MANCHESTER
1824

The University of Manchester

The embedding problem for probabilities on locally compact groups

McCrudden, M.

2006

MIMS EPrint: **2006.327**

Manchester Institute for Mathematical Sciences
School of Mathematics

The University of Manchester

Reports available from: http://eprints.maths.manchester.ac.uk/
And by contacting: The MIMS Secretary
School of Mathematics
The University of Manchester
Manchester, M13 9PL, UK

ISSN 1749-9097

Probability Measures on Groups: Recent Directions and Trends
Editors: S.G. Dani and P. Graczyk
Copyright © 2006 Tata Institute of Fundamental Research
Publisher: Narosa Publishing House, New Delhi, India

The Embedding Problem for Probabilities on Locally Compact Groups

Mick McCrudden

1 Introduction

Let G be a locally compact group and let $P(G)$ denote the topological semigroup of probability measures on G, where the multiplication in $P(G)$ is convolution of measures, and the topology on $P(G)$ is the weak topology. A measure $\mu \in P(G)$ is said to be *infinitely divisible on* G if μ has an nth root in $P(G)$ for each $n \in \mathbb{N}$, and is said to be *continuously embedded on* G if there is a continuous one-parameter semigroup $(\mu_t)_{t\geq 0}$ in $P(G)$ such that $\mu = \mu_1$.

The first explicit statement of what became known as the *embedding problem* (for connected Lie groups) occurs in the 1967 paper of K.R. Parthasarathy [20], where he asks "whether one can directly imbed an infinitely divisible distribution (on a connected Lie group) in a one-parameter convolution semigroup." But we should also note the earlier important paper of Böge [1], where the relationship between the compactness of the root sets of the measure and (rational) embedding of the measure is first indicated.

Taking a wider viewpoint, the embedding problem is now seen as the problem of understanding the relationship between two classes of measures, the infinitely divisible measures and the continuously embedded measures, on any locally compact group. The problem has been an active research area for nearly forty years, and has attracted the attention of a number of authors. Yet in spite of the very considerable progress that has been made to date, the question is still not settled for all connected Lie groups.

Between 1991 and 1996, the embedding problem was solved for certain important classes of locally compact groups. The paper of Shah [22] solves the embedding problem for p-adic algebraic groups, the papers of Dani and McCrudden [5], [6] solve the problem for connected coverings of linear Lie groups, and discrete linear groups respectively, and the paper of Dani and Shah [7] solves it for finitely generated matrix groups with entries in any

number field. All these proofs depend on the concept of an *almost factor compact group*, and the realisation that real almost algebraic groups and p-adic algebraic groups are indeed almost factor compact (see Theorem 2.3). But the property of almost factor compactness also finds application in the work of Dani and colleagues on asymptotic behaviour of measures, and plays an important role in the lecture course by Professor Dani.

Newcomers to this area of research may find it initially useful to consult the author's article [16], where an overview of the proofs of the three embedding results mentioned above is presented. While there is some overlap between [16] and the present lecture course (particularly in sections 2 and 3 below), the focus of the present course is on the connected Lie case, and includes recent work on the embedding problem for subsemigroups of connected Lie groups.

For work on the embedding problem prior to 1977, there is no better source than Chapter III of Heyer's monograph [10]; the historical comments and references at the end of the chapter are particularly useful. The 1986 and 1989 papers by the same author ([11], [12]) can also be recommended for an overview of work on the problem between 1977 and the end of the 1980's.

Acknowledgements It is a pleasure to thank both the organisers of the conference (S. G. Dani, Piotr Graczyk and Yves Guivarc'h) for their kind invitation to present these lectures, and CIMPA and the Tata Institute for financial support and hospitality.

2 Factors and Factor Compactness

Let G be a locally compact group, and denote by $P(G)$ the topological semigroup of probability measures on G, furnished with the weak topology and with convolution as the multiplication ([10], Theorem 1.2.2; [21], Chapters 2, 3).

For $\mu \in P(G)$ we denote by $G(\mu)$ the smallest closed subgroup of G containing $\mathrm{supp}\mu$ (the support of μ), and we write $N(\mu, G)$ for the normaliser of $G(\mu)$ in G, and $Z(\mu, G)$ for the centraliser of $G(\mu)$ in G. We use $F(\mu, G)$ for the *two-sided factor set of μ in G*, namely

$$F(\mu, G) = \{\lambda \in P(G) : \mu = \nu\lambda = \lambda\nu \text{ for some } \nu \in P(G)\}.$$

We write $T(\mu, G) = \left\{x \in G : x\mu x^{-1} = \mu\right\}$, and we note that $T(\mu, G)$ is a closed subgroup of $N(\mu, G)$, and that $Z(\mu, G) \subseteq T(\mu, G) \subseteq F(\mu, G)$, while

$$T(\mu, G) F(\mu, G) = F(\mu, G) = F(\mu, G) T(\mu, G).$$

Proposition 2.1 (i) *$F(\mu, G)$ is a closed subset of $P(G)$, and for every $\lambda \in F(\mu, G)$ there exists $x \in N(\mu, G)$ such that* $\mathrm{supp}\lambda \subseteq xG(\mu)$.

(ii) *If $G(\mu)$ is abelian, then every $\lambda \in F(\mu, G)$ is supported on $T(\mu, G)$.*

Proof (i) The second assertion is 1.1 of [3], and the first assertion follows from 1.2.21(ii) of [10].

(ii) Suppose $\lambda \in F(\mu, G)$, then there exists $\nu \in F(\mu, G)$ such that $\lambda\nu = \nu\lambda = \mu$. By (i), there exists $x, y \in N(\mu, G)$ such that

$$\mathrm{supp}\lambda \subseteq xG(\mu),\ \mathrm{supp}\nu \subseteq yG(\mu).$$

Then if $p : N(\mu, G) \to N(\mu, G)/G(\mu)$ is the canonical homomorphism, we have

$$1 = p(\mu) = p(\lambda)\, p(\nu) = p(x)\, p(y),$$

which implies $p(y) = p\left(x^{-1}\right)$. Hence

$$\mathrm{supp}\lambda \subseteq xG(\mu),\ \mathrm{supp}\nu \subseteq G(\mu)\, x^{-1}.$$

So we can write $\lambda = x\alpha$ and $\nu = \beta x^{-1}$, for some $\alpha, \beta \in P(G(\mu))$. Then since $G(\mu)$ is abelian,

$$\alpha\beta = \beta\alpha = \nu\lambda = \mu = \lambda\nu = x\alpha\beta x^{-1},$$

which implies that $x \in T(\mu, G)$. But clearly $G(\mu) \subseteq T(\mu, G)$, so $\mathrm{supp}\lambda \subseteq T(\mu, G)$ as required.

□

For $\mu \in P(G)$ we write

$$F(\mu, G)/Z(\mu, G) \text{ for } \{p(\lambda) : \lambda \in F(\mu, G)\},$$

where $p : N(\mu, G) \to N(\mu, G)/Z(\mu, G)$ is the canonical homomorphism, and p is also used for the corresponding induced map from $P(N(\mu, G))$ into $P(N(\mu, G)/Z(\mu, G))$. We note that $Z(\mu, G)$ is a normal subgroup of $N(\mu, G)$.

Definition 2.2 (i) A measure $\mu \in P(G)$ is said to be *factor compact on G* if and only if $F(\mu, G)$ is compact.

(ii) A measure $\mu \in P(G)$ is said to be *almost factor compact on G* if and only if $F(\mu, G)/Z(\mu, G)$ is a relatively compact subset of $P(N(\mu, G)/Z(\mu, G))$.

(iii) A locally compact group G is called an *almost factor compact group* if and only if every $\mu \in P(G)$ is almost factor compact on G.

Theorem 2.3 (The AFC Theorem) *The following locally compact groups are almost factor compact groups.*

(i) *Any real almost algebraic group.*

(ii) *Any p-adic algebraic group.*

(iii) *Any discrete subgroup of* $GL(d,\mathbb{R})$*,* $d \in \mathbb{N}$*.*

(iv) *Any covering of a real almost algebraic group.*

Proof Result (i) is Theorem 3.2 of [5], and a similar argument suitably adapted gives (ii) as Theorem 2 of [22]. Result (iii) is an easy consequence of (i) and is given as Theorem 2.1 in [6]. Result (iv) follows from (i) and Proposition 6.2 of [5].

Problem A Which other locally compact groups are almost factor compact groups?

Example 2.4 ([3, Remark 3.5(ii)]) There is a three-dimensional connected nilpotent Lie group which is not almost factor compact.

Let G be the Lie group whose underlying space is $\mathbb{R}^2 \times S^1$, and whose multiplication is given by

$$\left(x_1, y_1, e^{i\theta_1}\right)\left(x_2, y_2, e^{i\theta_2}\right) = \left(x_1 + x_2, y_1 + y_2, e^{i(\theta_1+\theta_2+x_1y_2)}\right).$$

G is a quotient of the three-dimensional simply connected nilpotent Heisenberg group by a discrete central subgroup. The centre of G is a circle and equals the commutator subgroup of G, so writing Z for the centre we have that G/Z is abelian.

Let $\lambda \in P(G)$ such that $G(\lambda) = G$, and let $\mu = w_Z\lambda$, where w_Z is a normalised Haar measure on Z. Then μ is Z-invariant, and because G/Z is abelian, any Z-invariant measure on G is a factor of μ. But $Z(\mu, G) = Z$, so $F(\mu, G)/Z(\mu, G) = P(G/Z) = P\left(\mathbb{R}^2\right)$ and G is not almost factor compact. But we also have $T(\mu, G) = G$, hence $F(\mu, G)/T(\mu, G)$ is a point, so it is compact.

Definition 2.5 (i) A measure $\mu \in P(G)$ is said to be *weakly factor compact on* G if and only if $F(\mu, G)/T(\mu, G)$ is a relatively compact set in $P(N(\mu, G)/T(\mu, G))$.

(ii) A locally compact group G is called a *weakly factor compact group* if and only if every $\mu \in P(G)$ is weakly factor compact on G.

Problem B Which locally compact groups are weakly factor compact groups?

Let $\mathbb{R}_+^*$ denote the additive semigroup of positive reals. Any subsemigroup S of $\mathbb{R}_+^*$ is called a *real directed semigroup* (also called a *submonogeneous semigroup*) if and only if for any $s, t \in S$, there exists $u \in S$ such that $s = mu$ and $t = nu$, for some $m, n \in \mathbb{N}$.

Given a real directed semigroup S and a locally compact group G, a homomorphism $t \mapsto \mu_t$ of S into $P(G)$ is said to be *locally tight* if and only if for each $r \in S$, the set $\{\mu_t : t \in S, t \leq r\}$ is a relatively compact set in $P(G)$.

Definition 2.6 A locally compact group G is called *convolution bounded* (abbreviated to *CB group*) if and only if for every real directed semigroup S, every homomorphism of S into $P(G)$ is locally tight.

Theorem 2.7 *Any closed subgroup of any connected locally compact group is a CB group.*

Strategy of Proof (i) It is clearly enough to prove that any locally compact connected group is a CB group.

(ii) By an easy shift compactness argument (i.e. an argument using [10, 1.2.21(iii)]) it is easy to see that if G contains a compact normal subgroup K such that G/K is a CB group, then G a CB group. But any connected locally compact group is a projective limit of connected Lie groups ([10, Theorem G, p. 12]) so it suffices to prove the CB property for connected Lie groups.

