



CENTER FOR
MACHINE PERCEPTION



CZECH TECHNICAL
UNIVERSITY IN PRAGUE

MASTER'S THESIS

Semidefinite Programming for Geometric Problems in Computer Vision

Pavel Trutman

pavel.trutman@fel.cvut.cz

May 4, 2017

Available at
<http://cmp.felk.cvut.cz/~trutmpav/master-thesis/thesis/thesis.pdf>

Thesis Advisor: Ing. Tomáš Pajdla, PhD.

Center for Machine Perception, Department of Cybernetics
Faculty of Electrical Engineering, Czech Technical University
Technická 2, 166 27 Prague 6, Czech Republic
fax +420 2 2435 7385, phone +420 2 2435 7637, www: <http://cmp.felk.cvut.cz>

Acknowledgements

Author's declaration

I declare that I have work out the presented thesis independently and that I have listed all information sources used in accordance with the Methodical Guidelines about Maintaining Ethical Principles for Writing Academic Theses.

Prohlášení autora práce

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

V Praze dne

.....

Podpis autora práce

Abstract

Keywords:

Abstrakt

Keywords:

Contents

| | |
|---|-----------|
| 1. Introduction | 4 |
| 2. Semidefinite programming | 5 |
| 2.1. Preliminaries on semidefinite programs | 5 |
| 2.1.1. Symmetric matrices | 5 |
| 2.1.2. Semidefinite programs | 6 |
| 2.2. State of the art review | 7 |
| 2.3. Nesterov's approach | 8 |
| 2.3.1. Self-concordant functions | 8 |
| 2.3.2. Self-concordant barriers | 11 |
| 2.3.3. Barrier function for semidefinite programming | 15 |
| 2.4. Implementation details | 18 |
| 2.4.1. Package installation | 19 |
| 2.4.2. Usage | 20 |
| 2.5. Comparison with the state of the art methods | 22 |
| 2.5.1. Problem description | 22 |
| 2.5.2. Time measuring | 24 |
| 2.5.3. Results | 26 |
| 3. Optimization over polynomials | 27 |
| 3.1. State of the art review | 27 |
| 3.2. Algebraic preliminaries | 27 |
| 3.2.1. The polynomial ring, ideals and varieties | 27 |
| 3.2.2. Solving systems of polynomial equations by multiplication matrices | 29 |
| 3.3. Moment matrices | 29 |
| 3.4. Polynomial optimization | 29 |
| 3.5. Solving systems of polynomial equations | 29 |
| 4. Conclusion | 30 |
| A. Contents of the enclosed CD | 31 |
| Bibliography | 32 |

List of Figures

| | |
|--|----|
| 2.1. Example of a simple semidefinite problem for $y \in \mathbb{R}^2$. Boundary of the feasible set $\{y \mid F(y) \succeq 0\}$ is shown as a black curve. The minimal value of the objective function $b^\top y$ is attained at y^* | 7 |
| 2.2. Illustration of the logarithmic barrier function for different values of t . . | 17 |
| 2.3. Hyperbolic paraboloid $z = y_2^2 - y_1^2$ | 18 |
| 2.4. Illustration of the sets $\text{Dom } F(y)$ and $\{y \mid X(y) \succeq 0\}$ | 19 |
| 2.5. Graph of the semidefinite optimization problem stated in Example 2.6. . | 22 |
| 2.6. Graph of execution times based on the size of semidefinite problems solved by selected toolboxes. | 26 |

List of Tables

| | |
|--|----|
| 2.1. Execution times of different sizes of semidefinite problems solved by selected toolboxes. | 25 |
|--|----|

List of Algorithms

| | |
|---|----|
| 2.1. Newton method for minimization of self-concordant functions. | 10 |
| 2.2. Damped Newton method for analytic centers. | 13 |
| 2.3. Path following algorithm. | 15 |

List of Listings

| | |
|--|----|
| 2.1. Installation of the package Polyopt. | 20 |
| 2.2. Typical use of the class <code>SDPSolver</code> of the Polyopt package. | 20 |
| 2.3. Code for solving semidefinite problem stated in Example 2.6. | 23 |

List of Symbols and Abbreviations

| | |
|--|---|
| \mathbb{C} | Set of complex numbers. |
| $\text{cl}(S)$ | Closure of the set S . |
| $\deg(p)$ | Total degree of the polynomial p . |
| $\text{diag}(x)$ | Diagonal matrix with components of x on the diagonal. |
| $\text{dom } f$ | Domain of the function f . |
| $\text{Dom } f$ | $\text{cl}(\text{dom } f)$. |
| $f'(x)$ | First derivative of the function $f(x)$. |
| $f''(x)$ | Second derivative of the function $f(x)$. |
| $\mathcal{I}(V)$ | Vanishing ideal of the variety V . |
| \mathcal{I}^n | Identity matrix of size $n \times n$. |
| \sqrt{I} | Radical ideal of the ideal I . |
| $\sqrt[n]{I}$ | Real radical ideal of the ideal I . |
| $\langle f_1, f_2, \dots, f_n \rangle$ | Ideal generated by the polynomials f_1, f_2, \dots, f_n . |
| $\text{int } S$ | Interior of the set S . |
| $\{\lambda_i(A)\}_{i=1}^n$ | Set of all eigenvalues of the matrix $A \in \mathbb{R}^{n \times n}$. |
| LMI | Linear matrix inequality. |
| LP | Linear program. |
| \mathbb{N} | Set of natural numbers (including zero). |
| $\mathcal{N}_{\mathcal{B}}(f)$ | Normal form of the polynomial f modulo ideal I with respect to the basis \mathcal{B} . |
| \mathcal{P}^n | Cone of positive semidefinite $n \times n$ matrices. |
| QCQP | Quadratically constrained quadratic program. |
| \mathbb{R} | Set of real numbers. |
| $\mathbb{R}[x]$ | Ring of polynomials with coefficients in \mathbb{R} in n variables $x \in \mathbb{R}^n$. |
| \mathcal{S}^n | Space of $n \times n$ real symmetric matrices. |
| SDP | Semidefinite programming. |
| $\text{tr}(A)$ | Trace of the matrix A . |
| $V_{\mathbb{C}}(I)$ | Algebraic variety of the ideal I . |
| $V_{\mathbb{R}}(I)$ | Real algebraic variety of the ideal I . |
| $x^{(i)}$ | i -th element of the vector x . |
| x^{\top} | Transpose of the vector x . |
| \mathcal{X}_f | Multiplication matrix by the polynomial f . |
| \mathbb{Z} | Set of integers. |

1. Introduction

2. Semidefinite programming

The goal of the semidefinite programming (SDP) is to optimize a linear function on a given set, which is an intersection of a cone of positive semidefinite matrices with an affine space. This set is called a spectrahedron and it is a convex set. As in SDP we are optimizing a convex function on a convex set, SDP is a special case of convex optimization.

Since SDP can be solved efficiently in polynomial time using interior-point methods, it has many applications in practise. For example, any linear program (LP) and quadratically constrained quadratic program (QCQP) can be written as a semidefinite program. However, this may be not the best idea to do as more efficient algorithms exist for solving LPs and QCQPs. On the other hand, there exist many useful applications of SDP, e.g. many NP-complete problems in combinatorial optimization can be approximated by semidefinite programs. One of the combinatorial problem worth mentioning is the MAX CUT problem (one of the Karp's original NP-complete problems [7]), for which M. Goemans and D. P. Williamson created the first approximation algorithm based on SDP [5]. Also in control theory, there are many problems based on linear matrix inequalities, which are solvable by SDP.

Special application of SDP comes from polynomial optimization since global solution of polynomial optimization problems can be found by hierarchies of semidefinite programs. Also systems of polynomial equations can be solved by hierarchies of semidefinite problems. This approach has the advantage that there exists a method, which allows us to compute real solutions only. Since in many applications, we are not interested in complex solutions, this method may be the right tool for polynomial systems solving. We will focus in details on SDP application on polynomial optimization and polynomial systems solving in Chapter 3.

2.1. Preliminaries on semidefinite programs

In this section, we introduce some notation and preliminaries about symmetric matrices and semidefinite programs. We will introduce further notation and preliminaries later on in the text when needed.

At the beginning, let us denote the inner product for two vectors $x, y \in \mathbb{R}^n$

$$\langle x, y \rangle = \sum_{i=1}^n x^{(i)} y^{(i)} \quad (2.1)$$

and the Frobenius inner product for two matrices $X, Y \in \mathbb{R}^{n \times m}$.

$$\langle X, Y \rangle = \sum_{i=1}^n \sum_{j=1}^m X^{(i,j)} Y^{(i,j)} \quad (2.2)$$

2.1.1. Symmetric matrices

Let \mathcal{S}^n denotes the space of $n \times n$ real symmetric matrices.

For a matrix $M \in \mathcal{S}^n$, the notation $M \succeq 0$ means that M is positive semidefinite. $M \succeq 0$ if and only if any of the following equivalent properties holds.

2. Semidefinite programming

1. $x^\top Mx \geq 0$ for all $x \in \mathbb{R}^n$.
2. All eigenvalues of M are nonnegative.

The set of all positive semidefinite matrices is a cone. We will denote it as \mathcal{P}^n and it is called a cone of positive semidefinite matrices.

For a matrix $M \in \mathcal{S}^n$, the notation $M \succ 0$ means that M is positive definite. $M \succ 0$ if and only if any of the following equivalent properties holds.

1. $M \succeq 0$ and $\text{rank } M = n$.
2. $x^\top Mx > 0$ for all $x \in \mathbb{R}^n$.
3. All eigenvalues of M are positive.

2.1.2. Semidefinite programs

The standard (primal) form of a semidefinite program in variable $X \in \mathcal{S}^n$ is defined as follows:

$$\begin{aligned} p^* &= \sup_{X \in \mathcal{S}^n} \langle C, X \rangle \\ \text{s.t.} \quad &\langle A_i, X \rangle = b^{(i)} \quad (i = 1, \dots, m) \\ &X \succeq 0 \end{aligned} \tag{2.3}$$

where $C, A_1, \dots, A_m \in \mathcal{S}^n$ and $b \in \mathbb{R}^m$ are given.

