# Application of Carathéodory bounds for integer cones in verification

Ruzica Piskac

Presentation of papers:

1. Friedrich Eisenbrand, Gennady Shmonin: Carathéodory bounds for integer cones. Oper. Res. Lett. 34(5): 564-568 (2006)
2. Ruzica Piskac, Viktor Kuncak: Linear Arithmetic with Stars. In Proceedings of CAV 2008, to appear.

Mathematical models and algorithms for decision-making support

Friedrich Eisenbrand, Gennady Shmonin:
Carathéodory bounds for integer cones
Oper. Res. Lett. 34(5): 564-568 (2006)

# Basic Definitions

## Definition

Let $S \in \mathbb{Z}^d$ be a finite set of integer vectors. The integer cone of $S$ is the set

$$\text{cone}(X) = \{\lambda_1 x_1 + \ldots + \lambda_n x_n \mid n \geq 0; x_i \in S; \lambda_i \in \mathbb{Z}; \lambda_i \geq 0\}$$

## Definition

- For a vector $x$, the infinity norm is $||x||_\infty = \max\{|x_1|, \ldots, |x_n|\}$
- For a set of vectors $S$, let $M_S$ denote a number $M_S = \max_{x \in S} ||x||_\infty$

# Problem Formulation

## Question we want to answer

Let $X \subseteq \mathbb{Z}^d$ be a set of integer vectors and let $b \in \text{cone}(X)$.

- Question: how many vectors from $X$ are needed to generate $b$?
- (If those would be vectors with real coefficients, Carathéodory theorem states that $b$ is generated with at most $d$ vectors)

# Towards Solution

**Theorem**

*Let $X \subseteq \mathbb{Z}^d$ be a set of integer vectors and let $b \in cone(X)$. If $|X| > d \log_2(2|X|M_x + 1)$, then there exists a proper subset $\tilde{X} \subset X$ such that $b \in cone(\tilde{X})$.*

**Proof.**

□

## Towards Solution

### Theorem

*Let $X \subseteq \mathbb{Z}^d$ be a set of integer vectors and let $b \in cone(X)$. If $|X| > d \log_2(2|X|M_X + 1)$, then there exists a proper subset $\tilde{X} \subset X$ such that $b \in cone(\tilde{X})$.*

### Proof.

- assume that $b = \sum_{x \in X} \lambda_x x, \ \lambda_x > 0$

□

## Towards Solution

### Theorem

*Let $X \subseteq \mathbb{Z}^d$ be a set of integer vectors and let $b \in cone(X)$. If $|X| > d\log_2(2|X|M_X + 1)$, then there exists a proper subset $\tilde{X} \subset X$ such that $b \in cone(\tilde{X})$.*

### Proof.

- assume that $b = \sum_{x \in X} \lambda_x x,\ \lambda_x > 0$
- for every subset $S$, $||\sum_{x \in S} x||_\infty \leq |X|M_X$

$\square$

# Towards Solution

## Theorem

*Let $X \subseteq \mathbb{Z}^d$ be a set of integer vectors and let $b \in cone(X)$. If $|X| > d\log_2(2|X|M_x + 1)$, then there exists a proper subset $\tilde{X} \subset X$ such that $b \in cone(\tilde{X})$.*

## Proof.

- assume that $b = \sum_{x \in X} \lambda_x x, \ \lambda_x > 0$
- for every subset $S$, $||\sum_{x \in S} x||_\infty \leq |X|M_X$
- the number of different vectors which are representable as the sum of vectors of $S \subseteq X$ is bounded by $(2|X|M_x + 1)^d$, because coordinates are in $\{-|X|M_X, \ldots, |X|M_X\}$

$\square$

# Towards Solution

**Theorem**

*Let $X \subseteq \mathbb{Z}^d$ be a set of integer vectors and let $b \in cone(X)$. If $|X| > d \log_2(2|X|M_x + 1)$, then there exists a proper subset $\tilde{X} \subset X$ such that $b \in cone(\tilde{X})$.*

**Proof.**

- assume that $b = \sum_{x \in X} \lambda_x x, \;\; \lambda_x > 0$
- for every subset $S$, $||\sum_{x \in S} x||_\infty \le |X|M_X$
- the number of different vectors which are representable as the sum of vectors of $S \subseteq X$ is bounded by $(2|X|M_x + 1)^d$, because coordinates are in $\{-|X|M_X, \ldots, |X|M_X\}$
- theorem assumption: $2^{|X|} > (2|X|M_x + 1)^d \;\; \Rightarrow$ there are two different subsets $A, B$ such that $\sum_{x \in A} x = \sum_{x \in B} x$

