J. Math. Cryptol. **7** (2013), 147–179
DOI 10.1515/jmc-2013-5000

Strongly aperiodic logarithmic signatures

Reiner Staszewski and Tran van Trung

Communicated by Spyros Magliveras

Abstract. Logarithmic signatures for finite groups are the essential constituent of public key cryptosystems MST_1 and MST_3. Especially they form the main component of the private key of MST_3. Regarding the use of MST_3, it has become a vital issue to construct new classes of logarithmic signatures having features that do not share with the well-known class of transversal or fused transversal logarithmic signatures. For this purpose Baumeister and de Wiljes recently presented an interesting method of constructing aperiodic logarithmic signatures for abelian groups. In this paper we introduce the concept of strongly aperiodic logarithmic signatures and show their constructions for abelian p-groups on the basis of the Baumeister–de Wiljes method.

Keywords. Public-key cryptosystem MST_3, aperiodic logarithmic signature, strongly aperiodic logarithmic signature, Baumeister–de Wiljes method.

2010 Mathematics Subject Classification. 94A60, 20K01.

1 Introduction

The public key cryptosystems MST_1 (see [8]) and MST_3 (see [5,11]) are developed on the basis of logarithmic signatures, a kind of factorization of finite groups. The basic idea for building MST_3 is to construct trapdoor one-way functions using random covers for finite non-abelian groups having a large center. An integrated trapdoor information, which forms the main part of the private key of the scheme, employs logarithmic signatures of the center. The Suzuki 2-groups have been proposed as the underlying groups for an instantiation of MST_3. The first analysis of the simple version of MST_3 (see [5]) due to Magliveras, Svaba, Tran van Trung and Zajac [9] shows that transversal logarithmic signatures are unfit for use in the scheme. A further investigation of Blackburn, Cid and Mullan [2] proves that the use of fused transversal logarithmic signatures also makes the simple version of MST_3 insecure. However, for the strengthened version of MST_3 (see [11]), it is shown that fused transversal logarithmic signatures still withstand the powerful matrix-permutation attack (see [11]). It is therefore essential to study further

classes of logarithmic signatures having features that would be more suitable for use in public key cryptosystems like MST_3.

In a recent paper [1] Baumeister and de Wiljes propose an interesting method for constructing aperiodic logarithmic signatures for abelian groups, in particular, for abelian 2-groups, that thwart the Blackburn–Cid–Mullan attack. It is worth mentioning that transversal or fused transversal logarithmic signatures have the property of being periodic. In this paper we introduce the concept of strongly aperiodic logarithmic signatures and present their constructions for abelian p-groups based on the Baumeister–de Wiljes method. Aperiodic and strongly aperiodic logarithmic signatures provide classes of logarithmic signatures having features befitting the use of MST_3. Moreover, we are convinced that strongly aperiodic logarithmic signatures for abelian groups are also of theoretical interest in their own right.

2 Preliminaries

In this section we briefly present notation, definitions and some basic facts about logarithmic signatures, covers for finite groups and their induced mappings. For more details the reader is referred to [6, 8]. The group theoretic notation used is standard and may be found in any textbook.

Let $\mathcal{G}$ be a finite abstract group, we define the *width* of $\mathcal{G}$ to be the positive integer $w = \lceil \log |\mathcal{G}| \rceil$. Let $\mathcal{S}$ be a subset of $\mathcal{G}$ and let $\alpha = [A_1, A_2, \ldots, A_s]$ be an ordered collection of ordered subsets $A_i = \{a_{i,1}, \ldots, a_{i,r_i}\}$ of $\mathcal{G}$, such that $\sum_{i=1}^{s} |A_i|$ is bounded by a polynomial in $\log |\mathcal{S}|$. Then we say that α is a *cover* for $\mathcal{S}$, if every product $a_{1,j_1} \cdots a_{s,j_s}$ lies in $\mathcal{S}$ and if every $g \in \mathcal{S}$ can be written as

$$g = a_{1,j_1} \cdots a_{s,j_s} \tag{2.1}$$

with $a_{i,j_i} \in A_i$. If, moreover, the expression in (2.1) is unique for every $g \in \mathcal{S}$, then α is called a *logarithmic signature* for $\mathcal{S}$. We denote by $\mathcal{C}(\mathcal{S} \subseteq \mathcal{G})$ and $\Lambda(\mathcal{S} \subseteq \mathcal{G})$ the respective collections of *covers* and *logarithmic signatures* for $\mathcal{S} \subseteq \mathcal{G}$. When $\mathcal{S} = \mathcal{G}$, we simply write $\mathcal{C}(\mathcal{G})$ and $\Lambda(\mathcal{G})$ instead of $\mathcal{C}(\mathcal{G} \subseteq \mathcal{G})$ and $\Lambda(\mathcal{G} \subseteq \mathcal{G})$. A cover or a logarithmic signature $\alpha = [A_1, A_2, \ldots, A_s]$ for a group $\mathcal{G}$ is said to be *proper* if $|A_i| \neq 1$ and $A_i \neq \mathcal{G}$, for every i, $1 \leq i \leq s$. We assume that all covers and logarithmic signatures are proper. The product $a_{1,j_1} \cdots a_{s,j_s}$ in (2.1) is called a *factorization* of g with respect to α.

Let $\alpha = [A_1, \ldots, A_s]$ be a cover for $\mathcal{G}$ with $r_i = |A_i|$, then the A_i are called the *blocks* of α and the vector $(r_1, \ldots, r_s)$ of block lengths r_i the *type* of α. We define the *length* of α to be the integer $\ell(\alpha) = \sum_{i=1}^{s} r_i$.

