# Linear Inequalities*

Ralph Bottesch[1], Alban Reynaud[2], and René Thiemann[1]

[1]University of Innsbruck
[2]ENS Lyon

March 17, 2025

**Abstract**

We formalize results about linear inqualities, 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 in 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* $\beta$ *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* $|y_i| \leq (n+1) \cdot \sqrt{n^n} \cdot \beta^n$ *for each entry* $y_i$ *of* $y$.

The verified bound in Theorem 1 in particular implies that integer-satisfiability of linear-inqualities 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** $v \in$ *set vs* **and** $w \in$ *set vs*
**shows** $(v \cdot w = 0) = (v \neq w)$
⟨*proof*⟩

**lemma** *zero-mat-mult-vector*[*simp*]: $x \in$ *carrier-vec nc* $\Longrightarrow 0_m$ *nr nc* $*_v$ $x = 0_v$ *nr*
  ⟨*proof*⟩

**lemma** *add-diff-cancel-right-vec*:
  $a \in$ *carrier-vec n* $\Longrightarrow$ ($b$ :: $'a$ :: *cancel-ab-semigroup-add vec*) $\in$ *carrier-vec n* $\Longrightarrow$
    $(a + b) - b = a$
  ⟨*proof*⟩

**lemma** *elements-four-block-mat-id*:
  **assumes** *c*: $A \in$ *carrier-mat nr1 nc1* $B \in$ *carrier-mat nr1 nc2*
    $C \in$ *carrier-mat nr2 nc1* $D \in$ *carrier-mat nr2 nc2*
  **shows**
    *elements-mat* (*four-block-mat* $A$ $B$ $C$ $D$) =
   *elements-mat* $A$ $\cup$ *elements-mat* $B$ $\cup$ *elements-mat* $C$ $\cup$ *elements-mat* $D$
    (**is** *elements-mat ?four* = *?X*)
⟨*proof*⟩

**lemma** *elements-mat-append-rows*: $A \in$ *carrier-mat nr n* $\Longrightarrow B \in$ *carrier-mat nr2 n* $\Longrightarrow$
  *elements-mat* ($A$ $@_r$ $B$) = *elements-mat* $A$ $\cup$ *elements-mat* $B$

⟨*proof*⟩

**lemma** *elements-mat-uminus*[*simp*]: *elements-mat* $(-A)$ = *uminus* ‘ *elements-mat* *A*
⟨*proof*⟩

**lemma** *vec-set-uminus*[*simp*]: *vec-set* $(-A)$ = *uminus* ‘ *vec-set* *A*
⟨*proof*⟩

**definition** *append-cols* :: *'a* :: *zero mat* ⇒ *'a mat* ⇒ *'a mat* (**infixr** ‹$@_c$› *65*)
**where**
$A\ @_c\ B = (A^T\ @_r\ B^T)^T$

**lemma** *carrier-append-cols*[*simp*, *intro*]:
*A* ∈ *carrier-mat nr nc1* ⟹
*B* ∈ *carrier-mat nr nc2* ⟹ $(A\ @_c\ B)$ ∈ *carrier-mat nr* (*nc1* + *nc2*)
⟨*proof*⟩

**lemma** *elements-mat-transpose-mat*[*simp*]: *elements-mat* $(A^T)$ = *elements-mat* *A*
⟨*proof*⟩

**lemma** *elements-mat-append-cols*: *A* ∈ *carrier-mat n nc* ⟹ *B* ∈ *carrier-mat n nc1*
⟹ *elements-mat* $(A\ @_c\ B)$ = *elements-mat* *A* ∪ *elements-mat* *B*
⟨*proof*⟩

**lemma** *vec-first-index*:
**assumes** *v*: *dim-vec v* ≥ *n*
**and** *i*: *i* < *n*
**shows** (*vec-first v n*) $ *i* = *v* $ *i*
⟨*proof*⟩

**lemma** *vec-last-index*:
**assumes** *v*: *v* ∈ *carrier-vec* (*n* + *m*)
**and** *i*: *i* < *m*
**shows** (*vec-last v m*) $ *i* = *v* $ (*n* + *i*)
⟨*proof*⟩

**lemma** *vec-first-add*:
**assumes** *dim-vec x* ≥ *n*
**and** *dim-vec y* ≥ *n*
**shows***vec-first* (*x* + *y*) *n* = *vec-first x n* + *vec-first y n*
⟨*proof*⟩

**lemma** *vec-first-zero*[*simp*]: *m* ≤ *n* ⟹ *vec-first* ($0_v$ *n*) *m* = $0_v$ *m*
⟨*proof*⟩

**lemma** *vec-first-smult*:
⟦ *m* ≤ *n*; *x* ∈ *carrier-vec n* ⟧ ⟹ *vec-first* ($c \cdot_v x$) *m* = $c \cdot_v$ *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** $a :: 'a :: ordered\text{-}ab\text{-}group\text{-}add\ vec$
**shows** $(a \leq b) = (a - b \leq 0_v\ (dim\text{-}vec\ a))$
⟨*proof*⟩

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

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

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

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

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

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

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

**lemma** *append-rows-nth*:
**assumes** $A \in carrier\text{-}mat\ nr1\ nc$
**and** $B \in carrier\text{-}mat\ nr2\ nc$
**shows** $i < nr1 \Longrightarrow row\ (A\ @_r\ B)\ i = row\ A\ i$
**and** $[\![\ i \geq nr1;\ i < nr1 + nr2\ ]\!] \Longrightarrow row\ (A\ @_r\ B)\ i = row\ B\ (i - nr1)$
⟨*proof*⟩

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

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

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

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

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

⟨*proof*⟩

**lemma** *mat-col-first-dim*[*simp*]:
*dim-row* (*mat-col-first A n*) = *dim-row A*
*dim-col* (*mat-col-first A n*) = *n*
⟨*proof*⟩

**lemma** *mat-col-last-carrier*[*simp*]: *mat-col-last A n* ∈ *carrier-mat* (*dim-row A*) *n*
⟨*proof*⟩

**lemma** *mat-col-last-dim*[*simp*]:
*dim-row* (*mat-col-last A n*) = *dim-row A*
*dim-col* (*mat-col-last A n*) = *n*
⟨*proof*⟩

**lemma** *mat-col-first-nth*[*simp*]:
⟦ *i* < *n*; *i* < *dim-col A* ⟧ ⟹ *col* (*mat-col-first A n*) *i* = *col A i*
⟨*proof*⟩

**lemma** *append-cols-nth*:
**assumes** *A* ∈ *carrier-mat nr nc1*
**and** *B* ∈ *carrier-mat nr nc2*
**shows** *i* < *nc1* ⟹ *col* (*A* $@_c$ *B*) *i* = *col A i*
**and** ⟦ *i* ≥ *nc1*; *i* < *nc1* + *nc2* ⟧ ⟹ *col* (*A* $@_c$ *B*) *i* = *col B* (*i* − *nc1*)
⟨*proof*⟩

