리듬이 무한히 진행된다면 다음의 오름사슬 아이디얼을 만들 수 있다.

$$\mathrm{LT}(G^1) \subsetneq \mathrm{LT}(G^2) \subsetneq \cdots.$$

이것은 힐버트 기저 정리에 모순되므로 Buchberger 알고리듬은 유한 번 안에 종료된다. 그리고 Buchberger 알고리듬이 출력하는 G는 Buchberger 정리에 의해 $\langle F \rangle$의 Gröbner 기저가 된다.

예 8. 예 4의 $\langle h_1, h_2\rangle$의 Gröbner 기저를 구해보자.
초기화: $G := \{h_1, h_2\}, \mathcal{G} := \{\{h_1, h_2\}\}$
첫 번째 반복단계:
$\{h_1, h_2\}$ 선정, $\mathcal{G} := \emptyset$
$S(h_1, h_2) = x - y \to_+^G x - y$
$x - y \neq 0$이므로 $h_3 := x - y$
$\mathcal{G} := \{\{h_1, h_3\}, \{h_2, h_3\}\}$
$G := \{h_1, h_2, h_3\}$
두 번째 반복단계:
$\{h_1, h_3\}$ 선정, $\mathcal{G} := \{\{h_2, h_3\}\}$
$S(h_1, h_3) = y^2 - 1 \to_+^G 0$
세 번째 반복단계:
$\{h_2, h_3\}$ 선정, $\mathcal{G} := \emptyset$
$S(h_2, h_3) = y^3 - x \to_+^G 0$
$\mathcal{G} = \emptyset$이므로 반복 끝.
그래서 $\{h_1, h_2, h_3\}$이 $\langle h_1, h_2\rangle$의 Gröbner 기저이다.

위에서 Buchberger 알고리듬의 유한성에 대해 살펴보았다. 그 후 많은 연구자들이 Buchberger 알고리듬의 complexity에 대해 연구했는데, 다음 두 가지 이유로 계산시간이 매우 커짐을 알 수 있다.

- 알고리듬 중간에 생성되는 다항식의 차수가 매우 크다. 최초 주어진 다항식의 차수가 모두 d차 이하여도 중간에 생성되는 다항식의 차수가 2^{2^d}의 비율로 커지는 예가 있다.

- 처음 주어진 다항식의 계수가 간단하더라도 Gröbner 기저에 포함된 다항식의 계수는 매우 복잡한 유리수가 될 수 있다.

Quotient algebra $\mathbb{R}[x]/\boldsymbol{I}$

$\mathbb{R}[x]$의 아이디얼 $\boldsymbol{I}$에 대하여 quotient 공간 $\mathbb{R}[x]/\boldsymbol{I}$는 coset $[f] := f + \boldsymbol{I} = \{f + q | q \in \boldsymbol{I}\}$을 원소로 갖는 집합이다.

- $[f] = [g]$의 의미: $f = g + q$인 $q \in I$가 존재.
- $\mathbb{R}[x]/\boldsymbol{I}$은 $\lambda \in \mathbb{R}, f, g \in \mathbb{R}[x]$에 대해서 덧셈 $[f] + [g] = [f + g]$과 스칼라 곱셈 $\lambda[f] = [\lambda f]$로 정의되는 $\mathbb{R}$-벡터 공간.
- $[f][g] = [fg]$으로 정의된 곱셈 연산을 추가하면 환이 된다.

- cosets 집합 $\{[b_1], \ldots, [b_L]\}$이 다음을 만족하면 $\mathbb{R}[x]/\boldsymbol{I}$을 생성한다고 부른다: 임의의 실수 다항식 f에 대하여 $[f] = \sum_{i=1}^{L} \lambda_i [b_i]$를 만족시키는 $\lambda \in \mathbb{R}^L$가 존재한다. 즉, $f = \sum_{i=1}^{L} \lambda_i b_i + q$를 만족시키는 $\lambda \in \mathbb{R}^L$와 $q \in \boldsymbol{I}$가 존재한다.

- $\sum_{i=1}^{L} \lambda_i [b_i] = [0]$ 또는 $\sum_{i=1}^{L} \lambda_i b_i \in \boldsymbol{I}$을 만족시키는 λ가 0밖에 없을 때 $[b_1], \ldots, [b_L]$을 $\mathbb{R}[x]/\boldsymbol{I}$에서 선형 독립이라고 부른다.

- $\{[b_1], \ldots, [b_L]\}$가 $\mathbb{R}[x]/\boldsymbol{I}$을 생성하고 선형 독립이면 $\mathbb{R}[x]/\boldsymbol{I}$의 기저라고 부른다.

정의 7. 주어진 아이디얼 $\boldsymbol{I}$에 대하여

$$\boldsymbol{B}_{\succ} := \mathbb{T}^n \setminus \mathrm{LT}(\boldsymbol{I}) = \{x^\alpha | \forall f \in \boldsymbol{I},\ \mathrm{lt}(f)\text{가 나눌 수 없는 } x^\alpha\}$$

을 표준단항(standard monomials)의 집합이라 한다.

성질 4. *$\boldsymbol{B}_\succ$에 속한 단항의 cosets의 집합은 벡터 공간 $\mathbb{R}[x]/\boldsymbol{I}$의 기저이다.*

증명: 일단 임의의 $f \in \mathbb{R}[x]$를 $\boldsymbol{I}$의 Gröbner 기저 G로 나눈 나머지를 r이라 하자. 그러면 r의 모든 항이 G로 나누어지지 않기 때문에 $r = \sum_i \lambda_i b_i$를 만족시키는 $b_i \in \boldsymbol{B}_\succ$와 $\lambda_i \in \mathbb{R}$가 존재한다. 그리고 $[f] = [r]$이기 때문에 $[f] = \sum_i \lambda_i [b_i]$로 표현된다. 따라서 $\boldsymbol{B}_\succ$에 속한 단항의 cosets의 집합은 벡터 공간 $\mathbb{R}[x]/\boldsymbol{I}$을 생성한다. 그리고 임의의 $f \in \mathbb{R}[x]$를 G로 나눈 나머지는 유일하기 때문에 $\boldsymbol{B}_\succ$에 속한 단항의 cosets은 선형 독립이 된다. (만약 그렇지 않다고 하자. 즉, $|\boldsymbol{B}_\succ| = L$라 하면 $\sum_{i=1}^{L} \lambda_i [b_i] = [0]$이 되는 0이 아닌 $\lambda \in \mathbb{R}^L$가 존재한다. $\lambda_j \neq 0$에 해당하는 b_j에 대해 $b_j = q - 1/\lambda_j \sum_{i \neq j} \lambda_i b_i$를 만족시키는 $q \in \boldsymbol{I}$가 존재한다. 그러면 b_j를 G로 나눈 나머지가 2개 (b_j와 $-1/\lambda_j \sum_{i \neq j} \lambda_i b_i$) 존재하여 모순이다.) □

그래서 아이디얼 $\boldsymbol{I}$의 Gröbner 기저를 구한 다음 그에 대응하는 $\boldsymbol{B}_\succ$를 구하면 quotient 벡터 공간 $\mathbb{R}[x]/\boldsymbol{I}$의 기저를 구할 수 있다. 앞으로 우리는 모호함이 발생하지 않는 경우에 $f \in \mathbb{R}[x]$와 $[f]$를 동일시한다.

다음 정리는 $V_{\mathbb{C}}(\boldsymbol{I})$의 원소 수와 $\mathbb{R}[x]/\boldsymbol{I}$의 차원과의 관계를 나타낸다.

정리 14. *다음 세 가지는 동치이다.*

(i) *아이디얼 $\boldsymbol{I}$가 0 차원이다. 즉, $|V_{\mathbb{C}}(\boldsymbol{I})| < \infty$이다.*

(ii) *모든 $i = 1, \ldots, n$에 대하여 다음을 만족하는 g_j가 $\boldsymbol{I}$의 Gröbner 기저 G에 존재한다.*

$$\text{어떤 } \gamma \in \mathbb{N} \text{에 대하여, } \mathrm{lp}(g_j) = x_i^{\gamma}.$$

(iii) *벡터공간 $\mathbb{R}[x]/\boldsymbol{I}$의 차원이 유한하다.*

증명:

(i) $\Rightarrow$ (ii). $|V_{\mathbb{C}}(\boldsymbol{I})| < \infty$라 하자. 만약 $|V_{\mathbb{C}}(\boldsymbol{I})| = 0$이면 힐버트의 weak Nullstellensatz에 의해 $1 \in G$이다. 따라서 (ii)가 성립한다. 이제 $|V_{\mathbb{C}}(\boldsymbol{I})| > 0$라 하자. $i \in \{1, \ldots, n\}$를 고정하자. l을 $V_{\mathbb{C}}(\boldsymbol{I})$에 속한 점의 i번째 좌표 값 중 서로 다른 값의 개수라 하고 그 값을 a_{ij} $(1 \leqslant j \leqslant l)$라 하자. 그리고 $f = \prod_{j=1}^{l}(x_i - a_{ij})$라 하자. 그러면 $f \in \mathbb{R}[x_i]$이고 $f \in \boldsymbol{I}(V_{\mathbb{C}}(\boldsymbol{I}))$이다. 힐버트의 strong Nullstellensatz에 의해 $\boldsymbol{I}(V_{\mathbb{C}}(\boldsymbol{I})) = \sqrt{\boldsymbol{I}}$이므로 $f \in \sqrt{\boldsymbol{I}}$가 되어 $f^m \in \boldsymbol{I}$가 되는 자연수 m이 존재한다. 따라서 $\mathrm{lp}(f^m) = x_i^{ml}$는 G에 속한 어떤 다항식 g_j의 $\mathrm{lp}(g_j)$로 나누어 떨어진다.

(ii) $\Rightarrow$ (iii). G에 속한 다항식으로 나누어 떨어지지 않는 단항의 coset 집합은 $\mathbb{R}[x]/\boldsymbol{I}$의 기저이다. 그런데 모든 $i = 1, \ldots, n$에 대하여 x_i의 어떤 거듭제곱이 어떤 $g_j \in G$의 선두항과 같으므로 G로 나누어 떨어지지 않는 항의 집합은 유한하다. 그래서 $\mathbb{R}[x]/\boldsymbol{I}$의 기저도 유한하다.

(iii) $\Rightarrow$ (i). $k := \dim \mathbb{R}[x]/\boldsymbol{I} < \infty$라 하자. 그러면 $\{1, x_1, \ldots, x_1^k\}$은 $\mathbb{R}[x]/\boldsymbol{I}$에서 선형 종속이다. 그래서 $f(x) := \sum_{h=0}^{k} \lambda_h x_1^h$가 $\boldsymbol{I}$에 속하게 만드는 $\lambda_0, \ldots, \lambda_k$가 존재하므로 임의의 $v \in V_{\mathbb{C}}(\boldsymbol{I})$는 $f(v) = 0$을 만족한다. 따라서 v_1이 취할 수 있는 값은 k개 이하이다. 다른 좌표에도 같은 방법을 적용하면 $V_{\mathbb{C}}(\boldsymbol{I})$는 유한집합이다. $\square$

따름정리 4. *$\boldsymbol{I}$가 0 차원 아이디얼이라 하고 G를 $\boldsymbol{I}$의 Gröbner 기저라 하자. (여기서 Gröbner 기저는 $x_1 \succ x_2 \succ \cdots \succ x_n$인 사전편찬식순서를 이용함) 그러면 $g_1, \ldots, g_t$를 다음과 같이 재배열할 수 있다. $i = 1, \ldots, n$에 대하여 $g_i \in \mathbb{R}[x_i, x_{i+1}, \ldots, x_n]$이고 $\mathrm{lp}(g_i)$는 x_i의 거듭제곱이다.*

증명: 앞의 증명에 의해서 모든 $i = 1, \ldots, n$에 대하여 x_i^γ가 어떤 다항식 $g_j \in G$의 선두항이 되는 다항식이 반드시 존재한다. 그런데 $x_1 \succ x_2 \succ \cdots \succ x_n$인 사전편찬식순서를 사용했기 때문에 $g_i \in \mathbb{R}[x_i, x_{i+1}, \ldots, x_n]$이다. □

참고 문헌

[1] J. Bochhak, M. Coste, and M.-F. Roy, *Real algebraic geometry*, Springer, 1998.

[2] D.A. Cox, J.B. Little, and D. O'shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer, 1997.

[3] G. Strang, *Linear Algebra and its applications*, Brooks/Cole, 2006.

다항최적화문제의 계층적 완화 방법의 원리

서울대 홍성필, 박명주

차례

- 다항함수의 비음성 그리고 제곱합 문제
- 다항최적화문제
- 계층적 완화방법
- 계층적 완화방법의 다항시간 복잡성
- 계층적 완화방법의 수렴성

함수의 비음성 문제

"함수 f가 모든 점 $x \in \mathbb{R}^n$ 위에서 비음인가?"

- 다른 표현: '$f \geqslant 0$,' 'f가 PSD(positive semidefinite).'
- 다양한 맥락에서 발생. 예를 들어, $\min_{x \in \mathbb{R}^n} f(x) = \max_{\rho \in \mathbb{R}} \ \rho$ s.t. $f - \rho \geqslant 0$.
- f가 일반적인 경우, 이 결정문제는 "decidable" 하지 않을 수 있음 (즉, 이를 결정할 수 있는 "효과적인" 방법이 없음).
- 따라서, 추가 가정으로 f를 다항함수로 가정하자: $f \in \mathbb{R}[x_1, \ldots, x_n]$.

표기: $\mathcal{P}$ = PSD 다항식 집합. $\mathcal{P}_{n,m}$ = 변수 n 개, 차수 m인 PSD 다항식 집합.

힐버트의 17번째 문제

"모든 PSD 다항식은 유리 함수들의 제곱합인가?"

-1900년 파리의 ICM에서.

- 아틴 (E. Artin)에 의해 1920년대에 '예'가 증명됨.
- Artin-Schreier theory of real closed fields
- Real algebraic geometry의 시작점이 됨.
- 오늘날까지도 다양한 연구가 지속되고 있음: E.g p가 PD이면 충분히 큰 r이 존재하여, $\left(\sum x_i^2\right)^r p$가 SOS이다 -Reznick, 1995.
- 그 중에서도 유리함수가 아닌 '다항함수의 제곱합은 $\mathcal{P}$를 얼마나 표현할 수 있을까' 하는 질문은 계산적인 이유로 매우 중요하다.

조금 더 강한 질문: PSD이면 SOS인가?

표기: 다항식의 제곱합(SOS, Sum Of Squares)들의 집합을 Σ로 표현하자. 특히, $\Sigma_{n,m}$을 변수가 n 개, 차수가 m인 SOS 다항식들의 집합이라고 하자.

다음의 질문을 생각해보자.

$$\mathcal{P}_{n,m} \stackrel{?}{=} \Sigma_{n,m}.$$

$\mathcal{P}_{n,m} \supseteq \Sigma_{n,m}$임을 쉽게 알 수 있다. 그러나 등호는 다음 세가지 경우에만 성립한다.

$$m = 2;\ n = 2;\ n = 3 \text{ 이고 } m = 4.$$

반례 : 모츠킨 다항식 $M(x, y, z) = x^4y^2 + x^2y^4 + z^6 - 3x^2y^2z^2 \in \mathcal{P}_{n,m} \setminus \Sigma_{n,m}$.

(일반적으로, $(x_1^2 + \cdots + x_{n-1}^2 - nx_n^2)x_1^2 \cdots x_{n-1}^2 + x_n^{2n} \in \mathcal{P}_{n,2n} \setminus \Sigma_{n,2n}$.)

- $M(x, y, z) \geqslant 0$은 산술-기하 평균 관계 $\frac{a+b+c}{3} \geqslant (abc)^{\frac{1}{3}}$에서 쉽게 알수있다.
- $M(x, y, z)$가 SOS가 아닌 것은 '계수비교법'을 통하여 보일 수 있다. 그러나 이러한 방법을 일반화하면 지수적으로 많은 계산이 필요하다. $\binom{n+m/2}{m/2}$ 정도의 단항들을 가진 다항식을 제곱했을 때 나올수 있는 항들을 모두 고려해야 하기 때문이다.
- 우리는 앞으로 m을 고정 하자. 이 경우에도, 계수비교법은 $O\left(\binom{n+m/2}{m/2}^2\right)$ 개의 미지수를 가진 연립 2차방정식을 푸는 작업을 요한다.
- 그러나 변수 개수가 고정되지 않은 연립 2차방정식은 NP-hard문제이다.

더 좋은 방법은 없는가?

지금까지

임의의 $p \in \mathbb{R}[x]$에 대하여, 다음의 질문을 얼마나 효율적으로 해결할 수 있는가?

- p는 PSD인가, 즉, $p \in \mathcal{P}$인가?
- p는 SOS인가, 즉, $p \in \Sigma$인가?

결정문제 $p \stackrel{?}{\in} \mathcal{P}$

- 'Quantifier elimination'의 하나인 'Tarski-Seidenberg procedure'로 풀 수 있다. 하지만 다항시간 해법은 아니다.

- 실제로 결정문제 '$p \stackrel{?}{\in} \mathcal{P}$'는 NP-hard ('co-NP-complete') 이다: 'Matrix Copositivity' 문제는, 주어진 대칭행렬 $Q = (q_{ij})$에 대해

$$\forall x \in \mathbb{R}^n, \sum_{ij} q_{ij} x_i^2 x_j^2 \stackrel{?}{\geqslant} 0.$$

  이 문제는 co-NP-complete이다. 그리고 다항함수 비음문제의 특수한 경우임을 쉽게 알 수 있다.

- 하지만 결정문제 $p \stackrel{?}{\in} \Sigma$는 (고정된 차수에 대해) 효율적으로 풀 수 있는 문제이다.

결정문제 $p \stackrel{?}{\in} \Sigma$

'그램 행렬 방법 (Gram matrix method) + SDP'를 사용하면 효율적으로 풀 수 있다.

성질 5. *차수가 $2d$ 이하인 실수 다항식 $p(x) = \sum_{\alpha \in \mathbb{N}^n_{2d}} p_\alpha x^\alpha \in \mathbb{R}[x]$에 대하여 다음 둘은 동치이다.*

(i) p는 SOS이다.

(ii) 행렬 변수 $X = (X_{\alpha,\beta})_{\alpha,\beta \in \mathbb{N}^n_d}$로 정의된 다음 시스템이 가능해를 가진다.

$$\begin{cases} X \succeq 0 \\ p_\alpha = \sum_{\beta,\gamma \in \mathbb{N}^n_d | \beta+\gamma=\alpha} X_{\beta,\gamma} \ (|\alpha| \leqslant 2d) \end{cases} \tag{11}$$

증명 (E.g. Choi, Lam and Reznick, 1991)

p가 SOS $\Leftrightarrow \exists u_j \in \mathbb{R}[x]_d$ s.t. $p(x) = \sum_j (u_j(x))^2$.

