Chapter 11
Evolution by Permutation

In what follows a very brief account of reversible evolution and, in particular, reversible computation by permutation will be presented. We shall follow Mermin's account [368] (also available as his *Lecture Notes on Quantum Computation* [367]) and introduce reversible computation in terms of vector spaces: Thereby the computational states, and the state evolution are represented as elements of Cartesian standard bases, and permutation matrices acting on these base vectors, respectively.

11.1 Representation Entities by Vectors and Matrices

Let us repeat and rehearse some conventions involving the representation and creation of state related entities.

A *ket vector* $|\mathbf{x}\rangle$ can be represented by a column vector, that is, by vertically arranged tuples of scalars, or, equivalently, as $n \times 1$ matrices; that is,

$$|\mathbf{x}\rangle \equiv \left(x_1, x_2, \ldots, x_n\right)^{\mathsf{T}} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}. \tag{11.1}$$

Their linear span is a one-dimensional subspace.

A bra vector $\langle \mathbf{x}|$ from the dual space can be represented by a row vector, that is, by horizontally arranged tuples of scalars, or, equivalently, as $1 \times n$ matrices; that is,

$$\langle \mathbf{x}| = \left(|\mathbf{x}\rangle\right)^{\dagger} \equiv \left(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}\right). \tag{11.2}$$

K. Svozil, *Physical (A)Causality*, Fundamental Theories of Physics 192,
https://doi.org/10.1007/978-3-319-70815-7_11

Their linear spans

$$\begin{aligned}\mathfrak{M} = \operatorname{span}(|\mathbf{x}\rangle) &= \{|\mathbf{y}\rangle \mid |\mathbf{y}\rangle = \lambda|\mathbf{x}\rangle, |\mathbf{x}\rangle \in \mathfrak{V}, \lambda \in \mathbb{R} \text{ or } \mathbb{C}\}, \\ \operatorname{span}(\langle\mathbf{x}|) &= \left\{\langle\mathbf{y}| \mid \langle\mathbf{y}| = \lambda\langle\mathbf{x}|, \langle\mathbf{x}| \in \mathfrak{V}^*, \lambda \in \mathbb{R} \text{ or } \mathbb{C}\right\}\end{aligned} \tag{11.3}$$

are one-dimensional subspaces of the base space $\mathfrak{V}$ and the dual space $\mathfrak{V}^*$, respectively.

If $|\mathbf{x}\rangle$ is a unit vector, the associated orthogonal projection $\mathbf{E}_\mathbf{x}$ of $\mathfrak{V}$ onto $\mathfrak{M}$ can be written as the *dyadic product*, or *tensor product*, or *outer product*

$$\begin{aligned}\mathbf{E}_\mathbf{x} = |\mathbf{x}\rangle\langle\mathbf{x}| &\equiv \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \left(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}\right) \\ &= \begin{pmatrix} x_1 \left(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}\right) \\ x_2 \left(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}\right) \\ \vdots \\ x_n \left(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}\right) \end{pmatrix} = \begin{pmatrix} x_1\overline{x_1} & x_1\overline{x_2} & \cdots & x_1\overline{x_n} \\ x_2\overline{x_1} & x_2\overline{x_2} & \cdots & x_2\overline{x_n} \\ \vdots & \vdots & \vdots & \vdots \\ x_n\overline{x_1} & x_n\overline{x_2} & \cdots & x_n\overline{x_n} \end{pmatrix}\end{aligned} \tag{11.4}$$

is the projection associated with $|\mathbf{x}\rangle$.

If the vector $\mathbf{x}$ is not normalized, then the associated projection is $\mathbf{E}_\mathbf{x} = |\mathbf{x}\rangle\langle\mathbf{x}|/\left(\langle\mathbf{x}|\mathbf{x}\rangle\right)$.

