

Article

Sequences over Finite Fields Defined by OGS and BN-Pair Decompositions of $PSL_2(q)$ Connected to Dickson and Chebyshev Polynomials[†]

Robert Schwartz^{1,*}  and Hadas Yadayi²¹ Department of Mathematics, Ariel University, Ariel 4070000, Israel² Graduated at the Department of Mathematics, Ariel University, Ariel 4070000, Israel

* Correspondence: robertsh@ariel.ac.il

[†] This work is an improvement by Robert Schwartz of the project in partial fulfillment of the B.A. in mathematics of Hadas Yadayi under the supervision of Robert Schwartz.

Abstract: The factorization of groups into a Zappa–Szép product, or more generally into a k -fold Zappa–Szép product of its subgroups, is an interesting problem, since it eases the multiplication of two elements in a group and has recently been applied to public-key cryptography. We provide a generalization of the k -fold Zappa–Szép product of cyclic groups, which we call OGS decomposition. It is easy to see that the existence of an OGS decomposition for all the composition factors of a non-abelian group G implies the existence of an OGS for G itself. Since the composition factors of a soluble group are cyclic groups, it has an OGS decomposition. Therefore, the question of the existence of an OGS decomposition is interesting for non-soluble groups. The Jordan–Hölder theorem motivates us to consider the existence of an OGS decomposition for finite simple groups. In 1993, Holt and Rowley showed that $PSL_2(q)$ and $PSL_3(q)$ can be expressed as a product of cyclic groups. In this paper, we consider an OGS decomposition of $PSL_2(q)$ from a different point of view to that of Holt and Rowley. We look at its connection to the BN -pair decomposition of the group. This connection leads to sequences over $\mathbb{F}_q$, which can be defined recursively, with very interesting properties, and are closely connected to Dickson and Chebyshev polynomials. Since every finite simple Lie-type group exhibits BN -pair decomposition, the ideas in this paper might be generalized to further simple Lie-type groups.



Citation: Schwartz, R.; Yadayi, H. Sequences over Finite Fields Defined by OGS and BN-Pair Decompositions of $PSL_2(q)$ Connected to Dickson and Chebyshev Polynomials. *Mathematics* **2023**, *11*, 965. <https://doi.org/10.3390/math11040965>

Academic Editor: Clemente Cesarano

Received: 23 January 2023

Revised: 8 February 2023

Accepted: 11 February 2023

Published: 13 February 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: finite simple Lie-type groups; OGS decomposition; BN-pair decomposition; recursive sequences over finite fields; Dickson polynomials; Chebyshev polynomials

MSC: 20G07; 20G40; 20E42; 20D06; 20D60; 20F05

1. Introduction

The fundamental theorem of finitely generated abelian groups states the following: Let A be a finitely generated abelian group; then, there exist generators $a_1, a_2, \dots, a_n$ such that every element a in A has a unique presentation of the following form:

$$g = a_1^{i_1} \cdot a_2^{i_2} \cdot \dots \cdot a_n^{i_n},$$

where $i_1, i_2, \dots, i_n$ are n integers such that for $1 \leq k \leq n$, $0 \leq i_k < |g_k|$, where a_k has a finite order of $|a_k|$ in A , and $i_k \in \mathbb{Z}$, where a_k has an infinite order in A . Further, the meaning of the theorem is that every abelian group A is a direct sum of finitely many cyclic subgroups A_i (where $1 \leq i \leq k$), for some $k \in \mathbb{N}$.

The previously mentioned property of abelian groups yields a natural question: can a finite group (not necessarily abelian) be factorized into its subgroups?

Definition 1 ([1–3]). Let G be a group, and let H and K be its subgroups such that the following hold:

- $|G| = |H| \cdot |K|$;
- $H \cap K = \{1\}$;
- $G = HK$.

Then, obviously, every element $g \in G$ has a unique presentation of the form $g = hk$ such that $h \in H$; $k \in K$; and G is called the Zappa–Szép product of its subgroups H and K , denoted by $G = H \bowtie K$.

The Zappa–Szép product of H and K involves appropriate actions of H on K and of K on H , which allow easy multiplication of elements in pair form. Therefore, a great deal of work has been carried out in respect of the factorization of a group into a Zappa–Szép product of its subgroups, and the literature contains several hundreds of papers in the last 30 years regarding the factorization of simple groups by Walls, Praeger, Jones, Heng Li, Giudici, Wiegold, Williamson, Baumeister, Liebeck, Saxl, and many others. In 1984, Arad and Fishman [4] completely classified which simple groups G can be written as the Zappa–Szép product $G = A \bowtie B$. The factorization of a group G into the Zappa–Szép product can be generalized to a k -fold Zappa–Szép product for subgroups $H_1, H_2, \dots, H_k$, where the product of the k -subgroups $H_1 H_2 \cdots H_k$ represents uniquely every element in G . For example, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ can be considered as a 3-fold Zappa–Szép product for subgroups H_1, H_2 , and H_3 , where $H_i \simeq \mathbb{Z}_2$ for $1 \leq i \leq 3$. In 1928, Hall [5] proved that every soluble group is a product of its Sylow subgroups. By [6], the simple groups $PSL_2(q)$, $PSL_3(q)$, and some alternating groups can also be expressed as the product of their Sylow subgroup. In 2003, Vasco, Rötteler, and Steinweidt [7] proved that the five sporadic Mathieu groups (M_{11} , M_{12} , M_{22} , M_{23} , and M_{24}) are also products of their Sylow subgroups, and they motivated the factorizations to public-key cryptography.

There is special interest in the k -fold Zappa–Szép product for cyclic subgroups, which generalize the fundamental theorem of finitely generated abelian groups to the non-abelian case. The problem of factoring a group G into a Zappa–Szép product of two cyclic subgroups was posed by Ore in 1937 [8]. It was considered in a series of papers by Jesse Douglas in the early 1950s [9–12]. However, the problem is still open. In [13], an interesting generalization of the problem, which is called OGS, was proposed. We start by recalling the definition of the OGS decomposition.

Definition 2. Let G be a non-abelian group. The ordered sequence of n elements $\langle g_1, g_2, \dots, g_n \rangle$ is called an ordered generating system of the group G , or by shortened notation $OGS(G)$, if every element $g \in G$ has a unique presentation of the form

$$g = g_1^{i_1} \cdot g_2^{i_2} \cdots g_n^{i_n},$$

where $i_1, i_2, \dots, i_n$ are n integers such that for $1 \leq k \leq n$, $0 \leq i_k < r_k$, where $r_k | |g_k|$ if the order of g_k is finite in G , or $i_k \in \mathbb{Z}$ if g_k has infinite order in G .

For example, the quaternion group Q_8 has an OGS decomposition, although Q_8 cannot be expressed as a Zappa–Szép product of its cyclic subgroups. Let

$$Q_8 = \langle a, b | a^4 = 1, a^2 = b^2, bab^{-1} = a^{-1} \rangle$$

Then, every element of Q_8 has a unique presentation of the form $a^i \cdot b^j$, where $0 \leq i < 4$ and $0 \leq j < 2$ (although $|b| = 4$). Considering the defining relation $ba = a^{-1}b$, we can easily multiply two elements of the form

$$x_1 = a^{i_1} \cdot b^{j_1}, \quad x_2 = a^{i_2} \cdot b^{j_2}.$$

- If $j_1 = 0$, then $x_1 \cdot x_2 = a^{i_1+i_2} \cdot b^{j_1+j_2}$;

- If $j_1 = 1, j_2 = 0$, then $x_1 \cdot x_2 = a^{i_1-i_2} \cdot b^{j_1+j_2}$;
- If $j_1 = 1, j_2 = 1$, then $x_1 \cdot x_2 = a^{i_1-i_2+2}$.

Another example is the alternating group Alt_6 . By [1], the following hold:

- Alt_{2n+1} is isomorphic to a Zappa–Szép product of Alt_{2n} and $\mathbb{Z}_{2n+1}$;
- Alt_{4n} is isomorphic to a Zappa–Szép product of Alt_{4n-1} and Dih_{2n} (the dihedral group $\mathbb{Z}_{2n} \rtimes \mathbb{Z}_2$);
- Alt_6 cannot be expressed as a Zappa–Szép product of its subgroups.

However, by [14], there exists an OGS for Alt_n for every n (including $n = 6$) with very interesting multiplication laws.

The last examples (quaternion group Q_8 , alternating group Alt_6) demonstrate that there are non-abelian groups with an OGS decomposition that does not coincide with any k -fold Zappa–Szép product. Therefore, the requirement $r_k || g_k|$ (and not necessarily $r_k = |g_k|$) is essential in Definition 2, which generalizes the definition of a k -fold Zappa–Szép product of cyclic groups.

Similarly to Zappa–Szép products, the OGS decomposition of a group G can ease the multiplication of two elements in G . Moreover, the definition of OGS decomposition for the classical Coxeter groups [15] has close connections to the Coxeter length function [16] and, more generally, in the case of the complex reflection groups [17], the OGS decomposition is closely connected to the dimensions of components of an algebraic function such that the complex reflection group acts on it (for details, see [13]). Therefore, it is interesting to see whether a generic non-abelian group has an OGS decomposition.

The question of the existence of an OGS decomposition for a finite group G can be reduced to the existence of an OGS decomposition of all its composition factors. Therefore, we now mention the composition factors of a finite group and its connection to an OGS decomposition of it.

Let G be a finite group. Consider the series

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = 1,$$

where G_i is a maximal normal subgroup of G_{i-1} for every $1 \leq i \leq n$. Then, $K_i = G_{i-1}/G_i$ is a finite simple group for $1 \leq i \leq n$, and

$$|G| = |K_1| \cdot |K_2| \cdots |K_n|.$$

The Jordan–Hölder theorem states that the multi-set $\{K_1, K_2, \dots, K_n\}$ is an invariant of the group G , which does not depend on the choice of the maximal subgroup G_i [18–21]. Thus, $K_1, K_2, \dots, K_n$ are called the composition factors of the group G . If K_i has an OGS for every $1 \leq i \leq n$, then by taking the elements of G that are the corresponding representatives to the cosets in the sub-quotients K_i , we obtain an OGS for G . A group G is called soluble if all composition factors of the group are cyclic. Thus, every finite soluble group G has an OGS; these are the coset representatives corresponding to the generators of the cyclic sub-quotients $K_1, K_2, \dots, K_n$. This motivates us to check whether a non-soluble group has an OGS presentation. Since all the composition factors of a finite group G are simple groups, we can reduce the question of the existence of an OGS decomposition to simple groups only. The classification of finite simple groups was announced in 1981 by Gorenstein [22] and was completed in 2004 by Aschbacher and Smith [23]. The classification states that there are three categories of non-abelian simple groups:

- The alternating group Alt_n for $n \geq 5$ (the even permutations);
- The simple Lie-type groups;
- Twenty-six sporadic finite simple groups.