$\square$

# Towards Solution

## Theorem

*Let $X \subseteq \mathbb{Z}^d$ be a set of integer vectors and let $b \in cone(X)$. If $|X| > d \log_2(2|X|M_x + 1)$, then there exists a proper subset $\tilde{X} \subset X$ such that $b \in cone(\tilde{X})$.*

## Proof.

- so far: assume $b = \sum_{x \in X} \lambda_x x, \ \lambda_x > 0$; there are two different disjoint subsets $A, B$ such that $\sum_{x \in A} x = \sum_{x \in B} x$

$\square$

# Towards Solution

## Theorem

*Let $X \subseteq \mathbb{Z}^d$ be a set of integer vectors and let $b \in cone(X)$. If $|X| > d \log_2(2|X|M_X + 1)$, then there exists a proper subset $\tilde{X} \subset X$ such that $b \in cone(\tilde{X})$.*

## Proof.

- so far: assume $b = \sum_{x \in X} \lambda_x x, \; \lambda_x > 0$; there are two different disjoint subsets $A, B$ such that $\sum_{x \in A} x = \sum_{x \in B} x$
- let $\lambda = \min\{\lambda_x \mid x \in A\}$

□

# Towards Solution

**Theorem**

*Let $X \subseteq \mathbb{Z}^d$ be a set of integer vectors and let $b \in cone(X)$. If $|X| > d \log_2(2|X|M_x + 1)$, then there exists a proper subset $\tilde{X} \subset X$ such that $b \in cone(\tilde{X})$.*

**Proof.**

- so far: assume $b = \sum_{x \in X} \lambda_x x,\ \lambda_x > 0$; there are two different disjoint subsets $A, B$ such that $\sum_{x \in A} x = \sum_{x \in B} x$
- let $\lambda = \min\{\lambda_x \mid x \in A\}$
- $b = \sum_{x \in X} \lambda_x x = \sum_{x \in X \setminus A} \lambda_x x + \sum_{x \in A} \lambda_x x$
  $= \sum_{x \in X \setminus A} \lambda_x x + \sum_{x \in A} (\lambda_x - \lambda) x + \lambda \sum_{x \in A} x$
  $= \sum_{x \in X \setminus A} \lambda_x x + \sum_{x \in A} (\lambda_x - \lambda) x + \lambda \sum_{x \in B} x$
  $= \sum_{x \in X} \mu_x x$

$\square$

# Towards Solution

## Theorem

*Let $X \subseteq \mathbb{Z}^d$ be a set of integer vectors and let $b \in cone(X)$. If $|X| > d \log_2(2|X|M_X + 1)$, then there exists a proper subset $\tilde{X} \subset X$ such that $b \in cone(\tilde{X})$.*

## Proof.

- so far: assume $b = \sum_{x \in X} \lambda_x x, \ \lambda_x > 0$; there are two different distinct subsets $A, B$ such that $\sum_{x \in A} x = \sum_{x \in B} x$; $b = \sum_{x \in X} \mu_x x$, where

□

# Towards Solution

## Theorem

*Let $X \subseteq \mathbb{Z}^d$ be a set of integer vectors and let $b \in cone(X)$. If $|X| > d \log_2(2|X|M_X + 1)$, then there exists a proper subset $\tilde{X} \subset X$ such that $b \in cone(\tilde{X})$.*

## Proof.

- so far: assume $b = \sum_{x \in X} \lambda_x x,\ \lambda_x > 0$; there are two different distinct subsets $A, B$ such that $\sum_{x \in A} x = \sum_{x \in B} x$; $b = \sum_{x \in X} \mu_x x$, where
- $\mu_x = \begin{cases} \lambda_x, & x \in X \setminus (A \cup B) \\ \lambda_x - \lambda, & x \in A \\ \lambda_x + \lambda, & x \in B \end{cases}$

□

# Towards Solution

## Theorem

*Let $X \subseteq \mathbb{Z}^d$ be a set of integer vectors and let $b \in cone(X)$. If $|X| > d \log_2(2|X|M_X + 1)$, then there exists a proper subset $\tilde{X} \subset X$ such that $b \in cone(\tilde{X})$.*

## Proof.

- so far: assume $b = \sum_{x \in X} \lambda_x x,\ \lambda_x > 0$; there are two different distinct subsets $A, B$ such that $\sum_{x \in A} x = \sum_{x \in B} x$; $b = \sum_{x \in X} \mu_x x$, where
- $\mu_x = \begin{cases} \lambda_x, & x \in X \setminus (A \cup B) \\ \lambda_x - \lambda, & x \in A \\ \lambda_x + \lambda, & x \in B \end{cases}$
- at least one $\mu_x$ is zero