$z_d := (x^\alpha)_{\alpha \in \mathbb{N}^n_d} = [1, x_1, \ldots, x_n, x_1^2, x_1x_2, \ldots, x_n^d]^T$라 하고, u_j를 $u_j(x)$의 계수 벡터라 하자. (즉, $u_j(x) = u_j^T z_d = z_d^T u_j$.)

$$p(x) = \sum_j (u_j(x))^2 = \sum_j z_d^T u_j u_j^T z_d = z_d^T (\sum_j u_j u_j^T) z_d.$$

어떤 행렬이 rank 1 곱의 합으로 분해되는 것과 그 행렬이 PSD임은 동치.
그래서 p가 SOS $\Leftrightarrow \exists X \succeq 0 : p(x) = z_d^T X z_d$.

표기 예: $n = 2,\ d = 2$

$$X \cdot z_d z_d^T =$$

$$\begin{array}{c} \\ (0,0) \\ (1,0) \\ (0,1) \\ (2,0) \\ (1,1) \\ (0,2) \end{array} \begin{array}{c} \begin{array}{cccccc} (0,0) & (1,0) & (0,1) & (2,0) & (1,1) & (0,2) \end{array} \\ \begin{pmatrix} X_{(0,0),(0,0)} & X_{(0,0),(1,0)} & X_{(0,0),(0,1)} & X_{(0,0),(2,0)} & X_{(0,0),(1,1)} & X_{(0,0),(0,2)} \\ X_{(1,0),(0,0)} & X_{(1,0),(1,0)} & X_{(1,0),(0,1)} & X_{(1,0),(2,0)} & X_{(1,0),(1,1)} & X_{(1,0),(0,2)} \\ X_{(0,1),(0,0)} & X_{(0,1),(1,0)} & X_{(0,1),(0,1)} & X_{(0,1),(2,0)} & X_{(0,1),(1,1)} & X_{(0,1),(0,2)} \\ X_{(2,0),(0,0)} & X_{(2,0),(1,0)} & X_{(2,0),(0,1)} & X_{(2,0),(2,0)} & X_{(2,0),(1,1)} & X_{(2,0),(0,2)} \\ X_{(1,1),(0,0)} & X_{(1,1),(1,0)} & X_{(1,1),(0,1)} & X_{(1,1),(2,0)} & X_{(1,1),(1,1)} & X_{(1,1),(0,2)} \\ X_{(0,2),(0,0)} & X_{(0,2),(1,0)} & X_{(0,2),(0,1)} & X_{(0,2),(2,0)} & X_{(0,2),(1,1)} & X_{(0,2),(0,2)} \end{pmatrix} \end{array}.$$

$$\begin{array}{c} \\ (0,0) \\ (1,0) \\ (0,1) \\ (2,0) \\ (1,1) \\ (0,2) \end{array} \begin{array}{c} \begin{array}{cccccc} (0,0) & (1,0) & (0,1) & (2,0) & (1,1) & (0,2) \end{array} \\ \begin{pmatrix} 1 & x_1 & x_2 & x_1^2 & x_1x_2 & x_2^2 \\ x_1 & x_1^2 & x_1x_2 & x_1^3 & x_1^2x_2 & x_1x_2^2 \\ x_2 & x_1x_2 & x_2^2 & x_1^2x_2 & x_1x_2^2 & x_2^3 \\ x_1^2 & x_1^3 & x_1^2x_2 & x_1^4 & x_1^3x_2 & x_1^2x_2^2 \\ x_1x_2 & x_1^2x_2 & x_1x_2^2 & x_1^3x_2 & x_1^2x_2^2 & x_1x_2^3 \\ x_2^2 & x_1x_2^2 & x_2^3 & x_1^2x_2^2 & x_1x_2^3 & x_2^4 \end{pmatrix} \end{array}$$

$p(x) = z_d^T X z_d = X \circ z_d z_d^T$가 항등식이 되기 위해서는

모든 $\alpha \in \mathbb{N}^n_{2d}$에 대하여 양변의 x^α의 계수가 같아야 한다.

따라서 $p(x)$가 SOS인 것과 다음을 만족시키는 $X \succeq 0$이 있는 것은 동치:

$$p_\alpha = \sum_{\beta,\gamma \in \mathbb{N}^n_d | \beta+\gamma=\alpha} X_{\beta,\gamma}, \ \forall \alpha \in \mathbb{N}^n_{2d}, \ \square$$

따름정리 5. *SOS를 식별하는 것은 SDP로 모형화할 수 있으며, 최대 차수가 상수이면 다항시간에 풀 수 있는 결정문제가 된다.*

예제

$p = x^4 + 2x^3y + 3x^2y^2 + 2xy^3 + 2y^4$가 SOS?

$p(x)$가 4차 제차 다항식(homogeneous polynomials, forms)이므로

$$p(x) \equiv \begin{bmatrix} x^2 & xy & y^2 \end{bmatrix} \underbrace{\begin{bmatrix} a & b & c \\ b & d & e \\ c & e & f \end{bmatrix}}_{X \succeq 0} \begin{bmatrix} x^2 \\ xy \\ y^2 \end{bmatrix}$$

계수 비교법을 적용하면

$$\begin{aligned} x^4 = x^2 \cdot x^2 &\quad\Rightarrow\quad 1 = a \\ x^3y = x^2 \cdot xy &\quad\Rightarrow\quad 2 = 2b \\ x^2y^2 = xy \cdot xy = x^2 \cdot y^2 &\quad\Rightarrow\quad 3 = d + 2c \\ xy^3 = xy \cdot y^2 &\quad\Rightarrow\quad 2 = 2e \\ y^4 = y^2 \cdot y^2 &\quad\Rightarrow\quad 2 = f \\ & \qquad\quad X \succeq 0 \end{aligned}$$

$$X = \begin{bmatrix} 1 & 1 & c \\ 1 & 3-2c & 1 \\ c & 1 & 2 \end{bmatrix} \succeq 0 \;\Leftrightarrow\; -1 \leqslant c \leqslant 1.$$

$c = -1$을 대입하면 X가 다음과 같이 분해된다.

$$X = \begin{bmatrix} 1 & 1 & -1 \\ 1 & 5 & 1 \\ -1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 2 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & -1 \\ 0 & 2 & 1 \end{bmatrix}$$

따라서 $p(x) = (x^2 + xy - y^2)^2 + (2xy + y^2)^2$는 SOS이다.

다항최적화의 SOS완화의 원리

이러한 관찰은 'SOS'를 다항최적화의 다항시간 완화문제를 구성하는데 사용 할 수 있음을 시사한다. 예를 들어, 제약조건이 없는 최적화 문제를 생각해보자.

$$p^{\min} = \min \{p(x) : x \in \mathbb{R}^n\}.$$

동치의 쌍대문제는 다음과 같다.

$$\max \{\rho : p(x) - \rho \geqslant 0 \; \forall x \in \mathbb{R}^n\} \equiv \max \{\rho : p - \rho \in \mathcal{P}\}.$$

쌍대문제를 다음의 문제로 대체하자.

$$p^{\mathrm{put}} = \max\{\rho : p - \rho\text{는 SOS.}\} \equiv \max\{\rho : p - \rho \in \Sigma\}.$$

이는 원문제의 다항시간 완화문제가 된다.

- $p^{\mathrm{put}} \leqslant p^{\mathrm{min}}$.
- p의 차수 d가 상수인 경우, p^{put}는 다항시간에 구할 수 있다.

$\Sigma \subsetneq \mathcal{P}$이기 때문에 일반적으로 간격이 존재한다: $p^{\mathrm{put}} < p^{\mathrm{min}}$. "약쌍대문제"

다항최적화문제

주어진 실수 다항식 $p(x),\ g_i(x)(i=1,\ldots,m)$에 대하여

$$\text{원문제} \quad \begin{aligned} p^{\min} = \inf \quad & p(x) \\ \text{s.t.} \quad & x \in K := \{x \in \mathbb{R}^n | g_i(x) \geqslant 0, i = 1, \ldots, m\}. \end{aligned} \tag{12}$$

- 선형계획문제, 볼록2차계획문제, SDP, SOCP, $\cdots$
- 0-1 정수계획문제(조합최적화문제): $x_i \in \{0,1\} \Leftrightarrow x_i^2 - x_i = 0$. 따라서, 다항최적화문제는 NP-hard.
- 다항함수 비음문제가 NP-hard라는 사실로 부터, 이미 제약조건이 없는 경우에도 다항최적화문제는 NP-hard라는 것을 쉽게 알 수 있다.

- 다항최적화문제는 NP-hard라는 구체적인 증명의 예를 보면, 정수집합 $\{a_1, a_2, \ldots, a_n\}$을 합이 같도록 두 집합으로 분할하는 문제는 다음과 같은 다항식 방정식의 해가 존재하는지와 동치:

$$\left(\sum_{i=1}^{n} a_i x_i\right)^2 + \sum_{i=1}^{n} (x_i^2 - 1)^2 = 0.$$

  따라서, (제약조건이 없는) 다항최적화문제도 NP-hard임을 이미 알수 있다.

- 응용분야: 정유, 화학, 열전달, 시스템 컨트롤, 포트폴리오 최적화 등.

- KKT 조건 풀 때 $\cdots$.

접근법

원문제의 쌍대문제를 쓰면, $\sup\{\rho | p(x) - \rho \geqslant 0, \forall x \in K\}$가 되어, K 위에서 비음인 실수 다항식들의 집합을 $\mathcal{P}(K)$로 표기 하면,

$$\text{쌍대문제} \quad \begin{aligned} p^{\min} = \sup \quad & \rho \\ \text{s.t.} \quad & p(x) - \rho \in \mathcal{P}(K). \end{aligned} \tag{13}$$

앞에서 보았듯이 $\mathcal{P}(K)$는 하나의 다항식이 그에 속하는지 결정하는 문제조차 어려운 문제이다. 그래서, 이를 다루기 어떤 집합 $\mathcal{C}$로 대체하여 "약 쌍대" 완화문제를 만든다.

$$\text{쌍대완화문제} \quad \begin{aligned} p^{\mathcal{C}} = \sup \quad & \rho \\ \text{s.t.} \quad & p(x) - \rho \in \mathcal{C} \subseteq \mathcal{P}(K). \end{aligned} \tag{14}$$

$$p^{\mathcal{C}} \leqslant p^{\min}.$$

접근법

표기: $\beta \in \mathbb{N}^m$에 대하여 $g^\beta = \prod_{i=1}^m g_i^{\beta_i}$, $g^0 = g_0 = 1$. $|\beta| = \sum_{i=1}^m \beta_i$.

- **대안 1 : PrePrime**

$$\mathcal{C} = \mathcal{H}_t(g) := \left\{ \sum_{\beta \in \mathbb{N}^m} \lambda_\beta g^\beta | \ \lambda_\beta \in \mathbb{R}_+, \ \deg(g^\beta) \leqslant t \right\}.$$

- **대안 2 : Preorder**

$$\mathcal{C} = \mathcal{T}_t(g) := \left\{ \sum_{\beta \in \{0,1\}^m} s_\beta g^\beta | \ s_\beta \in \Sigma, \ \deg(s_\beta g^\beta) \leqslant t \right\}.$$

- **대안 3 : Quadratic module**

$$\mathcal{C} = \mathcal{M}_t(g) := \left\{ \sum_{i=0}^{m} s_i g_i \middle| \; s_i \in \Sigma, \; \deg(s_i g_i) \leqslant t \right\}.$$

$$\forall t, \; \mathcal{H}_t(g) \subseteq \mathcal{T}_t(g), \mathcal{M}_t(g) \subseteq \mathcal{T}_t(g).$$

계층적 완화 방법(Hierarchies)

$$
\begin{array}{lllll}
\text{한델만(Handelman):} & p_t^{\text{han}} & = & \sup\ \rho & \text{s.t. } p(x) - \rho \in \mathcal{H}_t(g) \\
\text{슈미젠(Schmüdgen):} & p_t^{\text{sch}} & = & \sup\ \rho & \text{s.t. } p(x) - \rho \in \mathcal{T}_t(g) \\
\text{푸티나(Putinar):} & p_t^{\text{put}} & = & \sup\ \rho & \text{s.t. } p(x) - \rho \in \mathcal{M}_t(g)
\end{array}
$$

$$
\begin{array}{lll}
\mathcal{H}_1(g) \subseteq \mathcal{H}_2(g) \subseteq \cdots \subseteq \mathcal{P}(K) & \Rightarrow & p_1^{\text{han}} \leqslant p_2^{\text{han}} \leqslant \cdots \leqslant p^{\min} \\
\mathcal{T}_1(g) \subseteq \mathcal{T}_2(g) \subseteq \cdots \subseteq \mathcal{P}(K) & \Rightarrow & p_1^{\text{sch}} \leqslant p_2^{\text{sch}} \leqslant \cdots \leqslant p^{\min} \\
\mathcal{M}_1(g) \subseteq \mathcal{M}_2(g) \subseteq \cdots \subseteq \mathcal{P}(K) & \Rightarrow & p_1^{\text{put}} \leqslant p_2^{\text{put}} \leqslant \cdots \leqslant p^{\min}
\end{array}
$$

모든 t에 대하여,

$$
\begin{array}{lll}
\mathcal{H}_t(g) \subseteq \mathcal{T}_t(g) & \Rightarrow & p_t^{\text{han}} \leqslant p_t^{\text{sch}} \\
\mathcal{M}_t(g) \subseteq \mathcal{T}_t(g) & \Rightarrow & p_t^{\text{put}} \leqslant p_t^{\text{sch}}
\end{array}
$$

t가 상수일 때 한델만 완화의 다항성

$$\sup\ \rho \text{ s.t. } p(x) - \rho \in \left\{ \sum_{\beta \in \mathbb{N}^m} \lambda_\beta g^\beta | \lambda_\beta \in \mathbb{R}_+, \deg(g^\beta) \leqslant t \right\}$$

$$\min -x^2 \text{ s.t. } \underbrace{x+1}_{g_1} \geqslant 0, \underbrace{-x+1}_{g_2} \geqslant 0.$$

$$\begin{aligned} p_1^{\text{han}} = \sup \quad & \rho \\ \text{s.t.} \quad & -x^2 - \rho \quad \equiv \lambda_0 + \lambda_1(x+1) + \lambda_2(-x+1) \\ & \qquad\qquad \rho \in \mathbb{R}, \lambda_0, \lambda_1, \lambda_2 \in \mathbb{R}_+. \end{aligned}$$

$$p_1^{\text{han}} = -\infty.$$

t가 상수일 때 한델만 완화의 다항성

$$\sup\ \rho \text{ s.t. } p(x)-\rho \in \left\{ \sum_{\beta\in\mathbb{N}^m} \lambda_\beta g^\beta | \lambda_\beta \in \mathbb{R}_+, \deg(g^\beta) \leqslant t \right\}$$

$$\min -x^2 \text{ s.t. } \underbrace{x+1}_{g_1} \geqslant 0, \underbrace{-x+1}_{g_2} \geqslant 0.$$

$$\begin{aligned} p_2^{\text{han}} = \sup\ & \rho \\ \text{s.t.}\ & -x^2-\rho \equiv \lambda_0+\lambda_1(x+1)+\lambda_2(-x+1)+\lambda_3(x+1)^2 \\ & \quad +\lambda_4(x+1)(-x+1)+\lambda_5(-x+1)^2 \\ & \rho\in\mathbb{R}, \lambda_i \in \mathbb{R}_+. \end{aligned}$$

$$\begin{aligned} p_2^{\text{han}} = \sup\ & \rho \\ \text{s.t.}\ & \lambda_0+\lambda_1+\lambda_2+\lambda_3+\lambda_4+\lambda_5 = -\rho && (x^0) \\ & \lambda_1-\lambda_2+2\lambda_3-2\lambda_5 = 0 && (x^1) \\ & \lambda_3-\lambda_4+\lambda_5 = -1 && (x^2) \\ & \rho\in\mathbb{R}, \lambda_i \in \mathbb{R}_+. \end{aligned}$$

$t=2$일 때 위 문제의 최적해는 다음과 같다.

$$p_2^{\text{han}} = -1, \rho = -1, \lambda_4 = 1, \lambda_j = 0, j = 0, 1, 2, 3, 5.$$

t가 상수일 때 푸티나 완화의 다항성

$$\sup\ \rho \text{ s.t. } p(x) - \rho \in \{\textstyle\sum_{i=0}^{m} s_i g_i | s_i \in \Sigma, \deg(s_i g_i) \leqslant t\}$$

$$\min -x^2 \text{ s.t. } \underbrace{x+1}_{g_1} \geqslant 0, \underbrace{-x+1}_{g_2} \geqslant 0.$$

$$\begin{aligned} p_1^{\text{put}} = \sup \quad & \rho \\ \text{s.t.} \quad & -x^2 - \rho \equiv \lambda_0 + \lambda_1(x+1) + \lambda_2(-x+1) \\ & \lambda_0, \lambda_1, \lambda_2 \in \mathbb{R}_+. \end{aligned}$$

$$p_1^{\text{put}} = -\infty.$$

t가 상수일 때 푸티나 완화의 다항성

$$\sup\ \rho \text{ s.t. } p(x) - \rho \in \{\textstyle\sum_{i=0}^{m} s_i g_i | s_i \in \Sigma, \deg(s_i g_i) \leqslant t\}$$

$$\min -x^2 \text{ s.t. } \underbrace{x+1}_{g_1} \geqslant 0, \underbrace{-x+1}_{g_2} \geqslant 0.$$

$$\begin{aligned} p_2^{\text{put}} = \sup \quad & \rho \\ \text{s.t.} \quad & -x^2 - \rho \equiv s_0 + \lambda_1(x+1) + \lambda_2(-x+1) \\ & s_0 \in \Sigma_{1,2}, \lambda_1, \lambda_2 \in \mathbb{R}_+. \end{aligned}$$

$$p_2^{\text{put}} = -\infty.$$

t가 상수일 때 푸티나 완화의 다항성

$$\sup\ \rho \text{ s.t. } p(x) - \rho \in \{\textstyle\sum_{i=0}^{m} s_i g_i | s_i \in \Sigma, \deg(s_i g_i) \leqslant t\}$$

$$\min -x^2 \text{ s.t. } \underbrace{x+1}_{g_1} \geqslant 0, \underbrace{-x+1}_{g_2} \geqslant 0.$$

$$\begin{aligned} p_3^{\text{put}} = \sup \quad & \rho \\ \text{s.t.} \quad & -x^2 - \rho \equiv s_0 + s_1(x+1) + s_2(-x+1) \\ & s_0, s_1, s_2 \in \Sigma_{1,2}. \end{aligned}$$

$$
\begin{aligned}
\sup \quad & \rho \\
\text{s.t.} \quad & -x^2-\rho \equiv \begin{bmatrix} 1 & x \end{bmatrix} X_0 \begin{bmatrix} 1 \\ x \end{bmatrix} + \begin{bmatrix} 1 & x \end{bmatrix} X_1 \begin{bmatrix} 1 \\ x \end{bmatrix} (x+1) \\
& \quad + \begin{bmatrix} 1 & x \end{bmatrix} X_2 \begin{bmatrix} 1 \\ x \end{bmatrix} (-x+1), \\
& \quad X_0 = \begin{bmatrix} a & b \\ b & c \end{bmatrix}, X_1 = \begin{bmatrix} g & h \\ h & i \end{bmatrix}, X_2 = \begin{bmatrix} j & k \\ k & l \end{bmatrix} \succeq 0.
\end{aligned}
$$

$$
\begin{aligned}
\sup \quad & \rho \\
\text{s.t.} \quad & a+g+j = -\rho && (x^0) \\
& 2b+2h+g+2k-j = 0 && (x^1) \\
& c+i+2h+l-2k = -1 && (x^2) \\
& i-l = 0 && (x^3) \\
& \begin{bmatrix} a & b \\ b & c \end{bmatrix}, \begin{bmatrix} g & h \\ h & i \end{bmatrix}, \begin{bmatrix} j & k \\ k & l \end{bmatrix} \succeq 0.
\end{aligned}
$$

t가 상수일 때 푸티나 완화의 다항성

$$\sup\ \rho \text{ s.t. } p(x) - \rho \in \{\textstyle\sum_{i=0}^{m} s_i g_i | s_i \in \Sigma, \deg(s_i g_i) \leqslant t\}$$

$$\min -x^2 \text{ s.t. } \underbrace{x+1}_{g_1} \geqslant 0, \underbrace{-x+1}_{g_2} \geqslant 0.$$

$$\begin{aligned} p_3^{\text{put}} = \sup \quad & \rho \\ \text{s.t.} \quad & -x^2 - \rho \equiv s_0 + s_1(x+1) + s_2(-x+1) \\ & s_0, s_1, s_2 \in \Sigma_{1,2}. \end{aligned}$$

$t = 3$일 때 위 문제의 최적해는 다음과 같다.

$$p_3^{\text{put}} = -1, X_0 = 0, X_1 = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}, X_2 = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.$$

따라서 $-x^2 + 1 = \frac{1}{2}(x-1)^2(x+1) + \frac{1}{2}(x+1)^2(-x+1)$로 표현할 수 있다.

