Random spanning trees of Cayley graphs and an associated compactification of semigroups

Steven N. Evans*

Revised March 20, 1998

Abstract

A sequential construction of a random spanning tree for the Cayley graph of a finitely generated, countably infinite subsemigroup V of a group G is considered. At stage n, the spanning tree T is approximated by a finite tree T_n rooted at the identity. The approximation T_{n+1} is obtained by connecting edges to the points of V that are not already vertices of T_n but can be obtained from vertices of T_n via multiplication by a random walk step taking values in the generating set of V. This construction leads to a compactification of the semigroup V in which a sequence of elements of V that is not eventually constant is convergent if the random geodesic through the spanning tree T that joins the identity to the n^{th} element of the sequence converges in distribution as $n \to \infty$. The compactification is identified in a number of examples. Also, it is shown that if $h(T_n)$ and $\#(T_n)$ denote, respectively, the height and size of the approximating tree T_n, then there are constants $0 < c_h \leq 1$ and $0 \leq c_\# \leq \log 2$ such that $\lim_{n\to\infty} n^{-1} h(T_n) = c_h$ and $\lim_{n\to\infty} n^{-1} \log \#(T_n) = c_\#$ almost surely.

Running head: Random spanning trees.
Mathematics Subject Classification: Primary 60B99, 20F32; Secondary 20P05, 54D35.

*Research supported in part by Presidential Young Investigator Award and NSF Grant DMS-9703845

1 Introduction

The Cayley graph of a finitely generated free group is a regular tree. This provides a natural way of compactifying such a group: one just adjoins the collection of "ends". That is, a sequence of group elements converges in the compactification if and only if the sequence is either eventually constant or initial segments of the unique shortest path connecting the identity to the n^{th} element of the sequence converge as $n \to \infty$.

The Gromov compactification of word hyperbolic groups (cf. [1, 3, 4]) is a far-reaching generalisation of this idea that is based on the observation that such groups have Cayley graphs which in some sense are almost tree–like.

Our main aim in this paper is to carry something of the spirit of such constructions over to a general finitely generated discrete subsemigroup of a group. We do this by replacing the full Cayley graph with a natural randomly generated spanning tree and declaring that a sequence of semigroup elements converges in the compactification if and only if the the sequence is eventually constant or initial segments of the random path through the spanning tree that joins the origin to the n^{th} element of the sequence converges in distribution as $n \to \infty$. We describe the spanning tree in §2 and give a number of examples of the associated compactification in §3

The spanning tree is constructed from a sequence of finite approximating trees. The asymptotic behaviour of the height and size of these approximating trees is studied in §§4 and 5, respectively.

2 Construction of the spanning tree

Let G be a countable group with identity e. Fix a finite subset $S \subseteq G$ and write V for the subsemigroup of G that consists of all finite products of elements of S (where we interpret the empty product as e so that $e \in V$). We will always suppose that V is infinite.

Fix a probability measure $p = (p_s)_{s \in S}$ on S with $p^* := \min_{s \in S} p_s > 0$. Let $(X_n)_{n \in \mathbb{N}}$ be a sequence of independent S-valued random variables, each distributed according to p.

Define a rooted random tree, T, with root e, vertex set almost surely V, and (random) directed edge set E by the following procedure. For $g \in V \backslash \{e\}$

put

$$N_g := \inf\{N \geq 1 \,:\, \exists 1 \leq m_1 < \ldots < m_\ell = N \text{ such that } X_{m_1} \cdots X_{m_\ell} = g\},$$

and declare that $(gX_{N_g}^{-1}, g) \in E$.

