

Linear Inequalities*

Ralph Bottesch¹, Alban Reynaud², and René Thiemann¹

¹University of Innsbruck

²ENS Lyon

March 8, 2026

Abstract

We formalize results about linear inequalities, mainly from Schrijver's book [3]. The main results are the proof of the fundamental theorem on linear inequalities, Farkas' lemma, Carathéodory's theorem, the Farkas-Minkowsky-Weyl theorem, the decomposition theorem of polyhedra, and Meyer's result that the integer hull of a polyhedron is a polyhedron itself. Several theorems include bounds on the appearing numbers, and in particular we provide an a-priori bound on mixed-integer solutions of linear inequalities.

Contents

1	Introduction	2
2	Missing Lemmas on Vectors and Matrices	3
3	Missing Lemmas on Vector Spaces	9
4	Basis Extension	11
5	Sum of Vector Sets	12
6	Integral and Bounded Matrices and Vectors	13
7	Cones	18
8	Convex Hulls	21
9	Normal Vectors	24

*Supported by FWF (Austrian Science Fund) project Y757.

10 Dimension of Spans	26
11 The Fundamental Theorem of Linear Inequalities	27
12 Farkas' Lemma	30
13 The Theorem of Farkas, Minkowsky and Weyl	30
14 The Decomposition Theorem	31
15 Mixed Integer Solutions	34
16 Integer Hull	37

1 Introduction

The motivation for this formalization is the aim of developing a verified theory solver for linear integer arithmetic. Such a solver can be a combination of a simplex-implementation within a branch-and-bound approach, that might also utilize Gomory cuts [1, Section 4 of the extended version]. However, the branch-and-bound algorithm does not terminate in general, since the search space is infinite. To solve this latter problem, one can use results of Papadimitriou: he showed that whenever a set of linear inequalities has an integer solution, then it also has a small solution, where the bound on such a solution can be computed easily from the input [2].

In this entry, we therefore formalize several results on linear inequalities which are required to obtain the desired bound, by following the proofs of Schrijver's textbook [3, Sections 7 and 16].

We start with basic definitions and results on cones, convex hulls, and polyhedra. Next, we verify the fundamental theorem of linear inequalities, which in our formalization shows the equivalence of four statements to describe a cone. From this theorem, one easily derives Farkas' Lemma and Carathéodory's theorem. Moreover we verify the Farkas-Minkowsky-Weyl theorem, that a convex cone is polyhedral if and only if it is finitely generated, and use this result to obtain the decomposition theorem for polyhedra, i.e., that a polyhedron can always be decomposed into a polytope and a finitely generated cone. For most of the previously mentioned results, we include bounds, so that in particular we have a quantitative version of the decomposition theorem, which provides bounds on the vectors that construct the polytope and the cone, and where these bounds are computed directly from the input polyhedron that should be decomposed.

We further prove the decomposition theorem also for the integer hull of a polyhedron, using the same bounds, which gives rise to small integer solutions for linear inequalities. We finally formalize a direct proof for the

more general case of mixed integer solutions, where we also permit both strict and non-strict linear inequalities.

Theorem 1. Consider $A_1 \in \mathbb{Z}^{m_1 \times n}$, $b_1 \in \mathbb{Z}^{m_1}$, $A_2 \in \mathbb{Z}^{m_2 \times n}$, $b_2 \in \mathbb{Z}^{m_2}$. Let β be a bound on A_1, b_1, A_2, b_2 , i.e., $\beta \geq |z|$ for all numbers z that occur within A_1, b_1, A_2, b_2 . Let $n = n_1 + n_2$. Then if $x \in \mathbb{Z}^{n_1} \times \mathbb{R}^{n_2} \subseteq \mathbb{R}^n$ is a mixed integer solution of the linear inequalities, i.e., $A_1 x \leq b_1$ and $A_2 x < b_2$, then there also exists a mixed integer solution $y \in \mathbb{Z}^{n_1} \times \mathbb{R}^{n_2}$ where $|y_i| \leq (n+1) \cdot \sqrt{n} \cdot \beta^n$ for each entry y_i of y .

The verified bound in Theorem 1 in particular implies that integer-satisfiability of linear-inequalities with integer coefficients is in NP.

2 Missing Lemmas on Vectors and Matrices

We provide some results on vector spaces which should be merged into Jordan-Normal-Form/Matrix.

theory *Missing-Matrix*

imports *Jordan-Normal-Form.Matrix*

begin

lemma *orthogonalD'*: **assumes** *orthogonal vs*

and $v \in \text{set } vs$ **and** $w \in \text{set } vs$

shows $(v \cdot w = 0) = (v \neq w)$

<proof>

lemma *zero-mat-mult-vector[simp]*: $x \in \text{carrier-vec } nc \implies 0_m \text{ nr } nc *_{\cdot} x = 0_v$
nr

<proof>

lemma *add-diff-cancel-right-vec*:

$a \in \text{carrier-vec } n \implies (b :: 'a :: \text{cancel-ab-semigroup-add vec}) \in \text{carrier-vec } n \implies$

$(a + b) - b = a$

<proof>

lemma *elements-four-block-mat-id*:

assumes $c: A \in \text{carrier-mat } nr1 \ nc1$ $B \in \text{carrier-mat } nr1 \ nc2$

$C \in \text{carrier-mat } nr2 \ nc1$ $D \in \text{carrier-mat } nr2 \ nc2$

shows

$\text{elements-mat } (\text{four-block-mat } A \ B \ C \ D) =$

$\text{elements-mat } A \cup \text{elements-mat } B \cup \text{elements-mat } C \cup \text{elements-mat } D$

(**is** $\text{elements-mat } ?four = ?X$)

<proof>

lemma *elements-mat-append-rows*: $A \in \text{carrier-mat } nr \ n \implies B \in \text{carrier-mat } nr^2$
 $n \implies$

$\text{elements-mat } (A @_r B) = \text{elements-mat } A \cup \text{elements-mat } B$

<proof>

lemma *elements-mat-uminus[simp]*: $\text{elements-mat } (-A) = \text{uminus } \text{'elements-mat } A$

<proof>

lemma *vec-set-uminus[simp]*: $\text{vec-set } (-A) = \text{uminus } \text{'vec-set } A$

<proof>

definition *append-cols* :: $\text{'a} :: \text{zero mat} \Rightarrow \text{'a mat} \Rightarrow \text{'a mat}$ (**infixr** $\langle @_c \rangle$ 65)

where

$$A @_c B = (A^T @_r B^T)^T$$

lemma *carrier-append-cols[simp, intro]*:

$$A \in \text{carrier-mat } nr \ nc1 \Longrightarrow$$

$$B \in \text{carrier-mat } nr \ nc2 \Longrightarrow (A @_c B) \in \text{carrier-mat } nr \ (nc1 + nc2)$$

<proof>

lemma *elements-mat-transpose-mat[simp]*: $\text{elements-mat } (A^T) = \text{elements-mat } A$

<proof>

lemma *elements-mat-append-cols*: $A \in \text{carrier-mat } n \ nc \Longrightarrow B \in \text{carrier-mat } n \ nc1$

$$\Longrightarrow \text{elements-mat } (A @_c B) = \text{elements-mat } A \cup \text{elements-mat } B$$

<proof>

lemma *vec-first-index*:

assumes $v: \text{dim-vec } v \geq n$

and $i: i < n$

shows $(\text{vec-first } v \ n) \ \$ \ i = v \ \$ \ i$

<proof>

lemma *vec-last-index*:

assumes $v: v \in \text{carrier-vec } (n + m)$

and $i: i < m$

shows $(\text{vec-last } v \ m) \ \$ \ i = v \ \$ \ (n + i)$

<proof>

lemma *vec-first-add*:

assumes $\text{dim-vec } x \geq n$

and $\text{dim-vec } y \geq n$

shows $\text{vec-first } (x + y) \ n = \text{vec-first } x \ n + \text{vec-first } y \ n$

<proof>

lemma *vec-first-zero[simp]*: $m \leq n \Longrightarrow \text{vec-first } (0_v \ n) \ m = 0_v \ m$

<proof>

lemma *vec-first-smult*:

$$\llbracket m \leq n; x \in \text{carrier-vec } n \rrbracket \Longrightarrow \text{vec-first } (c \cdot_v x) \ m = c \cdot_v \text{vec-first } x \ m$$

<proof>

lemma *elements-mat-mat-of-row*[simp]: *elements-mat (mat-of-row v) = vec-set v*
<proof>

lemma *vec-set-append-vec*[simp]: *vec-set (v @_v w) = vec-set v ∪ vec-set w*
<proof>

lemma *vec-set-vNil*[simp]: *set_v vNil = {}* *<proof>*

lemma *diff-smult-distrib-vec*: *((x :: 'a::ring) - y) ·_v v = x ·_v v - y ·_v v*
<proof>

lemma *add-diff-eq-vec*: **fixes** *y :: 'a :: group-add vec*
shows *y ∈ carrier-vec n ⇒ x ∈ carrier-vec n ⇒ z ∈ carrier-vec n ⇒ y + (x - z) = y + x - z*
<proof>

definition *mat-of-col v = (mat-of-row v)^T*

lemma *elements-mat-mat-of-col*[simp]: *elements-mat (mat-of-col v) = vec-set v*
<proof>

lemma *mat-of-col-dim*[simp]: *dim-row (mat-of-col v) = dim-vec v*
dim-col (mat-of-col v) = 1
mat-of-col v ∈ carrier-mat (dim-vec v) 1
<proof>

lemma *col-mat-of-col*[simp]: *col (mat-of-col v) 0 = v*
<proof>

lemma *mult-mat-of-col*: *A ∈ carrier-mat nr nc ⇒ v ∈ carrier-vec nc ⇒*
*A * mat-of-col v = mat-of-col (A *_v v)*
<proof>

lemma *mat-mult-append-cols*: **fixes** *A :: 'a :: comm-semiring-0 mat*
assumes *A: A ∈ carrier-mat nr nc1*
and *B: B ∈ carrier-mat nr nc2*
and *v1: v1 ∈ carrier-vec nc1*
and *v2: v2 ∈ carrier-vec nc2*
shows *(A @_c B) *_v (v1 @_v v2) = A *_v v1 + B *_v v2*
<proof>

lemma *vec-first-append*:
assumes *v ∈ carrier-vec n*
shows *vec-first (v @_v w) n = v*
<proof>

lemma *vec-le-iff-diff-le-0*: **fixes** $a :: 'a :: \text{ordered-ab-group-add vec}$
shows $(a \leq b) = (a - b \leq 0_v (\text{dim-vec } a))$
 $\langle \text{proof} \rangle$

definition *mat-row-first* $A \ n \equiv \text{mat } n \ (\text{dim-col } A) \ (\lambda \ (i, j). \ A \ \$\$ \ (i, j))$

definition *mat-row-last* $A \ n \equiv \text{mat } n \ (\text{dim-col } A) \ (\lambda \ (i, j). \ A \ \$\$ \ (\text{dim-row } A - n + i, j))$

lemma *mat-row-first-carrier[simp]*: $\text{mat-row-first } A \ n \in \text{carrier-mat } n \ (\text{dim-col } A)$
 $\langle \text{proof} \rangle$

lemma *mat-row-first-dim[simp]*:
 $\text{dim-row } (\text{mat-row-first } A \ n) = n$
 $\text{dim-col } (\text{mat-row-first } A \ n) = \text{dim-col } A$
 $\langle \text{proof} \rangle$

lemma *mat-row-last-carrier[simp]*: $\text{mat-row-last } A \ n \in \text{carrier-mat } n \ (\text{dim-col } A)$
 $\langle \text{proof} \rangle$

lemma *mat-row-last-dim[simp]*:
 $\text{dim-row } (\text{mat-row-last } A \ n) = n$
 $\text{dim-col } (\text{mat-row-last } A \ n) = \text{dim-col } A$
 $\langle \text{proof} \rangle$

lemma *mat-row-first-nth[simp]*: $i < n \implies \text{row } (\text{mat-row-first } A \ n) \ i = \text{row } A \ i$
 $\langle \text{proof} \rangle$

lemma *append-rows-nth*:
assumes $A \in \text{carrier-mat } nr1 \ nc$
and $B \in \text{carrier-mat } nr2 \ nc$
shows $i < nr1 \implies \text{row } (A \ @_r \ B) \ i = \text{row } A \ i$
and $\llbracket i \geq nr1; i < nr1 + nr2 \rrbracket \implies \text{row } (A \ @_r \ B) \ i = \text{row } B \ (i - nr1)$
 $\langle \text{proof} \rangle$

lemma *mat-of-row-last-nth[simp]*:
 $i < n \implies \text{row } (\text{mat-row-last } A \ n) \ i = \text{row } A \ (\text{dim-row } A - n + i)$
 $\langle \text{proof} \rangle$

lemma *mat-row-first-last-append*:
assumes $\text{dim-row } A = m + n$
shows $(\text{mat-row-first } A \ m) \ @_r \ (\text{mat-row-last } A \ n) = A$
 $\langle \text{proof} \rangle$

definition *mat-col-first* $A \ n \equiv (\text{mat-row-first } A^T \ n)^T$

definition *mat-col-last* $A \ n \equiv (\text{mat-row-last } A^T \ n)^T$

lemma *mat-col-first-carrier[simp]*: $\text{mat-col-first } A \ n \in \text{carrier-mat } (\text{dim-row } A) \ n$

