Low-dimensional Affine Synchronizing Groups

Ana Filipa Costa da Silva

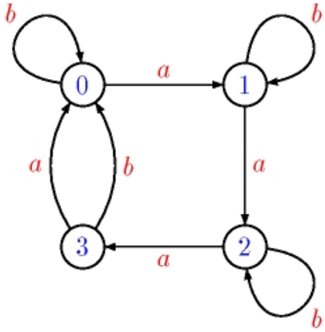
Master's Thesis Defense

Faculdade de Ciências
Departamento de Matemática

November 21, 2012

What is Synchronization?

$w = ba^3ba^3b$ is a synchronizing word for the automaton at the right.

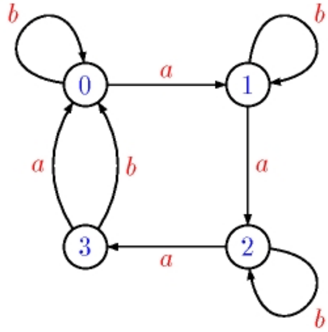


Cerny Conjecture (1964)

A synchronizing automaton with n states admits a synchronizing word of length at most $(n-1)^2$.

What is Synchronization?

$w = ba^3ba^3b$ is a synchronizing word for the automaton at the right.



Cerny Conjecture (1964)

A synchronizing automaton with n states admits a synchronizing word of length at most $(n-1)^2$.

Synchronizing Permutation Groups

Let $G \leq \mathrm{Sym}(\Omega)$ be a non-trivial group.

Definition (Ben Steinberg)

G is synchronizing if $\langle G, t \rangle$ contains a constant map for all $t \in T(\Omega) \backslash \mathrm{Sym}(\Omega)$.

Definition (João Araújo - CAUL)

G is synchronizing if there is no non-trivial partition $\mathcal{P}$ and subset S of Ω such that

$$Sg \text{ is a section of } \mathcal{P}, \quad \forall g \in G.$$

Such a partition is said to be section-regular.

Synchronizing Permutation Groups

Let $G \leq \mathrm{Sym}(\Omega)$ be a non-trivial group.

Definition (Ben Steinberg)

G is synchronizing if $\langle G, t \rangle$ contains a constant map for all $t \in T(\Omega) \backslash \mathrm{Sym}(\Omega)$.

Definition (João Araújo - CAUL)

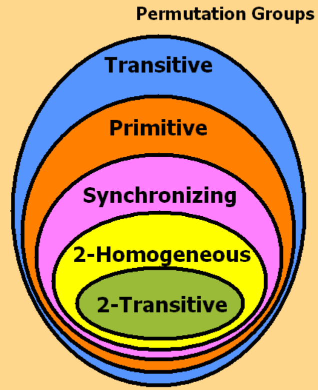
G is synchronizing if there is no non-trivial partition $\mathcal{P}$ and subset S of Ω such that

$$Sg \text{ is a section of } \mathcal{P}, \ \forall g \in G.$$

Such a partition is said to be section-regular.

Synchronization Tools

Group theory



Proposition (Neumann, 2009)

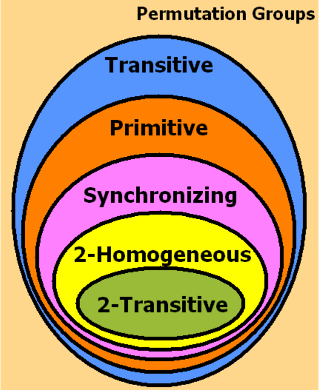
A section-regular partition for a transitive group is uniform.

Proposition

A primitive group acting on p or on $2p$ points is synchronizing, where p is a prime.

Synchronization Tools

Group theory



Proposition (Neumann, 2009)

A section-regular partition for a transitive group is uniform.

Proposition

A primitive group acting on p or on $2p$ points is synchronizing, where p is a prime.

Theorem

Let $H \leq \mathrm{GL}(2,p)$ irreducible. Let $G = (\mathbb{F}_p)^2 \rtimes H \leq \mathrm{Sym}((\mathbb{F}_p)^2)$.

(1) If H preserves $(\mathbb{F}_p)^2 = V_1 \oplus \cdots \oplus V_s \Rightarrow G$ is non-synchronizing.

Assume that (1) does not hold.

(2) If $\mathrm{SL}(2,p) \leq H$ then G is synchronizing.