**lemma** *mat-of-col-last-nth*[*simp*]:
⟦ *i* < *n*; *i* < *dim-col A* ⟧ ⟹ *col* (*mat-col-last A n*) *i* = *col A* (*dim-col A* − *n* + *i*)
⟨*proof*⟩

**lemma** *mat-col-first-last-append*:
**assumes** *dim-col A* = *m* + *n*
**shows** (*mat-col-first A m*) $@_c$ (*mat-col-last A n*) = *A*
⟨*proof*⟩

**lemma** *mat-of-row-dim-row-1*: (*dim-row A* = *1*) = (*A* = *mat-of-row* (*row A 0*))
⟨*proof*⟩

**lemma** *mat-of-col-dim-col-1*: (*dim-col A* = *1*) = (*A* = *mat-of-col* (*col A 0*))
⟨*proof*⟩

**definition** *vec-of-scal* :: *'a* ⇒ *'a vec* **where** *vec-of-scal x* ≡ *vec 1* (λ *i*. *x*)

**lemma** *vec-of-scal-dim*[*simp*]:
*dim-vec* (*vec-of-scal x*) = *1*
*vec-of-scal x* ∈ *carrier-vec 1*
⟨*proof*⟩

**lemma** *index-vec-of-scal*[*simp*]: (*vec-of-scal x*) \$ *0* = *x*
⟨*proof*⟩

**lemma** *row-mat-of-col*[*simp*]: *i* < *dim-vec v* ⟹ *row* (*mat-of-col v*) *i* = *vec-of-scal* (*v* \$ *i*)
⟨*proof*⟩

**lemma** *vec-of-scal-dim-1*: (*v* ∈ *carrier-vec 1*) = (*v* = *vec-of-scal* (*v* \$ *0*))
⟨*proof*⟩

**lemma** *mult-mat-of-row-vec-of-scal*: **fixes** *x* :: *'a* :: *comm-ring-1*
**shows** *mat-of-col v* $*_v$ *vec-of-scal x* = *x* $\cdot_v$ *v*
⟨*proof*⟩

**lemma** *smult-pos-vec*[*simp*]: **fixes** *l* :: *'a* :: *linordered-ring-strict*
**assumes** *l*: *l* > *0*
**shows** (*l* $\cdot_v$ *v* ≤ $0_v$ *n*) = (*v* ≤ $0_v$ *n*)
⟨*proof*⟩

**lemma** *finite-elements-mat*[*simp*]: *finite* (*elements-mat A*)
⟨*proof*⟩

**lemma** *finite-vec-set*[*simp*]: *finite* (*vec-set A*)
⟨*proof*⟩

**lemma** *lesseq-vecI*: **assumes** *v* ∈ *carrier-vec n* *w* ∈ *carrier-vec n*
⋀ *i*. *i* < *n* ⟹ *v* \$ *i* ≤ *w* \$ *i*
**shows** *v* ≤ *w*
⟨*proof*⟩

**lemma** *lesseq-vecD*: **assumes** *w* ∈ *carrier-vec n*
**and** *v* ≤ *w*
**and** *i* < *n*
**shows** *v* \$ *i* ≤ *w* \$ *i*
⟨*proof*⟩

**lemma** *vec-add-mono*: **fixes** *a* :: *'a* :: *ordered-ab-semigroup-add vec*
**assumes** *dim*: *dim-vec b* = *dim-vec d*
**and** *ab*: *a* ≤ *b*
**and** *cd*: *c* ≤ *d*
**shows** *a* + *c* ≤ *b* + *d*
⟨*proof*⟩

**lemma** *smult-nneg-npos-vec*: **fixes** *l* :: *'a* :: *ordered-semiring-0*
**assumes** *l*: *l* ≥ *0*
**and** *v*: *v* ≤ $0_v$ *n*
**shows** *l* $\cdot_v$ *v* ≤ $0_v$ *n*
⟨*proof*⟩

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

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

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

**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** $A$: $A \subseteq carrier\text{-}vec\ n$
  **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** $f$: $f \in U \rightarrow carrier\text{-}vec\ n$
    **and** $w$: $w \in carrier\text{-}vec\ n$
  **shows** $w \cdot finsum\ V\ f\ U = sum\ (\lambda u.\ w \cdot f\ u)\ U$
  $\langle proof \rangle$

**lemma** *lincomb-scalar-prod-left*: **assumes** $W \subseteq carrier\text{-}vec\ n\ v \in carrier\text{-}vec\ n$
  **shows** $lincomb\ a\ W \cdot v = (\sum w \in W.\ a\ w * (w \cdot v))$
  $\langle proof \rangle$

**lemma** *lincomb-scalar-prod-right*: **assumes** $W \subseteq carrier\text{-}vec\ n\ v \in carrier\text{-}vec\ n$
  **shows** $v \cdot lincomb\ a\ W = (\sum w \in W.\ a\ w * (v \cdot w))$
  $\langle proof \rangle$

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

⟨*proof*⟩

**lemma** *span-carrier-lin-indpt-card-n*:
**assumes** $W \subseteq$ *carrier-vec n card W* $=$ *n lin-indpt W*
**shows** *span W* $=$ *carrier-vec n*
⟨*proof*⟩

**lemma** *ortho-span*: **assumes** *W*: $W \subseteq$ *carrier-vec n*
**and** *X*: $X \subseteq$ *carrier-vec n*
**and** *ortho*: $\bigwedge$ *w x*. $w \in W \Longrightarrow x \in X \Longrightarrow w \cdot x = 0$
**and** *w*: $w \in$ *span W* **and** *x*: $x \in X$
**shows** $w \cdot x = 0$
⟨*proof*⟩

**lemma** *ortho-span'*: **assumes** *W*: $W \subseteq$ *carrier-vec n*
**and** *X*: $X \subseteq$ *carrier-vec n*
**and** *ortho*: $\bigwedge$ *w x*. $w \in W \Longrightarrow x \in X \Longrightarrow x \cdot w = 0$
**and** *w*: $w \in$ *span W* **and** *x*: $x \in X$
**shows** $x \cdot w = 0$
⟨*proof*⟩

**lemma** *ortho-span-span*: **assumes** *W*: $W \subseteq$ *carrier-vec n*
**and** *X*: $X \subseteq$ *carrier-vec n*
**and** *ortho*: $\bigwedge$ *w x*. $w \in W \Longrightarrow x \in X \Longrightarrow w \cdot x = 0$
**and** *w*: $w \in$ *span W* **and** *x*: $x \in$ *span X*
**shows** $w \cdot x = 0$
⟨*proof*⟩

**lemma** *lincomb-in-span*[*intro*]:
**assumes** *X*: $X \subseteq$ *carrier-vec n*
**shows** *lincomb a X* $\in$ *span X*
⟨*proof*⟩

**lemma** *generating-card-n-basis*: **assumes** *X*: $X \subseteq$ *carrier-vec n*
**and** *span*: *carrier-vec n* $\subseteq$ *span X*
**and** *card*: *card X* $=$ *n*
**shows** *basis X*
⟨*proof*⟩

