Integer Quadratic Programming is in NP

Alberto Del Pia[1] Santanu S. Dey[2] Marco Molinaro[2]

[1]IBM T. J. Watson Research Center, Yorktown Heights.

[2]School of Industrial and Systems Engineering, Atlanta

Outline

1

Introduction and Main Result

Integer Quadratic Program: Definition

Definition (IQP)

$$
\begin{aligned}
\min \quad & x^\top Q x + c^\top x \\
\text{s.t.} \quad & Ax \leq b \\
& x \in \mathbb{Z}^n,
\end{aligned}
$$

Integer Quadratic Program: Definition

Definition (IQP)

$$\begin{aligned} \min \quad & x^\top Q x + c^\top x \\ \text{s.t.} \quad & Ax \leq b \\ & x \in \mathbb{Z}^n, \end{aligned}$$

We do no assume that $x^\top Qx$ is convex i.e., Q is not necessarily positive semi-definite.

Integer Quadratic Program: Definition

Definition (IQP)

$$\begin{aligned} \min \quad & x^\top Q x + c^\top x \\ \text{s.t.} \quad & Ax \leq b \\ & x \in \mathbb{Z}^n, \end{aligned}$$

We do no assume that $x^\top Qx$ is convex i.e., Q is not necessarily positive semi-definite.

Decision Version of IQP

Does there exist x satisfying:

$$\left.\begin{array}{rcl} x^\top Qx + c^\top x + d & \leq & 0 \\ Ax & \leq & b \\ x & \in & \mathbb{Z}^n, \end{array}\right\} \quad \mathcal{F}(Q, c, d, A, b)$$

where we assume all the data is rational.

Main Result

Theorem

Let $n, m \in \mathbb{Z}_{++}$. Let $Q \in \mathbb{Q}^{n\times n}$, $c \in \mathbb{Q}^n$, $d \in \mathbb{Q}$, $A \in \mathbb{Q}^{m\times n}$, $b \in \mathbb{Q}^m$.

Main Result

Theorem

Let $n, m \in \mathbb{Z}_{++}$. Let $Q \in \mathbb{Q}^{n \times n}$, $c \in \mathbb{Q}^n$, $d \in \mathbb{Q}$, $A \in \mathbb{Q}^{m \times n}$, $b \in \mathbb{Q}^m$.
If $\mathcal{F}(Q, c, d, A, b)$ is non-empty, then there exists $x^0 \in \mathcal{F}(Q, c, d, A, b)$

Main Result

Theorem

Let $n, m \in \mathbb{Z}_{++}$. Let $Q \in \mathbb{Q}^{n\times n}$, $c \in \mathbb{Q}^n$, $d \in \mathbb{Q}$, $A \in \mathbb{Q}^{m\times n}$, $b \in \mathbb{Q}^m$.
If $\mathcal{F}(Q, c, d, A, b)$ is non-empty, then there exists $x^0 \in \mathcal{F}(Q, c, d, A, b)$ such that the binary encoding size of x^0 is bounded from above by a polynomial function of the size of binary encoding of Q, c, d, A, b.

Main Result

Theorem

Let $n, m \in \mathbb{Z}_{++}$. Let $Q \in \mathbb{Q}^{n\times n}$, $c \in \mathbb{Q}^n$, $d \in \mathbb{Q}$, $A \in \mathbb{Q}^{m\times n}$, $b \in \mathbb{Q}^m$.
If $\mathcal{F}(Q, c, d, A, b)$ is non-empty, then there exists $x^0 \in \mathcal{F}(Q, c, d, A, b)$ such that the binary encoding size of x^0 is bounded from above by a polynomial function of the size of binary encoding of Q, c, d, A, b.

Consequences

1. Integer Quadratic Programming is in NP . In particular, the decision version of IQP is NP-complete.
2. Broadly speaking, this implies that these exists an algorithm to solve IQP, i.e. not undecidable.

Comparison 1: More quadratic inequalities?

Undecidable!

Determing the feasibility of a system with

1. Number of quadratic inequalities: $2\left(\binom{58}{2} + 58 + 1\right) = 3424.$
2. Number of linear inequalities: 58
3. Number of integer variables: $\left(\binom{58}{2} + 2 * 58\right) = 1769.$

is Undecidable.