(3) If $H \cong C_r$ or $H \cong C_r \rtimes C_2$ then set $m = (p^2-1)/r$.
- *(a) If $m = 1 \Rightarrow G$ is synchronizing.*
- *(b) If $m > 1$ and $m \mid p+1 \Rightarrow G$ is non-synchronizing.*
- *(c) If $m = 3$ then G is non-synchronizing $\Leftrightarrow 3 \mid p+1$.*

(4) If $H \cong C_r \cdot C_2$ then set $m = (p^2-1)/r$.
- *(a) If $m = 2 \Rightarrow G$ is synchronizing.*
- *(b) If $m > 2$ and $m \mid p+1 \Rightarrow G$ is non-synchronizing.*

Why Is This Interesting?

1. Synchronizing groups are primitive.
2. Which primitive groups are synchronizing?
3. The O'Nan-Scott Theorem divides the primitive permutation groups into several classes.
4. Some of these types of groups are non-synchronizing groups.
5. Affine groups constitute an interesting class.

Theorem (J. E. Pin, 1979)

The affine groups acting on 1-dimensional vector-spaces are synchronizing.

What Happens in Dimension 2?

Why Is This Interesting?

1. Synchronizing groups are primitive.
2. Which primitive groups are synchronizing?
3. The O'Nan-Scott Theorem divides the primitive permutation groups into several classes.
4. Some of these types of groups are non-synchronizing groups.
5. Affine groups constitute an interesting class.

Theorem (J. E. Pin, 1979)

The affine groups acting on 1-dimensional vector-spaces are synchronizing.

What Happens in Dimension 2?

Why Is This Interesting?

1. Synchronizing groups are primitive.
2. Which primitive groups are synchronizing?
3. The O'Nan-Scott Theorem divides the primitive permutation groups into several classes.
4. Some of these types of groups are non-synchronizing groups.
5. Affine groups constitute an interesting class.

Theorem (J. E. Pin, 1979)

The affine groups acting on 1-dimensional vector-spaces are synchronizing.

What Happens in Dimension 2?

Why Is This Interesting?

1. Synchronizing groups are primitive.
2. Which primitive groups are synchronizing?
3. The O'Nan-Scott Theorem divides the primitive permutation groups into several classes.
4. Some of these types of groups are non-synchronizing groups.
5. Affine groups constitute an interesting class.

Theorem (J. E. Pin, 1979)

The affine groups acting on 1-dimensional vector-spaces are synchronizing.

What Happens in Dimension 2?

Theorem

Let $H \leq \mathrm{GL}(2,p)$ irreducible. Let $G = (\mathbb{F}_p)^2 \rtimes H \leq \mathrm{Sym}((\mathbb{F}_p)^2)$.

(1) If H preserves $(\mathbb{F}_p)^2 = V_1 \oplus \cdots \oplus V_s \Rightarrow G$ is non-synchronizing.

Assume that (1) does not hold.

(2) If $\mathrm{SL}(2,p) \leq H$ then G is synchronizing.

(3) If $H \cong C_r$ or $H \cong C_r \rtimes C_2$ then set $m = (p^2-1)/r$.
- *(a) If $m = 1 \Rightarrow G$ is synchronizing.*
- *(b) If $m > 1$ and $m \mid p+1 \Rightarrow G$ is non-synchronizing.*
- *(c) If $m = 3$ then G is non-synchronizing $\Leftrightarrow 3 \mid p+1$.*

(4) If $H \cong C_r \cdot C_2$ then set $m = (p^2-1)/r$.
- *(a) If $m = 2 \Rightarrow G$ is synchronizing.*
- *(b) If $m > 2$ and $(m/2) \mid p+1 \Rightarrow G$ is non-synchronizing.*
- *(c) If $m = 6$ then G is non-synchronizing $\Leftrightarrow 3 \mid p+1$.*

Tools for the Proof

Group Theory

(1) If H preserves $(\mathbb{F}_p)^2 = V_1 \oplus \cdots \oplus V_s$ then G is non-synchronizing.

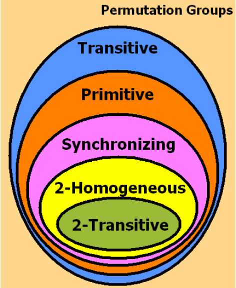
A *Cartesian decomposition* of a set Ω is a set $\Sigma = \{\mathscr{P}_1, \ldots, \mathscr{P}_t\}$ of non-trivial partitions of Ω such that

$$|P_1 \cap \cdots \cap P_t| = 1 \text{ for all } P_1 \in \mathscr{P}_1, \ldots, P_t \in \mathscr{P}_t.$$

Lemma

A group which preserves a Cartesian decomposition is non-synchronizing.

