Math 599: The Locally Compact Haar Measure and the Fully Quantum Slepian Wolf Protocol

Eric Hanson (# 260444061)

McGill University, Montreal, Quebec, Canada
(Dated: December 16, 2013)

CONTENTS

I. INTRODUCTION

The Haar measure allows integration over topological groups, which has many applications; for example, the use of the Haar measure in proving the Fully Quantum Slepian Wolf (or state transfer) protocol fundamental to quantum information theory is briefly discussed in section VI. But first we build the definitions necessary to define the Haar measure, and state some fundamental theorems. Next, we show a left Haar measure exists on locally compact Hausdorff topological groups, and is unique (up to scale) on such groups which are also σ-compact. While of course the Haar measure is unique up to scale on all locally compact Hausdorff groups, the simpler case admits an elegant proof. Lastly, the relationship between the right and left Haar measure is investigated.

II. PRELIMINARIES

The following definitions are taken from Folland [Fol99].

Def. 1 An algebra of sets on a set X is a non-empty collection of subsets that is closed under finite unions and complements.

Def. 2 A σ-algebra is an algebra of sets on X that is closed under countable unions.

Def. 3 If (X, τ) is a topological space, then the intersection of all σ-algebras containing τ is called the Borel σ-algebra. An element of the Borel σ-algebra is called a Borel set.

Remark. It's easy to see that this is truly a σ-algebra.

Def. 4 Let X be a set and $\mathcal{M}$ a σ-algebra on $\mathcal{M}$. Then a function $\mu : \mathcal{M} \to [0, \infty]$ is called a measure on $\mathcal{M}$ if

1. $\mu(\varnothing) = 0$
2. For any countable family $\{E_j\}_1^\infty$ of disjoint sets in $\mathcal{M}$, $\mu\left(\bigcup_{j=1}^\infty E_j\right) = \sum_{j=1}^\infty \mu(E_j)$.

Def. 5 A Radon measure for a topological space (X, τ) is a measure on the Borel σ-algebra of (X, τ) (a Borel measure) that is finite on all compact sets, and is

Inner regular on open sets:

$$\mu(V) = \sup\{\mu(K) : K \subset V,\, K \text{ compact}\} \tag{1}$$

for any open set V, and

Outer regular on Borel sets:

$$\mu(E) = \inf\{\mu(U) : U \supset E,\, U \text{ open}\} \tag{2}$$

for any Borel set E.

Def. 6 $C_c(X)$ is the space of all continuous functions on a topological space (X, τ) with compact support.

Additionally,

$$C_c^+ := \{f \in C_c(X) : f \geq 0 \text{ and } \|f\| > 0\}$$

where the inequality $f \geq 0$ is taken pointwise (as will be the convention for the rest of the document).

Def. 7 We define the characteristic function of $E \subset X$ as

$$\chi_E = \begin{cases} 1 & \text{if } x \in E \\ 0 & \text{if } x \notin E \end{cases}$$

Def. 8 Given a function $f \in C_c(X)$ and an open set $U \subset X$, we write $f \prec U$ if $0 \leq f \leq 1$ and $\text{supp}(f) \subset U$.

Remark. The requirement $f \prec U$ is stronger than $0 \leq f \leq \chi_U$, because the second only requires $\text{supp}(f) \subset \overline{U}$.

Theorem 9 ***(Riesz Representation Theorem)*** *If I is a positive linear functional on $C_c(X)$, there is a unique Radon measure μ on X such that $I(f) = \int f \, \mathrm{d}\mu$ for all $f \in C_c(X)$. Moreover, μ satisfies*

$$\mu(U) = \sup\{I(f) : f \in C_c(X), f \prec U\} \text{ for all open } U \subset X \tag{3}$$

and

$$\mu(K) = \inf\{I(f) : f \in C_c(X), f \geq \chi_K\} \text{ for all compact } K \subset X \tag{4}$$

Def. 10 A topological group is a group endowed with a topology such that the group operations are continuous.

Def. 11 A left Haar measure on a topological group G is a nonzero Radon measure that is left-invariant:

$$\mu(xE) = \mu(E)$$

for all $x \in G$ and all Borel sets E.

A right Haar measure on a topological group G is similarly a nonzero Radon measure that is right invariant: $\mu(Ex) = \mu(E)$ for all $x \in G$ and all Borel sets E.

Lemma 12 If $I : G \to \mathbb{R}$ is left-invariant and satisfies the conditions of the Riesz Representation Theorem, then a left Haar measure exists.

