A lemma on polyhedral sets of lattice points

Bruno Haible
Mathematisches Institut II
Universität Karlsruhe
D – W 7500 Karlsruhe 1 (until 30 June 1993)
D – 76131 Karlsruhe (from 1st July 1993 on)
Email: <haible@ma2s2.mathematik.uni-karlsruhe.de>

4 May 1993

This paper proves a lemma on decompositions of polyhedral sets of lattice points. It is a summary of the Lemma in section 4.1 of [1].

1. Results

Lemma 1:
Let $A \in \mathbb{Z}^{m\times n}$, $b \in \mathbb{Z}^m$ and $\substack{\geq \\ = \\ <}$ be a set of m equality or inequality signs. Then the set $\left\{x \in \mathbb{N}_0{}^n : Ax \substack{\geq \\ = \\ <} b\right\}$ can be written as disjoint union of finitely many sets of type $u + V \cdot \mathbb{N}_0{}^k$ with $u \in \mathbb{N}_0{}^n$ and $V \in \mathbb{Z}^{n\times k}$, $\operatorname{rank} V = k$.

Proof:
For $u \in \mathbb{N}_0{}^n$ and $V \in \mathbb{Z}^{n\times k}$ we call the set $u + V \cdot \mathbb{N}_0{}^k = \bigcup_{z\in\mathbb{N}_0{}^k} \{u + V \cdot z\}$ a *lattice cone* if this union is disjoint, i.e. if $\operatorname{rank} V = k$. Every finite disjoint union of lattice cones is called a *lattice cone union*.
Case 1: The case of one equality. We prove that $\{x \in \mathbb{N}_0{}^n : Ax = b\}$ with $A \in \mathbb{Z}^{1\times n}$ and $b \in \mathbb{Z}$ is a lattice cone union. Write $A = (a_1, \ldots, a_n)$.
Case 1a: all $a_i \in \{-1, 0, 1\}$.
Let r denote the number of i with $a_i = 1$ and s denote the number of i with $a_i = -1$. We prove the claim by induction on $r + s$. In the case $s = 0$, we have an equation $x_1 + \cdots + x_r = b$, which leads to a finite disjoint union of copies of $\mathbb{N}_0{}^{n-r}$ (consider the cases $b < 0$; $b = 0$; $b > 0, r = 0$; $b > 0, r > 0$ separately). The case $r = 0$ is similar.
In the case $r \geq 1$, $s \geq 1$ we may assume $a_1 = 1$ and $a_2 = -1$. We split the set $\{x \in \mathbb{N}_0{}^n : Ax = b\}$ according to whether $x_1 \geq x_2$ or $x_1 < x_2$ holds. To get $\{x \in \mathbb{N}_0{}^n : Ax = b, x_1 \geq x_2\}$, one has to multiply $\left\{\begin{pmatrix} y \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{N}_0{}^n : y + a_3x_3 + \cdots + a_nx_n = b\right\}$ (which is a lattice cone union by induction hypothesis) by $\begin{pmatrix} 1 & 1 & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} \in \mathrm{GL}_n(\mathbb{Z})$. The set $\{x \in \mathbb{N}_0{}^n : Ax = b, x_1 + 1 \leq x_2\}$ is handled in a similar way.
$\{x \in \mathbb{N}_0{}^n : Ax = b\}$ is the disjoint union of both.
Case 1b: the general case $A \in \mathbb{Z}^{1\times n}$, $A \neq 0$.

Let g be the least common multiple of those $|a_i|$ that are non-zero. Put $d_i = 1$ if $a_i = 0$ and $d_i = \frac{g}{|a_i|}$ otherwise. We have $d_i \in \mathbb{N}$ and $a_i \cdot d_i = g \cdot \operatorname{sgn} a_i$ for $i = 1, \ldots, n$.

We split the set $\{x \in {\mathbb{N}_0}^n : Ax = b\}$ according to $x_i \mod d_i$. For $r = (r_1, \ldots, r_n)$, $0 \le r_1 < d_1$, ..., $0 \le r_n < d_n$ let $X_r = \{x \in {\mathbb{N}_0}^n : Ax = b, \forall i : x_i \equiv r_i \mod d_i\}$. Then $X_r = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix} \cdot Y_r + \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}$ with $Y_r = \left\{ y \in {\mathbb{N}_0}^n : (\operatorname{sgn} a_1)y_1 + \cdots (\operatorname{sgn} a_n)y_n = \frac{b - a_1 r_1 - \cdots - a_n r_n}{g} \right\}$ if g divides $b - a_1 r_1 - \cdots - a_n r_n$ and $Y_r = \emptyset$ otherwise. Thus X_r is a lattice cone union, and so is X, the disjoint union of all these X_r.

Case 2: The case of one inequality.