The dual form of the primal form is the following program in variable $y \in \mathbb{R}^m$.

$$\begin{aligned} d^* &= \inf_{y \in \mathbb{R}^m} b^\top y \\ \text{s.t.} \quad &\sum_{i=1}^m A_i y^{(i)} - C \succeq 0 \end{aligned} \tag{2.4}$$

The constraint

$$F(y) = \sum_{i=1}^m A_i y^{(i)} - C \succeq 0 \tag{2.5}$$

of the problem (2.4) is called a linear matrix inequality (LMI) in the variable y . The feasible region defined by LMI is called a spectrahedron. It can be shown, that this constraint is convex since if $F(x) \succeq 0$ and $F(y) \succeq 0$, then $\forall \alpha : 0 \leq \alpha \leq 1$ holds

$$F(\alpha x + (1 - \alpha)y) = \alpha F(x) + (1 - \alpha)F(y) \succeq 0. \tag{2.6}$$

The objective function of the problem (2.4) is linear, and therefore convex too. Because the semidefinite program (2.4) has convex objective function and convex constraint, it is a convex optimization problem and can be solved by standard convex optimization methods. To get a general picture, how a simple semidefinite problem may look like, see Figure 2.1.

The optimal solution y^* of any semidefinite program lies on the boundary of the feasible set, supposing the problem is feasible and the solution exists. The boundary of the feasible set is not smooth in general, but it is piecewise smooth as each piece is an algebraic surface.

Example 2.1 (Linear programming). Semidefinite programming can be seen as an extension to the linear programming since the componentwise inequalities between

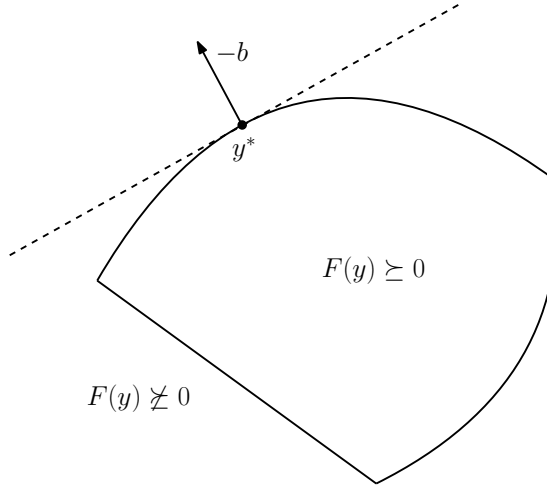


Figure 2.1. Example of a simple semidefinite problem for $y \in \mathbb{R}^2$. Boundary of the feasible set $\{y \mid F(y) \succeq 0\}$ is shown as a black curve. The minimal value of the objective function $b^\top y$ is attained at y^* .

vectors in linear programming can be replaced by LMI. Consider a linear program in a standard form

$$\begin{aligned} y^* &= \arg \min_{y \in \mathbb{R}^m} b^\top y \\ \text{s.t.} \quad & Ay - c \geq 0 \end{aligned} \quad (2.7)$$

with $b \in \mathbb{R}^m$, $c \in \mathbb{R}^n$ and $A = [a_1 \ \cdots \ a_m] \in \mathbb{R}^{n \times m}$. This program can be transformed into the semidefinite program (2.4) by assigning

$$C = \text{diag}(c), \quad (2.8)$$

$$A_i = \text{diag}(a_i). \quad (2.9)$$

2.2. State of the art review

An early paper by R. Bellman and K. Fan about theoretical properties of semidefinite programs [2] was issued in 1963. Later on, many researchers worked on the problem of minimizing the maximal eigenvalue of a symmetric matrix, which can be done by solving a semidefinite program. Selecting a few from many: J. Cullum, W. Donath, P. Wolfe [4], M. Overton [14] and G. Pataki [15]. In 1984, the interior-point methods for LPs solving were introduced by N. Karmarkar [6]. It was the first reasonably efficient algorithm that solves LPs in polynomial time with excellent behavior in practise. The interior-point algorithms were then extended to be able to solve convex quadratic programs.

In 1988, Y. Nesterov and A. Nemirovski [12] did an important breakthrough. They showed that interior-point methods developed for LPs solving can be generalized to all convex optimization problems. All that is required, is the knowledge of a self-concordant barrier function for the feasible set of the problem. Y. Nesterov and A. Nemirovski have shown that a self-concordant barrier function exists for every convex set. However, their proposed universal self-concordant barrier function and its first and second derivatives are not easily computable. Fortunately for SDP, which is an important class of convex optimization programs, computable self-concordant barrier functions are known, and therefore the interior-point methods can be used.

2. Semidefinite programming

Nowadays, there are many libraries and toolboxes that one can use for solving semidefinite programs. They differ to each other in used methods and their implementations. Before starting solving a problem, one should know the details of the problem to solve and choose the library accordingly to it as not every method and its implementation is suitable for the given problem.

Most methods are based on interior-point methods, which are efficient and robust for general semidefinite programs. The main disadvantage of these methods is that they need to store and factorize usually large Hessian matrix. Most modern implementations of the interior-point methods do not need the knowledge of an interior feasible point in advance. SeDuMi [16] casts the standard semidefinite program into the homogeneous self-dual form, which has a trivial feasible point. SDPA [19] uses an infeasible interior-point method, which can be initialized by an infeasible point. Some of the libraries (e.g. MOSEK [10]) have started out as LPs solvers and were extended for QCQPs solving and convex optimization later on.

Another type of methods used in SDP are the first-order methods. They avoid storing and factorizing Hessian matrices, and therefore they are able to solve much larger problems than interior-point methods, but at some cost in accuracy. This method is implemented, for instance, in the SCS solver [13].

2.3. Nesterov's approach

In this section, we will follow Chapter 4 of [11] by Y. Nesterov, which is devoted to the convex optimization problems. This chapter describes the state of the art interior-point methods for solving convex optimization problems. We will extract from it the only minimum, just to be able to introduce an algorithm for semidefinite programs solving. We will present some basic definitions and theorems, but we will not prove them. For the proofs and more details look into [11].

2.3.1. Self-concordant functions

Definition 2.1 (Self-concordant function in \mathbb{R}). A closed convex function $f : \mathbb{R} \mapsto \mathbb{R}$ is self-concordant if there exist a constant $M_f \geq 0$ such that the inequality

$$|f'''(x)| \leq M_f f''(x)^{3/2} \quad (2.10)$$

holds for all $x \in \text{dom } f$.

For better understanding of self-concordant functions, we provide several examples.

Example 2.2.

1. Linear and convex quadratic functions.

$$f'''(x) = 0 \text{ for all } x \quad (2.11)$$

Linear and convex quadratic functions are self-concordant with constant $M_f = 0$.

2. Negative logarithms.

$$f(x) = -\ln(x) \text{ for } x > 0 \quad (2.12)$$

$$f'(x) = -\frac{1}{x} \quad (2.13)$$

$$f''(x) = \frac{1}{x^2} \quad (2.14)$$

$$f'''(x) = -\frac{2}{x^3} \quad (2.15)$$

$$\frac{|f'''(x)|}{f''(x)^{3/2}} = 2 \quad (2.16)$$

Negative logarithms are self-concordant functions with constant $M_f = 2$.

3. Exponential functions.

$$f(x) = e^x \quad (2.17)$$

$$f''(x) = f'''(x) = e^x \quad (2.18)$$

$$\frac{|f'''(x)|}{f''(x)^{3/2}} = e^{-x/2} \rightarrow +\infty \text{ as } x \rightarrow -\infty \quad (2.19)$$

Exponential functions are not self-concordant functions.

Definition 2.2 (Self-concordant function in \mathbb{R}^n). A closed convex function $f : \mathbb{R}^n \mapsto \mathbb{R}$ is self-concordant if function $g : \mathbb{R} \mapsto \mathbb{R}$

$$g(t) = f(x + tv) \quad (2.20)$$

is self-concordant for all $x \in \text{dom } f$ and all $v \in \mathbb{R}^n$.

Now, let us focus on the main properties of self-concordant functions.

Theorem 2.1. Let functions f_i be self-concordant with constants M_i and let $\alpha_i > 0$, $i = 1, 2$. Then the function

$$f(x) = \alpha_1 f_1(x) + \alpha_2 f_2(x) \quad (2.21)$$

is self-concordant with constant

$$M_f = \max \left\{ \frac{1}{\sqrt{\alpha_1}} M_1, \frac{1}{\sqrt{\alpha_2}} M_2 \right\} \quad (2.22)$$

and

$$\text{dom } f = \text{dom } f_1 \cap \text{dom } f_2. \quad (2.23)$$

Corollary 2.1. Let function f be self-concordant with some constant M_f and $\alpha > 0$. Then the function $\phi(x) = \alpha f(x)$ is also self-concordant with the constant $M_\phi = \frac{1}{\sqrt{\alpha}} M_f$.

We call function $f(x)$ as the standard self-concordant function if $f(x)$ is some self-concordant function with the constant $M_f = 2$. Using Corollary 2.1, we can see that any self-concordant function can be transformed into the standard self-concordant function by scaling.

Theorem 2.2. Let function f be self-concordant. If $\text{dom } f$ contains no straight line, then the Hessian $f''(x)$ is nondegenerate at any x from $\text{dom } f$.

2. Semidefinite programming

For some self-concordant function $f(x)$, for which we assume, that $\text{dom } f$ contains no straight line (which implies that all $f''(x)$ are nondegenerate, see Theorem 2.2), we denote two local norms as

$$\|u\|_x = \sqrt{u^\top f''(x)u} \quad (2.24)$$

$$\|u\|_x^* = \sqrt{u^\top f''(x)^{-1}u}. \quad (2.25)$$

Consider following minimization problem

$$x^* = \arg \min_{x \in \text{dom } f} f(x) \quad (2.26)$$

as the minimization of the self-concordant function $f(x)$. Algorithm 2.1 is describing the iterative process of solving the optimization problem (2.26). The algorithm is divided into two stages by the value of $\|f'(x_k)\|_{x_k}^*$. The splitting parameter β guarantees quadratic convergence rate for the second part of the algorithm. The parameter β is chosen from interval $(0, \bar{\lambda})$, where

$$\bar{\lambda} = \frac{3 - \sqrt{5}}{2}, \quad (2.27)$$

which is a root of the equation

$$\frac{\lambda}{(1 - \lambda)^2} = 1. \quad (2.28)$$

Algorithm 2.1. Newton method for minimization of self-concordant functions.

