A conjecture on the Hall topology for the free group

Jean-Eric Pin[*] and Christophe Reutenauer[†]

Abstract

The Hall topology for the free group is the coarsest topology such that every group morphism from the free group onto a finite discrete group is continuous. It was shown by M. Hall Jr that every finitely generated subgroup of the free group is closed for this topology. We conjecture that if $H_1, H_2, \ldots, H_n$ are finitely generated subgroups of the free group, then the product $H_1 H_2 \cdots H_n$ is closed. We discuss some consequences of this conjecture. First, it would give a nice and simple algorithm to compute the closure of a given rational subset of the free group. Next, it implies a similar conjecture for the free monoid, which, in turn, is equivalent to a deep conjecture on finite semigroup, for the solution of which J. Rhodes has offered \$100. We hope that our new conjecture will shed some light on the Rhodes's conjecture.

1 A conjecture on the Hall topology for the free group

Let A be a finite set, called the alphabet. We denote by A^* the free monoid over A, and by $F(A)$ the free group over A. The identity of $F(A)$ is denoted by 1.

The Hall (or profinite) topology for the free group was introduced by M. Hall in [6]. It is the coarsest topology on $F(A)$ such that every group morphism from $F(A)$ onto a finite discrete group is continuous. That is, a sequence u_n of elements of $F(A)$ converges to an element u of $F(A)$, if and only if, for every group morphism $\varphi : F(A) \to G$ (where G is a finite group), there exists an integer n_φ such that for every $n \geq n_\varphi$, $\varphi(u_n) = \varphi(u)$.

This topology can also be defined by a distance. Since the free group is residually finite, two distinct elements u and v of the free group can always be "separated" by a finite group. More precisely, there exists a group morphism

[*] LITP, Tour 55-65, Université Paris VI et CNRS, 4 Place Jussieu, 75252 Paris Cedex 05, FRANCE

[†] UQAM, Dept. Math. Informatique Case Postale 8888, succursale A, Montréal, Québec H3C 3P8 CANADA

φ from $F(A)$ onto some finite group G such that $\varphi(u) \neq \varphi(v)$. Now, make the usual conventions $\min \emptyset = \infty$ and $e^{-\infty} = 0$ and set

$$r(u,v) = \min\{\operatorname{Card} G \mid G \text{is a finite group that separates } u \text{ and } v\}$$

and

$$d(u,v) = e^{-r(u,v)}.$$

Then d is a distance (in fact an ultrametric distance) which defines the Hall topology, and it is not difficult to see that the multiplication $(u,v) \rightarrow uv$ is uniformly continuous for this topology. Thus the free group is now a topological group.

Here is an example of converging sequences :

Proposition 1.1 [14] *For every $x, y, u \in F(A)$, $\lim_{n\to\infty} xu^{n!}y = xy$.*

Proof. Since the multiplication is continuous, it suffices to show that

$$\lim_{n\to\infty} u^{n!} = 1.$$

Let G be a finite group, and let $\varphi : F(A) \rightarrow G$ be a group morphism. Then, for every $n \geq |G|$, $|G|$ divides $n!$, and thus $\varphi(u^{n!}) = 1$. □

Note that the same result clearly holds if $n!$ is replaced by $\operatorname{lcm}\{1, 2, \ldots, n\}$. The following important result was proved by M. Hall.

Theorem 1.2 [6] *Every finitely generated subgroup of the free group is closed.*

The proof of Theorem 1.2 is based on a well-known "separation" result: if G is a finitely generated subgroup of a free group, and if $g \in G$, then there exists a subgroup of finite index containing G but not g. See [7, 17]. Given two subsets X and Y of the free group, recall that the product XY is the set

$$XY = \{xy \mid x \in X \text{ and } y \in Y\}.$$

We propose the following conjecture, which obviously extends the theorem of Hall.

Conjecture 1. *If $H_1, \ldots, H_n$ is a finite sequence of finitely generated subgroups of the free group, then the product $H_1H_2 \cdots H_n$ is closed.*

The conjecture itself seems to be difficult, even in particular cases. However, it has some elegant consequences, which are discussed in sections 2 and 3, and an intuitive meaning, that we try to explain in the conclusion.

