Monatshefte für Mathematik (2021) 196:431–455
https://doi.org/10.1007/s00605-021-01514-y

Rigid commutators and a normalizer chain

Riccardo Aragona[1] · **Roberto Civino**[1] · **Norberto Gavioli**[1] · **Carlo Maria Scoppola**[1]

Received: 26 November 2020 / Accepted: 5 January 2021 / Published online: 15 January 2021

Abstract
The notion of rigid commutators is introduced to determine the sequence of the logarithms of the indices of a certain normalizer chain in the Sylow 2-subgroup of the symmetric group on 2^n letters. The terms of this sequence are proved to be those of the partial sums of the partitions of an integer into at least two distinct parts, that relates to a famous Euler's partition theorem.

Keywords Symmetric group on 2^n elements · Elementary abelian regular subgroups · Sylow 2-subgroups · Normalizers · Euler's partition theorem

Mathematics Subject Classification 20B30 · 20B35 · 20D20 · 11P81 · 05A17

Communicated by John S. Wilson.

All the authors are members of INdAM-GNSAGA (Italy) and of the group "Crittografia e Codici" of the Italian Mathematical Union. R. Civino is partially funded by the Centre of Excellence EX-EMERGE at University of L'Aquila. N. Gavioli is a member of the Centre of Excellence EX-EMERGE at University of L'Aquila.

✉ Roberto Civino
roberto.civino@univaq.it

Riccardo Aragona
riccardo.aragona@univaq.it

Norberto Gavioli
norberto.gavioli@univaq.it

Carlo Maria Scoppola
carlo.scoppola@univaq.it

[1] Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica, Università degli Studi dell'Aquila, Via Vetoio, 67100 Coppito, AQ, Italy

1 Introduction

In a recent paper [5], the authors observed a rather surprising coincidence between the sequence of integers

$$1, 2, 4, 7, 11, 16, 23, 32, 43, 57 \ldots$$

representing the partial sums of the famous sequence $\{b_j\}$ of the number of partitions of the integer j into at least two distinct parts, already studied by Euler [15], and a sequence of group-theoretical invariants. Our sequence arises in connection with a problem in algebraic cryptography, namely the study of the conjugacy classes of affine elementary abelian regular subgroups of the symmetric group on 2^n letters [4,9,10]. This is relevant in the cryptanalysis of block ciphers, since it may trigger a variation of the well-known *differential attack* [7]: a statistical attack which allows us to recover information on the secret unknown key by detecting a bias in the distribution of the *differences* on a given set of ciphertexts when the corresponding plaintext difference is known. In particular, if $\mathbb{F}_2^n$ serves as the message space of a block cipher (see e.g. [12]) which has been proven secure with respect to differential cryptanalysis [22] and if T represents the translation group on $\mathbb{F}_2^n$, any conjugate of T can be potentially used to define new alternative operations on $\mathbb{F}_2^n$ for a successful differential attack [11]. In [5], on the basis of the aforementioned motivation, the authors studied a chain of normalizers, which begins with the normalizer N_n^0 of T in a suitable Sylow 2-subgroup Σ_n of $\mathrm{Sym}(2^n)$ and whose ith term N_n^i is defined as the normalizer in Σ_n of the previous one. After providing some experimental as well as theoretical evidence, the authors conjectured [5, Conjecture 1] that the number $\log_2 \left|N_n^i : N_n^{i-1}\right|$ is independent of n for $1 \leq i \leq n-2$, and indeed is equal to the $(i+2)$th term of the sequence of the partial sums of the sequence[1] $\{b_j\}$ mentioned above [1, https://oeis.org/A317910]. In this paper we completely settle this conjecture. The first attempts to solve this problem were based on theoretical techniques which clashed with their own growing computational complexity. For this reason, we develop here a framework to approach the problem from a different point of view. In this new approach, indeed, we take into account both the imprimitivity and the nilpotence of the Sylow 2-subgroup Σ_n to represent its elements in terms of a special family of left-normed commutators, that we call *rigid commutators*, in a fixed set of generators. Any such commutator $[X]$ can be identified with a subset X of $\{1, \ldots, n\}$. The subgroups of Σ_n that can be generated by rigid commutators are called here *saturated subgroups*. A careful inspection led us to prove that the normalizers N_n^i are saturated subgroups. In particular, a set of generators of N_n^i can be obtained from a set of generators of N_n^{i-1} by adding the rigid commutators of the form $[X]$ for all X such that the elements of the complementary set of X in $\{1, \ldots, k\}$, where $k = \max X \leq n$, yield a partition of $i + 2 - n + k$ into at least two distinct parts. This is the key to prove the conjecture.

[1] The sequence $b_j + 1$ appears in several others areas of mathematics, from number theory to commutative algebra [14]. In particular, it was already known to Euler that $b_j + 1$ corresponds to the number of partitions of j into odd parts (see [15, Chapter 16] and [3, §3]). Several proofs of this Euler's partition theorem have been offered ever since [2,20,24], and several important refinements have been obtained [6,8,16,23,24].

The advantage of adopting rigid commutators is twofold. In the first place, they prove to be handy in calculations with the use of the *rigid commutator machinery*, a dedicated set of rules which we develop in this paper. Secondly, rigid commutators can be seen as factors in a *unique factorization formula* for the elements of any given saturated subgroup. This representation is crucial in showing that the normalizers N_n^i are saturated. By means of this result and of the machinery, we derive an algorithm which efficiently computes the normalizer chain.

The paper is organized as follows: in Sect. 2 some basic facts on the Sylow 2-subgroup Σ_n of $\mathrm{Sym}(2^n)$ are recalled. Section 3 is totally devoted to the introduction and the study of rigid commutators and to the construction of the rigid commutator machinery. In Sect. 4 the rigid commutator machinery is used to prove the conjecture on the normalizer chain previously mentioned [5, Conjecture 1]. In Sect. 5 it is shown that each term of the normalizer chain is a saturated group and an efficient procedure to determine the rigid generators of the normalizers is derived. An explicit construction of the normalizer chain in a specific case is provided in Section 6, and some open problems arising from computational evidence are discussed. Finally, some hints for future investigations are presented in Sect. 7.

2 The Sylow 2-subgroup of $\mathrm{Sym}(2^n)$

Let n be a non-negative integer. We start recalling some well-known facts about the Sylow 2-subgroup Σ_n of the symmetric group on 2^n letters.

Let us consider the set

$$\mathcal{T}_n = \left\{ w_1 \dots w_n \mid w_i \in \{0, 1\} \right\}$$

of binary words of length n, where $\mathcal{T}_0$ contains only the empty word. The infinite rooted binary tree $\mathcal{T}$ is defined as the graph whose vertices are $\bigcup_{j\geq 0} \mathcal{T}_j$ and where two vertices, say $w_1 \dots w_n$ and $v_1 \dots v_m$, are connected by an edge if $|m - n| = 1$ and $w_i = v_i$ for $1 \leq i \leq \min(m, n)$. The empty word is the root of the tree and it is connected with both the two words of length 1.

We can define a sequence $\{s_i\}_{i\geq 1}$ of automorphisms of this tree. Each s_i necessarily fixes the root, which is the only vertex of degree 2. The automorphism s_1 changes the value w_1 of the first letter of every non-empty word into $\bar{w}_1 \stackrel{\text{def}}{=} (w_1 + 1) \bmod 2$ and leaves the other letters unchanged. If $i \geq 2$, we define

$$(w_1 \dots w_n)s_i \stackrel{\text{def}}{=} \begin{cases} \text{empty word} & \text{if } n = 0 \\ w_1 \dots \bar{w}_i \dots w_n & \text{if } n \geq i \text{ and } w_1 = \dots = w_{i-1} = 0 \\ w_1 \dots w_n & \text{otherwise.} \end{cases} \tag{1}$$

In general, s_i leaves a word unchanged unless the word has length at least i and the letters preceding the ith one are all zero, in which case the ith letter is increased by 1 modulo 2. If $i \leq n$ and the word $w_1 \dots w_n \in \mathcal{T}_n$ is identified with the integer $1 + \sum_{i=1}^{n} 2^{n-i} w_i \in \{1, \dots, 2^n\}$, then s_i acts on $\mathcal{T}_n$ as the the permutation whose cyclic decomposition is

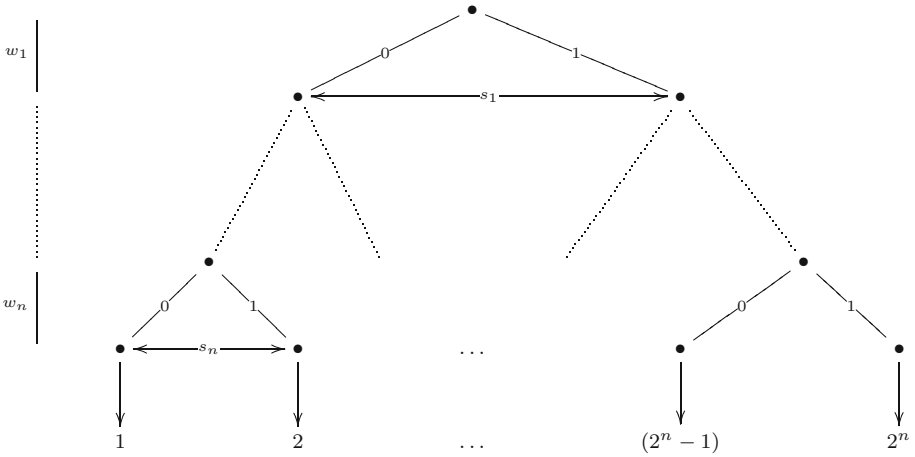

Fig. 1 The action of Σ_n on the subtree $\bigcup_{i=0}^{n} \mathcal{T}_i$

$$\prod_{j=1}^{2^{n-i}} (j, j+2^{n-i})$$

which has order 2. In particular, the group $\langle s_1, \ldots, s_n \rangle$ acts faithfully on the set $\mathcal{T}_n$, whose cardinality is 2^n, as a Sylow 2-subgroup Σ_n of the symmetric group $\mathrm{Sym}(2^n)$ (see also Fig. 1).

It is also well known that

$$\Sigma_n = \langle s_n \rangle \wr \Sigma_{n-1} = \langle s_n \rangle \wr \cdots \wr \langle s_1 \rangle \cong \wr_{i=1}^{n} C_2$$

is the iterated wreath product of n copies of the cyclic group C_2 of order 2.

