8.372 Quantum Information Science III **Fall 2024**

Lecture 15: October 31, 2024

Scribe: Daniel Z. Lee *Unitary k-designs and Representation Theory*

15.0 Context and recap from last few lectures

In the last several lectures, we've been discussing random states/unitaries as well as state/unitary k-designs. In particular, in order to even be able to talk about constructing these designs, we need to understand what we're even trying to achieve: that is, what the moments of truly random states and unitaries are. For random states, we directly computed these using some Gaussian integration tricks.

In this lecture, we'll build the background for a more principled approach to these calculations.

15.1 What we know about unitary k-designs

For 1 designs, we have the Pauli ensemble, and for 2-designs we know that random cliffords or free fermion rotations work (though we haven't done a proof yet for the 2-design claims).

Note that we also actually know that random Cliffords are at least 3 designs (and sometimes 4 designs for some d, where d is the dimension of your hilbert space)

Random circuits for larger k

For larger k, we don't have a systematic way of constructing *exact* k-designs. One approach to *approximate* k-designs is using random circuits.

Proposition 15.1.1 (informal)**.** *If you place independent Haar random 2-qubit gates in a brickwork circuit in 1D with depth* $n\text{poly}(k)\log\frac{1}{\epsilon}$*, then this is an* ϵ *approximate* k*-design.*

Comments

- One can also often get away with choosing the 2 qubit gates uniformly from any *universal* gate set.
- Aram made the comment that for most purposes, 2 designs are sufficient, although higher k can improve on things like concentration of entanglement entropy
- Are there interesting state designs which don't come from unitary designs (since all the ones we've seen so far do come from unitary designs)? It turns out that there's a nice class of examples called *phase states* which are defined as

$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1} e^{i\phi(x)}\,|x\rangle$$

for some choice of ϕ. These are nice for applications because they're often efficiently computable. E.g. they're used in Ji, Liu, Song 2018 as a construction of pseudorandom quantum states.

15.2 Representation Theory

Here, we'll present the basics of representation theory, motivated by this connection we've observed previously between invariant subspaces and randomizing maps.

15.2.1 What is a representation?

Definition 15.2.1 (Representation)**.** *A representation (R, V) for a group G is a homomorphism $R : G \to Aut(V)$ that sends a group to an operator on V. Homomorphism meaning that for any $g, h \in G$, $R(gh) = R(g)R(h)$ where on the RHS multiplication just means standard matrix multiplication/function composition.*

It turns out WLOG, we can take $R : G \to U(V)$ do only use unitary operators

It's common practice to refer to a representation just by its vector space V.

15.2.2 Basic definitions

Equivalence. We say two representations $(R_1, V_1), (R_2, V_2)$ are equivalent if there exists an invertible $T : V_1 \to V_2$ such that for every $g \in G$,

$$TR_1(g) = R_2(g)T^{-1}$$

That is, if there exists a uniform change of basis that takes all your $R_1(g)$s to $R_2(g)$s.

Reducibility. We say that a representation is reducible if there's a basis in which every representation $R(g)$ is block diagonal.

Equivalently, a representation is reducible if it has an *invariant subspace.* That is, if there's a non-trivial linear subspace $W \subset V$ s.t. $\forall g, R(g)W = W$.

Irreducible Representations (Irreps). A representation is called irreducible if..... it is not reducible!

Let $\hat{G}$ denote all the irreducible representations of a group G.

Any representation can be decomposed into irreducible representations as

$$V \cong \sum_{\lambda \in \hat{G}} V_\lambda \otimes \mathbb{C}^{m_\lambda}$$

where m_λ is an integer denoting the multiplicity of irrep λ.

Group algebra. In particular, the *group algebra* $\mathbb{C}[G]$ is a representation with

- orthonormal basis vectors $\{|g\rangle : g \in G\}$
- $R_L(x)(g) = |xg\rangle$
- We label this with L, because there's also actually a right action $R_R(x)(g) = |gx^{-1}\rangle$

The following is an important fact:

$$\mathbb{C}[G] = \bigoplus_{\lambda \in \hat{G}} V_\lambda \otimes V_\lambda^*$$

One quick consequence of this is that $\dim(\mathbb{C}[G]) = \sum_\lambda \dim(V_\lambda)^2$

Note that this can be somewhat seen as a consequence of the existance of these two representations R_L and R_R which commute with each other.

Dual representation

(R^*, V^*) is defined by $R^*(g) = R(g^{-1})^T$. For example, if you take the representation $U \to U^{\otimes n}$, then the dual representation is $U \to (U^*)^{o \times n}$ where U^* is the complex conjugate (as opposed to conjugate transpose).

15.2.3 Group/Quantum Fourier Transform

Abelian fourier transform stated in fancy language. For an abelian group A, all its irreducible representations are one dimensional. This is because, since all the matrices in the representation commute with each other, they are all simultaneously diagonalizable, and so every basis vector gives an invariant subspace. Applying the yellow box above, this in particular means that $|\hat{G}| = |G|$.

