Elements of Geometry for Robotics

Translation of Euclid's Elements by Adelardus Bathensis (1080–1152)

Tomas Pajdla

pajdla@cvut.cz

Monday 1st November, 2021

Contents

1 Notation

$\varnothing$	...	the empty set [1]
$\exp U$	...	the set of all subsets of set U [1]
$U \times V$	...	Cartesian product of sets U and V [1]
$\mathbb{Z}$	...	whole numbers [1]
$\mathbb{Z}_{\geqslant 0}$	...	non-negative $\mathbb{Z}$ [2] (i.e. $0, 1, 2, \ldots$)
$\mathbb{Q}$	...	rational numbers [3]
$\mathbb{R}$	...	real numbers [3]
i	...	imaginary unit [3]
$(S, +, \ )$	...	space of geometric scalars
A	...	affine space (space of geometric vectors)
$(A_o, \oplus, \odot)$	...	space of geometric vectors bound to point o
$(V, \boxplus, \boxdot)$	...	space of free vectors
$\mathbb{A}^2$	...	real affine plane
$\mathbb{A}^3$	...	three-dimensional real affine space
$\mathbb{P}^2$	...	real projective plane
$\mathbb{P}^3$	...	three-dimensional real projective space
$\vec{x}$	...	vector
$\mathtt{A}$	...	matrix
$\mathtt{A}_{ij}$	...	ij element of $\mathtt{A}$
$\mathtt{A}^\top$	...	transpose of $\mathtt{A}$
$\mathtt{A}^\dagger$	...	conjugate transpose of $\mathtt{A}$
$\lvert\mathtt{A}\rvert$	...	determinant of $\mathtt{A}$
$\mathtt{I}$	...	identity matrix
$\mathtt{R}$	...	rotation matrix
$\otimes$	...	Kronecker product of matrices
$\beta = [\vec{b}_1, \vec{b}_2, \vec{b}_3]$	...	basis (an ordered triple of independent generator vectors)
$\beta^\star, \bar{\beta}$	...	the dual basis to basis β
$\vec{x}_\beta$	...	column matrix of coordinates of $\vec{x}$ w.r.t. the basis β
$\vec{x} \cdot \vec{y}$	...	Euclidean scalar product of $\vec{x}$ and $\vec{y}$ ($\vec{x} \cdot \vec{y} = \vec{x}_\beta^\top \, \vec{y}_\beta$ in an orthonormal basis β)
$\vec{x} \times \vec{y}$	...	cross (vector) product of $\vec{x}$ and $\vec{y}$
$[\vec{x}]_\times$	...	the matrix such that $[\vec{x}]_\times \, \vec{y} = \vec{x} \times \vec{y}$
$\lVert\vec{x}\rVert$	...	Euclidean norm of $\vec{x}$ ($\lVert\vec{x}\rVert = \sqrt{\vec{x} \cdot \vec{x}}$)
orthogonal vectors	...	mutually perpendicular vectors
equi-orthogonal vectors	...	orthogonal vectors of equal length
orthonormal vectors	...	unit orthogonal vectors
orthogonal matrix	...	matrix with non-zero equi-orthogonal columns and rows
orthonormal matrix	...	matrix with orthonormal columns and rows
$P \circ l$	...	point P is incident to line l
$P \vee Q$	...	line(s) incident to points P and Q
$k \wedge l$	...	point(s) incident to lines k and l

2 Linear algebra

We rely on linear algebra [4, 5, 6, 7, 8, 9]. We recommend excellent text books [7, 4] for acquiring basic as well as more advanced elements of the topic. Monograph [5] provides a number of examples and applications and provides a link to numerical and computational aspects of linear algebra. We will next review the most crucial topics needed in this text.

2.1 Change of coordinates induced by the change of basis

Let us discuss the relationship between the coordinates of a vector in a linear space, which is induced by passing from one basis to another. We shall derive the relationship between the coordinates in a three-dimensional linear space over real numbers, which is the most important when modeling the geometry around us. The formulas for all other n-dimensional spaces are obtained by passing from 3 to n.

§ 1 Coordinates Let us consider an ordered basis $\beta = \begin{bmatrix} \vec{b}_1 & \vec{b}_2 & \vec{b}_3 \end{bmatrix}$ of a three-dimensional vector space V^3 over scalars $\mathbb{R}$. A vector $\vec{v} \in V^3$ is uniquely expressed as a linear combination of basic vectors of V^3 by its *coordinates* $x, y, z \in \mathbb{R}$, i.e. $\vec{v} = x\,\vec{b}_1 + y\,\vec{b}_2 + z\,\vec{b}_3$, and can be represented as an ordered triple of coordinates, i.e. as $\vec{v}_\beta = \begin{bmatrix} x & y & z \end{bmatrix}^\top$.

We see that an ordered triple of scalars can be understood as a triple of coordinates of a vector in V^3 w.r.t. a basis of V^3. However, at the same time, the set of ordered triples $\begin{bmatrix} x & y & z \end{bmatrix}^\top$ is also a three-dimensional *coordinate linear space* $\mathbb{R}^3$ over $\mathbb{R}$ with $\begin{bmatrix} x_1 & y_1 & z_1 \end{bmatrix}^\top + \begin{bmatrix} x_2 & y_2 & z_2 \end{bmatrix}^\top = \begin{bmatrix} x_1 + x_2 & y_1 + y_2 & z_1 + z_2 \end{bmatrix}^\top$ and $s \begin{bmatrix} x & y & z \end{bmatrix}^\top = \begin{bmatrix} s\,x & s\,y & s\,z \end{bmatrix}^\top$ for $s \in \mathbb{R}$. Moreover, the ordered triple of the following three particular coordinate vectors

$$\sigma = \begin{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \end{bmatrix} \tag{2.1}$$

forms an ordered basis of $\mathbb{R}^3$, the *standard basis*, and therefore a vector $\vec{v} = \begin{bmatrix} x & y & z \end{bmatrix}^\top$ is represented by $\vec{v}_\sigma = \begin{bmatrix} x & y & z \end{bmatrix}^\top$ w.r.t. the standard basis in $\mathbb{R}^3$. It is noticeable that the vector $\vec{v}$ and the coordinate vector $\vec{v}_\sigma$ of its coordinates w.r.t. the standard basis of $\mathbb{R}^3$, are identical.

§ 2 Two bases Having two ordered bases $\beta = \begin{bmatrix} \vec{b}_1 & \vec{b}_2 & \vec{b}_3 \end{bmatrix}$ and $\beta' = \begin{bmatrix} \vec{b}'_1 & \vec{b}'_2 & \vec{b}'_3 \end{bmatrix}$ leads to expressing one vector $\vec{x}$ in two ways as $\vec{x} = x\,\vec{b}_1 + y\,\vec{b}_2 + z\,\vec{b}_3$ and $\vec{x} = x'\,\vec{b}'_1 + y'\,\vec{b}'_2 + z'\,\vec{b}'_3$. The vectors of the basis β can also be expressed in the basis β' using their coordinates. Let us introduce

$$\begin{aligned} \vec{b}_1 &= a_{11}\,\vec{b}'_1 + a_{21}\,\vec{b}'_2 + a_{31}\,\vec{b}'_3 \\ \vec{b}_2 &= a_{12}\,\vec{b}'_1 + a_{22}\,\vec{b}'_2 + a_{32}\,\vec{b}'_3 \\ \vec{b}_3 &= a_{13}\,\vec{b}'_1 + a_{23}\,\vec{b}'_2 + a_{33}\,\vec{b}'_3 \end{aligned} \tag{2.2}$$

§ 3 Change of coordinates We will next use the above equations to relate the coordinates of $\vec{x}$ w.r.t. the basis β to the coordinates of $\vec{x}$ w.r.t. the basis β'

$$\begin{aligned} \vec{x} &= x\,\vec{b}_1 + y\,\vec{b}_2 + z\,\vec{b}_3 \\ &= x\,(a_{11}\,\vec{b}'_1 + a_{21}\,\vec{b}'_2 + a_{31}\,\vec{b}'_3) + y\,(a_{12}\,\vec{b}'_1 + a_{22}\,\vec{b}'_2 + a_{32}\,\vec{b}'_3) + z\,(a_{13}\,\vec{b}'_1 + a_{23}\,\vec{b}'_2 + a_{33}\,\vec{b}'_3) \\ &= (a_{11}\,x + a_{12}\,y + a_{13}\,z)\,\vec{b}'_1 + (a_{21}\,x + a_{22}\,y + a_{23}\,z)\,\vec{b}'_2 + (a_{31}\,x + a_{32}\,y + a_{33}\,z)\,\vec{b}'_3 \\ &= x'\,\vec{b}'_1 + y'\,\vec{b}'_2 + z'\,\vec{b}'_3 \end{aligned} \tag{2.3}$$

Since coordinates are unique, we get

$$x' = a_{11}\,x + a_{12}\,y + a_{13}\,z \tag{2.4}$$

$$y' = a_{21}\,x + a_{22}\,y + a_{23}\,z \tag{2.5}$$

$$z' = a_{31}\,x + a_{32}\,y + a_{33}\,z \tag{2.6}$$

Coordinate vectors $\vec{x}_\beta$ and $\vec{x}_{\beta'}$ are thus related by the following matrix multiplication

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \tag{2.7}$$

which we concisely write as

$$\vec{x}_{\beta'} = \mathtt{A}\,\vec{x}_\beta \tag{2.8}$$

The columns of matrix A can be viewed as vectors of coordinates of basic vectors, $\vec{b}_1, \vec{b}_2, \vec{b}_3$ of β in the basis β'

$$\mathtt{A} = \begin{bmatrix} | & | & | \\ \vec{b}_{1_{\beta'}} & \vec{b}_{2_{\beta'}} & \vec{b}_{3_{\beta'}} \\ | & | & | \end{bmatrix} \tag{2.9}$$

and the matrix multiplication can be interpreted as a linear combination of the columns of A by coordinates of $\vec{x}$ w.r.t. β

$$\vec{x}_{\beta'} = x\,\vec{b}_{1_{\beta'}} + y\,\vec{b}_{2_{\beta'}} + z\,\vec{b}_{3_{\beta'}} \tag{2.10}$$

Matrix A plays such an important role here that it deserves its own name. Matrix A is very often called the *change of basis matrix from basis β to β'* or the *transition matrix from basis β to basis β'* [5, 10] since it can be used to pass from coordinates w.r.t. β to coordinates w.r.t. β' by Equation 2.8.

However, literature [6, 11] calls A the *change of basis matrix from basis β' to β*, i.e. it (seemingly illogically) swaps the bases. This choice is motivated by the fact that A relates vectors of β and vectors of β' by Equation 2.2 as

$$\begin{aligned} \begin{bmatrix} \vec{b}_1 & \vec{b}_2 & \vec{b}_3 \end{bmatrix} &= \Big[a_{11}\,\vec{b}'_1 + a_{21}\,\vec{b}'_2 + a_{31}\,\vec{b}'_3 \quad a_{12}\,\vec{b}'_1 + a_{22}\,\vec{b}'_2 + a_{32}\,\vec{b}'_3 \\ &\qquad\qquad a_{13}\,\vec{b}'_1 + a_{23}\,\vec{b}'_2 + a_{33}\,\vec{b}'_3 \Big] \end{aligned} \tag{2.11}$$

$$\begin{bmatrix} \vec{b}_1 & \vec{b}_2 & \vec{b}_3 \end{bmatrix} = \begin{bmatrix} \vec{b}'_1 & \vec{b}'_2 & \vec{b}'_3 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \tag{2.12}$$

and therefore giving

$$\begin{bmatrix} \vec{b}_1 & \vec{b}_2 & \vec{b}_3 \end{bmatrix} = \begin{bmatrix} \vec{b}'_1 & \vec{b}'_2 & \vec{b}'_3 \end{bmatrix} \mathtt{A} \tag{2.13}$$

or equivalently

$$\begin{bmatrix} \vec{b}'_1 & \vec{b}'_2 & \vec{b}'_3 \end{bmatrix} = \begin{bmatrix} \vec{b}_1 & \vec{b}_2 & \vec{b}_3 \end{bmatrix} \mathtt{A}^{-1} \tag{2.14}$$

where the multiplication of a row of column vectors by a matrix from the right in Equation 2.13 has the meaning given by Equation 2.11 above. Yet another variation of the naming appeared in [8, 9] where $\mathtt{A}^{-1}$ was named the *change of basis matrix from basis β to β'*.

We have to conclude that the meaning associated with the *change of basis matrix* varies in the literature and hence we will avoid this confusing name and talk about $\mathtt{A}$ as about the *matrix transforming coordinates of a vector from basis β to basis β'*.

There is the following interesting variation of Equation 2.13

$$\begin{bmatrix} \vec{b}'_1 \\ \vec{b}'_2 \\ \vec{b}'_3 \end{bmatrix} = \mathtt{A}^{-\top} \begin{bmatrix} \vec{b}_1 \\ \vec{b}_2 \\ \vec{b}_3 \end{bmatrix} \tag{2.15}$$

where the basic vectors of β and β' are understood as elements of column vectors. For instance, vector $\vec{b}'_1$ is obtained as

$$\vec{b}'_1 = a^\star_{11}\,\vec{b}_1 + a^\star_{12}\,\vec{b}_2 + a^\star_{13}\,\vec{b}_3 \tag{2.16}$$

where $[a^\star_{11}, a^\star_{12}, a^\star_{13}]$ is the first row of $\mathtt{A}^{-\top}$.

§ 4 Example We demonstrate the relationship between vectors and bases on a concrete example. Consider two bases α and β represented by coordinate vectors, which we write into matrices

$$\alpha = \begin{bmatrix} \vec{a}_1 & \vec{a}_2 & \vec{a}_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \tag{2.17}$$

$$\beta = \begin{bmatrix} \vec{b}_1 & \vec{b}_2 & \vec{b}_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \tag{2.18}$$

and a vector $\vec{x}$ with coordinates w.r.t. the basis α

$$\vec{x}_\alpha = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \tag{2.19}$$

We see that basic vectors of α can be obtained as the following linear combinations of basic vectors of β

$$\vec{a}_1 = +1\,\vec{b}_1 + 0\,\vec{b}_2 + 0\,\vec{b}_3 \tag{2.20}$$

$$\vec{a}_2 = +1\,\vec{b}_1 - 1\,\vec{b}_2 + 1\,\vec{b}_3 \tag{2.21}$$

$$\vec{a}_3 = -1\,\vec{b}_1 + 0\,\vec{b}_2 + 1\,\vec{b}_3 \tag{2.22}$$

or equivalently

$$\begin{bmatrix} \vec{a}_1 & \vec{a}_2 & \vec{a}_3 \end{bmatrix} = \begin{bmatrix} \vec{b}_1 & \vec{b}_2 & \vec{b}_3 \end{bmatrix} \begin{bmatrix} 1 & 1 & -1 \\ 0 & -1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} \vec{b}_1 & \vec{b}_2 & \vec{b}_3 \end{bmatrix} \mathtt{A} \tag{2.23}$$

Coordinates of $\vec{x}$ w.r.t. β are hence obtained as

$$\vec{x}_\beta = \mathtt{A}\,\vec{x}_\alpha, \qquad \mathtt{A} = \begin{bmatrix} 1 & 1 & -1 \\ 0 & -1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \tag{2.24}$$

$$\begin{bmatrix} 1 \\ -1 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & -1 \\ 0 & -1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \tag{2.25}$$

We see that

$$\alpha = \beta\,\mathtt{A} \tag{2.26}$$

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & -1 \\ 0 & -1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \tag{2.27}$$

The following questions arises: When are the coordinates of a vector $\vec{x}$ (Equation 2.8) and the basic vectors themselves (Equation 2.15) transformed in the same way? In other words, when $\mathtt{A} = \mathtt{A}^{-\top}$. We shall give the answer to this question later in paragraph 2.4.

2.2 Determinant

Determinat [4] of a matrix $\mathtt{A}$, denoted by $|\mathtt{A}|$, is a very interesting and useful concept. It can be, for instance, used to check the linear independence of a set of vectors or to define an orientation of the space.

2.2.1 Permutations

A *permutation* [4] π on the set $[n]= \{1,\ldots,n\}$ of integers is a one-to-one function from $[n]$ onto $[n]$. The identity permutation will be denoted by ϵ, i.e. $\epsilon(i) = i$ for all $i \in [n]$.

§ 1 Composition of permutations Let σ and π be two permutations on $[n]$. Then, their composition, i.e. $\pi(\sigma)$, is also a permutation on $[n]$ since a composition of two one-to-one onto functions is a one-to-one onto function. We see that if $\pi(\sigma(i)) = \pi(\sigma(j))$, then $\sigma(i) = \sigma(j)$ and therefore $i = j$ since π and σ are one-to-one functions. On the other hand, if $i = j$, then $\pi(\sigma(i)) = \pi(\sigma(j))$. To simplify the notation when composing a large number of permutations, we will sometimes write $\pi\,\sigma$ for the composition $\pi(\sigma)$ and π^k for the sequence of k compositions of π. For instance $\pi(\pi(i)) = \pi\,\pi(i) = \pi^2(i)$. Let us not forget that $\pi\,\sigma \neq \sigma\,\pi$ in general.

Let us next show that every permutation can be written as a composition of some simple permutations. We first define particularly simple permutations.

§ 2 Cycles Take $i \in [n]$ and look at the values in the sequence $[i, \pi(i), \pi^2(i), \ldots]$. Since the range of π has n values, there must be $1 \leqslant j \leqslant m \leqslant n$ such that $\pi^j(i) = \pi^m(i)$. Hence $\epsilon = (\pi^j(i))^{-1}(\pi^m(i)) = \pi^{m-j}(i)$. Let k be the smallest number among all such numbers $m - j$. Then, the sequence $c(i) = [i, \pi(i), \ldots, \pi^{k-1}(i)]$ has pairwise distinct elements. We can now define a new permutation $\pi_{c(i)}$ as follows. If $j \in c(i)$, then $\pi_{c(i)}(j) = \pi(j)$ and if $j \in [n]$ but $j \notin c$, then $\pi_{c(i)}(j) = j$. Now, if $k \geqslant 2$, then permutation $\pi_{c(i)}$ is called the *cycle* of π generated by i. We could at this point also include the permutations for $k = 1$, which are equal to the identity ϵ, but then we would loose the nice property of unique decomposition of permutations, which are not identities, into a composition of their disjoint cycles. Notice that when $j \in c(i)$, then $\pi_{c(j)} = \pi_{c(i)}$, i.e. although sequences $c(i)$ and $c(j)$ are not the same, functions $\pi_{c(j)}$ and $\pi_{c(i)}$ are equal. We say that π_c is a cycle of π, or in short a cycle, when π_c

is a cycle of π generated by some $i \in [n]$. A cycle π_c of length k can be represented as a sequence of numbers $c = [i_1, i_2, \ldots, i_k]$, such that $i_{(j \bmod k + 1)} = \pi_c(i_j)$. To be economical, this representation does not list the fixed elements of π_c, i.e. those for which $\pi_c(i) = i$.

§ **3 Transpositions** A shortest cycle, which is of length two, is called a *transposition*.

It is important to notice that every cycle can be written as a composition of transpositions. All shortest cycles are transpositions. Consider a cycle of length $k+1$ represented by the sequence $c_{k+1} = [i_1, i_2, \ldots, i_k, i_{k+1}]$ and the cycle $c_k = [i_1, i_2, \ldots, i_k]$ of length k and the transposition $t = [i_1, i_{k+1}]$. We see that $\pi_{c_{k+1}} = \pi_t(\pi_{c_k})$. Thus, by the principle of mathematical induction [1], every cycle can be written as a composition of transpositions.

There are many ways how to write a cycle as a composition of transpositions. A particularly useful way is as follows. All shortest cycles are transpositions, which can be represented by $[i_1, i_2]$ for some $i_1, i_2 \in [n]$. Consider a cycle of length $k+1$ represented by the sequence $c_{k+1} = [i_1, i_2, \ldots, i_k, i_{k+1}]$ and the cycle $c_k = [i_1, i_2, \ldots, i_k]$ of length k and the transposition $t = [i_k, i_{k+1}]$. We see that $\pi_{c_{k+1}} = \pi_{c_k}(\pi_t)$. Thus, by the principle of mathematical induction [1] a cycle $\pi_{[i_1, i_2, \ldots, i_k]}$ can be written as a composition of transpositions $\pi_{[i_1, i_2, \ldots, i_k]} = \pi_{[i_1, i_2]}\, \pi_{[i_2, i_3]} \cdots \pi_{[i_{k-2}, i_{k-1}]}\, \pi_{[i_{k-1}, i_k]}$ for every k.

§ **4 Decomposition of a permutation into disjoint cycles** Let us now show that every permutation π, which is not the identity, can be uniquely written as a composition of cycles of π and thus also as a composition of permutations of π. We introduce the equivalence relation [1] $\equiv_\pi$ on $[n]$ by $i \equiv_\pi j$ when $\pi_{c(i)} = \pi_{c(j)}$. This equivalence relation partitions [1] $[n]$ uniquely into $1 \leqslant m \leqslant n$ disjoint equivalence classes. We distinguish two types of the classes. There are classes of the size equal to one, which correspond to ϵ, and there are classes of the size larger than one, which are cycles. Let C be the set of $k \leqslant m$ classes c_i, $i = 1 \ldots, k$ corresponding to cycles of the size $|c_i| \geqslant 2$, which are uniquely represented by increasing sequences c_i of integres. The set C is empty when π is the identity. Otherwise C is non-empty and we claim that

$$\pi = \pi_{c_1} \pi_{c_2} \cdots \pi_{c_k} \tag{2.28}$$

To prove this, we have to show that the function on the left is equal to the function on the right. First, $j \in [n]$ is exactly in one of the equivalence classes. If it is in the equivalence class corresponding to ϵ, then it is in no c_i and therefore it is mapped by all π_{c_i} to itself, i.e. $\pi_{c_i}(j) = j$ for all $1 \leqslant i \leqslant k$. Therefore, $\pi_{c_1} \pi_{c_2} \cdots \pi_{c_k}(j) = j = \pi(j)$. If j is in a c_i, then $\pi_{c_i}(j) = \pi(j)$ and $\pi_{c_m}(j) = j$ for all $m \neq i$ Thus, $\pi_{c_1} \pi_{c_2} \cdots \pi_{c_k}(j) = \pi_{c_i}(j) = \pi(j)$. Notice that since $c_i \cap c_j = \emptyset$, we have here $\pi_{c_i} \pi_{c_j} = \pi_{c_j} \pi_{c_i}$ for all $1 \leqslant i, j \leqslant k$ and thus all π_{c_i} commute. We see that every permutation $\pi \neq \epsilon$ can be written as a unique composition of disjoint cycles. The term "disjoint" is related to the fact that the sequences representing the cycles are disjoint.

§ **5 Decomposition of a permutation into transpositions** Every permutation, which is not the identity, can be written as a composition of cycles. Every cycle can be written as a composition of transpositions. Therefore, every permutation, which is not the identity, can be written as a composition of transpositions. Since $\epsilon = \tau\, \tau$ for every transposition, ϵ can also be written as a composition of transpositions. Hence, we can say that any permutation can be written as a composition of transpositions.

There are many ways how to compose a cycle from transpositions and there are many ways how to write ϵ using transpositions, and therefore the decomposition of a permutation into transpositions is not unique.

§ **6 Sign of a permutation** We will now introduce another important concept related to permutations. *Sign*, $\operatorname{sgn}(\pi)$, of a permutation π is defined as

$$\operatorname{sgn}(\pi) = (-1)^{N(\pi)} \tag{2.29}$$

where $N(\pi)$ is equal to the number of *inversions* in π, i.e. the number of pairs $[i, j]$ such that $i, j \in [n]$, $i < j$ and $\pi(i) > \pi(j)$.

§ 7 Hierarchy of permutations Consider a partition [1] of $[n]$ into two subsets I, J of $[n]$, i.e. $[n] = I \cup J$ and $I \cap J = \emptyset$. Let $|I| = k$ and $|J| = m$. Thus $k + m = n$.

Let us next study the set $S_{[n]}$ of all permutations on $[n]$ and its relation to the sets S_I of all permutations of set I and S_J of all permutations of set J.

Let us use the following notation $\pi(I) = \{\pi(i) \,|\, i \in I\}$ for a permutation π and a set of integers I. We introduce the equivalence relation $\sim$ on $S_{[n]}$ by $\pi \sim \sigma$ for $\pi, \sigma \in S_{[n]}$ when $\pi(I) = \sigma(I)$. This equivalence relation partitions $S_{[n]}$ into the set E of (disjoint) equivalence classes.

As designed a permutation $\pi \in \Pi$ is a composition of three permutations, $\pi = \pi^I(\pi^J(\pi^{IJ}))$, where π^I permutes I, π^J permutes J and π^{IJ} maps I onto I_Π and J onto J_Π such that for all $i, j \in I$ $\pi^{IJ}(i) < \pi^{IJ}(j) \Leftrightarrow i < j$ and for all $i, j \in J$ $\pi^{IJ}(i) < \pi^{IJ}(j)$.

Let us see that $|E| = \binom{n}{k}$. A member Π of E contains all one-to-one functions from $[n]$ onto $[n]$ that map I onto a fixed set I_Π of size k chosen out of $[n]$. There are $\binom{n}{k}$ sets I_Π of size k. We further claim that $|\Pi| = k!\,(n-k)!$. An equivalence class Π contains all one-to-one functions that map I onto I_Π and J onto $J_\Pi = [n] \backslash I_\Pi$. There are $k!\,(n-k)!$ such functions. Thus, all equivalence classes in E contain the same number $k!\,(n-k)!$ of functions and we see that $\binom{n}{k}\,k!\,(n-k)! = n!$, which is the size of $S_{[n]}$.

exchanges some elements between I and J. Consider that every permutation π can be decomposed into a composition of disjoint cycles

$$\pi = (\pi_1^I \pi_2^I \cdots \pi_p^I)(\pi_1^{IJ} \pi_2^{IJ} \cdots \pi_q^{IJ})(\pi_1^J \pi_2^J \cdots \pi_r^J) \tag{2.30}$$

for some integers $p, q, r \geqslant 0$ and cycles π_i^I, $i = 1, \ldots, p$ that keep J fixed, cycles π_i^J, $i = 1, \ldots, q$ that keep I fixed, and cycles π_i^{IJ}, $i = 1, \ldots, r$ that map at least one element from I to J and at least one element from J to I.

Now, take a cycle π^{IJ}, which exchanges some elements between I and J. We claim that the number of exchanges between I and J induced by cycle π^{IJ} is always even. Let us write π^{IJ} as a sequence of k transpositions $\pi^{IJ} = \tau_{[i_1,i_2]}\tau_{[i_2,i_3]} \cdots \tau_{[i_{k-1},i_k]}$. Let us start with a singleton set $I_1 = \{i\}$. Then, there are exactly two transpositions $\tau_{[i-1,i]}, \tau_{[i,i+1]}$ from J to I and back. Now, let there be I_k with k exchanges and add one more element j to I_k to get I_{k+1}. Then, three possibilities may arrise: (1) $j-1$ and $j+1$ are in I_k and then two exchanges are removed, (2) exactly one of $j-1$, $j+1$ is in I_k and then on exchage is added and one removed, i.e. the number of echanges remains the same, (3) none of $j-1$, $j+1$ is in I_k and then two exhanges are added. In all cases, the number of exchanges is changed by an even number. Since the number of exchanges in I_1 is even, the number of exchanges in I_k is even for all integers k by the principle of mathematical induction [1].

$\pi_I(i) = \pi(i)$ for all $i \in I$ and $\pi_I(i) = i$ for $i \in J$ and $\pi_J(i) = \pi(i)$ for all $i \in J$ and $\pi_J(i) = i$ for $i \in I$. Functions π_I, π_J commute since I and J are disjoint. Clearly, we see that $\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi_I)\operatorname{sgn}(\pi_J)$.

2.2.2 Determinant

Let S_n be the set of all permutations on $[n]$ and $\mathtt{A}$ be an $n \times n$ matrix. Then, *determinant* $|\mathtt{A}|$ of $\mathtt{A}$ is defined by the formula

$$|\mathtt{A}| = \sum_{\pi \in S_n} \operatorname{sgn}(\pi)\, \mathtt{A}_{1,\pi(1)}\, \mathtt{A}_{2,\pi(2)} \cdots \mathtt{A}_{n,\pi(n)} \tag{2.31}$$

Notice that for every $\pi \in S_n$ and for $j \in [n]$ there is exactly one $i \in [n]$ such that $j = \pi(i)$. Hence

$$\{[1, \pi(1)], [2, \pi(2)], \ldots, [n, \pi(n)]\} = \{[\pi^{-1}(1), 1], [\pi^{-1}(2), 2], \ldots, [\pi^{-1}(n), n]\} \tag{2.32}$$

and since the multiplication of elements of $\mathtt{A}$ is commutative, we get

$$|\mathtt{A}| = \sum_{\pi \in S_n} \operatorname{sgn}(\pi)\, \mathtt{A}_{\pi^{-1}(1),1}\, \mathtt{A}_{\pi^{-1}(2),2} \cdots \mathtt{A}_{\pi^{-1}(n),n} \tag{2.33}$$

Next, let $\sigma \in S_n$, then $\{\pi\sigma \,|\, \forall \pi \in S_n\} = S_n$ since for every $\tau \in S_n$ there is $\pi = \tau\sigma^{-1} \in S_m$ and therefore $\tau = \pi\sigma \in \{\pi\sigma \,|\, \forall \pi \in S_n\}$. The other incluson is obvious. An analogical argument shows that $\{\sigma\pi \,|\, \forall \pi \in S_n\} = S_n$ too. Thus

$$\begin{aligned} & \sum_{\pi \in S_n} \operatorname{sgn}(\sigma\pi\sigma^{-1})\, \mathtt{A}_{1,\sigma\pi\sigma^{-1}(1)}\, \mathtt{A}_{2,\sigma\pi\sigma^{-1}(2)} \cdots \mathtt{A}_{n,\sigma\pi\sigma^{-1}(n)} && (2.34) \\ = & \sum_{\pi \in S_n} \operatorname{sgn}(\sigma)\operatorname{sgn}(\pi)\operatorname{sgn}(\sigma^{-1})\, \mathtt{A}_{\sigma^{-1}(1),\pi\sigma^{-1}(1)}\, \mathtt{A}_{\sigma^{-1}(2),\pi\sigma^{-1}(2)} \cdots \mathtt{A}_{\sigma^{-1}(n),\pi\sigma^{-1}(n)} \\ = & \sum_{\pi \in S_n} \operatorname{sgn}(\pi)\, \mathtt{A}_{\sigma^{-1}(1),\pi\sigma^{-1}(1)}\, \mathtt{A}_{\sigma^{-1}(2),\pi\sigma^{-1}(2)} \cdots \mathtt{A}_{\sigma^{-1}(n),\pi\sigma^{-1}(n)} && (2.35) \\ = & \sum_{\pi \in S_n} \operatorname{sgn}(\pi)\, \mathtt{A}_{1,\pi(1)}\, \mathtt{A}_{2,\pi(2)} \cdots \mathtt{A}_{n,\pi(n)} = |\mathtt{A}| && (2.36) \end{aligned}$$

Let us next define a submatrix of $\mathtt{A}$ and find its determinant. Consider $k \leqslant n$ and two one-to-one *monotonic* functions $\rho, \nu\colon [k] \rightarrow [n]$, $i < j \Rightarrow \rho(i) < \rho(j), \nu(i) < \nu(j)$. We define $k \times k$ submatrix $\mathtt{A}^{\rho,\nu}$ of an $n \times n$ matrix $\mathtt{A}$ by

$$\mathtt{A}^{\rho,\nu}_{i,j} = \mathtt{A}_{\rho(i),\nu(j)} \quad \text{for} \quad i, j \in [k] \tag{2.37}$$

We get the determinant of $\mathtt{A}^{\rho,\nu}$ as follows

$$\begin{aligned} |\mathtt{A}^{\rho,\nu}| &= \sum_{\pi \in S_k} \operatorname{sgn}(\pi)\, \mathtt{A}^{\rho,\nu}_{1,\pi(1)}\, \mathtt{A}^{\rho,\nu}_{2,\pi(2)} \cdots \mathtt{A}^{\rho,\nu}_{k,\pi(k)} && (2.38) \\ &= \sum_{\pi \in S_k} \operatorname{sgn}(\pi)\, \mathtt{A}_{\rho(1),\nu(\pi(1))}\, \mathtt{A}_{\rho(2),\nu(\pi(2))} \cdots \mathtt{A}_{\rho(k),\nu(\pi(k))} && (2.39) \end{aligned}$$

Let us next split the rows of the matrix $\mathtt{A}$ into two groups of k and m rows and find the relationship between $|\mathtt{A}|$ and the determinants of certain $k \times k$ and $m \times m$ submatrices of $\mathtt{A}$. Take $1 \leqslant k, m \leqslant n$ such that $k + m = n$ and define a one-to-one function $\rho\colon [m] \rightarrow [k+1, n] = \{k+1, \ldots, n\}$, by $\rho(i) = k + i$. Next, let $\Omega \subseteq \exp[n]$ be the set of all subsets of $[n]$ of size k. Let $\omega \in \Omega$. Then, there is exactly one one-to-one monotonic function φ_ω from $[k]$ onto ω since $[k]$ and ω are finite sets of integers of the same size. Let $\overline{\omega} = [n] \backslash \omega$. Then, there is exactly one one-to-one monotonic function $\varphi_{\overline{\omega}}$ from $[k+1, n]$ onto $\overline{\omega}$. Let further there be $\pi_k \in S_k$ and $\pi_m \in S_m$. With the notation introduced above, we are getting a version of the generalized Laplace expansion of the determinant [12, 13]

$$|\mathtt{A}| = \sum_{\omega \in \Omega} \left(\prod_{i \in [k], j \in [k+1,n]} \operatorname{sgn}(\varphi_{\overline{\omega}}(j) - \varphi_\omega(i)) \right) |\mathtt{A}^{\epsilon,\varphi_\omega}| \left|\mathtt{A}^{\rho,\varphi_{\overline{\omega}}(\rho)}\right| \tag{2.40}$$

2.3 Vector product

Let us look at an interesting mapping from $\mathbb{R}^3 \times \mathbb{R}^3$ to $\mathbb{R}^3$, the *vector product* in $\mathbb{R}^3$ [7] (which it also often called the cross product [5]). Vector product has interesting geometrical properties but we shall motivate it by its connection to systems of linear equations.

§ 1 Vector product Assume two linearly independent coordinate vectors $\vec{x} = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix}^\top$ and $\vec{y} = \begin{bmatrix} y_1 & y_2 & y_3 \end{bmatrix}^\top$ in $\mathbb{R}^3$. The following system of linear equations

$$\begin{bmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{bmatrix} \vec{z} = 0 \tag{2.41}$$

has a one-dimensional subspace V of solutions in $\mathbb{R}^3$. The solutions can be written as multiples of one non-zero vector $\vec{w}$, the basis of V, i.e.

$$\vec{z} = \lambda\, \vec{w}, \quad \lambda \in \mathbb{R} \tag{2.42}$$

Let us see how we can construct $\vec{w}$ in a convenient way from vectors $\vec{x}$, $\vec{y}$.

Consider determinants of two matrices constructed from the matrix of the system (2.41) by adjoining its first, resp. second, row to the matrix of the system (2.41)

$$\left|\begin{bmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ x_1 & x_2 & x_3 \end{bmatrix}\right| = 0 \qquad \left|\begin{bmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ y_1 & y_2 & y_3 \end{bmatrix}\right| = 0 \tag{2.43}$$

which gives

$$x_1\,(x_2\,y_3 - x_3\,y_2) + x_2\,(x_3\,y_1 - x_1\,y_3) + x_3\,(x_1\,y_2 - x_2\,y_1) = 0 \tag{2.44}$$

$$y_1\,(x_2\,y_3 - x_3\,y_2) + y_2\,(x_3\,y_1 - x_1\,y_3) + y_3\,(x_1\,y_2 - x_2\,y_1) = 0 \tag{2.45}$$

and can be rewritten as

$$\begin{bmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{bmatrix} \begin{bmatrix} x_2\,y_3 - x_3\,y_2 \\ -x_1\,y_3 + x_3\,y_1 \\ x_1\,y_2 - x_2\,y_1 \end{bmatrix} = 0 \tag{2.46}$$

We see that vector

$$\vec{w} = \begin{bmatrix} x_2\,y_3 - x_3\,y_2 \\ -x_1\,y_3 + x_3\,y_1 \\ x_1\,y_2 - x_2\,y_1 \end{bmatrix} \tag{2.47}$$

solves Equation 2.41.

Notice that elements of $\vec{w}$ are the three two by two minors of the matrix of the system (2.41). The rank of the matrix is two, which means that at least one of the minors is non-zero, and hence $\vec{w}$ is also non-zero. We see that $\vec{w}$ is a basic vector of V. Formula 2.47 is known as the *vector product* in $\mathbb{R}^3$ and $\vec{w}$ is also often denoted by $\vec{x} \times \vec{y}$.

§ 2 Vector product under the change of basis Let us next study the behavior of the vector product under the change of basis in $\mathbb{R}^3$. Let us have two bases β, β' in $\mathbb{R}^3$ and two vectors $\vec{x}$, $\vec{y}$ with coordinates $\vec{x}_\beta = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix}^\top$, $\vec{y}_\beta = \begin{bmatrix} y_1 & y_2 & y_3 \end{bmatrix}^\top$ and $\vec{x}_{\beta'} = \begin{bmatrix} x'_1 & x'_2 & x'_3 \end{bmatrix}^\top$, $\vec{y}_\beta = \begin{bmatrix} y'_1 & y'_2 & y'_3 \end{bmatrix}^\top$. We introduce

$$\vec{x}_\beta \times \vec{y}_\beta = \begin{bmatrix} x_2\,y_3 - x_3\,y_2 \\ -x_1\,y_3 + x_3\,y_1 \\ x_1\,y_2 - x_2\,y_1 \end{bmatrix} \qquad \vec{x}_{\beta'} \times \vec{y}_{\beta'} = \begin{bmatrix} x'_2 y'_3 - x'_3 y'_2 \\ -x'_1 y'_3 + x'_3 y'_1 \\ x'_1 y'_2 - x'_2 y'_1 \end{bmatrix} \tag{2.48}$$

To find the relationship between $\vec{x}_\beta \times \vec{y}_\beta$ and $\vec{x}_{\beta'} \times \vec{y}_{\beta'}$, we will use the following fact. For every three vectors $\vec{x} = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix}^\top$, $\vec{y} = \begin{bmatrix} y_1 & y_2 & y_3 \end{bmatrix}^\top$, $\vec{z} = \begin{bmatrix} z_1 & z_2 & z_3 \end{bmatrix}^\top$ in $\mathbb{R}^3$ there holds

$$\vec{z}^\top(\vec{x} \times \vec{y}) = \begin{bmatrix} z_1 & z_2 & z_3 \end{bmatrix} \begin{bmatrix} x_2\,y_3 - x_3\,y_2 \\ -x_1\,y_3 + x_3\,y_1 \\ x_1\,y_2 - x_2\,y_1 \end{bmatrix} = \left|\begin{bmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{bmatrix}\right| = \left|\begin{bmatrix} \vec{x}^\top \\ \vec{y}^\top \\ \vec{z}^\top \end{bmatrix}\right| \tag{2.49}$$

We can write

$$
\begin{aligned}
\vec{x}_{\beta'} \times \vec{y}_{\beta'} &= \begin{bmatrix} [1\,0\,0]\,(\vec{x}_{\beta'} \times \vec{y}_{\beta'}) \\ [0\,1\,0]\,(\vec{x}_{\beta'} \times \vec{y}_{\beta'}) \\ [0\,0\,1]\,(\vec{x}_{\beta'} \times \vec{y}_{\beta'}) \end{bmatrix} = \begin{bmatrix} \left|\begin{bmatrix} \vec{x}_{\beta'}^\top \\ \vec{y}_{\beta'}^\top \\ 1\,0\,0 \end{bmatrix}\right| & \left|\begin{bmatrix} \vec{x}_{\beta'}^\top \\ \vec{y}_{\beta'}^\top \\ 0\,1\,0 \end{bmatrix}\right| & \left|\begin{bmatrix} \vec{x}_{\beta'}^\top \\ \vec{y}_{\beta'}^\top \\ 0\,0\,1 \end{bmatrix}\right| \end{bmatrix}^\top \\
&= \begin{bmatrix} \left|\begin{bmatrix} \vec{x}_{\beta}^\top \mathtt{A}^\top \\ \vec{y}_{\beta}^\top \mathtt{A}^\top \\ 1\,0\,0 \end{bmatrix}\right| & \left|\begin{bmatrix} \vec{x}_{\beta}^\top \mathtt{A}^\top \\ \vec{y}_{\beta}^\top \mathtt{A}^\top \\ 0\,1\,0 \end{bmatrix}\right| & \left|\begin{bmatrix} \vec{x}_{\beta}^\top \mathtt{A}^\top \\ \vec{y}_{\beta}^\top \mathtt{A}^\top \\ 0\,0\,1 \end{bmatrix}\right| \end{bmatrix}^\top \\
&= \begin{bmatrix} \left|\begin{bmatrix} \vec{x}_{\beta}^\top \\ \vec{y}_{\beta}^\top \\ [1\,0\,0]\;\mathtt{A}^{-\top} \end{bmatrix} \mathtt{A}^\top\right| & \left|\begin{bmatrix} \vec{x}_{\beta}^\top \\ \vec{y}_{\beta}^\top \\ [0\,1\,0]\;\mathtt{A}^{-\top} \end{bmatrix} \mathtt{A}^\top\right| & \left|\begin{bmatrix} \vec{x}_{\beta}^\top \\ \vec{y}_{\beta}^\top \\ [0\,0\,1]\;\mathtt{A}^{-\top} \end{bmatrix} \mathtt{A}^\top\right| \end{bmatrix}^\top \\
&= \begin{bmatrix} [1\,0\,0]\,\mathtt{A}^{-\top}(\vec{x}_\beta \times \vec{y}_\beta) \\ [0\,1\,0]\,\mathtt{A}^{-\top}(\vec{x}_\beta \times \vec{y}_\beta) \\ [0\,0\,1]\,\mathtt{A}^{-\top}(\vec{x}_\beta \times \vec{y}_\beta) \end{bmatrix} |\mathtt{A}^\top| \\
&= \frac{\mathtt{A}^{-\top}}{|\mathtt{A}^{-\top}|}\,(\vec{x}_\beta \times \vec{y}_\beta)
\end{aligned}
\tag{2.50}
$$

§ **3 Vector product as a linear mapping** It is interesting to see that for all $\vec{x}, \vec{y} \in \mathbb{R}^3$ there holds

$$
\vec{x} \times \vec{y} = \begin{bmatrix} x_2\,y_3 - x_3\,y_2 \\ -x_1\,y_3 + x_3\,y_1 \\ x_1\,y_2 - x_2\,y_1 \end{bmatrix} = \begin{bmatrix} 0 & -x_3 & x_2 \\ x_3 & 0 & -x_1 \\ -x_2 & x_1 & 0 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}
\tag{2.51}
$$

and thus we can introduce matrix

$$
[\vec{x}]_\times = \begin{bmatrix} 0 & -x_3 & x_2 \\ x_3 & 0 & -x_1 \\ -x_2 & x_1 & 0 \end{bmatrix}
\tag{2.52}
$$

and write

$$
\vec{x} \times \vec{y} = [\vec{x}]_\times\,\vec{y}
\tag{2.53}
$$

Notice also that $[\vec{x}]_\times^\top = -\,[\vec{x}]_\times$ and therefore

$$
(\vec{x} \times \vec{y})^\top = ([\vec{x}]_\times\,\vec{y})^\top = -\vec{y}^\top\,[\vec{x}]_\times
\tag{2.54}
$$

The result of §2 can also be written in the formalism of this paragraph. We can write for every $\vec{x}, \vec{y} \in \mathbb{R}^3$

$$
\left[\mathtt{A}\,\vec{x}_\beta\right]_\times \mathtt{A}\,\vec{y}_\beta = (\mathtt{A}\,\vec{x}_\beta) \times (\mathtt{A}\,\vec{y}_\beta) = \frac{\mathtt{A}^{-\top}}{|\mathtt{A}^{-\top}|}\,(\vec{x}_\beta \times \vec{y}_\beta) = \frac{\mathtt{A}^{-\top}}{|\mathtt{A}^{-\top}|}\,\left[\vec{x}_\beta\right]_\times \vec{y}_\beta
\tag{2.55}
$$

and hence we get for every $\vec{x} \in \mathbb{R}^3$

$$
\left[\mathtt{A}\,\vec{x}_\beta\right]_\times \mathtt{A} = \frac{\mathtt{A}^{-\top}}{|\mathtt{A}^{-\top}|}\,\left[\vec{x}_\beta\right]_\times
\tag{2.56}
$$

2.4 Dual space and dual basis

Let us start with a three-dimensional linear space L over scalars S and consider the set $L^\star$ of all linear functions $f\colon L \to S$, i.e. the functions on L for which the following holds true

$$
f(a\,\vec{x} + b\,\vec{y}) = a\,f(\vec{x}) + b\,f(\vec{y})
\tag{2.57}
$$

for all $a, b \in S$ and all $\vec{x}, \vec{y} \in L$.

Let us next define the addition $+^\star : L^\star \times L^\star \rightarrow L^\star$ of linear functions $f, g \in L^\star$ and the multiplication $\cdot^\star : S \times L^\star \rightarrow L^\star$ of a linear function $f \in L^\star$ by a scalar $a \in S$ such that

$$\begin{aligned} (f +^\star g)(\vec{x}) &= f(\vec{x}) + g(\vec{x}) & (2.58)\\ (a \cdot^\star f)(\vec{x}) &= a\, f(\vec{x}) & (2.59) \end{aligned}$$

holds true for all $a \in S$ and for all $\vec{x} \in L$. One can verify that $(L^\star, +^\star, \cdot^\star)$ over $(S, +,)$ is itself a linear space [4, 7, 6]. It makes therefore a good sense to use arrows above symbols for linear functions, e.g. $\vec{f}$ instead of f.

The linear space $L^\star$ is derived from, and naturally connected to, the linear space L and hence deserves a special name. Linear space $L^\star$ is called [4] the *dual (linear) space* to L.