The *support* of a permutation is the set of the letters which are moved by the permutation. We say that two permutations σ and τ are *disjoint* if they have disjoint supports; two disjoint permutations always commute.

The *closure*

$$S_i \stackrel{\text{def}}{=} \langle s_i \rangle^{\langle s_1, \ldots, s_i \rangle}$$

is generated by disjoint conjugates of s_i, hence S_i is an elementary abelian 2-group which is normalized by S_j if $j \leq i$. Moreover, $\Sigma_n = S_1 \ltimes \cdots \ltimes S_n \cong \Sigma_{n-1} \ltimes S_n$.

3 Rigid commutators

The *commutator* of two elements h and k in a group G is defined as $[h, k] \stackrel{\text{def}}{=} h^{-1}k^{-1}hk = h^{-1}h^k$. The *left-normed commutator* of the m elements $g_1, \ldots, g_m \in G$

is the usual commutator if $m = 2$ and is recursively defined by

$$[g_1, \ldots, g_{n-1}, g_m] \stackrel{\text{def}}{=} \big[[g_1, \ldots, g_{m-1}], g_m\big]$$

if $m \geq 3$. It is well known that the commutator subgroup G' of a finitely generated nilpotent group G can be generated by left-normed commutators involving only generators of G [19, III.1.11]. From now on, we will focus on left-normed commutators in $s_1, \ldots, s_n$. For the sake of simplicity, we write $[i_1, \ldots, i_k]$ to denote the left-normed commutator $[s_{i_1}, \ldots, s_{i_k}]$, when $k \geq 2$, and we also write $[i]$ to denote the element s_i.

Definition 1 A left-normed commutator $[i_1, \ldots, i_k]$ is called *rigid, based at* i_1 *and hanging from* i_k, if $i_1 > i_2 > \cdots > i_k$. Given a subset $X = \{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ such that $i_1 > i_2 > \cdots > i_k$, the *rigid commutator indexed by* X, denoted by $[X]$, is the left-normed commutator $[i_1, \ldots, i_k]$. We set $[X] \stackrel{\text{def}}{=} 1$ when $X = \emptyset$. The set of all the rigid commutators of Σ_n is denoted by $\mathcal{R}$ and we let $\mathcal{R}^* \stackrel{\text{def}}{=} \mathcal{R} \setminus \{[\emptyset]\}$.

At the end of this section we prove that every permutation in the Sylow 2-subgroup Σ_n can be expressed, in a unique way, as a product of the objects previously defined. To this purpose, we develop below a set of rules to perform computations with (rigid) commutators.

3.1 Rigid commutator machinery

Let $1 \leq i_1, i_2, \ldots, i_k \leq n$ be integers and let us consider the commutator $[i_1, \ldots, i_k]$. The following facts are easily checked.

Fact 1 Denoting by $i = \max\{i_1, \ldots, i_k\}$, the commutator $[i_1, \ldots, i_k]$ is a product of conjugates of s_i by way of elements in $\langle s_{i_1}, \ldots, s_{i_k} \rangle$ and thus it belongs to S_i. Any two such conjugates commute, since they belong to the same S_i.

Fact 2 As a direct consequence of Fact 1, if $\max\{i_1, \ldots, i_k\} = \max\{j_1, \ldots, j_l\}$ then $[i_1, \ldots, i_k]$ and $[j_1, \ldots, j_l]$ commute.

Note that if $g \in S_i$ and $h \in S_j$, then $[g, h] \in S_k$, where $k = \max\{i, j\}$, so $[g, h]^2 = 1$ since S_k is elementary abelian. It follows that $[g, h, h] = [g, h]^2[g, h, h] = [g, h^2] = [g, 1] = 1$. As a consequence we have:

Fact 3 If $k \geq 2$ and $i_j = i_{j+1}$ for some $1 \leq j \leq k-1$, then $[i_1, \ldots, i_k] = 1$.

The following result is crucial since it allows us to rewrite every commutator as a rigid commutator.

Lemma 1 *Let* $k \geq 2$ *and* $l \geq 1$ *be integers. If*

$$c \stackrel{\text{def}}{=} [[i_1, \ldots, i_k], [j_1, \ldots, j_l]]$$

is the commutator of the two rigid commutators $[i_1, \ldots, i_k]$ *and* $[j_1, \ldots, j_l]$*, then*

1. *the order of c divides 2, so* $c = [[j_1, \ldots, j_l], [i_1, \ldots, i_k]]$*;*

2. *if* $i_1 = j_1$, *then* $c = 1$;
3. *if* $l \geq 2$ *and* $i_k > j_l$, *then* j_l *can be dropped, i.e.*

$$c = [[i_1, \ldots, i_k], [j_1, \ldots, j_{l-1}]];$$

4. *if* $i_1 > j_1$, $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\} = \emptyset$, *and* $s \stackrel{\text{def}}{=} \max\{h \mid i_h > j_1\}$, *then*

$$c = [i_1, \ldots, i_s, j_1];$$

5. *if* $l \geq 2$ *and* $i_k = j_l$, *then*

$$c = [[i_1, \ldots, i_{k-1}], [j_1, \ldots, j_{l-1}], j_l];$$

6. *if* $i_s > j_1 \geq i_{s+1}$, *then*

$$c = [i_1, \ldots, i_s, j_1, h_1, \ldots, h_t],$$

where $h_1 > \cdots > h_t$ *and* $\{h_1, \ldots, h_t\} \stackrel{\text{def}}{=} \{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\}$. *Moreover,* $c = 1$ *if* $j_1 \in \{i_1, \ldots, i_k\}$.

Proof Let us prove each claim separately.

1. The claim $c^2 = 1$ depends on the fact that $c \in S_i$, where the index i is defined as $i \stackrel{\text{def}}{=} \max\{i_1, \ldots, i_k, j_1, \ldots, j_l\}$.
2. If $i_1 = j_1$, then both of $[i_1, \ldots, i_k]$ and $[j_1, \ldots, j_l]$ belong to S_{i_1} which is abelian, thus the claim follows.
3. Assume that $l \geq 2$ and $j_l < i_k$. In this case

$$\begin{aligned} c &= [i_1, \ldots, i_k][i_1, \ldots, i_k]^{[j_1, \ldots, j_{l-1}]s_{j_l}[j_1, \ldots, j_{l-1}]s_{j_l}} \\ &= [i_1, \ldots, i_k]\left([i_1, \ldots, i_k]^{[j_1, \ldots, j_{l-1}]}\right)^{s_{j_l}[j_1, \ldots, j_{l-1}]s_{j_l}}. \end{aligned}$$

The permutations $s_{j_l}[j_1, \ldots, j_{l-1}]s_{j_l}$ and $[i_1, \ldots, i_k]^{[j_1, \ldots, j_{l-1}]}$ are disjoint: the first one has support contained in $\left\{2^{n-j_l} + 1, \ldots, 2^{n-j_l+1}\right\}$ and the support of the second one is contained in

$$\left\{1, \ldots, 2^{n-\min(i_k, j_{l-1})+1}\right\} \subseteq \left\{1, \ldots, 2^{n-j_l}\right\}.$$

Hence

$$c = [i_1, \ldots, i_k][i_1, \ldots, i_k]^{[j_1, \ldots, j_{l-1}]} = [[i_1, \ldots, i_k], [j_1, \ldots, j_{l-1}]],$$

which proves the claim.
4. The claim follows by a repeated applications of items (3) and (1).

5. For every $x, y \in G \stackrel{\text{def}}{=} \langle s_n, \ldots, s_{i_l+1} \rangle$ the permutations x and $y^{s_{j_l}}$ are disjoint and so they commute. In particular, if $x^2 = 1$, then $[x, s_{j_l}]^2 = (xx^{s_{j_l}})^2 = x^2(x^2)^{s_{j_l}} = 1$. If $a, b \in G$ are such that $a^2 = b^2 = 1$, then

$$\begin{aligned}[[a, b], s_{j_l}] &= [abab, s_{j_l}] \\ &= ababa^{s_{j_l}} b^{s_{j_l}} a^{s_{j_l}} b^{s_{j_l}} = aa^{s_{j_l}} bb^{s_{j_l}} aa^{s_{j_l}} bb^{s_{j_l}} \\ &= [a, s_{j_l}][b, s_{j_l}][a, s_{j_l}][b, s_{j_l}] \\ &= [a, s_{j_l}]^{-1}[b, s_{j_l}]^{-1}[a, s_{j_l}][b, s_{j_l}] = [[a, s_{j_l}], [b, s_{j_l}]].\end{aligned}$$

For $a \stackrel{\text{def}}{=} [i_1, \ldots, i_{k-1}]$ and $b \stackrel{\text{def}}{=} [j_1, \ldots, j_{l-1}]$, we have

$$[[i_1, \ldots, i_{k-1}, j_l], [j_1, \ldots, j_{l-1}, j_l]] = [[i_1, \ldots, i_{k-1}], [j_1, \ldots, j_{l-1}], j_l],$$

as required.

6. An iterated use of items (1), (3) and (5) yields

$$c = [[i_1, \ldots, i_s], [j_1, \ldots, j_v], h_1, \ldots, h_t]$$

if $j_1 > i_{s+1} \geq h_1$, where the intersection $\{i_1, \ldots, i_s\} \cap \{j_1, \ldots, j_v\} = \emptyset$ is trivial, while, if $j_1 = h_1 = i_{s+1}$, then $c = [[[i_1, \ldots, i_s, h_1], h_1], \ldots, h_t]$. By Fact 3, the commutator $[[i_1, \ldots, i_s, h_1], h_1]$ is trivial, and so $c = 1$. We may then assume that $j_1 > i_{s+1} \geq h_1$. By (4), we obtain the equality $[[i_1, \ldots, i_s], [j_1, \ldots, j_v]] = [i_1, \ldots, i_s, j_1]$, therefore

$$c = [i_1, \ldots, i_s, j_1, h_1, \ldots, h_t]$$

as claimed. □

A repeated application of Lemma 1 shows that every left-normed commutator $[i_1, \ldots, i_k]$ can be written as a commutator $[j_1, \ldots, j_l]$, where $\{j_1, \ldots, j_l\} \subseteq \{i_1, \ldots, i_k\}$ and $j_h \geq j_{h+1}$ for all $1 \leq h \leq l-1$. If $j_h = j_{h+1}$ for some h, then Fact 3 shows that $[j_1, \ldots, j_h, j_{h+1}] = 1$, which in turn implies $[j_1, \ldots, j_l] = 1$. This fact is summarized in the following result.