Comparison 1: More quadratic inequalities?

Undecidable!

Determing the feasibility of a system with

1. Number of quadratic inequalities: $2\left(\binom{58}{2} + 58 + 1\right) = 3424.$
2. Number of linear inequalities: 58
3. Number of integer variables: $\left(\binom{58}{2} + 2 * 58\right) = 1769.$

is Undecidable.

Reduction from undecidability of determining the feasibility of a quartic equation in 58 non-negative integer variables.

[Jones (1982)], See discussion and additional references in [Köppe (2012)].

Comparison 2: Two quadratic inequalities?

Exponential size solution!

Consider the system for $d = 5^{2n+1}$:

$$\begin{aligned} x^2 - dy^2 + 1 &\leq 0, \\ -x^2 + dy^2 - 1 &\leq 0 \\ x, y &\in \mathbb{Z}. \end{aligned}$$

Comparison 2: Two quadratic inequalities?

Exponential size solution!

Consider the system for $d = 5^{2n+1}$:

$$\begin{aligned} x^2 - dy^2 + 1 &\leq 0, \\ -x^2 + dy^2 - 1 &\leq 0 \\ x, y &\in \mathbb{Z}. \end{aligned}$$

1. The binary encoding length of smallest integer solution with minimal binary encoding length has an encoding length of: $\Omega(5^n)$.

Comparison 2: Two quadratic inequalities?

Exponential size solution!

Consider the system for $d = 5^{2n+1}$:

$$\begin{aligned} x^2 - dy^2 + 1 &\leq 0, \\ -x^2 + dy^2 - 1 &\leq 0 \\ x, y &\in \mathbb{Z}. \end{aligned}$$

1. The binary encoding length of smallest integer solution with minimal binary encoding length has an encoding length of: $\Omega(5^n)$.
2. The binary encoding length of instance: $\Theta(n)$.

[Lagarias (1980)], See discussion and additional references in [Köppe (2012)]

Comparison 3: More convex quadratic inequalities?

Exponential size solution!

Consider the system:

$$\begin{aligned} x_1 &\geq 2 \\ x_j &\geq x_{j-1}^2 \ \forall j \in \{2, \dots, n\} \\ x_j &\in \mathbb{Z} \ \forall j \in \{1, \dots, n\}. \end{aligned}$$

Comparison 3: More convex quadratic inequalities?

Exponential size solution!

Consider the system:

$$\begin{aligned} x_1 &\geq 2 \\ x_j &\geq x_{j-1}^2 \ \forall j \in \{2, \ldots, n\} \\ x_j &\in \mathbb{Z} \ \forall j \in \{1, \ldots, n\}. \end{aligned}$$

1. The binary encoding length of smallest size solution is: $\Omega(2^n)$.

Comparison 3: More convex quadratic inequalities?

Exponential size solution!

Consider the system:

$$\begin{aligned} x_1 &\geq 2 \\ x_j &\geq x_{j-1}^2 \ \forall j \in \{2, \dots, n\} \\ x_j &\in \mathbb{Z} \ \forall j \in \{1, \dots, n\}. \end{aligned}$$

1. The binary encoding length of smallest size solution is: $\Omega(2^n)$.
2. The binary encoding length of instance: $\Theta(n)$.

In Conclusion...

1. In the presence of exactly one rational quadratic inequality, there exists “small" poly-size feasible solutions.

In Conclusion...

1. In the presence of exactly one rational quadratic inequality, there exists “small" poly-size feasible solutions.

2. With even two inequality, the binary encoding of the smallest solution may be exponential in size.
3. With “many" inequalities, (a) the problem become undecidables with general quadratics, or (b) binary encoding of all solutions may be exponential in size in the convex quadratics case.