Proof. Let μ be the unique Radon measure given by the Reisz Representation theorem; that is, μ satisfies equations eqs. (1) to (4).

Then we have, for any open set $U \subset G$,

$$\mu(U) = \sup\{I(f) : f \in C_c(G), f \prec U\}$$

Since I is left invariant, for any $y \in G$, we have

$$\mu(U) = \sup\{I(L_y f) : f \in C_c(G), f \prec U\} = \sup\{I(f) : f \in C_c(G), L_{y^{-1}} f \prec U\} \tag{$\star$}$$

We have $0 \leq L_y f \leq 1 \iff 0 \leq f \leq 1$. Consider $\mathrm{supp}(L_{y^{-1}} f) \subset U$. That is, for $x \in G$, $f(yx) \geq 0 \implies x \in U$. This is the same as $\forall\, x \in G$, $f(x) \geq 0 \implies y^{-1}x \in U \iff x \in yU$. So $\mathrm{supp}(L_{y^{-1}} f) \subset U \implies \mathrm{supp}(f) \subset yU$.

Then we have, by ($\star$),

$$\mu(U) = \sup\{I(f) : f \in C_c(G), f \prec yU\} = \mu(yU)$$

for any open set U.

Then, by outer regularity (equation 2), we have for any Borel set E, and $y \in G$,

$$\begin{aligned}\mu(E) &= \inf\{\mu(U) : U \supset E,\, U \text{ open}\} = \inf\{\mu(yU) : U \supset E,\, U \text{ open}\}\\ &= \inf\{\mu(yU) : yU \supset yE,\, yU \text{ open}\} = \mu(yE)\end{aligned}$$

So μ is a left Haar measure. □

Def. 13 A locally compact topological space is one in which every point has a compact neighborhood. A locally compact topological group is, as one would expect, a topological group that is also locally compact as a topological space.

Notation: For a function on a topological group G, $f : G \to \mathbb{R}$, set $\|f\| = \sup_{x \in G} |f(x)|$, the supremum norm.

Def. 14 We say a function $f : G \to \mathbb{R}$ on a topological group G is left uniformly continuous (resp. right uniformly continuous) if for every $\varepsilon > 0$, there is a neighborhood V of e such that $\|L_y f - f\| < \varepsilon$ (resp., $\|R_y f - f\| < \varepsilon$) for $y \in V$.

Proposition 15 If $f \in C_c(G)$ for a locally compact topological group, then f is left and right uniformly continuous.

Remark. The proof is very similar to that given in class of the same result for compact groups.

Finally, for completeness, we have

Theorem 16 ***(Tychonoff's Theorem)*** *If $\{X_\alpha\}_{\alpha\in A}$ is any family of compact topological spaces, then $X = \prod_{\alpha\in A} X_\alpha$ (with the product topology) is compact.*

III. THE EXISTENCE OF THE LEFT HAAR MEASURE

The idea of the proof is of course, to find a left-invariant positive linear functional (i.e., something that acts like an integral), and then apply lemma 12. To do this, we develop a notion of relative size between a Borel set and an open set, and reformulate the notion in terms of functions with compact support to find an approximately linear left-invariant positive functional, from which we can find an truly linear functional by exploiting local compactness.

Let G be a Hausdorff locally compact topological group.

Def. 17 For a Borel set E and $V \subset G$ open and non-empty, define $(E : V)$ as

$$(E : V) = \inf\{\#(A) : E \subset \bigcup_{x\in A} xV\}$$

Remark. $(E : V)$ is the smallest number of left translates of V needed to cover E, so it gives an estimate of the relative sizes of the two sets.

We can formulate this in terms of functions: For $f, \varphi \in C_c^+(G)$, the set $\left\{x : \varphi(x) > \frac{1}{2}\|\varphi\|\right\}$ is open (by continuity) and non-empty (since the norm is the supremum). Since $\operatorname{supp}(f)$ is compact, we can cover it with finite subcover of tranlations of this set:

Since $\{x : \varphi(x) > \frac{1}{2}\|\varphi\|\}$ is non-empty, pick $x_0 \in \left\{x : \varphi(x) > \frac{1}{2}\|\varphi\|\right\}$. Then

$$\operatorname{supp}(f) \subset \bigcup_{y\in\operatorname{supp}(f)} y \subset \bigcup_{y\in\operatorname{supp}(f)} \left\{yx_0^{-1}x : \varphi(x) > \frac{1}{2}\|\varphi\|\right\}$$