Let $\Gamma = \{(\mathcal{G}_\ell, \alpha_\ell)\}_{\ell \in \mathbb{N}}$ be a family of pairs, indexed by the security parameter ℓ, where the $\mathcal{G}_\ell$ are groups in a common representation, and where α_ℓ is a specific

cover for $\mathcal{G}_\ell$ of length polynomial in ℓ. We say that Γ is *tame* if there exists a probabilistic polynomial time algorithm $\mathcal{A}$ such that for each $g \in \mathcal{G}_\ell$, $\mathcal{A}$ accepts (α_ℓ, g) as input, and outputs a factorization of g with respect to α_ℓ (as in equation (2.1)) with overwhelming probability of success. We say that Γ is *wild* if for any probabilistic polynomial time algorithm $\mathcal{A}$, the probability that $\mathcal{A}$ succeeds in factorizing a random element g of $\mathcal{G}_\ell$ is negligible. In other words Γ is tame if there exists an algorithm by means of which the factorization in (2.1) for each instance $\{(\mathcal{G}, \alpha_\ell)\}$ can be achieved in time polynomial in $\lceil \log |\mathcal{G}_\ell| \rceil$; and Γ is wild if it is not tame. Often we simply say α_ℓ is tame or wild.

For finite groups there are instances $\{(\mathcal{G}, \alpha_\ell)\}_\ell$ where the factorization in (2.1) is believed to be hard: For example, let q be a prime power for which the discrete logarithm problem in the multiplicative group of a finite field $\mathbb{F}_q$ is believed to be hard. Suppose that $2^{\ell-1} \leq q - 1 < 2^\ell$, and let $\mathcal{G}_\ell$ be the multiplicative group $\mathbb{F}_q^*$ just mentioned. Let f be a generator of $\mathcal{G}_\ell$. If $\alpha_\ell = [A_1, A_2, \ldots, A_\ell]$, where $A_i = [1, f^{2^{i-1}}]$, then α_ℓ is a cover of $\mathcal{G}_\ell$, and factorization with respect to α_ℓ amounts to solving the discrete logarithm problem (DLP) in $\mathcal{G}_\ell$.

Let $\alpha = [A_1, A_2, \ldots, A_s]$ be a cover of type $(r_1, r_2, \ldots, r_s)$ for $\mathcal{S} \subseteq \mathcal{G}$ with $A_i = [a_{i,1}, a_{i,2}, \ldots, a_{i,r_i}]$ and let $m = \prod_{i=1}^{s} r_i$. Let $m_1 = 1$ and $m_i = \prod_{j=1}^{i-1} r_j$ for $i = 2, \ldots, s$. Let τ denote the canonical bijection from $Z_{r_1} \oplus \mathbb{Z}_{r_2} \oplus \cdots \oplus \mathbb{Z}_{r_s}$ on $\mathbb{Z}_m$; i.e.,

$$\tau : \mathbb{Z}_{r_1} \oplus \mathbb{Z}_{r_2} \oplus \cdots \oplus \mathbb{Z}_{r_s} \to \mathbb{Z}_m, \quad \tau(j_1, j_2, \ldots, j_s) := \sum_{i=1}^{s} j_i m_i.$$

Using τ we now define the surjective mapping $\breve{\alpha}$ induced by α.

$$\breve{\alpha} : \mathbb{Z}_m \to \mathcal{S}, \quad \breve{\alpha}(x) := a_{1,j_1} \cdot a_{2,j_2} \cdots a_{s,j_s},$$

where $(j_1, j_2, \ldots, j_s) = \tau^{-1}(x)$. Since τ and τ^{-1} are efficiently computable, the mapping $\breve{\alpha}(x)$ is efficiently computable.

Conversely, given a cover α and an element $y \in \mathcal{S}$, to determine any element $x \in \breve{\alpha}^{-1}(y)$ it is necessary to obtain any one of the possible factorizations of type (2.1) for y and determine indices $j_1, j_2, \ldots, j_s$ such that $y = a_{1,j_1} \cdot a_{2,j_2} \cdots a_{s,j_s}$. This is possible if and only if α is tame. Once a vector $(j_1, j_2, \ldots, j_s)$ has been determined, $\breve{\alpha}^{-1}(y) = \tau(j_1, j_2, \ldots, j_s)$ can be computed efficiently.

Two covers (logarithmic signatures) α, β are said to be *equivalent* if $\breve{\alpha} = \breve{\beta}$.

It is worth noting that random covers and logarithmic signatures have been used to construct pseudorandom number generators which are suitable for cryptographic applications [7, 10].

3 The cryptosystem MST_3

Let $\mathcal{G}$ be a finite non-abelian group with nontrivial center $\mathcal{Z}$ such that $\mathcal{G}$ does not split over $\mathcal{Z}$. Assume further that $\mathcal{Z}$ is sufficiently large so that exhaustive search problems are computationally not feasible in $\mathcal{Z}$. We describe the strengthened version of MST_3 (see [11]).

Alice chooses a large group $\mathcal{G}$ as described above and generates

(1) a tame logarithmic signature $\beta = [B_1, B_2, \ldots, B_s] := (b_{ij})$ of type $(r_1, r_2, \ldots, r_s)$ for $\mathcal{Z}$;

(2) a random cover $\alpha = [A_1, A_2, \ldots, A_s] := (a_{ij})$ of the same type as β for a certain subset $\mathcal{J}$ of $\mathcal{G}$ such that $A_1, \ldots, A_s \subseteq \mathcal{G} \setminus \mathcal{Z}$.