**lemma** *lincomb-list-append*:
**assumes** *Ws*: *set Ws* $\subseteq$ *carrier-vec n*
**shows** *set Vs* $\subseteq$ *carrier-vec n* $\Longrightarrow$ *lincomb-list f* (*Vs* @ *Ws*) $=$
*lincomb-list f Vs* $+$ *lincomb-list* ($\lambda$ *i*. *f* (*i* $+$ *length Vs*)) *Ws*
⟨*proof*⟩

**lemma** *lincomb-list-snoc*[*simp*]:
**shows** *set Vs* $\subseteq$ *carrier-vec n* $\Longrightarrow$ $x \in$ *carrier-vec n* $\Longrightarrow$
*lincomb-list f* (*Vs* @ [*x*]) $=$ *lincomb-list f Vs* $+$ *f* (*length Vs*) $\cdot_v$ *x*
⟨*proof*⟩

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

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

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

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

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

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

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

**lemma** *exists-lin-indpt-sublist*: **assumes** *X*: $X \subseteq$ *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* $\Longrightarrow$ $B \subseteq$ *carrier-vec n* $\Longrightarrow$ *A* + *B* $\subseteq$ *carrier-vec n*
⟨*proof*⟩

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

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

**definition** *Ints-vec* (‹$\mathbb{Z}_v$›) **where**
$\mathbb{Z}_v = \{x.\ \forall\ i <$ *dim-vec* $x.\ x\ \$\ i \in \mathbb{Z}\}$

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

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

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

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

**definition** *Ints-mat* (‹$\mathbb{Z}_m$›) **where**
$\mathbb{Z}_m = \{A.\ \forall\ i <$ *dim-row* $A.\ \forall\ j <$ *dim-col* $A.\ A\ \$\$\ (i,j) \in \mathbb{Z}\}$

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

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

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

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

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

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

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

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

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

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

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

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

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

**lemma** *Bounded-vec-rows-Bounded-mat*[*simp*]: $set\ (rows\ A) \subseteq Bounded\text{-}vec\ B \longleftrightarrow A \in Bounded\text{-}mat\ B$
⟨*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** $i < nr \Longrightarrow j < nc \Longrightarrow$ *abs* ($A$ \$\$ ($i$,$j$)) $\leq b$
⟨*proof*⟩

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

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

**lemma** *finite-Bounded-vec-Max*:
**assumes** *A*: $A \subseteq$ *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* :: (*nat* $\Rightarrow$ *'a* :: *linordered-idom* $\Rightarrow$ *'a*) $\Rightarrow$ *bool* **where**
*is-det-bound f* = ($\forall$ *A n x*. $A \in$ *carrier-mat n n* $\longrightarrow A \in$ *Bounded-mat x* $\longrightarrow$ *abs* (*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* :: *nat* $\Rightarrow$ *'a* :: *linordered-idom* $\Rightarrow$ *'a* **where**
*det-bound-fact n x* = *fact n* $*$ ($x$^$n$)

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

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

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

**and** *Bnd*: $A \in$ *Bounded-mat c*
**shows**
($abs$ ($det$ $A$))$\hat{}2 \leq$ *of-nat n* $\hat{}$ $n * c$ $\hat{}$ $(2 * n)$
⟨*proof*⟩

**lemma** *det-bound-hadamard-squared*: **fixes** *A*::′*a* :: *trivial-conjugatable-linordered-field mat*
**assumes** *A*: $A \in$ *carrier-mat n n*
**and** *Bnd*: $A \in$ *Bounded-mat c*
**shows** ($abs$ ($det$ $A$))$\hat{}2 \leq$ *of-nat n* $\hat{}$ $n * c$ $\hat{}$ $(2 * n)$
⟨*proof*⟩

**definition** *det-bound-hadamard* :: *nat* ⇒ *int* ⇒ *int* **where**
*det-bound-hadamard n c* = (*sqrt-int-floor* ((*int n* ∗ *c*ˆ*2*)ˆ*n*))

**lemma** *det-bound-hadamard-altdef*[*code*]:
*det-bound-hadamard n c* = (*if n* = *1* ∨ *even n then int n* ˆ(*n div 2*) ∗ (*abs c*)ˆ*n else sqrt-int-floor* ((*int n* ∗ *c*ˆ*2*)ˆ*n*))
⟨*proof*⟩

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

**lemma** *n-pow-n-le-fact-square*: *n* ˆ *n* ≤ (*fact n*)ˆ*2*
⟨*proof*⟩

**lemma** *sqrt-int-floor-bound*: *0* ≤ *x* ⟹ (*sqrt-int-floor x*)ˆ*2* ≤ *x*
⟨*proof*⟩

**lemma** *det-bound-hadamard-improves-det-bound-fact*: **assumes** *c*: *c* ≥ *0*
**shows** *det-bound-hadamard n c* ≤ *det-bound-fact n c*
⟨*proof*⟩

**context**
**begin**
**private fun** *syl* :: *int* ⇒ *nat* ⇒ *int mat* **where**
*syl c 0* = *mat 1 1* (λ -. *c*)
| *syl c* (*Suc n*) = (*let A* = *syl c n in*
*four-block-mat A A* (−*A*) *A*)

**private lemma** *syl*: **assumes** *c*: *c* ≥ *0*
**shows** *syl c n* ∈ *Bounded-mat c* ∧ *syl c n* ∈ *carrier-mat* (*2*ˆ*n*) (*2*ˆ*n*)
∧ *det* (*syl c n*) = *det-bound-hadamard* (*2*ˆ*n*) *c*
⟨*proof*⟩

**lemma** *det-bound-hadamard-tight*:
**assumes** *c*: *c* ≥ *0*
**and** *n* = *2*ˆ*m*

**shows** ∃ *A*. *A* ∈ *carrier-mat n n* ∧ *A* ∈ *Bounded-mat c* ∧ *det A* = *det-bound-hadamard n c*
⟨*proof*⟩
**end**

**lemma** *Ints-matE*: **assumes** $A \in \mathbb{Z}_m$
**shows** ∃ *B*. *A* = *map-mat of-int B*
⟨*proof*⟩

**lemma** *is-det-bound-of-int*: **fixes** *A* :: *′a* :: *linordered-idom mat*
**assumes** *db*: *is-det-bound db*
**and** *A*: *A* ∈ *carrier-mat n n*
**and** $A \in \mathbb{Z}_m \cap$ *Bounded-mat* (*of-int bnd*)
**shows** *abs* (*det A*) ≤ *of-int* (*db n bnd*)
⟨*proof*⟩

**lemma** *minus-in-Bounded-vec*[*simp*]:
(−*x*) ∈ *Bounded-vec b* ⟷ *x* ∈ *Bounded-vec b*
⟨*proof*⟩

**lemma** *sum-in-Bounded-vecI*[*intro*]: **assumes**
*xB*: *x* ∈ *Bounded-vec B1* **and**
*yB*: *y* ∈ *Bounded-vec B2* **and**
*x*: *x* ∈ *carrier-vec n* **and**
*y*: *y* ∈ *carrier-vec n*
**shows** *x* + *y* ∈ *Bounded-vec* (*B1* + *B2*)
⟨*proof*⟩

