Congruences in Commutative Semigroups

Joram Hirshfeld*

December 6, 1993

Abstract

A simple elementary proof is given that every congruence on a finitely generated commutative semigroup is finitely generated and is moreover a semilinear relation.

It was proved in [5] (see also [1]) that every congruence on a finitely generated commutative semigroup is finitely generated. Freyd in [3] shortened the lengthy proof to half a page by an elegant use of Hilbert's Basis Theorem. His proof does not reveal much on the generators of the congruences and does not lend itself easily to further analysis. Recently Jančar returned to [5] and [1] and modified the proof to show that every congruence on N^k is a semilinear relation [4]. Here we shall give these theorems new simple and elementary proofs that give some insight into the structure of the congruences. In particular we show that every congruence R is generated by the pairs which are minimal in R under the natural partial order (theorem 1) and that the set of pairs which are minimal in a weaker sense generate R as a semiliner set (theorem 2)[1].

We do the analysis in N^k, the set of vectors of length k of natural numbers with vector addition (every finitely generated commutative semigroup is a homomorphic image of such an algebra). A relation R on N^k is a *Congruence* if it is an equivalence relation and whenever $(v, w) \in R$ then $(v + u, w + u) \in R$. Every congruence is closed under substitutions; i.e, if $(v, v_1) \in R$ then $(v + u, w) \in R$ iff $(v_1 + u, w) \in R$. N^k is naturally (partially) ordered by $v \leq w$ iff $v + u = w$ for some u. We shall freely identify $N^k \times N^k$ with N^{2k} so that this defined also a partial order on pairs of vectors.

The following finiteness principle [2] goes back (at least) to 1913 and was often rediscovered since:

Lemma

Every infinite set of vectors contains an infinite increasing sequence.
In particular every set of mutually incomparable vectors is finite.

---

*Currently at LFCS, Edinburgh University, Permanently at Tel Aviv University

[1] These results were obtained while the author and others researchers (S.Christensen, P. Jančar and F. Moller) were studying the structure of the bisimulation congruence for some process algebras. It was recently brought to our attention that similar results were obtained by Eilenberg and Schützenberger in [6]. We feel however that the directness of our proof and the concrete description of the generators of the congruences justify the existence of this report.

Proof
If the first coordinate is bounded pick a subsequence with a constant entry in the first place else pick a subsequence with an increasing entry in the first place. Repeat this move with all the coordinates.

The notions that we discuss are:

(a) The congruence R is *generated* by the set S of pairs if R is the smallest congruence that contains S.

(b) A *Linear set* in N^k is a set of the form

$$v + span\{w_1, \cdots w_l\} = \{v + n_1 w_1 + \cdots + n_l w_l \mid n_1 \cdots n_l \in N\}$$

(c) A *Semilinear set* is a finite union of linear sets.

Definition
Let R be a congruence. A pair $(v, w) \in R$ with $v \neq w$ is *minimal* in R if only pairs of the form (u, u) are smaller than (v, w) in R. Also the pairs (ϵ_i, ϵ_i) where ϵ_i is the vector with 1 in the i-th place and zeros elsewhere,will be called minimal.

By the lemma (applied to N^{2k}) every congruence has only finitely many minimal pairs.

Theorem 1
Every congruence is generated by the set of its minimal pairs.

Proof
We order N^k by another order: $v <_1 v'$ if $v_i < v'_i$ for the first coordinate i where they differ. For pairs we define $(v, w) <_1 (v', w')$ if $v_i + w_i < v'_i + w'_i$ for the first coordinate i where the sums differ. These orders refine the natural partial order and they are well founded: every non empty set has a minimal member and there are no infinite decreasing sequences. Let R be the congruence and S the set of minimal pairs in R and assume for contradiction that $(v_1, w_1) \in R$ is a $<_1$-minimal counterexample not generated by S. Since (v_1, w_1) is not in S there is a pair $(v, w) \in S$ such that $v \neq w$ and $(v, w) \leq (v_1, w_1)$. Without loss of generality assume that $v <_1 w$. There is some u such that $(v_1, w_1) = (v_1, w + u)$. Substituting v for w we conclude that $(v_1, v + u) \in R$. But $(v_1, v + u) <_1 (v_1, w + u)$ so that by the minimality of the counterexample we conclude that $(v_1, v + u)$ is generated by S. But then also $(v_1, w + u)$ is generated by S. Contradiction.