She further selects $t_0, t_1, \ldots, t_s \in \mathcal{G} \setminus \mathcal{Z}$, a homomorphism $f : \mathcal{G} \to \mathcal{Z}$ and computes

(3) $\gamma = (h_{i,j})$, $h_{i,j} = t_{i-1}^{-1} \cdot a_{i,j} \cdot f(a_{i,j}) \cdot b_{i,j} \cdot t_i$.

Alice publishes her public key (α, γ), keeping $(\beta, t_0, t_1, \ldots, t_s, f)$ as her private key.

To encrypt a message $x \in \mathcal{Z}$ Bob chooses a random number $R \in \mathbb{Z}_{|\mathcal{Z}|}$, $R \neq 0$, computes

$$y_1 = \breve{\alpha}(R) \cdot x, \quad y_2 = \breve{\gamma}(R) \cdot x = t_0^{-1} \cdot \breve{\alpha}(R) \cdot f(\breve{\alpha}(R)) \cdot \breve{\beta}(R) \cdot t_s \cdot x,$$

and sends $y = (y_1, y_2)$ to Alice. To decrypt $y = (y_1, y_2)$ Alice computes

$$\breve{\beta}(R) = f(\breve{\alpha}(R))^{-1} \cdot y_1^{-1} \cdot t_0 \cdot y_2 \cdot t_s^{-1} = f(y_1)^{-1} \cdot y_1^{-1} \cdot t_0 \cdot y_2 \cdot t_s^{-1}$$

by using the fact that $f(y_1) = f(\breve{\alpha}(R))$, she then computes R from $\breve{\beta}(R)$ which is efficiently computable as β is tame. She computes $\breve{\alpha}(R)$ and recovers x from y_1.

In the description above if we choose f as the trivial homomorphism, i.e., $f(g) = 1_{\mathcal{G}}$ for all $g \in \mathcal{G}$, we obtain the simple version of the cryptosystem MST_3 (see [5]). The use of nontrivial homomorphism f considerably strengthens the scheme as shown in [11]. The homomorphism f is used to mask the secret logarithmic signature β with information computed from cover α. We refer the reader to [5, 11] for more detailed information about MST_3.

As an instantiation of MST_3 it has been suggested that the Suzuki 2-groups [3] might be used for the underlying groups [5, 11]. Let $q = 2^m$ with $3 \leq m \in \mathbb{N}$ such that the field $\mathbb{F}_q$ has a nontrivial automorphism θ of odd order, i.e., m is not a power of 2. Then a Suzuki 2-group $\mathcal{G}$ can be briefly described as follows:

$$\mathcal{G} := \{(a, b) \in \mathbb{F}_q \times \mathbb{F}_q \mid (a_1, b_1) \times (a_2, b_2) = (a_1 + a_2, b_1 + b_2 + a_1^{\theta} a_2)\}.$$

Thus $\mathcal{G}$ has order q^2 and $\mathbb{Z}(\mathcal{G}) = \Phi(\mathcal{G}) = \mathcal{G}' = \Omega_1(\mathcal{G}) = \{(0, b) \mid b \in \mathbb{F}_q\}$. In particular the center $\mathbb{Z}(\mathcal{G})$ is elementary abelian of order q.

4 Classes and transformations of logarithmic signatures

In this section we briefly discuss *classes* of logarithmic signatures and basic *transformations* on logarithmic signatures for a group $\mathcal{G}$.

Let $\gamma : 1_{\mathcal{G}} = \mathcal{G}_0 < \mathcal{G}_1 < \cdots < \mathcal{G}_s = \mathcal{G}$ be a chain of subgroups of $\mathcal{G}$, and let A_i be an ordered, complete set of right (or left) coset representatives of $\mathcal{G}_{i-1}$ in $\mathcal{G}_i$. Then $[A_1, \ldots, A_s]$ forms a logarithmic signature for $\mathcal{G}$, called *exact transversal logarithmic signature*. We denote the collection of all exact transversal logarithmic signatures for a group $\mathcal{G}$ by $\mathcal{ET}(\mathcal{G})$. A logarithmic signature α for a group $\mathcal{G}$ is called *transversal* if α is equivalent to a $\beta \in \mathcal{ET}(\mathcal{G})$, otherwise α is called *non-transversal*. Further, if none of the blocks of α is a coset of a non-trivial subgroup of $\mathcal{G}$, then α is called *totally non-transversal*. We will denote the class of transversal, non-transversal, and totally non-transversal logarithmic signatures for $\mathcal{G}$ by $\mathcal{T}(\mathcal{G})$, $\mathcal{NT}(\mathcal{G})$, and $\mathcal{TNT}(\mathcal{G})$ respectively.

We list some basic transformations on logarithmic signatures. By applying certain transformations on a logarithmic signature, new logarithmic signatures will be derived. Let $\alpha = [A_1, \ldots, A_s] \in \Lambda(\mathcal{G})$.