□

# Towards Solution

**Theorem**

*Let $X \subseteq \mathbb{Z}^d$ be a set of integer vectors and let $b \in cone(X)$. If $|X| > d \log_2(2|X|M_x + 1)$, then there exists a proper subset $\tilde{X} \subset X$ such that $b \in cone(\tilde{X})$.*

**Proof.**

- so far: $b = \sum_{x \in X} \mu_x x$ and at least one $\mu_x$ is zero

$\square$

## Towards Solution

### Theorem

*Let $X \subseteq \mathbb{Z}^d$ be a set of integer vectors and let $b \in cone(X)$. If $|X| > d \log_2(2|X|M_x + 1)$, then there exists a proper subset $\tilde{X} \subset X$ such that $b \in cone(\tilde{X})$.*

### Proof.

- so far: $b = \sum_{x \in X} \mu_x x$ and at least one $\mu_x$ is zero
- $\tilde{X} = \{x \in X \mid \mu_x > 0\}$

$\square$

# Towards Solution

## Theorem

*Let $X \subseteq \mathbb{Z}^d$ be a set of integer vectors and let $b \in \text{cone}(X)$. If $|X| > d \log_2(2|X|M_X + 1)$, then there exists a proper subset $\tilde{X} \subset X$ such that $b \in \text{cone}(\tilde{X})$.*

## Proof.

- so far: $b = \sum_{x \in X} \mu_x x$ and at least one $\mu_x$ is zero
- $\tilde{X} = \{x \in X \mid \mu_x > 0\}$
- $\tilde{X} \subset X$ and $b \in \text{cone}(\tilde{X})$

$\square$

# Solution

## Theorem

*Let $X \subset \mathbb{Z}^d$ be a finite set of integer vectors and let $b \in cone(X)$. Then there exists a subset $\tilde{X}$ such that $b \in cone(\tilde{X})$ and $|\tilde{X}| \leq 2d \log_2(4dM_x)$.*

## Proof.

- Let $\tilde{X}$ be a minimal subset such that $b \in \text{cone}(\tilde{X})$ and let us assume that $|\tilde{X}| > 2d \log_2(4dM_x)$

$\square$

## Solution

**Theorem**

*Let $X \subset \mathbb{Z}^d$ be a finite set of integer vectors and let $b \in cone(X)$. Then there exists a subset $\tilde{X}$ such that $b \in cone(\tilde{X})$ and $|\tilde{X}| \leq 2d \log_2(4dM_x)$.*

**Proof.**

- Let $\tilde{X}$ be a minimal subset such that $b \in \text{cone}(\tilde{X})$ and let us assume that $|\tilde{X}| > 2d \log_2(4dM_x)$
- we will show that it implies that $|\tilde{X}| > d \log_2(2|X|M_x + 1)$ and using previous theorem, we conclude that there exist $X_1$, a proper subset of $\tilde{X}$ such that $b \in \text{cone}(X_1)$

$\square$

## Solution

### Theorem

*Let $X \subset \mathbb{Z}^d$ be a finite set of integer vectors and let $b \in cone(X)$. Then there exists a subset $\tilde{X}$ such that $b \in cone(\tilde{X})$ and $|\tilde{X}| \leq 2d \log_2(4dM_x)$.*

### Proof.

- Let $\tilde{X}$ be a minimal subset such that $b \in \text{cone}(\tilde{X})$ and let us assume that $|\tilde{X}| > 2d \log_2(4dM_x)$
- we will show that it implies that $|\tilde{X}| > d \log_2(2|X|M_x + 1)$ and using previous theorem, we conclude that there exist $X_1$, a proper subset of $\tilde{X}$ such that $b \in \text{cone}(X_1)$
- contradicts minimality of $\tilde{X}$

□

# Solution

## Left to Prove:

- If $|X| > 2d\log_2(4dM_x)$, then $|X| > d\log_2(2|X|M_x + 1)$

## Proof.

$\square$

# Solution

## Left to Prove:

- If $|X| > 2d \log_2(4dM_x)$, then $|X| > d \log_2(2|X|M_x + 1)$

## Proof.

- $|X| > 2d \log_2(4dM_x) \Rightarrow M_x < 2^{|X|/(2d)}/(4d)$

$\square$

# Solution

## Left to Prove:

- If $|X| > 2d\log_2(4dM_x)$, then $|X| > d\log_2(2|X|M_x + 1)$

## Proof.

- $|X| > 2d\log_2(4dM_x) \Rightarrow M_x < 2^{|X|/(2d)}/(4d)$
- $\Rightarrow 2|X|M_x + 1 < |X|/(2d) * 2^{|X|/(2d)} + 1 \leq 2^{|X|/(2d)}(|X|/(2d) + 1)$

