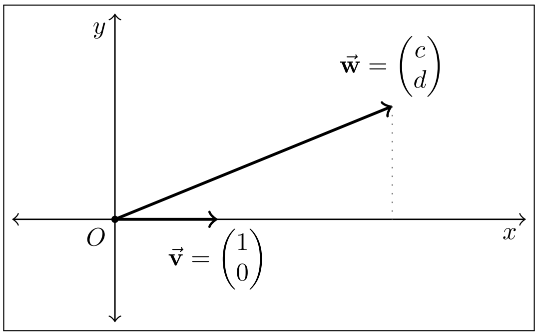
# 1 Inner products

We describe points in 2D-space by their $x$- and $y$-coordinate. For example: $\begin{pmatrix} a \\ b \end{pmatrix}$ is the point with $x$-coordinate $a$ and $y$-coordinate $b$. If we have two points $\vec{\mathbf{v}} = \begin{pmatrix} a \\ b \end{pmatrix}$ and $\vec{\mathbf{w}} = \begin{pmatrix} c \\ d \end{pmatrix}$, the "inner product" of $\vec{\mathbf{v}}$ and $\vec{\mathbf{w}}$ is:

$$\vec{\mathbf{v}} \cdot \vec{\mathbf{w}} = a \times c \; + \; b \times d.$$

In the exercises below, we will see why this definition is nice and meaningful.

**(a)** Simplify the inner product in the special case when the first vector is $\vec{\mathbf{v}} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Then: $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} c \\ d \end{pmatrix} = \dots$



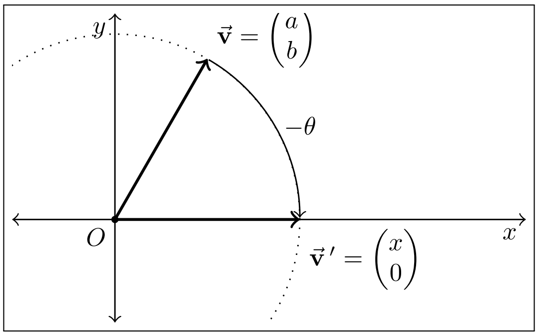

**(b)** How does this relate to $\vec{\mathbf{w}}$? If $\vec{\mathbf{v}} \cdot \vec{\mathbf{w}} = 0$, what is the angle between $\vec{\mathbf{v}}$ and $\vec{\mathbf{w}}$?

**(c)** Now look at the inner product with $\vec{\mathbf{v}} = \begin{pmatrix} a \\ 0 \end{pmatrix}$. Compute: $\dfrac{\vec{\mathbf{v}} \cdot \vec{\mathbf{w}}}{\vec{\mathbf{v}} \cdot \vec{\mathbf{v}}} \times \vec{\mathbf{v}} = \begin{pmatrix} \quad \cdots \quad \\ 0 \end{pmatrix}$.[1]

**(d)** We can rotate a point $\vec{\mathbf{v}} = \begin{pmatrix} a \\ b \end{pmatrix}$ counter-clockwise by an angle of $\theta$ as follows: $\vec{\mathbf{v}}\,' = \begin{pmatrix} a\cos(\theta) - b\sin(\theta) \\ a\sin(\theta) + b\cos(\theta) \end{pmatrix}$.

**(1)** Verify the equation for $\theta = 90°$. Then: $\vec{\mathbf{v}}\,' = \begin{pmatrix} \quad \cdots \quad \\ \cdots \end{pmatrix}$.

**(2)** Write $\vec{\mathbf{w}}\,'$ for the rotation of $\vec{\mathbf{w}}$ by an angle of $\theta$. Show: $\vec{\mathbf{v}} \cdot \vec{\mathbf{w}} = \vec{\mathbf{v}}\,' \cdot \vec{\mathbf{w}}\,'$.[2]




**(e)** Describe the angle $\theta$ (using $a, b$ and $\sin / \cos / \tan$) that rotates $\vec{\mathbf{v}} = \begin{pmatrix} a \\ b \end{pmatrix}$ to $\vec{\mathbf{v}}\,' = \begin{pmatrix} x \\ 0 \end{pmatrix}$ for some $x > 0$. What is $x$?

**(f)** The length of a vector $\vec{\mathbf{v}} = \begin{pmatrix} a \\ b \end{pmatrix}$ is given by $\|\vec{\mathbf{v}}\| = \sqrt{a^2 + b^2}$. Prove: $\|\vec{\mathbf{v}}\|^2 = \vec{\mathbf{v}} \cdot \vec{\mathbf{v}}$.

