

Introduction to Unification Theory

Solving Systems of Linear Diophantine Equations

Temur Kutsia

RISC, Johannes Kepler University of Linz, Austria
kutsia@risc.jku.at



ACU-Unification

- ▶ We saw an example how to solve ACU-unification problem.
- ▶ Reduction to systems of linear Diophantine equations (LDEs) over natural numbers.



Elementary ACU-Unification

- ▶ Elementary ACU-unification problem

$$\{f(x, f(x, y)) \doteq_{ACU}^? f(z, f(z, z))\}$$

reduces to homogeneous linear Diophantine equation

$$2x + y = 3z.$$

- ▶ Each equation in the unification problem gives rise to one linear Diophantine equation.
- ▶ A most general ACU-unifier is obtained by combining all the unifiers corresponding to the minimal solutions of the system of LDEs.



Elementary ACU-Unification

- ▶ $\Gamma = \{f(x, f(x, y)) \stackrel{?}{\dot{=}}_{ACU} f(z, f(z, z))\}$ and $S = \{2x + y = 3z\}$.
- ▶ S has three minimal solutions: $(1, 1, 1), (0, 3, 1), (3, 0, 2)$.
- ▶ Three unifiers of Γ :

$$\sigma_1 = \{x \mapsto v_1, y \mapsto v_1, z \mapsto v_1\}$$

$$\sigma_2 = \{x \mapsto e, y \mapsto f(v_2, f(v_2, v_2)), z \mapsto v_2\}$$

$$\sigma_3 = \{x \mapsto f(v_3, f(v_3, v_3)), y \mapsto e, z \mapsto f(v_3, v_3)\}$$

- ▶ A most general unifier of Γ :

$$\sigma = \{x \mapsto f(v_1, f(v_3, f(v_3, v_3))), y \mapsto f(v_1, f(v_2, f(v_2, v_2))), \\ z \mapsto f(v_1, f(v_2, f(v_3, v_3)))\}$$



ACU-Unification with constants

- ▶ ACU-unification problem with constants

$$\Gamma = \{f(x, f(x, y)) \stackrel{?}{\doteq}_{ACU} f(a, f(z, f(z, z)))\}$$

reduces to inhomogeneous linear Diophantine equation

$$S = \{2x + y = 3z + 1\}.$$

- ▶ The minimal nontrivial natural solutions of S are $(0, 1, 0)$ and $(2, 0, 1)$.



ACU-Unification with constants

- ▶ ACU-unification problem with constants

$$\Gamma = \{f(x, f(x, y)) \doteq_{ACU}^? f(a, f(z, f(z, z)))\}$$

reduces to inhomogeneous linear Diophantine equation

$$S = \{2x + y = 3z + 1\}.$$

- ▶ Every natural solution of S is obtained by as the sum of one of the minimal solution and a solution of the corresponding homogeneous LDE $2x + y = 3z$.
- ▶ One element of the minimal complete set of unifiers of Γ is obtained from the combination of one minimal solution of S with the set of all minimal solutions of $2x + y = 3z$.



ACU-Unification with constants

- ▶ ACU-unification problem with constants

$$\Gamma = \{f(x, f(x, y)) \stackrel{?}{\doteq}_{ACU} f(a, f(z, f(z, z)))\}$$

reduces to inhomogeneous linear Diophantine equation

$$S = \{2x + y = 3z + 1\}.$$

- ▶ The minimal complete set of unifiers of Γ is $\{\sigma_1, \sigma_2\}$, where

$$\begin{aligned}\sigma_1 &= \{x \mapsto f(v_1, f(v_3, f(v_3, v_3))), \\ &\quad y \mapsto f(a, f(v_1, f(v_2, f(v_2, v_2)))), \\ &\quad z \mapsto f(v_1, f(v_2, f(v_3, v_3)))\} \\ \sigma_2 &= \{x \mapsto f(a, f(a, f(v_1, f(v_3, f(v_3, v_3))))) , \\ &\quad y \mapsto f(v_1, f(v_2, f(v_2, v_2))), \\ &\quad z \mapsto f(a, f(v_1, f(v_2, f(v_3, v_3))))\}\end{aligned}$$



How to Solve Systems of LDEs over Naturals?