$\square$

## Solution

### Left to Prove:

- If $|X| > 2d \log_2(4dM_x)$, then $|X| > d \log_2(2|X|M_x + 1)$

### Proof.

- $|X| > 2d \log_2(4dM_x) \Rightarrow M_x < 2^{|X|/(2d)}/(4d)$
- $\Rightarrow 2|X|M_x + 1 < |X|/(2d) * 2^{|X|/(2d)} + 1 \leq 2^{|X|/(2d)}(|X|/(2d) + 1)$
- $\Rightarrow d \log_2(2|X|M_x + 1) < |X|/2 + d \log_2(|X|/(2d) + 1) \leq |X|/2 + d * |X|/(2d)$

$\square$

# Solution

## Left to Prove:

- If $|X| > 2d \log_2(4dM_x)$, then $|X| > d \log_2(2|X|M_x + 1)$

## Proof.

- $|X| > 2d \log_2(4dM_x) \Rightarrow M_x < 2^{|X|/(2d)}/(4d)$
- $\Rightarrow 2|X|M_x + 1 < |X|/(2d) * 2^{|X|/(2d)} + 1 \leq 2^{|X|/(2d)}(|X|/(2d) + 1)$
- $\Rightarrow d \log_2(2|X|M_x + 1) < |X|/2 + d \log_2(|X|/(2d) + 1) \leq |X|/2 + d * |X|/(2d)$
- $\Rightarrow d \log_2(2|X|M_x + 1) < |X|$

$\square$

# Multisets

## Definition

- Multiset (bag) is a collection of elements where an element can occur several times
- Formally, multiset $m$ is a function $m : E \to \{0, 1, 2, \ldots\}$ ($E$ - finite universe)

## Example

$$m_1 = \{a, a, b, b, b\} \;\Rightarrow\; m_1(a) = 2 \; m_1(b) = 3 \; m_1(c) = 0$$
$$m_2 = \{a, b, c\} \;\Rightarrow\; m_2(a) = 1 \; m_2(b) = 1 \; m_2(c) = 1$$

## Definition

- Multiset (bag) is a collection of elements where an element can occur several times
- Formally, multiset $m$ is a function $m : E \rightarrow \{0, 1, 2, \ldots\}$ ($E$ - finite universe)

## Example

$m_1 = \{a, a, b, b, b\} \;\Rightarrow\; m_1(a) = 2\; m_1(b) = 3\; m_1(c) = 0$
$m_2 = \{a, b, c\} \;\Rightarrow\; m_2(a) = 1\; m_2(b) = 1\; m_2(c) = 1$

Selected operations and relations on multisets:

- Plus $(m_1 \uplus m_2)(e) = m_1(e) + m_2(e)$
  $m_1 \uplus m_2 = \{a, a, b, b, b, b, c\}$

# Multisets

## Definition

- Multiset (bag) is a collection of elements where an element can occur several times
- Formally, multiset $m$ is a function $m : E \to \{0, 1, 2, \ldots\}$ ($E$ - finite universe)

## Example

$$m_1 = \{a, a, b, b, b\} \;\Rightarrow\; m_1(a) = 2 \; m_1(b) = 3 \; m_1(c) = 0$$
$$m_2 = \{a, b, c\} \;\Rightarrow\; m_2(a) = 1 \; m_2(b) = 1 \; m_2(c) = 1$$

Selected operations and relations on multisets:

- Plus $(m_1 \uplus m_2)(e) = m_1(e) + m_2(e)$
- Intersection $(m_1 \cap m_2)(e) = \min\{m_1(e), m_2(e)\}$
  $m_1 \cap m_2 = \{a, b\}$

## Definition

- Multiset (bag) is a collection of elements where an element can occur several times
- Formally, multiset $m$ is a function $m : E \to \{0, 1, 2, \ldots\}$ ($E$ - finite universe)

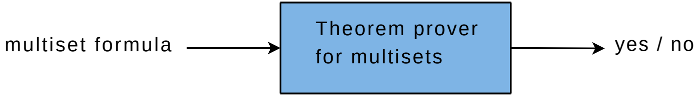
## Example

$m_1 = \{a, a, b, b, b\} \;\Rightarrow\; m_1(a) = 2 \; m_1(b) = 3 \; m_1(c) = 0$
$m_2 = \{a, b, c\} \;\Rightarrow\; m_2(a) = 1 \; m_2(b) = 1 \; m_2(c) = 1$