Now, consider a basis $\beta = [\vec{b}_1, \vec{b}_2, \vec{b}_3]$ of L. We will construct a basis $\beta^\star$ of $L^\star$, in a certain natural and useful way. Let us take three linear functions $\vec{b}_1^\star, \vec{b}_2^\star, \vec{b}_3^\star \in L^\star$ such that

$$\begin{matrix} \vec{b}_1^\star(\vec{b}_1) = 1 & \vec{b}_1^\star(\vec{b}_2) = 0 & \vec{b}_1^\star(\vec{b}_3) = 0 \\ \vec{b}_2^\star(\vec{b}_1) = 0 & \vec{b}_2^\star(\vec{b}_2) = 1 & \vec{b}_2^\star(\vec{b}_3) = 0 \\ \vec{b}_3^\star(\vec{b}_1) = 0 & \vec{b}_3^\star(\vec{b}_2) = 0 & \vec{b}_3^\star(\vec{b}_3) = 1 \end{matrix} \qquad (2.60)$$

where 0 and 1 are the zero and the unit element of S, respectively. First of all, one has to verify [4] that such an assignment is possible with linear functions over L. Secondly one can show [4] that functions $\vec{b}_1^\star, \vec{b}_2^\star, \vec{b}_3^\star$ are determined by this assignment uniquely on all vectors of L. Finally, one can observe [4] that the triple $\beta^\star = [\vec{b}_1^\star, \vec{b}_2^\star, \vec{b}_3^\star]$ forms an (ordered) basis of $\vec{L}$. The basis $\beta^\star$ is called the *dual basis* of $L^\star$, i.e. it is the basis of $L^\star$, which is related in a special (dual) way to the basis β of L.

§ **1 Evaluating linear functions** Consider a vector $\vec{x} \in L$ with coordinates $\vec{x}_\beta = [x_1, x_2, x_3]^\top$ w.r.t. a basis $\beta = [\vec{b}_1, \vec{b}_2, \vec{b}_3]$ and a linear function $\vec{h} \in L^\star$ with coordinates $\vec{h}_{\beta^\star} = [h_1, h_2, h_3]^\top$ w.r.t. the dual basis $\beta^\star = [\vec{b}_1^\star, \vec{b}_2^\star, \vec{b}_3^\star]$. The value $\vec{h}(\vec{x}) \in S$ is obtained from the coordinates $\vec{x}_\beta$ and $\vec{h}_{\beta^\star}$ as

$$\begin{aligned} \vec{h}(\vec{x}) &= \vec{h}(x_1\, \vec{b}_1 + x_2\, \vec{b}_2 + x_3\, \vec{b}_3) & (2.61)\\ &= (h_1\, \vec{b}_1^\star + h_2\, \vec{b}_2^\star + h_3\, \vec{b}_3^\star)(x_1\, \vec{b}_1 + x_2\, \vec{b}_2 + x_3\, \vec{b}_3) & (2.62)\\ &= h_1\, \vec{b}_1^\star(\vec{b}_1)\, x_1 + h_1\, \vec{b}_1^\star(\vec{b}_2)\, x_2 + h_1\, \vec{b}_1^\star(\vec{b}_3)\, x_3 \\ & +h_2\, \vec{b}_2^\star(\vec{b}_1)\, x_1 + h_2\, \vec{b}_2^\star(\vec{b}_2)\, x_2 + h_2\, \vec{b}_2^\star(\vec{b}_3)\, x_3 & (2.63)\\ & +h_3\, \vec{b}_3^\star(\vec{b}_1)\, x_1 + h_3\, \vec{b}_3^\star(\vec{b}_2)\, x_2 + h_3\, \vec{b}_3^\star(\vec{b}_3)\, x_3 \\ &= \begin{bmatrix} h_1 & h_2 & h_3 \end{bmatrix} \begin{bmatrix} \vec{b}_1^\star(\vec{b}_1) & \vec{b}_1^\star(\vec{b}_2) & \vec{b}_1^\star(\vec{b}_3) \\ \vec{b}_2^\star(\vec{b}_1) & \vec{b}_2^\star(\vec{b}_2) & \vec{b}_2^\star(\vec{b}_3) \\ \vec{b}_3^\star(\vec{b}_1) & \vec{b}_3^\star(\vec{b}_2) & \vec{b}_3^\star(\vec{b}_3) \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} & (2.64)\\ &= \begin{bmatrix} h_1 & h_2 & h_3 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} & (2.65)\\ &= \begin{bmatrix} h_1, h_2, h_3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} & (2.66)\\ &= \vec{h}_{\beta^\star}^\top\, \vec{x}_\beta & (2.67) \end{aligned}$$

The value of $\vec{h} \in L^\star$ on $\vec{x} \in L$ is obtained by multiplying $\vec{x}_\beta$ by the transpose of $\vec{h}_{\beta^\star}$ from the left.

Notice that the middle matrix on the right in Equation 2.64 evaluates into the identity. This is the consequence of using the pair of a basis and its dual basis. The formula 2.67 can be generalized to the situation when bases are not dual by evaluating the middle matrix accordingly. In general

$$\vec{h}(\vec{x}) = \vec{h}_{\bar{\beta}}^{\top} \, [\vec{\bar{b}}_i(\vec{b}_j)] \, \vec{x}_\beta \tag{2.68}$$

where matrix $[\vec{\bar{b}}_i(\vec{b}_j)]$ is constructed from the respective bases β, $\bar{\beta}$ of L and $L^\star$.

§ 2 Changing the basis in a linear space and in its dual Let us now look at what happens with coordinates of vectors of $L^\star$ when passing from the dual basis $\beta^\star$ to the dual basis $\beta'^\star$ induced by passing from a basis β to a basis β' in L. Consider vector $\vec{x} \in L$ and a linear function $\vec{h} \in L^\star$ and their coordinates $\vec{x}_\beta$, $\vec{x}_{\beta'}$ and $\vec{h}_{\beta^\star}$, $\vec{h}_{\beta'^\star}$ w.r.t. the respective bases. Introduce further matrix $\mathtt{A}$ transforming coordinates of vectors in L as

$$\vec{x}_{\beta'} = \mathtt{A}\,\vec{x}_\beta \tag{2.69}$$

when passing from β to β'.

Basis $\beta^\star$ is the dual basis to β and basis $\beta'^\star$ is the dual basis to β' and therefore

$$\vec{h}_{\beta^\star}^{\top}\,\vec{x}_\beta = \vec{h}(\vec{x}) = \vec{h}_{\beta'^\star}^{\top}\,\vec{x}_{\beta'} \tag{2.70}$$

for all $\vec{x} \in L$ and all $\vec{h} \in L^\star$. Hence

$$\vec{h}_{\beta^\star}^{\top}\,\vec{x}_\beta = \vec{h}_{\beta'^\star}^{\top}\,\mathtt{A}\,\vec{x}_\beta \tag{2.71}$$

for all $\vec{x} \in L$ and therefore

$$\vec{h}_{\beta^\star}^{\top} = \vec{h}_{\beta'^\star}^{\top}\,\mathtt{A} \tag{2.72}$$

or equivalently

$$\vec{h}_{\beta^\star} = \mathtt{A}^{\top}\vec{h}_{\beta'^\star} \tag{2.73}$$

Let us now see what is the meaning of the rows of matrix $\mathtt{A}$. It becomes clear from Equation 2.72 that the columns of matrix $\mathtt{A}^\top$ can be viewed as vectors of coordinates of basic vectors of $\beta'^\star = [\vec{b}_1'^\star, \vec{b}_2'^\star, \vec{b}_3'^\star]$ in the basis $\beta^\star = [\vec{b}_1^\star, \vec{b}_2^\star, \vec{b}_3^\star]$ and therefore

$$\mathtt{A} \;=\; \begin{bmatrix} \vec{b}_{1\beta^\star}'^{\star\top} \\ \vec{b}_{2\beta^\star}'^{\star\top} \\ \vec{b}_{3\beta^\star}'^{\star\top} \end{bmatrix} \tag{2.74}$$

which means that the rows of $\mathtt{A}$ are coordinates of the dual basis of the primed dual space in the dual basis of the non-primed dual space.

Finally notice that we can also write

$$\vec{h}_{\beta'^\star} = \mathtt{A}^{-\top}\vec{h}_{\beta^\star} \tag{2.75}$$

which is formally identical with Equation 2.15.

§ 3 When do coordinates transform the same way in a basis and in its dual basis It is natural to ask when it happens that the coordinates of linear functions in $L^\star$ w.r.t. the dual basis $\beta^\star$ transform the same way as the coordinates of vectors of L w.r.t. the original basis β, i.e.

$$\vec{x}_{\beta'} \;=\; \mathtt{A}\,\vec{x}_\beta \tag{2.76}$$

$$\vec{h}_{\beta'^\star} \;=\; \mathtt{A}\,\vec{h}_{\beta^\star} \tag{2.77}$$

for all $\vec{x} \in L$ and all $\vec{h} \in L^\star$. Considering Equation 2.75, we get

$$\begin{aligned} \mathtt{A} &= \mathtt{A}^{-\top} && (2.78)\\ \mathtt{A}^\top \mathtt{A} &= \mathtt{I} && (2.79) \end{aligned}$$

Notice that this is, for instance, satisfied when A is a rotation [5]. In such a case, one often does not anymore distinguish between vectors of L and $L^\star$ because they behave the same way and it is hence possible to represent linear functions from $L^\star$ by vectors of L.

§4 Coordinates of the basis dual to a general basis We denote the standard basis in $\mathbb{R}^3$ by σ and its dual (standard) basis in $\mathbb{R}^{3\star}$ by $\sigma^\star$. Now, we can further establish another basis $\gamma = \begin{bmatrix}\vec{c}_1 & \vec{c}_2 & \vec{c}_3\end{bmatrix}$ in $\mathbb{R}^3$ and its dual basis $\gamma^\star = \begin{bmatrix}\vec{c}_1^{\,\star} & \vec{c}_2^{\,\star} & \vec{c}_3^{\,\star}\end{bmatrix}$ in $\mathbb{R}^{3\star}$. We would like to find the coordinates $\gamma^\star_{\sigma^\star} = \begin{bmatrix}\vec{c}^{\,\star}_{1\sigma^\star} & \vec{c}^{\,\star}_{2\sigma^\star} & \vec{c}^{\,\star}_{3\sigma^\star}\end{bmatrix}$ of vectors of $\gamma^\star$ w.r.t. $\sigma^\star$ as a function of coordinates $\gamma_\sigma = \begin{bmatrix}\vec{c}_{1\sigma} & \vec{c}_{2\sigma} & \vec{c}_{3\sigma}\end{bmatrix}$ of vectors of γ w.r.t. σ.

Considering Equations 2.60 and 2.67, we are getting

$$\vec{c}^{\,\star\top}_{i\sigma^\star}\vec{c}_{j\sigma} = \begin{cases} 1 \text{ if } i = j \\ 0 \text{ if } i \neq j \end{cases} \quad \text{for } i,j = 1,2,3 \tag{2.80}$$

which can be rewritten in a matrix form as

$$\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix} = \begin{bmatrix}\vec{c}^{\,\star\top}_{1\sigma^\star}\\ \vec{c}^{\,\star\top}_{2\sigma^\star}\\ \vec{c}^{\,\star\top}_{3\sigma^\star}\end{bmatrix}\begin{bmatrix}\vec{c}_{1\sigma} & \vec{c}_{2\sigma} & \vec{c}_{3\sigma}\end{bmatrix} = \gamma^{\star\top}_{\sigma^\star}\,\gamma_\sigma \tag{2.81}$$

and therefore

$$\gamma^\star_{\sigma^\star} = \gamma_\sigma^{-\top} \tag{2.82}$$

§5 Remark on higher dimensions We have introduced the dual space and the dual basis in a three-dimensional linear space. The definition of the dual space is exactly the same for any linear space. The definition of the dual basis is the same for all finite-dimensional linear spaces [4]. For any n-dimensional linear space L and its basis β, we get the corresponding n-dimensional dual space $L^\star$ with the dual basis $\beta^\star$.

2.5 Operations with matrices & tensors

Matrices are a powerful tool which can be used in many ways. Here we review a few useful rules for matrix manipulation. The rules are often studied in multi-linear algebra and tensor calculus. We shall not review the theory of multi-linear algebra but will look at the rules from a phenomenological point of view. They are useful identities making an effective manipulation and concise notation possible.

§1 Kronecker product Let A be a $k \times l$ matrix and B be a $m \times n$ matrix

$$\mathtt{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1l}\\ a_{21} & a_{22} & \cdots & a_{2l}\\ \vdots & \vdots & \ddots & \vdots\\ a_{k1} & a_{k2} & \cdots & a_{kl}\end{bmatrix} \in \mathbb{R}^{k\times l} \quad \text{and} \quad \mathtt{B} \in \mathbb{R}^{m\times n} \tag{2.83}$$

then $k\,m \times l\,n$ matrix

$$\mathtt{C} = \mathtt{A} \otimes \mathtt{B} = \begin{bmatrix} a_{11}\,\mathtt{B} & a_{12}\,\mathtt{B} & \cdots & a_{1l}\,\mathtt{B}\\ a_{21}\,\mathtt{B} & a_{22}\,\mathtt{B} & \cdots & a_{2l}\,\mathtt{B}\\ \vdots & \vdots & \ddots & \vdots\\ a_{k1}\,\mathtt{B} & a_{k2}\,\mathtt{B} & \cdots & a_{kl}\,\mathtt{B}\end{bmatrix} \tag{2.84}$$

is the matrix of the *Kronecker product of matrices* $\mathtt{A}$, $\mathtt{B}$ (in this order).

Notice that this product is associative, i.e. $(\mathtt{A} \otimes \mathtt{B}) \otimes \mathtt{C} = \mathtt{A} \otimes (\mathtt{B} \otimes \mathtt{C})$, but it is not commutative, i.e. $\mathtt{A} \otimes \mathtt{B} \neq \mathtt{B} \otimes \mathtt{A}$ in general. There holds a useful identity $(\mathtt{A} \otimes \mathtt{B})^\top = \mathtt{A}^\top \otimes \mathtt{B}^\top$.

§ 2 Matrix vectorization Let $\mathtt{A}$ be an $m \times n$ matrix

$$\mathtt{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \in \mathbb{R}^{m \times n} \tag{2.85}$$

We define operator $v(.)\colon \mathbb{R}^{m \times n} \to \mathbb{R}^{m\,n}$ which reshapes an $m \times n$ matrix $\mathtt{A}$ into a $m\,n \times 1$ matrix (i.e. into a vector) by stacking columns of $\mathtt{A}$ one above another

$$v(\mathtt{A}) = \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \\ a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \\ a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{bmatrix} = \tag{2.86}$$

Let us study the relationship between $v(\mathtt{A})$ and $v(\mathtt{A}^\top)$. We see that vector $v(\mathtt{A}^\top)$ contains permuted elements of $v(\mathtt{A})$ and therefore we can construct permutation matrices [5] $\top_{m \times n}$ and $\top_{n \times m}$ such that

$$\begin{aligned} v(\mathtt{A}^\top) &= \top_{m \times n}\, v(\mathtt{A}) \\ v(\mathtt{A}) &= \top_{n \times m}\, v(\mathtt{A}^\top) \end{aligned}$$

We see that there holds

$$\top_{n \times m} \top_{m \times n}\, v(\mathtt{A}) = \top_{n \times m}\, v(\mathtt{A}^\top) = v(\mathtt{A}) \tag{2.87}$$

for every $m \times n$ matrix $\mathtt{A}$. Hence

$$\top_{n \times m} = \top_{m \times n}^{-1} \tag{2.88}$$

Consider a permutation $\top$. It has exactly one unit element in each row and in each column. Consider the i-th row with 1 in the j-th column. This row sends the j-th element of an input vector to the i-th element of the output vector. The i-the column of the transpose of $\top$ has 1 in the j-th row. It is the only non-zero element in that row and therefore the j-th row of $\top^\top$ sends the i-th element of an input vector to the j-th element of the output vector. We see that $\top^\top$ is the inverse of $\top$, i.e. permutation matrices are orthogonal. We see that

$$\top_{m \times n}^{-1} = \top_{m \times n}^\top \tag{2.89}$$

and hence conclude

$$\top_{n \times m} = \top_{m \times n}^\top \tag{2.90}$$

We also write $v(\mathtt{A}) = \top_{m \times n}^\top\, v(\mathtt{A}^\top)$.

§ 3 From matrix equations to linear systems Kronecker product of matrices and matrix vectorization can be used to manipulate matrix equations in order to get systems of linear equations in the standard matrix form $\mathtt{A}\,\mathtt{x} = \mathtt{b}$. Consider, for instance, matrix equation

$$\mathtt{A}\,\mathtt{X}\,\mathtt{B} = \mathtt{C} \tag{2.91}$$

with matrices $\mathtt{A} \in \mathbb{R}^{m\times k}$, $\mathtt{X} \in \mathbb{R}^{k\times l}$, $\mathtt{B} \in \mathbb{R}^{l\times n}$, $\mathtt{C} \in \mathbb{R}^{m\times n}$. It can be verified by direct computation that

$$v(\mathtt{A}\,\mathtt{X}\,\mathtt{B}) \;=\; (\mathtt{B}^\top \otimes \mathtt{A})\,v(\mathtt{X}) \tag{2.92}$$

This is useful when matrices $\mathtt{A}$, $\mathtt{B}$ and $\mathtt{C}$ are known and we use Equation 2.91 to compute $\mathtt{X}$. Notice that matrix Equation 2.91 is actually equivalent to $m\,n$ scalar linear equations in $k\,l$ unknown elements of $\mathtt{X}$. Therefore, we should be able to write it in the standard form, e.g., as

$$\mathtt{M}\,v(\mathtt{X}) = v(\mathtt{C}) \tag{2.93}$$

with some $\mathtt{M} \in \mathbb{R}^{(m\,n)\times(k\,l)}$. We can use Equation 2.92 to get $\mathtt{M} = \mathtt{B}^\top \otimes \mathtt{A}$ which yields the linear system

$$\begin{aligned} v(\mathtt{A}\,\mathtt{X}\,\mathtt{B}) &= v(\mathtt{C}) && (2.94)\\ (\mathtt{B}^\top \otimes \mathtt{A})\,v(\mathtt{X}) &= v(\mathtt{C}) && (2.95) \end{aligned}$$

for unknown $v(\mathtt{X})$, which is in the standard form.

Let us next consider two variations of Equation 2.91. First consider matrix equation

$$\mathtt{A}\,\mathtt{X}\,\mathtt{B} = \mathtt{X} \tag{2.96}$$

Here unknowns $\mathtt{X}$ appear on both sides but we are still getting a linear system of the form

$$(\mathtt{B}^\top \otimes \mathtt{A} - \mathtt{I})\,v(\mathtt{X}) = \mathbb{0} \tag{2.97}$$

where $\mathtt{I}$ is the $(m\,n) \times (k\,l)$ identity matrix.

Next, we add yet another constraints: $\mathtt{X}^\top = \mathtt{X}$, i.e. matrix $\mathtt{X}$ is symmetric, to get

$$\mathtt{A}\,\mathtt{X}\,\mathtt{B} = \mathtt{X} \quad \text{and} \quad \mathtt{X}^\top = \mathtt{X} \tag{2.98}$$

which can be rewritten in the vectorized form as

$$(\mathtt{B}^\top \otimes \mathtt{A} - \mathtt{I})\,v(\mathtt{X}) = \mathbb{0} \quad \text{and} \quad (\top_{m\times n} - \mathtt{I})\,v(\mathtt{X}) = \mathbb{0} \tag{2.99}$$

and combined it into a single linear system

$$\begin{bmatrix} \top_{m\times n} - \mathtt{I} \\ \mathtt{B}^\top \otimes \mathtt{A} - \mathtt{I} \end{bmatrix} v(\mathtt{X}) = \mathbb{0} \tag{2.100}$$

3 Algebraic geometry for solving polynomial equations

We will explain some elements of algebraic geometry in order to understand how to solve systems of polynomial (algebraic) equations in several unknowns that have a finite number of solutions. We will follow the nomenclature in [2]. See [2] for more complete exposition of algebraic geometry and [14] for more on how to solve systems of polynomial equations in several unknowns.

3.1 Polynomials

We will consider polynomials in n unknowns $x_1, x_2, \ldots, x_n$ with rational coefficients $a_0, a_1, \ldots, a_n$. Polynomials are linear combinations of a finite number of *monomials* $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ where non-negative integers $\alpha_i \in \mathbb{Z}_{\geqslant 0}$ are exponents. To simplify the notation, we will write x^α instead of $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ an for n-tuple $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ of exponents. N-tuple α is called the *multidergree* of monomial x^α. For instance, for $\alpha = (2, 0, 1)$ we get $x^\alpha = x_1^2 x_2^0 x_3^1 = x_1^2 x_3$. We define the *total degree d* of a non-zero monomial with exponent $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ as $d = \alpha_1 + \alpha_2 + \cdots + \alpha_n$. Hence, $x^{(2,0,1)}$ has total degree equal to three. The total degree, $\deg(f)$, of a polynomial f is the maximum of the total degrees of its monomials. The zero polynomial has no degree.

With this notation, polynomials with rational coefficients can be written in the form

$$f = \sum_\alpha a_\alpha x^\alpha, \quad a_\alpha \in \mathbb{Q} \tag{3.1}$$

where the sum is over a finite set of n-tuples $\alpha \in \mathbb{Z}^n_{\geqslant 0}$. The set of all polynomials in unknowns $x_1, x_2, \ldots, x_n$ with rational coefficients will be denoted by $\mathbb{Q}[x_1, x_2, \ldots, x_n]$.

There is an infinite (countable) number of monomials. If we totally order monomials[1] such that 1 is the smallest monomial[2] in some way (and we will discuss some useful orderings later), we can also understand polynomials as infinite sequences of rational numbers with a finite number of non-zero elements. For instance, polynomial $x_1\,x_2^2 + 2\,x_2^2 + 3\,x_1 + 4$ can be understood as infinite sequence

$$\begin{array}{ccccccccccccc} (& 4 & 3 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & \ldots &) \\ & 1 & x_1 & x_1^2 & x_1^3 & x_2 & x_1\,x_2 & x_1^2 x_2 & x_2^2 & x_1\,x_2^2 & x_2^3 & \ldots & \end{array}$$

with exactly four non-zero elements $1, 2, 3, 4$.

Polynomials with rational coefficients can be also understood as complex functions. We evaluate polynomial f on a point $\vec{p} \in \mathbb{C}^n$ as

$$f(\vec{p}) = \left(\sum_\alpha a_\alpha x^\alpha\right)(\vec{p}) = \sum_\alpha a_\alpha x^\alpha(\vec{p}) = \sum_\alpha a_\alpha \vec{p}^{\,\alpha} = \sum_\alpha a_\alpha \vec{p}_1^{\,\alpha_1} \vec{p}_2^{\,\alpha_2} \cdots \vec{p}_n^{\,\alpha_n}$$

which reflects that the evaluated polynomial is a linear combination of the evaluated monomials. For instance, we may write $(x_1\,x_2^2 + 2\,x_2^2 + 3\,x_1 + 4)([1,2]^\top) = x_1\,x_2^2([1,2]^\top) + 2\,x_1^0 x_2^2([1,2]^\top) + 3\,x_1 x_2^0([1,2]^\top) + 4\,x_1^0 x_2^0([1,2]^\top) = 4 + 8 + 3 + 4 = 19$.

3.1.1 Univariate polynomials

Polynomials in single unknown are often called *univariate polynomials*. In this case α becomes a trivial sequence containing a single number. The total degree $\deg(f)$ of f is then called *degree*.

[1] Total (linear) ordering of a set S is an ordering when every two elements of S are comparable.

[2] This can allways be done by finding a bijection from integrers to the monomials.

3.1.2 Long division of univariate polynomials

The set of all polynomials in a single unknown x over rational numbers, $\mathbb{Q}[x]$, forms a *ring*. Polynomials are almost as real numbers except for the division. Polynomials can't be in general divided. In fact, polynomials behave in many aspects as whole numbers $\mathbb{Z}$.

In particular, it is easy to introduce *long polynomial division* in the same way as it is used with whole numbers. Consider polynomials $f, g \in \mathbb{Q}[x]$, $g \neq 0$. Then, there are [2] unique polynomials $q, r \in \mathbb{Q}[x]$ such that

$$f = q\,g + r \quad \text{with} \quad \deg(r) < \deg(g) \quad \text{or} \quad r = 0$$

where q is the *quotient* and r is the *remainder* (of f on division by g). Equivalently, one also often writes $f \equiv r \pmod{g}$ and $r = f \bmod g$.

Word "division" in "long polynomial division" is indeed somewhat misleading when $r \neq 0$ since there is no real division in that case. We could perhaps better name it "expressing f using g in the most efficient way".

3.2 Systems of linear polynomial equations in several unknowns

Solving systems of linear polynomial equations is well understood. Let us give a typical example. Consider the following system of three linear polynomial equations in three unknowns

$$\begin{aligned} 2\,x_1 + 1\,x_2 + 3\,x_3 &= 0 \\ 4\,x_1 + 3\,x_2 + 2\,x_3 &= 0 \\ 2\,x_1 + 1\,x_2 + 1\,x_3 &= 2 \end{aligned}$$

and write it in the standard matrix form

$$\begin{bmatrix} 2 & 1 & 3 \\ 4 & 3 & 2 \\ 2 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 2 \end{bmatrix}$$

Using the Gaussian elimination [5], we obtain an equivalent system

$$\begin{bmatrix} 2 & 1 & 3 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix}$$

We see that the system has exactly one solution $x_1 = 7/2$, $x_2 = -4$, $x_3 = -1$.

We notice that the key point of this method is to produce a system in a "triangular shape" such that there is an equation $f_3(x_3) = 0$ in single unknown x_3, an equation in two unknowns $f_2(x_2, x_3)$, and so on. We can thus solve for x_3 and then transform f_2 by a substitution into an equation in a single unknown and solve for x_2, and so on.

3.3 One non-linear polynomial equation in one unknown

Solving one (non-linear) polynomial equation in one unknown is also well understood. The problem can be formulated as computation of eigenvalues of a matrix. Let us illustrate the approach on a simple example. Consider the following polynomial equation

$$f = x^3 - 6\,x^2 + 11\,x - 6 = 0$$

We can construct a *companion matrix* [5]

$$\mathtt{M}_x = \begin{bmatrix} 0 & 0 & 6 \\ 1 & 0 & -11 \\ 0 & 1 & 6 \end{bmatrix}$$

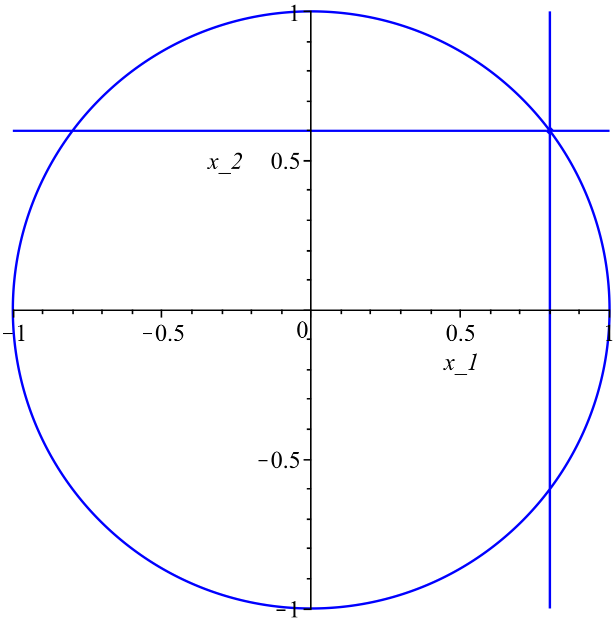


Figure 3.1: Solution to (3.2) is the intersection of a circle and a pair of lines. Solution at $[\frac{3}{5}, \frac{4}{5}]$ has multiplicity two.

of polynomial f and compute the characteristic polynomial of $\mathtt{M}_x$

$$|x\,\mathtt{I} - \mathtt{M}_x| = \left|\begin{bmatrix} x & 0 & -6 \\ -1 & x & 11 \\ 0 & -1 & x-6 \end{bmatrix}\right| = x^3 - 6\,x^2 + 11\,x - 6$$

to see that we are getting polynomial f. Hence, eigenvalues of $\mathtt{M}_x$, 1, 2, 3, are the solutions to equation $f = 0$.

This procedure applies in general when the coefficient at the monomial of f with the highest degree is equal to one [5], i.e. when we normalize the equation. Obviously, such a normalization, which amounts to division by a non-zero coefficient at the monomial of the highest degree, produces an equivalent equation with the same solutions.

The general rule for constructing the companion matrix $\mathtt{M}_x$ for polynomial $f = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$ is [5]

$$\mathtt{M}_x = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ & & \vdots & & \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}$$

Notice that eigenvalue computation must be in general approximate. In general, roots of polynomials of degrees higher than four can't be expressed as finite formulas in coefficients a_i using addition, multiplication and radicals [11].

3.4 Several non-linear polynomial equations in several unknowns

Let us now present a technique for transforming a system of polynomial equations with a finite number of solutions into a system that will contain a polynomial in the "last" unknown, say x_n, only. Achieving that will allow for solving for x_n and reducing the problem from n to $n-1$ unknowns and so on until we solve for all unknowns. Let us illustrate the technique on an example.

Consider the following system

$$\begin{aligned} f_1 &= x_2^2 + x_1^2 - 1 \;=\; 0 \\ f_2 &= 25\,x_1x_2 - 20\,x_2 - 15\,x_1 + 12 \;=\; 0 \end{aligned} \tag{3.2}$$

and rewrite it in a matrix form

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 25 & -20 & 0 & -15 & 12 \end{bmatrix} \begin{bmatrix} x_2^2 \\ x_1x_2 \\ x_2 \\ x_1^2 \\ x_1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \text{ or in short as } \begin{bmatrix} x_2^2 & x_1x_2 & x_2 & x_1^2 & x_1 & 1 \\ 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 25 & -20 & 0 & -15 & 12 \end{bmatrix} \tag{3.3}$$

Now, it is clear that $f = 0$ implies $gf = 0$ for any $g \in \mathbb{Q}[x_1, \dots, x_n]$. For instance $x_1^2 + x_2^2 - 1 = 0$ implies, e.g., $x_1(x_1^2 + x_2^2 - 1) = 0$ and $25\,x_1x_2 - 15\,x_1 - 20\,x_2 + 12$ implies $x_2(25\,x_1x_2 - 15\,x_1 - 20\,x_2 + 12)$.

Hence, adding such "new" equations to the original system produces a new system with the same solutions. On the other hand, polynomials f, xf are certainly linearly independent when $f \neq 0$ since then xf has degree strictly greater than is the degree of f. Thus, by adding xf, we have a chance to add another independent row to the matrix (3.3).

Let us now, e.g., add equations $x_1(x_1^2 + x_2^2 - 1) = 0$ and $x_2(25\,x_1x_2 - 15\,x_1 - 20\,x_2 + 12)$ to system (3.2) and write it in the matrix form as

$$\begin{array}{r} \\ f_1 \\ f_2 \\ x_1f_1 \\ x_2f_2 \end{array} \begin{bmatrix} x_1x_2^2 & x_2^2 & x_1x_2 & x_2 & x_1^3 & x_1^2 & x_1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 25 & -20 & 0 & 0 & -15 & 12 \\ 1 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 25 & -20 & -15 & 12 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{3.4}$$

We have marked each row of the coefficients with its corresponding equation. We see that two more rows have been added but also two new monomials, $x_1x_2^2$ and x_1^3, emerged. The next step will be to eliminate (3.4) by the Gaussian eliminations to get

$$\begin{array}{r} \\ x_1f_1 \\ f_1 \\ f_3 \\ f_4 \end{array} \begin{bmatrix} x_1x_2^2 & x_2^2 & x_1x_2 & x_2 & x_1^3 & x_1^2 & x_1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 25 & -20 & 0 & 0 & -15 & 12 \\ 0 & 0 & 0 & 0 & -125 & 100 & 80 & -64 \end{bmatrix} \tag{3.5}$$

We see that the last row of coefficients gives an equation in single unknown x_1

$$f_4 = -125\,x_1^3 + 100\,x_1^2 + 80\,x_1 - 64 = 0$$

Notice that we have been ordering the monomials corresponding to the columns of the matrix such that we have all monomials in sole x_1 at the end.

It can be shown [2] that the above procedure works for every system of polynomial equations $\{f_1, f_2, \dots, f_k\}$ from $\mathbb{Q}[x_1, \dots, x_n]$ with a finite number of solutions. In particular, there always are k finite sets $M_i, i = 1, \dots, k$ of monomials such that the extended system

$$\{f_1, f_2, \dots, f_k\} \cup \{m\, f_j | m \in M_j, j = 1, \dots, k\}$$

obtained by adding for each f_j its multiples by all monomials in M_j, has matrix $\mathtt{A}$ with the following nice property. If the last columns of $\mathtt{A}$ correspond to all monomials in a single unknown x_i (including 1, which is x_j^0), then the last non-zero row of matrix $\mathtt{B}$, obtained by Gaussian elimination of A, produces a polynomials in single unknown x_i.

This is a very powerful technique. It gives us a tool how to solve all systems of polynomial equations with a finite number of solutions. In practice, the main problem is how to find small sets M_i in acceptable time. Consider that the number of monomials of total degree at most d in n unknowns is given by the combination number $\binom{n+d}{d}$. Hence, in general, the size of the matrix is growing very quickly as a function of n and d needed to get the result. Practical algorithms, e.g. F4 [2], use many tricks how to select small sets of monomials and how to efficiently compute in exact arithmetic over rational numbers.

Let us now return to our example above. We can solve the $f_4 = 0$ for x_1 and substitute all solutions to $f_3 = 0$ from the third row, which, for known x_1, is an equation in single unknown x_2

$$f_3 = 25\,x_1x_2 - 20\,x_2 - 15\,x_1 + 12 = (25\,x_1 - 20)\,x_2 - 15\,x_1 + 12 = 0$$

That gives us solutions for x_2.

3.5 Solving a polynomial system as an eigenvector problem

Solving polynomial systems for one unknown after another by the procedure given in the previous paragraph calls for back-substitution that may be non-trivial to implement in general. Also notice that in the example above, we did not really see that there are four solutions since one, $[\frac{3}{5}, \frac{4}{5}]$ in Figure 3.1, had multiplicity two but that was "masked" by other solution that we aligned with it.

Let us now present an alternative approach often allowing to compute all solutions at once as an eigenvector problem. We will first illustrate the technique on an example in a single unknown given in paragraph 3.3.

3.5.1 Solving a univariate polynomial equation by eigenvectors

Consider a polynomial system consisting of a single equation

$$f = x^3 - 6\,x^2 + 11\,x - 6 = (x-1)\,(x-2)\,(x-3) = 0$$

in one unknown x with roots 1, 2, 3. We have seen how to solve this system by computing eigenvalues of the companion matrix $\mathtt{M}_x$ of polynomial f. Let us now see how to do the same by computing eigenvectors of $\mathtt{M}_x^\top$.

Let us first consider remainders of all polynomials g in $\mathbb{Q}[x]$ on division by f. It is the set of all polynomials r of degree at most two. All polynomials of degrees at most two are left unchanged by the long division by f and all monomials of a higher degree will get rewritten using f in terms of polynomials of degree at most two. We can thus write

$$r = a_2x^2 + a_1x + a_0 \quad \text{for} \quad a_0, a_1, a_2 \in \mathbb{Q} \quad \textit{i.e.} \quad r \equiv \begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix} \in \mathbb{Q}^3$$

and hence identify each remainder with a three-dimensional vector from $\mathbb{Q}^3$. We see that the set of all such remainders is in one-to-one correspondence with $\mathbb{Q}^3$.

Secondly, consider the mapping $\mathcal{M}_x\colon \mathbb{Q}[x] \to \mathbb{Q}[x]$ on polynomials given by

$$\mathcal{M}_x(h) = (x\,h) \mod f$$

It maps monomials of degree at most two back to polynomials of degree at most two, i.e.

$$\begin{aligned} \mathcal{M}_x(1) &= x\,1 \mod f = x \mod f = x \\ \mathcal{M}_x(x) &= x\,x \mod f = x^2 \mod f = x^2 \\ \mathcal{M}_x(x^2) &= x\,x^2 \mod f = x^3 \mod f = 6\,x^2 - 11\,x + 6 \end{aligned} \tag{3.6}$$

We see that $\mathcal{M}_x$ is a linear mapping since for all $g, h \in \mathbb{Q}[x]$, $a \in \mathbb{Q}$ we have

$$\begin{aligned}\mathcal{M}_x(g+h) &= (x\,g + x\,h) \bmod f = (x\,g) \bmod f + (x\,h) \bmod f = \mathcal{M}_x(g) + \mathcal{M}_x(h)\\ \mathcal{M}_x(a\,g) &= (a\,x\,g) \bmod f = a\,(x\,g) \bmod f = a\,\mathcal{M}_x(g)\end{aligned}$$

Every linear mapping has a matrix of the mapping w.r.t. a basis [4]. We can write

$$\begin{aligned}\mathcal{M}_x(a_2x^2 + a_1x + a_0) &= a_2\mathcal{M}_x(x^2) + a_1\mathcal{M}_x(x) + a_0\mathcal{M}_x(1) &(3.7)\\ &= [a_0,\ a_1,\ a_2]\begin{bmatrix}\mathcal{M}_x(1)\\ \mathcal{M}_x(x)\\ \mathcal{M}_x(x_2)\end{bmatrix} &(3.8)\\ &= [a_0,\ a_1,\ a_2]\begin{bmatrix}x\\ x^2\\ 6\,x^2 - 11\,x + 6\end{bmatrix} &(3.9)\\ \mathcal{M}_x\left([1,\ x,\ x^2]\begin{bmatrix}a_0\\ a_1\\ a_2\end{bmatrix}\right) &= [a_0,\ a_1,\ a_2]\begin{bmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 6 & -11 & 6\end{bmatrix}\begin{bmatrix}1\\ x\\ x^2\end{bmatrix} &(3.10)\end{aligned}$$

and thus

$$\mathcal{M}_x\left([1,\ x,\ x^2]\begin{bmatrix}a_0\\ a_1\\ a_2\end{bmatrix}\right) = [1,\ x,\ x^2]\begin{bmatrix}0 & 0 & 6\\ 1 & 0 & -11\\ 0 & 1 & 6\end{bmatrix}\begin{bmatrix}a_0\\ a_1\\ a_2\end{bmatrix} \tag{3.11}$$

We can interpret the above as choosing the *standard monomial basis* $[1, x, x^2]$ in the linear space of $\mathbb{Q}[x]$ of degree at most two, and writing the above represented by vectors in $\mathbb{Q}^3$. Then, expressing monomials as vectors using basis $[1, x, x^2]$ we get

$$\begin{aligned}\mathcal{M}_x(1) \equiv \mathcal{M}_x\left(\begin{bmatrix}1\\0\\0\end{bmatrix}\right) &= \begin{bmatrix}0\\1\\0\end{bmatrix}\\ \mathcal{M}_x(x) \equiv \mathcal{M}_x\left(\begin{bmatrix}0\\1\\0\end{bmatrix}\right) &= \begin{bmatrix}0\\0\\1\end{bmatrix}\\ \mathcal{M}_x(x^2) \equiv \mathcal{M}_x\left(\begin{bmatrix}0\\0\\1\end{bmatrix}\right) &= \begin{bmatrix}6\\-11\\6\end{bmatrix}\end{aligned}$$

We see that the matrix of the mapping $\mathcal{M}_x$ is obtained by

$$\mathcal{M}_x\left(\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}\right) = \begin{bmatrix}0 & 0 & 6\\ 1 & 0 & -11\\ 0 & 1 & 6\end{bmatrix} = \mathtt{M}_x$$

and observe that $\mathtt{M}_x$ is the matrix of $\mathcal{M}_x$ w.r.t. the standard monomial basis $\mathtt{B} = [1, x, x^2]$, is the companion matrix of f, i.e.

$$\mathcal{M}_x(\vec{f_{\mathtt{B}}}) = \mathtt{M}_x\,\vec{f_{\mathtt{B}}} \tag{3.12}$$

as well as

$$\begin{aligned}\mathcal{M}_x(\mathtt{B}^\top) &= \mathtt{B}^\top\mathtt{M}_x &(3.13)\\ \mathcal{M}_x(\mathtt{B}) &= \mathtt{M}_x^\top\mathtt{B} &(3.14)\end{aligned}$$

Now, let us evaluate polynomials $g \in \mathbb{Q}[x]$ on the roots of f. Consider a root p of f, i.e. a solution to equation $f = 0$, and evaluate g on p using its remainder r on division by f

$$g(p) = q(p)\, f(p) + r(p) = q(p)\, 0 + r(p) = r(p)$$

since $f(p) = 0$. We see that polynomials evaluate on roots of f to the values of their remainders on division by f. Let us now evaluate polynomials x, x^2, x^3 on roots $\vec{p} = [p_1, p_2, p_3]^\top$ of f.

$$\begin{array}{rclclclcl} x(p_i) &=& p_i &=& p_i\, 1 &=& p_i\, 1(p_i) &=& x(p_i)\, 1(p_i) \\ x^2(p_i) &=& p_i^2 &=& p_i\, p_i &=& p_i\, x(p_i) &=& x(p_i)\, x(p_i) \\ x^3(p_i) &=& p_i^3 &=& p_i\, p_i^2 &=& p_i\, x^2(p_i) &=& x(p_i)\, x^2(p_i) \end{array} \tag{3.15}$$

Now, since

$$\begin{aligned} x^3(p_i) &= x^3 - 6\,x^2 + 11\,x - 6 + (6\,x^2 - 11\,x + 6) && (3.16) \\ &= f(p_i) + \mathcal{M}_x(x^2)(p_i) && (3.17) \\ &= 0 + (6\,x^2 - 11\,x + 6)(p_i) && (3.18) \end{aligned}$$

we get

$$x(p_i)\, x^2(p_i) = (6\,x^2 - 11\,x + 6)(p_i) \tag{3.19}$$

We can rewrite identities (3.15) and (3.19) as the following sequence of matrix identities

$$\begin{aligned} x(p_i) \begin{bmatrix} 1(p_i) \\ x(p_i) \\ x^2(p_i) \end{bmatrix} &= \begin{bmatrix} x(p_i) \\ x^2(p_i) \\ x^3(p_i) \end{bmatrix} = \begin{bmatrix} x(p_i) \\ x^2(p_i) \\ (6\,x^2 - 11\,x + 6)(p_i) \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ f(p_i) \end{bmatrix} \\ x(p_i) \begin{bmatrix} 1(p_i) \\ x(p_i) \\ x^2(p_i) \end{bmatrix} &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 6 & -11 & 6 \end{bmatrix} \begin{bmatrix} 1(p_i) \\ x(p_i) \\ x^2(p_i) \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \\ x(p_i) \begin{bmatrix} 1 \\ p_i \\ p_i^2 \end{bmatrix} &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 6 & -11 & 6 \end{bmatrix} \begin{bmatrix} 1 \\ p_i \\ p_i^2 \end{bmatrix} \\ p_i\, \vec{v}_i &= \mathtt{M}_x^\top \vec{v}_i \end{aligned}$$

showing that $(p_i, \vec{v}_i)$ are eigenvalue-eigenvector pairs of $\mathtt{M}_x^\top$. Eigenvalues p_i are evaluations of x on roots of f and eigenvectors $\vec{v}_i$ are evaluations of the monomials of the standard basis $[1, x, x^2]$ on the roots of f. The above observation holds true in general [14]. For a polynomial f of degree n, we are getting an $n \times n$ matrix with n eigenvalues, counting the multiplicities.

When matrix $\mathtt{M}_x$ has separated one-dimensional eigenspaces, which, e.g., happens always when eigenvalues are pairwise distinct, i.e. when f has all roots of multiplicity one, we can (numerically) compute basis $\vec{w}_i$ of each eigenspace[3] and get $\vec{v}_i$ as

$$\vec{v}_i = \frac{1}{\vec{w}_{i1}} \vec{w}, \quad i = 1, \ldots, n$$

We see that solutions to f are obtained from $\vec{v}_i$ as $p_i = x(p_i) = \vec{v}_{i2}$.

It is possible to generalize the above to a more general mapping $\mathcal{M}_g \colon \mathbb{Q}[x] \to \mathbb{Q}[x]$ by replacing unknown x by a general polynomial $g \in \mathbb{Q}[x]$ to get

$$\mathcal{M}_g(h) = (g\,h) \mod f$$

Now, consider that $g(p_i) = r(p_i)$ where $r = a_2 x^2 + a_1 x + a_0$ is the remainder of g on division by f. Thus

$$g(p_i) = r(p_i) = a_2 x^2(p_i) + a_1 x(p_i) + a_0 1(p_i) \tag{3.20}$$

[3] Many algorithms, e.g. in Matlab, deliver $\vec{w}_i$'s with $\|\vec{w}_i\| = 1$.