- *Element shuffle:* Permute the elements within each block of α.
- *Block shuffle:* If $\mathcal{G}$ is non-abelian, permuting two blocks of α may result in a cover for a certain subset of $\mathcal{G}$. If $\mathcal{G}$ is abelian, then the result of a block shuffle is indeed a logarithmic signature.
- *Two sided transformation:* Let $g_0, g_1, \ldots, g_s \in \mathcal{G}$. Define a new logarithmic signature $\beta = [B_1, \ldots, B_s]$ by $B_i = g_{i-1}^{-1} A_i g_i$. Then β is called a *two sided transform* of α. When $g_0 = g_s = 1$, we say that β is a *sandwich* of α. When $g_0 = 1$, β is said to be a *right translation* of α by g_s. If $g_s = 1$, then β is called a *left translation* of α by g_0.
- *Fusion:* If $\mathcal{G}$ is non-abelian, then replacing two consecutive blocks A_i and A_{i+1}, $1 \le i \le s-1$, by a single block $B = A_i A_{i+1} := \{xy \mid x \in A_i,\ y \in A_{i+1}\}$ will result in a logarithmic signature. B is called a *fused* block. If $\mathcal{G}$ is abelian, the fusion transformation can be done on any two blocks of α.
- *Automorphism action:* If φ is an automorphism of $\mathcal{G}$, then $\beta = [B_1, \ldots, B_s]$ with $B_i = \varphi(A_i)$, $1 \le i \le s$, is a logarithmic signature for $\mathcal{G}$.

5 Aperiodic logarithmic signatures and the Baumeister–de Wiljes construction

Investigating tame aperiodic logarithmic signatures for abelian groups is a problem of theoretical interest and of practical importance. They present a new class

of logarithmic signatures beyond the well-known classes of transversal and their fused logarithmic signatures which are all periodic. Regarding cryptosystem MST_3 aperiodic logarithmic signatures appear to be especially significant.

Definition 5.1. A non-empty subset X of a group $\mathcal{G}$ is called *periodic* if there exists an element $g \in \mathcal{G} \setminus \{1_{\mathcal{G}}\}$ such that $gX = X$. Such an element g is called a *period* of X. The set of all periods of X will be denoted by $P(X)$, i.e., $P(X) = \{g \in \mathcal{G} \setminus \{1_{\mathcal{G}}\} : gX = X\}$.

Definition 5.2. A logarithmic signature $\alpha = [A_1, \ldots, A_s] \in \Lambda(\mathcal{G})$ is called *aperiodic* if none of the blocks A_i is periodic. The set of all aperiodic logarithmic signatures for $\mathcal{G}$ is denoted by $\mathcal{A}(\mathcal{G})$.

In [1], Baumeister and de Wiljes present an interesting method for constructing aperiodic signatures for abelian groups. The method is based on the theory in the book of Szabó [12], and it describes an approach to construct aperiodic logarithmic signatures for abelian groups. The method is not an algorithm in the strict sense, since the requirement posed by the method prohibits quickly its computational feasibility even for groups of moderate order. However, the basic idea of the method has proved to be useful, since it provides a technique for searching aperiodic logarithmic signatures for abelian groups. We now describe the Baumeister–de Wiljes construction.

Baumeister–de Wiljes construction. Let $\mathcal{G}$ be a finite abelian group. Let $\mathcal{H}$ be a subgroup of $\mathcal{G}$ and let $\mathcal{T}$ be a transversal of $\mathcal{H}$ in $\mathcal{G}$ (i.e., $\mathcal{T}$ is a complete set of coset representatives of $\mathcal{H}$ in $\mathcal{G}$).

(i) Let $\theta = [T_1, \ldots, T_s]$ be a logarithmic signature of type $(r_1, \ldots, r_s)$ for $\mathcal{T}$, where $T_i = \{t_{i,1}, \ldots, t_{i,r_i}\}$.

(ii) Suppose that for each i with $1 \le i \le s$ there exists a collection

$$\mathcal{L}_i = \{A_{i,1}, \ldots, A_{i,r_i}\}$$

of subsets $A_{i,j}$ of $\mathcal{H}$ such that any choice $[A_{1,j_1}, \ldots, A_{s,j_s}]$ with $A_{i,j_i} \in \mathcal{L}_i$ forms a logarithmic signature for $\mathcal{H}$.

(iii) Then $\beta := [B_1, \ldots, B_s]$ defined by $B_i = t_{i,1}A_{i,1} \cup \ldots \cup t_{i,r_i}A_{i,r_i}$ for $1 \le i \le s$ forms a logarithmic signature of type $(\ell_1, \ldots, \ell_s)$ for $\mathcal{G}$, where $\ell_i = \sum_{j=1}^{r_i} |A_{i,j}|$.

For any subsets A, B of a group $\mathcal{G}$ we say that B is a *translate* of A if there is an element $g \in \mathcal{G}$ such that $gA = B$. The translate B is called *proper* if $A \neq B$.

Baumeister and de Wiljes give the following characterization of aperiodicity for the constructed logarithmic signature β.

Proposition 5.3. *Suppose that $A_{i,j}$ is not a translate of $A_{i,k}$ for any $j,k \in \{1,\dots,r_i\}$. Then B_i is periodic if and only if*

$$\bigcap_{j=1}^{r_i} P(A_{i,j}) \neq \emptyset.$$

The main idea of the Baumeister–de Wiljes construction of aperiodic logarithmic signatures is to find sets $\mathcal{L}_i$ satisfying condition (ii).