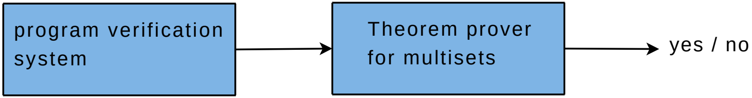
Selected operations and relations on multisets:

- Plus $(m_1 \uplus m_2)(e) = m_1(e) + m_2(e)$
- Intersection $(m_1 \cap m_2)(e) = \min\{m_1(e), m_2(e)\}$
- Subset $m_1 \subseteq m_2 \iff \forall e.\, m_1(e) \leq m_2(e)$

# Multisets in Software Analysis and Verification: Overview



# Multisets in Software Analysis and Verification: Overview



# Multisets in Software Analysis and Verification: Example

## Example

```
public void add(Object x)
ensures List = old List ⊎ {x}
{
    Node n = new Node();
    n.data = x;
    n.next = first;
    first = n;
}
```

- Formula expressing the correctness of insertion:
  $$|x| = 1 \rightarrow |L \uplus x| = |L| + 1$$
- To prove that it is valid, it is equivalent to show that its negation is unsatisfiable:
  $$|x| = 1 \wedge |L \uplus x| \neq |L| + 1$$

# Decision Procedure: Overview

1. reduce to normal form
2. replace multiset sums with“star” operator
3. find semilinear sets characterizing the set of solutions of formulas under the sum
4. generate PA formula for the results of sums
5. check satisfiability of resulting formula

## Presburger Arithmetic

Presburger Arithmetic (PA) is an arithmetic of natural numbers $(\mathbb{N}, \leq, +)$, without multiplication. It is decidable and there are decision procedures for deciding PA formulas.

# Decision Procedure: Example

## Example

- express all multiset expressions using $\forall e.\, F$

# Decision Procedure: Example

## Example

- express all multiset expressions using $\forall e.\, F$
  - $|x| = 1 \wedge |L \uplus x| \neq |L| + 1$

# Decision Procedure: Example

## Example

- express all multiset expressions using $\forall e.\, F$
  - $|x| = 1 \wedge |L \uplus x| \neq |L| + 1$
  - $|x| = 1 \wedge |y| \neq |L| + 1 \wedge y = L \uplus x$

# Decision Procedure: Example

## Example

- express all multiset expressions using $\forall e. F$
  - $|x| = 1 \land |L \uplus x| \neq |L| + 1$
  - $|x| = 1 \land |y| \neq |L| + 1 \land y = L \uplus x$
  - $|x| = 1 \land |y| \neq |L| + 1 \land \forall e. y(e) = L(e) + x(e)$

# Decision Procedure: Example

## Example

- express all multiset expressions using $\forall e.\ F$
- group all sums into one, using vectors:
  $\sum t_1 = k_1 \wedge \sum t_2 = k_2 \rightsquigarrow \sum(t_1, t_2) = (k_1, k_2)$

# Decision Procedure: Example

## Example

- express all multiset expressions using $\forall e.\, F$
- group all sums into one, using vectors:
  $\sum t_1 = k_1 \wedge \sum t_2 = k_2 \rightsquigarrow \sum (t_1, t_2) = (k_1, k_2)$
    - $\sum x(e) = 1 \wedge \sum y(e) \neq \sum L(e) + 1 \wedge$
      $\forall e.\, y(e) = L(e) + x(e)$

# Decision Procedure: Example

## Example

- express all multiset expressions using $\forall e.\, F$
- group all sums into one, using vectors:
  $\sum t_1 = k_1 \wedge \sum t_2 = k_2 \leadsto \sum (t_1, t_2) = (k_1, k_2)$
  - $\sum x(e) = 1 \wedge \sum y(e) \neq \sum L(e) + 1 \wedge$
    $\forall e.\, y(e) = L(e) + x(e)$
  - $\sum x(e) = 1 \wedge \sum y(e) = k_1 \wedge \sum L(e) = k_2 \wedge k_1 \neq k_2 + 1 \wedge$
    $\forall e.\, y(e) = L(e) + x(e)$