계층적 완화 방법의 문제 크기

t가 커질수록 변수와 제약식의 개수가 지수적으로 증가!

	$\mathcal{H}_t$	$\mathcal{T}_t$	$\mathcal{M}_t$
변수 수	$\binom{m+t}{t}$	$\binom{n+\lfloor t/2 \rfloor}{\lfloor t/2 \rfloor} \times \binom{n+\lfloor t/2 \rfloor}{\lfloor t/2 \rfloor}$ PSD 행렬 $\binom{m+t}{t}$개	$\binom{n+\lfloor t/2 \rfloor}{\lfloor t/2 \rfloor} \times \binom{n+\lfloor t/2 \rfloor}{\lfloor t/2 \rfloor}$ PSD 행렬 $m+1$개
제약식 수	$\binom{n+t}{t}$	$\binom{n+t}{t}$	$\binom{n+t}{t}$

Recall:

$$
\begin{aligned}
\mathcal{H}_t(g) &:= \left\{ \sum_{\beta \in \mathbb{N}^m} \lambda_\beta g^\beta \middle| \ \lambda_\beta \in \mathbb{R}_+, \ \deg(g^\beta) \leqslant t \right\}, \\
\mathcal{T}_t(g) &:= \left\{ \sum_{\beta \in \{0,1\}^m} s_\beta g^\beta \middle| \ s_\beta \in \Sigma, \ \deg(s_\beta g^\beta) \leqslant t \right\}, \\
\mathcal{M}_t(g) &:= \left\{ \sum_{i=0}^{m} s_i g_i \middle| \ s_i \in \Sigma, \ \deg(s_i g_i) \leqslant t \right\}.
\end{aligned}
$$

계층적 완화 방법들의 수렴성

한델만의 Positivstellensatz, 1988

집합 K가 내부점이 있는 compact한 볼록다면체라고 하자. 실수 다항식 $p(x)$가 K 위에서 양이면 $p(x) \in \mathcal{H}(g)$이다.

따름정리: $\lim_{t\to\infty} p_t^{\text{han}} = p^{\min}$.
증명: 임의의 $\epsilon > 0$에 대해, K 위에서 $p(x) - p^{\min} + \epsilon > 0$이므로, 한델만의 Positivstellensatz에 의하여, $p(x) - p^{\min} + \epsilon \in \mathcal{H}(g)$.

따라서, 다음과 같은 t가 존재한다: $p(x) - (p^{\min} - \epsilon) \in \mathcal{H}_t(g)$. 이러한 t에 대해, 한델만의 t번째 계층문제의 최적해 p_t^{han}은 가능해 $p^{\min} - \epsilon$보다 같거나 크다.

지금까지 임의의 $\epsilon > 0$에 대해, 다음을 만족하는 t가 존재함을 보였다:

$$p^{\min} - \epsilon \leqslant p_t^{\text{han}}. \ \square$$

계층적 완화 방법들의 수렴성

슈미젠의 Positivstellensatz, 1991
집합 K가 compact하다고 하자. 실수 다항식 $p(x)$가 K 위에서 양이면 $p(x) \in \mathcal{T}(g)$이다.

따름정리: $\lim_{t\to\infty} p_t^{\mathrm{sch}} = p^{\min}$.

계층적 완화 방법들의 수렴성

푸티나의 Positivstellensatz, 1993

집합 $\mathcal{M}(g)$가 Archimedean이라 하자. 즉, $\exists N \in \mathbb{N}$ s.t. $N - \|x\|^2 \in \mathcal{M}(g)$. 실수 다항식 $p(x)$가 K 위에서 양이면 $p(x) \in \mathcal{M}(g)$이다.

따름정리: $\lim_{t\to\infty} p_t^{\text{put}} = p^{\min}$.

참고 문헌

[1] E. Artin, *Über die Zerlegung definiter Funktionen in Quadrate*, Hamb. Abh. 5, 100-115, 1927; See also *Collected Papers*, Edited by S. Lang, J.T. Tate, Springer, New York, 273-288, 1965.

[2] M.-D. Choi, T.-Y. Lam, and B. Reznick, *Sums of Squares of real polynomials*, Proceedings of Symposia in Pure mathematics, 58, 103-126, 1995.

[3] D. Handelman, *Representing polynomials by positive linear functions on compact convex polyhedra*, Pacific Journal of Mathematics, 132, 35-62, 1988.

[4] P.A. Parrilo, *Semidefinite programming relaxations for semialgebraic problems*, Mathematical Programming B, 96, 293-320, 2003.

[5] M. Putinar, *Positive polynomials on compact semi-algebraic sets*, Indiana University Mathematics Journal, 42, 969-984, 1993.

[6] B. Reznick, *Some concrete aspects of Hilbert's 17th problem*, In Real Algebraic Geometry and Ordered Structures, C.N. Delzell and J.J. Madden (Eds.), Contemporary Mathematics, 253, 251-272, 1996.

[7] K. Schmüdgen, *The K-moment problem for compact semi-algebraic sets*, Mathematische Annalen, 289, 203-206, 1991.

모멘트 수열과 행렬을 이용한 계층적 완화 방법

차례

- 모멘트 수열
- 모멘트 행렬
- 완화 유도
- 푸티나와 모멘트 완화 방법의 쌍대성

모멘트 수열

정의 8. $\mathbb{R}^n$에서의 비음 보렐 측도(Borel measure): 다음을 만족하는 $\mathbb{R}^n$의 부분집합의 집합에서 $\mathbb{R}_+ \cup \{\infty\}$으로 가는 함수.

i) $\mu(\emptyset) = 0$

ii) $\mu(\bigcup_{i\in\mathbb{N}} A_i) = \sum_{i\in\mathbb{N}} \mu(A_i)$ $\forall$ 서로 소인 집합 $A_i \subseteq \mathbb{R}^n$.

정의 9. $\mathbb{R}^n$ 위에 정의된 측도 μ의 받침(support), $\mathrm{supp}(\mu)$는

$$\mu(\mathbb{R}^n \setminus S) = 0$$

을 만족하는 가장 작은 닫힌 집합 $S \subseteq \mathbb{R}^n$이다.

$\mathrm{supp}(\mu) \subseteq K$이면 μ가 K 위의 측도라고 부른다.

정의 10. $x \in \mathbb{R}^n$에 대해 $\mu(\{x\}) = 1$이고 $\mu(\mathbb{R}^n \setminus \{x\}) = 0$인 측도를 x에서의 디락 측도(Dirac measure)라고 부르고, δ_x로 표기한다.

정의에 의해, $z \in \mathbb{R}^n$에서의 디락측도 δ_z의 받침, $\mathsf{supp}(\delta_z) = \{z\}$이다.

정의 11. $\mathbb{R}^n$ 위에 정의된 측도 μ에 대해, $y_\alpha := \int_{\mathbb{R}^n} x^\alpha \mu(dx)$를 μ의 α차 모멘트라 부른다. 이때, 수열 $(y_\alpha)_{\alpha \in \mathbb{N}^n}$을 μ의 모멘트 수열(moment sequence)이라고 부르고, 유한 수열 $(y_\alpha)_{\alpha \in \mathbb{N}^n_t}$를 t차 모멘트 수열(truncated moment sequence)이라 부른다.

앞으로의 논의에서는 수열 $(y_\alpha)_{\alpha \in \mathbb{N}^n}$의 인덱스 α는 $x_1 \prec x_2 \prec \cdots \prec x_n$인 차수사전편찬식순서를 따른다고 가정한다.

예 9. $z=(1,2)$인 디락측도 δ_z의 모멘트 수열 ζ_z은 다음과 같다.

$$(\zeta_z)_\alpha = \int_{\mathbb{R}^n} x^\alpha \delta_z(dx) = \sup_{A_i\text{는 }\mathbb{R}^n\text{의 partition}} \sum_i \left[\inf_{x\in A_i} x^\alpha\right] \delta_z(A_i) = (1,2)^\alpha$$

$$\zeta_z = \begin{matrix}(0,0)\\(1,0)\\(0,1)\\(2,0)\\(1,1)\\(0,2)\\\vdots\end{matrix}\begin{bmatrix}1\\1\\2\\1\\2\\4\\\vdots\end{bmatrix}, \zeta_{1,z} = \begin{matrix}(0,0)\\(1,0)\\(0,1)\end{matrix}\begin{bmatrix}1\\1\\2\end{bmatrix}, \zeta_{2,z} = \begin{matrix}(0,0)\\(1,0)\\(0,1)\\(2,0)\\(1,1)\\(0,2)\end{matrix}\begin{bmatrix}1\\1\\2\\1\\2\\4\end{bmatrix}$$

이때, ζ_z를 z에서의 제타 벡터(zeta vector)라고 부른다. 그리고 $\zeta_{t,z}\in\mathbb{R}^{\mathbb{N}_t^n}$를 z에서의 t차 제타 벡터라 부른다.

정의 12. 어떤 수열 y가 측도 μ의 모멘트 수열이면 μ를 y의 표현 측도(representing measure)라고 부른다.

모멘트 이론에서 수열 $y = (y_\alpha)_\alpha$가 어떤 측도의 모멘트 수열인지 여부를 알려주는 특징을 연구한다. 특히, 주어진 $K \subseteq \mathbb{R}^n$에 대하여 K-모멘트 문제는 받침이 K인 측도의 모멘트 수열의 특징을 연구한다.

모멘트 행렬

정의 13. 수열 $(y_\alpha)_{\alpha\in\mathbb{N}^n}$에 대해서 모멘트 행렬 $M(y)$를 다음과 같이 정의하자.

$$(M(y))_{\alpha,\beta} = y_{\alpha+\beta},\ \alpha,\beta\in\mathbb{N}^n.$$

예 10. $y=\zeta_{(1,2)}$인 경우

$$M(y) = \begin{matrix}(0,0)\\(1,0)\\(0,1)\\(2,0)\\(1,1)\\(0,2)\\\vdots\end{matrix}\begin{bmatrix} 1 & 1 & 2 & 1 & 2 & 4 & \cdots\\ 1 & 1 & 2 & 1 & 2 & 4 & \cdots\\ 2 & 2 & 4 & 2 & 4 & 8 & \cdots\\ 1 & 1 & 2 & 1 & 2 & 4 & \cdots\\ 2 & 2 & 4 & 2 & 4 & 8 & \cdots\\ 4 & 4 & 8 & 4 & 8 & 16 & \cdots\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

y가 t차 수열(유한 수열)인 경우의 모멘트 행렬?

예 11. $t_0 := \lfloor \frac{t}{2} \rfloor$차 모멘트 행렬 정의

$$y = \begin{matrix} (0,0) \\ (1,0) \\ (0,1) \\ (2,0) \\ (1,1) \\ (0,2) \end{matrix} \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{bmatrix}, \quad M(y) \stackrel{?}{=} \begin{matrix} (0,0) \\ (1,0) \\ (0,1) \\ (2,0) \\ (1,1) \\ (0,2) \\ (3,0) \\ \vdots \end{matrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & & \cdots \\ 2 & 4 & 5 & & & & & \cdots \\ 3 & 5 & 6 & & & & & \cdots \\ 4 & & & & & & & \cdots \\ 5 & & & & & & & \cdots \\ 6 & & & & & & & \cdots \\ & & & & & & & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

$$M_1(y) = \begin{matrix} (0,0) \\ (1,0) \\ (0,1) \end{matrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix}$$

정의 14. 다항식 $g \in \mathbb{R}[x]$와 수열 $y \in \mathbb{R}^{\mathbb{N}^n}$에 대해서, $g*y := M(y)g$를 shifted vector라 부르자.
즉, $\forall \alpha \in \mathbb{N}^n$에 대하여 $(g*y)_\alpha = \sum_\beta g_\beta y_{\alpha+\beta}$이다.

예 12. $y = \zeta_{(1,2)}$이고, $g(x) = 1 + 2x_2$인 경우:

$$g*y := \begin{matrix}(0,0)\\(1,0)\\(0,1)\\(2,0)\\(1,1)\\(0,2)\\\vdots\end{matrix}\begin{bmatrix} 1 & 1 & 2 & 1 & 2 & 4 & \cdots \\ 1 & 1 & 2 & 1 & 2 & 4 & \cdots \\ 2 & 2 & 4 & 2 & 4 & 8 & \cdots \\ 1 & 1 & 2 & 1 & 2 & 4 & \cdots \\ 2 & 2 & 4 & 2 & 4 & 8 & \cdots \\ 4 & 4 & 8 & 4 & 8 & 16 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}\begin{bmatrix} 1 \\ 0 \\ 2 \\ 0 \\ 0 \\ 0 \\ \vdots \end{bmatrix} = \begin{bmatrix} 5 \\ 5 \\ 10 \\ 5 \\ 10 \\ 20 \\ \vdots \end{bmatrix} \in \mathbb{R}^{\mathbb{N}^2}.$$

y가 t차 수열(유한 수열)인 경우에는

예 13. $g(x) = 1 + 2x_2$와

$$y = \begin{matrix}(0,0)\\(1,0)\\(0,1)\\(2,0)\\(1,1)\\(0,2)\end{matrix}\begin{bmatrix}1\\2\\3\\4\\5\\6\end{bmatrix}, \quad g * y \stackrel{?}{=} \begin{matrix}(0,0)\\(1,0)\\(0,1)\\(2,0)\\(1,1)\\(0,2)\\(3,0)\\\vdots\end{matrix}\begin{bmatrix}1 & 2 & 3 & 4 & 5 & 6 & & \cdots\\ 2 & 4 & 5 & & & & & \cdots\\ 3 & 5 & 6 & & & & & \cdots\\ 4 & & & & & & & \cdots\\ 5 & & & & & & & \cdots\\ 6 & & & & & & & \cdots\\ & & & & & & & \cdots\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots\end{bmatrix}\begin{bmatrix}1\\0\\2\\0\\0\\0\\0\\\vdots\end{bmatrix}$$

$g * y$을 행렬의 곱이 정의되는 차수까지의 부분 행렬의 곱으로 정의하자.

$$g * y := \begin{matrix}(0,0)\\(1,0)\\(0,1)\end{matrix}\begin{bmatrix}1 & 2 & 3\\ 2 & 4 & 5\\ 3 & 5 & 6\end{bmatrix}\begin{bmatrix}1\\0\\2\end{bmatrix} = \begin{bmatrix}7\\12\\15\end{bmatrix}$$

정의 15. y가 t차 수열인 경우 $g * y$는 $t - \deg(g)$차 수열로 다음과 같다.

$$g * y := M_{t-\deg(g),\deg(g)}(y)g.$$

즉, $\forall \alpha \in \mathbb{N}^n_{t-\deg(g)}$에 대하여 $(g * y)_\alpha = \sum_{|\beta| \leqslant \deg(g)} g_\beta y_{\alpha+\beta}$이다.

$g * y$도 하나의 수열이므로 $g * y$의 모멘트 행렬을 정의할 수 있다. 이 행렬을 localizing matrix라 부른다.

예 14. $g(x) = 1 + 2x_2$이고 $y = \zeta_{3,(1,2)}$인 경우에는 $g * y$가 $t - \deg(g) = 3 - 1 = 2$차까지 정의되므로 그의 모멘트 행렬은

$$M_1(g * y) = \begin{bmatrix} 5 & 5 & 10 \\ 5 & 5 & 10 \\ 10 & 10 & 20 \end{bmatrix}.$$

따라서 y가 t차 수열인 경우 $g * y$의 모멘트 행렬은 $t_g := \left\lfloor \frac{t-\deg(g)}{2} \right\rfloor$차 이다.

모멘트 행렬과 선형변환(linear transformation)

t차 수열 $y \in \mathbb{R}^{\mathbb{N}_t^n}$를 이용하여 $\mathbb{R}[x]_t \mapsto \mathbb{R}$ 선형변환을 다음과 같이 정의하자.

$$L_y(p) := y^T p = \sum_{|\alpha| \leqslant t} y_\alpha p_\alpha, \quad p \in \mathbb{R}[x]_t.$$

를 정의한다.

