symmetry

MDPI

Article

A Computational Approach to Verbal Width for Engel Words in Alternating Groups †

Jorge Martínez Carracedo

School of Computing, Jordanstown Campus, Ulster University, Northern Ireland BT37 0QB, UK; j.martinez-carracedo@ulster.ac.uk

† This paper is an extended version of our paper published in Lecture Notes of the XVII 'Jacques-Louis Lions' Spanish-French School. Computational Mathematics, Numerical Analysis and Applications (Springer, 2017).

Received: 18 June 2019; Accepted: 2 July 2019; Published: 3 July 2019

Abstract: It is known that every element in the alternating group A_n, with $n \geq 5$, can be written as a product of at most two Engel words of arbitrary length. However, it is still unknown if every element in an alternating group is an Engel word of Arbitrary length. In this paper, a different approach to this problem is presented, getting new results for small alternating groups.

Keywords: group theory; symmetry; Engel words; alternating group

1. Introduction

In recent times, many novel cryptosystems based on Group Theory have been proposed. Even when the ideas behind these group-based cryptosystems are interesting in their own right, these cryptosystems cannot yet compete with more standardized schemes such as Diffie-Hellman or RSA.

The word problem and the conjugacy problem are two of the fundamental decision problems in group theory proposed by Max Dehn in 1911 [1]. The study and understanding of these problems in particular groups have played an important role on group-based cryptosystems.

Braid groups (see Reference [2]), for example, are the mathematical structures behind many cryptographic schemes proposed in the last thirty years. One of the main reasons why these groups are suitable to be used in cryptography is the existence of *normal forms* that facilitates an efficient solution of the word problem [3].

The conjugacy search problem (i.e., given two elements x and y of a group G that are conjugated, find the element $z \in G$ such that $x = y^z$) is the ground from which it is possible to build an scheme similar to ElGalmal in braid groups ([4]).

Solving the conjugacy problem in braid groups is the most direct way to attack this scheme. Garside ([5]) proposed the first algorithm in 1969 to solve this problem in a braid group. However, Garside's proposal is not efficient and a polynomial time algorithm has not been found yet. Heuristics algorithms (as proposed by Hofheinz and Steinwandt in Reference [6]) have achieved a large quota of success though.

Another example of key agreement protocol where the conjugacy search problem plays an important role was proposed by Anshel et al. [7] in 1999. Broadly speaking, in this protocol the two parties agree on a common key by computing a commutator. It was first proposed for braid groups for two reasons: the existence of normal forms and the fact that the conjugacy search problem is considered difficult in these groups.

Cryptography based on group theory has brought about new and interesting pure mathematical questions. The word problem and the conjugacy problem play an important role in some cryptographic schemes based in group theory. Therefore, its study in particular groups seems unavoidable.

Let us consider now an arbitrary group G and a word in the free group of rank r, $\omega \in \mathbb{F}_r$, with r a natural number. We can define the map

$$\omega : \overbrace{G \times \cdots \times G}^{r} \longrightarrow G$$

where each tuple $(g_1, g_2, ..., g_r)$ is mapped to $\omega(g_1, g_2, ..., g_r)$.

We denote the image of the map ω by $\omega(G)$. The verbal subgroup of G related to ω is defined as the subgroup generated by $\omega(G)$.

The surjectivity of the map ω, the cardinality of the set $\omega(G)$, if the verbal subgroup $\langle \omega(G) \rangle = G$ or if it is possible to find a constant k for which $\omega(G)^k = \langle \omega(G) \rangle$ are essential questions to answer.

In 1951, O. Ore proved ([8]) that every element in an alternating group A_n, with $n \geq 5$, can be written as a commutator in A_n.

In other words, Ore's result states that if we consider the word $\tau := x_1^{-1} x_2^{-1} x_1 x_2$ in the free group of rank 2, $\mathbb{F}_2$, then $\tau(A_n) = A_n$, for every $n \geq 5$.

In the same work, he proposed a conjecture: "Every element in a finite simple group G is a commutator in G". This is known as the Abstract Ore's Conjecture and was an open question until 2010.

One initial progress on this conjecture was done in 1994 by Wilson [9]. He proved that for any finite simple group, there exists a constant k such that, $\tau(G)^k = G$.

In this line of work, some new results were obtained considering the word $\xi := x^n$, with n a natural number. In 1996, Martínez and Zelmanov [10] and in 1997, Saxl and Wilson [11] proved, independently, that for every finite simple group big enough, there exists a constant k such that $\xi(G)^k = G$.

In 2010, M. W. Liebeck, E. A. O'Brien, A. Shalev and P. H. Tiep [12] published the proof of the Ore Conjecture. They proved that for every finite simple group G, $G = \tau(G)$, where $\tau := x_1^{-1} x_2^{-1} x_1 x_2$ denotes the commutator. The proof of this result is highly non trivial and makes use of Character Theory and computation where algebraic computer programs were specially designed.