Since the most significant category of simple groups is the Lie-type simple groups, it is interesting enough to try to answer the question of whether a finite simple Lie-type group has an OGS presentation.

BN-Pair Decomposition

Lie-type simple groups can be considered by matrix presentation. Moreover, J. Tits introduced the *BN-pair* decomposition [24,25] for every simple Lie-type group—i.e., there exist specific subgroups B and N such that the simple Lie-type group is the product BNB , with the properties that we now describe. We use the notation of [26].

Definition 3. Let G be a group; then, the subgroups B and N of G form a *BN-pair* if the following axioms are satisfied:

1. $G = \langle B, N \rangle$;
2. $H = B \cap N$ is normal in N ;
3. $W = N/H$ is generated by a set S of involutions, and (W, S) is a Coxeter system;
4. If $\dot{w} \in N$ maps to $w \in W$ and $\dot{s} \in N$ maps to $s \in S$ (under $N \rightarrow W$), then for every $\dot{v}$ and $\dot{s}$,
 - $\dot{s}B\dot{w} \subseteq B\dot{s}\dot{w}B \cup B\dot{w}B$;
 - $\dot{s}B\dot{s} \neq B$.

Definition 4. Let G be a group with a *BN-pair*, (B, N) . It is a *split BN-pair* with a characteristic p if the following additional hypotheses are satisfied:

1. $B = UH$, with $U = O_p(B)$, the largest normal p -subgroup of B , and H a complement of U ;
2. $\bigcap_{n \in N} nBn^{-1} = H$.

The finite simple Lie-type groups have a *split BN-pair* with a characteristic p , where p is the characteristic of the field over which the matrix group is defined. Consider the easiest case of a simple Lie-type group, which is $PSL_2(q)$. Although by [6] there is an OGS for $PSL_2(q)$ and for $PSL_3(q)$, in this paper we observe it from a different point of view, connecting the OGS to the *BN-pair* decomposition. This connection motivates generalizing this case to further simple Lie-type groups, even those that are not mentioned in [6]. Moreover, the connection yields interesting recursive sequences over finite fields, which also involve Dickson polynomials of the second kind [27]. Since Dickson polynomials of the second kind are closely connected to Chebyshev polynomials of the second kind [28]—namely, $U_n(x) = E_n(2x, 1)$ (where U_n is the Chebyshev polynomial of the second kind and E_n is the Dickson polynomial of the second kind)—studying the recursive sequences that are connected to the OGS and the *BN-pair* decomposition of $PSL_2(q)$ also helps us to understand interesting properties of the Chebyshev polynomials.

2. Basic Properties of BN-Pair Decompositions and the Dickson and Chebyshev Polynomials

In this section, we present some basic properties of the *BN-pair* decompositions for $PSL_2(q)$, and the Dickson and Chebyshev polynomials, which we use for the results of the paper.

We start by considering $PSL_2(q)$; then, the following properties are satisfied:

Claim 1. Let $G = PSL_2(q)$, and let B, N, H, U, S be the groups as defined in Definitions 3 and 4; then, the following observations hold:

- B is the subgroup in which coset representatives are the upper triangular matrices in $SL_2(q)$.
- N is the subgroup in which coset representatives are the monomial matrices in $SL_2(q)$ (i.e., there is exactly one non-zero entry in each row and each column).
- $H = B \cap N$ is the subgroup in which coset representatives are the diagonal matrices in $SL_2(q)$. Thus, H is isomorphic to a quotient of the multiplicative group of $\mathbb{F}_q^*$. Thus, we denote the elements of H by $h(y)$, where $y \in \mathbb{F}_q^*$.
- $S = N/H$ is isomorphic to $\mathbb{Z}_2$. We denote by s the element of $PSL_2(q)$, which corresponds to the non-trivial element of S .

- U is the subgroup in which coset representatives are the upper unipotent matrices in $SL_2(q)$ (i.e., the upper triangular matrices with diagonal entry 1). Thus, U is isomorphic to the additive group of $\mathbb{F}_q$. Thus, we denote the elements of U by $u(x)$, where $x \in \mathbb{F}_q$.

By Definition 3, $PSL_2(q)$ is generated by $u(x)$, $h(y)$, and s , where $x \in \mathbb{F}_q$, $y \in \mathbb{F}_q^*$, and the following proposition holds:

Proposition 1. Let $G = PSL_2(q)$, where $\mathbb{F}_q$ is a finite field; then, the BN-pair presentation of an element $g \in G$ is as follows:

- If $g \notin B$, then $g = u(a) \cdot s \cdot u(x) \cdot h(y)$, where $a, x \in \mathbb{F}_q$ and $y \in \mathbb{F}_q^*$;
- If $g \in B$, then $g = u(x) \cdot h(y)$, where $x \in \mathbb{F}_q$ and $y \in \mathbb{F}_q^*$.

The proof is an immediate conclusion of the properties of U , H , and S , which have been described in Definitions 3 and 4. One can easily conclude from Proposition 1 the following property:

Conclusion 1. Let $G = PSL_2(q)$, where $\mathbb{F}_q$ is a finite field, and let g_1, g_2 be two elements of G , where

$$g_1 = u(a_1) \cdot s \cdot u(x_1) \cdot h(y_1)$$

and

$$g_2 = u(a_2) \cdot s \cdot u(x_2) \cdot h(y_2).$$

Then,

$$a_1 = a_2$$

if and only if

$$g_1 B = g_2 B \quad (\text{i.e., } g_2^{-1} g_1 \in B).$$

Definition 5. Let $G = PSL_2(q)$, $x \in \mathbb{F}_q$, and $y \in \mathbb{F}_q^*$; let $u(x)$, $h(y)$, and s be as defined in Claim 1; and let $\hat{u}(x)$, $\hat{h}(y)$, and $\hat{s}$ be the corresponding coset representatives in $SL_2(q)$.

Then, we can choose the representative matrices as follows:

- $\hat{u}(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$;
- $\hat{h}(y) = \begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix}$;
- $\hat{s} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Now, we easily conclude the following multiplication laws between $u(x)$, $h(y)$, and s .

Proposition 2. Let $G = PSL_2(q)$, $x \in \mathbb{F}_q$, and $y \in \mathbb{F}_q^*$; let $u(x)$, $h(y)$, and s be as defined in Claim 1. Then, the following relations hold:

- $u(x_1) \cdot u(x_2) = u(x_1 + x_2)$;
- $h(y_1) \cdot h(y_2) = h(y_1 \cdot y_2)$;
- $h(y) \cdot u(x) = u(x \cdot y^2) \cdot h(y)$;
- $s \cdot u(x) \cdot s = u(-x^{-1}) \cdot s \cdot u(-x) \cdot h(x)$;
- $s \cdot h(y) = h(y^{-1}) \cdot s$.

The proof comes directly from the properties of 2×2 matrix multiplications.

Dickson Polynomials and Related Polynomials over Finite Fields

Now, we recall the definition of the Dickson polynomials of the second kind [27] over a finite field $\mathbb{F}_q$, show some important properties of these, and define some other polynomials over $\mathbb{F}_q$, which are closely related to Dickson polynomials and are used in the paper.

Definition 6. For $a \in \mathbb{F}_q$, define $\alpha_{-1}(a)$ to be 0, and for $k \geq 0$, define $\alpha_k(a)$ to be $E_k(a, 1)$ —the Dickson polynomial of the second kind of degree k [27] over $\mathbb{F}_q$ —on variable a and with parameter 1, as follows:

- For $k = 2r$:

$$\alpha_{2r}(a) = E_{2r}(a, 1) = \sum_{i=0}^r (-1)^i \binom{2r-i}{i} a^{2r-2i}$$

- For $k = 2r + 1$:

$$\alpha_{2r+1}(a) = E_{2r+1}(a, 1) = \sum_{i=0}^r (-1)^i \binom{2r-i+1}{i} a^{2r-2i+1}.$$

Remark 1. In the case of odd q , the Dickson polynomial of the second kind on variable a and with parameter 1 is the same as the Chebyshev polynomial of the second kind over $\mathbb{F}_q$ on variable $\frac{a}{2}$ [28].

Proposition 3. For $a \in \mathbb{F}_q$ and $k \geq 0$, the following holds:

$$\alpha_{k+1}(a) = a \cdot \alpha_k(a) - \alpha_{k-1}(a).$$

Proof. The proof follows directly from the properties of the Dickson polynomials. $\square$

Definition 7. For $a, b \in \mathbb{F}_q$ and $k \geq -1$, define $\beta_k(a, b)$ and $\gamma_k(a, b)$ as follows:

- $\beta_{-1}(a, b) = 1$;
- $\beta_k(a, b) = b \cdot \alpha_k(a) - \alpha_{k-1}(a)$, where $k \geq 0$;
- $\gamma_k(a, b) = \alpha_k(a) + b \cdot \beta_k(a, b)$.

Remark 2. Since for every $k \geq 1$, both $\beta_k(a, b)$ and $\gamma_k(a, b)$ are linear combinations of elements of the form $\alpha_r(a)$, we have the following recurrence relations

$$\beta_{k+1}(a, b) = a \cdot \beta_k(a, b) - \beta_{k-1}(a, b), \quad \gamma_{k+1}(a, b) = a \cdot \gamma_k(a, b) - \gamma_{k-1}(a, b).$$

Proposition 4. Let $q = p^n$ such that p is an odd prime and, for every $k \geq 0$, $a, b \in \mathbb{F}(q)$, let $\alpha_k(a)$ and $\beta_k(a, b)$ be as defined in Definitions 6 and 7. Assume $b = \frac{a}{2}$. Then, for every $k \geq 0$, the following hold:

- $\beta_{k-1}(a, b) = T_k(b)$, where $T_k(b)$ is the Chebyshev polynomial of the first kind of degree k on variable b over $\mathbb{F}_q$;
- $\alpha_k(a) = U_k(b)$, where $U_k(b)$ is the Chebyshev polynomial of the second kind of degree k on variable b over $\mathbb{F}_q$.

