The 5/8 theorem

for compact Hausdorff topological groups

Timo Rohner

timo.rohner@student.uj.edu.pl

April 19, 2021

Table of Contents

Let us randomly choose two elements a, b of a finite group G.

Let us randomly choose two elements a, b of a finite group G.

What does the probability $P(ab = ba)$ tell us about the group G?

Let us randomly choose two elements a, b of a finite group G.

What does the probability $P(ab = ba)$ tell us about the group G?

If the probability exceeds 62.5%, then the group must be abelian.

This result has been known for a long time, with the first formal proof showing up in a paper by Erdös and Turan.

To show that the 5/8 theorem holds, we will first explore some examples that will guarantee that we cannot improve the constant $\frac{5}{8}$.

First, let's consider the center of a finite group G and ask how big the center can be relative to the group G.

First, let's consider the center of a finite group G and ask how big the center can be relative to the group G.
If G is abelian, then the center Z is the whole group, i.e. $Z = G$.

First, let's consider the center of a finite group G and ask how big the center can be relative to the group G.
If G is abelian, then the center Z is the whole group, i.e. $Z = G$.
Let's assume that G is not abelian. By Lagrange's theorem we know that $\frac{|G|}{|Z|}$ is an integer. Since G is non-abelian clearly $\frac{|G|}{|Z|} > 1$.

First, let's consider the center of a finite group G and ask how big the center can be relative to the group G.
If G is abelian, then the center Z is the whole group, i.e. $Z = G$.
Let's assume that G is not abelian. By Lagrange's theorem we know that $\frac{|G|}{|Z|}$ is an integer. Since G is non-abelian clearly $\frac{|G|}{|Z|} > 1$.
Since we want to find an upper bound for $\frac{|Z|}{|G|}$, this is the same as finding a lower bound for $|G|/|Z|$ under the assumption that G is non-abelian.

What about $\frac{|G|}{|Z|} = 2$?

What about $\frac{|G|}{|Z|} = 2$?
The center of a group is always a normal subgroup, which means that G/Z is a group of size $\frac{|G|}{|Z|}$. This means that if $\frac{|G|}{|Z|} = 2$, then $G/Z = \mathbb{Z}/2$, which means that G is generated by Z and one element.

What about $\frac{|G|}{|Z|} = 2$?
The center of a group is always a normal subgroup, which means that G/Z is a group of size $\frac{|G|}{|Z|}$. This means that if $\frac{|G|}{|Z|} = 2$, then $G/Z = \mathbb{Z}/2$, which means that G is generated by Z and one element. But this element commutes with everything in the center, which means that G is abelian, which is a contradiction. Therefore $\frac{|G|}{|Z|} > 2$.

What about $\frac{|G|}{|Z|} = 3$?

What about $\frac{|G|}{|Z|} = 3$?
The same argument as before applies to this case, since the only group of order 3 is the group $\mathbb{Z}/3$, which is generated by one element.

What about $\frac{|G|}{|Z|} = 4$?

What about $\frac{|G|}{|Z|} = 4$?
The only groups of order 4 are $\mathbb{Z}/4$ and the Klein four-group $\mathbb{Z}/2 \times \mathbb{Z}/2$.

What about $\frac{|G|}{|Z|} = 4$?
The only groups of order 4 are $\mathbb{Z}/4$ and the Klein four-group $\mathbb{Z}/2 \times \mathbb{Z}/2$. Since both those groups are abelian we may wrongly conclude that $\frac{|G|}{|Z|} > 4$. But nothing guarantees that the commutativity of $G/Z \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$ is preserved when passing to G, which is generated by Z and $\mathbb{Z}/2 \times \mathbb{Z}/2$.

So we are left with the task of determining whether we can find a non-abelian group G such that $G/Z \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$. G/Z is abelian, but elements from G don't have to commute despite commuting after being mapped to G/Z.

So we are left with the task of determining whether we can find a non-abelian group G such that $G/Z \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$. G/Z is abelian, but elements from G don't have to commute despite commuting after being mapped to G/Z.
Is there such a group?

