Contejean-Devie Algorithm for Solving Systems of Linear Diophantine Equations

Temur Kutsia

RISC

March 15, 2012

Sailors, a Monkey, and Coconuts

- Five sailors and a monkey survive a shipwreck and reach an island with coconuts. Before dawn, they gather a few of them and decide to sleep first and share the next day.

Sailors, a Monkey, and Coconuts

- Five sailors and a monkey survive a shipwreck and reach an island with coconuts. Before dawn, they gather a few of them and decide to sleep first and share the next day.
- Soon one of them wakes up, divides the nuts into five parts, gives the only remaining nut to the monkey, saves his share away and sleeps again. Later, the other four do the same.

Sailors, a Monkey, and Coconuts

- Five sailors and a monkey survive a shipwreck and reach an island with coconuts. Before dawn, they gather a few of them and decide to sleep first and share the next day.
- Soon one of them wakes up, divides the nuts into five parts, gives the only remaining nut to the monkey, saves his share away and sleeps again. Later, the other four do the same.
- When they all wake up in the morning, they count the nuts, divide them into five parts, take their share, and give the last remaining nut to the monkey.

Sailors, a Monkey, and Coconuts

- Five sailors and a monkey survive a shipwreck and reach an island with coconuts. Before dawn, they gather a few of them and decide to sleep first and share the next day.
- Soon one of them wakes up, divides the nuts into five parts, gives the only remaining nut to the monkey, saves his share away and sleeps again. Later, the other four do the same.
- When they all wake up in the morning, they count the nuts, divide them into five parts, take their share, and give the last remaining nut to the monkey.

How many nuts were there at the beginning?

Coconuts and Diophantine Systems

- x_0: The total number of nuts.
- x_i: The number of nuts taken away by i's sailor.
- x_6: The number of nuts obtained by each at the last sharing.

Coconuts and Diophantine Systems

- x_0: The total number of nuts.
- x_i: The number of nuts taken away by i's sailor.
- x_6: The number of nuts obtained by each at the last sharing.
- Natural solutions of the linear Diophantine system:

$$\begin{aligned} x_0 &= 5x_1 + 1 \\ 4x_1 &= 5x_2 + 1 \\ 4x_2 &= 5x_3 + 1 \\ 4x_3 &= 5x_4 + 1 \\ 4x_4 &= 5x_5 + 1 \\ 4x_5 &= 5x_6 + 1 \end{aligned}$$

- How to find these solutions?

Contejean-Devie Algorithm

Evelyne Contejean and Hervé Devie.
An Efficient Incremental Algorithm for Solving Systems of Linear Diophantine Equations.
Information and Computation 113(1): 143–172 (1994).

Contejean-Devie Algorithm

Evelyne Contejean and Hervé Devie.
An Efficient Incremental Algorithm for Solving Systems of Linear Diophantine Equations.
Information and Computation 113(1): 143–172 (1994).

Generalizes Fortenbacher's Algorithm for solving a single equation:

Michael Clausen and Albrecht Fortenbacher.
Efficient Solution of Linear Diophantine Equations.
J. Symbolic Computation 8(1,2): 201–216 (1989).

Homogeneous Case

Homogeneous linear Diophantine system with m equations and n variables:

$$\begin{cases} a_{11}x_1 & + \cdots + & a_{1n}x_n & = & 0 \\ \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + \cdots + & a_{mn}x_n & = & 0 \end{cases}$$

- a_{ij}'s are integers.
- Looking for nontrivial natural solutions.

Homogeneous Case

Example

$$\begin{cases} - x_1 + x_2 + 2x_3 - 3x_4 = 0 \\ - x_1 + 3x_2 - 2x_3 - x_4 = 0 \end{cases}$$

Nontrivial solutions:

- $s_1 = (0, 1, 1, 1)$
- $s_2 = (4, 2, 1, 0)$
- $s_3 = (0, 2, 2, 2)$
- $s_4 = (8, 4, 2, 0)$
- $s_5 = (4, 3, 2, 1)$
- $s_6 = (8, 5, 3, 1)$
- $\ldots$

Homogeneous Case

Example

$$\begin{cases} -x_1 + x_2 + 2x_3 - 3x_4 = 0 \\ -x_1 + 3x_2 - 2x_3 - x_4 = 0 \end{cases}$$

Nontrivial solutions:

- $s_1 = (0, 1, 1, 1)$
- $s_2 = (4, 2, 1, 0)$
- $s_3 = (0, 2, 2, 2) = 2s_1$
- $s_4 = (8, 4, 2, 0) = 2s_2$
- $s_5 = (4, 3, 2, 1) = s_1 + s_2$
- $s_6 = (8, 5, 3, 1) = s_1 + 2s_2$
- $\ldots$

Homogeneous Case

Homogeneous linear Diophantine system with m equations and n variables:

$$\begin{cases} a_{11}x_1 & + \cdots + & a_{1n}x_n & = & 0 \\ \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + \cdots + & a_{mn}x_n & = & 0 \end{cases}$$

- a_{ij}'s are integers.
- Looking for a basis in the set of nontrivial natural solutions.