Another way of putting this is that T is the limit of the increasing sequence of finite, rooted, trees $(T_n)_{n=0}^\infty$ defined inductively as follows. The tree T_0 has the single vertex $\{e\}$ (and no edges). Suppose that T_i, $0 \leq i \leq n$, have been defined with T_i having vertex set $V_i \subseteq V$ and directed edge set $E_i \subseteq V_i \times V_i$. Then T_{n+1} has vertex set

$$V_{n+1} = V_n \cup \{gX_{n+1} \,:\, g \in V_n\}$$

and directed edge set

$$E_{n+1} = E_n \cup \{(g, gX_{n+1}) \,:\, g \in V_n,\, gX_{n+1} \notin V_n\}.$$

Of course, it may happen that $T_n = T_{n+1}$ for certain values of n.

Recall that the Cayley graph, say Γ, of the semigroup V with respect to the generating set S is the directed graph with vertex set V and edge set consisting of ordered pairs (v, w) where $w = vs$ for somes $s \in S$. The rooted tree T is a spanning tree for Γ; that is, T has the same vertex set as Γ and the edge set of T is a subset of the edge set of Γ.

Example 1 Suppose that G is the free group on n letters $\alpha_1, \ldots, \alpha_n$. Put $S = \{\alpha_1, \alpha_1^{-1}, \ldots, \alpha_n, \alpha_n^{-1}\}$, so that $V = G$. Then E is almost surely the fixed set of ordered pairs of the form $(g_1 \cdots g_{k-1}, g_1 \cdots g_k)$ with $g_i \neq g_{i+1}^{-1}$ for $1 \leq i \leq k-1$.

Example 2 Suppose that $G = \mathbb{Z} \times \mathbb{Z}$ and $S = \{(1,0), (0,1)\}$, so that $V = \mathbb{Z}_+ \times \mathbb{Z}_+$.

Put $Y_0 := 0$ and $Y_n := X_1 + \cdots + X_n$ for $n \geq 1$. Write (Y_n', Y_n'') for the components of Y_n. Note that

$$V_n = \{(a, b) \,:\, a \leq Y_n',\, b \leq Y_n''\}$$

and

$$\{(Y_0, Y_1), (Y_1, Y_2), \ldots, (Y_{n-1}, Y_n)\} \subseteq E_n.$$

Put

$$V_n^{\rightarrow} := \{(a,b) \in V_n \backslash \{Y_1, \ldots, Y_n\} : a > Y'_m, b = Y''_m \text{ for some } 1 \leq m \leq n\}$$

and

$$V_n^{\uparrow} := \{(a,b) \in V_n \backslash \{Y_1, \ldots, Y_n\} : a = Y'_m, b > Y''_m \text{ for some } 1 \leq m \leq n\}.$$

Observe that if $X_{n+1} = (1,0)$, then $V_{n+1}^{\rightarrow} \backslash V_n^{\rightarrow} = \{(Y'_n+1, b) : 0 \leq b \leq Y''_n - 1\}$, $V_{n+1}^{\uparrow} = V_n^{\uparrow}$, and $E_{n+1} \backslash E_n = \{((Y'_n, b), (Y'_n + 1, b)) : 0 \leq b \leq Y''_n - 1\}$. Similarly, if $X_{n+1} = (0,1)$, then $V_{n+1}^{\rightarrow} = V_n^{\rightarrow}$, $V_{n+1}^{\uparrow} \backslash V_n^{\uparrow} = \{(a, Y''_n + 1) : 0 \leq a \leq Y'_n - 1\}$, and $E_{n+1} \backslash E_n = \{((a, Y''_n), (a, Y''_n + 1)) : 0 \leq a \leq Y'_n - 1\}$. It is now clear by induction that if $(a,b) \in V_n^{\rightarrow}$, then $((a-1,b),(a,b)) \in E_n$, and if $(a,b) \in V_n^{\uparrow}$, then $((a, b-1), (a,b)) \in E_n$.

Thus $((a-1,b),(a,b)) \in E \backslash \{(Y_0, Y_1), (Y_1, Y_2), \ldots\}$ if and only if $Y'_n < a$ and $Y''_n = b$ for some n, and $((a, b-1), (a,b)) \in E$ if and only if $Y'_n = a$ and $Y''_n < b$ for some n.