So we are left with the task of determining whether we can find a non-abelian group G such that $G/Z \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$. G/Z is abelian, but elements from G don't have to commute despite commuting after being mapped to G/Z.
Is there such a group?
Yes, namely the 8-element quaternion group.

$$Q = \{\pm 1, \pm i, \pm j, \pm k\},$$

where

$$\begin{aligned} i^2 = j^2 = k^2 &= -1, \\ ij &= k, \\ jk &= i, \\ ki &= j, \\ ji &= -k, \\ kj &= -i, \\ ik &= -j. \end{aligned}$$

$$Q = \{\pm 1, \pm i, \pm j, \pm k\},$$

where

$$\begin{aligned} i^2 = j^2 = k^2 &= -1, \\ ij &= k, \\ jk &= i, \\ ki &= j, \\ ji &= -k, \\ kj &= -i, \\ ik &= -j. \end{aligned}$$

$Z = \{-1, 1\}$, $Q/Z = \mathbb{Z}/2 \times \mathbb{Z}/2$.

$$Q = \{\pm 1, \pm i, \pm j, \pm k\},$$

where

$$\begin{aligned} i^2 = j^2 = k^2 &= -1, \\ ij &= k, \\ jk &= i, \\ ki &= j, \\ ji &= -k, \\ kj &= -i, \\ ik &= -j. \end{aligned}$$

$Z = \{-1, 1\}$, $Q/Z = \mathbb{Z}/2 \times \mathbb{Z}/2$.
$Q/Z = \{1, i, j, k\}$ and all elements commute.

$$Q = \{\pm 1, \pm i, \pm j, \pm k\},$$

where

$$\begin{aligned} i^2 = j^2 = k^2 &= -1, \\ ij &= k, \\ jk &= i, \\ ki &= j, \\ ji &= -k, \\ kj &= -i, \\ ik &= -j. \end{aligned}$$

$Z = \{-1, 1\}$, $Q/Z = \mathbb{Z}/2 \times \mathbb{Z}/2$.
$Q/Z = \{1, i, j, k\}$ and all elements commute.
Thus Q is a nonabelian finite group with $|Q|/4$ elements in the center.

So what is the probability that two randomly chosen elements of Q commute?

So what is the probability that two randomly chosen elements of Q commute?
Let a and b be randomly chosen elements from Q.

So what is the probability that two randomly chosen elements of Q commute?
Let a and b be randomly chosen elements from Q.
$P(ab = ba) = P(a \in Z) + P(a \notin Z) \cdot P(ab = ba | a \notin Z)$.

So what is the probability that two randomly chosen elements of Q commute?
Let a and b be randomly chosen elements from Q.
$P(ab = ba) = P(a \in Z) + P(a \notin Z) \cdot P(ab = ba | a \notin Z)$.
Clearly $P(a \in Z) = 1/4$, $P(a \notin Z) = 3/4$.

What is $P(ab = ba | a \notin Z)$?

What is $P(ab = ba | a \notin Z)$?
Recall the definition of Q:

$$\begin{aligned} i^2 = j^2 = k^2 &= -1, \\ ij &= k, \\ jk &= i, \\ ki &= j, \\ ji &= -k, \\ kj &= -i, \\ ik &= -j. \end{aligned}$$

What is $P(ab = ba | a \notin Z)$?
Recall the definition of Q:

$$\begin{aligned} i^2 = j^2 = k^2 &= -1, \\ ij &= k, \\ jk &= i, \\ ki &= j, \\ ji &= -k, \\ kj &= -i, \\ ik &= -j. \end{aligned}$$

Let $a \in Q \setminus Z$. What choices are there for $b \in Q$ such that $ab = ba$?

What is $P(ab = ba | a \notin Z)$?
Let $a \in Q \setminus Z$. What choices are there for $b \in Q$ such that $ab = ba$?

What is $P(ab = ba | a \notin Z)$?
Let $a \in Q \setminus Z$. What choices are there for $b \in Q$ such that $ab = ba$?
If $a = \pm i$, then $b \in \{1, -1, i, -i\}$.
If $a = \pm j$, then $b \in \{1, -1, j, -j\}$.
If $a = \pm k$, then $b \in \{1, -1, k, -k\}$.

What is $P(ab = ba | a \notin Z)$?
Let $a \in Q \setminus Z$. What choices are there for $b \in Q$ such that $ab = ba$?
If $a = \pm i$, then $b \in \{1, -1, i, -i\}$.
If $a = \pm j$, then $b \in \{1, -1, j, -j\}$.
If $a = \pm k$, then $b \in \{1, -1, k, -k\}$.
Thus we have $P(ab = ba | a \notin Z) = 1/2$.

What is $P(ab = ba|a \notin Z)$?
Let $a \in Q \setminus Z$. What choices are there for $b \in Q$ such that $ab = ba$?
If $a = \pm i$, then $b \in \{1, -1, i, -i\}$.
If $a = \pm j$, then $b \in \{1, -1, j, -j\}$.
If $a = \pm k$, then $b \in \{1, -1, k, -k\}$.
Thus we have $P(ab = ba|a \notin Z) = 1/2$.
This means that $P(ab = ba) = 1/4 + 3/4 * 1/2 = 5/8$.