**lemma** (**in** *gram-schmidt*) *lincomb-card-bound*: **assumes** *XBnd*: *X* ⊆ *Bounded-vec Bnd*
**and** *X*: *X* ⊆ *carrier-vec n*
**and** *Bnd*: *Bnd* ≥ *0*
**and** *c*: ⋀ *x*. *x* ∈ *X* ⟹ *abs* (*c x*) ≤ *1*
**and** *card*: *card X* ≤ *k*
**shows** *lincomb c X* ∈ *Bounded-vec* (*of-nat k* ∗ *Bnd*)
⟨*proof*⟩

**lemma** *bounded-vecset-sum*:
**assumes** *Acarr*: *A* ⊆ *carrier-vec n*
**and** *Bcarr*: *B* ⊆ *carrier-vec n*
**and** *sum*: *C* = *A* + *B*
**and** *Cbnd*: ∃ *bndC*. *C* ⊆ *Bounded-vec bndC*
**shows** *A* ≠ {} ⟹ (∃ *bndB*. *B* ⊆ *Bounded-vec bndB*)
**and** *B* ≠ {} ⟹ (∃ *bndA*. *A* ⊆ *Bounded-vec bndA*)
⟨*proof*⟩

**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* = (*lincomb c Vs* = *b* ∧ *c* ‘ *Vs* ⊆ {*x*. *x* ≥ *0*})
**definition** *nonneg-lincomb-list c Vs b* = (*lincomb-list c Vs* = *b* ∧ (∀ *i* < *length Vs*. *c i* ≥ *0*))

**definition** *finite-cone* :: ′*a vec set* ⇒ ′*a vec set* **where**
  *finite-cone Vs* = ({ *b*. ∃ *c*. *nonneg-lincomb c* (*if finite Vs then Vs else* {}) *b*})

**definition** *cone* :: ′*a vec set* ⇒ ′*a vec set* **where**
  *cone Vs* = ({ *x*. ∃ *Ws*. *finite Ws* ∧ *Ws* ⊆ *Vs* ∧ *x* ∈ *finite-cone Ws*})

**definition** *cone-list* :: ′*a vec list* ⇒ ′*a vec set* **where**
  *cone-list Vs* = {*b*. ∃ *c*. *nonneg-lincomb-list c Vs b*}

**lemma** *finite-cone-iff-cone-list*: **assumes** *Vs*: *Vs* ⊆ *carrier-vec n*
  **and** *id*: *Vs* = *set Vsl*
**shows** *finite-cone Vs* = *cone-list Vsl*
⟨*proof*⟩

**lemma** *cone-alt-def*: **assumes** *Vs*: *Vs* ⊆ *carrier-vec n*
  **shows** *cone Vs* = ({ *x*. ∃ *Ws*. *set Ws* ⊆ *Vs* ∧ *x* ∈ *cone-list Ws*})
  ⟨*proof*⟩

**lemma** *cone-mono*: *Vs* ⊆ *Ws* ⟹ *cone Vs* ⊆ *cone Ws*
  ⟨*proof*⟩

**lemma** *finite-cone-mono*: **assumes** *fin*: *finite Ws*
  **and** *Ws*: *Ws* ⊆ *carrier-vec n*
  **and** *sub*: *Vs* ⊆ *Ws*
**shows** *finite-cone Vs* ⊆ *finite-cone Ws*
⟨*proof*⟩

**lemma** *finite-cone-carrier*: *A* ⊆ *carrier-vec n* ⟹ *finite-cone A* ⊆ *carrier-vec n*
  ⟨*proof*⟩

**lemma** *cone-carrier*: *A* ⊆ *carrier-vec n* ⟹ *cone A* ⊆ *carrier-vec n*

$\langle proof \rangle$

**lemma** *cone-iff-finite-cone*: **assumes** $A$: $A \subseteq$ *carrier-vec* $n$
**and** *fin*: *finite* $A$
**shows** *cone* $A$ = *finite-cone* $A$
$\langle proof \rangle$

**lemma** *set-in-finite-cone*:
**assumes** $Vs$: $Vs \subseteq$ *carrier-vec* $n$
**and** *fin*: *finite* $Vs$
**shows** $Vs \subseteq$ *finite-cone* $Vs$
$\langle proof \rangle$

**lemma** *set-in-cone*:
**assumes** $Vs$: $Vs \subseteq$ *carrier-vec* $n$
**shows** $Vs \subseteq$ *cone* $Vs$
$\langle proof \rangle$

**lemma** *zero-in-finite-cone*:
**assumes** $Vs$: $Vs \subseteq$ *carrier-vec* $n$
**shows** $0_v$ $n \in$ *finite-cone* $Vs$
$\langle proof \rangle$

**lemma** *lincomb-in-finite-cone*:
**assumes** $x$ = *lincomb* $l$ $W$
**and** *finite* $W$
**and** $\forall i \in W .\ l\ i \geq 0$
**and** $W \subseteq$ *carrier-vec* $n$
**shows** $x \in$ *finite-cone* $W$
$\langle proof \rangle$

**lemma** *lincomb-in-cone*:
**assumes** $x$ = *lincomb* $l$ $W$
**and** *finite* $W$
**and** $\forall i \in W .\ l\ i \geq 0$
**and** $W \subseteq$ *carrier-vec* $n$
**shows** $x \in$ *cone* $W$
$\langle proof \rangle$

**lemma** *zero-in-cone*: $0_v$ $n \in$ *cone* $Vs$
$\langle proof \rangle$

**lemma** *cone-smult*:
**assumes** $a$: $a \geq 0$
**and** $Vs$: $Vs \subseteq$ *carrier-vec* $n$
**and** $x$: $x \in$ *cone* $Vs$
**shows** $a \cdot_v x \in$ *cone* $Vs$
$\langle proof \rangle$

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

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

**lemma** *cone-elem-sum*:
**assumes** *Vs*: *Vs* ⊆ *carrier-vec n*
**and** *x*: *x* ∈ *cone Vs*
**and** *y*: *y* ∈ *cone Vs*
**shows** *x* + *y* ∈ *cone Vs*
⟨*proof*⟩

**lemma** *cone-cone*:
**assumes** *Vs*: *Vs* ⊆ *carrier-vec n*
**shows** *cone* (*cone Vs*) = *cone Vs*
⟨*proof*⟩

**lemma** *cone-smult-basis*:
**assumes** *Vs*: *Vs* ⊆ *carrier-vec n*
**and** *l*: *l* ' *Vs* ⊆ {*x*. *x* > *0*}
**shows** *cone* {*l v* $\cdot_v$ *v* | *v* . *v* ∈ *Vs*} = *cone Vs*
⟨*proof*⟩