Input:

- f a self-concordant function to minimize
- $x_0 \in \text{dom } f$ a starting point
- $\beta \in (0, \bar{\lambda})$ a parameter of size of the region of quadratic convergence
- ε a precision

Output:

- x^* an optimal solution to the minimization problem (2.26)

```

1:  $k \leftarrow 0$ 
2: while  $\|f'(x_k)\|_{x_k}^* \geq \beta$  do
3:    $x_{k+1} \leftarrow x_k - \frac{1}{1 + \|f'(x_k)\|_{x_k}^*} f''(x_k)^{-1} f'(x_k)$ 
4:    $k \leftarrow k + 1$ 
5: end while
6: while  $\|f'(x_k)\|_{x_k}^* > \varepsilon$  do
7:    $x_{k+1} \leftarrow x_k - f''(x_k)^{-1} f'(x_k)$ 
8:    $k \leftarrow k + 1$ 
9: end while
10: return  $x^* \leftarrow x_k$ 

```

The first while loop (lines 2 – 5) represents damped Newton method, where at each iteration we have

$$f(x_k) - f(x_{k+1}) \geq \beta - \ln(1 + \beta) \text{ for } k \geq 0, \quad (2.29)$$

where

$$\beta - \ln(1 + \beta) > 0 \text{ for } \beta > 0, \quad (2.30)$$

and therefore the global convergence of the algorithm is ensured. It can be shown that the local convergence rate of the damped Newton method is also quadratic, but the presented switching strategy is preferred as it gives better complexity bounds.

The second while loop of the algorithm (lines 6 – 9) is the standard Newton method with quadratic convergence rate.

The algorithm terminates when the required precision ε is reached.

2.3.2. Self-concordant barriers

To be able to introduce self-concordant barriers, let us denote $\text{Dom } f = \text{cl}(\text{dom } f)$.

Definition 2.3 (Self-concordant barrier). Let $F(x)$ be a standard self-concordant function. We call it a ν -self-concordant barrier for set $\text{Dom } F$, if

$$\sup_{u \in \mathbb{R}^n} (2u^\top F'(x) - u^\top F''(x)u) \leq \nu \quad (2.31)$$

for all $x \in \text{dom } F$. The value ν is called the parameter of the barrier.

The inequality (2.31) can be rewritten into the following equivalent matrix notation:

$$F''(x) \succeq \frac{1}{\nu} F'(x) F'(x)^\top. \quad (2.32)$$

In Definition 2.3, the hessian $F''(x)$ is not required to be nondegenerate. However, in case that $F''(x)$ is nondegenerate, the inequality (2.31) is equivalent to

$$F'^\top(x) F''(x)^{-1} F'(x) \leq \nu. \quad (2.33)$$

Let us explore, which basic functions are self-concordant barriers.

Example 2.3.

1. Linear functions.

$$F(x) = \alpha + a^\top x, \text{ dom } F = \mathbb{R}^n \quad (2.34)$$

$$F''(x) = 0 \quad (2.35)$$

From (2.32) and for $a \neq 0$ follows, that linear functions are not self-concordant barriers.

2. Convex quadratic functions.

For $A = A^\top \succ 0$:

$$F(x) = \alpha + a^\top x + \frac{1}{2} x^\top A x, \text{ dom } F = \mathbb{R}^n \quad (2.36)$$

$$F'(x) = a + A x \quad (2.37)$$

$$F''(x) = A \quad (2.38)$$

After substitution into (2.33) we obtain

$$(a + A x)^\top A^{-1} (a + A x) = a^\top A^{-1} a + 2a^\top x + x^\top A x, \quad (2.39)$$

which is unbounded from above on \mathbb{R}^n . Therefore, quadratic functions are not self-concordant barriers.

2. Semidefinite programming

3. Logarithmic barrier for a ray.

$$F(x) = -\ln x, \text{ dom } F = \{x \in \mathbb{R} \mid x > 0\} \quad (2.40)$$

$$F'(x) = -\frac{1}{x} \quad (2.41)$$

$$F''(x) = \frac{1}{x^2} \quad (2.42)$$

From (2.33), when $F'(x)$ and $F''(x)$ are both scalars, we get

$$\frac{F'(x)^2}{F''(x)} = \frac{x^2}{x^2} = 1. \quad (2.43)$$

Therefore, the logarithmic barrier for a ray is a self-concordant barrier with parameter $\nu = 1$ on domain $\{x \in \mathbb{R} \mid x > 0\}$.

Now, let us focus on the main properties of self-concordant barriers.

Theorem 2.3. Let $F(x)$ be a self-concordant barrier. Then the function $c^\top x + F(x)$ is a self-concordant function on $\text{dom } F$.

Theorem 2.4. Let F_i be ν_i -self-concordant barriers, $i = 1, 2$. Then the function

$$F(x) = F_1(x) + F_2(x) \quad (2.44)$$

is a self-concordant barrier for convex set

$$\text{Dom } F = \text{Dom } F_1 \cap \text{Dom } F_2 \quad (2.45)$$

with the parameter

$$\nu = \nu_1 + \nu_2. \quad (2.46)$$

Theorem 2.5. Let $F(x)$ be a ν -self-concordant barrier. Then for any $x \in \text{Dom } F$ and $y \in \text{Dom } F$ such that

$$(y - x)^\top F'(x) \geq 0, \quad (2.47)$$

we have

$$\|y - x\|_x \leq \nu + 2\sqrt{\nu}. \quad (2.48)$$

There is one special point of convex set, which is important for solving convex minimization problem. It is called the analytic center of convex set and we will focus on its properties.

Definition 2.4. Let $F(x)$ be a ν -self-concordant barrier for the set $\text{Dom } F$. The point

$$x_F^* = \arg \min_{x \in \text{Dom } F} F(x) \quad (2.49)$$

is called the analytic center of convex set $\text{Dom } F$, generated by the barrier $F(x)$.

Theorem 2.6. Assume that the analytic center of a ν -self-concordant barrier $F(x)$ exists. Then for any $x \in \text{Dom } F$ we have

$$\|x - x_F^*\|_{x_F^*} \leq \nu + 2\sqrt{\nu}. \quad (2.50)$$

This property clearly follows from Theorem 2.5 and the fact, that $F'(x_F^*) = 0$.

Thus, if $\text{Dom } F$ contains no straight line, then the existence of x_F^* (which leads to nondegenerate $F''(x_F^*)$) implies, that the set $\text{Dom } F$ is bounded.

Now, we describe the algorithm and its properties for obtaining an approximation to the analytic center. To find the analytic center, we need to solve the minimization problem (2.49). For that, we will use the standard implementation of the damped Newton method with termination condition

$$\|F'(x_k)\|_{x_k}^* \leq \beta, \text{ for } \beta \in (0, 1). \quad (2.51)$$

The pseudocode of the whole minimization process is shown in Algorithm 2.2.

Algorithm 2.2. Damped Newton method for analytic centers.

Input:

F a ν -self-concordant barrier

$x_0 \in \text{Dom } F$ a starting point

$\beta \in (0, 1)$ a centering parameter

Output:

x_F^* an approximation of the analytic center of the set $\text{Dom } F$

```

1:  $k \leftarrow 0$ 
2: while  $\|F'(x_k)\|_{x_k}^* > \beta$  do
3:    $x_{k+1} \leftarrow x_k - \frac{1}{1 + \|F'(x_k)\|_{x_k}^*} F''(x_k)^{-1} F'(x_k)$ 
4:    $k \leftarrow k + 1$ 
5: end while
6: return  $x_F^* \leftarrow x_k$ 

```

Theorem 2.7. Algorithm 2.2 terminates no later than after N steps, where

$$N = \frac{1}{\beta - \ln(1 + \beta)} (F(x_0) - F(x_F^*)). \quad (2.52)$$

The knowledge of analytic center allows us to solve the standard minimization problem

$$x^* = \arg \min_{x \in Q} c^\top x \quad (2.53)$$

with bounded closed convex set $Q \equiv \text{Dom } F$, which has nonempty interior, and which is endowed with a ν -self-concordant barrier $F(x)$. Denote

$$f(t, x) = tc^\top x + F(x), \text{ for } t \geq 0 \quad (2.54)$$

as a parametric penalty function. Using Theorem 2.3 we can see, that $f(t, x)$ is self-concordant in x . Let us introduce new minimization problem using the parametric penalty function $f(t, x)$

$$x^*(t) = \arg \min_{x \in \text{dom } F} f(t, x). \quad (2.55)$$

This trajectory is called the central path of the problem (2.53). We will reach the solution $x^*(t) \rightarrow x^*$ as $t \rightarrow +\infty$. Moreover, since the set Q is bounded, the analytic center x_F^* of this set exists and

$$x^*(0) = x_F^*. \quad (2.56)$$

2. Semidefinite programming

From the first-order optimality condition, any point of the central path satisfies equation

$$tc + F'(x^*(t)) = 0 \quad (2.57)$$

Since the analytic center lies on the central path and can be found by Algorithm 2.2, all we have to do, to find the solution x^* , is to follow the central path. This enables us an approximate centering condition:

$$\|f'(t, x)\|_x^* = \|tc + F'(x)\|_x^* \leq \beta, \quad (2.58)$$

where the centering parameter β is small enough.

Assuming $x \in \text{dom } F$, one iteration of the path-following algorithm consists of two steps:

$$t_+ = t + \frac{\gamma}{\|c\|_x^*}, \quad (2.59)$$

$$x_+ = x - F''(x)^{-1}(t_+c + F'(x)). \quad (2.60)$$

Theorem 2.8. Let x satisfy the approximate centering condition (2.58)

$$\|tc + F'(x)\|_x^* \leq \beta \quad (2.61)$$

with $\beta < \bar{\lambda} = \frac{3-\sqrt{5}}{2}$. Then for γ , such that

$$|\gamma| \leq \frac{\sqrt{\beta}}{1 + \sqrt{\beta}} - \beta, \quad (2.62)$$

we have again

$$\|t_+c + F'(x_+)\|_{x_+}^* \leq \beta. \quad (2.63)$$

This theorem ensures the correctness of the presented iteration of the path-following algorithm. For the whole description of the path-following algorithm please see Algorithm 2.3.