Is this bound sharp?

Is this bound sharp?
Suppose G is non-abelian and we choose a random element g.

Is this bound sharp?
Suppose G is non-abelian and we choose a random element g.
As we saw earlier, if $g \in Z$, then g commutes with all elements of G and we already established that $|Z|/|G| \leq 1/4$.

Is this bound sharp?
Suppose G is non-abelian and we choose a random element g.
As we saw earlier, if $g \in Z$, then g commutes with all elements of G and we already established that $|Z|/|G| \leq 1/4$.
What if $g \notin Z$? g commutes exactly with elements belonging to the centralizer $C(g)$.

How big can $C(g)$ be?

How big can $C(g)$ be?
$C(g)$ is a subgroup of G and by Langrange's theorem $|G|/|C(g)|$ is an integer.

How big can $C(g)$ be?
$C(g)$ is a subgroup of G and by Langrange's theorem $|G|/|C(g)|$ is an integer.
Clearly $|G|/|C(g)| > 1$, since we assumed that $g \notin Z$. Thus the first choice is $|G|/|C(g)| = 2$, which is the same as $|C(g)|/|G| = 1/2$.

How big can $C(g)$ be?
$C(g)$ is a subgroup of G and by Langrange's theorem $|G|/|C(g)|$ is an integer.
Clearly $|G|/|C(g)| > 1$, since we assumed that $g \notin Z$. Thus the first choice is $|G|/|C(g)| = 2$, which is the same as $|C(g)|/|G| = 1/2$.
But we already saw earlier that for Q we have $|C(i)|/|Q| = 1/2$, thus we know that there exists a group for which $|C(g)|/|G| = 1/2$ for all $g \notin Z$.

Thus we have

$$
\begin{aligned}
P(ab = ba) &= P(a \in Z) + P(a \notin Z) \cdot P(b \in C(a) \mid a \notin Z) \\
&= P(a \in Z) + (1 - P(a \in Z)) \cdot P(b \in C(a) \mid a \notin Z) \\
&\leq P(a \in Z) + \frac{1 - P(a \in Z)}{2} \\
&= \frac{1 + P(a \in Z)}{2} \\
&\leq \frac{1 + 1/4}{2} = \frac{5}{8}.
\end{aligned}
$$

This means the quaternion group is as commutative as possible without being abelian.

This means the quaternion group is as commutative as possible without being abelian.
Moreover, one can show that the following are equivalent

- The probability that two elements commute is $5/8$.
- The inner automorphism group of G is of order 4.
- The inner automorphism group of G is the Klein four group.

This means the quaternion group is as commutative as possible without being abelian.
Moreover, one can show that the following are equivalent

- The probability that two elements commute is $5/8$.
- The inner automorphism group of G is of order 4.
- The inner automorphism group of G is the Klein four group.

The probability $5/8$ can only be attained if

- $|Z|/|G| = 1/4$,
- $|C(g)|/|G| = 1/2$ for all $g \notin Z$.

So far we have only discussed finite groups. Is there a way to generalize this statement to non-finite groups?

So far we have only discussed finite groups. Is there a way to generalize this statement to non-finite groups? Yes.

So far we have only discussed finite groups. Is there a way to generalize this statement to non-finite groups? Yes.
Moreover: Is there a way that we can replicate the arguments given earlier involving computing the probability for elements to commute for non-finite groups?

So far we have only discussed finite groups. Is there a way to generalize this statement to non-finite groups? Yes.
Moreover: Is there a way that we can replicate the arguments given earlier involving computing the probability for elements to commute for non-finite groups?
The answer is yes and involves the Haar measure.

Preliminaries

$(G, \cdot)$ is a locally compact Hausdorff topological group.

Preliminaries

$(G, \cdot)$ is a locally compact Hausdorff topological group.
We have a Borel algebra generated by all open subsets of G.

Preliminaries

$(G, \cdot)$ is a locally compact Hausdorff topological group.
We have a Borel algebra generated by all open subsets of G.
We define the left and right translates of a subset S of G by an element g of G:

- left translate:
$$gS = \{g \cdot s : s \in S\},$$
- right translate:
$$Sg = \{s \cdot g : s \in S\}.$$

Preliminaries

$(G, \cdot)$ is a locally compact Hausdorff topological group.
We have a Borel algebra generated by all open subsets of G.
We define the left and right translates of a subset S of G by an element g of G:

- left translate:
$$gS = \{g \cdot s : s \in S\},$$
- right translate:
$$Sg = \{s \cdot g : s \in S\}.$$

If S is a Borel set, then so are gS and Sg.