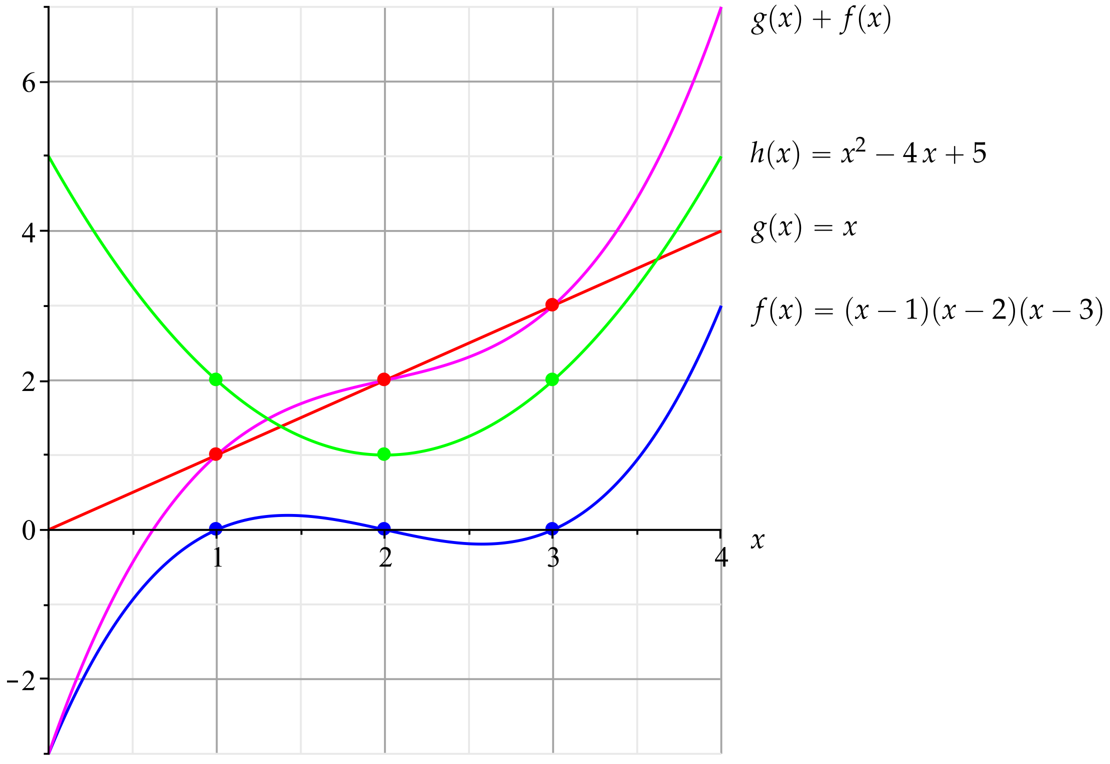


Figure 3.2: Polynomial $f(x)$ and its roots 1, 2, 3. All remainders on division by f, e.g. $g(x)$, $h(x)$, which are of degree not larger than two, are uniquely determined by their values on the roots 1, 2, 3 of f. See the text for more detailed explanation.

Further, considering that

$$\begin{aligned}\lambda\,\vec{v} &= \mathtt{A}\,\vec{v}\\ \lambda\,\mathtt{A}\,\vec{v} &= \mathtt{A}^2\,\vec{v}\\ \lambda^2\,\vec{v} &= \mathtt{A}^2\,\vec{v}\end{aligned}$$

we can write

$$\begin{aligned}
g(p_i)\begin{bmatrix}1(p_i)\\ x(p_i)\\ x^2(p_i)\end{bmatrix} &= \left(a_2x^2(p_i)+a_1x(p_i)+a_0 1(p_i)\right)\begin{bmatrix}1(p_i)\\ x(p_i)\\ x^2(p_i)\end{bmatrix}\\
g(p_i)\begin{bmatrix}1(p_i)\\ x(p_i)\\ x^2(p_i)\end{bmatrix} &= \left(a_2\,(\mathtt{M}_x^\top)^2+a_1\,\mathtt{M}_x^\top+a_0\mathtt{I}\right)\begin{bmatrix}1(p_i)\\ x(p_i)\\ x^2(p_i)\end{bmatrix}\\
g(p_i)\begin{bmatrix}1\\ p_i\\ p_i^2\end{bmatrix} &= \left(a_2\,(\mathtt{M}_x^\top)^2+a_1\,\mathtt{M}_x^\top+a_0\mathtt{I}\right)\begin{bmatrix}1\\ p_i\\ p_i^2\end{bmatrix}\\
g(p_i)\,\vec{v}_i &= \mathtt{M}_g^\top\vec{v}_i \qquad (3.21)
\end{aligned}$$

showing that $(g(p_i), \vec{v}_i)$ are eigenvalue-eigenvector pairs of $\mathtt{M}_g^\top = (a_2\,\mathtt{M}_x^2 + a_1\,\mathtt{M}_x + a_0\mathtt{I})^\top$.

We saw that remainders r on division by f could be identified with $\mathbb{Q}^3$ via their coefficients. Let us now present another representation of r by vectors from $\mathbb{C}^3$. Figure 3.2 shows $f(x) = (x-1)(x-2)(x-3)$ and its roots $p_1 = 1, p_2 = 1, p_3 = 3$. Each remainder on division by f, e.g. g and h, which has degree not larger than two, is uniquely defined by its values on the roots $p_1 = 1, p_2 = 1, p_3 = 3$ of f. In general, roots of f are from $\mathbb{C}$ and hence their polynomial evaluations are from $\mathbb{C}$ as well. This way, every remainder r on division by f is on one to one correspondence with a vector from $\mathbb{C}^3$, i.e. $r(x) \equiv [r(p_1), r(p_2), r(p_3)]^\top$.

All polynomials can be written as $q(x)\, f(x) + r(x)$, and thus every polynomial can be assigned its reminder on division by f. This way, the set of polynomials is partitioned into equivalence classes and a bijection between the sets of the equivalence classes and the remainders on division by f is obtained.

Eigenvalue problem 3.21 thus can be seen as expressing the representative of $g(x)\, f(x)$ by multiplication by of the representative of $f(x)$ by $\mathtt{M}_g^\top$.

3.5.2 Solving systems of multivariate polynomial equations by eigenvectors

To generalize the procedure above to systems of polynomial equations in several unknowns, we have to generalize the concept of "remainder on division by a single polynomial in one unknown" to more polynomials in more unknowns. It will require to address several issues. Let us first lay down a general strategy, then deal with particular issues, and, finally, provide a method for finding the solutions to a polynomial system with a finite number of solutions by computing eigenvectors.

We have seen that the key concept for deriving the relationship between the solutions to $f = 0$ and the eigenvectors of $\mathtt{M}_h$ in the univariate case was that the remainder r of h on division by f gave the values of h on the roots of f.

Long division produced $r = h - q\, f$ such that r was "the simplest" polynomial evaluating on roots of f to the same values as h. We could also see this as removing from h all what can be generated by f, i.e. all what is in $\langle f \rangle = \{h\, f \,|\, h \in \mathbb{Q}[x]\}$. We can also say that r is equivalent[4] to f, writing $h \equiv r$, when $h - r = q\, f \in I = \langle f \rangle$.

In the multivariate case, this motivates introducing *ideal* I generated by polynomials $f_1, \ldots, f_k$, denoted by $\langle f_1, \ldots, f_k \rangle$, as

$$I = \langle f_1, \ldots, f_k \rangle = \{\sum_{i=1}^{k} g_i\, f_i \,|\, g_i \in \mathbb{Q}[x_1, \ldots, x_n]\}$$

Ideal I is the set of all polynomials that can be generated from $f_1, \ldots, f_k$ by polynomial combinations. All polynomials in I evaluate to zero (*are satisfied*) on the solutions of the system $f_1, \ldots, f_k$.

In the univariate case, monomials were naturally ordered by their degree. The total degrees of univariate monomials, i.e. the powers of the unknown, provided a total ordering [1] of the monomials in one unknown[5]. In the multivariate case, however, total degrees do not provide a total ordering. For instance, consider that $\deg(x^2 y) = 3 = \deg(x\, y^2)$ but $x^2 y \neq x y^2$, which means that $x^2 y$, $x\, y^2$ are not comparable when ordered by the total degree. We see that the total degree makes only a partial ordering of monomials. Hence, we need to introduce another way of ordering the monomials to get a total ordering. We will discuss this in more detail in paragraph 3.5.3.

From the point of view of the eigenvector method in the univariate case, the remainders r on the long division by f had the good property that all monomials of r were strictly smaller (when ordered by the degree) than the largest (leading) monomial of f. The maximal degree of r was equal to the number m of solutions minus one and hence r was a linear combination of exactly m monomials. That gave $m \times m$ multiplication matrices $\mathcal{M}_g$ and thus m one-dimensional sub-spaces of eigenvectors. This was thanks to the fact that ideal $\langle f \rangle$ was in one-to-one correspondence with its generator f.

Now, in the multivariate case, when ideals are generated by more generators $F = \{f_1, \ldots, f_k\}$, $I = \langle F \rangle$ can be generated by infinitely many different sets of generators and, in general, there is no

[4] Equivalence $\equiv$ is a relation on a set S, i.e. a subset of $S \times S$, satisfying three axioms: $\forall a, b, c \in S$: (reflexivity) $a \equiv a$, (transitivity) $a \equiv b$ and $b \equiv c$ implies $a \equiv c$, (symmetry) $a \equiv b$ implies $b \equiv a$ [1].

[5] Ordering $<_o$ is a relation on a set S, i.e. a subset of $S \times S$, satisfying three axioms: $\forall a, b, c \in R \subseteq S$: (reflexivity) $a <_o a$, (transitivity) $a <_o b$ and $b <_o c$ implies $a <_o c$, (antisymmetry) $a <_o b$ and $b <_o a$, then $a = b$. Ordering that is defined for all members of S, i.e. when $R = S$ is called *total ordering* (or *linear ordering*). An ordering is called *partial ordering* when $R \subset S$ [1].

direct connection between the multidegrees of the leading monomials of a particular generator set and the number of solutions. Further, with a general set of generators F of I, there is no good way of defining the remainder on division by F because when algorithmically writing a polynomial g as a polynomial combination $g = q_1 f_1 + \cdots + q_n f_n + r$, different r's can be obtained when changing the order in which f_i's are used in the rewriting of g.

Fortunately, one can always find a "good set" G of generators of I, called reduced *Gröbner basis* of I, that "behaves well". It is possible to generalize the univariate long division to a multivariate long division by several polynomials such that it, for every $g \in \mathbb{Q}[x_1, \ldots, n_n]$, produces a unique reminder r on division by G independently on the order in which the generators G are used in the division process. Remainder $r = g \bmod_{<_o} G$ is thus defined uniquely by the ideal I and monomial ordering $<_o$ used. Further, r becomes a linear combination of monomials that are not divisible by any leading monomial of the generators G. The actual monomials may be different depending on the monomial ordering used but their number l will always be the same.

The relationship of l to the number of solutions m is more intricate. In general $l \geqslant m$. The equality occurs exactly when I is a *radical ideal*, which means that I is such that $f^k \in I$ for some k implies $f \in I$. Intuitively, radicality is connected to multiplicity of solutions. Fix an unknown x_i and look at all polynomials in I that are only in x_i. They form an ideal I_i. The ideal I_i is univariate and hence is generated by a single polynomial $e_i(x_i)$. Roots of e_i are the projections on the solutions of F on the x_i axis. Now, if the roots of $e_i(x_i)$ are of multiplicity one for all unknowns, then I is radical. Radical ideals have no multiplicities in any coordinate.

For ideals $I = \langle F \rangle$ with a finite number of solutions, we can construct its radical ideal $\sqrt{I}$ by removing all multiplicities from each $e_i(x_i)$. This can be done [14] by constructing polynomials

$$p_{i,red} = \frac{e_i}{\mathtt{GCD}(e_i, e_i')}$$

where e_i' is the derivative of e_i w.r.t. x_i and GCD is the greatest common divisor of two polynomials. Radical ideal of I is obtained as

$$\sqrt{I} = \langle f_1, \ldots, f_k, p_{1,red}, \ldots, p_{n,red} \rangle$$

A generalization of the long division for the multi-variate and multi-polynomial case will be described in paragraph 3.5.4 and an algorithm for finding Gröbner basis of I will be given in paragraph 3.5.5.

We are now ready to generalize the eigenvector-method to polynomial systems $F = \{f_1, \ldots, f_k\}$ in multiple unknowns $x_1, \ldots, x_n$:

1. Fix a particular monomial ordering $<_o$.

2. Construct the reduced Gröbner basis G of $I = \langle F \rangle$ for $<_o$.

3. Construct the set B of all monomials that are divisible by no leading monomial of all polynomial in G.

4. Fix a polynomial $g \in \mathbb{Q}[x_1, \ldots, x_n]$ such that g has different values on different solutions, e.g. take a random linear polynomial. This, guarantees isolated one-dimensional eigenspaces for radical ideals $\langle F \rangle$.

5. Construct the multiplication matrix $\mathcal{M}_g$ by finding remainders of $g\,b$ for all $g \in B$ on division by G w.r.t. $<_o$.

6. Find eigenvalues and eigenvectors of $\mathcal{M}_g$. Check if all eigenspaces are one-dimensional. If not, extend F by setting $F := F \cup \{p_{1,red}, \ldots, p_{n,red}\}$ and start again from the beginning with extended F.

7. Recover the solutions from the eigenvalues, eigenvectors and G.

We will illustrate the above procedure in paragraph 3.5.6.

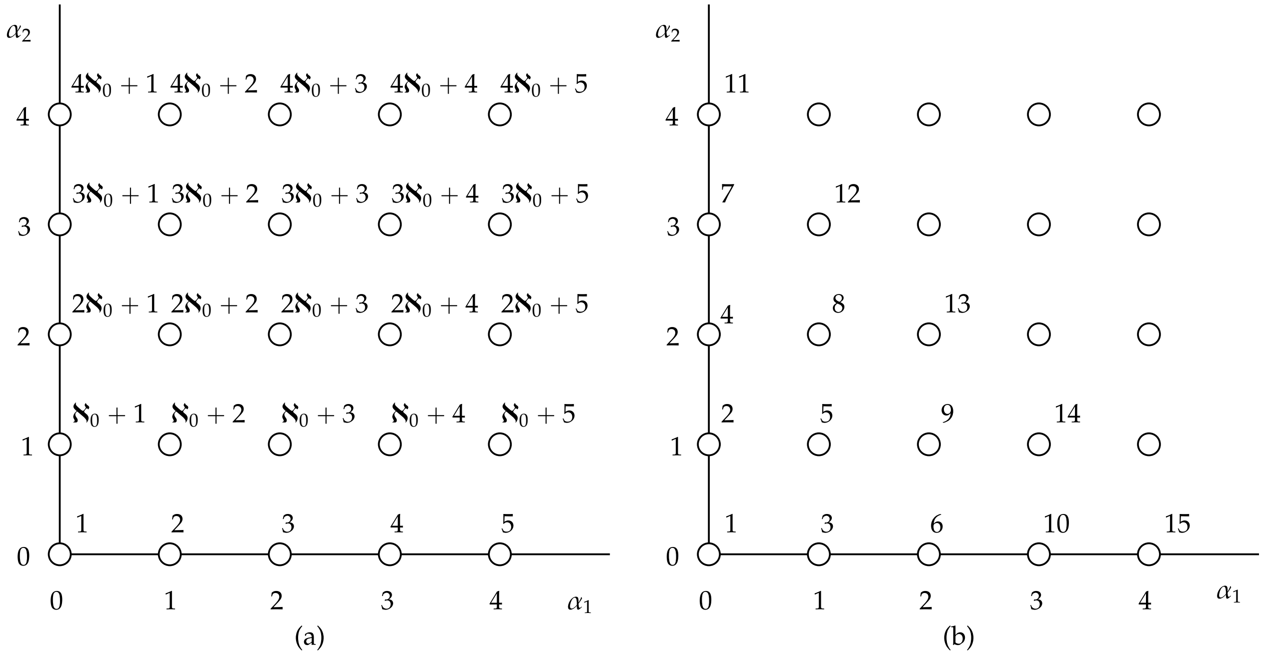

α_2
$4\aleph_0+1$ $4\aleph_0+2$ $4\aleph_0+3$ $4\aleph_0+4$ $4\aleph_0+5$
$3\aleph_0+1$ $3\aleph_0+2$ $3\aleph_0+3$ $3\aleph_0+4$ $3\aleph_0+5$
$2\aleph_0+1$ $2\aleph_0+2$ $2\aleph_0+3$ $2\aleph_0+4$ $2\aleph_0+5$
$\aleph_0+1$ $\aleph_0+2$ $\aleph_0+3$ $\aleph_0+4$ $\aleph_0+5$
1 2 3 4 5
0 1 2 3 4
α_1
(a)
α_2
11
7 12
4 8 13
2 5 9 14
1 3 6 10 15
0 1 2 3 4
α_1
(b)

Figure 3.3: (a) Lex monomial ordering $x_1^{\alpha}y^{\alpha_2}$ with $x <_{lex} y$ orders monomials as $1, x, x^2, \ldots, y, x\,y, x^2y, \ldots, y^2, x\,y^2, \ldots$ while (b) the GRevLex monomial ordering orders monomials as $1, y, x, y^2, x\,y, x^2, y^3, x\,y^2, x^2y, x^3, \ldots$. We see that $y \equiv \alpha = (0,1) <_{grevlex} x \equiv \beta = (1,0)$ since they both have total degree equal to one and $\beta - \alpha = (1,0)-(0,1) = (1,-1)$, i.e. the last non-zero coordinate of $\beta - \alpha$ is negative.

3.5.3 Monomial ordering

We saw that a useful total ordering of monomials in single unknown was obtained by ordering the monomials by their degree, giving

$$[x^0, x^1, x^2, \ldots] \tag{3.22}$$

Unfortunately, ordering monomials in more unknowns by their total degree produces only a partial ordering, i.e. we can't compare all monomials. Consider, e.g., monomials $x^2\,y$, $x\,y^2$. They both have total degree equal to three

$$\deg(x^2\,y) = 3 = \deg(x\,y^2) \quad \text{but} \quad x^2\,y \neq x\,y^2 \tag{3.23}$$

and hence we see that the total degree does not define ordering of this two monomials. For multivariate polynomials, we have to introduce another way how to order them.

Every set can be totally ordered such that it has the least element [1] but we have to satisfy additional constraints to make the ordering useful for our case. The ordering by the degree in the univariate case had two important properties we have to preserve. First, (i) constant 1 was the smallest element. Secondly, (ii) the ordering "worked nicely" together with the multiplication by monomials, i.e.

$$\deg(m_1) < \deg(m_2) \quad \Rightarrow \quad \deg(m\,m_1) < \deg(m\,m_2)$$

for all monomials $m \in \mathbb{Q}[x_1, \ldots, x_n]$.

To get a useful ordering for the multivariate case, we have to preserve the above two properties. Since monomials are in one-to-ne correspondece with their multidegrees, literature talks about *monomial ordering* $<_o$ as any total ordering of $\mathbb{Z}^n_{\geqslant 0}$ satisfying properties (i) and (ii) above. There are infinitely many ways how to construct a monomial ordering [15]. Let us now present two classical orderings that, in a way, represent all different monomial orderings.

Lex Monomial Ordering (Lex) $<_{lex}$ orders monomials as words in a dictionary. An important parameter of $<_{lex}$ order (i.e. ordering of words) is the order of the unknowns (i.e. ordering of letters). For instance, monomial $x\,y^2z = x\,y\,y\,z <_{lex} x\,y\,z\,z = x\,y\,z^2$ when $x <_{lex} y <_{lex} z$ (i.e. $x\,y\,y\,z$ is before $x\,y\,z\,z$ in a standard dictionary). However, when $z <_{lex} y <_{lex} x$, then $x\,y\,z^2 = x\,y\,z\,z <_{lex} x\,y\,y\,z = x\,y^2z$. We see that there are $n!$ possible $<_{lex}$ orderings when dealing with n unknowns.

Formally, we say that monomial $x^\alpha <_{lex} x^\beta$, as well as $\alpha <_{lex} \beta$ for exponents, when either $\beta - \alpha = 0$ or the first non-zero element of $\beta - \alpha$ is positive.

For instance $(0,3,4) <_{lex} (1,2,0)$ since $(1,2,0) - (0,3,4) = (1,-1,-4)$ and $(3,2,1) <_{lex} (3,2,4)$ since $(3,2,4) - (3,2,1) = (0,0,3)$.

Graded Reverse Lex Monomial Ordering (GRevLex) $<_{grevlex}$ is an extension of the partial ordering by the total degree to a total monomial ordering.

Formally, we say that monomial $x^\alpha <_{grevlex} x^\beta$, as well as $\alpha <_{grevlex} \beta$ for exponents, when either $\deg(\alpha) < \deg(\beta)$ or $\deg(\alpha) = \deg(\beta)$ and the last non-zero element of $\beta - \alpha$ is negative.

For instance $y^3z \sim (0,3,1) <_{grevlex} (1,2,2) \sim x\,y^2z^2$ since $0 + 3 + 1 = 4 < 5 = 1 + 2 + 2$ but $x\,y^2z^2 \sim (1,2,2) <_{grevlex} (1,3,1) \sim x\,y^3\,z$ since $1+2+2 = 5 = 1+3+1$ and $(1,3,1)-(1,2,2) = (0,1,-1)$.

Figure 3.3 shows a few first monomials in two unknowns labeled by the Lex (a) and GRevLex (b) orderings. It has been noted that Lex is often harder to use for computation than "graded" orderings, such as GRevLex ordering. On the other hand, Lex orderings provide us with univariate polynomials.

The main difference between the above two orderings is that $<_{grevlex}$ is an *archimedean ordering*, which means that for every monomials $m_1, m_2 \in \mathbb{Q}[x_1, \ldots, x_n]$, $1 \neq m_1 <_{grevlex} m_2$, there is $k \in \mathbb{Z}_{\geqslant 0}$ such that $m_2 <_{grevlex} m_1^k$. It also means that with $<_{grevlex}$, there are always only a finitely many monomials smaller than any monomial. Lex orderings are not archimedean. Consider, for instance, $<_{lex}$ with $x <_{lex} y$. We see that $x^k <_{lex} y$ for all $k \in \mathbb{Z}_{\geqslant 0}$ and hence there are infinitely many smaller monomials than y. Lex orderings are useful for constructing a polynomial in a single unknown when a system of polynomial equations has a finite number of solutions. Graded orderings, such as GRevLex, appear to keep total degrees in computations low and often lead to results faster than when using Lex orderings.

With a fixed monomial ordering $<_o$, we can talk about the *leading monomial*, $\mathtt{LM}(f)$, of a polynomial f, which is the largest monomial of the polynomial w.r.t. $<_o$. The coefficient at the leading monomial is *leading coefficient*, $\mathtt{LC}(f)$, their product is *leading term*, $\mathtt{LT}(f) = \mathtt{LC}(f)\,\mathtt{LM}(f)$. For instance, consider polynomial $f = 1\,y^2 + 2\,x^2y + 3$. With $x <_{lex} y$, we get $\mathtt{LM}(f) = y^2$, $\mathtt{LC}(f) = 1$ and $\mathtt{LT}(f) = 1\,y^2$ but with $x <_{grevlex} y$ we get $\mathtt{LM}(f) = x^2\,y$, $\mathtt{LC}(f) = 2$ and $\mathtt{LT}(f) = 2\,x^2y$.

3.5.4 Multivariate and multipolynomial long division

We will now discuss a generalization of the long division of a univariate polynomial by one univariate polynomial to a long division of a multivariate polynomial by several multivariate polynomials.

Let us first present an algorithm, then show two examples demonstrating an important feature of the algorithm, and finally state the general fact about the reminder obtained.

Consider a polynomial $f \in \mathbb{Q}[x_1, \ldots, x_n]$ and another s polynomials $f_1, \ldots, f_s \in \mathbb{Q}[x_1, \ldots, x_n]$. Now, we want to express f as

$$f = a_1\,f_1 + a_2\,f_2 + \cdots + a_s f_s + r \tag{3.24}$$

with the *quotients* a_i and the remainder r in $\mathbb{Q}[x_1, x_2, \ldots, x_n]$. To do so, we will rewrite f by the following algorithm [2].

Long polynomial division algorithm

```
Input: $f_1, \ldots, f_s, f \in \mathbb{Q}[x_1, \ldots, x_n]$, monomial ordering $<_o$
Output: $a_1, \ldots, a_s, r \in \mathbb{Q}[x_1, \ldots, x_n]$
$a_1 := 0; \ldots, a_s := 0; r := 0$
$p := f$
while $p \neq 0$ do
```

```
    $i := 1$
    divisionoccured := false
    while $i \leqslant s$ and divisionoccured = false do
      if $\mathtt{LT}(f_i)$ divides $p$ then
        $a_i := a_i + \mathtt{LT}(p)/\mathtt{LT}(f_i)$
        $p := p - (\mathtt{LT}(p)/\mathtt{LT}(f_i))\, f_i$
        divisionoccured := true
      else
        $i := i + 1$
      end if
    end while
    if divisionoccured = false then
      $r := r + \mathtt{LT}(p)$
      $p := p - \mathtt{LT}(p)$
    end if
  end while
```

The above algorithm is a generalization of the algorithm for long polynomial division in one unknown. Let us look at some examples that illustrate some of the important features of the algorithm.

Example 1 Let us divide $f = x\,y^2 + x + 1$ by $f_1 = x\,y + 1$, $f_2 = y + 1$ with monomial ordering $y <_{lex} x$.

#	f	$=$	$a_1 f_1$	$+$	$a_2 f_2$	$+$	p	$+$	r
0		$=$	$0\,(x\,y+1)$	$+$	$0\,(y+1)$	$+$	$x\,y^2+x+1$	$+$	0
1		$=$	$y\,(x\,y+1)$	$+$	$0\,(y+1)$	$+$	$x-y+1$	$+$	0
2		$=$	$y\,(x\,y+1)$	$+$	$0\,(y+1)$	$+$	$-y+1$	$+$	x
3		$=$	$y\,(x\,y+1)$	$-$	$1\,(y+1)$	$+$	2	$+$	x
4		$=$	$y\,(x\,y+1)$	$-$	$1\,(y+1)$	$+$	0	$+$	$x+2$

Symbol # represents the number of executions of the outer while loop above. We initialize at #0 by setting p to f. Then, at #1, we try to divide $\mathtt{LT}(p) = x\,y^2$ by $\mathtt{LT}(f_1) = x\,y$. We succeed and update a_1 to y and p to $x - y + 1$. This resets i to 1 and hence at #2 we again try to divide $\mathtt{LT}(p) = x$ by $\mathtt{LT}(f_1) = x\,y$. We fail and hence increment i and try to divide $\mathtt{LT}(p) = x$ by $\mathtt{LT}(f_2) = y$. We fail again and thus move $\mathtt{LT}(p) = x$ to r, update p and reset i. At #3 we try to divide $\mathtt{LT}(p) = -y$ by $\mathtt{LT}(f_1) = x\,y$. We fail. Hence we try to divide $\mathtt{LT}(p) = -y$ by $\mathtt{LT}(f_2) = y$. We succeed, update a_2 to -1, and update p. Finally, at #4, we fail to divide $\mathtt{LT}(p) = 2$ by $\mathtt{LT}(f_1)$ as well as by $\mathtt{LT}(f_2)$ and thus add 2 to r. This terminates the algorithm with $p = 0$.

We can first notice that no monomial of r is divisible by $\mathtt{LT}(f_1)$ or by $\mathtt{LT}(f_2)$. Secondly we also see that multideg$(a_1 f_1) = [1,2] \leqslant [1,2] =$ multideg(f) as well as multideg$(a_2 f_2) = [0,1] \leqslant [1,2] =$ multideg(f). This holds true in general and bring us to the following important general fact about the long division algorithm.

Fact [2] Consider a fixed monomial ordering $<_o$ and an ordered s-tuple $F = (f_1, \dots, f_s)$ of polynomials. Then, every polynomial f can rewritten using the long division algorithm as

$$f = a_1\, f_1 + a_2\, f_2 + \cdots + a_s f_s + r$$

with polynomials a_i and r such that

1. if $r \neq 0$, then no monomial of r is divisible by $\mathtt{LT}(f_1), \dots, \mathtt{LT}(f_s)$ and
2. if $a_i f_i \neq 0$, then multideg$(f) \geqslant$ multideg$(a_i f_i)$.

Polynomial r is called a remainder of f on division by F, denoted as $r = \overline{f}^F$.

Now, recall that in order to solve a polynomial f in one unknown with eigenvectors, we have used that the remainders on division by f were defined by f uniquely. Since the number of coefficients in r was equal to the degree of f, each r was uniquely determined by its values on the roots of f. We could thus represent remainders as vectors in a linear space with coordinates being coefficients of r or values of r on the roots of f. This interplay between coefficients for r and values of r on the roots of f brought the eigenvector problem with the (companion) matrix composed of the coefficients of f and its eigenvectors containing evaluations of the standard monomials on the roots of f.

Unfortunately, the remainder on division by more than one polynomial in more than one unknown, as provided by the long division algorithm above, does not produce unique r. To see this, consider $f = x\,y^2 - x$ and $f_1 = x\,y + 1$, $f_2 = y^2 - 1$ and fix the monomial ordering as $y <_{lex} x$. Then, for the two possible orders of f_1 and f_2, we are getting different r's:

1. $f : (f_1, f_2)$

f	$=$	$a_{11} f_1$	$+$	$a_{12} f_2$	$+$	r_1
$x\,y^2 - x$	$=$	$y\,(x\,y + 1)$	$+$	$0\,(y^2 - 1)$	$+$	$(-x - y)$

2. $f : (f_2, f_1)$

f	$=$	$a_{21} f_2$	$+$	$a_{22} f_1$	$+$	r_2
$x\,y^2 - x$	$=$	$x\,(y^2 - 1)$	$+$	$0\,(x\,y + 1)$	$+$	0

Notice that no monomial of r_1, r_2 is divisible by any $\mathtt{LT}(f_k)$ as well as that multidegrees of $a_{ij} f_k$ are not larger than the multidegree of $\mathtt{LT}(f)$. We see that the properties in the Fact 3.5.4 does not uniquely define the remainders in multivariate and multipolynomial case.

Fortunately, we can always replace polynomials F by another set of more convenient polynomials G such that G generate the same ideal as F, i.e. $\langle G \rangle = \langle F \rangle$ in the standard notation, and the remainder on division of f by G is *unique* w.r.t. the change of the order of polynomials in G. The remainder still depends on $<_o$ chosen. Sets G with the above property are called *Gröbner bases* of ideal $\langle F \rangle$.

Gröbner bases G generate exactly the same set of solutions as polynomials F and can be obtained as "polynomial combinations" of polynomials F. We will next show how to do it by introducing a very classical Buchberger algorithm [2] for constructing a Gröbner basis G from given polynomials F.

After constructing a Gröbner basis G of F, we will be able to obtain unique remainders on division by G and, as in the univariate case, thus obtain a one-to-one mapping from remainders to a fine-dimensional vector space over $\mathbb{C}$ for polynomial systems with a finite number of solutions. We will thus get an eigenvalue/eigenvector problem providing the desired solutions to a multivariate and multipolynomial systems with a finite number of solutions.

3.5.5 Gröbner basis construction

Let us now present the most classical algorithm for constructing the *reduced Gröbner basis* G of an ideal $\langle F \rangle$ [2].

3.5.5.1 Gröbner basis construction for linear polynomial systems

To motivate the general algorithm, we will first look at the most familiar systems of polynomial equations, systems of linear polynomial equations. We have already presented an example above in paragraph 3.2. Here, we will introduce a more general system to illustrate additional effects related to the monomial ordering.

Consider the following system of linear polynomial equations

$$\begin{bmatrix} 2 & 4 & 2 & 1 & 7 \\ 2 & 4 & 1 & 2 & 8 \\ 1 & 2 & 3 & 1 & 4 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

and compute the reduced row echelon form [5] of the matrix of the above system by the Gauss-Jordan elimination [5] to get

$$\begin{bmatrix} 1 & 2 & 0 & 0 & 3 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

The reduced row echelon form is unique for a given order of unknowns. It provides the reduced Gröbner basis

$$G_1 = \{x_1 + 2\,x_2 + 3\,x_5, x_3, x_4 + x_5\}$$

of the ideal generated by $F = \{2\,x_1 + 4\,x_2 + 2\,x_3 + x_4 + 7\,x_5, 2\,x_1 + 4\,x_2 + x_3 + 2\,x_4 + 8\,x_5, x_1 + 2\,x_2 + 3\,x_3 + x_4 + 4\,x_5\}$ for monomial ordering $<_{lex1} = x_5 <_{lex} x_4 <_{lex} x_3 <_{lex} x_2 <_{lex} x_1$. Now, using the monomial ordering $<_{lex2} = x_2 <_{lex} x_1 <_{lex} x_5 <_{lex} x_4 <_{lex} x_3$, we reorder the columns of the matrix of the original system to [3 4 5 1 2] and thus get the corresponding "reordered" system

$$\begin{bmatrix} 2 & 1 & 7 & 2 & 4 \\ 1 & 2 & 8 & 2 & 4 \\ 3 & 1 & 4 & 1 & 2 \end{bmatrix} \begin{bmatrix} x_3 \\ x_4 \\ x_5 \\ x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

The reduced row echelon form of the reordered system is

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1/3 & -2/3 \\ 0 & 0 & 1 & 1/3 & 2/3 \end{bmatrix} \begin{bmatrix} x_3 \\ x_4 \\ x_5 \\ x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

which is the reduced Gröbner basis of

$$G_2 = \{x_3, x_4 - \frac{1}{3}x_1 - \frac{2}{3}x_2, x_5 + \frac{1}{3}x_1 + \frac{2}{3}x_2\}$$

of $\langle F \rangle$ w.r.t. the monomial ordering $<_{lex2}$.

We see that the matrix of the reduced row echelon form w.r.t. $<_{lex1}$ is not equal to the matrix of the reduced row echelon form w.r.t. $<_{lex2}$ and the corresponding reduced Gröbner bases are also different. In general, the reduced Gröbner basis obtained depends on the monomial ordering used. On the other hand, when there is a fininte number of sollutions to a linear system, i.e. one solution, then the row reduced echelon form is the identity for all orderings of unknowns.

3.5.5.2 Gröbner basis construction for non-linear polynomial systems

Let us now look at sytems of general polynomial equations. We will introduce Buchberger algorithm on a very simple example. Refer to [2] for complete theory and more examples.

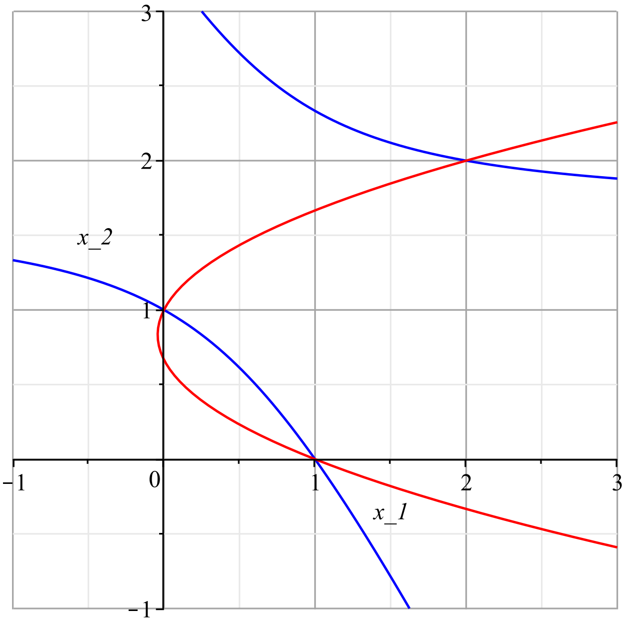


Figure 3.4: Solution to two conics $f_1 = 6\,x_1x_2 + 3\,x_2^2 - 10\,x_1 - 13\,x_2 + 10$, $f_2 = 3\,x_2^2 - 2\,x_1 - 5\,x_2 + 2$ are $[0,1], [1,0], [2,2]$ of multiplicity one.

Consider a polynomial system $F = [f_1, f_2]$ with

$$\begin{aligned} f_1 &= 6\,x_1x_2 + 3\,x_2^2 - 10\,x_1 - 13\,x_2 + 10 \\ f_2 &= 3\,x_2^2 - 2\,x_1 - 5\,x_2 + 2 \end{aligned} \tag{3.25}$$

Figure 3.4 shows that the system F has three solutions, all of multiplicity one. Ideal $\langle F\rangle$ is radical. We will use monomial ordering

$$<_o \equiv x_2 <_{grevlex} x_1$$

Monomials of F will be thus ordered as

$$1 <_o x_2 <_o x_1 <_o x_2^2 <_o x_1x_2$$

System 3.25 has three solutions. To get an eigenvalue/eigenvector problem, we need to find a multiplication matrix for a polynomial w.r.t. three monomials that will generate all remainders on the division by Gröbner basis of $\langle F\rangle$. With GRevLex ordering, we expect these to be the three smallest monomials $1, x_1, x_2$. Thus, all larger monomials, in particular x_1^2 must be reduced by the long division. However, polynomials in F do not reduce x_1^2 since there is no polynomial with leading term dividing x_1^2. We have to add more polynomials to the basis to be able to get x_1 as a remainder on the division by the basis.

The idea is to multiply f_1 and f_2 by the smallest monomials w.r.t. $<_o$ to cancel the leading terms and to construct a new polynomial, *S-polynomial* of f_1, f_2, which could potentially be reduceed to polynomial with leading x_1^2. This is a generalization of one step of Gaussian elimination when a new polynomial was constructed by canceling the leading unknown, the leading monomial of degree one.

Leading monomials of f_1, f_2 have the least common multiple $\mathtt{LCM}(x_1x_2, x_2^2) = x_1x_2^2$. Hence, to cancel the leading terms, we have to combine f_1 and f_2 by monomial coefficients as follows

$$\begin{aligned} S(f_1, f_2) &= \frac{x_2}{6}f_1 - \frac{x_1}{3}f_2 = \frac{x_1x_2^2}{6\,x_1x_2}f_1 - \frac{x_1x_2^2}{2\,x_2^2}f_2 = \frac{\mathtt{LCM}(\mathtt{LM}(f_1,f_2))}{\mathtt{LT}(f_1)}\,f_1 - \frac{\mathtt{LCM}(\mathtt{LM}(f_1,f_2))}{\mathtt{LT}(f_2)}\,f_2 \\ &= (3\,x_2^3 + 4\,x_1^2 - 13\,x_2^2 - 4\,x_1 + 10\,x_2)/6 \end{aligned} \tag{3.26}$$

Now, we will simplify $S(f_1, f_2)$ by reducing it by long division by f_1, f_2. This will remove large part of $S(f_1, f_2)$ that is contained in $\langle F\rangle$ and will guarantee that the $\mathtt{LM}(r)$ will not be too large, since it can't be divided by any `LM` of any polynomial in F.

$$f_3 = \overline{S(f_1, f_2)}^F = S(f_1, f_2) :_{<_o} (f_1, f_2) = 3\,x_1^2 - 5\,x_1 - 2\,x_2 + 2 \tag{3.27}$$

Next, construct a new set of polynomials $G = [f_1, f_2, 6\,f_3]$ with

$$\begin{aligned} f_1 &= 6\,x_1x_2 + 3\,x_2^2 - 10\,x_1 - 13\,x_2 + 10 \\ f_2 &= 3\,x_2^2 - 2\,x_1 - 5\,x_2 + 2 \\ f_3 &= 3\,x_1^2 - 5\,x_1 - 2\,x_2 + 2 \end{aligned}$$

The above procedure has to be iterated further. For every pair of polynomials in G, we construct their S-polynomial and reduce it by G, add the remainder on division by G, by which we enlarge G, and so on.

Let us do one more step of the above procedure

$$\begin{aligned} \overline{S(f_1, f_2)}^G &= f_3 \\ \overline{S(f_1, f_3)}^G &= \overline{3\,x_1x_2^2 - 10\,x_1^2 - 3\,x_1x_2 + 4\,x_2^2 + 10\,x_1 - 4\,x_2}^G = 0 \\ \overline{S(f_2, f_3)}^G &= \overline{-2\,x_1^3 - 5\,x_1^2x_2 + 5\,x_1x_2^2 + 2\,x_2^3 + 2\,x_1^2 - 2\,x_2^2}^G = 0 \end{aligned}$$

We see that no new non-zero remainder has been generated and thus the set G become stable w.r.t. to generating S-polynomials from G followed by reduction by G. We have obtained a Gröbner basis G of $\langle F\rangle$.

We can still further simplify G to obtain the unique reduced Gröbner basis of $\langle F\rangle$. The idea is to remove all monomials from polynomials of G that can be divided by the leading terms of G. It is a generalization of Gauss-Jordan elimination. The reduced Gröbner basis is to a Gröbner basis as is the reduced row echelon form to a mere "Gaussian eliminated" system.

In our example, we see that there is monomial x_2^2 in f_1 that is divisible by the leading term x_2^2 of f_2, hence we can remove it by subtracting f_2 from f_1 (and then normalizing the resulting polynomial to get the leading coefficients equal to one) to get the reducer Gröbner basis $G_r = [g_1, g_2, g_3]$ with

$$\begin{aligned} g_1 &= x_1x_2 - \frac{4}{3}\,x_1 - \frac{4}{3}\,x_2 + \frac{4}{3} \\ g_2 &= x_2^2 - \frac{2}{3}\,x_1 - \frac{5}{3}\,x_2 + \frac{2}{3} \\ g_3 &= x_1^2 - \frac{5}{3}\,x_1 - \frac{2}{3}\,x_2 + \frac{2}{3} \end{aligned} \tag{3.28}$$

See Figure 3.5.

Notice that leading monomials of G_r, i.e. x_1x_2, x_2^2, and x_1^2 reduce all monomials except for the three monomials $1, x_1$, and x_2. These are the three desired monomials that will provide the basis of the linear space to form a multiplication matrix and to obtain an eigenvalue/eigenvector problem providing us with the solution to the original system F. See Figure 3.6.

3.5.6 Solving general radical systems by eigenvectors of a multiplication matrix

We will now generalize the procedure from paragraph 3.5.1 to ideals $\langle F\rangle$ generated by multiple multivariate polynomials F. We will illustrate the generalization on an example in two unknowns x_1, x_2.

We consider mapping $\mathcal{M}_g\colon \mathbb{Q}[x_1, x_2] \to \mathbb{Q}[x_1, x_2]$ by a polynomial $g \in \mathbb{Q}[x_1, x_2]$ defined by

$$\mathcal{M}_g(h) = \overline{(g\,h)}^G \quad \text{with a Gröbner basis } G \text{ of } F$$

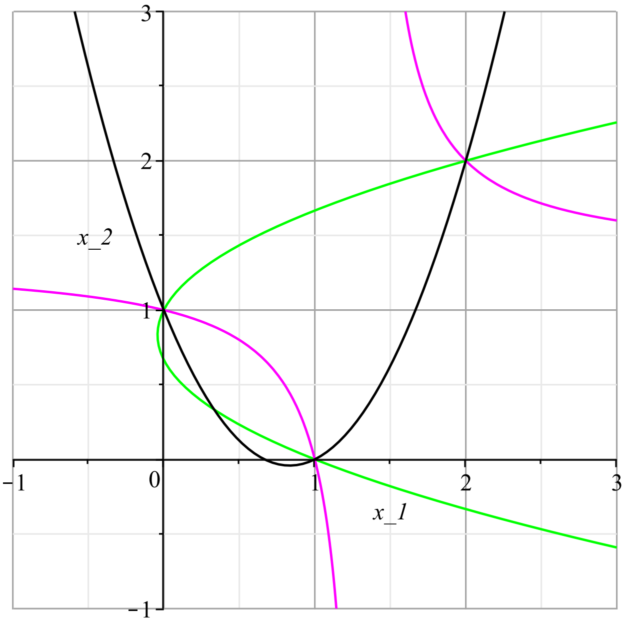


Figure 3.5: Three polynomials $g_1 = 3\,x_1x_2 - 4\,x_1 - 4\,x_2 + 4$, $g_2 = 3\,x_2^2 - 2\,x_1 - 5\,x_2 + 2$, $g_3 = 3\,x_1^2 - 5\,x_1 - 2\,x_2 + 2$ of the (un-normalized) reduced Gröbner basis G of $\langle F \rangle$.

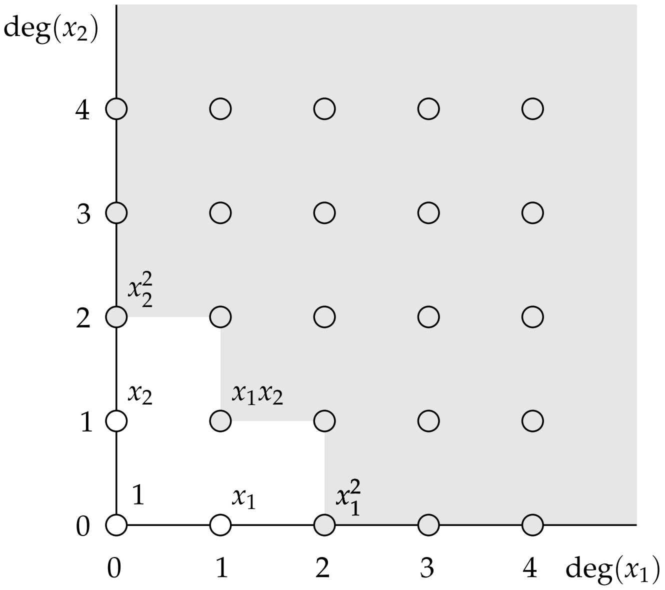


Figure 3.6: Standard monomials $x_1, x_2, 1$ of G from Equation 3.28 are not divisible by leading monomials x_1^2, x_1x_2, x_2^2 of G. All other monomials, shown in gray, are divisible by at least on of the leading monomials of G.

The reduction of $g\,h$ as well as the computation of G is carried out w.r.t. the same monomial ordering.

Next, consider that for a point $p_i = [p_{i1}, p_{i2}]^\top$, $g(p_i) = r(p_i)$ where $r = a_2x_2 + a_1x_1 + a_0$ is the remainder of g on division by G, i.e. $\overline{g}^G$. Thus

$$g(p_i) = r(p_i) = a_1x_1(p_i) + a_2x_2(p_i) + a_0 1(p_i) \tag{3.29}$$

We can thus write

$$\begin{aligned}
g(p_i)\begin{bmatrix} 1(p_i) \\ x_1(p_i) \\ x_2(p_i) \end{bmatrix} &= (a_1x_1(p_i) + a_2x_2(p_i) + a_0 1(p_i))\begin{bmatrix} 1(p_i) \\ x_1(p_i) \\ x_2(p_i) \end{bmatrix} \\
g(p_i)\begin{bmatrix} 1(p_i) \\ x_1(p_i) \\ x_2(p_i) \end{bmatrix} &= \left(a_1\,\mathtt{M}_{x_1}^\top + a_2\,\mathtt{M}_{x_2}^\top + a_0\mathtt{I}\right)\begin{bmatrix} 1(p_i) \\ x_1(p_i) \\ x_2(p_i) \end{bmatrix} \\
g(p_i)\begin{bmatrix} 1 \\ p_{i1} \\ p_{i2} \end{bmatrix} &= \left(a_1\,\mathtt{M}_{x_1}^\top + a_2\,\mathtt{M}_{x_2}^\top + a_0\mathtt{I}\right)\begin{bmatrix} 1 \\ p_{i1} \\ p_{i2} \end{bmatrix} \\
g(p_i)\,\vec{v}_i &= \mathtt{M}_g^\top\vec{v}_i
\end{aligned}$$

showing that $(g(p_i), \vec{v}_i)$ are eigenvalue-eigenvector pairs of $\mathtt{M}_g^\top = (a_1\,\mathtt{M}_{x_1} + a_2\,\mathtt{M}_{x_2} + a_0\mathtt{I})^\top$.

