Quantum Computing — Some Maths

Last updated: February 11$^{\text{th}}$ 2019, at 12.59pm

Contents

Lesson Plan

- Week 17: Modelling classical circuits

  Some maths to prepare for quantum circuits
- Week 19: Quantum systems

  Modelling quantum properties (superposition, entanglement)
- Week 20: Quantum circuits

1 Complex Numbers

1.1 Imaginary and complex numbers

1.1.1 The square root of -1

Complex numbers are built around the square root of -1. Any two positive numbers multiplied together give a positive result, as do any two negative numbers multiplied together. It follows that the square of any number must be positive. The square root of -1 cannot therefore be an ordinary number. The *imaginary number* i (or sometimes j) is defined to be the square root of -1. I.e. $i \times i = -1$.

1.1.2 Complex numbers

A complex number consists of a *real part* and an *imaginary part.* For example, $3 + 4i$ is a complex number.

1.1.3 Complex conjugate

A useful concept is the *(complex) conjugate* of a complex number. The complex conjugate, $\overline{c}$, of a complex number c simply changes the sign (operator) between the real and imaginary parts of c. E.g.

$$\overline{-3+4i} = -3 - 4i, \text{ and } \overline{2-6i} = 2 + 6i.$$

1.1.4 Magnitude

The *magnitude* of a complex number is a measure of its size. The notation $|c|$ is used.

$$|a + bi| = \sqrt{a^2 + b^2}$$

Note that $|c| = \sqrt{c \times \overline{c}}$. Let $c = a+bi$, then $c \times \overline{c} = (a+bi)(a-bi) = a^2 - b^2 i^2 = a^2 - b^2(-1) = a^2 + b^2$, so $\sqrt{c \times \overline{c}} = \sqrt{a^2 + b^2} = |c|$.

1.2 Arithmetic

Arithmetic on complex numbers works just as arithmetic on ordinary numbers. Whenever $i \times i$ appears it can be replaced by -1.

1.2.1 Addition and Subtraction

In addition and subtraction the real and imaginary parts are added (subtracted) separately. E.g.

$$\begin{aligned}(3+4i)+(2-6i) &= 5-2i,\\ (3+4i)-(2-6i) &= 1+10i.\end{aligned}$$

1.2.2 Multiplication

In multiplication the complex pairs are multiplied out, and $i \times i$ replaced by -1. E.g.

$$\begin{aligned}(3+4i)(2-6i) &= 3(2-6i)+4i(2-6i)\\ &= 6-18i+8i-24(i\times i)\\ &= 6-10i-24(-1)\\ &= 6-10i+24\\ &= 30-10i.\end{aligned}$$

1.2.3 Division

We probably won't need division, but the easiest way to do division is to multiply both numerator and denominator by the conjugate of the denominator. The denominator is then a real number, and the numerator is a simple multiplication. E.g.

$$\begin{aligned}\frac{3+4i}{2-6i} &= \frac{3+2i}{2-6i}\times\frac{2+6i}{2+6i}\\ &= \frac{(3+4i)(2+6i)}{(2-6i)(2+6i)}\\ &= \frac{6+18i+8i+24i^2}{2^2+6^2}\\ &= \frac{6+26i-24}{4+16}\\ &= \frac{-18+24i}{20}\\ &= -0\cdot 9+1\cdot 2i\end{aligned}$$

2 Matrices

A *matrix* (plural — matrices) is a two-dimensional array — e.g.:

$$\begin{bmatrix} 2 & 7 & -3 \\ -4 & 0 & 0 \end{bmatrix}$$

This is referred to as a 2×3 matrix, as it has two rows and three columns. The individual entries in a matrix are identified by subscripts. E.g. the third entry in the second row of a matrix M would be identified by $M_{2,3}$. A generic 2×3 matrix M would be:

$$\begin{bmatrix} m_{1,1} & m_{1,2} & m_{1,3} \\ m_{2,1} & m_{2,2} & m_{2,3} \end{bmatrix}$$

2.1 Addition and Subtraction

Matrix addition/subtraction is just piecewise addition/subtraction of the elements. E.g.