# Decision Procedure: Example

## Example

- express all multiset expressions using $\forall e.\, F$
- group all sums into one, using vectors:
  $\sum t_1 = k_1 \wedge \sum t_2 = k_2 \rightsquigarrow \sum (t_1, t_2) = (k_1, k_2)$
  - $\sum x(e) = 1 \wedge \sum y(e) \neq \sum L(e) + 1 \wedge$
    $\forall e.\, y(e) = L(e) + x(e)$
  - $\sum x(e) = 1 \wedge \sum y(e) = k_1 \wedge \sum L(e) = k_2 \wedge k_1 \neq k_2 + 1 \wedge$
    $\forall e.\, y(e) = L(e) + x(e)$
  - $k_1 \neq k_2 + 1 \wedge$
    $(1, k_1, k_2) = \sum (x(e), y(e), L(e)) \ \wedge\ \forall e.\, y(e) = L(e) + x(e)$

# Decision Procedure: Example

## Example

- express all multiset expressions using $\forall e. F$
- group all sums into one, using vectors:
  $\sum t_1 = k_1 \wedge \sum t_2 = k_2 \rightsquigarrow \sum(t_1, t_2) = (k_1, k_2)$
- replace multiset constraints with integer constraints enriched with "star" operator

# Decision Procedure: Example

## Example

- express all multiset expressions using $\forall e.\, F$
- group all sums into one, using vectors:
  $\sum t_1 = k_1 \land \sum t_2 = k_2 \rightsquigarrow \sum(t_1, t_2) = (k_1, k_2)$
- replace multiset constraints with integer constraints enriched with "star" operator
  - $k_1 \neq k_2 + 1 \land$
    $(1, k_1, k_2) = \sum(x(e), y(e), L(e)) \ \land \ \forall e.\, y(e) = L(e) + x(e)$

# Decision Procedure: Example

## Example

- express all multiset expressions using $\forall e.\, F$
- group all sums into one, using vectors:
  $\sum t_1 = k_1 \wedge \sum t_2 = k_2 \rightsquigarrow \sum(t_1, t_2) = (k_1, k_2)$
- replace multiset constraints with integer constraints enriched with “star” operator
  - $k_1 \neq k_2 + 1 \wedge$
    $(1, k_1, k_2) = \sum(x(e), y(e), L(e)) \;\wedge\; \forall e.\, y(e) = L(e) + x(e)$
  - $k_1 \neq k_2 + 1 \;\wedge\; (1, k_1, k_2) \in \{(x, y, L) \mid y = L + x\}^*$,

# Decision Procedure: Example

## Example

- express all multiset expressions using $\forall e.\, F$
- group all sums into one, using vectors:
  $\sum t_1 = k_1 \wedge \sum t_2 = k_2 \rightsquigarrow \sum(t_1, t_2) = (k_1, k_2)$
- replace multiset constraints with integer constraints enriched with "star" operator
  - $k_1 \neq k_2 + 1 \wedge$
    $(1, k_1, k_2) = \sum(x(e), y(e), L(e)) \ \wedge \ \forall e.\, y(e) = L(e) + x(e)$
  - $k_1 \neq k_2 + 1 \ \wedge \ (1, k_1, k_2) \in \{(x, y, L) \mid y = L + x\}^*$,
    where $S^* = \{x_1 + \ldots + x_n \mid x_i \in S \wedge n \geq 0\}$
    Note: $S^* = \text{cone}(S)$

# Multiset Elimination

## Theorem

*A formula in the sum normal form:*

$$P \ \wedge \ (u_1, \ldots, u_n) = \sum_{e \in E} (t_1, \ldots, t_n) \ \wedge \ \forall e.F$$

*is equisatisfiable with the formula*

$$P \ \wedge \ (u_1, \ldots, u_n) \in \{(t'_1, \ldots, t'_n) \mid F; \ x_1, \ldots, x_p \in \mathbb{N}\}^*$$

*where $t'_i$ is $t_i$ in which each $m_k(e)$ is replaced by fresh var $x_k$ and $C^* = \{v_1 + \ldots + v_n \mid v_i \in C \wedge n \geq 0\}$*

## Example

$$(1, k_1, k_2) = \sum (x(e), y(e), L(e)) \ \wedge \ \forall e.\, y(e) = L(e) + x(e)$$

$$(1, k_1, k_2) \in \{(x, y, L) \mid y = L + x; \ y, x, L \in \mathbb{N}\}^*$$

# Multiset Elimination

**Example**

$$(1, k_1, k_2) = \sum (x(e), y(e), L(e)) \;\wedge\; \forall e.\, y(e) = L(e) + x(e)$$

$$(1, k_1, k_2) \in \{(x, y, L) \mid y = L + x, y, x, L \in \mathbb{N}\}^*$$

**Proof.**

$\Leftarrow$ assume that $(u_1, \ldots, u_n) = (t_1^1, \ldots, t_n^1) + \ldots + (t_1^k, \ldots, t_n^k)$
We define set $E$ to have $k$ elements: $E = \{e_1, \ldots, e_k\}$
$m_i(e_j)$ has the value of corresponding $x_i^j$.
$\Rightarrow$ analogous, except that $E$ is given

$\square$

# Semilinear Sets

# Semilinear Sets

## Question

Can we describe $(u_1, \ldots, u_n) \in \{(t_1, \ldots, t_n) \mid F\}^*$ by PA formula?

