On the generation of discrete and topological Kac-Moody groups.

Inna Capdeboscq [a],

[a] *Mathematics Institute, University of Warwick, Coventry, UK, CV4 7AL*

Abstract

This article shows that discrete or topological Kac-Moody groups defined over finite fields are in many cases 2-generated. We provide explicit bounds on the minimal number of generators for arbitrary Kac-Moody groups.

1. Introduction

Kac-Moody groups over arbitrary fields were defined by J. Tits [13]. In this article we discuss Kac-Moody groups $G(q)$ defined over finite fields $\mathbb{F}_q$. In [1] Abramenko and Muhlherr have shown that with some restrictions (if the groups are 2-spherical and there are some mild bounds on the size of $\mathbb{F}_q$), Kac-Moody groups over $\mathbb{F}_q$ are finitely presented with the number of generators depending on q and the Lie rank of $G(q)$ [1]. In [3], the author has shown that the family of affine Kac-Moody groups over $\mathbb{F}_q$ (of rank at least 3) possesses bounded presentations: there exists $C > 0$ such that if $G(q)$ is an affine Kac-Moody group corresponding to an indecomposable generalised Cartan matrix (IGCM) of rank at least 3 and with $q \geq 4$, then $G(q)$ has a presentation with $d(G)$ generators and $r(G)$ relations satisfying $d(G) + r(G) \leq C$. Related results for other Kac-Moody groups over finite fields were also proved in [3]. As a consequence, the number of generators of a 2-spherical Kac-Moody group is independent of q and depends on the type of Dynkin diagram of $G(q)$ rather than the rank of G. We make use of this observation to provide bounds on the minimal number of generators of G.

Theorem 1.1 *Let $G = G(q)$ be a simply connected Kac-Moody group of rank m corresponding to an IGCM A and defined over a finite field $\mathbb{F}_q$. Let $\pi = \{\alpha_1, ..., \alpha_m\}$ be the set of simple roots of G and Δ be the Dynkin diagram of G whose vertices are labelled by $\alpha_1, ..., \alpha_m$. Suppose further that for any $\alpha_{i_1}, ..., \alpha_{i_k} \in \pi$, $\Delta(\alpha_{i_1}, ..., \alpha_{i_k})$ denotes the subdiagram of Δ spanned by $\alpha_{i_1}, ..., \alpha_{i_k}$. Let $d(G)$ denote the minimal number of elements of G that are required to generate G. Then for q large enough there holds:*

(i) If $m = 2$, then $d(G) \leq 3$.

Email address: I.Capdeboscq@warwick.ac.uk (Inna Capdeboscq).

1. An existence of finite generating set of $G(q)$ can be derived directly from the original presentation of $G(q)$.

(ii) If G is affine with $m \geq 3$, then $d(G) = 2$.

(iii) If G is (symmetrizable) strictly hyperbolic and $m \geq 3$, then $d(G) = 2$.

(iv) If G is (symmetrizable) hyperbolic, then if $m \geq 5$, then $d(G) = 2$, and if $m = 3$ or 4, then $d(G) \leq 3$ (with $d(G) = 2$ in at least 34 out of 72 cases) at the possible exception of three rank 3 diagrams with Δ of type (∞, ∞, ∞). In each of those three cases $d(G) \leq 4$.

(v) Suppose that we may subdivide π into k mutually disjoint subsets $\pi_i = \{\alpha_{i_1}, ..., \alpha_{i_{l(i)}}\}$, $1 \leq i \leq k$, such that for each $i \in \{1, ..., k-1\}$, $\Delta(\alpha_{i_1}, ..., \alpha_{i_{l(i)}}) = \bigsqcup_{j=1}^{s(i)} \Delta_{ij}$ with Δ_{ij} an irreducible Dynkin diagram of finite type. Then

(a) If $\Delta(\alpha_{k_1}, ..., \alpha_{k_{l(k)}}) = \bigsqcup_{j=1}^{s(k)} \Delta_{kj}$ with Δ_{kj} an irreducible Dynkin diagram of finite type, then $d(G) \leq 2k$.

