# THE BASE OF THE INTERSECTION OF TWO FREE SUBMONOIDS* 

Ronald V. BOOK<br>Department of Mathematics, University of California at Santa Barbara, Santa Barbara, CA 93106, USA

Received 13 February 1984
Revised 18 December 1984


#### Abstract

Given two free submonoids of a free monoid, one wishes to find a specification for the base of the intersection. An algorithm to construct a graph-theoretic specification of the base is presented. From this specification it can easily be determined whether the base is finite. In addition, a polynomial-time algorithm to determine if a regular set is a circular code is presented.


## 1. Introduction

It is known [6] that the intersection of two finitely generated subgroups of a free group is again finitely generated. Recently, Avenhaus and Madlener [1] have given a polynomial time algorithm for computing a set of generators for such an intersection. In the case of monoids, the situation is different. First, a submonoid of a free monoid is not necessarily free. Second, while the intersection of two finitely generated free submonoids is again free, this intersection is not necessarily finitely generated.

It is well known that it is decidable whether the submonoid of a free monoid which is generated by a finite set (or even a regular set) is free. The purpose of this paper is to present a polynomial time algorithm to generate a graph-theoretic specification of the base of the intersection of two free submonoids that are regular sets. Each submonoid is specified by a deterministic finite-state acceptor for its base. The running time of the algorithm is linear in the product of the sizes of the transition tables for the two finite-state acceptors. From this specification of the base of the intersection, it is easy to determine whether the base is finite.

This algorithm is a minor modification of an algorithm due to Even [4,5] that is useful in the study of variable-length codes. Comments on Even's original work are given in Section 3 and circular codes are considered. A polynomial-time algorithm to determine whether a regular set is a circular code is presented.

[^0]
## 1. Submonoids of a free monoid

For a finite set $\Sigma$ of symbols, let $\Sigma^{*}$ denote the free monoid generated by $\Sigma$. If $A \subseteq \Sigma^{*}$, then let $A^{*}$ denote the submonoid of $\Sigma^{*}$ generated by $A$, that is, $A^{*}=\left\{y_{i_{1}} \ldots y_{u_{n}} \mid n \geq 1\right.$, each $\left.y_{i_{j}} \in A\right\} \cup\{e\}$ where $e$ is the empty string, the string of length 0 . For every $A \subseteq \Sigma^{*}$, there is a unique minimal generating set $B_{A} \subseteq \Sigma^{*}$ such that $B_{A}^{*}=A^{*}$; the set $B_{A}$ is $A^{+}-A^{+} A^{+}$, where $A^{+}=A^{*}-\{e\}$, and is called the base of $A^{*}$. Recall that the submonoid $A^{*}$ is free if and only if every string in $A^{*}$ has a unique factorization as a concatenation of strings in $B_{A}$.

We assume that the reader is familiar with the fundamentals of the theory of regular sets, for example, that a subset of $\Sigma^{*}$ is regular if and only if it is recognized by a deterministic or nondeterministic finite-state acceptor if and only if it is denoted by a regular expression. Recall that the class of regular subsets of $\Sigma^{*}$ is the smallest class containing the finite subsets and closed under union, concatenation, and *.

It is easy to see that there is a nondeterministic procedure that on input a regular set $A \subseteq \Sigma^{*}$ (say $A$ is specified by a finite-state acceptor) will determine whether $A$ is not a base, and that operates within $\log n$ work space. Hence, there is a deterministic polynomial time algorithm to determine whether a regular set is a base. Further, the algorithm of Even $[4,5,3]$ that determines whether $A^{*}$ is free when $A$ is a finite base can be extended to regular sets, and this extension again operates deterministically in polynomial time.

Now it is clear that if $A^{*}$ and $B^{*}$ are free submonoids of $\Sigma^{*}$, then so is $A^{*} \cap B^{*}$, and it is well known that if $A^{*}$ and $B^{*}$ are regular sets, then so are $A^{*} \cap B^{*}$ and the base of $A^{*} \cap B^{*}$. On the other hand, if $A$ and $B$ are finite, then the base of $A^{*} \cap B^{*}$ is not necessarily finite. For example, let $\Sigma=\{a, b\}, A=\{a, a b\}$, and $B=\{a, b a\}$. It is clear that $A^{*}$ and $B^{*}$ are free. Let $C=\left\{(a b)^{i} a \mid i \geq 0\right\}$. Clearly, $C$ is a base and $C^{*}$ is free. We claim that $C^{*}=A^{*} \cap B^{*}$ so that $A^{*} \cap B^{*}$ is not finitely generated. For any $i,(a b)^{i} a$ is in $A^{*}$ and $a(b a)^{i}$ is in $B^{*}$ so that $(a b)^{i} a \in A^{*} \cap B^{*}$; hence, $C^{*} \subseteq A^{*} \cap B^{*}$. To show that $A^{*} \cap B^{*} \subseteq C^{*}$, consider the base of $A^{*} \cap B^{*}$, say $D$, and argue by induction on the length of strings in $D$ that $D \subseteq C$, concluding $D=C$; the details are left to the reader.

## 2. Computing a specification of the basis

Theorem 1. Consider the following problem:
INSTANCE: Two deterministic finite-state acceptors $M_{A}$ and $M_{B}$ specifying the regular sets $A$ and $B$ respectively, where $A$ is a base, $A^{*}$ is free, $B$ is a base, and $B^{*}$ is free.
QUESTION: Is the base of $A^{*} \cap B^{*}$ finite?
There is an algorithm to construct a labeled directed graph to specify the base of $A^{*} \cap B^{*}$. This algorithm runs in time $\mathrm{O}\left(\left|\delta_{A}\right| \cdot\left|\delta_{B}\right|\right)$ where $\left|\delta_{A}\right|\left(\left|\delta_{B}\right|\right)$ is the size of the
table specifying the transition function of $M_{A}\left(\right.$ resp., $\left.M_{B}\right)$. From the graph constructed by this algorithm, one can determine whether the base of $A^{*} \cap B^{*}$ is finite in time $\mathrm{O}\left(\left|\delta_{A}\right|^{2} \cdot\left|\delta_{B}\right|^{2}\right)$.

The remainder of this section is devoted to the proof of Theorem 1. It will be assumed throughout that $A$ and $B$ are regular sets. The other portions of the hypothesis will be explicitly stated whenever they are used.

Let $A$ be a regular set and let $M_{A}=\left(K_{A}, \Sigma, \delta_{A}, q_{A}, F_{A}\right)$ be a deterministic finitestate acceptor that recognizes $A$. (That is, $K_{A}$ is a finite set of states, $\delta_{A}: K_{A} \times \Sigma \rightarrow K_{A}$ is the transition function, $q_{A} \in K_{A}$ is the initial state, and $F_{A} \subseteq K_{A}$ is the set of accepting states; $\delta_{A}$ is extended to $\delta_{A}^{*}: K_{A} \times \Sigma^{*} \rightarrow K_{A}$ by $\delta_{A}^{*}(q, e)=q$ and $\delta_{A}^{*}(q, w a)=\delta_{A}\left(\delta_{A}^{*}(q, w), a\right)$ for all $q \in K_{A}, a \in \Sigma$, and $w \in \Sigma^{*}$; the set of strings recognized by $M_{A}$ is $\left\{w \in \Sigma^{*} \mid \delta_{A}^{*}\left(q_{A}, w\right) \in F_{A}\right\}$.) Construct the following labelled directed graph $G_{A}=\left(K_{A} \cup\left\{s_{A}, f_{A}\right\}, \Sigma, \delta(A), \lambda_{A}, f_{A}\right)$ as follows:
(a) The set of vertices is $K_{A} \cup\left\{s_{A}, f_{A}\right\}$, where $s_{A} \neq f_{A}$ and $\left\{s_{A}, f_{A}\right\} \cap K_{A}=\emptyset$.
(b) The set of directed edges is $\delta(A)=\left\{(p, q) \mid p, q \in K_{A}\right.$ and for some $a \in \Sigma$, $\left.\delta_{A}(p, a)=q\right\} \cup\left\{\left(s_{A}, q\right) \mid\right.$ for some $\left.a \in \Sigma, \delta_{A}\left(q_{0}, a\right)=q\right\} \cup\left\{\left(p, f_{A}\right) \mid\right.$ for some $a \in \Sigma$, $\left.\delta_{A}(p, a) \in F_{A}\right\} \cup\left\{\left(s_{A}, f_{A}\right) \mid\right.$ for some $\left.a \in \Sigma, \delta_{A}\left(q_{0}, a\right) \in F_{A}\right\}$.
(c) The labelling function is $\lambda_{A}:\left(K_{A} \cup\{s, f\}\right) \times\left(K_{A} \cup\{s, f\}\right) \rightarrow 2^{\Sigma}$ where for every $p, q \in K_{A}, a \in \Sigma$,
(i) $a \in \lambda_{A}(p, q) \quad$ if and only if $\quad \delta_{A}(p, a)=q$,
(ii) $a \in \lambda_{A}\left(p, f_{A}\right) \quad$ if and only if $\quad \delta_{A}(p, a) \in F_{A}$,
(iii) $a \in \lambda_{A}\left(s_{A}, q\right)$ if and only if $\delta_{A}\left(q_{0}, a\right)=q$,
(iv) $a \in \lambda_{A}\left(s_{A}, f_{A}\right) \quad$ if and only if $\quad \delta_{A}\left(q_{0}, a\right) \in F_{A}$.

The labelled directed graph $G_{A}$ is a modification of the state graph of $M_{A}$. The vertex $s_{A}$ has in-degree zero and is a 'copy' of $q_{A}$. The vertex $f_{A}$ has out-degree zero and 'copies' all of the states in $F_{A}$ simultaneously. Since $M_{A}$ is deterministic, for each $w \in \Sigma^{*}$, there is a unique computation of $M_{A}$ on $w$ that begins at $q_{A}$. It is easy to see from the construction of $G_{A}$ that for every $w \in A$, there is a unique sequence $p_{0}, p_{1}, \ldots, p_{|w|}$ of vertices in $G_{A}$ such that $p_{0}=s_{A}, p_{|w|}=f_{A}$, and for each $i=1, \ldots,|w|, a_{i} \in \lambda_{A}\left(p_{i-1}, p_{i}\right)$ where $w=a_{1} \ldots a_{|w|}$. Since $A$ is a base, $e \notin A$.

The coding graph $C(A)=\left(K_{A} \cup\left\{s_{A}\right\}, \Sigma, \delta^{A}, \lambda^{A}, s_{A}, s_{A}\right)$ is obtained from the graph $G_{A}$ as follows:
(a) The set of vertices is $K_{A} \cup\left\{s_{A}\right\}$.
(b) The set of directed edges is $\delta^{A}=\left(\delta(A)-\left\{\left(p, f_{A}\right) \mid p \in K_{A} \cup\left\{s_{A}\right\}\right\}\right) \cup\left\{\left(p, s_{A}\right) \mid\right.$ $p \in K_{A} \cup\left\{s_{A}\right\}$ and $\left.\left(p, f_{A}\right) \in \delta(A)\right\}$.
(c) The labelling function is $\lambda^{A}:\left(K_{A} \cup\left\{s_{A}\right\}\right) \times\left(K_{A} \cup\left\{s_{A}\right\}\right) \rightarrow 2^{\Sigma}$ where for $p \in K_{A} \cup\left\{s_{A}\right\} \quad$ and $\quad q \in K_{A}, \quad \lambda^{A}(p, q)=\lambda_{A}(p, q), \quad$ and $\quad$ for $\quad p \in K_{A} \cup\left\{s_{A}\right\}$, $\lambda^{A}\left(p, s_{A}\right)=\lambda_{A}\left(p, f_{A}\right)$.

The coding graph $C(A)$ is obtained from $G_{A}$ by identifying $s_{A}$ and $f_{A}$. Clearly, for $n \geq 1$ and $a_{1}, \ldots, a_{n} \in \Sigma, a_{1} \ldots a_{n} \in A^{*}$ if and only if there is a sequence $p_{0}$, $p_{1}, \ldots, p_{n} \in K_{A} \cup\left\{s_{A}\right\}$ such that $p_{0}=p_{n}=s_{A}$ and for each $i=1, \ldots, n$, $a_{i} \in \lambda^{A}\left(p_{i-1}, p_{i}\right)$; the sequence $p_{0}, p_{1}, \ldots, p_{n}$ is a path-sequence that witnesses $a_{1} \ldots a_{n} \in A^{*}$.

Claim 1. Suppose that $A$ is $a$ base and $A^{*}$ is free. Then, for $n \geq 1$ and $a_{1}, \ldots, a_{n} \in \Sigma, a_{1} \ldots a_{n} \in A^{*}$ if and only if in $C(A)$ there is a unique path-sequence that witnesses $a_{1} \ldots a_{n} \in A^{*}$.

This fact follows immediately from the definitions and the construction of $G_{A}$ and of $C(A)$.

Now we construct a 'testing graph' that provides the basis for our result.
For regular sets $A$ and $B$, let $G_{A}=\left(K_{A} \cup\left\{s_{A}, f_{A}\right\}, \Sigma, \lambda_{A}, \delta(A), s_{A}, f_{A}\right)$ and $G_{B}=\left(K_{B} \cup\left\{s_{B}, f_{B}\right\} ; \Sigma, \lambda_{B}, \delta(B), s_{B}, f_{B}\right)$ be the corresponding labelled directed graphs as described in the last paragraph. Define the testing graph $T\left(G_{A}, G_{B}\right)=(V, E, \lambda)$, where $V$ is the set of vertices, $E$ is the set of edges, and $\lambda: E \rightarrow 2^{\Sigma}$ is the labelling function, as follows:
(a) $V=\left(\left(K_{A} \cup\left\{s_{A}\right\}\right) \times\left(K_{B} \cup\left\{s_{B}\right\}\right)\right) \cup\left\{\left(f_{A}, f_{B}\right)\right\}$.
(b) $E$ is defined as follows: let $p_{1} \in K_{A} \cup\left\{s_{A}\right\}$ and $p_{2} \in K_{B} \cup\left\{s_{B}\right\}$,
(i) for each $q_{1} \in K_{A}$ and $q_{2} \in K_{B}$, there is an edge from ( $p_{1}, p_{2}$ ) to ( $q_{1}, q_{2}$ ) if and only if $\lambda_{A}\left(p_{1}, q_{1}\right) \cap \lambda_{B}\left(p_{2}, q_{2}\right) \neq \emptyset$;
(ii) for each $q_{2} \in K_{B}$, there is an edge from ( $p_{1}, p_{2}$ ) to ( $s_{A}, q_{2}$ ) if and only if $\lambda_{A}\left(p_{1}, f_{A}\right) \cap \lambda_{B}\left(p_{2}, q_{2}\right) \neq \emptyset ;$
(iii) for each $q_{1} \in K_{A}$, there is an edge from $\left(p_{1}, p_{2}\right)$ to ( $q_{1}, s_{B}$ ) if and only if $\lambda_{A}\left(p_{1}, q_{1}\right) \cap \lambda_{B}\left(p_{2}, f_{B}\right) \neq \emptyset ;$
(iv) there is an edge from $\left(p_{1}, p_{2}\right)$ to $\left(f_{A}, f_{B}\right)$ if and only if $\lambda_{A}\left(p_{1}, f_{A}\right) \cap$ $\lambda_{B}\left(p_{2}, f_{B}\right) \neq \theta ;$
(c) The definition of $\lambda$ parallels (b):
(i) $\lambda\left(\left(p_{1}, p_{2}\right),\left(q_{1}, q_{2}\right)\right)=\lambda_{A}\left(p_{1}, q_{1}\right) \cap \lambda_{B}\left(p_{2}, q_{2}\right)$,
(ii) $\lambda\left(\left(p_{1}, p_{2}\right),\left(s_{A}, q_{2}\right)\right)=\lambda_{A}\left(p_{1}, f_{A}\right) \cap \lambda_{B}\left(p_{2}, q_{2}\right)$,
(iii) $\lambda\left(\left(p_{1}, p_{2}\right),\left(q_{1}, s_{B}\right)\right)=\lambda_{A}\left(p_{1}, q_{1}\right) \cap \lambda_{B}\left(p_{2}, f_{B}\right)$,
(iv) $\lambda\left(\left(p_{1}, p_{2}\right),\left(f_{A}, f_{B}\right)\right)=\lambda_{A}\left(p_{1}, f_{A}\right) \cap \lambda_{B}\left(p_{2}, f_{B}\right)$.

It is clear from the definition of $T\left(G_{A}: G_{B}\right)$ that the in-degree of $\left(s_{A}, s_{B}\right)$ and the out-degree of $\left(f_{A}, f_{B}\right)$ are both zero.

The set $W(A, B)$ of word paths of $T\left(G_{A}, G_{B}\right)$ is the set of strings $a_{1} \ldots a_{n}, n \geq 1$, such that there is a sequence $r_{0}, r_{1}, \ldots, r_{n}, r_{0}=\left(s_{A}, s_{B}\right), r_{n}=\left(f_{A}, f_{B}\right)$, where $r_{i} \in\left(K_{A} \cup\left\{s_{A}\right\}\right) \times\left(K_{B} \cup\left\{s_{B}\right\}\right)$ for $0<i<n$, and for each $i=1, \ldots, n, a_{i} \in \Sigma$ and $a_{i} \in \lambda\left(r_{i-1}, r_{i}\right)$; the sequence $r_{0}, r_{1}, \ldots, r_{n}$ is a path-sequence that witnesses $a_{1} \ldots a_{n} \in W(A, B)$.

Let $r_{0}, r_{1}, \ldots, r_{n}$ witness $a_{1} \ldots a_{n} \in W(A, B)$. For each $i=1, \ldots, n-1$, let $r_{i}=\left(p_{i}, q_{i}\right)$
where $p_{i} \in K_{A} \cup\left\{s_{A}\right\}$ and $q_{i} \in K_{B} \cup\left\{s_{B}\right\}$. It is clear that the sequence $S_{A}, p_{1}, \ldots, p_{n-1}, s_{A}$ in $C(A)$ witnesses $a_{1} \ldots a_{n} \in A^{*}$ and the sequence $s_{B}, q_{1}, \ldots, q_{n-1}, s_{B}$ in $C(B)$ witnesses $a_{1} \ldots a_{n} \in B^{*}$. Thus, $W(A, B) \subseteq A^{*} \cap B^{*}$.

Claim 2. $W(A, B)^{*}=A^{*} \cap B^{*}$.
Proof. Since $W(A, B) \subseteq A^{*} \cap B^{*}$ and $A^{*} \cap B^{*}=\left(A^{*} \cap B^{*}\right)^{*}$, it is sufficient to show that if $D$ is the base of $A^{*} \cap B^{*}$, then $D \subseteq W(A, B)^{*}$. In fact, we show that $D \subseteq W(A, B)$.

Let $a_{1} \ldots a_{n} \in D$ where $n \geq 1$ and each $a_{i}$ is in $\Sigma$. Since $D$ is the base of $A^{*} \cap B^{*}$, $a_{1} \ldots a_{n}$ is in $A^{*} \cap B^{*}$ and $a_{1} \ldots a_{n}$ has no factorization as the concatenation of two or more nonempty strings in $A^{*} \cap B^{*}$. Hence, there is a path-sequence $p_{0}, p_{1}, \ldots, p_{n}$ in $C(A)$ witnessing $a_{1} \ldots a_{n} \in A^{*}$ and a path-sequence $q_{0}, q_{1}, \ldots, q_{n}$ in $C(B)$ witnessing $a_{1}, \ldots, a_{n} \in B^{*}$, so that $p_{0}=p_{n}=s_{A}$ and $q_{0}=q_{n}=s_{B}$, and for each $i=1, \ldots, n-1$, either $p_{i} \neq s_{A}$ or $q_{i} \neq s_{B}$ (for otherwise, $a_{1} \ldots a_{n}$ would have a factorization as the concatenation of two or more nonempty strings in $\left.A^{*} \cap B^{*}\right)$. Let $r_{0}=\left(p_{0}, q_{0}\right)$ $\left(=\left(s^{A}, s_{B}\right)\right), r_{n}=\left(f_{A}, f_{B}\right)$, and for each $i=1, \ldots, n-1, r_{i}=\left(p_{i}, q_{i}\right)$; then it is clear that $r_{0}, r_{1}, \ldots, r_{n}$ witnesses $a_{1} \ldots a_{n} \in W(A, B)$.

In general, $W(A, B)$ is not a base: let $A=\{a b a b a b, a b a, b a b, a a a\}$ and $B=$ $\{a b a b a b, a b a, b a b, b b b\}$, so that $\{a b a b a b, a b a, b a b\} \subseteq W(A, B)$.

Claim 3. Suppose that $A$ is a base, $A^{*}$ is free, $B$ is a base, and $B^{*}$ is free. Then $W(A, B)$ is the base of $A^{*} \cap B^{*}$.

Proof. From the proof of Claim 2, we have $D \subseteq W(A, B)$ where $D$ is the base of $A^{*} \cap B^{*}$. Since $W(A, B) \subseteq A^{*} \cap B^{*}, D^{*}=W(A, B)^{*}=A^{*} \cap B^{*}$ so that it is sufficient to show that $W(A, B)$ is a base.

Assume that $W(A, B)$ is not a base. Let $a_{1} \ldots a_{n}, n \geq 1$, each $a_{i} \in \Sigma$, be a string in $W(A, B)$ with a factorization as the concatenation of two or more strings in $W(A, B)$, say $a_{1} \ldots a_{n}=w_{1} \ldots w_{k}$ with $k>1$ and $w_{i} \in W(A, B)$ for each $i=1, \ldots, k$. For each $i=0,1, \ldots, n$, let $r_{i}=\left(p_{i}, q_{i}\right)$ where $r_{0}, \ldots, r_{n}$ is a path-sequence in $T\left(G_{A}, G_{B}\right)$ witnessing $a_{1} \ldots a_{n} \in W(A, B)$. By construction of $T\left(G_{A}, G_{B}\right), r_{i} \neq\left(S_{A}, S_{B}\right)$ if $i \neq 0$. Since $A$ is a base and $A^{*}$ is free, there is a unique path-sequence in $C(A)$ witnessing $a_{1} \ldots a_{n} \in A^{*}$ and by construction this sequence is $s_{A}, p_{1}, \ldots, p_{n-1}, s^{a}$. Also, since $B$ is a base and $B^{*}$ is free, there is a unique path-sequence in $C(B)$ witnessing $a_{1} \ldots a_{n} \in B^{*}$ and by construction this sequence is $s_{B}, q_{1}, \ldots, q_{n-1}, s_{B}$. Now each $w_{i}$ is in $A^{*} \cap B^{*}$ and so for each $w_{i}$ there is a path-sequence in $C(A)$ witnessing $w_{i} \in A^{*}$ and a path-sequence in $C(B)$ witnessing $w_{i} \in B^{*}$. From this collection of pathsequences, we can construct a path-sequence $\overline{p_{0}}, \ldots, \overline{p_{n}}$ in $C(A)$ witnessing $w_{1} \ldots w_{k} \in A^{*}$ and a path-sequence $\overline{q_{0}}, \ldots, \overline{q_{n}}$ in $C(B)$ witnessing $w_{1} \ldots w_{k} \in B^{*}$, where $\overline{p_{0}}=\overline{p_{n}}=s_{A}$ and $\overline{q_{0}}=\overline{q_{n}}=s_{B}$. Since $w_{1} \ldots w_{k}$ is the concatenation of $k$ strings in $A^{*} \cap B^{*}$, there are $k-1$ integers $j$ in $\{1, \ldots, n-1\}$ such that $\left(\overline{p_{j}}, \overline{q_{j}}\right)=\left(s_{A}, s_{B}\right)$.

Thus, the sequence $\left(p_{0}, q_{0}\right), \ldots,\left(p_{n-1}, q_{n-1}\right),\left(s_{A}, s_{B}\right)$ is not equal to the sequence $\left(\overline{p_{0}}, \overline{q_{0}}\right), \ldots,\left(\overline{p_{n}}, \overline{q_{n}}\right)$. Since $a_{1} \ldots a_{n}=w_{1} \ldots w_{k}$, this means that there are two or more path-sequences in $C(A)$ witnessing $a_{1} \ldots a_{n} \in A^{*}$ or there are two or more path-sequences in $C(B)$ witnessing $a_{1} \ldots a_{n} \in B^{*}$, a contradiction.

We are concerned with the cardinality of $W(A, B)$.
Claim 4. $W(A, B)$ is infinite if and only if there are infinitely many paths from $\left(s_{A}, s_{B}\right)$ to $\left(f_{A}, f_{B}\right)$ in $T\left(G_{A}, G_{B}\right)$ if and only if there is a path from $\left(s_{A}, s_{B}\right)$ to $\left(f_{A}, f_{B}\right)$ in $T\left(G_{A}, G_{B}\right)$ that contains a circuit if and only if there is a path from $\left(s_{A}, s_{B}\right)$ to ( $f_{A}, f_{B}$ ) in $T\left(G_{A}, G_{B}\right)$ of length greater than $m-1$ and less than $2 m-1$ where $m$ is the number of vertices in $T\left(G_{A}, G_{B}\right)$.

It is clear that the graph $T\left(G_{A}, G_{B}\right)$ can be constructed from $M_{A}$ and $M_{B}$ in time $\mathrm{O}\left(\left|\delta_{A}\right| \cdot\left|\delta_{B}\right|\right)$, where $\left|\delta_{A}\right|\left(\left|\delta_{B}\right|\right)$ is the size of the table specifying the transition function of $M_{A}$ (resp., $M_{B}$ ). Breadth-first search can be used to determine whether $W(A, B)$ is infinite and this can be done in time $\mathrm{O}\left(\left|\delta_{A}\right|^{2} \cdot\left|\delta_{B}\right|^{2}\right)$. Hence, there is a polynomial time algorithm that on input $M_{A}$ and $M_{B}$ will determine whether $W(A, B)$ is infinite.

Notice that if $A$ is a base, $A^{*}$ is free, $B$ is a base, and $B^{*}$ is free, then a specification by means of a finite labelled directed graph is provided for the base of $A^{*} \cap B^{*}$ by pruning from $T\left(G_{A}, G_{B}\right)$ those vertices which do not lie on a path from ( $s_{A}, s_{B}$ ) to $\left(f_{A}, f_{B}\right)$.

## 3. Even's algorithm and circular codes

Even's original work [4,5] was to describe a graph-theoretic algorithm to determine whether a finite set $A \subset \Sigma^{*}$ is such that $A^{*}$ is free on $A$, that is, $A$ is a base and $A^{*}$ is free. This was presented in the context of $A$ being a variable length code so that $A$ is a base and $A^{*}$ is free if and only if that $A$ is a uniquely decipherable code. In the original work $A$ was taken as a finite set; here we describe the construction for the extension to the case of $A$ being a regular set such that $e \notin A$.

Let $M_{A}$ be a deterministic finite-state acceptor recognizing regular set $A$, and let $G_{A}$ and $C(A)\left(=\left(K_{A} \cup\left\{s_{A}\right\}, \Sigma, \delta^{A}, \lambda^{A}, s_{A}, s_{A}\right)\right.$ be the graphs described in Section 2. Construct the testing graph $T(A)$ of $A$ as follows:
(i) The set of vertices is $\left(K_{A} \cup\left\{s_{A}\right\}\right) \times\left(K_{A} \cup\left\{s_{A}\right\}\right) \cup\{I\}$, where $I$ is not in $\left(K_{A} \cup\left\{s_{A}\right\}\right) \times\left(K_{A} \cup\left\{s_{A}\right\}\right)$.
(ii) The set of edges is defined inductively as follows:
if $p, q \in K_{A} \cup\left\{s_{A}\right\}$ and for some $a \in \Sigma, a \in \lambda^{A}\left(s_{A}, p\right) \cap \lambda^{A}\left(s_{A}, q\right)$, then there is an edge from $I$ to $(p, q)$;
if $p, q, r, s \in K_{A} \cup\left\{s_{A}\right\}$, there is a path from $I$ to $(p, q)$, and for some $a \in \Sigma$, $a \in \lambda^{A}(p, r) \cap \lambda^{A}(q, s)$, then there is an edge from $(p, q)$ to $(r, s)$.

Then $A$ is a base and $A^{*}$ is free if and only if there is no $p \in K_{A}$ such that there exist a path in $T(A)$ from $I$ to $\left(p, s_{A}\right)$ and a path in $T(A)$ from $\left(p, s_{A}\right)$ to $\left(s_{A}, s_{A}\right)$.

By generating the pairs ( $p, s_{A}$ ), $p \neq s_{A}$, that are accessible from $I$ and then determining whether $\left(s_{A}, s_{A}\right)$ is accessible from such a pair, one can determine whether $A^{*}$ is free. We summarize in the following way.

Theorem 2. Consider the following problem:
INSTANCE: A deterministic finite-state acceptor with $n$ states recognizing a regular set $A$ such that $A$ is a base.

QUESTION: Is $A^{*}$ free?
There is an algorithm that will solve this problem in time at most $\mathrm{O}\left(n^{4}\right)$.
Now we consider an application of these techniques to the question of whether a uniquely decipherable code is circular.

A set $A \subset \Sigma^{*}$ is a circular code if $A$ is uniquely decipherable and for all choices of $x_{1}, \ldots, x_{n}, y_{1}, \ldots, y_{m} \in A$ and $u, v \in \Sigma^{*}, v \neq e$, if $v x_{2} \ldots x_{n} u=y_{1} \ldots y_{m}$ and $x_{1}=u v$, then $u=e$.

We will describe a polynomial-time algorithm that on input a deterministic finitestate acceptor $M_{A}$ recognizing regular set $A$ will determine whether $A$ is a circular code. From the last result we can assume that it is already known that $A$ is uniquely decipherable.

Let $C(A)=\left(K_{A} \cup\left\{s_{A}\right\}, \Sigma, \delta^{A}, \lambda^{A}, s_{A}, s_{A}\right)$ be the graph described in Section 2. For $p \in K_{A}$, let $C_{p}(A)$ be the graph $\left(K_{A} \cup\left\{s_{A}\right\}, \Sigma, \delta^{A}, \lambda^{A}, p, p\right)$. Let $T_{p}$ be the graph $T\left(C(A), C_{p}(A)\right)$ as described in Section 2.

Now $A$ is a circular code if and only if for every $p \in K_{A}$, there is no nonempty path from $\left(s_{A}, p\right)$ to ( $s_{A}, p \&$ in $T_{p}$.

This yields the following result.
Theorem 3. Consider the following problem:
INSTANCE: A deterministic finite-state acceptor with $n$ states recognizing a regular set $A$ such that $A$ is a base and $A^{*}$ is free.

QUESTION: Is A a circular code?
There is an algorithm that will solve this problem in time at most $\mathrm{O}\left(n^{5}\right)$.
The bound of $\mathrm{O}\left(n^{5}\right)$ results from the fact that $T_{p}$ has $n^{2}$ states so determining whether $T_{p}$ has no path from $\left(s_{A}, p\right)$ to $\left(s_{A}, p\right)$ requires time at most $\mathrm{O}\left(n^{4}\right)$. There are $n$ states and $T_{p}$ must be checked for each choice of $p$.

## Acknowledgment

I am happy to thank Dr. Craig Squier for some stimulating conversations on this topic. Dr. Friedrich Otto observed that the original 'proof' of Theorem 2 was not correct and provided the necessary alteration.

## References

[1] J. Avenhaus and K. Madlener, How to compute generators for the intersection of subgroups in free groups, CAAP '81, Lecture Notes in Computer Science 112 (1981) 88-100.
[2] J. Berstel and D. Perrin, Codes circulaires, in: L. Cummings, ed., Combinatorics on Words: Progress and Perspectives (Academic Press, New York, 1983) 133-165.
[3] R. Book, S. Even, S. Greibach, and G. Ott, Ambiguity in graphs and expressions, IEEE Trans. Computers 20 (1971) 149-153.
[4] S. Even, On Information Lossless Automata, Ph.D. dissertation, Harvard University, 1963.
[5] S. Even, On information lossless automata of finite order, IEEE Trans. Computers 14 (1965) 561-569.
[6] A. Howson, On the intersection of finitely generated free groups, J. London Math. Soc. 29 (1954) 428-434.


[^0]:    * This research was supported in part by the National Science Foundation under Grants MCS81-16327 and DCR83-14977.