Proof. By Definition 7, $\beta_{-1}(a, b) = 1$ and $\beta_0(a, b) = b$. Now, since $a = 2b$, by applying Remark 2, we have $\beta_{k+1}(a, b) = 2b \cdot \beta_k(a, b) - \beta_{k-1}(a, b)$, which implies $\beta_{k-1}(a, b) = T_k(b)$ for every $k \geq -1$. Since $b = \frac{a}{2}$, we have $\alpha_k(a) = U_k(b)$ by immediate application of Remark 1. $\square$

Proposition 5. Let $q = p^n$ such that p is an odd prime and, for every $k \geq 0$, $a, b \in \mathbb{F}(q)$, let $\alpha_k(a)$ and $\beta_k(a, b)$ be as defined in Definitions 6 and 7, and let Fib_k be the k -th element of the Fibonacci sequence over $\mathbb{F}_q$. If $a = 3$ and $b = 1$, then for every $k \geq 0$ the following are satisfied:

- $\beta_k = \text{Fib}_{2k+1}$;
- $\alpha_k = \text{Fib}_{2k+2}$.

Proof. Since for every $k \geq 0$, $\text{Fib}_{k+2} = \text{Fib}_{k+1} + \text{Fib}_k$, the following recurrence relation is satisfied:

$$\text{Fib}_{k+4} = 2 \cdot \text{Fib}_{k+2} + \text{Fib}_{k+1} = 3 \cdot \text{Fib}_{k+2} - (\text{Fib}_{k+2} - \text{Fib}_{k+1}) = 3 \cdot \text{Fib}_{k+2} - \text{Fib}_k.$$

By Definition 6, $\alpha_0(3) = 1 = \text{Fib}_2$ and $\alpha_1(3) = 3 = \text{Fib}_4$, and since $b = 1$, by Definition 7, $\beta_0(3, 1) = b = 1 = \text{Fib}_1$ and $\beta_1(3, 1) = \alpha_1(3) - \alpha_0(3) = 3 - 1 = 2 = \text{Fib}_3$. Since by Proposition 3, $\alpha_{k+1}(3) = 3\alpha_k(3) - \alpha_{k-1}(3)$, and by Proposition 2, $\beta_{k+1}(3, 1) = 3 \cdot \beta_k(3, 1) - \beta_{k-1}(3, 1)$, we conclude the results of the proposition. $\square$

In this paper, we generalize Proposition 1 in the following way: Theorem 1 demonstrates that every element of $g \in \text{PSL}_2(q)$ has a unique presentation of the form

$$g = [u(a) \cdot s]^k \cdot u(x) \cdot h(y),$$

where $0 \leq k \leq q$, $\mathbb{F}_q$ has characteristic 2, $x, y \in \mathbb{F}_q$ such that $y \neq 0$. The element $a \in \mathbb{F}_q$ is chosen such that the polynomial $\lambda^2 - a\lambda + 1$ is an irreducible polynomial over $\mathbb{F}_q$ and the root ω of the polynomial has order $q + 1$ in $\mathbb{F}_{q^2}^*$:

$$g = [u(a) \cdot s]^k \cdot [u(b) \cdot s \cdot u(-b)]^\ell \cdot u(x) \cdot h(y),$$

where $0 \leq k < \frac{q+1}{2}$, $0 \leq \ell \leq 1$ (i.e., $\ell = 0$ or $\ell = 1$), and $\mathbb{F}_q$ does not have characteristic 2, $x, y \in \mathbb{F}_q$ such that $y \neq 0$. The element $a \in \mathbb{F}_q$ is chosen such that the polynomial $\lambda^2 - a\lambda + 1$ is an irreducible polynomial over $\mathbb{F}_q$ and the root ω of the polynomial has order $q + 1$ in $\mathbb{F}_{q^2}^*$. The element $b \in \mathbb{F}_q$ is chosen in such a way that $u(b) \cdot s$ is not a left-coset representative of $[u(a) \cdot s]^k$ in B for any $0 \leq k \leq q$.

Remark 3. Since U and H are abelian groups, where U is a direct sum of copies of $\mathbb{Z}_p$ such that $q = p^\kappa$ for some κ (i.e., p is the characteristic of $\mathbb{F}_q$), and H is abelian as a quotient of the multiplicative group of $\mathbb{F}_q$, the elements $u(a) \cdot s$, $u(b) \cdot s \cdot u(-b)$, the κ copies of $\mathbb{Z}_p$ (which generate the additive group of $\mathbb{F}_q$), and an OGS of H form an OGS for $\text{PSL}_2(q)$.

Then, we look at the BN -pair presentation of the elements $[u(a) \cdot s]^k$ and $[u(a) \cdot s]^\ell \cdot [u(b) \cdot s \cdot u(-b)]$, for $1 \leq k \leq t - 1$, and $0 \leq \ell \leq t - 1$, where $t = \frac{q+1}{\gcd(2, q+1)}$:

$$[u(a) \cdot s]^k = u(a_k) \cdot s \cdot u(x_k) \cdot h(y_k)$$

$$[u(a) \cdot s]^\ell \cdot [u(b) \cdot s \cdot u(-b)] = u(b_\ell) \cdot s \cdot u(x'_\ell) \cdot h(y'_\ell).$$

We show that $a_k, x_k, y_k, b_\ell, x'_\ell$, and y'_ℓ are closely connected to the Dickson polynomial of the second kind over $\mathbb{F}_q$ (in the case where $b = \frac{a}{2}$, by Proposition 4, the sequences b_ℓ, x'_ℓ , and y'_ℓ are also closely connected to the Dickson and the Chebyshev polynomials of the first kind), and we connect it to the structure of the finite simple group $\text{PSL}_2(q)$.

3. Results

In this section, we introduce recursive sequences over $\mathbb{F}_q$, which connect an OGS presentation to the BN -pair presentation of $\text{PSL}_2(q)$. We show some interesting properties of the sequences and show that the sequences are closely connected to Dickson and Chebyshev polynomials over $\mathbb{F}_q$.

Definition 8. For $a \in \mathbb{F}$, define $P_a(\lambda)$ to be the polynomial

$$P_a(\lambda) = \lambda^2 - a \cdot \lambda + 1.$$

Proposition 6. Let $P_a(\lambda)$ be the polynomial as defined in Definition 8; then, the following hold:

- $P_a(\lambda)$ is the characteristic polynomial of the representative matrix for $u(a) \cdot s$;
- $P_a(0) = P_a(a) = 1$;
- $P_a(r) = P_a(a - r)$ for every $a, r \in \mathbb{F}_q$;
- $P_a(\lambda) = r$ has a double root if and only if the following hold:
 - q is odd;

- The root $\lambda = \frac{a}{2}$;
- $r = 1 - \frac{a^2}{4}$.
- $P_3(1) = -1$.

Proposition 7. Let $a \in \mathbb{F}_q$ such that the polynomial $P_a(\lambda)$ is irreducible over $\mathbb{F}_q$; then, the following hold:

- The root ω of $P_a(\lambda)$ has an order that divides $q + 1$ in the multiplicative group $\mathbb{F}_{q^2}^*$;
- It is possible to choose $a \in \mathbb{F}_q$ such that the root ω of $P_a(\lambda)$ has order $q + 1$ in the multiplicative group $\mathbb{F}_{q^2}^*$;
- For $a \in \mathbb{F}_q$ such that the root of $P_a(\lambda)$ has order $q + 1$ in the multiplicative group $\mathbb{F}_{q^2}^*$, it is satisfied that the order of the element $u(a) \cdot s$ in $PSL_2(q)$ is $\frac{q+1}{\gcd(2, q+1)}$.

Proof. The first two parts of the proposition are obvious from the basic theory of finite fields. Since Proposition 6, $P_a(\lambda)$ is the characteristic polynomial of $u(a) \cdot s$. The third part is obvious by the Cayley–Hamilton theorem. $\square$

Theorem 1. Let $G = PSL_2(q)$, where $\mathbb{F}_q$ is a finite field of order q . Let $a \in \mathbb{F}_q$ such that the polynomial $P_a(\lambda)$ is irreducible over $\mathbb{F}_q$ and the root ω of the polynomial has order $q + 1$ in $\mathbb{F}_{q^2}^*$. In the case of an odd q , let $b \in \mathbb{F}_q$ such that $u(b) \cdot s$ is not a left-coset representative of $[u(a) \cdot s]^k$ in B for any $0 \leq k < \frac{q+1}{2}$. Then, every $g \in G$ has a unique presentation of the following form:

- If the field $\mathbb{F}_q$ has characteristic 2,

$$g = [u(a) \cdot s]^k \cdot u(x) \cdot h(y)$$

where $x \in \mathbb{F}_q$, $y \in \mathbb{F}_q^*$, and $0 \leq k \leq q$;

- If the field $\mathbb{F}_q$ has an odd characteristic,

$$g = [u(a) \cdot s]^k \cdot [u(b) \cdot s \cdot u(-b)]^\ell \cdot u(x) \cdot h(y)$$

where $x \in \mathbb{F}_q$, $y \in \mathbb{F}_q^*$, $0 \leq k < \frac{q+1}{2}$, and $0 \leq \ell \leq 1$ (i.e., $\ell = 0$ or $\ell = 1$).

