Appendices

7.14 Properties of functions

Consider two sets, X and Y. A *function* (or *map*) f from X to Y is defined such that, for each element x belonging to X (denoted as $x \in X$), there exists a unique element y in Y associated with x. We represent this element as $y = f(x)$ and call it the image of x under the function f. We write it as:

$$f: \ X \to Y \quad , \quad x \mapsto y = f(x) \, . \tag{7.129}$$

The set X is called the *domain* of f, and Y is its *image*. The set of elements in Y, which are images under f of elements in X, is called the image of X under f and is denoted as $f(X)$. In general, $f(X)$ is a subset of Y (we write $f(X) \subset Y$) and is not necessarily identical to Y.

The function f is *injective* if:

$$f(x) = f(x') \ \Rightarrow \ x = x' \, . \tag{7.130}$$

For an injective function, two elements of X cannot have the same image in Y. A function is *surjective* if $f(X) = Y$. For a surjective function, every element of Y is the image of at least one element of X. A function that is both injective and surjective is called *bijective*.

Let f be a function from X to Y and g be a function from Y to Z. The *composition* or *product* of these two functions $h : X \to Z$ is defined as:

$$h(x) = g\left(f(x)\right) \, . \tag{7.131}$$

The function h acts from X to Z and is denoted as:

$$h = g * f \tag{7.132}$$

or simply gf when there is no possibility of confusion with other operations. It should be noted that $f * g$ is not necessarily well-defined, and when it exists, it is not necessarily equal to $g * f$. For example, consider real-valued functions $f(x) = x^2$ and $g(y) = \mathrm{e}^y$. We have:

$$(g * f)(x) = g\left(x^2\right) = \mathrm{e}^{x^2} \tag{7.133}$$

and

$$(f * g)(x) = f\left(\mathrm{e}^x\right) = \mathrm{e}^{2x} \, . \tag{7.134}$$

The composition of functions is associative, meaning that if u, v, and w are functions from X to Y, Y to Z, and Z to W, respectively, then:

$$(w * (v * u))(x) = ((w * v) * u)(x) \, . \tag{7.135}$$

For each $x \in X$, both sides of this equation correspond to the element:

$$w(v(u(x))) \tag{7.136}$$

in W. Therefore, we can write:

$$(w * (v * u))(x) = ((w * v) * u)(x) = w * v * u \, . \tag{7.137}$$

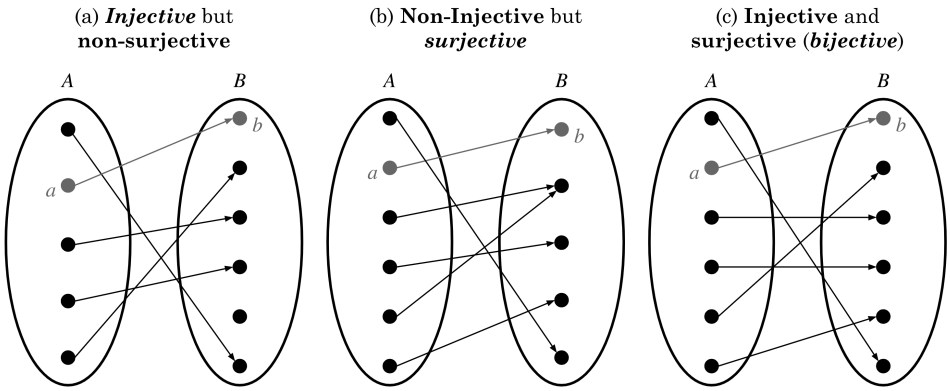

Figure 7.17: Diagram of injective, surjective and bijective functions: (Wiki page on functions).)

If $f : X \to Y$ is a bijective application, then for each element y in Y, there is a unique element x in X such that $f(x) = y$, and, naturally, each element x has an image in Y. Therefore, we can define a bijective application $Y \to X$, $y \mapsto x$ such that $y = f(x)$. This application is called the *inverse* of f and is denoted by f^{-1}.

