MATH 1800: Quantum Information Theory with Applications to Cryptography

Bonus 1

Definition 1. A **unit sphere of dimension n** is the subset of vectors with norm 1 in $n+1$-dimensional real vector space:

$$S^n := \{v \in \mathbb{R}^{n+1} \mid |v| = \sqrt{x_1^2 + x_2^2 + \ldots + x_{n+1}^2} = 1\}.$$

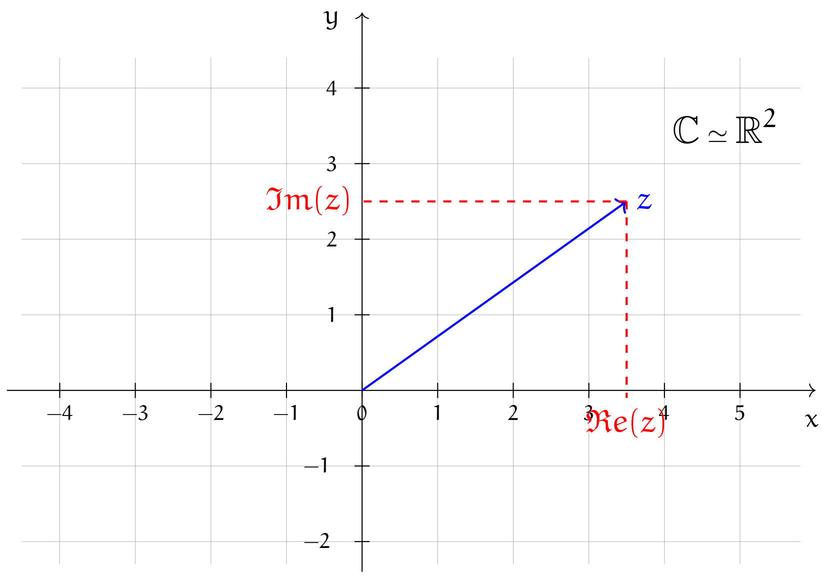
Notice that as $|v| > 0$, we have $|v| = 1 \Leftrightarrow |v|^2 = x_1^2 + x_2^2 + \ldots + x_{n+1}^2 = 1$.

Example 2. Let's consider a few low-dimensional cases.

$n = 1$: $S^1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$.

$n = 2$: $S^2 = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$.

Let $z \in \mathbb{C}$ be a complex number with $\mathfrak{Re}(z), \mathfrak{Im}(z)$ the real and imaginary parts of z:



Recall that $\mathbb{C}^2 \simeq \mathbb{R}^4$ via $(\alpha, \beta) \mapsto (\mathfrak{Re}(\alpha), \mathfrak{Im}(\alpha), \mathfrak{Re}(\beta), \mathfrak{Im}(\beta))$. Notice that if we write $\alpha \in \mathbb{C}$ in the standard form $\alpha = \alpha_1 + i\alpha_2$, then $\mathfrak{Re}(\alpha) = \alpha_1$ and $\mathfrak{Im}(\alpha) = \alpha_2$. Therefore, under the identification of vector spaces above, the pair (α, β) corresponds to the quadruple $(\alpha_1, \alpha_2, \beta_1, \beta_2)$. The unit sphere $S^3 \subset \mathbb{C}^2 \simeq \mathbb{R}^4$ is the subset $\{(\alpha_1, \alpha_2, \beta_1, \beta_2) \in \mathbb{R}^4 \mid \alpha_1^2 + \alpha_2^2 + \beta_1^2 + \beta_2^2 = 1\}$. Henceforth we assume that $(\alpha, \beta) \in S^3$.

Problem (3 pts) Let $\lambda = \cos(\varphi) + i\sin(\varphi) \in \mathbb{C}$ be a number of norm 1.[1]

(a) Find the 4 coordinates of the vector $(\lambda\alpha, \lambda\beta)$ as a vector in $\mathbb{R}^4$ (this will be functions of φ).

[1] Notice that such numbers form the unit circle $S^1 = \{\lambda \in \mathbb{C} \simeq \mathbb{R}^2 \mid |\lambda|^2 = \lambda\bar{\lambda} = \lambda_1^2 + \lambda_2^2 = 1\}$.

(b) Find the values of φ for which the first coordinate is zero (notice that if $\alpha = (\alpha_1, \alpha_2) = (0,0)$, then $(\lambda\alpha, \lambda\beta) = (0, \lambda\beta)$ for any $\lambda \in S^1$).

(c) Show that the quotient S^3/S^1 is *homeomorphic* to S^2.[2]

[2]**Hint:** in (b) for each $(\alpha, \beta) \in S^3, \alpha \neq 0$ you have found two representatives $\lambda_1, \lambda_2 \in S^1$, for which $(\lambda_1\alpha_1, \lambda_1\beta) = (0, a_1, a_2, a_3)$ and $(\lambda_2\alpha_1, \lambda_2\beta) = (0, -a_1, -a_2, -a_3)$. Show that $a_1^2 + a_2^2 + a_3^2 = 1$. It is straightforward to see that for any point $p = (x_1, x_2, x_3) \in S^2$ there is a point $(\alpha_1, \alpha_2, \beta_1, \beta_2) \in S^3$ with $(a_1, a_2, a_3) = (x_1, x_2, x_3)$. It remains to notice that a 2-dimensional sphere with antipodal points (a_1, a_2, a_3) and $(-a_1, -a_2, -a_3)$ identified (for $a_1 \neq 0$) and the equator $(0, a_2, a_3)$ contracted to a point (as $(0, \beta) \sim (0, \lambda\beta)$ for any $\lambda \in S^1$) is homeomorphic to a 2-dimensional sphere to conclude the statement in (c).