Homogeneous Case

Homogeneous linear Diophantine system with m equations and n variables:

$$\begin{cases} a_{11}x_1 & + \cdots + & a_{1n}x_n & = & 0 \\ \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + \cdots + & a_{mn}x_n & = & 0 \end{cases}$$

- a_{ij}'s are integers.
- Looking for a basis in the set of nontrivial natural solutions.
- Does it exist?

Homogeneous Case

The basis in the set S of nontrivial natural solutions of a homogeneous LDS is the set of $\gg$-minimal elements S.

$\gg$ is the ordering on tuples of natural numbers:

$$(x_1, \ldots, x_n) \gg (y_1, \ldots, y_n)$$

if and only if

- $x_i \geq y_i$ for all $1 \leq i \leq n$ and
- $x_i > y_i$ for some $1 \leq i \leq n$.

Matrix Form

Homogeneous linear Diophantine system with m equations and n variables:

$$Ax_{\downarrow} = 0_{\downarrow},$$

where

$$A := \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \quad x_{\downarrow} := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad 0_{\downarrow} := \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Matrix Form

- Canonical basis in $\mathbb{N}^n$: $(e_{1\downarrow}, \ldots, e_{n\downarrow})$.
- $e_{j\downarrow} = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$, with 1 in j's row.
- Then $Ax_\downarrow = x_1 Ae_{1\downarrow} + \cdots + x_n Ae_{n\downarrow}$.

Matrix Form

- Canonical basis in $\mathbb{N}^n$: $(e_{1\downarrow}, \ldots, e_{n\downarrow})$.
- $e_{j\downarrow} = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$, with 1 in j's row.
- Then $Ax_\downarrow = x_1 Ae_{1\downarrow} + \cdots + x_n Ae_{n\downarrow}$.
- a: The linear mapping associated to A.
- Then $a(x_\downarrow) = x_1 a(e_{1\downarrow}) + \cdots + x_n a(e_{n\downarrow})$.

Single Equation: Idea

Case $m = 1$: Single homogeneous LDE $a_1x_1 + \cdots + a_nx_n = 0$.
Fortenbacher's idea:

- Search minimal solutions starting from the elements in the canonical basis of $\mathbb{N}^n$.
- Suppose the current vector $v_\downarrow$ is not a solution.
- It can be nondeterministically increased, component by component, until it becomes a solution or greater than a solution.
- To decrease the search space, the following restrictions can be imposed:
  - If $a(v_\downarrow) > 0$, then increase by one some v_j with $a_j < 0$.
  - If $a(v_\downarrow) < 0$, then increase by one some v_j with $a_j > 0$.

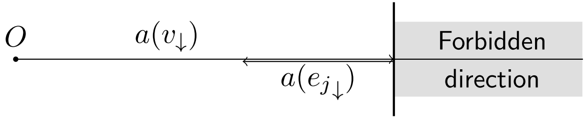
Single Equation: Idea

Case $m = 1$: Single homogeneous LDE $a_1x_1 + \cdots + a_nx_n = 0$.
Fortenbacher's idea:

- Search minimal solutions starting from the elements in the canonical basis of $\mathbb{N}^n$.
- Suppose the current vector $v_{\downarrow}$ is not a solution.
- It can be nondeterministically increased, component by component, until it becomes a solution or greater than a solution.
- To decrease the search space, the following restrictions can be imposed:
  - If $a(v_{\downarrow}) > 0$, then increase by one some v_j with $a_j < 0$.
  - If $a(v_{\downarrow}) < 0$, then increase by one some v_j with $a_j > 0$.
  - (If $a(v_{\downarrow})a(e_{j_{\downarrow}}) < 0$ for some j, increase v_j by one.)

Single Equation: Geometric Interpretation of the Idea

- Fortenbacher's condition
  If $a(v_\downarrow)a(e_{j_\downarrow}) < 0$ for some j, increase v_j by one.
- Increasing v_j by one: $a(v_\downarrow + e_{j_\downarrow}) = a(v_\downarrow) + a(e_{j_\downarrow})$.
- Going to the "right direction", towards the origin.



Single Equation: Algorithm

Case $m = 1$: Single homogeneous LDE $a_1x_1 + \cdots + a_nx_n = 0$.
Fortenbacher's algorithm:

Single Equation: Algorithm

Case $m = 1$: Single homogeneous LDE $a_1 x_1 + \cdots + a_n x_n = 0$.
Fortenbacher's algorithm:

- Start with the pair P, M of the set of potential solutions $P = \{e_{1\downarrow}, \ldots, e_{n\downarrow}\}$ and the set of minimal nontrivial solutions $M = \emptyset$.