Example 3 Suppose that $G = \mathbb{Z} \times \mathbb{Z}$ and $S = \{(\pm 1, 0), (0, \pm 1)\}$, so that $V = \mathbb{Z} \times \mathbb{Z}$.

Consider (a,b) with $a > 0$ and $b \geq 0$. By definition of $N_{(a,b)}$, exactly a of $X_1, \ldots, X_{N_{(a,b)}}$ must have the value $(+1, 0)$ and exactly b must have the value $(0, +1)$. Hence, $V_{N_{(a,b)}}$ also contains the point $(a-1, b)$ and so $((a,b),(a-1,b)) \notin E$. A similar argument shows that if $a \geq 0$ and $b > 0$, then $((a,b),(a,b-1)) \notin E$. Thus for every point $(a,b) \in V_{++} := \{(c,d) : c \geq 0,\ d \geq 0\}$ we have that $((a',b'),(a,b)) \in E$ with $(a',b') \in V_{++}$ and either $(a,b) = (a',b') + (1,0)$ or $(a,b) = (a',b') + (0,1)$.

Let T_{++} be the subtree of T that has vertex set V_{++} and edge set $E_{++} := \{(u,v) \in E : u \in V_{++}, v \in V_{++}\}$. It is clear from what we have just observed that T_{++} has the same description as T from the previous example, with the role of Y_n being played by $Y_n^{++} := X_1^{++} + \cdots + X_n^{++}$, where $(X_n^{++})_{n \in \mathbb{N}}$ is the subsequence of $(X_n)_{n \in \mathbb{N}}$ consisting of terms that take on the values $(+1, 0)$ and $(0, +1)$. Similar remarks apply to the three other quadrants, with the trees for adjacent quadrants intersecting in a ray that passes through the vertices on the shared axis.

We remark that if the random walk $e, X_1, X_1X_2, \ldots$ is recurrent, then the procedure in [2] gives another mechanism for constructing a random spanning tree of V using $(X_n)_{n \in \mathbb{N}}$.

3 The associated compactification

Given a rooted tree τ and a vertex v of τ, let $H(v,\tau)$ denote the *height* of v, that is, the number of edges on the unique path joining the root to v. For $v \in V$, define $Z_k(v)$, $0 \le k \le H(v,T)$, to be the successive vertices passed through by the unique path in T that leads from e to v. That is, $Z_0(v) = e$, $Z_{H(v,T)}(v) = v$, and $(Z_k(v), Z_{k+1}(v)) \in E$ for $0 \le k \le H(v,T) - 1$. Put $Z_k(v) := v$ for $k > H(v,T)$. Note that $Z_k(v) \in B_k$, the set of elements of V that can be written as the product of k or fewer elements of S. Set $\zeta_m(v) := (Z_0(v), \dots, Z_m(v))$.

Equip V with the metric

$$\Delta(u,v) := \sum_{m=0}^{\infty} 2^{-(m+1)} \sum_{w \in V^{(m+1)}} \Big| \mathbb{P}\{\zeta_m(u) = w\} - \mathbb{P}\{\zeta_m(v) = w\} \Big|,$$

and let $\overline{V}$ denote the completion of V in this metric. Put $\partial V := \overline{V} \backslash V$.

Observe that a sequence $(v_n)_{n \in \mathbb{N}}$ drawn from V is Cauchy for Δ if and only if for all m the distribution of $\zeta_m(v_n) = (Z_0(v_n), \dots, Z_m(v_n))$ converges weakly (or, equivalently, in total variation) as $n \to \infty$.

Lemma 4 *The space $\overline{V}$ is compact.*

Proof. It suffices to show that $\overline{V}$ is sequentially compact. Note that for each m the distribution of $(Z_0(v), \dots, Z_m(v))$ is supported on the finite subset $B_0 \times B_1 \times \cdots B_m \subseteq V^{m+1}$. The result now follows from a diagonal argument and the fact that the space of probability measures on a finite set is compact for the coincident topologies of weak and total variation convergence.