Let us now see how we can extract matrices $\mathtt{M}_{x_1}, \mathtt{M}_{x_2}$ given by G_r from Equation 3.28. We write G_r in a matrix form as

$$\begin{array}{c|cccccc|} & x_1^2 & x_1x_2 & x_2^2 & x_1 & x_2 & 1 \\ g_3 & 1 & 0 & 0 & -\frac{5}{3} & -\frac{2}{3} & \frac{2}{3} \\ g_1 & 0 & 1 & 0 & -\frac{4}{3} & -\frac{4}{3} & \frac{4}{3} \\ g_2 & 0 & 0 & 1 & -\frac{2}{3} & -\frac{5}{3} & \frac{2}{3} \end{array} \tag{3.30}$$

We see that

$$\begin{aligned}
\overline{x_1\begin{bmatrix} 1 \\ x_1 \\ x_2 \end{bmatrix}}^G &= \overline{\begin{bmatrix} x_1 \\ x_1^2 \\ x_1x_2 \end{bmatrix}}^G = \begin{bmatrix} 0 & 1 & 0 \\ -\frac{2}{3} & \frac{5}{3} & \frac{2}{3} \\ -\frac{4}{3} & \frac{4}{3} & \frac{4}{3} \end{bmatrix}\begin{bmatrix} 1 \\ x_1 \\ x_2 \end{bmatrix} \quad \text{and thus} \quad \mathtt{M}_{x_1} = \begin{bmatrix} 0 & 1 & 0 \\ -\frac{2}{3} & \frac{5}{3} & \frac{2}{3} \\ -\frac{4}{3} & \frac{4}{3} & \frac{4}{3} \end{bmatrix} \\
\overline{x_2\begin{bmatrix} 1 \\ x_1 \\ x_2 \end{bmatrix}}^G &= \overline{\begin{bmatrix} x_2 \\ x_1x_2 \\ x_2^2 \end{bmatrix}}^G = \begin{bmatrix} 0 & 1 & 0 \\ -\frac{4}{3} & \frac{4}{3} & \frac{4}{3} \\ -\frac{2}{3} & \frac{2}{3} & \frac{5}{3} \end{bmatrix}\begin{bmatrix} 1 \\ x_1 \\ x_2 \end{bmatrix} \quad \text{and thus} \quad \mathtt{M}_{x_2} = \begin{bmatrix} 0 & 1 & 0 \\ -\frac{4}{3} & \frac{4}{3} & \frac{4}{3} \\ -\frac{2}{3} & \frac{2}{3} & \frac{5}{3} \end{bmatrix}
\end{aligned}$$

Now, since the system F has three solutions with multiplicity one, ideal $\langle F \rangle$ is radical. Also, since all three solutions have pairwise distinct x_1 (as well as x_2) coordinates $0, 1, 2$, Figure 3.4, we can choose $g = x_1$ and thus $\mathtt{M}_g = \mathtt{M}_{x_1}$. We calculate eigenvectors of $\mathtt{M}_{x_1}$ and get three one-dimensional bases of the three respective separated one-dimensional eigenspaces

$$\text{eigenvectors}(\mathtt{M}_{x_1}) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 2 \\ 0 & 1 & 2 \end{bmatrix} \text{ corresponding to evaluation of } \begin{bmatrix} 1 \\ x_1 \\ x_2 \end{bmatrix} \text{ on solutions } (p_1, p_2, p_3)$$

We thus get three solutions $[1, 0], [0, 1], [2, 2]$ to the system F.

3.5.6.1 Recovering the solutions from the eigenvectors of the multiplication matrix

In the above example, the standard monomial basis $[1, x_1, x_2]$ contained all unknowns and thus it was easy to "read off" the solutions from the eigenvectors of $\mathtt{M}_g$. This is not a general behavior.

For instance, when the number of solutions is smaller than the number of unknowns, the standard monomial basis can't include all unknowns.

To recover solutions in a general case, we realize that every unknown x_i can be expressed as a linear combination of the basis B an thus evaluated at a solution p_j as

$$x_i(p_j) = (x_i \bmod J)(p_j) = (\sum_{b \in \mathtt{B}} a_b\, b)(p_j) = \sum_{b \in \mathtt{B}} a_b\, b((p_j) \tag{3.31}$$

3.5.6.2 Maple implementation

The following Maple [16] implementation[6] of a method for solving polynomial equations works for a general system of polynomial equations with a finite number of solutions.

The coefficient vector of a polynomial f w.r.t. a monomial basis B

```
> fB2Coffs:=proc(f,B)
                local m, t;
                t:=table(zip((a,b)->b=a,[coeffs(f,B,'m')],[m]));
                map(b->`if`(assigned(t[b]),t[b],0),B)
            end proc:
```

Take a general (non-radical) polynomial system with a finite number of solutions

> F:= $\{(x1^2 + x2^2 + x3^2 - 1)^2, (3 * x1 - 1)^2, (3 * x2 - 2)^2\}$:

and compute its radical ideal.

```
> J:=PolynomialIdeals[Radical](PolynomialIdeals[PolynomialIdeal](F)):
```

J := $< 3 * x1 - 1, 3 * x2 - 2, 9 * x3^2 - 4 >$

Use GRevLex monomial ordering

```
> o:=tdeg(op(indets(F)));
  o := tdeg(x1, x2, x3)
```

Construct the standard monomial basis of QQ[x1,x2,x3]/J for tdeg(x1, x2, x3)

```
> B:=Groebner[NormalSet](J,o)[1];
  B := [1, x3]
```

Take a random (but accidentally a very nice :-) linear function f

```
> f:=add(zip((x,y)->x*y,convert(RandomVector(nops(o)),list),[op(o)]));
  f := 9*x1+9*x2+9*x3
```

and find f*B mod J

```
> fBmJ:=Groebner[NormalForm](map(b->f*b,B),J,o);
  fBmJ := [9*x3+9, 9*x3+4]
```

Construct matrix $\mathtt{M}^\top$ such that f*B mod J = M*B

```
> Mt:=Matrix(map(f->fB2Coffs(f,B),fBmJ));
```

Mt := $\begin{bmatrix} 9 & 9 \\ 4 & 9 \end{bmatrix}$

Eigenvectors of $\mathtt{M}^T$

```
> V:=LinearAlgebra[Eigenvectors](Mt)[2];
```

V := $\begin{bmatrix} 3/2 & -3/2 \\ 1 & 1 \end{bmatrix}$

Normalize V to have ones in the first row

```
> V:=V.LinearAlgebra[MatrixInverse](LinearAlgebra[DiagonalMatrix](V[1]));
```

Mt := $\begin{bmatrix} 1 & 1 \\ 2/3 & -2/3 \end{bmatrix}$

Express unknowns x1, x2, x3 in the basis B

```
> N:=Groebner[NormalForm]([op(o)],J,o);
  N := [1/3, 2/3, x3]
```

[6] This implementation was obtained in collaboration with Justin Chen.

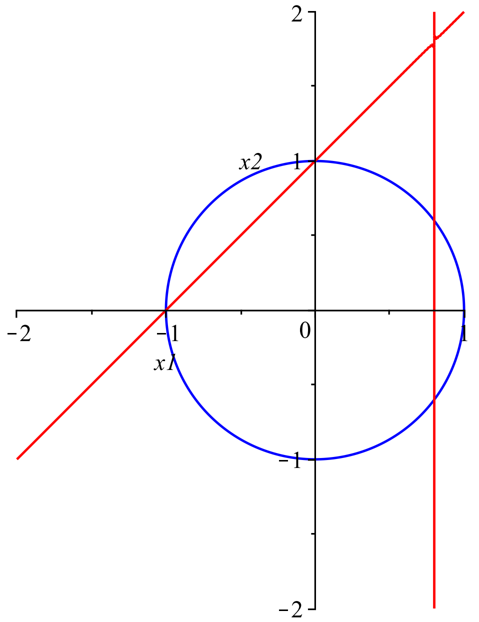


Figure 3.7: System $F = [x_1^2 + x_2^2 - 1, (5\,x_1 - 4)\,(x_2 - x_1 - 1)]$ generates radical ideal but has higher-dimensional eigenspace of the multiplication matrix w.r.t. x_1.

```
> C:=map(n->fB2Coffs(n,B),N);
  C := [[1/3, 0], [2/3, 0], [0, 1]]
Evaluate unknowns by combining the basis B with coefficients C
> S:=[ListTools[Transpose](map(c->convert(Matrix(c).V,list),C)),[op(o)]];
  S := [[[1/3, 2/3, 2/3], [1/3, 2/3, -2/3]], [x1, x2, x3]]
```

The important step in the above implementation is the construction of a radial ideal of the input system. This is computationally intensive process in general. Let us next present examples of radical and non-radical systems to understand what happens when we tried to use the above procedure on a system that generates a non-radical ideal.

3.5.6.3 General method for radical ideals

Radical ideals still may produce eigenspaces of higher dimension than one. Consider, for instance the system

$$F = [x_1^2 + x_2^2 - 1, (5\,x_1 - 4)\,(x_2 - x_1 - 1)]$$

see Figure 3.7.

Ideal $I = \langle F \rangle$ is radical. The generators for the elimination ideals $I \cap \mathbb{C}[x_1]$, resp. $I \cap \mathbb{C}[x_2]$, are $x_1\,(1 + x_1)\,(5\,x_1 - 4)$, resp. $x_2\,(-1 + x_2)\,(5\,x_2 - 3)(5\,x_2 + 3)$, which are square-free.

When selecting the standard monomials as $\begin{bmatrix} 1 & x_1 & x_2 & x_1^2 \end{bmatrix}$, we get the corresponding multiplication matrix

$$\mathtt{M}_{x_1} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ -\frac{4}{5} & \frac{1}{5} & \frac{4}{5} & 1 \\ 0 & \frac{4}{5} & 0 & -\frac{1}{5} \end{bmatrix} \text{ with e/v } -1/\left\langle \begin{bmatrix} 1 \\ -1 \\ 0 \\ 1 \end{bmatrix} \right\rangle,\ (\frac{4}{5})^2/\left\langle \begin{bmatrix} 1 & 0 \\ \frac{4}{5} & 0 \\ 0 & 1 \\ \frac{16}{25} & 0 \end{bmatrix} \right\rangle \text{ and } 0/\left\langle \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} \right\rangle$$

Hence we can't read out the two complete solutions for $\frac{4}{5}$ directly from the basis of the corresponding eigenspace.

However, we can find a suitable polynomial f such that $\mathtt{M}_f$ has one-dimensional eigenspaces only. In this case, for instance, we may construct

$$\mathtt{M}_{x_1+x_2} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ -\frac{4}{5} & \frac{1}{5} & \frac{4}{5} & 2 \\ \frac{1}{5} & \frac{1}{5} & \frac{4}{5} & 0 \\ -\frac{16}{25} & -\frac{24}{25} & \frac{16}{25} & \frac{3}{5} \end{bmatrix} \text{ with e/v } \frac{1}{5}/\left\langle\begin{bmatrix} 1 \\ \frac{4}{5} \\ -\frac{3}{5} \\ \frac{16}{25} \end{bmatrix}\right\rangle, 1/\left\langle\begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}\right\rangle, \frac{7}{5}/\left\langle\begin{bmatrix} 1 \\ \frac{4}{5} \\ \frac{3}{5} \\ \frac{16}{25} \end{bmatrix}\right\rangle, -1/\left\langle\begin{bmatrix} 1 \\ -1 \\ 0 \\ 1 \end{bmatrix}\right\rangle$$

and thus get complete solutions from the second and third coordinate of the bases of the eigenspaces.

3.5.7 Solving general "non-radical" systems by eigenvectors of a multiplication matrix

Let us now look at systems that are not radical. This means, for systems with a finite number of solutions, that some of the solutions have multiplicity greater than one. In this situation, in general, the multiplication matrices for a general polynomial g may have eigenvalues of greater multiplicities and thus eigenspaces of dimension greater than one. In such a case, it is not so clear how to extract solutions from the bases of the eigenspaces.

In principal, there are three approaches how to solve this. The first approach is to obtain a radical ideal $\sqrt{\langle F \rangle}$ of $\langle F \rangle$ and proceed as above. The second approach would be to use the fact that eigenvectors common to all multiplication matrices by all polynomials are in one dimensional eigenspaces [14], and, third, it would be possible to follow [17] and to get a more general algorithm for non-radical systems. Let us next show an example of using the first approach.

Consider the system $F = [f_1, f_2]$, Equation 3.2,

$$\begin{aligned} f_1 &= x_2^2 + x_1^2 - 1 = 0 \\ f_2 &= 25\,x_1 x_2 - 20\,x_2 - 15\,x_1 + 12 = 0 \end{aligned}$$

This system does not generate a radical ideal since some of the solutions have higher multiplicities.

Let us follow the procedure above. The (up to multiplication by a constant) reduced Gröbner basis G of F is, w.r.t. $x_1 <_{lex} x_2$,

$$G = [x_2^2 + x_1^2 - 1, 25\,x_1 x_2 - 20\,x_2 - 15\,x_1 + 12, 125\,x_1^3 - 100\,x_1^2 - 80\,x_1 + 64]$$

which actually consists of the polynomials f_1, f_3, f_4 from Equation 3.5. The standard monomials w.r.t. to G are $[1, x_1, x_1^2, x_2]$. These are all the monomials smaller than the leading monomials of polynomials in G, i.e. $x_2^2, x_1 x_2, x_1^3$, w.r.t. $x_1 <_{lex} x_2$.

Also notice that these standard monomials are not all in x_1 despite using $x_1 <_{lex} x_2$. The reason is that the four solutions (when counting the multiplicities) project only to two solutions in x_1 with one solution of multiplicity two. The solution $[\frac{4}{5}, \frac{3}{5}]^\top$ of multiplicity two "masks" the simple solution $[\frac{4}{5}, -\frac{3}{5}]^\top$.

The matrix representing the multiplication by x_1 modulo G is

$$\mathtt{M}_{x_1} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -\frac{64}{125} & \frac{16}{25} & \frac{4}{5} & 0 \\ -\frac{12}{25} & \frac{3}{5} & 0 & \frac{4}{5} \end{bmatrix} \text{ with eigenvalue/eigenspace } \frac{4}{5}/\left\langle\begin{bmatrix} 0 & 1 \\ 0 & \frac{4}{5} \\ 0 & \frac{16}{25} \\ 1 & 0 \end{bmatrix}\right\rangle \text{ and } -\frac{4}{5}/\left\langle\begin{bmatrix} 1 \\ -\frac{4}{5} \\ \frac{16}{25} \\ \frac{3}{5} \end{bmatrix}\right\rangle$$

The multiplicity of eigenvalue $\frac{4}{5}$ is three and it has associated a two-dimensional eigenspace. The multiplicity of eigenvalue $-\frac{4}{5}$ is one and thus it has associated a one-dimensional eigenspace. The basis of the eigenspace associated to eigenvalue $\frac{4}{5}$ does not directly provide the two solutions related to $x_1 = \frac{4}{5}$. On the other hand the basis of the one-dimensional eigenspace corresponding to the eigenvalue $-\frac{4}{5}$ provides the solution $[-\frac{4}{5}, \frac{3}{5}]^\top$.

Let's try to multiply by another polynomial, e.g. by $x_2 - x_1$. We keep the same Gröbner basis as well as monomial ordering $x_1 <_{lex} x_2$. So, now we get the multiplication matrix

$$\mathtt{M}_{x_2-x_1} = \begin{bmatrix} 0 & -1 & 0 & 1 \\ -\frac{12}{25} & \frac{3}{5} & -1 & \frac{4}{5} \\ \frac{16}{125} & -\frac{16}{25} & -\frac{1}{5} & \frac{16}{25} \\ \frac{37}{25} & -\frac{3}{5} & -1 & -\frac{4}{5} \end{bmatrix} \text{ with } -\frac{1}{5}/\left\langle \begin{bmatrix} 1 \\ \frac{4}{5} \\ \frac{16}{25} \\ \frac{3}{5} \end{bmatrix} \right\rangle, -\frac{7}{5}/\left\langle \begin{bmatrix} 1 \\ \frac{4}{5} \\ \frac{16}{25} \\ -\frac{3}{5} \end{bmatrix} \right\rangle \text{ and } \frac{7}{5}/\left\langle \begin{bmatrix} 1 \\ -\frac{4}{5} \\ \frac{16}{25} \\ \frac{3}{5} \end{bmatrix} \right\rangle$$

and we see that, in this case, we were lucky to find a polynomial $x_2 - x_1$ that provided three separated one-dimensional eigenspaces. The reason is that the double eigenvalue $-\frac{1}{5}$ has a "defective eigenspace" [5] of dimension only one and hence we do not suffer from having a derogatory matrix with a higher-dimensional eigenspace.

We can read out the solutions from the second and the third coordinate of the three normalized eigenvectors above.

In general, unfortunately, there are systems for which the multiplication by no polynomial gives only one-dimensional eigenspaces for all eigenvalues [14]. To illustrate this, we will consider the system

$$F = [(x_1 - 1)^2, (x_2 - 1)^2]$$

The reduced Gröbner basis G of F is w.r.t. $x_2 <_{lex} x_1$

$$G = [x_1^2 - 2\,x_1 + 1, x_2^2 - 2\,x_2 + 1]$$

The standard monomials w.r.t. to G are $[1, x_2, x_1, x_1x_2]$. The matrix representing the multiplication by x_1 modulo G is

$$\mathtt{M}_{x_1} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 2 & 0 \\ 0 & -1 & 0 & 2 \end{bmatrix} \text{ with eigenvalue/eigenspace } 1/\left\langle \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \right\rangle$$

The matrix representing the multiplication by $x_2 - x_1$ modulo G is

$$\mathtt{M}_{x_2-x_1} = \begin{bmatrix} 0 & 1 & -1 & 0 \\ -1 & 2 & 0 & -1 \\ 1 & 0 & -2 & 1 \\ 0 & 1 & -1 & 0 \end{bmatrix} \text{ with eigenvalue/eigenspace } 1/\left\langle \begin{bmatrix} 1 & 1 \\ 0 & \frac{1}{2} \\ 0 & \frac{1}{2} \\ -1 & 0 \end{bmatrix} \right\rangle$$

We see that we always get a two-dimensional eigenspace and it is not possible to just read out the solutions from the basic vectors of the eigenspaces.

3.5.7.1 General solution

To present a general method, we will consider a system obtained from 3.2 by squaring the first equation, i.e.

$$F = [(x_2^2 + x_1^2 - 1)^2, 25\,x_1x_2 - 20\,x_2 - 15\,x_1 + 12]$$

The Gröbner basis (reduced up to a multiplication by a constant) G of F is, w.r.t. $x_1 <_{lex} x_2$,

$$\begin{aligned} G = \; [\;& 3125\,x_1^5 - 1875\,x_1^4 - 2250\,x_1^3 + 1350\,x_1^2 + 405\,x_1 - 243, \\ & 25\,x_1\,x_2 - 20\,x_1 - 15\,x_2 + 12, \\ & 625\,x_1^4 + 625\,x_2^4 - 450\,x_1^2 - 800\,x_2^2 + 337 \quad] \end{aligned}$$

The standard monomials w.r.t. to G and $x_1 <_{lex} x_2$

$$[1, x_1, x_1^2, x_1^3, x_1^4, x_2, x_2^2, x_2^3]$$

The matrix representing the multiplication by a general linear polynomial $3\,x_1 + 4\,x_2$ modulo G w.r.t. $x_1 <_{lex} x_2$ is

$$\mathtt{M}_{3\,x_1+4\,x_2} = \begin{bmatrix} 0 & 3 & 0 & 0 & 0 & 5 & 0 & 0 \\ -\frac{12}{5} & 4 & 3 & 0 & 0 & 3 & 0 & 0 \\ -\frac{36}{25} & 0 & 4 & 3 & 0 & \frac{9}{5} & 0 & 0 \\ -\frac{108}{125} & 0 & 0 & 4 & 3 & \frac{27}{25} & 0 & 0 \\ -\frac{891}{3125} & -\frac{243}{625} & -\frac{162}{125} & \frac{54}{25} & \frac{29}{5} & \frac{81}{125} & 0 & 0 \\ -\frac{36}{25} & \frac{12}{5} & 0 & 0 & 0 & \frac{9}{5} & 5 & 0 \\ -\frac{144}{125} & \frac{48}{25} & 0 & 0 & 0 & 0 & \frac{9}{5} & 5 \\ -\frac{2261}{625} & \frac{192}{125} & \frac{18}{5} & 0 & -5 & 0 & \frac{32}{5} & \frac{9}{5} \end{bmatrix}$$

The eigenvalue/eigenspace of $\mathtt{M}_{3\,x_1+4\,x_2}$ are as follows

$$\frac{29}{5}/\left\langle \begin{bmatrix} 1 & 1 \\ \frac{19}{15} & \frac{47}{45} \\ \frac{29}{21} & \frac{67}{75} \\ \frac{117}{125} & \frac{87}{125} \\ \frac{441}{625} & \frac{321}{625} \\ \frac{2}{5} & \frac{8}{15} \\ 0 & \frac{16}{75} \\ \frac{32}{125} & 0 \end{bmatrix} \right\rangle, \frac{11}{5}/\left\langle \begin{bmatrix} 1 \\ -\frac{3}{5} \\ \frac{9}{25} \\ -\frac{27}{125} \\ \frac{81}{625} \\ \frac{4}{5} \\ \frac{16}{25} \\ \frac{64}{125} \end{bmatrix} \right\rangle, -\frac{11}{5}/\left\langle \begin{bmatrix} 1 \\ \frac{3}{5} \\ \frac{9}{25} \\ \frac{27}{125} \\ \frac{81}{625} \\ -\frac{4}{5} \\ \frac{16}{25} \\ -\frac{64}{125} \end{bmatrix} \right\rangle \text{ corresponding to } \begin{bmatrix} 1 \\ x_1 \\ x_1^2 \\ x_1^3 \\ x_1^4 \\ x_2 \\ x_2^2 \\ x_2^3 \end{bmatrix}$$

Eigenvalues $\frac{11}{5}$ and $-\frac{11}{5}$ are of multiplicity two and both have defective eigenspaces of dimension one. Eigenvalue $\frac{29}{5}$ is of multiplicity four and has a defective eigenspace of dimension two.

We see that the solution $[\frac{3}{5}, \frac{4}{5}]$ is buried in a two dimensional eigenspace and can't be directly read out. Since we were using a random generic polynomial $3\,x_1 + 4\,x_2$, we can't expect to solve this system as is by the eigenvector method.

Let us now find the radical system generating $\sqrt{\langle F \rangle}$ and use it to compute the solutions to the original system F. To do that, we need to generate univariate polynomials in x_1 and x_2 in $\langle F \rangle$ and get their corresponding square-free polynomials, which we then add to F.

One way to get the univariate polynomials is to construct Gröbner bases G_{x_1} w.r.t. $x_1 <_{lex} x_2$ and G_{x_2} w.r.t. $x_2 <_{lex} x_1$. We get

$$\begin{aligned} G_{x_1} &= [\,(5\,x_1+3)^2\,(5\,x_1-3)^3, (5\,x_1-3)\,(5\,x_2-4), 625\,x_1^4 + 625\,x_2^4 - 450\,x_1^2 - 800\,x_2^2 + 337\,] \\ G_{x_2} &= [\,(5\,x_2+4)^2\,(5\,x_2-4)^3, (5\,x_1-3)\,(5\,x_2-4), 625\,x_1^4 + 625\,x_2^4 - 450\,x_1^2 - 800\,x_2^2 + 337\,] \end{aligned}$$

The univariate polynomial in G_{x_1}, resp. G_{x_2}, is

$$g_1 = (5\,x_1+3)^2\,(5\,x_1-3)^3 \quad \text{resp.} \quad g_2 = (5\,x_2+4)^2\,(5\,x_2-4)^3$$

We want to construct square-free polynomials

$$\begin{aligned}
f_3 &= \frac{g_1}{\mathrm{GCD}\left(g_1, \frac{\partial g_1}{\partial x_1}\right)} = \frac{(5\,x_1+3)^2\,(5\,x_1-3)^3}{\mathrm{GCD}\left((5\,x_1+3)^2\,(5\,x_1-3)^3, 5\,(5\,x_1+3)\,(5\,x_1-3)^2(25\,x_1+3)\right)} \\
&= \frac{(5\,x_1+3)^2\,(5\,x_1-3)^3}{(5\,x_1+3)(5\,x_1-3)^2} = (5\,x_1+3)(5\,x_1-3) \\
f_4 &= \frac{g_2}{\mathrm{GCD}\left(g_2, \frac{\partial g_2}{\partial x_2}\right)} = \frac{(5\,x_2+4)^2\,(5\,x_2-4)^3}{\mathrm{GCD}\left((5\,x_2+4)^2\,(5\,x_2-4)^3, 5\,(5\,x_2+4)(5\,x2-4)^2(25\,x_2+4)\right)} \\
&= \frac{(5\,x_2+4)^2\,(5\,x_2-4)^3}{(5\,x_2+4)(5\,x_2-4)^2} = (5\,x_2+4)(5\,x_2-4)
\end{aligned}$$

The radical ideal $\sqrt{\langle F\rangle}$ will now be

$$\sqrt{\langle F\rangle} = \langle (x_2^2+x_1^2-1)^2, 25\,x_1x_2-20\,x_2-15\,x_1+12, (5\,x_1+3)(5\,x_1-3), (5\,x_2+4)(5\,x_2-4)\rangle$$

giving Gröbner basis $\sqrt{G} = [25\,x_1^2-9, 25\,x_1x_2-20\,x_1-15\,x_2+12, 25\,x_2^2-16]$ w.r.t. $x_1 <_{lex} x_2$. The standard monomials w.r.t. $x_1 <_{lex} x_2$ are $[1, x_1, x_2]$ and the multiplication matrix for $3\,x_1+4\,x_2$ is

$$\mathtt{M}_{3\,x_1+4\,x_3} = \begin{bmatrix} 0 & 3 & 5 \\ -\frac{33}{25} & 4 & 3 \\ \frac{44}{25} & \frac{12}{5} & \frac{9}{5} \end{bmatrix} \text{ with e/v as } \frac{11}{5}/\left\langle \begin{bmatrix} 1 \\ -\frac{3}{5} \\ \frac{4}{5} \end{bmatrix} \right\rangle, \frac{29}{5}/\left\langle \begin{bmatrix} 1 \\ \frac{3}{5} \\ \frac{4}{5} \end{bmatrix} \right\rangle, -\frac{11}{5}/\left\langle \begin{bmatrix} 1 \\ \frac{3}{5} \\ -\frac{4}{5} \end{bmatrix} \right\rangle$$

We see that, now, we can directly read out all the solutions to the system.

4 Affine space

Let us study the affine space, an important structure underlying geometry and its algebraic representation. The affine space is closely connected to the linear space. The connection is so intimate that the two spaces are sometimes not even distinguished. Consider, for instance, function $f\colon \mathbb{R} \to \mathbb{R}$ with non-zero $a, b \in \mathbb{R}$

$$f(x) = a\,x + b \tag{4.1}$$

It is often called "linear" but it is not a *linear function* [6, 7, 5] since for every $\alpha \in \mathbb{R}$ there holds

$$f(\alpha\,x) = \alpha\,a\,x + b \neq \alpha\,(a\,x + b) = \alpha\,f(x) \tag{4.2}$$

In fact, f is an *affine function*, which becomes a linear function only for $b = 0$.

In geometry, we need to be very precise and we have to clearly distinguish affine from linear. Let us therefore first review the very basics of linear spaces, and in particular their relationship to geometry, and then move to the notion of affine spaces.

4.1 Vectors

Let us start with geometric vectors and study the rules of their manipulation.

Figure 4.1(a) shows the space of points P, which we live in and intuitively understand. We know what is an oriented line segment, which we also call a *marked ruler* (or just a ruler). A marked ruler is oriented from its origin towards its end, which is actually a mark (represented by an arrow in Figure 4.1(b)) on a thought infinite ruler, Figure 4.1(b). We assume that we are able to align the ruler with any pair of points x, y, so that the ruler begins in x and a mark is made at the point y. We also know how to align a marked ruler with any pair of distinct points u, v such that the ruler begins in u and aligns with the line connecting u and v in the direction towards point v. The mark on so aligned ruler determines another point, call it z, which is collinear with points u, v. We know how to translate, Figure 4.1(c), a ruler in this space.

To define geometric vectors, we need to first define geometric scalars.

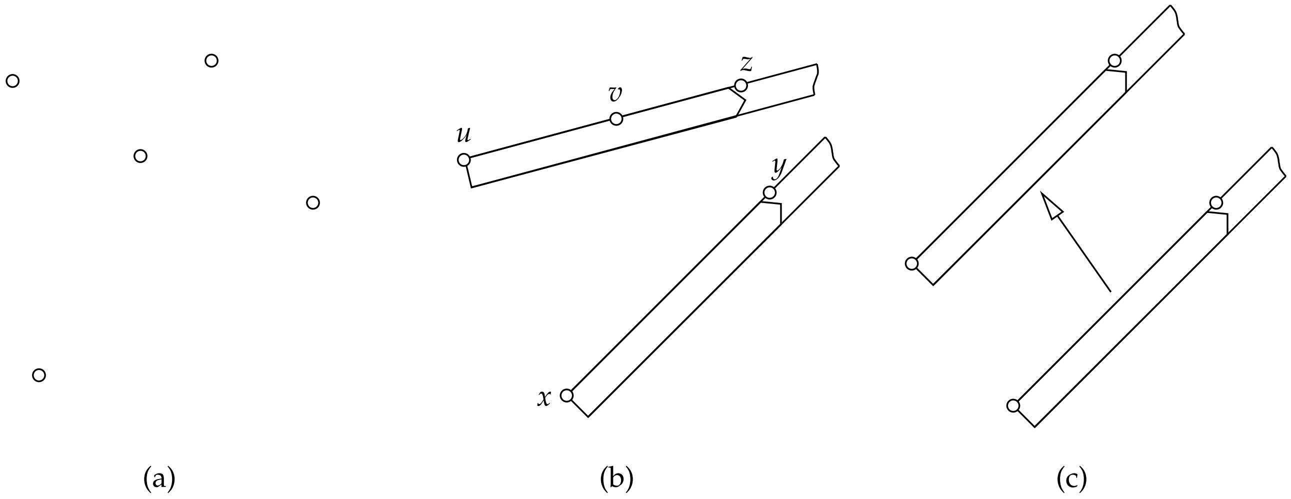


Figure 4.1: (a) The space around us consists of points. Rulers (marked oriented line segments) can be aligned (b) and translated (c) and thus used to transfer, but not measure, distances.

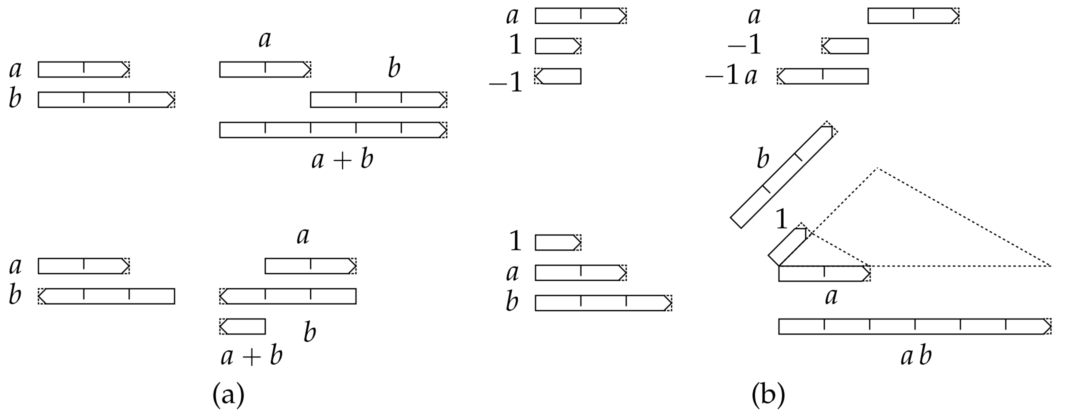


Figure 4.2: Scalars are represented by oriented rulers. They can be added (a) and multiplied (b) purely geometrically by translating and aligning rulers. Notice that we need to single out a unit scalar "1" to perform geometric multiplication.

4.1.1 Geometric scalars

Geometric scalars S are horizontal oriented rulers. The ruler, which has its origin identical with its end is called 0. Geometric scalars are equipped with two geometric operations, addition $a + b$ and multiplication $a\, b$, defined for every two elements $a, b \in S$.

Figure 4.2(a) shows addition $a + b$. We translate ruler b to align origin of b with the end of a and obtain ruler $a + b$.

Figure 4.2(b) shows multiplication $a\, b$. To perform multiplication, we choose a unit ruler "1" and construct its additive inverse -1 using $1 + (-1) = 0$. This introduces orientation to scalars. Scalars aiming to the same side as 1 are *positive* and scalars aiming to the same side as -1 are *negative*. Scalar 0 is neither positive, nor negative. Next we define multiplication by -1 such that $-1\, a = -a$, i.e. -1 times a equals the additive inverse of a. Finally, we define multiplication of non-negative (i.e. positive and zero) rulers a, b as follows. We align a with 1 such that origins of 1 and a coincide and such that the rulers contain an acute non-zero angle. We align b with 1 and construct ruler $a\, b$ by a translation, e.g. as shown in Figure 4.2(b)[1].

All constructions used were purely geometrical and were performed with real rulers. We can verify that so defined addition and multiplication of geometric scalars satisfy all rules of addition and multiplication of real numbers. Geometric scalars form a field [11, 18] w.r.t. to $a + b$ and $a\, b$.

4.1.2 Geometric vectors

Ordered pairs of points, such as (x, y) in Figure 4.3(a), are called *geometric vectors* and denoted as $\vec{xy}$, i.e. $\vec{xy} = (x, y)$. Symbol $\vec{xy}$ is often replaced by a simpler one, e.g. by $\vec{a}$. The set of all geometric vectors is denoted by A.

4.1.3 Bound vectors

Let us now choose one point o and consider all pairs (o, x), where x can be any point, Figure 4.3(a). We obtain a subset A_o of A, which we call *geometric vectors bound to* o, or just *bound vectors* when it is clear to which point they are bound. We will write $\vec{x} = (o, x)$. Figure 4.3(f) shows another bound vector $\vec{y}$. The pair (o, o) is special. It will be called the *zero bound vector* and denoted by $\vec{0}$. We will introduce two operations $\oplus, \odot$ with bound vectors.

[1] Notice that $a\, b$ is well defined since it is the same for all non-zero angles contained by a and 1.

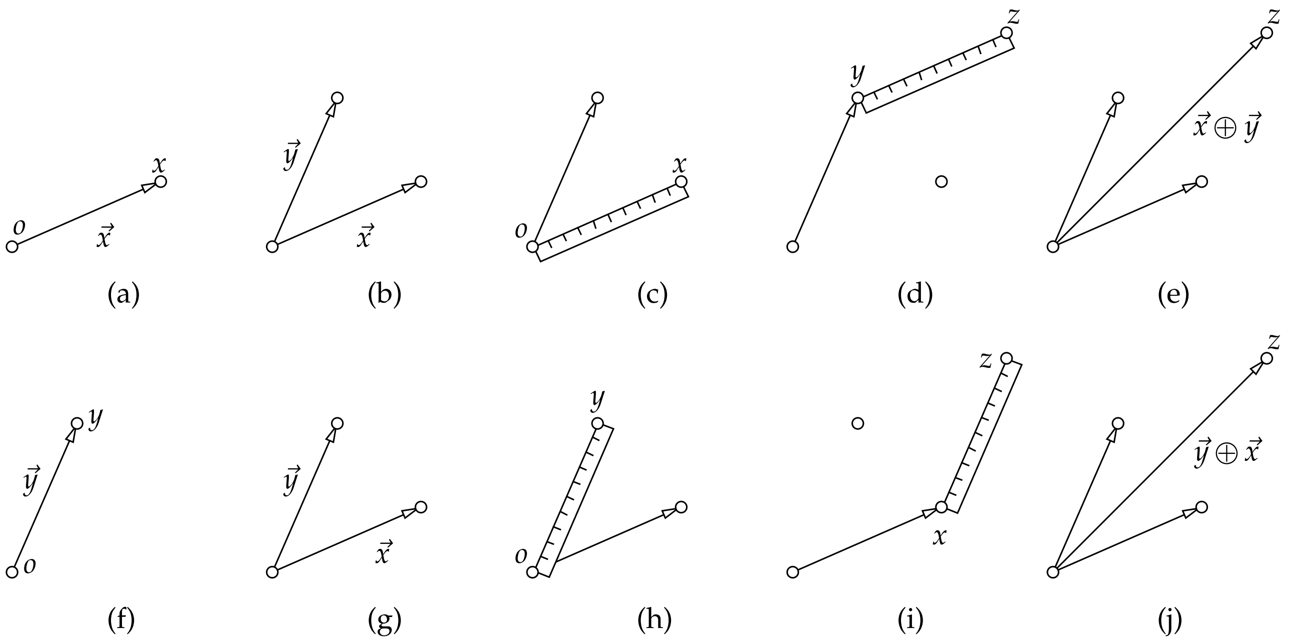


Figure 4.3: Bound vectors are (ordered) pairs of points (o, x), i.e. arrows $\vec{x} = (o, x)$. Addition of the bound vectors $\vec{x}$, $\vec{y}$ is realized by parallel transport (using a ruler). We see that the result is the same whether we add $\vec{x}$ to $\vec{y}$ or $\vec{y}$ to $\vec{x}$. Addition is commutative.

First we define *addition of bound vectors* $\oplus$: $A_o \times A_o \rightarrow A_o$. Let us add vector $\vec{x}$ to $\vec{y}$ as shown on Figure 4.3(b). We take a ruler and align it with $\vec{x}$, Figure 4.3(c). Then we translate the ruler to align its begin with point y, Figure 4.3(d). The end of the ruler determines point z. We define a new bound vector, which we denote $\vec{x} \oplus \vec{y}$, as the pair (o, z), Figure 4.3(e). Figures 4.3(f-j) demonstrate that addition gives the same result when we exchange (*commute*) vectors $\vec{x}$ and $\vec{y}$, i.e. $\vec{x} \oplus \vec{y} = \vec{y} \oplus \vec{x}$. We notice that for every point x, there is exactly one point x' such that $(o, x) \oplus (o, x') = (o, o)$, i.e. $\vec{x} \oplus \vec{x}' = \vec{0}$. Bound vector $\vec{x}'$ is the *inverse* to $\vec{x}$ and is denoted as $-\vec{x}$. Bound vectors are invertible w.r.t. operation $\oplus$. Finally, we see that $(o, x) \oplus (o, o) = (o, x)$, i.e. $\vec{x} \oplus \vec{0} = \vec{x}$. Vector $\vec{0}$ is the *identity element* of the operation $\oplus$. Clearly, operation $\oplus$ behaves exactly as addition of scalars – it is a commutative group [11, 18].

Secondly, we define the *multiplication of a bound vector by a geometric scalar* $\odot$: $S \times A_o \rightarrow A_o$, where S are geometric scalars and A_o are bound vectors. Operation $\odot$ is a mapping which takes a geometric scalar (a ruler) and a bound vector and delivers another bound vector.

Figure 4.4 shows that to multiply a bound vector $\vec{x} = (o, x)$ by a geometric scalar a, we consider the ruler b whose origin can be aligned with o and end with x. We multiply scalars a and b to obtain scalar

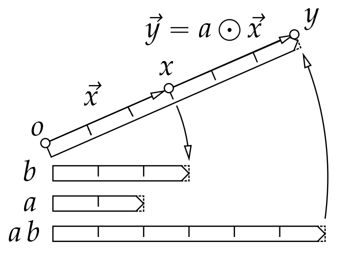


Figure 4.4: Multiplication of the bound vector $\vec{x}$ by a geometric scalar a is realized by aligning rulers to vectors and multiplication of geometric scalars.

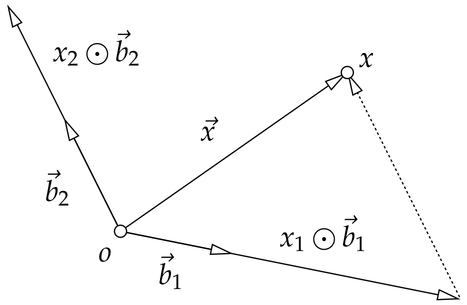


Figure 4.5: Coordinates are the unique scalars that combine independent basic vectors $\vec{b}_1$, $\vec{b}_2$ into $\vec{x}$.

$a\,b$ and align $a\,b$ with $\vec{x}$ such that the origin of $a\,b$ coincides with o and $a\,b$ extends along the line passing through $\vec{x}$. We obtain end point y of so placed $a\,b$ and construct the resulting vector $\vec{y} = a \odot \vec{x} = (o, y)$.

We notice that addition $\oplus$ and multiplication $\odot$ of horizontal bound vectors coincides exactly with the addition and multiplication of scalars.

4.2 Linear space

We can verify that for every two geometric scalars $a, b \in S$ and every three bound vectors $\vec{x}, \vec{y}, \vec{z} \in A_o$ with their respective operations, there holds the following eight rules

$$\begin{aligned}
\vec{x} \oplus (\vec{y} \oplus \vec{z}) &= (\vec{x} \oplus \vec{y}) \oplus \vec{z} && (4.3)\\
\vec{x} \oplus \vec{y} &= \vec{y} \oplus \vec{x} && (4.4)\\
\vec{x} \oplus \vec{0} &= \vec{x} && (4.5)\\
\vec{x} \oplus -\vec{x} &= \vec{0} && (4.6)\\
1 \odot \vec{x} &= \vec{x} && (4.7)\\
(a\,b) \odot \vec{x} &= a \odot (b \odot \vec{x}) && (4.8)\\
a \odot (\vec{x} \oplus \vec{y}) &= (a \odot \vec{x}) \oplus (a \odot \vec{y}) && (4.9)\\
(a + b) \odot \vec{x} &= (a \odot \vec{x}) \oplus (b \odot \vec{x}) && (4.10)
\end{aligned}$$

These rules are known as axioms of a *linear space* [6, 7, 4]. Bound vectors are one particular model of the linear space. There are many other very useful models, e.g. n-tuples of real or rational numbers for any natural n, polynomials, series of real numbers and real functions. We will give some particularly simple examples useful in geometry later.

The next concept we will introduce are *coordinates of bound vectors*. To illustrate this concept, we will work in a plane. Figure 4.5 shows two non-collinear bound vectors $\vec{b}_1$, $\vec{b}_2$, which we call *basis*, and another bound vector $\vec{x}$. We see that there is only one way how to choose scalars x_1 and x_2 such that vectors $x_1 \odot \vec{b}_1$ and $x_2 \odot \vec{b}_2$ add to $\vec{x}$, i.e.

$$\vec{x} = x_1 \odot \vec{b}_1 \oplus x_2 \odot \vec{b}_2 \tag{4.11}$$

Scalars x_1, x_2 are *coordinates* of $\vec{x}$ in (ordered) basis $[\vec{b}_1, \vec{b}_2]$.

4.3 Free vectors

We can choose any point from A to construct bound vectors and all such choices will lead to the same manipulation of bound vector and to the same axioms of a linear space. Figure 4.6 shows two such choices for points o and o'.

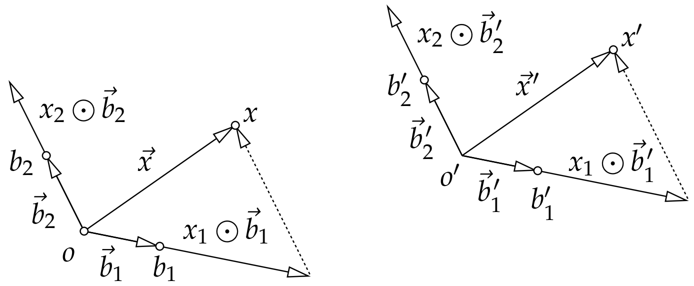


Figure 4.6: Two sets of bound vectors A_o and $A_{o'}$. Coordinates of $\vec{x}$ w.r.t. $[\vec{b}_1, \vec{b}_2]$ are equal to coordinates of $\vec{x}'$ w.r.t. $[\vec{b}_1', \vec{b}_2']$.

We take bound vectors $\vec{b}_1 = (o, b_1)$, $\vec{b}_2 = (o, b_2)$, $\vec{x} = (o, x)$ at o and construct bound vectors $\vec{b}_1' = (o', b_1')$, $\vec{b}_2' = (o', b_2')$, $\vec{x}' = (o', x')$ at o' by translating x to x', b_1 to b_1' and b_2 to b_2' by the same translation. Coordinates of $\vec{x}$ w.r.t. $[\vec{b}_1, \vec{b}_2]$ are equal to coordinates of $\vec{x}'$ w.r.t. $[\vec{b}_1', \vec{b}_2']$. This interesting property allows us to construct another model of a linear space, which plays an important role in geometry.

Let us now consider the set of all geometric vectors A. Figure 4.7(a) shows an example of a few points and a few geometric vectors. Let us *partition* [1] the set A of geometric vectors into disjoint subsets $A_{(o,x)}$ such that we choose one bound vector (o, x) and put to $A_{(o,x)}$ all geometric vectors that can be obtained by a translation of (o, x). Figure 4.7(b) shows two such partitions $A_{(o,x)}$, $A_{(o,y)}$. It is clear that $A_{(o,x)} \cap A_{(o,x')} = \emptyset$ for $x \neq x'$ and that every geometric vector is in some (and in exactly one) subset $A_{(o,x)}$.

Two geometric vectors (o, x) and (o', x') form two subsets $A_{(o,x)}$, $A_{(o',x')}$ which are equal if and only if (o', x') is related by a translation to (o, x).

"To be related by a translation" is an equivalence relation [1]. All geometric vectors in $A_{(o,x)}$ are equivalent to (o, x).