2

Proof Outline

Overview of the proof

$$
\begin{aligned}
x^\top Q x + c^\top x + d &\leq 0 \\
\boxed{Ax \leq b} & \qquad \qquad \ldots\ldots\ldots\ldots \ (\mathcal{P}) \\
x &\in \mathbb{Z}^n
\end{aligned}
$$

Overview of the proof

$$\begin{array}{rcl} x^\top Q x + c^\top x + d & \leq & 0 \\ \boxed{Ax \leq b} & & \quad \ldots\ldots\ldots\ldots\ldots (\mathcal{P}) \\ x & \in & \mathbb{Z}^n \end{array}$$

Definition: Simplicial cone

A simplicial cone is a cone generated by a simplex.

Overview of the proof

$$\begin{aligned} x^\top Q x + c^\top x + d &\leq 0 \\ \boxed{Ax \leq b} & \qquad \ldots\ldots\ldots\ldots\ldots (\mathcal{P}) \\ x &\in \mathbb{Z}^n \end{aligned}$$

Definition: Simplicial cone

A simplicial cone is a cone generated by a simplex.

Proof Steps

1. Step 1: It is sufficient to prove the result where $\mathcal{P}$ is a full-dimensional simplicial cone.

Overview of the proof

$$\begin{aligned} x^\top Q x + c^\top x + d &\leq 0 \\ \boxed{Ax \leq b} & \qquad \ldots\ldots\ldots\ldots\ (\mathcal{P}) \\ x &\in \mathbb{Z}^n \end{aligned}$$

Definition: Simplicial cone

A simplicial cone is a cone generated by a simplex.

Proof Steps

1. Step 1: It is sufficient to prove the result where $\mathcal{P}$ is a full-dimensional simplicial cone.
   - $\rightarrow$ Standard techniques to show Integer linear programming is in NP.
   - $\rightarrow$ Carathéodory Theorem.
   - $\rightarrow$ Some careful rotation using (poly-size) unimodular matrices.

Overview of the proof

$$\begin{aligned} x^\top Q x + c^\top x + d &\le 0 \\ \boxed{Ax \le b} & \qquad \ldots\ldots\ldots\ldots\ (\mathcal{P}) \\ x &\in \mathbb{Z}^n \end{aligned}$$

Definition: Simplicial cone

A simplicial cone is a cone generated by a simplex.

Proof Steps

1. Step 1: It is sufficient to prove the result where $\mathcal{P}$ is a full-dimensional simplicial cone.
   - $\rightarrow$ Standard techniques to show Integer linear programming is in NP.
   - $\rightarrow$ Carathéodory Theorem.
   - $\rightarrow$ Some careful rotation using (poly-size) unimodular matrices.
2. Step 2: Verify the result for the case where $\mathcal{P}$ is a full-dimensional simplicial cone.

2.1
Step 2

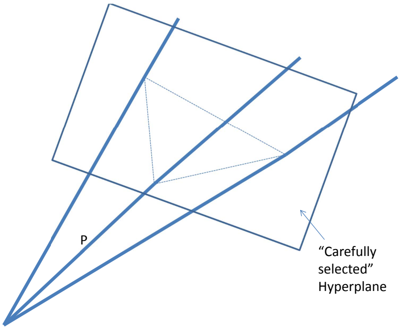
Getting Started

$$\begin{aligned} x^\top Q x + c^\top x + d &\leq 0 \\ Ax &\leq 0 \quad \ldots\ldots\ldots\ldots\ (\mathcal{P}) \\ x &\in \mathbb{Z}^n \end{aligned}$$

1. $\{x \mid Ax \leq 0\}$ is a simplicial cone.
2. We may assume $d > 0$.

$\mathcal{P}$ is a full-dimensional simplicial cone.

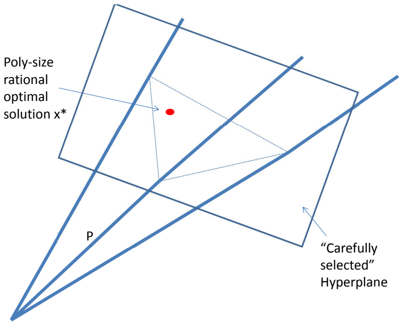
- "Slice " the cone $\mathcal{P}$ with a "carefully selected" hyperplane $\mathcal{H}$



$\mathcal{P}$ is a full-dimensional simplicial cone.