Proposition 1 *Any left-normed commutator $[i_1, \ldots, i_k]$ can be written as a rigid commutator $[j_1, \ldots, j_l]$, for a suitable subset $\{j_1, \ldots, j_l\} \subseteq \{i_1, \ldots, i_k\}$.*

It is worth noticing here that rigid commutators are the images of P. Hall's basic commutators [18] under the presentation of the group Σ_n as a factor of the n-generated free group, once the order of the generators is reversed.

3.2 Saturated subgroups

In this section we give a representation of the elements of Σ_n in terms of rigid commutators.

Lemma 2 *The set of all the rigid commutators* $[X] \in \mathcal{R}$*, where* X *varies among the subsets of* $\{1, \ldots, n\}$ *such that* $\max(X) = i$*, is a basis for* S_i*.*

Proof Let $1 \leq i \leq n$. To prove the claim, we look at S_i as a 2^{i-1}-dimensional vector space over $\mathbb{F}_2$. Proceeding by backward induction on j, for $i \geq j \geq 1$, we show that the set of all the rigid commutators based at i and hanging from h, for some $h \geq j$, is linearly independent. When $j = i$ there is nothing to prove. Assume

$$\prod_{i>i_1>\cdots>i_t\geq j} [i, i_1, \ldots, i_t]^{e_{i,i_1,\ldots,i_t}} = 1, \tag{2}$$

where the exponents are in $\mathbb{F}_2$. We aim at proving that all the exponents are 0. From Eq. (2) we have

$$\prod_{i>i_1>\cdots>i_t>j} [i, i_1, \ldots, i_t]^{e_{i,i_1,\ldots,i_t}} \prod_{i>i_1>\cdots>i_{t-1}>i_t=j} [i, i_1, \ldots, i_{t-1}, j]^{e_{i,i_1,\ldots,i_{t-1},j}} = 1,$$

and so

$$\prod_{i>i_1>\cdots>i_t>j} [i, i_1, \ldots, i_t]^{e_{i,i_1,\ldots,i_t}} = \left[\left(\prod_{i>i_1>\cdots>i_{t-1}>i_t=j} [i, i_1, \ldots, i_{t-1}]^{e_{i,i_1,\ldots,i_{t-1},j}} \right), j \right]. \tag{3}$$

Note that if the permutation on the right-hand side of Eq. (3) is non-trivial, then it moves some x with $x > 2^{n-j}$, which is fixed by the one on the left-hand side. Hence the permutations on both sides are trivial. By induction, the exponents in the left-hand side of Eq. (3) are all 0. Now, the commutator map

$$[\cdot, s_j] \colon \langle s_{j+1}, \ldots, s_n \rangle \to \langle s_j, \ldots, s_n \rangle$$

is injective, hence the equality

$$\left[\left(\prod_{i>i_1>\cdots>i_{t-1}>i_t=j} [i, i_1, \ldots, i_{t-1}]^{e_{i,i_1,\ldots,i_{t-1},j}} \right), j \right] = 1$$

implies

$$\prod_{i>i_1>\cdots>i_{t-1}>i_t=j} [i, i_1, \ldots, i_{t-1}]^{e_{i,i_1,\ldots,i_{t-1},j}} = 1.$$

Again, by the inductive hypothesis, we find $e_{i,i_1,\ldots,i_{t-1},j} = 0$ for every choice of $i_1 > \cdots > i_{t-1}$. As the number of rigid commutators based at i equals the dimension of S_i, the proof is complete. □

We can now state our first main result as a straightforward consequence of Lemma 2. Let us call a *proper order* $\prec$ on $\mathcal{R}^*$ any total order refining the partial order defined by $[i_1, \ldots, i_t] \prec [j_1, \ldots, j_l]$ if $i_1 < j_1$. Here we denote by $\mathcal{P}_n$ the power set of $\{1, \ldots, n\}$.

Theorem 1 *Given a proper order $\prec$ in $\mathcal{R}^*$, every element $g \in \Sigma_n$ can be uniquely represented in the form*

$$g = \prod_{Y \in \mathcal{P}_n \setminus \{\emptyset\}} [Y]^{e_g(Y)},$$

where the factors are ordered with respect to $\prec$ and $e_g : \mathcal{P}_n \setminus \{\emptyset\} \to \{0, 1\}$ is a function depending on g.

Proof Since $\Sigma_n = S_1 \ltimes \cdots \ltimes S_n$, the claim is a straightforward consequence of Lemma 2. □

Some of the following corollaries are straightforward and their proof will be omitted.

Corollary 1 *If G is a subgroup of Σ_n containing k distinct rigid commutators, then $|G| \geq 2^k$.*

We now need a new concept which plays a key role in the remainder of this work.

Definition 2 A subset $\mathcal{G}$ of $\mathcal{R}$ is called *saturated* if $\mathcal{G} \cup \{[\emptyset]\}$ is closed under taking commutators and the subgroup $G \stackrel{\text{def}}{=} \langle\, \mathcal{G} \,\rangle \leq \Sigma_n$ is called a *saturated subgroup*.

Remark 1 A subgroup $G \leq \Sigma_n$ is saturated if and only if it can be generated by some subset $\mathcal{X}$ of $\mathcal{R}$: indeed G is also generated by the smallest saturated subset of $\mathcal{G} \cap \mathcal{R}$ containing $\mathcal{X}$.

Corollary 2 *Let $G \leq \Sigma_n$ be a saturated subgroup generated by a saturated set $\mathcal{G} \subseteq \mathcal{R}^*$ and let $\prec$ be any given proper order on $\mathcal{G}$. Every element $g \in G$ has a unique representation*

$$g = \prod_{c \in \mathcal{G}} c^{e_c(g)},$$

where the commutators in the product are ordered with respect to $\prec$ and $e_c(g) \in \{0, 1\}$. In particular $|G| = 2^{|\mathcal{G}|}$.

Corollary 3 *Let $G \leq \Sigma_n$ be a saturated subgroup generated by a saturated set $\mathcal{G} \subseteq \mathcal{R}^*$ and let $\prec$ any given proper order on $\mathcal{G}$. If the product $c_1 \cdots c_k \in G$, where $c_i \in \mathcal{R}^*$, and $c_1 \precneqq c_2 \precneqq \cdots \precneqq c_k$, then $c_i \in \mathcal{G}$ for all $1 \leq i \leq k$.*

Proof Note that since every rigid commutator belongs to some S_i, the group G has the semidirect product decomposition $G = (G \cap S_1) \ltimes \cdots \ltimes (G \cap S_n)$. In particular every element of G can be written as an ordered product of elements of $\mathcal{G}$. Write $c_1 \cdots c_k = g_1 \cdots g_t$ where $g_i \in \mathcal{G}$ and $g_1 \precneqq \cdots \precneqq g_t$. By Theorem 1, we have $k = t$ and $c_i = g_i \in \mathcal{G}$. □

The next statement follows immediately from Corollary 3.

Corollary 4 *Let $G \leq \Sigma_n$ be a saturated subgroup. If $g = g_1 \cdots g_n$, where $g_i \in S_i$ for $1 \leq i \leq n$, then $g \in G$ if and only if $g_i \in G \cap S_i$ for $1 \leq i \leq n$. Moreover if $g = h_1 \cdots h_n$, where $h_i \in S_i$ for $1 \leq i \leq n$, then $h_i = g_i$ for $1 \leq i \leq n$.*

4 Elementary abelian regular 2-groups and their chain of normalizers

A vector space T of dimension n over $\mathbb{F}_2$ acts regularly over itself as a group of translations. By way of this action, T can be seen as a regular elementary abelian subgroup of $\mathrm{Sym}(2^n)$, and any other regular elementary abelian subgroup of $\mathrm{Sym}(2^n)$ is conjugate to T in $\mathrm{Sym}(2^n)$ [13]. The normalizer of T in $\mathrm{Sym}(2^n)$ is the affine group $\mathrm{AGL}(T)$, where T embeds as the normal subgroup of translations. For this reason, we refer to any of the conjugates of T as a *translation subgroup* of $\mathrm{Sym}(2^n)$. Every chief series $\mathfrak{F} = \{T_i\}_{i=0}^n$ of T, where $1 = T_0 < T_1 < \cdots < T_n = T$, is normalized by exactly one Sylow 2-subgroup $U_{\mathfrak{F}}$ of $\mathrm{AGL}(T)$. In [21, Theorem p. 226] it is proved that every chief series $\mathfrak{F}$ of T corresponds to a Sylow 2-subgroup $\Sigma_{\mathfrak{F}}$ of $\mathrm{Sym}(2^n)$ containing T and having a chief series that intersects T in $\mathfrak{F}$. The correspondence $\mathfrak{F} \mapsto \Sigma_{\mathfrak{F}}$ is a bijection between the sets of the chief series of T and the set of Sylow 2-subgroups of $\mathrm{Sym}(2^n)$ containing T. In [5] it is also pointed out that $U_{\mathfrak{F}} = N_{\Sigma_{\mathfrak{F}}}(T) = \Sigma_{\mathfrak{F}} \cap \mathrm{AGL}(T)$. From now on the chief series $\mathfrak{F}$ will be fixed, and so, without ambiguity, we will write Σ_n and U_n to denote respectively $\Sigma_{\mathfrak{F}}$ and $U_{\mathfrak{F}}$. In [4] it is proved that U_n contains, as normal subgroups, exactly two conjugates of T, namely T and $T_{U_n} = T^g$, for some $g \in \mathrm{Sym}(2^n)$. It is also shown that the normalizer $N_n^1 = N_{\mathrm{Sym}(2^n)}(U_n)$ interchanges by conjugation these two subgroups and that N_n^1 contains U_n as a subgroup of index 2. In particular, $N_n^1 \leq \Sigma_n$. In the following section we will extend these results on T, U_n, N_n^1 to the entire chain of normalizers, which is defined below.