(iii) If G is a connected Lie group with centre Z and G/Z is a CB group, then G is a CB group.

(iv) For any connected Lie group G, G/Z can be realised as a closed subgroup of some $\mathrm{SL}(d, \mathbb{R})$.

(v) $\mathrm{SL}(d, \mathbb{R})$ is a CB group. This is the substantial step in the argument and relies on the AFC Theorem for almost algebraic groups, which is Theorem 2.3(i).

Full details of the proof of Theorem 2.7, for G a connected Lie group, are given in [3, Section 2].

3 Root Compact Measures, Rational and Continuous Embedding

For $\mu \in P(G)$, where G is a locally compact group, we write for $n \in \mathbb{N}$,

$$R_n(\mu, G) = \{\nu \in P(G) : \nu^n = \mu\}$$
$$R(\mu, G) = \bigcup \{R_n(\mu, G) : n \in \mathbb{N}\}$$
$$\overline{R}_n(\mu, G) = \left\{\nu^k : \nu \in R_n(\mu, G), 1 \leq k \leq n\right\}$$

and

$$\overline{R}(\mu, G) = \bigcup \left\{\overline{R_n}(\mu, G) : n \in \mathbb{N}\right\}.$$

We note that $\overline{R}(\mu, G)$ is a subset of $F(\mu, G)$.

Definition 3.1 Let $\mu \in P(G)$.

(i) μ is said to be *infinitely divisible on* G if and only if for each $n \in \mathbb{N}$, $R_n(\mu, G) \neq \emptyset$.

(ii) μ is said to be *root compact on* G if and only if for all $n \in \mathbb{N}$, $R_n(\mu, G)$ is compact in $P(G)$.

(iii) μ is said to be *strongly root compact on* G if and only if $\overline{R}(\mu, G)$ is a relatively compact subset of $P(G)$.

(iv) μ is said to be *rationally embedded on* G if and only if there exists a homomorphism $t \mapsto \mu_t$ of $\mathbb{Q}_+^*$ into $P(G)$ such that $\mu_1 = \mu$.

(v) μ is said to be *locally tightly rationally embedded on* G if and only if there exists a homomorphism $t \mapsto \mu_t$ of $\mathbb{Q}_+^*$ into $P(G)$, which is locally tight, and such that $\mu_1 = \mu$.

(vi) μ is said to be *continuously embedded on* G if and only if there exists a continuous homomorphism $t \mapsto \mu_t$ of $\mathbb{R}_+$ into $P(G)$ such that $\mu = \mu_1$.

Theorem 3.2 *Let G be a locally compact group, suppose $\mu \in P(G)$ is infinitely divisible on G.*

(i) *If μ is root compact on G, then μ is rationally embedded on G. If further G is a CB group, then μ is locally tightly rationally embedded on G.*

(ii) *If μ is strongly root compact on G, then μ is locally tightly rationally embedded on G.*

Proof Assuming μ is root compact on G, a rational embedding is obtained as follows. For m, $n \in \mathbb{N}$ such that $n|m$, we define $f_{n,m}$ to be the $(m/n)^{\text{th}}$ power map on $P(G)$. Then $f_{n,m} : R_m(\mu, G) \to R_n(\mu, G)$, and we have a projective system of non-empty compact spaces and maps, so the projective limit is not empty, which implies we have a map $n \mapsto \mu_{\frac{1}{n}}$ of $\mathbb{N}$ into $P(G)$ such that for all $n \in \mathbb{N}$,

$$\mu_{\frac{1}{n}} \in R_n(\mu, G) \text{ and for all } r, s \in \mathbb{N},\ (\mu_{\frac{1}{rs}})^r = \mu_{\frac{1}{s}}.$$

This map extends uniquely to a homomorphism $r \mapsto \mu_r$ of $\mathbb{Q}_+^*$ into $P(G)$, with $\mu_1 = \mu$. This homomorphism is automatically locally tight if G is a CB-group, and in the case where μ is strongly root compact on G, local tightness follows because $\overline{R}(\mu, G)$ is relatively compact and contains $\{\mu_r : r \in \mathbb{Q}_+^*, r \leq 1\}$.

□

Definition 3.3 For any locally tight homomorphism $t \mapsto \mu_t$ of $\mathbb{Q}_+^*$ into $P(G)$, we can form

$$K((\mu_t)) = \bigcap_{0<t\leq 1} \overline{\{\mu_r : r \in \mathbb{Q}_+^*, 0 < r < t\}}.$$

It can be shown (see [10, Sections 3.4, 3.5] for details) that $K((\mu_t))$ is a compact, abelian, divisible, and so connected subgroup of $P(G)$, which is called the *accumulation group of* $\{\mu_t : t \in \mathbb{Q}_+^*\}$. It is also clear that for all $\nu \in K((\mu_t))$, and all $r \in \mathbb{Q}_+^*$, $\nu\mu_r = \mu_r\nu$. The identity of $K((\mu_t))$ is the normalised Haar measure ω_H of some compact group H, and if $M(\omega_H)$ denotes the maximal subgroup of $P(G)$ which contains ω_H, the continuous map $x \mapsto \omega_H x$ is a homomorphism from $N(H, G)$ (the normaliser of H in G) onto $M(\omega_H)$, whose kernel is H. From this it follows that there is a compact subgroup K_1 of $N(H, G)$ such that $H \subseteq K_1$, and $K_1/H \cong K((\mu_t))$. Furthermore the connectedness of $K((\mu_t))$ shows that $HK_1^0 = K_1$.

This brings us to what is an indispensible tool in most work on the embedding problem. The result is really a result from the existence theory for one-parameter semigroups in topological semigroups, adapted for $P(G)$. Full details of its proof appear in [10, Sections 3.4, 3.5].

Theorem 3.4 *Suppose $t \mapsto \mu_t$ is a locally tight homomorphism of $\mathbb{Q}_+^*$ into $P(G)$, where G is locally compact. Then there is a continuous convolution semigroup $\{\nu_t : t \in \mathbb{R}_+\}$ in $P(G)$, and a map $t \mapsto \lambda_t$ of $\mathbb{Q}_+^*$ into $K = K((\mu_t))$ such that*

(i) *for all $t \in \mathbb{Q}_+^*$, $\nu_t = \mu_t\lambda_t = \lambda_t\mu_t$ and*
(ii) *$\nu_0 = \omega_H$, the identity of the accumulation group K.*

Definition 3.5 A locally compact group G will be called *indecent* if and only if there exist compact subgroups $H_1 \lhd H_2$ in G, such that H_2/H_1 is abelian and connected, but is not arcwise connected; otherwise G is called *decent*. We note that Dixmier [8] has given an example of an abelian, compact, connected (and indeed locally connected) group which is not arcwise connected, so indecent groups do exist. It is easy to see that all Lie groups and all totally disconnected groups are decent.

Theorem 3.6 *Let G be a decent locally compact group. Then for $\mu \in P(G)$, μ is continuously embedded on G if and only if μ is locally tightly rationally embedded on G.*

Proof Let $t \mapsto \mu_t$ be a locally tight rational embedding of μ, then as G is decent, the accumulation group $K = K((\mu_t))$ is compact, abelian and arcwise connected, so in the notation of Theorem 3.4, λ_1 lies on a continuous one-parameter semigroup $\{\alpha_t : t \in \mathbb{R}\}$ in K, with $\alpha_1 = \lambda_1$, and then μ_1 lies on the continuous semigroup $t \mapsto \nu_t \alpha_t^{-1}$.

□

Corollary 3.7 *Let G be a decent locally compact group.*

(i) *If $\mu \in P(G)$ is infinitely divisible and strongly root compact on G then μ is continuously embedded on G.*
(ii) *If $\mu \in P(G)$ is infinitely divisible and root compact on G, and G is a CB group, then μ is continuously embedded on G.*

Proof Immediate from Theorem 3.2 and Theorem 3.6.

□

Remark 3.8 Suppose G is locally compact and totally disconnected. If $t \mapsto \mu_t$ is a locally tight homomorphism of $\mathbb{Q}_+^*$ into $P(G)$, then $t \mapsto \mu_t$ is continuous. This is because the accumulation group $K((\mu_t))$ is connected and totally disconnected, so is trivial, and the result now follows from Theorem 3.4.

Definition 3.9 A locally compact group G is called *Böge strongly root compact* if and only if for any compact $C \subseteq G$ there exists a compact set $C_0 \subseteq G$ such that, for each $n \in \mathbb{N}$, and each finite sequence $\{x_1, \ldots, x_n\}$ of elements of G, with $x_n = 1$, satisfying

$$Cx_iCx_j \cap Cx_{i+j} \neq \emptyset$$

for all $2 \leq i + j \leq n$, we have $x_i \in C_0$ for all $1 \leq i \leq n$.

This rather awkward looking condition on G was introduced by Böge [1] and exploited by Siebert [23] to solve the embedding problem for a number of classes of locally compact groups. The notion is important because of the following result.

Theorem 3.10 ([10, 3.1.13]) *If G is Böge strongly root compact then every $\mu \in P(G)$ is strongly root compact on G.*

Example 3.11 The following groups are Böge strongly root compact. (i) Every compact group. (ii) Every discrete free abelian group. (iii) Every compactly generated locally compact abelian group. (iv) Every connected solvable Lie group with "real roots". The reader is referred to [10, Section 3.1] for a comprehensive account of the ideas and consequences associated with the Definition 3.9.

The next proposition is an elementary result which is nevertheless often useful when dealing with roots of a measure.

Proposition 3.12 ([5, Proposition 3.4]) *Let G and H be locally compact second countable groups and suppose there is a continuous surjective homomorphism $f : H \to G$ whose kernel is a compactly generated central subgroup of H. If $\mu \in P(H)$, and $X \subseteq \overline{R}(\mu, H)$, then*

(i) *if $f(X)$ is relatively compact in $P(G)$, X is relatively compact in $P(H)$, and*
(ii) *if X is closed in $P(H)$, $f(X)$ is closed in $P(G)$.*

Definition 3.13 Suppose G is a locally compact group and $t \mapsto \mu_t$ is a continuous homomorphism of $\mathbb{R}_+$ into $P(G)$. The *supporting subgroup* of $(\mu_t)_{t\geq 0}$ is defined to be

$$S((\mu_t)) := \overline{\left\langle \bigcup_{t\geq 0} \mathrm{supp}\mu_t \right\rangle},$$

the smallest closed subgroup of G containing the supports of every μ_t, for $t \geq 0$.

Definition 3.14 We say that a locally compact group G *has Property A* if and only if for each continuous homomorphism $t \mapsto \mu_t$ of $\mathbb{R}_+$ into $P(G)$, there exists some $N \in \mathbb{N}$ such that $\mu_{\frac{1}{N}}$ is strongly root compact on $S = S((\mu_t))$.

Proposition 3.15 *Every almost algebraic group has Property A.*

Proof Let G be almost algebraic, and let $t \mapsto \mu_t$ be a continuous homomorphism of $\mathbb{R}_+$ into $P(G)$. Write μ for μ_1, and let $\widetilde{G}(\mu)$ be the smallest almost algebraic subgroup of G containing suppμ. We write $\widetilde{N}(\mu, G)$ for the normaliser of $\widetilde{G}(\mu)$ in G, and we note that $\widetilde{N}(\mu, G)$ is an almost algebraic subgroup of G.