Proof. First, we consider the case in which $\mathbb{F}_q$ has characteristic 2. In that case, $PSL_2(q) = SL_2(q)$, and by Proposition 7, there exists an element $a \in \mathbb{F}_q$ such that the order of the element $u(a) \cdot s$ is $q + 1$. By Claim 1, the elements of the form $u(x) \cdot h(y)$ such that $x \in \mathbb{F}_q$ and $y \in \mathbb{F}_q^*$ form the subgroup B , which can be considered as the upper triangular matrices in $SL_2(q)$ (which is $PSL_2(q)$ in the case of $q = 2^m$). Therefore, $B = \{u(x) \cdot h(y) | x \in \mathbb{F}_q, y \in \mathbb{F}_q^*\}$ is a subgroup of order $q \cdot (q - 1)$, where in the case of $q = 2^m$ that order is prime to $q + 1$, in the order of $u(a) \cdot s$. Since the index of B in $PSL_2(q)$ is also $q + 1$, the $q + 1$ left-coset representatives of B in $PSL_2(q)$ can be considered the elements that have the form $[u(a) \cdot s]^k$, where $0 \leq k \leq q$. Thus, every $g \in PSL_2(q)$ has a unique presentation of the form

$$g = [u(a) \cdot s]^k \cdot u(x) \cdot h(y)$$

where $0 \leq k \leq q$ and the $\mathbb{F}_q$ has characteristic 2. Now, we consider the case where q is an odd prime. In this case, $PSL_2(q)$ is a proper quotient of $SL_2(q)$. As in the case of $q = 2^m$, the subgroup $B = \{u(x) \cdot h(y) | x \in \mathbb{F}_q, y \in \mathbb{F}_q^*\}$ has index $q + 1$ in $PSL_2(q)$, but the order of B is $\frac{q \cdot (q+1)}{2}$ (since $h(y) = h(-y)$ for every $y \in \mathbb{F}_q^*$), and by Proposition 7, there exists an element $a \in \mathbb{F}_q$ such that the order of the element $u(a) \cdot s$ is simply $\frac{q+1}{2}$. Thus, all the elements are of the form

$$[u(a) \cdot s]^k,$$

where $0 \leq k < \frac{q+1}{2}$ gives only half of the left-coset representatives of B in $PSL_2(q)$, where q is an odd prime. Now, we choose an element $b \in \mathbb{F}_q$ such that

$$u(b) \cdot s \notin [u(a) \cdot s]^k B,$$

for any $0 \leq k < \frac{q+1}{2}$. Then,

$$u(b) \cdot s \cdot u(-b)$$

is an involution conjugate to s , which does not belong to

$$[u(a) \cdot s]^k B,$$

for any $0 \leq k < \frac{q+1}{2}$ either. Now, we show that the $q+1$ elements of the form

$$[u(a) \cdot s]^k \cdot [u(b) \cdot s \cdot u(-b)]^\ell,$$

where $0 \leq k < \frac{q+1}{2}$ and $0 \leq \ell \leq 1$, form a full left-coset representative of B in $PSL_2(q)$ for an odd q . It is enough to show that all $q+1$ cosets of the form

$$[u(a) \cdot s]^k \cdot [u(b) \cdot s \cdot u(-b)]^\ell B$$

are different, where $0 \leq k < \frac{q+1}{2}$ and $0 \leq \ell \leq 1$. Assume

$$[u(a) \cdot s]^{k_1} \cdot [u(b) \cdot s \cdot u(-b)]^{\ell_1} B = [u(a) \cdot s]^{k_2} \cdot [u(b) \cdot s \cdot u(-b)]^{\ell_2} B,$$

where $0 \leq k_1, k_2 < \frac{q+1}{2}$ and $0 \leq \ell_1, \ell_2 \leq 1$. If $\ell_1 = \ell_2 = 0$, the equation implies that

$$[u(a) \cdot s]^{k_1 - k_2} \in B,$$

which is possible only if $k_1 - k_2 = 0$, since the order of $[u(a) \cdot s]^{k_1 - k_2}$ is otherwise prime to the order of B . If $\ell_1 = \ell_2 = 1$, the equation implies that

$$[u(b) \cdot s \cdot u(-b)] \cdot [u(a) \cdot s]^{k_1 - k_2} \cdot [u(b) \cdot s \cdot u(-b)] \in B,$$

which is also possible only if $k_1 - k_2 = 0$ for the same reason. If $\ell_1 = 1$ and $\ell_2 = 0$, the equation implies that

$$[u(b) \cdot s \cdot u(-b)]B = [u(a) \cdot s]^{k_1 - k_2} B,$$

which is impossible by the definition of b . Thus, all the $q+1$ cosets of the form

$$[u(a) \cdot s]^k \cdot [u(b) \cdot s \cdot u(-b)]^\ell B$$

are different. $\square$

The rest of the paper deals with the OGS of $PSL_2(q)$, which has been shown in Theorem 1, and its connection to the BN -pair decomposition and the Dickson and Chebyshev polynomials over $\mathbb{F}_q$. Hence, from now on, we use the following notation:

- Denote by a an element of $\mathbb{F}_q$ such that the polynomial $P_a(\lambda)$ is irreducible over $\mathbb{F}_q$ and the root ω of the polynomial has order $q+1$ in $\mathbb{F}_{q^2}^*$;
- In the case of an odd q , denote by b an element of $\mathbb{F}_q$ such that $u(b) \cdot s$ is not a left-coset representative of $[u(a) \cdot s]^k$ in B for any $0 \leq k < \frac{q+1}{2}$;
- Denote by t the order of $u(a) \cdot s$ (i.e., $t = \frac{q+1}{\gcd(2, q-1)}$).

Proposition 8. Let $G = PSL_2(q)$. Consider the BN -pair presentation of

$$[u(a) \cdot s]^k,$$

for $1 \leq k \leq t-1$, and in the case of odd q , consider the BN-pair presentation of

$$[u(a) \cdot s]^\ell \cdot [u(b) \cdot s \cdot u(-b)]$$

also, for $0 \leq \ell \leq t-1$. If

$$[u(a) \cdot s]^k = u(a_k) \cdot s \cdot u(x_k) \cdot h(y_k),$$

for some $x_k \in \mathbb{F}_q$, $y_k \in \mathbb{F}_q^*$, and

$$[u(a) \cdot s]^\ell \cdot [u(b) \cdot s \cdot u(-b)] = u(b_k) \cdot s \cdot u(x'_\ell) \cdot h(y'_\ell),$$

for some $x'_\ell \in \mathbb{F}_q$, $y'_\ell \in \mathbb{F}_q^*$,

we make the following observations:

- In the case where $\mathbb{F}_q$ has characteristic 2, the q elements $a_1, a_2, \dots, a_q$ are all the q different elements of $\mathbb{F}_q$;
- In the case where $\mathbb{F}_q$ has an odd characteristic, the q elements $a_1, a_2, \dots, a_{t-1}, b_0, b_1, \dots, b_{t-1}$ are all the q different elements of $\mathbb{F}_q$.

Proof. By Theorem 1, the q elements of the form

$$[u(a) \cdot s]^k$$

are the q different left-coset representatives of all the elements that are not in B in the case where $\mathbb{F}_q$ has characteristic 2. Thus, by applying Conclusion 1, $a_1, a_2, \dots, a_q$ are q different elements of $\mathbb{F}_q$, and since q is finite, obviously these elements are all the q different elements of $\mathbb{F}_q$. Similarly, in the case of odd q , the elements

$$[u(a) \cdot s]^k,$$

where $1 \leq k < t$, and

$$[u(a) \cdot s]^\ell \cdot [u(b) \cdot s \cdot u(-b)],$$

where $0 \leq \ell < t$ are the q different left-coset representatives of all the elements that are not in B . Thus, by the same argument as in the case of even q , we obtain the desired result. $\square$

Now, we present a recursive algorithm to find a_k and b_ℓ , and we describe some interesting properties of these elements.

Proposition 9. Let $G = \text{PSL}_2(q)$ and $t = \frac{q+1}{\gcd(2, q+1)}$. For $1 \leq k \leq t-1$, let a_k be elements of $\mathbb{F}_q$ as defined in Proposition 8. Then, $a_{t-1} = 0$.

Proof.

$$[u(a) \cdot s]^{t-1} = [u(a) \cdot s]^{-1} = s \cdot u(-a) = u(0) \cdot s \cdot u(-a) \cdot h(1).$$

Thus, by its definition in Proposition 8,

$$a_{t-1} = 0.$$

$\square$

Proposition 10. Let $G = \text{PSL}_2(q)$. For every $1 \leq k \leq t-1$ and $0 \leq \ell \leq t-1$, let a_k, b_ℓ be elements of $\mathbb{F}_q$ as defined in Propositions 8. Then, the following hold:

- $a_{k+1} = a - a_k^{-1}$;
- $b = b_0 = a - b_{t-1}^{-1}$;
- $b_{\ell+1} = a - b_\ell^{-1}$.

Proof. By Proposition 8,

$$[u(a) \cdot s]^{k+1} = u(a_{k+1}) \cdot s \cdot u(x_{k+1}) \cdot h(y_{k+1}),$$

for some $x_{k+1} \in \mathbb{F}_q$, $y_{k+1} \in \mathbb{F}_q^*$. However,

$$[u(a) \cdot s]^{k+1} = u(a) \cdot s \cdot [u(a) \cdot s]^k = u(a) \cdot s \cdot u(a_k) \cdot s \cdot u(x_k) \cdot h(y_k),$$

for some $x_k \in \mathbb{F}_q$, $y_k \in \mathbb{F}_q^*$. Now, by Proposition 2,

$$s \cdot u(a_k) \cdot s = u(-a_k^{-1}) \cdot s \cdot u(-a_k) \cdot h(a_k).$$

Therefore,

$$[u(a) \cdot s]^{k+1} = u(a) \cdot u(-a_k^{-1}) \cdot s \cdot u(-a_k) \cdot h(a_k) \cdot u(x_k) \cdot h(y_k).$$

Hence,

$$[u(a) \cdot s]^{k+1} = u(a - a_k^{-1}) \cdot s \cdot u(x_{k+1}) \cdot h(y_{k+1}),$$

for some $x_k \in \mathbb{F}_q$, $y_k \in \mathbb{F}_q^*$. Thus,

$$a_{k+1} = a - a_k^{-1}.$$

Similarly, by Proposition 8,

$$[u(a) \cdot s]^{l+1} \cdot [u(b) \cdot s \cdot u(-b)] = u(b_{l+1}) \cdot s \cdot u(x'_{l+1}) \cdot h(y'_{l+1}).$$

However,

$$\begin{aligned} [u(a) \cdot s]^{\ell+1} \cdot [u(b) \cdot s \cdot u(-b)] &= u(a) \cdot s \cdot [u(a) \cdot s]^{\ell} \cdot [u(b) \cdot s \cdot u(-b)] = \\ &= u(a) \cdot s \cdot u(b_{\ell}) \cdot s \cdot u(x'_{\ell}) \cdot h(y'_{\ell}). \end{aligned}$$

Now, by Proposition 2,

$$s \cdot u(b_{\ell}) \cdot s = u(-b_{\ell}^{-1}) \cdot s \cdot u(-b_{\ell}) \cdot h(b_{\ell}).$$

Hence,

$$[u(a) \cdot s]^{\ell+1} \cdot [u(b) \cdot s \cdot u(-b)] = u(a - b_{\ell}^{-1}) \cdot s \cdot u(x'_{\ell+1}) \cdot h(y'_{\ell+1}).$$

Thus,

$$b_{\ell+1} = a - b_{\ell}^{-1}.$$

□

The next theorem demonstrates interesting connections of the sequences a_k and b_{ℓ} for $1 \leq k \leq t-1$ and $0 \leq \ell \leq t-1$ to $\alpha_r(a)$ (the Dickson polynomial of the second kind on variable a over $\mathbb{F}_q$) and $\beta_r(a, b)$ (where, by Definition 7, $\beta_r(a, b)$ is a linear combination of $\alpha_r(a)$ and $\alpha_{r-1}(a)$, and in the case $b = \frac{a}{2}$, by Proposition 4, $\beta_r(a, b)$ is the Chebyshev polynomial of the first kind on variable b over $\mathbb{F}_q$).

