Synchronizing groups and semigroups

York Semigroups Seminar: Wednesday 14 December 2011

Peter M. Neumann: The Queen's College, Oxford

- **Introduction**
- **Synchronizing semigroups and groups**
- **Separating groups**
- **Graphs and their endomorphism semigroups**
- **Spreading and representation theory**
- **Some open questions; some references**

Introduction

Theme. A question asked by **Dr João Araújo** (Lisbon), [e-mail 19 October 2006], and developments.

Notation

- X: a finite set; $n := |X|$, we assume $n \geqslant 3$;
- $T(X)$:= monoid of all maps $X \to X$;
- for $t \in T(X)$, rank(t) := $|$Image$(t)|$;
- G is always a subgroup of Sym(X), contained in $T(X)$.

Recall (or accept): G is **transitive** if $(\forall x, y \in X)(\exists g \in G) : x^g = y$. Transitive group is **primitive** if there is no non-trivial proper G-invariant partition of X.

Synchronizing semigroups

Monoid $M \leqslant T(X)$ is said to be **synchronizing** if there exists $t^* \in M$ with $\text{rank}(t^*) = 1$ (so t^* is a constant map).

In fact interest is in subsets $T_0 \subseteq T(X)$ with $M = \langle T_0 \rangle$.

Ask for $w = t_1 t_2 \cdots t_k \in M$ (all $t_i \in T_0$) such that $\text{rank}(w) = 1$. Known as a **reset word.**

Comes from automata theory: X = set of states, T_0 = set of transition maps.

Černý Conjecture: for a synchronizing automaton with n states there is always a reset word of length $k \leqslant (n-1)^2$.

Synchronizing groups, section-regular partitions

Araújo, Steinberg: Non-trivial group G is **synchronizing** if $\langle G, t \rangle$ is a synchronizing semigroup for each $t \in T(X) \setminus \mathrm{Sym}(X)$.

A partition (equivalence relation) ρ of X is **section-regular** if there exists $S \subseteq X$ such that S^g is a section of ρ for all $g \in G$.

Equivalently: S is section of ρ^g for all $g \in G$;

equivalently: S^g is section of ρ^h for all $g, h \in G$.

Theorem [Araújo]. Non-trivial group G is synchronizing if and only if there is **no** non-trivial proper section-regular partition for G.

First steps

Examples. Sym(X), Alt(X) are synchronizing.
Generally, any 2-homogeneous group (transitive on unordered pairs) is synchronizing.

Examples. If G is not transitive then G is not synchronizing.

If G is transitive but not primitive then G is not synchronizing.

Corollary. A synchronizing group is primitive.

Question [Araújo]. Does the converse hold?

Examples.

Example. Sym(m) Wr Sym(k) in product action, degree m^k, is primitive if $m \geqslant 3$ and non-synchronizing if $k \geqslant 2$.

Example. Sym(m) acting on pairs, degree $\frac{1}{2}m(m-1)$, is primitive if $m \geqslant 5$ and is non-synchronizing when m is even.

Example. Many affine groups are primitive non-synchronizing—the smallest is ${C_3}^2.C_4$ (alias $\frac{1}{2}$AGL$(1,9)$).

Note. O'Nan–Scott taxonomy of primitive groups provides guidance.

A basic theorem

Theorem (ΠMN). Suppose G is transitive. A section-regular partition is uniform (all classes have same size).

Then define the parameters of a section-regular partition to be (n, r, s) where it has s parts each of size r, so $r\,s = n$.

Fact. If G is primitive then the parameters of a non-trivial proper section-regular partition satisfy $r > 2$, $s > 2$.

Problem. What primitive groups G can have non-trivial proper section-regular partitions with small r or small s? (E.g. $3 \leqslant \text{small} \leqslant 6$.)

A contextual theorem: density, I

For this lecture only: define integer n to be **primitive** if there exists $G \leqslant \mathrm{Sym}(n)$, $G \neq \mathrm{Sym}(n)$, $\mathrm{Alt}(n)$, G primitive.

Examples: if n is an odd prime, or if $n = p + 1$ where p is prime, or if $n = \frac{1}{2}m(m-1)$ or $n = m^2$ (with $m \geqslant 3$), then n is primitive.

Fact (mod CFSG) [Cameron, Neumann & Teague, 1982]. Define

$$e(x) := \#\{n \leqslant x \mid n \text{ is primitive}\}$$

Then

$$e(x) = 2\pi(x) + (1 + \sqrt{2})\sqrt{x} + O(\sqrt{x}/\log x),$$

where $\pi(x)$ is the prime number enumerator.

In particular, $e(x) \sim 2\,x/\log x$ as $x \to \infty$.