Let $p : \widetilde{N}(\mu, G) \to \widetilde{N}(\mu, G)/\widetilde{G}(\mu)$ be the canonical homomorphism, then $t \to p(\mu_t)$ is a continuous homomorphism of $\mathbb{R}_+$ into $\widetilde{N}(\mu, G)/\widetilde{G}(\mu)$, with $p(\mu_0) = p(\mu_1)$, so if we write $T = \{p(\mu_t) : t \in \mathbb{R}_+\}$, then either

$$\text{(i) } T = \{1\} \quad \text{or (ii)} \quad T \text{ is a circle group.}$$

In case (i) μ is almost factor compact on $\widetilde{G}(\mu)$ by the AFC theorem, and $Z(\mu, \widetilde{G}(\mu)) = Z(\widetilde{G})$, the centre of $\widetilde{G}(\mu)$. Then by Proposition 3.12, μ is strongly root compact on $\widetilde{G}(\mu)$, and clearly $\widetilde{G}(\mu) = S((\mu_t))$ so Property A holds here with $N = 1$.

In case (ii), we write $M = p^{-1}(T)$, then clearly $S \subseteq M$. Also M is a subgroup of the almost algebraic group $\widetilde{N}(\mu, G)$, and contains the normal subgroup $\widetilde{G}(\mu)$ with $M/\widetilde{G}(\mu)$ compact, so M is almost algebraic by [5, Lemma 2.2].

By [3, Lemma 2.3], there exists $t \in \mathbb{Q}_+^*$ such that for all $s \in \mathbb{Q}_+^*$, μ_s is supported on $A = Z(Z(\mu_t, M), M)$, the centraliser of $Z(\mu_t, M)$ in M. Then by continuity,

$$\text{for all } s \in \mathbb{R}_+, \text{supp}\mu_s \subseteq A$$

and so $S = S((\mu_t)) \subseteq A$. As M is the smallest almost algebraic subgroup of $\widetilde{N}(\mu, G)$ containing S, we conclude that $M = A$.

Let $t = \frac{m}{N}$, for some $m, N \in \mathbb{N}$, then since $Z(\mu_{\frac{1}{N}}, M) \subseteq Z(\mu_t, M)$, and since by the proof of [3, Lemma 2.3], the choice of t ensures $Z(\mu_t, M)$ is minimal among all $Z(\mu_s, M)$, for all $s \in \mathbb{R}_+$, we have $Z(\mu_{\frac{1}{N}}, M) = Z(\mu_t, M)$, and so $M = Z(Z(\mu_{\frac{1}{N}}, M), M)$. We conclude that $Z(\mu_{\frac{1}{N}}, M)$ is central in M.

By the AFC theorem for M, $F(\mu_{\frac{1}{N}}, M)/Z(\mu_{\frac{1}{N}}, M)$ is relatively compact, so $\overline{R}(\mu_{\frac{1}{N}}, M)/Z(\mu_{\frac{1}{N}}, M)$ is relatively compact. By Proposition 3.12(i), this is enough to ensure that $\overline{R}(\mu_{\frac{1}{N}}, M)$ is relatively compact, and so $\mu_{\frac{1}{N}}$ is strongly root compact on M. Since S is a closed subgroup of M it follows that $\mu_{\frac{1}{N}}$ is strongly root compact on S. This completes the proof that G has Property A.

□

Corollary 3.16 *Any closed subgroup of an almost algebraic group has Property A.*

Proposition 3.17 *Suppose G is locally compact and Z is a compactly generated closed central subgroup of G such that G/Z has Property A. Then G has Property A.*

Proof Let $p : G \to G/Z$ be the canonical homomorphism and suppose $t \mapsto \mu_t$ is a continuous homomorphism of $\mathbb{R}_+$ in $P(G)$. Then $t \mapsto p(\mu_t)$ is a continuous homomorphism of $\mathbb{R}_+$ into $P(G/Z)$. We note that

$$S((\mu_t)) \subseteq p^{-1}(S((p(\mu_t)))).$$

Since G/Z has Property A, there exists $N \in \mathbb{N}$ such that $p(\mu_{\frac{1}{N}})$ is strongly root compact on $S_1 := S((p(\mu_t)))$. By Proposition 3.12, this is enough to ensure that $\mu_{\frac{1}{N}}$ is strongly root compact on $p^{-1}(S_1)$. Since $S((\mu_t))$ is a closed subgroup of $p^{-1}(S_1)$, we conclude that $\mu_{\frac{1}{N}}$ is strongly root compact on $S((\mu_t))$. Hence G/Z has Property A.

□

Corollary 3.18 *Any connected Lie group has Property A.*

Proof Let G be a connected Lie group, whose centre we denote by Z. Then as in Theorem 2.7(iv), G/Z can be realised as a closed subgroup of some $GL(d, \mathbb{R})$, and so G/Z has Property A by Corollary 3.16. Hence G has Property A by Proposition 3.17.

□

Theorem 3.19 *Any closed subgroup of a connected locally compact group has Property A.*

Proof It is enough to show that any connected locally compact group has Property A. Any such group contains a compact normal subgroup K, such that G/K is a connected Lie group. By Corollary 3.18, G/K has Property A. Let $p : G \to G/K$ be the canonical homomorphism. Given a continuous homomorphism $t \mapsto \mu_t$ of $\mathbb{R}_+$ into $P(G)$, there is some $N \in \mathbb{N}$ such that $p(\mu_{\frac{1}{N}})$ is strongly root compact on $S((p(\mu_t)))$. Also

$$S((\mu_t)) \subseteq p^{-1}(S((p(\mu_t)))) := W.$$

We note that

$$p(\overline{R}(\mu_{\frac{1}{N}}, W)) \subseteq \overline{R}(p(\mu_{\frac{1}{N}}), S((p(\mu_t)))).$$

Because the second set is relatively compact in $P(G/K)$, and K is compact, this suffices to show that $\overline{R}(\mu_{\frac{1}{N}}, W)$ is relatively compact is $P(W)$. Since $S((\mu_t))$ is a closed subgroup of W, it follows that $\mu_{\frac{1}{N}}$ is strongly root compact in $S((\mu_t))$. Hence G has Property A.

□

Theorem 3.20 *Let G be a closed subgroup of a decent, connected, locally compact group. Then for $\mu \in P(G)$, μ is continuously embeddable on G if and only if there is some closed subgroup W of G and some $N \in \mathbb{N}$ such that*

(i) *there exists some $\lambda \in P(W)$ such that $\lambda^N = \mu$, and*
(ii) *λ is infinitely divisible and strongly root compact on W.*

Proof ($\Rightarrow$) Suppose $t \mapsto \mu_t$ is a continuous embedding of μ, with $\mu = \mu_1$. By Theorem 3.19, there exists $N \in \mathbb{N}$ such that $\mu_{\frac{1}{N}}$ is strongly root compact on $S((\mu_t))$. Now take $W = S((\mu_t))$, and clearly $\mu_{\frac{1}{N}}$ is infinitely divisible on W.

($\Leftarrow$) Clearly W is decent, so by Corollary 3.7(i) λ is continuously embedded on W, so $\mu = \lambda^N$ is continuously embedded on G.

□

4 The Three Major Embedding Theorems

In this section we give the statements of the major embedding theorems currently known for (i) p-adic linear groups, (ii) discrete (real) linear groups and (iii) connected coverings of linear (real) Lie groups. All three results rely for their proof on the AFC Theorem 2.3 above.

For any prime p we denote by $\mathbb{Q}_p$ the field of p-adic numbers. By a *p-adic algebraic group* we mean an algebraic subgroup of $GL_n(\mathbb{Q}_p)$, for some $n \in \mathbb{N}$. By a *p-adic linear group* we mean a topologically closed subgroup of $GL_n(\mathbb{Q}_p)$ for some $n \in \mathbb{N}$. These groups are locally compact and totally disconnected. We call an element of $GL_n(\mathbb{Q}_p)$ *unipotent* if all its eigenvalues are 1.

Lemma 4.1 ([17, Proposition 5]) *If G is a totally disconnected locally compact group and $(\mu_t)_{t>0}$ is a continuous, one-parameter semigroup in $P(G)$, then for all $s, \mathrm{t} \in \mathbb{R}_+^*$, $G(\mu_t) = G(\mu_s)$, and so $Z(\mu_t, G) = Z(\mu_s, G)$.*

So for any continuous, one-parameter semigroup $(\mu_t)_{t>0}$ in $P(G)$, where G is totally disconnected, we use the notation $Z\left((\mu_t)_{t>0}, G\right)$ to denote the common centraliser $Z(\mu_s, G)$ (any $s > 0$).

The embedding problem for p-adic algebraic groups was solved in 1991 by R. Shah [22], and her arguments were later extended in 1999, by McCrudden and Walker [17], to all linear p-adic groups.

Theorem 4.2 (Embedding Theorem for linear p-adic groups) *Let G be a linear p-adic group. Then $\nu \in P(G)$ is infinitely divisible on G if and only if there exists a continuous one-parameter semigroup $(\mu_t)_{t>0}$ in $P(G)$, and some $x \in Z\left((\mu_t)_{t>0}, G\right)$, such that*

(i) *x is infinitely divisible in $Z\left((\mu_t)_{t>0}, G\right)$, and*
(ii) *$\nu = x\mu_1$.*

Remark 4.3 The element x appearing in the statement of Theorem 4.2 is necessarily unimodular, and belongs to the centre of $G(\nu)$. We give no details of the proof of Theorem 4.2 here, but refer the interested reader to [22], [17] and [16, Section 5].

The embedding problem for discrete linear groups was solved by Dani and McCrudden in 1996 [6]. Their result is as follows.

Theorem 4.4 (Embedding theorem for discrete linear groups) *Let D be a discrete subgroup of $GL(d, \mathbb{R})$ for some d, and suppose $\mu \in P(D)$ is infinitely divisible on D. Then there is a continuous one-parameter semigroup $t \mapsto \theta_t$ in $P(D(\mu))$ and an element $z \in Z(D(\mu))$, the centre of $D(\mu)$, such that*

(i) *z is infinitely divisible in $Z(\mu, D)$, and*
(ii) *$\mu = z\theta_1 = \theta_1 z$.*

Remark 4.5 (i) There is a discrete subgroup D of $SL(2, \mathbb{R})$ such that $-I \in D$, $-I$ is infinitely divisible in D, but is not rationally embedded on D ([6, Remark 6.1]).

(ii) If in the statement of Theorem 4.4 we add the assumption that D is a subgroup of a finitely generated subgroup of $GL(d, \mathbb{R})$, then we can conclude that μ is in fact continuously embedded on $D(\mu)$ ([6, Theorem 1.1]).

We omit the details of the proof of Theorem 4.4, and refer the interested reader to [6] and [16, Section 7].

We now turn to the case where G is a connected (real) Lie group. A group G is said to have the *embedding property* if and only if every $\mu \in P(G)$ which is infinitely divisible on G is continuously embedded on G. It has long been conjectured that every connected Lie group has the embedding property. The result for the special case of point masses is true and has been known since 1981.