(b) If $\Delta(\alpha_{k_1}, ..., \alpha_{k_{l(k)}}) = \bigsqcup_{j=1}^{s(k)} \Delta_{kj}$ with Δ_{kj} an irreducible Dynkin diagram of rank 2 of infinite type, then $d(G) \leq 2k + 2$ (and if we increase q, $d(G) \leq 2k + 1$).

The bound $d(G) = 2$ is optimal and was obtained in cases (ii), (iii) and part of (iv). Note that the bound $d(G) \leq 2m$ follows from $(v)(a)$. Below are few examples of application of $(v)(a)$.

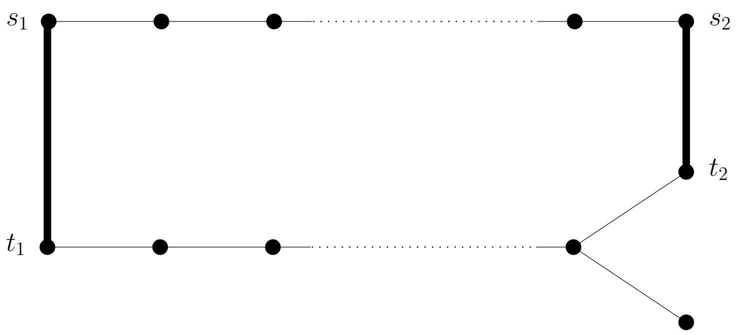
Example 1 If the nodes of Δ can be partitioned into two disjoint subsets π_1 and π_2 such that for every two-element subset $\{\alpha_{i_s}, \alpha_{i_t}\} \subset \pi_i$, $\Delta(\alpha_{i_s}, \alpha_{i_t})$ is of type $A_1 \times A_1$ (i.e., α_{i_s} and α_{i_t} are not connected in Δ), then for q large enough, $d(G) \leq 4$.

Partition corresponding to Example 1 can often be obtained, one possible obstacle being the existence of many cycles of length 3 in Δ. Example 2 is a special case of Example 1.

Example 2 If Δ is a finite rooted tree and has rank m, then $d(G) \leq 4$ provided that $q \geq \sqrt{m}$.

The following example illustrates the fact that infinite subdiagrams of Δ can sometimes be ignored.

Example 3 If Δ is the diagram below, then $d(G) \leq 4$.



The groups discussed so far are often called the *minimal* Kac-Moody groups. They are discrete infinite groups. In recent years there has been a significant progress in the study of topological Kac-Moody groups. Those are either completions of minimal Kac-Moody groups $G(q)$, $q = p^a$, achieved by various methods (e.g., a completion of Carbone and Garland $G^{c\lambda}$ obtained via methods of representation theory, a Caprace-Rémy-Ronan completion G^{crr} obtained via geometric methods) or a topological group G^{ma+} explicitly constructed by Mathieu. All of these are discussed in details in a recent paper of Rousseau [12]. There it is further shown that provided that p is large enough, $G^{ma+} \twoheadrightarrow G^{c\lambda} \twoheadrightarrow G^{crr}$ and $G(q)$ is dense in each of those topological groups. In [4] it was shown that under the same restriction on p (and modulo the centres), $G^{ma+} \cong G^{c\lambda} \cong G^{crr}$. Thus one can simply talk about a topological Kac-Moody group $\overline{G} = \overline{G}(q)$ that corresponds to $G = G(q)$ without any ambiguity. We now observe that since for p

large enough $G(q)$ is dense in $\overline{G}(q)$, an immediate consequence of Theorem 1.1 is a bound on the number of (topological) generators of $\overline{G}(q)$.

