Twirling and Unitary Designs

Name: Nate Stemen (20906566)
Email: nate@stemen.email

Due: March 31, 2021
Course: AMATH 876

Contents

In these notes we work to understand the action of quantum twirling and it's implementation which leads naturally into the development of unitary t-designs. Throughout we provide some of the mathematical detail needed to base our work on.

1 Preliminaries

It'll be helpful to have some concepts defined before we try and understand unitary designs in full.

Definition 1.1. Let P_1 be the standard 1 qubit Pauli group generated by X, Y, Z as seen in Emerson [2021]. Define, in general, the (n qubit) **Pauli Group** to be the n-fold tensor product of P_1 with itself. That is $P_n = P_1^{\otimes n}$. This naturally forms a group under matrix multiplication and can be shown to be generated by X_i and Z_i (where i ranges to n).

Definition 1.2. The **Clifford group** is the set of unitary matrices[1] that leave the Pauli group unchanged upon conjugation:

$$C_n := \left\{ U \in \mathsf{U}(2^n) : U P_n U^\dagger = P_n \right\}. \tag{1}$$

Again, this naturally forms a group under matrix multiplication.

2 Twirling

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be Hilbert spaces, and denote by $\mathrm{L}(\mathcal{H})$ by the set of linear operators on $\mathcal{H}$. Given a quantum channel $\Lambda : \mathrm{L}(\mathcal{H}_A) \to \mathrm{L}(\mathcal{H}_B)$, then we can define twirling Λ with respect to the unitary group as

$$\mathcal{T}[\Lambda](\rho) := \int_{\mathsf{U}(n)} U^\dagger \Lambda(U \rho U^\dagger) U \,\mathrm{d}\eta(U) \tag{2}$$

[1] Equipped with the group operation of matrix multiplication

where η is the unique unitary invariant measure on $\mathsf{U}(n)$ called the Haar measure. In fact a Haar measure can be constructed on any locally compact topological group, but we will not go further than the unitary group here. To better understand this integral we will have a quick aside on what the Haar measure is, and why it's necessary.

2.1 *The* Haar Measure

The set of all ideal operations that one can perform on n qubits—also known as the Unitary group $\mathsf{U}(n)$—has some very nice properties that allow us to define integration on this space. In particular the group is *compact* which can be seen from the fact that $UU^\dagger = \mathbb{1}$ for all $U \in \mathsf{U}(n)$ and hence the column vectors $U = \begin{bmatrix} u_1 & \cdots & u_n \end{bmatrix}$ are orthonormal for all U. Thus each U is characterized by n points on the surface of a hypersphere. This implies, when embedded into $\mathbb{R}^{2n^2}$, $\mathsf{U}(n)$ is a space of finite volume, and by the usual Lebesgue integral in $\mathbb{R}^N$, we can integrate over $\mathsf{U}(n)$. That said, this sense of measure inherited from $\mathbb{R}^N$ is not invariant under the action of an element $U \in \mathsf{U}(n)$. To make it invariant, we use something similar to "Weyl's Unitary Trick" to average measure over the action of each element in $\mathsf{U}(n)$. One can then show this is first of all invariant under unitary action[2], and is also the unique up to a complex number which explains why we say *the* Haar measure.

2.2 A simple example

Suppose we have a 2-level quantum system represented by ρ. We can then take the identity channel $\hat{I}(\rho) = \mathbb{1}\rho\mathbb{1} = \rho$ and twirl it to see it's effect. Here we denote superoperators with a hat $\hat{U}$ and their action is defined as $\hat{U}(\rho) = U\rho U^\dagger$.

$$\mathcal{T}[\hat{I}](\rho) = \int_{\mathsf{U}(2)} U^\dagger \hat{I}(U\rho U^\dagger) U \, \mathrm{d}\eta(U) = \int_{\mathsf{U}(2)} \rho \, \mathrm{d}\eta(U) = \rho = \hat{I}(\rho) \tag{3}$$

2.3 Implementing Twirls

As we've seen twirling quantum channels can yield lots of useful information about a channel and it's properties, but the question of implementing such a thing remains. As modern quantum computers stand, doing an arbitrary unitary $U \in \mathsf{U}(n)$ is nearly impossible to do efficiently. In Emerson et al. [2003] the authors find an algorithm to implement a random unitary gate using $\mathcal{O}\left(n^2 2^{2n}\right)$ single and double qubit gates. Not only is this exponential, but if we had to do this for all unitaries (or even an ε-net for that matter) we would need significantly more compute power than we have now. This leads naturally to the question: can we find a finite set of unitaries that "represent" or "simulate" the entire unitary group? If we could such a set that reproduced some of the statistical properties of $\mathsf{U}(n)$, then we might have a way to physically realize a twirl. Luckily, mathematicians have been studying the objects we need for sometime, albeit in different contexts, in the form of designs.

[2]By both multiplication from the left and right.