Theorem 4.6 ([15]) *Let G be a connected Lie group. Then $x \in G$ is infinitely divisible in G if and only if x lies on a one-parameter group in G.*

Proof (i) We first suppose G is a closed connected subgroup of some $GL(d,\mathbb{R})$, and let $\widetilde{G}$ denote the Zariski closure of G in $GL(d,\mathbb{R})$. Since G is connected it is normal in $\widetilde{G}$, and so for $g \in G$, $Z(g,G)$ is normal in $Z(g,\widetilde{G})$. Now $Z^0(g,\widetilde{G})/Z^0(g,G)$ is a connected Lie group, and $Z(g,G) \cap Z^0(g,\widetilde{G})/Z^0(g,G)$ is a discrete normal subgroup, so is central in $Z^0(g,\widetilde{G})/Z^0(g,G)$. In particular $Z(g,G) \cap Z^0(g,\widetilde{G})/Z^0(g,G)$ is finitely generated and abelian.

Since $Z(g,\widetilde{G})$ is real algebraic, $Z^0(g,\widetilde{G})$ is of finite index and normal in $Z(g,\widetilde{G})$, so $Z(g,G) \cap Z^0(g,\widetilde{G})$ is of finite index and normal in $Z(g,G) \cap Z(g,\widetilde{G}) = Z(g,G)$. So $Z(g,G) \cap Z^0(g,\widetilde{G})/Z^0(g,G)$ is of finite index and normal in $Z(g,G)/Z^0(g,G)$.

To summarise, for all $g \in G$, the group of components of $Z(g,G)$ contains a finitely generated abelian normal subgroup of finite index.

(ii) Now let G be a general connected Lie group, and let Z be the centre of G. By the trick used in (iv) of the (strategy of) proof of Theorem 2.7, we can realise G/Z as a closed subgroup of some $GL(d,\mathbb{R})$. So if $p : G \to G/Z$ is the natural homomorphism, we see from (i) that for all $g \in G$,

$$Z(p(g), G/Z)/Z^0(p(g), G/Z)$$

is a finite extension of a finitely generated abelian group. Take $g \in G$, and write

$$K = p^{-1}\left(Z\left(p\left(g\right), G/Z\right)\right)$$
$$K_1 = p^{-1}\left(Z^0\left(p\left(g\right), G/Z\right)\right).$$

Suppose g is infinitely divisible on G, then all roots of g lie in $Z\left(g,G\right)$, and so in K, since $Z\left(g,G\right) \subseteq K$. But

$$K/K_1 \cong Z\left(p\left(g\right), G/Z\right)/Z^0\left(p\left(g\right), G/Z\right)$$

so we conclude that g is contained in and infinitely divisible in K_1.

Since $p : G \to G/Z$ is surjective and $Z^0\left(p\left(g\right), G/Z\right)$ is an analytic subgroup of G/Z, it follows by an obvious Lie algebra argument that $p\left(K_1^0\right) = Z^0\left(p\left(g\right), G/Z\right)$. We can write $Z = Z^0 \cdot D$, as a direct product, where D is a discrete subgroup of Z, and so is finitely generated and abelian.

We have $K_1 = Z \cdot K_1^0 = DK_1^0$, since clearly $Z^0 \subseteq K_1^0$. So we can define a homomorphism $\phi : D \to K_1/K_1^0$ by $\phi\left(d\right) = dK_1^0$ for all $d \in D$, and this map

is surjective. Hence K_1/K_1^0 is finitely generated and abelian, from which we conclude that g belongs to K_1^0 and is infinitely divisible in K_1^0. Then g belongs to and is infinitely divisible in the subgroup $L = Z(g, G) \cap K_1^0$.

We check that $Z(g, G)$ is normal in K, so L is a normal subgroup of the connected Lie group K_1^0. But the group of components of a closed normal subgroup of a connected Lie group is a finitely generated abelian group; this is because when we go modulo the identity component of the subgroup, we have a discrete normal subgroup of a connected Lie group, which therefore has to be central.

Hence g must be contained in and infinitely divisible in the connected Lie group L^0, and is also central in this group. But then g lies the image of the exponential map of L^0, by [13, Theorem 1.2, Chapter XVI]. This completes the proof.

□

Note The above argument is more direct than that given in [15]; it is a previously unpublished argument due to S.G. Dani, who has kindly allowed me to present it here.

In 1992, Dani and McCrudden [5] gave a proof of the embedding property for a class of Lie groups that includes all connected semisimple Lie groups and all simply-connected Lie groups. Their result is as follows.

Theorem 4.7 (Embedding theorem for connected coverings of linear Lie groups) *Let G be a connected Lie group which admits a representation $\rho : G \to GL(d, \mathbb{R})$ for some $d \in \mathbb{N}$, such that* $\ker \rho$ *is discrete. Then G has the embedding property.*

Remarks on the proof of 4.7 (i) The theorem follows for the general case fairly simply, once it is established for the "middle case" when $\rho(G)$ is almost algebraic (see [5, Section 7]).

(ii) To deal with the middle case, we must first deal with the case when G is almost algebraic, and this is the most technical part of the proof. We first need a "reduction theorem" which allows us to replace G by an almost algebraic subgroup G', such that the infinitely divisible $\mu \in P(G)$ which we start with is in fact infinitely divisible in $P(G')$, and such that $Z(\mu, G')$ is (essentially) simply connected and nilpotent. We are now in what we term the "reduced almost algebraic case," which we look at in detail in the next section.

(iii) In order to be able to deduce the middle case from the almost algebraic case, we require the added complication in the almost algebraic proof of working throughout with a subset $E \subseteq P(G)$ which is a so called

admissible root set for μ (see [5, Section 5]). But in our discussion of the reduced almost algebraic case in the next section we choose to work throughout with $P(G)$ rather than with a general admissible root set for μ. We hope that this simplification will make the essential structure of the proof more transparent to the reader.

5 Proof for the Reduced Almost Algebraic Case

In this section we give a proof of the embedding theorem for the reduced almost algebraic case. Specifically we prove the following.

Theorem 5.1 *Let G be an almost algebraic group, and suppose that $\mu \in P(G)$ is infinitely divisible on G. Suppose also that $Z^0(\mu, G)$ contains an almost algebraic simply connected nilpotent Lie group L, with L normal in $N(\mu, G)$, such that $Z^0(\mu, G)/L$ is compact. Then there exists $m \in \mathbb{N}$ and $\nu \in R_m(\mu, G)$ such that, if $W = Z(Z^0(\nu, L), G)$ (i.e. the centraliser in G of the subgroup $Z^0(\nu, L)$), then ν is infinitely divisible and strongly root compact on W. Hence μ is continuously embedded on W, and so also on G.*

Two properties of nilpotent Lie groups

Definition 5.2 Let G be a topological group. We say that G is *affine root rigid* if the following condition holds: given any $m \in \mathbb{N}$, a sequence $\{\alpha_k\}_{k\geq 1}$ of continuous automorphisms of G and a sequence $\{h_k\}_{k\geq 1}$ in G such that

(i) $\alpha_k^m = \mathrm{Id}_G$ for all $k \in \mathbb{N}$ and

(ii) the sequence $\left\{\alpha_k(h_k)\,\alpha_k^2(h_k)\cdots\alpha_k^m(h_k)\right\}_{k\geq 1}$ is relatively compact,

there exist sequences $\{f_k\}_{k\geq 1}$ and $\{g_k\}_{k\geq 1}$ in G such that

(a) $h_k = g_k f_k$ for all $k \in \mathbb{N}$,

(b) $\{f_k\}_{k\geq 1}$ is relatively compact and

(c) $\alpha_k(g_k)\,\alpha_k^2(g_k)\cdots\alpha_k^m(g_k) = e$ where e is the identity element in G.

We note that if τ is an automorphism of a group G, such that $\tau^m = \mathrm{Id_G}$ and $g \in G$, then the element $\tau(g)\,\tau^2(g)\cdots\tau^m(g)$ of G is the same as the mth power of the affine automorphism τg in the usual multiplication in the group $\mathrm{Aff}(G)$ of affine automorphisms. The property above therefore signifies that if for a sequence of affine automorphisms $\{\alpha_k h_k\}_{k\geq 1}$ where

$\alpha_k^m = \mathrm{Id}_G$ for all k, the mth powers are bounded, then up to a bounded perturbation, $\{\alpha_k h_k\}_{k\geq 1}$ are actually solutions in $\mathrm{Aff}(G)$ of the equation $x^m = \mathrm{Id}_{\mathrm{Aff}}(G)$. This is the motivation for the term affine root rigidity.

Lemma 5.3 ([5, Theorem 4.2]) *Any connected nilpotent Lie group is affine root rigid.*

Lemma 5.4 (D-McC, unpublished) *Let N be a simply connected nilpotent Lie group, and suppose $\alpha \in \mathrm{Aut}(N)$ and $x \in N$ such that $\alpha^n = 1$ and $(\alpha x)^n = 1$ in $\mathrm{Aff}(N)$. Then there exists $y \in N$ such that $\alpha x = y\alpha y^{-1}$ in $\mathrm{Aff}(N)$.*

Proof We argue by induction of the nilpotent length of N.

Base case: $N = V$, a vector space. Then $\alpha \in \mathrm{Aut}(V)$, $x \in V$ and

$$\alpha^m = 1 = (\alpha x)^m \text{ in } \mathrm{Aff}(V).$$

Then

$$(\alpha x)^m = (\alpha x)(\alpha x)\cdots(\alpha x) = \left(\alpha x \alpha^{-1}\right)\left(\alpha^2 x \alpha^{-2}\right)\cdots\left(\alpha^m x \alpha^{-m}\right)\alpha^m = 1$$

and so in V

$$\alpha(x)\,\alpha^2(x)\cdots\alpha^m(x) = 1$$

in multiplicative notation. Switch to additive notation, to get

$$\left(\alpha + \alpha^2 + \cdots + \alpha^m\right)(x) = 0,$$

hence

$$\left(I + \alpha + \cdots + \alpha^{m-1}\right)(x) = 0. \tag{5.1}$$

Since α has finite order, we have a decomposition

$$V = U \oplus W$$

such that U, W are α-invariant, $\alpha|_W = id_W$, and $(I - \alpha)$ is invertible on W. All eigenvalues of $\alpha|_W$ are non-trivial mth roots of unity, so for all $t \in W$,

$$\left(I + \alpha + \cdots + \alpha^{m-1}\right)(t) = 0. \tag{5.2}$$

We write $x = x_1 + x_2$, $x_1 \in U$, $x_2 \in W$. Then by (5.1) and (5.2),

$$0 = \left(I + \alpha + \cdots + \alpha^{m-1}\right)(x_1 + x_2) = \left(1 + \alpha + \cdots + \alpha^{m-1}\right)(x_1) = mx_1,$$

from which we conclude $x_1 = 0$. Hence $x = x_2 \in W$. So $\alpha(x) \in W$, so as

$(I-\alpha)$ is invertible on W, there exists $y \in W$ such that

$$\alpha(x) = (I-\alpha)(y) = y - \alpha(y).$$

Going back to multiplicative notation gives

$$\alpha(x) = y\alpha\left(y^{-1}\right) \text{ in } V.$$

In $\mathrm{Aff}(V)$, this gives

$$\alpha x \alpha^{-1} = y\alpha y^{-1}\alpha^{-1},$$

so

$$\alpha x = y\alpha y^{-1},$$

as required.