Once this conjecture was proved, it seems natural to consider Engel words of arbitrary length instead of the commutator τ. That is considering the word $E_m = [...[x, y], y], ..., y]$. Ore's Conjecture can be easily extended to Engel words, is it still true that $G = E_m(G)$ for every finite simple group G and any natural number m?

In Reference [13], a first approach was given for alternating simple groups. The author proved that every element in A_n, with $n \geq 5$, can be written as a product of at most two Engel words of arbitrary length, that is

$$A_n = E_{m_1}(A_n) E_{m_2}(A_n),$$

for any natural numbers $m_1, m_2 \geq 2$ and $n \geq 5$. However, the general case for alternating groups (if $A_n = E_m(A_n)$ for any natural numbers $m \geq 2$ and $n \geq 5$) remains unknown.

In Sections 2 and 3 two new approaches to this problem are presented. First, in Section 2, we study special sequences of Engel words, getting interesting properties about their length. In Section 3 we define a graph, depending on an alternating group and a fixed permutation and study the relation between this graph and the fact of an element $y \in A_n$ being an Engel word of arbitrary length.

In Section 4, we work with an alternating group A_n, $5 \leq n \leq 14$ and a fixed permutation y in A_n. We build a graph related to them in order to empirically study the Engel words $E_m(\cdot, y)$ in A_n.

2. Engel Chains

In this section, we define a particular type of sequence of Engel words and study some of their properties. We also analyze computationally the maximal length of these sequences for small alternating groups.

Let y be a fixed element in the alternating group A_n, $n \geq 5$. For each element $x \in A_n$ we can consider the following sequence of Engel words

$$E^y(x) := \{x, E_1(x,y), E_2(x,y), ...\}.$$

There always exist two integers $1 \leq k_1 < k_2$ such that $E_{k_1}(x,y) = E_{k_2}(x,y)$ in $E^y(x)$. Let us consider the first occurrence of k_1 and k_2 and the set

$$B^y(x) := \{E_{k_1}(x,y), ..., E_{k_2-1}(x,y)\}.$$

Definition 1. *Let x and y be two fixed elements in A_n. The set $E^y(x)$ is called the y-Engel Chain associated to the element x and $B^y(x)$ is called y-Engel Loop associated to the element x.*

The length of the Chain $E^y(x)$ is $l(E^y(x)) = k_2 - 1$ and the length of the loop is $l(B^y(x)) = k_2 - k_1$.

Lemma 1. *Given $n \geq 5$ we have that for every $m \in \mathbb{N}$*

$$E_m(x,y)E_{m+1}(x,y) = E_m(x^y, y).$$

Proof. Given $y \in A_n$, for every $m \in \mathbb{N}$ we have that

$$E_m(x,y)^y = E_m(x^y, y).$$

Then

$$E_m(x^y, y) = E_m(x,y)(E_m(x,y))^{-1}y^{-1}E_m(x,y)y = E_m(x,y)E_{m+1}(x,y).$$

□

That is, the product of two consecutive Engel words in the Chain $E^y(x)$ is an Engel word of the Chain $E^y(x^y)$.

Definition 2. *Given two elements $x, y \in A_n$, with $n \geq 5$, the Engel loop $B^y(x)$ is stable by y-conjugation if $(B^y(x))^y = B^y(x)$.*

We give now a characterization of an y-Engel loop stable by y-conjugation.

Lemma 2. *Given $x, y \in A_n$, with $n \geq 5$, the loop $B^y(x)$ is stable by y-conjugation if an only if for every $E_m(x,y) \in B^y(x)$ we have that*

$$E_m(x,y)E_{m+1}(x,y) \in B^y(x).$$

Proof. It is enough to see that

$$(B^y(x))^y := \{E_m(x,y)^y \mid E_m(x,y) \in B^y(x)\},$$

and that $E_m(x,y)^y = E_m(x^y, y)$.

Applying Lemma 1 we get the result. □

Let G be a group and let us consider an element $g \in G$. From now on, $o(g)$ denotes the order of the element g and $C_G(g)$ denotes the centralizer of g of the group G.

Lemma 3. *Let y be a cycle with maximal length in A_n and $B^y(x)$ a loop stable by y-conjugation. Let us take $\delta \in B^y(x)$, we have that*

1. *For every $z \in C_{A_n}(y)\delta$ we have that $[\delta, y] = [z, y]$.*
2. *For every $z \in \delta C_{A_n}(y)$ we have that $[z, y] \in B^y(x)$.*

Proof. (1) is evident. To prove (2), as $C_{A_n}(y) = \langle y \rangle$ we have that

$$[\delta, y]^y = y^{-1}\delta^{-1}y^{-1}\delta yy = [\delta y, y],$$

and therefore, it is also true for every power of y. □

Using Lemma 3, we know that if we consider an element δ in a loop $B^y(x)$ stable by y-conjugation, every element in the set $C_{A_n}(y)\delta$ produces the same element when it is commuted by y. Note that δ is the only element in the set $C_{A_n}(y)\delta$ which belongs to $B^y(x)$.