**lemma** *cone-add-cone*:
**assumes** *C*: *C* ⊆ *carrier-vec n*
**shows** *cone C* + *cone C* = *cone C*
⟨*proof*⟩

**lemma** *orthogonal-cone*:
**assumes** *X*: *X* ⊆ *carrier-vec n*
**and** *W*: *W* ⊆ *carrier-vec n*
**and** *finX*: *finite X*
**and** *spanLW*: *span* (*set Ls* ∪ *W*) = *carrier-vec n*
**and** *ortho*: ⋀ *w x*. *w* ∈ *W* ⟹ *x* ∈ *set Ls* ⟹ *w* • *x* = *0*
**and** *WWs*: *W* = *set Ws*
**and** *spanL*: *span* (*set Ls*) = *span X*
**and** *LX*: *set Ls* ⊆ *X*
**and** *lin-Ls-Bs*: *lin-indpt-list* (*Ls* @ *Bs*)
**and** *len-Ls-Bs*: *length* (*Ls* @ *Bs*) = *n*
**shows** *cone* (*X* ∪ *set Bs*) ∩ {*x* ∈ *carrier-vec n*. ∀ *w*∈*W*. *w* • *x* = *0*} = *cone X*
⋀ *x*. ∀ *w*∈*W*. *w* • *x* = *0* ⟹ *Z* ⊆ *X* ⟹ *B* ⊆ *set Bs* ⟹ *x* = *lincomb c* (*Z* ∪ *B*)
⟹ *x* = *lincomb c* (*Z* − *B*)
⟨*proof*⟩

**definition** *polyhedral-cone* (*A* :: *'a mat*) = { *x* . *x* ∈ *carrier-vec n* ∧ *A* $*_v$ *x* ≤ $0_v$ (*dim-row A*)}

**lemma** *polyhedral-cone-carrier*: **assumes** $A \in$ *carrier-mat nr n*
**shows** *polyhedral-cone* $A \subseteq$ *carrier-vec n*
⟨*proof*⟩

**lemma** *cone-in-polyhedral-cone*:
**assumes** *CA*: $C \subseteq$ *polyhedral-cone A*
**and** *A*: $A \in$ *carrier-mat nr n*
**shows** *cone* $C \subseteq$ *polyhedral-cone A*
⟨*proof*⟩

**lemma** *bounded-cone-is-zero*:
**assumes** *Ccarr*: $C \subseteq$ *carrier-vec n* **and** *bnd*: *cone* $C \subseteq$ *Bounded-vec bnd*
**shows** *cone* $C = \{0_v\ n\}$
⟨*proof*⟩

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

**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* = (*nonneg-lincomb c Vs b* $\wedge$ *sum c Vs* = *1*)

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

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

**lemma** *convex-hull-carrier*[*intro*]: *Vs* $\subseteq$ *carrier-vec n* $\Longrightarrow$ *convex-hull Vs* $\subseteq$ *carrier-vec n*
⟨*proof*⟩

**lemma** *convex-hull-mono*: *Vs* $\subseteq$ *Ws* $\Longrightarrow$ *convex-hull Vs* $\subseteq$ *convex-hull Ws*

⟨*proof*⟩

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

**lemma** *set-in-convex-hull*:
**assumes** $A \subseteq$ *carrier-vec n*
**shows** $A \subseteq$ *convex-hull A*
⟨*proof*⟩

**lemma** *convex-hull-empty*[*simp*]:
*convex-hull* {} = {}
$A \subseteq$ *carrier-vec n* $\Longrightarrow$ *convex-hull A* = {} $\longleftrightarrow$ *A* = {}
⟨*proof*⟩

**lemma** *convex-hull-bound*: **assumes** *XBnd*: $X \subseteq$ *Bounded-vec Bnd*
**and** *X*: $X \subseteq$ *carrier-vec n*
**shows** *convex-hull X* $\subseteq$ *Bounded-vec Bnd*
⟨*proof*⟩

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

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

**lemma** *set-in-convex-hull-list*: **fixes** *Vs* :: *'a vec list*
**assumes** *set Vs* $\subseteq$ *carrier-vec n*
**shows** *set Vs* $\subseteq$ *convex-hull-list Vs*
⟨*proof*⟩

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

**lemma** *convex-hull-list-mono*:
**assumes** *set Ws* $\subseteq$ *carrier-vec n*
**shows** *set Vs* $\subseteq$ *set Ws* $\Longrightarrow$ *convex-hull-list Vs* $\subseteq$ *convex-hull-list Ws*
⟨*proof*⟩

**lemma** *convex-hull-list-eq-set*:
*set Vs* $\subseteq$ *carrier-vec n* $\Longrightarrow$ *set Vs* = *set Ws* $\Longrightarrow$ *convex-hull-list Vs* = *convex-hull-list Ws*

⟨*proof*⟩

**lemma** *find-indices-empty*: (*find-indices* $x$ *Vs* = []) = ($x \notin$ *set Vs*)
⟨*proof*⟩

**lemma** *distinct-list-find-indices*:
**shows** ⟦ $i <$ *length Vs*; *Vs* ! $i = x$; *distinct Vs* ⟧ $\Longrightarrow$ *find-indices* $x$ *Vs* = [$i$]
⟨*proof*⟩

**lemma** *finite-convex-hull-iff-convex-hull-list*: **assumes** *Vs*: *Vs* $\subseteq$ *carrier-vec* $n$
**and** *id'*: *Vs* = *set Vsl'*
**shows** *convex-hull Vs* = *convex-hull-list Vsl'*
⟨*proof*⟩

**definition** *convex* $S$ = (*convex-hull* $S = S$)

**lemma** *convex-convex-hull*: *convex* $S \Longrightarrow$ *convex-hull* $S = S$
⟨*proof*⟩

**lemma** *convex-hull-convex-hull-listD*: **assumes** $A$: $A \subseteq$ *carrier-vec* $n$
**and** $x$: $x \in$ *convex-hull* $A$
**shows** $\exists$ *as*. *set as* $\subseteq A \wedge x \in$ *convex-hull-list as*
⟨*proof*⟩

**lemma** *convex-hull-convex-sum*: **assumes** $A$: $A \subseteq$ *carrier-vec* $n$
**and** $x$: $x \in$ *convex-hull* $A$
**and** $y$: $y \in$ *convex-hull* $A$
**and** $a$: $0 \leq a$ $a \leq 1$
**shows** $a \cdot_v x + (1 - a) \cdot_v y \in$ *convex-hull* $A$
⟨*proof*⟩

**lemma** *convexI*: **assumes** $S$: $S \subseteq$ *carrier-vec* $n$
**and** *step*: $\bigwedge a\ x\ y.\ x \in S \Longrightarrow y \in S \Longrightarrow 0 \leq a \Longrightarrow a \leq 1 \Longrightarrow a \cdot_v x + (1 - a) \cdot_v y \in S$
**shows** *convex* $S$
⟨*proof*⟩

**lemma** *convex-hulls-are-convex*: **assumes** $A \subseteq$ *carrier-vec* $n$
**shows** *convex* (*convex-hull* $A$)
⟨*proof*⟩

**lemma** *convex-hull-sum*: **assumes** $A$: $A \subseteq$ *carrier-vec* $n$ **and** $B$: $B \subseteq$ *carrier-vec* $n$
**shows** *convex-hull* $(A + B)$ = *convex-hull* $A$ + *convex-hull* $B$
⟨*proof*⟩