Corollary 1.2 *Let G be a minimal Kac-Moody group defined over the field $\mathbb{F}_q$, with $q = p^a$ and $p \geq max_{i \neq j}|a_{ij}|$ (where $A = (a_{ij})$ is the IGCM of G). Let $\overline{G}$ denote the topological Kac-Moody group corresponding to G. Then Theorem 1.1 holds if we replace G by $\overline{G}$ and $d(\overline{G})$ stands for the minimal number of topological generators of $\overline{G}$.*

We make an extensive use of a result of Guralnick and Kantor [9] regarding the generation of finite groups of Lie type. We also use recent estimates obtained by Menezes, Quick and Roney-Dougal [11].

2. Outline of a Proof

Let $G = G(q)$ be a simply connected Kac-Moody group. Let A be its IGCM of size m and $\alpha_1, ..., \alpha_m$ its fundamental roots. In the next paragraph we will assume Proposition 2.1 of [7] that defines a simply connected Kac-Moody group via its presentation.

The group G is generated by its root elements $x_\alpha(u)$, $\alpha \in \Phi$ (the set of real roots), $t \in \mathbb{F}_q$. For each $u \in \mathbb{F}_q$ and each $1 \leq i \leq m$, write $x_i(u) = x_{\alpha_i}(u)$ and $x_{-i}(u) = x_{-\alpha_i}(u)$. Then for each $a \in \mathbb{F}_q^*$ and $1 \leq i \leq m$, put $n_i(a) = x_i(a)x_{-i}(a^{-1})x_i(a)$, $n_i = n_i(1)$, and let $h_i(a) = n_i(a)n_i^{-1}$. For $\alpha \in \Phi$, $X_\alpha := \langle x_\alpha(u), u \in \mathbb{F}_q\rangle \cong (\mathbb{F}_q, +)$ and $M_\alpha := \langle X_\alpha, X_{-\alpha}\rangle \cong A_1(q)$. In particular, $X_i := \langle x_i(u), u \in \mathbb{F}_q\rangle$ and $M_i := \langle X_i, X_{-i}\rangle$. Moreover, G is a group with a BN-pair, $(B,\ N)$ where N is generated by a subgroup T and elements n_i, $1 \leq i \leq m$, and $T = \langle h_i(a), a \in \mathbb{F}_q^*, 1 \leq i \leq m\rangle \cong C_{q-1}^m$ is a torus of G. Remark that T normalises each M_i, $1 \leq i \leq m$. Also, $N/T \cong W$, the Weyl group of G, and as each $n_i \in M_i$ projects onto a generator w_i of W, we obtain the first basic ingredient of our proof.

Lemma 2.1 *If we have generated all M_i, $1 \leq i \leq m$, we have generated G.*

Notice that the notations above work just as well for finite groups of Lie type which can be thought of as a special case of Kac-Moody groups over $\mathbb{F}_q$.

Lemma 2.2 *Let $\Sigma(q)$ be a finite (quasi-) simple group of Lie type that is defined over $\mathbb{F}_q$ and corresponding to a root system $\Sigma = A_2, C_2$ or G_2. Let α_1 and α_2 be the fundamental roots of Σ with $|\alpha_1| \leq |\alpha_2|$. Then $\Sigma(q)$ is generated by M_1 and n_2.*

Proof. This is achieved by an easy calculation. □

In the future, we will denote by M_{ij} the semi-simple subgroup of G that corresponds to $\Delta(\alpha_i, \alpha_j)$. We now prove our main result.

Proposition 2.3 *Let G be an affine simply connected Kac-Moody group of rank $(m+1) \geq 3$, corresponding to an IGCM, defined over a field $\mathbb{F}_q$, q large enough. Then $d(G) = 2$.*

Proof. For the affine groups, we use the notations from the book of Carter [6]. In particular, we denote the fundamental roots of G by $\alpha_0, ..., \alpha_m$. For the type $\widetilde{C}'_m$ we use the description given on p.585 of [6].