Theorem 2.9. Algorithm 2.3 terminates no more than after N steps, where

$$N \leq \mathcal{O}\left(\sqrt{\nu} \ln \frac{\nu \|c\|_{x_F}^*}{\varepsilon}\right). \quad (2.64)$$

The parameters β and γ in Algorithm 2.2 and Algorithm 2.3 can be fixed. The reasonable values are:

$$\beta = \frac{1}{9}, \quad (2.65)$$

$$\gamma = \frac{\sqrt{\beta}}{1 + \sqrt{\beta}} - \beta = \frac{5}{36}. \quad (2.66)$$

The union of Algorithm 2.2 and Algorithm 2.3 can be easily used to solve the standard minimization problem (2.53), supposing we have a feasible point $x_0 \in Q$.

Algorithm 2.3. Path following algorithm.

Input: F a ν -self-concordant barrier $x_0 \in \text{dom } F$ a starting point satisfying $\|F'(x_0)\|_{x_0}^* \leq \beta$, e.g. the analytic center x_F^* of the set $\text{Dom } F$ $\beta \in (0, 1)$ a centering parameter γ a parameter satisfying $|\gamma| \leq \frac{\sqrt{\beta}}{1+\sqrt{\beta}} - \beta$ $\varepsilon > 0$ an accuracy**Output:** x^* an optimal solution to the minimization problem (2.53)

```

1:  $t_0 \leftarrow 0$ 
2:  $k \leftarrow 0$ 
3: while  $\varepsilon t_k < \nu + \frac{(\beta + \sqrt{\nu})\beta}{1-\beta}$  do
4:    $t_{k+1} \leftarrow t_k + \frac{\gamma}{\|c\|_{x_k}^*}$ 
5:    $x_{k+1} \leftarrow x_k - F''(x_k)^{-1}(t_{k+1}c + F'(x_k))$ 
6:    $k \leftarrow k + 1$ 
7: end while
8: return  $x^* \leftarrow x_k$ 

```

2.3.3. Barrier function for semidefinite programming

In this section, we are going to show, how to find a self-concordant barrier for the semidefinite program (2.4), so that we can use Algorithm 2.2 and Algorithm 2.3 to solve it. For the purpose of this section, we are interested only in the constraints of the problem. The constraints are defining us the feasibility set Q :

$$Q = \left\{ y \in \mathbb{R}^m \mid A_0 + \sum_{i=1}^m A_i y^{(i)} \succeq 0 \right\}, \quad (2.67)$$

where $A_0, \dots, A_m \in \mathcal{S}^n$. Let us denote $X(y) = A_0 + \sum_{i=1}^m A_i y^{(i)}$. If the matrix $X(y)$ is block diagonal

$$X(y) = \begin{bmatrix} X_1(y) & 0 & \cdots & 0 \\ 0 & X_2(y) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & X_k(y) \end{bmatrix} \quad (2.68)$$

with $X_j(y) \in \mathcal{S}^{n_j}$ for $j = 1, \dots, k$ and $\sum_{j=1}^k n_j = n$, then the feasibility set Q can be expressed as

$$Q = \{ y \in \mathbb{R}^m \mid X_j(y) \succeq 0, j = 1, \dots, k \}. \quad (2.69)$$

This rule allows us to easily add or remove some constraints without touching the others and to keep the sizes of the used matrices small, which can significantly speed up the computation.

Instead of the set Q , which is parametrized by y , we can directly optimize over the set of positive semidefinite matrices. This set \mathcal{P}^n is defined as

$$\mathcal{P}^n = \{ X \in \mathcal{S}^n \mid X \succeq 0 \} \quad (2.70)$$

2. Semidefinite programming

and it is called the cone of positive semidefinite $n \times n$ matrices. This cone is a closed convex set, which interior is formed by positive definite matrices and on its boundary lie matrices, which have at least one eigenvalue equal to zero.

Now, we are looking for a self-concordant barrier function, which will enable us to optimize over the cone \mathcal{P}^n . The domain of this function needs to contain the set \mathcal{P}^n and the values of the function have to be growing to $+\infty$ as we are getting closer to the boundary of the set \mathcal{P}^n . This will create us a repelling force from the boundary of \mathcal{P}^n , when following the central path (2.55). Consider the function $F(X)$ as the self-concordant barrier function for the set \mathcal{P}^n :

$$F(X) = -\ln \prod_{i=1}^n \lambda_i(X), \quad (2.71)$$

where $X \in \text{int } \mathcal{P}^n$ and $\{\lambda_i(X)\}_{i=1}^n$ is the set of eigenvalues of the matrix X . To avoid the computation of eigenvalues, the function $F(X)$ can be also expressed as:

$$F(X) = -\ln \det(X). \quad (2.72)$$

Theorem 2.10. Function $F(X)$ is an n -self-concordant barrier for \mathcal{P}^n .

Example 2.4. Consider one-dimensional problem with linear constraint $x \geq 0$. Then, the set Q is

$$Q = \{x \in \mathbb{R} \mid x \geq 0\} \quad (2.73)$$

and one of the barrier functions for this set Q is

$$F(x) = -\ln(x). \quad (2.74)$$

Then, when following the central path (2.55), the function $F(x)$ allows us to reach the boundary of Q as t grows to $+\infty$. This situation is showed in Figure 2.2 for different values of t .

Note, that $\text{Dom } F \supseteq \mathcal{P}^n$ because $\det(X) \geq 0$ when the number of negative eigenvalues of X is even. Therefore, the set $\text{Dom } F$ is made by disjoint subsets, which one of them is \mathcal{P}^n . As Algorithm 2.2 and Algorithm 2.3 are interior point algorithms, when the starting point is from $\text{int } \mathcal{P}^n$, then we never leave \mathcal{P}^n during the execution of the algorithms and the optimal solution is found.

Similarly, the self-concordant barrier function for the set Q is a function

$$F(y) = -\ln \det(X(y)). \quad (2.75)$$

Example 2.5. To make it clearer, what is the difference between the set Q and $\text{Dom } F(y)$, we have prepared this example. Let

$$X(y) = \begin{bmatrix} y_2 & y_1 \\ y_1 & y_2 \end{bmatrix}, \quad (2.76)$$

where $y = [y_1 \ y_2]^\top$. The equation

$$z = \det(X(y)) = y_2^2 - y_1^2 \quad (2.77)$$

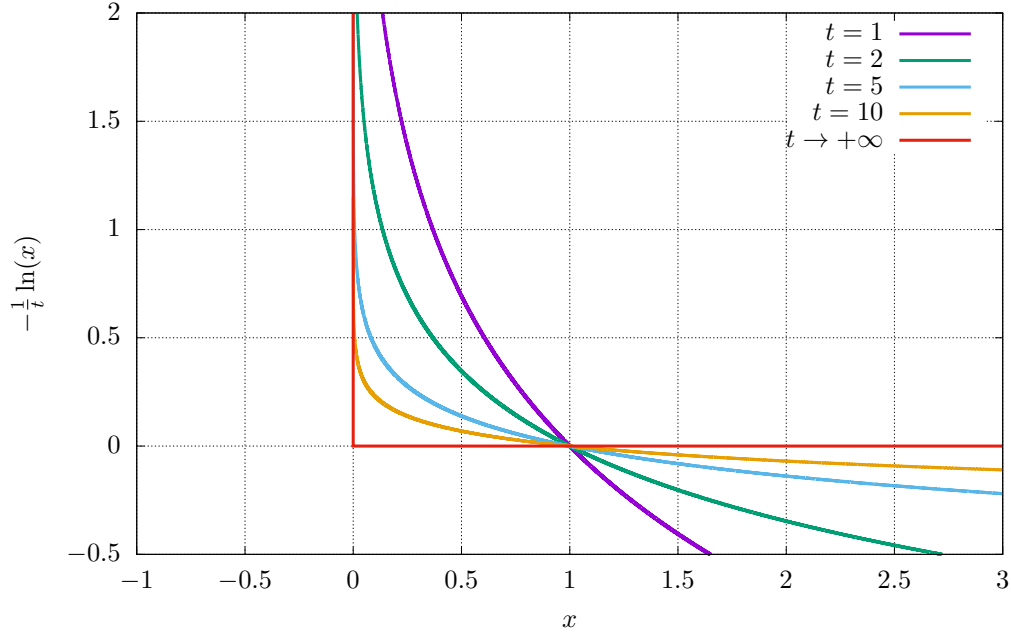


Figure 2.2. Illustration of the logarithmic barrier function for different values of t .

represents a hyperbolic paraboloid, which you can see in Figure 2.3. Therefore, the equation $z = 0$ is a slice of it, denoted by the purple color in Figure 2.4. The domain of the self-concordant barrier function is

$$\text{Dom } F(y) = \{y \mid \det(X(y)) \geq 0\} \quad (2.78)$$

and is shaded by the blue color. We can see, that the set $\text{Dom } F(y)$ consists of two disjoint parts. One of them is the set, where $X(y) \succeq 0$ (denoted by the orange color) and the second part is an area, where both eigenvalues of $X(y)$ are negative. Therefore, one has to pick his starting point x_0 from the interior of the set $Q = \{y \in \mathbb{R}^2 \mid X(y) \succeq 0\}$ to obtain the optimal solution from the set Q .