Theorem 2. Let $G = \text{PSL}_2(q)$. For every $1 \leq k \leq t-1$, $0 \leq \ell \leq t-1$, and $-1 \leq r \leq t-1$, let $a_k, b_{\ell}, \alpha_r(a)$, and $\beta_r(a, b)$ be elements of $\mathbb{F}_q$ as defined in Proposition 8 and in Definitions 6 and 7. Then, the following hold:

- $a_k = \alpha_k(a) \cdot \alpha_{k-1}^{-1}(a)$;
- $b_{\ell} = \beta_{\ell}(a, b) \cdot \beta_{\ell-1}^{-1}(a, b)$;
- $\alpha_k(a) = \prod_{i=1}^k a_i$, where $1 \leq k \leq t-1$;
- $\beta_{\ell}(a, b) = \prod_{i=0}^{\ell} b_i$, where $0 \leq \ell \leq t-1$.

Proof. The proof is by induction on k . By Definition 7,

$$\beta_{-1}(a, b) = 1$$

and

$$\beta_k(a, b) = b \cdot \alpha_k(a) - \alpha_{k-1}(a),$$

for $0 \leq k \leq t-1$. Thus,

$$\beta_0(a, b) = b \cdot \alpha_0(a) - \alpha_{-1}(a) = b \cdot 1 - 0 = b.$$

Now, by Definition 6,

$$a_1 = a = \alpha_1(a) \cdot \alpha_0^{-1}(a)$$

and by Proposition 10,

$$b_0 = b = \beta_0(a, b) \cdot \beta_{-1}^{-1}(a, b)$$

and

$$\begin{aligned} b_1 &= a - b^{-1} = (ab - 1) \cdot b^{-1} = \\ &= [b \cdot \alpha_1(a) - \alpha_0(a)] \cdot [b \cdot \alpha_0(a) - \alpha_{-1}(a)]^{-1} = \beta_1(a, b) \cdot \beta_0^{-1}(a, b). \end{aligned}$$

$$a_\ell = \alpha_\ell(a) \cdot \alpha_{\ell-1}^{-1}(a)$$

and

$$b_\ell = [b \cdot \alpha_\ell(a) - \alpha_{\ell-1}(a)] \cdot [b \cdot \alpha_{\ell-1}(a) - \alpha_{\ell-2}(a)]^{-1}$$

for every $\ell \leq k$. By Proposition 10,

$$a_{k+1} = a - a_k^{-1}$$

and

$$b_{k+1} = a - b_k^{-1}.$$

Then, by the induction hypothesis,

$$a_{k+1} = a - \alpha_{k-1}(a) \cdot \alpha_k^{-1}(a)$$

and

$$b_{k+1} = a - [b \cdot \alpha_{k-1}(a) - \alpha_{k-2}(a)] \cdot [b \cdot \alpha_k(a) - \alpha_{k-1}(a)]^{-1}.$$

Thus,

$$a_{k+1} = [a \cdot \alpha_k(a) - \alpha_{k-1}(a)] \cdot \alpha_k^{-1}(a)$$

and

$$b_{k+1} = [b \cdot [a \cdot \alpha_k(a) - \alpha_{k-1}(a)] - [a \cdot \alpha_{k-1}(a) - \alpha_{k-2}(a)]] \cdot [b \cdot \alpha_k(a) - \alpha_{k-1}(a)]^{-1}.$$

Then, by Proposition 3,

$$a_{k+1} = \alpha_{k+1}(a) \cdot \alpha_k^{-1}(a)$$

and

$$b_{k+1} = [b \cdot \alpha_{k+1}(a) - \alpha_k(a)] \cdot [b \cdot \alpha_k(a) - \alpha_{k-1}(a)]^{-1}.$$

Thus, the proposition holds for every $1 \leq k \leq t-1$. $\square$

The next proposition shows some interesting relations that arise from the definitions of a_k , b_ℓ , $\alpha_r(a)$, $\beta_r(a, b)$, and $\gamma_r(a, b)$ over $\mathbb{F}_q$, where $1 \leq k \leq t-1$, $0 \leq \ell \leq t-1$, and $-1 \leq r \leq t-1$. For a detailed proof of the relations in Proposition 11, see [29].

Proposition 11. Let $G = \text{PSL}_2(q)$. For every $1 \leq k \leq t-1$, $0 \leq \ell \leq t-1$, and $-1 \leq r \leq t-1$, let $a_k, b_\ell, \alpha_r(a), \beta_r(a, b)$, and $\gamma_r(a, b)$ be elements of $\mathbb{F}_q$ as defined in Proposition 8 and in Definitions 6 and 7. Then, the following relations hold:

- $a_k \cdot a_{t-k-1} = 1$ for $1 \leq k \leq t-2$;
- $a_k + a_{t-k} = a$;
- $a_{\frac{q}{2}} = 1$ in the case where $\text{char}(\mathbb{F}_q) = 2$;
- $a_{\frac{q-1}{4}} = 1$ or $a_{\frac{q-1}{4}} = -1$ in the case where $\text{char}(\mathbb{F}_q) \neq 2$ and $4|q-1$;
- $a_{\frac{q+1}{4}} = \frac{a}{2}$ in the case where $\text{char}(\mathbb{F}_q) \neq 2$ and $4|q+1$;
- $a_k = a_\ell - [(a_1 \cdot a_2 \cdots a_{\ell-1}) \cdot (a_{k-\ell} \cdots a_{k-3} \cdot a_{k-2}) \cdot a_{k-1}]^{-1}$, for every $1 \leq \ell < k \leq t-1$;
- In particular, $a_k = a_{k-1} - [a_1^2 \cdot a_2^2 \cdots a_{k-2}^2 \cdot a_{k-1}]^{-1}$;
- $b_\ell = (a_\ell \cdot b - 1) \cdot (b - a_{\ell-1}^{-1})^{-1} = (a_\ell \cdot b - 1) \cdot (b - a_{t-\ell})^{-1} = (1 - a_\ell \cdot b) \cdot (a - b - a_\ell)^{-1}$, where $1 \leq \ell \leq t-1$;
- $b_{t-1} = (a - b)^{-1}$;
- $(b_\ell \cdot b_{\ell+1}) \cdot (a_\ell \cdot a_{\ell-1})^{-1} = (a_{\ell+1} \cdot b - 1) \cdot (a_{\ell-1} \cdot b - 1)^{-1}$, where $2 \leq \ell \leq t-2$;
- $\alpha_{t-1}(a) = 0$;
- $\alpha_{t-2}(a) = 1$ or $\alpha_{t-2}(a) = -1$;
- $\alpha_{t-k-2}(a) = \alpha_k$ or $\alpha_{t-k-2}(a) = -\alpha_k(a)$, where $-1 \leq k \leq t-1$;
- $\alpha_\ell(a) \cdot \alpha_{k-1}(a) - \alpha_{\ell-1}(a) \cdot \alpha_k(a) = \alpha_{k-\ell-1}(a)$, where $0 \leq \ell \leq k \leq t-1$;
- $\alpha_k^2(a) - \alpha_{k+1}(a) \cdot \alpha_{k-1}(a) = 1$, where $0 \leq k \leq t-2$;
- $P_a(a_k) = \alpha_{k-1}^{-2}(a)$, where $1 \leq k \leq t-1$;
- $\alpha_k(a) \cdot \beta_{k-1}(a, b) - \alpha_{k-1}(a) \cdot \beta_k(a, b) = 1$, where $0 \leq k \leq t-1$;
- $\gamma_k(a, b) \cdot \beta_{k-1}(a, b) - \gamma_{k-1}(a, b) \cdot \beta_k(a, b) = 1$, where $0 \leq k \leq t-1$;
- If $b = \frac{a}{2}$, then for every $0 \leq k \leq t-1$ the following hold:
 - $b_k + b_{t-k} = a$, where $b_t = b_0 = b$;
 - $b_k \cdot b_{t-k-1} = 1$;
 - $\beta_{t-1}(a, b) = 1$ or $\beta_{t-1}(a, b) = -1$ (which means the Chebyshev polynomial of the first kind on variable b satisfies $T_t(b) = 1$ or $T_t(b) = -1$ over $\mathbb{F}_q$ for every $q \equiv 1 \pmod{4}$);
 - $\beta_k(a, b) = \beta_{t-1}(a, b) \cdot \beta_{t-k-2}(a, b)$;
 - $\beta_k^2(a, b) - \beta_{k+1}(a, b) \cdot \beta_{k-1}(a, b) = 1 - b^2$;
 - $P_a(b_k) = (1 - b^2) \cdot \beta_{k-1}^{-2}(a, b)$.
- It is possible to choose either $b = 1$ or $b = -1$;
- If $b = 1$ or $b = -1$, then for all $0 \leq k \leq t-1$:
 - $b_k \cdot b_{t-k} = 1$, where $b_t = b_0 = b$;
 - $b_k + b_{t-k+1} = a$;
 - $\beta_{t-k-1}(a, b) = b \cdot \beta_k(a, b)$.

Remark 4. By Theorem 1, the group $\text{PSL}_2(q)$, for an odd q , has an OGS presentation of the form

$$[u(a) \cdot s]^k \cdot [u(b) \cdot s \cdot u(-b)]^\ell \cdot g,$$

such that

- $0 \leq k \leq t-1$;
- $\ell = 0$ or $\ell = 1$;
- g is an element of the soluble subgroup B of $\text{PSL}_2(q)$.