There are as many sets in the partition as there are bound vectors at a point. We can define the partition by geometric vectors bound to any point o because if we choose another point o', then for every point x, there is exactly one point x' such that (o, x) can be translated to (o', x').

We denote the set of subsets $A_{(o,x)}$ by V. Let us see that we can equip set V with a meaningful addition $\boxplus$: $V \times V \rightarrow V$ and multiplication $\boxdot$: $S \times V \rightarrow V$ by geometric scalars S such that it will become a model of the linear space. Elements of V will be called *free vectors*.

We define the sum of $\vec{x} = A_{(o,x)}$ and $\vec{y} = A_{(o,y)}$, i.e. $\vec{z} = \vec{x} \boxplus \vec{y}$ is the set $A_{(o,x) \oplus (o,y)}$. Multiplication of $\vec{x} = A_{(o,x)}$ by geometrical scalar a is defined analogically, i.e. $a \boxdot \vec{x}$ equals the set $A_{a \odot (o,x)}$. We see that

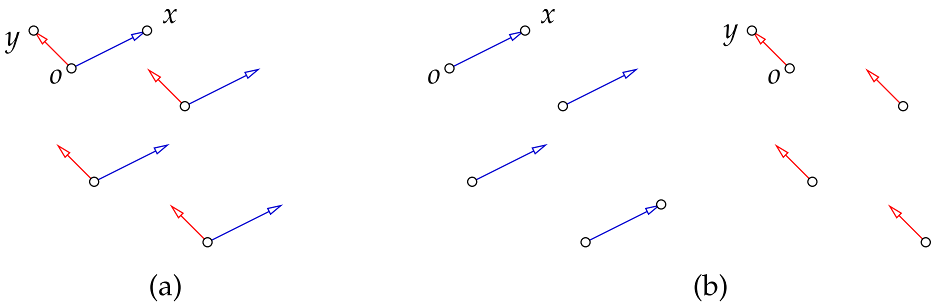


Figure 4.7: The set A of all geometric vectors (a) can be partitioned into subsets which are called free vectors. Two free vectors $A_{(o,x)}$ and $A_{(o,y)}$, i.e. subsets of A, are shown in (b).

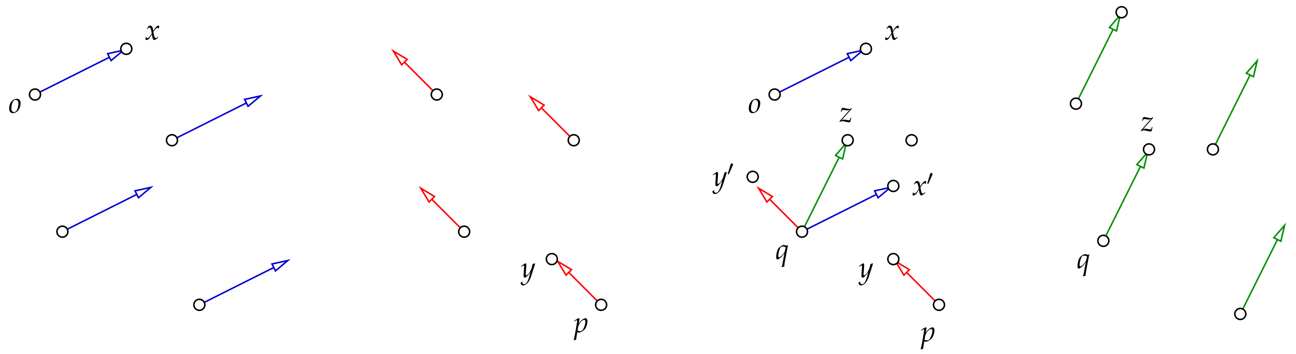


Figure 4.8: Free vector $A_{(o,x)}$ is added to free vector $A_{(p,y)}$ by translating (o, x) to (q, x') and (p, y) to (q, y'), adding bound vectors $(q, z) = (q, x') \oplus (q, y')$ and setting $A_{(o,x)} \boxplus A_{(p,y)} = A_{(q,z)}$

the result of $\boxplus$ and $\boxdot$ does not depend on the choice of o. We have constructed the linear space V of free vectors.

§ 1 Why so many vectors? In the literature, e.g. in [4, 5, 8], linear spaces are often treated purely axiomatically and their geometrical models based on geometrical scalars and vectors are not studied in detail. This is a good approach for a pure mathematician but in engineering we use the geometrical model to study the space we live in. In particular, we wish to appreciate that good understanding of the geometry of the space around us calls for using bound as well as free vectors.

4.4 Affine space

We saw that bound vectors and free vectors were (models of) a linear space. On the other hand, we see that the set of geometric vectors A is not (a model of) a linear space because we do not know how to meaningfully add (by translation) geometric vectors which are not bound to the same point. The set of geometric vectors is an *affine space*.

The affine space connects points, geometric scalars, bound geometric vectors and free vectors in a natural way.

Two points x and y, in this order, give one geometric vector (x, y), which determines exactly one free vector $\vec{v} = A_{(x,y)}$. We define function $\varphi\colon A \to V$, which assigns to two points $x, y \in P$ their corresponding free vector $\varphi(x, y) = A_{(x,y)}$.

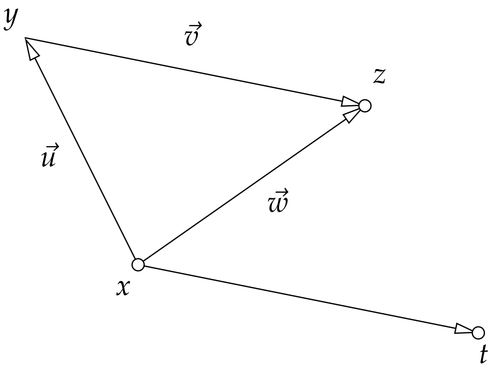


Figure 4.9: Free vectors $\vec{u}$, $\vec{v}$ and $\vec{w}$ defined by three points x, y and z satisfy triangle identity $\vec{u} \boxplus \vec{v} = \vec{w}$.

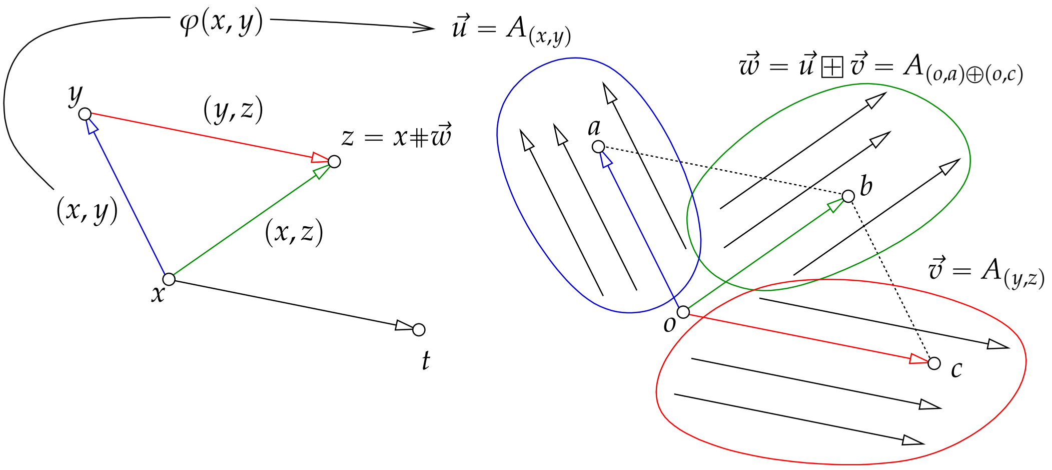


Figure 4.10: Affine space (P, L, φ), its geometric vectors $(x, y) \in A = P \times P$ and free vector space L and the canonical assignment of pairs of points (x, y) to the free vector $A_{(x,y)}$. Operations $\oplus$, $\boxplus$, combining vectors with vectors, and $\#$, combining points with vectors, are illustrated.

Consider a point $a \in P$ and a free vector $\vec{x} \in V$. There is exactly one geometric vector (a, x), with a at the first position, in the free vector $\vec{x}$. Therefore, point a and free vector $\vec{x}$ uniquely define point x. We define function $\# \colon P \times V \to P$, which takes a point and a free vector and delivers another point. We write $a\#\vec{x} = x$ and require $\vec{x} = \varphi(a, x)$.

Consider three points $x, y, z \in P$, Figure 4.9. We can produce three free vectors $\vec{u} = \varphi(x, y) = A_{(x,y)}$, $\vec{v} = \varphi(y, z) = A_{(y,z)}$, $\vec{w} = \varphi(x, z) = A_{(x,z)}$. Let us investigate the sum $\vec{u} \boxplus \vec{v}$. Chose the representatives of the free vectors, such that they are all bound to x, i.e. bound vectors $(x, y) \in A_{x,y}$, $(x, t) \in A_{(y,z)}$ and $(x, z) \in A_{(x,z)}$. Notice that we could choose the pairs of original points to represent the first and the third free vector but we had to introduce a new pair of points, (x, t), to represent the second free vector. Clearly, there holds $(x, y) \oplus (x, t) = (x, z)$. We now see, Figure 4.9, that (y, z) is related to (x, t) by a translation and therefore

$$\vec{u} \boxplus \vec{v} = A_{(x,y)} \boxplus A_{(y,z)} = A_{(x,y)} \boxplus A_{(x,t)} = A_{(x,y)\oplus(x,t)} = A_{(x,z)} = \vec{w} \tag{4.12}$$

Figure 4.10 shows the operations explained above in Figure 4.9 but realized using the vectors bound to another point o.

The above rules are known as *axioms of affine space* and can be used to define even more general affine spaces.

§ 1 Remark on notation We were carefully distinguishing operations $(+, \ )$ over scalars, $(\oplus, \odot)$ over bound vectors, $(\boxplus, \boxdot)$ over free vectors, and function $\#$ combining points and free vectors. This is very correct but rarely used. Often, only the symbols introduced for geometric scalars are used for all operations, i.e.

$$+ \;\equiv\; +, \oplus, \boxplus, \# \tag{4.13}$$
$$\;\equiv\; \ , \odot, \boxdot \tag{4.14}$$

§ 2 Affine space Triple (P, L, φ) with a set of points P, linear space $(L, \boxplus, \boxdot)$ (over some field of scalars) and a function $\varphi \colon P \times P \to L$, is an affine space when

A1 $\varphi(x, z) = \varphi(x, y) \boxplus \varphi(y, z)$ for every three points $x, y, z \in P$

A2 for every $o \in P$, the function $\varphi_o \colon P \to L$, defined by $\varphi_o(x) = \varphi(o, x)$ for all $x \in P$ is a bijection [1].

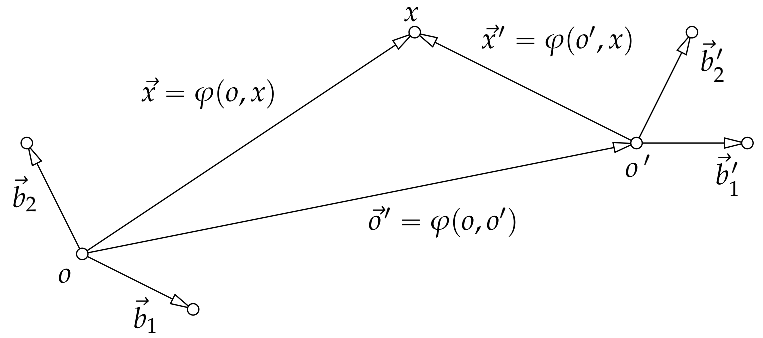

x
$\vec{x}' = \varphi(o', x)$
$\vec{b}_2'$
$\vec{x} = \varphi(o, x)$
$\vec{b}_2$
o'
$\vec{b}_1'$
$\vec{o}' = \varphi(o, o')$
o
$\vec{b}_1$

Figure 4.11: Point x is represented in two affine coordinate systems.

Axiom A1 calls for an assignment of pairs of point to vectors. Axiom A2 then makes this assignmet such that it is one-to-one when the first argument of φ is fixed.

We can define another function $\#: P \times L \to P$, defined by $o \# \vec{x} = \varphi_o^{-1}(\vec{x})$, which means $\varphi(o, o \# \vec{x}) = \vec{x}$ for all $\vec{x} \in L$. This function combines points and vectors in a way that is very similar to addition and hence is sometimes denoted by $+$ instead of more correct $\#$.

In our geometrical model of A discussed above, function φ assigned to a pair of points x, y their corresponding free vector $A_{(x,y)}$. Function $\#$, on the other hand, takes a point x and a free vector $\vec{v}$ and gives another points y such that the bound vector (x, y) is a representative of $\vec{v}$, i.e. $A_{(x,y)} = \vec{v}$.

4.5 Coordinate system in affine space

We see that function φ assigns the same vector from L to many different pairs of points from P. To represent uniquely points by vectors, we select a point o, called the *origin of affine coordinate system* and represent point $x \in P$ by its *position vector* $\vec{x} = \varphi(o, x)$. In our geometric model of A discussed above, we thus represent point x by bound vector (o, x) or by point o and free vector $A_{(o,x)}$.

To be able to compute with points, we now pass to the representation of points in A by coordinate vectors. We choose a basis $\beta = (\vec{b}_1, \vec{b}_2, \ldots)$ in L. That allows us to represent point $x \in P$ by a coordinate vector

$$\vec{x}_\beta = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \end{bmatrix}, \quad \text{such that} \quad \vec{x} = x_1 \vec{b}_1 + x_2 \vec{b}_2 + \cdots \tag{4.15}$$

The pair (o, β), where $o \in P$ and β is a basis of L is called an *affine coordinate system* (often shortly called just coordinate system) of affine space (P, L, φ).

Let us now study what happens when we choose another point o' and another basis $\beta' = (\vec{b}_1', \vec{b}_2', \ldots)$ to represent $x \in P$ by coordinate vectors, Figure 4.11. Point x is represented twice: by coordinate vector $\vec{x}_\beta = \varphi(o, x)_\beta = A_{(o,x)\beta}$ and by coordinate vector $\vec{x}'_{\beta'} = \varphi(o', x)_{\beta'} = A_{(o',x)\beta'}$.

To get the relationship between the coordinate vectors $\vec{x}_\beta$ and $\vec{x}'_{\beta'}$, we employ the triangle equality

$$\begin{aligned} \varphi(o, x) &= \varphi(o, o') \boxplus \varphi(o', x) && (4.16) \\ \vec{x} &= \vec{o}' \boxplus \vec{x}' && (4.17) \end{aligned}$$

which we can write in basis β as (notice that we replace $\boxplus$ by $+$ to emphasize that we are adding coordinate vectors)

$$\vec{x}_\beta = \vec{x}'_\beta + \vec{o}'_\beta \tag{4.18}$$

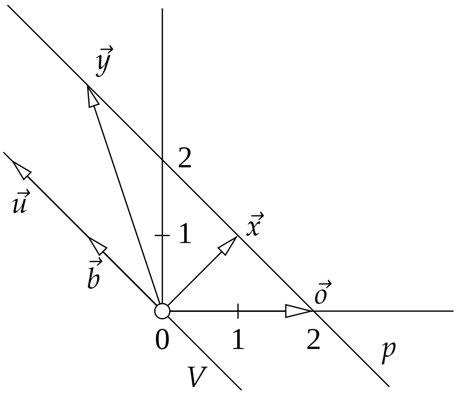


Figure 4.12: Affine space (P, V, φ) of solutions to a linear system is the set of vectors representing points on line p. In coordinate system $(\vec{o}, \vec{u})$, vector $\vec{x}$ has coordinate 1. The subspace V of solutions to the associated homogeneous system is the associated linear space. Function φ assigns to two points $\vec{o}, \vec{x}$ the vector $\vec{u} = \vec{y} - \vec{x}$.

and use the matrix $\mathtt{A}$ transforming coordinates of vectors from basis β' to β to get the desired relationship

$$\vec{x}_\beta \quad = \quad \mathtt{A}\,\vec{x}'_{\beta'} + \vec{o}'_\beta \tag{4.19}$$

Columns of $\mathtt{A}$ correspond to coordinate vectors $\vec{b}'_{1\beta'}, \vec{b}'_{2\beta'}, \ldots$. When presented with a situation in a real affine space, we can measure those coordinates by a ruler on a particular representation of L by geometrical vectors bound to, e.g., point o.

4.6 An example of affine space

Let us now present an important example of affine space.

4.6.1 Affine space of solutions of a system of linear equations

When looking at the following system of linear equations in $\mathbb{R}^2$

$$\begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} \vec{x} = \begin{bmatrix} 2 \\ -2 \end{bmatrix} \tag{4.20}$$

we immediately see that there is an infinite number of solutions. They can be written as

$$\vec{x} = \begin{bmatrix} 2 \\ 0 \end{bmatrix} + \tau \begin{bmatrix} 1 \\ -1 \end{bmatrix}, \quad \tau \in \mathbb{R} \tag{4.21}$$

or as a sum of a particular solution $[2, 0]^\top$ and the set of solutions $\vec{v} = \tau\,[-1, 1]^\top$ of the accompanied homogeneous system

$$\begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} \vec{v} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \tag{4.22}$$

Figure 4.12 shows that the affine space (P, V, φ) of solutions to the linear system (4.20) is the set of vectors representing points on line p. The subspace V of solutions to the accompanied homogeneous system (4.22) is the linear space associated to A by function φ, which assigns to two points $\vec{x}, \vec{y} \in A$ the vector $\vec{u} = \vec{y} - \vec{x} \in V$. If we choose $\vec{o} = [2, 0]^\top$ as the origin in A and vector $\vec{b} = \varphi(\vec{o}, \vec{x}) = \vec{x} - \vec{o}$ as the basis of V, vector $\vec{x}$ has coordinate 1.

We see that, in this example, points of A are actually vectors of $\mathbb{R}^2$, which are the solution to the system (4.20). The vectors of V are the vectors of $\mathbb{R}^2$, which are solutions to the associated homogeneous linear system (4.22).

5 Motion

Let us introduce a mathematical model of rigid motion in three-dimensional Euclidean space. The important property of rigid motion is that it only relocates objects without changing their shape. Distances between points on rigidly moving objects remain unchanged. For brevity, we will use "motion" for "rigid motion".

5.1 Change of position vector coordinates induced by motion

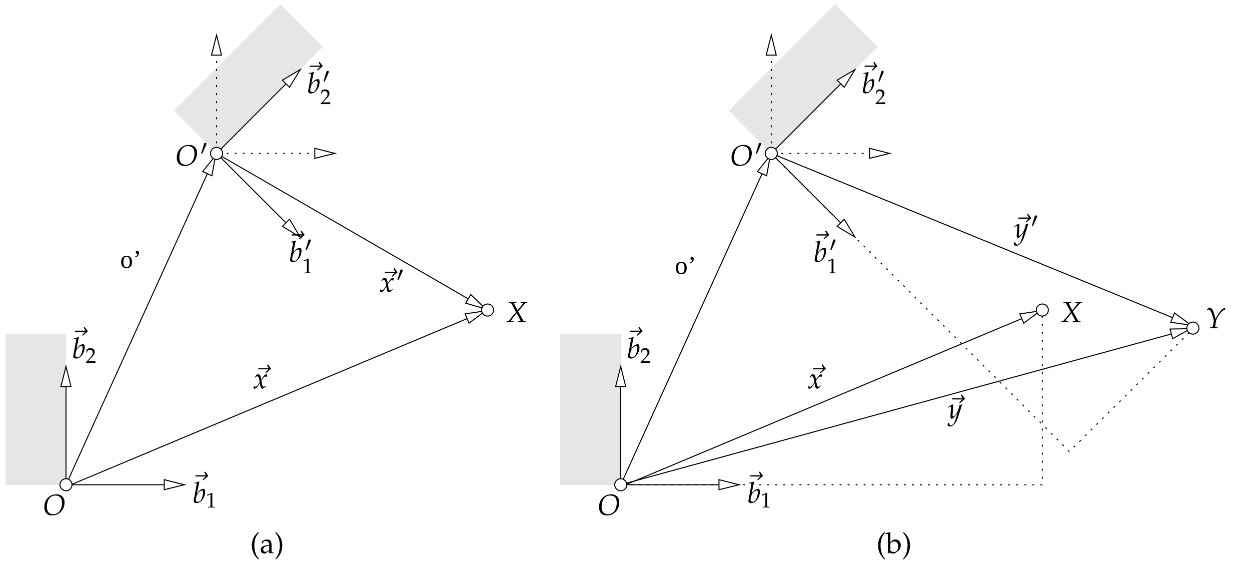


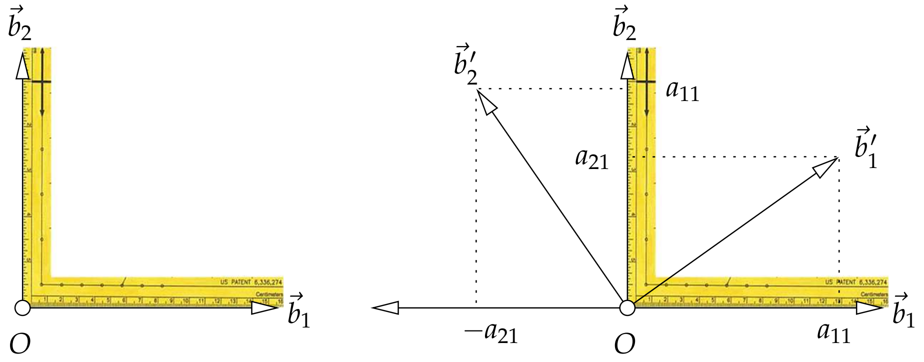
Figure 5.1: Representation of motion. (a) Alias representation: Point X is represented in two coordinate systems. (b) Alibi representation: Point X move tohetjer with the coordinate system into point Y.

§ **1 Alias representation of motion**[1]. Figure 5.1(a) illustrates a model of motion using coordinate systems, points and their position vectors. A coordinate system (O, β) with origin O and basis β is attached to a moving rigid body. As the body moves to a new position, a new coordinate system (O', β') is constructed. Assume a point X in a general position w.r.t. the body, which is represented in the coordinate system (O, β) by its position vector $\vec{x}$. The same point X is represented in the coordinate system (O', β') by its position vector $\vec{x}'$. The motion induces a mapping $\vec{x}'_{\beta'} \mapsto \vec{x}_\beta$. Such a mapping also determines the motion itself and provides its convenient mathematical model.

Let us derive the formula for the mapping $\vec{x}'_{\beta'} \mapsto \vec{x}_\beta$ between the coordinates $\vec{x}'_{\beta'}$ of vector $\vec{x}'$ and coordinates $\vec{x}_\beta$ of vector $\vec{x}$. Consider the following equations:

$$\begin{aligned}
\vec{x} &= \vec{x}' + \vec{o}' && (5.1)\\
\vec{x}_\beta &= \vec{x}'_\beta + \vec{o}'_\beta && (5.2)\\
\vec{x}_\beta &= \begin{bmatrix} \vec{b}'_{1_\beta} & \vec{b}'_{2_\beta} & \vec{b}'_{3_\beta} \end{bmatrix} \vec{x}'_{\beta'} + \vec{o}'_\beta && (5.3)\\
\vec{x}_\beta &= \mathtt{R}\, \vec{x}'_{\beta'} + \vec{o}'_\beta && (5.4)
\end{aligned}$$

[1] The terms *alias* and *alibi* were introduced in the classical monograph [18].



(a) (b)

Figure 5.2: Rotation in two-dimensional space.

Vector $\vec{x}$ is the sum of vectors $\vec{x}'$ and $\vec{o}'$, Equation 5.1. We can express all vectors in (the same) basis β, Equation 5.2. To pass to the basis β' we introduce matrix $\mathtt{R} = \begin{bmatrix} \vec{b}'_{1_\beta} & \vec{b}'_{2_\beta} & \vec{b}'_{3_\beta} \end{bmatrix}$, which transforms the coordinates of vectors from β' to β, Equation 5.4. Columns of matrix $\mathtt{R}$ are coordinates $\vec{b}'_{1_\beta}, \vec{b}'_{2_\beta}, \vec{b}'_{3_\beta}$ of basic vectors $\vec{b}'_1, \vec{b}'_2, \vec{b}'_3$ of basis β' in basis β.

§ **2 Alibi representation of motion.** An alternative model of motion can be developed from the relationship between the points X and Y and their position vectors in Figure 5.1(b). The point Y is obtained by moving point X altogether with the moving object. It means that the coordinates $\vec{y}'_{\beta'}$ of the position vector $\vec{y}'$ of Y in the coordinate system (O', β') equal the coordinates $\vec{x}_\beta$ of the position vector $\vec{x}$ of X in the coordinate system (O, β), i.e.

$$\begin{aligned} \vec{y}'_{\beta'} &= \vec{x}_\beta \\ \vec{y}_{\beta'} - \vec{o}'_{\beta'} &= \vec{x}_\beta \\ \mathtt{R}^{-1}\left(\vec{y}_\beta - \vec{o}'_\beta\right) &= \vec{x}_\beta \\ \vec{y}_\beta &= \mathtt{R}\,\vec{x}_\beta + \vec{o}'_\beta \end{aligned} \tag{5.5}$$

Equation 5.5 describes how is the point X moved to point Y w.r.t. the coordinate system (O, β).

5.2 Rotation matrix

Motion that leaves at least one point fixed is called rotation. Choosing such a fixed point as the origin leads to $O = O'$ and hence to $\vec{o} = \vec{0}$. The motion is then fully described by matrix $\mathtt{R}$, which is called *rotation matrix*.

§ **1 Two-dimensional rotation.** To understand the matrix $\mathtt{R}$, we shall start with an experiment in two-dimensional plane. Imagine a right-angled triangle ruler as shown in Figure 5.2(a) with arms of equal length and let us define a coordinate system as in the figure. Next, rotate the triangle ruler around its tip, i.e. around the origin O of the coordinate system. We know, and we can verify it by direct physical measurement, that, thanks to the symmetry of the situation, the parallelograms through the tips of $\vec{b}'_1$ and $\vec{b}'_2$ and along $\vec{b}_1$ and $\vec{b}_2$ will be rotated by 90 degrees. We see that

$$\vec{b}'_1 = a_{11}\,\vec{b}_1 + a_{21}\,\vec{b}_2 \tag{5.6}$$

$$\vec{b}'_2 = -a_{21}\,\vec{b}_1 + a_{11}\,\vec{b}_2 \tag{5.7}$$

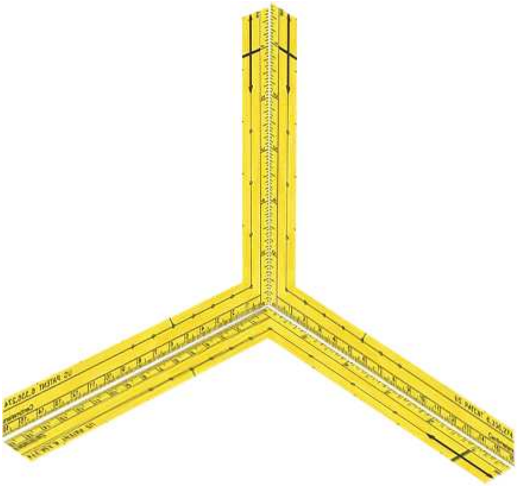


Figure 5.3: A three-dimensional coordinate system.

for some real numbers a_{11} and a_{21}. By comparing it with Equation 5.3, we conclude that

$$\mathtt{R} = \begin{bmatrix} a_{11} & -a_{21} \\ a_{21} & a_{11} \end{bmatrix} \tag{5.8}$$

We immediately see that

$$\mathtt{R}^\top \mathtt{R} \;=\; \begin{bmatrix} a_{11} & a_{21} \\ -a_{21} & a_{11} \end{bmatrix} \begin{bmatrix} a_{11} & -a_{21} \\ a_{21} & a_{11} \end{bmatrix} = \begin{bmatrix} a_{11}^2 + a_{21}^2 & 0 \\ 0 & a_{11}^2 + a_{21}^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{5.9}$$

since $(a_{11}^2 + a_{21}^2)$ is the squared length of the basic vector of b_1, which is one. We derived an interesting result

$$\mathtt{R}^{-1} \;=\; \mathtt{R}^\top \tag{5.10}$$

$$\mathtt{R} \;=\; \mathtt{R}^{-\top} \tag{5.11}$$

Next important observation is that for coordinates $\vec{x}_\beta$ and $\vec{x}'_{\beta'}$, related by a rotation, there holds true

$$(x')^2 + (y')^2 = \vec{x}'^{\top}_{\beta'} \vec{x}'_{\beta'} = \left(\mathtt{R}\vec{x}_\beta\right)^\top \mathtt{R}\vec{x}_\beta = \vec{x}_\beta^\top \left(\mathtt{R}^\top \mathtt{R}\right) \vec{x}_\beta = \vec{x}_\beta^\top \vec{x}_\beta = x^2 + y^2 \tag{5.12}$$

Now, if the basis β was constructed as in Figure 5.2, in which case it is called an *orthonormal basis*, then the parallelogram used to measure coordinates x, y of $\vec{x}$ is a rectangle, and hence $x^2 + y^2$ is the squared length of $\vec{x}$ by the Pythagoras theorem. If β' is related by rotation ro β, then also $(x')^2 + (y')^2$ is the squared length of $\vec{x}$, again thanks to the Pythagoras theorem.

We see that $\vec{x}_\beta^\top \vec{x}_\beta$ is the squared length of $\vec{x}$ when β is orthonormal and that this length is preserved by computing it in the same way from the new coordinates of $\vec{x}$ in the new coordinate system after motion. The change of coordinates induced by motion is modeled by rotation matrix $\mathtt{R}$, which has the desired property $\mathtt{R}^\top \mathtt{R} = \mathtt{I}$ when the bases β, β' are both orthonormal.

§ 2 Three-dimensional rotation. Let us now consider three dimensions. It would be possible to generalize Figure 5.2 to three dimensions, construct orthonormal bases, and use rectangular parallelograms to establish the relationship between elements of $\mathtt{R}$ in three dimensions. However, the figure and the derivations would become much more complicated.

We shall follow a more intuitive path instead. Consider that we have found that with two-dimensional orthonormal bases, the lengths of vectors could be computed by the Pythagoras theorem since the parallelograms determining the coordinates were rectangular. To achieve this in three dimensions, we need (and can!) use bases consisting of three orthogonal vectors. Then, again, the parallelograms will be rectangular and hence the Pythagoras theorem for three dimensions can be used analogically as in two dimensions, Figure 5.3.

Considering orthonormal bases β, β', we require the following to hold true for all vectors $\vec{x}$ with $\vec{x}_\beta = \begin{bmatrix} x & y & z \end{bmatrix}^\top$ and $\vec{x}'_{\beta'} = \begin{bmatrix} x' & y' & z' \end{bmatrix}^\top$

$$\begin{aligned}
(x')^2 + (y')^2 + (z')^2 &= x^2 + y^2 + z^2 \\
\vec{x}'^\top_{\beta'} \vec{x}'_{\beta'} &= \vec{x}^\top_\beta \vec{x}_\beta \\
\left(\mathtt{R}\,\vec{x}_\beta\right)^\top \mathtt{R}\,\vec{x}_\beta &= \vec{x}^\top_\beta \vec{x}_\beta \\
\vec{x}^\top_\beta \left(\mathtt{R}^\top \mathtt{R}\right) \vec{x}_\beta &= \vec{x}^\top_\beta \vec{x}_\beta \\
\vec{x}^\top_\beta \mathtt{C}\, \vec{x}_\beta &= \vec{x}^\top_\beta \vec{x}_\beta \qquad (5.13)
\end{aligned}$$

Equation 5.13 must hold true for all vectors $\vec{x}$ and hence also for special vectors such as those with coordinates

$$\begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}, \begin{bmatrix}1\\1\\0\end{bmatrix}, \begin{bmatrix}1\\0\\1\end{bmatrix}, \begin{bmatrix}0\\1\\1\end{bmatrix} \qquad (5.14)$$

Let us see what that implies, e.g., for the first vector

$$\begin{aligned}
\begin{bmatrix}1 & 0 & 0\end{bmatrix} \mathtt{C} \begin{bmatrix}1\\0\\0\end{bmatrix} &= 1 \qquad (5.15) \\
c_{11} &= 1 \qquad (5.16)
\end{aligned}$$

Taking the second and the third vector leads similarly to $c_{22} = c_{33} = 1$. Now, let's try the fourth vector

$$\begin{aligned}
\begin{bmatrix}1 & 1 & 0\end{bmatrix} \mathtt{C} \begin{bmatrix}1\\1\\0\end{bmatrix} &= 2 \qquad (5.17) \\
1 + c_{12} + c_{21} + 1 &= 2 \qquad (5.18) \\
c_{12} + c_{21} &= 0 \qquad (5.19)
\end{aligned}$$

Again, taking the fifth and the sixth vector leads to $c_{13} + c_{31} = c_{23} + c_{32} = 0$. This brings us to the following form of $\mathtt{C}$

$$\mathtt{C} = \begin{bmatrix} 1 & c_{12} & c_{13} \\ -c_{12} & 1 & c_{23} \\ -c_{13} & -c_{23} & 1 \end{bmatrix} \qquad (5.20)$$

Moreover, we see that $\mathtt{C}$ is symmetric since

$$\mathtt{C}^\top = \left(\mathtt{R}^\top \mathtt{R}\right)^\top = \mathtt{R}^\top \mathtt{R} = \mathtt{C} \qquad (5.21)$$

which leads to $-c_{12} = c_{12}$, $-c_{13} = c_{13}$ and $-c_{23} = c_{23}$, i.e. $c_{12} = c_{13} = c_{23} = 0$ and allows us to conclude that

$$\mathtt{R}^\top \mathtt{R} = \mathtt{C} = \mathtt{I} \qquad (5.22)$$

Interestingly, not all matrices $\mathtt{R}$ satisfying Equation 5.22 represent motions in three-dimensional space.

Consider, e.g., matrix

$$\mathtt{S} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \qquad (5.23)$$

Matrix S does not correspond to any rotation of the space since it keeps the plane xy fixed and reflects all other points w.r.t. this xy plane. We see that some matrices satisfying Equation 5.22 are rotations but there are also some such matrices that are not rotations. Can we somehow distinguish them?

Notice that $|\mathtt{S}| = -1$ while $|\mathtt{I}| = 1$. It might be therefore interesting to study the determinant of $\mathtt{C}$ in general. Consider that

$$1 = |\mathtt{I}| = \left|(\mathtt{R}^\top \mathtt{R})\right| = \left|\mathtt{R}^\top\right| |\mathtt{R}| = |\mathtt{R}|\,|\mathtt{R}| = (|\mathtt{R}|)^2 \tag{5.24}$$

which gives that $|\mathtt{R}| = \pm 1$. We see that the sign of the determinant splits all matrices satisfying Equation 5.22 into two groups – rotations, which have a positive determinant, and reflections, which have a negative determinant. The product of any two rotations will again be a rotation, the product of a rotation and a reflection will be a reflection and the product of two reflections will be a rotation.

To summarize, rotation in three-dimensional space is represented by a 3×3 matrix $\mathtt{R}$ with $\mathtt{R}^\top \mathtt{R} = \mathtt{I}$ and $|\mathtt{R}| = 1$. The set of all such matrices, and at the same time also the corresponding rotations, will be called $SO(3)$, for *special orthonormal three-dimensional group*. Two-dimensional rotations will be analogically denoted as $SO(2)$.

5.3 Coordinate vectors

We see that the matrix $\mathtt{R}$ induced by motion has the property that coordinates and the basic vectors are transformed in the same way. This is particularly useful observation when β is formed by the standard basis, i.e.

$$\beta = \left(\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right) \tag{5.25}$$

For a rotation matrix $\mathtt{R}$, Equation 2.15 becomes

$$\begin{bmatrix} \vec{b}_1' \\ \vec{b}_2' \\ \vec{b}_3' \end{bmatrix} = \mathtt{R} \begin{bmatrix} \vec{b}_1 \\ \vec{b}_2 \\ \vec{b}_3 \end{bmatrix} = \begin{bmatrix} r_{11} & r_{12} & r_{13} \\ r_{21} & r_{22} & r_{23} \\ r_{31} & r_{32} & r_{33} \end{bmatrix} \begin{bmatrix} \vec{b}_1 \\ \vec{b}_2 \\ \vec{b}_3 \end{bmatrix} = \begin{bmatrix} r_{11}\,\vec{b}_1 + r_{12}\,\vec{b}_2 + r_{13}\,\vec{b}_3 \\ r_{21}\,\vec{b}_1 + r_{22}\,\vec{b}_2 + r_{23}\,\vec{b}_3 \\ r_{31}\,\vec{b}_1 + r_{32}\,\vec{b}_2 + r_{33}\,\vec{b}_3 \end{bmatrix} \tag{5.26}$$

and hence

$$\vec{b}_1' = r_{11}\,\vec{b}_1 + r_{12}\,\vec{b}_2 + r_{13}\,\vec{b}_3 = r_{11} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + r_{12} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + r_{13} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} r_{11} \\ r_{12} \\ r_{13} \end{bmatrix} \tag{5.27}$$

and similarly for $\vec{b}_2'$ and $\vec{b}_3'$. We conclude that

$$\begin{bmatrix} \vec{b}_1' & \vec{b}_2' & \vec{b}_3' \end{bmatrix} = \begin{bmatrix} r_{11} & r_{21} & r_{31} \\ r_{12} & r_{22} & r_{32} \\ r_{13} & r_{23} & r_{33} \end{bmatrix} = \mathtt{R}^\top \tag{5.28}$$

This also corresponds to solving for $\mathtt{R}$ in Equation 2.13 with $\mathtt{A} = \mathtt{R}$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \vec{b}_1' & \vec{b}_2' & \vec{b}_3' \end{bmatrix} \mathtt{R} \tag{5.29}$$

6 Rotation

6.1 Properties of rotation matrix

Let us study additional properties of the rotation matrix in three-dimensional space.

6.1.1 Inverse of $\mathtt{R}$

Let

$$\mathtt{R} = \begin{bmatrix} r_{11} & r_{12} & r_{13} \\ r_{21} & r_{22} & r_{23} \\ r_{31} & r_{32} & r_{33} \end{bmatrix} = \begin{bmatrix} \mathbf{r}_1 & \mathbf{r}_2 & \mathbf{r}_3 \end{bmatrix} \tag{6.1}$$

be a rotation matrix with columns $\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3$. We can find the inverse of $\mathtt{R}$ by evaluating its adjugate matrix [5] and use $\mathtt{R}^{-1} = \mathtt{R}^\top$ and $|\mathtt{R}| = 1$

$$\begin{aligned} \mathtt{R}^{-1} &= \frac{1}{|\mathtt{R}|}\,\mathtt{Adj}(\mathtt{R}) & (6.2)\\ \mathtt{R}^\top &= \mathtt{Adj}(\mathtt{R}) & (6.3)\\ &= \begin{bmatrix} \mathbf{r}_2 \times \mathbf{r}_3 & \mathbf{r}_3 \times \mathbf{r}_1 & \mathbf{r}_1 \times \mathbf{r}_2 \end{bmatrix}^\top & (6.4)\\ &= \begin{bmatrix} r_{22}\,r_{33} - r_{23}\,r_{32} & r_{13}\,r_{32} - r_{12}\,r_{33} & r_{12}\,r_{23} - r_{13}\,r_{22} \\ r_{23}\,r_{31} - r_{21}\,r_{33} & r_{11}\,r_{33} - r_{13}\,r_{31} & r_{13}\,r_{21} - r_{11}\,r_{23} \\ r_{21}\,r_{32} - r_{22}\,r_{31} & r_{12}\,r_{31} - r_{11}\,r_{32} & r_{11}\,r_{22} - r_{12}\,r_{21} \end{bmatrix} & (6.5) \end{aligned}$$

which also gives an alternative expression of

$$\mathtt{R} = \begin{bmatrix} r_{11} & r_{12} & r_{13} \\ r_{21} & r_{22} & r_{23} \\ r_{31} & r_{32} & r_{33} \end{bmatrix} = \begin{bmatrix} r_{22}\,r_{33} - r_{23}\,r_{32} & r_{23}\,r_{31} - r_{21}\,r_{33} & r_{21}\,r_{32} - r_{22}\,r_{31} \\ r_{13}\,r_{32} - r_{12}\,r_{33} & r_{11}\,r_{33} - r_{13}\,r_{31} & r_{12}\,r_{31} - r_{11}\,r_{32} \\ r_{12}\,r_{23} - r_{13}\,r_{22} & r_{13}\,r_{21} - r_{11}\,r_{23} & r_{11}\,r_{22} - r_{12}\,r_{21} \end{bmatrix} \tag{6.6}$$

6.1.2 Eigenvalues of $\mathtt{R}$

Let $\mathtt{R}$ be a rotation matrix. Then for every $\vec{v} \in \mathbb{C}^3$

$$(\mathtt{R}\,\vec{v})^\dagger \mathtt{R}\,\vec{v} = \vec{v}^\dagger \mathtt{R}^\top \mathtt{R}\,\vec{v} = \vec{v}^\dagger\,(\mathtt{R}^\top \mathtt{R})\,\vec{v} = \vec{v}^\dagger \vec{v} \tag{6.7}$$

where † is the conjugate transpose[1]. We see that for all $\vec{v} \in \mathbb{C}^3$ and $\lambda \in \mathbb{C}$ such that

$$\mathtt{R}\,\vec{v} = \lambda\,\vec{v} \tag{6.8}$$

[1] *Conjugate transpose* [5] on vectors with complex coordinates means, e.g., that

$$\begin{bmatrix} a_{11} + b_{11}\,i & a_{12} + b_{12}\,i \\ a_{21} + b_{21}\,i & a_{22} + b_{22}\,i \end{bmatrix}^\dagger = \begin{bmatrix} a_{11} - b_{11}\,i & a_{21} - b_{21}\,i \\ a_{12} - b_{12}\,i & a_{22} - b_{22}\,i \end{bmatrix}$$

for all $a_{11}, a_{12}, a_{21}, a_{22}, b_{11}, b_{12}, b_{21}, b_{22} \in \mathbb{R}$. Also recall [3] that $\overline{a\,b} = \overline{a}\,\overline{b}$ for all $a, b \in \mathbb{C}$, † becomes $\top$ for real matrices and $\lambda^\dagger = \overline{\lambda}$ for scalar $\lambda \in \mathbb{C}$. Conjugate transpose is a natural generalization of the Euclidean scalar product in real vector spaces to complex vector spaces. As $\vec{x}^\top \vec{x} = \|\vec{x}\|^2$ gives the squared Euclidean norm for real vectors, $\vec{x}^\dagger \vec{x} = \|\vec{x}\|^2$ gives the squared "Euclidean" norm for complex vectors. It therefore also makes a good sense to extend the notion of angle between complex vectors to $\vec{x}, \vec{y}$ as $\cos\angle(\vec{x}, \vec{y}) = \frac{Re(\vec{x}^\dagger\,\vec{y})}{\sqrt{\vec{x}^\dagger\,\vec{x}}\sqrt{\vec{y}^\dagger\,\vec{y}}}$.

there holds true

$$
\begin{aligned}
(\lambda \vec{v})^\dagger (\lambda \vec{v}) &= (\vec{v}^\dagger \vec{v}) && (6.9)\\
\overline{\lambda}\, \lambda\, (\vec{v}^\dagger \vec{v}) &= (\vec{v}^\dagger \vec{v}) && (6.10)\\
|\lambda|^2 (\vec{v}^\dagger \vec{v}) &= (\vec{v}^\dagger \vec{v}) && (6.11)
\end{aligned}
$$

and hence $|\lambda|^2 = 1$ for all $\vec{v} \neq \vec{0}$. We conclude that the absolute value of eigenvalues of $\mathtt{R}$ is one.

Next, by looking at the characteristic polynomial of $\mathtt{R}$

$$
\begin{aligned}
p(\lambda) &= |(\lambda\, \mathtt{I} - \mathtt{R})| = \left| \left(\begin{bmatrix} \lambda - r_{11} & -r_{12} & -r_{13} \\ -r_{21} & \lambda - r_{22} & -r_{23} \\ -r_{31} & -r_{32} & \lambda - r_{33} \end{bmatrix} \right) \right| && (6.12)\\
&= \lambda^3 - (r_{11} + r_{22} + r_{33})\, \lambda^2 \\
&\quad + (r_{11}\, r_{22} - r_{21}\, r_{12} + r_{11}\, r_{33} - r_{31}\, r_{13} + r_{22}\, r_{33} - r_{23}\, r_{32})\, \lambda && (6.13)\\
&\quad + r_{11}\, (r_{23}\, r_{32} - r_{22}\, r_{33}) - r_{21}\, (r_{32}\, r_{13} - r_{12}\, r_{33}) + r_{31}\, (r_{13}\, r_{22} - r_{12}\, r_{23}) \\
&= \lambda^3 - (r_{11} + r_{22} + r_{33})\, \lambda^2 + (r_{33} + r_{22} + r_{11})\, \lambda - |\mathtt{R}| && (6.14)\\
&= \lambda^3 - \operatorname{trace} \mathtt{R}\, (\lambda^2 - \lambda) - 1 && (6.15)\\
&= (\lambda - 1)\left(\lambda^2 + (1 - \operatorname{trace} \mathtt{R})\, \lambda + 1\right) && (6.16)
\end{aligned}
$$

we conclude that 1 is always an eigenvalue of $\mathtt{R}$. Notice that we have used identities in Equation 6.6 to pass from Equation 6.13 to Equation 6.14[2].

Let us denote the eigenvalues as $\lambda_1 = 1$, $\lambda_2 = x + y i$ and $\lambda_3 = x - y i$ with real x, y. It follows from the above that $x^2 + y^2 = 1$. We see that there is either one real or three real solutions since if $y = 0$, then $x^2 = 1$ and hence $\lambda_2 = \lambda_3 = \pm 1$. We conclude that we encounter only two situations when all eigenvalues are real. Either $\lambda_1 = \lambda_2 = \lambda_3 = 1$, or $\lambda_1 = 1$ and $\lambda_2 = \lambda_3 = -1$.

6.1.3 Eigenvectors of R

Let us now look at eigenvectors of $\mathtt{R}$ and let's first investigate the situation when all eigenvalues of $\mathtt{R}$ are real.