Haar's theorem

Let $(G, \cdot)$ be a locally compact Hausdorff topological group.

Haar's theorem

Let $(G, \cdot)$ be a locally compact Hausdorff topological group.
There exists a countably additive, nontrivial measure μ on Borel subsets of G such that

Haar's theorem

Let $(G, \cdot)$ be a locally compact Hausdorff topological group.
There exists a countably additive, nontrivial measure μ on Borel subsets of G such that

- μ is left-translation-invariant, i.e.
  $\mu(gS) = \mu(S)$ for all $g \in G$ and Borel sets $S \subseteq G$,

Haar's theorem

Let $(G, \cdot)$ be a locally compact Hausdorff topological group.
There exists a countably additive, nontrivial measure μ on Borel subsets of G such that

- μ is left-translation-invariant, i.e.
  $\mu(gS) = \mu(S)$ for all $g \in G$ and Borel sets $S \subseteq G$,
- μ is finite on compact sets, i.e. $\mu(K) < \infty$ for all compact $K \subseteq G$,

Haar's theorem

Let $(G, \cdot)$ be a locally compact Hausdorff topological group.
There exists a countably additive, nontrivial measure μ on Borel subsets of G such that

- μ is left-translation-invariant, i.e. $\mu(gS) = \mu(S)$ for all $g \in G$ and Borel sets $S \subseteq G$,
- μ is finite on compact sets, i.e. $\mu(K) < \infty$ for all compact $K \subseteq G$,
- μ is outer regular on Borel sets $S \subseteq G$, i.e. $\mu(S) = \inf\{\mu(U) : S \subseteq U,\ U \text{ open}\}$,

Haar's theorem

Let $(G, \cdot)$ be a locally compact Hausdorff topological group.
There exists a countably additive, nontrivial measure μ on Borel subsets of G such that

- μ is left-translation-invariant, i.e. $\mu(gS) = \mu(S)$ for all $g \in G$ and Borel sets $S \subseteq G$,
- μ is finite on compact sets, i.e. $\mu(K) < \infty$ for all compact $K \subseteq G$,
- μ is outer regular on Borel sets $S \subseteq G$, i.e. $\mu(S) = \inf\{\mu(U) : S \subseteq U,\ U \text{ open}\}$,
- μ is inner regular on open sets $U \subseteq G$, i.e. $\mu(U) = \sup\{\mu(K) : K \subseteq U,\ K \text{ compact}\}$.

Haar's theorem

Let $(G, \cdot)$ be a locally compact Hausdorff topological group.
There exists a countably additive, nontrivial measure μ on Borel subsets of G such that

- μ is left-translation-invariant, i.e. $\mu(gS) = \mu(S)$ for all $g \in G$ and Borel sets $S \subseteq G$,
- μ is finite on compact sets, i.e. $\mu(K) < \infty$ for all compact $K \subseteq G$,
- μ is outer regular on Borel sets $S \subseteq G$, i.e. $\mu(S) = \inf\{\mu(U) : S \subseteq U,\ U \text{ open}\}$,
- μ is inner regular on open sets $U \subseteq G$, i.e. $\mu(U) = \sup\{\mu(K) : K \subseteq U,\ K \text{ compact}\}$.

Moreover, this Haar measure is unique up to a positive multiplicative constant.

There are various ways of showing the existence of a Haar measure satisfying the properties given in Haar's theorem.

There are various ways of showing the existence of a Haar measure satisfying the properties given in Haar's theorem.
The traditional proof given by Haar and Weil involves constructing the Haar measure using compact subsets.

For 2 subsets $S, T \subseteq G$ we define $[T : S]$ to be the smallest number of left translates of S that fully covers T. This means that $[T : S]$ is a non-negative integer or infinity.

For 2 subsets $S, T \subseteq G$ we define $[T : S]$ to be the smallest number of left translates of S that fully covers T. This means that $[T : S]$ is a non-negative integer or infinity.
For disjoint comapct sets K, L and an open set U that is a sufficiently small neighborhood of the identity of G we have $[K : U] + [L : U] = [K \cup L : U]$, but $[-, U]$ is not additive on compact sets.

For 2 subsets $S, T \subseteq G$ we define $[T : S]$ to be the smallest number of left translates of S that fully covers T. This means that $[T : S]$ is a non-negative integer or infinity.
For disjoint comapct sets K, L and an open set U that is a sufficiently small neighborhood of the identity of G we have
$[K : U] + [L : U] = [K \cup L : U]$, but $[-, U]$ is not additive on compact sets.
We now fix a compact set A with nonempty interior. Such a set exists since G is locally compact.

