

Foundations of Quantum Computation: A Workbook

Howard A. Blair

Copyright © 2007–2009 Howard A. Blair. All commercial rights reserved.

Part I: Sets, Relations, Functions

- **Definition:** (*subset*) For any sets A and S , A is a *subset* of S if, and only if, every member of A is a member of S . We denote that A is a subset of S by $A \subseteq S$.
- **Definition:** (*powerset*) For any set S , the *power set* of S , denoted by $\mathbf{P}(S)$, is the set of all subsets of S . That is,

$$\mathbf{P}(S) = \{B \mid B \subseteq S\}.$$

- **Definition:** (*relation from set A to set B*) Let A and B be sets. $A \times B$ is the set of all ordered pairs whose first member is a member of A and whose second member is a member of B . A *binary relation* from A to B is a triple (A, B, R) , where R is a subset of $A \times B$. If $A = B$ then we say that R is a binary relation *on* A . The expressions $(x, y) \in R$, $R(x, y)$ and $x R y$ are used interchangeably to denote the statement that (x, y) is a member of R . A is called the *domain* of the relation and Y is called the *codomain* of the relation. When the domain and codomain of the relation are clear, we refer to the relation by simply referring to R , as in the following definitions.
- **Definition:** (*function from set A to set B*) A *function from A to B* is a relation (A, B, f) from A to B such that for each $a \in A$ there is exactly one element b in B such that $(a, b) \in f$. We write the function (A, B, f) as $f : A \rightarrow B$. For each a in f , the unique element b in B such that (a, b) is in f is denoted by $f(a)$.
- **Definition:** (*reflexivity*) A binary relation R on a set A is *reflexive* if, and only if, for every $x \in A$, $x R x$.
- **Definition:** (*symmetry*) A binary relation R on a set A is *symmetric* if, and only if, for every $x \in A$, if $x R y$, then $y R x$.

- **Definition:** (*transitivity*) A binary relation R on a set A is *transitive* if, and only if, for every $x \in A$, $y \in A$ and $z \in A$, if xRy and yRz , then xRz .

Definition: (*equivalence relation*) A binary relation R on a set A is an *equivalence relation* if, and only if, R is reflexive, symmetric and transitive.

- **Definition:** (*antisymmetry*) A binary relation R on a set A is *antisymmetric* iff for every $x \in A$ and $y \in A$: if xRy and yRx then $a = b$.

- **Definition:** (*partial ordering*) A partial ordering on set A is a binary relation from A to A which is reflexive, anti-symmetric and transitive. (We typically use some such as symbol as \sqsubseteq to denote an ordering relation, and write it in infix position. e.g. $x \sqsubseteq y$.)

- **Definition:** (*partial order, aka po, poset*) A partial order is a pair (D, \sqsubseteq) such that D is a nonempty set and \sqsubseteq is a partial ordering on D .

- **Definition:** (*minimum, maximum*) Let (D, \sqsubseteq) be a poset and let $A \subseteq D$. a is a *minimum element* of A iff $a \in A$ and for every $b \in A$, $a \sqsubseteq b$. a is a *maximum element* of A iff $a \in A$ and for every $b \in A$, $b \sqsubseteq a$.

- **Definition:** (*minimal*) Let (D, \sqsubseteq) be a poset and let $A \subseteq D$. a is a *minimal element* of A iff $a \in A$ and for every $b \in A$, if $b \sqsubseteq a$, then $b = a$. **Comment:** Less formally, a minimal element of A is an element a of A such that there is no element of A below a .

- **Definition:** (*maximal*) Let (D, \sqsubseteq) be a poset and let $A \subseteq D$. a is a *maximal element* of A iff $a \in A$ and for every $b \in A$, if $a \sqsubseteq b$, then $a = b$.