<proof>

lemma *mat-col-first-dim*[simp]:

$dim\text{-row } (mat\text{-col-first } A \ n) = dim\text{-row } A$

$dim\text{-col } (mat\text{-col-first } A \ n) = n$

<proof>

lemma *mat-col-last-carrier*[simp]: $mat\text{-col-last } A \ n \in carrier\text{-mat } (dim\text{-row } A) \ n$

<proof>

lemma *mat-col-last-dim*[simp]:

$dim\text{-row } (mat\text{-col-last } A \ n) = dim\text{-row } A$

$dim\text{-col } (mat\text{-col-last } A \ n) = n$

<proof>

lemma *mat-col-first-nth*[simp]:

$\llbracket i < n; i < dim\text{-col } A \rrbracket \implies col \ (mat\text{-col-first } A \ n) \ i = col \ A \ i$

<proof>

lemma *append-cols-nth*:

assumes $A \in carrier\text{-mat } nr \ nc1$

and $B \in carrier\text{-mat } nr \ nc2$

shows $i < nc1 \implies col \ (A \ @_c \ B) \ i = col \ A \ i$

and $\llbracket i \geq nc1; i < nc1 + nc2 \rrbracket \implies col \ (A \ @_c \ B) \ i = col \ B \ (i - nc1)$

<proof>

lemma *mat-of-col-last-nth*[simp]:

$\llbracket i < n; i < dim\text{-col } A \rrbracket \implies col \ (mat\text{-col-last } A \ n) \ i = col \ A \ (dim\text{-col } A - n + i)$

<proof>

lemma *mat-col-first-last-append*:

assumes $dim\text{-col } A = m + n$

shows $(mat\text{-col-first } A \ m) \ @_c \ (mat\text{-col-last } A \ n) = A$

<proof>

lemma *mat-of-row-dim-row-1*: $(dim\text{-row } A = 1) = (A = mat\text{-of-row } (row \ A \ 0))$

<proof>

lemma *mat-of-col-dim-col-1*: $(dim\text{-col } A = 1) = (A = mat\text{-of-col } (col \ A \ 0))$

<proof>

definition *vec-of-scal* :: $'a \Rightarrow 'a \ vec$ **where** $vec\text{-of-scal } x \equiv vec \ 1 \ (\lambda \ i. \ x)$

lemma *vec-of-scal-dim*[simp]:

$dim\text{-vec } (vec\text{-of-scal } x) = 1$

$vec\text{-of-scal } x \in carrier\text{-vec } 1$

<proof>

lemma *index-vec-of-scal[simp]*: $(\text{vec-of-scal } x) \$ 0 = x$
<proof>

lemma *row-mat-of-col[simp]*: $i < \text{dim-vec } v \implies \text{row } (\text{mat-of-col } v) i = \text{vec-of-scal } (v \$ i)$
<proof>

lemma *vec-of-scal-dim-1*: $(v \in \text{carrier-vec } 1) = (v = \text{vec-of-scal } (v \$ 0))$
<proof>

lemma *mult-mat-of-row-vec-of-scal*: **fixes** $x :: 'a :: \text{comm-ring-1}$
shows $\text{mat-of-col } v *_v \text{vec-of-scal } x = x \cdot_v v$
<proof>

lemma *smult-pos-vec[simp]*: **fixes** $l :: 'a :: \text{linordered-ring-strict}$
assumes $l: l > 0$
shows $(l \cdot_v v \leq 0_v n) = (v \leq 0_v n)$
<proof>

lemma *finite-elements-mat[simp]*: $\text{finite } (\text{elements-mat } A)$
<proof>

lemma *finite-vec-set[simp]*: $\text{finite } (\text{vec-set } A)$
<proof>

lemma *lesseq-vecI*: **assumes** $v \in \text{carrier-vec } n \ w \in \text{carrier-vec } n$
 $\bigwedge i. i < n \implies v \$ i \leq w \$ i$
shows $v \leq w$
<proof>

lemma *lesseq-vecD*: **assumes** $w \in \text{carrier-vec } n$
and $v \leq w$
and $i < n$
shows $v \$ i \leq w \$ i$
<proof>

lemma *vec-add-mono*: **fixes** $a :: 'a :: \text{ordered-ab-semigroup-add } \text{vec}$
assumes $\text{dim}: \text{dim-vec } b = \text{dim-vec } d$
and $ab: a \leq b$
and $cd: c \leq d$
shows $a + c \leq b + d$
<proof>

lemma *smult-nneg-npos-vec*: **fixes** $l :: 'a :: \text{ordered-semiring-0}$
assumes $l: l \geq 0$
and $v: v \leq 0_v n$
shows $l \cdot_v v \leq 0_v n$
<proof>

lemma *smult-vec-nonneg-eq*: **fixes** $c :: 'a :: field$
shows $c \neq 0 \implies (c \cdot_v x = c \cdot_v y) = (x = y)$
 $\langle proof \rangle$

lemma *distinct-smult-nonneg*: **fixes** $c :: 'a :: field$
assumes $c: c \neq 0$
shows $distinct\ lC \implies distinct\ (map\ ((\cdot_v)\ c)\ lC)$
 $\langle proof \rangle$

lemma *exists-vec-append*: $(\exists x \in carrier-vec\ (n + m). P\ x) \longleftrightarrow (\exists x1 \in carrier-vec\ n. \exists x2 \in carrier-vec\ m. P\ (x1 @_v x2))$
 $\langle proof \rangle$

end

3 Missing Lemmas on Vector Spaces

We provide some results on vector spaces which should be merged into other AFP entries.

theory *Missing-VS-Connect*

imports

Jordan-Normal-Form.VS-Connect

Missing-Matrix

Polynomial-Factorization.Missing-List

begin

context *vec-space*

begin

lemma *span-diff*: **assumes** $A: A \subseteq carrier-vec\ n$

and $a: a \in span\ A$ **and** $b: b \in span\ A$

shows $a - b \in span\ A$

$\langle proof \rangle$

lemma *finsum-scalar-prod-sum'*:

assumes $f: f \in U \rightarrow carrier-vec\ n$

and $w: w \in carrier-vec\ n$

shows $w \cdot finsum\ V\ f\ U = sum\ (\lambda u. w \cdot f\ u)\ U$

$\langle proof \rangle$

lemma *lincomb-scalar-prod-left*: **assumes** $W \subseteq carrier-vec\ n\ v \in carrier-vec\ n$

shows $lincomb\ a\ W \cdot v = (\sum_{w \in W}. a\ w * (w \cdot v))$

$\langle proof \rangle$

lemma *lincomb-scalar-prod-right*: **assumes** $W \subseteq carrier-vec\ n\ v \in carrier-vec\ n$

shows $v \cdot lincomb\ a\ W = (\sum_{w \in W}. a\ w * (v \cdot w))$

$\langle proof \rangle$

lemma *lin-indpt-empty[simp]*: $lin-indpt\ \{\}$

<proof>

lemma *span-carrier-lin-indpt-card-n*:

assumes $W \subseteq \text{carrier-vec } n$ $\text{card } W = n$ $\text{lin-indpt } W$

shows $\text{span } W = \text{carrier-vec } n$

<proof>

lemma *ortho-span*: **assumes** $W: W \subseteq \text{carrier-vec } n$

and $X: X \subseteq \text{carrier-vec } n$

and *ortho*: $\bigwedge w x. w \in W \implies x \in X \implies w \cdot x = 0$

and $w: w \in \text{span } W$ **and** $x: x \in X$

shows $w \cdot x = 0$

<proof>

lemma *ortho-span'*: **assumes** $W: W \subseteq \text{carrier-vec } n$

and $X: X \subseteq \text{carrier-vec } n$

and *ortho*: $\bigwedge w x. w \in W \implies x \in X \implies x \cdot w = 0$

and $w: w \in \text{span } W$ **and** $x: x \in X$

shows $x \cdot w = 0$

<proof>

lemma *ortho-span-span*: **assumes** $W: W \subseteq \text{carrier-vec } n$

and $X: X \subseteq \text{carrier-vec } n$

and *ortho*: $\bigwedge w x. w \in W \implies x \in X \implies w \cdot x = 0$

and $w: w \in \text{span } W$ **and** $x: x \in \text{span } X$

shows $w \cdot x = 0$

<proof>

lemma *lincomb-in-span*[*intro*]:

assumes $X: X \subseteq \text{carrier-vec } n$

shows $\text{lincomb } a X \in \text{span } X$

<proof>

lemma *generating-card-n-basis*: **assumes** $X: X \subseteq \text{carrier-vec } n$

and *span*: $\text{carrier-vec } n \subseteq \text{span } X$

and *card*: $\text{card } X = n$

shows *basis* X

<proof>

lemma *lincomb-list-append*:

assumes $Ws: \text{set } Ws \subseteq \text{carrier-vec } n$

shows $\text{set } Vs \subseteq \text{carrier-vec } n \implies \text{lincomb-list } f (Vs @ Ws) =$

$\text{lincomb-list } f Vs + \text{lincomb-list } (\lambda i. f (i + \text{length } Vs)) Ws$

<proof>

lemma *lincomb-list-snoc*[*simp*]:

shows $\text{set } Vs \subseteq \text{carrier-vec } n \implies x \in \text{carrier-vec } n \implies$

$\text{lincomb-list } f (Vs @ [x]) = \text{lincomb-list } f Vs + f (\text{length } Vs) \cdot_v x$

<proof>

lemma *lincomb-list-smult*:
 set $Vs \subseteq \text{carrier-vec } n \implies \text{lincomb-list } (\lambda i. a * c i) Vs = a \cdot_v \text{lincomb-list } c Vs$
 ⟨*proof*⟩

lemma *lincomb-list-index*:
assumes $i: i < n$
shows set $Xs \subseteq \text{carrier-vec } n \implies$
 $\text{lincomb-list } c Xs \$ i = \text{sum } (\lambda j. c j * (Xs ! j) \$ i) \{0..<\text{length } Xs\}$
 ⟨*proof*⟩

end
end

4 Basis Extension

We prove that every linear indepent set/list of vectors can be extended into a basis. Similarly, from every set of vectors one can extract a linear independent set of vectors that spans the same space.

theory *Basis-Extension*
imports
LLL-Basis-Reduction.Gram-Schmidt-2
begin

context *cof-vec-space*
begin

lemma *lin-indpt-list-length-le-n*: **assumes** *lin-indpt-list* xs
shows $\text{length } xs \leq n$
 ⟨*proof*⟩

lemma *lin-indpt-list-length-eq-n*: **assumes** *lin-indpt-list* xs
and $\text{length } xs = n$
shows $\text{span } (\text{set } xs) = \text{carrier-vec } n \text{ basis } (\text{set } xs)$
 ⟨*proof*⟩

lemma *expand-to-basis*: **assumes** *lin*: *lin-indpt-list* xs
shows $\exists ys. \text{set } ys \subseteq \text{set } (\text{unit-vecs } n) \wedge \text{lin-indpt-list } (xs @ ys) \wedge \text{length } (xs @ ys) = n$
 ⟨*proof*⟩

definition *basis-extension* $xs = (\text{SOME } ys.$
 $\text{set } ys \subseteq \text{set } (\text{unit-vecs } n) \wedge \text{lin-indpt-list } (xs @ ys) \wedge \text{length } (xs @ ys) = n)$

lemma *basis-extension*: **assumes** *lin-indpt-list* xs
shows set $(\text{basis-extension } xs) \subseteq \text{set } (\text{unit-vecs } n)$
 $\text{lin-indpt-list } (xs @ \text{basis-extension } xs)$