Single Equation: Algorithm

Case $m = 1$: Single homogeneous LDE $a_1 x_1 + \cdots + a_n x_n = 0$.
Fortenbacher's algorithm:

- Start with the pair P, M of the set of potential solutions $P = \{e_{1\downarrow}, \ldots, e_{n\downarrow}\}$ and the set of minimal nontrivial solutions $M = \emptyset$.
- Apply repeatedly the rules:

Single Equation: Algorithm

Case $m = 1$: Single homogeneous LDE $a_1 x_1 + \cdots + a_n x_n = 0$.
Fortenbacher's algorithm:

- Start with the pair P, M of the set of potential solutions $P = \{e_{1\downarrow}, \ldots, e_{n\downarrow}\}$ and the set of minimal nontrivial solutions $M = \emptyset$.
- Apply repeatedly the rules:

  1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M$,
     if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.

Single Equation: Algorithm

Case $m = 1$: Single homogeneous LDE $a_1 x_1 + \cdots + a_n x_n = 0$.
Fortenbacher's algorithm:

- Start with the pair P, M of the set of potential solutions $P = \{e_{1\downarrow}, \ldots, e_{n\downarrow}\}$ and the set of minimal nontrivial solutions $M = \emptyset$.
- Apply repeatedly the rules:
  1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M$,
     if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
  2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M$,
     if $a(v_\downarrow) = 0$ and rule 1 is not applicable.

Single Equation: Algorithm

Case $m = 1$: Single homogeneous LDE $a_1 x_1 + \cdots + a_n x_n = 0$.
Fortenbacher's algorithm:

- Start with the pair P, M of the set of potential solutions $P = \{e_{1\downarrow}, \ldots, e_{n\downarrow}\}$ and the set of minimal nontrivial solutions $M = \emptyset$.
- Apply repeatedly the rules:

  1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M$,
     if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
  2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M$,
     if $a(v_\downarrow) = 0$ and rule 1 is not applicable.
  3. $P, M \Longrightarrow \{v_\downarrow + e_{j\downarrow} \mid v_\downarrow \in P,\ a(v_\downarrow)a(e_{j\downarrow}) < 0,\ j \in 1..n\}, M$,
     if rules 1 and 2 are not applicable.

Single Equation: Algorithm

Case $m = 1$: Single homogeneous LDE $a_1 x_1 + \cdots + a_n x_n = 0$.
Fortenbacher's algorithm:

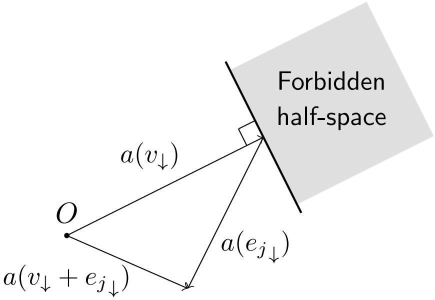
- Start with the pair P, M of the set of potential solutions $P = \{e_{1\downarrow}, \ldots, e_{n\downarrow}\}$ and the set of minimal nontrivial solutions $M = \emptyset$.
- Apply repeatedly the rules:
  1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M$,
     if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
  2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M$,
     if $a(v_\downarrow) = 0$ and rule 1 is not applicable.
  3. $P, M \Longrightarrow \{v_\downarrow + e_{j\downarrow} \mid v_\downarrow \in P,\ a(v_\downarrow)a(e_{j\downarrow}) < 0,\ j \in 1..n\}, M$,
     if rules 1 and 2 are not applicable.
- If $\emptyset, M$ is reached, return M.

System of Equations: Idea

- General case: System of homogeneous LDEs.
- $a(x_{\downarrow}) = 0_{\downarrow}$.
- Generalizing Fortenbacher's idea:
  - Search minimal solutions starting from the elements in the canonical basis of $\mathbb{N}^n$.
  - Suppose the current vector $v_{\downarrow}$ is not a solution.
  - It can be nondeterministically increased, component by component, until it becomes a solution or greater than a solution.
  - To decrease the search space, increase only those components that lead to the "right direction".

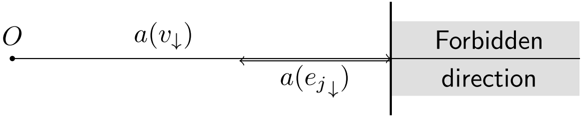
System of Equations: How to Restrict

- "Right direction": Towards the origin.
- If $a(v_\downarrow) \neq 0_\downarrow$, then do $a(v_\downarrow + e_{j_\downarrow}) = a(v_\downarrow) + a(e_{j_\downarrow})$.
- $a(v_\downarrow) + a(e_{j_\downarrow})$ should lie in the half-space containing O.
- Contejean-Devie condition: If $a(v_\downarrow) \cdot a(e_{j_\downarrow}) < 0$ for some j, increase v_j by one. ($\cdot$ is the scalar product.)

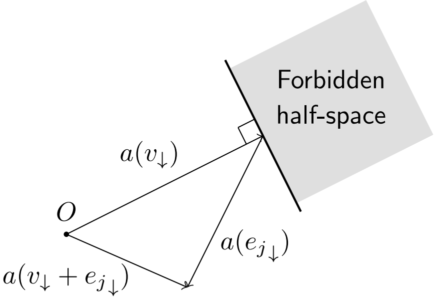


How to Restrict: Comparison

- Fortenbacher's condition
  If $a(v_\downarrow)a(e_{j\downarrow}) < 0$ for some j, increase v_j by one.