(2) If $\mathrm{SL}(2, p) \leq H$ then G is synchronizing.



Tools for the Proof

Group Theory

(1) If H preserves $(\mathbb{F}_p)^2 = V_1 \oplus \cdots \oplus V_s$ then G is non-synchronizing.

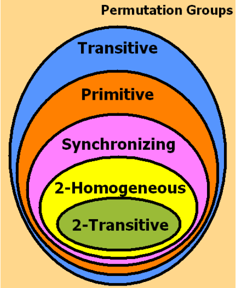
A *Cartesian decomposition* of a set Ω is a set $\Sigma = \{\mathscr{P}_1, \ldots, \mathscr{P}_t\}$ of non-trivial partitions of Ω such that

$$|P_1 \cap \cdots \cap P_t| = 1 \text{ for all } P_1 \in \mathscr{P}_1, \ldots, P_t \in \mathscr{P}_t.$$

Lemma

A group which preserves a Cartesian decomposition is non-synchronizing.

(2) If $\mathrm{SL}(2,p) \leq H$ then G is synchronizing.



Tools for the Proof

Group Theory

(1) If H preserves $(\mathbb{F}_p)^2 = V_1 \oplus \cdots \oplus V_s$ then G is non-synchronizing.

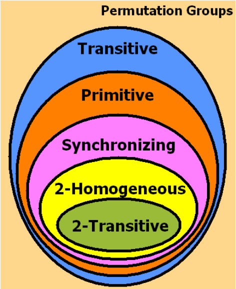
A *Cartesian decomposition* of a set Ω is a set $\Sigma = \{\mathscr{P}_1, \ldots, \mathscr{P}_t\}$ of non-trivial partitions of Ω such that

$$|P_1 \cap \cdots \cap P_t| = 1 \text{ for all } P_1 \in \mathscr{P}_1, \ldots, P_t \in \mathscr{P}_t.$$

Lemma

A group which preserves a Cartesian decomposition is non-synchronizing.

(2) If $\mathrm{SL}(2, p) \leq H$ then G is synchronizing.



Tools for the Proof

Graph Theory

(3), (4) If $H \cong C_r$ or $H \cong C_r \rtimes C_2$ or $H \cong C_r \cdot C_2$ then set $m = (p^2 - 1)/r$.

Theorem (Neumann, 2009)

Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive group. Then

G is non-synchronizing $\Leftrightarrow$ There exists a non-trivial G-invariant graph $\Gamma = (\Omega, E)$ such that $\omega(\Gamma) = \chi(\Gamma)$ (suitable graph).

- The edge-set of G-invariant graphs is a union of G-orbits on $\Omega^{\{2\}}$.
- The $(\mathbb{F}_p^2 \rtimes C_r)$-invariant graphs with one orbit are isomorphic to the generalized Paley graph $\Gamma_{p^2,m}$.

Tools for the Proof

Graph Theory

(3), (4) If $H \cong C_r$ or $H \cong C_r \rtimes C_2$ or $H \cong C_r \cdot C_2$ then set $m = (p^2 - 1)/r$.

Theorem (Neumann, 2009)

Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive group. Then

G is non-synchronizing $\Leftrightarrow$ There exists a non-trivial G-invariant graph $\Gamma = (\Omega, E)$ such that $\omega(\Gamma) = \chi(\Gamma)$ (suitable graph).

- The edge-set of G-invariant graphs is a union of G-orbits on $\Omega^{\{2\}}$.
- The $(\mathbb{F}_p^2 \rtimes C_r)$-invariant graphs with one orbit are isomorphic to the generalized Paley graph $\Gamma_{p^2,m}$.

Tools for the Proof

Graph Theory

(3), (4) If $H \cong C_r$ or $H \cong C_r \rtimes C_2$ or $H \cong C_r \cdot C_2$ then set $m = (p^2 - 1)/r$.

Theorem (Neumann, 2009)

Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive group. Then

G is non-synchronizing $\Leftrightarrow$ There exists a non-trivial G-invariant graph $\Gamma = (\Omega, E)$ such that $\omega(\Gamma) = \chi(\Gamma)$ (suitable graph).

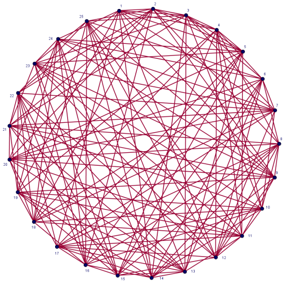
- The edge-set of G-invariant graphs is a union of G-orbits on $\Omega^{\{2\}}$.
- The $(\mathbb{F}_p^2 \rtimes C_r)$-invariant graphs with one orbit are isomorphic to the generalized Paley graph $\Gamma_{p^2,m}$.