2 Rational subsets of the free group

The concept of rational subset originates from theoretical computer science (see [5]) and can be given for an arbitrary monoid M. Intuitively, a set is rational if and only if it can be constructed from a singleton by a finite number of "elementary operations". These "elementary operations" are union, product, and star (or submonoid generated by). More precisely, we have the following definition.

Définition 2.1 The rational subsets of a monoid M form the smallest class $\mathrm{Rat}(M)$ of subsets of M such that

(a) the empty set and every singleton $\{m\}$ belong to $\mathrm{Rat}(M)$,

(b) if S and T are in $\mathrm{Rat}(M)$, then so are ST and $S \cup T$,

(c) if S is in $\mathrm{Rat}(M)$, then so is S^*, the submonoid of M generated by S.

The following proposition summarizes the main properties of the rational subsets of a free group $F(A)$.

Proposition 2.1 [1, 2, 3]

(a) $\mathrm{Rat}(F(A))$ *is closed under boolean operations (union, intersection and complement in* $F(A)$*).*

(b) *A subgroup* G *of* $F(A)$ *is rational if and only if it is finitely generated.*

For technical purposes it is convenient to introduce another class of sets, obtained by considering a slightly different set of elementary operations.

Définition 2.2 Let $\mathcal{F}$ be the smallest class of subsets of the free group such that

(1) the empty set and every singleton $\{m\}$ belong to $\mathcal{F}$,

(2) if S and T are in $\mathcal{F}$, then so are ST and $S \cup T$,

(3) if S is in $\mathcal{F}$, then so is $\langle S \rangle$, the subgroup of $F(A)$ generated by S.

The following proposition gives an equivalent description of $\mathcal{F}$.

Proposition 2.2 $\mathcal{F}$ *is the class of all subsets of* $F(A)$ *which are equal to a finite union of sets of the form* $gG_1G_2\cdots G_r$*, where* $g \in F(A)$ *and* $G_1, \ldots, G_r$ *are finitely generated subgroups of* $F(A)$*.*

Proof. . Let $\mathcal{S}$ be the class of all subsets of $F(A)$ which are finite union of sets of the form $gG_1G_2\cdots G_r$, where $g \in F(A)$ and $G_1, \ldots, G_r$ are finitely generated subgroups of $F(A)$. Every finitely generated group is rational by Proposition 2.1, and thus every element of $\mathcal{S}$ is rational.

Since a finite set is a finite union of singletons, $\mathcal{F}$ contains the finite subsets of $F(A)$. Therefore, it also contains the finitely generated subgroups, and all the elements of $\mathcal{S}$. Thus $\mathcal{S}$ is contained in $\mathcal{F}$.

Conversely, $\mathcal{S}$ contains the empty set (obtained as an empty union), the singletons (take $r = 0$), and is obviously closed under finite union. $\mathcal{S}$ is also closed under product, since if $g, h \in F(A)$ and $G_1, \ldots, G_r$, $H_1, \ldots, H_s$ are finitely generated subgroups of $F(A)$, then

$$(gG_1G_2 \cdots Gr)(hH_1H_2 \cdots H_s) = \\ gh(h^{-1}G_1h)(h^{-1}G_2h) \cdots (h^{-1}G_rh)H_1H_2 \cdots H_s$$

and $(h^{-1}G_1h)$, ..., $(h^{-1}G_rh)$ are finitely generated subgroups of $F(A)$.

Finally, let $S \in \mathcal{S}$. Then S is rational, and $\langle S \rangle = (S \cup S')^*$, where $S' = \{s^{-1} \mid s \in S\}$. Then S' is rational, and hence $\langle S \rangle$ is rational. Thus $\langle S \rangle$ is a rational subgroup of $F(A)$ and is finitely generated by Proposition 2.1. Therefore $\langle S \rangle \in \mathcal{S}$. It follows that $\mathcal{S}$ is closed under the operation $S \to \langle S \rangle$ and thus contains $\mathcal{F}$. □

The next proposition is a first consequence of Conjecture 1.

Proposition 2.3 *If Conjecture 1 is true, every element of $\mathcal{F}$ is a closed rational subset of $F(A)$.*

Proof. According to Conjecture 1, every product of the form $G_1G_2 \ldots G_r$, where $G_1, \ldots, G_r$ are finitely generated subgroups of $F(A)$, is closed. Since the multiplication is continuous, a set of the form $gG_1G_2 \ldots G_r$, where $g \in F(A)$, is also closed, and thus every element of $\mathcal{F}$ is a rational closed subset of $F(A)$. □

Conjecture 1, if true, would give a nice algorithm to compute the (topological) closure of a given rational set.