When the matrix X has the block diagonal form (2.68), we can rewrite the barrier function (2.75) into summation form

$$F(y) = - \sum_{j=1}^k \ln \det(X_j(y)). \quad (2.79)$$

For the purposes of Algorithm 2.2 and Algorithm 2.3, we need the first and the second partial derivatives of this function. Let us denote $X_j(y) = A_{j,0} + \sum_{i=1}^m A_{j,i} y^{(i)}$ for $j = 1, \dots, k$, then the derivatives are:

$$\frac{\partial F}{\partial y^{(u)}}(y) = - \sum_{j=1}^k \text{tr}(X_j(y)^{-1} A_{j,u}), \quad (2.80)$$

$$\frac{\partial^2 F}{\partial y^{(u)} \partial y^{(v)}}(y) = \sum_{j=1}^k \text{tr}\left((X_j(y)^{-1} A_{j,u})(X_j(y)^{-1} A_{j,v})\right), \quad (2.81)$$

for $u, v = 1, \dots, m$.

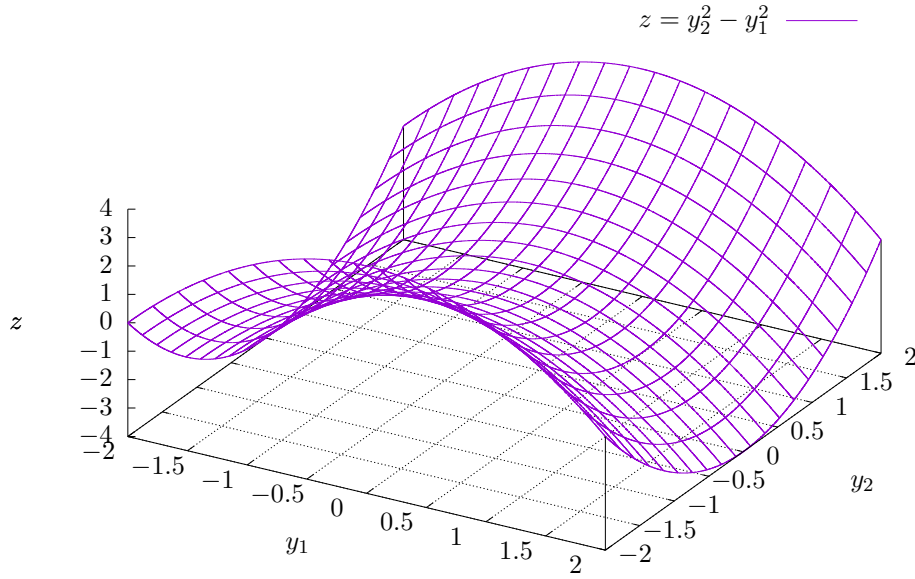


Figure 2.3. Hyperbolic paraboloid $z = y_2^2 - y_1^2$.

The computation of the derivatives is the most expensive part of each step of Algorithm 2.2 and Algorithm 2.3. Therefore, the estimated number of arithmetic operations of computation of the derivatives is also the complexity of each step in the algorithms. The number of arithmetic operations for j -th constraint in form $\{y \mid X_j(y) \succeq 0\}$ is:

- the computation of $X_j(y) = A_{j,0} + \sum_{i=1}^m A_{j,i}y^{(i)}$ needs mn^2 operations,
- the computation of the inversion $X_j(y)^{-1}$ needs n^3 operations,
- to compute all matrices $X_j(y)^{-1}A_{j,u}$ for $u = 1, \dots, m$ is needed mn^3 operations,
- to compute $\text{tr}(X_j(y)^{-1}A_{j,u})$ for $u = 1, \dots, m$ is needed mn operations,
- the computation of $\text{tr}\left((X_j(y)^{-1}A_{j,u})(X_j(y)^{-1}A_{j,v})\right)$ for $u, v = 1, \dots, m$ needs m^2n^2 operations.

The most expensive parts requires mn^3 and m^2n^2 arithmetic operations on each constraint. Typically, the value k , the number of constraints, is small and it keeps constant, when the semidefinite programs are generated as subproblems, when solving more complex problems, e.g. polynomial optimization. Therefore, we can say, that k is constant and we can omit it from the complexity estimation. To sum up, one step of Algorithm 2.2 and Algorithm 2.3 requires

$$\mathcal{O}(m(m+n)n^2) \tag{2.82}$$

arithmetic operations.

2.4. Implementation details

To be able to study the algorithms described previously in this section, we have implemented them in the programming language Python [17]. The full knowledge of

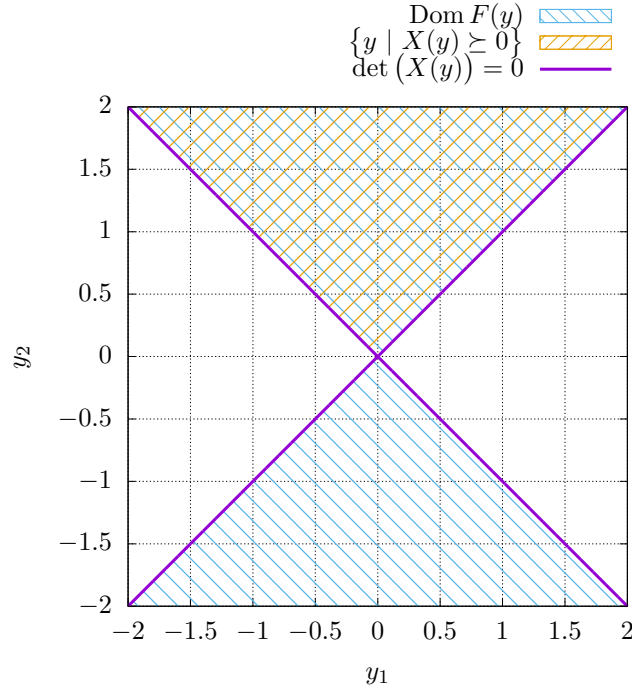


Figure 2.4. Illustration of the sets $\text{Dom } F(y)$ and $\{y \mid X(y) \succeq 0\}$.

the code allows us to trace the algorithms step by step and inspect their behaviors. Instead of using some state of the art toolboxes for semidefinite programming, e.g. SeDuMi [16] and MOSEK [10], which are more or less black boxes for us, the knowledge of the used algorithms allows us to decide, if the chosen algorithm is suitable for the given semidefinite problem or not. Moreover, if we would like to create some specialized solver for some class of semidefinite problems, we can easily reuse the code, edit it as required and build the solver very quickly. On the other hand, we can not expect that our implementation will be as fast as the implementation of some state of the art toolboxes, as much more time and people was used to develop them.

The implementation is compatible with Python version 3.5 and higher. The package NumPy is used for linear algebra computations. Please refer to the installation guide of NumPy for your system to ensure, that it is correctly set to use the linear algebra libraries, e.g. LAPACK [1], ATLAS [18] and BLAS [8]. The incorrect setting of these libraries causes significant drop of the performance. Other Python packages are required as well, e.g. SymPy and SciPy, but their settings are not so crucial for the performance of this implementation.

2.4.1. Package installation

The package with implementation of Algorithm 2.2 and Algorithm 2.3 is named Polyopt, as the semidefinite programming part of this package is only a tool, which is used for polynomial optimization and polynomial systems solving, which will be described in Chapter 3. The newest version of the package is available at <http://cmp.felk.cvut.cz/~trutmpav/master-thesis/polyopt/>. To install the package on your system, you have to clone and checkout the Git repository with the source codes of the package. To install other packages that are required, the preferred way is to use the

2. Semidefinite programming

`pip`¹ installer. The required packages are listed in the `requirements.txt` file. Then, install the package using the script `setup.py`. For the exact commands for the whole installation process please see Listing 2.1.

Listing 2.1. Installation of the package Polyopt.

```
1: git clone https://github.com/PavelTrutman/polyopt.git
2: cd polyopt
3: pip3 install -r requirements.txt
4: python3 setup.py install
```

To check, whether the installation was successful, run command `python3 setup.py test`, which will execute the predefined tests. If no error emerges, then the package is installed and ready to use.

2.4.2. Usage

The Polyopt package is created to be able to solve semidefinite programs in a form

$$\begin{aligned} y^* &= \arg \min_{y \in \mathbb{R}^m} c^\top y \\ \text{s.t.} \quad & A_{j,0} + \sum_{i=1}^m A_{j,i} y^{(i)} \succeq 0 \text{ for } j = 1, \dots, k, \end{aligned} \quad (2.83)$$

where $A_{j,i} \in \mathcal{S}^{n_j}$ for $i = 0, \dots, m$ and $j = 1, \dots, k$, $c \in \mathbb{R}^m$ and k is the number of constraints. In addition, a strictly feasible point $y_0 \in \mathbb{R}^m$ must be given.

The semidefinite program solver is implemented in the class `SDPSolver` of the Polyopt package. Firstly, the problem is initialized by the matrices $A_{j,i}$ and the vector c . Then, the function `solve` is called with parameter y_0 as the starting point and with the method for the analytic center estimation. A choice from two methods is available, firstly, the method `dampedNewton`, which corresponds to Algorithm 2.2, and secondly, the method `auxFollow`, which is the implementation of the Auxiliary path-following scheme [11]. However, the `auxFollow` method is unstable and it fails in some cases, and therefore it is not recommended to use. The function `solve` returns the optimal solution y^* . The minimal working example is shown in Listing 2.2.

Listing 2.2. Typical use of the class `SDPSolver` of the Polyopt package.

```
1: import polyopt
2:
3: # supposing the matrices Aij and the vectors c and y0 are already
   defined
4: problem = polyopt.SDPSolver(c, [[A10, A11, ..., A1m], ..., [Ak0,
   Ak1, ..., Akm]])
5: yStar = problem.solve(y0, problem.dampedNewton)
```

Detailed info can be printed out during the execution of the algorithm. This option can be set by `problem.setPrintOutput(True)`. Then, in each iteration of Algorithm 2.2 and Algorithm 2.3, the values k , x_k and eigenvalues of $X_j(x_k)$ are printed.

If n , the dimension of the problem, is equal to 2, boundary of the set $\text{Dom } F$ (2.78) and all intermediate points x_k can be plotted. This can be enabled by setting `problem.setDrawPlot(True)`. An example of such a graph is shown in Figure 2.5.

¹The PyPA recommended tool for installing Python packages. See <https://pip.pypa.io>.

The parameters β and γ are predefined to the same values as in (2.65) and (2.66). These parameters can be set to different values by assigning to the variables `problem.beta` and `problem.gamma` respectively. The default value for the accuracy parameter ε is 10^{-3} . This value can be changed by overwriting the variable `problem.eps`.

