Elementary abelian regular subgroups of $\mathrm{Sym}(2^n)$

Riccardo Aragona
joint work[*] with R. Civino, N. Gavioli, C. M. Scoppola
University of L'Aquila

Ischia Group Theory 2022

[*]Aragona, R., Civino, R., Gavioli, N., Scoppola, C. M.: Regular subgroups with large intersection. Ann. Mat. Pura Appl. 198(6), 2043–2057 (2019)

Aragona, R., Civino, R., Gavioli, N., Scoppola, C.M.: A chain of normalizers in the Sylow 2-subgroups of the symmetric group on 2^n letters. Indian J. Pure Appl. Math. 52(3), 735–746 (2021)

Conjugates of an elementary abelian regular subgroup of $\mathrm{Sym}(2^n)$

Let $V \stackrel{\text{def}}{=} (\mathbb{F}_2)^n$ and T be the translation group on V,

$$T \stackrel{\text{def}}{=} \{\sigma_b \mid b \in V, x \mapsto x + b\},$$

then

$$a + b = a\sigma_b.$$

Conjugates of an elementary abelian regular subgroup of $\mathrm{Sym}(2^n)$

Let $V \overset{\text{def}}{=} (\mathbb{F}_2)^n$ and T be the translation group on V,

$$T \overset{\text{def}}{=} \{\sigma_b \mid b \in V, x \mapsto x + b\},$$

then

$$a + b = a\sigma_b.$$

Analogously, if $T^g < \mathrm{Sym}(V)$ is conjugated to T in $\mathrm{Sym}(V)$, i.e. another elementary abelian regular subgroup of $\mathrm{Sym}(V)$.

Let τ_b be the unique element in T^g which maps 0 into b, then

$$T^g = \{\tau_b \mid b \in V\},$$

and another operation induced by T^g is defined on V as

$$a \circ b \overset{\text{def}}{=} a\tau_b$$

Motivation

Let $V \stackrel{\text{def}}{=} (\mathbb{F}_2)^n$ be the message space

Block cipher

A block cipher $\mathcal{C}$ is a set of permutations of V (encryption functions)

$$\{\varphi_k\}_{k\in\mathcal{K}} \subseteq \mathrm{Sym}(V),$$

each of which is individuated by a key k in the space $\mathcal{K} = (\mathbb{F}_2)^\kappa$.

Motivation

Let $V \stackrel{\text{def}}{=} (\mathbb{F}_2)^n$ be the message space

Block cipher

A block cipher $\mathcal{C}$ is a set of permutations of V (encryption functions)

$$\{\varphi_k\}_{k \in \mathcal{K}} \subseteq \mathrm{Sym}(V),$$

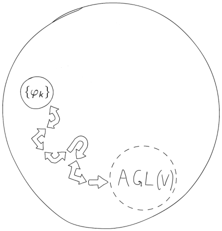
each of which is individuated by a key k in the space $\mathcal{K} = (\mathbb{F}_2)^\kappa$.

Each encryption function is usually obtained as the composition of different layers. Some of those layers provide entropy to the encryption process by bitwise addition mod 2 with round keys in V, computed starting from the user-selected key in $\mathcal{K}$.

Motivation

The encryption functions should be chosen judiciously:
some choices may offer the possibility for a successful attack

In particular, the encryption functions should lie "far" from the set
$\mathrm{AGL}(V) \cong N_{\mathrm{Sym}(V)}(T)$

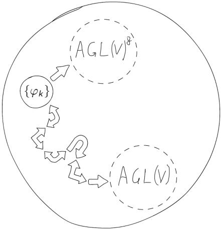


for avoiding, for example, differential cryptanalysis*.

*Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Crypt. 4(1), 3–72 (1991)

Motivation

However, several isomorphic copies of $\mathrm{AGL}(V)$, its conjugates, are contained in $\mathrm{Sym(V)}$, and so the encryptions functions could be approximate by elements of $\mathrm{AGL}(V)^g \cong N_{\mathrm{Sym}(V)}(T^g)$, for some $g \in \mathrm{Sym(V)}$



This fact is exploited by Civino, Blondeau and Sala** for designing a cipher which is resistant to the classical differential cryptanalysis but may be attacked using the operation on V created from $T^g < \mathrm{AGL}(V)$, for some $g \in \mathrm{Sym}(V)$ such that $|T \cap T^g| = 2^{n-2}$.

**Civino, R., Blondeau, C., Sala, M.: Differential attacks: using alternative operations. Designs Codes Cryptogr. 87(2–3), 225–247 (2019)

What makes the case $|T \cap T^g| = 2^{n-2}$ special?

T^g conjugated to T such that $|T \cap T^g| = 2^{n-2}$, are called second-maximal intersection subgroups (2MI)

---

*Calderini, M., Civino, R., Sala, M.: On properties of translation groups in the affine general linear group with applications to cryptography. J. Algebra 569, 658–680 (2021)

What makes the case $|T \cap T^g| = 2^{n-2}$ special?