기본정리 3. *$y \in \mathbb{R}^{\mathbb{N}_t^n}$이고 $f, g \in \mathbb{R}[x]_{t_0}$일 때, $(t_0 := \lfloor \frac{t}{2} \rfloor)$*

$$L_y(fg) = f^T M_{t_0}(y) g.$$

증명: $fg = \sum_{|\gamma| \leqslant t} (\sum_{|\alpha|,|\beta| \leqslant t_0, \alpha+\beta=\gamma} f_\alpha g_\beta) x^\gamma$이므로,

$$L_y(fg) = \sum_{|\gamma| \leqslant t} \Big(\sum_{|\alpha|,|\beta| \leqslant t_0, \alpha+\beta=\gamma} f_\alpha g_\beta \Big) y_\gamma = \sum_{|\alpha| \leqslant t_0} \sum_{|\beta| \leqslant t_0} f_\alpha g_\beta y_{\alpha+\beta} = f^T M_{t_0}(y) g.$$

기본정리 4. $y \in \mathbb{R}^{\mathbb{N}_t^n}$ 이고 $g \in \mathbb{R}[x]_t$, $f, h \in \mathbb{R}[x]_{t_g}$ 일 때, $(t_g := \left\lfloor \frac{t-\deg(g)}{2} \right\rfloor)$

$$L_y(fgh) = f^T M_{t_g}(g * y)h.$$

증명:

$$\begin{aligned} L_y(fgh) &= \sum_{|\alpha| \leqslant t_g} \sum_{|\beta| \leqslant \deg(g)} \sum_{|\gamma| \leqslant t_g} f_\alpha g_\beta h_\gamma y_{\alpha+\beta+\gamma} \\ &= \sum_{|\alpha| \leqslant t_g} \sum_{|\gamma| \leqslant t_g} f_\alpha h_\gamma \sum_{|\beta| \leqslant \deg(g)} g_\beta y_{\alpha+\gamma+\beta} \\ &= \sum_{|\alpha| \leqslant t_g} \sum_{|\gamma| \leqslant t_g} f_\alpha h_\gamma (g * y)_{\alpha+\gamma} \\ &= \sum_{|\alpha| \leqslant t_g} \sum_{|\gamma| \leqslant t_g} f_\alpha h_\gamma M_{t_g}(g * y)_{\alpha,\gamma} \\ &= f^T M_{t_g}(g * y)h. \end{aligned}$$

□

$$M_{t_0}(y) \succeq 0 \Leftrightarrow \text{모든 } f \in \mathbb{R}[x]_{t_0} \text{에 대하여 } L_y(f^2) \geqslant 0.$$
$$M_{t_g}(g * y) \succeq 0 \Leftrightarrow \text{모든 } f \in \mathbb{R}[x]_{t_g} \text{에 대하여 } L_y(gf^2) \geqslant 0.$$

모멘트 수열을 위한 필요조건

기본정리 5. *만약 y가 측도 μ의 t차 모멘트 수열이면,*

(i) $M_{t_0}(y) \succeq 0$,

(ii) $\mathsf{supp}(\mu) \subseteq \{x \in \mathbb{R}^n | g(x) \geqslant 0\}$이면 $M_{t_g}(g * y) \succeq 0$.

증명: (i) 임의의 $p \in \mathbb{R}[x]_{t_0}$에 대해,

$$p^T M_{t_0}(y) p = \sum_{\alpha,\beta \in \mathbb{N}^n_{t_0}} p_\alpha p_\beta y_{\alpha+\beta} = \sum_{\alpha,\beta \in \mathbb{N}^n_{t_0}} p_\alpha p_\beta \int x^{\alpha+\beta} \mu(dx) = \int p(x)^2 \mu(dx) \geqslant 0$$

이므로, $M_{t_0}(y) \succeq 0$이다.

(ii) 임의의 $p \in \mathbb{R}[x]_{t_g}$에 대해,

$$p^T M_{t_g}(g*y)p = \sum_{\alpha,\beta \in \mathbb{N}^n_{t_g}} p_\alpha p_\beta \sum_{\gamma \in \mathbb{N}^n_{\deg(g)}} g_\gamma y_{\alpha+\beta+\gamma} = \int_K g(x)p(x)^2 \mu(dx) \geqslant 0$$

이므로, $M_{t_g}(g*y) \succeq 0$이다. □

따름정리 6. *y가 측도 μ의 모멘트 수열(무한 수열)이면,*

(i) $M(y) \succeq 0$,

(ii) $supp(\mu) \subseteq \{x \in \mathbb{R}^n | g(x) \geqslant 0\}$이면, $M(g*y) \succeq 0$,

증명: 앞의 기본정리에서 $t \to \infty$로 하면 증명. □

다항함수 최적화를 위한 모멘트 완화

집합 $K := \{x \in \mathbb{R}^n | g_i(x) \geqslant 0,\ i = 1, \ldots, m\}$ 위에서 다항함수 $p(x)$를 최소화하는 문제를 생각하자.

$$p^{\min} := \inf_{x \in K \subseteq \mathbb{R}^n} p(x). \tag{15}$$

이 문제는 다음의 정리에 의해 $\mathsf{supp}(\mu) \subseteq K$를 만족하는 확률측도 μ를 이용하여 표현할 수 있다. 여기서 확률측도란 $\mu(\mathbb{R}^n) = \mu(K) = 1$인 측도이다.

성질 6. *(Lasserre, 2001) $\mathsf{supp}(\mu) \subseteq K$를 만족하는 확률측도 μ의 집합을 $\mathcal{F}(K)$라 할 때,*

$$p^{\min} = \inf_{\mu \in \mathcal{F}(K)} \int_K p(x)\mu(dx) \tag{16}$$

증명: 임의의 가능해 $z \in K$에 대하여, μ를 디락 측도 δ_z로 놓으면

$$\int_K p(x)\mu(dx) = \int_K p(x)\delta_z(dx) = p(z).$$

따라서 임의의 가능해 $z \in K$에 대하여,
$p(z) \geqslant \inf_{\mu \in \mathcal{F}(K)} \int_K p(x)\mu(dx)$이다.

$$p^{\min} \geqslant \inf_{\mu \in \mathcal{F}(K)} \int_K p(x)\mu(dx).$$

역으로, 모든 $z \in K$에 대하여 $p(z) \geqslant p^{\min}$이므로, 임의의 확률측도 μ에 대하여

$$\int_K p(x)\mu(dx) \geqslant \int_K p^{\min}\mu(dx) = p^{\min}\mu(K) = p^{\min}. \quad \square$$

계층적 모멘트 완화 방법 유도 I by Lasserre

원문제 성질 6 **동치문제 1**

$$\begin{array}{ll} \inf & p(x) \\ \text{s.t.} & g_i(x) \geqslant 0 \quad i = 1, \ldots, m. \end{array} \quad \Leftrightarrow \quad \begin{array}{ll} \inf & \int_K p(x)\mu(dx) \\ \text{s.t.} & \mu\text{는 } K \text{ 위의 확률측도.} \end{array}$$

y를 K 위의 측도 μ의 모멘트 수열로 두면

$$\int_K p(x)\mu(dx) = \int_K \sum_\alpha p_\alpha x^\alpha \mu(dx) = \sum_\alpha p_\alpha \int_K x^\alpha \mu(dx) = \sum_\alpha p_\alpha y_\alpha$$

μ가 확률측도이므로

$$y_0 = \int_K x^0 \mu(dx) = \mu(K) = 1.$$

동치문제 1 **동치문제 2**

$$\begin{array}{lll} \inf & \int_K p(x)\mu(dx) & \Leftrightarrow \quad \inf \quad \sum_\alpha p_\alpha y_\alpha \\ \text{s.t.} & \mu\text{는 } K \text{ 위의 확률측도.} & \text{s.t.} \quad y_0 = 1 \end{array}$$

y는 K 위의 측도의 모멘트 수열.

따름정리 6을 이용하면 다음과 같은 완화문제를 얻는다.

$$\begin{aligned} p^{\text{mom}} := \inf_{y \in \mathbb{R}^{\mathbb{N}^n}} \quad & \sum_\alpha p_\alpha y_\alpha \\ \text{s.t.} \quad & y_0 = 1 \\ & M(y) \succeq 0 \\ & M(g_i * y) \succeq 0 \quad i = 1, \ldots, m. \end{aligned}$$

행렬의 PSD 조건을 principal 부분행렬의 PSD 조건으로 완화.
$t \geqslant \max(\deg(p), \deg(g_1), \ldots, \deg(g_m))$인 모든 t에 대하여

$$\begin{aligned} p_t^{\mathrm{mom}} := \inf_{y \in \mathbb{R}^{\mathbb{N}_t^n}} \quad & \textstyle\sum_{|\alpha| \leqslant t} p_\alpha y_\alpha \\ \text{s.t.} \quad & y_0 = 1 \\ & M_{t_0}(y) \succeq 0 \\ & M_{t_i}(g_i * y) \succeq 0 \quad i = 1, \ldots, m. \end{aligned} \tag{17}$$

여기서 $t_i = \left\lfloor \frac{t - \deg(g_i)}{2} \right\rfloor, i = 1, \ldots, m.$
문제 (17)을 다항최적화문제의 t차 계층적 모멘트 완화 방법이라 부른다.

계층적 모멘트 완화 방법 유도 II by Nie.

원문제 **동치문제 1**

$$\begin{array}{lll} \inf & p(x) & \\ \text{s.t.} & g_i(x) \geqslant 0 \quad i = 1, \ldots, m. \end{array} \quad \Leftrightarrow \quad \begin{array}{lll} \inf & p(x) & \\ \text{s.t.} & 1 \geqslant 0 & \\ & g_i(x) \geqslant 0 \quad i = 1, \ldots, m. \end{array}$$

편의상 $g_0(x) := 1$이라 하자.
임의의 PSD 행렬 A에 대해

$$g_i(x) \geqslant 0 \Leftrightarrow g_i(x)A \succeq 0.$$

모든 x에 대해 $\zeta_{t_i,x}\zeta_{t_i,x}^T$는 rank 1 곱이므로 PSD 행렬이다.

$$g_i(x) \geqslant 0 \Leftrightarrow g_i(x)\zeta_{t_i,x}\zeta_{t_i,x}^T \succeq 0.$$

동치문제 1 **동치문제 2**

$$\begin{array}{lll} \inf & p(x) & \\ \text{s.t.} & 1 \geqslant 0 & \\ & g_i(x) \geqslant 0 \quad i = 1, \ldots, m. & \end{array} \quad \Leftrightarrow \quad \begin{array}{lll} \inf & \sum_{|\alpha| \leqslant t} p_\alpha x^\alpha & \\ \text{s.t.} & \zeta_{t_0,x} \zeta_{t_0,x}^T \succeq 0 & \\ & g_i(x) \zeta_{t_i,x} \zeta_{t_i,x}^T \succeq 0 \quad i = 1, \ldots, m. & \end{array}$$

$y_\alpha = x^\alpha$로 치환. ($x^{\alpha+\beta} = x^\alpha x^\beta$이지만 $y_{\alpha+\beta} = y_\alpha y_\beta$일 필요는 없음.)

$$\begin{array}{lll} p_t^{\text{mom}} := \inf\limits_{y \in \mathbb{R}^{\mathbb{N}_t^n}} & \sum_{|\alpha| \leqslant t} p_\alpha y_\alpha & \\ \text{s.t.} & y_0 = 1 & \\ & M_{t_0}(y) \succeq 0 & \\ & M_{t_i}(g_i * y) \succeq 0 \quad i = 1, \ldots, m. & \end{array}$$

예제

$$\min -x^2 \text{ s.t. } \underbrace{1+x}_{g_1} \geqslant 0, \underbrace{1-x}_{g_2} \geqslant 0.$$

$$\begin{aligned} p_3^{\text{mom}} = \inf_{y \in \mathbb{R}^{\mathbb{N}_3^1}} \quad & -y_2 \\ \text{s.t.} \quad & y_0 = 1 \\ & M_1(y) := \begin{bmatrix} y_0 & y_1 \\ y_1 & y_2 \end{bmatrix} \succeq 0 \\ & M_1(g_1 * y) := \begin{bmatrix} y_0 + y_1 & y_1 + y_2 \\ y_1 + y_2 & y_2 + y_3 \end{bmatrix} \succeq 0 \\ & M_2(g_1 * y) := \begin{bmatrix} y_0 - y_1 & y_1 - y_2 \\ y_1 - y_2 & y_2 - y_3 \end{bmatrix} \succeq 0 \end{aligned}$$

위 문제의 최적해는 다음과 같다.

$$p_3^{\text{mom}} = -1, y = (1,1,1,1).$$

계층적 모멘트 완화 방법

p_t^{mom}은 SDP를 이용하여 계산할 수 있으며,

$$p_t^{\text{mom}} \leqslant p_{t+1}^{\text{mom}} \leqslant p^{\text{mom}} \leqslant p^{\min}.$$

게다가 $p_t^{\text{put}} \leqslant p_t^{\text{mom}}$이다.
$\because\ p(x) - \rho \in \mathcal{M}_t(g_1, \ldots, g_m)$이고 $y_0 = 1, M_{t_0}(y) \succeq 0,\ M_{t_i}(g_i * y) \succeq 0\ (i = 1, \ldots, m)$이면

$$L_y(p - \rho) = L_y(s_0) + \sum_{i=1}^{m} L_y(s_i g_i) \geqslant 0$$

이므로 $p^T y \geqslant y_0 \rho = \rho$이다.

푸티나와 모멘트 완화 방법의 쌍대성

t차 푸티나 완화 방법은 다음과 같이 쓸 수 있다.

$$\begin{aligned} p_t^{\text{put}} := \sup \quad & \rho \\ \text{s.t.} \quad & p(x) - \rho = \sum_{i=0}^{m} z_{t_i}^T X_i z_{t_i} g_i(x) \\ & X_i \succeq 0, \ i = 0, \ldots, m. \end{aligned}$$

$|\alpha| \leqslant t$인 α와 $i = 0, \ldots, m$에 대하여 $\binom{n+t_i}{t_i} \times \binom{n+t_i}{t_i}$행렬 A_i^α를 다음과 같이 정의하자. $\forall |\beta|, |\gamma| \leqslant t_i$,

$$[A_i^\alpha]_{\beta,\gamma} = \begin{cases} [g_i]_{\alpha-(\beta+\gamma)}, & \text{if } \beta + \gamma \leqslant \alpha \\ 0, & \text{o.w.} \end{cases}$$

예 15. $i = 0$인 경우에는 $g_0(x) = 1$이므로 A_i^α는 $\beta + \gamma = \alpha$인 경우만 $[A_0^\alpha]_{\beta,\gamma}$ 값이 1이고, 나머지 경우에는 0인 행렬이다. 특히, $i = 0$이고, $\alpha = 0$인 경우에는 $[A_0^0]_{0,0} = 1$이고, 나머지 원소는 0인 행렬이다.

성질 7. $i = 0, \ldots, m$에 대하여 $g_i(x) z_{t_i} z_{t_i}^T = \sum_{|\alpha| \leqslant t} A_i^\alpha x^\alpha$.

증명: 임의의 $|\beta|, |\gamma| \leqslant t_i$에 대하여

$$[\text{좌변}]_{\beta,\gamma} = g_i(x) x^\beta x^\gamma = \sum_{|\delta| \leqslant \deg(g_i)} [g_i]_\delta x^{\beta+\gamma+\delta}.$$

$$[\text{우변}]_{\beta,\gamma} = \sum_{|\alpha| \leqslant t} [A_i^\alpha]_{\beta,\gamma} x^\alpha = \sum_{|\alpha| \leqslant t, \alpha \geqslant \beta+\gamma} [g_i]_{\alpha-(\beta+\gamma)} x^\alpha = \sum_{|\delta| \leqslant t-|\beta+\gamma|} [g_i]_\delta x^{\beta+\gamma+\delta}.$$

그런데 $|\beta|, |\gamma| \leqslant t_i$이므로 $\deg(g_i) \leqslant t - 2t_i \leqslant t - |\beta+\gamma|$이고 $|\delta| > \deg(g_i)$인 δ에 대해서 $[g_i]_\delta = 0$이므로

$$[\text{우변}]_{\beta,\gamma} = \sum_{|\delta| \leqslant \deg(g_i)} [g_i]_\delta x^{\beta+\gamma+\delta} = [\text{좌변}]_{\beta,\gamma}. \quad \square$$

성질 8과 $z_{t_i}^T X_i z_{t_i} g_i(x) = X_i \circ g_i(x) z_{t_i} z_{t_i}^T$를 이용하면 t차 푸티나 완화 방법은 다음과 같이 쓸 수 있다.

$$\begin{array}{ll} \sup & \rho \\ \text{s.t.} & p(x) - \rho = \sum_{i=0}^m \sum_{|\alpha| \leqslant t} X_i \circ A_i^\alpha x^\alpha \\ & X_i \succeq 0, \ i = 0, \ldots, m. \end{array}$$

$\sum_{i=0}^m \sum_{|\alpha| \leqslant t} X_i \circ A_i^\alpha x^\alpha = \sum_{|\alpha| \leqslant t} (\sum_{i=0}^m X_i \circ A_i^\alpha) x^\alpha$이므로 위 문제에 계수 비교법을 적용하면 t차 푸티나 완화 방법은 다음과 같이 쓸 수 있다.

$$\begin{array}{lll} \sup & \rho & \\ \text{s.t.} & \rho \ + & \sum_{i=0}^m A_i^0 \circ X_i = p_0 \\ & & \sum_{i=0}^m A_i^\alpha \circ X_i = p_\alpha, \quad \forall \alpha \in \{\alpha \in \mathbb{R}^n | 1 \leqslant |\alpha| \leqslant t\} \\ & & X_i \succeq 0, \qquad\qquad i = 0, \ldots, m. \end{array} \tag{18}$$

문제 (18)의 쌍대문제를 써보면 다음과 같다.

$$\begin{array}{ll} \inf & \sum_{|\alpha|\leqslant t} p_\alpha y_\alpha \\ \text{s.t.} & y_0 = 1 \\ & \sum_{|\alpha|\leqslant t} y_\alpha A_0^\alpha \succeq 0 \\ & \sum_{|\alpha|\leqslant t} y_\alpha A_i^\alpha \succeq 0, \quad i = 1, \ldots, m. \end{array}$$

그러면 $\sum_{|\alpha|\leqslant t} y_\alpha A_0^\alpha = M_{t_0}(y)$임을 보일 수 있다. 모든 $\beta, \gamma \in \mathbb{N}^n_{t_0}$에 대하여,

$$[\text{좌변}]_{\beta,\gamma} = \left[\sum_{|\alpha|\leqslant t} y_\alpha A_0^\alpha\right]_{\beta,\gamma} = \sum_{|\alpha|\leqslant t} y_\alpha [A_0^\alpha]_{\beta,\gamma} = y_{\beta+\gamma} = [\text{우변}]_{\beta,\gamma}\,.$$

세 번째 등식은 $g_0(x) = 1$이므로 $\alpha = \beta + \gamma$인 경우에만 $[A_0^\alpha]_{\beta,\gamma} = 1$이고 나머지 경우에는 0이기 때문에 성립한다.