$length (xs @ basis-extension xs) = n$
 ⟨proof⟩

lemma *exists-lin-indpt-sublist*: **assumes** $X \subseteq carrier-vec\ n$
shows $\exists Ls. lin-indpt-list\ Ls \wedge span (set\ Ls) = span\ X \wedge set\ Ls \subseteq X$
 ⟨proof⟩

lemma *exists-lin-indpt-subset*: **assumes** $X \subseteq carrier-vec\ n$
shows $\exists Ls. lin-indpt\ Ls \wedge span (Ls) = span\ X \wedge Ls \subseteq X$
 ⟨proof⟩
end

end

5 Sum of Vector Sets

We use Isabelle's Set-Algebra theory to be able to write $V + W$ for sets of vectors V and W , and prove some obvious properties about them.

theory *Sum-Vec-Set*
imports
 Missing-Matrix
 HOL-Library.Set-Algebras
begin

lemma *add-0-right-vecset*:
assumes $(A :: 'a :: monoid-add\ vec\ set) \subseteq carrier-vec\ n$
shows $A + \{0_v\ n\} = A$
 ⟨proof⟩

lemma *add-0-left-vecset*:
assumes $(A :: 'a :: monoid-add\ vec\ set) \subseteq carrier-vec\ n$
shows $\{0_v\ n\} + A = A$
 ⟨proof⟩

lemma *assoc-add-vecset*:
assumes $(A :: 'a :: semigroup-add\ vec\ set) \subseteq carrier-vec\ n$
and $B \subseteq carrier-vec\ n$
and $C \subseteq carrier-vec\ n$
shows $A + (B + C) = (A + B) + C$
 ⟨proof⟩

lemma *sum-carrier-vec[intro]*: $A \subseteq carrier-vec\ n \implies B \subseteq carrier-vec\ n \implies A + B \subseteq carrier-vec\ n$
 ⟨proof⟩

lemma *comm-add-vecset*:
assumes $(A :: 'a :: ab-semigroup-add\ vec\ set) \subseteq carrier-vec\ n$

and $B \subseteq \text{carrier-vec } n$
shows $A + B = B + A$
 ⟨*proof*⟩

end

6 Integral and Bounded Matrices and Vectors

We define notions of integral vectors and matrices and bounded vectors and matrices and prove some preservation lemmas. Moreover, we prove two bounds on determinants.

theory *Integral-Bounded-Vectors*

imports

Missing-VS-Connect

Sum-Vec-Set

LLL-Basis-Reduction.Gram-Schmidt-2

begin

lemma *sq-norm-unit-vec[simp]*: **assumes** $i: i < n$

shows $\|\text{unit-vec } n \ i\|^2 = (1 :: 'a :: \{\text{comm-ring-1, conjugatable-ring}\})$
 ⟨*proof*⟩

definition *Ints-vec* ($\langle \mathbb{Z}_v \rangle$) **where**

$\mathbb{Z}_v = \{x. \forall i < \text{dim-vec } x. x \ \$ \ i \in \mathbb{Z}\}$

definition *indexed-Ints-vec* **where**

indexed-Ints-vec $I = \{x. \forall i < \text{dim-vec } x. i \in I \longrightarrow x \ \$ \ i \in \mathbb{Z}\}$

lemma *indexed-Ints-vec-UNIV*: $\mathbb{Z}_v = \text{indexed-Ints-vec UNIV}$

⟨*proof*⟩

lemma *indexed-Ints-vec-subset*: $\mathbb{Z}_v \subseteq \text{indexed-Ints-vec } I$

⟨*proof*⟩

lemma *Ints-vec-vec-set*: $v \in \mathbb{Z}_v = (\text{vec-set } v \subseteq \mathbb{Z})$

⟨*proof*⟩

definition *Ints-mat* ($\langle \mathbb{Z}_m \rangle$) **where**

$\mathbb{Z}_m = \{A. \forall i < \text{dim-row } A. \forall j < \text{dim-col } A. A \ \$ \$ \ (i,j) \in \mathbb{Z}\}$

lemma *Ints-mat-elements-mat*: $A \in \mathbb{Z}_m = (\text{elements-mat } A \subseteq \mathbb{Z})$

⟨*proof*⟩

lemma *minus-in-Ints-vec-iff[simp]*: $(-x) \in \mathbb{Z}_v \longleftrightarrow (x :: 'a :: \text{ring-1 vec}) \in \mathbb{Z}_v$

⟨*proof*⟩

lemma *minus-in-Ints-mat-iff*[simp]: $(-A) \in \mathbf{Z}_m \longleftrightarrow (A :: 'a :: \text{ring-1 mat}) \in \mathbf{Z}_m$
 ⟨proof⟩

lemma *Ints-vec-rows-Ints-mat*[simp]: $\text{set } (\text{rows } A) \subseteq \mathbf{Z}_v \longleftrightarrow A \in \mathbf{Z}_m$
 ⟨proof⟩

lemma *unit-vec-integral*[simp,intro]: $\text{unit-vec } n \ i \in \mathbf{Z}_v$
 ⟨proof⟩

lemma *diff-indexed-Ints-vec*:
 $x \in \text{carrier-vec } n \implies y \in \text{carrier-vec } n \implies x \in \text{indexed-Ints-vec } I \implies y \in \text{indexed-Ints-vec } I$
 $\implies x - y \in \text{indexed-Ints-vec } I$
 ⟨proof⟩

lemma *smult-indexed-Ints-vec*: $x \in \mathbf{Z} \implies v \in \text{indexed-Ints-vec } I \implies x \cdot_v v \in \text{indexed-Ints-vec } I$
 ⟨proof⟩

lemma *add-indexed-Ints-vec*:
 $x \in \text{carrier-vec } n \implies y \in \text{carrier-vec } n \implies x \in \text{indexed-Ints-vec } I \implies y \in \text{indexed-Ints-vec } I$
 $\implies x + y \in \text{indexed-Ints-vec } I$
 ⟨proof⟩

lemma (in *vec-space*) *lincomb-indexed-Ints-vec*: **assumes** $cI: \bigwedge x. x \in C \implies c \ x \in \mathbf{Z}$
and $C: C \subseteq \text{carrier-vec } n$
and $CI: C \subseteq \text{indexed-Ints-vec } I$
shows $\text{lincomb } c \ C \in \text{indexed-Ints-vec } I$
 ⟨proof⟩

definition *Bounded-vec* ($b :: 'a :: \text{linordered-idom}$) = $\{x . \forall i < \text{dim-vec } x . \text{abs } (x \$ i) \leq b\}$

lemma *Bounded-vec-vec-set*: $v \in \text{Bounded-vec } b \longleftrightarrow (\forall x \in \text{vec-set } v . \text{abs } x \leq b)$
 ⟨proof⟩

definition *Bounded-mat* ($b :: 'a :: \text{linordered-idom}$) =
 $\{A . (\forall i < \text{dim-row } A . \forall j < \text{dim-col } A . \text{abs } (A \$\$ (i,j)) \leq b)\}$

lemma *Bounded-mat-elements-mat*: $A \in \text{Bounded-mat } b \longleftrightarrow (\forall x \in \text{elements-mat } A . \text{abs } x \leq b)$
 ⟨proof⟩

lemma *Bounded-vec-rows-Bounded-mat*[simp]: $\text{set } (\text{rows } A) \subseteq \text{Bounded-vec } B \longleftrightarrow A \in \text{Bounded-mat } B$
 ⟨proof⟩

lemma *unit-vec-Bounded-vec*[*simp,intro*]: *unit-vec n i* \in *Bounded-vec (max 1 Bnd)*
 ⟨*proof*⟩

lemma *unit-vec-int-bounds*: *set (unit-vecs n)* \subseteq $\mathbb{Z}_v \cap$ *Bounded-vec (of-int (max 1 Bnd))*
 ⟨*proof*⟩

lemma *Bounded-matD*: **assumes** $A \in$ *Bounded-mat b*
 $A \in$ *carrier-mat nr nc*
shows $i < nr \implies j < nc \implies \text{abs } (A \ \$\$ (i,j)) \leq b$
 ⟨*proof*⟩

lemma *Bounded-vec-mono*: $b \leq B \implies$ *Bounded-vec b* \subseteq *Bounded-vec B*
 ⟨*proof*⟩

lemma *Bounded-mat-mono*: $b \leq B \implies$ *Bounded-mat b* \subseteq *Bounded-mat B*
 ⟨*proof*⟩

lemma *finite-Bounded-vec-Max*:
assumes $A \subseteq$ *carrier-vec n*
and *fin*: *finite A*
shows $A \subseteq$ *Bounded-vec (Max { abs (a \$ i) | a i. a \in A \wedge i < n })*
 ⟨*proof*⟩

definition *is-det-bound* :: $(\text{nat} \Rightarrow 'a :: \text{linordered-idom} \Rightarrow 'a) \Rightarrow \text{bool}$ **where**
is-det-bound f = $(\forall A \ n \ x. A \in$ *carrier-mat n n* $\longrightarrow A \in$ *Bounded-mat x* \longrightarrow
 $\text{abs } (\text{det } A) \leq f \ n \ x)$

lemma *is-det-bound-ge-zero*: **assumes** *is-det-bound f*
and $x \geq 0$
shows $f \ n \ x \geq 0$
 ⟨*proof*⟩

definition *det-bound-fact* :: $\text{nat} \Rightarrow 'a :: \text{linordered-idom} \Rightarrow 'a$ **where**
det-bound-fact n x = $\text{fact } n * (x \hat{=} n)$

lemma *det-bound-fact*: *is-det-bound det-bound-fact*
 ⟨*proof*⟩

lemma (**in** *gram-schmidt-fs*) *Gramian-determinant-det*: **assumes** $A \in$ *carrier-mat n n*
shows *Gramian-determinant (rows A) n* = $\text{det } A * \text{det } A$
 ⟨*proof*⟩

lemma (**in** *gram-schmidt-fs-lin-indpt*) *det-bound-main*: **assumes** *rows*: *rows A* =
fs
and $A \in$ *carrier-mat n n*
and $n0$: $n > 0$

and $Bnd: A \in Bounded\text{-}mat\ c$
shows
 $(abs\ (det\ A))^{\wedge}2 \leq of\text{-}nat\ n \wedge n * c \wedge (2 * n)$
 $\langle proof \rangle$

lemma *det-bound-hadamard-squared*: **fixes** $A::'a :: trivial\text{-}conjugatable\text{-}linordered\text{-}field$
 mat

assumes $A: A \in carrier\text{-}mat\ n\ n$
and $Bnd: A \in Bounded\text{-}mat\ c$
shows $(abs\ (det\ A))^{\wedge}2 \leq of\text{-}nat\ n \wedge n * c \wedge (2 * n)$
 $\langle proof \rangle$

definition *det-bound-hadamard* :: $nat \Rightarrow int \Rightarrow int$ **where**
 $det\text{-}bound\text{-}hadamard\ n\ c = (sqrt\text{-}int\text{-}floor\ ((int\ n * c^{\wedge}2)^{\wedge}n))$

lemma *det-bound-hadamard-altdef*[code]:
 $det\text{-}bound\text{-}hadamard\ n\ c = (if\ n = 1 \vee even\ n\ then\ int\ n \wedge (n\ div\ 2) * (abs\ c)^{\wedge}n$
 $else\ sqrt\text{-}int\text{-}floor\ ((int\ n * c^{\wedge}2)^{\wedge}n))$
 $\langle proof \rangle$

lemma *det-bound-hadamard*: *is-det-bound* *det-bound-hadamard*
 $\langle proof \rangle$

lemma *n-pow-n-le-fact-square*: $n \wedge n \leq (fact\ n)^{\wedge}2$
 $\langle proof \rangle$

lemma *sqrt-int-floor-bound*: $0 \leq x \Longrightarrow (sqrt\text{-}int\text{-}floor\ x)^{\wedge}2 \leq x$
 $\langle proof \rangle$

lemma *det-bound-hadamard-improves-det-bound-fact*: **assumes** $c: c \geq 0$
shows $det\text{-}bound\text{-}hadamard\ n\ c \leq det\text{-}bound\text{-}fact\ n\ c$
 $\langle proof \rangle$