Case 2a: Let $L = \{x \in {\mathbb{N}_0}^n : Ax \le b\}$. Introduce an auxiliary variable y and consider

$$M = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \\ y \end{pmatrix} \in {\mathbb{N}_0}^{n+1} : a_1 x_1 + \cdots a_n x_n + y = b \right\}.$$

M is a lattice cone union by case 1, and since the projection $\left\{ \begin{matrix} M & \to L \\ \begin{pmatrix} x \\ y \end{pmatrix} & \mapsto x \end{matrix} \right\}$ is bijective, L is a lattice cone union.

Case 2b: $\{x \in {\mathbb{N}_0}^n : Ax < b\} = \{x \in {\mathbb{N}_0}^n : Ax \le b - 1\}$.

Case 2c: $\{x \in {\mathbb{N}_0}^n : Ax \ge b\} = \{x \in {\mathbb{N}_0}^n : (-A)x \le -b\}$.

Case 2d: $\{x \in {\mathbb{N}_0}^n : Ax > b\} = \{x \in {\mathbb{N}_0}^n : Ax \ge b + 1\}$.

Case 3: The general case of several equations and inequalities. Proceed by induction on m, the number of equality/inequality signs. $m = 0$ is trivial: ${\mathbb{N}_0}^n$. Assume we have proven $\left\{x \in {\mathbb{N}_0}^n : Ax \underset{<}{\overset{>}{=}} b\right\}$ to be a disjoint union $\bigcup_i \left(u_i + V_i \cdot {\mathbb{N}_0}^k\right)$ (with k depending on i), and we add one more equality/inequality $A'x \underset{<}{\overset{>}{=}} b'$. What we get is $\bigcup_i \left(u_i + V_i \cdot \left\{z \in {\mathbb{N}_0}^k : A'V_i z \underset{<}{\overset{>}{=}} b' - A'u_i\right\}\right)$ which is a lattice cone union by cases 1 and 2: $\bigcup_i \left(u_i + V_i \cdot \bigcup_j \left(u_{i,j} + V_{i,j} \cdot {\mathbb{N}_0}^{k_{i,j}}\right)\right) = \bigcup_i \bigcup_j \left(u_i + V_i u_{i,j} + V_i V_{i,j} \cdot {\mathbb{N}_0}^{k_{i,j}}\right)$. **q.e.d.**

Corollary 2:

Let R be an integral domain and $P(x) \in R[x_1, \ldots, x_n]$ a polynomial. Then

$$F(Z) = \sum_{\substack{x \in {\mathbb{N}_0}^n \\ Ax \underset{<}{\overset{>}{=}} b}} P(x) Z^x$$

is a rational function[1]: $F \in R(Z_1, \ldots, Z_n)$.

Proof:

Case 1: The case $F(Z) = \sum_{x \in {\mathbb{N}_0}^n} P(x) Z^x$. This is proved to be rational by considering the derivatives of

$$\sum_{x \in {\mathbb{N}_0}^n} Z^x = \prod_{i=1}^n \frac{1}{1 - Z_i},$$

namely

$$\sum_{x \in {\mathbb{N}_0}^n} x_1 \cdots (x_1 - c_1 + 1) \cdots x_n \cdots (x_n - c_n + 1) Z^x = \left(\frac{\partial}{\partial Z_1}\right)^{c_1} \cdots \left(\frac{\partial}{\partial Z_n}\right)^{c_n} \prod_{i=1}^n \frac{1}{1 - Z_i} = \prod_{i=1}^n \frac{1}{(1 - Z_i)^{c_i + 1}}.$$

[1] ^{1}) $R(Z_1, \ldots, Z_n)$ denotes the quotient field of the polynomial ring $R[Z_1, \ldots, Z_n]$.

Case 2: The general case. By the lemma, $F(Z)$ can be written as a finite sum of functions of the form

$$\sum_{x \in \mathbb{N}_0{}^k} P(u + V \cdot x) Z^{u+V\cdot x} = Z^u \sum_{x \in \mathbb{N}_0{}^k} Q(x) Z^{V\cdot x} = Z^u G(Z_1{}^{v_{11}} \cdots Z_n{}^{v_{n1}}, \ldots, Z_1{}^{v_{1k}} \cdots Z_n{}^{v_{nk}})$$

where $Q(x) := P(u + V \cdot x)$ is a polynomial and $G(T) = \sum_{x \in \mathbb{N}_0{}^k} Q(x) T^x$ is in $R(T_1, \ldots, T_k)$ by case 1. Since V has rank k, the substitution $T_1 = Z_1{}^{v_{11}} \cdots Z_n{}^{v_{n1}}, \ldots, T_k = Z_1{}^{v_{1k}} \cdots Z_n{}^{v_{nk}}$ gives rise to an injective ring homomorphism $R[T_1, \ldots, T_k] \to R(Z_1, \ldots, Z_n)$ and thus to a field homomorphism $R(T_1, \ldots, T_k) \to R(Z_1, \ldots, Z_n)$. This implies that $F(Z)$ is rational. **q.e.d.**

2. Reference

[1] Bruno Haible: D-finite Potenzreihen in mehreren Variablen. Diplomarbeit, Universität Karlsruhe, June 1989.