- **Definition:** (*lower bound, upper bound*) Let (D, \sqsubseteq) be a poset and let $A \subseteq D$. An element x in D is a *lower bound* of A iff for every a in A , $x \sqsubseteq a$. An element x in D is an *upper bound* of A iff for every a in A , $a \sqsubseteq x$. We use the notation $x \sqsubseteq A$ to say that x is a lower bound of A . Similarly, we write $A \sqsubseteq x$ to say that x is an upper bound of A . **Comment:** An upper bound of A may or may not be an element of A .

- **Proposition:** Let (D, \sqsubseteq) be a poset and let $A \subseteq D$. Then,
 - a is a *least* element of A iff a is a greatest lower bound of A , and $a \in A$.
 - a is a *greatest* element of A iff a is a least upper bound of A , and $a \in A$.

■

- **Proposition:** Let (D, \sqsubseteq) be a poset and let $A \subseteq D$. Then,
 - a is a *least* element of A iff a is a greatest lower bound of A , and $a \in A$.

(ii) a is a *greatest* element of A iff a is a least upper bound of A , and $a \in A$. ■

- **Task:** Find an example of an infinite poset D and subset A of D that has a *unique* minimal element that is not the least element of A . (You may find it helpful to sketch posets by using Hasse diagrams.)

Answer: The isolated element on the left of the descending sequence is the unique minimal element, but it is not least because there are elements (all of them) in the descending column that are not above it.



- **Task:** Let (D, \sqsubseteq) be a poset and let $A \subseteq D$. Show that there is at most one greatest lower bound of A . (Therefore, if A has a greatest lower bound, then it is unique.) Show that there is at most one least upper bound of A .

Proof: Suppose that x_1 and x_2 are two distinct greatest lower bounds of A . Let L_A be the set of lower bounds of A . Then both x_1 and x_2 are maximum elements in L_A . Since x_1 is in L_A and x_2 is maximum in L_A , $x_1 \sqsubseteq x_2$. Similarly, $x_2 \sqsubseteq x_1$. By antisymmetry, $x_1 = x_2$.

- **Notation:** The least upper bound of a subset A of a po, if it exists, is denoted by $\sqcup A$.
- **Definition: images** Let S_1 and S_2 be sets and let $f : S_1 \longrightarrow S_2$. Let $A \subseteq S_1$. The f -image of A is $\{f(x) \mid x \in A\}$.
- **Definition: (continuous function)** Let (D, \sqsubseteq_D) and (E, \sqsubseteq_E) be po's. $f : D \longrightarrow E$ is *continuous* iff for every subset A of D , if $\sqcup A$ exists, then $\sqcup f(A)$ exists and $f(\sqcup A) = \sqcup f(A)$. **Warning:** This is not the standard definition given in the literature on the mathematical foundations of programming languages, but it is, for nonconstructive set-theoretic reasons, equivalent to the

usual definition on *directed-complete* po's (dcpo's). This is an issue tangential to our present purposes.

- **Definition:** (*monotonic function*) Let (D, \sqsubseteq_D) and (E, \sqsubseteq_E) be po's. $f : D \longrightarrow E$ is *monotonic* iff for every $x, y \in D$, if $x \sqsubseteq_D y$ then $f(x) \sqsubseteq_E f(y)$.
- **Task:** Prove that every continuous function from a po to a po is monotonic.
- **Task:** Find an example of a function $f : D \longrightarrow D$ that is monotonic but not continuous.

Part II: Applying partial orders

Task: Given a nonempty set S , we may consider the *flat* partially ordered set $\ddot{S} = (S, \sqsubseteq)$ whose partial order is defined by

$$s_1 \sqsubseteq s_2 \text{ iff } s_1 = s_2.$$

Show that \ddot{S} is a po.

