Linear Inequalities*

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

[1]University of Innsbruck
[2]ENS Lyon

December 14, 2021

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

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

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* 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* $|y_i| \leq (n+1)! \cdot \beta^n$ *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 ∪ *elements-mat B* ∪ *elements-mat C* ∪ *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* ∪ *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*]:
$A \in$ *carrier-mat nr nc1* ⟹
$B \in$ *carrier-mat nr nc2* ⟹ $(A\ @_c\ B) \in$ *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*: $A \in$ *carrier-mat n nc* ⟹ $B \in$ *carrier-mat n nc1*
⟹ *elements-mat* $(A\ @_c\ B)$ = *elements-mat* $A \cup$ *elements-mat* B
⟨*proof*⟩

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

lemma *vec-last-index*:
assumes v: $v \in$ *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* $x \geq n$
and *dim-vec* $y \geq n$
shows*vec-first* $(x + y)\ n$ = *vec-first* $x\ n$ + *vec-first* $y\ n$
⟨*proof*⟩

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

lemma *vec-first-smult*:
⟦ $m \leq n$; $x \in$ *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-ab-group-add vec*

shows $(a \leq b) = (a - b \leq 0_v\ (\textit{dim-vec}\ a))$
⟨*proof*⟩

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

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

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

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

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

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

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

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

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

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

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

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

lemma *mat-col-first-carrier*[*simp*]: $\textit{mat-col-first}\ A\ n \in \textit{carrier-mat}\ (\textit{dim-row}\ A)\ n$
⟨*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*]: $i < \textit{dim-vec}\ v \Longrightarrow \textit{row}\ (\textit{mat-of-col}\ v)\ i = \textit{vec-of-scal}\ (v\ \$\ i)$
⟨*proof*⟩

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

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

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

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

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

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

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

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

lemma *smult-nneg-npos-vec*: **fixes** $l :: 'a :: \textit{ordered-semiring-0}$
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** $c :: 'a :: \textit{field}$

shows $c \neq 0 \Longrightarrow (c \cdot_v x = c \cdot_v y) = (x = y)$
⟨*proof*⟩

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

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

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 $a - b \in span\ A$
⟨*proof*⟩

lemma *finsum-scalar-prod-sum'*:
assumes *f*: $f \in U \to carrier\text{-}vec\ n$
and *w*: $w \in carrier\text{-}vec\ n$
shows $w \cdot finsum\ V\ f\ U = sum\ (\lambda u.\ w \cdot f\ u)\ U$
⟨*proof*⟩

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

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

lemma *lin-indpt-empty*[*simp*]: *lin-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* (λ *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* (λ *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* (λ *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 a bound 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 $\|\textit{unit-vec } n\ i\|^2 = (1 :: 'a :: \{\textit{comm-ring-1}, \textit{conjugatable-ring}\})$
⟨*proof*⟩

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

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

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

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

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

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

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

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

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

⟨*proof*⟩

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

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

lemma *diff-indexed-Ints-vec*:
x ∈ *carrier-vec n* ⟹ *y* ∈ *carrier-vec n* ⟹ *x* ∈ *indexed-Ints-vec I* ⟹ *y* ∈ *indexed-Ints-vec I*
⟹ *x* − *y* ∈ *indexed-Ints-vec I*
⟨*proof*⟩

lemma *smult-indexed-Ints-vec*: *x* ∈ $\mathbb{Z}$ ⟹ *v* ∈ *indexed-Ints-vec I* ⟹ *x* ·$_v$ *v* ∈ *indexed-Ints-vec I*
⟨*proof*⟩

lemma *add-indexed-Ints-vec*:
x ∈ *carrier-vec n* ⟹ *y* ∈ *carrier-vec n* ⟹ *x* ∈ *indexed-Ints-vec I* ⟹ *y* ∈ *indexed-Ints-vec I*
⟹ *x* + *y* ∈ *indexed-Ints-vec I*
⟨*proof*⟩