Theorem 2.4 *If Conjecture 1 is true, the closure of a rational set belongs to $\mathcal{F}$ (and hence, is rational). Furthermore, this closure can be computed using the following formulas, where S and T are rational subsets of the free group:*

(1) $\overline{S} = S$ *if S finite,*
(2) $\overline{S} \cup \overline{T} = \overline{S \cup T}$
(3) $\overline{ST} = \overline{S}\,\overline{T}$
(4) $\overline{S^*} = \langle S \rangle$.

Proof. . Let $\mathcal{R}$ be the class of all rational sets whose closure belongs to $\mathcal{F}$. We first show that (1)-(4) hold for every $S, T \in \mathcal{R}$. First (1) and (2) hold in every metric space. Next, suppose $S, T \in \mathcal{R}$. Then $\overline{S}, \overline{T} \in \mathcal{F}$ by definition, and $\overline{S}\,\overline{T} \subset \overline{ST}$ since the multiplication is continuous. On the other hand, $ST \subset \overline{S}\,\overline{T}$, and since $\overline{S}\,\overline{T} \in \mathcal{F}$, $\overline{S}\,\overline{T}$ is closed, by Proposition 2.3, so that $\overline{ST} \subset \overline{S}\,\overline{T}$. Thus $\overline{ST} = \overline{S}\,\overline{T}$, proving (3).

Finally, S^* is contained in $\langle S \rangle$, which is a rational subgroup of $F(A)$. Therefore $\langle S \rangle$ is finitely generated, by Proposition 2.1 and closed, by Theorem 1.2. Thus $\overline{S^*} \subset \langle S \rangle$ and $\langle S \rangle \in \mathcal{F}$. On the other hand, we claim that $\overline{S^*}$ is a subgroup of $F(A)$. It is a submonoid of $F(A)$, as the closure of the submonoid S^* of $F(A)$ (since the multiplication is continuous). Furthermore, for every $x \in \overline{S^*}$ and every $n > 0$, $x^{n!-1} \in \overline{S^*}$, whence $x^{-1} = \lim_{n\to\infty} x^{n!-1} \in \overline{S^*}$, proving the claim. It follows that $\langle S \rangle \subset \overline{S^*}$, and thus (4) also holds.

We now show that $\mathcal{R}$ contains the rational sets of $F(A)$. $\mathcal{R}$ clearly contains the empty set and the singletons. Furthermore, by (2) and (3), $\mathcal{R}$ is closed under finite union and product. Finally, if $S \in \mathcal{R}$, then $\overline{S^*} = \langle S \rangle \in \mathcal{F}$, and thus $S^* \in \mathcal{R}$. □

Corollary 2.5 *If the conjecture is true, $\mathcal{F}$ is the set of all closed rational subsets of $F(A)$.*

Proof. By Proposition 2.3, every element of $\mathcal{F}$ is a closed rational set. Conversely, if S is a closed rational set, then $\overline{S} = S$ belongs to $\mathcal{F}$, by Theorem 2.4. □

Thus our conjecture implies that the closure of a rational set is rational and gives an algorithm to compute this closure.

3 A consequence of Conjecture 1

We were not able to prove (or disprove!) our conjecture, even for $n = 2$. However, we have decided to publish it, because it implies a deep conjecture on finite semigroups, for the solution of which J. Rhodes [16] has recently offered \$100. Rhodes' conjecture has been proved in some significant particular cases, giving some evidence that it might be true. We shall not state the conjecture of Rhodes in this paper, but we shall state a third conjecture, which has been proved to be equivalent to that of Rhodes [12, 9]. The reader interested directly in the conjecture of Rhodes is referred to [11] for a survey. We consider the free monoid A^* as embedded into the free group $F(A)$. The Hall topology for A^*, induced by the Hall topology for the free group, was first considered in [14]. The terms "rational" and "closure" will now refer to A^* (unless a reference to $F(A)$ is explicitely mentionned). In [12, 13, 9], the following conjecture was stated and proved to be equivalent to the conjecture of Rhodes. For every $u \in A^*$, set

$$u^+ = \{u^n \mid n > 0\}.$$

Conjecture 2. Let L be a rational subset of A^*. Then L is closed if and only if it satisfies the following condition:

(C) For every $x, u, y \in A^*$, if $xu^+y \subset L$, then $xy \in L$.