- **Informal Definition:** (*state*) Assume we have a fixed set of programming language variables \mathbf{Var} . A *state* is a function that maps variables in \mathbf{Var} to values that respects the type of the variable; e.g. integer variables must be mapped to integer values.
- **Task:** Show that if D is a po, then so is the *lifted* set D_\perp , where $D_\perp = D \cup \{\perp_D\}$ and the partial ordering on D is extended by putting for all $x, y \in D_\perp$,

$$x \sqsubseteq y \text{ iff } x = \perp_D \text{ or } x \sqsubseteq_D y$$

- **Task:** Let D be the lifted flat po on two elements a and b . Describe the ordering on $D \longrightarrow D$ equipped with the point-wise ordering. (Just draw a diagram.)
- **Task 5:** Let D be a po and S just an ordinary nonempty set. Show that the set $S \longrightarrow D$, ordered by

$$f \sqsubseteq g \text{ iff for all } s \in S : f(s) \sqsubseteq_D g(s)$$

is a po.

- **Task:** Let D be a po with a bottom element \perp and let $f : D \longrightarrow D$ be continuous. Show that $\bigsqcup_{i=0}^{\infty} f^i(\perp)$ is the least fixed point of f . i.e. if $a = \bigsqcup_{i=0}^{\infty} f^i(\perp)$ then $f(a) = a$ and for all d such that $f(d) = d$, $a \sqsubseteq d$.

- **Discussion:** Let **States** be the set of states. Let β be a function from **States** to $\llbracket \mathbf{bool} \rrbracket$. Let κ be a function from **States** to **States**. Now, define

$$\Gamma_{\beta, \kappa} : (\mathbf{States} \longrightarrow \mathbf{States}) \longrightarrow (\mathbf{States} \longrightarrow \mathbf{States})$$

by

$$\Gamma_{\beta, \kappa}(c) = \lambda s. \begin{cases} c(\kappa(s)) & \text{if } \beta(s) = \text{true} \\ s & \text{if } \beta(s) = \text{false} \\ \perp & \text{if } \beta(s) = \perp \end{cases}$$

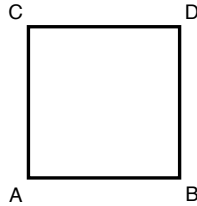
(The above definition uses “lambda-notation”; you may have to look that up if you are not already familiar with it.)

- **Difficult Task:** Show that $\Gamma_{\beta, \kappa}$ is continuous.

Part III: Symmetries

The following sequence of tasks and short problems shows how a vector space, or sometimes just a *ring module*, arises from an Abelian *regular action* on a structure. These terms will be defined in the sequence.

- Consider a graph (which is a set, each of whose members is called a *vertex* (plural: *vertices*)) together with a symmetric relation on the set of vertices called the edge relation) represented as a square in the Euclidean plane.



- List the ordered pairs in the edge relation of the above graph.
- Consider all of the permutations of vertices A, B, C, D of the graph that preserve the edge relation. In other words, π preserves the edge relation if (X, Y) is an edge and π is a permutation of the vertices, then $(\pi(X), \pi(Y))$ and $(\pi^{-1}(X), \pi^{-1}(Y))$ are edges. For example, if π swaps A and B but leaves C and D fixed, then π does not preserve the edge relation because (B, D) is an edge, but (A, D) is not. An edge preserving permutation of the vertices of the graph is called an *automorphism* of the graph.

Example: Here are four automorphisms of the square:

- (1) $\pi_{00}(X) = X$ for every vertex X of the graph.
 $\pi_{01}(A) = C, \pi_{01}(C) = A, \pi_{01}(B) = D, \pi_{01}(D) = B$. π_{01} flips the figure over a horizontal axis.
 $\pi_{10}(A) = B, \pi_{10}(B) = A, \pi_{10}(C) = D, \pi_{10}(D) = C$. π_{10} flips the figure over a vertical axis.
 $\pi_{11}(A) = D, \pi_{11}(D) = A, \pi_{11}(B) = C, \pi_{11}(C) = B$. π_{11} rotates the figure 180 degrees, or π radians.