**(g)** Suppose the angle between $\vec{\mathbf{v}}$ and $\vec{\mathbf{w}}$ is $\theta$. Prove (using the previous exercises):[3]

$$\vec{\mathbf{v}} \cdot \vec{\mathbf{w}} = \cos(\theta) \times \|\vec{\mathbf{v}}\| \times \|\vec{\mathbf{w}}\|.$$

[1] Note: this fraction is a number. If $z$ is some number, then $z \times \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} za \\ zb \end{pmatrix}$.

[2] Hint: recall $\cos^2(\theta) + \sin^2(\theta) = 1$.

[3] Hint: use (5) to rotate $\vec{\mathbf{w}}$ with the same angle that rotates $\vec{\mathbf{v}}$ onto the $x$-axis.

## 2 Parallelograms

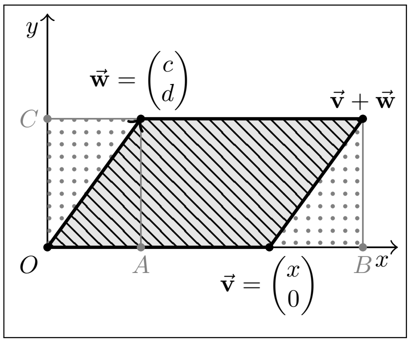



Figure 1: One tile

Recall that a basis for a lattice gives a tiling of space.

For **(a)**, **(b)** and **(c)**, assume $\vec{\mathbf{v}}$ is on the $x$-axis. First, we relate the area of the parallelogram to the basis.

**(a)** Show: the parallelogram $O, \vec{\mathbf{v}}, \vec{\mathbf{v}} + \vec{\mathbf{w}}, \vec{\mathbf{w}}$, and the rectangle $O, A, \vec{\mathbf{w}}, C$ have equal area.[4]

**(b)** Show: replacing $\vec{\mathbf{w}}$ by $\vec{\mathbf{w}} + z\vec{\mathbf{v}}$ does not change the area for any $z$ (the area is independent of $c$).

**(c)** What is the area in terms of $x$ and $d$?

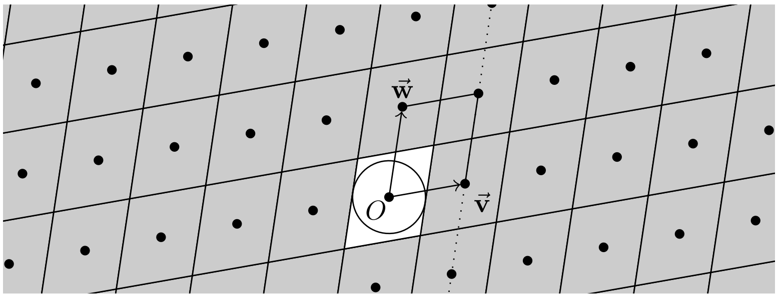



Figure 2: Tiling of 2D-space by the lattice basis $[\vec{\mathbf{v}}, \vec{\mathbf{w}}]$

Now consider the general case of $\vec{\mathbf{v}} = \begin{pmatrix} a \\ b \end{pmatrix}$ and $\vec{\mathbf{w}} = \begin{pmatrix} c \\ d \end{pmatrix}$.

**(d)** Using **(b)**, slide $\vec{\mathbf{v}}$ to a point on the $x$-axis. Show: the parallelogram has area $ad - bc$.[5]

**(e)** How does the area change when you:

- **(1)** swap $\vec{\mathbf{v}}$ and $\vec{\mathbf{w}}$?
- **(2)** replace $\vec{\mathbf{w}}$ by $\vec{\mathbf{w}} + \vec{\mathbf{v}}$?
- **(3)** multiply $\vec{\mathbf{v}}$ and $\vec{\mathbf{w}}$ by 2?

**(f)** Conclude from (1) and (2) that the area stays the same during lattice reduction.

**(g)** Show: the circle in Figure 3 has radius $r = \frac{1}{2}\|\vec{\mathbf{v}}\|$.
Show: the circle in Figure 2 has radius $r' = \frac{1}{2}\|\vec{\mathbf{v}}\| \times \sin(\theta) \leq r$, where $\theta$ is the angle between $\vec{\mathbf{v}}$ and $\vec{\mathbf{w}}$.