Inductive step Now suppose the result is true for groups of nilpotent length d, and let N be of nilpotent length $d+1$ and write Z for the centre of N. Write $\overline{N} = N/Z$, which is of nilpotent length d. Suppose $\alpha \in \mathrm{Aut}(N)$ and $x \in N$ such that in $\mathrm{Aff}(N)$

$$(\alpha x)^m = 1 = \alpha^m.$$

As above, the condition $(\alpha x)^m = 1$ implies

$$\alpha(x)\alpha^2(x)\cdots\alpha^m(x) = 1 \text{ in } N. \tag{5.3}$$

Let $\overline{\alpha}$ be the automorphism of $\overline{N}$ induced by α, then by (5.3), for all $x \in N$,

$$\overline{\alpha}(\overline{x})\,\overline{\alpha}^2(\overline{x})\cdots\overline{\alpha}^m(\overline{x}) = 1 \text{ in } \overline{N},$$

and $\overline{\alpha}^m = id$ on $\overline{N}$. Therefore by inductive hypothesis, there exists $\overline{y} \in \overline{N}$ such that

$$\overline{\alpha}(\overline{x}) = \overline{y}\,\overline{\alpha}\left(\overline{y}^{-1}\right).$$

Then there exists $z \in Z$ such that

$$\alpha(x) = y\alpha\left(y^{-1}\right)z \text{ in } N. \tag{5.4}$$

We substitute this into (5.3) to give

$$\left(y\alpha\left(y^{-1}\right)z\right)\left(\alpha(y)\,\alpha^2\left(y^{-1}\right)\alpha(z)\right)\cdots\left(\alpha^{m-1}(y)\,\alpha^m\left(y^{-1}\right)\alpha^{m-1}(z)\right) = 1.$$

As z is central we can rearrange to get

$$z\alpha(z)\,\alpha^2(z)\cdots\alpha^{m-1}(z)\,y\alpha\left(y^{-1}\right)\alpha(y)\,\alpha^2\left(y^{-1}\right)\alpha^2(y)\cdots$$
$$\alpha^{m-1}\left(y^{-1}\right)\alpha^{m-1}(y)\,\alpha^m\left(y^{-1}\right) = 1.$$

Therefore

$$z\alpha(z)\,\alpha^2(z)\cdots\alpha^{m-1}(z)\,y\alpha^m\left(y^{-1}\right)=1.$$

Since $\alpha^m=1$, this gives

$$z\alpha(z)\cdots\alpha^{m-1}(z)=1,$$

whence $\alpha(z)\cdots\alpha^m(z)=1$, so $(\alpha z)^m=1$ in $\mathrm{Aff}(Z)$. By the result of base case (since Z is a vector space) we see there exists $w\in Z$ such that

$$\alpha z=w\alpha w^{-1}\,(\text{in Aff}(Z)).$$

Therefore

$$\alpha(z)=w\alpha\left(w^{-1}\right)\ \text{in } Z. \tag{5.5}$$

From (5.4) and (5.5),

$$\alpha(x)=y\alpha\left(y^{-1}\right)z \text{ in } N \text{ and } z=w^{-1}\alpha^{-1}(w) \text{ in } Z.$$

So in N,

$$\begin{aligned}\alpha(x)=y\alpha\left(y^{-1}\right)w^{-1}\alpha^{-1}(w)&=y\alpha^{-1}(w)\,\alpha\left(y^{-1}\right)\alpha\left(\alpha^{-1}\left(w^{-1}\right)\right)\\&=y\alpha^{-1}(w)\,\alpha\left(y^{-1}\left(\alpha^{-1}(w)\right)^{-1}\right).\end{aligned}$$

Set $t=y\alpha^{-1}(w)$, to give

$$\alpha(x)=t\alpha\left(t^{-1}\right)\ \text{in } N,$$

or in $\mathrm{Aff}(N)$,

$$\alpha x\alpha^{-1}=t\alpha t^{-1}\alpha^{-1},\ \text{ so }\ \alpha x=t\alpha t^{-1},$$

as required.

□

Proof of Theorem 5.1

Step 1. Construction of a root set sequence. Let L be the subgroup as in the hypothesis of Theorem 5.1. Let $L=L_0\supseteq L_1\supseteq\cdots\supseteq L_n=\{e\}$ denote the usual central series of L. Let $\underline{L}$ be the Lie algebra of L and for each $j=0,\ldots,n$ let $\underline{L}_j$ be the Lie subalgebra of $\underline{L}$ corresponding to L_j. We define a homomorphism $p:N(\mu,G)\to\mathrm{Aut}(L)$, where $\mathrm{Aut}(L)$ is the group of Lie automorphisms of L, by $p(x)(h)=xhx^{-1}$ for all x $\in$ N(μ,G) and $h\in L$. For each $x\in N(\mu,G)$, $p(x)$ leaves invariant L_j, for all j, and hence induces quotient automorphisms on L_{j-1}/L_j, $1\le j\le n$. Let $p_j:N(\mu,G)\to\mathrm{Aut}(L_{j-1}/L_j)$, where $1\le j\le n$, be the homomorphism

such that for all $x \in N(\mu, G)$, $p_j(x)$ is the quotient of $p(x)$ on L_{j-1}/L_j; namely $p_j(x)(hL_j) = p(x)(h)L_j = xhx^{-1}L_j$ for all $h \in L_{j-1}$.

For each $j = 1, \ldots, n$ let $\delta_j : \mathrm{Aut}(L_{j-1}/L_j) \to \mathrm{Aut}(\underline{L}_{j-1}/\underline{L}_j)$ be the homomorphism associating to each Lie group automorphism its derivative, and write $\widetilde{p}_j$ for $\delta_j p_j$.

Clearly $\widetilde{p}_j(\mu)$ is the point mass at the identity automorphism of $\underline{L}_{j-1}/\underline{L}_j$. This implies that for any root λ of μ, $\widetilde{p}_j(\lambda)$ is a point mass at an element of finite order in $\mathrm{Aut}\left(\underline{L}_{j-1}/\underline{L}_j\right)$; we write $d_j(\lambda)$ for the dimension of the 1-eigenspace of the automorphism of $\underline{L}_{j-1}/\underline{L}_j$ supporting $\widetilde{p}_j(\lambda)$, for each $1 \leq j \leq n$, and we denote by $d(\lambda)$ the ordered n-tuple $(d_1(\lambda), d_2(\lambda), \ldots, d_n(\lambda))$.

□

Proposition 5.5 *Let $\{m_k\}$ be a sequence of positive integers. Then there exists a sequence $\{R_k^*(\mu)\}$ of closed subsets of $P(G)$ such that the following conditions are satisfied:*

(i) $R_0^*(\mu) = \{\mu\}$;
(ii) *if $k \geq 1$ and $\lambda \in R_k^*(\mu)$ then $\lambda^{m_k} \in R_{k-1}^*(\mu)$;*
(iii) *if $\lambda_1, \lambda_2 \in R_k^*(\mu)$, for some $k \geq 1$, then $d(\lambda_1) = d(\lambda_2)$;*
(iv) *if $\lambda \in R_k^*(\mu)$, for some $k \geq 1$, and $\nu \in P(G)$ is such that*

a) $\nu^{m_1 m_2 \cdots m_k} = \mu$, *and*
b) $(\widetilde{p}_1(\lambda), \widetilde{p}_2(\lambda), \ldots, \widetilde{p}_n(\lambda)) = (\widetilde{p}_1(\nu), \widetilde{p}_2(\nu), \ldots, \widetilde{p}_n(\nu))$,

then $\nu \in R_k^*(\mu)$;
(v) *for all $k \geq 1$ and $q \geq 1$ there exists a $\lambda \in P(G)$ such that $\lambda^q \in R_k^*(\mu)$.*

Proof We construct the sequence $R_k^*(\mu)$ inductively. Let $R_0^*(\mu) = \{\mu\}$. To define $R_1^*(\mu)$ we write

$$R_1(\mu) = \{\lambda \in P(G) : \lambda^{m_1} = \mu\},$$

and we note that infinite divisibility of μ on G implies that $R_1(\mu) \neq \{\emptyset\}$ and

$$\text{for all } n \geq 1 \text{ there exists } \nu \in P(G) \text{ such that } \nu^n \in R_1(\mu). \tag{5.6}$$

The set $\{d(\lambda) : \lambda \in R_1(\mu)\}$ is clearly finite (its cardinality is no more than $(a+1)^n$, where $a = \dim L$); let its distinct elements be $d_1, d_2, \ldots, d_{r_1}$, and for $1 \leq j \leq r_1$ write

$$R_1(\mu, d_j) = \{\lambda \in R_1(\mu) : d(\lambda) = d_j\}.$$

Then

$$R_1(\mu) = \bigcup_{j=1}^{r_1} R_1(\mu, d_j) \text{ (disjointly).} \tag{5.7}$$

We claim that for some $1 \leq j \leq r_1$, $R_1(\mu, d_j)$ contains an n-divisible element for all $n \geq 1$. For if not then for each $1 \leq j \leq r_1$, we can find N_j such that no element of $R_1(\mu, d_j)$ is N_j-divisible, and if we set $N = \prod_{j=1}^{r_1} N_j$, then by (5.7), no element of $R_1(\mu)$ is N-divisible, which contradicts (5.6).

We can therefore select $1 \leq j_o \leq r_1$, such that for all $n \geq 1, R_1(\mu, d_{j_o})$ contains an n-divisible element, and we write $R_1^*(\mu)$ for $R_1(\mu, d_{j_o})$. It is easy to check that $R_1^*(\mu)$ is closed in $P(G)$ and that (ii), (iii), (iv), (v) of the statement of the proposition hold good for $k = 1$.

We now show how to construct $R_{s+1}^*(\mu)$, given that $R_0^*(\mu), \ldots, R_s^*(\mu)$ have already been defined, and that conditions (i), (ii), (iii), (iv), (v) hold for all $0 \leq k \leq s$.

Write $R_1(R_s^*(\mu)) = \{\lambda \in P(G) : \lambda^{m_{s+1}} \in R_s^*(\mu)\}$, and note that by property (v) for s, $R_1(R_s^*(\mu))$ contains n-divisible elements for all $n \in \mathbb{N}$. The set $\{d(\lambda) : \lambda \in R_1(R_s^*(\mu))\}$ is finite; let its distinct elements be $d_1, d_2, \ldots, d_{r_{s+1}}$. If we write

$$R_1(R_s^*(\mu), d_j) = \{\lambda \in R_1(R_s^*(\mu)) : d(\lambda) = d_j\}$$

then

$$R_1(R_s^*(\mu)) = \bigcup_{j=1}^{r_{s+1}} R_1(R_s^*(\mu), d_j),$$

where the right hand side is a disjoint union of closed subsets of $P(G)$. An argument as before shows that there is some $1 \leq j_s \leq r_{s+1}$ such that $R_1(R_s^*(\mu), d_{j_s})$ contains an n-divisible element for all $n \in \mathbb{N}$. We set $R_{s+1}^*(\mu) = R_1(R_s^*(\mu), d_{j_s})$.