- Contejean-Devie condition
  If $a(v_\downarrow) \cdot a(e_{j\downarrow}) < 0$ for some j, increase v_j by one.



System of Equations: Algorithm

System of homogeneous LDEs: $a(x_\downarrow) = 0_\downarrow$.
Contejean-Devie algorithm:

- Start with the pair P, M where
  - $P = \{e_{1\downarrow}, \dots, e_{n\downarrow}\}$ is the set of potential solutions,
  - $M = \emptyset$ is the set of minimal nontrivial solutions.
- Apply repeatedly the rules:

  1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M$,
     if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
  2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M$,
     if $a(v_\downarrow) = 0_\downarrow$ and rule 1 is not applicable.
  3. $P, M \Longrightarrow \{v_\downarrow + e_{j\downarrow} \mid v_\downarrow \in P,\, a(v_\downarrow) \cdot a(e_{j\downarrow}) < 0,\, j \in 1..n\}, M$,
     if rules 1 and 2 are not applicable.

- If $\emptyset, M$ is reached, return M.

Contejean-Devie Algorithm on an Example

$$\begin{cases} - & x_1 & + & x_2 & + & 2x_3 & - & 3x_4 & = & 0 \\ - & x_1 & + & 3x_2 & - & 2x_3 & - & x_4 & = & 0 \end{cases}$$

$$e_{1\downarrow} = (1,0,0,0)^T \quad e_{2\downarrow} = (0,1,0,0)^T$$
$$e_{3\downarrow} = (0,0,1,0)^T \quad e_{4\downarrow} = (0,0,0,1)^T$$

1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M$,
   if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M$,
   if $a(v_\downarrow) = 0_\downarrow$ and rule 1 is not applicable.
3. $P, M \Longrightarrow \{v_\downarrow + e_{j\downarrow} \mid v_\downarrow \in P, a(v_\downarrow) \cdot a(e_{j\downarrow}) < 0,\ j \in 1..n\}, M$,
   if rules 1 and 2 are not applicable.

Contejean-Devie Algorithm on an Example

$$\begin{cases} -\ x_1 + x_2 + 2x_3 - 3x_4 = 0 \\ -\ x_1 + 3x_2 - 2x_3 - x_4 = 0 \end{cases}$$

$e_{1\downarrow} = (1,0,0,0)^T \quad e_{2\downarrow} = (0,1,0,0)^T$

$e_{3\downarrow} = (0,0,1,0)^T \quad e_{4\downarrow} = (0,0,0,1)^T$

1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M$,
   if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M$,
   if $a(v_\downarrow) = 0_\downarrow$ and rule 1 is not applicable.
3. $P, M \Longrightarrow \{v_\downarrow + e_{j\downarrow} \mid v_\downarrow \in P,$
   $a(v_\downarrow) \cdot a(e_{j\downarrow}) < 0,\ j \in 1..n\}, M$,
   if rules 1 and 2 are not applicable.

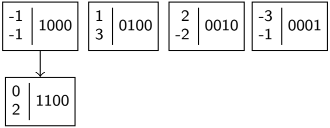
$\boxed{\begin{array}{r|l} -1 & \\ & 1000 \\ -1 & \end{array}}$ $\boxed{\begin{array}{r|l} 1 & \\ & 0100 \\ 3 & \end{array}}$ $\boxed{\begin{array}{r|l} 2 & \\ & 0010 \\ -2 & \end{array}}$ $\boxed{\begin{array}{r|l} -3 & \\ & 0001 \\ -1 & \end{array}}$

Contejean-Devie Algorithm on an Example

$$\left\{\begin{array}{rrrrrrrrrr} - & x_1 & + & x_2 & + & 2x_3 & - & 3x_4 & = & 0 \\ - & x_1 & + & 3x_2 & - & 2x_3 & - & x_4 & = & 0 \end{array}\right.$$

$$e_{1\downarrow} = (1,0,0,0)^T \quad e_{2\downarrow} = (0,1,0,0)^T$$
$$e_{3\downarrow} = (0,0,1,0)^T \quad e_{4\downarrow} = (0,0,0,1)^T$$

1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M$, if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M$, if $a(v_\downarrow) = 0_\downarrow$ and rule 1 is not applicable.
3. $P, M \Longrightarrow \{v_\downarrow + e_{j\downarrow} \mid v_\downarrow \in P, a(v_\downarrow)\cdot a(e_{j\downarrow}) < 0,\ j \in 1..n\}, M$, if rules 1 and 2 are not applicable.