Furthermore, every element in the set $\delta C_{A_n}(y)$ belongs to the loop $B^y(x)$ when it is commuted by y and since y is a cycle with maximal length in A_n, we have that

$$\delta C_{A_n}(y) = \{[\delta, y]^{y^j} \mid j = 1, ..., o(\delta)\}.$$

Therefore condition (2) in Lemma 3 is necessary and sufficient to guarantee that the loop $B^y(x)$ is stable by y-conjugation.

Let us study the amount of conjugated loops in an alternating group A_p, with p prime.

Lemma 4. *Let p be a prime number and $y \in A_p$ a p-cycle. If the loop $B^y(x)$ is not stable by y-conjugation, it has exactly p conjugated loops in the set $S := \{B^y(x) \mid x \in A_p\}$.*

Proof. Let us consider the following action

$$\begin{aligned} \phi : \langle y \rangle \times S &\longrightarrow S \\ (y, B^y(x)) &\mapsto (B^y(x))^y \end{aligned}$$

We have that $\mid Orb(B^y(x)) \mid$ is exactly $\langle y \rangle / \mid Stab_{\langle y \rangle}(B^y(x)) \mid$.

Then if $B^y(x)$ is not stable by y-conjugation, we have that $Stab_{\langle y \rangle}(B^y(x)) = e$ and then $\mid Orb(B^y(x)) \mid = p$. □

Fix an element y in an alternating group A_n, $n \geq 5$ and consider the loop $B^y(x)$ associated to the element x in A_n, we have that

$$B^y(x) := \{E_{k_1}(x, y), ..., E_{k_2-1}(x, y)\},$$

where $E_{k_2}(x, y) = E_{k_1}(x, y)$.

Let us fix z an element in the loop $B^y(x)$, since $z = [\tau, y]$ for some element $\tau \in B^y(x)$, we have that $z = [\sigma\tau, y]$ for every $\sigma \in C_{A_n}(y)$. Therefore, the set of elements that, when commuted by y, produces z as a result is

$$A := \{\sigma\tau \mid \sigma \in C_{A_n}(y)\}.$$

Since z and τ are elements in $B^y(x)$, we have that there is only one element in A which also belongs to $B^y(x)$: τ.

Then, for every element z_1 in the loop $B^y(x)$, we have that there is only one element z_2 in $B^y(x)$ such that, when commuted by y, the result is z_1 and there are $\mid C_{A_n}(y) \mid -1$ elements outside of the loop $B^y(x)$ such that commuted by y gives as a result z_1.

Definition 3. *Given an element y in an alternating group A_n, $n \geq 5$, we define the annihilator of y as the set of elements x in A_n such that there exists $k \in \mathbb{N}$ with $E_k(x, y) = e$. We denote this set by $\mathcal{T}_y$.*

The annihilator of y is the set of elements in A_n whose chain 'finishes' in the identity element. If $\mathcal{C}_y$ defines the set of elements in A_n whose chain goes to a loop different from the identity element, we have that

$$A_n = \mathcal{T}_y \cup \mathcal{C}_y.$$

We also know that $\mathcal{C}_y = \cup_{i=0}^{\alpha(y)} \mathcal{C}_y^i$, where $\mathcal{C}_y^0$ is the set of non-identity elements that belong to the loop $B^y(x)$, $\mathcal{C}_y^1$ is the set of elements in A_n which do not belong to $\mathcal{C}_y^0$ but its commutator with y belongs to $\mathcal{C}_y^0$ and, inductively,

$$\mathcal{C}_y^{i+1} := \{x \in A_n \backslash \mathcal{C}_y^i \mid [x, y] \in \mathcal{C}_y^i\}.$$

Note that there exists an index $\alpha(y) \in \mathbb{N}$ such that $\mathcal{C}_y^{\alpha(y)+1} = \emptyset$.

We performed a brute-force search (using GAP) to study the length of the y-Engel chains that finishes in the identity element for small alternating groups A_n, $5 \leq n \leq 14$.

The results we obtained were that the maximal length of these chains were 2 or 3 for the considered alternating groups. We summarize all the information in Table 1.

Table 1. Computational results for Engel Chains' length.

Alternating Group	Max. Length
A_5	2
A_6	2
A_7	2
A_8	2
A_9	3
A_{10}	3
A_{11}	2
A_{12}	2
A_{13}	2
A_{14}	2

This output is quite interesting as it seems to indicate that the y-Engel Chains that finish in the identity element are usually short.

In the following lines, we prove that under certain conditions, the maximal length of an Engel Chain that end in the identity element is 2. Note that $N_{A_n}(C_{A_n}(y))$ denotes the normalizer of $C_{A_n}(y)$ in A_n.