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).



How to Solve Systems of LDEs over Naturals?

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:

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

- ▶ 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:

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



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:

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



Homogeneous Case

Homogeneous linear Diophantine system with m equations and n variables:

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

- ▶ 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:

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

- ▶ 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:

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

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 : $(e_{1\downarrow}, \dots, e_{n\downarrow})$.

- ▶ $e_{j\downarrow} = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$, with 1 in j 's row.

- ▶ Then $Ax_{\downarrow} = x_1 Ae_{1\downarrow} + \dots + x_n Ae_{n\downarrow}$.



Matrix Form

- ▶ Canonical basis in \mathbb{N}^n : $(e_{1\downarrow}, \dots, e_{n\downarrow})$.

- ▶ $e_{j\downarrow} = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$, with 1 in j 's row.

- ▶ Then $Ax_{\downarrow} = x_1 Ae_{1\downarrow} + \dots + x_n Ae_{n\downarrow}$.
- ▶ a : The linear mapping associated to A .
- ▶ Then $a(x_{\downarrow}) = x_1 a(e_{1\downarrow}) + \dots + x_n a(e_{n\downarrow})$.



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.)



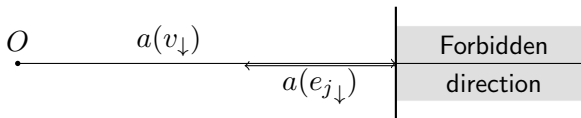
Single Equation: Geometric Interpretation of the Idea

- ▶ 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 $a_1x_1 + \cdots + a_nx_n = 0$.

Fortenbacher's algorithm:

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



Single Equation: Algorithm

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

Fortenbacher's algorithm:

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



Single Equation: Algorithm

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

Fortenbacher's algorithm:

- ▶ Start with the pair P, M of the set of potential solutions $P = \{e_{1\downarrow}, \dots, e_{n\downarrow}\}$ and the set of minimal nontrivial solutions $M = \emptyset$.
- ▶ Apply repeatedly the rules:
 1. $\{v_{\downarrow}\} \cup P', M \implies P', M$,
if $v_{\downarrow} \gg u_{\downarrow}$ for some $u_{\downarrow} \in M$.



Single Equation: Algorithm

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

Fortenbacher's algorithm:

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



Single Equation: Algorithm

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

Fortenbacher's algorithm:

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



Single Equation: Algorithm

Case $m = 1$: Single homogeneous LDE $a_1x_1 + \dots + a_nx_n = 0$.

Fortenbacher's algorithm:

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



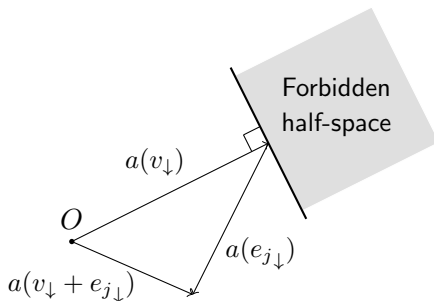
System of Equations: Idea

- ▶ 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

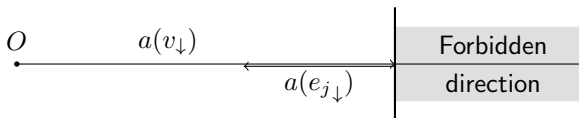
- ▶ “Right direction”: Towards the origin.
- ▶ If $a(v_{\downarrow}) \neq 0_{\downarrow}$, then do $a(v_{\downarrow} + e_{j\downarrow}) = a(v_{\downarrow}) + a(e_{j\downarrow})$.
- ▶ $a(v_{\downarrow}) + a(e_{j\downarrow})$ should lie in the half-space containing O .
- ▶ **Contejean-Devie condition:** 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