context

begin

private fun *syl* :: $int \Rightarrow nat \Rightarrow int\ mat$ **where**

$syl\ c\ 0 = mat\ 1\ 1\ (\lambda\ -. c)$
 $| syl\ c\ (Suc\ n) = (let\ A = syl\ c\ n\ in$
 $four\text{-}block\text{-}mat\ A\ A\ (-A)\ A)$

private lemma *syl*: **assumes** $c: c \geq 0$

shows $syl\ c\ n \in Bounded\text{-}mat\ c \wedge syl\ c\ n \in carrier\text{-}mat\ (2^{\wedge}n)\ (2^{\wedge}n)$
 $\wedge det\ (syl\ c\ n) = det\text{-}bound\text{-}hadamard\ (2^{\wedge}n)\ c$
 $\langle proof \rangle$

lemma *det-bound-hadamard-tight*:

assumes $c: c \geq 0$
and $n = 2^{\wedge}m$

shows $\exists A. A \in \text{carrier-mat } n \ n \wedge A \in \text{Bounded-mat } c \wedge \det A = \text{det-bound-hadamard } n \ c$
 $\langle \text{proof} \rangle$
end

lemma *Ints-matE*: **assumes** $A \in \mathbb{Z}_m$
shows $\exists B. A = \text{map-mat of-int } B$
 $\langle \text{proof} \rangle$

lemma *is-det-bound-of-int*: **fixes** $A :: 'a :: \text{linordered-idom mat}$
assumes $db: \text{is-det-bound } db$
and $A: A \in \text{carrier-mat } n \ n$
and $A \in \mathbb{Z}_m \cap \text{Bounded-mat } (\text{of-int } bnd)$
shows $\text{abs } (\det A) \leq \text{of-int } (db \ n \ bnd)$
 $\langle \text{proof} \rangle$

lemma *minus-in-Bounded-vec[simp]*:
 $(-x) \in \text{Bounded-vec } b \longleftrightarrow x \in \text{Bounded-vec } b$
 $\langle \text{proof} \rangle$

lemma *sum-in-Bounded-vecI[intro]*: **assumes**
 $xB: x \in \text{Bounded-vec } B1$ **and**
 $yB: y \in \text{Bounded-vec } B2$ **and**
 $x: x \in \text{carrier-vec } n$ **and**
 $y: y \in \text{carrier-vec } n$
shows $x + y \in \text{Bounded-vec } (B1 + B2)$
 $\langle \text{proof} \rangle$

lemma (*in gram-schmidt*) *lincomb-card-bound*: **assumes** $XBnd: X \subseteq \text{Bounded-vec } Bnd$
and $X: X \subseteq \text{carrier-vec } n$
and $Bnd: Bnd \geq 0$
and $c: \bigwedge x. x \in X \implies \text{abs } (c \ x) \leq 1$
and $\text{card}: \text{card } X \leq k$
shows $\text{lincomb } c \ X \in \text{Bounded-vec } (\text{of-nat } k * Bnd)$
 $\langle \text{proof} \rangle$

lemma *bounded-vecset-sum*:
assumes $Acarr: A \subseteq \text{carrier-vec } n$
and $Bcarr: B \subseteq \text{carrier-vec } n$
and $\text{sum}: C = A + B$
and $Cbnd: \exists bndC. C \subseteq \text{Bounded-vec } bndC$
shows $A \neq \{\} \implies (\exists bndB. B \subseteq \text{Bounded-vec } bndB)$
and $B \neq \{\} \implies (\exists bndA. A \subseteq \text{Bounded-vec } bndA)$
 $\langle \text{proof} \rangle$

end

7 Cones

We define the notions like cone, polyhedral cone, etc. and prove some basic facts about them.

theory *Cone*

imports

Basis-Extension

Missing-VS-Connect

Integral-Bounded-Vectors

begin

context *gram-schmidt*

begin

definition *nonneg-lincomb* $c\ Vs\ b = (\text{lincomb } c\ Vs = b \wedge c \cdot Vs \subseteq \{x. x \geq 0\})$

definition *nonneg-lincomb-list* $c\ Vs\ b = (\text{lincomb-list } c\ Vs = b \wedge (\forall i < \text{length } Vs. c\ i \geq 0))$

definition *finite-cone* $:: 'a\ \text{vec set} \Rightarrow 'a\ \text{vec set}$ **where**

finite-cone $Vs = (\{ b. \exists c. \text{nonneg-lincomb } c\ (\text{if finite } Vs\ \text{then } Vs\ \text{else } \{\})\ b})$

definition *cone* $:: 'a\ \text{vec set} \Rightarrow 'a\ \text{vec set}$ **where**

cone $Vs = (\{ x. \exists\ Ws. \text{finite } Ws \wedge Ws \subseteq Vs \wedge x \in \text{finite-cone } Ws\})$

definition *cone-list* $:: 'a\ \text{vec list} \Rightarrow 'a\ \text{vec set}$ **where**

cone-list $Vs = \{b. \exists c. \text{nonneg-lincomb-list } c\ Vs\ b\}$

lemma *finite-cone-iff-cone-list*: **assumes** $Vs: Vs \subseteq \text{carrier-vec } n$

and *id*: $Vs = \text{set } Vsl$

shows *finite-cone* $Vs = \text{cone-list } Vsl$

<proof>

lemma *cone-alt-def*: **assumes** $Vs: Vs \subseteq \text{carrier-vec } n$

shows *cone* $Vs = (\{ x. \exists\ Ws. \text{set } Ws \subseteq Vs \wedge x \in \text{cone-list } Ws\})$

<proof>

lemma *cone-mono*: $Vs \subseteq Ws \Longrightarrow \text{cone } Vs \subseteq \text{cone } Ws$

<proof>

lemma *finite-cone-mono*: **assumes** *fin*: *finite* Ws

and $Ws: Ws \subseteq \text{carrier-vec } n$

and *sub*: $Vs \subseteq Ws$

shows *finite-cone* $Vs \subseteq \text{finite-cone } Ws$

<proof>

lemma *finite-cone-carrier*: $A \subseteq \text{carrier-vec } n \Longrightarrow \text{finite-cone } A \subseteq \text{carrier-vec } n$

<proof>

lemma *cone-carrier*: $A \subseteq \text{carrier-vec } n \Longrightarrow \text{cone } A \subseteq \text{carrier-vec } n$

<proof>

lemma *cone-iff-finite-cone*: **assumes** $A: A \subseteq \text{carrier-vec } n$
and $\text{fin}: \text{finite } A$
shows $\text{cone } A = \text{finite-cone } A$
<proof>

lemma *set-in-finite-cone*:
assumes $Vs: Vs \subseteq \text{carrier-vec } n$
and $\text{fin}: \text{finite } Vs$
shows $Vs \subseteq \text{finite-cone } Vs$
<proof>

lemma *set-in-cone*:
assumes $Vs: Vs \subseteq \text{carrier-vec } n$
shows $Vs \subseteq \text{cone } Vs$
<proof>

lemma *zero-in-finite-cone*:
assumes $Vs: Vs \subseteq \text{carrier-vec } n$
shows $0_v \ n \in \text{finite-cone } Vs$
<proof>

lemma *lincomb-in-finite-cone*:
assumes $x = \text{lincomb } l \ W$
and $\text{finite } W$
and $\forall i \in W . l \ i \geq 0$
and $W \subseteq \text{carrier-vec } n$
shows $x \in \text{finite-cone } W$
<proof>

lemma *lincomb-in-cone*:
assumes $x = \text{lincomb } l \ W$
and $\text{finite } W$
and $\forall i \in W . l \ i \geq 0$
and $W \subseteq \text{carrier-vec } n$
shows $x \in \text{cone } W$
<proof>

lemma *zero-in-cone*: $0_v \ n \in \text{cone } Vs$
<proof>

lemma *cone-smult*:
assumes $a: a \geq 0$
and $Vs: Vs \subseteq \text{carrier-vec } n$
and $x: x \in \text{cone } Vs$
shows $a \cdot_v x \in \text{cone } Vs$
<proof>

lemma *finite-cone-empty[simp]*: $\text{finite-cone } \{\} = \{0_v \ n\}$
 ⟨proof⟩

lemma *cone-empty[simp]*: $\text{cone } \{\} = \{0_v \ n\}$
 ⟨proof⟩

lemma *cone-elem-sum*:
 assumes $Vs: Vs \subseteq \text{carrier-vec } n$
 and $x: x \in \text{cone } Vs$
 and $y: y \in \text{cone } Vs$
 shows $x + y \in \text{cone } Vs$
 ⟨proof⟩

lemma *cone-cone*:
 assumes $Vs: Vs \subseteq \text{carrier-vec } n$
 shows $\text{cone } (\text{cone } Vs) = \text{cone } Vs$
 ⟨proof⟩

lemma *cone-smult-basis*:
 assumes $Vs: Vs \subseteq \text{carrier-vec } n$
 and $l: l \text{ ' } Vs \subseteq \{x. x > 0\}$
 shows $\text{cone } \{l \ v \cdot_v \ v \mid v \cdot v \in Vs\} = \text{cone } Vs$
 ⟨proof⟩

lemma *cone-add-cone*:
 assumes $C: C \subseteq \text{carrier-vec } n$
 shows $\text{cone } C + \text{cone } C = \text{cone } C$
 ⟨proof⟩

lemma *orthogonal-cone*:
 assumes $X: X \subseteq \text{carrier-vec } n$
 and $W: W \subseteq \text{carrier-vec } n$
 and $\text{fin}X: \text{finite } X$
 and $\text{span}LW: \text{span } (\text{set } Ls \cup W) = \text{carrier-vec } n$
 and $\text{ortho}: \bigwedge w \ x. w \in W \implies x \in \text{set } Ls \implies w \cdot x = 0$
 and $WWs: W = \text{set } Ws$
 and $\text{span}L: \text{span } (\text{set } Ls) = \text{span } X$
 and $LX: \text{set } Ls \subseteq X$
 and $\text{lin-Ls-Bs}: \text{lin-indpt-list } (Ls \ @ \ Bs)$
 and $\text{len-Ls-Bs}: \text{length } (Ls \ @ \ Bs) = n$
 shows $\text{cone } (X \cup \text{set } Bs) \cap \{x \in \text{carrier-vec } n. \forall w \in W. w \cdot x = 0\} = \text{cone } X$
 $\bigwedge x. \forall w \in W. w \cdot x = 0 \implies Z \subseteq X \implies B \subseteq \text{set } Bs \implies x = \text{lincomb } c \ (Z \cup B)$
 $\implies x = \text{lincomb } c \ (Z - B)$
 ⟨proof⟩

definition *polyhedral-cone* ($A :: \text{'a mat}$) = $\{x \cdot x \in \text{carrier-vec } n \wedge A \cdot_v x \leq 0_v$
 ($\text{dim-row } A\}$

lemma *polyhedral-cone-carrier*: **assumes** $A \in \text{carrier-mat } nr \ n$
shows $\text{polyhedral-cone } A \subseteq \text{carrier-vec } n$
 $\langle \text{proof} \rangle$

lemma *cone-in-polyhedral-cone*:
assumes $CA: C \subseteq \text{polyhedral-cone } A$
and $A: A \in \text{carrier-mat } nr \ n$
shows $\text{cone } C \subseteq \text{polyhedral-cone } A$
 $\langle \text{proof} \rangle$

lemma *bounded-cone-is-zero*:
assumes $Carr: C \subseteq \text{carrier-vec } n$ **and** $bnd: \text{cone } C \subseteq \text{Bounded-vec } bnd$
shows $\text{cone } C = \{0_v \ n\}$
 $\langle \text{proof} \rangle$

lemma *cone-of-cols*: **fixes** $A :: 'a \ \text{mat}$ **and** $b :: 'a \ \text{vec}$
assumes $A: A \in \text{carrier-mat } n \ nr$ **and** $b: b \in \text{carrier-vec } n$
shows $b \in \text{cone } (\text{set } (\text{cols } A)) \longleftrightarrow (\exists x. x \geq 0_v \ nr \wedge A *_{\text{v}} x = b)$
 $\langle \text{proof} \rangle$

end
end

8 Convex Hulls

We define the notion of convex hull of a set or list of vectors and derive basic properties thereof.