Often, we consider applications from a set X to itself. An example is given by real (complex) functions of a real (complex) variable. We define the identity application as:

$$e : \ X \to X \quad , \quad x \mapsto e(x) = x \, . \tag{7.138}$$

This application is clearly bijective. If $f : X \to Y$ is a bijective application, f^{-1} exists, and we have:

$$(f^{-1} * f)(x) = x \tag{7.139}$$

for each x. Therefore, we write:

$$f^{-1} * f = e_X \tag{7.140}$$

where we denote the identity application of X by e_X. Note that we also have:

$$f * f^{-1} = e_Y \tag{7.141}$$

Theorem. Let X and Y be two sets containing the same finite number n of elements[29]. The following three statements are equivalent:

(i) $f : X \to Y$ is surjective,

(ii) $f : X \to Y$ is injective,

(iii) $f : X \to Y$ is bijective.

Proof:

(i) $\Rightarrow f(X) = Y$. Thus, $f(X)$ is composed of n elements, which implies (ii).

(ii) $\Rightarrow f(X)$ is composed of n elements. It follows that $f(X) = Y$, which can be reduced to property (i).

Since (i) and (ii) are each a consequence of the other, (iii) is also true, and the theorem is thus proved.

[29]Note that this theorem is not valid for two sets with different numbers of elements.

7.14.1 Proof of Lagrange Theorem, Right and Left cosets

Let G be a group and H one of its proper subgroups. We can define an equivalence relation —different from the last one— between the elements of G as follows: if $x, y \in G$ and $x^{-1}y \in H$ then x and y are equivalent and we write $x \sim y$.

This is indeed an equivalence relation:

- $a^{-1}a = e \; \forall a \in G$, and $e \in H$, so that $a \sim a$.
- if $a \sim b$ then $a^{-1}b \in H$. The inverse of $a^{-1}b$ is $b^{-1}a$ and since H is a group, $b^{-1}a \in H$, so that $b \sim a$.
- if $a \sim b$ and $b \sim c$, then $a^{-1}b$ and $b^{-1}c$ are both in H, thus so is the their product $a^{-1}bb^{-1}c = a^{-1}c$.

This equivalence relation therefore makes it possible to divide the elements of G into disjoint classes. If $x^{-1}y \in H$, then y is equal to an element of H multiplied on the left by x. We indicate the set thus constructed by the symbol

$$C_x = xH \tag{7.142}$$

which the call the *left co-set associated to* x.

The map $H \to xH$ is one-to-one (bijective). Indeed, each element $z \in xH$ is the image of $x^{-1}z \in H$ so that the map is surjective. But the map is also injective since for $y, y' \in H$, we have $xy = xy' \Rightarrow y = y'$.

We could also define a second equivalence relation $x \sim y$ if $yx^{-1} \in H$ and which this case, we can define the concept of right co-set Hx in the same way as before.

These concepts are very useful, and allows in particular to prove Lagrange Theorem:

Demo. Consider the co-sets on the left of H. They are all disjoint or identical (since they are equivalence classes). If there are n distinct left co-sets, their union is G. So, if we denote by g and h the orders of G and H respectively, then $g = nh$ and the theorem is proved. □

Let us give an example for the following order 4 group

$$G = \begin{array}{c|cccc} * & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array} \tag{7.143}$$

that has the subgroup $H = \{e, a\}$:

$$H = \begin{array}{c|cc} * & e & a \\ \hline e & e & a \\ a & a & e \end{array} \tag{7.144}$$

We can now construct the left co-sets:

$$C_e = eH = \{e, a\} \tag{7.145}$$
$$C_a = aH = \{a, e\} = C_e \tag{7.146}$$
$$C_b = bH = \{b, c\} \tag{7.147}$$
$$C_c = cH = \{c, b\} = C_b \tag{7.148}$$

And we see indeed that we have *two* left co-set of order 2.