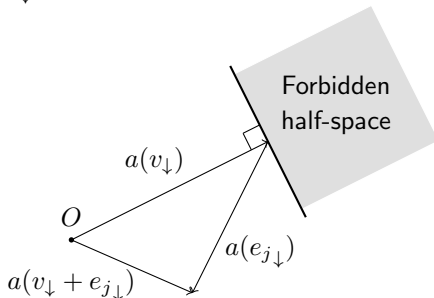
► Fortenbacher's condition

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



Contejean-Devie Algorithm on an Example

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

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

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

$\begin{array}{c c} -1 & 1000 \\ -1 & \end{array}$	$\begin{array}{c c} 1 & 0100 \\ 3 & \end{array}$	$\begin{array}{c c} 2 & 0010 \\ -2 & \end{array}$	$\begin{array}{c c} -3 & 0001 \\ -1 & \end{array}$
--	--	---	--

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

$\begin{array}{c c} -1 & 1000 \\ -1 & \end{array}$	$\begin{array}{c c} 1 & 0100 \\ 3 & \end{array}$	$\begin{array}{c c} 2 & 0010 \\ -2 & \end{array}$	$\begin{array}{c c} -3 & 0001 \\ -1 & \end{array}$
--	--	---	--

↓

$\begin{array}{c c} 0 & 1100 \\ 2 & \end{array}$
--



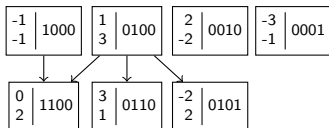
Contejean-Devie Algorithm on an Example

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

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

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

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



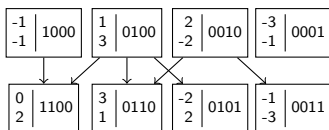
Contejean-Devie Algorithm on an Example

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

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

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

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



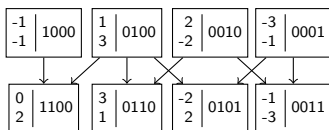
Contejean-Devie Algorithm on an Example

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

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

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

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



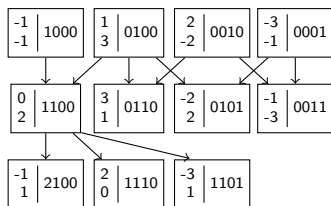
Contejean-Devie Algorithm on an Example

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

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

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

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



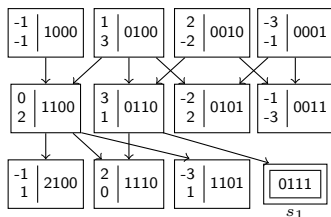
Contejean-Devie Algorithm on an Example

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

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

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

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



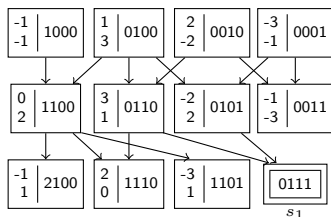
Contejean-Devie Algorithm on an Example

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

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

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

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



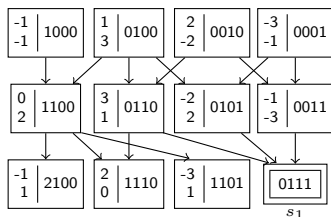
Contejean-Devie Algorithm on an Example

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

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

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

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