It is easy to see that (C) is a necessary condition : indeed, if L is closed, and if $xu^ny \in L$ for every $n > 0$, then $\lim_{n\to\infty} xu^{n!}y = xy \in L$. Our two conjectures are related as follows.

Theorem 3.1 *Conjecture 1 implies Conjecture 2.*

Proof. For any subset L of A^*, put

$$F(L) = \{v \in A^* \mid \text{there exists a factorization } v = xy \text{ and } u \in A^* \text{ such that } xu^+y \subset L\}.$$

The operator $\mathcal{F}$ can be iterated by setting, for every $n > 0$, $F^{(0)}(L) = L$ and $F^{n+1}(L) = F(F^n(L))$. Finally, put $F^*(L) = \cup_{n \geq 0} F^n(L)$. We shall prove the following three statements, where L is a rational subset of A^*.

(a) if L satisfies (C), then $F^*(L) = L$,

(b) $F^*(L)$ is contained in $\overline{L}$ and

(c) if Conjecture 1 is true, then $F^*(L) = \overline{L}$.

(a) is easy, because if L satisfies condition (C), then $F(L) \subset L$, and hence $F^*(L) = L$.

(b) Since L is contained in $\overline{L}$, $F^*(L)$ is contained in $F^*(\overline{L})$, and by induction it suffices to prove that $F(\overline{L})$ is contained in $\overline{L}$. Let $v \in F(\overline{L})$. Then by definition, there exist a factorization $v = xy$ and $u \in A^*$ such that $xu^+y \subset \overline{L}$. Since $\overline{L}$ is closed, it follows that $v = xy = \lim_{n\to\infty} xu^{n!}y$ belongs to $\overline{L}$.

(c) Let us call a *simple* set a set of the form $L_0^*u_1L_1^*u_2 \cdots u_kL_k^*$, where L_0, $\ldots$, L_k are rational subsets of A^* and $u_1, \ldots, u_k \in A^*$. It is not difficult to prove that every rational subset of A^* is a finite union of simple sets [13, Proposition 7.7]. The next step consists in proving the following lemma:

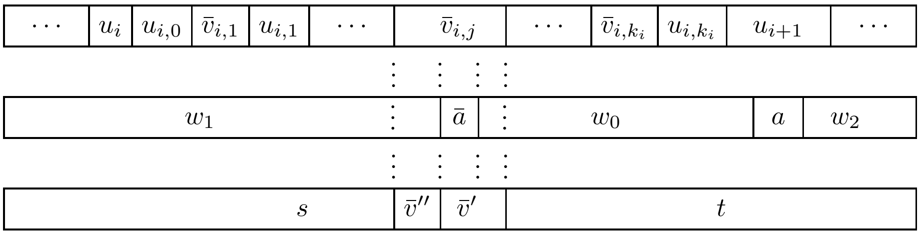
Lemma 3.2 *Let $L = L_0^*u_1L_1^*u_2 \cdots u_kL_k^*$ be a simple set. Then $F^*(L)$ contains $\langle L_0\rangle u_1\langle L_1\rangle u_2 \cdots u_k\langle L_k\rangle \cap A^*$.*

Set $A' = \{\bar{a} \mid a \in A\}$, and let $\pi : (A \cup A')^* \to F(A)$ be the monoid morphism defined by $\pi(a) = a$ and $\pi(\bar{a}) = a^{-1}$. Set, for $u = a_1 \ldots a_r \in A^*$, $\bar{u} = \bar{a}_r \ldots \bar{a}_1$, and put, for $0 \leq i \leq n$, $L'_i = \{\bar{u} \mid u \in L_i\}$. Now since

$$\pi((L_0 \cup L'_0)^*u_1(L_1 \cup L'_1)^*u_2 \cdots u_k(L_k \cup L'_k)^*) = \langle L_0\rangle u_1\langle L_1\rangle u_2 \cdots u_k\langle L_k\rangle,$$

it suffices to show that, for each $w \in (L_0 \cup L'_0)^*u_1(L_1 \cup L'_1)^*u_2 \cdots u_k(L_k \cup L'_k)^*$, $\pi(w) \in A^*$ implies $\pi(w) \in F^*(L)$. This is done by induction on the number n of occurrences of letters of A' in w. Put $x = \pi(w)$.