7.15 Composition of Conjugacy classes theorem statement and proof

Theorem 7.15.1 ("Composition" of conjugacy classes)**.** *Let G be a group, and C_x and C_y two of its conjugacy classes. Then we have*

$$C_\nu * C_\mu = \sum_\lambda n_{\mu\nu\lambda} C_\lambda \tag{7.149}$$

with $n_{\mu\nu\lambda}$ integer. Here the multiplication $C_\nu * C_\mu$ is defined as the entire set $[xy]$ for all $x \in C_\nu$ and $y \in C_\mu$. Additionally, $n_{\nu\mu\lambda} = n_{\mu\nu\lambda}$ and $n_{1\nu\lambda} = n_{\nu 1\lambda} = \delta_{\nu,\lambda}$.

To prove this, let us first prove a variant of the reordering theorem:

Theorem 7.15.2 (Reordering theorem within conjugacy classes)**.** *Let G be a group, m one of its elements, and C one of the conjugate classes. Then the application $C \to m^{-1}Cm$ is bijective into itself: The ensemble $m^{-1}Cm$ is thus a re-ordering of C.*

Demo. First notice that this is a map into itself since for any $y \in C$, $m^{-1}ym \in C$ (conjugacy class property). Second, the map is surjective. Indeed, for any $y \in C$, it exists $x = mym^{-1} \in G$ such that $y = m^{-1}xm$. By definition, x is thus also in C and therefore for all $y \in C$ there is an antecedent in C. Third, the map $x \to mx$ is injective (it maps distinct elements to distinct elements). For any x, x', we have $m^{-1}xm = m^{-1}x'm$ implies that $mm^{-1}xmm^{-1} = mm^{-1}x'mm^{-1}$ so that $x = x'$. □

We shall soon prove that $n_{\nu\mu\lambda}$ is indeed an integer. But first, let us note indeed that $n_{\nu\mu\lambda} = n_{\mu\nu\lambda}$, because the two sets $C_\nu * C_\mu$ and $C_\mu * C_\nu$ are identical. Indeed

$$C_\nu * C_\mu = [uv] = \left[uv(u^{-1}u)\right] = \left[u(vu^{-1}u)\right] = \left[uvu^{-1}u\right] = \left[(uvu^{-1})u\right] = C_\mu * C_\nu$$

since u represents all the element of C_ν, and since, from the previous theorem, (uvu^{-1}) represent a re-ordering of the all the element of C_μ as v changes. Additionally, we also see that, denoting the class that contains e are C_1, that $C_1 * C_\nu = C_\nu$ so that $n_{1\nu\lambda} = n_{\nu 1\lambda} = \delta_{\nu,\lambda}$.

Let us now prove that $n_{\nu\mu\lambda}$ is an integer. First we prove the following lemma:

Lemme 7.15.3. *A necessary and sufficient condition for a set $[R]$ to be composed uniquely of a set of entire classes of a group G is that*

$$\forall u \in G\,,\ u^{-1}[R]u = [R]$$

Demo. The condition is necessary because, if indeed $[R]$ is composed of entire sets, then in each of these sets S, $u^{-1}[S]u$ is itself the set S by the reordering theorem.
To see that the condition is sufficient, let us proceed by contradiction and write

$$[R] = [R'] + [R'']$$

where $[R']$ is the largest subset of $[R]$ made of entire classes, and the reminder $[R'']$ thus must contain elements that are not an entire class. Since $[R']$ satisfy $u^{-1}[R']u = [R']$ then

$$u^{-1}[R'']u = [R'']\,.$$

e cannot be in $[R'']$ since it is, itself, a class. Let us suppose $[R'']$ is not empty, and $x \in [R'']$. Then it must exists $y \in G$, conjugated to x, which is *not* in $[R'']$. Since y is conjugated to x we have $u^{-1}xu = y$ for some $u \in G$. But then since $u^{-1}[R'']u = [R'']$ for all u, y must be in $[R'']$. We have thus reach a contradiction, and $[R'']$ is empty. □