Note for example that $\pi_{10} \circ \pi_{01} = \pi_{11}$, where \circ is the function composition operation. In particular, for example,

$$(\pi_{10} \circ \pi_{01})(A) = \pi_{10}(\pi_{01}(A)) = \pi_{10}(C) = D$$

Task 1: Fill in the rest of the table below:

\circ	π_{00}	π_{01}	π_{10}	π_{11}
π_{00}				
π_{01}				π_{11}
π_{10}				
π_{11}				

Notice that the table defines an Abelian group. (Look up definitions of such terms as *group* as necessary. This group is isomorphic to the group $(\mathbf{Z}_2 \oplus \mathbf{Z}_2, +)$.)

The elements of $(\mathbf{Z}_2 \oplus \mathbf{Z}_2, +)$ are the column vectors $\begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$ where $b_1, b_2 \in \{0, 1\}$.

The vectors are added mod 2.

- The group $(\{\pi_{00}, \pi_{01}, \pi_{10}, \pi_{11}\}, \circ)$ is a group of automorphisms, i.e. a group of symmetries, of the square, or, at least, the graph depicted by the square. All groups, Abelian or otherwise, are groups of symmetries of some structure. We say that a groups of symmetries of a structure, as well as the symmetries themselves, *act* on the structure. We can extend the concept of *action* quite a lot of useful ways. But one way that is important to us is that a group that is isomorphic to a group of symmetries acting on a structure itself acts on the structure. Each of the element of the latter group acts on the structure by applying the symmetry corresponding via the isomorphism to the element. For example, the vector $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ acts on the square by applying the permutation π_{01} .

We are being deliberately vague about what we mean by the term *structure*. All topological spaces and all graphs and all directed graphs are structures, for example. The details do not concern us. In this workbook we will be concerned with only a few structures that are either completely familiar or will be defined.

A group acting on a structure is said to be a *regular action* if, and only if, for every two elements of the structure (possibly the two elements are the same, and vertices in the case of graphs, points in the case of spaces) there is exactly one element of the group that maps the first element to the second.

- **Task 2:** Show: If a group G acting on a structure S is a regular action, then the elements of G and the elements of S are in one-to-one correspondence. [Pick any one element of the structure and call it the origin. Then show describe the correspondence. [\[It is not necessary to know what a structure is to prove this.\]](#)
- **Task 3:** In the above square, let A be origin. Let $(\mathbf{Z}_2 \oplus \mathbf{Z}_2, +)$ act according to the isomorphism φ from $(\mathbf{Z}_2 \oplus \mathbf{Z}_2, +)$ to $(\{\pi_{00}, \pi_{01}, \pi_{10}, \pi_{11}\}, \circ)$ given by $\varphi\left(\begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\right) = \pi_{b_1, b_2}$. Specify the correspondence between the elements of $(\mathbf{Z}_2 \oplus \mathbf{Z}_2, +)$ and the vertices of the square.
- The elements of a group that have a regular action on S are called *translations* of S .

The elements of $(\mathbf{Z}_2 \oplus \mathbf{Z}_2, +)$ are translations of the square. These elements add the way they do because as translations that is the way they compose; i.e. if we apply one translation and then another, i.e. we apply one symmetry π_{b_1, b_2} and then another, π_{c_1, c_2} , the combined translation is the symmetry resulting from the composition of the two symmetries: $\pi_{c_1, c_2} \circ \pi_{b_1, b_2}$. The additive part of a vector space is (literally) an Abelian regular action on a structure. The converse is not always true, but comes close. An Abelian regular action on a structure always produces a ring module. Every vector space is a ring module. Next we take up the matter of where the scalars come from.

- An endomorphism of a group is a function $h : G \longrightarrow G$ such that $h(x \cdot y) = h(x) \cdot h(y)$ for every $x, y \in G$.
- **Task 4:** Show that an endomorphism of G must map the identity element of G to itself.