If $n = 0$, then $x \in L$ and the result is trivial. Otherwise, w has a factorization of the form $w = w_0u_1 \cdots u_kw_k$ where each $w_i \in (L_i \cup L'_i)^*$. Thus each w_i can be further factorized as $w_i = u_{i,0}\bar{v}_{i,1}u_{i,1} \cdots \bar{v}_{i,k_i}u_{i,k_i}$, where the $u_{i,j}$'s and the $v_{i,j}$'s belong to L_i. Now, it is well known [3] that x can be derived from the word w by applying rewriting rules of the form $a\bar{a} \to 1$ or $\bar{a}a \to 1$ (where $a \in A$). Consider the *last* rule applied, which may be supposed to be of the form $\bar{a}a \to 1$ (the other case would be dual). Then x admits a factorization $x = x_1x_2$ (such that $x_1\bar{a}ax_2 \to x_1x_2$ is the last derivation), where $x_1, x_2 \in A^*$, and w admits a factorization of the form $w = w_1\bar{a}w_0aw_2$ where $\pi(w_1) = x_1$, $\pi(w_2) = x_2$, and $\pi(w_0) = 1$, whence $\pi(\bar{a}w_0aw_2) = x_2$. The occurrence of $\bar{a}$ defined by this factorization defines an occurrence of $\bar{a}$ in some $\bar{v}_{i,j}$, that is, $\bar{v}_{i,j} = \bar{v}''\bar{v}'$, where $\bar{a}$ is the first letter of $\bar{v}'$. Setting $w = s\bar{v}''\bar{v}'t$, we have $s\bar{v}'' = w_1$ and $\bar{v}'t = \bar{a}w_0aw_2$, according to the following diagram.



Now $\bar{v}''\bar{v}' \in L'_i$, that is, $v'v'' \in L_i \cap A^+$, $s \in (L_0 \cup L'_0)^*u_1 \cdots u_i(L_i \cup L'_i)^*$ and $t \in (L_i \cup L'_i)^*u_{i+1} \cdots u_k(L_k \cup L'_k)^*$. Consequently, we have, for each $n > 0$,

$$w_n = s(v'v'')^{n-1}t \in (L_0 \cup L'_0)^*u_1 \cdots u_k(L_k \cup L'_k)^*$$

and

$$\begin{aligned}\pi(w_n) &= \pi(s\bar{v}''(v''v')^n\bar{v}'t) = \pi(s\bar{v}'')(\pi(v''v'))^n\pi(\bar{v}'t)\\ &= \pi(w_1)\pi((v''v')^n)\pi(\bar{a}w_0aw_2) = x_1\pi((v''v'))^nx_2 \in A^*\end{aligned}$$

Furthermore, the number of occurrences of letters from A' in w_n is strictly smaller than in w. It follows, by the induction hypothesis, that $\pi(w_n) \in F^*(L)$. Therefore

$$x_1(\pi(v''v'))^+x_2 \subset F^*(L),$$

and thus $x = x_1x_2 \in F^*(L)$ by definition of $F^*(L)$. This concludes the induction and the proof of the lemma. □

Let L be a rational subset of A^*. Then $L = \bigcup_{1 \leq i \leq n} L_i$, where each L_i is a rational simple set. Put $L_i = L^*_{0,i}u_{1,i}L^*_{1,i}u_{2,i} \cdots u_{k_i,i}L^*_{k_i,i}$. Then $F^*(L)$ contains $F^*(L_i)$ for every i, and by Lemma 3.2, $F^*(L_i)$ contains

$$\langle L_{0,i}\rangle u_{1,i}\langle L_{1,i}\rangle u_{2,i} \cdots u_{k_i,i}\langle L_{k_i,i}\rangle \cap A^*.$$

Thus, by (b), we have the inclusions

$$L \subset \bigcup_{1 \leq i \leq n} (\langle L_{0,i}\rangle u_{1,i}\langle L_{1,i}\rangle u_{2,i} \cdots u_{k_i,i}\langle L_{k_i,i}\rangle \cap A^*) \subset F^*(L) \subset \overline{L}.$$

Now every set of the form $\langle L_0\rangle u_1\langle L_1\rangle u_2 \cdots u_k\langle L_k\rangle$ belongs to $\mathcal{F}$ by construction, and by Proposition 2.3, is closed in $F(A)$ if Conjecture 1 is true. Therefore, every set of the form $\langle L_0\rangle u_1\langle L_1\rangle u_2 \cdots u_k\langle L_k\rangle \cap A^*$ is closed in A^*, and thus $F^*(L) = \overline{L}$.

Finally, if Conjecture 1 is true, a rational set which satisfies (C) is closed by (a) and (c). □

4 Conclusion

Our hope is that Conjecture 1 will provide new algebraic tools to attack the conjecture of Rhodes. In fact, even a negative answer to Conjecture 1 would probably be illuminating for this problem. The intuitive content of Conjecture 1 is summarized in the following sentence :

"To compute the closure of a rational set, the formula $\lim\limits_{n \to \infty} u^{n!} = 1$ suffices."

In the case of A^*, this corresponds to the formula $F^*(L) = \overline{L}$. In fact, we do not know of any explicit example of converging sequence, which is not more or less of the type $u^{n!}$ (or $u^{\mathrm{lcm}\{1, \ldots n\}}$), or derived from this type by using the continuity of the multiplication. However, such examples *may* exist (an explicit example for a related topology, obtained by replacing finite groups by p-groups in the definition, is given in [4]). Our conjecture states that even if such weird examples exist, they are not useful to compute the closure of a rational set. The idea is that rational sets are sufficently "simple" or "regular" to avoid these complicated examples.

References

[1] A. Anissimov and A.W. Seifert, Zur algebraischen Charakteristik der durch kontext-freie Sprachen definierten Gruppen. *Elektron. Inform. Verarb. Kybern.* **11**, (1975), 695–702.

[2] M. Benois, Parties rationnelles du groupe libre. *C.R. Acad. Sci. Paris, Sér. A*, **269**, (1969), 1188–1190.

[3] J. Berstel, *Transductions and Context-free Languages*, Teubner, Stuttgart, (1979).

[4] J. Berstel, M. Crochemore and J.E. Pin, Thue-Morse sequence and p-adic topology for the free monoid. *Discrete Mathematics* **76**, (1989), 89–94.

[5] S. Eilenberg, *Automata, Languages and Machines*, Academic Press, New York, Vol. A, 1974; Vol B, 1976.

[6] M. Hall Jr., A topology for free groups and related groups, *Ann. of Maths*, **52**, (1950), 127-139.

[7] R.C. Lyndon and P.E. Schupp, *Combinatorial Group Theory*, Springer Verlag, 1977.

[8] S.W. Margolis and J.E. Pin, Varieties of finite monoids and topology for the free monoid, *Proceedings of the Marquette Semigroup Conference* (Marquette University, Milwaukee), (1984), 113–130.

[9] S.W. Margolis and J.E. Pin, New results on the conjecture of Rhodes and on the topological conjecture, *J. Pure Appl. Algebra* **80**, (1992), 305–313.

[10] J.E. Pin, Finite group topology and p-adic topology for free monoids, *12th ICALP*, Lecture Notes in Computer Science **194**, Springer, Berlin, (1985), 445–455.

[11] J.E. Pin, On a conjecture of Rhodes, *Semigroup Forum* **39**, (1989), 1–15.

[12] J.E. Pin, A topological approach to a conjecture of Rhodes, *Bulletin of the Australian Mathematical Society* **38**, (1988), 421–431.

[13] J.E. Pin, Topologies for the free monoid, *Journal of Algebra* **137**, (1991), 297–337.

[14] Ch. Reutenauer, Une topologie du monoïde libre, *Semigroup Forum* **18**, (1979), 33–49.

[15] Ch. Reutenauer, Sur mon article "Une topologie du monoïde libre", *Semigroup Forum* **22**, (1981), 93–95.

[16] J. Rhodes, New techniques in global semigroup theory, *Semigroups and Their Applications*, ed. S.M. Goberstein and P.M. Higgins, Reidel, Dordrecht, (1987), 169–181.

[17] J. Stallings, Topology of finite graphs, *Invent. Math.* **71**, (1983), 551–565.