Now we can proceed. Let H be a finite group of order h and conjugacy classes $C_1 = \{e\}$, $C_2, \ldots, C_\mu, \ldots, C_{N_C}$ its classes. We shall denote by n_μ the number of elements in the class C_μ and by N_C the total number of classes. We have, of course

$$\sum_{\mu=1}^{N_c} n_\mu = h \tag{7.150}$$

Let C_μ and C_ν be two classes of H, and consider the product

$$C_\mu * C_\nu = [uv] \tag{7.151}$$

where u and v are elements of C_μ and C_ν. Then for each $x \in H$, we have

$$x^{-1}C_\mu * C_\nu x = [x^{-1}uvx] = [x^{-1}u(xx^{-1})vx] = [(x^{-1}ux)(x^{-1}vx)] \tag{7.152}$$

Using the theorem of rearrangement, we see that $[(x^{-1}ux)(x^{-1}vx)]$ is just a reordering of $[uv]$ so that

$$x^{-1}C_\mu * C_\nu x = C_\mu * C_\nu \tag{7.153}$$

Applying lemma 7.15.3 then prove theorem 7.15.1.

7.16 Proof of Schur's lemma

Let us prove Schur's lemma. We are going to need the definition of "kernel" and "image" of an operator.

Definition 7.16.1 (Kernel of an operator)**.** The kernel Ker$A$ of an operator $A : V_1 \to V_2$ is the set of vector $\boldsymbol{v}_1 \in V_1$ such that $Av_1 = 0$.

Definition 7.16.2 (Image of an operator)**.** The image ImA of an operator $A : V_1 \to V_2$ is the set of vector $\boldsymbol{v}_2 \in V_2$ for which $\exists v_1 \in V_1$ such that $v_2 = Av_1$.

Theorem 7.16.3 (Rank-Nullity theorem)**.** *For any operator* $A : V_1 \to V_2$*, define* Rank(A) = dim[Im(A)] *and* Nullity(A) = dim[Ker(A)]*, then* dim$[V_1]$ = Nullity(A) + Rank(A).

7.16.1 Proof of lemma 1

Demo. For all $g \in G$ we have:

- $\forall \boldsymbol{v}_1 \in$ Ker$A$ we have $A(R_1(g)\boldsymbol{v}_1) = R_2(g)A\boldsymbol{v}_1 = 0$. This means that the vector $R_1(g)\boldsymbol{v}_1$ is also in the kernel of A. In other words a vector in $W = \ker A$ stays in W upon transformation by $R_1(g), \forall g$: W is thus a stable sub-space of $R_1(g)$.
- From a similar reasoning, we can deduce that the image $W' =$ ImA is also a stable subspace for $R_2(g)$. Indeed, this requires implies that if a vector can be written as $\boldsymbol{v}_2 = A\boldsymbol{v}_1$, then $R_2(g)\boldsymbol{v}_2$ can also be written as $A\boldsymbol{v}_1'$. This is the case since $R_2(g)\boldsymbol{v}_2 = R_2(g)A\boldsymbol{v}_1 = AR_1(g)\boldsymbol{v}_1 = A\boldsymbol{v}'$.

We thus conclude that$W =$ Ker$A$ is a stable subspace $R_1(g)$ and that $W' = A$ is a stable subspace of $R_2(g)$. However, by assumption, both representations are irreducible, so the only subspaces are either 0 or the entire space. We thus have either:

- Ker$A = 0$, in which case the image is not empty, so that im$A = V_2$. But this implies that the transformation A is invertible, but then $A^{-1}R_2(g)A = R_1(g)\forall g$, and R_2 and R_1 are equivalent, which contradicts the hypothesis.
- Ker$A = V_1$, in which case $A = 0$ (and the image is empty:im$A = 0$).

□

7.16.2 Proof of lemma 2

In this case, we have a map between either the same, or between equivalent representations. Additionally, $V_1 = V_2 = V$, and A is a square matrix. If the representation are equivalent, we can always rotate the space so that they are indeed identical.

Let us consider then that $R_1(g) = R_2(g) = R(g) \forall g$.