□

Example 5 Suppose that G is the free group on n letters $\alpha_1, \dots, \alpha_n$. Put $S = \{\alpha_1, \alpha_1^{-1}, \dots, \alpha_n, \alpha_n^{-1}\}$, as in Example 1. Then ∂V is just the set of ends of the fixed tree described in Example 1.

Example 6 Suppose that $G = \mathbb{Z}$ and $S = \{\alpha, -\beta\}$, where α and β are positive and relatively prime, so that $V = \mathbb{Z}$.

Write

$$M := \inf\{n : \#\{1 \le k \le n : X_k = -\beta\} = \alpha - 1\}.$$

Of course, M is finite almost surely. Observe that V_M contains at least one representative for every congruence class $\mod \alpha$. For $n \geq M$ and $r = 0, 1, \ldots, \alpha - 1$, write R_n^r for the largest element of V_n that is congruent to $r \mod \alpha$. Observe that if $X_{n+1} = \alpha$ (respectively, $X_{n+1} = -\beta$) or $n \geq M$, then $R_{n+1}^r = R_n^r + \alpha$ and $(R_n^r, R_{n+1}^r) \in E_{n+1}$ (respectively, $R_{n+1}^r = R_n^r$) for $r = 0, 1, \ldots, \alpha - 1$. Therefore, if $v \equiv r \mod \alpha$ and $v \geq R_M^r$, then $v = R_k^r$ for some $k \geq M$ and $(Z_{H(v,T)-k+M}(v), \ldots, Z_{H(v,T)}(v)) = (R_M^r, \ldots, R_k^r) = (R_M^r, \ldots, R_M^r + (k - M)\alpha)$. This, and a similar observation with the roles of α and $-\beta$ reversed, shows that a sequence $(v_n)_{n \in \mathbb{N}}$ that is not eventually constant will be Cauchy if and only if one of the following conditions holds:

(i) $v_n \to +\infty$ and, for some $r = 0, 1, \ldots, \alpha - 1$, $v_n \equiv r \mod \alpha$ for all sufficiently large n,

(ii) $v_n \to -\infty$ and, for some $r = 0, 1, \ldots, \beta - 1$, $v_n \equiv r \mod \beta$ for all sufficiently large n,

and each possibility leads to a different limit point. Thus ∂V consists of $\alpha + \beta$ points, with "α boundary points at $+\infty$ and β boundary points at $-\infty$". Note that this conclusion agrees with that of the previous example when $\alpha = \beta = 1$.

Example 7 Suppose that $G = \mathbb{Z}$ and $V = \mathbb{Z}_+$, so that S is a finite set of nonnegative integers that contains 1. Let σ denote the largest element of S. Note that with probability one there are infinitely many times n such that $X_{n+1} = \ldots = X_{n+\sigma} = 1$. It is clear from the construction of T that if $v \geq X_1 + \cdots + X_n$ for such an n, then $Z_k(v) = Z_k(X_1 + \cdots + X_n) = X_1 + \cdots + X_k$ for $0 \leq k \leq n = H(X_1 + \cdots + X_n, T)$. Therefore, a sequence $(v_n)_{n \in \mathbb{N}}$ that is not eventually constant will be Cauchy if and only if $v_n \to +\infty$, and each such sequence converges to the same limit point. Thus $\overline{V}$ coincides with $\mathbb{Z}_+^* = \mathbb{Z}_+ \cup \{+\infty\}$, the usual one-point compactification of $\mathbb{Z}_+$.

Example 8 Suppose that $G = \mathbb{Z} \times \mathbb{Z}$ and $S = \{(1,0), (0,1)\}$, so that $V = \mathbb{Z}_+ \times \mathbb{Z}_+$, as in Example 2.