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

definition *Bounded-vec* (*b* :: *'a* :: *linordered-idom*) = {*x* . ∀ *i* < *dim-vec x* . *abs* (*x* $ *i*) ≤ *b*}

lemma *Bounded-vec-vec-set*: *v* ∈ *Bounded-vec b* ⟷ (∀ *x* ∈ *vec-set v*. *abs x* ≤ *b*)
⟨*proof*⟩

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

lemma *Bounded-mat-elements-mat*: *A* ∈ *Bounded-mat b* ⟷ (∀ *x* ∈ *elements-mat A*. *abs x* ≤ *b*)
⟨*proof*⟩

lemma *Bounded-vec-rows-Bounded-mat*[*simp*]: *set* (*rows A*) ⊆ *Bounded-vec B* ⟷ *A* ∈ *Bounded-mat B*
⟨*proof*⟩

lemma *unit-vec-Bounded-vec*[*simp*,*intro*]: *unit-vec n i* ∈ *Bounded-vec* (*max 1 Bnd*)

⟨*proof*⟩

lemma *Bounded-matD*: **assumes** $A \in$ *Bounded-mat b*
A ∈ *carrier-mat nr nc*
shows $i < nr \Longrightarrow j < nc \Longrightarrow$ *abs* (*A* $$ (*i*,*j*)) ≤ *b*
⟨*proof*⟩

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

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

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

definition *det-bound* :: *nat* ⇒ *'a* :: *linordered-idom* ⇒ *'a* **where**
det-bound n x = *fact n* ∗ (*x*^*n*)

lemma *det-bound*: **assumes** *A*: *A* ∈ *carrier-mat n n*
and *x*: *A* ∈ *Bounded-mat x*
shows *abs* (*det A*) ≤ *det-bound n x*
⟨*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*: $A \subseteq$ *carrier-vec n*
and *Bcarr*: $B \subseteq$ *carrier-vec n*
and *sum*: $C = A + B$
and *Cbnd*: $\exists$ *bndC*. $C \subseteq$ *Bounded-vec bndC*
shows $A \neq \{\} \Longrightarrow (\exists$ *bndB*. $B \subseteq$ *Bounded-vec bndB*)
and $B \neq \{\} \Longrightarrow (\exists$ *bndA*. $A \subseteq$ *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*: $Ws \subseteq$ *carrier-vec n*
and *sub*: $Vs \subseteq Ws$
shows *finite-cone Vs* $\subseteq$ *finite-cone Ws*
⟨*proof*⟩

lemma *finite-cone-carrier*: $A \subseteq$ *carrier-vec n* $\Longrightarrow$ *finite-cone A* $\subseteq$ *carrier-vec n*
⟨*proof*⟩

lemma *cone-carrier*: $A \subseteq$ *carrier-vec n* $\Longrightarrow$ *cone A* $\subseteq$ *carrier-vec n*
⟨*proof*⟩

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

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

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

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

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*
⟨*proof*⟩

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*
⟨*proof*⟩

lemma *zero-in-cone*: $0_v\ n \in cone\ Vs$
⟨*proof*⟩

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

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

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

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

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

lemma *orthogonal-cone*:
assumes *X*: $X \subseteq carrier\text{-}vec\ n$
and *W*: $W \subseteq carrier\text{-}vec\ n$
and *finX*: *finite X*
and *spanLW*: $span\ (set\ Ls \cup W) = carrier\text{-}vec\ n$
and *ortho*: $\bigwedge w\ x.\ w \in W \Longrightarrow x \in set\ Ls \Longrightarrow w \cdot x = 0$
and *WWs*: $W = set\ Ws$
and *spanL*: $span\ (set\ Ls) = span\ X$