theory *Convex-Hull*
imports *Cone*
begin

context *gram-schmidt*
begin

definition *convex-lincomb* $c \ Vs \ b = (\text{nonneg-lincomb } c \ Vs \ b \wedge \text{sum } c \ Vs = 1)$

definition *convex-lincomb-list* $c \ Vs \ b = (\text{nonneg-lincomb-list } c \ Vs \ b \wedge \text{sum } c \ \{0..<\text{length } Vs\} = 1)$

definition *convex-hull* $Vs = \{x. \exists \text{ } Ws \ c. \text{finite } Ws \wedge Ws \subseteq Vs \wedge \text{convex-lincomb } c \ Ws \ x\}$

lemma *convex-hull-carrier[intro]*: $Vs \subseteq \text{carrier-vec } n \implies \text{convex-hull } Vs \subseteq \text{carrier-vec } n$
 $\langle \text{proof} \rangle$

lemma *convex-hull-mono*: $Vs \subseteq Ws \implies \text{convex-hull } Vs \subseteq \text{convex-hull } Ws$

<proof>

lemma *convex-lincomb-empty[simp]*: $\neg (\text{convex-lincomb } c \ \{ \} \ x)$
<proof>

lemma *set-in-convex-hull*:
 assumes $A \subseteq \text{carrier-vec } n$
 shows $A \subseteq \text{convex-hull } A$
<proof>

lemma *convex-hull-empty[simp]*:
 $\text{convex-hull } \{ \} = \{ \}$
 $A \subseteq \text{carrier-vec } n \implies \text{convex-hull } A = \{ \} \longleftrightarrow A = \{ \}$
<proof>

lemma *convex-hull-bound*: **assumes** $XBnd$: $X \subseteq \text{Bounded-vec } Bnd$
 and X : $X \subseteq \text{carrier-vec } n$
shows $\text{convex-hull } X \subseteq \text{Bounded-vec } Bnd$
<proof>

definition *convex-hull-list* $Vs = \{x. \exists c. \text{convex-lincomb-list } c \ Vs \ x\}$

lemma *lincomb-list-elem*:
 $\text{set } Vs \subseteq \text{carrier-vec } n \implies$
 $\text{lincomb-list } (\lambda j. \text{if } i=j \text{ then } 1 \text{ else } 0) \ Vs = (\text{if } i < \text{length } Vs \text{ then } Vs \ ! \ i \text{ else } 0_v$
 $n)$
<proof>

lemma *set-in-convex-hull-list*: **fixes** $Vs :: 'a \ \text{vec list}$
 assumes $\text{set } Vs \subseteq \text{carrier-vec } n$
 shows $\text{set } Vs \subseteq \text{convex-hull-list } Vs$
<proof>

lemma *convex-hull-list-combination*:
 assumes Vs : $\text{set } Vs \subseteq \text{carrier-vec } n$
 and x : $x \in \text{convex-hull-list } Vs$
 and y : $y \in \text{convex-hull-list } Vs$
 and $l0$: $0 \leq l$ **and** $l1$: $l \leq 1$
 shows $l \cdot_v x + (1 - l) \cdot_v y \in \text{convex-hull-list } Vs$
<proof>

lemma *convex-hull-list-mono*:
 assumes $\text{set } Ws \subseteq \text{carrier-vec } n$
 shows $\text{set } Vs \subseteq \text{set } Ws \implies \text{convex-hull-list } Vs \subseteq \text{convex-hull-list } Ws$
<proof>

lemma *convex-hull-list-eq-set*:
 $\text{set } Vs \subseteq \text{carrier-vec } n \implies \text{set } Vs = \text{set } Ws \implies \text{convex-hull-list } Vs = \text{convex-hull-list } Ws$

<proof>

lemma *find-indices-empty*: $(\text{find-indices } x \text{ } Vs = []) = (x \notin \text{set } Vs)$
<proof>

lemma *distinct-list-find-indices*:

shows $\llbracket i < \text{length } Vs; Vs ! i = x; \text{distinct } Vs \rrbracket \implies \text{find-indices } x \text{ } Vs = [i]$
<proof>

lemma *finite-convex-hull-iff-convex-hull-list*: **assumes** $Vs: Vs \subseteq \text{carrier-vec } n$
and $id': Vs = \text{set } Vsl'$

shows $\text{convex-hull } Vs = \text{convex-hull-list } Vsl'$
<proof>

definition *convex* $S = (\text{convex-hull } S = S)$

lemma *convex-convex-hull*: $\text{convex } S \implies \text{convex-hull } S = S$
<proof>

lemma *convex-hull-convex-hull-listD*: **assumes** $A: A \subseteq \text{carrier-vec } n$
and $x: x \in \text{convex-hull } A$

shows $\exists \text{ as. set as } \subseteq A \wedge x \in \text{convex-hull-list as}$
<proof>

lemma *convex-hull-convex-sum*: **assumes** $A: A \subseteq \text{carrier-vec } n$

and $x: x \in \text{convex-hull } A$
and $y: y \in \text{convex-hull } A$
and $a: 0 \leq a \leq 1$
shows $a \cdot_v x + (1 - a) \cdot_v y \in \text{convex-hull } A$
<proof>

lemma *convexI*: **assumes** $S: S \subseteq \text{carrier-vec } n$

and *step*: $\bigwedge a \ x \ y. x \in S \implies y \in S \implies 0 \leq a \implies a \leq 1 \implies a \cdot_v x + (1 - a) \cdot_v y \in S$
shows $\text{convex } S$
<proof>

lemma *convex-hulls-are-convex*: **assumes** $A \subseteq \text{carrier-vec } n$

shows $\text{convex } (\text{convex-hull } A)$
<proof>

lemma *convex-hull-sum*: **assumes** $A: A \subseteq \text{carrier-vec } n$ **and** $B: B \subseteq \text{carrier-vec } n$

shows $\text{convex-hull } (A + B) = \text{convex-hull } A + \text{convex-hull } B$
<proof>

lemma *convex-hull-in-cone*:

$\text{convex-hull } C \subseteq \text{cone } C$
<proof>

```

lemma convex-cone:
  assumes  $C: C \subseteq \text{carrier-vec } n$ 
  shows convex (cone  $C$ )
   $\langle \text{proof} \rangle$ 

end
end

```

9 Normal Vectors

We provide a function for the normal vector of a half-space (given as $n-1$ linearly independent vectors). We further provide a function that returns a list of normal vectors that span the orthogonal complement of some subspace of R^n . Bounds for all normal vectors are provided.

```

theory Normal-Vector

```

```

  imports
    Integral-Bounded-Vectors
    Basis-Extension

```

```

begin

```

```

context gram-schmidt

```

```

begin

```

```

lemma ortho-sum-in-span:
  assumes  $W: W \subseteq \text{carrier-vec } n$ 
  and  $X: X \subseteq \text{carrier-vec } n$ 
  and ortho:  $\bigwedge w x. w \in W \implies x \in X \implies x \cdot w = 0$ 
  and inspan:  $\text{lincomb } l1 X + \text{lincomb } l2 W \in \text{span } X$ 
  shows  $\text{lincomb } l2 W = 0_v n$ 
   $\langle \text{proof} \rangle$ 

```

```

lemma ortho-lin-indpt: assumes  $W: W \subseteq \text{carrier-vec } n$ 
  and  $X: X \subseteq \text{carrier-vec } n$ 
  and ortho:  $\bigwedge w x. w \in W \implies x \in X \implies x \cdot w = 0$ 
  and linW: lin-indpt  $W$ 
  and linX: lin-indpt  $X$ 
shows lin-indpt ( $W \cup X$ )
   $\langle \text{proof} \rangle$ 

```

```

definition normal-vector :: 'a vec set  $\Rightarrow$  'a vec where
  normal-vector  $W = (\text{let } ws = (\text{SOME } ws. \text{set } ws = W \wedge \text{distinct } ws);$ 
     $m = \text{length } ws;$ 
     $B = (\lambda j. \text{mat } m m (\lambda(i, j'). ws ! i \$ (\text{if } j' < j \text{ then } j' \text{ else } \text{Suc } j'))))$ 
     $\text{in } \text{vec } n (\lambda j. (-1)^{\wedge(m+j)} * \text{det } (B j)))$ 

```

```

lemma normal-vector: assumes fin: finite  $W$ 

```

and *card*: $Suc (card W) = n$
and *lin*: *lin-indpt* W
and W : $W \subseteq carrier-vec\ n$
shows *normal-vector* $W \in carrier-vec\ n$
normal-vector $W \neq 0_v\ n$
 $w \in W \implies w \cdot normal-vector\ W = 0$
 $w \in W \implies normal-vector\ W \cdot w = 0$
lin-indpt (*insert* (*normal-vector* W) W)
normal-vector $W \notin W$
is-det-bound $db \implies W \subseteq \mathbb{Z}_v \cap Bounded-vec\ (of-int\ Bnd) \implies normal-vector\ W$
 $\in \mathbb{Z}_v \cap Bounded-vec\ (of-int\ (db\ (n-1)\ Bnd))$
 $\langle proof \rangle$

lemma *normal-vector-span*:
assumes *card*: $Suc (card D) = n$
and D : $D \subseteq carrier-vec\ n$ **and** *fin*: *finite* D **and** *lin*: *lin-indpt* D
shows *span* $D = \{ x. x \in carrier-vec\ n \wedge x \cdot normal-vector\ D = 0 \}$
 $\langle proof \rangle$

definition *normal-vectors* :: 'a *vec list* \implies 'a *vec list* **where**
normal-vectors $ws = (let\ us = basis-extension\ ws$
 $in\ map\ (\lambda\ i.\ normal-vector\ (set\ (ws\ @\ us) - \{us\ !\ i\}))\ [0..<length\ us])$

lemma *normal-vectors*:
assumes *lin*: *lin-indpt-list* ws
shows *set* (*normal-vectors* ws) $\subseteq carrier-vec\ n$
 $w \in set\ ws \implies nv \in set\ (normal-vectors\ ws) \implies nv \cdot w = 0$
 $w \in set\ ws \implies nv \in set\ (normal-vectors\ ws) \implies w \cdot nv = 0$
lin-indpt-list ($ws\ @\ normal-vectors\ ws$)
 $length\ ws + length\ (normal-vectors\ ws) = n$
 $set\ ws \cap set\ (normal-vectors\ ws) = \{ \}$
is-det-bound $db \implies set\ ws \subseteq \mathbb{Z}_v \cap Bounded-vec\ (of-int\ Bnd) \implies$
 $set\ (normal-vectors\ ws) \subseteq \mathbb{Z}_v \cap Bounded-vec\ (of-int\ (db\ (n-1)\ (max\ 1\ Bnd)))$
 $\langle proof \rangle$

definition *pos-norm-vec* :: 'a *vec set* \implies 'a *vec* \implies 'a *vec* **where**
pos-norm-vec $D\ x = (let\ c' = normal-vector\ D;$
 $c = (if\ c' \cdot x > 0\ then\ c'\ else\ -c')\ in\ c)$

lemma *pos-norm-vec*:
assumes D : $D \subseteq carrier-vec\ n$ **and** *fin*: *finite* D **and** *lin*: *lin-indpt* D
and *card*: $Suc (card D) = n$
and *c-def*: $c = pos-norm-vec\ D\ x$
shows $c \in carrier-vec\ n$ *span* $D = \{ x. x \in carrier-vec\ n \wedge x \cdot c = 0 \}$
 $x \notin span\ D \implies x \in carrier-vec\ n \implies c \cdot x > 0$
 $c \in \{ normal-vector\ D, -normal-vector\ D \}$
 $\langle proof \rangle$

end

end

10 Dimension of Spans

We define the notion of dimension of a span of vectors and prove some natural results about them. The definition is made as a function, so that no interpretation of locales like subspace is required.

theory *Dim-Span*

imports *Missing-VS-Connect*

begin

context *vec-space*

begin

definition *dim-span* $W = \text{Max} (\text{card } \{V. V \subseteq \text{carrier-vec } n \wedge V \subseteq \text{span } W \wedge \text{lin-indpt } V\})$

lemma fixes $V W :: 'a \text{ vec set}$

shows

card-le-dim-span:

$V \subseteq \text{carrier-vec } n \implies V \subseteq \text{span } W \implies \text{lin-indpt } V \implies \text{card } V \leq \text{dim-span } W$

and

card-eq-dim-span-imp-same-span:

$V \subseteq \text{carrier-vec } n \implies V \subseteq \text{span } W \implies \text{lin-indpt } V \implies \text{card } V = \text{dim-span } W$