$$\begin{bmatrix} 3 & -5 & 7 \\ 0 & 2 & -1 \\ 12 & 0 & -4 \\ -1 & 2 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 4 & 2 \\ -3 & -2 & 5 \\ -6 & 0 & -8 \\ -5 & 6 & 12 \end{bmatrix} = \begin{bmatrix} 3 & -1 & 9 \\ -3 & 0 & 4 \\ 6 & 0 & -12 \\ -6 & 8 & 12 \end{bmatrix}$$

$$\begin{bmatrix} 3 & -5 & 7 \\ 0 & 2 & -1 \\ 12 & 0 & -4 \\ -1 & 2 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 4 & 2 \\ -3 & -2 & 5 \\ -6 & 0 & -8 \\ -5 & 6 & 12 \end{bmatrix} = \begin{bmatrix} 3 & -9 & 5 \\ 3 & 4 & -6 \\ 18 & 0 & 4 \\ 4 & -4 & -12 \end{bmatrix}$$

The two matrices must have the same *dimensions* (here both are 4×3).

2.2 Multiplication

2.2.1 Scalar Multiplication

Scalar multiplication is multiplying a matrix by an ordinary number. Each entry in the matrix is simply multiplied by that number. E.g.:

$$3 \cdot \begin{bmatrix} 3 & -5 & 7 \\ 0 & 2 & -1 \\ 12 & 0 & -4 \\ -1 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 9 & -15 & 21 \\ 0 & 6 & -3 \\ 36 & 0 & -12 \\ -3 & 6 & 0 \end{bmatrix}$$

2.2.2 Matrix Product

Two matrices can also be multiplied together. If A and B are matrices, then $A * B$ is a new matrix in which the $(i, j)^{\text{th}}$ entry — the entry in the j^{th} column of the i^{th} row— is formed by taking the sum of pairwise products from A's i^{th} row and B's j^{th} column. E.g.:

$$\begin{bmatrix} \cdot & \cdot & \cdot \\ -2 & 6 & 5 \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{bmatrix} * \begin{bmatrix} \cdot & \cdot & 3 & \cdot \\ \cdot & \cdot & 7 & \cdot \\ \cdot & \cdot & 1 & \cdot \end{bmatrix} = \begin{bmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 41 & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}$$

since $-2 \times 3 + 6 \times 7 + 5 \times 1 = 41$

If A is a $k \times m$ matrix, then B must be a $m \times n$ matrix (and vice versa), and the result will be a $k \times n$ matrix

2.2.3 Tensor Product

The tensor product of two matrices is given by taking the scalar product of the second matrix with each of the entries of the first matrix, and putting the whole thing together into one large matrix. E.g.:

$$\begin{bmatrix} 2 & 0 \\ -1 & -2 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 2 & -1 \\ 3 & 0 \end{bmatrix} = \begin{bmatrix} 2 \cdot \begin{bmatrix} 2 & -1 \\ 3 & 0 \end{bmatrix} & 0 \cdot \begin{bmatrix} 2 & -1 \\ 3 & 0 \end{bmatrix} \\ -1 \cdot \begin{bmatrix} 2 & -1 \\ 3 & 0 \end{bmatrix} & -2 \cdot \begin{bmatrix} 2 & -1 \\ 3 & 0 \end{bmatrix} \\ 0 \cdot \begin{bmatrix} 2 & -1 \\ 3 & 0 \end{bmatrix} & 1 \cdot \begin{bmatrix} 2 & -1 \\ 3 & 0 \end{bmatrix} \end{bmatrix}$$

$$= \begin{bmatrix} 4 & -2 & 0 & 0 \\ 6 & 0 & 0 & 0 \\ -2 & 1 & -4 & 2 \\ -3 & 0 & -6 & 0 \\ 0 & 0 & 2 & -1 \\ 0 & 0 & 3 & 0 \end{bmatrix}$$

If A is a $k \times l$ matrix, and B is a $m \times n$ matrix, then $A \otimes B$ is a $km \times ln$ matrix.