For 2 subsets $S, T \subseteq G$ we define $[T : S]$ to be the smallest number of left translates of S that fully covers T. This means that $[T : S]$ is a non-negative integer or infinity.
For disjoint comapct sets K, L and an open set U that is a sufficiently small neighborhood of the identity of G we have
$[K : U] + [L : U] = [K \cup L : U]$, but $[-, U]$ is not additive on compact sets.
We now fix a compact set A with nonempty interior. Such a set exists since G is locally compact.
Let K be a compact set. We define

$$\mu_A(K) = \lim_U \frac{[K : U]}{[A : U]},$$

where the limit is over directed set of open neighborhoods of the identity eventually contained in any given neighborhood.

For 2 subsets $S, T \subseteq G$ we define $[T : S]$ to be the smallest number of left translates of S that fully covers T. This means that $[T : S]$ is a non-negative integer or infinity.
For disjoint comapct sets K, L and an open set U that is a sufficiently small neighborhood of the identity of G we have $[K : U] + [L : U] = [K \cup L : U]$, but $[-, U]$ is not additive on compact sets.
We now fix a compact set A with nonempty interior. Such a set exists since G is locally compact.
Let K be a compact set. We define

$$\mu_A(K) = \lim_U \frac{[K : U]}{[A : U]},$$

where the limit is over directed set of open neighborhoods of the identity eventually contained in any given neighborhood.
Does there exist a directed set for which this limit exists? Yes, thanks to Tychonoff's theorem.

μ_A is additive on disjoint compact subsets of G and thus a regular content, i.e. a measure except that it's not necessarily countably additive and only finitely additive.

μ_A is additive on disjoint compact subsets of G and thus a regular content, i.e. a measure except that it's not necessarily countably additive and only finitely additive.
Any regular content can be extended into a measure. First extend μ_A to open sets by inner regularity, then to all sets by outer regularity and finally restricting to Borel sets.

For compact topological groups we can show the existence of a Haar measure without making use of any measure theory.

For compact topological groups we can show the existence of a Haar measure without making use of any measure theory.
Instead we can use convex sets and the Krein-Milman theorem.

For compact topological groups we can show the existence of a Haar measure without making use of any measure theory.
Instead we can use convex sets and the Krein-Milman theorem.
We denote by $G - \mathrm{Ban}$ the category of Banach representations of G.

For compact topological groups we can show the existence of a Haar measure without making use of any measure theory.
Instead we can use convex sets and the Krein-Milman theorem.
We denote by $G - \mathrm{Ban}$ the category of Banach representations of G.
Objects are Banach spaces X over $\mathbb{R}$ with a continuous norm preserving action $G \times X \to X$, i.e. $\|gx\| = \|x\| \ \forall g \in G, x \in X$.

For compact topological groups we can show the existence of a Haar measure without making use of any measure theory.
Instead we can use convex sets and the Krein-Milman theorem.
We denote by $G - \mathrm{Ban}$ the category of Banach representations of G.
Objects are Banach spaces X over $\mathbb{R}$ with a continuous norm preserving action $G \times X \to X$, i.e. $\|gx\| = \|x\| \ \forall g \in G, x \in X$.
Maps in $G - \mathrm{Ban}$ are short maps that happen to be G-equivariant.

For compact topological groups we can show the existence of a Haar measure without making use of any measure theory.
Instead we can use convex sets and the Krein-Milman theorem.
We denote by $G - \mathrm{Ban}$ the category of Banach representations of G.
Objects are Banach spaces X over $\mathbb{R}$ with a continuous norm preserving action $G \times X \to X$, i.e. $\|gx\| = \|x\| \; \forall g \in G, x \in X$.
Maps in $G - \mathrm{Ban}$ are short maps that happen to be G-equivariant.
Short maps are maps between metric spaces $f : X \to Y$ such that $d(f(a), f(b)) \leq d'(a, b)$, where d is the metric of Y and d' the metric of X.

For compact topological groups we can show the existence of a Haar measure without making use of any measure theory.
Instead we can use convex sets and the Krein-Milman theorem.
We denote by $G - \mathrm{Ban}$ the category of Banach representations of G.
Objects are Banach spaces X over $\mathbb{R}$ with a continuous norm preserving action $G \times X \to X$, i.e. $\|gx\| = \|x\| \; \forall g \in G, x \in X$.
Maps in $G - \mathrm{Ban}$ are short maps that happen to be G-equivariant.
Short maps are maps between metric spaces $f : X \to Y$ such that $d(f(a), f(b)) \leq d'(a, b)$, where d is the metric of Y and d' the metric of X.
(Being G-equivariant means that $f(gx) = gf(x)$)

$C(G)$, the vector space of continuous real-valued functionals with compact support on G, is one such banach representation and so is $\mathbb{R}$ if we take $gz = z$ for each $z \in \mathbb{R}$ and $g \in G$.