$W \implies \text{span } V = \text{span } W$ **and**

same-span-imp-card-eq-dim-span:

$V \subseteq \text{carrier-vec } n \implies W \subseteq \text{carrier-vec } n \implies \text{span } V = \text{span } W \implies \text{lin-indpt } V \implies \text{card } V = \text{dim-span } W$ **and**

dim-span-cong:

$\text{span } V = \text{span } W \implies \text{dim-span } V = \text{dim-span } W$ **and**

ex-basis-span:

$V \subseteq \text{carrier-vec } n \implies \exists W. W \subseteq \text{carrier-vec } n \wedge \text{lin-indpt } W \wedge \text{span } V = \text{span } W \wedge \text{dim-span } V = \text{card } W$

<proof>

lemma *dim-span-le-n:* **assumes** $W: W \subseteq \text{carrier-vec } n$ **shows** $\text{dim-span } W \leq n$

<proof>

lemma *dim-span-insert:* **assumes** $W: W \subseteq \text{carrier-vec } n$

and $v: v \in \text{carrier-vec } n$ **and** $vs: v \notin \text{span } W$

shows $\text{dim-span } (\text{insert } v W) = \text{Suc } (\text{dim-span } W)$

<proof>

end

end

11 The Fundamental Theorem of Linear Inequalities

The theorem states that for a given set of vectors A and vector b , either b is in the cone of a linear independent subset of A , or there is a hyperplane that contains $\text{span}(A, b) - 1$ linearly independent vectors of A that separates A from b . We prove this theorem and derive some consequences, e.g., Caratheodory's theorem that b is the cone of A iff b is in the cone of a linear independent subset of A .

theory *Fundamental-Theorem-Linear-Inequalities*

imports

Cone

Normal-Vector

Dim-Span

begin

context *gram-schmidt*

begin

The mentions equivances A-D are:

- A: b is in the cone of vectors A ,
- B: b is in the cone of a subset of linear independent of vectors A ,
- C: there is no separating hyperplane of b and the vectors A , which contains \dim many linear independent vectors of A
- D: there is no separating hyperplane of b and the vectors A

lemma *fundamental-theorem-of-linear-inequalities-A-imp-D:*

assumes $A: A \subseteq \text{carrier-vec } n$

and $\text{fin}: \text{finite } A$

and $b: b \in \text{cone } A$

shows $\nexists c. c \in \text{carrier-vec } n \wedge (\forall a_i \in A. c \cdot a_i \geq 0) \wedge c \cdot b < 0$

<proof>

The difficult direction is that C implies B. To this end we follow the proof that at least one of B and the negation of C is satisfied.

context

fixes $a :: \text{nat} \Rightarrow 'a \text{ vec}$

and $b :: 'a \text{ vec}$

and $m :: \text{nat}$

assumes $a: a \text{ ' } \{0 \dots m\} \subseteq \text{carrier-vec } n$

and $\text{inj-a}: \text{inj-on } a \text{ ' } \{0 \dots m\}$

and $b: b \in \text{carrier-vec } n$

and $\text{full-span}: \text{span } (a \text{ ' } \{0 \dots m\}) = \text{carrier-vec } n$

begin

private definition $goal = ((\exists I. I \subseteq \{0 \dots m\} \wedge card (a \cdot I) = n \wedge lin-indpt (a \cdot I) \wedge b \in finite-cone (a \cdot I)) \vee (\exists c I. I \subseteq \{0 \dots m\} \wedge c \in \{normal-vector (a \cdot I), - normal-vector (a \cdot I)\} \wedge Suc (card (a \cdot I)) = n \wedge lin-indpt (a \cdot I) \wedge (\forall i < m. c \cdot a_i \geq 0) \wedge c \cdot b < 0))$

private lemma $card-a-I[simp]: I \subseteq \{0 \dots m\} \implies card (a \cdot I) = card I$
 $\langle proof \rangle$ **lemma** $in-a-I[simp]: I \subseteq \{0 \dots m\} \implies i < m \implies (a_i \in a \cdot I) = (i \in I)$
 $\langle proof \rangle$ **definition** $valid-I = \{ I. card I = n \wedge lin-indpt (a \cdot I) \wedge I \subseteq \{0 \dots m\} \}$

private definition $cond$ where $cond I I' l c h k \equiv$
 $b = lincomb l (a \cdot I) \wedge$
 $h \in I \wedge l (a \cdot h) < 0 \wedge (\forall h'. h' \in I \longrightarrow h' < h \longrightarrow l (a \cdot h') \geq 0) \wedge$
 $c \in carrier-vec n \wedge span (a \cdot (I - \{h\})) = \{ x. x \in carrier-vec n \wedge c \cdot x = 0 \}$
 $\wedge c \cdot b < 0 \wedge$
 $k < m \wedge c \cdot a_k < 0 \wedge (\forall k'. k' < k \longrightarrow c \cdot a_{k'} \geq 0) \wedge$
 $I' = insert k (I - \{h\})$

private definition $step-rel = Restr \{ (I'', I). \exists l c h k. cond I I'' l c h k \} valid-I$

private lemma $finite-step-rel: finite step-rel$
 $\langle proof \rangle$ **lemma** $acyclic-imp-goal: acyclic step-rel \implies goal$
 $\langle proof \rangle$ **lemma** $acyclic-step-rel: acyclic step-rel$
 $\langle proof \rangle$

lemma $fundamental-theorem-neg-C-or-B-in-context:$
assumes $W: W = a \cdot \{0 \dots m\}$
shows $(\exists U. U \subseteq W \wedge card U = n \wedge lin-indpt U \wedge b \in finite-cone U) \vee$
 $(\exists c U. U \subseteq W \wedge$
 $c \in \{normal-vector U, - normal-vector U\} \wedge$
 $Suc (card U) = n \wedge lin-indpt U \wedge (\forall w \in W. 0 \leq c \cdot w) \wedge c \cdot b < 0)$
 $\langle proof \rangle$

end

lemma $fundamental-theorem-of-linear-inequalities-C-imp-B-full-dim:$
assumes $A: A \subseteq carrier-vec n$
and $fin: finite A$
and $span: span A = carrier-vec n$
and $b: b \in carrier-vec n$
and $C: \nexists c B. B \subseteq A \wedge c \in \{normal-vector B, - normal-vector B\} \wedge Suc (card B) = n$
 $\wedge lin-indpt B \wedge (\forall a_i \in A. c \cdot a_i \geq 0) \wedge c \cdot b < 0$
shows $\exists B \subseteq A. lin-indpt B \wedge card B = n \wedge b \in finite-cone B$
 $\langle proof \rangle$

lemma *fundamental-theorem-of-linear-inequalities-full-dim*: **fixes** $A :: 'a \text{ vec set}$
defines $\text{HyperN} \equiv \{b. b \in \text{carrier-vec } n \wedge (\nexists B \ c. B \subseteq A \wedge c \in \{\text{normal-vector } B, - \text{normal-vector } B\}$
 $\wedge \text{Suc} (\text{card } B) = n \wedge \text{lin-indpt } B \wedge (\forall a_i \in A. c \cdot a_i \geq 0) \wedge c \cdot b < 0)\}$
defines $\text{HyperA} \equiv \{b. b \in \text{carrier-vec } n \wedge (\nexists c. c \in \text{carrier-vec } n \wedge (\forall a_i \in A. c \cdot a_i \geq 0) \wedge c \cdot b < 0)\}$
defines $\text{lin-indpt-cone} \equiv \bigcup \{\text{finite-cone } B \mid B. B \subseteq A \wedge \text{card } B = n \wedge \text{lin-indpt } B\}$
assumes $A: A \subseteq \text{carrier-vec } n$
and $\text{fin}: \text{finite } A$
and $\text{span}: \text{span } A = \text{carrier-vec } n$
shows
 $\text{cone } A = \text{lin-indpt-cone}$
 $\text{cone } A = \text{HyperN}$
 $\text{cone } A = \text{HyperA}$
 $\langle \text{proof} \rangle$

lemma *fundamental-theorem-of-linear-inequalities-C-imp-B*:
assumes $A: A \subseteq \text{carrier-vec } n$
and $\text{fin}: \text{finite } A$
and $b: b \in \text{carrier-vec } n$
and $C: \nexists c \ A'. c \in \text{carrier-vec } n$
 $\wedge A' \subseteq A \wedge \text{Suc} (\text{card } A') = \text{dim-span} (\text{insert } b \ A)$
 $\wedge (\forall a \in A'. c \cdot a = 0)$
 $\wedge \text{lin-indpt } A' \wedge (\forall a_i \in A. c \cdot a_i \geq 0) \wedge c \cdot b < 0$
shows $\exists B \subseteq A. \text{lin-indpt } B \wedge \text{card } B = \text{dim-span } A \wedge b \in \text{finite-cone } B$
 $\langle \text{proof} \rangle$

lemma *fundamental-theorem-of-linear-inequalities*: **fixes** $A :: 'a \text{ vec set}$
defines $\text{HyperN} \equiv \{b. b \in \text{carrier-vec } n \wedge (\nexists c \ B. c \in \text{carrier-vec } n \wedge B \subseteq A$
 $\wedge \text{Suc} (\text{card } B) = \text{dim-span} (\text{insert } b \ A) \wedge \text{lin-indpt } B$
 $\wedge (\forall a \in B. c \cdot a = 0)$
 $\wedge (\forall a_i \in A. c \cdot a_i \geq 0) \wedge c \cdot b < 0)\}$
defines $\text{HyperA} \equiv \{b. b \in \text{carrier-vec } n \wedge (\nexists c. c \in \text{carrier-vec } n \wedge (\forall a_i \in A. c \cdot a_i \geq 0) \wedge c \cdot b < 0)\}$
defines $\text{lin-indpt-cone} \equiv \bigcup \{\text{finite-cone } B \mid B. B \subseteq A \wedge \text{card } B = \text{dim-span } A$
 $\wedge \text{lin-indpt } B\}$
assumes $A: A \subseteq \text{carrier-vec } n$
and $\text{fin}: \text{finite } A$
shows
 $\text{cone } A = \text{lin-indpt-cone}$
 $\text{cone } A = \text{HyperN}$
 $\text{cone } A = \text{HyperA}$
 $\langle \text{proof} \rangle$

corollary *Caratheodory-theorem*: **assumes** $A: A \subseteq \text{carrier-vec } n$
shows $\text{cone } A = \bigcup \{\text{finite-cone } B \mid B. B \subseteq A \wedge \text{lin-indpt } B\}$
 $\langle \text{proof} \rangle$

end
end

12 Farkas' Lemma

We prove two variants of Farkas' lemma. Note that type here is more general than in the versions of Farkas' Lemma which are in the AFP-entry Farkas-Lemma, which is restricted to rational matrices. However, there δ -rationals are supported, which are not present here.

theory *Farkas-Lemma*

imports *Fundamental-Theorem-Linear-Inequalities*

begin

context *gram-schmidt*

begin

lemma *Farkas-Lemma*: **fixes** $A :: 'a\ mat$ **and** $b :: 'a\ vec$

assumes $A: A \in carrier\ mat\ n\ nr$ **and** $b: b \in carrier\ vec\ n$

shows $(\exists x. x \geq 0_v\ nr \wedge A *_{v} x = b) \longleftrightarrow (\forall y. y \in carrier\ vec\ n \longrightarrow A^T *_{v} y \geq 0_v\ nr \longrightarrow y \cdot b \geq 0)$

<proof>

lemma *Farkas-Lemma'*:

fixes $A :: 'a\ mat$ **and** $b :: 'a\ vec$

assumes $A: A \in carrier\ mat\ nr\ nc$ **and** $b: b \in carrier\ vec\ nr$

shows $(\exists x. x \in carrier\ vec\ nc \wedge A *_{v} x \leq b)$

$\longleftrightarrow (\forall y. y \geq 0_v\ nr \wedge A^T *_{v} y = 0_v\ nc \longrightarrow y \cdot b \geq 0)$

<proof>

end

end

13 The Theorem of Farkas, Minkowsky and Weyl

We prove the theorem of Farkas, Minkowsky and Weyl that a cone is finitely generated iff it is polyhedral. Moreover, we provide quantitative bounds via determinant bounds.

theory *Farkas-Minkowsky-Weyl*

imports *Fundamental-Theorem-Linear-Inequalities*

begin

context *gram-schmidt*

begin

We first prove the one direction of the theorem for the case that the span of the vectors is the full n -dimensional space.