**lemma** *convex-hull-in-cone*:
*convex-hull* $C \subseteq$ *cone* $C$
⟨*proof*⟩

**lemma** *convex-cone*:
  **assumes** $C$: $C \subseteq$ *carrier-vec n*
  **shows** *convex* (*cone* $C$)
  ⟨*proof*⟩

**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** $W$: $W \subseteq$ *carrier-vec n*
    **and** $X$: $X \subseteq$ *carrier-vec n*
    **and** *ortho*: $\bigwedge w\ x.\ w \in W \Longrightarrow x \in X \Longrightarrow x \cdot w = 0$
    **and** *inspan*: *lincomb l1 X* + *lincomb l2 W* $\in$ *span X*
  **shows** *lincomb l2 W* = $0_v$ *n*
⟨*proof*⟩

**lemma** *ortho-lin-indpt*: **assumes** $W$: $W \subseteq$ *carrier-vec n*
  **and** $X$: $X \subseteq$ *carrier-vec n*
  **and** *ortho*: $\bigwedge w\ x.\ w \in W \Longrightarrow x \in X \Longrightarrow x \cdot w = 0$
  **and** *linW*: *lin-indpt W*
  **and** *linX*: *lin-indpt X*
**shows** *lin-indpt* ($W \cup X$)
⟨*proof*⟩

**definition** *normal-vector* :: *'a vec set* ⇒ *'a vec* **where**
  *normal-vector W* = (*let ws* = (*SOME ws. set ws* = $W$ ∧ *distinct ws*);
    *m* = *length ws*;
    $B$ = (λ *j. mat m m* (λ(*i*, *j'*). *ws* ! *i* \$ (*if j' < j then j' else Suc j'*)))
    *in vec n* (λ *j.* (−*1*)^(*m*+*j*) ∗ *det* (*B j*)))

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

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

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

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

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

**definition** *pos-norm-vec* :: *'a vec set ⇒ 'a vec ⇒ '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*: $D \subseteq carrier\text{-}vec\ n$ **and** *fin*: *finite D* **and** *lin*: *lin-indpt D*
**and** *card*: $Suc\ (card\ D) = n$
**and** *c-def*: $c = pos\text{-}norm\text{-}vec\ D\ x$
**shows** $c \in carrier\text{-}vec\ n$ $span\ D = \{\ x.\ x \in carrier\text{-}vec\ n \wedge x \cdot c = 0\}$
$x \notin span\ D \Longrightarrow x \in carrier\text{-}vec\ n \Longrightarrow c \cdot x > 0$
$c \in \{normal\text{-}vector\ D,\ -normal\text{-}vector\ D\}$
⟨*proof*⟩

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

**lemma fixes** $V\ W :: 'a\ vec\ set$
  **shows**
    *card-le-dim-span*:
    $V \subseteq carrier\text{-}vec\ n \Longrightarrow V \subseteq span\ W \Longrightarrow lin\text{-}indpt\ V \Longrightarrow card\ V \leq dim\text{-}span\ W$ **and**
    *card-eq-dim-span-imp-same-span*:
    $W \subseteq carrier\text{-}vec\ n \Longrightarrow V \subseteq span\ W \Longrightarrow lin\text{-}indpt\ V \Longrightarrow card\ V = dim\text{-}span\ W \Longrightarrow span\ V = span\ W$ **and**
    *same-span-imp-card-eq-dim-span*:
    $V \subseteq carrier\text{-}vec\ n \Longrightarrow W \subseteq carrier\text{-}vec\ n \Longrightarrow span\ V = span\ W \Longrightarrow lin\text{-}indpt\ V \Longrightarrow card\ V = dim\text{-}span\ W$ **and**
    *dim-span-cong*:
    $span\ V = span\ W \Longrightarrow dim\text{-}span\ V = dim\text{-}span\ W$ **and**
    *ex-basis-span*:
    $V \subseteq carrier\text{-}vec\ n \Longrightarrow \exists\ W.\ W \subseteq carrier\text{-}vec\ n \wedge lin\text{-}indpt\ W \wedge span\ V = span\ W \wedge dim\text{-}span\ V = card\ W$
⟨*proof*⟩

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

**lemma** *dim-span-insert*: **assumes** $W$: $W \subseteq carrier\text{-}vec\ n$
  **and** $v$: $v \in carrier\text{-}vec\ n$ **and** $vs$: $v \notin span\ W$
**shows** $dim\text{-}span\ (insert\ v\ W) = Suc\ (dim\text{-}span\ W)$
⟨*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 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*: $A \subseteq carrier\text{-}vec\ n$
    **and** *fin*: *finite A*
    **and** *b*: $b \in cone\ A$
  **shows** $\nexists\ c.\ c \in carrier\text{-}vec\ n \wedge (\forall\ a_i \in A.\ c \cdot a_i \geq 0) \wedge c \cdot b < 0$
⟨*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** $a :: nat \Rightarrow 'a\ vec$
    **and** $b :: 'a\ vec$
    **and** $m :: nat$
  **assumes** *a*: $a\ `\ \{0\ ..<\ m\} \subseteq carrier\text{-}vec\ n$
    **and** *inj-a*: $inj\text{-}on\ a\ \{0\ ..<\ m\}$
    **and** *b*: $b \in carrier\text{-}vec\ n$
    **and** *full-span*: $span\ (a\ `\ \{0\ ..<\ m\}) = carrier\text{-}vec\ n$
**begin**

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

**private lemma** *card-a-I*[*simp*]: $I \subseteq \{0\ ..<\ m\} \Longrightarrow card\ (a\ `\ I) = card\ I$
⟨*proof*⟩ **lemma** *in-a-I*[*simp*]: $I \subseteq \{0\ ..<\ m\} \Longrightarrow i < m \Longrightarrow (a\ i \in a\ `\ I) = (i \in I)$
⟨*proof*⟩ **definition** *valid-I* = $\{\ I.\ card\ I = n \wedge lin\text{-}indpt\ (a\ `\ I) \wedge I \subseteq \{0\ ..<\ m\}\}$

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

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

**private lemma** *finite-step-rel*: *finite step-rel*
⟨*proof*⟩ **lemma** *acyclic-imp-goal*: *acyclic step-rel* $\Longrightarrow$ *goal*
⟨*proof*⟩ **lemma** *acyclic-step-rel*: *acyclic step-rel*
⟨*proof*⟩

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

**end**

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

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

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

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

**corollary** *Caratheodory-theorem*: **assumes** $A$: $A \subseteq$ *carrier-vec* $n$
**shows** *cone* $A = \bigcup\ \{$*finite-cone* $B \mid B.\ B \subseteq A \wedge$ *lin-indpt* $B\}$
$\langle$*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 $\delta$-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** $(\exists\ x.\ x \geq 0_v\ nr \wedge A *_v x = b) \longleftrightarrow (\forall\ y.\ y \in \textit{carrier-vec}\ n \longrightarrow A^T *_v y \geq 0_v\ nr \longrightarrow y \cdot b \geq 0)$
⟨*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** $(\exists x.\ x\in \textit{carrier-vec}\ nc \wedge A *_v x \leq b)$
    $\longleftrightarrow (\forall y.\ y \geq 0_v\ nr \wedge A^T *_v y = 0_v\ nc \longrightarrow y \cdot b \geq 0)$
⟨*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 quantative 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*: $X \subseteq$ *carrier-vec n*
**and** *fin*: *finite X*
**and** *span*: *span X* = *carrier-vec n*
**shows** $\exists$ *nr A*. $A \in$ *carrier-mat nr n* $\wedge$ *cone X* = *polyhedral-cone A*
$\wedge$ (*is-det-bound db* $\longrightarrow$ $X \subseteq \mathbb{Z}_v \cap$ *Bounded-vec* (*of-int Bnd*) $\longrightarrow$ $A \in \mathbb{Z}_m \cap$ *Bounded-mat* (*of-int* (*db* (*n*−*1*) *Bnd*)))
⟨*proof*⟩

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

Now for the other direction.