Define $Y_0, Y_1, \ldots$ as in Example 2. For $v = (v', v'') \in V$ put

$$M(v) = \min\{n : Y_n' = v' \text{ or } Y_n'' = v''\}.$$

Then $Z_k(v) = Y_n$ for $0 \leq k \leq M(v)$. If $Y_{M(v)}' < v'$, then $Z_k(v) = (Y_{M(v)}' + k - M(v), Y_{M(v)}'')$ for $M(v) + 1 \leq k \leq H(v, T)$. Similarly, if $Y_{M(v)}'' < v''$, then $Z_k(v) = (Y_{M(v)}', Y_{M(v)}'' + k - M(v))$ for $M(v) + 1 \leq k \leq H(v, T)$.

It follows that a sequence $(v_n)_{n\in\mathbb{N}} = ((v'_n, v''_n))_{n\in\mathbb{N}}$ that is not eventually constant will be Cauchy if and only if one of the following three conditions holds:

(i) there exists a such that $v'_n = a$ for all n sufficiently large and $v''_n \to +\infty$ as $n \to \infty$,

(ii) $v'_n \to +\infty$ as $n \to \infty$ and there exists b such that $v''_n = b$ for all n sufficiently large,

(iii) $v'_n \to +\infty$ as $n \to \infty$ and $v''_n \to +\infty$ as $n \to \infty$.

If two sequences satisfy (i) with the same (respectively, different) choice of a, then they converge to the same (respectively, different) limit points. A similar remark holds for (ii). Any two sequences satisfying (iii) converge to the same limit point. Finally, if a sequence satisfies one of the conditions (i)-(iii) and another sequence satisfies one of the other conditions, then the two sequences converge to different limit points. Consequently, $\overline{V}$ is homeomorphic to $\mathbb{Z}_+^* \times \mathbb{Z}_+^*$.

Example 9 Suppose that $G = \mathbb{Z} \times \mathbb{Z}$ and $S = \{(\pm 1, 0), (0, \pm 1)\}$, so that $V = \mathbb{Z} \times \mathbb{Z}$.

It is clear from the previous Example and Example 3 that $\overline{V}$ is homeomorphic to $\mathbb{Z}^* \times \mathbb{Z}^*$, where $\mathbb{Z}^* = \mathbb{Z} \cup \{-\infty, +\infty\}$ is the usual two-point compactification of $\mathbb{Z}$.

Example 10 Suppose that G is the semidirect product of an aribitrary finite group H and $\mathbb{Z}$. Recall that this means that as a set G can be identified with the Cartesian product $H \times \mathbb{Z}$ and there is some automorphism π of H such that the group operation is given by $(h, z)(h', z') = (h\pi^z(h'), z + z')$. Write f for the identity of H. Take $S = \{(\alpha_1, 0), \ldots, (\alpha_m, 0), (f, +1), (f, -1)\}$, where $\alpha_1, \ldots, \alpha_m$ generate H as a semigroup, so that $V = G$.

With probability one there exist times $I \le J$ such that $X_I, \ldots, X_J \in \{(\alpha_1, 0), \ldots, (\alpha_m, 0)\}$ and the set of products of the form $X_{i_1} \cdots X_{i_k}$ with $I + 1 \le i_1 < \ldots < i_k \le J$ is all of $H \times \{0\}$. Put

$$K := \max\{k \in \mathbb{Z} : (h, k) \in V_I \text{ for some } h \in H\}$$

and

$$L := \min\{\ell \in \mathbb{Z} : (h, \ell) \in V_I \text{ for some } h \in H\}.$$

Note that V_J contains (h,K) for every choice of $h \in H$ and no point of the form (g,r) for $g \in H$ and $r > K$. Similarly, V_J contains (h,L) for every choice of $h \in H$ and no point of the form (g,r) for $g \in H$ and $r < L$. It follows that if $v = (h,z) \in V$ with $z \geq K$, then $Z_k(v) = Z_k((h,K))$ for $0 \leq k \leq H((h,K),T)$ and $Z_k(v) = (h, H((h,K),T)+k-K)$ for $H((h,K),T) \leq k \leq H(v,T) = H((h,K),T)+z-K$. Similarly, if $v = (h,z) \in V$ with $z \leq L$, then $Z_\ell(v) = Z_\ell((h,L))$ for $0 \leq \ell \leq H((h,L),T)$ and $Z_\ell(v) = (h, H((h,L),T)+L-\ell)$ for $H((h,L),T) \leq k \leq H(v,T) = H((h,L),T)+L-z$. Consequently, $\overline{V}$ is homeomorphic to $H \times \mathbb{Z}^*$.