Suppose first that G is neither of type $\widetilde{C}^t_m$, nor of type $\widetilde{A}_2$. Choose i so that α_0 and α_i are not joined by an edge in Δ. Take an element $x = n_0x_i \in G$ with $x_i \in M_i$ chosen so that if p is odd, $1 \neq x_i \in X_i$, while if $p = 2$, $x_i \in M_i$ of order $(q+1)$. Since $(o(n_0), o(x_i)) = 1$ and $[n_0, x_i] = 1$, we have that $1 \neq (n_0x_i)^{o(n_0)} = x_i^{o(n_0)} \in M_i$ and $1 \neq (n_0x_i)^{o(x_i)} = n_0^{o(x_i)} \in M_0$. Now consider a subgroup G_0 of G that corresponds to the Dynkin subdiagram $\Delta(\alpha_1, ..., \alpha_m)$. Notice that G_0 is a finite (possibly quasi-) simple group. By [9], there exists $y \in G_0$ such that G_0 is generated by $x_i^{o(n_0)}$ and y. Let $j \in \{1, 2, ..., m\}$ be such that α_j and α_0 are joined in Δ (e.g., $j = 1$ for $\widetilde{A}_n$, $\widetilde{F}_4$; $j = 2$ for $\widetilde{B}_n$, etc.). Notice that $G_0 \geq M_j$ for every such j. Consider M_{0j}. We have $M_{0j} \geq M_0$ and by Lemma 2.2, $M_{0j} = \langle M_j, n_0^{o(x_i)}\rangle$. Since $\langle G_0, M_{0j}\rangle \geq \langle M_i, 0 \leq i \leq m\rangle = G$, we obtain $G = \langle x, y \rangle$.

Suppose now that G is of type $\widetilde{C}_m^t$ with $m \geq 3$. Take $x = h_0(u)n_1x_m$ where $u^2 \neq \pm 1$ and $x_m \in M_m$ of odd order s co-prime to $t := o(h_0(u^2)h_1(-u^2))$. Notice that as $m \geq 3$, $[h_0(u)n_1, x_m] = 1$. Then $x^2 = h_0(u)h_0(u)^{n_1}n_1^2x_m^2 = h_0(u)h_0(u)h_1(u^{-A_{01}})h_1(-1)x_m^2 = h_0(u^2)h_1(-u^2)x_m^2$. An explicit calculation shows that $x^{2s} = h_0(u^{2s})h_1((-u^2)^s)$ induces a non-trivial inner-diagonal automorphism on M_0. Thus by [9], there exists $y_0 \in M_0$ such that $\langle x^{2s}, y_0 \rangle \geq M_0$. On the other hand, $1 \neq x^{2t} = x_m^{2t} \in M_m$. Let $H \leq G$ corresponding to $\Delta(\alpha_2, ..., \alpha_m)$. Again by [9], there exists $y_m \in H$ such that $\langle x_m^{2t}, y_m \rangle = H$. Take $y = y_0y_m$. Clearly $[y_0, y_m] = 1$, $[y_0, H] = 1$ and $[y_m, M_0] = 1$. It follows that $\langle x, y \rangle \geq \langle x^{2s}, y_0y_m \rangle \geq M_0$ and $\langle x, y \rangle \geq \langle x^{2t}, y_0y_m \rangle \geq H$. In particular, $h_0(u), x_m \in \langle x, y \rangle$, and so $n_1 \in \langle x, y \rangle$. But by Lemma 2.2, $\langle M_0, n_1 \rangle = M_{01} \geq M_1$, and so $G = \langle x, y \rangle$.