The product (state) of two ket vectors $|\mathbf{x}\rangle \equiv \left(x_1, x_2, \ldots, x_n\right)^\mathsf{T}$ and $|\mathbf{y}\rangle \equiv \left(y_1, y_2, \ldots, y_n\right)^\mathsf{T}$ can, up to normalization, be written as

$$|\mathbf{x}\rangle|\mathbf{y}\rangle \equiv |\mathbf{y}\mathbf{x}\rangle \equiv \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \otimes \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \\ x_2 \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \\ \vdots \\ x_n \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \end{pmatrix} = \begin{pmatrix} x_1y_1 \\ x_1y_2 \\ \vdots \\ x_1y_n \\ x_2y_1 \\ x_2y_2 \\ \vdots \\ x_2y_n \\ \vdots \\ x_ny_1 \\ x_ny_2 \\ \vdots \\ x_ny_n \end{pmatrix}. \tag{11.5}$$

The product (state) of two bra vectors $\langle \mathbf{x}| \equiv \left(x_1, x_2, \ldots, x_n\right)$ and $\langle \mathbf{y}| \equiv \left(y_1, y_2, \ldots, y_n\right)$ can, up to normalization, be written as

$$\begin{aligned} \langle \mathbf{x}|\langle \mathbf{y}| \equiv \langle \mathbf{yx}| \equiv \left(x_1, x_2, \ldots, x_n\right) \otimes \left(y_1, y_2, \ldots, y_n\right) = \\ = \left(x_1 \left(y_1, y_2, \ldots, y_n\right), x_2 \left(y_1, y_2, \ldots, y_n\right), \ldots, x_n \left(y_1, y_2, \ldots, y_n\right)\right) = \\ = \left(x_1 y_1, x_1 y_2, \ldots, x_1 y_n, x_2 y_1, x_2 y_2, \ldots, x_2 y_n, x_n y_1, x_n y_2, \ldots, x_n y_n\right). \end{aligned} \tag{11.6}$$

11.2 Reversibility by Permutation

A more restricted universe than a quantized one would be rendered by *real* finite dimensional Hilbert spaces $\mathbb{R}^n$, and by the permutations – more precisely, orthonormal (orthogonal) transformations; that is, a one-to-one (injective) transformation of identical (co)domains $\mathbb{R}^n$ preserving the scalar product therein. An even greater restriction comes with a discretization of states as elements of Cartesian standard bases and the use of permutation matrices.

Recall that a *function* $f(x) = y$ from a set X to a set Y maps inputs (or arguments) x from X into outputs (or values) y from Y such that each element of X has a *single* and thus *unique output.* X is called the *domain* and Y is called the *codomain*. The *image* $f(X)$ of the entire domain X is a subset of the codomain Y.

A function f is *one-to-one* or *injective* if different functional outputs originate from different functional inputs; that is, if "$f(x) = f(y)$ implies $x = y$," which is logically equivalent to the contrapositive "$x \neq y$ implies $f(x) \neq f(y)$" – that is, if different functional inputs result in different functional outputs.

As a consequence, if f is one-to-one it can be "inverted" (and thus its action "undone") by another function f^{-1} from its image $f[X]$ into its domain X such that $f^{-1}(y) = x$ if $f(x) = y$. Therefore, the functional mapping can be inverted through $x \overset{f}{\mapsto} y \overset{f^{-1}}{\mapsto} x$; in particular, $f^{-1}(f(x)) = x$.

A function f is *onto*, or *surjective* if every element y in its codomain Y corresponds to some (not necessarily unique) element x of its domain, such that $y = f(x)$. In this case, the functional image is the codomain.

A function f is *bijective*, or a *one-to-one correspondence* if it is both one-to-one (injective) and onto (surjective).

A function f is a *permutation* if it is a one-to-one correspondence (bijective), and if the domain X is identical with the codomain $Y = X$.

Usually, the (co)domain is a finite set. The *symmetric group* $\mathrm{S}(n)$ on a finite set of n elements (or symbols) is the group whose elements are all the permutations of the n elements, and whose group operation is the composition of such permutations. The identity is the identity permutation. The *permutations* are bijective functions from the set of elements onto itself. The order (number of elements) of $\mathrm{S}(n)$ is $n!$.