Clearly (i), (ii), (iii), (v) hold for $k = s + 1$, so it remains to check (iv). So suppose $\lambda = R_{s+1}^*(\mu)$ and $\nu \in P(G)$ such that $\nu^{m_1 m_2 \cdots m_{s+1}} = \mu$, and

$$(\widetilde{p}_1(\lambda), \widetilde{p}_2(\lambda), \ldots, \widetilde{p}_n(\lambda)) = (\widetilde{p}_1(\nu), \widetilde{p}_2(\nu), \ldots, \widetilde{p}_n(\nu)), \tag{5.8}$$

By property (ii), $\lambda^{m_{s+1}} \in R_s^*(\mu)$, and

$$(\widetilde{p}_1(\lambda^{m_{s+1}}), \widetilde{p}_2(\lambda^{m_{s+1}}), \ldots, \widetilde{p}_n(\lambda^{m_{s+1}})) = (\widetilde{p}_1(\nu^{m_{s+1}}), \widetilde{p}_2(\nu^{m_{s+1}}), \ldots, \widetilde{p}_n(\nu^{m_{s+1}})),$$

so by property (iv) for $k = s$, we conclude that $\nu^{m_{s+1}} \in R_s^*(\mu)$. Also by (5.8), $d(\nu) = d(\lambda)$, so by construction of $R_{s+1}^*(\mu)$, we get $\nu \in R_{s+1}^*(\mu)$. This completes the proof of the proposition.

□

We now choose and fix a sequence $\{m_k\}$ of positive integers with the property that for each positive integer q there exists an integer r such that q divides $m_1 m_2 \cdots m_r$. Let $R_k^*(\mu)$ be a corresponding root set sequence chosen according to Proposition 5.5 above.

Step 2. A relatively compact sequence of roots. For each $k \geq 1$ and $1 \leq j \leq n$, let $d_{j,k}$ be the dimension of the 1-eigenspace of (equivalently, of the largest subspace which is pointwise fixed by) the automorphism supporting $\widetilde{p}_j(\lambda)$, λ being any element of $R_k^*(\mu)$; by property (iii) of the sequence $\{R_k^*(\mu)\}_{k\geq 0}$, the dimension of the 1-eigenspace is independent of which λ we choose in $R_k^*(\mu)$. By property (ii) of $\{R_k^*(\mu)\}_{k\geq 0}$ we get that $d_{j,k+1} \leq d_{j,k}$ for all $j = 1, \ldots, n$ and all $k \geq 0$. Therefore there exists a positive integer K such that $d_{j,k} = d_{j,K}$ for all $j = 1, \ldots, n$ and all $k \geq K$.

We note that this condition on K is equivalent to the condition that $\sum_{j=1}^n d_{j,k} = \sum_{j=1}^n d_{j,K}$, for all $k \geq K$. We also note that since $\widetilde{p}(\lambda)$ is of finite order in $\mathrm{Aut}(\underline{L})$, for each $\lambda \in R_k^*(\mu)$, the dimension of the subspace of fixed points of $\widetilde{p}(\lambda)$ equals $\sum_{j=1}^{n} d_{j,k}$, and so

$$\dim Z^0(\lambda, L) = \sum_{j=1}^{n} d_{j,k}.$$

So the choice of K ensures that for all $k \geq K$ and all $\lambda \in R_k^*(\mu)$, the dimension of $Z^0(\lambda, L)$ is constant.

For each $k \geq 1$ we now select a $\lambda_k \in R_{k+K}^*(\mu)$ and write $\nu_k = \lambda_k^{r_k}$, where $r_k = m_{K+1} \cdots m_{K+k}$; by property (ii) of the root set sequence $\nu \in R_K^*(\mu)$. By Theorem 2.3 (the AFC theorem), $R(\mu, G)$ is relatively compact modulo $Z(\mu, G)$, so is relatively compact modulo $Z^0(\mu, G)$, since $Z(\mu, G)/Z^0(\mu, G)$ is finite. But by hypothesis, $Z^0(\mu, G)/L$ is compact, so $R(\mu, G)$ is relatively compact modulo L. Hence by shift compactness (cf. [20, Theorem 2.2, Chapter III]) there exists a sequence $\{h_k\}$ in L such that $\{\nu_k h_k : k \geq 1\}$ is relatively compact. Let $m = m_1 m_2 \cdots m_K$, then $\{(v_k h_k)^m : k \geq 1\}$ is also relatively compact.

We now need the following proposition.

Proposition 5.6 *Let $\nu \in P(G)$ be of the form λg where $\operatorname{supp}\lambda \subseteq \ker p$ and $g \in G$. Then for each $r \geq 1$ and all $x \in L$,*

$$(\nu x)^r = p(\nu)(x)\, p(\nu)^2(x) \cdots p(\nu)^r(x)\, \nu^r.$$

In particular this equation holds for any root ν of μ.

Proof As for [4, Proposition 2], and Proposition 2.1(i) above.

By the proposition and the fact that $\nu_k^m = \mu$ we have

$$(\nu_k h_k)^m = p(\nu_k)(h_k)\cdots p(\nu_k)^m(h_k)\,\mu \text{ for all } k \geq 1.$$

By our observation above, this implies that

$$\{p(\nu_k)(h_k)\cdots p(\nu_k)^m(h_k)\,|k \geq 1\}$$

is a relatively compact subset of L. Since L is a nilpotent Lie group, it is affine root rigid (cf. Lemma 5.3) and therefore under the above condition there exist sequences $\{f_k\}_{k\geq 1}$ and $\{g_k\}_{k\geq 1}$ in L such that $h_k = g_k f_k$ for all for all $k \geq 1$, $\{f_k|k \geq 1\}$ is relatively compact and

$$p(\nu_k)(g_k)\cdots p(\nu_k)^m(g_k) = 1 \text{ for all } k \geq 1.$$

We now have $p(\nu_k)^m = 1$ in $\mathrm{Aut}(L)$ and $(p(\nu_k)g_k)^m = 1$ in $\mathrm{Aff}L$, so by Lemma 5.4, for all $k \geq 1$ there exists x_k in L such that

$$p(\nu_k)g_k = x_k p(\nu_k) x_k^{-1}. \tag{5.9}$$

But by Proposition 2.1(i), we can write $\nu_k = \sigma_k a_k$, with $\mathrm{supp}\sigma_k \subseteq G(\mu)$ and $a_k \in N(\mu, G)$, and then $p(\nu_k) = p(a_k)$, for all $k \geq 1$. Then by (5.9), for all $k \geq 1$,

$$x_k \nu_k x_k^{-1} = \left(x_k \sigma_k x_k^{-1}\right) x_k a_k x_k^{-1} = \sigma_k a_k g_k = \nu_k g_k.$$

Since $\{\nu_k h_k : k \geq 1\}$ and $\{f_k : k \geq 1\}$ are relatively compact, so is $\{\nu_k g_k : k \geq 1\}$. Since $\widetilde{p}_j(g_k)$ is the identity automorphism for all $1 \leq j \leq n$, and $\nu_k \in R_K^*(\mu)$, we deduce from (iv) of Proposition 5.5 that $\nu_k g_k \in R_K^*(\mu)$, for all $k \geq 1$. We now write

$$C = \overline{\{\nu_k g_k : k \geq 1\}} = \overline{\left\{x_k \nu_k x_k^{-1} : k \geq 1\right\}}$$

and we note that C is a compact subset of $R_K^*(\mu)$.

□

Step 3. Compactness of the set $S_k(C)$. We now write, for all $k \geq 1$,

$$S_k(C) = \left\{\alpha \in R_{K+k}^*(\mu) : \alpha^{r_k} \in C\right\},$$

where as above, $r_k = m_{K+1}\cdots m_{K+k}$.

We note that since $\widetilde{p}_j(x_k)$ is the identity automorphism, for all $1 \leq j \leq n$, and $\lambda_k \in R_{K+k}^*(\mu)$, by (iv) of Proposition 5.5, $x_k \lambda_k x_k^{-1} \in R_{K+k}^*(\mu)$, and

$$\left(x_k \lambda_k x_k^{-1}\right)^{r_k} = x_k \nu_k x_k^{-1} \in C.$$

Hence $x_k\lambda_k x_k^{-1} \in S_k(C)$, and $S_k(C)$ is nonempty. Since C is compact and $R^*_{K+k}(\mu)$ is closed, it is also clear that $S_k(C)$ is closed.

Suppose $S_k(C)$ is not compact, then $S_k(C)$ contains a sequence $\{\alpha_q : q \geq 1\}$ which is not relatively compact. By the hypothesis of Theorem 5.1 and shift compactness, we can find a sequence $\{y_q\}_{q\geq 1}$ in L such that $\{\alpha_q y_q : q \geq 1\}$ is relatively compact, and then $\{y_q\}_{q\geq 1}$ is not relatively compact. Then there exists a largest index $1 \leq l \leq n$ such that $\{y_q L_{l-1} : q \geq 1\}$ is relatively compact in L/L_{l-1}. By translating on the right by a bounded sequence, we may assume without loss of generality that $y_q \in L_{l-1}$ for all $q \geq 1$.

By Proposition 5.6, we have for all $q \geq 1$

$$(\alpha_q y_q)^{r_k} = p(\alpha_q)(y_q)\, p(\alpha_q)^2(y_q)\cdots p(\alpha_q)^{r_k}(y_q)\,\alpha_q^{r_k}.$$

Since $\{\alpha_q^{r_k} | q \geq 1\}$ is contained in C, it is a relatively compact subset. Since $\{(\alpha_q y_q)^{r_k} | q \geq 1\}$ is also relatively compact, by choice, the above equation implies that $\{p(\alpha_q)(y_q)\cdots p(\alpha_q)^{r_k}(y_q) | q \geq 1\}$ is a relatively compact subset of L_{l-1}. Hence $\{p(\alpha_q)(y_q)\cdots p(\alpha_q)^{r_k}(y_q) L_l | q \geq 1\}$ is a relatively compact subset of L_{l-1}/L_l.

Since $y_q \in L_{l-1}$ we have $p_l(\alpha_q) = p_l(\alpha_q y_q)$ for all $q \geq 1$ and, since $\{\alpha_q y_q | q \geq 1\}$ is relatively compact, this implies that $\{p_l(\alpha_q) | q \geq 1\}$ is a relatively compact subset of $\mathrm{Aut}(L_{l-1}/L_l)$. Hence $\{\widetilde{p}_l(\alpha_q) | q \geq 1\}$ is a relatively compact subset of $\mathrm{Aut}\left(\underline{L}_{l-1}/\underline{L}_l\right)$. It follows that the set

$$T := \left\{ \sum_{s=1}^{r_k} \widetilde{p}_l(\alpha_q)^s \,|\, q \geq 1 \right\}$$

is a relatively compact subset of $\mathrm{End}\left(\underline{L}_{j-1}/\underline{L}_j\right)$.

Proposition 5.7 *There exists some $c > 0$ such that $\det(\beta) \geq c$, for all $\beta \in T$.*

Proof Let L_q be the 1-eigenspace of $\widetilde{p}_l(\alpha_q)$, and note that since $\alpha_q \in R^*_{K+k}(\mu)$, we have $\dim L_q = r$ (say), for all $q \geq 1$. Also $\alpha_q^{r_k} \in R^*_K(\mu)$, so by choice of K, the dimension of the 1-eigenspace of $\widetilde{p}_l\left(\alpha_q^{r_k}\right)$ is also r, and so L_q is also the 1-eigenspace of $\widetilde{p}_l\left(\alpha_q^{r_k}\right)$.