Sending $x \to x_0y^{-1}$

$$\operatorname{supp}(f) \subset \bigcup_{y\in\operatorname{supp}(f)} \left\{x : \varphi\left(x_0y^{-1}x\right) > \frac{1}{2}\|\varphi\|\right\} = \bigcup_{y\in\operatorname{supp}(f)} \left\{x : L_{yx_0^{-1}}\varphi(x) > \frac{1}{2}\|\varphi\|\right\}$$

By compactness of $\operatorname{supp} f$, we can find $x_1, \ldots, x_n \in G$ such that

$$\operatorname{supp}(f) \subset \bigcup_{j=1}^{n} \left\{x : L_{x_j}\varphi(x) > \frac{1}{2}\|\varphi\|\right\}$$

then for $x \in \operatorname{supp}(f)$, for some j, $f(x) \le \|f\| = \|f\|\frac{2\|\varphi\|}{2\|\varphi\|} \le \|f\|\frac{2}{\|\varphi\|}L_{x_j}\varphi(x)$.

Hence, $f < 2\frac{\|f\|}{\|\varphi\|}\sum_{j=1}^{n} L_{x_j}\varphi$.

We thus obtain a finite infimum over such left translates, which Folland describes as a "Haar covering number" of f with respect to φ:

Def. 18 For $f, \varphi \in C_c^+$,

$$(f : \varphi) = \inf\left\{\sum_{j=1}^{n} c_j : f \le \sum_{j=1}^{n} c_j L_{x_j}\varphi \text{ for some } n \in \mathbb{N} \text{ and } x_1, \ldots, x_n \in G\right\}$$

Remark. $(f:\varphi) \geq \frac{\|f\|}{\|\varphi\|} > 0$, as, choosing x_0 where the continuous f achieves its maximum on compact $\mathrm{supp}(f)$, $f(x_0) = \|f\| \geq \|f\| \frac{\varphi(x_0)}{\|\varphi\|}$.

Lemma 19 (Properties of $(f:\varphi)$) For $f, \varphi, g \in C_c^+(G)$, we have

1. $(f:\varphi) = (L_x f:\varphi)$ *for any* $x \in G$
2. $(cf:\varphi) = c(f:\varphi)$ *for* $c > 0$
3. $(f+g:\varphi) \leq (f:\varphi) + (g:\varphi)$
4. $(f:\varphi) \leq (f:g)(g:\varphi)$

Proof of lemma.

1. $(f:\varphi) = (L_x f:\varphi)$ for any $x \in G$:

$$(f:\varphi) = \inf_{\{x_j\}} \left\{ \sum_{j=1}^n c_j : f \leq \sum_{j=1}^n c_j L_{x_j}\varphi \right\} = \inf_{\{x_j\}} \left\{ \sum_{j=1}^n c_j : f \leq \sum_{j=1}^n c_j L_{x^{-1}x_j}\varphi \right\}$$
$$= \inf_{\{x_j\}} \left\{ \sum_{j=1}^n c_j : L_x f \leq \sum_{j=1}^n c_j L_{x_j}\varphi \right\} = (L_x f:\varphi)$$

2. $(cf:\varphi) = c(f:\varphi)$ for $c > 0$:

$$(cf:\varphi) = \inf_{\{x_j\}} \left\{ \sum_{j=1}^n c_j : cf \leq \sum_{j=1}^n c_j L_{x_j}\varphi \right\} = \inf_{\{x_j\}} \left\{ \sum_{j=1}^n c_j : f \leq \sum_{j=1}^n \frac{c_j}{c} L_{x_j}\varphi \right\}$$
$$= \inf_{\{x_j\}} \left\{ \sum_{j=1}^n cc_j : f \leq \sum_{j=1}^n c_j L_{x_j}\varphi \right\} = c \inf_{\{x_j\}} \left\{ \sum_{j=1}^n c_j : f \leq \sum_{j=1}^n c_j L_{x_j}\varphi \right\} = c(f:\varphi)$$

3. $(f+g:\varphi) \leq (f:\varphi) + (g:\varphi)$: Fix $\varepsilon > 0$. Then, choosing convenient labels, $\exists\, c_j$ and $x_j \in G$, $j = 1, 2, \ldots, m$ with $f \leq \sum_{j=1}^m c_j L_{x_j}\varphi$ such that $\sum_{j=1}^m c_j \leq (f:\varphi) + \varepsilon$, and c_j, $x_j \in G$ $j = m+1, m+2, \ldots, n$ with $g \leq \sum_{j=m+1}^n c_j L_{x_j}\varphi$ such that $\sum_{j=m+1}^n c_j \leq (g:\varphi) + \varepsilon$ (as $(f:\varphi), (g:\varphi)$ are infima).