lemma *farkas-minkowsky-weyl-theorem-1-full-dim:*

assumes $X: X \subseteq \text{carrier-vec } n$
and $\text{fin}: \text{finite } X$
and $\text{span}: \text{span } X = \text{carrier-vec } n$
shows $\exists \text{ nr } A. A \in \text{carrier-mat nr } n \wedge \text{cone } X = \text{polyhedral-cone } A$
 $\wedge (\text{is-det-bound } db \longrightarrow X \subseteq \mathbb{Z}_v \cap \text{Bounded-vec } (\text{of-int } Bnd) \longrightarrow A \in \mathbb{Z}_m \cap$
 $\text{Bounded-mat } (\text{of-int } (db \ (n-1) \ Bnd)))$
 $\langle \text{proof} \rangle$

We next generalize the theorem to the case where X does not span the full space. To this end, we extend X by unit-vectors until the full space is spanned, and then add the normal-vectors of these unit-vectors which are orthogonal to span X as additional constraints to the resulting matrix.

lemma *farkas-minkowsky-weyl-theorem-1:*

assumes $X: X \subseteq \text{carrier-vec } n$
and $\text{fin}X: \text{finite } X$
shows $\exists \text{ nr } A. A \in \text{carrier-mat nr } n \wedge \text{cone } X = \text{polyhedral-cone } A \wedge$
 $(\text{is-det-bound } db \longrightarrow X \subseteq \mathbb{Z}_v \cap \text{Bounded-vec } (\text{of-int } Bnd) \longrightarrow A \in \mathbb{Z}_m \cap$
 $\text{Bounded-mat } (\text{of-int } (db \ (n-1) \ (\text{max } 1 \ Bnd))))$
 $\langle \text{proof} \rangle$

Now for the other direction.

lemma *farkas-minkowsky-weyl-theorem-2:*

assumes $A: A \in \text{carrier-mat nr } n$
shows $\exists X. X \subseteq \text{carrier-vec } n \wedge \text{finite } X \wedge \text{polyhedral-cone } A = \text{cone } X$
 $\wedge (\text{is-det-bound } db \longrightarrow A \in \mathbb{Z}_m \cap \text{Bounded-mat } (\text{of-int } Bnd) \longrightarrow X \subseteq \mathbb{Z}_v \cap$
 $\text{Bounded-vec } (\text{of-int } (db \ (n-1) \ (\text{max } 1 \ Bnd))))$
 $\langle \text{proof} \rangle$

lemma *farkas-minkowsky-weyl-theorem:*

$(\exists X. X \subseteq \text{carrier-vec } n \wedge \text{finite } X \wedge P = \text{cone } X)$
 $\longleftrightarrow (\exists A \text{ nr}. A \in \text{carrier-mat nr } n \wedge P = \text{polyhedral-cone } A)$
 $\langle \text{proof} \rangle$

end

end

14 The Decomposition Theorem

This theory contains a proof of the fact, that every polyhedron can be decomposed into a convex hull of a finite set of points + a finitely generated cone, including bounds on the numbers that are required in the decomposition. We further prove the inverse direction of this theorem (without bounds) and as a corollary, we derive that a polyhedron is bounded iff it is the convex hull of finitely many points, i.e., a polytope.

theory *Decomposition-Theorem*

imports

Farkas-Minkowsky-Weyl

```

    Convex-Hull
begin

context gram-schmidt
begin

definition polytope  $P = (\exists V. V \subseteq \text{carrier-vec } n \wedge \text{finite } V \wedge P = \text{convex-hull } V)$ 

definition polyhedron  $A b = \{x \in \text{carrier-vec } n. A *_{\mathbf{v}} x \leq b\}$ 

lemma polyhedra-are-convex:
  assumes  $A: A \in \text{carrier-mat } nr \ n$ 
    and  $b: b \in \text{carrier-vec } nr$ 
    and  $P: P = \text{polyhedron } A \ b$ 
  shows  $\text{convex } P$ 
  <proof>

end

locale gram-schmidt- $m = n: \text{gram-schmidt } n \ f\text{-ty} + m: \text{gram-schmidt } m \ f\text{-ty}$ 
  for  $n \ m :: \text{nat}$  and  $f\text{-ty}$ 
begin

lemma vec-first-lincomb-list:
  assumes  $Xs: \text{set } Xs \subseteq \text{carrier-vec } n$ 
    and  $nm: m \leq n$ 
  shows  $\text{vec-first } (n.\text{lincomb-list } c \ Xs) \ m =$ 
     $m.\text{lincomb-list } c \ (\text{map } (\lambda v. \text{vec-first } v \ m) \ Xs)$ 
  <proof>

lemma convex-hull-next-dim:
  assumes  $n = m + 1$ 
    and  $X: X \subseteq \text{carrier-vec } n$ 
    and  $\text{finite } X$ 
    and  $Xm1: \forall y \in X. y \ \$ \ m = 1$ 
    and  $y\text{-dim}: y \in \text{carrier-vec } n$ 
    and  $y: y \ \$ \ m = 1$ 
  shows  $(\text{vec-first } y \ m \in m.\text{convex-hull } \{\text{vec-first } y \ m \mid y. y \in X\}) = (y \in n.\text{cone } X)$ 
  <proof>

lemma cone-next-dim:
  assumes  $n = m + 1$ 
    and  $X: X \subseteq \text{carrier-vec } n$ 
    and  $\text{finite } X$ 
    and  $Xm0: \forall y \in X. y \ \$ \ m = 0$ 

```

and y -dim: $y \in \text{carrier-vec } n$
and y : $y \ \$ \ m = 0$
shows $(\text{vec-first } y \ m \in m.\text{cone } \{\text{vec-first } y \ m \mid y. y \in X\}) = (y \in n.\text{cone } X)$
 $\langle \text{proof} \rangle$

end

context *gram-schmidt*
begin

lemma *decomposition-theorem-polyhedra-1*:

assumes A : $A \in \text{carrier-mat } nr \ n$
and b : $b \in \text{carrier-vec } nr$
and P : $P = \text{polyhedron } A \ b$
shows $\exists Q \ X. X \subseteq \text{carrier-vec } n \wedge \text{finite } X \wedge$
 $Q \subseteq \text{carrier-vec } n \wedge \text{finite } Q \wedge$
 $P = \text{convex-hull } Q + \text{cone } X \wedge$
 $(\text{is-det-bound } db \longrightarrow A \in \mathbb{Z}_m \cap \text{Bounded-mat } (\text{of-int } Bnd) \longrightarrow b \in \mathbb{Z}_v \cap$
 $\text{Bounded-vec } (\text{of-int } Bnd) \longrightarrow$
 $X \subseteq \mathbb{Z}_v \cap \text{Bounded-vec } (\text{of-int } (db \ n \ (\text{max } 1 \ Bnd))))$
 $\wedge Q \subseteq \text{Bounded-vec } (\text{of-int } (db \ n \ (\text{max } 1 \ Bnd))))$
 $\langle \text{proof} \rangle$

lemma *decomposition-theorem-polyhedra-2*:

assumes Q : $Q \subseteq \text{carrier-vec } n$ **and** $\text{fin-}Q$: $\text{finite } Q$
and X : $X \subseteq \text{carrier-vec } n$ **and** $\text{fin-}X$: $\text{finite } X$
and P : $P = \text{convex-hull } Q + \text{cone } X$
shows $\exists A \ b \ nr. A \in \text{carrier-mat } nr \ n \wedge b \in \text{carrier-vec } nr \wedge P = \text{polyhedron } A \ b$
 $\langle \text{proof} \rangle$

lemma *decomposition-theorem-polyhedra*:

$(\exists A \ b \ nr. A \in \text{carrier-mat } nr \ n \wedge b \in \text{carrier-vec } nr \wedge P = \text{polyhedron } A \ b)$
 \longleftrightarrow
 $(\exists Q \ X. Q \cup X \subseteq \text{carrier-vec } n \wedge \text{finite } (Q \cup X) \wedge P = \text{convex-hull } Q + \text{cone } X)$ (**is** ?l = ?r)
 $\langle \text{proof} \rangle$

lemma *polytope-equiv-bounded-polyhedron*:

$\text{polytope } P \longleftrightarrow$
 $(\exists A \ b \ nr \ bnd. A \in \text{carrier-mat } nr \ n \wedge b \in \text{carrier-vec } nr \wedge P = \text{polyhedron } A \ b$
 $\wedge P \subseteq \text{Bounded-vec } bnd)$
 $\langle \text{proof} \rangle$

end

end

15 Mixed Integer Solutions

We prove that if an integral system of linear inequalities $Ax \leq b \wedge A'x < b'$ has a (mixed)integer solution, then there is also a small (mixed)integer solution, where the numbers are bounded by $(n + 1) * db m n$ where n is the number of variables, m is a bound on the absolute values of numbers occurring in A, A', b, b' , and $db m n$ is a bound on determinants for matrices of size n with values of at most m .

theory *Mixed-Integer-Solutions*
imports *Decomposition-Theorem*
begin

definition *less-vec* :: 'a vec \Rightarrow ('a :: ord) vec \Rightarrow bool (**infix** $\langle <_v \rangle$ 50) **where**
 $v <_v w = (\dim\text{-vec } v = \dim\text{-vec } w \wedge (\forall i < \dim\text{-vec } w. v \$ i < w \$ i))$

lemma *less-vecD*: **assumes** $v <_v w$ **and** $w \in \text{carrier-vec } n$
shows $i < n \implies v \$ i < w \$ i$
 $\langle \text{proof} \rangle$

lemma *less-vecI*: **assumes** $v \in \text{carrier-vec } n$ $w \in \text{carrier-vec } n$
 $\bigwedge i. i < n \implies v \$ i < w \$ i$
shows $v <_v w$
 $\langle \text{proof} \rangle$

lemma *less-vec-lesseq-vec*: $v <_v (w :: 'a :: \text{preorder vec}) \implies v \leq w$
 $\langle \text{proof} \rangle$

lemma *floor-less*: $x \notin \mathbf{Z} \implies \text{of-int } \lfloor x \rfloor < x$
 $\langle \text{proof} \rangle$

lemma *floor-of-int-eq[simp]*: $x \in \mathbf{Z} \implies \text{of-int } \lfloor x \rfloor = x$
 $\langle \text{proof} \rangle$

locale *gram-schmidt-floor* = *gram-schmidt* n *f-ty*
for $n :: \text{nat}$ **and** *f-ty* :: 'a :: {*floor-ceiling*,
trivial-conjugatable-linordered-field} *itself*
begin

lemma *small-mixed-integer-solution-main*: **fixes** $A_1 :: 'a \text{ mat}$
assumes *db*: *is-det-bound* *db*
and *A1*: $A_1 \in \text{carrier-mat } nr_1 \ n$
and *A2*: $A_2 \in \text{carrier-mat } nr_2 \ n$
and *b1*: $b_1 \in \text{carrier-vec } nr_1$
and *b2*: $b_2 \in \text{carrier-vec } nr_2$
and *A1Bnd*: $A_1 \in \mathbf{Z}_m \cap \text{Bounded-mat } (\text{of-int } Bnd)$
and *b1Bnd*: $b_1 \in \mathbf{Z}_v \cap \text{Bounded-vec } (\text{of-int } Bnd)$

and $A2Bnd$: $A_2 \in \mathbb{Z}_m \cap \text{Bounded-mat (of-int Bnd)}$
and $b2Bnd$: $b_2 \in \mathbb{Z}_v \cap \text{Bounded-vec (of-int Bnd)}$
and x : $x \in \text{carrier-vec } n$
and xI : $x \in \text{indexed-Ints-vec } I$
and sol-nonstrict : $A_1 *_v x \leq b_1$
and sol-strict : $A_2 *_v x <_v b_2$
shows $\exists x$.
 $x \in \text{carrier-vec } n \wedge$
 $x \in \text{indexed-Ints-vec } I \wedge$
 $A_1 *_v x \leq b_1 \wedge$
 $A_2 *_v x <_v b_2 \wedge$
 $x \in \text{Bounded-vec (of-int (of-nat (n + 1) * db n (max 1 Bnd))}$
 $\langle \text{proof} \rangle$

We get rid of the max-1 operation, by showing that a smaller value of Bnd can only occur in very special cases where the theorem is trivially satisfied.