§ 1 $\lambda_1 = \lambda_2 = \lambda_3 = 1$**:** Let $\lambda_1 = \lambda_2 = \lambda_3 = 1$. Then $p(\lambda) = (\lambda - 1)^3 = \lambda^3 - 3\, \lambda^2 + 3\, \lambda - 1$. It means that $r_{11} + r_{22} + r_{33} = 3$ and since $r_{11} \leqslant 1$, $r_{22} \leqslant 1$, $r_{33} \leqslant 1$, it leads to $r_{11} = r_{22} = r_{33} = 1$, which implies $\mathtt{R} = \mathtt{I}$. Then $\mathtt{I} - \mathtt{R} = 0$ and all non-zero vectors of $\mathbb{R}^3$ are eigenvectors of $\mathtt{R}$. Notice that rank of $\mathtt{R} - \mathtt{I}$ is zero in this case.

Next, consider $\lambda_1 = 1$ and $\lambda_2 = \lambda_3 = -1$. The eigenvectors $\vec{v}$ corresponding to $\lambda_2 = \lambda_3 = -1$ are solutions to

$$
\mathtt{R}\, \vec{v} = -\vec{v} \qquad (6.17)
$$

There is always at least one one-dimensional space of such vectors. We also see that there is a rotation matrix

$$
\mathtt{R} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \qquad (6.18)
$$

[2] Alternatively, it follows from the Fundamental theorem of algebra [7] the $p(\lambda) = 0$ has always a solution in $\mathbb{C}$ and since coefficients of $p(\lambda)$ are all real, the solutions must come in complex conjugated pairs. The degree of $p(\lambda)$ is three and thus at least one solution must be real and hence equal to ± 1. Now, since $p(0) = -|(\mathtt{R})| = -1$, $\lim_{\lambda \to \infty} p(\lambda) = \infty$, and $p(\lambda)$ is a continuous function, it must (by the mean value theorem [3]) cross the positive side of the real axis and hence one of its eigenvalues has to be equal to one.

with real eigenvectors

$$r \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, r \neq 0, \qquad \text{and} \qquad s \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + t \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, s^2 + t^2 \neq 0, \tag{6.19}$$

which means that there is a one-dimensional space of real eigenvectors corresponding to 1 and a two-dimensional space of real eigenvectors corresponding to -1. Notice that rank of $\mathtt{R} - \mathtt{I}$ is two here.

§ 2 $\lambda_1 = 1, \lambda_2 = \lambda_3 = -1$**:** How does the situation look for a general $\mathtt{R}$ with eigenvalues $1, -1, -1$? Consider an eigenvector $\vec{v}_1$ corresponding to 1 and an eigenvector $\vec{v}_2$ corresponding to -1. They are linearly independent. Otherwise there has to be $s \in \mathbb{R}$ such that $\vec{v}_2 = s\,\vec{v}_1 \neq 0$ and then

$$\vec{v}_2 = s\,\vec{v}_1 \tag{6.20}$$

$$\mathtt{R}\,\vec{v}_2 = s\,\mathtt{R}\,\vec{v}_1 \tag{6.21}$$

$$-\vec{v}_2 = s\,\vec{v}_1 \tag{6.22}$$

leading to $s = -s$ and therefore $s = 0$ which contradicts $\vec{v}_2 \neq 0$. Now, let us look at vectors $\vec{v}_3 \in \mathbb{R}^3$ defined by

$$\begin{bmatrix} \vec{v}_1^\top \\ \vec{v}_2^\top \end{bmatrix} \vec{v}_3 = 0 \tag{6.23}$$

The above linear system has a one-dimensional space of solutions since the rows of its matrix are independent. Chose a fixed solution $\vec{v}_3 \neq 0$. Then

$$\begin{bmatrix} \vec{v}_1^\top \\ \vec{v}_2^\top \end{bmatrix} \mathtt{R}^\top \vec{v}_3 = \begin{bmatrix} \vec{v}_1^\top \mathtt{R}^\top \\ \vec{v}_2^\top \mathtt{R}^\top \end{bmatrix} \vec{v}_3 = \begin{bmatrix} \vec{v}_1^\top \\ -\vec{v}_2^\top \end{bmatrix} \vec{v}_3 = 0 \tag{6.24}$$

We see that $\mathtt{R}^\top \vec{v}_3$ and $\vec{v}_3$ are in the same one-dimensional space, i.e. they are linearly dependent and we can write

$$\mathtt{R}^\top \vec{v}_3 = s\,\vec{v}_3 \tag{6.25}$$

for some non-zero $s \in \mathbb{C}$. Multiplying equation 6.25 by $\mathtt{R}$ from the left and dividing both sides by s gives

$$\frac{1}{s}\vec{v}_3 = \mathtt{R}\,\vec{v}_3 \tag{6.26}$$

Clearly, $\vec{v}_3$ is an eigenvector of $\mathtt{R}$. Since it is not a multiple of $\vec{v}_1$, it must correspond to eigenvalue -1. Moreover, $\vec{v}_2^\top \vec{v}_3 = 0$ and hence they are linearly independent. We have shown that if -1 is an eigenvalue of $\mathtt{R}$, then there are always at least two linearly independent vectors corresponding to the eigenvalue -1, and therefore there is a two-dimensional space of eigenvectors corresponding to -1. Notice that the rank of $\mathtt{R} - \mathtt{I}$ is two in this case since the two-dimensional subspace corresponding to -1 can be complemented only by a one-dimensional subspace corresponding to 1 to avoid intersecting the subspaces in a non-zero vector.

§ 3 General $\lambda_1, \lambda_2, \lambda_3$**:** Finally, let us look at arbitrary (even non-real) eigenvalues. Assume $\lambda = x + yi$ for real x, y. Then we have

$$\mathtt{R}\,\vec{v} = (x + yi)\,\vec{v} \tag{6.27}$$

If $y \neq 0$, vector $\vec{v}$ must be non-real since otherwise we would have a real vector on the left and a non-real vector on the right.

Now, we also see that for $y \neq 0$, we have three pairwise distinct eigenvalues 1, $x + yi$, and $x - yi$ since the characteristic polynomial $p(\lambda)$ has real coefficients.

Let us next see that with pairwise distinct eigenvalues $\lambda_1 \neq \lambda_2 \neq \lambda_3 \neq \lambda_1$, the set $V = \{\vec{v}_1, \vec{v}_2, \vec{v}_3\}$, of eigenvectors $\vec{v}_i$ corresponding to λ_i for $i = 1, 2, 3$, is linearly independent. To show that, let us look at the sequence of nested sets $V_k = \{v_1, \dots, \vec{v}_k\}$ for $k = 1, 2, 3$. First, we see that the singleton set $V_1 = \{\vec{v}_1\}$ is linearly independent since $\vec{v}_1$ is non-zero. Now, assuming linearly dependent $V = V_3$, there is $k \in \{2, 3\}$ such that V_{k-1} is linearly independent and V_k is linearly dependent. Hence, we can write

$$v_k = a_1 v_1 + \cdots + a_k v_{k-1} \tag{6.28}$$

and multiply both sides by R to get

$$\begin{aligned} \mathtt{R}\, v_k &= a_1 \mathtt{R}\, v_1 + \cdots + a_k \mathtt{R}\, v_{k-1} & (6.29)\\ \lambda_k v_k &= a_1 \lambda_1 v_1 + \cdots + a_{k-1} \lambda_{k-1} v_{k-1} & (6.30) \end{aligned}$$

However, we can also get

$$\lambda_k v_k = a_1 \lambda_k v_1 + \cdots + a_k \lambda_k v_{k-1} \tag{6.31}$$

by multiplying both Equation 6.28 by λ_k. Now, we subtract Equation 6.31 from Equation 6.30 to get

$$0 = a_1(\lambda_1 - \lambda_k) v_1 + \cdots + a_k(\lambda_{k-1} - \lambda_k) v_{k-1} \tag{6.32}$$

We see that coefficients $a_i(\lambda_i - \lambda_k)$ for $i = 1, \dots, k-1$ must be zero since V_{k-1} is linearly independent. However, since $\lambda_i - \lambda_k$ are all non-zero, we conclude that all a_i must be equal to zero. However, this is in contradiction with Equation 6.28 and non-zero v_k. We see that V is linearly independent since there is no k where linearly independent V_{k-1} could turn into a linearly dependent V_k.

Thus, for a rotation R, there are in this case three one-dimensional subspaces of eigenvectors (we now understand the space as $\mathbb{C}^3$ over $\mathbb{C}$). In particular, there is exactly one one-dimensional subspace corresponding to the eigenvalue 1. The rank of $\mathtt{R} - \mathtt{I}$ is two.

Let $\vec{v}$ be an eigenvector of a rotation matrix R. Then

$$\begin{aligned} \mathtt{R}\,\vec{v} &= (x + yi)\,\vec{v} & (6.33)\\ \mathtt{R}^\top \mathtt{R}\,\vec{v} &= (x + yi)\,\mathtt{R}^\top \vec{v} & (6.34)\\ \vec{v} &= (x + yi)\,\mathtt{R}^\top \vec{v} & (6.35)\\ \frac{1}{(x + yi)}\,\vec{v} &= \mathtt{R}^\top \vec{v} & (6.36)\\ (x - yi)\,\vec{v} &= \mathtt{R}^\top \vec{v} & (6.37) \end{aligned}$$

We see that the eigenvector $\vec{v}$ of R corresponding to eigenvalue $x + yi$ is the eigenvector of $\mathtt{R}^\top$ corresponding to eigenvalue $x - yi$ and vice versa. Thus, there is the following interesting correspondence between eigenvalues and eigenvectors of R and $\mathtt{R}^\top$. Considering eigenvalue-eigenvector pairs $(1, \vec{v}_1)$, $(x + yi, \vec{v}_2)$, $(x - yi, \vec{v}_3)$ of R we have $(1, \vec{v}_1)$, $(x - yi, \vec{v}_2)$, $(x + yi, \vec{v}_3)$ pairs of $\mathtt{R}^\top$, respectively.

§4 Orthogonality of eigenvectors The next question to ask is what are the angles between eignevectors of R? We will considers pairs $(\lambda_1 = 1, \vec{v}_1)$, $(\lambda_2 = x + yi, \vec{v}_2)$, $(\lambda_3 = x - yi, \vec{v}_3)$ of eigenvectors associated with their respective eigenvalues. For instance, vector $\vec{v}_1$ denotes an eigenvector associated with egenvalue 1.

If all eigenvalues are equal to 1, i.e. $\mathtt{R} = \mathtt{I}$, then all non-zero vectors of $\mathbb{R}^3$ are eigenvectors of R and hence we can alway find two eignevectors containing a given angle. In particular, we can choose three mutually orthogonal eignevectors.

If $\lambda_1 = 1$ and $\lambda_2 = \lambda_3 = -1$, then we have seen that every $\vec{v}_1$ is perpendicular to $\vec{v}_2$ and $\vec{v}_3$ and that $\vec{v}_2$ and $\vec{v}_3$ can be any two non-zero vectors in a two-dimensional subspace of $\mathbb{R}^3$, which is orthogonal to $\vec{v}_1$. Therefore, for every angle, there are $\vec{v}_2$ and $\vec{v}_3$ which contain it. In particular, it is possible to choose $\vec{v}_2$ to be orthogonal to $\vec{v}_3$ and hence there are three mutually orthogonal eigenvectors.

Finally, if λ_2, λ_3 are non-real, i.e. $y \neq 0$, we have three mutually distinct eigenvalues and hence there are exactly three one-dimensional subspaces (each without the zero vector) of eigenvectors. If two eigenvectors are from the same subspace, then they are linearly dependent and hence they contain the zero angle.

Let us now evaluate $\vec{v}_1^\dagger \vec{v}_2$

$$\vec{v}_1^\dagger \vec{v}_2 = \vec{v}_1^\top \vec{v}_2 = \vec{v}_1^\top \mathtt{R}^\top \mathtt{R}\, \vec{v}_2 = \vec{v}_1^\top (x + yi)\, \vec{v}_2 = (x + yi)\, \vec{v}_1^\top \vec{v}_2 \tag{6.38}$$

We conclude that either $(x + yi) = 1$ or $\vec{v}_1^\top \vec{v}_2 = 0$. Since the latter can't be the case as $y \neq 0$, the former must hold true. We see that $\vec{v}_1$ is orthogonal to $\vec{v}_2$. We can show that $\vec{v}_1$ is orthogonal to $\vec{v}_3$ exactly in the same way.

Let us next consider the angle between eigenvectors $\vec{v}_2$ and $\vec{v}_3$

$$\begin{aligned}
\vec{v}_3^\dagger \vec{v}_2 = \vec{v}_3^\dagger \mathtt{R}^\top \mathtt{R}\, \vec{v}_2 = (\mathtt{R}\, \vec{v}_3)^\dagger \mathtt{R}\, \vec{v}_2 &= ((x - yi)\, \vec{v}_3)^\dagger (x + yi)\, \vec{v}_2 && (6.39)\\
&= \vec{v}_3^\dagger\, (x + yi)\, (x + yi)\, \vec{v}_2 && (6.40)\\
\vec{v}_3^\dagger \vec{v}_2 &= (x^2 + 2\,xyi - y^2)\, \vec{v}_3^\dagger \vec{v}_2 && (6.41)
\end{aligned}$$

We conclude that either $(x^2 + 2xyi - y^2) = 1$ or $\vec{v}_3^\dagger \vec{v}_2 = 0$. The former implies $xy = 0$ and threfore $x = 0$ since $y \neq 0$ but then $-y^2 = 1$, which is, for a real y, impossible. We see that $\vec{v}_3^\dagger \vec{v}_2 = 0$, i.e. vectors $\vec{v}_2$ are orthogonal to vectors $\vec{v}_3$.

Clearly, it is always possible to choose three mutually orhogonal eigenvectors. We can further normalize them to unit legth and thus obtain an orthonormal basis as non-zero orthogonal vectors are linearly independent. Therefore

$$\begin{aligned}
\mathtt{R}\begin{bmatrix}\vec{v}_1 & \vec{v}_2 & \vec{v}_3\end{bmatrix} &= \begin{bmatrix}\vec{v}_1 & \vec{v}_2 & \vec{v}_3\end{bmatrix}\begin{bmatrix}\lambda_1 & & \\ & \lambda_2 & \\ & & \lambda_3\end{bmatrix} && (6.42)\\
\begin{bmatrix}\vec{v}_1 & \vec{v}_2 & \vec{v}_3\end{bmatrix}^\dagger \mathtt{R}\begin{bmatrix}\vec{v}_1 & \vec{v}_2 & \vec{v}_3\end{bmatrix} &= \begin{bmatrix}\lambda_1 & & \\ & \lambda_2 & \\ & & \lambda_3\end{bmatrix} && (6.43)
\end{aligned}$$

Let us further investigate the structure of eigenvectors $\vec{v}_2, \vec{v}_3$. We shall show that they are "conjugated". Let's write $\vec{v}_2 = \vec{u} + \vec{w}i$ with real vectors $\vec{u}, \vec{w}$. There holds true

$$\begin{aligned}
\mathtt{R}\, \vec{v}_2 &= \mathtt{R}\, (\vec{u} + \vec{w}i) = \mathtt{R}\, \vec{u} + \mathtt{R}\, \vec{w}\, i && (6.44)\\
(x + yi)\, \vec{v}_2 &= (x + yi)\, (\vec{u} + \vec{w}i) = x\, \vec{u} - y\, \vec{w} + (x\vec{w} + y\vec{u})i && (6.45)
\end{aligned}$$

which implies

$$\mathtt{R}\, \vec{u} = x\, \vec{u} - y\, \vec{w} \quad \text{and} \quad \mathtt{R}\, \vec{w} = x\, \vec{w} + y\, \vec{u} \tag{6.46}$$

Now, let us compare two expressions: $\mathtt{R}\, (\vec{u} - \vec{w}i)$ and $(x - yi)\, (\vec{u} - \vec{w}i)$

$$\begin{aligned}
\mathtt{R}\, (\vec{u} - \vec{w}i) &= \mathtt{R}\, \vec{u} - \mathtt{R}\, \vec{w}i = x\, \vec{u} - y\, \vec{w} - (x\, \vec{w} + y\, \vec{u})\, i && (6.47)\\
(x - yi)\, (\vec{u} - \vec{w}i) &= x\, \vec{u} - y\, \vec{w} - (x\, \vec{w} + y\, \vec{u})\, i && (6.48)
\end{aligned}$$

We see that

$$\mathtt{R}\, (\vec{u} - \vec{w}i) = (x - yi)\, (\vec{u} - \vec{w}i) \tag{6.49}$$

which means that $(x - yi, \vec{u} - \vec{w}i)$ are an eigenvalue-eigenvector pair of $\mathtt{R}$. It is importatnt to understand what has been shown. We have shown that if $\vec{u} + \vec{w}i$ is an eigenvector of $\mathtt{R}$ corresponding to an eigenvalue λ, then the conjugated vector $\vec{u} - \vec{w}i$ is an eignevector of $\mathtt{R}$ corresponding to eigenvalue, which is conjugated to λ (This does not mean that every two eigenvectors corresponding to $x + yi$ and $x - yi$ must be conjugated).

The conclusion from the previous analysis is that the both non-real eigenvectors of $\mathtt{R}$ are generated by the same two real vectors $\vec{u}$ and $\vec{w}$. Let us look at the angle between $\vec{u}$ and $\vec{w}$. Consider that

$$\begin{align} 0 = \vec{v}_3^{\dagger}\vec{v}_2 &= (\vec{u} - \vec{w}i)^{\dagger}(\vec{u} + \vec{w}i) = (\vec{u}^{\top} + \vec{w}^{\top} i)(\vec{u} + \vec{w}i) \tag{6.50}\\ &= (\vec{u}^{\top}\vec{u} - \vec{w}^{\top}\vec{w}) + (\vec{u}^{\top}\vec{w} + \vec{w}^{\top}\vec{u})\, i \tag{6.51}\\ &= (\vec{u}^{\top}\vec{u} - \vec{w}^{\top}\vec{w}) + 2\,\vec{w}^{\top}\vec{u}\, i \tag{6.52} \end{align}$$

and therefore

$$\vec{u}^{\top}\vec{u} = \vec{w}^{\top}\vec{w} \quad \text{and} \quad \vec{w}^{\top}\vec{u} = 0 \tag{6.53}$$

which means that vectors $\vec{u}$ and $\vec{w}$ are orthogonal.

Finally, let us consider

$$0 = \vec{v}_1^{\top}\vec{v}_2 = \vec{v}_1^{\top}\vec{u} + \vec{v}_1^{\top}\vec{w}i \tag{6.54}$$

and hence

$$\vec{v}_1^{\top}\vec{u} = 0 \quad \text{and} \quad \vec{v}_1^{\top}\vec{w} = 0 \tag{6.55}$$

which means that $\vec{u}$ and $\vec{w}$ are also orthogonal to $\vec{v}_1$.

6.1.4 Rotation axis

A one-dimensional subspace generated by an eigenvector $\vec{v}_1$ of $\mathtt{R}$ corresponding to $\lambda = 1$, is called the *rotation axis* (or axis of rotation) of $\mathtt{R}$. If $\mathtt{R} = \mathtt{I}$, then there is an infinite number of rotation axes, otherwise there is exactly one. Vectors $\vec{v}$, which are in a rotation axis of rotation $\mathtt{R}$, remain unchanged by $\mathtt{R}$, i.e. $\mathtt{R}\,\vec{v} = \vec{v}$.

Consider that the eigenvector of $\mathtt{R}$ corresponding to 1 is also an eigenvector of $\mathtt{R}^{\top}$ since

$$\begin{align} \mathtt{R}\,\vec{v}_1 &= \vec{v}_1 \tag{6.56}\\ \mathtt{R}^{\top}\mathtt{R}\,\vec{v}_1 &= \mathtt{R}^{\top}\vec{v}_1 \tag{6.57}\\ \vec{v}_1 &= \mathtt{R}^{\top}\vec{v}_1 \tag{6.58} \end{align}$$

It implies

$$\begin{align} (\mathtt{R} - \mathtt{R}^{\top})\,\vec{v}_1 &= 0 \tag{6.59}\\ \begin{bmatrix} 0 & r_{12} - r_{21} & r_{13} - r_{31} \\ r_{21} - r_{12} & 0 & r_{23} - r_{32} \\ r_{31} - r_{13} & r_{32} - r_{23} & 0 \end{bmatrix} \vec{v}_1 &= 0 \tag{6.60} \end{align}$$

and we see that

$$\begin{bmatrix} 0 & r_{12} - r_{21} & r_{13} - r_{31} \\ r_{21} - r_{12} & 0 & r_{23} - r_{32} \\ r_{31} - r_{13} & r_{32} - r_{23} & 0 \end{bmatrix} \begin{bmatrix} r_{32} - r_{23} \\ r_{13} - r_{31} \\ r_{21} - r_{12} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \tag{6.61}$$

Clearly, we have a nice formula for an eigenvector corresponding to $\lambda_1 = 1$, when vector $\big[\, r_{32} - r_{23} \quad r_{13} - r_{31} \quad r_{21} -$ is non-zero. That is when $\mathtt{R} - \mathtt{R}^{\top}$ is a non-zero matrix, which is exactly when $\mathtt{R}$ is not symmetric.

Let us now investigate the situation when $\mathtt{R}$ is symmetric. Then, $\mathtt{R} = \mathtt{R}^{\top} = \mathtt{R}^{-1}$ and therefore

$$\mathtt{R}\,(\mathtt{R} + \mathtt{I}) = \mathtt{R}\,\mathtt{R} + \mathtt{R} = \mathtt{I} + \mathtt{R} = \mathtt{R} + \mathtt{I} \tag{6.62}$$

which shows that the non-zero columns of the matrix $\mathtt{R} + \mathtt{I}$ are eigenvectors corresponding to the unit eigenvalue. Clearly, at least one of the columns must be non-zero since otherwise, $\mathtt{R} = -\mathtt{I}$ and $|\mathtt{R}|$ would be minus one, which is impossible for a rotation.

6.1.5 Rotation angle

Rotation angle θ of rotation $\mathtt{R}$ is the angle between a non-zero real vector $\vec{x}$ which is orthogonal to $\vec{v}_1$ and its image $\mathtt{R}\,\vec{x}$. There holds

$$\cos\theta = \frac{\vec{x}^\top \mathtt{R}\,\vec{x}}{\vec{x}^\top \vec{x}} \tag{6.63}$$

Let us set

$$\vec{x} = \vec{u} + \vec{w} \tag{6.64}$$

Clearly, $\vec{x}$ is a real vector which is orthogonal to $\vec{v}_1$ since both $\vec{u}$ and $\vec{w}$ are. Let's see that it is non-zero. Vector $\vec{v}_2$ is an eigenvector and thus

$$0 \neq \vec{v}_2^\top \vec{v}_2 = \vec{u}^\top \vec{u} + \vec{w}^\top \vec{w} \tag{6.65}$$

and therefore $\vec{u} \neq \vec{0}$ or $\vec{w} \neq \vec{0}$. Vectors $\vec{u}, \vec{w}$ are orthogonal and therefore their sum can be zero only if they both are zero since otherwise for, e.g., a non-zero $\vec{u}$ we get the following contradiction

$$0 = \vec{u}^\top \vec{0} = \vec{u}^\top(\vec{u} + \vec{v}) = \vec{u}^\top \vec{u} + \vec{u}^\top \vec{v} = \vec{u}^\top \vec{u} \neq 0 \tag{6.66}$$

Let us now evaluate

$$\begin{aligned}\cos\theta &= \frac{\vec{x}^\top \mathtt{R}\,\vec{x}}{\vec{x}^\top \vec{x}} = \frac{(\vec{u}+\vec{w})^\top \mathtt{R}\,(\vec{u}+\vec{w})}{(\vec{u}+\vec{w})^\top(\vec{u}+\vec{w})} = \frac{(\vec{u}+\vec{w})^\top(x\,\vec{u} - y\,\vec{w} + x\,\vec{w} + y\,\vec{u})}{\vec{u}^\top\vec{u} + \vec{w}^\top\vec{w}} \\ &= \frac{x\,(\vec{u}^\top\vec{u} + \vec{w}^\top\vec{w}) + y\,(\vec{u}^\top\vec{u} - \vec{w}^\top\vec{w})}{\vec{u}^\top\vec{u} + \vec{w}^\top\vec{w}} \qquad (6.67) \\ &= x \qquad (6.68)\end{aligned}$$

We have used equation 6.46 and equation 6.53. We see that the rotation angle is given by the real part of λ_2 (or λ_3). Consider the characteristic equation of $\mathtt{R}$, Equation 6.13

$$\begin{aligned} 0 &= \lambda^3 - \operatorname{trace}\mathtt{R}\,\lambda^2 + (\mathtt{R}_{11} + \mathtt{R}_{22} + \mathtt{R}_{33})\,\lambda - |\mathtt{R}| \qquad (6.69) \\ &= (\lambda - 1)(\lambda - x - yi)(\lambda - x + yi) \qquad (6.70) \\ &= \lambda^3 - (2\,x + 1)\,\lambda^2 + (x^2 + 2\,x + y^2)\,\lambda - (x^2 + y^2) \qquad (6.71)\end{aligned}$$

We see that $\operatorname{trace}\mathtt{R} = 2\,x + 1$ and thus

$$\cos\theta = \frac{1}{2}(\operatorname{trace}\mathtt{R} - 1) \tag{6.72}$$

6.1.6 Matrix $(\mathtt{R} - \mathtt{I})$

§ 1 The range and the null space of $(\mathtt{R} - \mathtt{I})$. We have seen that $\operatorname{rank}(\mathtt{R} - \mathtt{I}) = 0$ for $\mathtt{R} = \mathtt{I}$ and $\operatorname{rank}(\mathtt{R} - \mathtt{I}) = 2$ for all rotation matrices $\mathtt{R} \neq \mathtt{I}$. Notice also that $\operatorname{rank}(\mathtt{R}^\top - \mathtt{I}) = \operatorname{rank}(\mathtt{R}^\top - \mathtt{I})^\top = \operatorname{rank}(\mathtt{R} - \mathtt{I})$ since rank of a matrix equals the rank of its transpose [6, 7].

Let us next investigate the relationship between the range and the null space of $(\mathtt{R} - \mathtt{I})$. The null space of $(\mathtt{R} - \mathtt{I})$ is generated by eigenvectors corresponding to 1 since $(\mathtt{R} - \mathtt{I})\,\vec{v} = 0$ implies $\mathtt{R}\,\vec{v} = \vec{v}$. Now assume that vector $\vec{v}$ is also in the range of $(\mathtt{R} - \mathtt{I})$. Then, there is a vector $\vec{a} \in \mathbb{R}^3$ such that $\vec{v} = (\mathtt{R} - \mathtt{I})\,\vec{a}$. Let us evaluate the square of the length of $\vec{v}$

$$\vec{v}^\top \vec{v} \;=\; \vec{v}^\top(\mathtt{R} - \mathtt{I})\,\vec{a} = (\vec{v}^\top \mathtt{R} - \vec{v}^\top)\,\vec{a} = (\vec{v}^\top - \vec{v}^\top)\,\vec{a} = 0 \tag{6.73}$$

which implies $\vec{v} = \vec{0}$. We have used result 6.37 with $x = 1$ and $y = 0$. Hence, the range of $\mathtt{R} - \mathtt{I}$ intersects the null space of $\mathtt{R} - \mathtt{I}$ in the zero vector.

We can show even more. Consider $\vec{v}$ in the null space of $(\mathtt{R} - \mathtt{I})$ and a vector $(\mathtt{R} - \mathtt{I})\,\vec{a}$ in the range of $(\mathtt{R} - \mathtt{I})$. Then, using 6.58,

$$\vec{v}^\top(\mathtt{R} - \mathtt{I})\,\vec{a} = 0\,\vec{a} = \vec{0} \tag{6.74}$$

shows that the range of $(\mathtt{R} - \mathtt{I})$ is orthogonal to the null space of [3] $(\mathtt{R} - \mathtt{I})$.

[3] In fact this also follows from $(\mathtt{R} - \mathtt{I})$ being a *normal matrix* [5], i.e., $(\mathtt{R} - \mathtt{I})^\top(\mathtt{R} - \mathtt{I}) = 2\mathtt{I} - \mathtt{R} - \mathtt{R}^\top = (\mathtt{R} - \mathtt{I})\,(\mathtt{R} - \mathtt{I})^\top$.

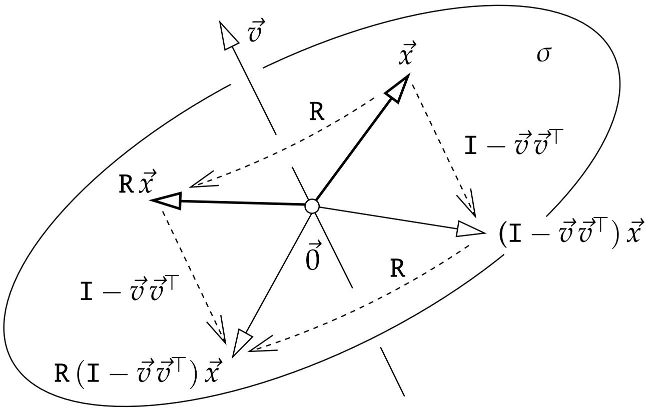

$\vec{v}$
$\vec{x}$
σ
R
$\mathtt{I} - \vec{v}\,\vec{v}^\top$
$\mathtt{R}\,\vec{x}$
$(\mathtt{I} - \vec{v}\,\vec{v}^\top)\,\vec{x}$
$\vec{0}$
R
$\mathtt{I} - \vec{v}\,\vec{v}^\top$
$\mathtt{R}\,(\mathtt{I} - \vec{v}\,\vec{v}^\top)\,\vec{x}$

Figure 6.1: $(\mathtt{R}-\mathtt{I})\,\vec{v}$ is the difference between the rotated projection of $\vec{x}$ to the range of $(\mathtt{R}-\mathtt{I})$ and the projection of $\vec{x}$ to the range of $(\mathtt{R}-\mathtt{I})$.

§ **2 Geometry of** $(\mathtt{R}-\mathtt{I})$**.** Let us now interpret $(\mathtt{R}-\mathtt{I})$ geometrically. The range of $(\mathtt{R}-\mathtt{I})$ is orthogonal to its null space. The null space of $(\mathtt{R}-\mathtt{I})$ is generated either by $\vec{v} = \vec{0}$, when its rank is zero, or by a unit vector $\vec{v}$, when its rank is two. In either case, the matrix of the projection onto the range of $\sigma = (\mathtt{R}-\mathtt{I})\,\vec{a}, \vec{a} \in \mathbb{R}^3$ can be written as $\mathtt{I} - \vec{v}\,\vec{v}^\top$ [5]. Now, let us look at a projection $\vec{x}_\sigma$ of a general vector $\vec{x}$ onto the range of $(\mathtt{R}-\mathtt{I})$, i.e. at $\vec{x}_\sigma = (\mathtt{I} - \vec{v}\,\vec{v}^\top)\,\vec{x}$. We can rotate it to $\mathtt{R}\,\vec{x}_\sigma$ and take their difference as

$$\mathtt{R}\,\vec{x}_\sigma - \vec{x}_\sigma = \mathtt{R}\,(\mathtt{I} - \vec{v}\,\vec{v}^\top)\,\vec{x} - (\mathtt{I} - \vec{v}\,\vec{v}^\top)\,\vec{x} = (\mathtt{R} - \vec{v}\,\vec{v}^\top)\,\vec{x} - (\mathtt{I} - \vec{v}\,\vec{v}^\top)\,\vec{x} = \mathtt{R}\,\vec{x} - \mathtt{I}\,\vec{x} = (\mathtt{R}-\mathtt{I})\,\vec{x}. \quad (6.75)$$

We see that $(\mathtt{R}-\mathtt{I})$ gives the difference between the rotated projection of $\vec{x}$ to the range of $(\mathtt{R}-\mathtt{I})$ and the projection of $\vec{x}$ to the range of $(\mathtt{R}-\mathtt{I})$, see Figure 6.1.

6.1.7 Tangent space to rotations

The set of rotation matrices

$$\mathcal{R} = \left\{\mathtt{R} \in \mathbb{R}^{3\times 3} \,|\, \mathtt{R}^\top \mathtt{R} = \mathtt{I},\ \ |\mathtt{R}| = 1\right\} \tag{6.76}$$

can be understood as a subset of $\mathbb{R}^9$ with

$$\mathtt{r} = \begin{bmatrix} r_{11} & r_{21} & r_{31} & r_{12} & r_{22} & r_{32} & r_{12} & r_{23} & r_3 \end{bmatrix}^\top \text{ representing } \mathtt{R} = \begin{bmatrix} r_{11} & r_{12} & r_{13} \\ r_{21} & r_{22} & r_{23} \\ r_{31} & r_{32} & r_{33} \end{bmatrix} \tag{6.77}$$

Rotation constraints in definition 6.76 are algebraic and thus $\mathcal{R}$ is a *an affine variety.*[4]. Let us investigate how does look the tangent space to $\mathcal{R}$.

To get the tangent space to $\mathcal{R}$, we will first find the normal $N_\mathtt{R}$ to $\mathcal{R}$ at rotation R and then take its orthogonal complement $T_\mathtt{R}$, which is tangent to $\mathcal{R}$ at R. In the end, we will write it all down in a convenient matrix form.

The space $N_\mathtt{R}$, normal to $\mathcal{R}$, is generated by columns of the *Jacobian matrix* [3] of constraints in 6.76, written in a matrix form as

$$\mathtt{C} = \begin{bmatrix} r_{11}\,r_{12} + r_{21}\,r_{22} + r_{31}\,r_{32} \\ r_{11}\,r_{13} + r_{21}\,r_{23} + r_{31}\,r_{33} \\ r_{12}\,r_{13} + r_{22}\,r_{23} + r_{32}\,r_{33} \\ r_{11}^2 + r_{21}^2 + r_{31}^2 - 1 \\ r_{12}^2 + r_{22}^2 + r_{32}^2 - 1 \\ r_{13}^2 + r_{23}^2 + r_{33}^2 - 1 \\ r_{11}\,r_{22}\,r_{33} - r_{11}\,r_{23}\,r_{32} - r_{12}\,r_{21}\,r_{33} + r_{12}\,r_{23}\,r_{31} + r_{13}\,r_{21}\,r_{32} - r_{13}\,r_{22}\,r_{31} - 1 \end{bmatrix} \tag{6.78}$$

[4] An affine variety is a subset of a linear space defined by algebraic constraints.

The Jacobian matrix of $\mathtt{C}$ is obtained as

$$\mathtt{J}_{ij} = \frac{\partial \mathtt{C}_i}{\partial \mathtt{r}_j}, \qquad \mathtt{J} = \begin{bmatrix} r_{12} & r_{22} & r_{32} & r_{11} & r_{21} & r_{31} & 0 & 0 & 0 \\ r_{13} & r_{23} & r_{33} & 0 & 0 & 0 & r_{11} & r_{21} & r_{31} \\ 0 & 0 & 0 & r_{13} & r_{23} & r_{33} & r_{12} & r_{22} & r_{32} \\ 2\,r_{11} & 2\,r_{21} & 2\,r_{31} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2\,r_{12} & 2\,r_{22} & 2\,r_{32} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2\,r_{13} & 2\,r_{23} & 2\,r_{33} \\ J_{71} & J_{72} & J_{73} & J_{74} & J_{75} & J_{76} & J_{77} & J_{78} & J_{79} \end{bmatrix}$$

with

$$\begin{aligned} J_{71} &= \quad r_{22}\,r_{33} - r_{23}\,r_{32} \\ J_{72} &= -r_{12}\,r_{33} + r_{13}\,r_{32} \\ J_{73} &= \quad r_{12}\,r_{23} - r_{13}\,r_{22} \\ J_{74} &= -r_{21}\,r_{33} + r_{23}\,r_{31} \\ J_{75} &= \quad r_{11}\,r_{33} - r_{13}\,r_{31} \\ J_{76} &= -r_{11}\,r_{23} + r_{13}\,r_{21} \\ J_{77} &= \quad r_{21}\,r_{32} - r_{22}\,r_{31} \\ J_{78} &= -r_{11}\,r_{32} + r_{12}\,r_{31} \\ J_{79} &= \quad r_{11}\,r_{22} - r_{12}\,r_{21} \end{aligned}$$

Jacobian matrix $\mathtt{J}$ is a 7×9 matrix. Rows $1, 2, 3$ of $\mathtt{J}$ have the property that each row contains elements of just two columns of $\mathtt{R}$. Rows $4, 5, 6$ of $\mathtt{J}$ have the property that each row contains elements of just one column of $\mathtt{R}$. It thus suggests to construct a basis $\mathtt{T}$ of the tangent space $T_{\mathtt{R}}$ to $\mathcal{R}$ from columns of $\mathtt{R}$. We can check that

$$\mathtt{J}\,\mathtt{T} = 0 \quad \text{with} \quad \mathtt{T} = \begin{bmatrix} 0 & -r_{13} & r_{12} \\ 0 & -r_{23} & r_{22} \\ 0 & -r_{33} & r_{32} \\ r_{13} & 0 & -r_{11} \\ r_{23} & 0 & -r_{21} \\ r_{33} & 0 & -r_{31} \\ -r_{12} & r_{11} & 0 \\ -r_{22} & r_{21} & 0 \\ -r_{32} & r_{31} & 0 \end{bmatrix}. \tag{6.79}$$

Next, we can see that each column of $\mathtt{T}$ contains two different columns of $\mathtt{R}$ and hence $\mathtt{T}\,\mathtt{x} = 0$ for a non-zero $\mathtt{x}$ implies that every two columns of $\mathtt{R}$ are linearly dependent, which is impossible. Therefore, $\mathtt{T}$ has rank equal to three at least.

Finally, the first six rows of $\mathtt{J}$ contain columns of $\mathtt{R}$. We see that $\begin{bmatrix}\mathtt{x}^\top & 0\end{bmatrix}\mathtt{J} = 0$ for a non-zero $\mathtt{x}$ implies that columns of $\mathtt{R}$ are linearly dependent, which is impossible. Therefore, the rank of $N_{\mathtt{R}}$ is not smaller than six. Hence, the dimension of the tangent space $T_{\mathtt{R}}$ is exactly three at every $\mathtt{R} \in \mathcal{R}$ and $\mathtt{T}$ is indeed a basis of $T_{\mathtt{R}}$.

Let us now rewrite the above back into a matrix form by inverting the matrix vectorization used in 6.77. We rewrite columns of $\mathtt{T}$ into three matrices

$$\mathtt{T}_1 = \begin{bmatrix} 0 & r_{13} & -r_{12} \\ 0 & r_{23} & -r_{22} \\ 0 & r_{33} & -r_{32} \end{bmatrix}, \; \mathtt{T}_2 = \begin{bmatrix} -r_{13} & 0 & r_{11} \\ -r_{23} & 0 & r_{21} \\ -r_{33} & 0 & r_{31} \end{bmatrix}, \; \mathtt{T}_3 = \begin{bmatrix} r_{12} & -r_{11} & 0 \\ r_{22} & -r_{21} & 0 \\ r_{32} & -r_{31} & 0 \end{bmatrix} \tag{6.80}$$

and then can write the reformated tangent space of rotations at $\mathtt{R}$ for some real vector $\mathtt{s} = \begin{bmatrix} s_1 & s_2 & s_3 \end{bmatrix}$ as

$$\begin{aligned}
\mathtt{T}_\mathtt{R}(\mathtt{s}) &= \mathtt{T}_1 s_1 + \mathtt{T}_2 s_2 + \mathtt{T}_3 s_3 && (6.81)\\
&= \begin{bmatrix} -s_2 \begin{bmatrix} r_{13} \\ r_{23} \\ r_{33} \end{bmatrix} + s_3 \begin{bmatrix} r_{12} \\ r_{22} \\ r_{32} \end{bmatrix}, & s_1 \begin{bmatrix} r_{13} \\ r_{23} \\ r_{33} \end{bmatrix} - s_3 \begin{bmatrix} r_{11} \\ r_{21} \\ r_{31} \end{bmatrix}, & -s_1 \begin{bmatrix} r_{12} \\ r_{22} \\ r_{32} \end{bmatrix} + s_2 \begin{bmatrix} r_{11} \\ r_{21} \\ r_{31} \end{bmatrix} \end{bmatrix} \\
&= \begin{bmatrix} r_{11} & r_{12} & r_{13} \\ r_{21} & r_{22} & r_{23} \\ r_{31} & r_{32} & r_{33} \end{bmatrix} \begin{bmatrix} 0 & -s_3 & s_2 \\ s_3 & 0 & -s_1 \\ -s_2 & s_1 & 0 \end{bmatrix} && (6.82)\\
&= \mathtt{R}\,[\mathtt{s}]_\times && (6.83)
\end{aligned}$$

The first order approximation of rotations around $\mathtt{R}$ is then obtained as

$$\mathtt{R} + \mathtt{T}_\mathtt{R}(\mathtt{s}) = \mathtt{R} + \mathtt{R}\,[\mathtt{s}]_\times = \mathtt{R}\,(\mathtt{I} + [\mathtt{s}]_\times) \tag{6.84}$$

In particular, vectors in the tangent spaces to the space of rotations at the identity, which are called *infinitesimal rotations*, are

$$\mathtt{T}_\mathtt{I}(\mathtt{s}) = [\mathtt{s}]_\times \tag{6.85}$$

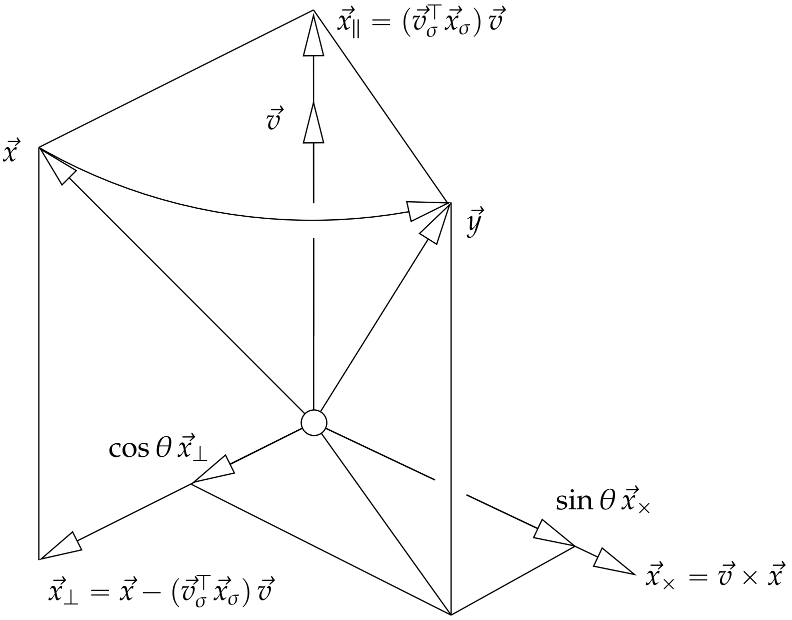
and the first order approximation of rotations at identity is

$$\mathtt{I} + \mathtt{T}_\mathtt{I}(\mathtt{s}) = \mathtt{I} + [\mathtt{s}]_\times \tag{6.86}$$

7 Rotation representation and parameterization

We have seen Chapter 6 that rotation can be represented by an orthonormal matrix $\mathtt{R}$. Matrix $\mathtt{R}$ has nine elements and there are six constraints $\mathtt{R}^\top \mathtt{R} = \mathtt{I}$ and one constratint $|\mathtt{R}| = 1$. Hence, we can view the space of all rotation matrices as a subset of $\mathbb{R}^9$. This subset[1] is determined by seven polynomial equations in nine variables. We will next investigate how to describe, i.e. *parameterize*, this set with fewer parameters and fewer constraints.

7.1 Angle-axis representation of rotation



$\vec{x}_{||} = (\vec{v}_\sigma^\top \vec{x}_\sigma)\, \vec{v}$
$\vec{v}$
$\vec{x}$
$\vec{y}$
$\cos\theta\, \vec{x}_\perp$
$\sin\theta\, \vec{x}_\times$
$\vec{x}_\perp = \vec{x} - (\vec{v}_\sigma^\top \vec{x}_\sigma)\, \vec{v}$
$\vec{x}_\times = \vec{v} \times \vec{x}$

Figure 7.1: Vector $\vec{y}$ is obtained by rotating vector $\vec{x}$ by angle θ around the rotation axis given by unit vector $\vec{v}$. Vector $\vec{y}$ can be written as a linear combination of an orthogonal basis $[\vec{x} - (\vec{v}_\sigma^\top \vec{x}_\sigma)\, \vec{v}, \vec{v} \times \vec{x}, (\vec{v}_\sigma^\top \vec{x}_\sigma)\, \vec{v}]$.

We know, Paragraph 6.1.4, that every rotation is etermined by a rotation axis and a rotation angle. Let us next give a classical construction of the rotation matrix from an axis and angle.