4.1 The normalizer chain

The *normalizer chain starting at T* is defined as

$$N_n^i \stackrel{\text{def}}{=} \begin{cases} U_n = N_{\Sigma_n}(T) & \text{if } i = 0, \\ N_{\Sigma_n}(N_n^{i-1}) & \text{if } i \geq 1. \end{cases} \tag{4}$$

In [5] the authors proved that $N_{\Sigma_n}(N_n^i) = N_{\mathrm{Sym}(2^n)}(N_n^i)$, for all $i \geq 0$, computed the normalizer chain for $n \leq 11$ by way of the computer algebra package GAP [17], and conjectured that the index $\left|N_n^{i+1} : N_n^i\right|$ does not depend on n for $n \geq i + 3$ [5, Conjecture 1]. In this section we prove this conjecture arguing by induction, by means of the rigid commutator machinery developed in Sect. 3.1. We start by defining

$$T \stackrel{\text{def}}{=} \langle\, t_1, \ldots, t_n \,\rangle$$

where

$$t_i \stackrel{\text{def}}{=} [s_i, s_{i-1}, \ldots, s_1] = [i, i-1, \ldots, 1] \in \mathcal{R}^*.$$

Lemma 3 *T is an elementary abelian regular subgroup of Σ_n. In particular, T is a translation subgroup of* $\mathrm{Sym}(2^n)$.

Proof T is a subgroup of Σ_n as it is generated by elements belonging to Σ_n. By item 6 of Lemma 1 it follows that $[t_i, t_j] = 1$, so that T is abelian. Note that $t_i^2 = 1$ as $t_i \in S_i$, and so T is elementary abelian of order at most 2^n. Let us now prove that T is transitive. Let $1 \leq x \leq 2^n$ be an integer represented as $x = 1 + \sum_{i=1}^{n} 2^{n-i} w_i$ in binary form and let $t = \prod_{i=1}^{n} t_i^{w_i}$. A direct check shows that t moves 1 to x. Since T has an orbit with 2^n elements and it has order at most 2^n, it follows that $|T| = 2^n$ and that every point stabilizer is trivial, therefore T is a regular permutation group on $\{1, \ldots, 2^n\}$. □

Let us now determine the permutations in Σ_n normalizing T. For $1 \leq j < i \leq n$ let us define $X_{ij} \stackrel{\text{def}}{=} \{1, \ldots, i\} \setminus \{j\}$ and

$$u_{ij} \stackrel{\text{def}}{=} [X_{ij}] = [i, \ldots, j+1, j-1, \ldots, 1] \in \mathcal{R}^*.$$

From now on we will set

$$\mathcal{U}_n \stackrel{\text{def}}{=} \left\{ t_1, \ldots, t_n, u_{ij} \mid 1 \leq j < i \leq n \right\} \subseteq \mathcal{R}^*.$$

Proposition 2 *The group $\langle \mathcal{U}_n \rangle$ is the normalizer of T in Σ_n, i.e.*

$$U_n = \left\langle T, u_{ij} \mid 1 \leq j < i \leq n \right\rangle.$$

Proof Let us set $U \stackrel{\text{def}}{=} \left\langle T, u_{ij} \mid 1 \leq j < i \leq n \right\rangle$ and let us prove that $U = U_n = N_{\Sigma_n}(T)$. By Lemma 1 we have

$$[t_h, u_{ij}] = \begin{cases} 1 & \text{if } h \neq j \\ t_i & \text{if } h = j. \end{cases}$$

This shows that $U \leq N_{\Sigma_n}(T) = U_n$ and that $\mathcal{U}_n$ is a saturated set. Therefore, from Corollary 2, $|U| = 2^{|\mathcal{U}_n|} = 2^{\frac{n(n+1)}{2}} = |U_n|$, which proves the claim. □

We aim at proving our second main result, providing the generators of the normalizer N_n^i in terms of rigid commutators. The result is proved by induction on $i \geq 1$.

Induction basis

Let us denote by η_n the rigid commutator based at n and hanging from 3 such that no intermediate integer is missing, i.e.

$$\eta_n \stackrel{\text{def}}{=} [n, n-1, \ldots, 3]. \tag{5}$$

We now prove that we can generate N_n^1 by appending η_n to the list $\mathcal{U}_n$ of the rigid commutators generating U_n.

Proposition 3 *If $n \geq 3$, then the group $\langle \mathcal{U}_n, \eta_n \rangle$ is the normalizer N_n^1 of U_n in Σ_n, i.e.*

$$N_n^1 = \left\langle T, u_{ij}, \eta_n \mid 1 \leq j < i \leq n \right\rangle.$$

Moreover, $\left|N_n^1 : U_n\right| = 2$.

Proof By Lemma 1,

$$[t_i, \eta_n] = \begin{cases} u_{n,2} & \text{if } i = 1 \\ t_n & \text{if } i = 2 \\ 1 & \text{otherwise} \end{cases} \quad \text{and} \quad [u_{ij}, \eta_n] = \begin{cases} u_{n,1} & \text{if } i = 2 \text{ and } j = 1 \\ 1 & \text{otherwise} \end{cases},$$

Thus the rigid commutator η_n belongs to $N_{\Sigma_n}(U_n)$, hence $\langle U_n, \eta_n \rangle \leq N_{\Sigma_n}(U_n)$. Moreover $U_n \cap S_n = \left\langle t_n, u_{n,1}, \ldots, u_{n,n-1} \right\rangle$ and so η_n, which is based at n, is such that $\eta_n \notin U_n$. The claim now follows from $\left|N_{\Sigma_n}(U_n) : U_n\right| = 2$ [4, Theorem 7]. □

Inductive step

Let $1 \leq b \leq n$ and let I be a (possibly empty) subset of $\{1, 2, \ldots, b-1\}$. We define the *rigid commutator based at b and punctured at I* as

$$\vee[b; I] \stackrel{\text{def}}{=} [\{1, \ldots, b\} \setminus I] \in \mathcal{R}^* \tag{6}$$

and, if $I = \{i_1, i_2, \ldots, i_k\}$ we also denote $\vee[b; I]$ by $\vee[b; i_1, i_2, \ldots, i_k]$.

For example, the permutation η_n defined in Eq. (5) is equal to $\vee[n; 2, 1]$.
We also define

$$\mathcal{W}_{ij} \stackrel{\text{def}}{=} \left\{ \vee[i; I] \in \mathcal{R}^* \;\middle|\; I \subseteq \{1, 2, \ldots, i-1\}, |I| \geq 2, \sum_{x \in I} x = j \right\} \tag{7}$$

for each $1 \leq i \leq n$ and j, and

$$\mathcal{N}_n^i \stackrel{\text{def}}{=} \begin{cases} \mathcal{U}_n & \text{if } i = 0 \\ \mathcal{N}_n^{i-1} \dot{\cup} \left(\dot{\bigcup}_{j=1}^{i} \mathcal{W}_{n+j-i,\, j+2} \right) & \text{for } i > 0. \end{cases} \tag{8}$$

Note that, if $j \leq i-2$, then $\left|\mathcal{W}_{i,j}\right| = b_j$, i.e. the number of partitions of j into at least two distinct parts. Our next goal is to prove that $N_n^i = \left\langle \mathcal{N}_n^i \right\rangle$ for each $0 \leq i \leq n-2$, where N_n^i is defined as in Eq. (4). Propositions 2 and 3 show that this is actually the case when $i \in \{0, 1\}$.

In order to prove the general result, we need the following reformulation of item 6 of Lemma 1 to compute commutators of rigid commutators written in punctured form.

Proposition 4 *Let $1 \leq a, b \leq n$ and let I and J subsets of $\{1, 2, \ldots, a-1\}$ and $\{1, 2, \ldots, b-1\}$ respectively. Then*

$$\left[\vee[a; I], \vee[b; J] \right] = \begin{cases} \vee[\max(a,b);\ (I \cup J) \setminus \{\min(a,b)\}] & \text{if } \min(a,b) \in I \cup J \\ 1 & \text{otherwise.} \end{cases}$$

Proof Let $c \stackrel{\text{def}}{=} \left[\vee[a; I], \vee[b; J] \right]$. If $a = b$, then $c = 1$. Without loss of generality, we can assume that $a > b$. By Lemma 1, if $b \notin I$, then $c = 1$. If $b \in I$, the claim follows from item 6 of Lemma 1. □

In the following facts, we summarize some properties that will be useful in the proof of the conjecture.

Fact 4 A commutator $\vee[a; J]$ such that $1 \leq a \leq n$ and $J \subseteq \{1, 2, \ldots, a-1\}$ belongs to $\mathcal{N}_n^i$ if and only if one of the following conditions is satisfied:

1. $J = \emptyset$, and so $\vee[a; J] = t_a$;
2. $|J| = 1$, and so $\vee[a; J] = u_{aj}$ where $J = \{j\}$;
3. $|J| \geq 2$, and $\sum_{j \in J} j \leq i + 2 - (n - a)$.

Fact 5 Note that for $2 \leq i \leq n-2$ the set $\mathcal{N}_n^i \cap (S_1 \ltimes \cdots \ltimes S_{n-1})$ is equal to $\mathcal{N}_{n-1}^{i-1}$. Indeed, at the ith iteration, the newly generated elements of $\mathcal{N}_n^i$, which are those in $\mathcal{N}_n^i \setminus \mathcal{N}_n^{i-1}$, are constructed by *lifting* the elements of $\mathcal{N}_n^{i-1} \setminus \mathcal{N}_n^{i-2}$, i.e. by replacing a rigid commutator based at j with the rigid commutator obtained by removing its left-most element, for $j \leq n$, and by adding some new rigid commutators based at n, in accordance with Eq. (8). Proceeding in this way it is easy to check that, disregarding all the commutators based at n in $\mathcal{N}_n^i$, the lifted elements are exactly the elements of $\mathcal{N}_{n-1}^{i-1}$. The reader is referred to Sect. 6 for explicit examples.