Let L_q^* be the unique $\widetilde{p}_l(\alpha_q)$-invariant subspace of L_{l-1}/L_l such that $\underline{L}_{l-1}/\underline{L}_l = L_q \oplus L_q^*$, then if we write M_l for $\underline{L}_{l-1}/\underline{L}_l$, we have

$$\overline{M}_l = \overline{L}_q \oplus \overline{L_q^*},$$

where the bar denotes complexification. Thinking of $\widetilde{p}_l(\alpha_q)$ as a linear map on $\overline{M}_l$, we can find a $\mathbb{C}$-basis $\{x_{q,1}, \ldots, x_{q,r}\}$ of $\overline{L}_q$, and a $\mathbb{C}$-basis

$\{y_{q,1}, \ldots, y_{q,t}\}$ of $\overline{L_q^*}$ (where $r + t = \dim \overline{M}_l$), with both bases consisting of eigenvectors of $\widetilde{p}_l(\alpha_q)$. Let $\beta_{q,j}$ be the eigenvalue of $\widetilde{p}_l(\alpha_q)$ corresponding to $y_{q,j}$, then clearly $\beta_{q,j} \neq 1$, but $\beta_{q,j}$ is a root of unity since $\widetilde{p}_l(\alpha_q)$ has finite order. Then

$$\sum_{s=1}^{r_k} \widetilde{p}_l(\alpha_q)^s (x_{j,i}) = r_k x_{j,i} \qquad (1 \leq i \leq r)$$

and

$$\sum_{s=1}^{r_k} \widetilde{p}_l(\alpha_q)^s (y_{q,j}) = (\beta_{q,j}\left(1 - \beta_{q,j}^{r_k}\right) / (1 - \beta_{q,j}))(y_{q,j}) \qquad (1 \leq j \leq t).$$

We note that $\beta_{q,j}^{r_k}$ is an eigenvalue of $\widetilde{p}_l\left(\alpha_q^{r_k}\right)$, but cannot equal 1 since $\overline{L}_q$ is also the 1-eigenspace of $\widetilde{p}_l\left(\alpha_q^{r_k}\right)$ (complexified). We conclude that for all $q \geq 1$,

$$\det\left[\sum_{s=1}^{r_k} \widetilde{p}_l(\alpha_q)^s\right] = r_k^r \prod_{j=1}^{t} [\beta_{q,j}(1 - \beta_{q,j}^{r_k})/(1 - \beta_{q,j})].$$

Since $\alpha_q^{r_k} \in R_K^*(\mu)$, $\beta_{q,j}^{r_k}$ is a nontrivial mth root of 1, hence for all $1 \leq j \leq t$ and for all $q \geq 1$,

$$|\beta_{q,j}\left(1 - \beta_{q,j}^{r_k}\right) / (1 - \beta_{q,j})| \geq \sin\frac{\pi}{m}.$$

Then for all $q \geq 1$,

$$\det\left[\sum_{s=1}^{r_k} \widetilde{p}_l(\alpha_q)^s\right] \geq r_k^r \left(\sin\frac{\pi}{m}\right)^t,$$

and setting $c = r_k^r \left(\sin\frac{\pi}{m}\right)^t$ completes Proposition 5.7.

□

Proposition 5.7 now implies that T is a relatively compact subset of $\mathrm{Aut}\left(\underline{L}_{l-1}/\underline{L}_l\right)$. By exponentiation this implies that if for all $q \geq 1$, $\tau_q \in \mathrm{Aut}\left(L_{l-1}/L_l\right)$ is the automorphism defined by

$$\tau_q(xL_l) = p_l(\alpha_q)(xL_l) \cdots p_l(\alpha_q)^{r_k}(xL_l)$$

for all $x \in L$, then $\{\tau_q | q \geq 1\}$ is a relatively compact subset of $\mathrm{Aut}\left(L_{l-1}/L_l\right)$.

Recall that $\{p_l(\alpha_q)(y_qL_l) \cdots p_l(\alpha_q)^{r_k}(y_qL_l) : q \geq 1\}$ is relatively compact. Hence the preceding conclusion implies that $\{y_qL_l : q \geq 1\}$ is a relatively compact subset of L_{l-1}/L_l and hence of L/L_l. But this contradicts

the choice of l. The contradiction shows that $S_k(C)$ must indeed be compact.

Step 4. The target measure ν and its embedding. We now write $C_k = \{\alpha^{r_k} : \alpha \in S_k(C)\}$, then each C_k is non-empty and compact, and by the properties of $\{R_k^*(\mu)\}_{k\geq 0}$ the $\{C_k\}_{k\geq 1}$ are decreasing. Hence there exists $\nu \in \bigcap_{k=1}^{\infty} C_k$. We write

$$W = Z\left(Z^0(\nu, L), G\right) = \left\{y \in G : yx = xy, \text{ for all } x \in Z^0(\nu, L)\right\}.$$

We shall now show that ν is infinitely divisible and strongly root compact on W.

Recall that by the choice of sequence $\{m_k\}_{k\geq 1}$ for any $q \in \mathbb{N}$ there exists a $r \in \mathbb{N}$ such that q divides $m_1 m_2 \cdots m_r$. It follows therefore that for any $n \in \mathbb{N}$ there exists a $k \in \mathbb{N}$ such that n divides $r_k = m_{K+1} m_{K+2} \cdots m_{K+k}$; choose $q = n(m_1 m_2 \cdots m_K)$ to see this. In view of this, to prove infinite divisibility of ν on W it is enough to prove that for each $k \in \mathbb{N}$, ν has an r_k-th root on W. Let $k \in \mathbb{N}$ be given. The choice of ν shows that there exists a $\lambda \in R_{K+k}^*(\mu)$ such that $\lambda^{r_k} = \nu$. We shall show that $\mathrm{supp}\lambda \subseteq W$.

We observed at step 2 that for all $k \geq K$, all $\lambda \in R_k^*(\mu)$, the dimension of $Z^0(\lambda, L)$ is constant. Since clearly $Z^0(\lambda, L) \subseteq Z^0(\nu, L)$, and both groups are connected, we conclude $Z^0(\lambda, L) = Z^0(\nu, L)$. Then

$$\mathrm{supp}\lambda \subseteq Z\left(Z^0(\lambda, L), G\right) = Z\left(Z^0(\nu, L), G\right) = W,$$

and λ is supported on W. Hence ν is infinitely divisible on W.

We now need to check that $F(\nu, W)/Z^0(\nu, L) \cap W$ is relatively compact in $P\left(W/Z^0(\nu, L) \cap W\right)$. The argument to show this depends on Theorem 2.3(i) applied to G; full details are given in the last two paragraphs of page 254 of [5], to which the (still) interested reader is referred.

The proof of the theorem is now completed by observing that since any root of ν in W belongs to $F(\nu, W)$, and $Z^0(\nu, L) \cap W$ is a compactly generated central subgroup of W, the strong root compactness of ν on W is assured by Proposition 3.12.

□

Remark on the proof of Theorem 5.1. The proof we have given above is mostly taken directly from the proof of [5, Theorem 5.1]. However, there are some differences.

(i) The use of Lemma 5.4 is new, and it avoids the need to use the concept of *affine root divisibility* introduced in [5]. It also highlights the fact

the set $\{\nu_k g_k : k \geq 1\}$ of m -roots of μ can be rewritten as conjugates of $\{\nu_k : k \geq 1\}$ by elements of L.

(ii) The construction of the root set sequence is different, in that in [5] two elements in $R_k^*(\mu)$ have to have the same spectrum, but here we require only that the dimensions of the 1-eigenspaces of the measures in $R_k^*(\mu)$, acting on the abelian quotients of $\underline{L}$, are the same.

6 Measures on Semigroups

Although there is an extensive theory of probabilities on locally compact semigroups ([9], [19]), it is only recently (in the thesis of Seth Walker [24]) that a start has been made on the embedding problem for probabilities on semigroups. Even when the semigroup is a subsemigroup of a linear connected Lie group, the problem seems very difficult.

For a (locally compact Hausdorff) topological semigroup S, we write $P(S)$ for the topological semigroup of probabilities on S, with the weak topology and convolution as the multiplication. The concepts presented in Definition 3.1 for groups carry over verbatim to semigroups, so making sense of notations such as $R_n(\mu, S)$ for $\mu \in P(S)$, and giving rise to the sets

$$I(S) = \{\mu \in P(S) : \mu \text{ is infinitely divisible on } S\}$$

and

$$E(S) = \{\mu \in P(S) : \mu \text{ is continuously embedded on } S\}.$$

We may then ask which semigroups S have the *embedding property* (i.e. $I(S) = E(S)$), or which have the *point embedding property* (i.e. $E(S) \cap S = I(S) \cap S$).

By a *subsemigroup* of a locally compact group G we shall mean a closed subset S of G which contains the identity, and is closed under multiplication.

Remark 6.1 The existence of the discrete subgroup D of $SL(2, \mathbb{R})$ mentioned in Remark 4.5(i) shows that the point embedding property is not possessed by all subsemigroups of a connected Lie group G. But a natural question to ask is whether every connected subsemigroup of a connected Lie group has the point embedding property. Even this fails spectacularly.

Example 6.2 ([24, Theorem 89]) Let D be the subsemigroup of $SL(2, \mathbb{R})$ as in Remark 6.1, and form the subset S of $GL^+(2, \mathbb{R})$ given by

$$S = [1, 2]\, D \cup [2, \infty) SL(2, \mathbb{R}).$$

It is easy to check that S is a closed subsemigroup of $GL^+(2,\mathbb{R})$, and contains the element $-I$, which is infinitely divisible on S by Remark 4.5(i). Clearly $C = [2,\infty)SL(2,\mathbb{R})$ is path connected, and for any $A \in [1,2]\,D$, the path $[1,2]\,A$ connects A to a point in C. Hence S is (path) connected. However, $-I$ is not continuously embedded on S, for if $\theta : \mathbb{R}_+ \to S$ is a continuous homomorphism such that $\theta(1) = -I$, then $t \mapsto |\,\theta(t)\,|$ is a continuous homomorphism of $(\mathbb{R}_+,+)$ into $(\mathbb{R}_+,\times)$ such that $\theta(1) = 1$, hence $|\,\theta(t)\,| = 1$ for all$t \in \mathbb{R}_+$. Then

$$\theta(t) \in SL(2,\mathbb{R}) \cap S = D \quad \text{for all } t \in \mathbb{R}_+,$$

and $-I$ is continuously embedded on D, contradicting discreteness of D. Walker calls this semigroup S the *discrete comb*.

Proposition 6.3 ([18, Theorem 2.1]) *Let S be a subsemigroup of a connected Lie group, and suppose $\mu \in I(S)$, with μ root compact on S. Then $\mu \in E(S)$.*

Proof The same argument as in Theorem 3.2(i) gives a rational embedding $t \to \mu_t$ of $\mathbb{Q}_+^*$ into $P(S)$ such that $\mu_1 = \mu$, and the result now goes through as for Corollary 3.7(ii), because the accumulation group $K((\mu_t))$ remains within $P(S)$.

□

Corollary *Let G be a connected Lie group in which every $\mu \in P(G)$ is root compact on G. Then every closed subsemigroup S of G has the embedding property. In particular any closed subsemigroup of any connected nilpotent Lie group has the embedding property.*

In view of Example 6.2 above, the next result seems rather surprising.

Proposition 6.4 *Any connected subsemigroup of $SL(2,\mathbb{R})$ has the embedding property.*

Proof The details, which are quite elementary, are contained in Proposition 2.3, 2.4 and Remark 2.5 of [18]. The point is that because the dimension is small there are only two types of measure which are not strongly root compact on $G = SL(2,\mathbb{R})$, and these can be dealt with by ad hoc argument.