한편 $\sum_{|\alpha|\leqslant t} y_\alpha A_i^\alpha = M_{t_i}(g_i * y)$임을 보일 수 있다. 모든 $\beta, \gamma \in \mathbb{N}^n_{t_i}$에 대하여,

$$\begin{aligned}
[\text{좌변}]_{\beta,\gamma} &= \left[\sum_{|\alpha|\leqslant t} y_\alpha A_i^\alpha\right]_{\beta,\gamma} = \sum_{|\alpha|\leqslant t} y_\alpha [A_i^\alpha]_{\beta,\gamma} \\
&= \sum_{|\alpha|\leqslant t, \alpha\geqslant\beta+\gamma} y_\alpha [g_i]_{\alpha-(\beta+\gamma)} = \sum_{|\delta|\leqslant t-|\beta+\gamma|} y_{\beta+\gamma+\delta}[g_i]_\delta \\
&= \sum_{|\delta|\leqslant \deg(g_i)} y_{\beta+\gamma+\delta}[g_i]_\delta = (g_i * y)_{\beta+\gamma} = [\text{우변}]_{\beta,\gamma}\,.
\end{aligned}$$

이 관계를 이용하여 쌍대문제를 다시 쓰면 다음과 같다.

$$\begin{aligned}
\min \quad & p^T y \\
\text{s.t.} \quad & y_0 = 1 \\
& M_{t_0}(y) \succeq 0 \\
& M_{t_i}(g_i * y) \succeq 0, \quad i = 1, \ldots, m.
\end{aligned} \tag{19}$$

(19)는 (17)과 같으므로 푸티나와 모멘트 완화 방법은 서로 쌍대이다.

정리 15. *K에 내부점이 존재하면 (5)와 (6)의 최적값은 같다. 즉, $p_t^{\text{put}} = p_t^{\text{mom}}$이다.*

증명: K에 내부점이 존재하면 문제 (6)에 내부해가 존재하는지 보이자. K가 내부점을 가지므로, K에 속하는 구(ball) B가 존재한다. 그리고 $x \in B$에 대해서 $g_i(x) > 0, i = 1, \ldots, m$이다. $\mathsf{supp}(\mu) = B$를 만족하는 임의의 측도 μ(예. $\mu(A) = \text{volumn}(A \cap B)$.)의 모멘트의 수열을 y라고 하자. 그러면 모든 $i = 0, \ldots, m$에 대해 $M(g_i * y) \succeq 0$가 된다는 것은 쉽게 확인할 수 있다. 이제 모든 $i = 0, \ldots, m$에 대해 $M(g_i * y) \succ 0$임을 보이자. 만약 어떤 다항식 $f \neq 0$에 대해 $f^T M(g_i * y) f = 0$이라고 하자. 그러면, $\int_K f(x)^2 g_i(x) \mu(dx) = \int_B f(x)^2 g_i(x) \mu(dx) = 0$이므로

$$B = \mathsf{supp}(\mu) \subseteq \{x \in \mathbb{R}^n | f(x)^2 g_i(x) = 0\}.$$

즉, 모든 $x \in B$에 대해서, $g_i(x) > 0$이므로, $f(x) = 0$이다. 이는 $f \neq 0$이라는 것에 모순이다. 즉, 문제 (6)는 내부해가 존재하므로 강쌍대정리에 의해 두 문제의 최적값은 같다. □

참고 문헌

[1] P. Billingsley, *Probability and Measure*, John Wiley & Sons, 1986.

[2] J.B. Lasserre, *Global optimization with polynomials and the problem of moments*, SIAM Journal on Optimization, 11, 796-817, 2001.

[3] M. Laurent, *Sums of squares, moment matrices and optimization over polynomials*, In Emerging Applications of Algebraic Geometry, Vol. 149 of IMA Volumes in Mathematics and its Applications, M. Putinar and S. Sullivant (eds.), Springer, 157-270, 2009.

[4] J. Nie, *Lecture note on MATH 271C in University of California, San Diego*, 2010.

계층적 완화 방법의 수렴성

차례

- 푸티나의 Positivstellensatz
- 파릴로(Parrilo)의 결과
- 유한 수렴성
- Software 소개

푸티나의 Positivstellensatz

정의 16. $M \subseteq \mathbb{R}[x]$에 대하여 $1 \in M, M + M \subseteq M, \Sigma M \subseteq M$을 만족하면 quadratic module이라 한다. 그리고 quadratic module M이 $-1 \notin M$이면 proper라 한다.

주어진 실수 다항식 $g_1, \ldots, g_m \in \mathbb{R}[x]$에 대하여

$$\mathcal{M}(g_1, \ldots, g_m) := \left\{ u_0 + \sum_{j=1}^{m} u_j g_j | u_0, u_j \in \Sigma \right\} \tag{20}$$

를 $g_1, \ldots, g_m$이 생성한 *quadratic module*이라 부른다.

다음의 조건을 생각하자.

$$\exists f \in \mathcal{M}(g_1, \ldots, g_m) \text{ s.t. } \{x \in \mathbb{R}^n | f(x) \geqslant 0\}\text{은 compact 집합이다.} \qquad (21)$$

- (21)이 성립하면 $K := \{x \in \mathbb{R}^n | g_i(x) \geqslant 0,\ i = 1, \ldots, m\}$가 compact하다: 임의의 $f \in \mathcal{M}(g_1, \ldots, g_m)$에 대하여 $K \subseteq \{x \in \mathbb{R}^n | f(x) \geqslant 0\}$가 성립.

- 어떤 g_i에 대해 $\{x \in \mathbb{R}^n | g_i(x) \geqslant 0\}$가 compact $\Rightarrow$ (21)은 자동으로 만족. 만약 K가 반지름이 R인 구에 포함된다는 것을 알고 있으면 K에 중복된 제약식 $R^2 - \sum_{i=1}^n x_i^2 \geqslant 0$을 추가하여 (21)을 만족하도록 만들 수 있다.

- 또한 g에 실근이 유한한 방정식 $h_1 = 0, \ldots, h_{m_0} = 0$를 포함하는 경우에도 (21)은 자동으로 만족된다. ($\because f := \sum_{i=1}^{m_0} -h_i^2 = \sum_{i=1}^{m_0} [(\frac{h_i - 1}{2})^2 h_i + (\frac{h_i+1}{2})^2 (-h_i)] \in \mathcal{M}(h_1, \ldots, h_m, -h_1, \ldots, -h_m)$이고 $f(x) \geqslant 0$과 $h_1 = 0, \ldots, h_{m_0} = 0$를 만족시키는 해집합은 동치이므로 compact하다.)

(21)과 동치인 조건들을 살펴보자.

$$\exists N \in \mathbb{N} \text{ s.t. } N - \sum_{i=1}^{n} x_i^2 \in \mathcal{M}(g_1, \ldots, g_m), \tag{22}$$

$$\forall p \in \mathbb{R}[x]\text{에 대하여 } \exists N \in \mathbb{N} \text{ s.t. } N - p \in \mathcal{M}(g_1, \ldots, g_m), \tag{23}$$

$$\exists p_1, \ldots, p_s \in \mathbb{R}[x] \text{ s.t. } \{x \in \mathbb{R}^n | p_1(x) \geqslant 0, \ldots, p_s(x) \geqslant 0\}\text{이 compact하고, } p_I \in \mathcal{M}(g_1, \ldots, g_m)\ \forall I \subseteq \{1, \ldots, s\}. \tag{24}$$

여기서 $I \subseteq \{1, \ldots, s\}$에 대하여 $p_I := \prod_{i \in I} p_i$이다.

기본정리 6. *조건 (21), (22), (23), (24)는 모두 동치이다.*

증명: (23) $\Rightarrow$ (22) $\Rightarrow$ (21) $\Rightarrow$ (24)가 성립하는 것은 자명하다. (24) $\Rightarrow$ (23)을 증명하기 위하여 $K_0 := \{x \in \mathbb{R}^n | p_1(x) \geqslant 0, \ldots, p_s(x) \geqslant 0\}$에 슈미젠의 Positivstellensatz를 적용하자. K_0이 compact이므로, 모든 실수 다항식 p에 대하여 K_0 위에서 $N - p > 0$이 성립하는 $N > 0$이 존재한다. 그리고 $K \subseteq K_0$이므로 $N - p$는 K 위에서도 양이 된다. 슈미젠의 Positivstellensatz에 의해 $N - p = \sum_{I \subseteq \{1,\ldots,s\}} s_I p_I$를 만족시키는 $s_I \in \Sigma$가 존재한다. 각각의 p_I가 $p_I \in \mathcal{M}(g_1, \ldots, g_m)$이므로 $N - p \in \mathcal{M}(g_1, \ldots, g_m)$도 성립한다. $\square$

정의 17. 주어진 실수 다항식 $g_1, \ldots, g_m \in \mathbb{R}[x]$이 생성하는 quadratic module $\mathcal{M}(g_1, \ldots, g_m)$이 조건 (23)을 만족시키면 Archimedean이라 부른다.

예 16. (Prestel and Delzell, 2001) $i = 1, \ldots, n$에 대하여 $g_i := x_i - 1/2$와 $g_{n+1} := 1 - \prod_{i=1}^{n} x_i$를 정의하자. 그러면 $\mathcal{M}(g_1, \ldots, g_{n+1})$은 Archimedean이 아니다.
증명: $\mathbb{R}[x]$의 다항식에 $x_1 \succ x_2 \succ \cdots \succ x_n$인 사전편찬식순서를 적용한 후 다음의 집합을 정의하자. M은 $p \in \mathbb{R}[x]$의 집합으로 $p = 0$이거나 p의 선두항 $p_\alpha x^\alpha$가 $p_\alpha > 0$이고 $\alpha \neq (1, \ldots, 1) \bmod 2$인 다항식이거나, $p_\alpha < 0$이고 $\alpha = (1, \ldots, 1) \bmod 2$인 다항식의 집합이다. 그러면 M은 quadratic module이고 $g_1, \ldots, g_{n+1} \in M$이다. 따라서 $\mathcal{M}(g_1, \ldots, g_{n+1}) \subseteq M$이 성립한다. 그런데 모든 $N \in \mathbb{R}$에 대하여 $N - \sum_{i=1}^{n} x_i^2$은 M의 원소가 아니므로 $\mathcal{M}(g_1, \ldots, g_{n+1})$의 원소도 아니다. 즉, $\mathcal{M}(g_1, \ldots, g_{n+1})$는 Archimedean이 아니다.

예 17. $g_1 := x + 1$와 $g_2 := -x + 1$로 정의된 $\mathcal{M}(g_1, g_2)$은 Archimedean이다. 왜냐하면 $1 - x^2 = \frac{1}{2}(x-1)^2 g_1 + \frac{1}{2}(x+1)^2 g_2$가 되어 (22)를 만족시키기 때문이다.

참고 2. Jacobi and Prestel 정리 4.2, 2001
$g_1, \ldots, g_m$이 일차다항식인 경우에는 $K := \{x \in \mathbb{R}^n | g_1(x) \geqslant 0, \ldots, g_m(x) \geqslant 0\}$가 compact하고 공집합이 아니면 $\mathcal{M}(g_1, \ldots, g_m)$이 Archimedean이다.

푸티나의 Positivstellensatz, 1993
집합 $\mathcal{M}(g_1, \ldots, g_m)$가 Archimedean이라 하자.
실수 다항식 $p(x)$가 $K := \{x \in \mathbb{R}^n | g_1(x) \geqslant 0, \ldots, g_m(x) \geqslant 0\}$ 위에서 양이면 $p(x) \in \mathcal{M}(g_1, \ldots, g_m)$이다.

푸티나의 Positivstellensatz 증명

기본정리 7. $M \subseteq \mathbb{R}[x]$이 *quadratic module*이면, $\boldsymbol{I} := M \cap -M$은 아이디얼이다.

증명: i) $f, g \in \boldsymbol{I} \Rightarrow f + g \in \boldsymbol{I}$임을 보이자.
M은 덧셈에 대해 닫혀 있으므로 $f, g \in M$이고 $-f, -g \in M$이면 $f+g \in M$이고 $-(f+g) \in M$이다. 즉, $f + g \in \boldsymbol{I}$가 된다.
ii) $\forall f \in \boldsymbol{I}$와 $\forall h \in \mathbb{R}[x]$에 대하여, $hf = (\frac{h+1}{2})^2 f + (\frac{h-1}{2})^2(-f) \in \boldsymbol{I}$이다. $\square$

기본정리 8. *$M \subseteq \mathbb{R}[x]$이 maximal proper quadratic module이라 하자. 그러면 $M \cup -M = \mathbb{R}[x]$이다.*

증명: 귀류법을 이용하자. $f \in \mathbb{R}[x] \setminus (M \cup -M)$가 있다고 하자. M의 maximality에 의해 $M + f\Sigma$와 $M - f\Sigma$는 proper가 아니다. 즉, $-1 = g_1 + s_1 f$를 만족하는 $g_1 \in M$과 $s_1 \in \Sigma$이 있고, $-1 = g_2 - s_2 f$를 만족하는 $g_2 \in M$와 $s_2 \in \Sigma$가 있다. 첫 번째 등식에 s_2를 곱하고, 두 번째 등식에 s_1을 곱해서 더하면 $s_1 + s_2 + s_1 g_2 + s_2 g_1 = 0$가 된다. 이것은 $s_1, s_2 \in \boldsymbol{I} := M \cap -M$를 의미한다. ($s_i \in \Sigma \subseteq M$이고 $-s_i = s_j + s_1 g_2 + s_2 g_1 \in M$이기 때문이다.) $\boldsymbol{I}$가 아이디얼이기 때문에, $s_1 f \in \boldsymbol{I} \subseteq M$이 되고, 그래서 $-1 = g_1 + s_1 f \in M$이 되어 M이 proper라는 것에 모순이다. □

기본정리 9. *$M \subseteq \mathbb{R}[x]$이 maximal proper quadratic module이고 Archimedean이라 하고, $\boldsymbol{I} := M \cap -M$, 그리고 $f \in \mathbb{R}[x]$라 하자. 그러면 $f - a \in \boldsymbol{I}$을 만족하는 $a \in \mathbb{R}$가 유일하게 존재한다.*

증명: 집합 $A := \{a \in \mathbb{R} | f - a \in M\}$와 $B := \{b \in \mathbb{R} | b - f \in M\}$을 생각하자. M이 Archimedean이기 때문에 A와 B는 공집합이 아니다. 우리는 $A \cap B$의 원소가 하나임을 보여야 한다. M은 proper이기 때문에 음의 실수를 포함하지 않는다. 그래서 $a \in A$이고 $b \in B$이면 $(f - a) + (b - f) \in M$이므로 $a \leqslant b$가 성립한다. $a_0 := \sup A$와 $b_0 := \inf B$로 정의하면 $a_0 \leqslant b_0$가 성립한다. 게다가, $a_0 = b_0$이다. 왜냐하면 만약 $a_0 < c < b_0$를 만족하는 c가 존재한다면, $f - c \notin M \cup -M$가 되어 기본정리 8의 $\mathbb{R}[x] = M \cup -M$에 모순이기 때문이다. 이제 $a_0 \in A$와 $b_0 \in B$를 증명하여 $A \cap B$의 원소가 하나임을 증명하자. 먼저 $a_0 \in A$임을 보이자. 귀류법을 적용하기 위해 $a_0 \notin A$라 하자. 즉, $f - a_0 \notin M$이라 하자. 그러면 M의 maximality에 의해 quadratic module $M' = M + (f - a_0)\Sigma$는 proper가 아니다; 즉, $-1 = g + (f - a_0)s$를 만족하는 $g \in M$과 $s \in \Sigma$가 존재한다. M이 Archimedean이기 때문에 $N - s \in M$을 만족시키는 $N \in \mathbb{N}$이 존재한다. 그리고 $\epsilon \in \mathbb{R}$을 $0 < \epsilon < 1/N$을 만족시키도록

선택하자. 그러면 $a_0 - \epsilon \in A$이기 때문에 $f - (a_0 - \epsilon) \in M$이 된다. 그래서 $-1 + \epsilon s = g + (f - a_0 + \epsilon)s \in M$이다. 또한 $N - s \in M$이므로 $\epsilon N - \epsilon s \in M$이다. 이 두 다항식을 더하면 $\epsilon N - 1 \in M$이 되어 $\epsilon N - 1 \geqslant 0$이 된다. 하지만 이것은 $\epsilon N - 1 < 0$에 모순이다. $b_0 \in B$도 비슷하게 증명할 수 있다. □

이제 다음의 두 기본정리를 중간 결과로 사용하여 푸티나의 정리를 증명하자.