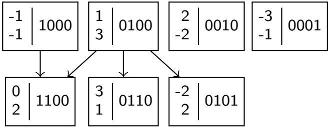
Contejean-Devie Algorithm on an Example

$$\begin{cases} -\ x_1 + x_2 + 2x_3 - 3x_4 = 0 \\ -\ x_1 + 3x_2 - 2x_3 - x_4 = 0 \end{cases}$$

$e_{1\downarrow} = (1,0,0,0)^T \quad e_{2\downarrow} = (0,1,0,0)^T$

$e_{3\downarrow} = (0,0,1,0)^T \quad e_{4\downarrow} = (0,0,0,1)^T$

1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M$, if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M$, if $a(v_\downarrow) = 0_\downarrow$ and rule 1 is not applicable.
3. $P, M \Longrightarrow \{v_\downarrow + e_{j\downarrow} \mid v_\downarrow \in P, a(v_\downarrow) \cdot a(e_{j\downarrow}) < 0,\ j \in 1..n\}, M$, if rules 1 and 2 are not applicable.

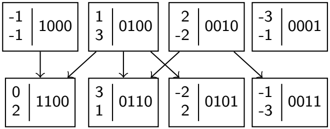


Contejean-Devie Algorithm on an Example

$$\left\{\begin{array}{rrrrrrrrr} - & x_1 & + & x_2 & + & 2x_3 & - & 3x_4 & = & 0 \\ - & x_1 & + & 3x_2 & - & 2x_3 & - & x_4 & = & 0 \end{array}\right.$$

$$e_{1\downarrow} = (1,0,0,0)^T \quad e_{2\downarrow} = (0,1,0,0)^T$$
$$e_{3\downarrow} = (0,0,1,0)^T \quad e_{4\downarrow} = (0,0,0,1)^T$$

1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M$,
   if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M$,
   if $a(v_\downarrow) = 0_\downarrow$ and rule 1 is not applicable.
3. $P, M \Longrightarrow \{v_\downarrow + e_{j\downarrow} \mid v_\downarrow \in P, a(v_\downarrow) \cdot a(e_{j\downarrow}) < 0,\ j \in 1..n\}, M$,
   if rules 1 and 2 are not applicable.



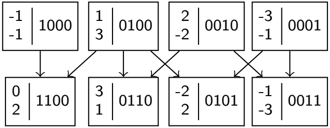
Contejean-Devie Algorithm on an Example

$$\begin{cases} -\ x_1 + x_2 + 2x_3 - 3x_4 = 0 \\ -\ x_1 + 3x_2 - 2x_3 - x_4 = 0 \end{cases}$$

$e_{1\downarrow} = (1,0,0,0)^T \quad e_{2\downarrow} = (0,1,0,0)^T$

$e_{3\downarrow} = (0,0,1,0)^T \quad e_{4\downarrow} = (0,0,0,1)^T$

1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M,$
   if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M,$
   if $a(v_\downarrow) = 0_\downarrow$ and rule 1 is not applicable.
3. $P, M \Longrightarrow \{v_\downarrow + e_{j\downarrow} \mid v_\downarrow \in P,$
   $a(v_\downarrow) \cdot a(e_{j\downarrow}) < 0,\ j \in 1..n\}, M,$
   if rules 1 and 2 are not applicable.



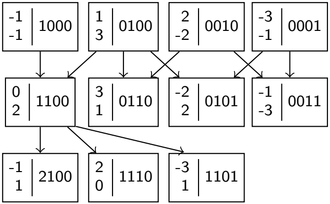
Contejean-Devie Algorithm on an Example

$$\begin{cases} -x_1 + x_2 + 2x_3 - 3x_4 = 0 \\ -x_1 + 3x_2 - 2x_3 - x_4 = 0 \end{cases}$$

$e_{1\downarrow} = (1,0,0,0)^T \quad e_{2\downarrow} = (0,1,0,0)^T$

$e_{3\downarrow} = (0,0,1,0)^T \quad e_{4\downarrow} = (0,0,0,1)^T$

1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M$, if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M$, if $a(v_\downarrow) = 0_\downarrow$ and rule 1 is not applicable.
3. $P, M \Longrightarrow \{v_\downarrow + e_{j\downarrow} \mid v_\downarrow \in P, a(v_\downarrow) \cdot a(e_{j\downarrow}) < 0,\ j \in 1..n\}, M$, if rules 1 and 2 are not applicable.



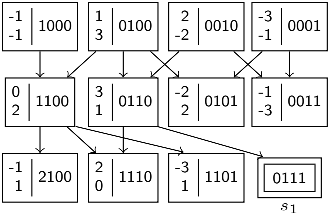
Contejean-Devie Algorithm on an Example

$$\begin{cases} -x_1 + x_2 + 2x_3 - 3x_4 = 0 \\ -x_1 + 3x_2 - 2x_3 - x_4 = 0 \end{cases}$$

$e_{1\downarrow} = (1,0,0,0)^T \quad e_{2\downarrow} = (0,1,0,0)^T$

$e_{3\downarrow} = (0,0,1,0)^T \quad e_{4\downarrow} = (0,0,0,1)^T$

1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M,$
   if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M,$
   if $a(v_\downarrow) = 0_\downarrow$ and rule 1 is not applicable.
3. $P, M \Longrightarrow \{v_\downarrow + e_{j_\downarrow} \mid v_\downarrow \in P, a(v_\downarrow) \cdot a(e_{j_\downarrow}) < 0,\ j \in 1..n\}, M,$
   if rules 1 and 2 are not applicable.



