Chapter 2

Preliminaries

Let $\mathbb{C}$ denote the field of complex numbers. For $\alpha \in \mathbb{C}$ let $\overline{\alpha}$ or $\alpha^*$ denote the complex conjugate of $\alpha$. Let $\omega^x = e^{2\pi ix}$. Unit length complex numbers will be written as $\omega^x$, where $x \in [0, 1]$, since we will want to think in terms of fractions of 1 and want to hide the $2\pi$. The principal nth root of unity $\omega^{1/n} = e^{2\pi i/n}$ will be written as $\omega_n$. Since we will almost always use the notation $\omega$ instead of $e^{2\pi i}$, we will use $i$ as an index (for example, $\omega_n^i$, but not when expanding the $\omega$ notation into the $e^{2\pi i}$ form).

All vector spaces will be over the field $\mathbb{C}$. Vectors will be written in Dirac’s ket notation. In this notation the standard basis of $\mathbb{C}^p$ for a positive integer $p$ is $\{|0\}, \ldots, |p-1\\}$. When a vector has a name it is placed inside the ket, for example the vector $v$ is denoted $|v\rangle$. We will also use coefficient names that are the same whenever possible, for example $|v\rangle = \sum_{i=0}^{p-1} v_i |i\rangle$, $v_i \in \mathbb{C}$.

An inner product space is a vector space $V$ over $\mathbb{C}$ with a function $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$ satisfying
1. \( \forall |v| \in V, \langle |v|, |v| \rangle \geq 0 \), and \( \langle |v|, |v| \rangle = 0 \) iff \( |v| = 0 \).

2. \( \forall |v|, |w|, |x| \in V, \langle \alpha|v| + \beta|w|, |x| \rangle = \alpha\langle |v|, |x| \rangle + \beta\langle |w|, |x| \rangle \), \( \alpha, \beta \in \mathbb{C} \).

3. \( \forall |v|, |w| \in V, \langle |v|, |w| \rangle = \overline{\langle |w|, |v| \rangle} \).

A Hilbert space is an inner product space \( V \) that is complete with respect to the induced norm \( \| |v| \| = \sqrt{\langle |v|, |v| \rangle} \), i.e., for any sequence \( \{|v_n|\} \) with \( |v_n| \in V \), if \( \lim_{n,m \to \infty} \| |v_n| - |v_m| \| \to 0 \) then \( \lim_{n \to \infty} |v_n| \in V \). Some examples:

- \( \mathbb{C}^p \) where \( p \) is a positive integer and \( \langle |v|, |w| \rangle = \sum_{i=0}^{p-1} v_i \overline{w_i} \).

- \( l^2 \) is the set of finite norm sequences with \( \langle |v|, |w| \rangle = \sum_{i=-\infty}^{\infty} v_i \overline{w_i} \), i.e., the set of complex-valued sequences \( \{v_i\} \) such that \( \sum_{i \in \mathbb{Z}} |v_i|^2 < \infty \). \( l^2 \) has basis \( \{|e_i| \mid i \in \mathbb{Z}\} \), where \( e_i(i) = 1 \) and \( e_i(j) = 0 \) if \( j \neq i \).

- \( L^2 \) is the set of all finite length functions on \( [0,1] \) with \( \langle f, g \rangle = \int_0^1 f(x) \overline{g(x)} \, dx \), i.e., the set of complex-valued functions on \( [0,1] \) such that \( \int_0^1 |f(x)|^2 < \infty \). \( L^2 \) has basis \( \{f(x) = \omega^{nx} \mid n \in \mathbb{Z}\} \).

The Fourier transform is a norm preserving map on \( \mathbb{C}^p \). Given a vector \( |v| = \sum_i v_i |i| \in \mathbb{C}^p \), the Fourier transform is the vector \( |\hat{v}| = \frac{1}{\sqrt{p}} \sum_i \hat{v}_i |i| \), where \( \hat{v}_i = \sum_j \omega_i^j v_i \).

The Fourier transform is also a distance preserving map from \( L^2 \) to \( l^2 \). Given a function \( f \in L^2 \), the Fourier transform of \( f \) is the sequence \( \{\hat{f}(n)\} \), where \( \hat{f}(n) = \langle f, e_n \rangle = \int_0^1 \omega^{nx} f(t) \, dt \).

The inverse is \( f(x) = \sum_{n=-\infty}^{\infty} \hat{f}(n) \omega^{nx} \).

A quantum state with \( n \) qubits is represented by a complex-valued unit vector in \( \mathbb{C}^{2^n} \), i.e. \( \sum_{i=0}^{2^n-1} |v_i| \), where \( \sum_{i=0}^{2^n-1} |v_i|^2 = 1 \). A probability distribution \( D_{|v|} \) is induced by measuring \( |v| \) and is given by \( D_{|v|}(i) = |v_i|^2 \).
All groups $G$ will be finite. If $H \subseteq G$ is a subgroup and $c \in G$ is a coset representative, the coset state is $|cH| = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |ch|$. The Hilbert space in this case is $\mathbb{C}[G]$, indexed by elements of the group. Indicator functions of one element or of a set are written as:

- For any $s$, $\delta_s(x) = \begin{cases} 1 & \text{if } x = s \\ 0 & \text{otherwise} \end{cases}$

- For any set $S$, $\delta_S(x) = \begin{cases} 1 & \text{if } x \in S \\ 0 & \text{otherwise} \end{cases}$

A character $\chi$ of an abelian group $G$ is a group homomorphism from $G$ into the multiplicative group of complex numbers of norm 1. The dual group $\hat{G}$ of an abelian group $G$ is the set of all characters of $G$. The group operation is pointwise multiplication of functions. Given a subgroup $H \subseteq G$, the dual of $G/H$ in $G$ is $H^\perp = \hat{G}/\hat{H} = \{ \chi \in \hat{G} | \chi(h) = 1 \text{ for all } h \in H \}$. 