**lemma** *farkas-minkowsky-weyl-theorem-2*:
**assumes** *A*: $A \in$ *carrier-mat nr n*
**shows** $\exists$ *X*. $X \subseteq$ *carrier-vec n* $\wedge$ *finite X* $\wedge$ *polyhedral-cone A* = *cone X*
$\wedge$ (*is-det-bound db* $\longrightarrow$ $A \in \mathbb{Z}_m \cap$ *Bounded-mat* (*of-int Bnd*) $\longrightarrow$ $X \subseteq \mathbb{Z}_v \cap$ *Bounded-vec* (*of-int* (*db* (*n*−*1*) (*max 1 Bnd*))))
⟨*proof*⟩

**lemma** *farkas-minkowsky-weyl-theorem*:
($\exists$ *X*. $X \subseteq$ *carrier-vec n* $\wedge$ *finite X* $\wedge$ *P* = *cone X*)
$\longleftrightarrow$ ($\exists$ *A nr*. $A \in$ *carrier-mat nr n* $\wedge$ *P* = *polyhedral-cone A*)
⟨*proof*⟩
**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* $P = (\exists\ V.\ V \subseteq \textit{carrier-vec}\ n \wedge \textit{finite}\ V \wedge P = \textit{convex-hull}\ V)$

**definition** *polyhedron* $A\ b = \{x \in \textit{carrier-vec}\ n.\ A *_v x \leq b\}$

**lemma** *polyhedra-are-convex*:
  **assumes** $A$: $A \in \textit{carrier-mat}\ nr\ n$
    **and** $b$: $b \in \textit{carrier-vec}\ nr$
    **and** $P$: $P = \textit{polyhedron}\ A\ b$
  **shows** *convex P*
⟨*proof*⟩

**end**

**locale** *gram-schmidt-m* = *n*: *gram-schmidt n f-ty* + *m*: *gram-schmidt m f-ty*
  **for** *n m* :: *nat* **and** *f-ty*
**begin**

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

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

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

**and** *y-dim*: $y \in$ *carrier-vec n*
**and** *y*: $y \ \$ \ m = 0$
**shows** (*vec-first y m* $\in$ *m.cone* {*vec-first y m* | *y*. $y \in X$}) = ($y \in$ *n.cone X*)
⟨*proof*⟩

**end**

**context** *gram-schmidt*
**begin**

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

**lemma** *decomposition-theorem-polyhedra-2*:
**assumes** *Q*: $Q \subseteq$ *carrier-vec n* **and** *fin-Q*: *finite Q*
**and** *X*: $X \subseteq$ *carrier-vec n* **and** *fin-X*: *finite X*
**and** *P*: $P =$ *convex-hull Q* + *cone X*
**shows** $\exists$ *A b nr*. $A \in$ *carrier-mat nr n* $\wedge$ $b \in$ *carrier-vec nr* $\wedge$ $P =$ *polyhedron A b*
⟨*proof*⟩

**lemma** *decomposition-theorem-polyhedra*:
($\exists$ *A b nr*. $A \in$ *carrier-mat nr n* $\wedge$ $b \in$ *carrier-vec nr* $\wedge$ $P =$ *polyhedron A b*) $\longleftrightarrow$
($\exists$ *Q X*. $Q \cup X \subseteq$ *carrier-vec n* $\wedge$ *finite* ($Q \cup X$) $\wedge$ $P =$ *convex-hull Q* + *cone X*) (**is** *?l* = *?r*)
⟨*proof*⟩

**lemma** *polytope-equiv-bounded-polyhedron*:
*polytope P* $\longleftrightarrow$
($\exists$ *A b nr bnd*. $A \in$ *carrier-mat nr n* $\wedge$ $b \in$ *carrier-vec nr* $\wedge$ $P =$ *polyhedron A b* $\wedge$ $P \subseteq$ *Bounded-vec bnd*)
⟨*proof*⟩
**end**

**end**

## 15 Mixed Integer Solutions

We prove that if an integral system of linear inequalities $Ax \le b \wedge A'x < b'$ 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** ‹$<_v$› *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** $w \in carrier\text{-}vec\ n$
  **shows** $i < n \Longrightarrow v\ \$\ i < w\ \$\ i$
  ⟨*proof*⟩

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

**lemma** *less-vec-lesseq-vec*: $v <_v (w :: 'a :: preorder\ vec) \Longrightarrow v \le w$
  ⟨*proof*⟩

**lemma** *floor-less*: $x \notin \mathbb{Z} \Longrightarrow of\text{-}int\ \lfloor x \rfloor < x$
  ⟨*proof*⟩

**lemma** *floor-of-int-eq*[*simp*]: $x \in \mathbb{Z} \Longrightarrow of\text{-}int\ \lfloor x \rfloor = x$
  ⟨*proof*⟩

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

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

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

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 mat*
**assumes** *db*: *is-det-bound db*
**and** *A1*: $A_1 \in$ *carrier-mat* $nr_1$ *n*
**and** *A2*: $A_2 \in$ *carrier-mat* $nr_2$ *n*
**and** *b1*: $b_1 \in$ *carrier-vec* $nr_1$
**and** *b2*: $b_2 \in$ *carrier-vec* $nr_2$
**and** *A1Bnd*: $A_1 \in \mathbb{Z}_m \cap$ *Bounded-mat* (*of-int Bnd*)
**and** *b1Bnd*: $b_1 \in \mathbb{Z}_v \cap$ *Bounded-vec* (*of-int Bnd*)
**and** *A2Bnd*: $A_2 \in \mathbb{Z}_m \cap$ *Bounded-mat* (*of-int Bnd*)
**and** *b2Bnd*: $b_2 \in \mathbb{Z}_v \cap$ *Bounded-vec* (*of-int Bnd*)
**and** *x*: $x \in$ *carrier-vec n*
**and** *xI*: $x \in$ *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*.
$x \in$ *carrier-vec n* $\wedge$
$x \in$ *indexed-Ints-vec I* $\wedge$
$A_1 *_v x \leq b_1 \wedge$
$A_2 *_v x <_v b_2 \wedge$
$x \in$ *Bounded-vec* (*of-int* (*int* ($n$+*1*) $*$ *db n Bnd*))
⟨*proof*⟩