The function `problem.getNu()` returns the ν parameter of the self-concordant barrier function used for the problem according to Theorem 2.10. When the problem is solved, we can obtain the eigenvalues of $X(y^*)$ by calling `problem.eigenvalues()`. We should observe, that some of them are positive and some of them are zero (up to the numerical precision). The zero eigenvalues mean, that we have reached the boundary of the set Q , because the optimal solution lies always on the boundary of the set Q .

It may happen, that the set $\text{Dom } F$ is not bounded, but the optimal solution can be attained. In this case, the analytic center does not exist and the proposed algorithms can not be used. By adding a constraint

$$X_{k+1}(y) = \begin{bmatrix} R^2 & y^{(1)} & y^{(2)} & \dots & y^{(m)} \\ y^{(1)} & 1 & 0 & \dots & 0 \\ y^{(2)} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ y^{(m)} & 0 & 0 & \dots & 1 \end{bmatrix} \text{ for } R \in \mathbb{R}, \quad (2.84)$$

we bound the set by the ball with radius R . The constraint (2.84) is equivalent to

$$\|y\|_2^2 \leq R^2. \quad (2.85)$$

This will make the set $\text{Dom } F$ bounded and the analytic center can be found in the standard way by Algorithm 2.2. When optimizing the linear function by Algorithm 2.3, the radius R may be set too small and the optimum may be found on the boundary of the constraint (2.84). Then, the found optimum is not the solution to the original problem and the algorithm has to be run again with bigger value of R . The optimum is found on the boundary of the constraint (2.84), if at least one of the eigenvalues of $X_{k+1}(y^*)$ is zero. In our implementation, the artificial bounding constraint (2.84) can be set by `problem.bound(R)`. When the problem is solved, we can list the eigenvalues of $X_{k+1}(y^*)$ by the function `problem.eigenvalues('bounded')`.

Example 2.6. Let us present a simple example to show a detailed usage of the package Polyopt. Let us have semidefinite program in a form

$$\begin{aligned} y^* &= \arg \min_{y \in \mathbb{R}^2} y^{(1)} + y^{(2)} \\ \text{s.t.} \quad & \begin{bmatrix} 1 + y^{(1)} & y^{(2)} & 0 \\ y^{(2)} & 1 - y^{(1)} & y^{(2)} \\ 0 & y^{(2)} & 1 - y^{(1)} \end{bmatrix} \succeq 0 \end{aligned} \quad (2.86)$$

with starting point

$$y_0 = [0 \ 0]^\top. \quad (2.87)$$

Listing 2.3 shows the Python code used to solve the given problem. The graph of the problem is showed in Figure 2.5. The analytic center of the feasible region of the problem is

$$y_F^* = [-0.317 \ 0]^\top, \quad (2.88)$$

2. Semidefinite programming

the optimal solution is attained at

$$y^* = [-0.778 \quad -0.592]^\top \quad (2.89)$$

and the objective function has value -1.37 . The eigenvalues of $X(y^*)$ are

$$\{\lambda_i(X(y^*))\}_{i=1}^3 = \{2.32 \cdot 10^{-4}; 1.32; 2.45\}. \quad (2.90)$$

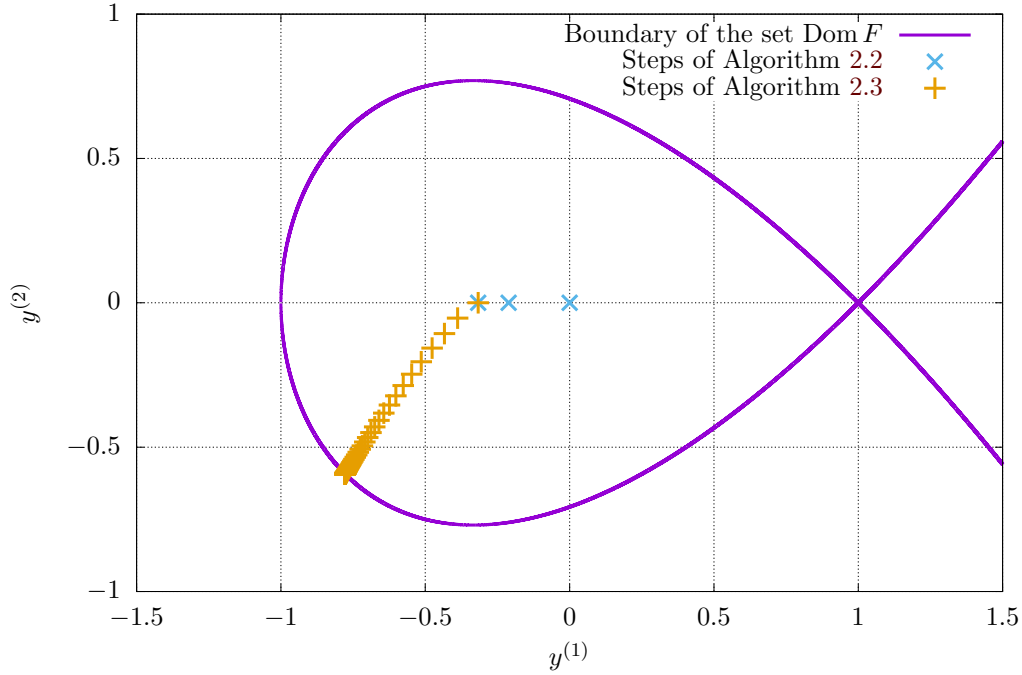


Figure 2.5. Graph of the semidefinite optimization problem stated in Example 2.6.

2.5. Comparison with the state of the art methods

Because a new implementation of a well-known algorithm was made, one should compare many properties of this implementation with the contemporary state of the art methods. For that reason, we have generated some random instances of semidefinite problems. We have solved these problems by our implementation from the Polyopt package and by selected state of the art toolboxes, namely SeDuMi [16] and MOSEK [10]. Firstly, we have verified the correctness of the implementation by checking that the optimal solution is the same as the solution obtained by SeDuMi and MOSEK for each instance of data. We have also measured execution times of all three libraries and compared them in Table 2.1 and Figure 2.6.

2.5.1. Problem description

Now, let us describe, how the random instances of the semidefinite problems were generated. From (2.82) we know that each step of Algorithm 2.2 and Algorithm 2.3 requires $m(m+n)n^2$ arithmetic operations, where m is the size of the matrices in the LMI constraint and n is the number of variables. Since in typical applications of SDP,

Listing 2.3. Code for solving semidefinite problem stated in Example 2.6.

```

1: from numpy import *
2: import polyopt
3:
4: # Problem statement
5: # min c1*y1 + c2*y2
6: # s.t. A0 + A1*y1 + A2*y2 >= 0
7: c = array([[1], [1]])
8: A0 = array([[1, 0, 0],
9:             [0, 1, 0],
10:            [0, 0, 1]])
11: A1 = array([[1, 0, 0],
12:            [0, -1, 0],
13:            [0, 0, -1]])
14: A2 = array([[0, 1, 0],
15:            [1, 0, 1],
16:            [0, 1, 0]])
17:
18: # starting point
19: y0 = array([[0], [0]])
20:
21: # create the solver object
22: problem = polyopt.SDPSolver(c, [[A0, A1, A2]])
23:
24: # enable graphs
25: problem.setDrawPlot(True)
26:
27: # enable informative output
28: problem.setPrintOutput(True)
29:
30: # solve!
31: yStar = problem.solve(y0, problem.dampedNewton)
32:
33: # print eigenvalues of X(yStar)
34: print(problem.eigenvalues())

```

2. Semidefinite programming

the size of the matrices grows with the number of variables, we have set $m = n$ to have just single parameter, which we call the size of the problem.

In our experiment, we have generated 30 unique LMI constraints for each size of the problem from 1 to 20. Each unique constraint has form

$$X_{k,l}(y) = \mathcal{I}^k + \sum_{i=1}^k A_{k,l,i} y^{(i)} \quad (2.91)$$

for the size of the problem $k = 1, \dots, 20$ and unique LMI constraint $l = 1, \dots, 30$, where $A_{k,l,i} \in \mathcal{S}^k$. The matrices $A_{k,l,i}$ were filled with random numbers from uniform distribution $(-1; 1)$ with symmetricity of the matrices preserved. The package Polyopt requires the starting point y_0 to be given by the user in advance. But from the structure of the constraint (2.91) we can see that $y_0 \in \mathbb{R}^k$

$$y_0 = [0 \ \dots \ 0]^\top \quad (2.92)$$

is a feasible point. We used the point y_0 to initialize problems for Polyopt package, but we have let SeDuMi and MOSEK use their own initialization process. However, since the LMI constraints were randomly generated, there is no guarantee that the sets, which they define, are bounded. Therefore, we have added constraint (2.84) for $R = 10^3$, which guarantees that we are optimizing over bounded sets.