$C(G)$, the vector space of continuous real-valued functionals with compact support on G, is one such banach representation and so is $\mathbb{R}$ if we take $gz = z$ for each $z \in \mathbb{R}$ and $g \in G$.
In fact, $C(G)$ is a locally convex tvs with the locally convex structure being given by the seminorms $\rho_K(f) = \sup_{x \in K} |f(x)|$, where K are compact subsets of G.

$C(G)$, the vector space of continuous real-valued functionals with compact support on G, is one such banach representation and so is $\mathbb{R}$ if we take $gz = z$ for each $z \in \mathbb{R}$ and $g \in G$.
In fact, $C(G)$ is a locally convex tvs with the locally convex structure being given by the seminorms $\rho_K(f) = \sup_{x \in K} |f(x)|$, where K are compact subsets of G.
A Radon measure on G can be fully given by a continuous linear functional

$$\int_G : C(G) \to \mathbb{R}.$$

$C(G)$, the vector space of continuous real-valued functionals with compact support on G, is one such banach representation and so is $\mathbb{R}$ if we take $gz = z$ for each $z \in \mathbb{R}$ and $g \in G$.
In fact, $C(G)$ is a locally convex tvs with the locally convex structure being given by the seminorms $\rho_K(f) = \sup\limits_{x \in K} |f(x)|$, where K are compact subsets of G.
A Radon measure on G can be fully given by a continuous linear functional

$$\int_G : C(G) \to \mathbb{R}.$$

Such a Radon measure yields a measure μ on the σ-algebra of Borel sets in the normal measure theoretic sense, i.e.

$$\mu(B) = \sup\{\int_G f : \mathrm{supp}(f) = K \subset B, \rho_K(f) = 1\}.$$

We say that a left Haar integral on G is a nonzero linear functional $\int_G$ such that $\int_G f \geq 0$ when $f \geq 0$ and $\int_G f^g = \int_G f$ for any $f \in C(G)$ and $g \in G$ where $f^g : G \to \mathbb{R}$ sends x to $f(gx)$.

We say that a left Haar integral on G is a nonzero linear functional $\int_G$ such that $\int_G f \geq 0$ when $f \geq 0$ and $\int_G f^g = \int_G f$ for any $f \in C(G)$ and $g \in G$ where $f^g : G \to \mathbb{R}$ sends x to $f(gx)$.
We then say that a Haar measure on G is a nonzero Radon measure μ such that $\mu(gB) = \mu(B)$ for all $g \in G$ and Borel sets B.

We say that a left Haar integral on G is a nonzero linear functional $\int_G$ such that $\int_G f \geq 0$ when $f \geq 0$ and $\int_G f^g = \int_G f$ for any $f \in C(G)$ and $g \in G$ where $f^g : G \to \mathbb{R}$ sends x to $f(gx)$.
We then say that a Haar measure on G is a nonzero Radon measure μ such that $\mu(gB) = \mu(B)$ for all $g \in G$ and Borel sets B.
$\mathbb{R}$ embedds into $C(G)$ as constant functions. This gives us an exact sequence

$$0 \to \mathbb{R} \to C(G) \to C(G)/\mathbb{R} \to 0.$$

If we show that $\mathbb{R}$ is an injective object in $G - \mathrm{Ban}$ then we are done.

If we show that $\mathbb{R}$ is an injective object in $G - \mathrm{Ban}$ then we are done.
An object Q is injective if for a monomorphism $f : X \to Y$ any $g : X \to Q$ can be extended to $h : Y \to Q$.

If we show that $\mathbb{R}$ is an injective object in $G - \mathrm{Ban}$ then we are done.
An object Q is injective if for a monomorphism $f : X \to Y$ any $g : X \to Q$ can be extended to $h : Y \to Q$.
Injectivity of $\mathbb{R}$ means that $1_{\mathbb{R}}$ lifts along the inclusion $0 \to \mathbb{R} \to C(G)$ and thus we have a retract $\int_G : C(G) \to \mathbb{R}$ for $0 \to \mathbb{R} \to C(G)$ in $G - \mathrm{Ban}$.