A contextual theorem: density, II

Theorem (mod CFSG) [ΠMN]. Define $e_0(x)$ similarly to measure the density of the set of degrees of primitive non-synchronizing groups. Then

$$e_0(x) = (1 + 1/\sqrt{2})\sqrt{x} + O(\sqrt{x}/\log x)\,.$$

Separation

Theorem [ΠMN et al. 1974]. Suppose G is transitive. Let R, S be subsets of X. Let $r := |R|$, $s := |S|$.

(1) if $rs < n$ then $\exists g \in G : R \cap S^g = \emptyset$;

(2) if $n = rs$ and $\forall g \in G : R \cap S^g \neq \emptyset$ then $\forall g \in G : |R \cap S^g| = 1$;

(3) if $\forall g \in G : |R \cap S^g| = 1$ then $n = rs$.

Call G **separating** if for all $R, S \subseteq X$ with $|R| > 1$, $|S| > 1$, and $n = |R| \times |S|$ there exists $g \in G$ such that $R \cap S^g = \emptyset$.

Separating groups and synchronization

Observation: a separating group is synchronizing.

Question [ΠMN, January 2008]: do there exist transitive G which are synchronizing but not separating?

Answer [Cameron, Schneider, Spiga]: Yes. Infinitely many. But not easy to come by.

Graphs, I

Graphs are to be undirected, no multiple edges, no loops. Clique number k is size of largest clique; independence number $\overline{k}$ is size of largest co-clique; chromatic number χ.

Observation [Cameron]. (1) Group G is non-synchronizing if and only if there is a G-invariant graph on X with $k \times \chi = n$;

(2) Group G is non-separating if and only if there is a G-invariant graph on X with $k \times \overline{k} = n$.

Graphs, II

For a graph Γ define its core as image of an endomorphism of minimal rank. Then core(Γ) is a minimal retract of Γ; it is unique up to isomorphism.

Proposition [Cameron]. Let $M \leqslant T(X)$, $M \nleqslant \mathrm{Sym}(X)$. Then M is not synchronizing if and only if there exists a non-trivial graph Γ with vertex set X such that core(Γ) is complete and $M \leqslant \mathrm{End}(\Gamma)$.

Cameron + Kazanidis, 2008: major progress towards classification of primitive rank-3 groups as synchronizing or not. But hard problems in finite geometry remain.
[Rank-3 means group is transitive both on edges and on non-edges of a graph.]

Spreading groups and QI-groups

Definition [Steinberg]. group G is **spreading** if for every non-empty proper subset S of X and every $t \in T(X) \setminus \mathsf{Sym}(X)$ there is $g \in G$ such that $|Sgt^{-1}| > |S|$.

Observation [Steinberg]. Černý Conjecture is easy to prove for $T \cup \{t\}$ if $T \subseteq \mathsf{Sym}(X)$ and $\langle T \rangle$ is a spreading group.

Definition. Group G is a **QI**-group if $\mathbb{Q}X = \mathbf{1} \oplus \mathbf{irreducible}$.

Theorem [Arnold + Steinberg, 2006]. QI $\Rightarrow$ spreading $\Rightarrow$ synchronizing.

A role for representation theory

Facts. 2-homogeneous $\Rightarrow$ QI
$\Rightarrow$ spreading
$\Rightarrow$ separating
$\Rightarrow$ synchronizing
$\Rightarrow$ primitive.

Big Question. Is it true that spreading $\Rightarrow$ QI ?

Compare: G is 2-transitive $\Leftrightarrow$ G is CI ;
G is 2-homogeneous $\Leftrightarrow$ G is RI .

Notes. The QI groups are classified [Saxl].
Other implications than 2nd are known not to be reversible [ΠMN, Cameron, Schneider, Spiga].

Conclusion

There is much to be done: **for example**

Question. Can one classify the primitive non-synchronizing groups?

- **e.g.** If G is of affine type G-regular partitions need not be affine;
- **e.g.** What are those of affine type over $\mathbb{F}_2$?
  For example, is 2^{101}He synchronizing?
- **e.g.** Can we classify those with rank 3 (rank 4, rank 5, etc.)?
  [Rank = number of orbits on ordered pairs.]

Question. Is every spreading group a QI-group—that is, is the G-module $\mathbb{Q}X$ almost irreducible?

Question. What does all this say for the original problems about semigroups and automata?

References

Fredrick Arnold and Benjamin Steinberg, ‘Synchronizing groups and automata’, *Theoretical Comp. Sci.*, 359 (2006), 101–110.

Peter J. Cameron and Priscila A. Kazanidis, ‘Cores of symmetric graphs’, *J. Austral. Math. Soc.*, 85 (2008), 145–154.

Peter M. Neumann, ‘Primitive permutation groups and their section-regular partitions’, *Michigan Math. J.*, 58 (2009), 309–322.

The Synchronization Co-op: João Araújo [Lisbon], Peter Cameron [London], Peter Neumann [Oxford], Csaba Schneider [Lisbon], Pablo Spiga [Padua], Benjamin Steinberg [Ottawa], and others, Various unpublished drafts, 2008–09.