Fact 6 In the proof of Proposition 3 we showed that $[\mathcal{N}_n^1, \mathcal{N}_n^0] \subseteq \mathcal{N}_n^0 \cup \{[\emptyset]\}$. Assuming by induction on $2 \leq i \leq n-2$ that $[\mathcal{N}_{n-1}^{i-1}, \mathcal{N}_{n-1}^{i-2}] \subseteq \mathcal{N}_{n-1}^{i-2} \cup \{[\emptyset]\}$ and using Fact 5, we can conclude that

$$\begin{aligned} &[\mathcal{N}_n^i \cap (S_1 \ltimes \cdots \ltimes S_{n-1}), \mathcal{N}_n^{i-1} \cap (S_1 \ltimes \cdots \ltimes S_{n-1})] = \\ &[\mathcal{N}_{n-1}^{i-1}, \mathcal{N}_{n-1}^{i-2}] \subseteq \mathcal{N}_{n-1}^{i-2} \cup \{1\} = \mathcal{N}_n^{i-1} \cap (S_1 \ltimes \cdots \ltimes S_{n-1}) \cup \{[\emptyset]\}. \end{aligned}$$

Similarly,

$$\begin{aligned} &[\mathcal{N}_n^i \cap (S_1 \ltimes \cdots \ltimes S_{n-1}), \mathcal{N}_n^i \cap (S_1 \ltimes \cdots \ltimes S_{n-1})] \\ &\quad \subseteq \mathcal{N}_n^i \cap (S_1 \ltimes \cdots \ltimes S_{n-1}) \cup \{[\emptyset]\}. \end{aligned}$$

From the previous fact we have that, in order to prove by induction on i that $[\mathcal{N}_n^i, \mathcal{N}_n^{i-1}] \subseteq \mathcal{N}_n^{i-1} \cup \{[\emptyset]\}$ and that $[\mathcal{N}_n^i, \mathcal{N}_n^i] \subseteq \mathcal{N}_n^i \cup \{[\emptyset]\}$, it suffices to show that $[\mathcal{W}_{n,i+2}, \mathcal{N}_n^{i-1}] \subseteq \mathcal{N}_n^{i-1} \cup \{[\emptyset]\}$ and that $[\mathcal{W}_{n,i+2}, \mathcal{N}_n^i] \subseteq \mathcal{N}_n^i \cup \{[\emptyset]\}$. This is accomplished in the following result.

Lemma 4 *If $i \leq n-2$, then $[\mathcal{N}_n^i, \mathcal{N}_n^{i-1}] \subseteq \mathcal{N}_n^{i-1} \cup \{[\emptyset]\}$ and $[\mathcal{N}_n^i, \mathcal{N}_n^i] \subseteq \mathcal{N}_n^i \cup \{[\emptyset]\}$.*

Proof If $\vee[n; I] \in \mathcal{W}_{n,i+2} \subseteq \mathcal{N}_n^i \backslash \mathcal{N}_n^{i-1}$ and $\vee[a; J] \in \mathcal{N}_n^{i-1}$ then, by Proposition 4,

$$c \stackrel{\text{def}}{=} \left[\vee[n; I], \vee[a; J] \right] = \begin{cases} \vee[n;\ (I \cup J) \backslash \{a\}] & \text{if } a \in I \\ 1 & \text{otherwise.} \end{cases}$$

We may assume $a \in I$. From Fact 4, if $\vee[a; J]$ is as in case (3), we have

$$\begin{aligned} \sum_{x \in (I \cup J) \backslash \{a\}} x &\leq \sum_{x \in J} x + \sum_{x \in I} x - a \\ &\leq i + 1 - (n - a) + i + 2 - (n - n) - a \\ &= i + 2 - (n - i - 1) \\ &\leq i + 2 - 1 = i + 1, \end{aligned}$$

and so $c \in \mathcal{N}_n^{i-1}$. If $\vee[a; J]$ is as in case (1), i.e. $\vee[a; J] = t_a$, then we have

$$\sum_{x \in (I \cup J) \backslash \{a\}} x = \sum_{x \in I} x - a = i + 2 - a \leq i + 1$$

and so, also in this case, $c \in \mathcal{N}_n^{i-1}$. Finally, if $\vee[a; J]$ is as in case (2), i.e. $\vee[a; J] = u_{a,j}$, we have

$$\sum_{x \in (I \cup J) \backslash \{a\}} x \leq \sum_{x \in I} x - a + j = i + 2 - (a - j) \leq i + 1$$

and again $c \in \mathcal{N}_n^{i-1}$. Similar computations prove that, if $\vee[a; J] \in \mathcal{N}_n^i$, then also $c \in \mathcal{N}_n^i$. □

The following result is now straightforward.

Proposition 5 *The set $\mathcal{N}_n^i$ is a saturated set of rigid commutators and $\langle \mathcal{N}_n^i \rangle \leq N_{\Sigma_n}(\langle \mathcal{N}_n^{i-1} \rangle)$. Moreover, $|\langle \mathcal{N}_n^i \rangle| = 2^{|\mathcal{N}_n^i|}$.*

Proof The claim follows from Lemma 4, Fact 6 and Corollary 2. □

We conclude this section with our main result showing that the ith term of the normalizer chain is actually generated by the set $\mathcal{N}_n^i$ of rigid commutators defined in Eq. (8). We prove, indeed, that the inclusion $\langle \mathcal{N}_n^i \rangle \leq N_{\Sigma_n}(\langle \mathcal{N}_n^{i-1} \rangle)$ shown in the previous proposition is actually an equality.

Theorem 2 *For $i \leq n-2$, the group $\left\langle \mathcal{N}_n^i \right\rangle$ is the ith term N_n^i of the normalizer chain.*

Proof The cases $i = 0$ and $i = 1$ has been addressed respectively in Propositions 2 and 3. We assume by induction on $i \geq 2$ that $N_m^j = \left\langle \mathcal{N}_m^j \right\rangle$ for all $m \leq n$ whenever $j < i \leq m-2$. In particular

$$N_m^j \cap \Sigma_{m-1} = N_{m-1}^{j-1} = \langle \mathcal{N}_{m-1}^{j-1} \rangle .$$

Notice that

$$\begin{aligned} \left\langle \mathcal{N}_n^i \right\rangle \cap \Sigma_{n-1} &= \left\langle \mathcal{N}_{n-1}^{i-1} \right\rangle \\ &= N_{n-1}^{i-1} = N_{\Sigma_{n-1}}(N_{n-1}^{i-2}) \\ &= N_{\Sigma_{n-1}}(N_n^{i-1} \cap \Sigma_{n-1}) \\ &= N_{\Sigma_{n-1}}(N_n^{i-1} \cap \Sigma_{n-1}) \cap N_{\Sigma_{n-1}}(N_n^{i-1} \cap S_n) = N_{\Sigma_{n-1}}(N_n^{i-1}), \end{aligned}$$

where the first equality in the last line holds since the following inclusions

$$[\mathcal{N}_{n-1}^{i-1}, \mathcal{N}_n^{i-1}] \subseteq [\mathcal{N}_n^i, \mathcal{N}_n^{i-1}] \subseteq \mathcal{N}_n^{i-1} \cup \{[\emptyset]\}$$

imply that $N_{\Sigma_{n-1}}(N_n^{i-1} \cap \Sigma_{n-1}) \subseteq N_{\Sigma_{n-1}}(N_n^{i-1} \cap S_n)$. As S_n is abelian, we have

$$\begin{aligned} N_n^i &= N_{\Sigma_n}(N_n^{i-1}) = N_{\Sigma_{n-1} \ltimes S_n}(N_n^{i-1}) \\ &= N_{\Sigma_{n-1}}(N_n^{i-1}) N_{S_n}(N_n^{i-1}) = \left\langle \mathcal{N}_{n-1}^{i-1} \right\rangle N_{S_n}(N_n^{i-1}). \end{aligned} \tag{9}$$

We are then left to determine $N_{S_n}(N_n^{i-1}) = \left\{ x \in S_n \mid [x, \mathcal{N}_{n-1}^{i-1}] \subseteq N_n^{i-1} \cap S_n \right\}$. Let us point out that, by Eqs. (7) and (8), the groups

$$A \stackrel{\text{def}}{=} \left\langle \mathcal{N}_n^i \cap S_n \right\rangle \text{ and } B \stackrel{\text{def}}{=} \langle \bigcup_{j \geq i+1} \mathcal{W}_{n,\, j+2} \rangle$$

have trivial intersection and that $S_n = A \times B$. By Lemma 4 we have that A is a subgroup of $N_n^i \cap S_n$, for $1 \leq j \leq i$, so that $N_n^i = A \times H$ where

$$H \stackrel{\text{def}}{=} \left\{ x \in \langle \bigcup_{j \geq i+1} \mathcal{W}_{n,\, j+2} \rangle \;\middle|\; [x, \mathcal{N}_{n-1}^{i-1}] \subseteq N_n^{i-1} \cap S_n \right\}.$$

We denote a generic element of H by

$$x \stackrel{\text{def}}{=} \prod_{I \in \mathcal{I}} \vee[n; I]^{e_I} ,$$

where the product is taken over the set $\mathcal{I}$ of all the subsets $I \subseteq \{1, \ldots, n-1\}$ such that $\sum_{y \in I} y \geq i+3$. For $1 \leq l \leq n$ let $\mathcal{I}_l = \{I \in \mathcal{I} \mid \min(I) = l\}$. Let $u = u_{l,\, l-1}$ if $l > 1$, or $u = t_1 = [1]$ if $l = 1$. Since $x \in H$, we have that

$$[x,u]=\begin{cases}\prod_{I\ni l}\vee[n;(I\cup\{l-1\})\setminus\{l\}]^{e_I} & \text{if } l>1\\ \prod_{I\ni 1}\vee[n;I\setminus\{1\}]^{e_I} & \text{if } l=1\end{cases}$$

belongs to $\mathcal{N}_n^{i-1}$, and in particular $e_I\neq 0$ implies

$$\sum_{y\in(I\cup\{l-1\})\setminus\{l\}} y\le i+1.$$

If $I\in\mathcal{I}_l$ then

$$\sum_{y\in(I\cup\{l-1\})\setminus\{l\}} y=\sum_{y\in I} y-l+(l-1)=\sum_{y\in I} y-1\ge i+2,$$

so that $e_I=0$ for $I\in\mathcal{I}_l$. As $\mathcal{I}=\bigcup_{l=1}^n\mathcal{I}_l$, we have $H=\{1\}$. This finally shows that $N_{S_n}(N_{i-1}^n)=A=N_i^n\cap S_n=\left\langle\mathcal{N}_n^i\cap S_n\right\rangle$ and, by Eq. (9), that

$$\begin{aligned}N_i^n=N_{\Sigma_n}(N_{i-1}^n)&=\left\langle\mathcal{N}_{n-1}^{i-1}\right\rangle N_{S_n}(N_n^{i-1})=\left\langle\mathcal{N}_{n-1}^{i-1}\cup(\mathcal{N}_n^i\cap S_n)\right\rangle\\&=\left\langle(\mathcal{N}_n^i\cap\Sigma_{n-1})\cup(\mathcal{N}_n^i\cap S_n)\right\rangle=\left\langle\mathcal{N}_n^i\right\rangle,\end{aligned}$$

as claimed. □

4.2 Partitions into at least two distinct parts

This work was motivated by the computational evidence that the number $c_i\overset{\text{def}}{=}\log_2\left|N_n^{i-2}:N_n^{i-3}\right|$ does not depend on n, if $3\le i\le n$ [5]. The first terms of the sequence $\{c_i\}$ coincide with those of the sequence $\{a_i\}$ defined in [1, https://oeis.org/A317910], where a_i is the ith partial sum of the sequence $\{b_i\}$, where b_i is the number of partitions of i into at least two distinct parts. Some values of the aforementioned sequences are displayed in Table 1.