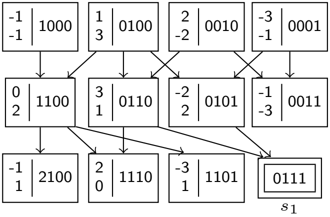
Contejean-Devie Algorithm on an Example

$$\begin{cases} -\ x_1 + x_2 + 2x_3 - 3x_4 = 0 \\ -\ x_1 + 3x_2 - 2x_3 - x_4 = 0 \end{cases}$$

$e_{1\downarrow} = (1,0,0,0)^T \quad e_{2\downarrow} = (0,1,0,0)^T$

$e_{3\downarrow} = (0,0,1,0)^T \quad e_{4\downarrow} = (0,0,0,1)^T$

1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M,$ if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M,$ if $a(v_\downarrow) = 0_\downarrow$ and rule 1 is not applicable.
3. $P, M \Longrightarrow \{v_\downarrow + e_{j\downarrow} \mid v_\downarrow \in P, a(v_\downarrow) \cdot a(e_{j\downarrow}) < 0,\ j \in 1..n\}, M,$ if rules 1 and 2 are not applicable.



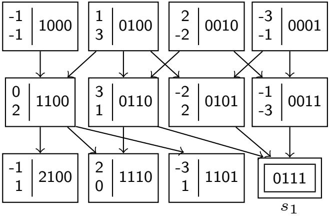
Contejean-Devie Algorithm on an Example

$$\left\{\begin{array}{rrrrrrrrr} - & x_1 & + & x_2 & + & 2x_3 & - & 3x_4 & = & 0 \\ - & x_1 & + & 3x_2 & - & 2x_3 & - & x_4 & = & 0 \end{array}\right.$$

$e_{1\downarrow} = (1,0,0,0)^T \quad e_{2\downarrow} = (0,1,0,0)^T$

$e_{3\downarrow} = (0,0,1,0)^T \quad e_{4\downarrow} = (0,0,0,1)^T$

1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M$,
   if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M$,
   if $a(v_\downarrow) = 0_\downarrow$ and rule 1 is not applicable.
3. $P, M \Longrightarrow \{v_\downarrow + e_{j_\downarrow} \mid v_\downarrow \in P, a(v_\downarrow) \cdot a(e_{j_\downarrow}) < 0,\ j \in 1..n\}, M$,
   if rules 1 and 2 are not applicable.

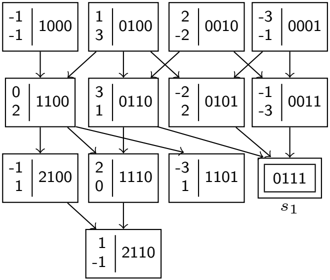


Contejean-Devie Algorithm on an Example

$$\begin{cases} -x_1 + x_2 + 2x_3 - 3x_4 = 0 \\ -x_1 + 3x_2 - 2x_3 - x_4 = 0 \end{cases}$$

$e_{1\downarrow} = (1,0,0,0)^T \quad e_{2\downarrow} = (0,1,0,0)^T$
$e_{3\downarrow} = (0,0,1,0)^T \quad e_{4\downarrow} = (0,0,0,1)^T$

1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M$,
   if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M$,
   if $a(v_\downarrow) = 0_\downarrow$ and rule 1 is not applicable.
3. $P, M \Longrightarrow \{v_\downarrow + e_{j\downarrow} \mid v_\downarrow \in P, a(v_\downarrow) \cdot a(e_{j\downarrow}) < 0,\ j \in 1..n\}, M$,
   if rules 1 and 2 are not applicable.

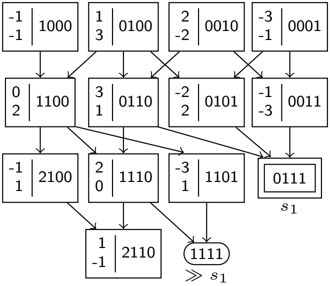


Contejean-Devie Algorithm on an Example

$$\begin{cases} -x_1 + x_2 + 2x_3 - 3x_4 = 0 \\ -x_1 + 3x_2 - 2x_3 - x_4 = 0 \end{cases}$$

$e_{1\downarrow} = (1,0,0,0)^T \quad e_{2\downarrow} = (0,1,0,0)^T$
$e_{3\downarrow} = (0,0,1,0)^T \quad e_{4\downarrow} = (0,0,0,1)^T$

1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M,$
   if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M,$
   if $a(v_\downarrow) = 0_\downarrow$ and rule 1 is not applicable.
3. $P, M \Longrightarrow \{v_\downarrow + e_{j\downarrow} \mid v_\downarrow \in P,$
   $a(v_\downarrow) \cdot a(e_{j\downarrow}) < 0,\ j \in 1..n\}, M,$
   if rules 1 and 2 are not applicable.