Example 11 Suppose that G is the semidirect of product of $\mathbb{Z}$ and $\mathbb{Z}_2$ (that is, the infinite dihedral group D_∞). More specifically, G can be identified with $\mathbb{Z} \times \mathbb{Z}_2$ as a set and if $\mathbb{Z}_2$ is written "multiplicatively" as $\{+1,-1\}$, then the group operation is given by $(z,\epsilon)(z',\epsilon') = (z+\epsilon z', \epsilon\epsilon')$. Take $S = \{(0,-1),(1,+1)\}$, so that $V = G$.

It is not hard to see that with probability one T is the fixed tree with

$$
\begin{aligned}
E = \, & \{((0,+1),(0,-1)),((1,+1),(1,-1)),((2,+1),(2,-1)),\ldots\} \\
& \cup \{((-1,-1),(-1,+1)),((-2,-1),(-2,+1)),((-3,-1),(-3,+1)),\ldots\} \\
& \cup \{((0,+1),(1,+1)),((1,+1),(2,+1)),((2,+1),(3,+1)),\ldots\} \\
& \cup \{((0,-1),(-1,-1)),((-1,-1),(-2,-1)),((-2,-1),(-3,-1)),\ldots\}.
\end{aligned}
$$

The following observations follow immediately:

(i) If $v = (z,+1)$ (respectively, $(z,-1)$) with $z > 0$, then $H(v,T) = z$ (respectively, $H(v,T) = z+1$) and $Z_k(v) = (k,+1)$ for $0 \leq k \leq z$.

(ii) If $v = (z,-1)$ (respectively, $v = (z,+1)$) with $z < 0$, then $H(v,T) = -z+1$ (respectively, $H(v,T) = -z+2$) and $Z_k(v) = (-k+1,-1)$ for $1 \leq k \leq -z+1$.

Thus ∂V has only two points and $\overline{V}$ is not homeomorphic to $\mathbb{Z}^* \times \mathbb{Z}_2$.

Remark 12 In all of the above examples, the compactification only depends on the set S and not on the probability distribution p. Also, the left and right actions of the semigroup V on itself have continuous extensions to $\overline{V}$. It would be interesting to know to what extent these two observations hold generally.

4 Growth of the height

For a rooted tree τ, define $h(\tau)$ to be the supremum of the heights of vertices of τ. Recall that $p^* := \min_{s \in S} p_s > 0$.

Theorem 13 *There exists a constant $c_h \in [p^*, 1]$ such that*

$$\lim_{n \to \infty} n^{-1} h(T_n) = c_h$$

almost surely.

Proof. Clearly, $h(T_n) \leq n$.

For $m, n \in \mathbb{N}$, write T_n^m for the tree built from $X_{m+1}, \ldots X_{m+n}$ in the same manner that T_n is built from $X_1, \ldots, X_n$. Write V_n^m for the vertex set of T_n^m. For $v \in V_m$, $H(v, T_m)$ is the minimum of those integers k for which we can find $1 \leq \ell_1 < \ldots < \ell_k \leq m$ such that $v = X_{\ell_1} \ldots X_{\ell_k}$, and similar comments apply to T_{m+n} and T_n^m. If $u \in V_{m+n}$, then there exists $v \in V_m$ and $w \in V_n^m$ such that $u = vw$ and we have $H(u, T_{m+n}) \leq H(v, T_m) + H(w, T_n^m)$ for all choices of v and w. Consequently, $h(T_{m+n}) \leq h(T_m) + h(T_n^m)$. Kingman's subadditive ergodic theorem [5] now shows that $n^{-1} h(T_n)$ converges almost surely as $n \to \infty$.