- **Task 5:** In the case of $(\mathbf{Z}_2 \oplus \mathbf{Z}_2, +)$, suppose h is an endomorphism and you know the values of $h\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right)$ and $h\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right)$. What is $h\left(\begin{bmatrix} 1 \\ 1 \end{bmatrix}\right)$ in terms of these known values?
- **Task 6:** Show that the endomorphisms of $(\mathbf{Z}_2 \oplus \mathbf{Z}_2, +)$ are represented by the sixteen possible 2×2 matrices whose entries are elements of $\{0, 1\}$. (Matrix addition and multiplication are done mod 2.) [In other words, let

$$\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$$

be any one of the sixteen matrices, and show that multiplication by it is an endomorphism of $(\mathbf{Z}_2 \oplus \mathbf{Z}_2, +)$.]

- **Task 7:** Show that the 16 endomorphisms form a ring with a multiplicative identity. This is special case of the next task. So it is sufficient to really just do the next task, but this one may be helpful to you because it is somewhat concrete.
- **Task 8:** Show that the endomorphisms of an Abelian group are a ring. (Multiplication is composition, and addition is pointwise addition; i.e. $(h_1 + h_2)(x) = h_1(x) + h_2(x)$. The addition operation on the righthand side is the Abelian group operation.)
- **Task 9:** Among the endomorphisms of $(\mathbf{Z}_2 \oplus \mathbf{Z}_2, +)$, identify the ones that are invertible, and determine their inverses. Find two of these invertible matrices that do not commute using matrix multiplication mod 2.
- **Task 10:** The additive component of $\text{Endo}(\mathbf{Z}_2 \oplus \mathbf{Z}_2, +)$ is itself an additive group with sixteen elements. A basic theorem in group theory, known as Lagrange's theorem (he had lots, this is just one basic theorem) is that the size of a subgroup of a finite group divides the size of the group. So, the possible sizes of the subgroups of $\text{Endo}(\mathbf{Z}_2 \oplus \mathbf{Z}_2, +)$ are 1, 2, 4, 8 and 16. There are lots of subgroups of $\text{Endo}(\mathbf{Z}_2 \oplus \mathbf{Z}_2, +)$ of size 2. Find one that contains the zero matrix plus one other self-invertible endomorphism A of $(\mathbf{Z}_2 \oplus \mathbf{Z}_2, +)$. A has to be among the ones you determined in the previous task.
- **Task 11:** Show that the size 2 subgroup you gave in task (10) forms a field isomorphic to $(\mathbf{Z}_2, +, \cdot)$. The two elements in your field are the scalars for $(\mathbf{Z}_2 \oplus \mathbf{Z}_2, +)$ that yield a 2-dimensional vector space.

- Are there any other subrings of $\text{Endo}(\mathbf{Z}_2 \oplus \mathbf{Z}_2)$ that give us a field? The additive component of such a field must be a subgroup of $\text{Endo}(\mathbf{Z}_2 \oplus \mathbf{Z}_2, +)$. Moreover, the nonzero part of such a subgroup must consist of multiplicatively invertible endomorphisms. There are not enough such elements to give us a field of size 8 or 16. What about size 4? The three nonzero elements themselves must form a multiplicative group of size 3.
- **Task 12:** By filling in a multiplication table for a hypothetical group of size 3 show that all groups of size 3 are isomorphic to $(\mathbf{Z}_3, +)$.
- **Task 13:** It must therefore be the case that the two endomorphisms in the multiplicative group of size 3 that we are seeking that are not the multiplicative identity must be multiplicative inverses of each other. Now find the 4 endomorphisms that as a subring of $\text{Endo}(\mathbf{Z}_2 \oplus \mathbf{Z}_2)$ form a field of size four and verify that they do form a field. Write out the addition and multiplication tables for this field.
- This field (up to isomorphism) is known as the Galois field \mathbf{GF}_4 . Notice that its addition table shows that the additive component of this field is isomorphic to $(\mathbf{Z}_2 \oplus \mathbf{Z}_2, +)$. Thus $(\mathbf{Z}_2 \oplus \mathbf{Z}_2)$ is a 1-dimensional vector space over \mathbf{GF}_4 .
- Now consider the Euclidean plane. If we recap the story about translations that we told about the square, but this time we do it with the Euclidean plane, we will get for our translations the vectors