The objective function of the problem is generated randomly too. For each unique instance, we have generated random vector $r \in \mathbb{R}^n$ from uniform distribution $(-1; 1)$. Then, the objective function to minimize is $r^\top y$. The final generated problem denoted as $P_{k,l}$ looks like

$$\begin{aligned} \min_{y \in \mathbb{R}^k} \quad & r_{k,l}^\top y \\ \text{s.t.} \quad & \mathcal{I}^k + \sum_{i=1}^k A_{k,l,i} y^{(i)} \succeq 0 \\ & \begin{bmatrix} R^2 & y^{(1)} & y^{(2)} & \dots & y^{(k)} \\ y^{(1)} & 1 & 0 & \dots & 0 \\ y^{(2)} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ y^{(k)} & 0 & 0 & \dots & 1 \end{bmatrix} \succeq 0. \end{aligned} \quad (2.93)$$

2.5.2. Time measuring

To eliminate influences that negatively affect the execution times on CPU, such as other processes competing for the same CPU core, processor caching, data loading delays, etc., we have executed each problem $P_{k,l}$ 30 times. So, for each problem $P_{k,l}$ we have obtained execution times $\tau_{k,l,s}$ for $s = 1, \dots, 30$. Because the influences mentioned above can only prolong the execution times, we have selected minimum of $\tau_{k,l,s}$ for each problem $P_{k,l}$.

$$\tau_{k,l} = \min_{s=1}^{30} \tau_{k,l,s} \quad (2.94)$$

Since the execution times of problems of the same sizes should be more or less the same, we have computed the average execution time τ_k for each size of the problem.

$$\tau_k = \frac{1}{30} \sum_{l=1}^{30} \tau_{k,l} \quad (2.95)$$

These execution times τ_k , where k is the size of the problem, were measured and computed separately for the Polyopt, SeDuMi and MOSEK toolboxes and are shown in Table 2.1 and Figure 2.6.

| Problem size | Toolbox | | |
|-----------------|----------|-------------|------------|
| | Polyopt | SeDuMi [16] | MOSEK [10] |
| 1 | 0.0212 s | 0.0390 s | 0.00307 s |
| 2 | 0.0280 s | 0.0567 s | 0.00328 s |
| 3 | 0.0329 s | 0.0619 s | 0.00348 s |
| 4 | 0.0392 s | 0.0690 s | 0.00414 s |
| 5 | 0.0451 s | 0.0745 s | 0.00424 s |
| 6 | 0.0536 s | 0.0839 s | 0.00460 s |
| 7 | 0.0677 s | 0.0823 s | 0.00488 s |
| 8 | 0.0757 s | 0.0799 s | 0.00517 s |
| 9 | 0.0910 s | 0.0807 s | 0.00578 s |
| 10 | 0.111 s | 0.0833 s | 0.00678 s |
| 11 | 0.135 s | 0.0904 s | 0.00765 s |
| 12 | 0.154 s | 0.0917 s | 0.00805 s |
| 13 | 0.179 s | 0.0891 s | 0.00901 s |
| 14 | 0.212 s | 0.0938 s | 0.00937 s |
| 15 | 0.241 s | 0.0943 s | 0.00993 s |
| 16 | 0.280 s | 0.0983 s | 0.0101 s |
| 17 | 0.299 s | 0.102 s | 0.0118 s |
| 18 | 0.348 s | 0.112 s | 0.0122 s |
| 19 | 0.392 s | 0.113 s | 0.0140 s |
| 20 | 0.429 s | 0.117 s | 0.0148 s |

Table 2.1. Execution times of different sizes of semidefinite problems solved by selected toolboxes.

It has to be mentioned, that the Polyopt toolbox is implemented in Python, but the toolboxes SeDuMi and MOSEK were run from MATLAB with precompiled MEX files (compiled C, C++ or Fortran code) and therefore the execution times are not readily comparable. On the other side, the Python package NumPy uses common linear algebra libraries, like LAPACK [1], ATLAS [18] and BLAS [8], and we can presume that SeDuMi and MOSEK use them too.

Our intention was to measure only the execution time of the solving phase, not of the preparation time. In case of the Polyopt package, we measured the execution time of the function `solve()`. For SeDuMi and MOSEK, we have used MATLAB framework YALMIP [9] for defining the semidefinite programs and calling the solvers. The execution time of the YALMIP code is quite long, because YALMIP makes an analysis of the problem and compiles it into a standard form. Only after that, an external solver (SeDuMi or MOSEK) is called to solve the problem. Fortunately, YALMIP internally measures the execution time of the solver, so we have used this time in our statistics.

The experiments were executed on Intel Core i5-3210M CPU 2.50 GHz based computer with sufficient amount of free system memory. The installed version of Python was 3.5.3 and MATLAB R2016b 64-bit was used.

2. Semidefinite programming

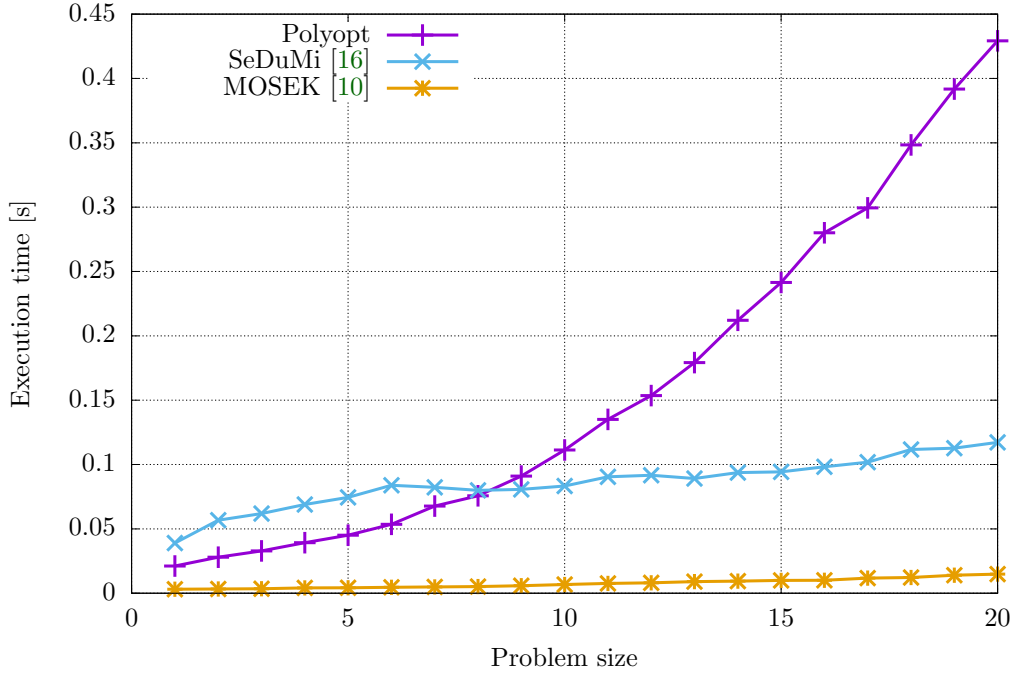


Figure 2.6. Graph of execution times based on the size of semidefinite problems solved by selected toolboxes.

2.5.3. Results

By the look of the graph in Figure 2.6, we can see that the MOSEK toolbox totally wins. The SeDuMi toolbox seems to have some constant overhead, but the execution time grows slowly with the increasing size of the problem. The Polyopt package accomplishes quite bad results compared to SeDuMi and MOSEK, especially for large sizes of problems. But this behavior was expected, as we know that the execution time should be proportional to k^4 , where k is the size of the problem. However, due to SeDuMi overhead, the Polyopt package is faster than SeDuMi for problem sizes up to 8.

3. Optimization over polynomials

3.1. State of the art review

3.2. Algebraic preliminaries

In this whole chapter focused on polynomial optimization and polynomial systems solving, we will follow the notation from [3]. Just to keep this chapter self-contained, we will recall some basics of polynomial algebra.

3.2.1. The polynomial ring, ideals and varieties

Firstly, the ring of multivariate polynomials in n variables with coefficients in \mathbb{R} is denoted as $\mathbb{R}[x]$, where $x = [x_1 \ x_2 \ \cdots \ x_n]^\top$. For $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{N}$, x^α denotes the monomial $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, with total degree $|\alpha| = \sum_{i=1}^n \alpha_i$, where $\alpha = [\alpha_1 \ \alpha_2 \ \cdots \ \alpha_n]^\top$. A polynomial $p \in \mathbb{R}[x]$ can be written as

$$p = \sum_{\alpha \in \mathbb{N}^n} p_\alpha x^\alpha \quad (3.1)$$

with total degree $\deg(p) = \max_{\alpha \in \mathbb{N}^n} |\alpha|$ for non-zero coefficients $p_\alpha \in \mathbb{R}$.

A linear subspace $I \subseteq \mathbb{R}[x]$ is an ideal if $p \in I$ and $q \in \mathbb{R}[x]$ implies $pq \in I$. Let f_1, f_2, \dots, f_m be polynomials in $\mathbb{R}[x]$. Then the set

$$\langle f_1, f_2, \dots, f_m \rangle = \left\{ \sum_{j=1}^m h_j f_j \mid h_1, h_2, \dots, h_m \in \mathbb{R}[x] \right\} \quad (3.2)$$

is called the ideal generated by f_1, f_2, \dots, f_m . Given the ideal $I \in \mathbb{R}[x]$, the algebraic variety of I is the set

$$V_{\mathbb{C}}(I) = \{x \in \mathbb{C}^n \mid f(x) = 0 \text{ for all } f \in I\} \quad (3.3)$$

and its real variety is

$$V_{\mathbb{R}}(I) = V_{\mathbb{C}}(I) \cap \mathbb{R}^n. \quad (3.4)$$

The ideal I is said to be zero-dimensional when its complex variety $V_{\mathbb{C}}(I)$ is finite. The vanishing ideal of a subset $V \subseteq \mathbb{C}^n$ is the ideal

$$\mathcal{I}(V) = \{f \in \mathbb{R}[x] \mid f(x) = 0 \text{ for all } x \in V\}. \quad (3.5)$$

The radical ideal of the ideal $I \subseteq \mathbb{R}[x]$ is the ideal

$$\sqrt{I} = \{f \in \mathbb{R}[x] \mid f^m \in I \text{ for some } m \in \mathbb{Z}^+\}. \quad (3.6)$$

The real radical ideal of the ideal $I \subseteq \mathbb{R}[x]$ is the ideal

$$\sqrt[\mathbb{R}]{I} = \{f \in \mathbb{R}[x] \mid f^{2m} + \sum_j h_j^2 \in I \text{ for some } h_j \in \mathbb{R}[x], m \in \mathbb{Z}^+\}. \quad (3.7)$$

The following two theorems are stating the relations between the vanishing and (real) radical ideals.