By Theorem 3, we will show the OGS presentation of

$$[u(b) \cdot s \cdot u(-b)] \cdot [u(a) \cdot s]^k.$$

We will also show some special interesting cases of it, which depend on some properties of the field $\mathbb{F}_q$.

Theorem 3. Let $q = p^n$, where p is an odd prime, and $n \in \mathbb{N}$. For every $1 \leq k \leq t-1$, $0 \leq \ell \leq t-1$, and $-1 \leq r \leq t-1$, let $a_k, b_\ell, \alpha_r(a), \beta_r(a, b)$, and $\gamma_r(a, b)$ be elements of $\mathbb{F}_q$ as defined in Proposition 8 and in Definitions 6 and 7. Then, for every k_1 and k_2 such that $0 \leq k_1, k_2 \leq t-1$, the following holds:

$$[u(b) \cdot s \cdot u(-b)] \cdot [u(a) \cdot s]^{k_1} \in [u(a) \cdot s]^{k_2} \cdot [u(b) \cdot s \cdot u(-b)]B$$

if and only if

$$(b - a_{t-k_2}) \cdot (a_{k_1} - b)^{-1} = (b - a + a_{k_2}) \cdot (a_{k_1} - b)^{-1} = P_a(b).$$

In particular, if b satisfies

$$P_a(b) = -1 \quad (\text{i.e., } b^2 - a \cdot b + 2 = 0),$$

then for every $0 \leq k \leq t-1$ we have

$$[u(b) \cdot s \cdot u(-b)] \cdot [u(a) \cdot s]^k \in [u(a) \cdot s]^{-k} \cdot [u(b) \cdot s \cdot u(-b)]B$$

Proof. First, consider $[u(b) \cdot s \cdot u(-b)] \cdot [u(a) \cdot s]^{k_1}$ and $[u(a) \cdot s]^{k_2} \cdot [u(b) \cdot s \cdot u(-b)]$. By Proposition 8, the following hold:

- $[u(a) \cdot s]^{k_1} = u(a_{k_1}) \cdot s \cdot g$ such that $g \in B$;
- $[u(a) \cdot s]^{k_2} \cdot [u(b) \cdot s \cdot u(-b)] = u(b_{k_2}) \cdot s \cdot g'$ such that $g' \in B$.

Hence, by Proposition 2,

$$\begin{aligned} [u(b) \cdot s \cdot u(-b)] \cdot [u(a) \cdot s]^{k_1} &= [u(b) \cdot s \cdot u(-b)] \cdot u(a_{k_1}) \cdot s \cdot g \\ &= u(b - [a_{k_1} - b]^{-1}) \cdot s \cdot g, \end{aligned}$$

such that $g \in B$. Thus, by Conclusion 1,

$$[u(b) \cdot s \cdot u(-b)] \cdot [u(a) \cdot s]^{k_1} \in [u(a) \cdot s]^{k_2} \cdot [u(b) \cdot s \cdot u(-b)]B,$$

if and only if

$$b - [a_{k_1} - b]^{-1} = b_{k_2}. \quad (1)$$

Now, by using Theorem 2, Definition 7, and Proposition 3, the following holds:

$$\begin{aligned} b - b_{k_2} &= b - \beta_{k_2}(a, b) \cdot \beta_{k_2-1}(a, b)^{-1} \\ &= b - [b \cdot \alpha_{k_2}(a) - \alpha_{k_2-1}(a)] \cdot [b \cdot \alpha_{k_2-1}(a) - \alpha_{k_2-2}(a)]^{-1} \\ &= \left[(b^2 + 1) \cdot \alpha_{k_2-1}(a) - b \cdot [\alpha_{k_2-2}(a) + \alpha_{k_2}(a)] \right] \cdot [b \cdot \alpha_{k_2-1}(a) - \alpha_{k_2-2}(a)]^{-1} \\ &= \left[(b^2 - a \cdot b + 1) \cdot \alpha_{k_2-1}(a) \right] \cdot [b \cdot \alpha_{k_2-1}(a) - \alpha_{k_2-2}(a)]^{-1}. \end{aligned}$$

Hence, by using Theorem 2 and Proposition 11, the following holds:

$$\begin{aligned} (b - b_{k_2})^{-1} &= \left[b - a_{k_2-1}^{-1} \right] \cdot \left[b^2 - a \cdot b + 1 \right]^{-1} \\ &= \left[b - a_{t-k_2} \right] \cdot \left[b^2 - a \cdot b + 1 \right]^{-1} \\ &= \left[b - a + a_{k_2} \right] \cdot \left[b^2 - a \cdot b + 1 \right]^{-1}. \end{aligned}$$

Therefore, by Equation 1, we conclude as follows:

$$\begin{aligned} a_{k_1} - b &= (b - b_{k_2})^{-1} = [b - a_{t-k_2}] \cdot [b^2 - a \cdot b + 1]^{-1} \\ &= [b - a + a_{k_2}] \cdot [b^2 - a \cdot b + 1]^{-1} \\ &= [b - a + a_{k_2}] \cdot [P_a(b)]^{-1}. \end{aligned}$$

Hence,

$$[u(b) \cdot s \cdot u(-b)] \cdot [u(a) \cdot s]^{k_1} \in [u(a) \cdot s]^{k_2} \cdot [u(b) \cdot s \cdot u(-b)]B$$

if and only if

$$(b - a_{t-k_2}) \cdot (a_{k_1} - b)^{-1} = (b - a + a_{k_2}) \cdot (a_{k_1} - b)^{-1} = P_a(b).$$

Now, we consider the case where $P_a(b) = -1$ (i.e., $b^2 - a \cdot b + 2 = 0$). Then, by the first part of the Theorem, we have

$$-1 = P_a(b) = (b - a_{t-k_2}) \cdot (a_{k_1} - b)^{-1},$$

which implies

$$b - a_{k_1} = b - a_{t-k_2}.$$

Therefore, the theorem holds. $\square$

The next corollary shows an interesting application of Theorem 3, in the special case where $b = \frac{a}{2}$ (the only case of b where there is no $r \neq b$ such that $P_a(b) = P_a(r)$). Since in that case, by Proposition 4, for every $0 \leq k \leq t-1$, $\alpha_k(a) = U_k(b)$ (the Chebyshev polynomial of the second kind of degree k on variable b), and $\beta_{k-1}(a, b) = T_k(b)$ (the Chebyshev polynomial of the first kind of degree k on variable b), we conclude by Theorem 2 that $a_k = U_k(b) \cdot U_{k-1}^{-1}(b)$ and $b_k = T_{k+1}(b) \cdot T_k^{-1}(b)$ (i.e., both a_k and b_k are quotients of Chebyshev polynomials on variable b).

Corollary 1. Let $q = p^n$, where p is an odd prime, $n \in \mathbb{N}$, and $4|q-1$. Assume $a = 2b$ (i.e., $b = \frac{a}{2}$). Then, for every k_1 and k_2 such that $0 \leq k_1, k_2 \leq t-1$, the following holds:

$$[u(b) \cdot s \cdot u(-b)] \cdot [u(a) \cdot s]^{k_1} \in [u(a) \cdot s]^{k_2} \cdot [u(b) \cdot s \cdot u(-b)]B$$

if and only if

$$(a_{k_2} - b) \cdot (a_{k_1} - b)^{-1} = P_a(b) = 1 - b^2.$$

Proof. Assume $q = p^n$, where p is an odd prime, $n \in \mathbb{N}$, and $4|q-1$. By Theorem 1, the order of the element $u(a) \cdot s$ is $t = \frac{q+1}{2}$ (which is odd, since $4|q-1$) in $PSL_2(q)$. By proposition 11, $a_{t-k} = a - a_k$ for every $1 \leq k \leq t-1$, and by Proposition 8, the $t-1$ elements of the form a_k are all different. Hence, there is no k such that $1 \leq k \leq t-1$, and $a_k = \frac{a}{2}$. Hence, it is possible to choose b such that $a = 2b$ and the left coset $(u(b) \cdot s)B$ is different from all left cosets of the form $[u(a) \cdot s]^k B$ for $0 \leq k < \frac{q+1}{2}$. Hence, the conditions of Theorems 1 and 3 hold, and by applying Theorem 3 for the case of $a = 2b$, we conclude the result of the corollary. $\square$

Proposition 4 and Corollary 1 demonstrate interesting properties of the OGS for $PSL_2(q)$, where q is odd and it is possible to choose $a, b \in \mathbb{F}_q$ such that $b = \frac{a}{2}$. By Proposition 11, $a_{\frac{q+1}{4}} = \frac{a}{2}$, in the case of $\mathbb{F}_q$, where $4|q+1$. Therefore, by Proposition 8, there is no possibility to choose $a, b \in \mathbb{F}_q$ such that $b = \frac{a}{2}$; however, the next corollary

demonstrates that the choice of $a, b \in \mathbb{F}_q$, such that $P_a(b) = -1$, leads to interesting properties of the defined OGS in Theorem 1 for the case where $4|q+1$.

Corollary 2. Let $q = p^n$, where p is an odd prime, $n \in \mathbb{N}$, and $4|q+1$. If b can be chosen such that $P_a(b) = -1$ (i.e., the polynomial $\lambda^2 - a \cdot \lambda + 2$ is reducible over $\mathbb{F}_q$), then for every $0 \leq k \leq t-1$ we have

$$[u(b) \cdot s \cdot u(-b)] \cdot [u(a) \cdot s]^k \in [u(a) \cdot s]^{-k} \cdot [u(b) \cdot s \cdot u(-b)]B.$$

Proof. By Proposition 11, $P_a(a_k) = \alpha_{k-1}^{-2}$. Since $4|q+1$, there is no element $x \in \mathbb{F}_q$ such that $x^2 = -1$. Hence, for every $0 \leq k \leq t-2$, $\alpha_{k-1}^{-2} \neq -1$. Thus, there is no a_k such that $P_{a_k} = a_k^2 - a \cdot a_k + 1 = -1$. However, since the polynomial $\lambda^2 - a \cdot \lambda + 2$ is reducible over $\mathbb{F}_q$, its root can be chosen as $b \neq a_k$ for any k such that $0 \leq k \leq t-2$. Then, by Theorem 3, we obtain the result of the corollary. $\square$

Remark 5. In contrast to Corollary 1, which is applicable in every $\mathbb{F}_q$ such that $4|q-1$, to apply Corollary 2, we require an element $a \in \mathbb{F}_q$ such that all of the following hold:

- The polynomial $P_a(\lambda)$ is an irreducible polynomial over $\mathbb{F}_q$;
- The root ω of the polynomial $P_a(\lambda)$ has an order $q+1$ over $\mathbb{F}_{q^2}$;
- The polynomial $P_a(\lambda) + 1$ (i.e., $\lambda^2 - a \cdot \lambda + 2$) is a reducible polynomial over $\mathbb{F}_q$ (otherwise, there is no possibility for a choice of $b \in \mathbb{F}_q$ such that $P_a(b) = -1$).