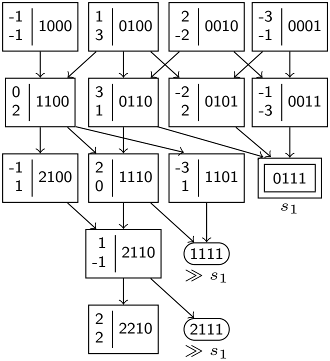
Contejean-Devie Algorithm on an Example

$$\left\{\begin{array}{rrrrrrrrr} - & x_1 & + & x_2 & + & 2x_3 & - & 3x_4 & = & 0 \\ - & x_1 & + & 3x_2 & - & 2x_3 & - & x_4 & = & 0 \end{array}\right.$$

$e_{1\downarrow} = (1,0,0,0)^T \quad e_{2\downarrow} = (0,1,0,0)^T$

$e_{3\downarrow} = (0,0,1,0)^T \quad e_{4\downarrow} = (0,0,0,1)^T$

1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M$,
   if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M$,
   if $a(v_\downarrow) = 0_\downarrow$ and rule 1 is not applicable.
3. $P, M \Longrightarrow \{v_\downarrow + e_{j\downarrow} \mid v_\downarrow \in P, a(v_\downarrow) \cdot a(e_{j\downarrow}) < 0, \; j \in 1..n\}, M$,
   if rules 1 and 2 are not applicable.



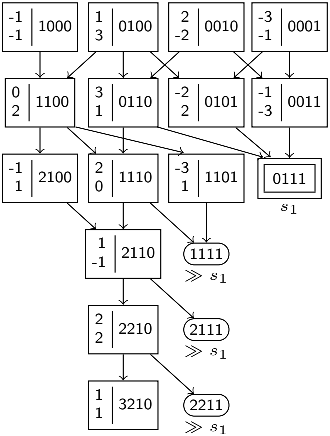
Contejean-Devie Algorithm on an Example

$$\begin{cases} -x_1 + x_2 + 2x_3 - 3x_4 = 0 \\ -x_1 + 3x_2 - 2x_3 - x_4 = 0 \end{cases}$$

$e_{1\downarrow} = (1,0,0,0)^T \quad e_{2\downarrow} = (0,1,0,0)^T$

$e_{3\downarrow} = (0,0,1,0)^T \quad e_{4\downarrow} = (0,0,0,1)^T$

1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M,$
   if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M,$
   if $a(v_\downarrow) = 0_\downarrow$ and rule 1 is not applicable.
3. $P, M \Longrightarrow \{v_\downarrow + e_{j\downarrow} \mid v_\downarrow \in P, a(v_\downarrow)\cdot a(e_{j\downarrow}) < 0,\ j \in 1..n\}, M,$
   if rules 1 and 2 are not applicable.



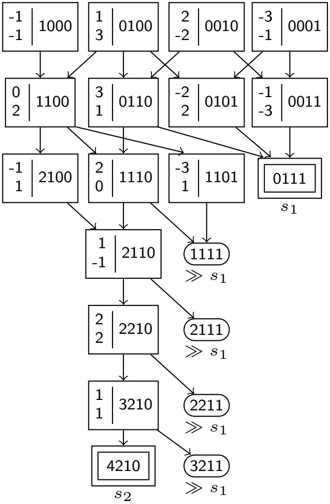
Contejean-Devie Algorithm on an Example

$$\begin{cases} -\ x_1 + x_2 + 2x_3 - 3x_4 = 0 \\ -\ x_1 + 3x_2 - 2x_3 - x_4 = 0 \end{cases}$$

$e_{1\downarrow} = (1,0,0,0)^T \quad e_{2\downarrow} = (0,1,0,0)^T$

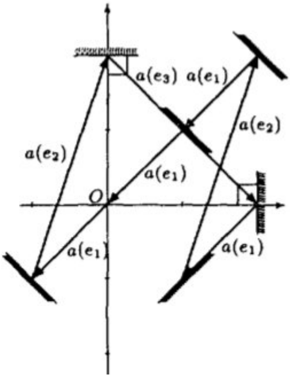
$e_{3\downarrow} = (0,0,1,0)^T \quad e_{4\downarrow} = (0,0,0,1)^T$

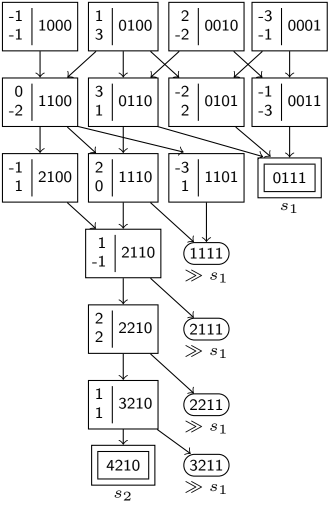
1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M$,
   if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M$,
   if $a(v_\downarrow) = 0_\downarrow$ and rule 1 is not applicable.
3. $P, M \Longrightarrow \{v_\downarrow + e_{j\downarrow} \mid v_\downarrow \in P,$
   $a(v_\downarrow)\cdot a(e_{j\downarrow}) < 0,\ j \in 1..n\}, M$,
   if rules 1 and 2 are not applicable.