Demo. By the fundamental theorem of algebra, it exists an eigenvalue $\lambda \in \mathbb{C}$ such that $\det(A - \lambda I) = 0$. Consider then the equation

$$(A - \lambda I)R(g) = R(g)(A - \lambda I)\,. \tag{7.154}$$

so that if $v \in \mathrm{Ker}(A - \lambda I)$ then $R(g)v$ also in $\mathrm{Ker}(A - \lambda I)$. $W = \mathrm{Ker}(A - \lambda I)$ is thus a stable subspace of transformation by $R(g) \forall g$. Given $R(g)$ is irreducible, either $W = 0$ or $W = V$. W cannot be zero, because at least the eigenvector of A corresponding to λ is in W! Therefore $W = V$.

We this have $\mathrm{Ker}(A - \lambda I) = V$, so that $(A - \lambda I) = 0$ and therefore $A = \lambda I$. □

7.17 Proof of grand orthogonality Lemma

Demo. Consider any matrix X and the matrix M defined as

$$M = \sum_{g \in G} R_1(g^{-1}) X R_2(g) \tag{7.155}$$

Then we have, for any $y \in G$

$$\begin{aligned}
MR_2(y) &= \sum_{g \in G} R_1(g^{-1}) X R_2(g) R_2(y) \\
&= \sum_{g \in G} R_1(y) R_1(y^{-1}) R_1(g^{-1}) X R_2(g) R_2(y) \\
&= R_1(y) \sum_{g \in G} R_1(y^{-1}) R_1(g^{-1}) X R_2(g) R_2(y) \\
&= R_1(y) \sum_{g \in G} R_1(y^{-1} g^{-1}) X R_2(gy) \\
&= R_1(y) \sum_{g \in G} R_1((gy)^{-1}) X R_2(gy) \\
&= R_1(y) \sum_{h \in G} R_1(h^{-1}) X R_2(h) = R_1(y) M
\end{aligned}$$

We can thus use Schur's lemmas on M. Since R_1 and R_2 are not equivalent we have $M = 0$ so that

$$\sum_{g \in G} \sum_{jl} [R_1(g^{-1})]_{kj} X_{jl} [R_2(g)]_{lm} = 0 \tag{7.156}$$

but $R_1(g^{-1})$ is $R_1(g)^\dagger$ so that

$$\begin{aligned}
\sum_{g \in G} \sum_{jl} [R_1(g)]^\dagger_{kj} X_{jl} [R_2(g)]_{lm} &= 0 \\
\sum_{g \in G} \sum_{jl} [R_1(g)]^*_{jk} X_{jl} [R_2(g)]_{lm} &= 0
\end{aligned} \tag{7.157}$$

Using $X_{jl} = 0$ except for one pair jl for which $X_{jl} = 1$ leads to eq.(7.82).

We now turn to eq.(7.83). If we construct the matrix M using the same representation, we get again $MR(x) = R(x)M$ and by the second Schur lemma:

$$\sum_{g\in G} R(g^{-1})XR(g) = c(X)I \tag{7.158}$$

which, in full matrix notation, means

$$\sum_{g\in G}\sum_{jl}[R(g)]^*_{jk}X_{jl}[R(g)]_{lm} = c(X)\delta_{km}$$

We just need to compute the constant. Let us work on the diagonal, when $k = m$, and sum over k so that we have

$$\begin{aligned}
\sum_{g\in G}\sum_{jlk}[R(g^{-1})]_{kj}X_{jl}[R(g)]_{lk} &= n_a c(X)\\
\sum_{g\in G}\sum_{jl}X_{jl}\sum_{k}[R(g^{-1})]_{kj}[R(g)]_{lk} &= n_a c(X)\\
\sum_{g\in G}\sum_{jl}X_{jl}[R(g)R(g^{-1})]_{lj} &= n_a c(X)\\
\sum_{g\in G}\sum_{jl}X_{jl}I_{lj} &= n_a c(X)\\
\sum_{g\in G}\mathrm{Tr}X &= n_a c(X)\\
c(X) &= \frac{N}{n_A}\mathrm{Tr}X
\end{aligned}$$

Using again $X_{jl} = 0$ except for one pair jl for which $X_{jl} = 1$ leads to eq.(7.83). □

7.18 Proof of Burnside Lemma

We can now prove Burnside lemma. Consider the regular representation (which we introduced in the previous chapter) that is obtained using $N \times N$ matrices for a finite group of order N. Then we have a amazing fact: Any irreducible representation D of G appears in the regular representation $dim(D)$ times:

Theorem 7.18.1 (Regular representation decomposition)**.** *Consider the regular representation of a group. Then we have the following decomposition in irrep*

$$R^r(g) = \oplus_{a,x}R_{a,x}(g) = \oplus_a R_a R_a(g) \tag{7.159}$$

where R_a is the dimension of the representation a.