We have developed the rigid commutator machinery as a theoretical tool of investigation. It is no longer surprising that the equality $b_i=\left|\mathcal{W}_{n,i}\right|$, where $\mathcal{W}_{n,i}$ is defined by Eq. (7), is the link with the mentioned sequence. This combinatorial identity, Eq. (1), Proposition 5 and Theorem 2 give at last a positive answer to Conjecture 1 in [5].

Corollary 5 *For $1\le i\le n-2$, the number $\log_2\left|N_n^i:N_n^{i-1}\right|$ is independent of n. It equals the $(i+2)$th term of the sequence $\{a_j\}$ of the partial sums of the sequence $\{b_j\}$ counting the number of partitions of j into at least two distinct parts.*

Table 1 First values of the sequences a_i and b_i

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

5 Normalizers of saturated subgroups

In this section we will prove that the normalizer $N \stackrel{\text{def}}{=} N_{\Sigma_n}(G)$ of a saturated subgroup G of Σ_n is also saturated, provided that $T \leq N$, and thus we can use our rigid commutator machinery in the computation of N. In particular, for $i \leq n-2$, the machinery could be used as an alternative tool to derive the theoretical description of N_n^i as in Theorem 2. Even if we do not have such a description when $i > n-2$, the machinery can be anyway used to efficiently compute via GAP the complete normalizer chain.

We denote below by N_i the intersection $N \cap S_i$.

Proposition 6 *If G is a saturated subgroup of Σ_n, and $N = N_{\Sigma_n}(G)$ is its normalizer in Σ_n, then*

$$N = N_1 \ltimes \cdots \ltimes N_n = \ltimes_{i=1}^{n} N_{S_i}(G).$$

In particular if $x \in N$ and $x = x_1 \cdots x_n$, with $x_i \in S_i$ for all $1 \leq i \leq n$, then $x_i \in N_i$ for all $1 \leq i \leq n$.

Proof Let $x \in N$ and write $x = x_{i_1} \dots x_{i_k}$ where $1 \leq i_1 < \cdots < i_k \leq i_{k+1} \stackrel{\text{def}}{=} n$ and $x_{i_j} \in S_{i_j}$, for $1 \leq j \leq k$. In order to prove our claim we first show that $[x_{i_1}, c] \in G$ for every non-trivial rigid commutator c of G. Since G is generated by its own non-trivial rigid commutators, it will follow that $x_{i_1} \in N$. As a consequence, also $x_{i_2} \dots x_{i_k} \in N$. Thus, we may argue by induction on k to obtain that $x_{i_j} \in N$ for all $1 \leq j \leq k$.

Let i be such that $c \in G \cap S_i$. Suppose first that $i < i_1$. If $[c, x_{i_1}] = 1$, then $[c, x_{i_1}] \in G$. If $[c, x_{i_1}] \neq 1$, then $[c, x] = [c, x_{i_1}]h \in G$, where $[c, x_{i_1}] \in S_{i_1}$ and $h \in \prod_{t > i_1} S_t$. By Corollary 4 we obtain that $[c, x_{i_1}] \in G \cap S_{i_1} \leq G$. If $i = i_1$, then trivially $[c, x_{i_1}] = 1 \in G$. The last possibility is $i_1 < \cdots < i_m < i \leq i_{m+1}$ for some $m \leq k$. Suppose that $[x_{i_1}, c] \neq 1$. In this case

$$\begin{aligned} G \ni [x, c] &= [x_{i_1} \dots x_{i_k}, c] = [x_{i_1}, c]^{x_{i_2} \cdots x_{i_k}} \cdot [x_{i_2} \dots x_{i_k}, c] \\ &= \left([x_{i_1}, c]^{x_{i_2} \cdots x_{i_m}}\right)^{x_{i_{m+1}} \cdots x_{i_k}} \cdot [x_{i_2} \dots x_{i_k}, c] \\ &= [x_{i_1}, c]^{x_{i_2} \cdots x_{i_m}} \cdot [[x_{i_1}, c]^{x_{i_2} \cdots x_{i_m}}, x_{i_{m+1}} \cdots x_{i_k}] \cdot [x_{i_2} \dots x_{i_k}, c]. \end{aligned}$$

Let us consider the commutators

$$\begin{aligned} [x_{i_1}, c]^{x_{i_2} \cdots x_{i_m}} &= [x_{i_1}, c][[x_{i_1}, c], x_{i_2} \cdots x_{i_m}] = d_1 \cdots d_t, \\ [[x_{i_1}, c]^{x_{i_2} \cdots x_{i_m}}, x_{i_{m+1}} \cdots x_{i_k}] &= m_1 \cdots m_r, \\ [x_{i_2} \cdots x_{i_m} \cdot x_{i_{m+1}} \cdots x_{i_k}, c] &= f_1 \cdots f_s \cdot l_1 \cdots l_u, \end{aligned}$$

written as ordered product of distinct rigid commutators

$$d_1, \dots, d_t, f_1, \dots, f_s \in G \cap S_i,$$

and

$$m_1, \ldots, m_r, l_1, \ldots, l_u \in G \cap (S_{i+1} \ltimes \cdots \ltimes S_n).$$

Notice that $\{d_1, \ldots, d_t\} \cap \{f_1, \ldots, f_s\} = \emptyset$ since the commutators d_i are of the form $[X]$ for some set X with $i_1 \in X$, whereas the commutators f_j are of the form $[Y]$ for some set Y with $i_1 \notin Y$. This yields $[x_{i_1}, c]^{x_{i_2} \cdots x_{i_m}} \in G \cap S_i$ and so $[x_{i_1}, c] \in G \cap S_i \leq G$. □

Lemma 5 *Suppose that G is a saturated subgroup of Σ_n normalized by T. If $x_1, \ldots, x_k \in S_j$ are distinct rigid commutators such that $x = x_1 \cdots x_k \in N$, then $x_i \in N$ for all $1 \leq i \leq k$.*

Proof Let $c_1, \ldots, c_h \in \mathcal{R}^*$ such that $G = \langle c_1, \ldots, c_h \rangle$ and let us write every c_s and x_t in punctured form: $c_s = \vee[m_s; C_s]$ and $x_t = \vee[j; X_t]$.

Suppose first that $m_s < j$, so that

$$[c_s, x] = \prod_{t=1}^{k} d_{s,t} \in G \cap S_j, \tag{10}$$

where $d_{s,t} \stackrel{\text{def}}{=} [c_s, x_t] = \vee[j; C_s \cup (X_t \setminus \{m_s\})]$. Notice that if the commutator $d_{s,t}$ appears only once in the product, then, by Corollary 3, $d_{s,t} \in G$. If $C_s \cap X_t = \emptyset$ for all $1 \leq t \leq k$, then all the non-trivial $d_{s,t}$ appearing in the product are distinct and hence they appear only once in the product, so that $d_{s,t} \in G$ for all $1 \leq t \leq k$. If $C_s \cap X_t \neq \emptyset$, then the commutator $d_{s,t}$ may appear more than once in the product displayed in Eq. (10). Let $l \in C_s \cap X_t$ and consider the commutator $c_{s,l} = [c_s, t_l] = \vee[m_s; C_s \setminus \{l\}] \in G$ as $t_l = [l, \ldots, 1] \in T \leq N_{\Sigma_n}(G)$. Notice that

$$\begin{aligned}[c_{s,l}, x_t] &= \vee[j; (C_s \setminus \{l\}) \cup (X_t \setminus \{m_s\})] \\ &= \vee[j; C_s \cup (X_t \setminus \{m_s\})] = [c_s, x_t] = d_{s,t}.\end{aligned}$$

Let $C = C_s \setminus \{l\}$. We have determined a new rigid commutator $c = c_{s,l} = \vee[m_s; C] \in G$ such that $|C \cap X_t| < |C_s \cap X_t|$, that $|C| < |C_s|$ and that $d_{s,t} = [c, x_t]$ appears in the expansion of $[c, x]$. Using the same strategy, after a finite number of steps, we obtain $c = \vee[m_s; C] \in G$ such that $C \cap X_t = \emptyset$. If $d_{s,t} = [c, x_t] = [c, x_{t_1}] = d_{s,t_1}$, for some $t_1 \neq t$, then $C \cap X_{t_1} \neq \emptyset$, since otherwise $X_t = X_{t_1}$ and consequently $x_t = x_{t_1}$ with $t \neq t_1$, contrary to the hypotheses. Thus we may proceed in the same way with d_{s,t_1}. Since at each step the cardinality of C is strictly decreasing, after a finite number of steps we find a $c \in G$ and x_{t_r} such that $d_{s,t} = d_{s,t_1} = \cdots = d_{s,t_r}$ appears only once in $[c, x]$ giving $d_{s,t} \in G$. This finally shows that $d_{s,t} \in G$ for all $1 \leq t \leq k$.

If $j = m_s$ then x_i and c_s commute for all i and there is nothing to prove.

We are left with the case when $m_s > j$. As above, we have

$$[c_s, x] = \prod_{t=1}^{k} d_{s,t} \in G \cap S_j,$$

where $d_{s,t} \stackrel{\text{def}}{=} [c_s, x_t] = \vee[m_s; (C_s \setminus \{j\}) \cup X_t]$. Reasoning as we did for $m_s < j$, we obtain that $d_{s,t} \in G$ for all $1 \leq t \leq k$.