주장 1. *$\mathcal{M}(g_1,\dots,g_m)$이 Archimedean이고 p가 K 위에서 양이면 $sp-1\in\mathcal{M}(g_1,\dots,g_m)$을 만족하는 $s\in\Sigma$가 존재한다.*

증명: quadratic module $M_0:=\mathcal{M}(g_1,\dots,g_m)-p\Sigma$이 proper가 아님을 보이면 된다. 만약 M_0이 proper라고 하자. 그러면 Zorn's lemma에 의해 M_0를 maximal proper quadratic module이고 $M\supseteq M_0$인 M으로 확장시킬 수 있다. $M\supseteq\mathcal{M}(g_1,\dots,g_m)$이므로 M도 Archimedean이 된다. 기본정리 8을 적용하면, 모든 $i\in\{1,\dots,n\}$에 대하여 $x_i-a_i\in\boldsymbol{I}:=M\cap -M$를 만족시키는 $a\in\mathbb{R}^n$가 존재한다. 그리고 $\boldsymbol{I}$가 아이디얼이기 때문에, 모든 $\alpha\in\mathbb{N}^n$에 대하여

$$\begin{aligned}
x^\alpha-a^\alpha &= x_1^{\alpha_1}\cdots x_n^{\alpha_n}-a_1^{\alpha_1}\cdots a_n^{\alpha_n}\\
&= \textstyle\sum_{i=1}^n(a_1^{\alpha_1}\cdots a_{i-1}^{\alpha_{i-1}}x_i^{\alpha_i}\cdots x_n^{\alpha_n}-a_1^{\alpha_1}\cdots a_i^{\alpha_i}x_{i+1}^{\alpha_{i+1}}\cdots x_n^{\alpha_n})\\
&= \textstyle\sum_{i=1}^n(x_i^{\alpha_i}-a_i^{\alpha_i})a_1^{\alpha_1}\cdots a_{i-1}^{\alpha_{i-1}}x_{i+1}^{\alpha_{i+1}}\cdots x_n^{\alpha_n}\\
&= \textstyle\sum_{i=1}^n(x_i-a_i)(\sum_{j=1}^{\alpha_i-1}x_i^{\alpha_i-1-j}a_i^j)a_1^{\alpha_1}\cdots a_{i-1}^{\alpha_{i-1}}x_{i+1}^{\alpha_{i+1}}\cdots x_n^{\alpha_n}\in\boldsymbol{I}.
\end{aligned}$$

그래서 임의의 실수 다항식 f에 대하여 $f - f(a) \in \boldsymbol{I}$이 된다. 특히 $f = g_j$인 경우에는 $g_j \in \mathcal{M}(g_1, \ldots, g_m) \subseteq M$이고 $-(g_j - g_j(a)) \in M$이기 때문에 $g_j(a) = g_j - (g_j - g_j(a)) \in M$가 성립하여 $g_j(a) \geqslant 0$이 된다. 그래서 $a \in K$가 된다. 마지막으로 $p - p(a) \in \boldsymbol{I} \subseteq M$이고 정의에 의해 $-p \in M_0 \subseteq M$이기 때문에 $-p(a) = (p - p(a)) - p \in M$가 성립한다. 그런데 이는 p가 K 위에서 양이라는 데에 모순이다. □

주장 2. *$\mathcal{M}(g_1, \ldots, g_m)$이 Archimedean이고 p가 K 위에서 양이면 $gp - 1 \in \mathcal{M}(g_1, \ldots, g_m)$이고 $N - g \in \Sigma$를 만족하는 $g \in \mathcal{M}(g_1, \ldots, g_m)$와 $N \in \mathbb{N}$가 존재한다.*

증명: (Marshall의 증명) 주장 1을 만족하는 s를 선택하자. 즉, s는 $s \in \Sigma$이고 $sp-1 \in \mathcal{M}(g_1, \ldots, g_m)$을 만족한다. 조건 (23)을 이용하면 $2k-s$, $2k-s^2p-1 \in \mathcal{M}(g_1, \ldots, g_m)$을 만족시키는 $k \in \mathbb{N}$가 존재한다. $g := s(2k - s)$와 $N := k^2$로 잡자. 그러면 $g \in \mathcal{M}(g_1, \ldots, g_m)$와 $N - g = k^2 - 2ks + s^2 = (k - s)^2 \in \Sigma$를 만족시킨다. 그리고 $gp - 1 = s(2k - s)p - 1 = 2k(sp - 1) + (2k - s^2p - 1)$가 되어 $\mathcal{M}(g_1, \ldots, g_m)$에 속하게 된다. □

주장 2를 만족시키는 g와 N을 고르자. $N > 0$으로 가정할 수 있다. 그리고 $k + p \in \mathcal{M}(g_1, \ldots, g_m)$을 만족시키는 $k \in \mathbb{N}$을 고르자. 그러면 다음이 성립한다:

$$(k - \frac{1}{N}) + p = \frac{1}{N}\left((N - g)(k + p) + (gp - 1) + kg\right) \in \mathcal{M}(g_1, \ldots, g_m).$$

이 과정을 kN번 반복하면 $p \in \mathcal{M}(g_1, \ldots, g_m)$가 성립함을 알 수 있다.

Parrilo의 결과

정리 16. *(Parrilo, 2002) 주어진 실수 다항식 $h_1, \ldots, h_{m_0}, g_1, \ldots, g_m$으로 정의되는 다음의 집합을 생각하자:*

$$K := \{x \in \mathbb{R}^n | h_i(x) = 0, i = 1, \ldots, m_0,\ g_j(x) \geqslant 0, j = 1, \ldots, m\}. \qquad (25)$$

단, $m_0 \geqslant 1, m \geqslant 0$이다. 만약 아이디얼 $\boldsymbol{I} := \langle h_1, \ldots, h_{m_0} \rangle$가 0 차원이고 래디칼일 때 f가 K 위에서 비음이면 $f \in \mathcal{M}(h, -h, g)$에 속한다.

기본정리 10. *$V \subseteq \mathbb{C}^n$이고 $|V| < \infty$이라 하자. 그러면 각 $v \in V$에 대해 다음을 만족하는 내삽다항식(interpolation polynomial) $p_v(x) \in \mathbb{C}[x]$가 존재한다.*

$$p_v(x) = \begin{cases} 1, & x = v \\ 0, & x \in V - \{v\} \end{cases}$$

그리고 V가 복소수 켤레에 대해서 닫혀있으면 모든 $v \in V$에 대해 $p_{\overline{v}} = \overline{p_v}$을 만족하는 복소수 내삽다항식을 만들 수 있다.

증명: $v \in V$를 고정하자. 그러면 임의의 $u \in V - \{v\}$는 $u_i \neq v_i$인 i가 존재한다. 이 중 임의로 하나를 골라 i_u라 하자. 그러면 다음과 같이 정의된 다항식은 위의 조건을 만족시킨다.

$$p_v(x) := \prod_{u \in V - \{v\}} \frac{x_{i_u} - u_{i_u}}{v_{i_u} - u_{i_u}} \tag{26}$$

그리고 $V = \overline{V}$인 경우에는 $p_{\overline{v}} = \overline{p_v}$을 만족하도록 p_v를 만들 수 있다. V가 복소수 켤레에 대해 닫혀있으므로 $V := S \cup T \cup \overline{T}$로 분할된다. 여기서 $S = V \cap \mathbb{R}^n$이고, T와 $\overline{T}$는 켤레 복소수를 나누는 $V \setminus S$의 partition이다. 그리고 각 $v \in V$에 대해 식 (26)에서 구한 $p_v(x)$가 실수 다항식 $R_v(x), I_v(x)$를 이용하여 $p_v(x) = R_v(x) + iI_v(x)$로 표시된다고 하자. 그러면

$$p'_v(x) = \begin{cases} R_v(x), & v \in S \\ R_v(x) + iI_v(x), & v \in T \\ R_{\overline{v}}(x) - iI_{\overline{v}}(x), & v \in \overline{T} \end{cases}$$

역시 각 $v \in V$에서 1이고 나머지에서는 0인 내삽다항식이 된다. 그리고 모든 $v \in V$에 대해 $p'_{\overline{v}} = \overline{p'_v}$을 만족한다. □

정리 16의 증명: $a(x)h_i(x) = (\frac{a(x)+1}{2})^2 h_i(x) + (\frac{a(x)-1}{2})^2(-h_i(x))$이므로 $\mathcal{M}(h,-h,g) = \mathcal{M}(g) + \boldsymbol{I}$이다. 그래서 $f = u_0 + \sum_{j=1}^{m} u_j g_j + q$을 만족시키는 $u_j \in \Sigma$와 $q \in \boldsymbol{I}$가 있음을 보이자. $V := V_{\mathbb{C}}(\boldsymbol{I})$를 $S \cup T \cup \overline{T}$로 분할하자. 여기서 $S = V \cap \mathbb{R}^n$이고, T와 $\overline{T}$는 켤레 복소수를 나누는 $V \setminus S$의 partition이다.

먼저 f가 S 위에서 비음인 실수 다항식이라 하자. $v \in S \cup T$에 대해서 $\gamma_v = \sqrt{f(v)}$로 정의하고, $q_v := \gamma_v p_v (v \in S)$이고, $q_v := \gamma_v p_v + \overline{\gamma_v}\ \overline{p_v} (v \in T)$로 정의하자. 그러면 $f - \sum_{v \in S \cup T} (q_v)^2$는 V의 모든 점에서 0이다; 그래서 $I(V)$에 속하고, I가 래디칼이므로 I에도 속한다. 따라서 $f = \sigma + q$로 표현된다. 여기서 $\sigma \in \Sigma$이고 $q \in I$이다.

이제 f가 K 위에서 비음이라고 하자. 우리는 V의 점에서 다음과 같은 값을 가지는 실수 다항식 $s_0, s_1, \ldots, s_m$를 정의한다. 만약 $v \in V \setminus S$이거나 $v \in S$이고 $f(v) \geqslant 0$이면 $s_0(v) = f(v)$이고 $s_j(v) = 0 (j = 1, \ldots, m)$이다. 만약 그렇지 않으면 $v \notin K$이므로 $g_{j_v}(v) < 0$을 만족하는 $j_v \in \{1, \ldots, m\}$가

있다. 그러면 $s_{j_v}(v) = \frac{f(v)}{g_{j_v}(v)}$이고 나머지 j에 대해서는 $s_j(v) = 0$이다. 따라서 각각의 $s_0, s_1, \ldots, s_m$은 S에서 비음이므로 첫 번째 경우에 해당되므로 $s_j = \sigma_j + q_j$로 표현할 수 있다. 여기서 $\sigma_j \in \Sigma$이고 $q_j \in I$이다. 그러면 $q := f - s_0 - \sum_{j=1}^{m} s_j g_j$로 두면 V의 모든 점에서 0이 되고 I에 속한다. 따라서 $f = s_0 + \sum_{j=1}^{m} s_j g_j + q = \sigma_0 + \sum_{j=1}^{m} \sigma_j g_j + q'$이 된다. 여기서 $q' := q + q_0 + \sum_{j=1}^{m} q_j g_j \in I$이고 $\sigma_0, \sigma_j \in \Sigma$가 된다. □

유한 수렴성

정리 17. *(Laurent, 2007)* $K = \{x \in \mathbb{R}^n | h_j(x) = 0\ (j = 1, \ldots, m_0),\ g_j(x) \geqslant 0\ (j = 1, \ldots, m)\}$*에서 다항식* $p \in \mathbb{R}[x]$*를 최소화시키는 문제를 생각하자. 그리고* $\mathcal{J} := \langle h_1, \ldots, h_{m_0} \rangle$*라 하자. 만약* $|V_{\mathbb{C}}(\mathcal{J})| < \infty$*이면, 충분히 큰* t*에 대해서* $p^{\min} = p_t^{\text{put}}$*가 성립한다.*

증명: $\epsilon > 0$을 고정하자. 그러면 다항식 $p - p^{\min} + \epsilon$은 K 위에서 양이다. 그러면 다항식 $u := -\sum_{j=1}^{m_0} h_j^2$는 $\{x \in \mathbb{R}^n | u(x) \geqslant 0\}$이 $V_{\mathbb{R}}(\mathcal{J})$과 같기 때문에 compact하다. 그리고 u는 $\pm h_1, \ldots, \pm h_{m_0}$가 생성하는 quadratic module에 속하므로 제약식이 만드는 quadratic module은 Archimedean이다. 푸티나의 Positivstellensatz에 의해 다음과 같이 분해된다:

$$p - p^{\min} + \epsilon = s_0 + \sum_{j=1}^{m} s_j g_j + q. \tag{27}$$

여기서 $s_0, s_j \in \Sigma$이고 $q \in \mathcal{J}$이다.

$\{f_1, \ldots, f_L\}$을 total degree 단항순서를 사용하여 구한 $\mathcal{J}$의 Gröbner 기저라고 하자. 그리고 $\mathcal{B}$를 $\mathbb{R}[x]/\mathcal{J}$의 기저라 하고, $d_{\mathcal{B}} := \max_{b\in\mathcal{B}} \deg(b)$로 정하자. 그리고 $s_j = \sum_i s_{i,j}^2$라 하고 $s_{i,j} = q_{i,j} + r_{i,j}$라 하자. 여기서 $r_{i,j}$는 $\mathcal{B}$에 속한 원소들의 선형 결합이고, $q_{i,j} \in \mathcal{J}$이다. 그래서 $\deg(r_{i,j}) \leqslant d_{\mathcal{B}}$가 된다. 이것을 이용하면 다음과 같은 형태의 분해가 가능하다:

$$p - p^{\min} + \epsilon = s_0' + \sum_{j=1}^{m} s_j' g_j + q'. \tag{28}$$

여기서 $s_0', s_j' \in \Sigma$이고, $q' \in \mathcal{J}$이고, $\deg(s_0'), \deg(s_j') \leqslant 2d_{\mathcal{B}}$이다. 이제 T_0를 다음과 같이 정의하자:

$$T_0 := \max(\deg(p), 2d_{\mathcal{B}} + \deg(g_1), \ldots, 2d_{\mathcal{B}} + \deg(g_m)). \tag{29}$$

그러면 $\deg(s_0'), \deg(s_j'), \deg(p - p^{\min} + \epsilon) \leqslant T_0$이 성립하므로 $\deg(q') \leqslant T_0$이 성립한다. 따라서 q'은 다음과 같이 분해된다: $q' = \sum_{l=1}^{L} u_l f_l$. 여기서 total

degree 단항순서를 사용하기 때문에 $\deg(u_l f_l) \leqslant \deg(q') \leqslant T_0$이 성립한다. 우리는 q'이 $\mathcal{J}$의 원래 기저에 차수 제약이 있는 다항식의 결합으로 표현되는 것을 보여야한다. 이것을 위하여 $f_l = \sum_{j=1}^{m_0} a_{l,j} h_j$로 두자. 그러면 $q' = \sum_{l=1}^{L} u_l (\sum_{j=1}^{m_0} a_{l,j} h_j) = \sum_{j=1}^{m_0} (\sum_{l=1}^{L} a_{l,j} u_l) h_j =: \sum_{j=1}^{m_0} b_j h_j$가 된다. 여기서 $b_j := \sum_{l=1}^{L} a_{l,j} u_l$이다. $\deg(u_l) \leqslant T_0$이기 때문에, $\deg(b_j h_j) \leqslant \deg(h_j) + T_0 + \max_{l=1}^{L} \deg(a_{l,j})$가 된다. 그래서 $T_g := T_0 + \max_{l,j}(\deg(a_{l,j}) + \deg(h_j))$로 두면 $\deg(b_j h_j) \leqslant T_g$가 성립한다. 이 때 T_g는 ϵ가 무관함을 기억하자. 따라서 $p^{\min} - \epsilon$은 모든 $t \geqslant T_g$에 대하여 계층적 푸티나 완화 방법의 가능해가 된다. 즉, $t \geqslant T_g$에 대하여 $p_t^{\text{put}} \geqslant p^{\min} - \epsilon$가 됨을 의미한다. 이 때 ϵ을 0으로 보내면 $p_t^{\text{put}} \geqslant p^{\min}$가 되어, 모든 $t \geqslant T_g$에 대하여 $p_t^{\text{put}} = p^{\min}$가 성립한다. □

Software

- 계층적 푸티나 완화 방법: SOSTOOLS, by S. Prajna, A. Papachristodoulou, and P. A. Parrilo. http://www.mit.edu/ parrilo/sostools/index.html

- 계층적 모멘트 완화 방법: GloptiPoly3, by D. Henrion, J.-B. Lasserre and J. Loefberg. http://homepages.laas.fr/henrion/software/gloptipoly3/

- SDP solver: SeDuMi, by J.F. Sturm. http://sedumi.ie.lehigh.edu/

예 최대안정집합문제(C_5)

$$\begin{array}{ll} \max & \sum_{i=1}^{5} x_i \\ \text{s.t.} & x_i x_j = 0 \qquad \forall ij \in E \\ & x_i - x_i^2 = 0 \quad i = 1, \ldots, 5. \end{array}$$

참고 문헌

[1] D. Henrion, J.-B. Lasserre, and J. Löfberg, *GloptiPoly 3: moments, optimization and semidefinite programming*, 2007.

[2] T. Jacobi and A. Prestel, *Distinguised representations of strictly positive polynomials*, Journal für die Reine und Angewandte Mathematik, 532, 223-235, 2001.

[3] M. Laurent, *Semidefinite representations for finte varieties*, Mathematical Programming, 109, 1-26, 2007.

[4] M. Marshall *Positive polynomials and sums of squares*, American Mathematical Society, 2008.

[5] P.A. Parrilo *An explicit construction of distinguished representations of polynomials nonnegative over finite sets*, IfA Technical Report AUT02-02, ETH Zürich, 2002.

[6] A. Prestel and C.N. Delzell, *Positive Polynomials - From Hilbert's 17th Problem to Real Algebra*, Springer, Berlin, 2001.

[7] M. Putinar, *Positive polynomials on compact semi-algebraic sets*, Indiana University Mathematics Journal, 42, 969-984, 1993.

계층적 완화 방법의 성능(계산오차)

차례

- 슈미젠과 푸티나 완화 방법에 대한 오차분석
- Hypercube 위에서의 다항최적화에 계층적 한델만 완화 방법을 적용한 경우 오차분석
- 배낭문제에 계층적 모멘트 완화 방법을 적용한 경우 오차분석

슈미젠과 푸티나 완화 방법에 대한 오차분석

- **Schweighofer, 2004** $K \subseteq (-1,1)^n$이면 $\exists c \in \mathbb{N}$ s.t.
  모든 d차 다항식 p와 모든 정수 $t \geqslant cd^c n^{cd}$에 대하여

$$p^{\min} - p_t^{\text{sch}} \leqslant \frac{cd^4 n^{2d}}{\sqrt[c]{t}} L_p.$$

  여기서 $L_p := \max_\alpha |p_\alpha| \frac{\alpha_1! \cdots \alpha_n!}{|\alpha|!} \leqslant \max_\alpha |p_\alpha|$.

- **Nie and Schweighofer, 2007** K가 Archimedean이면 $\exists c \in \mathbb{N}$ s.t.

$$p^{\min} - p_t^{\text{put}} \leqslant \mathcal{O}(\log t)^{-c} \quad \text{as} \quad t \to \infty.$$

Hypercube 위에서 다항최적화

주어진 $A \in \mathbb{R}^{n\times n}$와 $b \in \mathbb{R}^n$에 대하여,

$$\begin{aligned} p^{\min} := \min \quad & p(x) \\ \text{s.t.} \quad & g_i(x) := x_i \geqslant 0, \qquad i = 1, \ldots, n, \\ & g_{n+i}(x) := 1 - x_i \geqslant 0, \quad i = 1, \ldots, n. \end{aligned} \tag{30}$$

이 문제에 계층적 한델만 완화 방법을 적용하면 다음과 같다.

$$\begin{aligned} p_t^{\text{han}} := \sup \quad & \rho \\ \text{s.t.} \quad & p(x) - \rho = \textstyle\sum_{\alpha,\beta:|\alpha+\beta|\leqslant t} \lambda_{\alpha,\beta} x^\alpha (e-x)^\beta \\ & \lambda_{\alpha,\beta} \geqslant 0, \forall \alpha, \beta \ \text{ s.t. } |\alpha+\beta| \leqslant t. \end{aligned} \tag{31}$$

여기서 $e \in \mathbb{R}^n$은 모든 원소가 1인 벡터이다.