T^g conjugated to T such that $|T \cap T^g| = 2^{n-2}$, are called second-maximal intersection subgroups (2MI)

On the one hand, it is known* that $|T \cap T^g| \leq 2^{n-2}$.

*Calderini, M., Civino, R., Sala, M.: On properties of translation groups in the affine general linear group with applications to cryptography. J. Algebra 569, 658–680 (2021)

What makes the case $|T \cap T^g| = 2^{n-2}$ special?

T^g conjugated to T such that $|T \cap T^g| = 2^{n-2}$, are called second-maximal intersection subgroups (2MI)

On the one hand, it is known* that $|T \cap T^g| \leq 2^{n-2}$.

On the other hand

Theorem (A, Civino, Gavioli, Scoppola)

Let $g \in \mathrm{Sym}(V)$ such that T^g is a 2MI subgroup, then $T^g < \mathrm{AGL}(V)$

*Calderini, M., Civino, R., Sala, M.: On properties of translation groups in the affine general linear group with applications to cryptography. J. Algebra 569, 658–680 (2021)

What makes the case $|T \cap T^g| = 2^{n-2}$ special?

T^g conjugated to T such that $|T \cap T^g| = 2^{n-2}$, are called second-maximal intersection subgroups (2MI)

On the one hand, it is known* that $|T \cap T^g| \leq 2^{n-2}$.

On the other hand

Theorem (A, Civino, Gavioli, Scoppola)

Let $g \in \mathrm{Sym}(V)$ *such that* T^g *is a 2MI subgroup, then* $T^g < \mathrm{AGL}(V)$

- In the case when $|T \cap T^g| < 2^{n-2}$, there are some examples for which $T^g < \mathrm{Sym}(V) \setminus \mathrm{AGL}(V)$

*Calderini, M., Civino, R., Sala, M.: On properties of translation groups in the affine general linear group with applications to cryptography. J. Algebra 569, 658–680 (2021)

What makes the case $|T \cap T^g| = 2^{n-2}$ special?

T^g conjugated to T such that $|T \cap T^g| = 2^{n-2}$, are called second-maximal intersection subgroups (2MI)

On the one hand, it is known* that $|T \cap T^g| \leq 2^{n-2}$.

On the other hand

Theorem (A, Civino, Gavioli, Scoppola)

Let $g \in \mathrm{Sym}(V)$ *such that* T^g *is a 2MI subgroup, then* $T^g < \mathrm{AGL}(V)$

- In the case when $|T \cap T^g| < 2^{n-2}$, there are some examples for which $T^g < \mathrm{Sym}(V) \setminus \mathrm{AGL}(V)$
- 2MI subgroups play a role in the way Sylow 2-subgroups of $\mathrm{AGL}(V)$ are structured

*Calderini, M., Civino, R., Sala, M.: On properties of translation groups in the affine general linear group with applications to cryptography. J. Algebra 569, 658–680 (2021)

2MI subgroups and the Sylow 2-subgroups of AGL(V)

Theorem (A, Civino, Gavioli, Scoppola)

Every Sylow 2-subgroup Σ of $\mathrm{AGL}(V)$ *contains exactly one elementary abelian regular subgroup T_Σ intersecting T in a second-maximal subgroup of T and which is normal in Σ*

$$\begin{array}{c} \mathrm{AGL}(V) \\ | \\ \Sigma \\ |\, \trianglelefteq \\ T_\Sigma \end{array}$$

... conversely

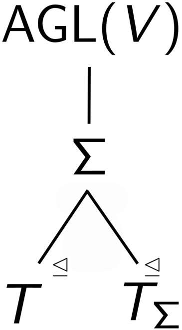
Theorem (A, Civino, Gavioli, Scoppola)

If $\bar{T}$ *is an elementary abelian regular subgroup of* $\mathrm{AGL}(V)$ *such that* $|\bar{T} \cap T| = 2^{n-2}$*, then there exists a Sylow* 2*-subgroup* Σ *of* $\mathrm{AGL}(V)$ *such that* $\bar{T} = T_\Sigma \trianglelefteq \Sigma$

Elementary abelian regular normal subgroups in the Σ

Theorem (A, Civino, Gavioli, Scoppola)

Let $g \in \mathrm{Sym}(V)$ and let Σ a Sylow 2-subgroup be of $\mathrm{AGL}(V)$ containing T^g. The subgroup T^g is normal in Σ if and only if $T^g \in \{ T, T_\Sigma \}$



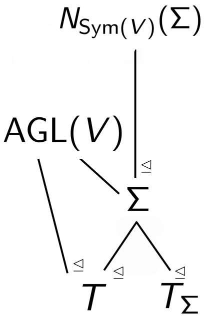
Sylow 2-subgroups and their normalizers

Corollary

Every $g \in N_{\mathrm{Sym}(V)}(\Sigma) \setminus \mathrm{AGL}(V)$ *interchanges by conjugation* T *and* T_Σ

Theorem (A, Civino, Gavioli, Scoppola)

If Σ *is a Sylow* 2*-subgroup of* $\mathrm{AGL}(V)$*, then* $|N_{\mathrm{Sym}(V)}(\Sigma) : \Sigma| = 2$



Self-normalising

It was already know to P. Hall that the Sylow 2-subgroups of $\mathrm{Sym}(V)$ are self-normalising. Similarly:

Theorem (A, Civino, Gavioli, Scoppola)

If Σ is a Sylow 2-subgroup of $\mathrm{AGL}(V)$, then $N_{\mathrm{AGL}(V)}(\Sigma) = \Sigma$.