## Definition

Let $C_1, C_2 \subseteq \mathbb{N}^k$ be sets of vectors of non-negative integers. We define:

$C_1 + C_2 = \{x_1 + x_2 \mid x_1 \in C_1 \wedge x_2 \in C_2\}$

$C_1^* = \{x_1 + \ldots + x_n \mid x_i \in C_1 \wedge n \geq 0\}$

# Semilinear Sets

## Question

Can we describe $(u_1, \ldots, u_n) \in \{(t_1, \ldots, t_n) \mid F\}^*$ by PA formula?

## Definition

Let $C_1, C_2 \subseteq \mathbb{N}^k$ be sets of vectors of non-negative integers. We define:

$C_1 + C_2 = \{x_1 + x_2 \mid x_1 \in C_1 \wedge x_2 \in C_2\}$

$C_1^* = \{x_1 + \ldots + x_n \mid x_i \in C_1 \wedge n \geq 0\}$

## Semilinear sets

Linear set = set of form $\{x\} + C^*$ for $x \in \mathbb{N}^n$ and $C \subseteq \mathbb{N}^n$ finite

Semilinear set = finite union of linear sets

# Semilinear Sets

## Question

Can we describe $(u_1, \ldots, u_n) \in \{(t_1, \ldots, t_n) \mid F\}^*$ by PA formula?

## Definition

Let $C_1, C_2 \subseteq \mathbb{N}^k$ be sets of vectors of non-negative integers. We define:

$C_1 + C_2 = \{x_1 + x_2 \mid x_1 \in C_1 \wedge x_2 \in C_2\}$
$C_1^* = \{x_1 + \ldots + x_n \mid x_i \in C_1 \wedge n \geq 0\}$

## Semilinear sets

Linear set = set of form $\{x\} + C^*$ for $x \in \mathbb{N}^n$ and $C \subseteq \mathbb{N}^n$ finite
Semilinear set = finite union of linear sets

## Example

$LS(2; 10) = \{2, 12, 22, 32, 42, 52, 62, \ldots\}$
$LS(5; 3, 5) = \{5, 8, 10, 11, 13, 14, 15, 16, 18, \ldots\}$

# Solution

- In [GinsburgSpanier1968] it was shown:
  - semilinear sets are closed under union, intersection and negation
  - a solution of PA formula is a semilinear set

# Solution

- In [GinsburgSpanier1968] it was shown:
  - semilinear sets are closed under union, intersection and negation
  - a solution of PA formula is a semilinear set
- We showed that if $S$ is a semilinear set, then $S^*$ is also a semilinear set

# Solution

- In [GinsburgSpanier1968] it was shown:
  - semilinear sets are closed under union, intersection and negation
  - a solution of PA formula is a semilinear set
- We showed that if $S$ is a semilinear set, then $S^*$ is also a semilinear set
- $$(u_1, \ldots, u_n) \in \{(t'_1, \ldots, t'_n) \mid F\}^*$$

  is effectively expressible as PA formula

# Example (Continued)

**Example**

- $k_1 \neq k_2 + 1 \wedge (1, k_1, k_2) \in \{(x, y, L) \mid y = L + x, y, x, L \in \mathbb{N}\}^*$

# Example (Continued)

**Example**

- $k_1 \neq k_2 + 1 \wedge (1, k_1, k_2) \in \{(x, y, L) \mid y = L + x, y, x, L \in \mathbb{N}\}^*$
- $\{(x, y, L) \mid y = L + x, y, x, L \in \mathbb{N}\}^*$ is described with semilinear set $LS((0,0,0); (1,1,0), (0,1,1))$