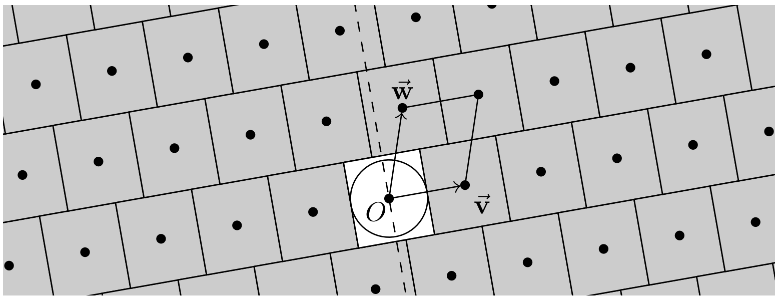



Figure 3: A different tiling of 2D-space, using a rectangular tile.

**Encryption with lattices.** With the secret key (the good basis $[\vec{\mathbf{v}}, \vec{\mathbf{w}}]$) only you can decrypt ciphertexts sent by others! Namely, a ciphertext is $\vec{\mathbf{t}} = \vec{\mathbf{m}} + \vec{\mathbf{e}}$, where $\vec{\mathbf{m}} = a\vec{\mathbf{v}} + b\vec{\mathbf{w}}$ ($a, b$ integer) corresponds to a message, and $\vec{\mathbf{e}}$ is a short vector. With the secret key, you can find the tile containing $\vec{\mathbf{t}}$ and recover $\vec{\mathbf{m}}$, *if* $\|\vec{\mathbf{e}}\|$ is small enough.

**(h)** Show: decrypting with the tile in Fig. 2 works if $\|\vec{\mathbf{e}}\| \leq r'$, and with the tile in Fig. 3, it works if $\|\vec{\mathbf{e}}\| \leq r$. Which of the two tilings works best at decryption?

[4] Hint: go from one to the other by adding a triangle and removing a triangle (of same area).

[5] Hint: first determine for which value of $z$, the point $\vec{\mathbf{v}} - z\vec{\mathbf{w}}$ is on the $x$-axis. Then determine the $x$-coordinate of this point.

# 3 Gram–Schmidt and projections

Instead of 2D-space ($\mathbb{R}^2$), in this exercise we will look at $n$-dimensional space ($\mathbb{R}^n$). Now, vectors are described by $n$ coordinates:

$$\vec{\mathbf{v}} = \begin{pmatrix} v_1 \\ v_2 \\ \cdots \\ v_n \end{pmatrix}$$

We still have the inner product, which is: $\vec{\mathbf{v}} \cdot \vec{\mathbf{w}} = v_1 \times w_1 + v_2 \times w_2 + \dots v_n \times w_n$.

**(a)** Prove the following, where $\vec{\mathbf{u}}, \vec{\mathbf{v}}, \vec{\mathbf{w}}$ are vectors and $z$ is any number:

$$\vec{\mathbf{u}} \cdot (\vec{\mathbf{v}} + \vec{\mathbf{w}}) = (\vec{\mathbf{u}} \cdot \vec{\mathbf{v}}) + (\vec{\mathbf{u}} \cdot \vec{\mathbf{w}}), \qquad \vec{\mathbf{v}} \cdot (z \times \vec{\mathbf{w}}) = z \times (\vec{\mathbf{v}} \cdot \vec{\mathbf{w}}).$$

**(b)** There is no simple "division" operation with vectors, because you cannot express $\vec{\mathbf{w}}$ in terms of $\vec{\mathbf{v}}$ whenever it is not pointing in the same direction. Still, using **(c)** from sheet 1, we can make a vector $\vec{\mathbf{w}}$ *orthogonal* to $\vec{\mathbf{v}}$ by computing the following:

$$\pi_{\vec{\mathbf{v}}}(\vec{\mathbf{w}}) = \vec{\mathbf{w}} - \frac{\vec{\mathbf{v}} \cdot \vec{\mathbf{w}}}{\vec{\mathbf{v}} \cdot \vec{\mathbf{v}}} \times \vec{\mathbf{v}}.$$

Show: $\pi_{\vec{\mathbf{v}}}(\vec{\mathbf{w}})$ satisfies $\vec{\mathbf{v}} \cdot \pi_{\vec{\mathbf{v}}}(\vec{\mathbf{w}}) = 0$ (use **(a)**).