In all the cases we have proved that $x_i \in N$ for all $1 \leq i \leq k$, which is our claim. □

As an easy consequence of Proposition 6 and Lemma 5 we find the following result.

Theorem 3 *The normalizer N in Σ_n of a saturated subgroup of Σ_n is also saturated, provided that N contains T.*

Remark 2 Let $\mathcal{A}$ and $\mathcal{B}$ be two subsets of $\mathcal{R}$ such that $\{t_1, \ldots, t_n\} \subseteq \mathcal{A} \subseteq \mathcal{B}$, let $A = \langle \mathcal{A} \rangle$ and $B = \langle \mathcal{B} \rangle$ be the corresponding saturated subgroups. It is easy to recognize that $N_B(A) = \langle\, b \in \mathcal{B} \mid [b, \mathcal{A}] \subseteq \mathcal{A} \cup \{[\emptyset]\} \,\rangle$. Similarly, the normal closure A^B of A in B is the subgroup generated by the intersection of all the subsets $\mathcal{C}$ of $\mathcal{R}$ such that $\mathcal{A} \subseteq \mathcal{C} \subseteq \mathcal{B}$ and $[\mathcal{C}, \mathcal{B}] \subseteq \mathcal{C} \cup \{[\emptyset]\}$. In particular, both the normalizer $N_B(A)$ and the normal closure A^B are saturated.

Remark 3 The condition that T is contained in the normalizer $N = N_{\Sigma_n}(G)$ of a saturated subgroup G cannot be removed from the hypotheses of Theorem 3. Indeed, if $G = \langle\, [n, \ldots, 3] \,\rangle$, then the product $[2] \cdot [2, 1]$ is contained in the centralizer of A, and hence also in the normalizer N of A, but none of the two rigid commutators $[2]$ or $[2, 1] \in T$ normalizes G. In particular, by Corollary 4, the subgroup N cannot be saturated.

Remark 4 Another proof of Theorem 2 can be obtained from Theorem 3. Indeed, it is not difficult, but rather tedious, to check that

$$\mathcal{N}_n^i = \left\{ c \in \mathcal{R}^* \mid [c, \mathcal{N}_n^{i-1}] \subseteq \mathcal{N}_n^{i-1} \cup \{[\emptyset]\} \right\}.$$

for $0 \leq i \leq n-2$. The result then follows by Proposition 5.

From Theorems 2 and 3 and from Remark 4 we derive a straightforward corollary resulting in an algorithm whose GAP implementation is publicly available at GitHub (see https://github.com/ngunivaq/normalizer-chain). This script produces a significant speed-up in the computation of the normalizer N of a saturated subgroup provided that N contains T. We could easily apply this script to compute our normalizer chain up to the dimension $n = 22$. For example, whereas the standard libraries required one month on a cluster to compute the terms of the normalizer chain in $\mathrm{Sym}(2^{10})$, our implementation of the rigid commutator machinery gives the result in a few minutes, even on a standalone PC. With a similar approach, we can also use rigid commutators to compute the normal closure of a saturated subgroup. Some explicit calculations are shown below in Sect. 6. Let $\mathcal{M}_n^i$ be the set of all the rigid commutators belonging to N_n^i. From Theorem 3, the subgroups N_n^i are saturated, hence $N_n^i = \langle\, \mathcal{M}_n^i \,\rangle$ for all $i \geq 1$.

Corollary 6 *The set $\mathcal{M}_n^i$ is the largest subset of $\mathcal{R}$ that normalizes $\mathcal{M}_n^{i-1}$, i.e.*

$$\mathcal{M}_n^i = \left\{ c \in \mathcal{R} \mid [c, \mathcal{M}_n^{i-1}] \subseteq \mathcal{M}_n^{i-1} \right\}.$$

Moreover, $\mathcal{N}_n^i = \mathcal{M}_n^i \setminus \{[\emptyset]\}$ *for* $1 \leq i \leq n-2$.

The construction of the terms of the normalizer chain is then reduced to the determination of the sets $\mathcal{M}_n^i$, a task which turns out to be way faster than computing the terms of the normalizer chains as subgroups of Σ_n via the `Normalizer` command provided by GAP.

6 A computational supplement

In this section we show an explicit construction of the first four groups in the normalizer chain when $n = 6$, i.e. in Sym(64). Let us start by determining the generators of T in terms of rigid commutators:

$$\begin{aligned}
t_1 &= [1] = (1,33)(2,34)(3,35)\dots(30,62)(31,63)(32,64),\\
t_2 &= [2,1] = (1,17)(2,18)(3,19)\dots(46,62)(47,63)(48,64),\\
t_3 &= [3,2,1] = (1,9)(2,10)(3,11)\dots(54,62)(55,63)(56,64),\\
t_4 &= [4,3,2,1] = (1,5)(2,6)(3,7)\dots(58,62)(59,63)(60,64),\\
t_5 &= [5,4,3,2,1] = (1,3)(2,4)(5,7)\dots(58,60)(61,63)(62,64),\\
t_6 &= [6,5,4,3,2,1] = (1,2)(3,4)(5,6)\dots(59,60)(61,62)(63,64).
\end{aligned}$$

We have that $T = \langle t_1, t_2, \dots, t_6 \rangle$ and, from Proposition 2, its normalizer in Σ_n is $N_6^0 = U_6 = \langle \mathcal{U}_6 \rangle = \left\langle T, u_{ij} \mid 1 \leq j < i \leq 6 \right\rangle$. Thus the generators of N_6^0, besides those of T, are

$$\begin{aligned}
\vee[6;5]\,, \vee[6;4]\,, \vee[6;3]\,, \vee[6;2]\,, \vee[6;1]\,,\\
\vee[5;4]\,, \vee[5;3]\,, \vee[5;2]\,, \vee[5;1]\,,\\
\vee[4;3]\,, \vee[4;2]\,, \vee[4;1]\,,\\
\vee[3;2]\,, \vee[3;1]\,,\\
\vee[2;1]\,,
\end{aligned}$$

consequently $|N_6^0| = 2^{21}$. Now, in accordance with Eq. (8) and Theorem 2, the normalizer N_6^1 is generated by the rigid commutators previously listed and by η_6, the only element of $\mathcal{W}_{6,3}$ (see Eq. (7)). The commutator η_6 is the punctured rigid commutator based at 6 and missing the integers 1 and 2, i.e.

$$\eta_6 = [6,5,4,3] = \vee[6;2,1]\,, \tag{11}$$

where 1 and 2 indeed represent the sole partition of 3 into at least two distinct parts. From this, $\log_2 \left|N_6^1 : N_6^0\right| = 1 = a_3$. Again from Eq. (8) and Theorem 2, the normalizer N_6^2 is generated, along with the elements already mentioned, by the rigid commutators in $\mathcal{W}_{5,3}$ and $\mathcal{W}_{6,4}$, i.e.

$$[5,4,3] = \vee[5;2,1]\,, \tag{12}$$

$$[6, 5, 4, 2] = \vee[6; 3, 1]\,. \tag{13}$$

The commutator of Eq. (12), which belongs to $\mathcal{W}_{5,3}$, is the punctured rigid commutator based at 5 and missing the integers 1 and 2. The commutator of Eq. (13) instead, which belongs to $\mathcal{W}_{6,4}$, is based at 6 and misses the integers 1 and 3, composing the sole partition of 4 into at least two distinct parts. Notice that $[5, 4, 3] = [\not{6}, 5, 4, 3]$. Indeed, as discussed in Fact. 5, the commutator of Eq. (12) is obtained by lifting the one of Eq. (11), i.e. by removing 6, the left-most element of η_6. We have $\log_2 \left|N_6^2 : N_6^1\right| = 2 = a_4$. Similarly, N_6^3 is generated by adding the new rigid commutators

$$[\not{5}, 4, 3] = [4, 3] = \vee[4; 2, 1]\,, \tag{14}$$

$$[\not{6}, 5, 4, 2] = [5, 4, 2] = \vee[5; 3, 1]\,, \tag{15}$$

$$[6, 5, 3, 2] = \vee[6; 4, 1]\,, \tag{16}$$

$$[6, 5, 4, 1] = \vee[6; 3, 2]\,, \tag{17}$$

where the commutators of Eqs. (14) and (15) are respectively obtained by lifting those of Eqs. (12) and (13), and the commutators of Eqs. (16) and (17) belong to $\mathcal{W}_{6,5}$, respectively corresponding to the partitions $4 + 1$ and $3 + 2$ of 5. At this stage, we have that $\log_2 \left|N_6^3 : N_6^2\right| = 4 = a_5$. Ultimately, the commutators

$$\begin{aligned}
[\not{4}, 3] = \quad [3] \quad &= \vee[3; 2, 1]\,,\\
[\not{5}, 4, 2] = \quad [4, 2] \quad &= \vee[4; 3, 1]\,,\\
[\not{6}, 5, 3, 2] = \quad [5, 3, 2] \quad &= \vee[5; 4, 1]\,,\\
[\not{6}, 5, 4, 1] = \quad [5, 4, 1] \quad &= \vee[5; 3, 2]\,,\\
[6, 4, 3, 2] \quad &= \vee[6; 5, 1]\,,\\
[6, 5, 3, 1] \quad &= \vee[6; 4, 2]\,,\\
[6, 5, 4] \quad &= \vee[6; 3, 2, 1]
\end{aligned}$$

complete the set of rigid generators of N_6^4, and $\log_2 \left|N_6^4 : N_6^3\right| = 7 = a_6$.

Using Corollary 6, we can find a saturated set of rigid generators for all the elements of the chain. Notice that for $i > 5$, the sequence $\log_2 \left|N_6^i : N_6^{i-1}\right|$ does not fit the pattern of the sequence $\{a_j\}$. Although we do not have a general formula to calculate the values of the relative indices between two consecutive terms in the normalizer chain, they can be explicitly determined by the algorithm in GitHub. Computational results are summarized in Table 2, where we list all the relative indices of the normalizer chain. In the second column, the logarithms of the sizes of the intersections of each term with each of the subgroups $S_6, \ldots, S_1$ are displayed.