Contejean-Devie Algorithm on an Example

$$\left\{\begin{array}{rrrrrrrrr} - & x_1 & + & x_2 & + & 2x_3 & - & 3x_4 & = & 0 \\ - & x_1 & + & 3x_2 & - & 2x_3 & - & x_4 & = & 0 \end{array}\right.$$





Properties of the Algorithm

Properties to be proved:

- Completeness
- Soundness
- Termination

In the theorems:

$a(x_\downarrow) = 0_\downarrow$: An n-variate system of homogeneous LDEs.

$(e_{1\downarrow}, \ldots, e_{n\downarrow})$: The canonical basis of $\mathbb{N}^n$.

$\mathcal{B}(a(x_\downarrow) = 0_\downarrow)$: Basis in the set of nontrivial natural solutions of $a(x_\downarrow) = 0_\downarrow$.

$\|v_\downarrow\|$: Euclidean norm of $v_\downarrow$.

Properties of the Algorithm

Theorem (Completeness)

Let $(e_{1\downarrow}, \ldots, e_{n\downarrow}), \emptyset \Longrightarrow^* \emptyset, M$ *be the sequence of transformations performed by the Contejean-Devie algorithm for* $a(x_\downarrow) = 0_\downarrow$*. Then*

$$\mathcal{B}(a(x_\downarrow) = 0_\downarrow) \subseteq M.$$

Properties of the Algorithm

Theorem (Soundness)

Let $(e_{1\downarrow}, \ldots, e_{n\downarrow}), \emptyset \Longrightarrow^* \emptyset, M$ *be the sequence of transformations performed by the Contejean-Devie algorithm for* $a(x_\downarrow) = 0_\downarrow$. *Then*

$$M \subseteq \mathcal{B}(a(x_\downarrow) = 0_\downarrow).$$

Properties of the Algorithm

Lemma (Limit Lemma)

Let $v_{1\downarrow}, v_{2\downarrow}, \ldots$ *be an infinite sequence satisfying the Contejean-Devie condition for* $a(x_\downarrow) = 0_\downarrow$*:*

- $v_{1\downarrow}$ *is a basic vector and for each* $i \geq 1$ *there exists* $1 \leq j \leq n$ *such that* $a(v_{i\downarrow}) \cdot a(e_{j\downarrow}) < 0$ *and* $v_{i+1\downarrow} = v_{i\downarrow} + e_{j\downarrow}$.

Then

$$\lim_{k \to \infty} \frac{\|a(v_{k\downarrow})\|}{k} = 0$$

Theorem (Termination)

Let $v_{1\downarrow}, v_{2\downarrow}, \ldots$ *be an infinite sequence satisfying the conditions of the Limit Lemma. Then there exist* $v_\downarrow$ *and* k *such that*

- $v_\downarrow$ *is a solution of* $a(x_\downarrow) = 0_\downarrow$*, and*
- $v_\downarrow \ll v_{k\downarrow}$.

Non-Homogeneous Case

Non-homogeneous linear Diophantine system with m equations and n variables:

$$\left\{\begin{array}{ccccc} a_{11}x_1 & + \cdots + & a_{1n}x_n & = & b_1 \\ \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + \cdots + & a_{mn}x_n & = & b_m \end{array}\right.$$

- a's and b's are integers.
- Matrix form: $a(x_\downarrow) = b_\downarrow$.

Non-Homogeneous Case. Solving Idea

Turn the system into a homogeneous one, denoted S_0:

$$\left\{\begin{array}{ccccccccc} -b_1 x_0 & + & a_{11}x_1 & + & \cdots & + & a_{1n}x_n & = & 0 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ -b_m x_0 & + & a_{m1}x_1 & + & \cdots & + & a_{mn}x_n & = & 0 \end{array}\right.$$

- Solve S_0 and keep only the solutions with $x_0 \leq 1$.
- $x_0 = 1$: a minimal solution for $a(x_\downarrow) = b_\downarrow$.
- $x_0 = 0$: a minimal solution for $a(x_\downarrow) = 0_\downarrow$.
- Any solution of the non-homogeneous system $a(x_\downarrow) = b_\downarrow$ has the form $x_\downarrow + y_\downarrow$ where:
  - $x_\downarrow$ is a minimal solution of $a(x_\downarrow) = b_\downarrow$.
  - $y_\downarrow$ is a linear combination (with natural coefficients) of minimal solutions of $a(x_\downarrow) = 0_\downarrow$.

Further Topics

- Optimizations:
  - From a dag to a forest: Depth-first version.
  - From a forest to a stack: Space-efficient version.
- Constrained systems: Add constraints like, e.g., $c_{\downarrow} \gg x_{\downarrow} \gg d_{\downarrow}$ for the set of minimal solutions $x_{\downarrow}$ "between" $c_{\downarrow}$ and $d_{\downarrow}$.
- Incrementality.
- Equations and Inequalities.
- Classification of algorithms. Approaches using
  - polynomial rings,
  - structure of solution cone,
  - dags.