and *LX*: *set Ls* $\subseteq$ *X*
and *lin-Ls-Bs*: *lin-indpt-list* (*Ls* @ *Bs*)
and *len-Ls-Bs*: *length* (*Ls* @ *Bs*) = *n*
shows *cone* (*X* $\cup$ *set Bs*) $\cap$ {*x* $\in$ *carrier-vec n*. $\forall$ *w*$\in$*W*. *w* $\cdot$ *x* = *0*} = *cone X*
$\bigwedge$ *x*. $\forall$ *w*$\in$*W*. *w* $\cdot$ *x* = *0* $\Longrightarrow$ *Z* $\subseteq$ *X* $\Longrightarrow$ *B* $\subseteq$ *set Bs* $\Longrightarrow$ *x* = *lincomb c* (*Z* $\cup$ *B*)
$\Longrightarrow$ *x* = *lincomb c* (*Z* $-$ *B*)
⟨*proof*⟩

definition *polyhedral-cone* (*A* :: *'a mat*) = { *x* . *x* $\in$ *carrier-vec n* $\wedge$ *A* $*_v$ *x* $\leq$ 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* ∧ *sum c* {*0*..<*length Vs*} = *1*)

definition *convex-hull Vs* = {*x*. ∃ *Ws c*. *finite Ws* ∧ *Ws* ⊆ *Vs* ∧ *convex-lincomb c Ws x*}

lemma *convex-hull-carrier*[*intro*]: *Vs* ⊆ *carrier-vec n* ⟹ *convex-hull Vs* ⊆ *carrier-vec n*
⟨*proof*⟩

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

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

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

lemma *convex-hull-empty*[*simp*]:
convex-hull {} = {}
A ⊆ *carrier-vec n* ⟹ *convex-hull A* = {} ⟷ *A* = {}
⟨*proof*⟩

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

definition *convex-hull-list Vs* = {*x*. ∃ *c*. *convex-lincomb-list c Vs x*}

lemma *lincomb-list-elem*:
set Vs ⊆ *carrier-vec n* ⟹
lincomb-list (λ *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* ⊆ *carrier-vec n*
shows *set Vs* ⊆ *convex-hull-list Vs*
⟨*proof*⟩

lemma *convex-hull-list-combination*:
assumes *Vs*: *set Vs* ⊆ *carrier-vec n*
and *x*: *x* ∈ *convex-hull-list Vs*
and *y*: *y* ∈ *convex-hull-list Vs*
and *l0*: *0* ≤ *l* **and** *l1*: *l* ≤ *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* ⊆ *carrier-vec n*
shows *set Vs* ⊆ *set Ws* ⟹ *convex-hull-list Vs* ⊆ *convex-hull-list Ws*
⟨*proof*⟩

lemma *convex-hull-list-eq-set*:
set Vs ⊆ *carrier-vec n* ⟹ *set Vs* = *set Ws* ⟹ *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* ⟧ ⟹ *find-indices x Vs* = [*i*]
⟨*proof*⟩

lemma *finite-convex-hull-iff-convex-hull-list*: **assumes** *Vs*: *Vs* ⊆ *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* ⟹ *convex-hull S* = *S*
⟨*proof*⟩

lemma *convex-hull-convex-hull-listD*: **assumes** *A*: *A* ⊆ *carrier-vec n*
and *x*: *x* ∈ *convex-hull A*
shows ∃ *as*. *set as* ⊆ *A* ∧ *x* ∈ *convex-hull-list as*
⟨*proof*⟩

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

lemma *convexI*: **assumes** *S*: *S* ⊆ *carrier-vec n*
and *step*: ⋀ *a x y*. *x* ∈ *S* ⟹ *y* ∈ *S* ⟹ *0* ≤ *a* ⟹ *a* ≤ *1* ⟹ $a \cdot_v x + (1 - a) \cdot_v y \in S$
shows *convex S*
⟨*proof*⟩