3. Optimization over polynomials

Theorem 3.1 (Hilbert's Nullstellensatz). Let $I \in \mathbb{R}[x]$ be an ideal. The radical ideal of I is equal to the vanishing ideal of its variety, i.e.

$$\sqrt{I} = \mathcal{I}(V_{\mathbb{C}}(I)). \quad (3.8)$$

Theorem 3.2 (Real Nullstellensatz). Let $I \in \mathbb{R}[x]$ be an ideal. The real radical ideal of I is equal to the vanishing ideal of its real variety, i.e.

$$\sqrt[\mathbb{R}]{I} = \mathcal{I}(V_{\mathbb{R}}(I)). \quad (3.9)$$

The quotient ring $\mathbb{R}[x]/I$ is the set of all equivalence classes of polynomials in $\mathbb{R}[x]$ for congruence modulo ideal I

$$\mathbb{R}[x]/I = \{[f] \mid f \in \mathbb{R}[x]\}, \quad (3.10)$$

where the equivalence class $[f]$ is

$$[f] = \{f + g \mid g \in I\}. \quad (3.11)$$

Because $\mathbb{R}[x]/I$ is a ring, it is equipped with addition and multiplication on the equivalence classes:

$$[f] + [g] = [f + g] \quad (3.12)$$

$$[f][g] = [fg] \quad (3.13)$$

for $f, g \in \mathbb{R}[x]$.

For zero-dimensional ideal I , there is a relation between the dimension of $\mathbb{R}[x]/I$ and the cardinality of the variety $V_{\mathbb{C}}(I)$:

$$|V_{\mathbb{C}}(I)| \leq \dim(\mathbb{R}[x]/I). \quad (3.14)$$

Moreover, if I is a radical ideal, then

$$|V_{\mathbb{C}}(I)| = \dim(\mathbb{R}[x]/I). \quad (3.15)$$

Assume that the number of complex roots is finite and let $N = \dim(\mathbb{R}[x]/I)$, and therefore $|V_{\mathbb{C}}(I)| \leq N$. Consider a set $\mathcal{B} = \{b_1, b_2, \dots, b_N\} \subseteq \mathbb{R}[x]$ for which the equivalence classes $[b_1], [b_2], \dots, [b_N]$ are pairwise distinct and $\{[b_1], [b_2], \dots, [b_N]\}$ is a basis of $\mathbb{R}[x]/I$. Then every polynomial $f \in \mathbb{R}[x]$ can be written in unique way as

$$f = \sum_{i=1}^N c_i b_i + p, \quad (3.16)$$

where $c_i \in \mathbb{R}$ and $p \in I$. The normal form of the polynomial f modulo I with respect to the basis \mathcal{B} is the polynomial

$$\mathcal{N}_{\mathcal{B}}(f) = \sum_{i=1}^N c_i b_i. \quad (3.17)$$

3.2.2. Solving systems of polynomial equations by multiplication matrices

Systems of polynomial equations can be solved by computing eigenvalues and eigenvectors of so called multiplication matrices. Given $f \in \mathbb{R}[x]$, we define the multiplication operator (by f) $\mathcal{X}_f : \mathbb{R}[x]/I \rightarrow \mathbb{R}[x]/I$ as

$$\mathcal{X}_f([g]) = [f][g] = [fg]. \quad (3.18)$$

It can be shown that \mathcal{X}_f is a linear mapping, and therefore can be represented by its matrix with respect to the basis \mathcal{B} of $\mathbb{R}[x]/I$. For simplicity, we again denote this matrix \mathcal{X}_f and it is called the multiplication matrix by f . When $\mathcal{B} = \{b_1, b_2, \dots, b_N\}$ and we set $\mathcal{N}_{\mathcal{B}}(fb_j) = \sum_{i=1}^N a_{i,j} b_i$ for $a_{ij} \in \mathbb{R}$, then the multiplication matrix is

$$\mathcal{X}_f = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,N} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ a_{N,1} & a_{N,2} & \cdots & a_{N,N} \end{bmatrix}. \quad (3.19)$$

Theorem 3.3 (Stickelberger theorem). Let I be a zero-dimensional ideal in $\mathbb{R}[x]$, let $\mathcal{B} = \{b_1, b_2, \dots, b_N\}$ be a basis of $\mathbb{R}[x]/I$, and let $f \in \mathbb{R}[x]$. The eigenvalues of the multiplication matrix \mathcal{X}_f are the evaluations $f(v)$ of the polynomial f at the points $v \in V_{\mathbb{C}}(I)$. Moreover, for all $v \in V_{\mathbb{C}}(I)$,

$$(\mathcal{X}_f)^{\top} [v]_{\mathcal{B}} = f(v) [v]_{\mathcal{B}}, \quad (3.20)$$

setting $[v]_{\mathcal{B}} = [b_1(v) \ b_2(v) \ \cdots \ b_N(v)]^{\top}$; that is, the vector $[v]_{\mathcal{B}}$ is a left eigenvector with eigenvalue $f(v)$ of the multiplication matrix \mathcal{X}_f .

Therefore, we can create the multiplication matrix \mathcal{X}_{x_i} for the variable x_i and then the eigenvalues of \mathcal{X}_{x_i} correspond to the x_i -coordinates of the points $V_{\mathbb{C}}(I)$. This means that the solutions of the whole system can be found by computing eigenvalues $\lambda_{x_i} = \{\lambda_j(\mathcal{X}_{x_i})\}_{j=1}^N$ of the multiplication matrix \mathcal{X}_{x_i} for all variables x_i . Then $V_{\mathbb{C}}(I)$ is a subset of the Cartesian product $\lambda_{x_1} \times \lambda_{x_2} \times \cdots \times \lambda_{x_n}$ and one has to select only the points that are solutions. However, this method becomes inefficient for large n , the number of variables, since n multiplication matrices have to be constructed and their eigenvalues computed.

For this reason, the second property of multiplication matrices is used. The roots can be recovered from left eigenvectors of \mathcal{X}_f when all eigenspaces of \mathcal{X}_f^{\top} have dimension one. This is the case when the values $f(v)$ for $v \in V_{\mathbb{C}}(I)$ are pairwise distinct and when the ideal I is radical. In that case, each left eigenvector of \mathcal{X}_f corresponds to one solution $v \in V_{\mathbb{C}}(I)$ and the values of the eigenvectors are the evaluations $b_i(v)$ for $b_i \in \mathcal{B}$, and therefore when the variable $x_i \in \mathcal{B}$, we can readily obtain its value.

3.3. Moment matrices

3.4. Polynomial optimization

3.5. Solving systems of polynomial equations

4. Conclusion

A. Contents of the enclosed CD

```
/
└─ thesis
    └─ thesis.pdf .....digital copy of this thesis
```

Bibliography

- [1] E. Anderson, Z. Bai, C. Bischof, S. Blackford, J. Demmel, J. Dongarra, J. Du Croz, A. Greenbaum, S. Hammarling, A. McKenney, and D. Sorensen. *LAPACK Users' Guide*. Society for Industrial and Applied Mathematics, Philadelphia, PA, 3rd edition, 1999. 19, 25
- [2] Richard Bellman and Ky Fan. On systems of linear inequalities in hermitian matrix variables. In *Convexity: Proceedings of Symposia in Pure Mathematics*, volume 7, pages 1–11. American Mathematical Society Providence, 1963. 7
- [3] David Cox, John Little, and Donald O'Shea. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer, New York, USA, 2nd edition, 1997. 27
- [4] Jane Cullum, W. E. Donath, and P. Wolfe. The minimization of certain nondifferentiable sums of eigenvalues of symmetric matrices. In *Nondifferentiable Optimization*, pages 35–55. Springer Berlin Heidelberg, Berlin, Heidelberg, 1975. 7
- [5] Michel X. Goemans and David P. Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *Journal of the ACM*, 42(6):1115–1145, November 1995. 5
- [6] Narendra Karmarkar. A new polynomial-time algorithm for linear programming. *Combinatorica*, 4:373–395, 1984. 7
- [7] Richard M. Karp. Reducibility among combinatorial problems. In *Complexity of Computer Computations*, pages 85–103. Springer US, Boston, MA, 1972. 5
- [8] C. L. Lawson, R. J. Hanson, D. R. Kincaid, and F. T. Krogh. Basic linear algebra subprograms for fortran usage. *ACM Trans. Math. Softw.*, 5(3):308–323, September 1979. 19, 25
- [9] J. Löfberg. YALMIP : A toolbox for modeling and optimization in MATLAB. In *Proceedings of the CACSD Conference*, Taipei, Taiwan, 2004. 25
- [10] MOSEK ApS. *The MOSEK optimization toolbox for MATLAB manual. Version 7.1 (Revision 28)*, 2015. <http://docs.mosek.com/7.1/toolbox/index.html> [Online; accessed 2017-04-25]. 8, 19, 22, 25, 26
- [11] Yurii Nesterov. *Introductory lectures on convex optimization : A basic course*. Springer, 2004. 8, 20
- [12] Yurii Nesterov and Arkadi Nemirovski. A general approach to polynomial-time algorithms design for convex programming. Technical report, Central Economical and Mathematical Institute, USSR Academy of Sciences, Moscow, USSR, 1988. 7
- [13] Brendan O'Donoghue, Eric Chu, Neal Parikh, and Stephen P. Boyd. SCS: Splitting conic solver, version 1.2.6. <https://github.com/cvxgrp/scs> [Online; accessed 2017-04-22], April 2016. 8

- [14] Michael Overton. On minimizing the maximum eigenvalue of a symmetric matrix. *SIAM Journal on Matrix Analysis and Applications*, 9:256–268, April 1988. 7
- [15] Gabor Pataki. *On the multiplicity of optimal eigenvalues*. University of Michigan, Ann Arbor, MI (United States), December 1994. 7
- [16] Jos F. Sturm. Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones. *Optimization Methods and Software*, 11–12:625–653, 1999. 8, 19, 22, 25, 26
- [17] Guido van Rossum and Fred L. Drake. *The Python Language Reference Manual*. Network Theory Ltd, 2011. 18
- [18] R. Clint Whaley and Antoine Petitet. Minimizing development and maintenance costs in supporting persistently optimized BLAS. *Software: Practice and Experience*, 35(2):101–121, February 2005. <http://www.cs.utsa.edu/~whaley/papers/spercw04.ps> [Online; accessed 2017-04-18]. 19, 25
- [19] Makoto Yamashita, Katsuki Fujisawa, Kazuhide Nakata, Maho Nakata, Mituhiro Fukuda, Kazuhiro Kobayashi, and Kazushige Goto. A high-performance software package for semidefinite programs: SDPA7. Technical report, Tokyo Japan, September 2010. 8