If G is of type $\widetilde{C}_2^t$, take $x = h_0(u_0)h_2(u_2)n_1$ with $o(h_0(u_0))$ and $o(h_2(u_2))$ as large as possible and such that $u_0^2u_2^{-2} \neq -1$. Then $x^2 = h_0(u_0)h_2(u_2)h_0(u_0)^{n_1}h_2(u_2)^{n_1}n_1^2 = h_0(u_0^2)h_2(u_2^2)h_1(-u_0^2u_2^2)$. Now choose $y_0 \in M_0 - T$ of order $q-1$ if q is even and $(q-1)/|Z(M_0)|$ if q is odd, and $y_2 \in M_2$ of order $q+1$ if q is even and $(q+1)/|Z(M_2)|$ if q is odd. A celebrated Theorem of Dickson (cf. 6.5.1 of [8]) implies that $\langle x^2, y_i^{o(y_j)} \rangle \geq M_i$, $\{i, j\} = \{0, 2\}$. Take $y = y_0y_2$. It follows that $\langle x, y \rangle$ contains M_0 and M_2; in particular, $n_1 \in \langle x, y \rangle$. Now Lemma 2.2 implies that $\langle x, y \rangle \geq \langle M_0, n_1 \rangle \geq M_1$. Thus $G = \langle x, y \rangle$.

Finally let G be of type $\widetilde{A}_2$. Take $x = n_0h_1(u)$ with $u^3 \neq \pm 1$. Then $x^2 = h_1(u)^{n_0}n_0^2h_1(u) = h_1(u)h_0(u^{-A_{10}})h_0(-1)h_1(u) = h_1(u^2)h_0(-u)$. An explicit calculation shows that x^2 acts non-trivially on M_{12} and so by [9], there exists $y \in M_{12}$ such that $\langle x^2, y \rangle \geq M_{12}$. In particular, $M_i \leq \langle x, y \rangle$ for $i = 1, 2$, and so $n_0 \in \langle x, y \rangle$. But by Lemma 2.2, $\langle M_1, n_0 \rangle = M_{01} \geq M_0$. Therefore $G = \langle x, y \rangle$. □

Proposition 2.4 *Let G be a simply connected Kac-Moody group of rank 2 defined over a field $\mathbb{F}_q$. Then $d(G) \leq 3$.*

Proof. We label the simple roots by α_1 and α_2. Choose $1 \neq x = h_1(u)h_2(v) \in T$ that induces a non-trivial inner-diagonal automorphisms on both M_1 and M_2. Now use [9] to choose $y_i \in M_i$ so that $\langle x, y_i \rangle \geq M_i$, $i = 1, 2$. The result follows immediately. □

Proposition 2.5 *Let G be a simply connected strictly hyperbolic (symmetrizable) Kac-Moody group of rank at least 3. Then if q is large enough, $d(G) = 2$.*

Proof. We use the list of diagrams and notations as in Table 2 of [2]. If G is of type BG_3, BG_3', GG_3 or $G'G3$, choose $x = h_1(u)n_2h_3(v)$ with appropriately chosen $u, v \in \mathbb{F}_q^*$ and $y_i \in M_i$ for $i \in \{1, 3\}$ so that $(o(y_1), o(y_3)) = 1$ and $\langle x^2, y_i^{o(y_j)} \rangle \geq M_i$, $\{i, j\} = \{1, 3\}$. Let $y = y_1y_3$. Then $\langle x, y \rangle$ contains M_1, M_3 and n_2. Apply Lemma 2.2 to conclude that $M_{12} = \langle M_1, n_2 \rangle \leq \langle x, y \rangle$. As $M_1 \leq M_{12}$, the result follows.

If G is of type CG_3', CG_3, $G'G_3'$, choose $x = n_1h_3(v)$ with appropriately chosen $v \in \mathbb{F}_q^*$ and $y \in M_2$ such that $\langle x^2, y \rangle \geq M_{23}$. Since $h_3(v) \in M_{23}$ and n_1 and M_2 generate M_{12}, we have that $G = \langle x, y \rangle$.