Demo. We simply apply

$$b_a = \frac{1}{N}\sum_{\mu} n_\mu \chi^*_a(C_\mu)\chi^r(C_\mu) \tag{7.160}$$

and using the fact that for the regular representation all characters are zero except for the one corresponding to e, we find

$$b_a = \frac{1}{N}\chi^*_a(C_e) = \frac{R_a}{N}N = R_a \tag{7.161}$$

□

This finally allows to prove Burnside's lemma, by simply counting the dimensions:

Lemme 7.18.2 (Burnside lemma)**.**

$$\sum_{i=1}^{N_r} d_i^2 = N \tag{7.162}$$

7.19 Representations of Lie Groups and Lie Algebras

The following theorems hold on the relationship between representations of Lie groups and Lie algebras [30]:

Theorem 7.19.1 ((Lie group reps induce Lie algebra reps))**.** *Let G be a matrix Lie group with Lie algebra $\mathfrak{g}$. If R is a representation of G on V, then there exists a unique representation r of $\mathfrak{g}$ on V given by*

$$r(J) = \frac{d}{dt}(R(e^{tX}))\Big|_{t=0}, \text{ for all } X \in \mathfrak{g}. \tag{7.163}$$

We call r the representation of $\mathfrak{g}$ induced by R.

Theorem 7.19.2 ((Lie algebra reps lift to simple Lie group representations))**.** *Let G be a simply connected matrix Lie group, and let r be a representation of the corresponding Lie algebra on V. Then there is a unique representation R of G with the property*

$$R(e^X) = e^{r(X)}, \text{ for all } X \in \mathfrak{g}. \tag{7.164}$$

Theorem 7.19.3 ((Lie algebra reps locally lift to Lie group reps).)**.** *Let G be a matrix Lie group, and let r be a representation of the corresponding Lie algebra on V. Then using Theorem 1, we can always locally define a representation R on G by the mapping*

$$R(g) = e^{r(X)}, \text{ defined for all } g = e^X \text{ nearby } I. \tag{7.165}$$

Here, by "nearby" we mean "wherever the exponential map is a diffeomorphism". Indeed, in this region, all g can be written as $g = e^X$.

[30] These statements are taken from Representation Theory for Geometric Quantum Machine Learning - see there for further discussion.

7.20 Examples of symmetries of quantum models

Here I show a list of examples of quantum models and their symmetries taken from Representation Theory for Geometric Quantum Machine Learning. While these examples are framed in a QML context they are more widely applicable.

Example 11: Discrete symmetries

Bit parity with bit-flip symmetry: Let n be an even number of qubits. Consider a problem of classifying computational basis product states according to their parity. Here, $\rho_i = |\psi_i\rangle\langle\psi_i|$, with $|\psi_i\rangle = |z_{i_1} z_{i_2} \dots z_{i_n}\rangle$, and where $z_{i_k} \in \{0,1\}$ the parity of $|\psi_i\rangle$ is defined as $y_i = f(|\psi_i\rangle) = \sum_{k=1}^{n} z_{i_k} \mod 2$. Defining the spin-flip operator $P = \bigotimes_{j=1}^{n} X_j$, where X_j is the Pauli-x operator acting on the j-th qubit. One can readily see that while $P|\psi_i\rangle \neq |\psi_i\rangle$, the parity is invariant under P, i.e. $f(P|\psi_i\rangle) = f(|\psi_i\rangle)$. For a concrete example, $f(P|01\rangle) = 1 = f(|10\rangle)$. In other words, the states are not invariant under the symmetry, but the labels are.