lemma *small-mixed-integer-solution*: **fixes** $A_1 :: 'a \text{ mat}$
assumes db : *is-det-bound db*
and $A1$: $A_1 \in \text{carrier-mat } nr_1 \ n$
and $A2$: $A_2 \in \text{carrier-mat } nr_2 \ n$
and $b1$: $b_1 \in \text{carrier-vec } nr_1$
and $b2$: $b_2 \in \text{carrier-vec } nr_2$
and $A1Bnd$: $A_1 \in \mathbb{Z}_m \cap \text{Bounded-mat (of-int Bnd)}$
and $b1Bnd$: $b_1 \in \mathbb{Z}_v \cap \text{Bounded-vec (of-int Bnd)}$
and $A2Bnd$: $A_2 \in \mathbb{Z}_m \cap \text{Bounded-mat (of-int Bnd)}$
and $b2Bnd$: $b_2 \in \mathbb{Z}_v \cap \text{Bounded-vec (of-int Bnd)}$
and x : $x \in \text{carrier-vec } n$
and xI : $x \in \text{indexed-Ints-vec } I$
and sol-nonstrict : $A_1 *_v x \leq b_1$
and sol-strict : $A_2 *_v x <_v b_2$
and non-degenerate : $nr_1 \neq 0 \vee nr_2 \neq 0 \vee Bnd \geq 0$
shows $\exists x$.
 $x \in \text{carrier-vec } n \wedge$
 $x \in \text{indexed-Ints-vec } I \wedge$
 $A_1 *_v x \leq b_1 \wedge$
 $A_2 *_v x <_v b_2 \wedge$
 $x \in \text{Bounded-vec (of-int (int (n+1) * db n Bnd))}$
 $\langle \text{proof} \rangle$

lemmas *small-mixed-integer-solution-hadamard* =
small-mixed-integer-solution[OF det-bound-hadamard, unfolded det-bound-hadamard-def of-int-mult of-int-of-nat-eq]

lemma *Bounded-vec-of-int*: **assumes** $v \in \text{Bounded-vec } bnd$
shows $(\text{map-vec of-int } v :: 'a \text{ vec}) \in \mathbb{Z}_v \cap \text{Bounded-vec (of-int } bnd)$
 $\langle \text{proof} \rangle$

lemma *Bounded-mat-of-int*: **assumes** $A \in \text{Bounded-mat } bnd$

shows $(\text{map-mat of-int } A :: 'a \text{ mat}) \in \mathbf{Z}_m \cap \text{Bounded-mat (of-int bnd)}$
 ⟨proof⟩

lemma *small-mixed-integer-solution-int-mat*: **fixes** $x :: 'a \text{ vec}$

assumes $db: \text{is-det-bound } db$

and $A1: A_1 \in \text{carrier-mat } nr_1 \ n$

and $A2: A_2 \in \text{carrier-mat } nr_2 \ n$

and $b1: b_1 \in \text{carrier-vec } nr_1$

and $b2: b_2 \in \text{carrier-vec } nr_2$

and $A1Bnd: A_1 \in \text{Bounded-mat } Bnd$

and $b1Bnd: b_1 \in \text{Bounded-vec } Bnd$

and $A2Bnd: A_2 \in \text{Bounded-mat } Bnd$

and $b2Bnd: b_2 \in \text{Bounded-vec } Bnd$

and $x: x \in \text{carrier-vec } n$

and $xI: x \in \text{indexed-Ints-vec } I$

and $\text{sol-nonstrict}: \text{map-mat of-int } A_1 *_v x \leq \text{map-vec of-int } b_1$

and $\text{sol-strict}: \text{map-mat of-int } A_2 *_v x <_v \text{map-vec of-int } b_2$

and $\text{non-degenerate}: nr_1 \neq 0 \vee nr_2 \neq 0 \vee Bnd \geq 0$

shows $\exists x :: 'a \text{ vec.}$

$x \in \text{carrier-vec } n \wedge$

$x \in \text{indexed-Ints-vec } I \wedge$

$\text{map-mat of-int } A_1 *_v x \leq \text{map-vec of-int } b_1 \wedge$

$\text{map-mat of-int } A_2 *_v x <_v \text{map-vec of-int } b_2 \wedge$

$x \in \text{Bounded-vec (of-int (of-nat (n+1)) * db n Bnd)}$

⟨proof⟩

lemmas *small-mixed-integer-solution-int-mat-hadamard* =

small-mixed-integer-solution-int-mat[OF det-bound-hadamard, unfolded det-bound-hadamard-def of-int-mult of-int-of-nat-eq]

end

lemma *of-int-hom-le*: $(\text{of-int-hom.vec-hom } v :: 'a :: \text{linordered-field vec}) \leq \text{of-int-hom.vec-hom}$

$w \iff v \leq w$

⟨proof⟩

lemma *of-int-hom-less*: $(\text{of-int-hom.vec-hom } v :: 'a :: \text{linordered-field vec}) <_v \text{of-int-hom.vec-hom}$

$w \iff v <_v w$

⟨proof⟩

lemma *Ints-vec-to-int-vec*: **assumes** $v \in \mathbf{Z}_v$

shows $\exists w. v = \text{map-vec of-int } w$

⟨proof⟩

lemma *small-integer-solution*: **fixes** $A_1 :: \text{int mat}$

assumes $db: \text{is-det-bound } db$

and $A1: A_1 \in \text{carrier-mat } nr_1 \ n$

and $A2: A_2 \in \text{carrier-mat } nr_2 \ n$

and $b1: b_1 \in \text{carrier-vec } nr_1$

```

and b2:  $b_2 \in \text{carrier-vec } nr_2$ 
and A1Bnd:  $A_1 \in \text{Bounded-mat } Bnd$ 
and b1Bnd:  $b_1 \in \text{Bounded-vec } Bnd$ 
and A2Bnd:  $A_2 \in \text{Bounded-mat } Bnd$ 
and b2Bnd:  $b_2 \in \text{Bounded-vec } Bnd$ 
and x:  $x \in \text{carrier-vec } n$ 
and sol-nonstrict:  $A_1 *_v x \leq b_1$ 
and sol-strict:  $A_2 *_v x <_v b_2$ 
and non-degenerate:  $nr_1 \neq 0 \vee nr_2 \neq 0 \vee Bnd \geq 0$ 
shows  $\exists x.$ 
   $x \in \text{carrier-vec } n \wedge$ 
   $A_1 *_v x \leq b_1 \wedge$ 
   $A_2 *_v x <_v b_2 \wedge$ 
   $x \in \text{Bounded-vec } (\text{of-nat } (n+1) * db \ n \ Bnd)$ 
<proof>

```

```

corollary small-integer-solution-nonstrict: fixes  $A :: \text{int mat}$ 
assumes  $db: \text{is-det-bound } db$ 
and  $A: A \in \text{carrier-mat } nr \ n$ 
and  $b: b \in \text{carrier-vec } nr$ 
and  $ABnd: A \in \text{Bounded-mat } Bnd$ 
and  $bBnd: b \in \text{Bounded-vec } Bnd$ 
and  $x: x \in \text{carrier-vec } n$ 
and  $sol: A *_v x \leq b$ 
and  $non-degenerate: nr \neq 0 \vee Bnd \geq 0$ 
shows  $\exists y.$ 
   $y \in \text{carrier-vec } n \wedge$ 
   $A *_v y \leq b \wedge$ 
   $y \in \text{Bounded-vec } (\text{of-nat } (n+1) * db \ n \ Bnd)$ 
<proof>

```

```

lemmas small-integer-solution-nonstrict-hadamard =
  small-integer-solution-nonstrict[OF det-bound-hadamard, unfolded det-bound-hadamard-def]

```

end

16 Integer Hull

We define the integer hull of a polyhedron, i.e., the convex hull of all integer solutions. Moreover, we prove the result of Meyer that the integer hull of a polyhedron defined by an integer matrix is again a polyhedron, and give bounds for a corresponding decomposition theorem.

```

theory Integer-Hull
imports
  Decomposition-Theorem
  Mixed-Integer-Solutions
begin

```

context *gram-schmidt*

begin

definition *integer-hull* $P = \text{convex-hull } (P \cap \mathbb{Z}_v)$

lemma *integer-hull-mono*: $P \subseteq Q \implies \text{integer-hull } P \subseteq \text{integer-hull } Q$
{*proof*}

end

lemma *abs-neg-floor*: $|\text{of-int } b| \leq \text{Bnd} \implies -(\text{floor } \text{Bnd}) \leq b$
{*proof*}

lemma *abs-pos-floor*: $|\text{of-int } b| \leq \text{Bnd} \implies b \leq \text{floor } \text{Bnd}$
{*proof*}

context *gram-schmidt-floor*

begin

lemma *integer-hull-integer-cone*: **assumes** $C: C \subseteq \text{carrier-vec } n$
and $CI: C \subseteq \mathbb{Z}_v$
shows $\text{integer-hull } (\text{cone } C) = \text{cone } C$
{*proof*}

theorem *decomposition-theorem-integer-hull-of-polyhedron*:

assumes $db: \text{is-det-bound } db$
and $A: A \in \text{carrier-mat } nr \ n$
and $b: b \in \text{carrier-vec } nr$
and $AI: A \in \mathbb{Z}_m$
and $bI: b \in \mathbb{Z}_v$
and $P: P = \text{polyhedron } A \ b$
and $\text{Bnd}: \text{of-int } \text{Bnd} \geq \text{Max } (\text{abs } ' (\text{elements-mat } A \cup \text{vec-set } b))$
shows $\exists H \ C. H \cup C \subseteq \text{carrier-vec } n \cap \mathbb{Z}_v$
 $\wedge H \subseteq \text{Bounded-vec } (\text{of-nat } (n + 1) * \text{of-int } (db \ n \ (\text{max } 1 \ \text{Bnd})))$
 $\wedge C \subseteq \text{Bounded-vec } (\text{of-int } (db \ n \ (\text{max } 1 \ \text{Bnd})))$
 $\wedge \text{finite } (H \cup C)$
 $\wedge \text{integer-hull } P = \text{convex-hull } H + \text{cone } C$
{*proof*}

corollary *integer-hull-of-polyhedron*: **assumes** $A: A \in \text{carrier-mat } nr \ n$

and $b: b \in \text{carrier-vec } nr$
and $AI: A \in \mathbb{Z}_m$
and $bI: b \in \mathbb{Z}_v$
and $P: P = \text{polyhedron } A \ b$
shows $\exists A' \ b' \ nr'. A' \in \text{carrier-mat } nr' \ n \wedge b' \in \text{carrier-vec } nr' \wedge$
 $\text{integer-hull } P = \text{polyhedron } A' \ b'$
{*proof*}

corollary *small-integer-solution-nonstrict-via-decomp*: **fixes** $A :: 'a \ \text{mat}$

```

assumes db: is-det-bound db
  and A:  $A \in \text{carrier-mat } nr \ n$ 
  and b:  $b \in \text{carrier-vec } nr$ 
  and AI:  $A \in \mathbb{Z}_m$ 
  and bI:  $b \in \mathbb{Z}_v$ 
  and Bnd: of-int Bnd  $\geq \text{Max } (\text{abs } ' (\text{elements-mat } A \cup \text{vec-set } b))$ 
  and x:  $x \in \text{carrier-vec } n$ 
  and xI:  $x \in \mathbb{Z}_v$ 
  and sol:  $A *_v x \leq b$ 
shows  $\exists y.$ 
   $y \in \text{carrier-vec } n \wedge$ 
   $y \in \mathbb{Z}_v \wedge$ 
   $A *_v y \leq b \wedge$ 
   $y \in \text{Bounded-vec } (\text{of-nat } (n+1) * \text{of-int } (db \ n \ (\text{max } 1 \ Bnd)))$ 
<proof>

lemmas small-integer-solution-nonstrict-via-decomp-hadamard =
  small-integer-solution-nonstrict-via-decomp[OF det-bound-hadamard, unfolded det-bound-hadamard-def]

end
end

```

References

- [1] B. Dutertre and L. M. de Moura. A fast linear-arithmetic solver for DPLL(T). In *Proc. Computer Aided Verification*, volume 4144 of *LNCS*, pages 81–94. Springer, 2006. Extended version available as Technical Report, CSL-06-01, SRI International.
- [2] C. H. Papadimitriou. On the complexity of integer programming. *J. ACM*, 28(4):765–768, 1981.
- [3] A. Schrijver. *Theory of linear and integer programming*. John Wiley & Sons, 1998.