lemma *convex-hulls-are-convex*: **assumes** *A* ⊆ *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 ⊆ *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* ∈ *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* ∪ *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* ⊆ *carrier-vec n*
shows *normal-vector W* ∈ *carrier-vec n*
normal-vector W ≠ 0_v *n*
w ∈ *W* ⟹ *w* · *normal-vector W* = *0*
w ∈ *W* ⟹ *normal-vector W* · *w* = *0*
lin-indpt (*insert* (*normal-vector W*) *W*)
normal-vector W ∉ *W*
W ⊆ $\mathbb{Z}_v$ ∩ *Bounded-vec Bnd* ⟹ *normal-vector W* ∈ $\mathbb{Z}_v$ ∩ *Bounded-vec* (*det-bound* (*n*−1) *Bnd*)
⟨*proof*⟩

lemma *normal-vector-span*:
assumes *card*: *Suc* (*card D*) = *n*
and *D*: *D* ⊆ *carrier-vec n* **and** *fin*: *finite D* **and** *lin*: *lin-indpt D*
shows *span D* = { *x. x* ∈ *carrier-vec n* ∧ *x* · *normal-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-vectors ws*) ⊆ *carrier-vec n*
w ∈ *set ws* ⟹ *nv* ∈ *set* (*normal-vectors ws*) ⟹ *nv* · *w* = *0*
w ∈ *set ws* ⟹ *nv* ∈ *set* (*normal-vectors ws*) ⟹ *w* · *nv* = *0*
lin-indpt-list (*ws* @ *normal-vectors ws*)
length ws + *length* (*normal-vectors ws*) = *n*
set ws ∩ *set* (*normal-vectors ws*) = {}
set ws ⊆ $\mathbb{Z}_v$ ∩ *Bounded-vec Bnd* ⟹
set (*normal-vectors ws*) ⊆ $\mathbb{Z}_v$ ∩ *Bounded-vec* (*det-bound* (*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'* · *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* $\Longrightarrow x \in$ *carrier-vec n* $\Longrightarrow c \cdot x > 0$
$c \in \{$*normal-vector D*, $-$*normal-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-vec n* $\wedge\ V \subseteq$ *span W* $\wedge$ *lin-indpt V*$\}$)

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

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

lemma *dim-span-insert*: **assumes** W: $W \subseteq$ *carrier-vec n*
and v: $v \in$ *carrier-vec n* **and** *vs*: $v \notin$ *span W*
shows *dim-span* (*insert v W*) = *Suc* (*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 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-vec n*
and *fin*: *finite A*
and b: $b \in$ *cone A*
shows $\nexists$ c. $c \in$ *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 $a :: nat \Rightarrow 'a\ vec$
    and $b :: 'a\ vec$
    and $m :: nat$
  assumes a: $a\ `\ \{0\ ..<\ m\} \subseteq carrier\text{-}vec\ n$
    and $inj\text{-}a$: $inj\text{-}on\ a\ \{0\ ..<\ m\}$
    and b: $b \in carrier\text{-}vec\ n$
    and $full\text{-}span$: $span\ (a\ `\ \{0\ ..<\ m\}) = carrier\text{-}vec\ n$
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 $card\text{-}a\text{-}I[simp]$: $I \subseteq \{0\ ..<\ m\} \Longrightarrow card\ (a\ `\ I) = card\ I$
  ⟨*proof*⟩ **lemma** $in\text{-}a\text{-}I[simp]$: $I \subseteq \{0\ ..<\ m\} \Longrightarrow i < m \Longrightarrow (a\ i \in a\ `\ I) = (i \in I)$
  ⟨*proof*⟩ **definition** $valid\text{-}I = \{\ I.\ card\ I = n \wedge lin\text{-}indpt\ (a\ `\ I) \wedge I \subseteq \{0\ ..<\ m\}\}$