Example 5.4. Let $\mathcal{G}$ be an elementary abelian 2-group of order 2^9 generated by $g_1, g_2, \dots, g_9$. Let $\mathcal{H} := \langle g_1, g_2, g_3, g_4, g_5, g_6\rangle$ and $\mathcal{T} = \langle g_7, g_8, g_9\rangle$. Set $\theta = [T_1, T_2, T_3]$ with $T_1 = \{1, g_7\}$, $T_2 = \{1, g_8\}$, $T_3 = \{1, g_9\}$. Define

$$\mathcal{L}_1 = \big\{A_{1,1} = \{1, g_1, g_2, g_1g_2\}, A_{1,2} = \{1, g_1g_3, g_2g_4, g_1g_3g_2g_4\}\big\},$$
$$\mathcal{L}_2 = \big\{A_{2,1} = \{1, g_3, g_4, g_3g_4\}, A_{2,2} = \{1, g_1g_2g_3, g_1g_4, g_2g_3g_4\}\big\},$$
$$\mathcal{L}_3 = \big\{A_{3,1} = \{1, g_5, g_6, g_5g_6\}, A_{3,2} = \{1, g_1g_3g_5, g_2g_4g_6, g_1g_2g_3g_4g_5g_6\}\big\}.$$

It can be checked that each of the eight combinations $[A_{1,j_1}, A_{2,j_2}, A_{3,j_3}]$ with $j_1, j_2, j_3 \in \{1,2\}$ forms a logarithmic signature for $\mathcal{H}$. We thus obtain an aperiodic logarithmic signature $\beta = [B_1, B_2, B_3]$ of type $(8,8,8)$ with

$$B_1 = \big\{1, g_1, g_2, g_1g_2, g_7, g_1g_3g_7, g_2g_4g_7, g_1g_3g_2g_4g_7\big\},$$
$$B_2 = \big\{1, g_3, g_4, g_3g_4, g_8, g_1g_2g_3g_8, g_1g_4g_8, g_2g_3g_4g_8\big\},$$
$$B_3 = \big\{1, g_5, g_6, g_5g_6, g_9, g_1g_3g_5g_9, g_2g_4g_6g_9, g_1g_2g_3g_4g_5g_6g_9\big\}.$$

The aperiodicity of β follows from Proposition 5.3, since $A_{i,1} \cap A_{i,2} = \{1\}$ for all $i = 1,2,3$.

An important property of logarithmic signatures constructed by the Baumeister–de Wiljes method is that they are tame when certain conditions are satisfied (see [1,4]). The result is given by the following theorem.

Theorem 5.5. *Let $\beta := [B_1, \dots, B_s]$ be a logarithmic signature constructed by the Baumeister–de Wiljes method. Assume that θ and all logarithmic signatures $[A_{1,j_1}, \dots, A_{s,j_s}]$, $1 \le j_i \le r_i$ and $1 \le i \le s$, are tame. If θ and $\mathcal{L}_1, \dots, \mathcal{L}_s$ are known, then β is tame.*

Proof. Let $g \in \mathcal{G}$ be an element that we want to factorize with respect to β. Then there exist unique elements $t \in \mathcal{T}$ and $h \in \mathcal{H}$ such that $g = ht$. Since θ is tame, we can find a factorization of $t = t_{1,j_1} \cdots t_{s,j_s}$ with respect to θ in time bounded by $O(w^{c_1})$, where $w = \lceil \log |\mathcal{G}| \rceil$ and c_1 is a constant. Having obtained $(j_1, \ldots, j_s)$ we can determine the logarithmic signature $[A_{1,j_1}, \ldots, A_{s,j_s}]$ which is tame by the assumption. So, the complexity of factoring $h = a_{1,k_1} \cdots a_{s,k_s}$ with respect to $[A_{1,j_1}, \ldots, A_{s,j_s}]$ is bounded by $O(w^{c_2})$, where c_2 is a constant. Thus

$$g = ht = a_{1,k_1} \cdots a_{s,k_s} t_{1,j_1} \cdots t_{s,j_s} = \underbrace{(a_{1,k_1} t_{1,j_1})}_{\in B_1} \cdots \underbrace{(a_{s,k_s} t_{s,j_s})}_{\in B_s}.$$

Finding $a_{i,k_i} t_{i,j_i} \in B_i$ only requires a time of $O(\log_2(|B_i|))$ when B_i is sorted. It follows that β is tame. □

6 Strongly aperiodic logarithmic signatures for abelian groups

Within the class $\mathcal{A}(\mathcal{G})$ of aperiodic logarithmic signatures, we are interested in a subclass called *strongly aperiodic logarithmic signatures*, which we denote by $\mathcal{SA}(\mathcal{G})$.

A simple observation shows that the aperiodicity property of a logarithmic signature is preserved under the transformations described above, except the fusion. Fusing two or more blocks of an aperiodic logarithmic signature may result in a periodic logarithmic signature. Observe that if we fuse all the blocks of a logarithmic signature β, we obtain one block, namely the group $\mathcal{G}$ itself, which is in turn a trivial periodic logarithmic signature. We will exclude this trivial case. Thus a fusion can be done on any set of at most $s - 1$ blocks of β. In general, we might expect that any nontrivial fusion is permitted, however it is not always so as we can see from the following results shown in the book of Szabó [12] for abelian p-groups.