Cayley's theorem [436] states that every group $\mathfrak{G}$ can be imbedded as – equivalently, is isomorphic to – a subgroup of the symmetric group; that is, it is isomorphic

to some permutation group. In particular, every finite group $\mathfrak{G}$ of order n can be imbedded as – equivalently, is isomorphic to – a subgroup of the symmetric group $\mathrm{S}(n)$.

Stated pointedly: permutations exhaust the possible structures of (finite) groups. The study of subgroups of the symmetric groups is no less general than the study of all groups.

A particular case where the codomain needs not to be finite is quantum mechanics. In quantum mechanics, the (co)domain will be identified with the Hilbert spaces. We will restrict our attention to *complex* finite dimensional Hilbert spaces $\mathbb{C}^n$ with the Euclidean scalar product. In one of the axioms of quantum mechanics the evolution is identified with some *isometric permutation* preserving the scalar product (or, equivalently, a mapping of one orthomodular basis into another one); that is, with unitary transformations $\mathbf{U}$, for which the adjoint (the conjugate transpose) is the inverse; that is, $\mathbf{U}^* = \mathbf{U}^\dagger = \mathbf{U}^{-1}$.

We shall now turn our attention to an even more restricted type of universe whose evolution is based upon permutations [193] on *countable* or even finite (co)domains [368]. Thereby we shall identify these (co)domains with very particular sets of unit vectors in $\mathbb{R}^n$: the Cartesian standard bases; namely all those ket (that is, column) vectors $|\mathbf{x}\rangle$ with a single coordinate being one, and all other components zero.

Suppose further that elements of the set $\{1, 2, \ldots, n\}$ of natural numbers are identified with the elements of the Cartesian standard bases $\mathfrak{B} = \{|\mathbf{e}_1\rangle, |\mathbf{e}_2, \ldots, |\mathbf{e}_n\rangle\}$ by $i \equiv |\mathbf{e}_i\rangle$.

The symmetric group $\mathrm{S}(n)$ of all permutations of n basis elements of $\mathfrak{B}$ can then be represented by the set of all $(n \times n)$ permutation matrices carrying only a single "1" in all rows and columns; all other entries vanish.

11.2.1 Representation as a Sum of Dyadic Products

For the sake of an example, consider the two-dimensional case with $n = 2$,

$$1 \equiv |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \text{ and } 2 \equiv |2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{11.7}$$

Then there exist only two permutation matrices, interpretable as the identity and the not matrix, respectively:

$$\mathbb{I}_2 = |1\rangle\langle 1| + |2\rangle\langle 2| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \text{ and } \mathbf{X} = |1\rangle\langle 2| + |2\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{11.8}$$

Note that the way these matrices are constructed follows the scheme of defining unitary transformations in terms of sums of basis state changes [460]. Indeed, all the $n!$ permutation matrixes transforming the n basis elements of the Cartesian standard

basis $\mathfrak{B} = \{|\mathbf{e}_1\rangle, |\mathbf{e}_2\rangle, \ldots, |\mathbf{e}_n\rangle\}$ in n dimensions can be constructed by varying the sums of such basis state changes. More explicitly, consider in Cauchy's two-line notation the jth permutation $\sigma_j = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma_j(1) & \sigma_j(2) & \ldots & \sigma_j(n) \end{pmatrix}$ so that the input i is mapped into $\sigma_j(i)$, with $1 \leq i \leq n$; then the jth permutation matrix can be defined by

$$\mathbf{P}_j = \sum_{i=1}^{n} |\mathbf{e}_i\rangle\langle\mathbf{e}_{\sigma_j(i)}| = \sum_{i=1}^{n} |\mathbf{e}_{\sigma_j(i)}\rangle\langle\mathbf{e}_i|. \tag{11.9}$$

11.2.2 No Coherent Superposition and Entanglement

Permutations cannot give rise to coherent superposition and entanglement – the latter one being just particular, non-factorizable superpositions in the multiple particle context. Syntactically this is due to the fact that, for a finite number of bits, permutation matrices contain only a single entry in each row and each column.