Generalized Paley Graphs?

Definition (Generalized Paley graph)

Let $m \in \mathbb{N}$ such that $2m \mid p^2 - 1$
and let $S_{p^2,m} = \{\delta^m : \delta \in \mathbb{F}^*_{p^2}\}$.

The *generalized Paley graph* of the field $\mathbb{F}_{p^2}$ *with* ***index*** m is the graph $\Gamma_{p^2,m} = (\mathbb{F}_{p^2}, E)$, where $\{\alpha, \beta\} \in E \Leftrightarrow \beta - \alpha \in S_{p^2,m}$



Theorem

The generalized Paley graph $\Gamma_{p^2,m}$ *is suitable* $\Leftrightarrow m \mid p + 1$.

Theorem

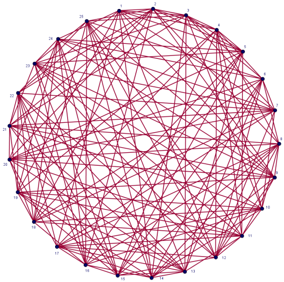
Let Γ *be an edge-transitive and vertex-transitive graph with* n *vertices. If* $\omega(\Gamma) = \chi(\Gamma) = k$ *then* $k - 1 \mid n/\partial(\Gamma)$.

Generalized Paley Graphs?

Definition (Generalized Paley graph)

Let $m \in \mathbb{N}$ such that $2m \mid p^2 - 1$ and let $S_{p^2,m} = \{\delta^m : \delta \in \mathbb{F}^*_{p^2}\}$.

The *generalized Paley graph* of the field $\mathbb{F}_{p^2}$ *with* ***index*** m is the graph $\Gamma_{p^2,m} = (\mathbb{F}_{p^2}, E)$, where $\{\alpha, \beta\} \in E \Leftrightarrow \beta - \alpha \in S_{p^2,m}$



Theorem

The generalized Paley graph $\Gamma_{p^2,m}$ *is suitable* $\Leftrightarrow m \mid p + 1$.

Theorem

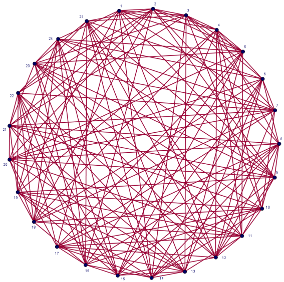
Let Γ *be an edge-transitive and vertex-transitive graph with* n *vertices. If* $\omega(\Gamma) = \chi(\Gamma) = k$ *then* $k - 1 \mid n/\partial(\Gamma)$.

Generalized Paley Graphs?

Definition (Generalized Paley graph)

Let $m \in \mathbb{N}$ such that $2m \mid p^2 - 1$
and let $S_{p^2,m} = \{\delta^m : \delta \in \mathbb{F}^*_{p^2}\}$.

The *generalized Paley graph* of the field $\mathbb{F}_{p^2}$ *with* ***index*** m is the graph $\Gamma_{p^2,m} = (\mathbb{F}_{p^2}, E)$, where $\{\alpha, \beta\} \in E \Leftrightarrow \beta - \alpha \in S_{p^2,m}$



Theorem

The generalized Paley graph $\Gamma_{p^2,m}$ *is suitable* $\Leftrightarrow m \mid p + 1$*.*

Theorem

Let Γ *be an edge-transitive and vertex-transitive graph with* n *vertices. If* $\omega(\Gamma) = \chi(\Gamma) = k$ *then* $k - 1 \mid n/\partial(\Gamma)$*.*

Back to the Main Result

(3) If $H \cong C_r$ or $H \cong C_r \rtimes C_2$ then set $m = (p^2 - 1)/r$.

(a) If $m = 1 \Rightarrow G$ is synchronizing.

$\Gamma_{p^2,1}$ is the complete graph $\Rightarrow G$ is 2-homogeneous.

(b) If $m > 1$ and $m \mid p+1 \Rightarrow G$ is non-synchronizing.

If $m \mid p+1 \Rightarrow \Gamma_{p^2,m}$ is suitable.

(c) If $m = 3$ then G is non-synchronizing $\Leftrightarrow 3 \mid p+1$.

If $3 \mid p+1 \Rightarrow \Gamma_{p^2,3}$ is suitable.

If $3 \nmid p+1 \Rightarrow \Gamma_{p^2,3}$ is not suitable. $\Rightarrow \Gamma'_{p^2,3}$ is not suitable.