Figure 7.1 shows how the vector $\vec{x}$ rotates by angle θ around an axis given by a unit vector $\vec{v}$ into vector $\vec{y}$. To find the relationship between $\vec{x}$ and $\vec{y}$, we shall construct a special basis of $\mathbb{R}^3$. Vector $\vec{x}$ either is, or it is not a multiple of $\vec{v}$. If it is, than $\vec{y} = \vec{x}$ and $\mathtt{R} = \mathtt{I}$. Let us alternatively consider $\vec{x}$, which is not a multiple of $\vec{v}$ (an hence is not the zero vector!). Futher, let us consider the standard basis σ of $\mathbb{R}^3$ and coordinates of vectors $\vec{x}_\sigma$ and $\vec{v}_\sigma$. We construct three non-zero vectors

$$\begin{aligned} \vec{x}_{||\sigma} &= (\vec{v}_\sigma^\top \vec{x}_\sigma)\, \vec{v}_\sigma && (7.1) \\ \vec{x}_{\perp\sigma} &= \vec{x} - (\vec{v}_\sigma^\top \vec{x}_\sigma)\, \vec{v}_\sigma && (7.2) \\ \vec{x}_{\times\sigma} &= \vec{v}_\sigma \times \vec{x}_\sigma && (7.3) \end{aligned}$$

[1] It is often called algebraic variaty in specialized literature [2].

which are mutually orthogonal and hence form a basis of $\mathbb{R}^3$. We may notice that cooridate vectors $\vec{x} \in \mathbb{R}^3$, are actually equal to their coordinates w.r.t. the standard basis σ. Hence we can drop σ index and write

$$\begin{aligned}
\vec{x}_{||} &= (\vec{v}^\top \vec{x})\,\vec{v} = \vec{v}\,(\vec{v}^\top \vec{x}) = (\vec{v}\,\vec{v}^\top)\,\vec{x} = [\vec{v}]_{||}\,\vec{x} && (7.4)\\
\vec{x}_{\perp} &= \vec{x} - (\vec{v}^\top \vec{x})\,\vec{v} = \vec{x} - (\vec{v}\,\vec{v}^\top)\,\vec{x} = (\mathtt{I} - \vec{v}\,\vec{v}^\top)\,\vec{x} = [\vec{v}]_{\perp}\,\vec{x} && (7.5)\\
\vec{x}_{\times} &= \vec{v} \times \vec{x} = [\vec{v}]_{\times}\,\vec{x} && (7.6)
\end{aligned}$$

We have introduced two new matrices

$$[\vec{v}]_{||} = \vec{v}\,\vec{v}^\top \quad \text{and} \quad [\vec{v}]_{\perp} = \mathtt{I} - \vec{v}\,\vec{v}^\top \tag{7.7}$$

Let us next study how the three matrices $[\vec{v}]_{||}$, $[\vec{v}]_{\perp}$, $[\vec{v}]_{\times}$ behave under the transposition and mutual multiplication. We see that the following indentities

$$\begin{array}{llll}
[\vec{v}]_{||}^\top = \ [\vec{v}]_{||}\,, & [\vec{v}]_{||}\,[\vec{v}]_{||} = [\vec{v}]_{||}\,, & [\vec{v}]_{||}\,[\vec{v}]_{\perp} = \mathbb{0}, & [\vec{v}]_{||}\,[\vec{v}]_{\times} = \mathbb{0},\\
[\vec{v}]_{\perp}^\top = \ [\vec{v}]_{\perp}\,, & [\vec{v}]_{\perp}\,[\vec{v}]_{||} = \mathbb{0}, & [\vec{v}]_{\perp}\,[\vec{v}]_{\perp} = [\vec{v}]_{\perp}\,, & [\vec{v}]_{\perp}\,[\vec{v}]_{\times} = [\vec{v}]_{\times}\,,\\
[\vec{v}]_{\times}^\top = -[\vec{v}]_{\times}\,, & [\vec{v}]_{\times}\,[\vec{v}]_{||} = \mathbb{0}, & [\vec{v}]_{\times}\,[\vec{v}]_{\perp} = [\vec{v}]_{\times}\,, & [\vec{v}]_{\times}\,[\vec{v}]_{\times} = -[\vec{v}]_{\perp}
\end{array} \tag{7.8}$$

hold true. The last identity is obtained as follows

$$\begin{aligned}
[\vec{v}]_{\times}\,[\vec{v}]_{\times} &= \begin{bmatrix} 0 & -v_3 & v_2\\ v_3 & 0 & -v_1\\ -v_2 & v_1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -v_3 & v_2\\ v_3 & 0 & -v_1\\ -v_2 & v_1 & 0 \end{bmatrix} && (7.9)\\
&= \begin{bmatrix} -v_2^2 - v_3^2 & v_1 v_2 & v_1 v_3\\ v_1 v_2 & -v_1^2 - v_3^2 & v_2 v_3\\ v_1 v_3 & v_2 v_3 & -v_1^2 - v_2^2 \end{bmatrix} && (7.10)\\
&= \begin{bmatrix} v_1^2 - 1 & v_1 v_2 & v_1 v_3\\ v_1 v_2 & v_2^2 - 1 & v_2 v_3\\ v_1 v_3 & v_2 v_3 & v_3^2 - 1 \end{bmatrix} = [\vec{v}]_{||} - \mathtt{I} = -[\vec{v}]_{\perp} && (7.11)
\end{aligned}$$

It is also interesting to investigate the norms of vectors $\vec{x}_{\perp}$ and $\vec{x}_{\times}$. Consider

$$\begin{aligned}
\|\vec{x}_{\times}\|^2 &= \vec{x}_{\times}^\top \vec{x}_{\times} = \vec{x}^\top\,[\vec{v}]_{\times}^\top\,[\vec{v}]_{\times}\,\vec{x} = \vec{x}^\top(-[\vec{v}]_{\times}^2)\vec{x} = \vec{x}^\top\,[\vec{v}]_{\perp}\,\vec{x} && (7.12)\\
\|\vec{x}_{\perp}\|^2 &= \vec{x}_{\perp}^\top \vec{x}_{\perp} = \vec{x}^\top\,[\vec{v}]_{\perp}^\top\,[\vec{v}]_{\perp}\,\vec{x} = \vec{x}^\top\,[\vec{v}]_{\perp}^2\,\vec{x} = \vec{x}^\top\,[\vec{v}]_{\perp}\,\vec{x} && (7.13)
\end{aligned}$$

Since norms are non-negaive, we conclude that $\|\vec{x}_{\perp}\| = \|\vec{x}_{\times}\|$.

We can now write $\vec{y}$ in the basis $[\vec{x}_{||}, \vec{x}_{\perp}, \vec{x}_{\times}]$ as

$$\begin{aligned}
\vec{y} &= \vec{x}_{||} + ||\vec{x}_{\perp}||\,\cos\theta\,\frac{\vec{x}_{\perp}}{||\vec{x}_{\perp}||} + ||\vec{x}_{\perp}||\,\sin\theta\,\frac{\vec{x}_{\times}}{||\vec{x}_{\times}||} && (7.14)\\
&= \vec{x}_{||} + \cos\theta\,\vec{x}_{\perp} + \sin\theta\,\vec{x}_{\times} && (7.15)\\
&= [\vec{v}]_{||}\,\vec{x} + \cos\theta\,[\vec{v}]_{\perp}\,\vec{x} + \sin\theta\,[\vec{v}]_{\times}\,\vec{x} && (7.16)\\
&= ([\vec{v}]_{||} + \cos\theta\,[\vec{v}]_{\perp} + \sin\theta\,[\vec{v}]_{\times})\,\vec{x} = \mathtt{R}\,\vec{x} && (7.17)
\end{aligned}$$

We obtained matrix

$$\mathtt{R} = [\vec{v}]_{||} + \cos\theta\,[\vec{v}]_{\perp} + \sin\theta\,[\vec{v}]_{\times} \tag{7.18}$$

Let us check that this indeed is a rotation matrix

$$\begin{aligned}
\mathtt{R}^\top\mathtt{R} &= \left([\vec{v}]_{||} + \cos\theta\,[\vec{v}]_{\perp} + \sin\theta\,[\vec{v}]_{\times}\right)^\top \left([\vec{v}]_{||} + \cos\theta\,[\vec{v}]_{\perp} + \sin\theta\,[\vec{v}]_{\times}\right)\\
&= \left([\vec{v}]_{||} + \cos\theta\,[\vec{v}]_{\perp} - \sin\theta\,[\vec{v}]_{\times}\right) \left([\vec{v}]_{||} + \cos\theta\,[\vec{v}]_{\perp} + \sin\theta\,[\vec{v}]_{\times}\right)\\
&= [\vec{v}]_{||} + \cos^2\theta\,[\vec{v}]_{\perp} + \sin\theta\,\cos\theta\,[\vec{v}]_{\times} - \sin\theta\,\cos\theta\,[\vec{v}]_{\times} + \sin^2\theta\,[\vec{v}]_{\perp}\\
&= [\vec{v}]_{||} + [\vec{v}]_{\perp} = \mathtt{I} && (7.19)
\end{aligned}$$

$\mathtt{R}$ can be written in many variations, which are useful in different situations when simplifying formulas. Let us provide the most common of them using $[\vec{v}]_{||} = \vec{v}\,\vec{v}^\top$, $[\vec{v}]_\perp = \mathtt{I} - [\vec{v}]_{||} = \mathtt{I} - \vec{v}\,\vec{v}^\top$ and $[\vec{v}]_\times$

$$\begin{aligned}
\mathtt{R} &= [\vec{v}]_{||} + \cos\theta\, [\vec{v}]_\perp + \sin\theta\, [\vec{v}]_\times && (7.20)\\
&= \vec{v}\,\vec{v}^\top + \cos\theta\,(\mathtt{I} - \vec{v}\,\vec{v}^\top) + \sin\theta\, [\vec{v}]_\times && (7.21)\\
&= \cos\theta\,\mathtt{I} + (1-\cos\theta)\,\vec{v}\,\vec{v}^\top + \sin\theta\, [\vec{v}]_\times && (7.22)\\
&= \cos\theta\,\mathtt{I} + (1-\cos\theta)\, [\vec{v}]_{||} + \sin\theta\, [\vec{v}]_\times && (7.23)\\
&= \cos\theta\,\mathtt{I} + (1-\cos\theta)\,(\mathtt{I} + [\vec{v}]_\times^2) + \sin\theta\, [\vec{v}]_\times && (7.24)\\
&= \mathtt{I} + (1-\cos\theta)\,[\vec{v}]_\times^2 + \sin\theta\,[\vec{v}]_\times && (7.25)
\end{aligned}$$

7.1.1 Angle-axis parameterization

Let us write $\mathtt{R}$ in more detail

$$\begin{aligned}
\mathtt{R} &= \cos\theta\,\mathtt{I} + (1-\cos\theta)\,\vec{v}\,\vec{v}^\top + \sin\theta\, [\vec{v}]_\times && (7.26)\\
&= (1-\cos\theta)\,\vec{v}\,\vec{v}^\top + \cos\theta\,\mathtt{I} + \sin\theta\, [\vec{v}]_\times && (7.27)\\
&= (1-\cos\theta)\begin{bmatrix} v_1v_1 & v_1v_2 & v_1v_3\\ v_2v_1 & v_2v_2 & v_2v_3\\ v_3v_1 & v_3v_2 & v_3v_3\end{bmatrix} + \cos\theta\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix} + \sin\theta\begin{bmatrix}0 & -v_3 & v_2\\ v_3 & 0 & -v_1\\ -v_2 & v_1 & 0\end{bmatrix}\\
&= \begin{bmatrix} v_1v_1(1-\cos\theta) + \cos\theta & v_1v_2(1-\cos\theta) - v_3\sin\theta & v_1v_3(1-\cos\theta) + v_2\sin\theta\\ v_2v_1(1-\cos\theta) + v_3\sin\theta & v_2v_2(1-\cos\theta) + \cos\theta & v_2v_3(1-\cos\theta) - v_1\sin\theta\\ v_3v_1(1-\cos\theta) - v_2\sin\theta & v_3v_2(1-\cos\theta) + v_1\sin\theta & v_3v_3(1-\cos\theta) + \cos\theta\end{bmatrix}
\end{aligned}$$
(7.28)

which allows us to parameterize rotation by four numbers

$$\begin{bmatrix}\theta & v_1 & v_2 & v_3\end{bmatrix}^\top \quad \text{with} \quad v_1^2 + v_2^2 + v_3^2 = 1 \tag{7.29}$$

The parameterization uses goniometric functions.

7.1.2 Computing the axis and the angle of rotation from R

Let us now discuss how to get a unit vector $\vec{v}$ of the axis and the corresponding angle θ of rotation from a rotation matrix $\mathtt{R}$, such that the pair $[\theta, \vec{v}]$ gives $\mathtt{R}$ by Equation 7.28. To avoid multiple representations due to periodicity of θ, we will confine θ to real interval $(-\pi, \pi]$.

We can get $\cos(\theta)$ from Equation 6.72.

If $\cos\theta = 1$, then $\sin\theta = 0$, and thus $\theta = 0$. Then, $\mathtt{R} = \mathtt{I}$ and any unit vector can be taken as $\vec{v}$, i.e. all paris $[0, \vec{v}]$ for unit vector $\vec{v} \in \mathbb{R}^3$ represent $\mathtt{I}$.

If $\cos\theta = -1$, then $\sin\theta = 0$, and thus $\theta = \pi$. Then $\mathtt{R}$ is a symmetrical matrix and we use Equation 6.62 to get $\vec{v}_1$, a non-zero multiple of $\vec{v}$, i.e. $\vec{v} = \alpha\,\vec{v}_1$, with real non-zero α, and therefore $\vec{v}_1/||\vec{v}_1|| = s\,\vec{v}$ with $s = \pm 1$. We are getting

$$\begin{aligned}
\mathtt{R} &= 2\,[\vec{v}]_{||} - \mathtt{I} = 2\,\vec{v}\,\vec{v}^\top - \mathtt{I} = 2\,s^2\vec{v}\,\vec{v}^\top - \mathtt{I} = 2\,(s\,\vec{v})\,(s\,\vec{v})^\top - \mathtt{I} && (7.30)\\
&= 2\left(\frac{\vec{v}_1}{\|\vec{v}_1\|}\right)\left(\frac{\vec{v}_1}{\|\vec{v}_1\|}\right)^\top - \mathtt{I} = 2\left(-\frac{\vec{v}_1}{\|\vec{v}_1\|}\right)\left(-\frac{\vec{v}_1}{\|\vec{v}_1\|}\right)^\top - \mathtt{I} && (7.31)
\end{aligned}$$

from Equation 7.27 and hence we can form two pairs

$$\left[\pi, +\frac{\vec{v}_1}{\|\vec{v}_1\|}\right], \quad \left[\pi, -\frac{\vec{v}_1}{\|\vec{v}_1\|}\right] \tag{7.32}$$

representing this rotation.

Let's now move to $-1 < \cos\theta < 1$. We construct matrix

$$\begin{aligned}
\mathtt{R} - \mathtt{R}^\top &= (1-\cos\theta)\ [\vec{v}]_{\|} + \cos\theta\,\mathtt{I} + \sin\theta\ [\vec{v}]_\times \\
&\qquad - \left((1-\cos\theta)\ [\vec{v}]_{\|} + \cos\theta\,\mathtt{I} + \sin\theta\ [\vec{v}]_\times\right)^\top && (7.33)\\
&= (1-\cos\theta)\ [\vec{v}]_{\|} + \cos\theta\,\mathtt{I} + \sin\theta\ [\vec{v}]_\times \\
&\qquad - \left((1-\cos\theta)\ [\vec{v}]_{\|} + \cos\theta\,\mathtt{I} - \sin\theta\ [\vec{v}]_\times\right) && (7.34)\\
&= 2\,\sin\theta\ [\vec{v}]_\times && (7.35)
\end{aligned}$$

which gives

$$\begin{bmatrix} 0 & r_{12}-r_{21} & r_{13}-r_{31} \\ r_{21}-r_{12} & 0 & r_{23}-r_{32} \\ r_{31}-r_{13} & r_{32}-r_{23} & 0 \end{bmatrix} = 2\,\sin\theta \begin{bmatrix} 0 & -v_3 & v_2 \\ v_3 & 0 & -v_1 \\ -v_2 & v_1 & 0 \end{bmatrix} \tag{7.36}$$

and thus

$$\sin\theta\,\vec{v} = \frac{1}{2}\begin{bmatrix} r_{32}-r_{23} \\ r_{13}-r_{31} \\ r_{21}-r_{12} \end{bmatrix} \tag{7.37}$$

We thus get

$$|\sin\theta|\,||\vec{v}|| = |\sin\theta| = \frac{1}{2}\sqrt{(r_{23}-r_{32})^2 + (r_{31}-r_{13})^2 + (r_{12}-r_{21})^2} \tag{7.38}$$

There holds

$$\sin\theta\,\vec{v} = \sin(-\theta)\,(-\vec{v}) \tag{7.39}$$

true and hence we define

$$\theta = \arccos\left(\frac{1}{2}(\operatorname{trace}(\mathtt{R}) - 1)\right), \quad \vec{r} = \frac{1}{2}\begin{bmatrix} r_{32}-r_{23} \\ r_{13}-r_{31} \\ r_{21}-r_{12} \end{bmatrix} \tag{7.40}$$

and write two pairs

$$\left[+\theta, +\frac{\vec{r}}{\sin\theta}\right], \quad \left[-\theta, -\frac{\vec{r}}{\sin\theta}\right] \tag{7.41}$$

representing rotation $\mathtt{R}$.

We see that all rotations are represented by two pairs of $[\theta, \vec{v}]$ except for the identity, which is represented by an infinite number of pairs.

7.2 Euler vector representation and the exponential map

Let us now discuss another classical and natural representation of rotations. It may seem as only a slight variation of the angle-axis representation but it leads to several interesting connections and properties.

Let us consider the *euler vector* defined as

$$\vec{e} = \theta\,\vec{v} \tag{7.42}$$

where θ is the rotation angle and $\vec{v}$ is the unit vector representing the rotation axis in the angle-axis representation as in Equation 7.27.

Next, let us recall the very fundamental real functions [3] and their related power series

$$\exp x = \sum_{n=0}^{\infty} \frac{x^n}{n!} \tag{7.43}$$

$$\sin x = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} x^{2n+1} \tag{7.44}$$

$$\cos x = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} x^{2n} \tag{7.45}$$

It makes sense to define the exponential function of an $m \times m$ real matrix $\mathtt{A} \in \mathbb{R}^{m\times m}$ as

$$\exp \mathtt{A} = \sum_{n=0}^{\infty} \frac{\mathtt{A}^n}{n!} \tag{7.46}$$

We will now show that the rotation matrix $\mathtt{R}$ corresponding to the angle-axis parameterization $[\theta, \vec{v}]$ can be obtained as

$$\mathtt{R}([\theta, \vec{v}]) = \exp\,[\vec{e}]_\times = \exp\,[\theta\,\vec{v}]_\times \tag{7.47}$$

The basic tool we have to employ is the relationship between $[\vec{e}]_\times^3$ and $[\vec{e}]_\times$. It will allow us to pass form the ifinite summantion of matrix powers to the infinite summation of the powers of θ and hence to $\sin\theta$ and $\cos\theta$, which will, at the end, give the Rodrigues formula. We write, Equation 7.11,

$$\begin{aligned}
[\theta\,\vec{v}]_\times^2 &= \theta^2\,(\vec{v}\,\vec{v}^\top - \mathtt{I}) \\
[\theta\,\vec{v}]_\times^3 &= -\theta^2\,[\theta\vec{v}]_\times \\
[\theta\,\vec{v}]_\times^4 &= -\theta^2\,[\theta\vec{v}]_\times^2 \\
[\theta\,\vec{v}]_\times^5 &= \theta^4\,[\theta\vec{v}]_\times \\
[\theta\,\vec{v}]_\times^6 &= \theta^4\,[\theta\vec{v}]_\times^2 \\
&\vdots
\end{aligned} \tag{7.48}$$

and substitute into Equation 7.46 to get

$$\exp\,[\theta\,\vec{v}]_\times = \sum_{n=0}^{\infty} \frac{[\theta\,\vec{v}]_\times^n}{n!} \tag{7.49}$$

$$= \sum_{n=0}^{\infty} \frac{[\theta\,\vec{v}]_\times^{2n}}{(2n)!} + \sum_{n=0}^{\infty} \frac{[\theta\,\vec{v}]_\times^{2n+1}}{(2n+1)!} \tag{7.50}$$

Let us notice the identities, which are obtained by generalizing Equations 7.48 to an arbitrary power n

$$[\theta\,\vec{v}]_\times^0 = \mathtt{I} \tag{7.51}$$

$$[\theta\,\vec{v}]_\times^{2n} = (-1)^{n-1}\,\theta^{2(n-1)}\,[\theta\,\vec{v}]_\times^2 \text{ for } n = 1, \ldots \tag{7.52}$$

$$[\theta\,\vec{v}]_\times^{2n+1} = (-1)^n\,\theta^{2n}\,[\theta\,\vec{v}]_\times \text{ for } n = 0, \ldots \tag{7.53}$$

and substitute them into Equation 7.50 to get

$$\begin{aligned}
\exp\,[\theta\,\vec{v}]_\times &= \mathtt{I} + \left(\sum_{n=1}^{\infty} \frac{(-1)^{n-1}\theta^{2(n-1)}}{(2n)!}\right)[\theta\,\vec{v}]_\times^2 + \left(\sum_{n=0}^{\infty}\frac{(-1)^n\theta^{2n}}{(2n+1)!}\right)[\theta\,\vec{v}]_\times \\
&= \mathtt{I} + \left(\sum_{n=1}^{\infty} \frac{(-1)^{n-1}\theta^{2n}}{(2n)!}\right)[\vec{v}]_\times^2 + \left(\sum_{n=0}^{\infty}\frac{(-1)^n\theta^{2n+1}}{(2n+1)!}\right)[\vec{v}]_\times \\
&= \mathtt{I} - \left(\sum_{n=0}^{\infty} \frac{(-1)^{n}\theta^{2n}}{(2n)!} - 1\right)[\vec{v}]_\times^2 + \sin\theta\,[\vec{v}]_\times \\
&= \mathtt{I} - (\cos\theta - 1)\,[\vec{v}]_\times^2 + \sin\theta\,[\vec{v}]_\times \\
&= \mathtt{I} + \sin\theta\,[\vec{v}]_\times + (1-\cos\theta)\,[\vec{v}]_\times^2 \\
&= \mathtt{I} + \sin\|\vec{e}\|\left[\frac{\vec{e}}{\|\vec{e}\|}\right]_\times + (1-\cos\|\vec{e}\|)\left[\frac{\vec{e}}{\|\vec{e}\|}\right]_\times^2 \\
&= \mathtt{R}([\theta,\vec{v}]) \qquad (7.54)
\end{aligned}$$

by the comparison with Equation 7.25.

7.3 Quaternion representation of rotation

7.3.1 Quaternion parameterization

We shall now introdude another parameterization of R by four numbers but this time we will not use goniometric functions but polynomials only. We shall see later that this parameterization has other useful properties.

This paramterization is known as *unit quaternion* parameterization of rotations since rotations are represented by unit vectors from $\mathbb{R}^4$. In general, it may sense to talk even about non-unit quaternions and we will see how to use them later when applying rotations represented by unit quaternions on points represented by non-unit quaternions. To simplify our notation, we will often write “quaternions” insted of more correct “unit quaternions”.

Let us do a seemingly unnecessary trick. We will pass from θ to $\frac{\theta}{2}$ and introduce

$$\vec{q} = \begin{bmatrix} \cos\frac{\theta}{2} \\ \vec{v}\sin\frac{\theta}{2}\end{bmatrix} = \begin{bmatrix} q_1 \\ q_2 \\ q_3 \\ q_4 \end{bmatrix} = \begin{bmatrix} \cos\frac{\theta}{2} \\ v_1\sin\frac{\theta}{2} \\ v_2\sin\frac{\theta}{2} \\ v_3\sin\frac{\theta}{2}\end{bmatrix} \qquad (7.55)$$

There still holds

$$\|\vec{q}\| = q_1^2 + q_2^2 + q_3^2 + q_4^2 = \cos^2\frac{\theta}{2} + \sin^2\frac{\theta}{2}\,v_1^2 + \sin^2\frac{\theta}{2}\,v_2^2 + \sin^2\frac{\theta}{2}\,v_3^2 = \cos^2\frac{\theta}{2} + \sin^2\frac{\theta}{2} = 1 \qquad (7.56)$$

true. We can verify that the following identities

$$\begin{aligned}
\cos\theta &= 2\,\cos^2\frac{\theta}{2} - 1 = 2\,q_1^2 - 1 && (7.57)\\
\sin\theta &= 2\,\cos\frac{\theta}{2}\,\sin\frac{\theta}{2} && (7.58)\\
\sin\theta\,\vec{v} &= 2\,\cos\frac{\theta}{2}\,\sin\frac{\theta}{2}\,\vec{v} = 2\,q_1\,\begin{bmatrix} q_2 & q_3 & q_4\end{bmatrix}^\top && (7.59)\\
\cos\theta &= 1 - 2\,\sin^2\frac{\theta}{2} = 1 - 2\,(q_2^2+q_3^2+q_4^2) = q_1^2 - q_2^2 - q_3^2 - q_4^2 && (7.60)\\
1-\cos\theta &= 2\,\sin^2\frac{\theta}{2} = 2\,(q_2^2+q_3^2+q_4^2) && (7.61)
\end{aligned}$$

hold true. We can now substitute the above into Equation 7.23 to get

$$\begin{aligned}
\mathtt{R} &= \mathtt{I} + \sin\theta\,[\vec{v}]_\times + (1-\cos\theta)\,[\vec{v}]_\times^2 && (7.62)\\
&= \mathtt{I} + 2\,\cos\frac{\theta}{2}\,\sin\frac{\theta}{2}\,[\vec{v}]_\times + 2\,\sin^2\frac{\theta}{2}\,[\vec{v}]_\times^2 && (7.63)\\
&= \mathtt{I} + 2\,\cos\frac{\theta}{2}\left[\sin\frac{\theta}{2}\vec{v}\right]_\times + 2\left[\sin\frac{\theta}{2}\vec{v}\right]_\times^2 && (7.64)\\
&= \mathtt{I} + 2\,q_1\left[\begin{bmatrix} q_2\\ q_3\\ q_4\end{bmatrix}\right]_\times + 2\left[\begin{bmatrix} q_2\\ q_3\\ q_4\end{bmatrix}\right]_\times^2 && (7.65)\\
&= \begin{bmatrix} 1 & -2\,q_1q_4 & 2\,q_1q_3\\ 2\,q_1q_4 & 1 & -2\,q_1q_2\\ -2\,q_1q_3 & 2\,q_1q_2 & 1\end{bmatrix} + 2\begin{bmatrix} -q_3^2-q_4^2 & q_2q_3 & q_2q_4\\ q_2q_3 & -q_2^2-q_4^2 & q_3q_4\\ q_2q_4 & q_3q_4 & -q_2^2-q_3^2\end{bmatrix} && (7.66)\\
&= \begin{bmatrix} q_1^2+q_2^2-q_3^2-q_4^2 & 2\,(q_2q_3-q_1q_4) & 2\,(q_2q_4+q_1q_3)\\ 2\,(q_2q_3+q_1q_4) & q_1^2-q_2^2+q_3^2-q_4^2 & 2\,(q_3q_4-q_1q_2)\\ 2\,(q_2q_4-q_1q_3) & 2\,(q_3q_4+q_1q_2) & q_1^2-q_2^2-q_3^2+q_4^2\end{bmatrix} && (7.67)
\end{aligned}$$

which uses only second order polynomials in elements of $\vec{q}$.

7.3.2 Computing quaternions from R

To get the quaternions representing a rotation matrix R, we start with Equation 7.64. Let us first confine θ to the real interval $(-\pi, \pi]$ as we did for the angle-axis parameterization.

Matrix R either is or it is not symmetric.

If R is symmetric, then either $\sin\theta/2\,\vec{v} = \vec{0}$ or $\cos\theta/2 = 0$. If $\sin\theta/2\,\vec{v} = \vec{0}$, then $\sin\theta/2 = 0$ since $\|\vec{v}\| = 1$ and thus $\cos\theta/2 = \pm 1$. However, $\cos\theta/2 = -1$ for no $\theta \in (-\pi, \pi]$ and hence $\cos\theta/2 = 1$. This corresponds to $\theta = 0$ and hence to $\mathtt{R} = \mathtt{I}$ which is thus represented by quaternion

$$\begin{bmatrix} 1 & 0 & 0 & 0\end{bmatrix}^\top \tag{7.68}$$

If $\cos\theta/2 = 0$, then $\sin\theta/2 = \pm 1$ but $\sin\theta/2 = -1$ for no $\theta \in (-\pi, \pi]$ and hence $\sin\theta/2 = 1$. This corresponds to the rotation the by $\theta = \pi$ around the axis given by unit $\vec{v} = [v_1, v_2, v_3]^\top$. This rotation is thus represented by quaternion

$$\begin{bmatrix} 0 & v_1 & v_2 & v_3\end{bmatrix}^\top \tag{7.69}$$

Notice that $\vec{v}$ and $-\vec{v}$ generate the same rotation matrix R and hence every rotation by $\theta = \pi$ is represented by two quaternions.

If R is not symmetric, then $\mathtt{R} - \mathtt{R}^\top \neq \mathtt{0}$ and hence we are geting a useful relationship

$$\mathtt{R} - \mathtt{R}^\top = 4\,\cos\frac{\theta}{2}\left[\sin\frac{\theta}{2}\vec{v}\right]_\times \tag{7.70}$$

and next continue with writing

$$\cos^2\frac{\theta}{2} = 1 - \sin^2\frac{\theta}{2} = 1 - \frac{1}{2}\,(1-\cos\theta) = 1 - \frac{1}{2}\left(1 - \frac{1}{2}(\operatorname{trace}\mathtt{R} - 1)\right) = \frac{1}{4}\,(1 + \operatorname{trace}\mathtt{R}) \tag{7.71}$$

using trace R, and thus

$$q_1 = \cos\frac{\theta}{2} = \frac{s}{2}\,\sqrt{\operatorname{trace}\mathtt{R} + 1} \tag{7.72}$$

with $s = \pm 1$. We can form equation

$$\begin{bmatrix} 0 & r_{12}-r_{21} & r_{13}-r_{31}\\ r_{21}-r_{12} & 0 & r_{23}-r_{32}\\ r_{31}-r_{13} & r_{32}-r_{23} & 0\end{bmatrix} = \left[\begin{bmatrix} r_{32}-r_{23}\\ r_{13}-r_{31}\\ r_{21}-r_{12}\end{bmatrix}\right]_\times = s\,\sqrt{\operatorname{trace}\mathtt{R} + 1}\left[\begin{bmatrix} q_2\\ q_3\\ q_4\end{bmatrix}\right]_\times \tag{7.73}$$

which gives the following two quaternions

$$\frac{+1}{2\,\sqrt{\operatorname{trace}\mathtt{R}+1}}\begin{bmatrix}\operatorname{trace}\mathtt{R}+1\\ r_{32}-r_{23}\\ r_{13}-r_{31}\\ r_{21}-r_{12}\end{bmatrix},\quad \frac{-1}{2\,\sqrt{\operatorname{trace}\mathtt{R}+1}}\begin{bmatrix}\operatorname{trace}\mathtt{R}+1\\ r_{32}-r_{23}\\ r_{13}-r_{31}\\ r_{21}-r_{12}\end{bmatrix} \tag{7.74}$$

which represent the same rotation as $\mathtt{R}$.

We see that all rotations are represented by the above by two quaternions $\vec{q}$ and $-\vec{q}$ except for the identity, which is represented by exactly one quaternion.

The quaternion representation of rotation presented above represents every rotation by a finite number of quaternions whereas angle-axis repesentation allowed for an infinite number of angle-axis pairs to correspond to the indentity. Yet, even this still has an "aesthetic flaw" at the identity, which has only one quaternion whereas all other rotations have two quaternions. The "flaw" can be removed by realizing that $\vec{q} = [-1,\,0,\,0,\,0]^\top$ also maps to the identity. However, if we look for θ that corresponds to $\cos\theta/2 = -1$ we see that such $\theta/2 = \pm k\,\pi$ and hence $\theta = \pm 2\,k\,\pi$ for $k = 1, 2, \ldots$, which are points isolated from $(-\pi,\,\pi]$. Now, if we allow θ to be in interval $(-2\,\pi, +2\,\pi]$, then the set

$$\left\{ \begin{bmatrix}\cos\theta/2\\ \vec{v}\,\sin\theta/2\end{bmatrix} \,\middle|\, \theta\in[-2\,\pi,\,+2\,\pi],\,\vec{v}\in\mathbb{R}^3,\,\|\vec{v}\|=1\right\} \tag{7.75}$$

of quaternions contains exactly two quaternions for every rotation matrix $\mathtt{R}$ and is obtained by a continuous mapping of a closed interval of angles, which is boundend, times a sphere in $\mathbb{R}^3$, which is also closed and bounded.

7.3.3 Quaternion composition

Consider two rotations represented by $\vec{q}_1$ and $\vec{q}_2$. The respective rotation matrices $\mathtt{R}_1$, $\mathtt{R}_2$ can be composed into rotation matrix $\mathtt{R}_{21} = \mathtt{R}_2\,\mathtt{R}_1$, which can be represented by $\vec{q}_{21}$. Let us investigate how to obtain $\vec{q}_{21}$ from $\vec{q}_1$ and $\vec{q}_2$. We shall use Equation 7.76 to relate $\mathtt{R}_1$ to $\vec{q}_1$ and $\mathtt{R}_2$ to $\vec{q}_1$, then evaluate $\mathtt{R}_{21} = \mathtt{R}_2\,\mathtt{R}_1$ and recover $\vec{q}_{21}$ from $\mathtt{R}_{21}$. We use Equation 7.23 to write

$$\mathtt{R} = 2\,\sin^2\frac{\theta}{2}\,\vec{v}\,\vec{v}^\top + (2\,\cos^2\frac{\theta}{2}-1)\,\mathtt{I} + 2\,\cos\frac{\theta}{2}\sin\frac{\theta}{2}\;[\vec{v}]_\times \tag{7.76}$$

and

$$\begin{aligned}
\mathtt{R}_1 &= 2\,(s_1\vec{v}_1)\,(s_1\vec{v}_1)^\top + (2\,c_1^2-1)\,\mathtt{I} + 2\,c_1\;[s_1\vec{v}_1]_\times &(7.77)\\
\mathtt{R}_2 &= 2\,(s_2\vec{v}_2)\,(s_2\vec{v}_2)^\top + (2\,c_2^2-1)\,\mathtt{I} + 2\,c_2\;[s_2\vec{v}_2]_\times &(7.78)\\
\mathtt{R}_{21} &= 2\,(s_{21}\vec{v}_{21})\,(s_{21}\vec{v}_{21})^\top + (2\,c_{21}^2-1)\,\mathtt{I} + 2\,c_{21}\;[s_{21}\vec{v}_{21}]_\times
\end{aligned}$$

with shortcuts

$$c_1 = \cos\frac{\theta_1}{2},\, s_1 = \sin\frac{\theta_1}{2},\, c_2 = \cos\frac{\theta_2}{2},\, s_2 = \sin\frac{\theta_2}{2},\, c_{21} = \cos\frac{\theta_{21}}{2},\, s_{21} = \sin\frac{\theta_{21}}{2}$$

Let us next assume that both $\mathtt{R}_1, \mathtt{R}_2$ are not identities. Then $\theta_1 \neq 0$ and $\theta_2 \neq 0$ and rotation axes $\vec{v}_1 \neq \vec{0}$, $\vec{v}_2 \neq \vec{0}$ are well defined. We can now distinguish two cases. Either $\vec{v}_1 = \pm\vec{v}_2$, and then $\vec{v}_{21} = \vec{v}_1 = \pm\vec{v}_2$, or $\vec{v}_1 \neq \pm\vec{v}_2$, and then

$$[\vec{v}_1,\,\vec{v}_2,\,\vec{v}_2\times\vec{v}_1] \tag{7.79}$$

forms a basis of $\mathbb{R}^3$. We also notice that $\vec{v}_1$, $\vec{v}_2$ always appear in $\mathtt{R}_1, \mathtt{R}_2$ in the product with s_1, s_2.

We can thus write

$$\sin\frac{\theta_{21}}{2}\,\vec{v}_{21} = a_1\sin\frac{\theta_1}{2}\,\vec{v}_1 + a_2\sin\frac{\theta_2}{2}\,\vec{v}_2 + a_3\,(\sin\frac{\theta_2}{2}\,\vec{v}_2\times\sin\frac{\theta_1}{2}\,\vec{v}_1) \tag{7.80}$$

with coefficients $a_1, a_2, a_3 \in \mathbb{R}$. To find coefficients a_1, a_2, a_3, we will consider the following special situations:

1. $\vec{v}_1 = \pm\vec{v}_2$ implies $\vec{v}_{21} = \vec{v}_1 = \pm\vec{v}_2$ and $\theta_{21} = \theta_1 \pm \theta_2$ for all real θ_1 and θ_2.
2. $\vec{v}_2^\top \vec{v}_1 = 0$ and $\theta_1 = \theta_2 = \pi$ implies

$$\begin{aligned} \mathtt{R}_1 &= 2\,\vec{v}_1\vec{v}_1^\top - \mathtt{I} && (7.81)\\ \mathtt{R}_2 &= 2\,\vec{v}_2\vec{v}_2^\top - \mathtt{I} && (7.82)\\ \mathtt{R}_{21} &= (2\,\vec{v}_2\vec{v}_2^\top - \mathtt{I})(2\,\vec{v}_1\vec{v}_1^\top - \mathtt{I}) = \mathtt{I} - 2\,(\vec{v}_2\vec{v}_2^\top + \vec{v}_1\vec{v}_1^\top) && (7.83)\end{aligned}$$

We see that in the former case we are getting

$$\sin\frac{\theta_{21}}{2}\,\vec{v}_1 = (a_1\sin\frac{\theta_1}{2} + a_2\sin\frac{\theta_2}{2})\,\vec{v}_1 \quad \text{for all}\ \theta_1, \theta_2 \in \mathbb{R} \tag{7.84}$$

which for $\vec{v}_1 \neq \vec{0}$ leads to

$$\begin{aligned} \sin\frac{\theta_{21}}{2} &= a_1\sin\frac{\theta_1}{2} + a_2\sin\frac{\theta_2}{2} && (7.85)\\ \sin\frac{\theta_1+\theta_2}{2} &= a_1\sin\frac{\theta_1}{2} + a_2\sin\frac{\theta_2}{2} && (7.86)\\ \sin\frac{\theta_1}{2}\cos\frac{\theta_2}{2} + \cos\frac{\theta_1}{2}\sin\frac{\theta_2}{2} &= a_1\sin\frac{\theta_1}{2} + a_2\sin\frac{\theta_2}{2} && (7.87)\end{aligned}$$

for all $\theta_1, \theta_2 \in \mathbb{R}$. But that means that

$$a_1 = \cos\frac{\theta_2}{2} \quad \text{and} \quad a_2 = \cos\frac{\theta_1}{2} \tag{7.88}$$

In the latter case we find that $\vec{v}_{21}$ is a non-zero multiple of $\vec{v}_2 \times \vec{v}_1$ since

$$\begin{aligned} \mathtt{R}_{21}\,(\vec{v}_2 \times \vec{v}_1) &= (\mathtt{I} - 2\,(\vec{v}_2\vec{v}_2^\top + \vec{v}_1\vec{v}_1^\top))\,(\vec{v}_2 \times \vec{v}_1) && (7.89)\\ &= \vec{v}_2 \times \vec{v}_1 - 2\,\vec{v}_2\vec{v}_2^\top\,(\vec{v}_2 \times \vec{v}_1) - 2\,\vec{v}_1\vec{v}_1^\top\,(\vec{v}_2 \times \vec{v}_1) && (7.90)\\ &= \vec{v}_2 \times \vec{v}_1 && (7.91)\end{aligned}$$

However, that means that

$$\sin\frac{\theta_{21}}{2}\,\vec{v}_{21} = a_3\,(\sin\frac{\theta_2}{2}\vec{v}_2 \times \vec{v}_1\sin\frac{\theta_1}{2}) \tag{7.92}$$

We next get θ_{21} using Equation 6.72 as

$$\cos\theta_{21} = \frac{1}{2}(\operatorname{trace}\mathtt{R} - 1) = \frac{1}{2}(3 - 2\,(\|\vec{v}_2\|^2 + \|\vec{v}_1\|^2) - 1) = \frac{1}{2}(3 - 4 - 1) = -1 \tag{7.93}$$

and hence $\theta_{21} = \pm\pi$ and thus

$$\vec{v}_{21} = a_3\,(\vec{v}_1 \times \vec{v}_2) \tag{7.94}$$

but since $\vec{v}_1$ is perpendicular to $\vec{v}_2$, $\vec{v}_1 \times \vec{v}_2$ is a unit vector and thus $a_3 = 1$. We can thus hypothesize that in general

$$\sin\frac{\theta_{21}}{2}\,\vec{v}_{21} = \cos\frac{\theta_2}{2}\left(\sin\frac{\theta_1}{2}\,\vec{v}_1\right) + \cos\frac{\theta_1}{2}\left(\sin\frac{\theta_2}{2}\,\vec{v}_2\right) + \left(\sin\frac{\theta_2}{2}\,\vec{v}_2\right) \times \left(\sin\frac{\theta_1}{2}\,\vec{v}_1\right) \tag{7.95}$$

Let's next find $\cos\frac{\theta_{21}}{2}$ consistent with the above hypothesis. We see that

$$\cos^2\frac{\theta_{21}}{2} = 1 - \sin^2\frac{\theta_{21}}{2} \tag{7.96}$$

and hence we evaluate

$$\begin{align}
\sin^2\frac{\theta_{21}}{2} &= \sin^2\frac{\theta_{21}}{2}\,\vec{v}_{21}^\top\vec{v}_{21} = \left(\sin\frac{\theta_{21}}{2}\,\vec{v}_{21}\right)^{\!\top}\!\left(\sin\frac{\theta_{21}}{2}\,\vec{v}_{21}\right) \tag{7.97}\\
&= \cos^2\frac{\theta_2}{2}\,\sin^2\frac{\theta_1}{2}+\cos^2\frac{\theta_1}{2}\,\sin^2\frac{\theta_2}{2} \tag{7.98}\\
&+ 2\cos\frac{\theta_2}{2}\,\cos\frac{\theta_1}{2}\,\left(\sin\frac{\theta_2}{2}\,\vec{v}_2\right)^{\!\top}\!\left(\sin\frac{\theta_1}{2}\,\vec{v}_1\right) \tag{7.99}\\
&+ \left[\left(\sin\frac{\theta_2}{2}\,\vec{v}_2\right)\times\left(\sin\frac{\theta_1}{2}\,\vec{v}_1\right)\right]^\top\left[\left(\sin\frac{\theta_2}{2}\,\vec{v}_2\right)\times\left(\sin\frac{\theta_1}{2}\,\vec{v}_1\right)\right] \tag{7.100}
\end{align}$$

We used the fact that $\vec{v}_1$, $\vec{v}_2$ are perpendicular to their vector product.

To move further, we will use that for every two unit vectors $\vec{u}$, $\vec{v}$ in $\mathbb{R}^3$ there holds

$$\begin{align}
(\vec{u}\times\vec{v})^\top(\vec{u}\times\vec{v}) &= \|(\vec{u}\times\vec{v})\|^2 = \|\vec{u}\|^2\|\vec{v}\|^2\sin^2\angle(\vec{u},\vec{v}) \tag{7.101}\\
&= \|\vec{u}\|^2\|\vec{v}\|^2(1-\cos^2\angle(\vec{u},\vec{v})) = \|\vec{u}\|^2\|\vec{v}\|^2-(\vec{u}^\top\vec{v})^2 \tag{7.102}
\end{align}$$

true.

Applying this to the last summand in Equation 7.100, we get

$$\begin{align}
\sin^2\frac{\theta_{21}}{2} &= \cos^2\frac{\theta_2}{2}\,\sin^2\frac{\theta_1}{2}+\cos^2\frac{\theta_1}{2}\,\sin^2\frac{\theta_2}{2} \tag{7.103}\\
&+ 2\cos\frac{\theta_2}{2}\,\cos\frac{\theta_1}{2}\,\left(\sin\frac{\theta_2}{2}\,\vec{v}_2\right)^{\!\top}\!\left(\sin\frac{\theta_1}{2}\,\vec{v}_1\right) \tag{7.104}\\
&+ \sin^2\frac{\theta_2}{2}\,\sin^2\frac{\theta_1}{2}-\left[\left(\sin\frac{\theta_2}{2}\,\vec{v}_2\right)^{\!\top}\!\left(\sin\frac{\theta_1}{2}\,\vec{v}_1\right)\right]^2 \tag{7.105}\\
&= \sin^2\frac{\theta_1}{2}+\cos^2\frac{\theta_1}{2}\,\sin^2\frac{\theta_2}{2} \tag{7.106}\\
&+ 2\cos\frac{\theta_2}{2}\,\cos\frac{\theta_1}{2}\,\left(\sin\frac{\theta_2}{2}\,\vec{v}_2\right)^{\!\top}\!\left(\sin\frac{\theta_1}{2}\,\vec{v}_1\right)-\left[\left(\sin\frac{\theta_2}{2}\,\vec{v}_2\right)^{\!\top}\!\left(\sin\frac{\theta_1}{2}\,\vec{v}_1\right)\right]^2 \notag\\
&= 1-\cos^2\frac{\theta_1}{2}\,\cos^2\frac{\theta_2}{2} \tag{7.107}\\
&+ 2\cos\frac{\theta_2}{2}\,\cos\frac{\theta_1}{2}\,\left(\sin\frac{\theta_2}{2}\,\vec{v}_2\right)^{\!\top}\!\left(\sin\frac{\theta_1}{2}\,\vec{v}_1\right)-\left[\left(\sin\frac{\theta_2}{2}\,\vec{v}_2\right)^{\!\top}\!\left(\sin\frac{\theta_1}{2}\,\vec{v}_1\right)\right]^2 \notag
\end{align}$$

where we used the fact that

$$\begin{align}
\sin^2\frac{\theta_1}{2}+\cos^2\frac{\theta_1}{2}\,\sin^2\frac{\theta_2}{2} &= 1-\cos^2\frac{\theta_1}{2}+\cos^2\frac{\theta_1}{2}\,\sin^2\frac{\theta_2}{2} \tag{7.108}\\
&= 1+\cos^2\frac{\theta_1}{2}\,\left(\sin^2\frac{\theta_2}{2}-1\right) = 1-\cos^2\frac{\theta_1}{2}\,\cos^2\frac{\theta_2}{2} \notag
\end{align}$$

We are thus obtaining

$$\begin{align}
\cos^2\frac{\theta_{21}}{2} &= 1-\sin^2\frac{\theta_{21}}{2} \tag{7.109}\\
&= \cos^2\frac{\theta_1}{2}\,\cos^2\frac{\theta_2}{2} \tag{7.110}\\
&- 2\cos\frac{\theta_2}{2}\,\cos\frac{\theta_1}{2}\,\left(\sin\frac{\theta_2}{2}\,\vec{v}_2\right)^{\!\top}\!\left(\sin\frac{\theta_1}{2}\,\vec{v}_1\right)+\left[\left(\sin\frac{\theta_2}{2}\,\vec{v}_2\right)^{\!\top}\!\left(\sin\frac{\theta_1}{2}\,\vec{v}_1\right)\right]^2 \notag\\
&= \left(\cos\frac{\theta_1}{2}\,\cos\frac{\theta_2}{2}-\left(\sin\frac{\theta_2}{2}\,\vec{v}_2\right)^{\!\top}\!\left(\sin\frac{\theta_1}{2}\,\vec{v}_1\right)\right)^2 \tag{7.111}
\end{align}$$

Our complete hypothesis will be

$$\begin{aligned}\sin\frac{\theta_{21}}{2}\,\vec{v}_{21} &= \cos\frac{\theta_2}{2}\left(\sin\frac{\theta_1}{2}\,\vec{v}_1\right)+\cos\frac{\theta_1}{2}\left(\sin\frac{\theta_2}{2}\,\vec{v}_2\right)+\left(\sin\frac{\theta_2}{2}\,\vec{v}_2\right)\times\left(\sin\frac{\theta_1}{2}\,\vec{v}_1\right)\\ \cos\frac{\theta_{21}}{2} &= \cos\frac{\theta_1}{2}\cos\frac{\theta_2}{2}-\left(\sin\frac{\theta_2}{2}\,\vec{v}_2\right)^{\top}\left(\sin\frac{\theta_1}{2}\,\vec{v}_1\right)\end{aligned}\tag{7.112}$$

To verify this, we will run the following Maple [16] program

```
> restart:
> with(LinearAlgebra):
> E:=IdentityMatrix(3):
> X_:=proc(u) <<0|-u[3]|u[2]>,<u[3]|0|-u[1]>,<-u[2]|u[1]|0>> end proc:
> v1:=<x1,y1,z1>:
> v2:=<x2,y2,z2>:
> R1:=2*(s1*v1).Transpose(s1*v1)+(2*c1^2-1)*E+2*c1*X_(s1*v1):
> R2:=2*(s2*v2).Transpose(s2*v2)+(2*c2^2-1)*E+2*c2*X_(s2*v2):
> R21:=expand~(R2.R1):
> c21:=c2*c1-Transpose(s2*v2).(s1*v1);
```

$$c21 := c2\,c1 - s1\,x1\,s2\,x2 - s1\,y1\,s2\,y2 - s1\,z1\,s2\,z2$$

```
> s21v21:=c2*s1*v1+s2*c1*v2+X_(s2*v2).(s1*v1);
```

$$s21v21 := \begin{bmatrix} c2\,s1\,x1 + s2\,c1\,x2 - s2\,z2\,s1\,y1 + s2\,y2\,s1\,z1 \\ c2\,s1\,y1 + s2\,c1\,y2 + s2\,z2\,s1\,x1 - s2\,x2\,s1\,z1 \\ c2\,s1\,z1 + s2\,c1\,z2 - s2\,y2\,s1\,x1 + s2\,x2\,s1\,y1 \end{bmatrix}$$

```
> RR21:=2*s21v21.Transpose(s21v21)+(2*c21^2-1)*E+2*c21*X_(s21v21):
> simplify(expand~(RR21-R21),[x1^2+y1^2+z1^2=1,x2^2+y2^2+z2^2=1,
                                   c1^2+s1^2=1,c2^2+s2^2=1]);
```

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

which verifies that our hypothesis was correct.