**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** $v \in$ *Bounded-vec bnd*
**shows** (*map-vec of-int v* :: *'a vec*) $\in \mathbb{Z}_v \cap$ *Bounded-vec* (*of-int bnd*)
⟨*proof*⟩

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

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

**lemma** *small-mixed-integer-solution-int-mat*: **fixes** *x* :: *'a vec*
**assumes** *db*: *is-det-bound db*
**and** *A1*: $A_1 \in$ *carrier-mat* $nr_1$ *n*
**and** *A2*: $A_2 \in$ *carrier-mat* $nr_2$ *n*
**and** *b1*: $b_1 \in$ *carrier-vec* $nr_1$
**and** *b2*: $b_2 \in$ *carrier-vec* $nr_2$
**and** *A1Bnd*: $A_1 \in$ *Bounded-mat Bnd*
**and** *b1Bnd*: $b_1 \in$ *Bounded-vec Bnd*
**and** *A2Bnd*: $A_2 \in$ *Bounded-mat Bnd*
**and** *b2Bnd*: $b_2 \in$ *Bounded-vec Bnd*
**and** *x*: $x \in$ *carrier-vec n*
**and** *xI*: $x \in$ *indexed-Ints-vec I*
**and** *sol-nonstrict*: *map-mat of-int* $A_1 *_v x \leq$ *map-vec of-int* $b_1$
**and** *sol-strict*: *map-mat of-int* $A_2 *_v x <_v$ *map-vec of-int* $b_2$
**and** *non-degenerate*: $nr_1 \neq 0 \vee nr_2 \neq 0 \vee Bnd \geq 0$
**shows** $\exists$ *x* :: *'a vec*.
$x \in$ *carrier-vec n* $\wedge$
$x \in$ *indexed-Ints-vec I* $\wedge$
*map-mat of-int* $A_1 *_v x \leq$ *map-vec of-int* $b_1 \wedge$
*map-mat of-int* $A_2 *_v x <_v$ *map-vec of-int* $b_2 \wedge$
$x \in$ *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*: (*of-int-hom.vec-hom v* :: *'a* :: *linordered-field vec*) $\leq$ *of-int-hom.vec-hom w* $\longleftrightarrow v \leq w$
⟨*proof*⟩

**lemma** *of-int-hom-less*: (*of-int-hom.vec-hom v* :: *'a* :: *linordered-field vec*) $<_v$ *of-int-hom.vec-hom w* $\longleftrightarrow v <_v w$
⟨*proof*⟩

**lemma** *Ints-vec-to-int-vec*: **assumes** $v \in \mathbb{Z}_v$
**shows** $\exists$ *w*. *v* = *map-vec of-int w*
⟨*proof*⟩

**lemma** *small-integer-solution*: **fixes** $A_1$ :: *int mat*
**assumes** *db*: *is-det-bound db*
**and** *A1*: $A_1 \in$ *carrier-mat* $nr_1$ *n*
**and** *A2*: $A_2 \in$ *carrier-mat* $nr_2$ *n*
**and** *b1*: $b_1 \in$ *carrier-vec* $nr_1$

**and** *b2*: $b_2 \in$ *carrier-vec* $nr_2$
**and** *A1Bnd*: $A_1 \in$ *Bounded-mat Bnd*
**and** *b1Bnd*: $b_1 \in$ *Bounded-vec Bnd*
**and** *A2Bnd*: $A_2 \in$ *Bounded-mat Bnd*
**and** *b2Bnd*: $b_2 \in$ *Bounded-vec Bnd*
**and** *x*: $x \in$ *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*.
$x \in$ *carrier-vec n* $\wedge$
$A_1 *_v x \leq b_1 \wedge$
$A_2 *_v x <_v b_2 \wedge$
$x \in$ *Bounded-vec* (*of-nat* (*n+1*) $*$ *db n Bnd*)
⟨*proof*⟩

**corollary** *small-integer-solution-nonstrict*: **fixes** *A* :: *int mat*
**assumes** *db*: *is-det-bound db*
**and** *A*: $A \in$ *carrier-mat nr n*
**and** *b*: $b \in$ *carrier-vec nr*
**and** *ABnd*: $A \in$ *Bounded-mat Bnd*
**and** *bBnd*: $b \in$ *Bounded-vec Bnd*
**and** *x*: $x \in$ *carrier-vec n*
**and** *sol*: $A *_v x \leq b$
**and** *non-degenerate*: $nr \neq 0 \vee Bnd \geq 0$
**shows** $\exists$ *y*.
$y \in$ *carrier-vec n* $\wedge$
$A *_v y \leq b \wedge$
$y \in$ *Bounded-vec* (*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* $P$ = *convex-hull* ($P \cap \mathbb{Z}_v$)

**lemma** *integer-hull-mono*: $P \subseteq Q \Longrightarrow$ *integer-hull* $P \subseteq$ *integer-hull* $Q$
⟨*proof*⟩

**end**

**lemma** *abs-neg-floor*: |*of-int* $b$| ≤ *Bnd* ⟹ − (*floor Bnd*) ≤ $b$
⟨*proof*⟩

**lemma** *abs-pos-floor*: |*of-int* $b$| ≤ *Bnd* ⟹ $b$ ≤ *floor Bnd*
⟨*proof*⟩

**context** *gram-schmidt-floor*
**begin**

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

**theorem** *decomposition-theorem-integer-hull-of-polyhedron*:
**assumes** *db*: *is-det-bound db*
**and** $A$: $A \in$ *carrier-mat nr n*
**and** $b$: $b \in$ *carrier-vec nr*
**and** *AI*: $A \in \mathbb{Z}_m$
**and** *bI*: $b \in \mathbb{Z}_v$
**and** $P$: $P$ = *polyhedron* $A$ $b$
**and** *Bnd*: *of-int Bnd* ≥ *Max* (*abs* ‘ (*elements-mat* $A$ ∪ *vec-set* $b$))
**shows** ∃ $H$ $C$. $H \cup C \subseteq$ *carrier-vec* $n \cap \mathbb{Z}_v$
∧ $H \subseteq$ *Bounded-vec* (*of-nat* ($n$ + *1*) ∗ *of-int* (*db* $n$ (*max 1 Bnd*)))
∧ $C \subseteq$ *Bounded-vec* (*of-int* (*db* $n$ (*max 1 Bnd*)))
∧ *finite* ($H \cup C$)
∧ *integer-hull* $P$ = *convex-hull* $H$ + *cone* $C$
⟨*proof*⟩

**corollary** *integer-hull-of-polyhedron*: **assumes** $A$: $A \in$ *carrier-mat nr n*
**and** $b$: $b \in$ *carrier-vec nr*
**and** *AI*: $A \in \mathbb{Z}_m$
**and** *bI*: $b \in \mathbb{Z}_v$
**and** $P$: $P$ = *polyhedron* $A$ $b$
**shows** ∃ $A'$ $b'$ $nr'$. $A' \in$ *carrier-mat* $nr'$ $n$ ∧ $b' \in$ *carrier-vec* $nr'$ ∧
*integer-hull* $P$ = *polyhedron* $A'$ $b'$
⟨*proof*⟩

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

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