Lemma 5. *Let us consider the group A_n, $n \geq 5$ odd and take $y = (1, 2, ..., n)$, a cycle with maximal length in A_n. We have that $C_{A_n}(y) = \langle y \rangle$ and that $\mid N_{A_n}(C_{A_n}(y)) \mid$ is either $n\varphi(n)$ or $n\varphi(n)/2$, where φ is the Euler's totient function.*

Proof. The number of conjugated elements of an n-cycle in S_n is $(1/n)V_n^n = (n-1)!$. Then, $\mid S_n : C_{S_n}(y) \mid = (n-1)!$. We have that

$$\mid C_{S_n}(y) \mid = \frac{\mid S_n \mid}{\mid Cl_{S_n}(y) \mid} = \frac{n!}{(n-1)!} = n.$$

Since $\mid \langle y \rangle \mid = n$, we have that $C_{S_n}(y) = \langle y \rangle$. In the group $\langle y \rangle$, there exist exactly $\phi(n)$ elements with the same decomposition as a product of disjoint cycles as y, so we have that $\mid N_{S_n}(\langle y \rangle) \mid = n\varphi(n)$.

By definition, $N_{A_n}(\langle y \rangle) = \{x \in A_n \mid y^x \in \langle y \rangle\}$. If for every i with $gcd(i, n) = 1$ we have that the elements y and y^i are conjugated in A_n, the number of groups in A_n conjugated to the group $\langle y \rangle$ would be half of the number of groups in S_n conjugated to $\langle y \rangle$. So $N_{A_n}(\langle y \rangle) = N_{S_n}(\langle y \rangle)$ and then

$$\mid N_{A_n}(\langle y \rangle) \mid = n\varphi(n).$$

If half of the powers of y are conjugated to y in A_n, we have that there exists $\sigma \in S_n \backslash A_n$ such that $\sigma \in N_{S_n}(\langle y \rangle)$. Then,

$$\mid N_{A_n}(\langle y \rangle) \mid = \frac{\mid N_{S_n}(\langle y \rangle) \mid}{2} = \frac{n\varphi(n)}{2}.$$

□

Lemma 6. *Let p be a prime number greater than 3. Let us consider y, a cycle of maximal length in A_p. The annihilator of y, $\mathcal{T}_y$, in A_p is the group $N_{A_p}(\langle y \rangle)$.*

Proof. Consider $Z = \langle y \rangle = C_{A_p}(y)$ and $N_1 = N_{A_p}(Z)$. We define $N_2 := \{x \in A_n \mid Z^x \subset N_1\}$ and inductively

$$N_r := \{x \in A_n \mid Z^x \subset N_{r-1}\}.$$

Note that $E_3(x,y) = 1$ if and only if $E_2(E_1(x,y),y) = e$, that is, $E_1(x,y) \in N_1$. Then, $x^{-1}y^{-1}xy$ is an element of N_1 and therefore $y \in Z \subset N_1$; $(y^{-1})^x$ is an element of N_1, that is, $Z^x \subset N_1$.

We have proved that $x \in N_2$ if an only if $E_3(x,y) = 1$. We will prove by induction that $E_{r+1}(x,y) = 1$ if an only if $x \in N_r$.

$E_{r+1}(x,y) = 1$ if and only if $E_r(E_1(x,y),y)$ that is (by induction), $E_1(x,y) \in N_{r-1}$ and therefore, $[x,y] \in N_{r-1}$.

Then $(y^{-1})^x \in N_{r-1}$, that is, $Z^x \subset N^{r-1}$ and by definition we have that $x \in N_r$.

We have two chains:

- $Z \subset N_1 \subset N_2 \subset N_3 \subset ...$
- $Z \subset N_{A_p}(Z) = N_1 \subset N_{A_p}(N_1) = \tilde{N_2} \subset N_{A_p}(N_2) = \tilde{N_3} \subset ...$

Since p is a prime number we have that $Z \in Syl_p(A_p)$ and, since N_1 is selfnormalizer, we have that $\tilde{N_2} = N_1$.

If we take x an element in N_2, we have that $Z^x \subset N_1$ and $Z, Z^x \in Syl_p(N_1)$. Then we have that $Z = Z^x$ and therefore $x \in N_1$. So, $N_1 = N_2$.

Since $\mathcal{T}_y = \cup_{i \geq 1} N_i$, we have that

$$\mathcal{T}_y = N_1 = N_{A_p}(\langle y \rangle).$$

□

Lemma 7. *Let n be a positive integer such that $gcd(n, \varphi(n)) = 1$ and let y be a n-cycle in A_n. The annihilator of y, $\mathcal{T}_y$, in A_n is the group $N_{A_n}(\langle y \rangle)$.*

Proof. Let p_i be a prime divisor of n. Given $P_i \in Syl_{p_i}(\langle y \rangle)$, we have that $P_i \trianglelefteq N_{A_n}(\langle y \rangle)$ and since $gcd(n, \varphi(n)) = 1$ we have that $\langle y \rangle$ is the only subgroup of $N_{A_n}(\langle y \rangle)$ with order n.

Using the arguments from Lemma 5, we have that $N_1 = N_2$. □

Corollary 1. *Let n be a positive integer such that $gcd(n, \varphi(n)) = 1$ and y be a cycle of maximal length in A_n. Then the maximal length of an Engel Chain $E^y(x) \subset \mathcal{T}_y$ which ends in the identity element is 2.*

Proof. If $E_m(x,y) = e$ we have that $E_{m-1}(x,y) \in \langle y \rangle$. Also we have that $E_{m-2}(x,y) \in N_{A_n}(\langle y \rangle)$.