- *States:* Bitstring product states $|\psi_i\rangle = |z_{i_1} z_{i_2} \dots z_{i_n}\rangle \in (\mathbb{C}^2)^{\otimes n}$, where $z_{i_k} \in \{0,1\}$ and n even
- *Labels:* Parity $y_i = f(|\psi_i\rangle) = \sum_{k=1}^{n} z_{i_k} \mod 2$
- *Group:* $\mathbb{Z}_2 = \{1, p\}$
- *Representation:* $R : G \mapsto GL((\mathbb{C}^2)^{\otimes n})$, where $1 \cdot |\psi_i\rangle = |\psi_i\rangle$, $\sigma \cdot |\psi_i\rangle = P|\psi_i\rangle$

Qubit reflection parity: Consider a problem of classifying states according to their qubit-reflection parity. Defining the qubit-reflection operator $R := R_{1,n} R_{2,n-1} \dots R_{\lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 1}$, where $R_{j,j'}$ swaps qubits j and j', and writing $\rho_i = |\psi_i\rangle\langle\psi_i|$, the states will have label $y_i = 0$ ($y_i = 1$) if ρ_i is an eigenstate of R with eigenvalue 1 (-1). Here, one can readily verify that $R\rho_i R^\dagger = \rho_i$.

Qubit permutations: Learning problems with permutation symmetries abound. Examples include learning over sets of elements, modeling relations between pairs (graphs) or multiplets (hypergraphs) of entities, problems defined on grids (such as condensed matter systems), molecular systems, evaluating genuine multipartite entanglement, or working with distributed quantum sensors. Consider for instance a problem where an n-qubit ρ is a graph state encoding the topology of an underlying graph. One can create such state by starting with the state $|+\rangle^{\otimes n}$, and applying a unitary $U^{(a,b)}$ for each edge (a,b) in the graph. Here $U^{(a,b)} = e^{-i\gamma(|0\rangle\langle 0|)^a \otimes \mathbb{1}^b + (|1\rangle\langle 1|)^a \otimes Z^b)}$ is an Ising-type interaction. By conjugating the state with an element of S_n, one obtains a new quantum state whose interaction graph is isomorphic to the original one.

- *States:* Quantum states on qubits, where the qubit labeling index do not matter.
- *Labels: (Here, any label will work, since the states themselves are invariant).*
- *Group:* $G = S_n$, the symmetric group on n letters
- *Representation:* $R : G \mapsto GL((\mathbb{C}^2)^{\otimes n})$, where the 2-cycle $(j,j') \cdot |\psi_i\rangle = \text{SWAP}_{j,j'} |\psi_i\rangle$. Note that since any permutation in S_n can be expressed as a product of swaps, this defines our representation on all permutations.

Translation invariance: Let H a Hamiltonian and consider the problem of classifying energies y_i of a set of eigenstates $|\psi_i\rangle$. Suppose $H = \sum_{j=1}^{n} h_{j,j+1}$, where $h_{j,j+1}$ is a nearest-neighbor interaction and we impose periodic boundary conditions so that $n+1 \equiv 1$. Then H commutes with the translation operator $\tau_g : (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes n}$, which translates the state $|\psi\rangle$ to the right by g sites (e.g. $\tau_0 = \mathbb{1}$ and $\tau_2 |01101\rangle = |01011\rangle$). We can then use Prop. 5 to argue that the energy label y_i is invariant under the group of translations, so $f(|\psi_i\rangle) = f(\tau_g |\psi_i\rangle)$ for all translations τ_g.

- *States:* Eigenstates $|\psi_i\rangle$ of a Hamiltonian H on a ring of n qubits
- *Labels:* Eigenenergies y_i, i.e. $H|\psi_i\rangle = y_i |\psi_i\rangle$
- *Group:* $G = \mathbb{Z}_n$, the cyclic group of order n.
- *Representation:* $\tau : G \mapsto GL((\mathbb{C}^2)^{\otimes n})$, where τ_g translates to the right by g sites

Figure 7.18:

Example 12: Continuous symmetries

Unitary transformations and purity: Consider a problem of classifying pure states from mixed states. The dataset here is composed of states with label $y_i = 0$ ($y_i \neq 0$) if ρ_i is pure (mixed). Since the purity is a spectral property, then the labels in $\mathcal{S}$ are invariant under the action of any unitary. Note that here $f(U\rho_i U^\dagger) = f(\rho_i)$, but in general $U\rho_i U^\dagger \neq \rho_i$.