   So, $\sum_{j=1}^n c_j \leq (f:\varphi) + (g:\varphi) + 2\varepsilon$, but $f + g \leq \sum_{j=1}^n c_j L_{x_j}\varphi$, so $(f+g,\varphi) \leq (f:\varphi) + (g:\varphi) + 2\varepsilon$; sending $\varepsilon \to 0$ yields the result.

4. $(f:\varphi) \leq (f:g)(g:\varphi)$: the proof is similar to (3). Fix $\varepsilon > 0$. Then we know there exists c_j and $x_j \in G$, $j = 1, 2, \ldots, m$ with $f \leq \sum_{j=1}^m c_j L_{x_j} g$ such that $\sum_{j=1}^m c_j \leq (f:g) + \varepsilon$, and d_k, $y_k \in G$ $k = 1, 2, \ldots, n$ with $g \leq \sum_{k=1}^n d_k L_{y_k}\varphi$ such that $\sum_{k=1}^n d_k \leq (g:\varphi) + \varepsilon$ (as $(f:\varphi), (g:\varphi)$ are infima).

   So, $\sum_{j=1}^m \sum_{k=1}^n c_j d_k \leq (f:g)(g:\varphi) + O(\varepsilon)$.

   On the other hand, we have $f \leq \sum_{j=1}^m c_j L_{x_j} g \leq \sum_{j=1}^m \sum_{k=1}^n c_j d_k L_{x_j} L_{y_k}\varphi$, that is,

$$\sum_{j=1}^m \sum_{k=1}^n c_j d_k \in \left\{ \sum_{j=1}^n c_j : f \leq \sum_{j=1}^n c_j L_{x_j}\varphi \right\}$$

so, as $(f:\varphi)$ is the infimum over that set,

$$(f:\varphi) \le \sum_{j=1}^{m}\sum_{k=1}^{n} c_j d_k \le (f:g)(g:\varphi) + O(\varepsilon)$$

Then taking $\varepsilon \to 0$ achieves the result. $\square$

Fix $f_0 \in C_c^+$, and define $I_\varphi(f) = \frac{(f:\varphi)}{(f_0:\varphi)}$ for $f, \varphi \in C_c^+$.

Remark. Thus, $I_\varphi(f)$ is left-invariant and positive, although, instead of linear, only subadditive:

$$I_\varphi(f+g) = \frac{(f+g:\varphi)}{(f_0:\varphi)} \le \frac{(f:\varphi)}{(f_0:\varphi)} + \frac{(g:\varphi)}{(f_0:\varphi)} = I_\varphi(f) + I_\varphi(g) \tag{5}$$

Next, using 19(4), we have

$$(f_0:\varphi) \le (f_0:f)(f:\varphi) \implies \frac{1}{(f_0:f)} \le \frac{(f:\varphi)}{(f_0:\varphi)} = I_\varphi(f)$$

and

$$(f:\varphi) \le (f:f_0)(f_0:\varphi) \implies I_\varphi(f) = \frac{(f:\varphi)}{(f_0:\varphi)} \le (f:f_0)$$

So we have that

$$(f_0:f)^{-1} \le I_\varphi(f) \le (f_0:f) \tag{6}$$

Next, we can show that $I_\varphi(f)$ is ε-close to additive whenever $\mathrm{supp}(\varphi)$ is "small":

Lemma 20 *For $f_1, f_2 \in C_c^+$ and $\varepsilon > 0$ given, there exists a neighborhood V of e such that $I_\varphi(f_1) + I_\varphi(f_2) \le I_\varphi(f_1 + f_2) + \varepsilon$ if $\mathrm{supp}(\varphi) \subset V$.*