Thanks to Lemma 7, we have that $N_{A_n}(\langle y \rangle)$ is self-normalizing. Then the maximal length of the chain $E^y(x)$ is $m - (m-2) = 2$. □

3. Engel Graphs

Let y be a fixed element in an alternating group A_n, with $n \geq 5$ and a $m \geq 1$, let us consider the following set of Engel words of length m:

$$E_m(y) := \{E_m(x,y) \mid x \in A_n\}.$$

Since for every $m \geq 1$ we have that $E_{m+1}(y) \subset E_m(y)$, $\{E_m(y)\}_{m\geq 0}$ is a descending chain of subsets in A_n.

Let us fix $m \geq 1$ and consider the set $E_m(y)$ as $\{[x,y] \mid x \in E_{m-1}(y)\}$, where $E_0 = A_n$. Then, if $x, z \in E_{m-1}(y)$ we have that

$$[x,y] = [z,y] \quad \text{if and only if} \quad C_{A_n}(y)x = C_{A_n}(y)z.$$

Let us consider the set $\Omega_m^y := \{C_{A_n}(y)x \mid x \in E_{m-1}(y)\}$. We can define the following map

$$\begin{array}{rccc} \varphi_m : & \Omega_m^y & \longrightarrow & E_m(y) \\ & C_{A_n}(y)x & \mapsto & [x,y] \end{array} \tag{1}$$

It is easy to see that for every $m \geq 1$ and every element $y \in A_n$, $n \geq 5$, the map φ_m is well defined and bijective.

Then, we can study the sets $E_m(y)$ by working with the set Ω_1^y of all right cosets of $C_{A_n}(y)$ in A_n.

Note that as $\{\Omega_m^y\}_{m\geq 1}$ is a descending chain of sets and A_n is a finite group, there exists $m \in \mathbb{N}$ such that $\Omega_m^y = \Omega_{m+1}^y$.

We are going to define a directed graph which will allow us the study of Engel words in A_n. Let us consider the set of nodes $V_n^y := \Omega_1^y$ and let us define the set of arrows $\mathbb{A}$ by the following relation:

- Given $z_1, z_2 \in V_n^y$, there exists an arrow from z_1 to z_2 if an only if $C_{A_n}(y)[z_1,y] = C_{A_n}(y)z_2$.

Definition 4. *Let y be an element in an alternating group A_n, the graph $(V_n^y, \mathbb{A})$ is called Engel graph associated to the element y and the group A_n.*

It is possible to use this graph in the study of Engel words in an alternating group as:

- If we consider a path of length k in the graph, starting in the node $C_{A_n}(y)z_1$ and finishing in the node $C_{A_n}(y)z_{k+1}$, we have that $E_k(z_1,y) = [z_{k+1},y]$. Once the graph is built, it is possible to easily compute Engel words of high lengths.
- Reciprocally, if we want to compute $E_k(x,y)$, it is enough to consider a path of length k starting in the node $C_{A_n}(y)x$ and commute by y any element of the coset associated to the last node of the path $C_{A_n}(y)z_{k_1}$. We have that
$$E_k(x,y) = [z_{k-1},y].$$
- We can study the 'dynamic' of the set $\{E_m(\cdot,y)\}_{m\geq 0}$ by studying the 'dynamic' of the graph $(V_n^y, \mathbb{A})$.

Once the graph is constructed, we want to use it to know whether or not an element in the alternating group A_n, $n \geq 5$, can be written as an Engel word of type $E_m(\cdot,y)$ for $m \geq 1$. The following lemma shows the relation between the graph $(V_n^y, \mathbb{A})$ and the fact of an element in the alternating group being an Engel word of arbitrary length.

Lemma 8. *Let φ_1 be the map defined in (1) with $m = 1$. If (W, β) is a directed cycle of $(V_n^y, \mathbb{A})$, every element in the set $\varphi_1(W)$ can be written as an Engel word of arbitrary length.*

Proof. Consider (W, β), a directed cycle in the Engel graph $(V_n^y, \mathbb{A})$.

Fixing an arbitrary element $C_{A_n}(y)x$ in W, we have that

$$\varphi_1(W) := \{E_k(x,y) \mid k \in \mathbb{N}\}.$$

As W is a directed cycle, there exists $k_1 \in \mathbb{N}$ such that $[x,y] = E_{k_1}(x,y)$.

Take an arbitrary $m \in \mathbb{N}$ and a permutation σ in $\varphi_1(W)$. We have that $\sigma = [z,y]$ for $z \in C_{A_n}(y)x$ and there exists $k_2 \in \mathbb{N}$ such that $[z,y] = E_{k_2}(z,y) = E_{2k_2}(z,y) = ...E_{rk_2}(z,y)$, with $r \in \mathbb{N}$.