If we show that $\mathbb{R}$ is an injective object in $G - \mathrm{Ban}$ then we are done.
An object Q is injective if for a monomorphism $f : X \to Y$ any $g : X \to Q$ can be extended to $h : Y \to Q$.
Injectivity of $\mathbb{R}$ means that $1_{\mathbb{R}}$ lifts along the inclusion $0 \to \mathbb{R} \to C(G)$ and thus we have a retract $\int_G : C(G) \to \mathbb{R}$ for $0 \to \mathbb{R} \to C(G)$ in $G - \mathrm{Ban}$.
This means that $\int_G$ has norm 1 and positivity follows.

So why is $\mathbb{R}$ injective?

So why is $\mathbb{R}$ injective?
Take $X \to Y$ an injection of Banach representations of G and $f : X \to \mathbb{R}$ a map of Banach representations of G.

So why is $\mathbb{R}$ injective?
Take $X \to Y$ an injection of Banach representations of G and $f : X \to \mathbb{R}$ a map of Banach representations of G.
By Hahn-Banach there exists $g : Y \to \mathbb{R}$ in the category of Banach spaces and short maps that extends f, but we aren't guaranteed G-invariance.

Now let's consider subsets of all extensions of f to Y. Let S be the collection of G-invariant compact convex subsets of this set.

Now let's consider subsets of all extensions of f to Y. Let S be the collection of G-invariant compact convex subsets of this set.
S contains the convex hull of Gg, where g is some chosen extension of f to Y, so S is nonempty.

Now let's consider subsets of all extensions of f to Y. Let S be the collection of G-invariant compact convex subsets of this set.
S contains the convex hull of Gg, where g is some chosen extension of f to Y, so S is nonempty.
By compactness and Zorn's lemma, we can find a minimal element of S in this collection, where we impose the order that $A \leq B$ whenever $A \subset B$. We call this minimal element H.

Now let's consider subsets of all extensions of f to Y. Let S be the collection of G-invariant compact convex subsets of this set.
S contains the convex hull of Gg, where g is some chosen extension of f to Y, so S is nonempty.
By compactness and Zorn's lemma, we can find a minimal element of S in this collection, where we impose the order that $A \leq B$ whenever $A \subset B$. We call this minimal element H.
H is clearly a singleton. If H contains a point which is not extremal then it contains the convex hull of the orbit of that point, which would be a proper G-invariant compact convex subset of H (Krein-Milman theorem).

Now let's consider subsets of all extensions of f to Y. Let S be the collection of G-invariant compact convex subsets of this set.
S contains the convex hull of Gg, where g is some chosen extension of f to Y, so S is nonempty.
By compactness and Zorn's lemma, we can find a minimal element of S in this collection, where we impose the order that $A \leq B$ whenever $A \subset B$. We call this minimal element H.
H is clearly a singleton. If H contains a point which is not extremal then it contains the convex hull of the orbit of that point, which would be a proper G-invariant compact convex subset of H (Krein-Milman theorem). This means that H is a singleton and its unique element is a G-invariant functional extending f.

Now let's consider subsets of all extensions of f to Y. Let S be the collection of G-invariant compact convex subsets of this set.
S contains the convex hull of Gg, where g is some chosen extension of f to Y, so S is nonempty.
By compactness and Zorn's lemma, we can find a minimal element of S in this collection, where we impose the order that $A \leq B$ whenever $A \subset B$. We call this minimal element H.
H is clearly a singleton. If H contains a point which is not extremal then it contains the convex hull of the orbit of that point, which would be a proper G-invariant compact convex subset of H (Krein-Milman theorem). This means that H is a singleton and its unique element is a G-invariant functional extending f.
Thus $\mathbb{R}$ is indeed injective.

Let G be a compact Hausdorff topological group.

Let G be a compact Hausdorff topological group.
G has a left Haar measure. Or put differently: We have a Borel measure μ with $\mu(U) > 0$ for all nonempty open subsets U of G and $\mu(x \cdot E) = \mu(E)$ for all Borel sets $E \subset G$ and all $x \in G$.

Let G be a compact Hausdorff topological group.
G has a left Haar measure. Or put differently: We have a Borel measure μ with $\mu(U) > 0$ for all nonempty open subsets U of G and $\mu(x \cdot E) = \mu(E)$ for all Borel sets $E \subset G$ and all $x \in G$.
By imposing $\mu(G) = 1$ we guarantee uniqueness of the Haar measure.

We impose the product measure $\mu \times \mu$ on the product space $G \times G$ and we define $C = \{(x, y) \in G \times G : xy = yx\}$.