- "Slice " the cone $\mathcal{P}$ with a "carefully selected" hyperplane $\mathcal{H}$
- Let x^* be a poly-size rational optimal solution to the problem

$$x^{*\top} Q x^* := \min \quad x^\top Q x \quad \text{s.t.} \quad x \in \mathcal{P} \cap \mathcal{H}$$

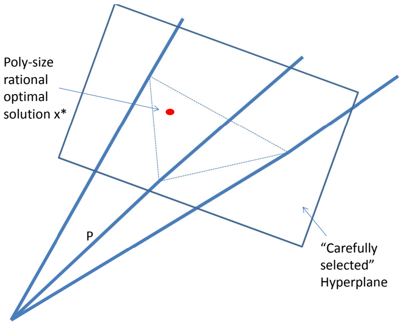


$\mathcal{P}$ is a full-dimensional simplicial cone.

- "Slice " the cone $\mathcal{P}$ with a "carefully selected" hyperplane $\mathcal{H}$
- Let x^* be a poly-size rational optimal solution to the problem

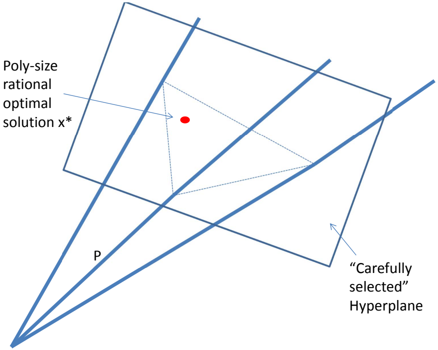
$$x^{*\top} Q x^* := \min \quad x^\top Q x \quad \text{s.t.} \quad x \in \mathcal{P} \cap \mathcal{H}$$

- The quadratic problem $\min\{x^\top V x \mid x \in \text{rational polytope}\}$ (where V is a rational matrix) has a rational globally optimal solution of poly-size with respect to the size of the instance. [Vavasis 1990]



Case analysis based on sign of ${x^*}^\top Q x^*$

$$\begin{aligned} {x^*}^\top Q x^* := \quad & \min \quad x^\top Q x \\ & \text{s.t.} \quad x \in \mathcal{P} \cap \mathcal{H} \end{aligned}$$



Case 1: ${x^*}^\top Q x^* < 0$

Scale and find a solution

Case 1: ${x^*}^\top Q x^* < 0$

Scale and find a solution

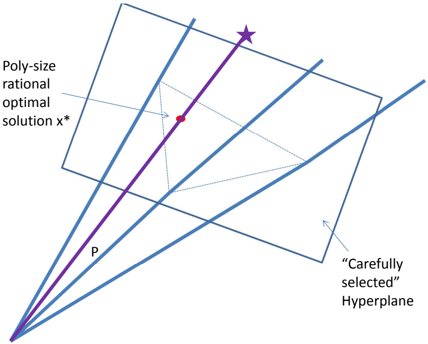
1. First scale x^* to $\bar{x}$ so that $\bar{x} \in \mathcal{P} \cap \mathbb{Z}^n$.

Case 1: $x^{*\top} Q x^* < 0$

Scale and find a solution

1. First scale x^* to $\bar{x}$ so that $\bar{x} \in \mathcal{P} \cap \mathbb{Z}^n$.
2. $\bar{\lambda} = \left\lceil \left| \frac{c^\top \bar{x}}{(\bar{x})^\top Q \bar{x}} \right| + \sqrt{-\frac{d}{(\bar{x})^\top Q \bar{x}}} \right\rceil$
3. Then $\lambda \bar{x} \in \mathcal{P} \cap \mathbb{Z}^n$ and

$$(\bar{\lambda}\bar{x})^\top Q(\bar{\lambda}\bar{x}) + c^\top(\bar{\lambda}\bar{x}) + d \leq 0.$$



Case 2: ${x^*}^\top Q x^* > 0$

Question: Can ${x^*}^\top Q x^*$ be arbitrarily close to zero?

Case 2: ${x^*}^\top Q x^* > 0$

Question: Can ${x^*}^\top Q x^*$ be arbitrarily close to zero?