Proof. Let $g \in C_c^+$ be such that $g = 1$ on $\mathrm{supp}(f_1 + f_2)$, and $\delta > 0$. Set $h = f_1 + f_2 + \delta g$, and $h_i = \frac{f_i}{h}$, $i = 1, 2$ (setting $h_i = 0$ outside of $\mathrm{supp}(f)$). Then $h_i \in C_c^+$, and so are left and right uniformly continuous, by proposition 15. Then, for $i = 1, 2$ there exists a neighborhood V_i of e such that $|h_i(x) - h_i(y)| < \delta$ for $yx^{-1} \in V_i$. Take $V = V_1 \cap V_2$. Choose $\varphi \in C_c^+$ such that $\mathrm{supp}(\varphi) \subset V$, and choose $c_j > 0$ and $x_j \in G$, $j = 1, 2, \dots, n$, so that $h \le \sum_{j=1}^n c_j L_{x_j}\varphi$. Then we have $|h_i(x) - h_i(x_j)| < \delta$ if $x_j^{-1}x \in \mathrm{supp}(\varphi)$. Hence,

$$f_i(x) = h(x)h_i(x) \le \sum_{j=1}^{n} c_j L_{x_j}\varphi(x) h_i(x) \le \sum_{j=1}^{n} c_j \varphi(x_j^{-1}x)[h_i(x_j) + \delta]$$

where the second inequality is achieved because $L_{x_j}\varphi(x) = \varphi(x_j^{-1}x)$ vanishes whenever $x_j^{-1}x \notin \mathrm{supp}(\varphi)$, and otherwise $h_i(x) < h_i(x_j) + \delta$.

Then we have $(f_i:\varphi) \le \sum_{j=1}^n c_j[h_i(x_j) + \delta]$, as $(f_i:\varphi)$ is an infimum. Additionally, $h_1 + h_2 = \frac{f_1+f_2}{f_1+f_2+\delta g} \le 1$, so

$$\begin{aligned}(f_1:\varphi) + (f_2:\varphi) &\le \sum_{j=1}^{n} c_j[h_1(x_j) + \delta] + \sum_{j=1}^{n} c_j[h_2(x_j) + \delta] = \sum_{j=1}^{n} c_j[h_1(x_j) + h_2(x_j) + 2\delta] \\ &\le \sum_{j=1}^{n} c_j[1 + 2\delta]\end{aligned}$$

We can choose $\sum_{j=1}^{c_j}$ such that $\sum_{j=1}^{n} c_j \leq (h:\varphi)+\kappa$ for any $\kappa > 0$. Then we have

$$(f_1:\varphi)+(f_2:\varphi) \leq ((h:\varphi)+\kappa)[1+2\delta]$$

Taking $\kappa \to 0$ and dividing by $(f_0:\varphi)$, we have

$$I_\varphi(f_1)+I_\varphi(f_2) \leq [1+2\delta]I_\varphi(h)$$

Using lemma 19, we have

$$I_\varphi(h) = I_\varphi(f_1+f_2+\delta g) \leq I_\varphi(f_1+f_2)+\delta I_\varphi(g)$$

So,

$$I_\varphi(f_1)+I_\varphi(f_2) \leq [1+2\delta](I_\varphi(f_1+f_2)+\delta I_\varphi(g))$$

Then, by equation 6, we have $I_\varphi(g) \leq (g:f_0)$ and $I_\varphi(f_1+f_2) \leq (f_1+f_2:f_0)$, so

$$2\delta(I_\varphi(f_1+_2))+\delta(1+2\delta)I_\varphi(g) \leq 2\delta((f_1+f_2:f_0))+\delta(1+2\delta)(g:f_0)$$

Hence, if we choose δ small enough so that $2\delta((f_1+f_2:f_0))+\delta(1+2\delta)(g:f_0)<\varepsilon$, we have

$$I_\varphi(f_1)+I_\varphi(f_2) \leq I_\varphi(f_1+f_2)+\varepsilon \qquad \square$$

Theorem 21 *Every locally compact Hausdorff topological group possesses a left Haar measure.*

Proof. For $f \in C_c^+$, let $X_f = [(f_0:f)^{-1},(f:f_0)] \subset \mathbb{R}$, and $X = \prod_{f\in C_c^+} X_f$. Since each interval X_f is compact, by Tychonoff's theorem (theorem 16), X is compact. By equation 6, we have that, for any φ, $(f_0:f)^{-1} \leq I_\varphi(f) \leq (f:f_0)$, so $I_\varphi \in X$.

For every compact neighborhood V of e, set $K(V) = \overline{\{I_\varphi : \mathrm{supp}(\varphi) \subset V\}} \subset X$. Then for any finite intersection of such $K(V)$, $\bigcap_{j=1}^n K(V_j) \supset K\left(\bigcap_{j=1}^n V_j\right)$, as the I_φ with support contained in every V_j are in every $K(V_j)$. But $\bigcap_{j=1}^n V_j$ is non-empty (it contains e), and is a neighborhood of e, so $K\left(\bigcap_{j=1}^n V_j\right)$ is non-empty too. That is, $\{K(V) : V \text{ compact neighborhood of } e\}$ is a family of closed sets with the finite intersection property, so, because X is compact, $\bigcap_V K(V)$ is non-empty too; let $I \in \bigcap_V K(V)$.