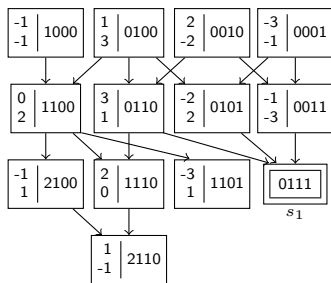
Contejean-Devie Algorithm on an Example

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

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

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

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



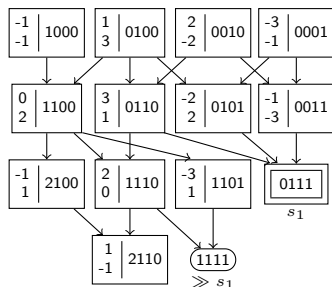
Contejean-Devie Algorithm on an Example

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

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

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

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



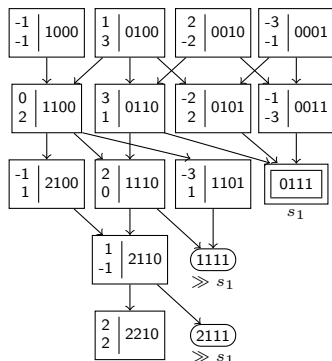
Contejean-Devie Algorithm on an Example

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

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

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

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



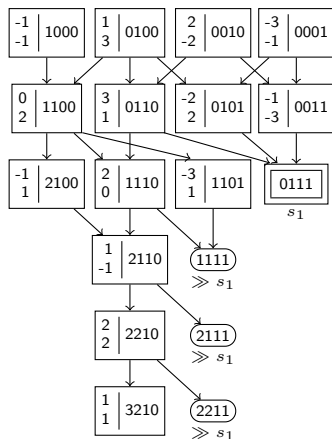
Contejean-Devie Algorithm on an Example

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

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

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

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



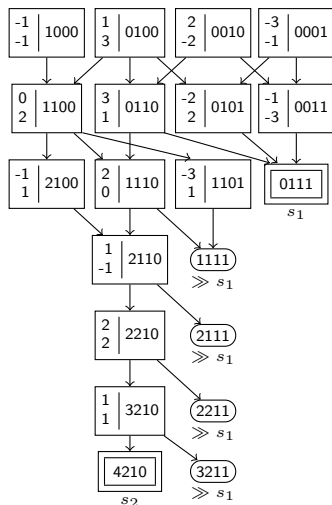
Contejean-Devie Algorithm on an Example

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

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

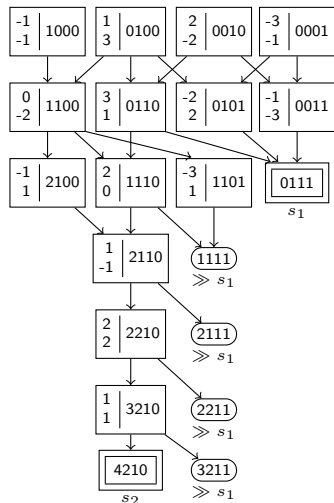
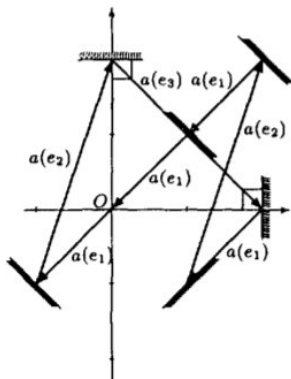
$$e_{3\downarrow} = (0, 0, 1, 0)^T \quad e_{4\downarrow} = (0, 0, 0, 1)^T$$

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



Contejean-Devie Algorithm on an Example

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



Properties of the Algorithm

- ▶ Completeness
- ▶ Soundness
- ▶ Termination

In the theorems:

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

$(e_{1\downarrow}, \dots, e_{n\downarrow})$: 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 $(e_{1\downarrow}, \dots, e_{n\downarrow}), \emptyset \Longrightarrow^ \emptyset, M$ 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 $(e_{1\downarrow}, \dots, e_{n\downarrow}), \emptyset \Longrightarrow^ \emptyset, M$ 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 $v_{1\downarrow}, v_{2\downarrow}, \dots$ 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

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

Theorem (Termination)

Let $v_{1\downarrow}, v_{2\downarrow}, \dots$ 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:

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

- ▶ 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 :

$$\begin{cases} -b_1x_0 + a_{11}x_1 + \cdots + a_{1n}x_n = 0 \\ \vdots \qquad \qquad \qquad \vdots \qquad \qquad \qquad \vdots \qquad \qquad \qquad \vdots \\ -b_mx_0 + a_{m1}x_1 + \cdots + a_{mn}x_n = 0 \end{cases}$$

- ▶ 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 $a(x_{\downarrow}) = 0_{\downarrow}$.