**(c)** Consider the following process, called "Gram–Schmidt orthogonalization":

$$\vec{\mathbf{b}}_1^* = \vec{\mathbf{b}}_1, \qquad \vec{\mathbf{b}}_2^* = \pi_{\vec{\mathbf{b}}_1^*}(\vec{\mathbf{b}}_2), \qquad \vec{\mathbf{b}}_3^* = \pi_{\vec{\mathbf{b}}_2^*}(\pi_{\vec{\mathbf{b}}_1^*}(\vec{\mathbf{b}}_3)), \qquad \dots.$$

Show: $\vec{\mathbf{b}}_3^*$ is orthogonal to both $\vec{\mathbf{b}}_1^*$ and $\vec{\mathbf{b}}_2^*$. *(in general show: $\vec{\mathbf{b}}_i^* \cdot \vec{\mathbf{b}}_j^* = 0$ for all $1 \le i < j \le n$)*

**(d)** For finding short basis vectors, we want to reduce $\vec{\mathbf{b}}_3$ by removing (integer) multiples of $\vec{\mathbf{b}}_1$ and $\vec{\mathbf{b}}_2$ that make $\vec{\mathbf{b}}_3$ as short as possible. Considering the tiling in Figure 3, we want that $\vec{\mathbf{b}}_3$ (when ignoring the third dimension) is in the tile containing the origin $O$, by removing some multiples of $\vec{\mathbf{b}}_1 = \vec{\mathbf{v}}$ and $\vec{\mathbf{b}}_2 = \vec{\mathbf{w}}$. This tile containing $O$ is given by the points $\vec{\mathbf{x}}$ for which $-\frac{1}{2} \le \frac{\vec{\mathbf{b}}_1^* \cdot \vec{\mathbf{x}}}{\vec{\mathbf{b}}_1^* \cdot \vec{\mathbf{b}}_1^*} \le \frac{1}{2}$ and similarly for $\vec{\mathbf{b}}_2^*$.

Write $\lceil x \rfloor$ for rounding a number to its nearest integer. This means $-\frac{1}{2} \le x - \lceil x \rfloor \le \frac{1}{2}$. Given $\vec{\mathbf{b}}_3$, show:

$$\vec{\mathbf{x}} = \vec{\mathbf{b}}_3 - \left\lceil \frac{\vec{\mathbf{b}}_2^* \cdot \vec{\mathbf{b}}_3}{\vec{\mathbf{b}}_2^* \cdot \vec{\mathbf{b}}_2^*} \right\rfloor \vec{\mathbf{b}}_2,$$

satisfies $-\frac{1}{2} \le \frac{\vec{\mathbf{b}}_2^* \cdot \vec{\mathbf{x}}}{\vec{\mathbf{b}}_2^* \cdot \vec{\mathbf{b}}_2^*} \le \frac{1}{2}$.

Given $\vec{\mathbf{x}}$ as above, show:

$$\vec{\mathbf{y}} = \vec{\mathbf{x}} - \left\lceil \frac{\vec{\mathbf{b}}_1^* \cdot \vec{\mathbf{x}}}{\vec{\mathbf{b}}_1^* \cdot \vec{\mathbf{b}}_1^*} \right\rfloor \vec{\mathbf{b}}_1,$$

is in the tile containing $O$, that is it satisfies: $-\dfrac{1}{2} \le \dfrac{\vec{\mathbf{b}}_1^* \cdot \vec{\mathbf{y}}}{\vec{\mathbf{b}}_1^* \cdot \vec{\mathbf{b}}_1^*} \le \dfrac{1}{2}$, and $-\dfrac{1}{2} \le \dfrac{\vec{\mathbf{b}}_2^* \cdot \vec{\mathbf{y}}}{\vec{\mathbf{b}}_2^* \cdot \vec{\mathbf{b}}_2^*} \le \dfrac{1}{2}$.

The process is called "size-reduction" and forms the basis of lattice reduction!

*In general, to size-reduce $\vec{\mathbf{b}}_n$, we update the value of $\vec{\mathbf{b}}_n$ $n-1$ times by computing the following first for $i = n-1$, then $i = n-2, \dots$ down to $i = 1$:*

$$\vec{\mathbf{b}}_n := \vec{\mathbf{b}}_n - \left\lceil \frac{\vec{\mathbf{b}}_i^* \cdot \vec{\mathbf{b}}_n}{\vec{\mathbf{b}}_i^* \cdot \vec{\mathbf{b}}_i^*} \right\rfloor \vec{\mathbf{b}}_i,$$