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

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

lemma $fundamental\text{-}theorem\text{-}neg\text{-}C\text{-}or\text{-}B\text{-}in\text{-}context$:
  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 $fundamental\text{-}theorem\text{-}of\text{-}linear\text{-}inequalities\text{-}C\text{-}imp\text{-}B\text{-}full\text{-}dim$:
  assumes A: $A \subseteq carrier\text{-}vec\ n$

and *fin*: *finite A*
and *span*: *span A* = *carrier-vec n*
and *b*: *b* ∈ *carrier-vec n*
and *C*: ∄ *c B*. *B* ⊆ *A* ∧ *c* ∈ {*normal-vector B*, − *normal-vector B*} ∧ *Suc* (*card B*) = *n*
∧ *lin-indpt B* ∧ (∀ *a*$_i$ ∈ *A*. *c* ⋅ *a*$_i$ ≥ *0*) ∧ *c* ⋅ *b* < *0*
shows ∃ *B* ⊆ *A*. *lin-indpt B* ∧ *card B* = *n* ∧ *b* ∈ *finite-cone B*
⟨*proof*⟩

lemma *fundamental-theorem-of-linear-inequalities-full-dim*: **fixes** *A* :: *'a vec set*
defines *HyperN* ≡ {*b*. *b* ∈ *carrier-vec n* ∧ (∄ *B c*. *B* ⊆ *A* ∧ *c* ∈ {*normal-vector B*, − *normal-vector B*}
∧ *Suc* (*card B*) = *n* ∧ *lin-indpt B* ∧ (∀ *a*$_i$ ∈ *A*. *c* ⋅ *a*$_i$ ≥ *0*) ∧ *c* ⋅ *b* < *0*)}
defines *HyperA* ≡ {*b*. *b* ∈ *carrier-vec n* ∧ (∄ *c*. *c* ∈ *carrier-vec n* ∧ (∀ *a*$_i$ ∈ *A*. *c* ⋅ *a*$_i$ ≥ *0*) ∧ *c* ⋅ *b* < *0*)}
defines *lin-indpt-cone* ≡ ⋃ { *finite-cone B* | *B*. *B* ⊆ *A* ∧ *card B* = *n* ∧ *lin-indpt B*}
assumes *A*: *A* ⊆ *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*
⟨*proof*⟩

lemma *fundamental-theorem-of-linear-inequalities-C-imp-B*:
assumes *A*: *A* ⊆ *carrier-vec n*
and *fin*: *finite A*
and *b*: *b* ∈ *carrier-vec n*
and *C*: ∄ *c A'*. *c* ∈ *carrier-vec n*
∧ *A'* ⊆ *A* ∧ *Suc* (*card A'*) = *dim-span* (*insert b A*)
∧ (∀ *a* ∈ *A'*. *c* ⋅ *a* = *0*)
∧ *lin-indpt A'* ∧ (∀ *a*$_i$ ∈ *A*. *c* ⋅ *a*$_i$ ≥ *0*) ∧ *c* ⋅ *b* < *0*
shows ∃ *B* ⊆ *A*. *lin-indpt B* ∧ *card B* = *dim-span A* ∧ *b* ∈ *finite-cone B*
⟨*proof*⟩

lemma *fundamental-theorem-of-linear-inequalities*: **fixes** *A* :: *'a vec set*
defines *HyperN* ≡ {*b*. *b* ∈ *carrier-vec n* ∧ (∄ *c B*. *c* ∈ *carrier-vec n* ∧ *B* ⊆ *A*
∧ *Suc* (*card B*) = *dim-span* (*insert b A*) ∧ *lin-indpt B*
∧ (∀ *a* ∈ *B*. *c* ⋅ *a* = *0*)
∧ (∀ *a*$_i$ ∈ *A*. *c* ⋅ *a*$_i$ ≥ *0*) ∧ *c* ⋅ *b* < *0*)}
defines *HyperA* ≡ {*b*. *b* ∈ *carrier-vec n* ∧ (∄ *c*. *c* ∈ *carrier-vec n* ∧ (∀ *a*$_i$ ∈ *A*. *c* ⋅ *a*$_i$ ≥ *0*) ∧ *c* ⋅ *b* < *0*)}
defines *lin-indpt-cone* ≡ ⋃ { *finite-cone B* | *B*. *B* ⊆ *A* ∧ *card B* = *dim-span A* ∧ *lin-indpt B*}
assumes *A*: *A* ⊆ *carrier-vec n*
and *fin*: *finite A*