Thus we see that

$$\vec{q}_{21}=\vec{q}_2\,\vec{q}_1=\begin{bmatrix}\cos\frac{\theta_{21}}{2}\\ \sin\frac{\theta_{21}}{2}\,\vec{v}_{21}\end{bmatrix}=\begin{bmatrix}\cos\frac{\theta_1}{2}\,\cos\frac{\theta_2}{2}-\sin\frac{\theta_2}{2}\,\sin\frac{\theta_1}{2}\,\vec{v}_2^{\top}\vec{v}_1\\ \cos\frac{\theta_2}{2}\,\sin\frac{\theta_1}{2}\,\vec{v}_1+\cos\frac{\theta_1}{2}\,\sin\frac{\theta_2}{2}\,\vec{v}_2+\sin\frac{\theta_2}{2}\,\sin\frac{\theta_1}{2}\,\vec{v}_2\times\vec{v}_1\end{bmatrix}\tag{7.113}$$

Considering two unit quaternions

$$\vec{p}=\begin{bmatrix}p_1\\p_2\\p_3\\p_4\end{bmatrix},\quad\text{and}\quad\vec{q}=\begin{bmatrix}q_1\\q_2\\q_3\\q_4\end{bmatrix}\tag{7.114}$$

we can now give their composition as

$$\vec{q}_{21} = \vec{q}\,\vec{p} \quad = \quad \begin{bmatrix} q_1 p_1 - q_2 p_2 - q_3 p_3 - q_4 p_4 \\ q_1 p_2 + q_2 p_1 + q_3 p_4 - q_4 p_3 \\ q_1 p_3 + q_3 p_1 + q_4 p_2 - q_2 p_4 \\ q_1 p_4 + q_4 p_1 + q_2 p_3 - q_3 p_2 \end{bmatrix} \tag{7.115}$$

$$= \begin{bmatrix} q_1 p_1 - q_2 p_2 - q_3 p_3 - q_4 p_4 \\ q_2 p_1 + q_1 p_2 - q_4 p_3 + q_3 p_4 \\ q_3 p_1 + q_4 p_2 + q_1 p_3 - q_2 p_4 \\ q_4 p_1 - q_3 p_2 + q_2 p_3 + q_1 p_4 \end{bmatrix} \tag{7.116}$$

$$= \begin{bmatrix} q_1 & -q_2 & -q_3 & -q_4 \\ q_2 & q_1 & -q_4 & q_3 \\ q_3 & q_4 & q_1 & -q_2 \\ q_4 & -q_3 & q_2 & q_1 \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{bmatrix} \tag{7.117}$$

7.3.4 Application of quaternions to vectors

Consider a rotation by angle θ around an axis with direection $\vec{v}$ represented by a unit quaternion $\vec{q} = \begin{bmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2}\,\vec{v} \end{bmatrix}$ and a vector $\vec{x} \in \mathbb{R}^3$. To rotate the vector, we may construct the rotation matrix $\mathtt{R}(\vec{q}\,)$ and apply it to the vector $\vec{x}$ as $\mathtt{R}(\vec{q}\,)\,\vec{x}$.

Interestingly enough, it is possible to accomplish this in somewhat different and more efficient way by first "embedding" vector $\vec{x}$ into a (non-unit!) quaternion

$$\vec{p}(\vec{x}) = \begin{bmatrix} 0 \\ \vec{x} \end{bmatrix} = \begin{bmatrix} 0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} \tag{7.118}$$

and then composing it with quaternion $\vec{q}$ from both sides

$$\vec{q}\,\vec{p}(\vec{x})\,\vec{q}^{-1} \quad = \quad \begin{bmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2}\,\vec{v} \end{bmatrix} \begin{bmatrix} 0 \\ \vec{x} \end{bmatrix} \begin{bmatrix} \cos\frac{\theta}{2} \\ -\sin\frac{\theta}{2}\,\vec{v} \end{bmatrix} \tag{7.119}$$

One can verify that the following

$$\begin{bmatrix} 0 \\ \mathtt{R}(\vec{q}\,)\,\vec{x} \end{bmatrix} = \vec{q}\,\vec{p}(\vec{x})\,\vec{q}^{-1} \tag{7.120}$$

holds true.

7.4 "Cayley transform" parameterization

We see that unit quaternions provide a nice parameterization. It is given as a matrix with polynomial entries of four parameters. However, unit quaternions still are somewhat redundant since every rotation is represented twice.

Let us now mention yet another classical rotation parameterization, which is known as "Cayley transform". This parameterization uses only three parameters to represent three-dimensional rotations. In a sense, it is as ecconomic as it can be. On the other hand, it can't represent rotations by 180°.

Actually, it can be proven [19] that there is no mapping (parameterization), which could be (i) continuous, (ii) one-to-one, (iii) onto, and (iv) three-dimensional (i.e. mapping a "three-dimensional box" onto all three-dimensional rotations).

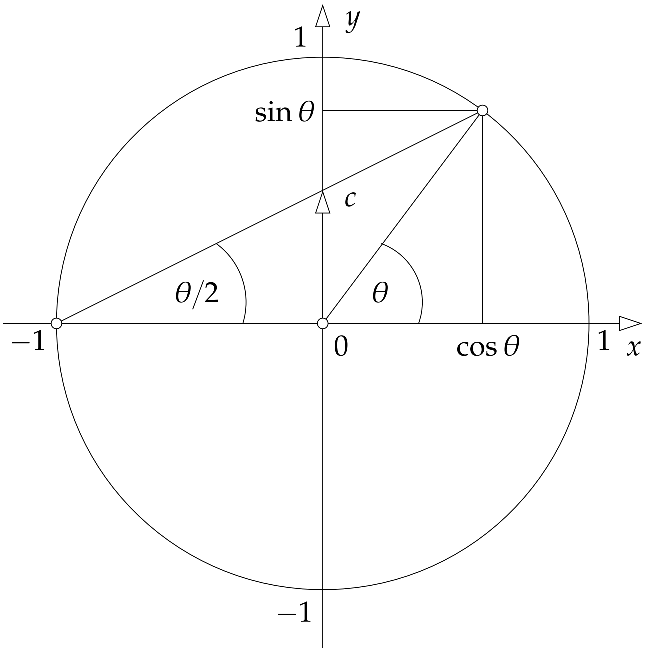


Figure 7.2: Cayley transform parameterization of two-dimensional rotations.

Axis-angle parameterization is continuous and onto but not one-to-one and not three-dimensional. Euler vector parameterization is continuous, onto, three-dimensional but not one-to one. Unit quaternions are continuous, onto but not three-dimensional and not one-to one (although they are close to that by being two-to-one). Finally, Cayley transform parameterization is continuous, one-to-one, three-dimensional but it not onto.

In addition, unit quaternions and Cayley transform parameterizations are "finite" in the sense that they are polynomial rational functions of their parameters while other above mentioned representations require some "infinite" process for computing trigonometric functions. This may be no problem if approximate evaluation of functions is acceptable but, as we will see, it is a fundamental obstacle to solving interesting engineering problems using computational algebra.

7.4.1 Cayley transform parameterization of two-dimensional rotations

Let us first look at two-dimesional roations. Figure 7.2 shows an illustartion of the relationship between parameter c and $\cos\theta$, $\sin\theta$ on the unit circle. We see that, using the similarity of triangles, $\frac{\sin\theta}{\cos\theta+1} = \frac{c}{1}$. Considering that $(\cos\theta)^2 + (\sin\theta)^2 = 1$ we are getting

$$\begin{aligned} 1-(\cos\theta)^2 &= (\sin\theta)^2 = c^2(\cos\theta+1)^2 = c^2((\cos\theta)^2 + 2\,\cos\theta + 1) &(7.121)\\ 0 &= (c^2+1)(\cos\theta)^2 + 2\,c^2\cos\theta + c^2 - 1 &(7.122)\end{aligned}$$

and thus

$$\cos\theta = \frac{-2\,c^2 \pm \sqrt{4\,c^4 - 4\,(c^2+1)(c^2-1)}}{2(c^2+1)} = \frac{-c^2 \pm \sqrt{c^4-(c^4-1)}}{c^2+1} = \frac{\pm 1 - c^2}{1+c^2} \tag{7.123}$$

gives either $\cos\theta = -1$ or

$$\cos\theta = \frac{1-c^2}{1+c^2} \tag{7.124}$$

The former case corresponds to point $[-1\ 0]^\top$. In the latter case, we have

$$\begin{aligned}(\sin\theta)^2 &= 1-(\cos\theta)^2 = 1-(\frac{1-c^2}{1+c^2})^2 = \frac{(1+c^2)^2-(1-c^2)^2}{(1+c^2)^2} && (7.125)\\ &= \frac{(1+2\,c^2+c^4)-(1-2\,c^2+c^4)}{(1+c^2)^2} = \frac{4\,c^2}{(1+c^2)^2} = \left(\frac{2\,c}{1+c^2}\right)^2 && (7.126)\end{aligned}$$

and thus $\sin\theta = \pm\frac{2\,c}{1+c^2}$. Now, we see from Figure 7.2 that we want $\sin\theta$ to be positive for positive c. Therefore, we conclude that

$$\sin\theta = \frac{2\,c}{1+c^2} \tag{7.127}$$

It is important to notice that with the parameterization given by Equation 7.124, we can never get $\cos\theta = -1$ for a real c since if that was true, we would get $-1-c^2 = 1-c^2$ and hence $-1 = 1$. On the other hand, we see that Cayley transform maps every $c \in \mathbb{R}$ into a point on the unit circle $[\cos\theta\ \ \sin\theta]^\top$, and hence to the corresponding rotation

$$\mathtt{R}(c) = \begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix} = \begin{bmatrix}\frac{1-c^2}{1+c^2} & -\frac{2\,c}{1+c^2}\\ \frac{2\,c}{1+c^2} & \frac{1-c^2}{1+c^2}\end{bmatrix} \tag{7.128}$$

The mapping $\mathtt{R}(c)\colon \mathbb{R} \to \mathtt{R}$ is one-to-one since when two c_1, c_2 map into the same point, then

$$\begin{aligned}\frac{2\,c_1}{1+c_1^2} &= \frac{2\,c_2}{1+c_2^2} && (7.129)\\ c_1(1+c_2^2) &= c_2(1+c_1^2) && (7.130)\\ c_1-c_2 &= c_1c_2(c_1-c_2) && (7.131)\end{aligned}$$

implies that either $c_1c_2 \neq 0$, and then $c_1 = c_2$, or $c_1c_2 = 0$, and then $c_1 = 0 = c_2$ because both $1+c_1^2$, $1+c_2^2$ are positive. Next, let us see that the mapping is also onto $\mathbb{R}\backslash\{[-1\ 0]^\top\}$. Consider a point $[\cos\theta\ \ \sin\theta]^\top \neq [-1\ 0]^\top$. Its preimage c, is obtained as

$$c = \frac{\sin\theta}{1+\cos\theta} \tag{7.132}$$

which is clearly defined for $\cos\theta \neq -1$.

7.4.1.1 Two-dimensional rational rotations

It is also important to notice that the $\mathtt{R}(c)$ is a rational function of c as well as c is a rational function or $\mathtt{R}$ (e.g. of the two elements in its first column). Hence, every rational number c gives a rational point $[a\ b]^\top$ on the unit circle as well as every rational point $[a\ b]^\top$ provides a rational c. This way, we can obtain all rational two-dimensional rotations by going over all rational c's plus the rotation $-\mathtt{I}_{2\times 2}$.

7.4.2 Cayley transform parameterization of three-dimensional rotations

We saw that we have obtained a bijective (one-to-one and onto) mapping between all real numbers and all two-dimensional rotations other than the rotation by 180° degrees. Now, since every three-dimensional rotation can be actually seen as a two-dimensional rotation after aligning the z-axis with the rotation axis, we may hint on having an analogous situation in three dimensions after removing all rotations by 180°. Let us investigate this further and see that we can indeed establish a bijective mapping between $\mathbb{R}^3$ and all three-dimensional rotations by other than 180° angle.

Let us consider that all rotations by 180° are represented by unit quaternions in the form $\begin{bmatrix} 0 & q_2 & q_3 & q_4 \end{bmatrix}$. Hence, to remove them, it is enough to remove from all cases when $c_1 = 0$. One way to do it, is to write down the rotation matrix in terms of (non-unit) quaternions $\vec{q}$

$$\mathtt{R}(\vec{q}) = \frac{1}{q_1^2 + q_2^2 + q_3^2 + q_4^2} \begin{bmatrix} q_1^2 + q_2^2 - q_3^2 - q_4^2 & 2\,(q_2 q_3 - q_1 q_4) & 2\,(q_2 q_4 + q_1 q_3) \\ 2\,(q_2 q_3 + q_1 q_4) & q_1^2 - q_2^2 + q_3^2 - q_4^2 & 2\,(q_3 q_4 - q_1 q_2) \\ 2\,(q_2 q_4 - q_1 q_3) & 2\,(q_3 q_4 + q_1 q_2) & q_1^2 - q_2^2 - q_3^2 + q_4^2 \end{bmatrix} \tag{7.133}$$

and then set $q_1 = 1$, $q_2 = c_1$, $q_3 = c_2$, $q_4 = c_3$, to get

$$\mathtt{R}(\vec{c}) = \frac{1}{1 + c_1^2 + c_2^2 + c_3^2} \begin{bmatrix} 1 + c_1^2 - c_2^2 - c_3^2 & 2\,(c_1 c_2 - c_3) & 2\,(c_1 c_3 + c_2) \\ 2\,(c_1 c_2 + c_3) & 1 - c_1^2 + c_2^2 - c_3^2 & 2\,(c_2 c_3 - c_1) \\ 2\,(c_1 c_3 - c_2) & 2\,(c_2 c_3 + c_1) & 1 - c_1^2 - c_2^2 + c_3^2 \end{bmatrix} \tag{7.134}$$

with $\vec{c} = \begin{bmatrix} c_1 & c_2 & c_3 \end{bmatrix}^\top \in \mathbb{R}^3$.

It can be verified that $\mathtt{R}(\vec{c})^\top \mathtt{R}(\vec{c}) = \mathtt{I}$ for all $\vec{c} \in \mathbb{R}^3$ and hence the mapping $\mathtt{R}(\vec{c})\colon \mathbb{R}^3 \to \mathtt{R}$ maps the space $\mathbb{R}^3$ into rotation matrices $\mathtt{R}$. Let us next see that the mapping is also one-to-one.

First, notice that by setting $c_1 = c_2 = 0$, we are getting

$$\mathtt{R}(c_3) = \frac{1}{1 + c_3^2} \begin{bmatrix} 1 - c_3^2 & -2\,c_3 & 0 \\ 2\,c_3 & 1 - c_3^2 & 0 \\ 0 & 0 & 1 + c_3^2 \end{bmatrix} = \begin{bmatrix} \frac{1-c_3^2}{1+c_3^2} & \frac{-2\,c_3}{1+c_3^2} & 0 \\ \frac{2\,c_3}{1+c_3^2} & \frac{1-c_3^2}{1+c_3^2} & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{7.135}$$

which is exactly the Cayley parameterization for two-dimensional rotation around the z-axis. In the same way, we get that $\mathtt{R}(c_1)$ are rotations around the x-axis and $\mathtt{R}(c_2)$ are rotations around the y-axis.

We have seen in Paragraph 7.3.2 that the mapping between the unit quaternions $\vec{q}$ and rotation matrices $\mathtt{R}(\vec{q})$ was "two-to-one" in the way that there were exactly two quaternions $\vec{q}$, $-\vec{q}$ mapping into one $\mathtt{R}$, i.e. $\mathtt{R}(\vec{q}) = \mathtt{R}(-\vec{q})$. Now, we are forcing the first coordinate of the unit quaternion $\vec{q} = \frac{\begin{bmatrix} 1 & c_1 & c_2 & c_3 \end{bmatrix}^\top}{1+c_1^2+c_2^3+c_3}$ be positive. Therefore, the mapping $\mathtt{R}(\vec{c})$ becomes one-to-one.

Now, let us see that by $\mathtt{R}(\vec{c})$ we can represent all rotations that are not by 180°. ...

8 Study motion parameterization

We understand, Chapter 5, that rotations can be represented in many ways. In particular, quaternions provide a very convenient parameterization. They provide a continuous bijection between the subset of non-isotropic points of the three-dimensional complex projective space $\mathbb{P}^3_{\mathbb{C}}$ and the rotation group $SO_{\mathbb{C}}(3)$ of the complex rotations acting on the three-dimensional complex space $\mathbb{P}^3_{\mathbb{C}}$. Our goal is to construct a nice parameterization of the three-dimensional motions $SE_{\mathbb{C}}(3)$, acting on $\mathbb{P}^3_{\mathbb{C}}$, by a subset of $\mathbb{P}^7_{\mathbb{C}}$.

Let us first look at the two-dimensional complex rotations $SO_{\mathbb{C}}(2)$ acting on $\mathbb{P}^2_{\mathbb{C}}$, which can be parameterized by a subset of the complex projective space $\mathbb{P}_{\mathbb{C}}$ as

$$\begin{bmatrix} c & s \end{bmatrix}^\top \text{ s.t. } c^2+s^2 \neq 0 \mapsto \begin{bmatrix} s^2-c^2 & -2\,c\,s & 0 \\ 2\,c\,s & s^2-c^2 & 0 \\ 0 & 0 & c^2+s^2 \end{bmatrix} \tag{8.1}$$

We can extend it to $SE_{\mathbb{C}}(2)$ acting on $\mathbb{P}^2_{\mathbb{C}}$ by

$$\begin{bmatrix} c & s & x & y \end{bmatrix}^\top \text{ s.t. } c^2+s^2 \neq 0 \mapsto \begin{bmatrix} s^2-c^2 & -2\,c\,s & c\,x-s\,y \\ 2\,c\,s & s^2-c^2 & s\,x+c\,y \\ 0 & 0 & c^2+s^2 \end{bmatrix} \tag{8.2}$$

First of all, we see that $\alpha \begin{bmatrix} c & s & x & y \end{bmatrix}^\top$ for $\alpha \in \mathbb{C}$ provides the α^2 multiple of the rotation matrix on the right hand side above, since the map is homogeneous of degree two. Next, we see that for every representative $\begin{bmatrix} t_1 & t_2 \end{bmatrix}^\top$ of a translation, we have exactly one

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} c & -s \\ s & c \end{bmatrix}^{-1} \begin{bmatrix} t_1 \\ t_2 \end{bmatrix} \tag{8.3}$$

since we can always do the inversion.

Let us now generalize the above construction to $SE_{\mathbb{C}}(3)$. We need to construct a homogeneous degree-two map acting on $\mathbb{P}^3_{\mathbb{C}}$. $SO_{\mathbb{C}}(3)$, acting on $\mathbb{P}^3_{\mathbb{C}}$, is parameterized by the non-isotropic quaternions 7.67 as

$$\mathsf{q} = \begin{bmatrix} q_1 \\ q_2 \\ q_3 \\ q_4 \end{bmatrix} \text{ s.t. } \|\mathsf{q}\|^2 \neq 0 \mapsto \begin{bmatrix} q_1^2+q_2^2-q_3^2-q_4^2 & 2\,(q_2q_3-q_1q_4) & 2\,(q_2q_4+q_1q_3) & 0 \\ 2\,(q_2q_3+q_1q_4) & q_1^2-q_2^2+q_3^2-q_4^2 & 2\,(q_3q_4-q_1q_2) & 0 \\ 2\,(q_2q_4-q_1q_3) & 2\,(q_3q_4+q_1q_2) & q_1^2-q_2^2-q_3^2+q_4^2 & 0 \\ 0 & 0 & 0 & q_1^2+q_2^2+q_3^2+q_4^2 \end{bmatrix} \tag{8.4}$$

Next, we need to construct a one-to-one homogeneous, degree-two map between the translations and one-dimensional subspaces of $\mathbb{P}^3$. Let us consider the following equation for $\mathbf{x} = \begin{bmatrix} x & y & z & w \end{bmatrix}$

$$\begin{bmatrix} q_1 & q_2 & q_3 & q_4 \\ -q_2 & q_1 & q_4 & -q_3 \\ -q_3 & -q_4 & q_1 & q_2 \\ -q_4 & q_3 & -q_2 & q_1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix} = \begin{bmatrix} 0 \\ -x\,q_2+y\,q_1+z\,q_4-w\,q_3 \\ -x\,q_3-y\,q_4+z\,q_1+w\,q_2 \\ -x\,q_4+y\,q_3-z\,q_2+w\,q_1 \end{bmatrix} = \begin{bmatrix} 0 \\ t_1 \\ t_2 \\ t_3 \end{bmatrix} \tag{8.5}$$

For every vector $\begin{bmatrix} t_1 & t_2 & t_3 \end{bmatrix}^\top$, we have a unique solution of for $\begin{bmatrix} x & y & z & w \end{bmatrix}^\top$ since the matrix on the left is of full rank for any non-zero $\begin{bmatrix} q_1 & q_2 & q_3 & q_4 \end{bmatrix}$. Thus, we can construct the map

$$\begin{bmatrix} q_1 \\ q_2 \\ q_3 \\ q_4 \\ x \\ y \\ z \\ w \end{bmatrix} \text{s.t.} \begin{bmatrix} \|\mathtt{q}\|^2 \neq 0 \\ \mathtt{x}^\top \mathtt{q} = 0 \end{bmatrix} \mapsto \begin{bmatrix} q_1^2+q_2^2-q_3^2-q_4^2 & 2\,(q_2q_3-q_1q_4) & 2\,(q_2q_4+q_1q_3) & -x\,q_2+y\,q_1+z\,q_4-w\,q_3 \\ 2\,(q_2q_3+q_1q_4) & q_1^2-q_2^2+q_3^2-q_4^2 & 2\,(q_3q_4-q_1q_2) & -x\,q_3-y\,q_4+z\,q_1+w\,q_2 \\ 2\,(q_2q_4-q_1q_3) & 2\,(q_3q_4+q_1q_2) & q_1^2-q_2^2-q_3^2+q_4^2 & -x\,q_4+y\,q_3-z\,q_2+w\,q_1 \\ 0 & 0 & 0 & q_1^2+q_2^2+q_3^2+q_4^2 \end{bmatrix} \tag{8.6}$$

from a subset to $\mathbb{P}^7_\mathbb{C}$ to $SE_\mathbb{C}(3)$, acting on $\mathbb{P}^3_\mathbb{C}$. This map is the Study motion parameterization [20, 21].

The key property of the parameterization is that it is given by homogeneous polynomials of degree two in the coordinates of representatives in $\mathbb{P}^7_\mathbb{C}$. Hence, it is well defined since it maps all representatives of a 1D subspace of $\mathbb{P}^7_\mathbb{C}$ into the representatives of a single subspace of $\mathbb{P}^{16}_\mathbb{C}$ of 4×4 complex motion matrices.

The domain of the map is the set difference $V_1 \backslash V_2$ of two six-dimensional projective varieties in $\mathbb{P}^7_\mathbb{C}$. The variety V_1 is given by $V_1 = V(\langle \mathtt{x}^\top \mathtt{q} \rangle = V(\langle x_1\,q_1 + x_2\,q_2 + x_3\,q_3 + x_4\,q_4 \rangle)$. The variety V_2 is given by $V_2 = V(\langle \|\mathtt{q}\|^2 \rangle) = V(\langle q_1^2 + q_2^2 + q_3^2 + q_4^2 \rangle)$. The map is one-to-one and onto.

9 Axis of Motion

We will study motion and show that every motion in three dimensional space has an axis of motion. *Axis of motion* is a line of points that remain in the line after the motion. The existence of such an axis will allow us to decompose every motion into a sequence of a rotation around the axis followed by a translation along the axis as shown in Figure 9.1(a).

9.1 Algebraic characterization of the axis of motion.

Consider Equation 5.5 and denote the motion so defined as $m(\vec{x}_\beta) = \mathtt{R}\,\vec{x}_\beta + \vec{o}'_\beta$ w.r.t. a fixed coordinate system (O, β). Now let us study the sets of points that remain fixed by the motion, i.e. sets F such that for all $\vec{x}_\beta \in F$ motion m leaves the $m(\vec{x}_\beta)$ in the set, i.e. $m(\vec{x}_\beta) \in F$. Clearly, complete space and the empty set are fixed sets. How do look other, non-trivial, fixed sets?

A nonempty F contains at least one $\vec{x}_\beta$. Then, both $\vec{y}_\beta = m(\vec{x}_\beta)$ and $\vec{z}_\beta = m(\vec{y}_\beta)$ must be in F, see Figure 9.1(b). Let us investigate such fixed points $\vec{x}_\beta$ for which

$$\vec{z}_\beta - \vec{y}_\beta = \vec{y}_\beta - \vec{x}_\beta \qquad (9.1)$$

holds true. We do not yet know whether such equality has to necessary hold true for points of all fixed sets F but we see that it holds true for the identity motion *id* that leaves all points unchanged, i.e. $id(\vec{x}_\beta) = \vec{x}_\beta$. We will find later that it holds true for all motions and all their fixed sets. Consider the following sequence of equalities

$$\begin{aligned}
\vec{z}_\beta - \vec{y}_\beta &= \vec{y}_\beta - \vec{x}_\beta \\
\mathtt{R}\,(\mathtt{R}\,\vec{x}_\beta + \vec{o}'_\beta) + \vec{o}'_\beta - \mathtt{R}\vec{x}_\beta - \vec{o}'_\beta &= \mathtt{R}\,\vec{x}_\beta + \vec{o}'_\beta - \vec{x}_\beta \\
\mathtt{R}^2\vec{x}_\beta + \mathtt{R}\,\vec{o}'_\beta - \mathtt{R}\,\vec{x}_\beta &= \mathtt{R}\,\vec{x}_\beta + \vec{o}'_\beta - \vec{x}_\beta \\
\mathtt{R}^2\vec{x}_\beta - 2\,\mathtt{R}\,\vec{x}_\beta + \vec{x}_\beta &= -\mathtt{R}\,\vec{o}'_\beta + \vec{o}'_\beta \\
\left(\mathtt{R}^2 - 2\,\mathtt{R} + \mathtt{I}\right)\,\vec{x}_\beta &= -(\mathtt{R} - \mathtt{I})\,\vec{o}'_\beta \\
(\mathtt{R} - \mathtt{I})(\mathtt{R} - \mathtt{I})\,\vec{x}_\beta &= -(\mathtt{R} - \mathtt{I})\,\vec{o}'_\beta && (9.2) \\
(\mathtt{R} - \mathtt{I})\,\Big((\mathtt{R} - \mathtt{I})\,\vec{x}_\beta + \vec{o}'_\beta\Big) &= 0 && (9.3)
\end{aligned}$$

Equation 9.3 always has a solution. Let us see why.

Recall that rank $(\mathtt{R} - \mathtt{I})$ is either two or zero. If it is zero, then $\mathtt{R} - \mathtt{I} = 0$ and (i) Equation 9.3 holds for every $\vec{x}_\beta$.

Let rank $(\mathtt{R} - \mathtt{I})$ be two. Vector $\vec{o}'_\beta$ either is zero or it is not zero. If it is zero, then Equation 9.3 becomes $(\mathtt{R} - \mathtt{I})^2\,\vec{x}_\beta = 0$, which has (ii) a one-dimensional space of solutions because the null space and the range of $\mathtt{R} - \mathtt{I}$ intersect only in the zero vector.

Let $\vec{o}'_\beta$ be non-zero. Vector $\vec{o}'_\beta$ either is in the span of $\mathtt{R} - \mathtt{I}$ or it is not. If $\vec{o}'_\beta$ is in the span of $\mathtt{R} - \mathtt{I}$, then $(\mathtt{R} - \mathtt{I})\,\vec{x}_\beta + \vec{o}'_\beta = 0$ has (iii) one-dimensional affine space of solutions.

If $\vec{o}'_\beta$ is not in the span of $\mathtt{R} - \mathtt{I}$, then $(\mathtt{R} - \mathtt{I})\,\vec{x}_\beta + \vec{o}'_\beta$ for $\vec{x}_\beta \in \mathbb{R}^3$ generates a vector in all one-dimensional subspaces of $\mathbb{R}^3$ which are not in the span of $\mathtt{R} - \mathtt{I}$. Therefore, it generates a non-zero vector $\vec{z}_\beta = (\mathtt{R} - \mathtt{I})\,\vec{y}_\beta + \vec{o}'_\beta$ in the one-dimensional null space of $\mathtt{R} - \mathtt{I}$, because the null space and the span of $(\mathtt{R} - \mathtt{I})$ intersect only in the zero vector. Equation $(\mathtt{R} - \mathtt{I})\,\vec{z}_\beta = 0$ is satisfied by (iv) a one-dimensional affine set of vectors.

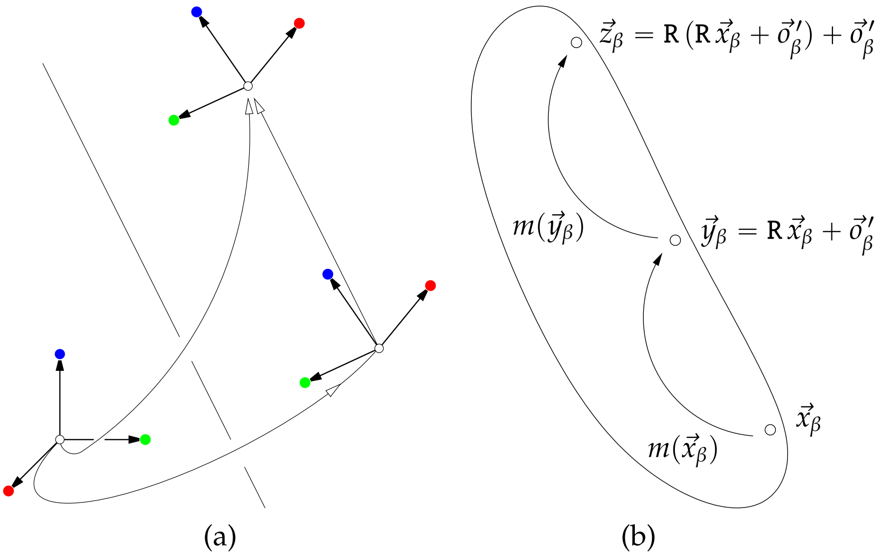

$\vec{z}_\beta = \mathtt{R}\,(\mathtt{R}\,\vec{x}_\beta + \vec{o}_\beta{}') + \vec{o}_\beta{}'$
$m(\vec{y}_\beta)$
$\vec{y}_\beta = \mathtt{R}\,\vec{x}_\beta + \vec{o}_\beta{}'$
$\vec{x}_\beta$
$m(\vec{x}_\beta)$
(a)
(b)

Figure 9.1: Axis of motion.

We can conclude that every motion has a fixed line of points for which Equation 9.1 holds. Therefore, every motion has a fixed line of points, every motion has an axis.

9.2 Geometrical characterization of the axis of motion

We now understand the algebraic description of motion. Can we also understand the situation geometrically? Figure 9.2 gives the answer. We shall concentrate on the general situation with $\mathtt{R} \neq \mathtt{I}$ and $\vec{o}_\beta{}' \neq 0$. The main idea of the figure is that the axis of motion a consists of points that are first

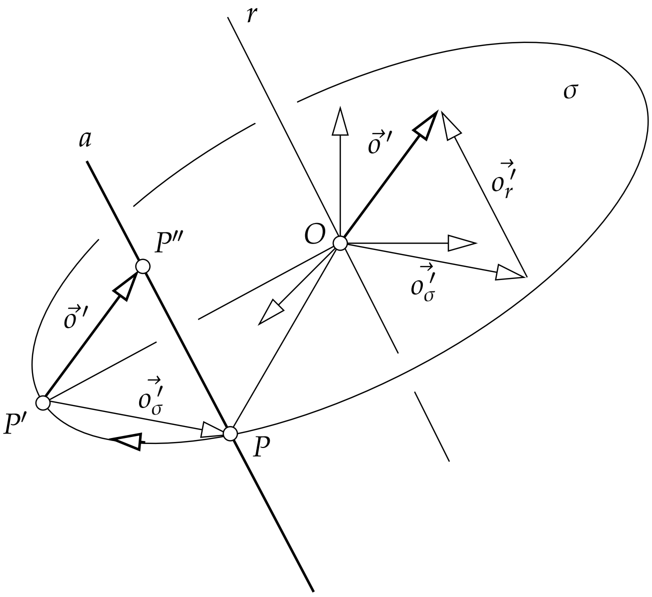


Figure 9.2: Axis a of motion is parallel to the axis of rotation r and intersects the perpendicular plane σ passing through the origin O at a point P, which is first rotated in σ away from a to P' and then returned back to P'' on a by translation $\vec{o}\,'$. Point P is determined by the component $\vec{o}_\sigma{}'$ of $\vec{o}\,'$, which is in the plane σ.

rotated away from a by the pure rotation $\mathtt{R}$ around r and then returned back to a by the pure translation $\vec{o}'_\beta$.

Figure 9.2 shows axis a of motion, which is parallel to the axis of rotation r and intersects the perpendicular plane σ passing through the origin O at a point P, which is first rotated in σ away from a to P' and then returned back to P'' on a by translation $\vec{o}'_\beta$. Point P is determined by the component $\vec{o}'_{\sigma\beta}$ of $\vec{o}'_\beta$, which is in the plane σ. Notice that every vector $\vec{o}'_\beta$ can be written as a sum of its component $\vec{o}'_{r\beta}$ parallel to r and component $\vec{o}'_{\sigma\beta}$ perpendicular to r.

§ 1 Motion axis is parallel to rotation axis. Let us verify algebraically that the rotation axis r is parallel to the motion axis a. Consider Equation 9.2, which we can rewrite as

$$(\mathtt{R}-\mathtt{I})^2\,\vec{x}_\beta \quad = \quad -(\mathtt{R}-\mathtt{I})\,\vec{o}'_\beta \tag{9.4}$$

Define axis r of motion as the set of points that are left fixed by the pure rotation $\mathtt{R}$, i.e.

$$(\mathtt{R}-\mathtt{I})\,\vec{x}_\beta \quad = \quad 0 \tag{9.5}$$

$$\mathtt{R}\,\vec{x}_\beta \quad = \quad \vec{x}_\beta \tag{9.6}$$

These are eigenvectors of $\mathtt{R}$ and the zero vector. Take any two solutions $\vec{x}_{1\beta}$, $\vec{x}_{2\beta}$ of Equation 9.4 and evaluate

$$(\mathtt{R}-\mathtt{I})^2(\vec{x}_{1\beta}-\vec{x}_{2\beta}) \quad = \quad -(\mathtt{R}-\mathtt{I})\,\vec{o}'_\beta + (\mathtt{R}-\mathtt{I})\,\vec{o}'_\beta = 0 \tag{9.7}$$

and thus a non-zero $\vec{x}_{1\beta}-\vec{x}_{2\beta}$ is an eigenvector of $\mathtt{R}$. We see that the direction vectors of a lie in the subspace of direction vectors of r.

9.3 Solving for the axis of motion

In Section 9.1, we have shown that every motion has a motion axis. Let us now give an explicit description of the axis, in the spirit of [20, p.212], by choosing a particularly convenient solution of Equation 9.2. Let us take a geometric approach. It follows from Section 9.2 that

$$\mathtt{R}\,\vec{x}_\sigma - \vec{x}_\sigma = -\vec{o}'_\sigma \tag{9.8}$$

Equation 6.75 and $\vec{o}'_\sigma = (\mathtt{I}-\vec{v}\vec{v}^\top)\,\vec{o}'$ give

$$(\mathtt{R}-\mathtt{I})\,\vec{x} = -(\mathtt{I}-\vec{v}\vec{v}^\top)\,\vec{o}' \tag{9.9}$$

Let us now express the projector $(\mathtt{I}-\vec{v}\vec{v}^\top)$ using matrix $\mathtt{R}$. Considering Equation 7.21, we can write

$$\mathtt{R} \quad = \quad \vec{v}\vec{v}^\top + \cos\theta\,(\mathtt{I}-\vec{v}\vec{v}^\top) + \sin\theta\;[\vec{v}]_\times \tag{9.10}$$

$$\mathtt{R}+\mathtt{R}^\top \quad = \quad 2\,\vec{v}\vec{v}^\top + 2\,\cos\theta\,(\mathtt{I}-\vec{v}\vec{v}^\top) \tag{9.11}$$

Now, we can use Equation 6.72 to rewrite $\cos\theta$ as $2\,\cos\theta = \operatorname{trace}\mathtt{R} - 1$ to get

$$\mathtt{R}+\mathtt{R}^\top \quad = \quad 2\,\vec{v}\vec{v}^\top + (\operatorname{trace}\mathtt{R}-1)\,(\mathtt{I}-\vec{v}\vec{v}^\top) \tag{9.12}$$

$$\mathtt{R}+\mathtt{R}^\top \quad = \quad (3-\operatorname{trace}\mathtt{R})\,\vec{v}\vec{v}^\top + (\operatorname{trace}\mathtt{R}-1)\,\mathtt{I} \tag{9.13}$$

and thus we get

$$\vec{v}\vec{v}^\top \quad = \quad \frac{\mathtt{R}+\mathtt{R}^\top + (1-\operatorname{trace}\mathtt{R})\,\mathtt{I}}{3-\operatorname{trace}\mathtt{R}} \tag{9.14}$$

$$\mathtt{I}-\vec{v}\vec{v}^\top \quad = \quad \frac{2\,\mathtt{I}-\mathtt{R}-\mathtt{R}^\top}{3-\operatorname{trace}\mathtt{R}} \tag{9.15}$$

Substituting Equation 9.15 into Equation 9.9 yields

$$(\mathtt{R}-\mathtt{I})\,\vec{x} \;=\; -(\mathtt{I}-\vec{v}\,\vec{v}^\top)\,\vec{o}\,' \tag{9.16}$$

$$(\mathtt{R}-\mathtt{I})\,\vec{x} \;=\; -\frac{2\,\mathtt{I}-\mathtt{R}-\mathtt{R}^\top}{3-\operatorname{trace}\mathtt{R}}\,\vec{o}\,' \tag{9.17}$$

Now, we will employ another very useful identity

$$2\,\mathtt{I}-\mathtt{R}-\mathtt{R}^\top = (\mathtt{R}-\mathtt{I})\,(\mathtt{R}^\top-\mathtt{I}) \tag{9.18}$$

to get $(\mathtt{R}-\mathtt{I})$ on the right hand side of Equation 9.17

$$(\mathtt{R}-\mathtt{I})\,\vec{x} \;=\; -\frac{(\mathtt{R}-\mathtt{I})\,(\mathtt{R}^\top-\mathtt{I})}{3-\operatorname{trace}\mathtt{R}}\,\vec{o}\,' \tag{9.19}$$

$$(\mathtt{R}-\mathtt{I})\,\vec{x} \;=\; (\mathtt{R}-\mathtt{I})\,\frac{(\mathtt{I}-\mathtt{R}^\top)}{3-\operatorname{trace}\mathtt{R}}\,\vec{o}\,' \tag{9.20}$$

and thus we see that

$$\vec{x}_0 = \frac{(\mathtt{I}-\mathtt{R}^\top)}{3-\operatorname{trace}\mathtt{R}}\,\vec{o}\,' \tag{9.21}$$

is a particular solution of Equation 9.9, i.e. it is a point in the motion axis.

Let us see that it is a particularly interesting point. We shall evaluate

$$\vec{v}^\top\vec{x}_0 = \frac{\vec{v}^\top(\mathtt{I}-\mathtt{R}^\top)}{3-\operatorname{trace}\mathtt{R}}\,\vec{o}\,' = 0\,\vec{o}\,' = 0 \tag{9.22}$$

to see that $\vec{x}_0$ is perpendicular to the rotation axis of $\mathtt{R}$ which means that point on the motion axis represented by $\vec{x}_0$ is the closest point to the origin O and also is the intersection of the motion axis with the plane perpendicular to the rotation axis and passing through the origin O.

A general point of the motion axis is thus obtained as

$$\vec{x} = \alpha\,\vec{v} + \frac{(\mathtt{I}-\mathtt{R}^\top)}{3-\operatorname{trace}\mathtt{R}}\,\vec{o}\,' \qquad \text{with} \qquad \mathtt{R}\,\vec{v} = 0 \qquad \text{and} \qquad \vec{v} \neq \vec{0} \qquad \text{for} \qquad \alpha \in \mathbb{R}. \tag{9.23}$$

Bibliography

[1] Paul R. Halmos. *Naive Set Theory*. Springer-Verlag, 1974.

[2] David Cox, John Little, and Donald O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, 3rd edition, 2015.

[3] Walter Rudin. *Principles of Mathematical Analysis*. McGraw-Hill, 1976.

[4] Paul R. Halmos. *Finite-Dimensional Vector Spaces*. Springer-Verlag, 2000.

[5] Carl Meyer. *Matrix Analysis and Applied Linear Algebra*. SIAM: Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2001.

[6] Petr Olšák. Úvod do algebry, zejména lineární. FEL ČVUT, Praha, 2007.

[7] Pavel Pták. Introduction to linear algebra. Vydavatelství ČVUT, Praha, 2007.

[8] Gilbert Strang. *Introduction to Linear Algebra*. Wellesley Cambridge, 3rd edition, 2003.

[9] Seymour Lipschutz. *3,000 Solved Problems in Linear Algebra*. McGraw-Hill, 1st edition, 1989.

[10] Jim Hefferon. *Linear Algebra*. Virginia Commonwealth University Mathematics, 2009.

[11] Michael Artin. *Algebra*. Prentice Hall, Upper Saddle River, NJ 07458, USA, 1991.

[12] Yoshiaki Ueno and Kazuhisa Maehara. An elementary proof of the generalized Laplace expansion formula. *Tokyo Polytechnic University Bulletin*, 25(1):61–63, 2003. http://www.t-kougei.ac.jp/research/bulletin_e/.

[13] Cyrus Colton MacDuffee. *The Theory of Matrices*. Dover Publications Inc., 2004. http://books.google.cz/books?id=8hQG7ByP53oC.

[14] David Cox, John Little, and Donald O'Shea. *Using Algebraic Geometry*. Springer, 2nd edition, 2005.

[15] Lorenzo Robbiano. Term orderings on the polynominal ring. In *EUROCAL '85, European Conference on Computer Algebra, Linz, Austria, April 1-3, 1985, Proceedings Volume 2: Research Contributions*, pages 513–517, 1985.

[16] Cybernet Systems Co. Ltd. Maple. http://www.maplesoft.com/products/maple/.

[17] Bernard Mourrain. Computing the isolated roots by matrix methods. *J. Symb. Comput.*, 26(6):715–738, 1998.

[18] Saunders MacLane and Garret Birkhoff. *Algebra*. Chelsea Pub. Co., 3rd edition, 1988.

[19] John Stuelpnagel. On the parametrization of the three-dimensional rotation group. *SIAM Review*, 6(4):422–430, October 1964.

[20] Jorge Angeles and Shaoping Bai. Kinematic synthesis. MECH541, McGill University, 2016. http://www.cim.mcgill.ca/ rmsl/Index/Documents/MECH541/LN-160305.pdf.

[21] J. M. Selig. On the geometry of the homogeneous representation for the group of proper rigid-body displacements. *The Romanian Journal of Technical Sciences. Applied Mechanics: New trends in advanced robotics*, 58(1-2), 2013.

Index

END