2.3 Unary Operators

2.3.1 Transpose

The transpose, A^T, of a matrix A is obtained by setting $a^T_{i,j}$ to be $a_{j,i}$ — i.e. the j^{th} element in the i^{th} row of the transpose matrix is taken from the i^{th} element of the j^{th} row of the original matrix. E.g.

$$\begin{bmatrix} 3 & 8 & -2 & 0 \\ 6 & -5 & 0 & 7 \end{bmatrix}^T = \begin{bmatrix} 3 & 6 \\ 8 & -5 \\ -2 & 0 \\ 0 & 7 \end{bmatrix}$$

2.3.2 Conjugate

The conjugate (only relevant to complex matrices) is obtained by taking the piecewise conjugate of the elements of the original array. E.g.

$$\overline{\begin{bmatrix} 2+i & -3+2i & 4 \\ 0 & 2-3i & i \end{bmatrix}} = \begin{bmatrix} 2-i & -3-2i & 4 \\ 0 & 2+3i & -i \end{bmatrix}$$

2.3.3 Adjoint

The adjoint of a matrix is formed by taking the combination of the conjugate and the transpose. It doesn't matter which way round you do them. I.e.

$$A^{\dagger} = \overline{A^T} = \overline{A}^T$$

E.g.

$$\begin{bmatrix} 2+i & -3+2i & 4 \\ 0 & 2-3i & i \end{bmatrix}^{\dagger} = \begin{bmatrix} 2-i & 0 \\ -3-2i & 2+3i \\ 4 & -i \end{bmatrix}$$

3 Another Look at Circuits

In this section we look at representing circuits as matrices.

3.1 Bits

We can represent bits as matrices:

$$\textbf{false} \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \textbf{true} \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

A '$|b\rangle$' notation is often used to represent these bits:

$$\textbf{false} \equiv |0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \textbf{true} \equiv |1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Bit sequences are calculated as the *tensor product* of bit matrices:

$$|01\rangle \equiv |0\rangle \otimes |1\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ 0 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

Note: a byte (e.g. $|0110\ 1001\rangle$) would have 256 rows (in this example, the 105^{th} entry (only) would be a 1).

3.2 Gates

Gates are also defined as matrices.

3.2.1 Not

$$\textbf{not} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

and application of a gate to a boolean value is modelled by matrix multiplication. So

$$\textbf{not true} \equiv \textbf{not}\,|1\rangle \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} * \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \equiv |0\rangle \equiv \textbf{false}$$

3.2.2 And

$$\textbf{and} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

with

$$\textbf{and}\,|01\rangle \equiv \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} * \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \equiv |0\rangle$$

Note: can derive matrix from truth table

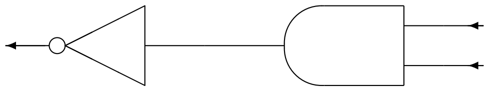
x	0	0	1	1	input
y	0	1	0	1	input
$x \wedge y$	0	0	0	1	output
$\|x \wedge y\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	output as matrix
	1	1	1	0	matrix expanded
	0	0	0	1	”

The matrix for the **and** gate is given by the bottom two lines of the table above.

3.3 Circuits

3.3.1 Sequential circuits

Sequential circuits are created using the matrix product. For example a **nand** gate is a sequence of an **and** gate and a **not** gate.



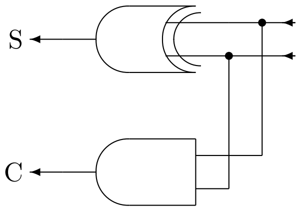
The **nand** matrix is the matrix product of the **and** matrix and the **not** matrix:

$$\textbf{nand} = \textbf{not} * \textbf{and} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} * \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

Note: the circuit has been drawn going right to left to emphasise that this is the order in which the matrix multiplication is written.

3.3.2 Parallel Circuits

Parallel circuits are constructed using the tensor product. For example a half-adder is constructed from an **and** gate and an **xor** gate in parallel.



So we take **xor** $\otimes$ **and**.

Note: Identify the "most significant bit" — here top to bottom.

The **and** matrix is $\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, and the **xor** matrix is $\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$ so the half-adder matrix is

$$\begin{aligned} & \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \\ = & \begin{bmatrix} 1 \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} & 0 \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} & 0 \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} & 1 \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \\ 0 \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} & 1 \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} & 1 \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} & 0 \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \end{bmatrix} \\ = & \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \end{aligned}$$