shows
cone A = lin-indpt-cone
cone A = HyperN
cone A = HyperA
⟨*proof*⟩

corollary *Caratheodory-theorem*: **assumes** *A*: $A \subseteq$ *carrier-vec n*
shows *cone A* $= \bigcup$ {*finite-cone B* |*B*. $B \subseteq A \wedge$ *lin-indpt B*}
⟨*proof*⟩
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* ∈ *carrier-mat n nr* **and** *b*: *b* ∈ *carrier-vec n*
shows (∃ *x*. $x \geq 0_v$ *nr* ∧ *A* $*_v$ *x* = *b*) ⟷ (∀ *y*. *y* ∈ *carrier-vec n* ⟶ A^T $*_v$ *y* $\geq 0_v$ *nr* ⟶ *y* · *b* ≥ 0)
⟨*proof*⟩

lemma *Farkas-Lemma'*:
fixes *A* :: *'a mat* **and** *b* :: *'a vec*
assumes *A*: *A* ∈ *carrier-mat nr nc* **and** *b*: *b*∈ *carrier-vec nr*
shows (∃*x*. *x*∈ *carrier-vec nc* ∧ *A* $*_v$ *x* ≤ *b*)
⟷ (∀ *y*. $y \geq 0_v$ *nr* ∧ A^T $*_v$ *y* = 0_v *nc* ⟶ *y* · *b* ≥ 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.

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*
$\wedge$ ($X \subseteq \mathbb{Z}_v \cap$ *Bounded-vec Bnd* $\longrightarrow$ $A \in \mathbb{Z}_m \cap$ *Bounded-mat* (*det-bound* (*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* $\wedge$
($X \subseteq \mathbb{Z}_v \cap$ *Bounded-vec Bnd* $\longrightarrow$ $A \in \mathbb{Z}_m \cap$ *Bounded-mat* (*det-bound* (*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*
$\wedge$ ($A \in \mathbb{Z}_m \cap$ *Bounded-mat Bnd* $\longrightarrow$ $X \subseteq \mathbb{Z}_v \cap$ *Bounded-vec* (*det-bound* (*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* $P = (\exists\ V.\ V \subseteq$ *carrier-vec* $n \wedge$ *finite* $V \wedge P =$ *convex-hull* $V)$

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

lemma *polyhedra-are-convex*:
assumes A: $A \in$ *carrier-mat* $nr\ n$
and b: $b \in$ *carrier-vec* nr
and P: $P =$ *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*: *set Xs* ⊆ *carrier-vec n*
and *nm*: $m \leq n$
shows *vec-first* (*n.lincomb-list c Xs*) *m* =
m.lincomb-list c (*map* (λ *v*. *vec-first v m*) *Xs*)
⟨*proof*⟩

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

⟨*proof*⟩

lemma *cone-next-dim*:
assumes $n = m + 1$
and X: $X \subseteq$ *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* $\mid$ *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* $\wedge$
($A \in \mathbb{Z}_m \cap$ *Bounded-mat Bnd* $\longrightarrow$ $b \in \mathbb{Z}_v \cap$ *Bounded-vec Bnd* $\longrightarrow$
$X \subseteq \mathbb{Z}_v \cap$ *Bounded-vec* (*det-bound n* (*max 1 Bnd*))
$\wedge$ $Q \subseteq$ *Bounded-vec* (*det-bound 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 $Ax \leq b \wedge A'x < b'$ has a (mixed)integer solution, there there is also a small (mixed)integer solution, where the numbers are bounded by $(n+1)! \cdot m^n$ where n is the number of variables and m is a bound on the absolute values of numbers occurring in A, A', b, b'.

