Regular subgroups with large intersection

Norberto Gavioli
joint work with R. Aragona, R. Civino and C. M. Scoppola
Annali di Matematica Pura ed Applicata (2019)
https://doi.org/10.1007/s10231-019-00853-w

Università degli Studi dell'Aquila

SandGAL 2019
Semigroups and Groups, Automata, Logics
Cremona 13 giugno 2019

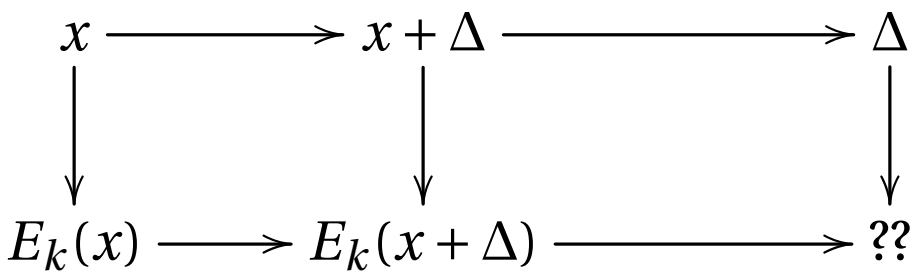
Block ciphers

A block cipher is a family $\{E_k\}_{k \in \mathcal{K}}$ of *non linear* key-dependent permutations $E_k \in \mathrm{Sym}(V)$ known as encryption functions. In this setting $V = \mathbb{Z}_2^n$ is the plaintext and ciphertex space.

Each encryption function is in general obtained as the composition of different layers. Some of those layers usually provide entropy to the encryption process by means of (bit-wise XOR) addition with elements of V, called *round keys*.

Differential cryptanalysis

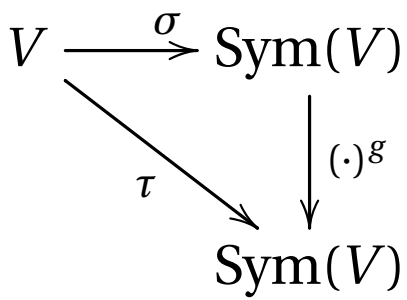
A typical attack against block ciphers is *differential cryptanalysis* in which linearities of the encryption functions can be exploited to achieve information on the key



This is the reason why blockciphers are designed to be far from being linear functions. The more a function is non-linear the more it is far to be a permutation in the affine group $\mathrm{AGL}(V) \leq \mathrm{Sym}(V)$.

Alternate sums

Beyond XOR, there are several operations that give V the structure of an elementary abelian 2-group. These alternate operations can be be obtained by conjugations of the Cayley regular embedding $\sigma\colon u \mapsto \sigma_u \in \mathrm{Sym}(V)$ of V within the symmetric group.



We have that $u + v = \sigma_u(v)$.

In a similar fashion we can define a new operation $\circ$ on V by letting

$$u \circ v = \tau_u(v).$$

Alternate differences

Although differential cryptanalysis can fail with respect to the XOR operation $+$, it may be possible to try to attack the cryptosystem considering differences with respect to an alternate operation $\circ$.

Even if the encryption functions are not linear with respect to $+$, it may happen they are with respect to some other operation $\circ$ induced by the conjugation by some $g \in \mathrm{Sym}(V)$.

Weak keys

The group theoretical counterpart is the study of the orbits of the action by conjugation of $\mathrm{Sym}(V)$ over the group $T := \sigma(V)$ and over $\mathrm{AGL}(V)$, which is the normalizer of T in $\mathrm{Sym}(V)$.

Assuming that $\circ$ is the operation induced on V by the conjugate subgroup $\tau(V) = T^g$ the subgroup W of V defined by

$$\sigma_W = T \cap T^g$$

is called the *weak key subspace*. Note that

$$W = \{u \in V \mid \sigma_u = \tau_u\}$$

Maximal intersection

Proposition

Let $g \in \mathrm{Sym}(V)$ be such that $T \neq T^g$. If $W \leq V$ is such that $\sigma_W = T \cap T^g$, then $\dim(W) \leq n-2$.

(Slightly improves a similar result by Calderini and Sala)

This shows that if the weak key space W is proper then it has codimension at least 2. We have the following

Theorem (Aragona, Civino, G., Scoppola)

If $g \in \mathrm{Sym}(V)$ is such that $\dim(W) = n-2$, then $T^g < \mathrm{AGL}(V)$.

Corollary

The group $\mathrm{Sym}(V)$ contains $\dfrac{(2^{n-2}-1)(2^{n-1}-1)(2^n-1)}{3}$ elementary abelian regular subgroups whose intersection with T is a second-maximal subgroup of T.

Sylow subgroup of $\mathrm{AGL}(V)$

It is well known that $\mathrm{AGL}(V)$ is the normalizer of $T = \sigma_V$ in $\mathrm{Sym}(V)$, so that T is contained in every Sylow 2-subgroup Σ of $\mathrm{AGL}(V)$.

Actually a Silow 2-subgroup Σ of $\mathrm{AGL}(V)$ is the semidirect produc $T \ltimes U$ where U is the stabilizer by conjugation in $\mathrm{GL}(V)$ of a maximal flag

$$\sigma_{\{0\}} \leq \sigma_{\{V_1\}} \leq \cdots \leq \sigma_{\{V_n\}}$$

of subgroups of $T = \sigma_V$.

Theorem (Aragona, Civino, G., 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.

Counting alternate sums

Theorem (Aragona, Civino, G., Scoppola)

Let Σ be a Sylow 2-subgroup of $\mathrm{AGL}(V)$ and $\sigma_{\{0\}} =< \sigma_{V_1} < \ldots < \sigma_{V_n} = T$ the associate invariant maximal flag of T. There exist $2^{d\binom{n-d}{2}}$ subgroups $T^g \leq \Sigma$, where $g \in \mathrm{Sym}(V)$, such that $\sigma_{V_d} \leq T \cap T_g$ and $T \leq N_{\mathrm{Sym}(V)}(T^g) = \mathrm{AGL}(V)^g$.

Theorem (Aragona, Civino, G., Scoppola)

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

Corollaries

Corollary

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

$$|N_{\mathrm{Sym}(V)}(\Sigma) : \Sigma| = 2.$$

In particular $N_{\mathrm{Sym}(V)}(\Sigma)$ interchanges T and T_Σ by conjugation, and Σ is self-normalizing in $\mathrm{AGL}(V)$.

Smaller intersections

Trying to generalize we would like to study the action by conjugation over T and over Σ of the sequence defined by

$$N_1 = N_{\mathrm{Sym}(V)}(\Sigma)$$

and

$$N_i = N_{\mathrm{Sym}(V)}(N_{i-1}) \text{ for } i \geq 2.$$

There is an evidence that $|N_{i+1} : N_i|$ is always a power of 2.

We observe that N_2 Conjugate T in subgroups intersecting T in a second or third maximal subgroup belonging to the maximal flag determined by Σ.

Ongoing research

Proposition

There is a unique Sylow 2-subgroup of $\mathrm{Sym}(V)$ containing Σ and all the N_i.

Sketch of proof.

The reason is that the flag associated to Σ determine a unique imprimitivity binary tree $\mathscr{T}$ for the action of Σ of V. This tree is acted over by all the normalizers N_i which are then contained in the automorphism group of $\mathscr{T}$, which is the relevant Sylow 2-subgroup of $\mathrm{Sym}(V)$. □

We know also that asymptotically, as $\dim V$ tends to infinity, the indices $|N_{i+1} : N_i|$ depends only on i, we computed some of them and we would like to find a general formula for these.