1 Question and Setting

Write $a^X := \{x^{-1}ax \mid x \in X\}$, $A^{(l)}$ for l-tuples from A.

Theorem 1 (Corollary 1.2)**.** *For any k, l, m, there is a $p < 1$ and a K such that whenever G is a group, $X_0 \subseteq G^{p,k}$ finite, and $X = X_0^{-1}X_0$:*

- $|X_0X| \leq k|X_0|$
- *With probability $\geq p$, an l-tuple $(a_1, \ldots, a_l) \in X^l$ satisfies $|a_1^X \cdots a_l^X| \geq |X|/m$*

Then there is a subgroup S of G, $S \subseteq X^2$, such that X is contained in $\leq K$ cosets of S.

Suppose not; then for some k, l, m and every p, K, there is a $G^{p,k}$, an $X_0^{p,k} \subseteq G^{p,k}$ finite, such that the conditions hold, but there is no subgroup S with X contained in K cosets of S.

Take an extension of the language of groups which adds predicates $m(\{\vec{x} \mid \phi(\vec{x}, \vec{a})\}) \geq r$ whenever ϕ is a formula and r a rational, and a distinguished predicate X_0. Then for each p, K, $(G^{p,K}, X_0^{p,K})$ gives a model of this language, interpreting $m(\{\vec{x} \mid \phi(\vec{x}, \vec{a})\}) \geq r$ to hold when $\frac{|\{\vec{x} \mid \phi(\vec{x}, \vec{a})\}|}{|X^{(|\vec{x}|)}|} \geq r$.

Take an ultraproduct of these models, giving a model (G, X_0) with G, X_0 infinite. We may define a measure μ on G-definable subsets of $G^{(l)}$: if $A = \{\vec{x} \mid \phi(\vec{x}, \vec{a})\}$, set $\mu(A) := \inf_r (G, X_0) \vDash m(\{\vec{x} \mid \phi(\vec{x}, \vec{a})\}) \geq r$.

If $C \subseteq G^2$ is a definable set, we define $C_a := \{x \mid (x, a) \in C\}$.

Note that if $A = \{\vec{x} \mid \phi(\vec{x}, \vec{a})\}$, it is not always the case that $\mu(A) \geq r$ is equivalent to $(G, X_0) \vDash m(\{\vec{x} \mid \phi(\vec{x}, \vec{a})\}) \geq r$: if $(G, X_0) \vDash m(\{\vec{x} \mid \phi(\vec{x}, \vec{a})\}) \geq s$ for every rational $s > r$ then we will have $\mu(A) = r$ even if $(G, x_0) \vDash \neg m(\{\vec{x} \mid \phi(\vec{x}, \vec{a})\}) \geq r$.

In particular, $\{a \mid \mu(C_a) > 0\}$ may not be definable. However, $\mu(C_a)$ is $\bigwedge$-definable: $\mu(C_a) > 0$ iff $(G, x_0) \vDash \neg m(C_a) \geq r$ for all $r > 0$.[1]

So $\{(a_1, \ldots, a_l) \in X^{(l)} \mid \mu(a_1^X \cdots a_l^X) \geq 1/m\}$ is not definable. However, if we choose $r \in (1/(m+1), 1/m)$, and set $Q = \{(a_1, \ldots, a_l) \in X^{(l)} \mid m(a_1^X \cdots a_l^X) \geq r\}$, Q is definable, and we will have $\mu(Q) = 1$ and $\mu(a_1^X \cdots a_l^X) \geq 1/m+1$ whenever $(a_l, \ldots, a_l) \in Q$.

Fix a countable elementary submodel $M \prec G$; for the remainder, we will always allow parameters from M.

The M-definable sets give a countable, finitely additive algebra of subsets of G, and μ is a finitely additive measure on them. The M-definable sets on $G^{(2)}$ are also a countable, finitely additive algebra, but much bigger than the product of the collection of definable subsets of G with itself. Since we have sufficient saturation, we could extend μ to a σ-additive measure on the σ-algebra generated by the definable sets, and the measure over $G^{(2)}$ would satisfy Fubini's Theorem relative to the measure over G; however we will be able to work with the following more elementary properties:

- $\mu(A \times B) = \mu(A)\mu(B)$

[1] Here we abuse notation by writing $m(C_a)$, which is not quite a formula of the language.

- If $\mu(A_a) = 0$ for all a then $\mu(A) = 0$

We have $\mu(X) = 1$, and $\mu(X^{(n)})$ is bounded.

Definition 2. *A* wide partial type *over a countable set D is an intersection of $M \cup D$-definable sets. A* wide type *is a partial type p such that, whenever B is $M \cup D$-definable, either $p \subseteq B$ or $p \subseteq \overline{B}$.*

We write $tp(a/D)$ for the set of b such that $\phi(a, \vec{d}) \Leftrightarrow \phi(b, \vec{d})$ whenever ϕ is a formula and $\vec{s} \in D^{(n)}$.

I will treat types as being the set of elements satisfying that type.

Note that being a type is relative to a particular choice of algebra: in general, a wide typeover a' is only a wide partial type over a, b.