(4) If $H \cong C_r \cdot C_2$ then set $m = (p^2 - 1)/r$.

(a) If $m = 2 \Rightarrow G$ is synchronizing.

(b) If $m > 2$ and $m \mid p+1 \Rightarrow G$ is non-synchronizing.

Back to the Main Result

(3) If $H \cong C_r$ or $H \cong C_r \rtimes C_2$ then set $m = (p^2 - 1)/r$.

(a) If $m = 1 \Rightarrow G$ is synchronizing.

$\Gamma_{p^2,1}$ is the complete graph $\Rightarrow G$ is 2-homogeneous.

(b) If $m > 1$ and $m \mid p + 1 \Rightarrow G$ is non-synchronizing.

If $m \mid p + 1 \Rightarrow \Gamma_{p^2,m}$ is suitable.

(c) If $m = 3$ then G is non-synchronizing $\Leftrightarrow 3 \mid p + 1$.

If $3 \mid p + 1 \Rightarrow \Gamma_{p^2,3}$ is suitable.

If $3 \nmid p + 1 \Rightarrow \Gamma_{p^2,3}$ is not suitable. $\Rightarrow \Gamma'_{p^2,3}$ is not suitable.

(4) If $H \cong C_r \cdot C_2$ then set $m = (p^2 - 1)/r$.

(a) If $m = 2 \Rightarrow G$ is synchronizing.

(b) If $m > 2$ and $m \mid p + 1 \Rightarrow G$ is non-synchronizing.

Back to the Main Result

(3) If $H \cong C_r$ or $H \cong C_r \rtimes C_2$ then set $m = (p^2 - 1)/r$.

(a) If $m = 1 \Rightarrow G$ is synchronizing.

$\Gamma_{p^2,1}$ is the complete graph $\Rightarrow G$ is 2-homogeneous.

(b) If $m > 1$ and $m \mid p + 1 \Rightarrow G$ is non-synchronizing.

If $m \mid p + 1 \Rightarrow \Gamma_{p^2,m}$ is suitable.

(c) If $m = 3$ then G is non-synchronizing $\Leftrightarrow 3 \mid p + 1$.

If $3 \mid p + 1 \Rightarrow \Gamma_{p^2,3}$ is suitable.

If $3 \nmid p + 1 \Rightarrow \Gamma_{p^2,3}$ is not suitable. $\Rightarrow \Gamma'_{p^2,3}$ is not suitable.

(4) If $H \cong C_r \cdot C_2$ then set $m = (p^2 - 1)/r$.

(a) If $m = 2 \Rightarrow G$ is synchronizing.

(b) If $m > 2$ and $m \mid p + 1 \Rightarrow G$ is non-synchronizing.

Back to the Main Result

(3) If $H \cong C_r$ or $H \cong C_r \rtimes C_2$ then set $m = (p^2 - 1)/r$.

(a) If $m = 1 \Rightarrow G$ is synchronizing.

$\Gamma_{p^2,1}$ is the complete graph $\Rightarrow G$ is 2-homogeneous.

(b) If $m > 1$ and $m \mid p + 1 \Rightarrow G$ is non-synchronizing.

If $m \mid p + 1 \Rightarrow \Gamma_{p^2,m}$ is suitable.

(c) If $m = 3$ then G is non-synchronizing $\Leftrightarrow 3 \mid p + 1$.

If $3 \mid p + 1 \Rightarrow \Gamma_{p^2,3}$ is suitable.

If $3 \nmid p + 1 \Rightarrow \Gamma_{p^2,3}$ is not suitable. $\Rightarrow \Gamma'_{p^2,3}$ is not suitable.

(4) If $H \cong C_r \cdot C_2$ then set $m = (p^2 - 1)/r$.

(a) If $m = 2 \Rightarrow G$ is synchronizing.

(b) If $m > 2$ and $m \mid p + 1 \Rightarrow G$ is non-synchronizing.

Bibliography

- Broere, I. and Döman, D. and Ridley, J. N
  The clique numbers and chromatic numbers of certain Paley graphs.
  Volume 11 of *Quaestiones Math.*, 1988.

- John D. Dixon and Brian Mortimer.
  Permutation Groups.
  Volume 163 of *Graduate Texts in Mathematics*, Springer,1996.

- László Lovász
  On the Shannon capacity of a graph
  Volume 25 of *IEEE Trans. Inform. Theory*, 1979.

- Peter M. Neumann.
  Primitive permutation groups and their section-regular partitions.
  Michigan Math. J., 58:309–322, 2009.