3 Designs

The original concept of a design came in the form of spherical t-designs introducted by Delsarte et al. [1977]. In particular the authors were interested in real polynomials whose average over a set of points in real Euclidean space was invariant under *all* orthogonal transformations. This notion was shown to be equivalent to sets of N points $x_i \in \mathbb{R}^n$ such that for all real polynomials f of degree t we have

$$\int_{S^{n-1}} f(x)\, \mathrm{d}\omega(x) = \frac{1}{N}\sum_{i=1}^{n} f(x_i) \tag{4}$$

where $S^{n-1} \subset \mathbb{R}^n$ is the $(n-1)$-sphere, and $\mathrm{d}\omega$ is an appropriated normalized measure on S^{n-1}. In other words, we can find the average values of any polynomial on the sphere by looking at these particular n points.

In Renes et al. [2004] the authors generalized this idea to polynomial functions operating on quantum states $|\psi\rangle$ instead of points in Euclidean space. Again in Dankert et al. [2009], the idea is taken a step further to polynomial function of unitary operators U. In particular Dankert et al. [2009] gives the following definition.

Definition 3.1. A **unitary t-design** (of dimension n) is a finite set $\{U_i\}_{i=1}^k \subset \mathsf{U}(n)$ such that for all polynomials $f_{(t,t)}(U)$ of degree t in the matrix elements of U, and degree t in the complex conjugate of those matrix elements we have

$$\int_{\mathsf{U}(n)} f_{(t,t)}(U)\, \mathrm{d}\eta(U) = \frac{1}{k}\sum_{i=1}^{k} f_{(t,t)}(U_i). \tag{5}$$

Here η represents the unique unitary invariant measure called the Haar measure on $\mathsf{U}(n)$.

A particularly interesting example is $t = 2$-designs where we have the following equivalent characterziation due to Gross et al. [2007].

Theorem 3.1. A set $\{U_i\}_{i=1}^k$ is a unitary 2-design if and only if for any quantum channel Λ we have

$$\frac{1}{k}\sum_{i=1}^{k} U_k^\dagger \Lambda(U_k \rho U_k^\dagger) U_k = \int_{\mathsf{U}(n)} U^\dagger \Lambda(U\rho U^\dagger) U\, \mathrm{d}\eta(U) \tag{6}$$

This result gives us a much more manageable way to implement a twirling operation since we no longer have to try to implement every possible unitary. The next natural question to ask then is do we know of any 2-designs? Thankfully Zhu [2015] showed that in fact the Clifford group defined in definition 1.2 is a 3-design. Well a 3-design is not a 2-design, but thankfully if we have a t-design we have *for free* an s-design for an $s \leq t$ by the fact that a degree s polynomial can always be a degree t polynomial with 0 as coefficients for any degree $n > s$.

The Clifford group is an important group in quantum information theory not just because it normalizes the Pauli group, but as shown in Gottesman [1998], circuits using only the Clifford group can be efficiently simulated on a classical computer. Clifford circuits have also been shown to to be in a much smaller computational complexity class ($\oplus$L) than the full power of quantum computers (BQP) Aaronson and Gottesman [2004].[3] These facts demonstrate that even though the Clifford group "represents" the entire unitary group in some statistical ways, it is not strong enough to do universal quantum computation.

[3]Although, like many things in theoretical computer science, they have not been shown to be completely distinct classes, even though it is believed by many in the field.

Bibliography

Joseph Emerson. Theory of quantum systems: From mathematical foundations to experimental methods, March 2021.

Joseph Emerson, Yaakov S. Weinstein, Marcos Saraceno, Seth Lloyd, and David G. Cory. Pseudo-random unitary operators for quantum information processing. *Science*, 302(5653):2098–2100, 2003. ISSN 0036-8075. doi: 10.1126/science.1090790. URL https://science.sciencemag.org/content/302/5653/2098.

P. Delsarte, J.M. Goethals, and J.J. Seidel. Spherical codes and designs. *Geometriae Dedicata*, 1977. URL https://doi.org/10.1007/BF03187604.

Joseph M. Renes, Robin Blume-Kohout, A. J. Scott, and Carlton M. Caves. Symmetric informationally complete quantum measurements. *Journal of Mathematical Physics*, 45(6):2171–2180, 2004. URL https://doi.org/10.1063/1.1737053.

Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Phys. Rev. A*, 80:012304, Jul 2009. doi: 10.1103/PhysRevA.80.012304. URL https://link.aps.org/doi/10.1103/PhysRevA.80.012304.

D. Gross, K. Audenaert, and J. Eisert. Evenly distributed unitaries: On the structure of unitary designs. *Journal of Mathematical Physics*, 48:052104–052104, 2007. doi: 10.1063/1.2716992.

Huangjun Zhu. Multiqubit clifford groups are unitary 3-designs. *Physical Review A*, 96, 10 2015. doi: 10.1103/PhysRevA.96.062336.

Daniel Gottesman. The Heisenberg Representation of Quantum Computers. *arXiv e-prints*, art. quant-ph/9807006, July 1998.

Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Phys. Rev. A*, 70: 052328, 11 2004. doi: 10.1103/PhysRevA.70.052328. URL https://link.aps.org/doi/10.1103/PhysRevA.70.052328.