Theorem 6.1. *Let p be a prime and let $\mathcal{G}$ be an abelian group of order p^n. Further let $r_1 \geq r_2 \geq \cdots \geq r_s \geq p$ be powers of p such that*

$$\prod_{i=1}^{s} r_i = p^n.$$

(i) ([12, Theorem 7.3.1]) *Suppose $p = 2$ and $\mathcal{G}$ is an elementary abelian 2-group. A logarithmic signature α of type $(r_1, \ldots, r_s)$ with $r_1 \geq \cdots \geq r_s \geq 2$ can only be aperiodic if we have*

- *$s = 2$ and $r_2 \geq 8$, or*
- *$s \geq 3$ and $r_1 \geq 8$, $r_2 \geq \cdots \geq r_s \geq 4$.*

α is always periodic for each of the following cases:

- $r_s = 2$,
- $s = 2$ *and* $r_2 | 4$,
- $s \geq 3$ *and* $r_1 | 4, \ldots, r_s | 4$.

(ii) ([12, Theorem 2.3.2]) *Suppose* $p = 3$ *and* $\mathcal{G}$ *is not cyclic or of type* $(3^{n-1}, 3)$. *Suppose further that* $(r_1, \ldots, r_s) \notin \{(3, \ldots, 3), (3^2, 3, \ldots, 3), (3^{n-1}, 3)\}$. *Then there exist aperiodic logarithmic signatures of type* $(r_1, \ldots, r_s)$ *for* $\mathcal{G}$.

(iii) ([12, Theorem 2.3.1]) *Suppose* $p \geq 5$, $\mathcal{G}$ *is not cyclic and* $(r_1, \ldots, r_s) \neq (p, \ldots, p)$. *Then there exist aperiodic logarithmic signatures of type* $(r_1, \ldots, r_s)$ *for* $\mathcal{G}$.

Now suppose that we have an aperiodic logarithmic signature $\beta = [B_1, \ldots, B_s]$ with $s \geq 3$ for an elementary abelian 2-group $\mathcal{G}$. Note that from Theorem 6.1 we have $|B_1| \geq 8$ and $|B_i| \geq 4$ for $2 \leq i \leq s$. If β is of type $|B_i| \geq 8$ for $1 \leq i \leq s$, then we say that β is strongly aperiodic when any fusion of at most $s - 1$ blocks results in an aperiodic logarithmic signature. However, suppose, for instance, $|B_1| = 8$ and $|B_2| = \cdots = |B_s| = 4$. Then β is strongly aperiodic if any fusion of its blocks results in an aperiodic logarithmic signature γ, when the type of γ satisfies the conditions of aperiodicity of Theorem 6.1. This says, in particular, that if block B_1 would be fused with $(s - 2)$ other blocks, we would obtain a logarithmic signature γ of type $(2^{3+2(s-2)}, 4)$, which is periodic due to Theorem 6.1. Hence, this type of fusion for β is "non-admissible". In other words, block B_1 can be fused with at most $(s - 3)$ other blocks. Moreover, fusing all blocks $B_2, \ldots, B_s$ of β together is admissible, as it will result in a logarithmic signature of type $(8, 2^{2(s-1)})$ that does not violate the aperiodicity condition of Theorem 6.1.

Theorem 6.1 motivates the following definition.

Definition 6.2. Let $\mathcal{G}$ be an abelian group and let $\beta = [B_1, \ldots, B_s] \in \mathcal{A}(\mathcal{G})$. A fusion of certain d blocks $B_{i_1}, \ldots, B_{i_d}$ is called *admissible*, if the type of the resulting logarithmic signature γ does not violate necessary conditions for being aperiodic. Let $\{d_1, \ldots, d_t\}$ be the set of positive integers whose d_i indicates the largest possible number of blocks permitted by an admissible fusion of a certain "type". The values $d_1, \ldots, d_t$ are called the *admissible fusion degrees* of β. We say that β achieves the admissible fusion degrees, if for each $d_i \in \{d_1, \ldots, d_t\}$, any "admissible" fusion of d_i blocks of β results in an aperiodic logarithmic signature.

For example, let $\beta = [B_1, B_2, \ldots, B_s]$, $s \geq 3$, be an aperiodic logarithmic signature of type $(8, 4, 4, \ldots, 4)$ for an elementary abelian group $\mathcal{G}$ of order 2^{2s+1}. Then from Theorem 6.1 and Definition 6.2, the admissible fusion degrees of β are $\{s-2, s-1\}$.

Definition 6.3. Let $\mathcal{G}$ be an abelian group and let $\beta = [B_1, \ldots, B_s] \in \mathcal{A}(\mathcal{G})$. The logarithmic signature β is called *strongly aperiodic* if it achieves its admissible fusion degrees.

Remark 6.4. It seems not meaningful to extend Definition 6.3 to non-abelian groups. This is because a fusion of non-consecutive blocks is almost prohibited, since the result is no longer a logarithmic signature in this case.

Example 6.5. We use the setup for $\mathcal{G}$, $\mathcal{H}$ and $\mathcal{T}$ and θ as in Example 5.4. Define

$$\mathcal{L}_1 = \{A_{1,1} = \{1, g_1, g_2, g_1g_2\}, A_{1,2} = \{1, g_1g_2g_4g_6, g_2g_3g_5, g_1g_3g_4g_5g_6\}\},$$
$$\mathcal{L}_2 = \{A_{2,1} = \{1, g_3, g_4, g_3g_4\}, A_{2,2} = \{1, g_1g_3, g_2g_4, g_1g_3g_2g_4\}\},$$
$$\mathcal{L}_3 = \{A_{3,1} = \{1, g_5, g_6, g_5g_6\}, A_{3,2} = \{1, g_1g_5, g_2g_6, g_1g_5g_2g_6\}\}.$$