We impose the product measure $\mu \times \mu$ on the product space $G \times G$ and we define $C = \{(x, y) \in G \times G : xy = yx\}$.
It is obvious that $C = f^{-1}(1)$, where $f : G \times G \to G$ is continuous and defined as $f(x, y) = xyx^{-1}y^{-1}$.

We impose the product measure $\mu \times \mu$ on the product space $G \times G$ and we define $C = \{(x, y) \in G \times G : xy = yx\}$.
It is obvious that $C = f^{-1}(1)$, where $f : G \times G \to G$ is continuous and defined as $f(x, y) = xyx^{-1}y^{-1}$.
This means that C is closed and thus measurable.

We impose the product measure $\mu \times \mu$ on the product space $G \times G$ and we define $C = \{(x, y) \in G \times G : xy = yx\}$.
It is obvious that $C = f^{-1}(1)$, where $f : G \times G \to G$ is continuous and defined as $f(x, y) = xyx^{-1}y^{-1}$.
This means that C is closed and thus measurable.
We use the notation $P(G)$ for the probability that two elements of G commute.

We impose the product measure $\mu \times \mu$ on the product space $G \times G$ and we define $C = \{(x, y) \in G \times G : xy = yx\}$.
It is obvious that $C = f^{-1}(1)$, where $f : G \times G \to G$ is continuous and defined as $f(x, y) = xyx^{-1}y^{-1}$.
This means that C is closed and thus measurable.
We use the notation $P(G)$ for the probability that two elements of G commute.
Since we can consider $\mu \times \mu$ as a probability measure we have $P(G) = (\mu \times \mu)(C)$.

We will now show the 5/8 theorem for G a compact Hausdorff topological group:

5/8 theorem for compact Hausdorff topological groups

Suppose G is non-abliean. Then $P(G) \leq 5/8$.

$$P(G) = (\mu \times \mu)(C) = \int_{G \times G} 1_C d(\mu \times \mu).$$

$$P(G) = (\mu \times \mu)(C) = \int_{G \times G} 1_C d(\mu \times \mu).$$

By Fubini's theorem we have

$$(\mu \times \mu)(C) = \int_G \int_G 1_C(x, y) d\mu(y) d\mu(x).$$

$$P(G) = (\mu \times \mu)(C) = \int_{G \times G} 1_C \, d(\mu \times \mu).$$

By Fubini's theorem we have

$$(\mu \times \mu)(C) = \int_G \int_G 1_C(x, y) d\mu(y) d\mu(x).$$

We have

$$\int_G 1_C(x, y) d\mu(y) = \mu(C_x),$$

where C_x is the centralizer of x in G.

As shown earlier, $|G|/|Z| \geq 4$, since for $1, 2, 3$ the only possiblities are that G is generated by Z and one additional element of G.

As shown earlier, $|G|/|Z| \geq 4$, since for $1, 2, 3$ the only possiblities are that G is generated by Z and one additional element of G.
Since G is the disjoint union of cosets of Z, it holds that $\mu(Z) \leq 1/4$.
Measurability of Z follows from closedness of Z.

If $x \in Z$, then $C_x = G$ and therefore $\mu(C_x) = 1$.

If $x \in Z$, then $C_x = G$ and therefore $\mu(C_x) = 1$.
On the other hand, if $x \notin Z$, then C_x must have an index of at least 2 in G and therefore $\mu(C_x) \leq 1/2$.

If $x \in Z$, then $C_x = G$ and therefore $\mu(C_x) = 1$.
On the other hand, if $x \notin Z$, then C_x must have an index of at least 2 in G and therefore $\mu(C_x) \leq 1/2$.
This means that we have

$$\begin{aligned} P(G) &= \int\limits_G \mu(C_x) d\mu(x) \\ &= \int\limits_Z \mu(C_x) d\mu(x) + \int\limits_{G\setminus Z} \mu(C_x) d\mu(x) \\ &\leq \mu(Z) + \mu(G \setminus Z) \cdot 1/2 \leq 5/8. \end{aligned}$$

References

P. Erdös, P. Turan, On some problems of a statistical group theory IV, ActaMath. Acad.Sci.Hung., 19 (1968), 413-435.

Angela Spalsbury, Joe Diestel,The Joys of Haar Measure, vol. 150, Graduate Studies in Mathematics, American Mathematical Society, 2014,isbn: 1470409356,9781470409357

Gustafson, W. H. "What Is the Probability That Two Group Elements Commute?" The American Mathematical Monthly 80, no. 9 (1973): 1031-034. Accessed April 11, 2021. doi:10.2307/2318778.

https://ncatlab.org/nlab/show/Haar+integral