We next show that the limit is almost surely at least p^*. Let $(g_k)_{k \in \mathbb{N}}$ be the sequence of elements of S guaranteed by Lemma 14 below. Define a sequence of independent random variables $(W_k)_{k \in \mathbb{N}}$ by

$$W_1 = \inf\{\ell \geq 1 : X_\ell = g_1\}$$

and

$$W_{k+1} = \inf\{\ell \geq 1 : X_{W_1 + \cdots + W_k + \ell} = g_{k+1}\}, \ k \geq 1.$$

Observe that W_k has a geometric distribution with success probability p_{g_k}. Hence W_k is stochastically dominated by a random variable having a geometric distribution with success probability p^*. By the strong law of large numbers,

$$\limsup_{k \to \infty} (W_1 + \cdots W_k)/k \leq 1/p^*.$$

Note that

$$\{h(T_n) < k\} \subseteq \{W_1 + \cdots + W_k > n\}$$

and so

$$\liminf_{n\to\infty} h(T_n)/n \geq p^*.$$

Finally, we show that the limit is almost surely constant. In the notation above,

$$h(T_n^m) \leq h(T_{m+n}) \leq h(T_m) + h(T_n^m) \leq m + h(T_n^m).$$

Thus, $h(T_{m+n}) - m \leq h(T_n^m) \leq h(T_{m+n})$, and we conclude that

$$\lim_{n\to\infty} h(T_n)/n = \lim_{n\to\infty} h(T_n^m)/n$$

for all m. Therefore $\lim_{n\to\infty} h(T_n)/n$ is a tail random variable for $(X_n)_{n\in\mathbb{N}}$, and the Kolmogorov zero–one law gives the result.

□

For $k = 0, 1, \ldots$ set $\partial B_k = B_k \backslash B_{k-1}$, where we put $B_{-1} = \emptyset$. A straightforward compactness argument establishes the following result.

Lemma 14 *There exists a sequence $(g_k)_{k\in\mathbb{N}}$ of elements of S such that $g_1 \cdots g_k \in \partial B_k$ for all k.*

Remark 15 Both the upper and lower bounds on the limit in Theorem 13 are attainable. To see that the upper bound is attainable, take G to be the free group on two generators α, β and put $p_\alpha = p_\beta = \frac{1}{2}$. Then $h(T_n) = n$ for all n. To see that the lower bound is attainable, take G to be $\mathbb{Z}$ and $p_{+1} = p_{-1} = \frac{1}{2}$. It is easy to see that

$$h(T_n) = \#\{1 \leq i \leq n : X_i = +1\} \vee \#\{1 \leq i \leq n : X_i = -1\}$$

and

$$\begin{aligned}&\lim_{n\to\infty} n^{-1}\#\{1 \leq i \leq n : X_i = +1\}\\ &\quad = \lim_{n\to\infty} n^{-1}\#\{1 \leq i \leq n : X_i = -1\}\\ &\quad = \frac{1}{2}.\end{aligned}$$

5 Growth of the size

Observe that $\#(\partial B_n) \leq (\#(S))^n$ for all n, and from Lemma 14 that $\partial B_n \neq \emptyset$ for all n. Also, $\partial B_{m+n} \subseteq \{uv : u \in \partial B_m,\ v \in \partial B_n\}$ for all m, n so that $\#(\partial B_{m+n}) \leq \#(\partial B_m)\#(\partial B_n)$. A standard subadditivity argument shows that there is $0 \leq b \leq \log \#(S)$ such that $\lim_{n\to\infty} n^{-1} \log \#(\partial B_n) = b$. It is not hard to see that b is zero when G is abelian. An example of a situation in which b is not zero is when V contains two or more free elements.

We will write $\#(T_n)$ for $\#(V_n)$.

Theorem 16 *There is a constant $c_\# \in [0, \log 2]$ such that*

$$\lim_{n\to\infty} n^{-1} \log \#(T_n) = c_\#, \ a.s.$$

The constant $c_\#$ is nonzero if and only if b is nonzero.