□

Definition 6.5 Let S be a closed subsemigroup of a locally compact group G, then the *edge of S* is the set

$$H(S) = S \cap S^{-1} \supseteq \{1\}.$$

Example 6.6 Let S be the semigroup S of Example 6.2. Then $H(S) = D$, the discrete subgroup of $SL(2, \mathbb{R})$, as in Remark 6.1. Hence S has a discrete edge.

Definition 6.7 A subsemigroup S of a group G is called *pointed* if and only if $H(S) = \{1\}$.

Proposition 6.8 ([18, Proposition 3.2]) *If S is a pointed subsemigroup of $G = SL(2, \mathbb{C})$, then every $\mu \in P(S)$ is strongly root compact on S, and so S has the embedding property.*

Problem C For which connected Lie groups G is it true that for each pointed subsemigroup S of G, every $\mu \in P(S)$ is (strongly) root compact on S?

Example 6.9 For $\alpha, \beta \in \mathbb{R}$ with $\beta > 0$, let us denote by G_α the simply connected solvable Lie group which is $\mathbb{C} \times \mathbb{R}$, with multiplication

$$(c, s)(d, t) = \left(c + e^{\alpha i s} d, s + t\right)$$

and write

$$S_\beta = \{(c, t) \in G_\alpha : |c| \leq \beta t\}.$$

Then S_β is a closed subsemigroup of G_α, which is pointed.

An elementary argument shows that S_β has the property that every $\mu \in P(S_\beta)$ is strongly root compact on S_β, whereas, if $\alpha \neq 0$, the smallest group containing S_β, G_α, is not itself strongly root compact. To see this, we note that the root set of the point mass at $(0, 2\pi/\alpha)$ contains the unbounded set of point masses $\{(c, \pi/\alpha) : c \in \mathbb{C}\}$.

We now write G_1 for the subgroup of upper triangular matrices in $SL(2, \mathbb{C})$.

Proposition 6.10 ([18, Theorem 3.4]) *Let S be a subsemigroup of G_1, and suppose that $H(S)$ is connected. Then S has the embedding property.*

Problem D For which connected Lie groups G is it true that every subsemigroup S of G which has a connected edge has the embedding property?

Definition 6.11 A subsemigroup S of a group G is called *invariant* if and only if $xSx^{-1} \subseteq S$, for all $x \in G$.

Theorem 6.12 ([18, Theorem 4.1]) *Let S be an invariant subsemigroup of a connected semisimple Lie group G. Then S has the point embedding property.*

Proof It is enough to show that for $x \in I(S) \cap S$ and all $n \in \mathbb{N}$, x has an nth root, $y \in S$, such that $y \in I(S)$. For given $x \in I(S) \cap S$, we can use this property repeatedly to construct a sequence $(y_m)_{m \geq 1}$ in $I(S) \cap S$ such that

$$y_1 = x \text{ and } (y_{m+1})^{m+1} = y_m \text{ for all } m \in \mathbb{N}.$$

If we then write, for $p, q \in \mathbb{N}$,

$$x(p/q) = (y_q)^{p(q-1)!},$$

then $r \mapsto x(r)$ is a well-defined homomorphism from $\mathbb{Q}_+^*$ into S, with $x(1) = x$. The conclusion that $x \in E(S)$ now follows from Theorem 2.7 and Theorem 3.6.

Fix $x \in I(S)$. For all $n \in \mathbb{N}$ write $\{R_{n,i} : i \in I_n\}$ for the set of conjugacy classes of $R_n(x, G)$ that intersect S non-trivially; as $x \in I(S)$ this is non-empty. Theorem 1 of [14] implies that we may choose $I_n = \{1, \ldots, l_n\}$ for some $l_n \in \mathbb{N}$. Also, as S is invariant,

$$R_{n,i} \subseteq S$$

for all $n \in \mathbb{N}$ and $1 \leq i \leq l_n$ giving that

$$R_n(x, S) = \bigcup_{i=1}^{l_n} R_{n,i}. \tag{6.1}$$

Now fix $n \in \mathbb{N}$. As $x \in I(S)$, there exists $y_k \in R_{k!n}(x, S)$ for all $k \in \mathbb{N}$. By (6.1), infinitely many of the elements from $\left\{(y_k)^{k!} : k \in \mathbb{N}\right\}$ lie in $R := R_{n,i}$ for some i. Note that choosing R like this means that for all $m \in \mathbb{N}$, there exists an $x_m \in S$ such that $(x_m)^m \in R$.

Choose $y \in R$. As all elements of R are conjugate, for all $m \in \mathbb{N}$ there exists a $z_m \in G$ such that

$$y = z_m (x_m)^m z_m^{-1} = \left(z_m x_m z_m^{-1}\right)^m$$

and as S is invariant, $z_m x_m z_m^{-1} \in R_m(y, S)$, as required.

□

Definition 6.13 For a subsemigroup S in a connected Lie group G we define the *tangent wedge* of S, denoted by $L(S)$, by

$$L(S) = \{X \in L(G) : \exp \mathbb{R}_+ X \subseteq S\},$$

where $L(G)$ is the Lie algebra of G. We say that a subsemigroup S is a *Lie subsemigroup* of G to mean that $S =< \exp L(S) >$, i.e. S is the smallest closed subsemigroup of G containing $\exp L(S)$.

Theorem 6.14 ([18, Theorem 4.3]) *Let S be a pointed, invariant, Lie subsemigroup of a simply connected solvable Lie group G. Then S has the point embedding property.*

Proposition 6.15 *The semigroup* $\mathrm{End}\,(V)$*, where V is a finite-dimensional real vector space, has the point embedding property.*

Proof We recall that if V is a finite-dimensional vector space and $A \in \mathrm{End}\,(V)$, there exists a unique direct sum decomposition $V = I_A \oplus N_A$ such that I_A, N_A are A-invariant, $A_{|I_A}$ is invertible and $A_{|N_A}$ is nilpotent.

Suppose $A \in \mathrm{End}\,(V)$ is infinitely divisible in $\mathrm{End}\,(V)$. Using the above decomposition, we easily conclude that if the above decomposition corresponding to A is $V = I \oplus N$, then

(i) $A_{|N}$ is the zero map, and
(ii) $A_1 := A_{|I}$ is infinitely divisible in $GL^+(I)$.

Then by Theorem 4.6, we have a continuous homomorphism $t \mapsto A'_t$ of $\mathbb{R}$ into $GL^+(I)$ such that $A'_1 = A_1$ and then $t \mapsto (A'_t, 0)$ is an embedding of A in $\mathrm{End}\,(V)$.

□

Problem E Does the subsemigroup

$$S^+ = \left\{A \in GL^+(d, \mathbb{R}) : \text{all entries of } A \text{ are non-negative}\right\}$$

of $GL^+(d, \mathbb{R})$ have the (point) embedding property?

Remark 6.16 Even for Lie subsemigroups of connected Lie groups, the results we have to date are far from impressive. So for example we do not know if every Lie subsemigroup of $SL(2, \mathbb{C})$ has the embedding property. Problem C above does seem to point to one area where further progress might be possible.

References

[1] W. Böge, *Zur Charakterisierung sukzessiv unendlich teilbarer Wahrscheinlichkeits-verteilungen auf lokalkompakten Gruppen*, Z. Wahrsch. Verw. Gebiete **2** (1964), 380–394.

[2] S.G. Dani, and M. McCrudden, *Factors, roots and embeddability of measures on Lie groups*, Math. Z. **199** (1988), 369–385.

[3] S.G. Dani and M. McCrudden, *On the factor sets of measures and local tightness of convolution semigroups over Lie groups*, J. Theoret. Probab. **1** (1988), 357–370.

[4] S.G. Dani and M. McCrudden, *Embedding infinitely divisible probabilities on the affine group*, in *Probability Measures on Groups IX, (Oberwolfach, 1988)*, pp. 36–49, (ed. by H. Heyer), Lecture Notes in Math. **1379**, Springer, 1989.

[5] S.G. Dani and M. McCrudden, *Embeddability of infinitely divisible distributions on linear Lie groups*, Invent. Math. **110** (1992), 237–261.

[6] S.G. Dani and M. McCrudden, *Infinitely divisible probabilities on discrete linear groups*, J. Theoret. Probab. **9** (1996), 215–229.

[7] S.G. Dani, and R. Shah, *On infinitely divisible measures on certain finitely generated groups*, Math. Z. **212** (1993), 631–636.

[8] J. Dixmier, *Quelques propriétés des groupes abélien localement compacts*, Bull. Sci. Math. Ser. II. **81** (1957), 113–121.

[9] U. Grenander, *Probabilities on Algebraic Structures*, Stockholm, Göteborg, Uppsala, Almquist and Wiksell, 1963.

[10] H. Heyer, *Probability Measures on Locally Compact Groups*, Springer, 1977.

[11] H. Heyer, *Recent contributions to the embedding problem for probability measures on a locally compact group*, J. Multivariate Anal. **19** (1986), 119–131.

[12] H. Heyer, *Das Einbettungsproblem der Wahrscheinlichkeitstheorie*, Österr. Zeits. Stat. Inf. (ZSI) **19** (1989), 191–213.

[13] G. Hochschild, *The Structure of Lie Groups*, Holden-Day, 1965.

[14] M. McCrudden, *On the n-th root set of an element in a connected semisimple Lie group*, Math. Proc. Cambridge Philos. Soc. **86** (1979), 219–225.

[15] M. McCrudden, *On n-th roots and infinitely divisible elements in a connected Lie group*, Math. Proc. Cambridge Philos. Soc. **89** (1981), 293–299.

[16] M. McCrudden, *An introduction to the embedding problem for probabilities on locally compact groups*, in *Positivity in Lie Theory: Open Problems*, (eds.: Hilgert, Lawson, Neeb and Vinberg), Walter de Gruyter, 1998.

[17] M. McCrudden and S. Walker, *Infinitely divisible probabilities on linear p-adic groups*, Proc. Indian Acad. Sci. (Math. Sci.) **109** (1999), 299–302.

[18] M. McCrudden and S. Walker, *Embedding infinitely divisible probabilities on subsemigroups of Lie groups*, Contemp. Math. **261** (2000), 43–57.

[19] A. Mukherjea and N.A. Tserpes, *Measures on Topological Semigroups*, Lecture Notes in Math. **547**, Springer, 1976.

[20] K.R. Parthasarathy, *On the imbedding of an infinitely divisible distribution in a one-parameter convolution semigroup*, Theory Probab. Appl. **12** (1967), 373–380.

[21] K.R. Parthasarathy, *Probability Measures on Metric Spaces*, Academic Press, 1967.

[22] Riddhi Shah, *Infinitely divisible measures on p-adic groups*, J. Theoret. Probab. **4** (1991), 391–405.

[23] E. Siebert, *Einbettung unendlich teilbarer Wahrscheinlichkeitsmasse auf topologischen Gruppen*, Z. Wahrsch. Verw. Gebiete **28** (1974), 227–247.

[24] S. Walker, *Probabilities on Semigroups*, Ph.D thesis, University of Manchester, 2001.

Department of Mathematics, University of Manchester, Oxford Road, Manchester, M13 9PL, UK

E-mail: mick@ma.man.ac.uk