It is enough to take $k_2 > m$ to get that $\sigma = E_m(\tau, y)$ for some $\tau \in A_n$. □

Lemma 8 implies that given an alternating group A_n, $n \geq 5$ and y an element in A_n, if we compute φ_1 of the directed cycles in the Engel graph we get a subset of A_n in which every element can be written as an Engel word of arbitrary length.

Corollary 2. *If (W, β) is a directed cycle of $(V_n^y, \mathbb{A})$ and φ_1 the map defined in (1) with $m = 1$, every element $\varphi_1(W)^{S_n}$ can be written as an Engel word of arbitrary length in A_n.*

Proof. This result can be directly deduced from Reference [13] and Lemma 8. □

The following results shows some of the properties that Engel Graphs have.

Lemma 9. *If $m \geq n$ and $\phi : A_n \longrightarrow A_m$ is the natural embedding, the image by ϕ of a directed cycle in an Engel graph $(V_n^y, \mathbb{A})$, is a directed cycle in the Engel graph $(V_m^y, \mathbb{B})$.*

Proof. Fix $y \in A_n$ and let W_1 be a directed cycle of the Engel graph $(V_n^y, \mathbb{A})$. Given a node $C_{A_n}(y)x$ of W_1, we can consider the directed cycle W_2 of $(V_m^y, \mathbb{B})$ that contains the node $C_{A_m}(y)x$.

If there exists an arrow between two nodes x, z of W_1, we have that

$$C_{A_n}(y)[x,y] = C_{A_n}(y)z.$$

Then $[x,y]z^{-1} \in C_{A_n}(y) \subset C_{A_m}(y)$ for every $m \geq n$. Then there is an arrow between the nodes $\phi(x)$ and $\phi(y)$ in W_2. As W_1 is a directed cycle, we have that W_2 is also a directed cycle of the same length that W_1. □

Corollary 3. *Every element in A_n that can be written as an Engel word of arbitrary length in A_n, is also an Engel word of arbitrary length in A_m, for every $m \geq n$.*

A sufficient condition for two Engel graphs to be isomorphic is presented in the following result.

Lemma 10. *If $z \in Cl_{S_n}(y)$ we have that the Engel graphs $(V_n^y, \mathbb{A})$ and $(V_n^z, \mathbb{B})$ are isomorphic.*

Proof. Denote $z := y^x$ for some $x \in S_n$. We define the next map

$$\begin{aligned} \phi : V_n^y &\longrightarrow V_n^z \\ C_{A_n}(y)\sigma &\mapsto C_{A_n}(z)\sigma^x \end{aligned}$$

If $C_{A_n}(y)x_1 = C_{A_n}(y)x_2$, we have that $x_1x_2^{-1} \in C_{A_n}(y)$. Then

$$(x_2x_1^{-1})^x y^x (x_1x_2^{-1})^x = y^x,$$

so $C_{A_n}(z)x_1^x = C_{A_n}(z)x_2^x$ and then ϕ is injective.

Surjectivity is obvious, so ϕ is a bijection.

Consider two nodes $C_{A_n}(y)x_1$ and $C_{A_n}(y)x_2$ in $(V_n^y, \mathbb{A})$, such that there is an arrow from $C_{A_n}(y)x_1$ to $C_{A_n}(y)x_2$, that is $C_{A_n}(y)[x_1.y] = C_{A_n}(y)x_2$.

We have that

$$x_2[x_1,y]^{-1}y[x_1,y]x_2^{-1}=y,$$

and then

$$(x_2[x_1,y]^{-1})^x y^x([x_1,y]x_2^{-1})^x=y^x,$$

so

$$C_{A_n}(z)[x_1^x,z]=C_{A_n}(z)x_2^x.$$

If there is an arrow between two nodes in $(V_n^y,\mathbb{A})$, there is also an arrow between the image of these nodes by ϕ in $(V_n^z,\mathbb{B})$. Then ϕ is a isomorphism of graphs. □

4. Engel Graphs for Small Alternating Groups

In this section, we use an Engel graph to prove that $A_n = E_m(A_n)$ for every $m \geq 1$ and every $n \leq 14$. We show here the explicit method performed for the alternating group A_5. For $6 \leq n \leq 14$, the procedure is analogous and we show the computational results at the end of this section.

Some results from Reference [13] are necessary to prove Theorem 2. We summarize those results in the following lemma.

Lemma 11. *Let $\sigma \in A_n$, $n \geq 5$, be a permutation of one of the following types: a product of two transpositions, a 3-cycle or a product of two 3-cycle . Then σ is an Engel word of arbitrary length in A_n.*

Consider $y := (1,2,3,4,5)$ a 5-cycle in A_5. We have that $C_{A_5}(y) = \langle y \rangle$, the cyclic group of order 5, so $V_5^y = \{\langle y \rangle x \mid x \in A_5\}$ is a set of order $\mid A_5/\langle y \rangle \mid = 12$.

Let us build the Engel graph $(V_5^y, \mathbb{A})$ in Figure 1. As we know, each node is associated to a coset module $C_{A_5}(y)$. We denote each node $C_{A_5}(y)\sigma$ by a permutation of the set $\{y^j\sigma \mid 1 \leq j \leq 4\}$.