1. No. In fact ${x^*}^\top Q x^* \geq \frac{1}{G^2}$ where $G \leq 2^{\text{size of } x^*}$ (Assuming Q is integral WLOG).

Case 2: ${x^*}^\top Q x^* > 0$

Question: Can ${x^*}^\top Q x^*$ be arbitrarily close to zero?

1. No. In fact ${x^*}^\top Q x^* \geq \frac{1}{G^2}$ where $G \leq 2^{\text{size of } x^*}$ (Assuming Q is integral WLOG).
2. Let $x \in \mathcal{P}$ and $x = \lambda \tilde{x}$ where $\tilde{x}$ belongs to slice of $\mathcal{P}$.

$$x^\top Q x + c^\top x + d = \lambda^2 \tilde{x}^\top Q \tilde{x} + \lambda c^\top \tilde{x} + d$$

Case 2: ${x^*}^\top Q x^* > 0$

Question: Can ${x^*}^\top Q x^*$ be arbitrarily close to zero?

1. No. In fact ${x^*}^\top Q x^* \geq \frac{1}{G^2}$ where $G \leq 2^{\text{size of } x^*}$ (Assuming Q is integral WLOG).
2. Let $x \in \mathcal{P}$ and $x = \lambda \tilde{x}$ where $\tilde{x}$ belongs to slice of $\mathcal{P}$.

$$\begin{aligned} x^\top Q x + c^\top x + d &= \lambda^2 \tilde{x}^\top Q \tilde{x} + \lambda c^\top \tilde{x} + d \\ &\geq \lambda^2 \frac{1}{G^2} - \lambda \|c\| M + d \end{aligned}$$

Case 2: ${x^*}^\top Q x^* > 0$

Question: Can ${x^*}^\top Q x^*$ be arbitrarily close to zero?

1. No. In fact ${x^*}^\top Q x^* \geq \frac{1}{G^2}$ where $G \leq 2^{\text{size of } x^*}$ (Assuming Q is integral WLOG).
2. Let $x \in \mathcal{P}$ and $x = \lambda \tilde{x}$ where $\tilde{x}$ belongs to slice of $\mathcal{P}$.

$$\begin{aligned} x^\top Q x + c^\top x + d &= \lambda^2 \tilde{x}^\top Q \tilde{x} + \lambda c^\top \tilde{x} + d \\ &\geq \lambda^2 \frac{1}{G^2} - \lambda \|c\| M + d \\ &> 0 \ \underline{\text{for sufficiently large}}\ \lambda \end{aligned}$$

Case 2: ${x^*}^\top Q x^* > 0$

Question: Can ${x^*}^\top Q x^*$ be arbitrarily close to zero?

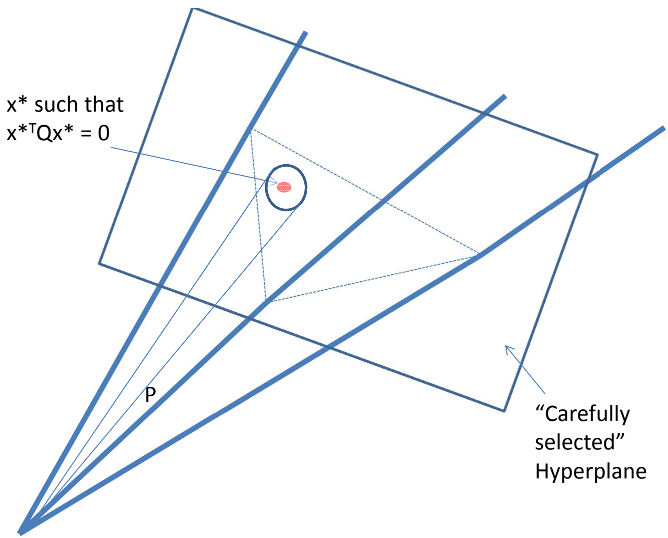
1. No. In fact ${x^*}^\top Q x^* \geq \frac{1}{G^2}$ where $G \leq 2^{\text{size of } x^*}$ (Assuming Q is integral WLOG).
2. Let $x \in \mathcal{P}$ and $x = \lambda \tilde{x}$ where $\tilde{x}$ belongs to slice of $\mathcal{P}$.