11.2.3 Universality with Respect to Boolean Functions

The following question arises naturally: is the set of permutations for arbitrary large-dimensional computationally universal in the sense of Turing; that is: can such a system of permutations compute all recursively enumerable functions [55, 222, 537]?

The three-bit *Fredkin gate* is *universal* with respect to the class of *Boolean functions*; that is, functions of binary inputs with binary output. Universality here means that any Boolean function can be constructed by the serial composition Fredki gates. Its permutation matrix $\mathbf{P}_F = \text{diag}\left(1, 1, 1, 1, 1, \mathbf{X}, 1\right)$ is almost diagonal. Thereby "diag$(\lambda_1, \lambda_2, \ldots, \lambda_n)$" stands for the diagonal matrix with entries $\lambda_1, \lambda_2, \ldots, \lambda_n$ in the main diagonal.

Based on the permutation $\sigma_F = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 1\,2\,3\,4\,5\,7\,6\,8 \end{pmatrix}$ this gate can be represented in terms of the sum decomposition (11.9) by $\mathbf{P}_F = \sum_{i=1}^{5} |\mathbf{e}_i\rangle\langle\mathbf{e}_i| + |\mathbf{e}_6\rangle\langle\mathbf{e}_7| + |\mathbf{e}_7\rangle\langle\mathbf{e}_6| + |\mathbf{e}_8\rangle\langle\mathbf{e}_8|$.

Likewise, the three-bit *Toffoli gate* is *universal* with respect to the class of Boolean functions. Its permutation matrix is $\mathbf{P}_T = \text{diag}\left(1, 1, 1, 1, 1, 1, \mathbf{X}\right)$. Based on the permutation $\sigma_T = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 1\,2\,3\,4\,5\,6\,8\,7 \end{pmatrix}$ this gate can be represented in terms of the sum decomposition (11.9) by $\mathbf{P}_T = \sum_{i=1}^{6} |\mathbf{e}_i\rangle\langle\mathbf{e}_i| + |\mathbf{e}_7\rangle\langle\mathbf{e}_8| + |\mathbf{e}_8\rangle\langle\mathbf{e}_7|$.

Indeed, the Fredkin and the Toffoli gates are equivalent up to permutations; and so is any quasi-diagonal matrix with one entry in 2×2 matrix block form $\mathbf{X}$, and all other entries 1 in the diagonal.

11.2.4 Universal Turing Computability from Boolean Functions

This author is not aware of any concrete, formal derivation of Turing universality from universality with respect to Boolean functions. Indeed, how could input-output circuits encode the kind of substitution and self-reference encountered in recursion theory [473–475]? One could conjectured that, of one allows an arbitrary *sequence* of Boolean functions, then this would entail universal Turing computability [69, 378], but this is still a far cry from coding, say, the Ackermann function in terms of reversible gates.

11.2.5 d-Ary Information Beyond Bits

While it is true that, at least in principle, Leibniz's binary atoms of information suffice for the construction of higher-dimensional entities, it is not entirely unreasonable to consider 3-ary, 4-ary, and, in general d-ary atoms of information. One conjecture would be that the set of universal operations with respect to d-ary generalisations of binary functions – that is, functions $f(x_1, \ldots, x_k) \in \{1, \ldots, d\}$ with k d-ary inputs $x_i \in \{1, \ldots, d\}$ with a d-ary output – are representable by a set of generalized Toffoli gates $\mathbf{P}_{T'} = \text{diag}\left(1, 1, 1, 1, 1, 1, \mathbf{P}_d\right)$, where $\mathbf{P}_d$ varies over all permutations of $\{1, \ldots, d\}$.

11.2.6 Roadmap to Quantum Computing

Quantum computing is about generalized states, which can be in a superposition of classical states; and about generalized permutations; that is, about bijections in complex vector spaces. For this it is sufficient to consider classical reversible computation, "augmented" with gates producing coherent superpositions of a classical bit (such as the Hadamard gate or quantum Fourier transforms) [371, 466].