Proof. It is clear from the construction that $\#(V_n \backslash V_{n-1}) \leq \#(V_{n-1})$ for all n and so $\#(T_n) \leq 2^n$ for all n.

In the notation of the proof of Theorem 13, $V_{m+n} = V_m V_n^m$, and hence $\log \#(V_{m+n}) \leq \log \#(V_m) + \log \#(V_n^m)$. An application of the subadditve ergodic theorem shows that $n^{-1} \log \#(T_n)$ converges almost surely as $n \to \infty$. An appeal to the Kolmogorov zero–one law similar to the one in the proof of Theorem 13 shows that the limit is constant.

As $c_\# \leq b$, it only remains to show that if b is not zero, then neither is $c_\#$. For this it certainly suffices to show that if we choose K sufficiently large, then with probability one $B_n \subseteq V_{Kn}$ for all n sufficiently large.

Consider $v \in B_n \backslash \{e\}$ written as a product $v = g_1 \cdots g_m$ of elements of S, where $1 \leq m \leq n$. Define a sequence of independent random variables $(W_k)_{k=1}^m$ by

$$W_1 = \inf\{\ell \geq 1 : X_\ell = g_1\}$$

and

$$W_{k+1} = \inf\{\ell \geq 1 : X_{W_1 + \cdots + W_k + \ell} = g_{k+1}\},\ 1 \leq k \leq m-1.$$

Observe that W_k has a geometric distribution with success probability p_{g_k}.

Note that

$$\{v \notin V_{Kn}\} \subseteq \{W_1 + \cdots + W_m > Kn\}.$$

The random variable $W_1+\cdots+W_m$ is stochastically dominated by a random variable of the form $\tilde{W}_1+\cdots\tilde{W}_n$, where $\tilde{W}_1,\ldots,\tilde{W}_n$ are iid with common distribution the geometric distribution with success probability p^*. Thus, by Markov's inequality,

$$\mathbb{P}\{v \notin V_{Kn}\} \leq e^{-\lambda K n}\phi(\lambda)^n,$$

where

$$\phi(\lambda)=\mathbb{P}[e^{\lambda \tilde{W}_1}]=\frac{p^* e^\lambda}{1-(1-p^*)e^\lambda}$$

for $0<\lambda<-\log(1-p^*)$. Therefore

$$\mathbb{P}\{B_n \not\subseteq V_{Kn}\} \leq \#(B_n)e^{-\lambda K n}\phi(\lambda)^n.$$

The sequence of terms given by the righthand side is summable when K is sufficiently large, and the result follows from the Borel-Cantelli lemma.

□

References

[1] J.M. Alonso, T. Brady, D. Cooper, V. Ferlini, M. Lustig, M. Mihalik, M. Shapiro, and H. Short, *Notes on word hyperbolic groups*, Group theory from a geometrical viewpoint (Trieste, 1990) (H. Short, ed.), World Sci. Publishing, River Edge, NJ, 1991, pp. 3–63.

[2] A. Broder, *Generating random spanning trees*, Proc. 30'th IEEE Symp. Found. Comp. Sci., 1989, pp. 442–447.

[3] M. Coornaert, T. Delzant, and A. Papadopoulos, *Géométrie et théorie des groupes*, Lecture Notes in Mathematics, vol. 1441, Springer, 1990.

[4] É. Ghys and P. de la Harpe (eds.), *Sur les groupes hyperboliques d'apres Mikhael Gromov: papers from the Swiss seminar on hyperbolic groups held in Bern, 1988*, Progress in Mathematics, vol. 83, Birkhäuser, Boston, MA, 1990.

[5] J.F.C. Kingman, *Subadditive ergodic theory*, Ann. Probab. **1** (1973), 883–909.

Department of Statistics #3860
University of California
367 Evans Hall
Berkeley, CA 94720-3860
U.S.A.