$$\begin{aligned} x^\top Q x + c^\top x + d &= \lambda^2 \tilde{x}^\top Q \tilde{x} + \lambda c^\top \tilde{x} + d \\ &\geq \lambda^2 \frac{1}{G^2} - \lambda \|c\| M + d \\ &> 0 \ \underline{\text{for sufficiently large}}\ \lambda \end{aligned}$$

Bound size of all potential solution

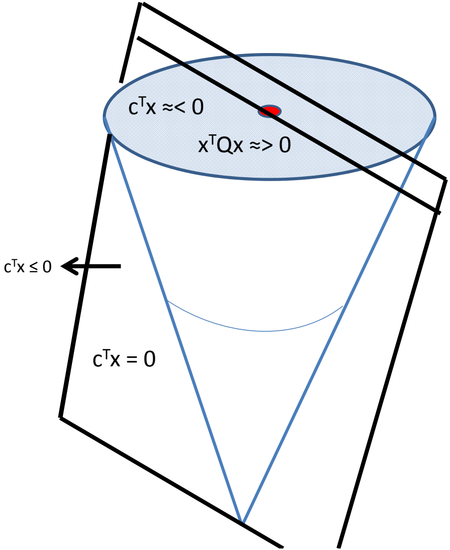
If $\|x\| > \|x^*\| \|c\| (R)^3$ and $x \in \mathcal{P}$, then $x^\top Q x + c^\top x + d > 0$ (R is the size of the largest extreme ray of $\mathcal{P}$.).

Case 3: $x^{*\top} Q x^* = 0$



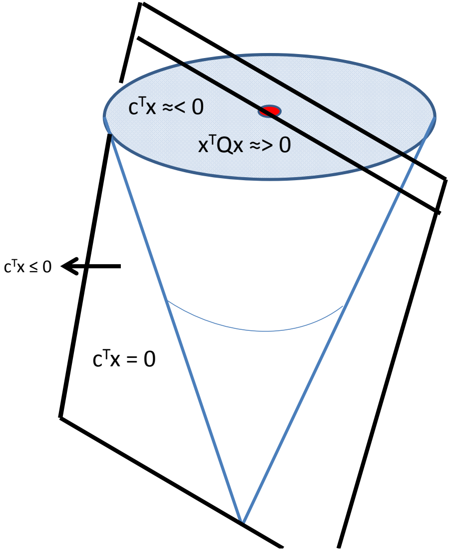
Looking around x^* ...

$$(x^\top Qx + c^\top x + d \leq 0)$$



Looking around x^* ...

$(x^\top Qx + c^\top x + d \leq 0)$



1. Not easy to bound size of feasible solution.
2. Not easy to find feasible solution of small size.

So far we have

If

$$0 = \begin{array}{ll} \min & x^T Q x \\ \text{s.t.} & x \in \text{slice of } \mathcal{P} \end{array}$$

then we need to tread more cautiously ...

So far we have

If

$$0 = \begin{array}{ll} \min & x^T Q x \\ \text{s.t.} & x \in \text{slice of } \mathcal{P} \end{array}$$

then we need to tread more cautiously ...

Lets see one possible approach.

Decomposing $\mathcal{P}$ further

Lemma

Let $\mathcal{P}$ be a full-dimensional simplicial cone such that $x^\top Qx \geq 0$ for every $x \in C$. Let $\mathcal{H}$ be a hyperplane such that $\mathcal{P} \cap \mathcal{H}$ is a simplex. Then there exist a finite family of full-dimensional simple cones C^i, $i \in I$ such that

(a) $\bigcup_{i \in I} C^i = \mathcal{P}$,

(b) for every $i \in I$, if a face F of C^i satisfies $\min\{x^\top Hx : x \in F \cap \mathcal{H}\} = 0$, then there exists an extreme ray v of F with $v^\top Hv = 0$,

(c) for every $i \in I$, the size of C^i is polynomial in the size of $\mathcal{P}$.