The fourier transform can be written as:

Definition 15.2.2 (Abelian fourier transform)**.** *Let A be a finite abelian group, and $\{R_\lambda\}_\lambda \in \hat{A}$ its irreducible representations. The fourier transform maps basis states as follows:*

$$|a\rangle \mapsto \frac{1}{\sqrt{|A|}} \sum_{\lambda \in \hat{A}} R_\lambda(a) |\lambda\rangle$$

This can be inverted by:

$$|\lambda\rangle \mapsto \frac{1}{\sqrt{|A|}} \sum_{a \in A} R_\lambda(a)^* |a\rangle$$

The unitarity of this transform is equivalent to the fact that these R_λs are mutually orthogonal.

Quantum/non-abelian version The reason the abelian setting was so nice was that, because $|A| = |\hat{A}|$, there was a natural way to get a basis out of the set of representations.

In general, this is not the case (any non-abelian group will have at least one higher dimensional representation). Instead, each λ gives us a $(\dim V_\lambda)^2$ dimensional space, and we pick some particular basis for each.

Definition 15.2.3 (Group fourier transform)**.** *Let G be a finite group, and $\{R_\lambda\}_{\lambda \in \hat{G}}$ its irreducible representations. The group fourier transform maps basis states as follows:*

$$|g\rangle \mapsto \frac{1}{\sqrt{|G|}} \sum_{\lambda \in \hat{G}} |\lambda\rangle \otimes \sum_{i,j \in [\dim V_\lambda]} R_\lambda(g)_{ij} |i\rangle \otimes |j\rangle$$

where $R_\lambda(g)_{ij}$ refers to the i, j matrix entropy of the representation.

The inverse fourier transform maps:

$$|\lambda\rangle |i\rangle |j\rangle \mapsto \frac{1}{\sqrt{|G|}} \sum_g R_\lambda(g)_{ij} |g\rangle$$

Unitary follows from the Schur orthogonality relations, which tell us that the set of $\{(R_\lambda(g)_{ij})_g\}_{\lambda,i,j}$ are all mutually orthogonal.

15.2.4 Schur's Lemma and the kth moments of a random state

In the last part of the lecture, we'll circle back to random states. In particular, we'll use Schur's lemma to prove that the kth moment of a random state is indeed the (normalized) projector onto the symmetric subspace.

Lemma 15.2.1 (Schur's Lemma)**.** *Let V_μ, V_ν be irreps of G. Let $L(V_\mu, V_\nu)^G$ be the set of G invariant maps from V_μ to V_ν (that is, maps which preserve the group action). There are two possibilities:*

1. *If $\mu \cong \nu$, then $L(V_\mu, V_\nu)^G = \mathbb{C}I$ (i.e. the set of all scalar multiples of the identity)*
2. *Otherwise, $L(V_\mu, V_\nu)^G = 0$*

In particular, this tells us that for any irrep V_μ, the only linear transform which commutes with all of the representations is the identity.

This let's us obtain as a corollary the kth moments of a random state.

Corollary 15.2.1.

$$\mathbb{E}[|\psi\rangle \langle\psi|^{\otimes k}] = \frac{\Pi_{sym}}{\operatorname{Tr} \Pi_{sym}}$$

Proof. First we observe that $\mathbb{E}[|\psi\rangle \langle\psi|^{\otimes k}]$ commutes with $U^{\otimes k}$ for any U.

$$\begin{aligned} U^{\otimes k} \mathbb{E}[|\psi\rangle \langle\psi|^{\otimes k}] U^{\dagger \otimes k} &= \mathbb{E}[U^{\otimes k} |\psi\rangle \langle\psi|^{\otimes k} U^{\dagger \otimes k}] \\ &= \mathbb{E}[|\psi\rangle \langle\psi|^{\otimes k}] \end{aligned}$$

This implies that $\mathbb{E}[|\psi\rangle \langle\psi|^{\otimes k}]$ must act proportionally to the identity on an irrep of the representation $U^{\otimes k}$.

Next, we observe that

$$\Pi_{sym} \mathbb{E}[|\psi\rangle \langle\psi|^{\otimes k}] = \mathbb{E}[|\psi\rangle \langle\psi|^{\otimes k}] \Pi_{sym} = \mathbb{E}[|\psi\rangle \langle\psi|^{\otimes k}]$$

This implies that $\mathbb{E}[|\psi\rangle \langle\psi|^{\otimes k}]$ only acts non-trivially on the symmetric subspace.

Finally, we use without proof the fact that $(U^{\otimes k}, \operatorname{Sym}^k \mathbb{C}^d)$ is an irreducible representation to conclude that $\mathbb{E}[|\psi\rangle \langle\psi|^{\otimes k}]$ must be proportional to the identity on the symmetric subspace (i.e. Π_{sym}).

□