Proof.

Since $|N_{\mathrm{Sym}(V)}(\Sigma) : \Sigma| = 2$, if $|\,\mathrm{AGL}(V)| = 2^m t$, with t an odd integer, then we have $|\Sigma| = 2^m$ and $|N_{\mathrm{Sym}(V)}(\Sigma)| = 2^{m+1}$. Since $N_{\mathrm{AGL}(V)}(\Sigma) \leq \mathrm{AGL}(V)$ and $N_{\mathrm{AGL}(V)}(\Sigma) \leq N_{\mathrm{Sym}(V)}(\Sigma)$, then $|N_{\mathrm{AGL}(V)}(\Sigma)| = 2^m$. $\square$

A normalizer chain

Let S_n be a Sylow 2-subgroup of $\mathrm{Sym}(2^n)$. Notice that

$$\Sigma_n = \mathrm{AGL}(V) \cap S_n = N_{\mathrm{Sym}(2^n)}(T) \cap S_n = N_{S_n}(T)$$

A normalizer chain

Let S_n be a Sylow 2-subgroup of $\mathrm{Sym}(2^n)$. Notice that

$$\Sigma_n = \mathrm{AGL}(V) \cap S_n = N_{\mathrm{Sym}(2^n)}(T) \cap S_n = N_{S_n}(T)$$

Let us define the sequence $\{N_n^k\}_{k \geq 0}$, where

$$N_n^0 \overset{\text{def}}{=} \Sigma_n, \quad N_n^1 \overset{\text{def}}{=} N_{\mathrm{Sym}(2^n)}(\Sigma_n),$$

and recursively, for $k > 1$,

$$N_n^k \overset{\text{def}}{=} N_{\mathrm{Sym}(2^n)}(N_n^{k-1}).$$

A chain of 2-groups

Theorem (A, Civino, Gavioli, Scoppola)

For every $k \geq 1$, we have $N_n^k = N_{S_n}(N_n^{k-1})$. In particular, N_n^k is a 2-group.

Spoiler of Norberto's talk

Using GAP we have computed $|N_n^i : N_n^{i-1}|$ up to $n = 11$, and we have obtained the following table

n	2	3	4	5	6	7	8	9	10	11	
$\log_2 \lvert\Sigma_n\rvert$	**3**	6	10	15	21	28	36	45	55	66	
$\log_2 \lvert N_n^1\rvert$	-	**7**	11	16	22	29	37	46	56	67	$+1$
$\log_2 \lvert N_n^2\rvert$	-	-	**13**	18	24	31	39	48	58	69	$+2$
$\log_2 \lvert N_n^3\rvert$	-	-	14	**22**	28	35	43	52	62	73	$+4$
$\log_2 \lvert N_n^4\rvert$	-	-	15	23	**35**	42	50	59	69	80	$+7$
$\log_2 \lvert N_n^5\rvert$	-	-	-	25	37	**53**	61	70	80	91	$+11$
$\log_2 \lvert N_n^6\rvert$	-	-	-	27	41	57	**77**	86	96	107	$+16$
$\log_2 \lvert N^7_{,n}\rvert$	-	-	-	28	45	64	84	**109**	119	130	$+23$
$\log_2 \lvert N_n^8\rvert$	-	-	-	29	46	67	89	113	**151**	162	$+32$
$\log_2 \lvert N_n^9\rvert$	-	-	-	30	47	71	95	122	155	**205**	$+43$

The logarithm of the size of the normalizers, when $n \leq 11$

Spoiler of Norberto's talk

We looked up at *The On-Line Encyclopedia of Integer Sequences* at `https://oeis.org/A317910` and found out that the numbers that appear in the last column, i.e. $\log_2 |N_n^i : N_n^{i-1}|$ with $1 \leq i \leq n-2$, coincide with the (i+2)-th terms of the sequence of the partial sums $\{a_j\}_{j\geq 1}$ of the sequence $\{b_j\}_{j\geq 1}$ counting the number of partitions of j into at least two distinct parts.

j	1	2	3	4	5	6	7	8	9	10	11	12	13	14
b_j	0	0	1	1	2	3	4	5	7	9	11	14	17	21
a_j	0	0	1	2	4	7	11	16	23	32	43	57	74	95

First values of the sequences a_j and b_j

Thanks for your attention!