- *States:* States $\rho_i \in \mathcal{D}(\mathcal{H})$.
- *Labels:* Pure $y_i = 0$ and mixed $y_i \neq 0$.
- *Group:* $G = U(d)$, the unitary group on $\mathcal{H}$.
- *Representation:* $U : G \mapsto U(d)$, where $g \cdot \rho_i = U_g \rho_i U_g^\dagger$.

Orthogonal transformations: Consider a problem of classifying orthogonal (real-valued) states from Haar-random states. The dataset here is composed of states with label $y_i = 0$ ($y_i \neq 0$) if ρ_i is a real-valued state (a Haar random state). Here, the labels $y_i = 0$ are invariant under the action of any orthogonal unitary, as conjugated a real-valued state by a real-valued unitary yields a real-valued state. Note that here $f(U\rho_i U^\dagger) = f(\rho_i)$, but in general $U\rho_i U^\dagger \neq \rho_i$.

- *States:* States $\rho_i \in \mathcal{D}(\mathcal{H})$.
- *Labels:* Orthogonal $y_i = 0$ and mixed $y_i \neq 0$.
- *Group:* $G = O(d)$, the orthogonal group on $\mathcal{H}$
- *Representation:* $U : G \mapsto O(d)$, where $g \cdot \rho_i = U_g \rho_i U_g^\dagger$

Local unitary transformations and the XXX model: Consider the problem of classifying ground states of the Heisenberg XXX model $H = J\sum_{j=1}^n (X_j X_{j+1} + Y_j Y_{j+1} + Z_j Z_{j+1})$. Here, $y_i = 0$ ($y_i = 1$) if ρ_i is a ferromagnetic (antiferromagnetic) ground state of H with $J < 0$ ($J > 0$). Since H commutes with the total magnetization operators $S_x = \sum_{j=1}^n X_j$, $S_y = \sum_{j=1}^n Y_j$, $S_z = \sum_{j=1}^n Z_j$, then the labels are invariant under the action of the same local unitary acting on all qubits. That is, $f((\bigotimes_i^n U)\rho_i(\bigotimes_i^n U^\dagger)) = f(\rho_i)$ for any local unitary U.

- *States:* Ground states of the XXX chain $\rho_i \in \mathcal{D}(\mathcal{H})$
- *Labels:* Ferromagnetic $y_i = 0$ and antiferromagnetic $y_i = 1$
- *Group:* $G = U(2)$
- *Representation:* $U : G \mapsto U(d)$, where $g \cdot \rho_i = (U_g \otimes \cdots \otimes U_g)\rho_i(U_g \otimes \cdots \otimes U_g)^\dagger$

Local unitary transformations and multipartite entanglement: Consider the problem of classifying pure quantum states according to the amount of multipartite entanglement they posses. Here, $y_i = 1$ if the states posses a large amount of multipartite entanglement (according to some measure), while $y_i = 0$ if the states are separable. Since local unitaries do not change the multipartite entanglement in a quantum state, then we have that $f((\bigotimes_j^n U_j)\rho_i(\bigotimes_j^n U_j^\dagger)) = f(\rho_i)$ for any local unitary U_j acting on the j-th qubit.

- *States:* Pure states $\rho_i \in \mathcal{D}(\mathcal{H})$
- *Labels:* $y_i \in [0, 1]$, where 0 means separable and 1 means "highly entangled"
- *Group:* $G = U(2) \times \cdots \times U(2)$, ($n$ times)
- *Representation:* $U : G \mapsto U(d)$, where $(g_1, \ldots, g_n) \cdot \rho_i = (U_{g_1} \otimes \cdots \otimes U_{g_n})\rho_i(U_{g_1} \otimes \cdots \otimes U_{g_n})^\dagger$

Figure 7.19: