Quasi-identities of Finite Semigroups and Symbolic Dynamics

Stuart W. Margolis Mark V. Sapir*

September 17, 1993

1 Introduction

Let us first recall some basic facts and definitions from universal algebra (see [Malcev], [Cohn]). *A variety* is a class of universal algebras given by *identities*, i.e. formulas of the type

$$(\forall x_1, \ldots, x_n)\ u = v$$

where $u = u(x_1, \ldots, x_n)$ and $v = v(x_1, \ldots, x_n)$ are terms. For example, the class of all abelian groups is a variety of groups given by the identity $(\forall x, y)\ xy = yx$.

A quasi-variety is a class of universal algebras given by *quasi-identities*, i.e. formulas of the type

$$(\forall x_1, \ldots, x_n)\ u_1 = v_1 \& \ldots \& u_m = v_m \to u = v$$

where u_i, v_i, u, v are terms of variables $x_1, \ldots, x_n$ (see [Malcev] for details). For example, the class of all torsion free groups is a quasi-variety of groups given by the following infinite set of quasi-identities:

$$\{x^p = 1 \to x = 1 | p \text{ is a prime}\}.$$

*Research of both authors were supported in part by NSF and the Center for Communication and Information Sciences of the University of Nebraska at Lincoln.

Here and below we do not write quantifiers in the expressions of identities and quasi-identities.

By theorems of Birkhoff and Malcev one can also define a variety as a class closed under taking direct products, homomorphisms, and subalgebras, and one can define a quasi-variety as a class closed under taking direct products, subalgebras, and ultraproducts [Malcev]. Given any algebra A one can define the variety $varA$ (quasi-variety $qvarA$) generated by A as the minimal variety (quasi-variety) containing A. If A is finite then $qvarA$ consists just of all subalgebras of direct products of A [Malcev]. To obtain the variety $varA$, one has to take all homomorphic images of algebras from $qvarA$.

It is almost clear that if A is finite then both $varA$ and $qvarA$ are *locally finite*, i.e. all finitely generated algebras from these classes are finite. The converse statement is not true: Not every locally finite variety (quasi-variety) is generated by a finite algebra.

One of the main problems in the theory of varieties and quasi-varieties is the problem of describing all finite algebras A such that $varA$ (resp., $qvarA$) may be given by a finite number of identities (resp., quasi-identities). An algebra A with $varA$ given by a finite number of identities (quasi-identities) is called finitely based (finitely Q-based).

Every finite group is finitely based. This is the well known and difficult theorem of Oates and Powell [Neumann]. A finite group is finitely Q-based if and only if its Sylow subgroups are abelian. This is a theorem of Ol'shanskii [Olsh]. Thus in the case of groups complete information is known.

In the general case the situation is far more complicated. There is the McKenzie type reduction theorem which reduces the question of the description of finitely based finite algebras to the case of groupoids (algebras with one binary operation) [McKenzie]. In order to reduce the class of algebras which need to be investigated, Mursky [Mursky] and Perkins [Perk2] introduced the concept of an inherently non-finitely based algebras.

A finite universal algebra is called *inherently non-finitely based* if it cannot belong to any locally finite variety given by a finite number of identities.

The importance of this concept is straightforward. If an algebra A is inherently non-finitely based then every algebra B having A as a subalgebra or a homomorphic image is inherently non-finitely based also, and, in particular, is not finitely based. Indeed, as was mentioned above, $varB$ is locally finite, and contains A. Thus it is enough to find one inherently non-finitely based algebra to significantly reduce the class of algebras under investigation.

There is a remarkable theorem of McNulty and Shallon [McNSh] which shows that the associativity of the operation has much to do with the property being finitely based".

Theorem 1 *(McNulty and Shallon). Let A be a groupoid with identity and zero elements. Suppose that A does not satisfy any identity of the type $x = f(x)$ where f is a non-trivial term. Then A is either inherently non-finitely based or a semigroup.*

Then it turned out that there are plenty of inherently non-finitely based finite semigroups, and the second author described them all [Sap3], [Sap4]. To present one of his descriptions, we need the definition of the so called Zimin words. *Zimin words* are defined by induction:

$$Z_1 \equiv x_1, \ldots, Z_{n+1} = Z_n x_{n+1} Z_n.$$

Theorem 2 *(M.Sapir). A finite semigroup S is inherently non-finitely based iff S does not satisfy a non-trivial identitity of the type $Z_n = W$ where $n = |S|^2$ and W is any word different from Z_n.*

Using the fact that $varS$ is locally finite, it is easy to verify that Theorem 2 gives an effective description of all finite inherently non-finitely based semigroups.

These results (and many others which we can not mention here for obvious reasons) show that the investigation of finite finitely based algebras, though not complete is quite successful.

The concept of an inherently non-finitely Q-based finite algebra is similar to that of an inherently non-finitely based finite algebra, and was explicitly introduced by Pigozzi in 1988 [Pigozzi]:

A finite universal algebra is called *inherently non-finitely Q-based* if it cannot belong to any locally finite quasi-variety given by a finite number of quasi-identities.

But unlike the case of inherently non-finitely based algebras, there are no known examples of finite inherently non-finitely Q-based algebra. And it seems to be difficult to construct such an example. This is strange because one can present very many examples of finite algebras with a slightly weaker property:

A finite algebra A is called *basic*[Sap1] if every finite algebra B containing A is not finitely Q-based.

¿From the results of Ol'shanskii [Olsh], and Sapir [Sap1], it follows, that every finite group and even every finite semigroup without two-sided ideals is either basic or finitely Q-based. In particular, every finite non-abelian nilpotent group is basic. From the results of [Sap2], it follows that many other classes of semigroups also contain basic semigroups.

This makes the following theorem, which is the main result of this paper, very surprising.

Theorem 3 *Every finite semigroup belongs to a locally finite finitely based quasi-variety, i.e. there is no inherently non-finitely Q-based finite semigroup.*

The Pigozzi problem of whether there exists an inherently non-finitely Q-based finite algebra remains open. As was mentioned in [Pigozzi], this problem is closely connected with the following one: For every finite algebra A, is there a finitely based quasi-variety between $qvar A$ and $var A$ (see [Pigozzi], problem 9.11). It is clear that if this problem has a positive solution then there are no inherently non-finitely Q-based finite algebras. This problem came from logic, and can be reformulated in the following way: Can the set of tautologies of any finite matrix be deduced from finitely many tautologies by using finitely many inference rules (all necessary definitions and other interesting related problems may be found in [Rautenberg] and [Pigozzi]).

Now it's time to mention a connection between identities, quasi-identities and symbolic dynamics. First of all we can reformulate the definitions of inherently non-finitely based and inherently non-finitely Q-based algebras in order to show that the problem of showing that an algebra is inherently non-finitely (Q-)based is in fact a Burnside type problem about infinite algebras.

Lemma 1 *A finite algebra A is inherently non-finitely (Q-)based iff for every n there exists an infinite finitely generated algebra B_n such that all $n-$generated subalgebras of B_n belong to $(q)var A$.*

Proof. Let A be an inherently non-finitely (Q-)based algebra. Then the (quasi-)variety defined by all (quasi-)identities of A containing no more than n variables is finitely based (see [Malcev]). Hence this (quasi-)variety cannot be locally finite. Therefore it contains a finitely generated infinite algebra B_n every $n-$generated subalgebra of this algebra satisfies all (quasi-)identities of A, and so it belongs to $(q)varA$.

Conversely, suppose A is not inherently non-finitely (Q-)based, but such algebras B_n exist. Since A is not inherently non-finitely (Q-)based, there exists a finitely based locally finite (quasi-)variety $\mathcal{V}$ containing A. Let n be the number of variables in (quasi)-identities which define $\mathcal{V}$. Then all these (quasi-)identities hold in the algebra B_n. Therefore $B_n \in \mathcal{V}$. This contradicts the facts that $\mathcal{V}$ is locally finite and B_n is infinite and finitely generated.

By this lemma, in order to prove that a semigroup is not inherently non-finitely (Q-) based, we have to prove the finiteness of certain finitely generated semigroups. As was shown in [Sap3] (see the remark before lemma 9 below) there is a natural way to assign to each finitely generated semigroup S, a symbolic dynamics $\Omega(S)$, i.e. a closed subset of the (Tikhonov) product space $X^{\mathbf{Z}}$ which is stable under the shift homeomorphism (this homeomorphism shifts every sequence from $X^{\mathbf{Z}}$ one position to the right). This symbolic dynamics consists of all irreducible infinite (in both directions) words over the set of generators of S. Many important properties of $\Omega(S)$ reflect useful properties of S. In particular the fact that every symbolic dynamics contains a uniformly recurrent trajectory, plays an important role in the proof of finiteness of finitely generated semigroups (see [Sap3], [Sap5]).

Another important connection that we are going to present in this paper exists between quasi-identities of semigroups and identities of inverse semigroups. Recall that an inverse semigroup is a semigroup S such that for all x in S there is a unique y in S such that $x = xyx$ and $y = yxy$. It is known [Petr] that a semigroup is inverse if and only if it is isomorphic to a semigroup of partial bijections on a set X, that is closed under inversion of partial functions. Furthermore S is inverse if and only if for each x in S, there is an element y in S such that $x = xyx$ and $ef = fe$ for all idempotents e, f in S. It follows that (just as for groups), inverse semigroups can be considered as a semigroup with additional unary involutory operation $^{-1}$. Inverse semigroups are a variety defined by the following laws: $xx^{-1}x = x$, $xx^{-1}yy^{-1} = yy^{-1}xx^{-1}$ (see [CP], [Petr]). In particular the famous Perkins semigroup [Perk1], the maltiplicative semigroup of the following matrices $\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}$, is an inverse semigroup where $^{-1}$ is the operation of transposition. It was proved in [Sap3] that Perkins semigroup considered as a semigroup is inherently non-finitely based . Recently the second author [Sap5] proved that Perkins semigroup considered as an inverse semigroup is no longer inherently non-finitely based . Moreover, the main theorem of [Sap5] proves that there are no inherently non-finitely based finite inverse semigroup! It turned out that the main structural property of inverse semigroups that is used in the proof of this theorem is expressible by identities. In the case of arbitrary semigroups an analogous property is only definable by quasi-identities. This observation helped us to formulate and prove the main theorem of this paper.

2 Proof of Main Theorem

Let S be a semigroup. Recall that Green's relation $\mathcal{R}$ [CP] is defined by $s\mathcal{R}t$ iff $sS^1 = tS^1$. We define $s\mathcal{R}^*t$ if and only if $sT^1 = tT^1$ in some semigroup T containing S. The following "internal" characterization of the relation R^* is known [Pas]. We include the proof here for the sake of completeness.

Lemma 2 *Let S be a semigroup. Then $s\mathcal{R}^*t$ if and only if for all $x, y \in S^1$,*

$$xs = ys \Longleftrightarrow xt = yt.$$

Proof. Assume that $s\mathcal{R}^*t$. Then $sT^1 = tT^1$ in some semigroup T containing S. Thus there are elements $u, v \in T^1$ such that $su = t$ and $tv = s$. Let $x, y \in S^1$. Then $xs = ys$ implies that $xt = xsu = ysu = yt$. Similarly, $xt = yt$ implies that $xs = ys$.

Conversely, assume that $xs = ys \Longleftrightarrow xt = yt$. Consider the right regular representation $\rho : S \to F_R(S^1)$ from S into the monoid $F_R(S^1)$ of functions acting on the right of (the set) S^1. It is easy to check [CP] that for any set X, two functions $f, g \in F_R(X)$, satisfy $fF_R(X) = gF_R(X)$ if and only if $Ker(f) = Ker(g)$ where $Ker(f) = \{(x, y)|xf = yf\}$. Clearly the condition $xs = ys \Longleftrightarrow xt = yt$ is equivalent to the fact that $Ker(\rho(s)) = Ker(\rho(t))$ and thus (identifying S with $\rho(S)$) we have $s\mathcal{R}t$ in $F_R(S^1)$ so that $s\mathcal{R}^*t$.

It is easy to verify that $\mathcal{R}^*$ is a left congruence and that $\mathcal{R} \subseteq \mathcal{R}^*$ on any semigroup S. We will also be interested in the associated quasi-order $\leq_{R^*}$ on S defined by $s \leq_{R^*} t$ iff $s \leq_R t$ in some T containing S, that is $sT^1 \subseteq tT^1$.

Lemma 3 *Let S be a semigroup. Then $s \leq_{R^*} t$ if and only if*

$$xt = yt \Rightarrow xs = ys.$$

Proof. Similar to Lemma 2 using the fact that $f \leq_R g$ in $F_R(X)$ if and only if $Ker(g) \subseteq Ker(f)$.

Recall that an element x of a semigroup S is regular if there is a $y \in S$ such that $xyx = x$. It is known that x is regular iff there is an idempotent $e = e^2 \in S$, such that $e\mathcal{R}x$. In this case $ex = x$. S is a regular semigroup if every element of S is regular.

Lemma 4 *Let S be a semigroup and let $x, y \in S$. If x and y are regular and $x \leq_{\mathcal{R}^*} y$, then $x \leq_{\mathcal{R}} y$. In particular, if S is a regular semigroup, then $\leq_{\mathcal{R}^*}=\leq_{\mathcal{R}}$ and $\mathcal{R}^* = \mathcal{R}$.*

Proof. Suppose $x \leq_{\mathcal{R}^*} y$. Let $e = e^2\mathcal{R}x$ and $f = f^2\mathcal{R}y$ where $e, f \in S$. Let T be such that $x \leq_{\mathcal{R}} y$ in T. Then $x = yt$ for some $t \in T^1$. Let $s \in S$ be such that $xs = e$. Then $e = yts$ so that $e \leq_{\mathcal{R}^*} y$. Since $y\mathcal{R}f$, and $\mathcal{R} \subseteq \mathcal{R}^* \subseteq \leq_{\mathcal{R}^*}$ we have $e \leq_{\mathcal{R}^*} f$. Thus $e = ft'$ for some $t \in T^1$ and thus $e = fe$. Therefore $x = ex = fex = yzex$, where $yz = e, z \in S^1$. Therefore, $x = y(zex)$ and since $zex \in S^1$, we have $x \leq_{\mathcal{R}} y$.

Let $A = \{a_1, a_2, \ldots\}$ be a countable alphabet. Let $u, v \in A^+$, the free semigroup on A. We say that a semigroup S satisfies $u \leq_{\mathcal{R}^*} v$ ($u \leq_{\mathcal{R}} v$, $u\mathcal{R}^*v$, $u\mathcal{R}v$) iff for all homomorphisms $\phi : A^+ \to S$, $u\phi \leq_{\mathcal{R}^*} v\phi$ ($u\phi \leq_{\mathcal{R}} v\phi$, $u\phi\mathcal{R}^*v\phi$, $u\phi\mathcal{R}v\phi$).

Lemma 5 *Let S be a semigroup and let $u, v \in A^+$. Let x and y be variables in A, not occurring in either u or v. Then S satisfies $u \leq_{\mathcal{R}^*} v$ if and only if S satisfies the quasi-identity $xv = yv \Rightarrow xu = yu$.*

The proof of lemma 5 is clear given lemma 3.

Corollary 1 *Let $u, v \in A^+$. Then $Q(u, v) = \{S | S$ satisfies $u \leq_{\mathcal{R}^*} v\}$ is a quasi-variety of semigroups.*

Notice that in general, the class $\{S|S$ satisfies $u \leq_{\mathcal{R}} v\}$ is not a quasi-variety. For example, the group of integers $\mathbf{Z}$ satisfies $x \leq_{\mathcal{R}} y$, but the semigroup of natural numbers $\mathbf{N} < \mathbf{Z}$ does not satisfy this condition. We note however that for inverse semigroups in signature $< 2, 1 >$ we have a stronger result.

Lemma 6 *Let u and v be in the free inverse semigroup on A, $FIS(A)$. Then $V(u,v)$ =$\{S|S$ is an inverse semigroup satisfying $u \leq_{\mathcal{R}^*} v\} =$
$\{S|S$ is an inverse semigroup satisfying $u \leq_{\mathcal{R}} v\} =$
$\{S|S$ satisfies the identity $uu^{-1}vv^{-1} = uu^{-1}\}$.*

Proof. The first equality follows from lemma 4. The second equality follows from the known fact that $u \leq_{\mathcal{R}} v$ in an inverse semigroup iff $uu^{-1}vv^{-1} = uu^{-1}$.

Corollary 2 *$V(u,v)$ defined above is a variety of inverse semigroups.*

Thus the condition "S satisfies $u \leq_{\mathcal{R}^*} v$" can be defined by an identity in the variety of inverse semigroups, but only a quasi-identity in the variety of semigroups. This is the main difference between the main result of this paper and that of [Sap5].

We say that a semigroup is of finite height h, if the longest chain $s_1 \leq_{\mathcal{R}} s_2 \leq_{\mathcal{R}} \ldots \leq_{\mathcal{R}} s_k$ has length h. Recall the definitions of the Zimin words $Z_1 = x_1, Z_{n+1} = Z_n x_{n+1} Z_n$ where x_{n+1} is a new variable. We define Z'_n to be the prefix of Z_n consisting of all but the last letter. (It is easy to see that the last letter of Z_n is x_1). Thus if we let $Z'_1 = 1$, the empty word, we have $Z'_{n+1} = Z_n x_{n+1} Z'_n$ for all $n \geq 1$.

Lemma 7 *Every semigroup of finite height h satisfies $Z'_n \mathcal{R} Z_n$ with $n = h+1$.*

Proof. Since $Z_n = Z'_n x_1$, it is clear that every semigroup satisfies $Z_n \leq_{\mathcal{R}} Z'_n$. Now assume S has height h. Let $\phi : \{x_1, \ldots, x_n\}^+ \to S$. We must show that $Z_n\phi \mathcal{R} Z'_n\phi$ in S where $n = h+1$. First note that it suffices to prove that $Z_i\phi \mathcal{R} Z'_i\phi$ for some $i \leq n$. This is because an easy induction shows that if $i \leq n$, then $Z_n = Y_i Z_i$ and $Z'_n = Y_i Z'_i$ where $Y_i = Z_i x_{i+1} Z_i x_{i+2} \ldots Z_i x_n \ldots Z_i x_{i+1}$. Therefore $Z_i\phi \mathcal{R} Z'_i\phi \Rightarrow Z_n\phi = (Y_i Z_i)\phi \mathcal{R} (Y_i Z'_i)\phi \mathcal{R} Z'_n\phi$ since $\mathcal{R}$ is a left congruence.

Now $Z_2'\phi \geq_{\mathcal{R}} Z_2\phi \geq_{\mathcal{R}} Z_3'\phi \ldots \geq_{\mathcal{R}} Z_n'\phi \geq_{\mathcal{R}} Z_n\phi$ is an $\mathcal{R}$-chain in S. Since $n > h$, one of the inequalities $Z_i'\phi \geq_{\mathcal{R}} Z_i\phi$ cannot be strict and thus $Z_i'\phi \mathcal{R} Z_i\phi$ as desired.

Corollary 3 *Let S be a semigroup of height h. Let x, y be variables not among $\{x_1, \ldots, x_n\}$ where $n = h + 1$. Then S satisfies the implication*

$$xZ_n = yZ_n \Rightarrow xZ_n' = yZ_n'.$$

Proof. By Lemma 7 S satisfies $Z_n \mathcal{R} Z_n'$ so S satisfies $Z_n' \leq_{\mathcal{R}} Z_n$ and thus $Z_n' \leq_{\mathcal{R}^*} Z_n$. The result follows from lemma 5.

Remarks. 1) Of course, the condition $Z_n \mathcal{R} Z_n'$ is stronger than $Z_n' \leq_{\mathcal{R}^*} Z_n$, but only this last condition can be defined by quasi-identities.

2) Let $Q_n = \{S | S \text{ satisfies } xZ_n = yZ_n \Rightarrow xZ_n' = yZ_n'\}$. Then Q_n is a quasi-variety. Notice that $Q_1 = \{S | S \text{ is right cancellative}\}$ so more generally Q_n consists of semigroups in which every element x_1 cancels in the context of left factors of the form (xZ_n', yZ_n').

It is known and easy to prove that a right cancellative semigroup S (i.e. a member of Q_1) is locally finite if and only if S is periodic and all subgroups of S are locally finite. The following non-trivial Lemma is an extension of this result to Q_n and is a key to the proof of the Main Theorem.

Lemma 8 *Let $n \geq 1$ and let $S \in Q_n$. Then S is locally finite if and only if S is periodic and all subgroups of S are locally finite.*

Proof. Clearly if S is locally finite, then S is periodic and all subgroups of S are locally finite. Assume then that S is a periodic semigroup in Q_n and that all subgroups of S are locally finite.

In the proof of this lemma we will crucially use so called *uniformly recurrent* words. Let us recall some definitions and results.

Let X be a finite alphabet, $X^{\mathbf{Z}}$ be the set of all sequences infinite in both directions. We simply refer to these as *infinite words*. An infinite word W is called *uniformly recurrent* if for every set of (finite) subwords $w_1, \ldots w_k$ of W there exists a number N such that every subword of W length N contains all $w_i, i = 1, \ldots, k$. It is an easy corollary from [Fur] (see [Sap3] for details) that for every infinite word W there exists a uniformly recurrent word W' such that every subword of W' is a subword of W.

The following argument first appeared in [Sap3] makes uniformly recurrent words a very useful tool in dealing with Burnside type problems.

Let $S =< X >$ be an infinite finitely generated semigroup (the same argument may be applied for any universal algebra). Then there is an infinite set T of words over X such that every element of S represented by a word of T cannot be represented by words over X of less length. Such words will be called *irreducible*. It is clear that every subword of an irreducible words is also irreducible. Now, in every word of T, mark a letter which is closest to the center of these word. There must be an infinite subset T_1 of T which have the same marked letters, an infinite subset T_2 of T_1 of words which have the same subwords of length 2 containing the marked letters, $\ldots$, an infinite subset T_n of T_{n-1} of words which have the same subwords of length n containing the marked letters, and so on. Therefore there is an infinite word W such that every subword of W is a subword of a word from T. Thus every subword of W is irreducible. Infinite words with this property will be called *irreducible* too. As was mentioned above there exists an uniformly recurrent irreducible word W'. Therefore we have proved the following result (see [Sap3]).

Lemma 9 *For every infinite finitely generated semigroup $S =< X >$ there exists a uniformly recurrent irreducible word over X.*

The proof of the following lemma is (a small) part of the proof of proposition 2.1 in [Sap3].

Lemma 10 *Let U be a uniformly recurrent word, U_1aU_2 be an occurrence of letter a in U where U_1 is a word infinite to the left, U_2 is a word infinite to the right. Then for every natural number n there exists an endomorphism ϕ of the free semigroup such that $U_3\phi_n(Z_n) = U_1a$ for some word U_3 infinite to the left, $\phi_n(x_1) = a$, and $|\phi_n(Z_n)| \leq A(n, U)$ where the number $A(n, U)$ depends only on U and n.*

Proof. For $n = 1$ the statement is trivial. Suppose that we have found $A(n, U)$ and ϕ_n. Let N be big enough that every subword of U of length N contains any subword of U length $A(n, U)$. Then we can represent $U_3\phi_n(Z_n)$ as $U_4\phi_n(Z_n)v\phi_n(Z_n)$ for some word U_4, infinite to the left, and finite nonempty word v, $|v| \leq N$. Let $\phi_{n+1}(x_i) = \phi_n(x_i)$ for $i \leq n$ and $\phi_{n+1}(x_{n+1}) = v$. Then $U_1a = U_4\phi_{n+1}(Z_{n+1}) = U_4\phi_n(Z_n)v\phi_n(Z_n)$ and $\phi_{n+1}(x_1) = a$. Therefore we can let $A(n+1, U) = N + 2A(n, U)$. The lemma is proved.

Lemma 11 *Let U be a uniformly recurrent word. Let u and v be consecutive subwords of U with $|u| \geq A(n, U)$. Then Q_n satisfies $uv\mathcal{R}^*u$ that is Q_n satisfies the quasi-identity $xuv = yuv \Rightarrow xu = yu$.*

Proof. Let p be the longest prefix of v such that the implication $xup = yup \Rightarrow xu = yu$ follows from the defining implication of Q_n. If $p = v$ we are done. Otherwise $v = paq$ for some $a \in A$, $q \in A^*$. Since upa is a subword of U and $|upa| \geq A(n, U)$, we can write $upa = u_1\phi(Z_n)$ for some homomorphism $\phi : \{x_1, \ldots, x_n\}^+ \to A^+$ where $\phi(x_1) = a$, by Lemma 10. It follows that $up = u_1\phi(Z'_n)$. Therefore, $xupa = yupa \Rightarrow xu_1\phi(Z_n) = yu_1\phi(Z_n) \Rightarrow$ (by definition of Q_n) $xu_1\phi(Z'_n) = yu_1\phi(Z'_n) \Rightarrow xup = yup \Rightarrow xu = yu$. This contradicts the choice of p and the Lemma is proved.

We can now complete the proof of Lemma 7. Suppose that there exists a periodic infinite finitely generated semigroup $S =< A >$ which belongs to Q_n. Then, by lemma 9, there exists a uniformly recurrent irreducible word U over A.

Let u be a subword of U of length $A(n, U)$. Since U is uniformly recurrent we can write U in the form $U = \ldots uv_1uv_2uv_3 \ldots$ where for all i $|uv_i| \leq B$ for some constant B. By lemma 11, S satisfies $u\mathcal{R}^*uv_iu$ for all i. Therefore, $u = uv_iut_i$ for some $t_i \in T_i$ and some semigroup T_i containing S. It follows that $u = (uv_i)^n ut_i^n$ for all $n > 0$. Since $uv_i \in S$ and S is periodic, $e_i = (uv_i)^n$ is an idempotent for some $n > 0$. It follows that $u = e_iu$. That is $u = (uv_i)^n u$ so that $(uv_i)^{n+1} = uv_i$. It follows that uv_i is in a subgroup of S and that $uv_i\mathcal{R}u$ in S.

We now have for any $i, j \in \mathbf{Z}$ the idempotents e_i and e_j generate the same principal right ideal. It is easy to check that this is equivalent to the fact that $e_ie_j = e_j$ and $e_je_i = e_i$. Let G_i be the maximal subgroup of S whose idempotent is e_i. It follows easily that right multiplication by e_i induces an isomorphism from G_j to G_i. Thus for all integers i and all $k \geq 0$, all products $(uv_{i-k}) \ldots (uv_i)$ are in the same subgroup G_i of S. Each such product can be rewritten as: $[(uv_{i-k})e_i] \ldots [(uv_{i-1})e_i](uv_i)$ where $e = (uv_i)^n = e^2$ is the identity element of G_i. All products above are in the subgroup H_i of G_i generated by $X_i = \{(uv_i), (uv_{i-j})(uv_i)^n | j \geq 0\}$. But each element of X_i has length bounded by $(n + 1)B$ and so X_i is finite. Therefore H_i is finite and it follows that there are $j \neq k$ such that $(uv_{i-j}) \ldots (uv_i) = (uv_{i-k}) \ldots (uv_i)$. This contradicts the fact that U is irreducible and completes the proof.

We have the following interesting corollary of the above proof.

Lemma 12 *Let $\phi : X^+ \to S$ be a surjective homomorphism and let S be periodic and in Q_n. Let U be a uniformly recurrent word over X. Then there is a natural number B such that if u and v are subwords of U of length $\geq B$, then $u\phi$ and $v\phi$ generate the same two sided ideal. Furthermore, if u is a subword of U of length $\geq B$, then $u\phi$ is regular.*

Proof. First note that since U is uniformly recurrent , U contains only a finite number of letters. Let $A(n, U)$ and B be the constants constructed in the above proof. We have seen that if u is a subword of U, $|u| \geq B$, then $u\phi$ is a regular element of S. Let v be any subword of U. Since U is uniformly recurrent , $uxvyu$ is a subword of U for some $x, y \in X^+$. The proof above implies that $uxvy\mathcal{R}u$ in S, that is $(uxvyz)\phi = u\phi$ for some word $z \in X^+$. Therefore $u\phi$ is in the two sided ideal generated by $v\phi$. We have shown that an arbitrary subword of U of length $\geq B$ is in the two sided ideal generated by any subword of U. Therefore any two subwords of U of length $\geq B$ generate the same two sided ideal.

In the language of the Green relations [CP], the above corollary shows that long enough subwords of a uniformly recurrent word are *J-equivalent* when mapped into a member of Q_n. This corollary can be thought of as a proof that members of Q_n satisfy a "uniform descending chain condition". That is, uniformly recurrent words only represent elements from a finite number of distinct principal two sided ideals. See [Sap5] for an example of a semigroup in Q_3 that does not satisfy the descending chain condition on principal two sided ideals.

We now complete the proof of the Main Theorem. Let S be a finite semigroup of height h, and let $qvar(S)$ be the quasi-variety generated by S. Then $S \in Q_n$ for any $n > h$. It is easy to see that the intersection of $qvar(S)$ and the class of all groups is the quasi-variety generated by all subgroups of S, or equivalently, the quasi-variety generated by G the direct product of all subgroups of S. This quasi-variety is contained in $var(G)$, the variety generated by G. Now $var(G)$ is defined by one identity $v(x_1, \ldots, x_m) = 1$ by the theorem of Oates-Powell. We may suppose that $m > h$. Let $F = F_m(qvar(S))$ be the free object in the quasi-variety generated by S on m generators. It is well known that F is a finite semigroup so has a minimal idempotent e. Let u be a word that represents e in F. Then S satisfies the identity:

$$u = u^2. \tag{1}$$

For every element x of F, exe belongs to the maximal subgroup of F that has e as identity element. Therefore, S satisfies the identity

$$v(ux_1u, \ldots, ux_nu) = u \tag{2}$$

Also S satisfies $x^p = x^{p+q}$ for some $p \geq 0$, $q > 0$.

We have seen that S is in the quasi-variety Q defined by the implication $xZ_n = yZ_n \Rightarrow xZ'_n = yZ'_n$, identity $x^p = x^{p+q}$, and identities (1), (2). Now any group H satisfying (1) and (2) satisfies $v = 1$. Thus $H \in var(G)$ and therefore H is locally finite. Therefore Q is locally finite by Lemma 8 and we are done.

References

[CP] A.Clifford and G.Preston, *Algebraic Theory of Semigroups*, Vol. 1 (1961), Vol. 2 (1967), American Math. Society, Providence, R.I.

[Cohn] P.M.Cohn, *Universal algebra*, Harper and Row, New York, 1965.

[Fur] H.Furstenberg, *Poincaré recurrence and number theory*, Bull. Amer. Math. Soc. 5 (1981), 211-234.

[Malcev] A.I.Mal'cev, *Algebraic systems*, Grundlehren der mathematischen Wissenschaften, Vol. 192, 1973, Springer-Verlag, New York.

[McKenzie] R.McKenzie, *A new product of algebras and a type reduction theorem*, Alg. Univ., 18 (1984), # 1, 29-69.

[McNSh] G.McNulty, C.Shallon, *Inherently nonfinitely based finite algebras*, Lect. Notes Math., 1983, 1004, 206-231.

[Mursky] V.L.Mursky, *On the number of k-element algebras with one binary operation without finite bases of identities*, Probl. Kibernetiki, 35 (1979), # 1, 5-27.

[Neumann] H.Neumann, *Varieties of groups*, Springer Verlag, New York, 1967.

[Olsh] A.Yu.Ol'shanskii, *Conditional identities of finite groups*, Sib. Matem. J., 15 (1974), # 6, 1409-1413 (Russian, English translation see in Sib. Matem. J., 1975, 1000-1003).

[Pas] F.Pastijn, *A representation of a semigroup by a semigroup of matrices over a group with zero*, Semigroup Forum, 10 (1975), 238-249.

[Perk1] P.Perkins, *Bases for equational theories of semigroups*, J. Algebra, 11 (1969), # 2, 293-314.

[Perk2] P.Perkins, *Basic questions for general algebras*, Algebra Universalis, 19 (1984), 16-23.

[Petr] M. Petrich, *Inverse semigroups*, Wiley, New York, 1984.

[Pigozzi] D.Pigozzi, *Finite basis theorem for relatively congruence-distributive quasi-varieties*, Trans. AMS, 310 (1988), # 2, 499- 533.

[Rautenberg] W.Rautenberg, *2-Element Matrices*, Studia Logica, 40 (1981), # 4, 315-353.

[Sap1] M.V.Sapir, *On the quasivarieties generated by finite semigroups*, Semigroup Forum 20 (1980), 73-88.

[Sap2] M.V.Sapir, *Quasivarieties of semigroups*, PhD thesis, Moscow Ped. In-t, 1983, 1-140 (Russian).

[Sap3] M.V. Sapir, *Burnside-type problems and finitely based semigroup varieties,* Izv. AN SSSR, Ser. Mat., 2, 51 (1987), 319-340.

[Sap4] M.V.Sapir, *Inherently non-finitely based finite semigroups*, Matem. Sbornik, 133, 2 (1987), 154-166.

[Sap5] M.V.Sapir, *Identities of finite inverse semigroups*, to appear, Int. J. Alg. and Comp.

[Zimin] A.I.Zimin, *Blocking sets of terms*, Matem. Sbornik, 119, 3 (1982), 363-375.

Mark V. Sapir
Department of Mathematics and Statistics,
Center for Communication and Information Sciences,
University of Nebraska-Lincoln
Lincoln, NE 68588
email: msapir@hoss.unl.edu