Let $U \subset X$ be a neighborhood of I. Then $U \cap \{I_\varphi : \mathrm{supp}(\varphi) \subset V\}$ is non-empty (because I is a closure point of $\{I_\varphi : \mathrm{supp}(\varphi) \subset V\}$), for any compact neighborhood V of e.

So for any compact neighborhood V of e, there exists $\varphi \in C_c^+$ with $\mathrm{supp}(\varphi) \subset V$ s.t. $I, I_\varphi \in U$. Hence, for any $\varepsilon > 0$ we can choose U and find φ such that for any $f_1,\ldots,f_n \in C_c^+$,

$$|I(f_j)-I_\varphi(f_j)| < \varepsilon \tag{$\star$}$$

for $j = 1,\ldots,n$. Thus, for $f,g \in C_c^+$, we can apply lemma 20 to find a neighborhood of V of e, wlog compact, and $\varphi \in C_c^+$ such that $I_\varphi(f)+I_\varphi(g) \leq I_\varphi(f+g)+\varepsilon$.

So, using equation 5, we have

$$I_\varphi(f+g)-2\varepsilon \leq I_\varphi(f)+I_\varphi(g)-2\varepsilon \leq I(f)+I(g) \leq I_\varphi(f)+I_\varphi(g)+2\varepsilon \leq I_\varphi(f+g)+3\varepsilon$$

Applying ($\star$) to $f+g$, we have

$$I(f+g)-3\varepsilon \leq I_\varphi(f+g)-2\varepsilon \leq I(f)+I(g) \leq I_\varphi(f+g)+3\varepsilon \leq I(f+g)+4\varepsilon$$

Taking $\varepsilon \to 0$ yields $I(f+g) = I(f) + I(g)$.

For general $f \in C_c$ (not necessarily positive), we can decompose $f = f^+ - f^-$ into it's positive and negative parts, such that $f^\pm \in C_c^+$ or $f^\pm = 0$. Then simply define $I(f) = I(f^+) - I(f^-)$, so I is a left-invariant linear functional on $C_c(G)$, and $I(f) > 0$ for $f \in C_c^+$, so f is positive.

Then, by lemma 12, a left Haar measure exists. □

IV. UNIQUENESS OF THE LEFT HAAR MEASURE

We will only consider the σ-compact case, because there's a short, interesting proof in this case. (Of course, the uniqueness of the left Haar measure can be proven for general Hausdorff locally compact spaces). This approach is given as an exercise in Terence Tao's work [Tao11], and is worked out more explicitly in [Ped00].

Def. 22 A topological space (X, τ) is called σ-compact if it is the union of countably many compact subspaces.

Example 23 Every connected, locally compact space is σ-compact.

Def. 24 A measure $\mu : X \to [0, \infty]$ is called σ-finite if X is the countable union of measurable sets of finite measure.

Remark. Clearly, every Radon measure on a σ-compact space is σ-finite.

Def. 25 Given two measures $\mu, \nu : X \to [0, \infty]$, we say ν is absolutely continuous with respect to μ, denoted $\nu \ll \mu$, if $\nu(E) = 0$ for every $E \in X$ such that $\mu(E) = 0$.

Example 26 Given two measures ν, μ, we have $\nu \ll \nu + \mu$.

Theorem 27 ***(The Radon-Nikodym Theorem)*** *Let X be a set and $\mathcal{M}$ a σ-algebra on X. Given σ-finite measures $\nu, \mu : \mathcal{M} \to [0, \infty]$ with $\nu \ll \mu$, there exists a μ-integrable function $h : X \to \mathbb{R}$ with $\nu(E) = \int_E h \, \mathrm{d}\mu$. Furthermore, any two such h are equal μ-a.e (that is, if the set of points N where the two h's disagree has $\mu(N) = 0$).*

Remark. This is a less general version of the theorem presented by Folland, but it is sufficient for our purposes.