*where $x := y$ means "put the value of $y$ in the slot of $x$.*

# 4 Lagrange reduction (dimension 2)

Lattice reduction in dimension 2 is easy. Namely, we can perform the following algorithm:

1. Perform size-reduction (Ex 3(d)) on $\vec{\mathbf{b}}_2$:
$$\vec{\mathbf{b}}_2' = \vec{\mathbf{b}}_2 - \left\lceil \frac{\vec{\mathbf{b}}_1 \cdot \vec{\mathbf{b}}_2}{\vec{\mathbf{b}}_1 \cdot \vec{\mathbf{b}}_1} \right\rfloor \vec{\mathbf{b}}_1, \tag{1}$$
(and replace $\vec{\mathbf{b}}_2$ by $\vec{\mathbf{b}}_2'$).
2. If $\|\vec{\mathbf{b}}_2\| \geq \|\vec{\mathbf{b}}_1\|$, the basis $[\vec{\mathbf{b}}_1, \vec{\mathbf{b}}_2]$ is reduced, so stop.
3. Otherwise, swap $\vec{\mathbf{b}}_1$ and $\vec{\mathbf{b}}_2$, then go back to step 1.

In Figure 4, $\vec{\mathbf{b}}_2$ becomes shorter than $\vec{\mathbf{b}}_1$ after size-reduction. Then, by size-reducing $\vec{\mathbf{b}}_1$ with respect to $\vec{\mathbf{b}}_2$ one may possibly shorten $\vec{\mathbf{b}}_1$ further.

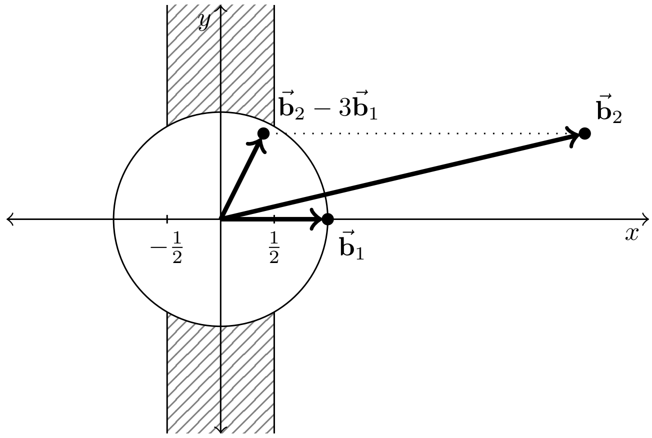



Figure 4: Example of one iteration of Lagrange reduction.

**(a)** Show that in each iteration (size reduction & swap) the length of $\vec{\mathbf{b}}_1$ stays the same, or decreases.

**(b)** Conclude that the number of iterations is finite.[6]

**(c)** When the process terminates, show that $\vec{\mathbf{b}}_2$ must be in the striped region.

**(d)** Show: the area of the parallelogram spanned by $\vec{\mathbf{b}}_1, \vec{\mathbf{b}}_2$ is the same as the area of the rectangle spanned by $\vec{\mathbf{b}}_1$ and $\vec{\mathbf{b}}_2^*$. Show: this area is
$$\|\vec{\mathbf{b}}_1\| \times \|\vec{\mathbf{b}}_2^*\|.$$

**(e)** Given a lattice in dimension 2, show that we can draw circles around each lattice point, with radius $\frac{1}{2}\|\vec{\mathbf{b}}_1\|$ if $\vec{\mathbf{b}}_1$ is one of the shortest vectors. Any lattice gives a so-called "sphere packing".

**(f)** What is the densest (largest radius) sphere packing for a lattice in dimension 2, when you require that $\|\vec{\mathbf{b}}_1\| \times \|\vec{\mathbf{b}}_2^*\| = 1$?

Hint: (1) look at the ratio $\dfrac{\left(\frac{1}{2}\|\vec{\mathbf{b}}_1\|\right)^2}{\|\vec{\mathbf{b}}_1\| \times \|\vec{\mathbf{b}}_2^*\|} = \dfrac{\|\vec{\mathbf{b}}_1\|}{4 \times \|\vec{\mathbf{b}}_2^*\|}$, and assume $\vec{\mathbf{b}}_1$ lies on the $x$-axis.
(2) What is the possible value of $\vec{\mathbf{b}}_2$ lying in the striped region that maximizes this ratio?
(3) What lattice is this?

[6]Hint: show if $\|\vec{\mathbf{b}}_1\|$ stays the same in one iteration that the algorithm stops and the shortest vectors are found.