Next we define for each $(v, w) \in R$ the following congruence:

$$S_{(v,w)} = \{\ (s, t) \mid (v + s, w + t) \in R\ \}$$

All the linear sets that we shall consider are of the form

$$L_{(v,w)} \ = \ (v, w) + span\{(s_1, t_1), \cdots (s_l, t_l)\ \}$$

Where $(v, w) \in R$ and $(s_1, t_1), \cdots (s_l, t_l)$ are the minimal pairs in $S_{(v,w)}$.

Claim 1:
(i) $L_{(v,w)} \subseteq R$
(ii) If also $(v', w') \in R$ and $(v, w) \leq (v', w')$, and if $S_{(v,w)} = S_{(v',w')}$ then $(v', w') \in L_{(v,w)}$.

Proof:
(i) is easy. For (ii) assume that (v', w') is a minimal counterexample. It follows that $(v+s, w+t) < (v', w')$ for some (s,t) which is minimal in $S_{(v,w)}$. Thus $(v', w') = (v+s+s', w+t+t')$ for some (s', t'). Since $S_{(v,w)} = S_{(v',w')}$ and $(v,w) \leq (v+s, w+t) \leq (v', w')$ we have $S_{(v+s,w+t)} = S_{(v,w)}$ so that (s', t') is also in $S_{(v,w)}$. Hence $(v+s', w+t') \in R$. For a similar reason also $S_{(v+s',w+t')} = S_{(v,w)}$ and as (v', w') was a minimal counterexample we may conclude that the smaller pair $(v+s', w+t')$ is in $L_{(v,w)}$. But then also $(v+s', w+t') + (s,t) \in L_{(v,w)}$. Contradiction.

Definition

A pair (v,w) in a congruence R is *Weakly Minimal* if there is no smaller pair (v', w') in R that satisfies $S_{(v,w)} = S_{(v',w')}$

Claim 2:
The set H of weakly minimal pairs in R is finite.

Proof:
Else by the lemma H includes an infinite increasing sequence (v_i, w_i). For every i we have $S_{(v_i,w_i)} \subseteq S_{(v_{i+1},w_{i+1})}$, and by theorem 1 the inclusion becomes equality from some i on, contradicting the weak minimality of (v_{i+1}, w_{i+1}).

Theorem 2
Every congruence R is semilinear. Specifically: If H is the set of weakly minimal pairs in R then

$$R \;=\; \bigcup\{\; L_{(v,w)} \mid (v,w) \in H \;\}$$

Proof:
One direction is claim 1(i). The other direction follows from claim 1(ii): If $(v,w) \in R$ then $(v,w) \in L_{(\bar{v},\bar{w})}$ where $(\bar{v},\bar{w})$ is a weakly minimal pair smaller or equal to (v,w) for which $S_{(v,w)} = S_{(\bar{v},\bar{w})}$.

References

[1] A.H. Clifford and G.B. Preston. The algebraic theory of semigroups. Volume 2. The American Mathematical Society (1967).

[2] L.E. Dickson. Finiteness of the odd perfect and primitive abundant numbers with distinct factors. American Journal of Math. 35 (1913), 413-422.

[3] P. Freyd. Redei's finiteness theorem for commutative Semigroups. Proc. of the AMS 19 (1968), page 1003.

[4] P. Jančar. Decidability questions for bisimilarity of Petri Nets and some related problems. LFCS Report Series ECS-LFCS-93-261. Department of computer science, Edinburgh University, April 1993.

[5] L. Redei. The theory of finitely generated commutative semigroups. Oxford University Press, NY (1965).

[6] S. Eilenberg and M.P. Schützenberger. Rational sets in Commutative Monoids. Journal of Algebra 13, 173-191(1969).