Notation: For measures μ, ν, when we have $\nu(E) = \int_E h \, \mathrm{d}\mu$, we write $\mathrm{d}\nu = h \, \mathrm{d}\mu$. This notation makes sense, as we have $\int_E f \, \mathrm{d}\nu = \int_E fh \, \mathrm{d}\mu$. Frequently, h is written as $\frac{\mathrm{d}\nu}{\mathrm{d}\mu}$ and is called the Radon-Nikodym derivative of ν with respect to μ.

Theorem 28 *If μ, ν are left Haar measures on σ-compact G, then $\exists\, c > 0$ s.t. $\mu = c\nu$.*

Proof. Consider $f \in C_c(G)$, and ν, μ two left Haar measures on G.

We know that $\int_E f \, \mathrm{d}\mu = \int_{xE} f \, \mathrm{d}\mu = \int_{xE} f(y) \, \mathrm{d}\mu(y) = \int_E f(x^{-1}y) \, \mathrm{d}\mu(y)$.

Using the Radon-Nikodym Theorem for μ and $\mu + \nu$, we know $\exists\, h$ with

$$\mathrm{d}\mu = h \, \mathrm{d}(\nu + \mu)$$

Then,

$$\int_E fh \, \mathrm{d}(\nu + \mu) = \int_E f \, \mathrm{d}\mu = \int_E L_x f \, \mathrm{d}\mu = \int_E L_x(f) h \, \mathrm{d}(\nu + \mu) = \int_E f L_{x^{-1}}(h) \, \mathrm{d}(\nu + \mu)$$

That is, for any $x \in G$,

$$\int_E f \, [h - L_{x^{-1}} h] \, \mathrm{d}(\nu + \mu) = 0$$

Then $h = L_{x^{-1}}h$ almost everywhere, and it follows that h is constant a.e.. That is,

$$\mu(E) = c\int_E \mathrm{d}(\nu+\mu) = c(\nu(E)+\mu(E)) \implies (1-c)\mu(E) = c\nu(E) \implies \nu(E) = \frac{1-c}{c}\mu(E)$$

Clearly, $c \neq 0$, because otherwise $\mu \equiv 0$ and so is not a Haar measure. Furthermore, $c > 0$ or else $\mu \not\to [0,\infty]$. □

V. THE RIGHT HAAR MEASURE

So far, we have worked out the existence and uniqueness (up to scale) of the left Haar measure. While in the case of compact groups, the right and left Haar measure are the same (up to scale), this is an example of a more general result, and in fact the left and right Haar measure are not always the same in general. In the interest of brevity, most proofs in the section will be left to Folland [Fol99].

Proposition 29 μ is a left Haar measure on G if and only if $\tilde{\mu}(E) = \mu(E^{-1})$ is a right Haar measure.

Proof. If μ is a left Haar measure, then $\tilde{\mu}(Ex) = \mu(x^{-1}E^{-1}) = \mu(E^{-1}) = \tilde{\mu}(E)$; conversely, if $\tilde{\mu}$ is a right Haar measure, $\mu(xE) = \tilde{\mu}(E^{-1}x^{-1}) = \tilde{\mu}(E^{-1}) = \mu(E)$. □

Remark. Then we have that not only a right Haar measure exists by 21, but also is unique up to scale by 28.

When are they equal? For $x \in G$, consider $\mu_x(E) := \mu(Ex)$; this is clearly another left Haar measure. Hence, $\exists\, \Delta(x) > 0$ such that $\mu_x = \Delta(x)\mu$, by theorem 28.

Def. 30 For a left Haar measure μ and μ_x defined as above, the function $\Delta : G \to [0,\infty)$ given by $x \mapsto \frac{\mu_x}{\mu}$ is called modular function of G.

Remark. This function is independent of choice of μ: if $\mu_x = \Delta(x)\mu$ and $\nu_x = \Delta'(x)\nu$, then by theorem 28, $\exists\, c > 0$ such that $\nu = c\mu$. Then $\nu_x(E) = \nu(xE) = c\mu(xE) = c\mu_x(E)$, so $\nu_x = c\mu_x = c\Delta(x)\mu = \Delta'(x)\nu = \Delta'(x)c\mu$. That is, $\Delta(x) = \Delta'(x)$.

Proposition 31 Δ is a continuous homomorphism from G to $\mathbb{R}^\times_{>0}$ and if μ is a left Haar measure on G, for any $f \in L^1(\mu)$ and $y \in G$,

$$\int R_y f\,\mathrm{d}\mu = \Delta(y^{-1})\int f\,\mathrm{d}\mu$$

Then we have that the left Haar measure is also a right Haar measure exactly when $\Delta \equiv 1$.