$$\begin{bmatrix} x \\ y \end{bmatrix}$$

and for our scalars the endomorphisms

$$\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}$$

Thus, the Euclidean plane is a 2-dimensional vector space over the real numbers \mathbf{R} . Are there any other fields of *continuous* endomorphisms of $(\mathbf{R}^2, +)$ of interest?

- **Task 14:** Show that the following collection of endomorphisms of $(\mathbf{R}^2, +)$ is a field, where multiplication is composition (matrix multiplication) and addition is pointwise addition (matrix addition):

$$\left\{ w \begin{bmatrix} x & -y \\ y & x \end{bmatrix} \mid w, x, y \in \mathbf{R}, x^2 + y^2 = 1 \right\}$$

- The endomorphisms of task (14) are symmetries of the Euclidean plane. The symmetries of the form

$$\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}$$

are radial expansions and contractions around a fixed point, the origin, (the origin as described above in task (2)) possibly combined with a reflection through the origin, and the symmetries of the form

$$\begin{bmatrix} x & -y \\ y & x \end{bmatrix}$$

with $w, x, y \in \mathbf{R}, x^2 + y^2 = 1$ are rigid rotations about the origin. All of the symmetries that can be generated by composing these two types of symmetries are the symmetries given by the endomorphisms of task (14).

- Thus, the symmetries

$$\begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} \begin{bmatrix} x & -y \\ y & x \end{bmatrix}$$

with $r, x, y \in \mathbb{R}$ and $x^2 + y^2 = 1$ are the complex numbers. The Euclidean plane is a 1-dimensional vector space over the field of complex numbers since any point $\begin{bmatrix} x \\ y \end{bmatrix}$ is obtainable by the application of exactly one of these symmetries to any fixed non-zero point such as $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$.

Also note that the values x and y in the rotations are square roots of the values in a probability distribution on two points.

- Suppose that we cast the type of r to the type of the symmetry given by the matrix

$$\begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix}$$

Then

$$r \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} rx \\ ry \end{bmatrix}$$

- Note also that

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

- If we give the *name* i to the symmetry given by the matrix

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

we obtain

$$ii = -1$$

- For x, y in \mathbb{R} such that $x^2 + y^2 = 1$, there is a unique $0 \leq \Theta < 2\pi$ such that

$$x = \cos \Theta, \quad y = \sin \Theta$$

We have

$$\begin{bmatrix} x & -y \\ y & x \end{bmatrix} = x + iy = \cos \Theta + i \sin \Theta$$

Note that

$$\begin{bmatrix} x & -y \\ y & x \end{bmatrix} \begin{bmatrix} u & -v \\ v & u \end{bmatrix} = \begin{bmatrix} xu - yv & -(xv + yu) \\ xv + yu & xu - yv \end{bmatrix}$$

If

$$\begin{bmatrix} u & -v \\ v & u \end{bmatrix} = \cos \phi + i \sin \phi$$

then

$$\begin{bmatrix} x & -y \\ y & x \end{bmatrix} \begin{bmatrix} u & -v \\ v & u \end{bmatrix} = \cos(\Theta + \phi) + i \sin(\Theta + \phi)$$

It follows that if we define

$$\xi(\Theta) = \cos \Theta + i \sin \Theta$$

then ξ is an exponential function mapping the real numbers to complex numbers, since

$$\xi(\Theta)\xi(\phi) = \xi(\Theta + \phi)$$