Then we obtain an aperiodic logarithmic signature $\beta = [B_1, B_2, B_3]$ of type $(8, 8, 8)$ for $\mathcal{G}$ with

$$B_1 = \{1, g_1, g_2, g_1g_2, g_7, g_1g_2g_4g_6g_7, g_2g_3g_5g_7, g_1g_3g_4g_5g_6g_7\},$$
$$B_2 = \{1, g_3, g_4, g_3g_4, g_8, g_1g_3g_8, g_2g_4g_8, g_1g_3g_2g_4g_8\},$$
$$B_3 = \{1, g_5, g_6, g_5g_6, g_9, g_1g_5g_9, g_2g_6g_9, g_1g_5g_2g_6g_9\}.$$

Now, it can be checked that the fusion of any two blocks of β yields an aperiodic block. Hence β is strongly aperiodic.

Remark 6.6. We note that the logarithmic signature β in Example 5.4 is aperiodic but not strongly aperiodic. For, when fusing B_1 with B_2 we obtain a periodic block. Even more, B_1B_2 is a subgroup of order 2^6 in $\mathcal{G}$.

As we will use the Baumeister–de Wiljes construction (*BW-construction* for short) to investigate strongly aperiodic logarithmic signatures, we make use of the following simple observation about the fusion operation on a logarithmic signature obtained from the BW-construction.

Lemma 6.7. *We use the notation as described in the BW-construction above. The fusion of blocks B_i and B_j, $i \neq j$, of β results in a logarithmic signature, which is again derived from the BW-construction, in which $\mathcal{L}_i$ and $\mathcal{L}_j$ are replaced by $\mathcal{L}_i\mathcal{L}_j$ and T_i and T_j by T_iT_j.*

The next lemma is useful for the query about the strong aperiodicity of a logarithmic signature.

Lemma 6.8. *Let $\mathcal{G}$ be an abelian group. Let $\beta = [B_1, \ldots, B_s]$ be a logarithmic signature for $\mathcal{G}$. Let $I \subseteq \{1, \ldots, s\}$. Suppose that the fused block $\prod_{i \in I} B_i$ is aperiodic. Then $\prod_{j \in J} B_j$ is aperiodic for any non-empty subset $J \subseteq I$.*

Proof. Recall that element shuffle does not effect periodicity. Assume, by contradiction, that $B_J := \prod_{j \in J} B_j$ is periodic for a subset $J \subseteq I$. Let $g \in \mathcal{G} \setminus \{1\}$ be a period for B_J. Set $B_I := \prod_{i \in I} B_i$. We may write $B_I = B_J \cdot C$, where $C := \prod_{k \in I \setminus J} B_k$ (note that B_I on the left side of equality $B_I = B_J \cdot C$ is considered as an unordered set, since permuting the elements of B_I does not effect the property of aperiodicity). Now, since g is a period for B_J, we have $gB_I = gB_J \cdot C = B_J \cdot C = B_I$. Thus g is a period for B_I, a contradiction. □

Lemma 6.8 is a crucial tool. Suppose we want to verify the strong aperiodicity of a logarithmic signature β having s blocks. Suppose further that we are allowed to fuse up to any $s - 1$ blocks of β. Without Lemma 6.8 we have to check all $\binom{s}{1} + \binom{s}{2} + \cdots + \binom{s}{s-1} = 2^s - 2$ possible fusions of the blocks of β. Whereas by using Lemma 6.8 we only need to check $\binom{s}{s-1} = s$ fusions of all combinations of $s - 1$ blocks of β.

In the remaining sections we present constructions of strongly aperiodic signatures for elementary abelian p-groups. The basic tool we use is the BW-construction. We first construct certain types of aperiodic logarithmic signatures, and then in a further more involved step we prove that they are strongly aperiodic.

From now on let $\mathcal{G}$ be an elementary abelian p-group. We use additive notation for the group operation and 0 will denote the identity of $\mathcal{G}$. In fact we identify $\mathcal{G}$ with the additive group of the Galois field $\mathbb{F}_{p^n}$. In this way $\mathcal{G}$ is viewed as a vector space of dimension n over $\mathbb{F}_p$, and thus we may freely use the language of linear algebra with respect to $\mathcal{G}$. For example, a minimal generator set for $\mathcal{G}$ may be called a basis for $\mathcal{G}$.

7 Strongly aperiodic logarithmic signatures of type $(p^3, \ldots, p^3)$

In this section we first construct a strongly aperiodic logarithmic signature of type $(p^3, \ldots, p^3)$ for an elementary abelian p-group $\mathcal{G}$ of order p^{3s}, where $p = 2$ or p is an odd prime and $s \geq 2$. Let $v_1, v_2, \ldots, v_{2s}, \ldots, v_{3s}$ be a generator set of $\mathcal{G}$. Using the BW-construction, we define

(i) $\mathcal{T} = \langle v_{2s+1}, \ldots, v_{3s} \rangle$ and $\theta = [T_1, \ldots, T_s]$ with

$$T_i = \{0, v_{2s+i}, 2v_{2s+i}, \ldots, (p-1)v_{2s+i}\}, \quad i = 1, \ldots, s;$$

(ii) $\mathcal{H} = \langle v_1, \ldots, v_{2s} \rangle$.