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

definition *less-vec* :: *'a vec* ⇒ (*'a* :: *ord*) *vec* ⇒ *bool* (**infix** $<_v$ *50*) **where**
  $v <_v w$ = (*dim-vec* v = *dim-vec* $w \wedge$ ($\forall$ $i <$ *dim-vec* w. $v \$ i < w \$ i$))

lemma *less-vecD*: **assumes** $v <_v w$ **and** $w \in$ *carrier-vec* n
  shows $i < n \Longrightarrow v \$ i < w \$ i$
  ⟨*proof*⟩

lemma *less-vecI*: **assumes** $v \in$ *carrier-vec* n $w \in$ *carrier-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*) $\Longrightarrow v \leq w$
  ⟨*proof*⟩

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

lemma *floor-of-int-eq*[*simp*]: $x \in \mathbb{Z} \Longrightarrow$ *of-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 *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 Bnd*
and *b1Bnd*: $b_1 \in \mathbb{Z}_v \cap$ *Bounded-vec Bnd*
and *A2Bnd*: $A_2 \in \mathbb{Z}_m \cap$ *Bounded-mat Bnd*
and *b2Bnd*: $b_2 \in \mathbb{Z}_v \cap$ *Bounded-vec 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* (*fact* (*n*+*1*) $*$ (*max 1 Bnd*)^*n*)
⟨*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 *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 Bnd*
and *b1Bnd*: $b_1 \in \mathbb{Z}_v \cap$ *Bounded-vec Bnd*
and *A2Bnd*: $A_2 \in \mathbb{Z}_m \cap$ *Bounded-mat Bnd*
and *b2Bnd*: $b_2 \in \mathbb{Z}_v \cap$ *Bounded-vec 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* (*fact* (*n*+*1*) $*$ *Bnd*^*n*)
⟨*proof*⟩

corollary *small-integer-solution-nonstrict*: **fixes** *A* :: *'a mat*
assumes *A*: $A \in$ *carrier-mat nr n*
and *b*: $b \in$ *carrier-vec nr*
and *ABnd*: $A \in \mathbb{Z}_m \cap$ *Bounded-mat Bnd*
and *bBnd*: $b \in \mathbb{Z}_v \cap$ *Bounded-vec Bnd*
and *x*: $x \in$ *carrier-vec n*
and *xI*: $x \in \mathbb{Z}_v$
and *sol*: $A *_v x \leq b$

and *non-degenerate*: $nr \neq 0 \vee Bnd \geq 0$
shows $\exists\ y.$
$y \in$ *carrier-vec* $n \wedge$
$y \in \mathbb{Z}_v \wedge$
$A *_v y \leq b \wedge$
$y \in$ *Bounded-vec* (*fact* $(n+1) * Bnd\hat{}n$)
⟨*proof*⟩

end
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* $b| \leq Bnd \Longrightarrow -$ (*floor* $Bnd) \leq b$
⟨*proof*⟩

lemma *abs-pos-floor*: $|$*of-int* $b| \leq Bnd \Longrightarrow b \leq$ *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** 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*: *Bnd* = *Max* (*abs* ' (*elements-mat A* ∪ *vec-set b*))
shows ∃ *H C*. $H \cup C \subseteq$ *carrier-vec n* ∩ $\mathbb{Z}_v$
∧ $H \subseteq$ *Bounded-vec* (*fact* (*n*+1) ∗ (*max* 1 *Bnd*)^*n*)
∧ $C \subseteq$ *Bounded-vec* (*fact n* ∗ (*max* 1 *Bnd*)^*n*)
∧ *finite* (*H* ∪ *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*′ ∈ *carrier-mat nr*′ *n* ∧ *b*′ ∈ *carrier-vec nr*′ ∧ *integer-hull P* = *polyhedron A*′ *b*′
⟨*proof*⟩

corollary *small-integer-solution-nonstrict-via-decomp*: **fixes** *A* :: *'a mat*
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 *Bnd*: *Bnd* = *Max* (*abs* ' (*elements-mat A* ∪ *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 ∃ *y*.
y ∈ *carrier-vec n* ∧
y ∈ $\mathbb{Z}_v$ ∧
$A *_v y \leq b$ ∧
y ∈ *Bounded-vec* (*fact* (*n*+1) ∗ (*max* 1 *Bnd*)^*n*)
⟨*proof*⟩

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.