

d. Suppose we have a monomial ordering \prec_{mon} and let C be the set of vectors $\nu \in \mathbb{Z}^n$ such that $\nu = a - b$ for monomials $\mathbf{x}^b \prec_{\text{mon}} \mathbf{x}^a$.

Result 1. If $\nu_1, \nu_2 \in C$ and $p, q \in \mathbb{Q}_+$ then $p\nu_1 + q\nu_2 \in C$ whenever $p\nu_1 + q\nu_2 \in \mathbb{Z}^n$.

Proof. Consider four monomials $\mathbf{x}^b \prec_{\text{mon}} \mathbf{x}^a$ and $\mathbf{x}^d \prec_{\text{mon}} \mathbf{x}^c$ in $\mathbb{F}[x_1, \dots, x_n]$. Suppose we have $p, q \in \mathbb{Q}_+$ such that $\nu = p(a - b) + q(c - d) \in \mathbb{Z}^n$. It is convenient to explicitly write p and q as fractions:

$$p = \frac{p_N}{p_D}, q = \frac{q_N}{q_D} \text{ with } p_D, q_D, p_N, q_N \in \mathbb{Z}_+$$

We know $(\mathbf{x}^b)^{p_N q_D} \prec_{\text{mon}} (\mathbf{x}^a)^{p_N q_D}$ and $(\mathbf{x}^d)^{p_D q_N} \prec_{\text{mon}} (\mathbf{x}^c)^{p_D q_N}$. Defining

$$f = p_N q_D a + p_D q_N c$$

$$g = p_N q_D b + p_D q_N d$$

we have $\mathbf{x}^g \prec_{\text{mon}} \mathbf{x}^f$ so $f - g \in C$. It is easy to check that $-\mu \notin C$ whenever $\mu \in C$. Now, choose $e \in \mathbb{Z}_{\geq 0}^n$ so that $e + \nu \in \mathbb{Z}_{\geq 0}^n$, then $(\mathbf{x}^e)^{p_D q_D} = \mathbf{x}^{p_D q_D e}$ and $(\mathbf{x}^{e+\nu})^{p_D q_D} = \mathbf{x}^{p_D q_D e + f - g}$. Because $f - g$ is in C and \prec_{mon} is a total ordering on monomials, we have $\mathbf{x}^{p_D q_D e} \prec_{\text{mon}} \mathbf{x}^{p_D q_D e + f - g}$ so $(\mathbf{x}^e)^{p_D q_D} \prec_{\text{mon}} (\mathbf{x}^{e+\nu})^{p_D q_D}$. But then it must be true that $\mathbf{x}^e \prec_{\text{mon}} \mathbf{x}^{e+\nu}$ so $\nu \in C$. \square

Suppose we are given a finite number of vectors $\nu_1, \nu_2, \dots, \nu_m \in C$ and consider the convex combination

$$(1) \quad \sum_{i=1}^m r_i \nu_i = 0$$

with $r_1, \dots, r_m \in \mathbb{R}_+$. Clearly $m \geq 2$. Let M be the $n \times m$ matrix with i -th column equal to ν_i and let $r = (r_1, \dots, r_m)$. The null space of the linear map L_M induced by M is nontrivial because $L_M(r) = 0$ and has a basis β consisting of vectors in \mathbb{Q}^m . This may be checked by Gaussian elimination on M . Say $\beta = \{u_1, \dots, u_l\}$ and write $r = c_1 u_1 + \dots + c_l u_l$. As r lies in \mathbb{R}_+^m we may find rationals c_1^*, \dots, c_l^* sufficiently close to c_1, \dots, c_l (respectively) such that $q = c_1^* u_1 + \dots + c_l^* u_l$ has positive components, *i.e.* $q \in \mathbb{Q}_+^m$. We can choose these rational coefficients so that the components of q add up to 1. But then $L_M(q) = 0$ and we have the rational convex combination

$$\sum_{i=1}^m (q)_i \nu_i = 0$$

More conveniently, we have positive integers n_1, \dots, n_m such that

$$\sum_{i=1}^m n_i \nu_i = 0$$

Using Result 1 inductively we obtain a contradiction because clearly $0 \notin C$. Note Equation 1 holds for vectors $\nu_1, \dots, \nu_m \in C$ iff 0 lies in the convex hull of C , denoted by $\text{ch}(C)$. Thus $0 \notin \text{ch}(C)$.

One separation theorem in convex analysis shows there exists an hyperplane $H^{(1)}$ of \mathbb{R}^n separating (not necessarily strictly) 0 and $\text{ch}(C)$, *i.e.* there exists a vector $v_1 \in \mathbb{R}^n \setminus \{0\}$ such that $v_1 \cdot x \geq 0$ for all $x \in \text{ch}(C)$. Actually v_1 has nonnegative components because C contains the canonical basis of \mathbb{R}^n . Moreover, if μ is a vector in $\mathbb{Z}^n \setminus \{0\}$ such that $v_1 \cdot \mu > 0$ then μ lies in C because either $\mu \in C$ or $-\mu \in C$ holds and in the later case we would have $v_1 \cdot \mu \leq 0$. We may simply define $H^{(1)} = v_1^\perp$, the orthogonal complement of v_1 .

Now, define the set $C^{(1)} = H^{(1)} \cap C$. If $C^{(1)} = \emptyset$ then we are done and we can tell apart any element of C via taking the dot product with v_1 . Otherwise, notice that $0 \notin \text{ch}(C^{(1)})$. Extending the separation theorem to arbitrary vector subspaces of \mathbb{R}^n we can find an hyperplane $H^{(2)}$ of $H^{(1)}$ separating 0 and $\text{ch}(C^{(1)})$, or equivalently, a vector $v_2 \in H^{(1)} \setminus \{0\}$ such that $v_2 \cdot x \geq 0$ for all $x \in \text{ch}(C^{(1)})$ so that $H^{(2)} = v_1^\perp \cap v_2^\perp$. Again, if for some $\mu \in \mathbb{Z}^n \setminus \{0\}$ we have $v_1 \cdot \mu = 0$ and $v_2 \cdot \mu > 0$, then μ lies in $C^{(1)} \subseteq C$. We then define $C^{(2)} = H^{(2)} \cap C^{(1)}$ and ask whether $C^{(2)} = \emptyset$. If true, we can tell apart vectors in C via first taking their dot product with v_1 and, in case of a 0 , subsequently taking the product with v_2 , which would suffice. If not true, we continue our inductive

process until we stop. It will have to stop necessarily when we find n vectors v_1, v_2, \dots, v_n : they are pairwise orthogonal by construction, so by linear independence they form a basis of \mathbb{R}^n and we would have $C^{(n)} = H^{(n)} \cap C^{(n-1)} = (v_1^\perp \cap v_2^\perp \cap \dots \cap v_n^\perp) \cap C^{(n-1)} \subseteq \{0\} \cap C = \emptyset$. In any case, we could complete the orthogonal basis without affecting the weight order.