If G is of type $AD_3^{(2)}$, AGG_3, $AC_2^{(1)}$ or $AG'G_3'$, choose $x = n_1h_2(u)$ and $y \in M_{23}$ such that $\langle x^2, y \rangle \geq M_{23}$. Now use the fact that $h_2(u) \in M_{23}$ and that $\langle n_1, M_2 \rangle = M_{12}$ to conclude that $G = \langle x, y \rangle$.

Finally, if G is of type $AC_3^{(1)}$, take $x = n_1h_4(u)$ and $y \in M_{234}$ such that $\langle x^2, y \rangle \geq M_{234}$ (such y exists by [9]). Since $\langle n_1, M_4 \rangle = M_{14}$ while $M_4 \leq M_{234}$, we conclude that $\langle x, y \rangle = G$. □

The proof of part (iv) of 1.1 for the hyperbolic groups follows by similar tricks and calculations done for every single group on the list of 130 diagrams (cf. [5]). The proof of part $(v)(a)$ and $(v)(b)$ of Theorem 1.1 are obvious if one uses an observation (cf. Lemma 5 of [10]) that two elements generate a product of finite simple groups $H_1^{m_1} \times ... \times H_n^{m_n}$ $(H_i \ncong H_j,\ i \neq j)$ if and only if their projections into each $H_i^{m_i}$ generate it, and from the estimates (recently obtained in [11]) on the number h in a direct product H^h (H is a finite simple group) for which it is possible to be generated by 2 elements .

Acknowledgement. I would like to thank Guy Rousseau and Bertrand Rémy for illuminating discussions on Kac-Moody groups.

References

[1] P. Abramenko, B. Muhlherr. *Presentations de certaines BN-paires jumeles comme sommes amalgames.* C. R. Acad. Sci. Paris Ser. I Math. 325 (1997), no. 7, 701706.

[2] H. Ben Messaoud. *Almost split real forms for hyperbolic Kac-Moody Lie algebras.* J. Phys. A 39 (2006), no. 44, 1365913690.

[3] Inna Capdeboscq, *Bounded presentations of Kac-Moody groups*, J. Group Theory, **16** (2013), no. 6, 899–905.

[4] Inna Capdeboscq and Bertrand Rémy, *On some pro-p groups from infinite-dimensional Lie theory.* Math. Z. 278 (2014), no. 1-2, 3954.

[5] L. Carbone, S. Chung, L. Cobbs, R. McRae, D. Nandi, Y. Naqvi, D. Penta. Classification of hyperbolic Dynkin diagrams, root lengths and Weyl group orbits. J. Phys. A 43 (2010), no. 15, 155209, 30 pp.

[6] R. Carter. *Lie algebras of finite and affine type.* Cambridge Studies in Advanced Mathematics, 96. Cambridge University Press, Cambridge, 2005.

[7] R.W. Carter, Y. Chen. *Automorphisms of affine Kac-Moody groups and related Chevalley groups over rings.* J. Algebra **155** (1993), no. 1, 4494.

[8] D. Gorenstein, R. Lyons, R. Solomon. *The Classification of the Finite Simple Groups, Number 1.* Amer.Math. Soc. Surveys and Monographs **40**, **#3** (1998).

[9] R. Guralnick, W. Kantor. *Probabilistic generation of finite simple groups.* Special issue in honor of Helmut Wielandt. J. Algebra **234** (2000), no. 2, 743792.

[10] W. Kantor, A. Lubotzky. *The probability of generating a finite classical group.* Geom. Dedicata 36 (1990), no. 1, 6787.

[11] N. Menezes, M. Quick, C. Roney-Dougal. *The probability of generating a finite simple group.* Israel J. Mathematics, **198** (2013), 371392.

[12] G. Rousseau. Groupes de Kac-Moody déployés sur un corps local, II. Masures ordonnées. preprint ArXiv:1009.0138v2, 2012.

[13] J. Tits. *Uniqueness and presentation of KacMoody groups over fields* J. Algebra **105** (1987), 542573.