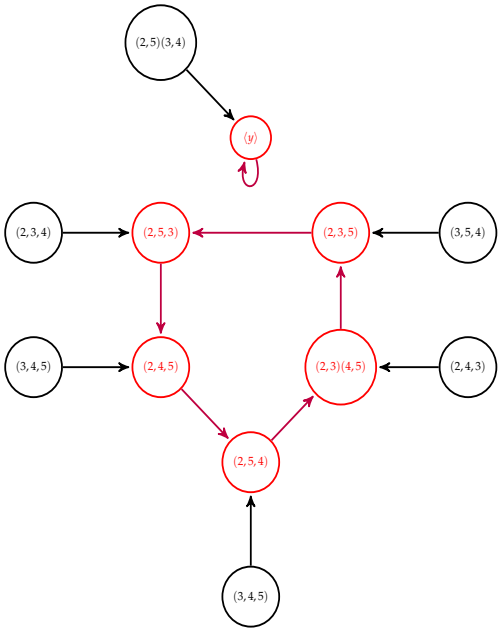

Figure 1. Engel Graph $(V_5^{(1,2,3,4,5)}, \mathbb{A})$.

The graph has two directed cycles. The first one, W_1, is a cycle with five elements and the other one, W_2, is only the identity node, $C_{A_5}(y)$.

By using Lemma 8, we just need to compute the sets $\varphi_1(W_1)$ and $\varphi_1(W_2)$ to get another set of elements in A_5 which can be written as an Engel word of arbitrary length in A_5. We have that:

$$\varphi_1(W_2) := \{e\},$$

$$\varphi_1(W_1) := \{(1,3,2,5,4),(1,3,5,4,2),(1,4,3,5,2),(1,5,2,4,3),(1,5,3,2,4)\}.$$

Thanks to Corollary 2 we have that every 5-cycle in A_5 can be written as an Engel word of arbitrary length in A_5.

This result together with Lemma 11 allows us to prove the following theorem:

Theorem 1. *Every element in A_5 can be written as an Engel word of arbitrary length. That is, for every $n \geq 1$ we have that $A_5 = E_n(A_5)$.*

It is also possible to use the adjacency matrix of the Engel graph to study which nodes belong to a directed cycle. If we consider Λ the adjacency matrix of the Engel graph $(V_n^y, \mathbb{A})$, it is known that the element a_{ij} of the matrix Λ^k gives us the number of directed paths of length k from the node i to the node j in the graph.

Computing the powers of the adjacency matrix and looking for the elements in the diagonal of Λ^k that are different to 0, we can compute which elements of the graph belong to a cycle.

Let us consider the graph $(V_5^y, \mathbb{A})$, with $y := (1,2,3,4,5)$. Its associated adjacency matrix Λ is:

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0
\end{pmatrix}$$

If we compute Λ^5, the result is:

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0
\end{pmatrix}$$

It is possible to see that there are 6 nodes in the Engel graph $(V_5^y, \mathbb{A})$ that belong to a directed cycle. However, as the size of the matrix corresponds to the number of nodes in the Engel graph, working with these kinds of matrices becomes impractical when we consider alternating groups of higher order. As an example, for $y = (1,2,3,4,5)$ in A_6 the set V_6^y has $\mid A_6 \mid / \mid C_{A_6}(y) \mid = 72$ elements. For A_7 and y a 7-cycle, we get 360.

To study bigger alternating groups, we used GAP to compute the directed cycles $\{W_k\}$ of the Engel graph associated to the group A_n and the element $y \in A_n$.

Later, we computed the set $\varphi_1(W_k)$ for each directed cycle W_k in the graph $(V_5^y, \mathbb{A})$. Then, we find out which types of permutations belongs to $\cup_k \varphi_1(W_k)$. To finish, we list every type of permutations in A_n that does not belong to $\cup_k \varphi_1(W_k)$.

This final list contains every type of permutation that cannot be written as an Engel word of arbitrary length of type $E_m(x,y)^\sigma = E_m(x^\sigma, y^\sigma)$.

Let us fix a cycle y of maximal length in A_n, $5 \leq n \leq 14$. We use the previous algorithm to search the directed cycles of the Engel graph $(V_n^y, \mathbb{A})$ in order to see if Theorem 1 is also true for bigger alternating groups.

We will compute the set $\Omega := \cup_k \varphi_1(W_k)$, where $\{W_k \mid 1 \leq k \leq r\}$ is the set of directed cycles in the Engel graph and we will see what types of permutations do not appear in Ω.

- Using the algorithm described above in GAP for A_6 and $y = (1,2,3,4,5)$, we get that the types of permutations in A_6 which do not appear in Ω are

$$\{(1,2)(3,4), (1,2,3), (1,2,3)(4,5,6)\}.$$

  Applying Lemma 11, we can get Theorem 1 for the group A_6.
- If we take A_n, with $7 \leq n \leq 14$ and we repeat the same process for $y = (1,2,3,...,n)$, if n is odd but $y = (1,2,3,...,n-1)$ if n is even, there is only one type of permutation that does not appear in the set Ω: $\{(1,2)(3,4)\}$.