There are finite fields $\mathbb{F}_q$, where $4|q+1$, but any $a \in \mathbb{F}_q$ does not satisfy the three mentioned conditions above (e.g., $\mathbb{F}_{11}$). The case where Corollary 2 is applicable for $a = 3$ is interesting, since then the choice of $b = 1$ is also applicable ($b = 1$ is a root of the polynomial $\lambda^2 - 3 \cdot \lambda + 2$) for satisfying Corollary 2. Then, by Proposition 5, both α_k and β_ℓ are Fibonacci numbers over $\mathbb{F}_q$ for $1 \leq k \leq t-1$ and $0 \leq \ell \leq t-1$, and by Theorem 2,

$$a_k = \text{Fib}_{2k+2} \cdot \text{Fib}_{2k+1}^{-1} \quad b_k = \text{Fib}_{2k+1} \cdot \text{Fib}_{2k}^{-1}.$$

The next theorem demonstrates very interesting connections between the BN-pair presentation of the element $[u(a) \cdot s]^k$ of $\text{PSL}_2(q)$ to $\alpha_r(a)$ (the Dickson polynomial of the second kind on variable a over $\mathbb{F}_q$), and the presentation of $[u(a) \cdot s]^\ell \cdot [u(b) \cdot s \cdot u(-b)]$ to $\beta_r(a, b)$ and $\gamma_r(a, b)$ (where, by Definition 7, both $\beta_r(a, b)$ and $\gamma_r(a, b)$ are linear combinations of $\alpha_r(a)$ and $\alpha_{r-1}(a)$, and in case $b = \frac{a}{2}$, by Proposition 4, $\beta_r(a, b)$ is the Chebyshev polynomial of the first kind on variable b over $\mathbb{F}_q$), for $1 \leq k \leq t-1$, $0 \leq \ell \leq t-1$, $-1 \leq r \leq t-1$, and $t = \frac{q+1}{\gcd(2, q+1)}$.

Theorem 4. Let $G = \text{PSL}_2(q)$. For every $1 \leq k \leq t-1$, $0 \leq \ell \leq t-1$, and $-1 \leq r \leq t-1$, let a_k and b_ℓ be elements of $\mathbb{F}_q$ as defined in Proposition 8, and let $\alpha_r(a)$, $\beta_r(a, b)$, and $\gamma_r(a, b)$ be elements of $\mathbb{F}_q$ as defined in Definitions 6 and 7. Then,

$$[u(a) \cdot s]^k = u(a_k) \cdot s \cdot u(x_k) \cdot h(y_k)$$

and

$$[u(a) \cdot s]^\ell \cdot [u(b) \cdot s \cdot u(-b)] = u(b_\ell) \cdot s \cdot u(x'_\ell) \cdot h(y'_\ell),$$

such that

- $x_k = -\alpha_{k-2}(a) \cdot \alpha_{k-1}(a)$;
- $y_k = \alpha_{k-1}(a)$;
- $x'_\ell = -\beta_{\ell-1}(a, b) \cdot \gamma_{\ell-1}(a, b)$;
- $y'_\ell = \beta_{\ell-1}(a, b)$.

Proof. We prove the results of the theorem for x_k , y_k , x'_k , and y'_k by induction on k . Recall, by Proposition 8,

$$[u(a) \cdot s]^k = u(a_k) \cdot s \cdot u(x_k) \cdot h(y_k)$$

and

$$[u(a) \cdot s]^k \cdot [u(b) \cdot s \cdot u(-b)] = u(b_k) \cdot s \cdot u(x'_k) \cdot h(y'_k).$$

By substituting $k = 1$, we have

$$\begin{aligned} u(a) \cdot s &= u(a) \cdot s \cdot u(0) \cdot h(1) \\ &= u(a_1) \cdot s \cdot u(-\alpha_{-1}(a) \cdot \alpha_0(a)) \cdot h(\alpha_0(a)) \\ &= u(a_1) \cdot s \cdot u(x_1) \cdot h(y_1). \end{aligned}$$

Thus, $x_1 = -\alpha_{-1}(a) \cdot \alpha_0(a)$ and $y_1 = \alpha_0(a)$.

By using the multiplication laws that we described in Proposition 2, we also have

$$\begin{aligned} u(a) \cdot s \cdot u(b) \cdot s \cdot u(-b) &= u(a - b^{-1}) \cdot s \cdot u(-b) \cdot h(b) \cdot u(-b) \\ &= u(b_1) \cdot s \cdot u(-b - b^3) \cdot h(b) \\ &= u(b_1) \cdot s \cdot u(-b \cdot [1 + b^2]) \cdot h(b) \\ &= u(b_1) \cdot s \cdot u(-\beta_0(a, b) \cdot \gamma_0(a, b)) \cdot h(\beta_0(a, b)) \\ &= u(b_1) \cdot s \cdot u(x'_1) \cdot h(y'_1). \end{aligned}$$

Thus,

$$x'_0 = -\beta_{-1}(a, b) \cdot [\alpha_{-1}(a) + b \cdot \beta_{-1}(a, b)]$$

and

$$y'_0 = \beta_{-1}(a, b).$$

Now, assume by induction that

$$x_r = -\alpha_{r-2}(a) \cdot \alpha_{r-1}(a),$$

$$y_r = \alpha_{r-1}(a),$$

$$x'_r = -\beta_{r-1}(a, b) \cdot [\alpha_{r-1}(a) + b \cdot \beta_{r-1}(a, b)],$$

and

$$y'_r = \beta_{r-1}(a, b)$$

for $r \leq k$, and we prove the correctness of the proposition for $r = k + 1$. By using our induction hypothesis, Proposition 2, and the identity

$$\alpha_{k-1}^2(a) = 1 + \alpha_k(a) \cdot \alpha_{k-2}(a)$$

from the last part of Proposition 11, the following hold:

$$\begin{aligned} [u(a) \cdot s]^{k+1} &= u(a) \cdot s \cdot [u(a) \cdot s]^k = \\ &= u(a) \cdot s \cdot u(a_k) \cdot s \cdot u(-\alpha_{k-2}(a) \cdot \alpha_{k-1}(a)) \cdot h(\alpha_{k-1}(a)) = \\ &= u(a - a_k^{-1}) \cdot s \cdot u(-a_k) \cdot h(a_k) \cdot u(-\alpha_{k-2}(a) \cdot \alpha_{k-1}(a)) \cdot h(\alpha_{k-1}(a)) = \\ &= u(a_{k+1}) \cdot s \cdot u(-\alpha_k(a) \cdot \alpha_{k-1}^{-1}(a)) \cdot h(\alpha_k(a) \cdot \alpha_{k-1}^{-1}(a)) \cdot \\ &= u(-\alpha_{k-2}(a) \cdot \alpha_{k-1}(a)) \cdot h(\alpha_{k-1}(a)) = \\ &= u(a_{k+1}) \cdot s \cdot u(-[\alpha_k(a) + \alpha_k^2(a) \cdot \alpha_{k-2}(a)] \cdot \alpha_{k-1}^{-1}(a)) \cdot h(\alpha_k(a)) = \\ &= u(a_{k+1}) \cdot s \cdot u(-[\alpha_k(a) \cdot [1 + \alpha_k(a) \cdot \alpha_{k-2}(a)]] \cdot \alpha_{k-1}^{-1}(a)) \cdot h(\alpha_k(a)) = \\ &= u(a_{k+1}) \cdot s \cdot u(-\alpha_k(a) \cdot \alpha_{k-1}(a)) \cdot h(\alpha_k(a)). \end{aligned}$$

Thus,

$$x_k = -\alpha_{k-2}(a) \cdot \alpha_{k-1}(a),$$

$$y_k = \alpha_{k-1}(a),$$

for every $1 \leq k \leq t-1$.

Similarly,

$$\begin{aligned} [u(a) \cdot s]^{k+1} \cdot [u(b) \cdot s \cdot u(-b)] &= u(a) \cdot s \cdot [u(a) \cdot s]^k \cdot [u(b) \cdot s \cdot u(-b)] = \\ u(a) \cdot s \cdot u(b_k) \cdot s \cdot u(-\beta_{k-1}(a, b) \cdot \gamma_{k-1}(a, b)) \cdot h(\beta_{k-1}(a, b)) &= \\ u(a - b_k^{-1}) \cdot s \cdot u(-b_k) \cdot h(b_k) \cdot \\ u(-\beta_{k-1}(a, b) \cdot \gamma_{k-1}(a, b)) \cdot h(\beta_{k-1}(a, b)) &= \\ u(b_{k+1}) \cdot s \cdot u(-\beta_k(a, b) \cdot \beta_{k-1}^{-1}(a, b)) \cdot h(\beta_k(a, b) \cdot \beta_{k-1}^{-1}(a, b)) \cdot \\ u(-\beta_{k-1}(a, b) \cdot \gamma_{k-1}(a, b)) \cdot h(\beta_{k-1}(a, b)) &= \\ u(b_{k+1}) \cdot s \cdot u(-[\beta_k(a, b) \cdot [1 + \beta_k(a, b) \cdot \gamma_{k-1}(a, b)]] \cdot \beta_{k-1}^{-1}(a, b)) \cdot h(\beta_k(a, b)) &= \\ u(b_{k+1}) \cdot s \cdot u(-\beta_k(a, b) \cdot \gamma_k(a, b)) \cdot h(\beta_k(a, b)). \end{aligned}$$