Table 2 The normalizer chain for $n = 6$

i	$\dim(N_6^i \cap S_j)$ $j = 6, 5, 4, 3, 2, 1$	$\log_2 \left\lvert N_6^i \right\rvert$	$\log_2 \left\lvert N_6^i : N_6^{i-1} \right\rvert$
0	6, 5, 4, 3, 2, 1	21	15
1	7, 5, 4, 3, 2, 1	22	1
2	8, 6, 4, 3, 2, 1	24	2
3	10, 7, 5, 3, 2, 1	28	4
4	13, 9, 6, 4, 2, 1	35	7
5	14, 10, 6, 4, 2, 1	37	2
6	16, 11, 7, 4, 2, 1	41	4
7	18, 12, 8, 4, 2, 1	45	4
8	19, 12, 8, 4, 2, 1	46	1
9	20, 12, 8, 4, 2, 1	47	1
10	21, 13, 8, 4, 2, 1	49	2
11	22, 14, 8, 4, 2, 1	51	2
12	23, 15, 8, 4, 2, 1	53	2
13	24, 16, 8, 4, 2, 1	55	2
14	25, 16, 8, 4, 2, 1	56	1
15	26, 16, 8, 4, 2, 1	57	1
16	27, 16, 8, 4, 2, 1	58	1
17	28, 16, 8, 4, 2, 1	59	1
18	29, 16, 8, 4, 2, 1	60	1
19	30, 16, 8, 4, 2, 1	61	1
20	31, 16, 8, 4, 2, 1	62	1
21	32, 16, 8, 4, 2, 1	63	1

7 Problems for future research

We conclude this work by highlighting some suggestions for further properties and structures of the set $\mathcal{R}$ of rigid commutators and providing some hints for future research.

7.1 Algebras of rigid commutators

The operation of commutation in $\mathcal{R}$ is commutative and $[\emptyset]$ represents the *zero* element. Moreover, for every $x, y \in \mathcal{R}$ the following identity is satisfied

$$[[x, x, y], x] = [[x, x], [y, x]] \qquad \text{(Jordan identity)}.$$

Let $\mathbb{F}$ be any field of characteristic 2 and let $\mathfrak{r}$ be the vector space over $\mathbb{F}$ having the set $\mathcal{R}^*$ of the non-trivial rigid commutators as a basis. The space $\mathfrak{r}$ is endowed with a natural structure of an algebra. The product $x \star y$ of two rigid commutators $x, y \in \mathcal{R}$

Table 3 Values of $\log_2|N_n^i : N_n^{i-1}|$ for small i and n

n	$\log_2\|N_n^i : N_n^{i-1}\|$ for $1 \le i \le 14$													
3	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0
4	**1**	**2**	1	1	0	0	0	0	0	0	0	0	0	0
5	**1**	**2**	**4**	1	2	2	1	1	1	1	0	0	0	0
6	**1**	**2**	**4**	**7**	2	4	4	1	1	2	2	2	2	1
7	**1**	**2**	**4**	**7**	**11**	4	7	3	4	2	2	4	4	4
8	**1**	**2**	**4**	**7**	**11**	**16**	7	5	6	2	6	6	3	3
9	**1**	**2**	**4**	**7**	**11**	**16**	**23**	4	9	4	11	4	12	9
10	**1**	**2**	**4**	**7**	**11**	**16**	**23**	**32**	4	14	5	20	7	19
11	**1**	**2**	**4**	**7**	**11**	**16**	**23**	**32**	**43**	5	22	7	32	4
12	**1**	**2**	**4**	**7**	**11**	**16**	**23**	**32**	**43**	**57**	7	32	12	43
13	**1**	**2**	**4**	**7**	**11**	**16**	**23**	**32**	**43**	**57**	**74**	12	42	18
14	**1**	**2**	**4**	**7**	**11**	**16**	**23**	**32**	**43**	**57**	**74**	**95**	8	24
15	**1**	**2**	**4**	**7**	**11**	**16**	**23**	**32**	**43**	**57**	**74**	**95**	**121**	8

For $i \le n-2$ these numbers do not depend on n and in the table are represented by bold digits

is defined as

$$x \star y \stackrel{\text{def}}{=} \begin{cases} [x, y] & \text{if } [x, y] \neq [\emptyset] \\ 0 & \text{otherwise.} \end{cases}$$

This operation is then extended to the whole $\mathfrak{r}$ by bilinearity and turns $\mathfrak{r}$ into a *Jordan algebra*, since it is commutative and $x \star x = 0$ for all $x \in \mathfrak{r}$. Moreover, if $\mathcal{H}$ is a saturated subset of $\mathcal{R}^*$, then, on the one hand the group $H = \langle \mathcal{H} \rangle$ is a saturated subgroup of Σ_n and, on the other hand, the $\mathbb{F}$-linear span $\mathfrak{h}$ of $\mathcal{H}$ is a subalgebra of $\mathfrak{r}$. The property $[\mathcal{R}, \mathcal{H}] \subseteq \mathcal{H} \cup \{[\emptyset]\}$ is a necessary and sufficient condition for H to be a normal subgroup of Σ_n and for $\mathfrak{h}$ to be an ideal of $\mathfrak{r}$. We point out that the fact that $\mathcal{R}$ is closed under commutation is crucial to check the previous statement. If c is the nilpotency class of Σ_n, then the product of $c+1$ elements of $\mathfrak{r}$ is always zero, so that $\mathfrak{r}$ is nilpotent. The study of the properties and the representations of this algebra seems to be a problem of independent interest, in connection with the study of the saturated subgroups of Σ_n.

7.2 Again on the normalizer chain

We have obtained from Theorem 2 an explicit description of the non-trivial rigid generators of the ith term of the normalizer chain when $1 \le i \le n-2$, i.e. the set $\mathcal{N}_n^i$. We have seen that $\mathcal{N}_n^i$ has a nice description by way of Eqs. (7) and (8), i.e. it is generated by some rigid commutators either belonging to $\mathcal{U}_n$ or having a punctured form corresponding to suitable partitions into at least two distinct parts. Although we can efficiently compute all the normalizers in the chain, as described in the lines following Corollary 6, it is an interesting problem to find a similar combinatorial

formula for the generating set $\mathcal{M}_n^i$ of N_n^i when $i > n-2$. Moreover, as already mentioned in Sect. 6, the values of the sequence $\log_2|N_n^i : N_n^{i-1}|$ do not seem to conform to any special known pattern when $i > n-2$. Table 3 contains the values of $\log_2|N_n^i : N_n^{i-1}|$ for $1 \leq i \leq 14$ and $3 \leq n \leq 15$. The determination of the general behavior of the sequence is an open problem.

7.3 An *odd* generalization

It appears natural to ask whether a similar rigid commutator machinery can be developed in a Sylow p-subgroup of the symmetric group $\mathrm{Sym}(p^n)$ when p is an odd prime. This seems to be an entirely different problem in terms of techniques and results. For example, a rigid commutator could contain repetitions. It may turn out interesting on a computational point of view, although such a machinery might have a weaker cryptographic application.

Acknowledgements We thank the staff of the *Department of Information Engineering, Computer Science and Mathematics* at the University of L'Aquila for helping us in managing the HPC cluster CALIBAN, which we extensively used to run our simulations (caliband.disim.univaq.it). We are also grateful to the *Istituto Nazionale d'Alta Matematica - F. Severi* for regularly hosting our research seminar *Gruppi al Centro* in which this paper was conceived.

Funding Open Access funding provided by Universitá degli Studi dell'Aquila

References

1. The On-Line Encyclopedia of Integer Sequences. Published electronically at https://oeis.org. Accessed 2020-03-01
2. Andrews, G.E.: Number Theory. Dover Publications Inc, New York (1994). (Corrected reprint of the 1971 original)
3. Andrews, G.E.: Euler's De Partitio numerorum. Bull. Am. Math. Soc. N.S. **44**(4), 561–573 (2007)
4. Aragona, R., Civino, R., Gavioli, N., Scoppola, C.M.: Regular subgroups with large intersection. Ann. Mat. Pura Appl. (4) **198**(6), 2043–2057 (2019)
5. 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. Preprint published electronically at arxiv:2008.13423: to appear in Indian J. Pure Appl. Math. (2020)
6. Bessenrodt, C.: A bijection for Lebesgue's partition identity in the spirit of Sylvester. Discrete Math. **132**(1–3), 1–10 (1994)
7. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)
8. Bousquet-Mélou, M., Eriksson, K.: Lecture hall partitions. Ramanujan J. **1**(1), 101–111 (1997)
9. 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)

10. Caranti, A., Dalla Volta, F., Sala, M.: Abelian regular subgroups of the affine group and radical rings. Publ. Math. Debrecen **69**(3), 297–308 (2006)
11. Civino, R., Blondeau, C., Sala, M.: Differential attacks: using alternative operations. Des. Codes Cryptogr. **87**(2–3), 225–247 (2019)
12. Daemen, J., Rijmen, V.: The Design of Rijndael: AES-The Advanced Encryption Standard. Springer, Berlin (2013)
13. Dixon, J.D.: Maximal abelian subgroups of the symmetric groups. Can. J. Math. **23**, 426–438 (1971)
14. Enkosky, T., Stone, B.: A sequence defined by M-sequences. Discrete Math. **333**, 35–38 (2014)
15. Euler, L.: Introductio in Analysin Infinitorum, vol 1. MM Bousquet, Lausanne (1748)
16. Fine, N.J.: Basic hypergeometric series and applications, vol. 27 of Mathematical Surveys and Monographs. American Mathematical Society, Providence (1988). With a foreword by George E. Andrews
17. The GAP Group. GAP—Groups, Algorithms, and Programming, Version 4.11.0 (2020)
18. Hall, P.: A contribution to the theory of groups of prime-power order. Proc. Lond. Math. Soc. **2**(36), 29–95 (1934)
19. Huppert, B.: Endliche Gruppen. I. Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer, Berlin (1967)
20. Kim, D., Yee, A.J.: A note on partitions into distinct parts and odd parts. Ramanujan J. **3**(2), 227–231 (1999)
21. Leinen, F.: Chief series and right regular representations of finite p-groups. J. Aust. Math. Soc. Ser. A **44**(2), 225–232 (1988)
22. Nyberg, K., Knudsen, L.R.: Provable security against a differential attack. J. Cryptol. **8**(1), 27–37 (1995)
23. Straub, A.: Core partitions into distinct parts and an analog of Euler's theorem. Eur. J. Combin. **57**, 40–49 (2016)
24. Sylvester, J.J., Franklin, F.: A constructive theory of partitions, arranged in three acts, an interact and an exodion. Am. J. Math. **5**(1–4), 251–330 (1882)