  And again, we can easily get the Theorem 1 for the groups A_n, with $7 \leq n \leq 14$.

We summarise all the results we have got computationally in Table 2.

Table 2. Computational results for Engel graphs

Group	Conj. Cl. Not Found	Run Time
A_5	$\{(1,2)(3,4)^{S_5}, (1,2,3)^{S_5}\}$	7 ms
A_6	$\{(1,2)(3,4)^{S_6}, (1,2,3)^{S_6}, (1,2,3)(4,5,6)^{S_6}\}$	18 ms
A_7	$\{(1,2)(3,4)^{S_7}\}$	40 ms
A_8	$\{(1,2)(3,4)^{S_8}\}$	201 ms
A_9	$\{(1,2)(3,4)^{S_9}\}$	4 s 12 ms
A_{10}	$\{(1,2)(3,4)^{S_{10}}\}$	40 s 809 ms
A_{11}	$\{(1,2)(3,4)^{S_{11}}\}$	5 min 37 s 139 m
A_{12}	$\{(1,2)(3,4)^{S_{12}}\}$	63 min 38 s 210 m
A_{13}	$\{(1,2)(3,4)^{S_{13}}\}$	21 h 6 min 54 s
A_{14}	$\{(1,2)(3,4)^{S_{14}}\}$	approx. 12 days

Theorem 2. *Every element in an alternating group A_n, $5 \leq n \leq 14$, can be written as an Engel word of arbitrary length in A_n. That is,*

$$A_n = E_m(A_n),$$

for every $m \geq 1$.

In this work, we have provided two new approaches that can be used in the study of Engel words in alternating groups: Engel chains and Engel graphs. Using them (and GAP), we have also proved that every element in an alternating group A_n, $5 \leq n \leq 14$, can be written as an Engel word of arbitrary length.

It is still unknown whether Theorem 2 holds for $n > 14$. However, computational results seems to indicate some consistency in the "behaviour" of the Engel words in an alternating group and it is

possible that a similar theorem holds for any alternating group A_n, $n \geq 5$. The techniques proposed in this paper might be helpful in the further study of the general problem.

Funding: This work has been partially supported by BES-2011-044790 (research fellowship associated to project MTM2010-18370-C04-01) and GRUPIN 14-142.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Dehn, M. Uber die topologie des dreidimensionalen raumes. *Math. Ann.* **1910**, *69*, 137–168. (In German) [CrossRef]
2. Artin, E. The theory of braids. *Ann. Math.* **1947**, *48*, 101–126. [CrossRef]
3. David B.A.; Epstein, M.S.; Paterson, J.W.; Cannon, D.F.; Holt, S.V.; Levy, W.P. Thurston. In *Word Processing in Groups*, 1st ed.; A K Peters/CRC Press: Boca Raton, FL, USA, 1992.
4. Ko, K.H.; Lee, S.J.; Cheon, J.H.; Han, J.W.; Kang, J.; Park, C. New public-key cryptosystem using braid group. In *Advances in Cryptology—CRYPTO 2000*; Bellare, M., Ed.; Lecture Notes in Computer Science 1880; Springer: Berlin, Germany, 2000; pp. 166–183.
5. Garside, F.A. The braid group and other groups. *Quart. J. Math. Oxf.* **1969**, *20*, 235–254. [CrossRef]
6. Hofheinz, D.; Steinwandt, R. A practical attack on some braid group based cryptographic primitives. In *Public Key Cryptography—PKC2003*; Desmedt, Y.G., Ed.; Lecture Notes in Computer Science 2384; Springer: Berlin, Germany, 2002; pp. 176–189.
7. Anshel, I.; Anshel, M.; Goldfeld, D. An algebraic methodfor public-key cryptography. *Math. Res. Lett.* **1999**, *6*, 287–291. [CrossRef]
8. Ore, O. Some Remarks on Commutators. *Proc. Am. Math. Soc.* **1951**, *2*, 307–314. [CrossRef]
9. Wilson, J.S. *First-Order Group Theory*; Infinite Groups (1994); Gruyter: Berlin, Germany, 1996; pp. 301–314.
10. Martinez, C.; Zelmanov, E.I. Product of powers in finite simple groups. *Isr. J. Math.* **1996**, *96*, 469–479. [CrossRef]
11. Saxl, J.; Wilson, J.S. A note on powers in simple groups. *Math. Proc. Camb. Philos. Soc.* **1997**, *122*, 91–94. [CrossRef]
12. Liebeck, M.W.; O'Brien, E.A.; Shalev, A.; Tiep, P.H. The Ore Conjecture. *J. Eur. Math. Soc.* **2010**, *12*, 939–1008. [CrossRef]
13. Carracedo, J.M. Engel Words in Alternating Groups. *J. Algebra Appl.* **2017**, *16*, 1750021. [CrossRef]