Thus,

$$x'_k = -\beta_{k-1}(a, b) \cdot [\alpha_{k-1}(a) + b \cdot \beta_{k-1}(a, b)] = -\beta_{k-1}(a, b) \cdot \gamma_{k-1}(a, b),$$

and

$$y'_k = \beta_{k-1}(a, b),$$

for every $0 \leq k \leq t-1$. $\square$

Proposition 12. Let $G = \text{PSL}_2(q)$. For every $1 \leq k \leq t-1$, $0 \leq \ell \leq t-1$, let a_k, b_ℓ be elements of $\mathbb{F}_q$ as defined in Proposition 8, and for $-1 \leq r \leq t-1$ let $\alpha_r(a)$, $\beta_r(a, b)$, and $\gamma_r(a, b)$ be elements of $\mathbb{F}_q$ as defined in Definitions 6 and 7. Then, the following hold:

•

$$\begin{aligned} [u(a) \cdot s]^k \cdot u(x) \cdot h(y) &= \\ u(a_k) \cdot s \cdot u(\alpha_{k-1}(a) \cdot [x - \alpha_{k-2}(a)]) \cdot h(\alpha_{k-1}(a) \cdot y) &= \\ u(a_k) \cdot s \cdot u(\alpha_{k-1}^2(a) \cdot [x - a_{t-k}]) \cdot h(\alpha_{k-1}(a) \cdot y) &= \\ u(a_k) \cdot s \cdot u(\alpha_{k-1}^2(a) \cdot [x + a_k - a]) \cdot h(\alpha_{k-1}(a) \cdot y); \end{aligned}$$

•

$$\begin{aligned} [u(a) \cdot s]^\ell \cdot [u(b) \cdot s \cdot u(-b)] \cdot u(x) \cdot h(y) &= \\ u(b_\ell) \cdot s \cdot u(\beta_{\ell-1}(a, b) \cdot [\beta_{\ell-1}(a, b) \cdot x - \gamma_{\ell-1}(a, b)]) \cdot h(\beta_{\ell-1}(a, b) \cdot y). \end{aligned}$$

Proof. The proof is straightforward, using Theorem 4 and Propositions 2 and 11. $\square$

Corollary 3. Let $g \in \text{PSL}_2(q)$ such that the matrix presentation of $\tilde{g}$ is as follows: $\tilde{g} = \begin{pmatrix} r_1 & -r_2^{-1} \\ r_2 & 0 \end{pmatrix}$ for some $r_1 \in \mathbb{F}_q$ and $r_2 \in \mathbb{F}_q^*$. Let $a_k \in \mathbb{F}_q$ as defined in Proposition 8, and $\alpha_k(a)$, $\beta_k(a, b)$, and $\gamma_k(a, b)$ as defined in Definitions 6 and 7. Then, $g = u(\tilde{a}) \cdot s \cdot h(\tilde{y})$ such that $\tilde{y} = r_2$, $\tilde{a} = r_1 \cdot r_2^{-1}$, and one of the following holds:

- If $\tilde{a} = a_k$ for $1 \leq k < \frac{q+1}{\gcd(2, q+1)}$, then $g = [u(a) \cdot s]^k \cdot u(x) \cdot h(y)$ such that $x = a_{t-k} = a - a_k$ ($t = \frac{q+1}{\gcd(2, q+1)}$);
- If $\tilde{a} = b_k$ for $0 \leq k < \frac{q+1}{\gcd(2, q+1)}$ and q is odd, then $g = [u(a) \cdot s]^k \cdot [u(b) \cdot s \cdot u(-b)] \cdot u(x) \cdot h(y)$ such that $x = \gamma_{k-1}(a, b) \cdot \beta_{k-1}^{-1}(a, b) = b + \alpha_{k-1}(a) \cdot \beta_{k-1}^{-1}(a, b)$.

Proof. The proof is a direct consequence of Proposition 12. $\square$

4. Conclusions

The results of this paper provide intriguing connections between the *BN-pair* presentation and the *OGS* presentation of $PSL_2(q)$, which is a family of finite simple groups, where $q \geq 4$. These connections allow us to study the interesting properties of some important recursive sequences over a finite field $\mathbb{F}_q$. These are closely connected to Dickson polynomials and Chebyshev polynomials of the second kind (and, in special cases, to Dickson and Chebyshev polynomials of the first kind). The results motivate us to further research the open questions regarding the connections between the mentioned presentations (*BN-pair* and *OGS*) of $PSL_n(q)$ for $n > 2$ and other families of simple Lie-type groups.

Author Contributions: Conceptualization, R.S.; Methodology, R.S.; Validation, R.S. and H.Y.; Formal analysis, R.S. and H.Y.; Investigation, R.S.; Resources, R.S.; Data curation, R.S.; Writing—original draft, R.S.; Writing—review & editing, R.S.; Visualization, R.S.; Supervision, R.S.; Project administration, R.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by the research authority of Ariel University.

Data Availability Statement: No new data were created in this study.

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

Abbreviations

The following abbreviations are used in this manuscript:

$\mathbb{F}_q$	The finite field with q elements
$\mathbb{F}_q^*$	The set of non-zero elements of the finite field with q elements
$PSL_n(q)$	The $n \times n$ projective special linear group over $\mathbb{F}_q$
$P_a(\lambda)$	The polynomial $\lambda^2 - a \cdot \lambda + 1$
$\gcd(x, y)$	The greatest common divisor of x and y
$ G $	The order of the group G
$G_1 \supseteq G_2$	G_2 is a normal subgroup of G_1
$\langle B, N \rangle$	The group that is generated by the elements of the sets B and N
$E_k(a, 1)$	The Dickson polynomial of the second kind of degree k over $\mathbb{F}_q$, on variable a and with parameter 1
$T_k(b)$	The Chebyshev polynomial of the first kind of degree k on variable b
$U_k(b)$	The Chebyshev polynomial of the second kind of degree k on variable b
Fib_k	The k -th element of the Fibonacci sequence

References

1. Miller, G.A. Groups which are the products of two permutable proper subgroups. *Proc. Natl. Acad. Sci. USA* **1935**, *21*, 469–472.
2. Szép, J. On the structure of groups which can be represented as the product of two subgroups. *Acta Sci. Math. Szeged* **1950**, *12*, 57–61.
3. Zappa, G. Sulla costruzione dei gruppi prodotto di due dati sottogruppi permutabili traloro. *Atti Secondo Congresso Un. Mat. Ital.* **1942**, *1942*, 119–125.
4. Arad, Z.; Fisman, E. On finite factorizable groups. *J. Algebra* **1984**, *86*, 522–548.
5. Hall, P. A note on soluble groups. *J. Lond. Math. Soc.* **1928**, *3*, 98–105.
6. Holt, D.; Rowley, P. On products of Sylow subgroups in finite groups. *Arch. Mathematik* **1993**, *60*, 105–107.
7. Vasco, M.; Rötteler, M.; Steinweidt, R. On minimal length factorizations of finite groups. *Exp. Math.* **2003**, *12*, 1–12.
8. Ore, O. Structures and group theory. *I. Duke Math. J.* **1937**, *3*, 149–174.
9. Douglas, J. On Finite Groups with Two Independent Generators I. *Proc. Natl. Acad. Sci. USA* **1951**, *37*, 604–610.
10. Douglas, J. On Finite Groups with Two Independent Generators II. *Proc. Natl. Acad. Sci. USA* **1951**, *37*, 677–691.
11. Douglas, J. On Finite Groups with Two Independent Generators III. *Proc. Natl. Acad. Sci. USA* **1951**, *37*, 749–760.
12. Douglas, J. On Finite Groups with Two Independent Generators IV. *Proc. Natl. Acad. Sci. USA* **1951**, *37*, 808–813.
13. Shwartz, R.; Adin, R.M.; Roichman, Y. Major Indices and Perfect Bases for Complex Reflection Groups. *Electron. J. Comb.* **2008**, *15*, 61.
14. Shwartz, R.; Fanrazi, L.; Khazkeia, S. Generalization of the basis theorem for alternating groups. *Funct. Differ. Equ.* **2019**, *26*, 125–140.
15. Bjorner, A.; Brenti, F. Combinatorics of Coxeter groups. In *Graduate Texts in Mathematics*; Springer: Berlin/Heidelberg, Germany, 2004; Volume 231.

16. Shwartz, R. Canonical forms for dihedral and symmetric groups. *Electron. J. Comb.* **2019**, *26*, P4.46.
17. Shephard, G.C.; Todd, J.A. Finite unitary reflection groups. *Can. J. Math.* **1954**, *6*, 274–304.
18. Hölder, O. Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen. *Math. Ann.* **1889**, *34*, 26–56.
19. Jordan, C. Théorème sur les équations algébriques. *Comptes Rendus Acad. Sci. Paris* **1869**, *68*, 257–258.
20. Jordan, C. Traité des substitutions et des équations algébriques. *Comptes Rendus Acad. Sci. Paris* **1870**, 114–125.
21. Schreier, O. Ueber den Jordan–Hölderschen Satz. *Abh. Math. Sem. Univ. Hamburg* **1928**, *6*, 300–302.
22. Gorenstein, D. *The Classification of Finite Simple Groups*; Plenum Press: New York, NY, USA, 1983; Volume MR86i, p. 20024.
23. Aschbacher, M.; Smith, S.D. The Classification of Quasithin Groups: I. Structure of Strongly Quasithin K-groups. *Math. Surv. Monogr.* **2004**, *111*, 477.
24. Tits, J. Algebraic and abstract simple groups. *Ann. Math. Second Ser.* **1964**, *80*, 313–329.
25. Tits, J. *Buildings of Spherical Type and Finite BN-Pairs*; Lecture Notes in Mathematics; Springer: Berlin, Germany; New York, NY, USA, 1974; Volume 386.
26. Steinberg, R. *Lectures on Chevalley Groups*; Yale University: New Haven, CT, USA, 1957.
27. Dickson, L.E. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group I,II. *Ann. Math.* **1897**, *11*, 65–120.
28. Rivlin, T.J. *Chebyshev Polynomials: From Approximation Theory to Algebra and Number Theory*, 2nd ed.; Pure and Applied Mathematics; Wiley: New York, NY, USA, 1990.
29. Shwartz, R.; Yadayi, H. Sequences over Finite Fields Defined by OGS and BN-pair Decomposition of $PSL_2(q)$ Recursively. Preprint. Available online: <https://arxiv.org/pdf/1812.05311.pdf> (accessed on 18 January 2023).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.