Bernstein operators on the hypercube

- 미지수가 한 개인 경우, k차 이하의 다항식 공간의 Bernstein 기저:

$$p_{k,\beta} := \binom{k}{\beta} x^{\beta}(1-x)^{k-\beta} \ (\beta = 0, \ldots, k). \tag{32}$$

($\beta = 0, \ldots, k$에 대해 $p_{k,\beta}$의 계수 벡터를 모아서 $(k+1) \times (k+1)$ 행렬을 만들면 대각이 $\binom{k}{\beta} \neq 0$인 lower-triangular 행렬이 되기 때문에 컬럼이 $\mathbb{R}^{k+1}$의 기저가 된다.)

- 함수 $f \in C[0,1]$의 k차 Bernstein 근사는 다음과 같이 정의된 다항식 $B_k(f) \in \mathbb{R}[x]_k$이다.

$$B_k(f) := \sum_{\beta=0}^{k} f\left(\frac{\beta}{k}\right) p_{k,\beta}.$$

- $B_k(f)$는 $k \to \infty$일수록 f로 uniformly 수렴한다.
  $(\lim_{k\to\infty} \sup\{|f(x) - B_k(f)(x)| : 0 \leqslant x \leqslant 1\} = 0)$

- B_k는 선형 operator이고 함수값의 부호를 유지한다. 즉, 임의의 실수 a, b와 임의의 함수 f, g에 대하여 $B_k(af + bg) = aB_k(f) + bB_k(g)$이고, f가 $[0, 1]$ 위에서 양이면 $B_k(f)$도 그렇다.

예 18.

$$
\begin{aligned}
B_k(1) &= \textstyle\sum_{\beta=0}^{k} p_{k,\beta} = (x+1-x)^k \\
&= 1 \\
B_k(x) &= \textstyle\sum_{\beta=0}^{k} \frac{\beta}{k} p_{k,\beta} \\
&= \textstyle\sum_{\beta=0}^{k} \frac{\beta}{k} \binom{k}{\beta} x^\beta (1-x)^{k-\beta} \\
&= \textstyle\sum_{\beta=1}^{k} \binom{k-1}{\beta-1} x^\beta (1-x)^{k-\beta} \\
&= x \textstyle\sum_{\beta-1=0}^{k-1} \binom{k-1}{\beta-1} x^{\beta-1} (1-x)^{(k-1)-(\beta-1)} \\
&= x(x+1-x)^{(k-1)} = x \\
B_k(x^2) &= \textstyle\sum_{\beta=0}^{k} \frac{\beta^2}{k^2} p_{k,\beta} \\
&= \textstyle\sum_{\beta=0}^{k} \frac{\beta^2}{k^2} \binom{k}{\beta} x^\beta (1-x)^{k-\beta} \\
&= \textstyle\sum_{\beta=0}^{k} \left(\frac{\beta}{k^2} + \frac{\beta(\beta-1)}{k^2}\right) \binom{k}{\beta} x^\beta (1-x)^{k-\beta} \\
&= \frac{1}{k}x + \textstyle\sum_{\beta=2}^{k} \frac{\beta(\beta-1)}{k(k-1)} \frac{k-1}{k} \binom{k}{\beta} x^\beta (1-x)^{k-\beta} \\
&= \frac{1}{k}x + \frac{k-1}{k}x^2 \textstyle\sum_{\beta-2=0}^{k-2} \binom{k-2}{\beta-1} x^{\beta-2} (1-x)^{(k-2)-(\beta-2)} \\
&= \frac{1}{k}x + \frac{k-1}{k}x^2 = x^2 + \frac{1}{k}x(1-x).
\end{aligned}
$$

- 미지수가 n개인 경우의 Bernstein 기저:

$$P_{k,\beta} := \prod_{i=1}^{n} p_{k,\beta_i}(x_i) = \prod_{i=1}^{n} \binom{k}{\beta_i} x_i^{\beta_i}(1-x_i)^{k-\beta_i} \ (\beta \in [k]_0^n := \{0,\dots,k\}^n). \tag{33}$$

- $P_{k,\beta}$는 각 미지수 x_i의 차수가 k차 이하인 다항식의 집합 $\mathbb{R}[x]_{k,\dots,k}$을 생성한다.

- 간단한 사실은 Bernstein 다항식을 모두 더하면 1이다.

$$\begin{array}{c} \sum_{\beta=0}^{k} p_{k,\beta} = (x+1-x)^k = 1, \ (\text{미지수가 } 1\text{개인 경우}), \\ \sum_{\beta\in[k]_0^n}^{k} P_{k,\beta} = \prod_{i=1}^{n}(x_i+1-x_i)^k = 1, \ (\text{미지수가 } n\text{개인 경우}). \end{array} \tag{34}$$

- 함수 $f \in C[0,1]^n$의 k차 Bernstein 근사 다항식 $B_k(f) \in \mathbb{R}[x]_{kn}$:

$$B_k(f) := \sum_{\beta_1=0}^{k} \cdots \sum_{\beta_n=0}^{k} f\left(\frac{\beta_1}{k}, \ldots, \frac{\beta_n}{k}\right) P_{k,\beta}.$$

- f와 g가 서로 다른 변수를 사용하는 경우

$$B_k(fg) = B_k(f)B_k(g)$$

- 특별히, $\forall \beta \in \{0,1\}^n$에 대하여

$$B_k(x_1^{\beta_1} \cdots x_n^{\beta_n}) = \prod_{i=1}^{n} B_k(x_i^{\beta_i}) = x^{\beta}.$$

p가 2차 다항식인 경우

$p(x) = x^T Ax + b^T x$인 2차 다항식의 k차 Bernstein 근사 B_k의 선형성과 $B_k(x_i^2) = x_i^2 + \frac{1}{k} x_i(1 - x_i)$를 이용하면 p에 대한 k차 Bernstein 근사는 다음과 같다.

$$B_k(p) = p + \frac{1}{k} \sum_{i=1}^{n} A_{ii} x_i (1 - x_i). \tag{35}$$

$-x_i(1 - x_i) = (x_i - 1)^2 + x_i - 1$을 이용하면

$$\begin{aligned} p &= B_k(p) + p - B_k(p) = B_k(p) - \tfrac{1}{k} \textstyle\sum_{i=1}^{n} A_{ii} x_i (1 - x_i) \\ &= B_k(p) - \tfrac{1}{k} \textstyle\sum_{i \in I_-} A_{ii} x_i (1 - x_i) + \tfrac{1}{k} \sum_{i \in I_+} A_{ii} ((x_i - 1)^2 + x_i) - \tfrac{1}{k} \sum_{i \in I_+} A_{ii}. \end{aligned}$$

여기서 $I_+ := \{i \in [n] | A_{ii} > 0\}$, $I_- := \{i \in [n] | A_{ii} < 0\}$.

양변에 $-p^{\min} + \frac{1}{k}\sum_{i\in I_+} A_{ii}$을 더하면

$$\begin{aligned} p - p^{\min} + \tfrac{1}{k}\textstyle\sum_{i\in I_+} A_{ii} \quad &= \quad B_k(p) - p^{\min} + \underbrace{\frac{1}{k}\sum_{i\in I_-} |A_{ii}| x_i(1-x_i)}_{:=q_1(x)} \\ &\quad + \underbrace{\frac{1}{k}\sum_{i\in I_+} A_{ii}\left((x_i-1)^2 + x_i\right)}_{:=q_2(x)}. \end{aligned} \tag{36}$$

$B_k(p) - p^{\min} = \sum_{\beta\in[k]_0^n} \left(p(\frac{\beta}{k}) - p^{\min}\right) P_{k,\beta} \in \mathcal{H}_{kn}(g)$이고 $q_1, q_2 \in \mathcal{H}_2(g)$이므로 $p - p^{\min} + \frac{1}{k}\sum_{i\in I_+} A_{ii} \in \mathcal{H}_{kn}(g)$.

$$p^{\min} - \frac{1}{k}\sum_{i\in I_+} A_{ii} \leqslant p_{kn}^{\text{han}} \text{ 또는는 } p^{\min} - p_{kn}^{\text{han}} \leqslant \frac{1}{k}\sum_{i\in I_+} A_{ii}.$$

Max-Cut 문제에 적용

$$\begin{aligned} p^{\min} := \max \quad & x^T A_G (e - x) \\ \text{s.t.} \quad & g_i(x) := x_i \geqslant 0, \qquad i = 1, \ldots, n, \\ & g_{n+i}(x) := 1 - x_i \geqslant 0, \quad i = 1, \ldots, n. \end{aligned} \tag{37}$$

여기서 A_G는 $ij \in E$인 경우에만 (i,j)번째 원소가 1이고, 나머지 경우에는 0인 행렬이다.

$A_{ii} = 0$이므로 n차 한델만 완화 방법은 최적값을 보장한다.

정리 18. ***(Park and Hong, 2011)*** *Max-Cut 문제에 한델만 완화 방법을 적용하면*

i) 랭크(rank)는 n이다.

ii) $p_t^{\text{han}} \leqslant \frac{n}{t} OPT, \ \forall t \leqslant n.$

p가 d차 다항식인 경우

정리 19. ***(Klerk and Laurent, 2010)*** *$k \geqslant 1$인 정수 k에 대하여 다음을 만족시키는 정수 $t \leqslant \max(kn, d)$이 존재한다.*

$$p - p^{\min} + \frac{L_p}{k}\binom{d+1}{3} n^d \in \mathcal{H}_t(g) \text{ 또는 } p^{\min} - p_t^{\text{han}} \leqslant \frac{L_p}{k}\binom{d+1}{3} n^d.$$

배낭문제에 대한 계층적 모멘트 완화 방법의 오차분석

원문제

$$\begin{aligned} \max \quad & \textstyle\sum_{i\in V} v_i x_i \\ \text{s.t.} \quad & g(x) := C - \textstyle\sum_{i\in V} c_i x_i \geqslant 0 \\ & g_i(x) := x_i^2 - x_i = 0, \qquad \forall i \in V. \end{aligned}$$

$2t$차 계층적 모멘트 완화

$$\begin{aligned} p_{2t}^{\mathrm{mom}}(C,V) := \max \quad & \textstyle\sum_{i\in V} v_i y_{e_i} \\ \text{s.t.} \quad & y_0 = 1 \\ & M_t(y) \succeq 0 \\ & M_{t-1}(g*y) \succeq 0 \\ & M_{t-1}(g_i*y) = 0, \quad \forall i \in V. \end{aligned} \tag{38}$$

여기서 $e_i \in \mathbb{N}^n$는 i번째가 1인 단위 벡터. $n = |V|$라 하자.

$$
\begin{aligned}
M_{t-1}(g_i * y) = 0 \quad &\Leftrightarrow \quad \forall \beta, \gamma \in \mathbb{N}^n_{t-1},\ M_{t-1}(g_i * y)_{\beta,\gamma} = 0 \\
&\Leftrightarrow \quad \forall \beta, \gamma \in \mathbb{N}^n_{t-1},\ (g_i * y)_{\beta+\gamma} = 0 \\
&\Leftrightarrow \quad \forall \beta, \gamma \in \mathbb{N}^n_{t-1},\ y_{\beta+\gamma+2e_i} = y_{\beta+\gamma+e_i} \\
&\Leftrightarrow \quad \forall \alpha \in \mathbb{N}^n_{2t-2},\ y_{\alpha+2e_i} = y_{\alpha+e_i}
\end{aligned}
$$

- $\alpha \in \mathbb{N}^n$ 대신 $\alpha \in \{0,1\}^n$을 고려.
- $\alpha \in \{0,1\}^n$는 V의 부분집합의 특성벡터가 되므로 앞으로 V의 부분집합을 index로 사용.
- $\mathcal{S}(V)$: V의 부분집합의 집합.
- $\mathcal{S}(V)_t$: 원소가 t 이하인 V의 부분집합의 집합.

- 모멘트 행렬(moment matrix): $\mathcal{S}(V)$의 부분집합 $\mathcal{T}$와 $y \in \mathbb{R}^{\mathcal{S}(V)}$에 대한 모멘트 행렬 $M_{\mathcal{T}}(y)$는 행과 열이 $\mathcal{T}$의 원소로 index된 행렬로 다음을 만족하는 행렬이다: $\forall I, J \subseteq \mathcal{T}$,

$$(M_{\mathcal{T}}(y))_{I,J} = y_{I \cup J}.$$

- 이동연산(shift operator): 주어진 벡터 $x, y \in \mathbb{R}^{\mathcal{S}(V)}$에 대해 $x * y \in \mathbb{R}^{\mathcal{S}(V)}$는 다음과 같다.

$$(x * y)_I = \sum_{J \subseteq V} x_J y_{I \cup J}, \ \forall I \subseteq V.$$

이 결과를 (38)에 대입하면 다음과 같이 변한다.

$$\begin{aligned} p_{2t}^{\mathrm{mom}}(C,V) := \max \quad & \textstyle\sum_{i\in V} v_i y_{\{i\}} \\ \text{s.t.} \quad & y_\emptyset = 1 \\ & M_{\mathcal{S}(V)_t}(y) \succeq 0 \\ & M_{\mathcal{S}(V)_{t-1}}(g*y) \succeq 0 \end{aligned} \tag{39}$$

문제 (39)의 가능해 영역을 $\mathrm{La}^{2t}(C,V)$라 하자. $y \in \mathrm{La}^{2t}(C,V)$라 가정하자.

정리 20. *배낭문제의 문제 예 (C,V)가 주어졌을 때, $t \geqslant 2$에 대해*

$$Value(y) \leqslant p_{2t}^{\mathrm{mom}}(C,V) \leqslant (1+\frac{1}{t-1})OPT(C,V).$$

$t \geqslant 2$에 대해 $k := t-1$로 잡고, 다음을 정의하자.

$$S = \{i \in V | v_i > OPT(C,V)/k\}.$$

기본정리 11. *임의의* $x, z \in \mathbb{R}^{\mathcal{S}(V)}$*에 대해* $x * (z * y) = z * (x * y)$*이다.*

증명:

$$(\text{좌변})_I = \sum_{J \subseteq V} x_J (z * y)_{I \cup J} = \sum_{J \subseteq V} x_J \sum_{K \subseteq V} z_K y_{I \cup J \cup K} = \sum_{J \subseteq V} \sum_{K \subseteq V} x_J z_K y_{I \cup J \cup K}.$$

$$(\text{우변})_I = \sum_{K \subseteq V} z_K (x * y)_{I \cup K} = \sum_{K \subseteq V} z_K \sum_{J \subseteq V} x_J y_{I \cup K \cup J} = \sum_{J \subseteq V} \sum_{K \subseteq V} x_J z_K y_{I \cup J \cup K}.$$

선형완화

$$\begin{aligned} Value(C, V) := \max \quad & \textstyle\sum_{i \in V} v_i x_i \\ \text{s.t.} \quad & C - \textstyle\sum_{i \in V} c_i x_i \geqslant 0 \\ & 0 \leqslant x_i \leqslant 1, \qquad \forall i \in V. \end{aligned}$$

성질 8.

$$Value(C, V) \leqslant OPT(C, V) + \max_{i \in V} v_i.$$

정의 18. (특성다항식(characteristic polynomial)) $X \subseteq S$에 대한 특성다항식 $P^X(x)$를 다음과 같이 정의하자:

$$P^X(x) := \prod_{i \in X} x_i \prod_{j \in S \setminus X} (1 - x_j) = \sum_{J : X \subseteq J \subseteq S} (-1)^{|J \setminus X|} \prod_{i \in J} x_i.$$

그리고 $P^X \in \mathbb{R}^{\mathcal{S}(V)}$는 J번째 원소가 $P^X(x)$에서 $\prod_{i \in J} x_i$의 계수인 벡터.

기본정리 12. *(inversion formula)* $y \in \mathbb{R}^{\mathcal{S}(V)}$와 $X \subseteq S$에 대해 $z^X := P^X * y$로 정의하자. 즉,

$$z_I^X := \sum_{J \in \mathcal{S}(V)} P_J^X y_{I \cup J} = \sum_{J : X \subseteq J \subseteq S} (-1)^{|J \setminus X|} y_{I \cup J}.$$

그러면 $y = \sum_{X \subseteq S} z^X$.

증명: $I \subseteq V$를 고정하자.

$$\sum_{X \subseteq S} z_I^X = \sum_{X \subseteq S} \sum_{J : X \subseteq J \subseteq S} (-1)^{|J \setminus X|} y_{I \cup J} = \sum_{J \subseteq S} \sum_{X \subseteq J} (-1)^{|J \setminus X|} y_{I \cup J}.$$

$\sum_{X \subseteq J} (-1)^{|J \setminus X|} = (1-1)^{|J|}$이므로 $\sum_{X \subseteq S} z_I^X = y_I$이다. □

기본정리 13. *$y \in \mathbb{R}^{\mathcal{S}(V)}$와 임의의 $X \subseteq S$에 대해 다음이 성립한다.*

$$\begin{array}{lll} 1. & z_I^X = z_{I\setminus X}^X, & \forall I \in \mathcal{S}(V) \\ 2. & z_I^X = z_\emptyset^X, & \text{if } I \subseteq X \\ 3. & z_I^X = 0, & \text{if } I \cap (S \setminus X) \neq \emptyset \end{array}$$

증명: $X \subseteq J$인 J에 대해서 $y_{I\cup J} = y_{(I\setminus X)\cup J}$가 성립한다. 그래서 첫 번째 등식은 성립한다. 그리고 두 번째 등식은 첫 번째 등식에서 바로 나온다. 세 번째 등식을 위해 $i \in I \cap (S \setminus X)$라 하자. 그러면 z_I^X를 정의하기 위해 사용되는 $J : X \subseteq J \subseteq S$는 $i \notin J$인 J와 $J \cup \{i\}$로 쌍 지어진다. 그리고 $i \in I$이므로 $I \cup J = I \cup (J \cup \{i\})$이다. 따라서

$$z_I^X = \sum_{J:X\subseteq J\subseteq S\setminus\{i\}} ((-1)^{|J\setminus X|} + (-1)^{|J\cup\{i\}\setminus X|}) y_{I\cup J} = 0. \quad \square$$

따름정리 7. *w^X를 다음과 같이 정의하자.*

$$w^X = \begin{cases} 0, & \text{if } z_\emptyset^X = 0 \\ z^X / z_\emptyset^X, & \text{if } z_\emptyset^X \neq 0 \end{cases}$$

그러면 $z_\emptyset^X \neq 0$인 경우 $j \in X$에 대해서는 $w_{\{j\}}^X = 1$이고 $j \in S \setminus X$에 대해서는 $w_{\{j\}}^X = 0$이다.