Def. 32 G is called unimodular if $\Delta \equiv 1$.

If G is abelian, it is clearly unimodular ($\mu(E) = \Delta(x)\mu(Ex) = \Delta(x)\mu(xE) = \Delta(x)\mu(E)$). Additionally, as we have shown in class, any compact group is unimodular.

We also have that

Proposition 33 For $[G,G] = \langle\{xyx^{-1}y^{-1} : x,y \in G\}\rangle$, if $G/[G,G]$ is finite, then G is unimodular.

Remark. This is interesting, because the size of $[G,G]$ can be thought of a measure of the “non-abelianness” of the group G, and so G is unimodular when this is large, (so that $G/[G,G]$ is finite), and when it is small (G abelian).

We also have, from [Tao11]

Proposition 34 If G has an associated Lie algebra $\mathfrak{g}$ which is semisimple and connected, then G is unimodular.

VI. THE FULLY QUANTUM SLEPIAN WOLF PROTOCOL

In quantum information theory, a common goal is to make optimal use of a noisy channel to transmit quantum information from one party to another. Many protocols were developed to perform such a feat subject to different conditions. These protocols were shown to fall into two families, called the mother and father; simple operations could transform the mother protocol or father protocol into any of the other protocols. In 2006, Anura Abeyesinghe, Igor Devetak, Patrick Hayden (of the computer science department here at McGill), and Andreas Winter developed a simple direct proof of the mother protocol and showed that the father protocol was related by a symmetry, collapsing the two families [ADHW09].

In this protocol, Alice holds a Hilbert space A, Bob, B, and there is a reference system R. At the start, a pure state $|\varphi\rangle^{RAB} \in R \otimes A \otimes B$. Alice wants to use quantum communication to transfer her part of the state to Bob. As a by-product of this transfer, Alice and Bob bipartite entangled states called ebits.

Instead of directly attempting to transfer the state from Alice to Bob, however, instead Alice attempts to decouple her system from the reference system and remove the information from her system. If Alice's part of the state is close to product with the part of the state in the reference system, and her state contains little information, then after tracing out Alice's system, Bob and the reference will share the information.

The main tool in proving that this protocol can be achieved according to a particular rate is the decoupling theorem. Alice needs to choose a unitary matrix to act on her part of the state in order to try to decouple her system from the reference while ending up with as little information in her state as possible (i.e. so that her portion of the state is close to the maximally mixed state). The decoupling theorem provides a bound on how well choosing a random unitary matrix according to the Haar measure fares in this task; as it turns out, quite well.

Thus, much of the proof of this foundational protocol is a relatively routine calculation of an integral over the compact group of unitary matricies using the Haar measure.

For more details, useful references are the original paper for this direct proof [ADHW09], the notes from Patrick Hayden's 2007 Quantum Information Theory course [Hay07], or Frédéick Dupuis's thesis on decoupling in quantum information theory [Dup10].

VII. CONCLUSION

Locally compact Hausdorff topological groups have an associated invariant measure, the Haar measure, which allows integration. After developing the necessary definitions to rigorously define such a measure, we prove that such a measure exists on any locally compact Hausdorff group by approximating a linear functional and using Riesz's theorem. Afterwards, we prove uniqueness in the σ-compact case using invariance of Radon-Nikodym derivatives of Haar measures. Lastly, we discuss an interesting application of the Haar measure to quantum information theory.

[ADHW09] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter. The mother of all protocols: restructuring quantum information's family tree. *Royal Society of London Proceedings Series A*, 465:2537–2563, June 2009.

[Dup10] F. Dupuis. *The decoupling approach to quantum information theory.* PhD thesis, PhD Thesis, 2010, 2010.

[Fol99] G.B. Folland. *Real analysis: modern techniques and their applications.* Pure and applied mathematics. Wiley, 1999.

[Hay07] Patrick Hayden. Comp-761: Quantum information theory. http://www.cs.mcgill.ca/~patrick/qit761.2009/index.html, 2007. Accessed: December 15, 2013.

[Ped00] Gert K. Pederson. The existence and uniqueness of the haar integral on a locally compact topological group. http://www.math.ku.dk/kurser/2004-2/mat3re/haarintegral.pdf, 2000. Accessed: December 15, 2013.

[Tao11] Terence Tao. Haar measure and the Peter-Weyl theroem. http://terrytao.wordpress.com/2011/09/27/254a-notes-3-haar-measure-and-the-peter-weyl-theorem/, 2011. Accessed: December 15, 2013.