Lemma 3. *Each type is contained in $X^{(n)}$ for a fixed n, or disjoint from all $X^{(n)}$.*

Proof. This follows from the fact that $X^{(n)}$ is definable for each n. □

From here on, we always assume that a type is contained in $X^{(n)}$ for some n.

Lemma 4. *Every wide partial type can be extended to a wide type.*

Proof. Let $B_1, \ldots, B_i, \ldots$ enumerate the definable sets. Define a sequence of partial types with $q_0 := q$ and, given q_n, if for some $A \supseteq q_n$, $\mu(A \cap B_n) = 0$, $q_{n+1} := q_n \cap \overline{B}_n$, otherwise $q_{n+1} := q_n \cap B_n$.

Let $q' := \bigcap_n q_n$. If q' is not wide, there must be some n such that q_{n+1} is not wide. Let n be least such that q_{n+1} is not wide. If $q_{n+1} \subseteq B_n$ then there is some $A \supseteq q_n$ with $\mu(B_n \cap A) = 0$; this contradicts the definition of q_{n+1}. So $q_{n+1} \subseteq \overline{B}_n$, and there is an $A \supseteq q_n$ with $\mu(A \cap B_n) = 0$. But there must be some $A' \supseteq q_n$ with $\mu(A' \cap \overline{B}_n) = 0$. Then $\mu(A \cap A') = 0$, contradicting the fact that $A \cap A' \supseteq q_n$ and q_n is wide. Therefore q' is wide. □

If $A, B \subseteq G$ (either definable or $\bigwedge$-definable), we write $Ab = \{ab \mid a \in A\}$, $bA = \{ba \mid a \in A\}$, $AB = \{ab \mid a \in A, b \in B\}$, $A^{-1} = \{a^{-1} \mid a \in A\}$.

Lemma 5.

- *If q is a type, so is q^{-1}*
- *If q is a type over D and $a \in D$, $qa = \{xa \mid x \in q\}$ is a type over D.*
- *If p, q are types, $pq = \{xy \mid x \in p, y \in q\}$ is a partial type.*

Proof.

- For any B, either $q \subseteq B^{-1}$ or $q \subseteq \overline{B^{-1}}$, and therefore either $q^{-1} \subseteq B$ or $q^{-1} \subseteq \overline{B}$ respectively.
- For any B, either $q \subseteq Ba^{-1}$ or $q \subseteq \overline{B}a^{-1}$, and therefore either $qa \subseteq B$ or $qa \subseteq \overline{B}$ respectively.
- We claim that pq is the intersection of all sets AB such that $p \subseteq A$ and $q \subseteq B$. Certainly, if $p \subseteq A$ and $q \subseteq B$, $pq \subseteq AB$. Conversely, if $x \in AB$ for every $A \supseteq p$, $B \supseteq q$, $\{(a, b) \mid a \in A, b \in B, ab = x\}$ is definable for each A, B, and therefore by saturation, there is a pair (a, b) such that $a \in p$, $b \in q$, and $ab = x$, so $x \in pq$.

□

2 Wide Types are Special

Definition 6. (b_i) *is a* sequence of indiscernibles *if whenever* $\phi(b_0, \ldots, b_n)$ *and* $m_0 < \cdots < m_n$, $\phi(b_{m_0}, \ldots, b_{m_n})$.

That is, for every n there is a type p_n of $n+1$-tuples such that $tp(b_{m_0}, \ldots, b_{m_n}) = p_n$ whenever $m_0 < \cdots < m_n$ is an increasing sequence.

Lemma 7. *Suppose* $\mu(A_b) > 0$ *holds and* (b_i) *is a sequence of indiscernibles with* $tp(b_i) = tp(b)$. *Then for any finite* $b_1, \ldots, b_n$, *there is an* $a \in \bigcap_{i \leq n} \phi_{b_i}$.

Proof. Suppose not: that is, for some k, $\bigcap_{i \leq k} A_{b_i}$ is empty. Let k be least such that $\mu(\bigcap_{i \leq k+1} A_{b_i}) = 0$; since $\mu(A_{b_0}) > 0$, $k \geq 0$. For $n \geq k$, let $C_n = \bigcap_{i<k} A_{b_i} \cap A_{b_n}$. Then $\mu(C_n) = \mu(\bigcap_{i \leq k} A_{b_i}) > 0$ since $k < k+1$. But for $n < m$, by indiscernibility, $\mu(C_n \cap C_m) = \mu(\bigcap_{i \leq k+1} A_{b_i}) = 0$. This is a contradiction since μ is a finite measure. $\square$

Lemma 8. *If* $tp(a/b)$ *is wide and* (b_i) *is a sequence of indiscernibles with* $tp(b_i) = tp(b)$ *then for any finite* $b_1, \ldots, b_n$, *there is an* a' *with* $tp(a', b_i) = tp(a, b)$ *for all* $i \leq n$.

Proof. Suppose $(a, b) \in A$. Then $a \in A_b$, so by the previous lemma, there is an a' so that $a' \in \bigcap_{i \leq n} A_{b_i}$, so $(a', b_i) \in A$ for each $i \leq n$. By saturation, there is an a' such that $(a', b_i) \in A$ simultaneously for all $i \leq n$, $A \ni (a, b)$. Therefore $tp(a', b_i) = tp(a, b)$ for all $i \leq n$. $\square$