정의 19. (이동연산에 닫힘) $\mathcal{T} \subseteq \mathcal{S}(V)$가 다음을 만족하면 $\mathcal{T}$가 S에 의한 이동연산에 대해 닫혀있다고 부른다.

$$J \in \mathcal{T} \Rightarrow \forall I \subseteq S, I \cup J \in \mathcal{T}.$$

기본정리 14. *$\mathcal{T}$가 S에 의한 이동연산에 대해 닫혀있다고 하자. 만약 $M_{\mathcal{T}}(y) \succeq 0$이면 모든 $X \subseteq S$에 대해 $M_{\mathcal{T}}(z^X) \succeq 0$이다.*

증명: $M_{\mathcal{T}}(y) \succeq 0$이므로 $M_{\mathcal{T}}(y) = U^T U$를 만족하는 $|\mathcal{T}| \times |\mathcal{T}|$ 행렬 U가 존재한다. U의 $I \in \mathcal{T}$번째 열을 u^I라 하자. 그러면 $\langle u^I, u^J \rangle = y_{I \cup J}$를 만족한다. 그리고 각 $I \in \mathcal{T}$에 대해 다음과 같이 벡터를 정의하자.

$$q^I := \sum_{J : X \subseteq J \subseteq S} (-1)^{|J \setminus X|} u^{I \cup J} = \sum_{H \subseteq S \setminus X} (-1)^{|H|} u^{I \cup X \cup H}.$$

$\mathcal{T}$가 S에 의한 이동연산에 대해 닫혀있으므로 잘 정의된다.

그러면 $I, J \in \mathcal{T}$에 대해 $\langle q^I, q^J \rangle = (z^X)_{I \cup J}$이 성립함을 보일 수 있다.

$$\begin{aligned} \langle q^I, q^J \rangle &= \textstyle\sum_{H \subseteq S \setminus X} \sum_{L \subseteq S \setminus X} (-1)^{|H|+|L|} \langle u^{I \cup X \cup H}, u^{J \cup X \cup L} \rangle \\ &= \textstyle\sum_{H \subseteq S \setminus X} \sum_{L \subseteq S \setminus X} (-1)^{|H|+|L|} y_{I \cup J \cup X \cup H \cup L} \end{aligned}$$

H가 공집합이 아닌 경우를 생각하자. $i \in H$라 하자. 그러면 $L \subseteq S \setminus X$은 $i \notin L$인 것과 $L \cup \{i\}$의 쌍이 존재한다. $H = H \cup \{i\}$이기 때문에

$$\sum_{L \subseteq S \setminus X} (-1)^{|H|+|L|} y_{I \cup J \cup X \cup H \cup L} = \sum_{L \subseteq (S \setminus \{i\}) \setminus X} ((-1)^{|H|+|L|} + (-1)^{|H|+|L \cup \{i\}|}) y_{I \cup J \cup X \cup H \cup L} = 0.$$

그래서 H가 공집합인 경우만 계산하면 된다.

$$\langle q^I, q^J \rangle = \sum_{L \subseteq S \setminus X} (-1)^{|L|} y_{I \cup J \cup X \cup L} = (z^X)_{I \cup J} = (M_{\mathcal{T}}(z^X))_{I,J}.$$

Q를 q^I가 I번째 열인 행렬이라 하면 $M_{\mathcal{T}}(z^X) = Q^T Q \succeq 0$이다. □

기본정리 15. $|I| \leqslant 2t$인 I가 $\sum_{i\in I\cap S} c_i > C$이면 $y_I = 0$이다.

증명: 일단 $\sum_{i\in I\cap S} c_i > C$라 하자. 그리고 $|I|$의 크기에 따라 다음과 같이 나누자.

1. $|I| \leqslant t-1$인 경우. $M_{\mathcal{S}(V)_{t-1}}(g*y) \succeq 0$이므로 대각원소인 $(g*y)_I$는 비음이다. $g(x) = C - \sum_{i\in V} c_i x_i$임을 기억하자. 그러면

$$0 \leqslant (g*y)_I = Cy_I - \sum_{i\in V} c_i y_{I\cup\{i\}} \leqslant Cy_I - \sum_{i\in I\cap S} c_i y_{I\cup\{i\}} = Cy_I - \sum_{i\in I\cap S} c_i y_I$$

위의 부등식은 $c_i \geqslant 0$이고 $M_{\mathcal{S}(V)_t}(y) \succeq 0$에 의해 $|J| \leqslant t$인 J에 대해서 $y_J \geqslant 0$이기 때문에 성립한다. 가정에 의해 $\sum_{i\in I\cap S} c_i > C$이므로 $y_I = 0$이다.

2. $t \leqslant |I| \leqslant 2t-2$인 경우. $|I_1|, |I_2| \leqslant t-1$인 I_1, I_2를 이용하여 I를 분할하자. ($I = I_1 \cup I_2$) 이때 $\sum_{i \in I_1 \cap S} c_i > C$이 되도록 I_1을 잡을 수 있다. (만약 $|I \cap S| \leqslant k \leqslant t-1$인 경우에는 $I \cap S \subseteq I_1$이 되도록 잡자. 그러면 $I \cap S = I_1 \cap S$이므로 $\sum_{i \in I_1 \cap S} c_i > C$가 만족된다. 그리고 $|I \cap S| \geqslant k+1$인 경우에는 $|I_1 \cap S| = k$가 되도록 I_1을 잡자. 그러면 $\sum_{i \in I_1 \cap S} v_i > OPT(C, V)$이므로 $\sum_{i \in I_1 \cap S} c_i > C$가 만족된다.) 그러면 앞의 1.에 의해 $y_{I_1} = 0$이다. 그리고 $M_{\mathcal{S}(V)_t}(y) \succeq 0$의 principal 부분행렬

$$M_{\{I_1, I_2\}}(y) = \begin{pmatrix} 0 & y_I \\ y_I & y_{I_2} \end{pmatrix} \succeq 0$$

이므로 $y_I = 0$이다.

3. $2t-1 \leqslant |I| \leqslant 2t$인 경우. $|I_1|, |I_2| \leqslant t$인 I_1, I_2를 이용하여 I를 분할하자. ($I = I_1 \cup I_2$) 이때 2.와 비슷하게 $\sum_{i \in I_1 \cap S} c_i > C$이 되도록 I_1을 잡을 수 있다. 그리고 2.에 의해 $y_{I_1} = 0$이 되고 2.와 비슷한 논리로 $y_I = 0$이다. □

따름정리 8. *$|I| \leqslant 2t$인 I에 대해 $|I \cap S| \geqslant k$이면 $y_I = 0$.*

기본정리 16. *$\mathcal{T}_1 = \{A \subseteq V || A \setminus S| \leqslant 1\}$ $\mathcal{T}_2 = \{B \subseteq V || B \setminus S| = 0\}$라 하면 모든 $X \subseteq S$에 대해 $M_{\mathcal{T}_1}(z^X) \succeq 0$, $M_{\mathcal{T}_2}(g * z^X) \succeq 0$이다.*

증명: 먼저 $M_{\mathcal{T}_1}(y) \succeq 0$를 보이자. $\mathcal{T}_1$의 정의에 의해 $I \in \mathcal{T}_1$이고 $|I| \geqslant t$이면 $|I \cap S| \geqslant k$가 성립하여 따름정리 8에 의해 $y_I = 0$이다. 따라서

$$M_{\mathcal{T}_1}(y) = \begin{pmatrix} M & 0 \\ 0 & 0 \end{pmatrix},$$

이고 M은 $M_{\mathcal{S}(V)_t}(y)$의 principal 부분행렬이다. 그래서 $M \succeq 0$이고 $M_{\mathcal{T}_1}(y) \succeq 0$이다. 정의에 의해 $\mathcal{T}_1$은 S에 의한 이동연산에 대해 닫혀 있고 $M_{\mathcal{T}_1}(y) \succeq 0$이므로 기본정리 14에 의해 $M_{\mathcal{T}_1}(z^X) \succeq 0$이다.

비슷하게 $M_{\mathcal{T}_2}(g*y) \succeq 0$를 보이자. $J \in \mathcal{T}_2$이고 $|J| \geqslant t-1$이면 $|J \cap S| \geqslant k$이므로 $y_J = 0$이다. 그리고 모든 $i \in V$에 대하여 $|(J \cup \{i\}) \cap S| \geqslant k$이므로

$y_{J\cup\{i\}} = 0$이다. 그래서 $g*y$의 정의에 의해 $(g*y)_J := Cy_J - \sum_i c_i y_{J\cup\{i\}} = 0$이다. 따라서

$$M_{\mathcal{T}_2}(g*y) = \begin{pmatrix} N & 0 \\ 0 & 0 \end{pmatrix},$$

이고 N은 $M_{\mathcal{S}(V)_{t-1}}(g*y)$의 principal 부분행렬이다. 그래서 $N \succeq 0$이고 $M_{\mathcal{T}_2}(g*y) \succeq 0$이다. 기본정리 11에 의해 $g*z^X = g*(P^X*y) = P^X*(g*y)$이다. 정의에 의해 $\mathcal{T}_2$는 S에 의한 이동연산에 대해 닫혀 있고 $M_{\mathcal{T}_2}(g*y) \succeq 0$이므로 기본정리 14에 의해 $M_{\mathcal{T}_2}(g*z^X) \succeq 0$이다. □

기본정리 17. *모든 $X \subseteq S$에 대해 다음이 성립한다.*

- $z_{\emptyset}^{X} \geqslant 0$.
- *만약 $z_{\emptyset}^{X} = 0$이면 $|I| \leqslant 2$인 모든 I에 대해서 $z_{I}^{X} = 0$이다.*

증명: 기본정리 16과 같이 $\mathcal{T}_1$을 정의하자. 그러면 기본정리 16에 의해 $M_{\mathcal{T}_1}(z^X) \succeq 0$이므로 대각원소인 $z_{\emptyset}^{X} \geqslant 0$이다.

두 번째 증명하기 위해 $|I| = 1$인 경우를 보자. 이 경우 $I \in \mathcal{T}_1$이다. 그래서 $M_{\mathcal{T}_1}(z^X) \succeq 0$의 principal 부분행렬 $M_{\{\emptyset, I\}}(z^X)$도 PSD이다. 따라서

$$M_{\{\emptyset, I\}}(z^X) = \begin{pmatrix} 0 & z_I^X \\ z_I^X & z_I^X \end{pmatrix} \succeq 0$$

이므로 $z_I^X = 0$이다.

$|I| = 2$인 경우를 보자. 그러면 $I = I_1 \cup I_2$이고 $|I_1|, |I_2| = 1$인 I_1과 I_2가 존재한다. 그래서 $z^X_{I_1} = z^X_{I_2} = 0$이다. 그리고 $M_{\mathcal{T}_1}(z^X) \succeq 0$의 principal 부분행렬 $M_{\{I_1,I_2\}}(z^X)$도 PSD이다. 따라서

$$M_{\{I_1,I_2\}}(z^X) = \begin{pmatrix} 0 & z^X_I \\ z^X_I & 0 \end{pmatrix} \succeq 0$$

이므로 $z^X_I = 0$이다. □

기본정리 18. *$X_i \subseteq S$에 대해 $g^{X_i}(x) = C - \sum_{j\in X_i} c_j - \sum_{j\in V\setminus S} c_j x_j$로 정의하자. 그러면 $(g * z^{X_i})_\emptyset = (g^{X_i} * z^{X_i})_\emptyset$.*

증명:

$$\begin{aligned}(g * z^{X_i})_\emptyset - (g^{X_i} * z^{X_i})_\emptyset &= ((g - g^{X_i}) * z^{X_i})_\emptyset \\ &= \textstyle\sum_{j\in X_i} c_j z_\emptyset^{X_i} - \sum_{j\in S} c_j z_{\{j\}}^{X_i} \\ &= \textstyle\sum_{j\in X_i} c_j z_\emptyset^{X_i} - \sum_{j\in X_i} c_j z_{\{j\}}^{X_i} - \sum_{j\in S\setminus X_i} c_j z_{\{j\}}^{X_i} \\ &= \textstyle\sum_{j\in X_i} c_j z_\emptyset^{X_i} - \sum_{j\in X_i} c_j z_{\{j\}}^{X_i} = 0\end{aligned}$$

위에서 네 번째 등식은 기본정리 13의 세 번째 성질에 의한 것이고, 다섯 번째 등식은 기본정리 13의 첫 번째 성질에 의한 것이다. □

집합 $\mathcal{T} \subseteq \mathcal{S}(V)$와 $y \in \mathbb{R}^{\mathcal{S}(V)}$가 주어졌을 때, $y|\mathcal{T}$는 y를 $\mathcal{T}$ 위로 투영시킨 벡터를 나타낸다.

정리 21. *$y|\mathcal{S}(V)_2$는 다음을 만족시키는 $w^{X_i} \in \mathbb{R}^{\mathcal{S}(V)}$의 $w^{X_i}|\mathcal{S}(V)_2$의 볼록 조합이다($i = 1, \ldots, m$).*

1. $X_1, \ldots, X_m$는 S의 부분집합이다.

2. $w^{X_i}_{\{j\}} = \begin{cases} 1, & \text{if } j \in X_i \\ 0, & \text{if } j \in S \setminus X_i \end{cases}$

3. $w^{X_i} \in \mathrm{La}^2(C, V)$

4. $w^{X_i}|\mathcal{S}(V \setminus S)_2 \in \mathrm{La}^2(C_i, V \setminus S)$. 여기서 $C_i := C - \sum_{j \in X_i} c_j$.

증명: 기본정리 12와 기본정리 17에 의해 다음이 성립한다.

$$y|\mathcal{S}(V)_2 = \sum_{X\subseteq S} z^X|\mathcal{S}(V)_2 = \sum_{X\subseteq S} z^X_\emptyset w^X|\mathcal{S}(V)_2.$$

$X \subseteq S$ 중에서 $z^X_\emptyset \neq 0$인 X의 집합을 $\{X_1, \ldots, X_m\}$이라 하자. 그러면 기본정리 12와 y의 정의에 의해 $\sum_{i=1}^m z^{X_i}_\emptyset = \sum_{X\subseteq S} z^X_\emptyset = y_\emptyset = 1$이다. 기본정리 17의 첫 부분에서 $z^{X_i}_\emptyset \geqslant 0$이므로 $y|\mathcal{S}(V)_2$는 $w^{X_i}|\mathcal{S}(V)_2$의 볼록조합이다.

X_i의 정의와 따름정리 7에 의해 첫 번째와 두 번째 조건은 만족된다.

기본정리 16에 의해 $M_{\mathcal{T}_1}(z^{X_i}) \succeq 0$이고 $M_{\mathcal{T}_2}(g * z^{X_i}) \succeq 0$이므로 이들의 principal 부분행렬인 $M_{\mathcal{S}(V)_1}(z^{X_i}) \succeq 0$이고 $M_{\mathcal{S}(V)_0}(g * z^{X_i}) \succeq 0$이다. 그러면 w^{X_i}의 정의에 의해 $w^{X_i}_\emptyset = 1$, $M_{\mathcal{S}(V)_1}(w^{X_i}) \succeq 0$이고 $M_{\mathcal{S}(V)_0}(g * w^{X_i}) \succeq 0$이다. 즉, $w^{X_i} \in \mathrm{La}^2(C, V)$이다.

$M_{\mathcal{S}(V\setminus S)_1}(w^{X_i})$은 $M_{\mathcal{S}(V)_1}(w^{X_i}) \succeq 0$의 principal 부분행렬이므로 PSD이

다. 비슷하게 $M_{\mathcal{S}(V)_0}(g * z^{X_i}) \succeq 0$이므로 $M_{\mathcal{S}(V\setminus S)_0}(g * z^{X_i}) \succeq 0$이다. 기본정리 18에 의해 $M_{\mathcal{S}(V\setminus S)_0}(g^{X_i} * z^{X_i}) = M_{\mathcal{S}(V\setminus S)_0}(g * z^{X_i}) \succeq 0$이다. 즉, $w^{X_i}|\mathcal{S}(V \setminus S)_2 \in \mathrm{La}^2(C_i, V \setminus S)$. $\square$

정리 20의 증명: 정리 21에 의해 $y|\mathcal{S}(V)_2$는 $X_i \subseteq S$인 $w^{X_i}|\mathcal{S}(V)_2$의 볼록 조합이기 때문에 $Value(y) \leqslant \max_i Value(w^{X_i})$가 된다. 정리 21의 두 번째와 네 번째 성질에 의해 다음이 성립한다.

$$Value(w^{X_i}) \leqslant \sum_{j \in X_i} v_j + p_2^{\mathrm{mom}}(C_i, V \setminus S).$$

그런데 계층적 모멘트 완화 방법의 성질과 성질 8에 의해

$$p_2^{\mathrm{mom}}(C_i, V \setminus S) \leqslant Value(C_i, V \setminus S) \leqslant OPT(C_i, V \setminus S) + OPT(C, V)/(t-1).$$

$$Value(y) \leqslant \max_{X_i \subseteq S} \left(\sum_{j \in X_i} v_j + OPT(C_i, V \setminus S) \right) + OPT(C, V)/(t-1).$$

그리고 정리 21의 세 번째 성질에 의해 $w^{X_i} \in \mathrm{La}^2(C, V)$이다. 그래서 $\sum_{j \in V} c_j w_{\{j\}}^{X_i} \leqslant C$가 된다. 그런데 $j \in X_i$에 대해서는 $w_{\{j\}}^{X_i} = 1$이므로

$\sum_{j \in X_i} c_j \leqslant C$가 되어 X_i는 배낭문제의 가능해이다. 그래서

$$Value(y) \leqslant \max_{\text{가능해 } X_i \subseteq S} \left(\sum_{j \in X_i} v_j + OPT(C_i, V \setminus S) \right) + OPT(C, V)/(t-1).$$

우변의 첫 번째 항은 $OPT(C, V)$와 같으므로

$$Value(y) \leqslant (1 + \frac{1}{t-1}) OPT(C, V). \quad \square$$

참고 문헌

[1] A.R. Karlin, C. Mathieuy, and C.T. Nguyen, *Integrality Gaps of Linear and Semi-definite Programming Relaxations for Knapsack*, working paper.

[2] E. De Klerk, M. Laurent, *Error bounds for some semidefinite programming approaches to polynomial minimization on the hypercube*, SIAM Journal on Optimization, 20, 3104-3120, 2010.

[3] J. Nie and M. Schweighofer, *On the complexity of Putinar's Positivstellensatz*, Journal of Complexity, 23, 135-150, 2007.

[4] M.-J. Park and S.-P. Hong, *Rank of Handelman hierarchy for Max-Cut*, Operations Research Letters, in press.

[5] M. Schweighofer, *On the complexity of Schmüdgen's Positivstellensatz*, Journal of Complexity, 20, 529-543, 2004.