# Example (Continued)

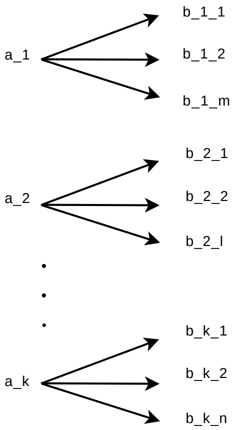
## Example

- $k_1 \neq k_2 + 1 \wedge (1, k_1, k_2) \in \{(x, y, L) \mid y = L + x, y, x, L \in \mathbb{N}\}^*$
- $\{(x, y, L) \mid y = L + x, y, x, L \in \mathbb{N}\}^*$ is described with semilinear set $LS((0,0,0); (1,1,0), (0,1,1))$
- $(1, k_1, k_2) \in \{(x, y, L) \mid y = L + x, y, x, L \in \mathbb{N}\}^*$ is equisatisfiable with:
  $(1, k_1, k_2) = \lambda_1\ (1,1,0) + \lambda_2(0,1,1)$

# Solution

- formula derived during the proof:

$$\exists \mu_i, \lambda_{ij}.\ (u_1, \ldots, u_n) = \sum_{i=1}^{k} (\mu_i a_i + \sum_{j=0}^{q_i} \lambda_{ij} b_{ij}) \wedge \bigwedge_{i=1}^{k} (\mu_i = 0 \implies \sum_{j=0}^{q_i} \lambda_{ij} = 0)$$



# Bounds on Solution Size

Our exponential formula looks like this:

$$P \wedge (u_1, \ldots, u_n) = \sum_{i=1}^{k} (\mu_i a_i + \sum_{j=1}^{q_i} \lambda_{ij} b_{ij}) \wedge \bigwedge_{i=1}^{k} (\mu_i = 0 \implies \sum_{j=1}^{q_i} \lambda_{ij} = 0)$$

Pottier 1991 - the solution set of $Ax = b$ is a semilinear set with $a_i, b_{ij}$ with polynomially many bits

Papadimitriou 1981 - bounds on PA formula solutions

- solution vector $(u_1, \ldots, u_n)$ has polynomially many bits, even for our exponential formulas!
- reason: formulas are exponential, but have polynomially many conjuncts

# Constructing Polynomially Large Formulas

# Picking Subset of $a_i$, $b_{ij}$

Our exponential formula looks like this:

$$P \wedge (u_1, \ldots, u_n) = \sum_{i=1}^{k} (\mu_i a_i + \sum_{j=1}^{q_i} \lambda_{ij} b_{ij}) \wedge \bigwedge_{i=1}^{k} (\mu_i = 0 \implies \sum_{j=1}^{q_i} \lambda_{ij} = 0)$$

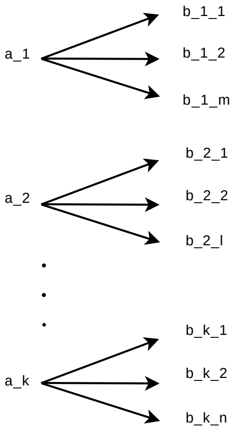
## Theorem

*If $u$ is generated by $a_i$, $b_{ij}$, then it is generated by polynomial subset of them.*

- proof generalizes results by Eisenbrand, Shmonin (2006)

# Proof

1. let $u = a + b$
2. apply Eisenbrand-Shmonin theorem as black box on $b_{ij}$ vectors
3. there are only polynomially vectors $b_{ij}$ needed to represent $b$
4. join them with associated $a_i$ vectors
5. apply Eisenbrand-Shmonin theorem on remaining $a_i$ vectors



# Idea: Guess $a_i$, $b_{ij}$?

Problem: how to check if a guessed vector is one of $a_i$ or $b_{ij}$?

Approach: instead of guessing $a_i$, $b_{ij}$, guess solutions $c$ where $F(c)$

Result:

$$P \wedge \vec{u} = \{\vec{v} \mid F\}^*$$

is equisatisfiable with

$$P \wedge \vec{u} = \sum_{i=1}^{Q} \lambda_i \vec{v}_i \wedge \bigwedge_{i=1}^{Q} F(\vec{v}_i)$$

where $Q$ polynomially large, can compute it from $F$

# Last Hurdle

$$P \wedge \vec{u} = \sum_{i=1}^{Q} \lambda_i \vec{v}_i \wedge \bigwedge_{i=1}^{Q} F(\vec{v}_i)$$

Polynomially large formula.

- but it multiplies variables $\lambda_i$, $v_i$ - not linear?
- nevertheless: vectors bounded, can expand multiplication

Result: NP completeness!

# Conclusions

Presented

- result on Carathéodory bounds for integer cones
- language used for reasoning about properties of data structures
- new decision procedure for quantifier-free multiset formulas with cardinality operator
- optimal complexity result: NP-completeness
- algorithm: generating polynomially large PA formulas