Illustration of Lemma

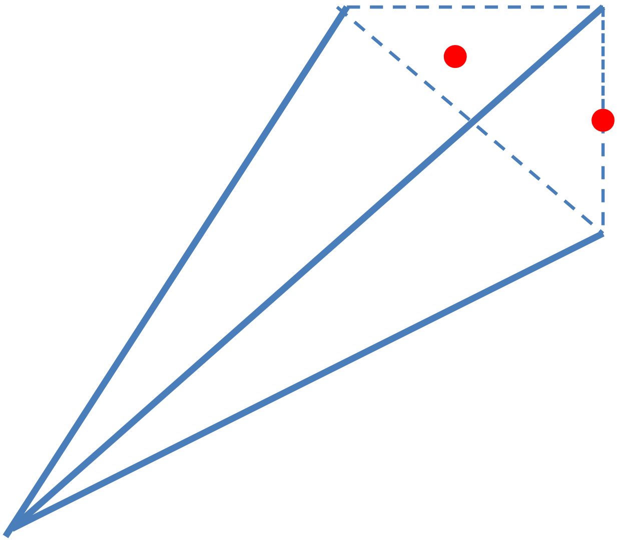
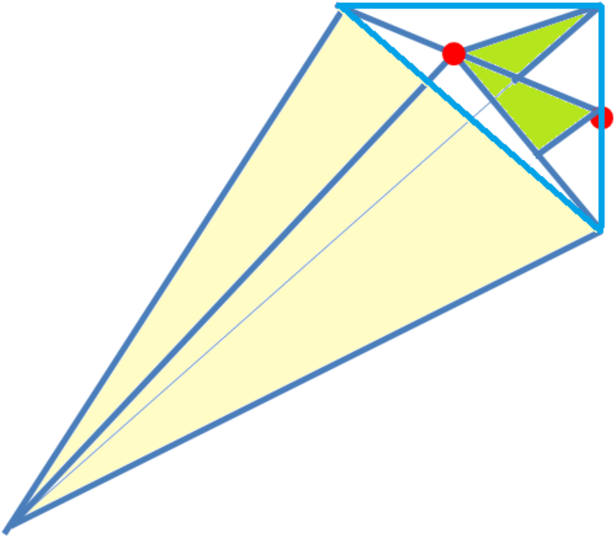


Illustration of Lemma



Working with one of these cones $\mathcal{C}$

1. $\mathcal{C}$ has n extreme rays $r^1, \ldots, r^n$.

Working with one of these cones $\mathcal{C}$

1. $\mathcal{C}$ has n extreme rays $r^1, \ldots, r^n$.
2. Let $J \subseteq \{1, \ldots, n\}$ such that $(r^j)^\top Q r^j = 0$ for all $j \in J$.

Working with one of these cones $\mathcal{C}$

1. $\mathcal{C}$ has n extreme rays $r^1, \ldots, r^n$.
2. Let $J \subseteq \{1, \ldots, n\}$ such that $(r^j)^\top Q r^j = 0$ for all $j \in J$.
3. $x \in \mathcal{C} \cap \mathbb{Z}^n$, then

$$x = \underbrace{x_0}_{\text{polysize integer point}} + \sum_{j=1}^{n} r^j y_j, \; y_j \in \mathbb{Z}_+ \; \forall j \in \{1, \ldots, n\}.$$

Working with one of these cones $\mathcal{C}$

1. $\mathcal{C}$ has n extreme rays $r^1, \ldots, r^n$.
2. Let $J \subseteq \{1, \ldots, n\}$ such that $(r^j)^\top Q r^j = 0$ for all $j \in J$.
3. $x \in \mathcal{C} \cap \mathbb{Z}^n$, then

$$x = \underbrace{x_0}_{\text{polysize integer point}} + \sum_{j=1}^{n} r^j y_j, \; y_j \in \mathbb{Z}_+ \; \forall j \in \{1, \ldots, n\}.$$

Now for each small x^0:

Working with one of these cones $\mathcal{C}$

1. $\mathcal{C}$ has n extreme rays $r^1, \ldots, r^n$.
2. Let $J \subseteq \{1, \ldots, n\}$ such that $(r^j)^\top Q r^j = 0$ for all $j \in J$.
3. $x \in \mathcal{C} \cap \mathbb{Z}^n$, then

$$x = \underbrace{x_0}_{\text{polysize integer point}} + \sum_{j=1}^{n} r^j y_j, \; y_j \in \mathbb{Z}_+ \; \forall j \in \{1, \ldots, n\}.$$

   Now for each small x^0:
4. Using (2) and (3) above:

Working with one of these cones $\mathcal{C}$

1. $\mathcal{C}$ has n extreme rays $r^1, \dots, r^n$.
2. Let $J \subseteq \{1, \dots, n\}$ such that $(r^j)^\top Q r^j = 0$ for all $j \in J$.
3. $x \in \mathcal{C} \cap \mathbb{Z}^n$, then

$$x = \underbrace{x_0}_{\text{polysize integer point}} + \sum_{j=1}^{n} r^j y_j, \quad y_j \in \mathbb{Z}_+ \ \forall j \in \{1, \dots, n\}.$$

Now for each small x^0:

4. Using (2) and (3) above: For each $j \in J$ either
   4.1 We can directly construct a small size solution or [$y_j > 0$ in this solution]
   4.2 If a solution exists, then there exist another solution with $y_j = 0$.

Working with one of these cones $\mathcal{C}$

1. $\mathcal{C}$ has n extreme rays $r^1, \dots, r^n$.
2. Let $J \subseteq \{1, \dots, n\}$ such that $(r^j)^\top Q r^j = 0$ for all $j \in J$.
3. $x \in \mathcal{C} \cap \mathbb{Z}^n$, then

$$x = \underbrace{x_0}_{\text{polysize integer point}} + \sum_{j=1}^{n} r^j y_j, \; y_j \in \mathbb{Z}_+ \; \forall j \in \{1, \dots, n\}.$$

Now for each small x^0:

4. Using (2) and (3) above: For each $j \in J$ either
   4.1 We can directly construct a small size solution or [$y_j > 0$ in this solution]
   4.2 If a solution exists, then there exist another solution with $y_j = 0$.
5. If we are not in case (4.1) above for all $j \in J$ then: If $x \in \mathcal{C} \cap \mathbb{Z}$ and $x^\top Q x + c^\top x + d \leq 0$, then there exists $\tilde{x} \in \mathcal{C} \cap \mathbb{Z}$ such that

$$x = x_0 + \sum_{j=1}^{n} r^j y_j, y_j \in \mathbb{Z}_+ \; \forall j \in \{1, \dots, n\} \setminus J.$$

Working with one of these cones $\mathcal{C}$

1. $\mathcal{C}$ has n extreme rays $r^1, \ldots, r^n$.
2. Let $J \subseteq \{1, \ldots, n\}$ such that $(r^j)^\top Q r^j = 0$ for all $j \in J$.
3. $x \in \mathcal{C} \cap \mathbb{Z}^n$, then

$$x = \underbrace{x_0}_{\text{polysize integer point}} + \sum_{j=1}^{n} r^j y_j, \; y_j \in \mathbb{Z}_+ \; \forall j \in \{1, \ldots, n\}.$$

Now for each small x^0:

4. Using (2) and (3) above: For each $j \in J$ either
   4.1 We can directly construct a small size solution or [$y_j > 0$ in this solution]
   4.2 If a solution exists, then there exist another solution with $y_j = 0$.
5. If we are not in case (4.1) above for all $j \in J$ then: If $x \in \mathcal{C} \cap \mathbb{Z}$ and $x^\top Q x + c^\top x + d \leq 0$, then there exists $\tilde{x} \in \mathcal{C} \cap \mathbb{Z}$ such that

$$x = x_0 + \sum_{j=1}^{n} r^j y_j, y_j \in \mathbb{Z}_+ \; \forall j \in \{1, \ldots, n\} \setminus J.$$

6. Finally, using the structure of the cone, (5) implies all the solutions are bounded, where the bound is polynomial size.

Open Problem

Is Integer Quadratic Programming in P for fixed dimension?

Thank You!