Let $u \in \{1, \ldots, p-1\} = \mathbb{F}_p \setminus \{0\}$ be a chosen parameter. For $i = 1, \ldots, s$ define the collection

$$\mathcal{L}_i = \{A_{i,0}, A_{i,1}, \ldots, A_{i,(p-1)}\}$$

as follows:

$$A_{1,0} = \langle v_1, v_2 \rangle,$$
$$A_{1,j} = \Big\langle v_1 + v_2 + j \cdot \sum_{\ell=2}^{s} v_{2\ell}, u \cdot v_2 + j \cdot \sum_{\ell=2}^{s} v_{2\ell-1} \Big\rangle, \quad j \in \{1, \ldots, p-1\},$$
$$A_{i,j} = \langle v_{2i-1} + j v_1, v_{2i} + j v_2 \rangle, \quad i \in \{2, \ldots, s\},\ j \in \{0, \ldots, p-1\}.$$

Remark 7.1. Note that in (i) we may replace $\mathcal{T}$ by any transversal $\mathcal{TR}$ of $\mathcal{H}$. Here $\mathcal{TR}$ is not a subgroup in general. In fact, it is simple to create a logarithmic signature for a transversal of $\mathcal{H}$ by passing to the quotient group $\bar{\mathcal{T}} = \mathcal{G}/\mathcal{H}$. Namely, let $\bar{\theta} = [\bar{T}_1, \ldots, \bar{T}_s]$ be a logarithmic signature for $\bar{\mathcal{T}}$, where $\bar{T}_i = [x_{i,0}\mathcal{H}, \ldots, x_{i,(p-1)}\mathcal{H}]$, $1 \le i \le s$. Note that there are $|\mathcal{H}|$ possibilities for choosing $x_{i,j}$ as coset representative. By lifting $\bar{\theta}$ to $\mathcal{G}$ we obtain a logarithmic signature $\theta = [T_1, \ldots, T_s]$ with $T_i = [x_{i,0}, \ldots, x_{i,(p-1)}]$ for a certain transversal $\mathcal{TR}$ of $\mathcal{H}$.

We now prove that the subsets $A_{i,j}$ of $\mathcal{L}_i$, $1 \le i \le s$, satisfy condition (ii) of the BW-construction. This means that for any $(j_1, j_2, \ldots, j_s) \in \{0, 1, \ldots, p-1\}^s$ the collection $[A_{1,j_1}, A_{2,j_2}, \ldots, A_{s,j_s}]$ forms a logarithmic signature for $\mathcal{H}$. This is equivalent to say that the basis elements of $A_{1,j_1}, A_{2,j_2}, \ldots, A_{s,j_s}$ are linearly independent.

We first consider the case $j_1 = 0$. We then have

$$\begin{aligned}
A_{1,j_1} &= \langle v_1, v_2 \rangle, \\
A_{2,j_2} &= \langle j_2 \cdot v_1 + v_3, j_2 \cdot v_2 + v_4 \rangle, \\
A_{3,j_3} &= \langle j_3 \cdot v_1 + v_5, j_3 \cdot v_2 + v_6 \rangle, \\
&\vdots \\
A_{s,j_s} &= \langle j_s \cdot v_1 + v_{2s-1}, j_s \cdot v_2 + v_{2s} \rangle.
\end{aligned}$$

When forming a linear combination of the basis elements of $A_{1,0}, A_{2,j_2}, \ldots, A_{s,j_s}$ for the zero element, we have

$$\begin{aligned}
0 = {} & \lambda_{1,1}.(v_1) + \lambda_{1,2}.(v_2) + \lambda_{2,1}.(v_{2i-1} + j_2 v_1) + \lambda_{2,2}.(v_{2i} + j_2 v_2) \\
& + \cdots + \lambda_{s,1}.(v_{2s-1} + j_s v_1) + \lambda_{s,2}.(v_{2s} + j_s v_2) \qquad (7.1)
\end{aligned}$$

with $\lambda_{i,j} \in \mathbb{F}_p$. The matrix form of equation (7.1) is given by

$$(\lambda_{1,1}, \lambda_{1,2}, \ldots, \lambda_{s,1}, \lambda_{s,2})M = (0, 0, \ldots, 0),$$

where M is the following $(2s \times 2s)$-matrix over $\mathbb{F}_p$:

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ j_2 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & j_2 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ j_3 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & j_3 & 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ j_s & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & j_s & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}.$$

As M is a lower triangular matrix with all 1 on the main diagonal, M is invertible and equation (7.1) has $\lambda_{i,j} = 0$ for all $1 \le i \le s$ and $1 \le j \le 2$ as the unique solution. Thus the basis elements of $A_{1,0}, A_{2,j_2}, \ldots, A_{s,j_s}$ are linearly independent. This says, in particular, that $[A_{1,0}, A_{2,j_2}, \ldots, A_{s,j_s}]$ forms a logarithmic signature for $\mathcal{H}$.

We now consider the case $j_1 \neq 0$. We then have

$$\begin{aligned} A_{1,j_1} &= \Big\langle v_1 + v_2 + j_1 \sum_{\ell=2}^{s} v_{2\ell}, u \cdot v_2 + j_1 \sum_{\ell=2}^{s} v_{2\ell-1} \Big\rangle, \\ A_{2,j_2} &= \langle j_2 \cdot v_1 + v_3, j_2 \cdot v_2 + v_4 \rangle, \\ A_{3,j_3} &= \langle j_3 \cdot v_1 + v_5, j_3 \cdot v_2 + v_6 \rangle, \\ &\vdots \\ A_{s,j_s} &= \langle j_s \cdot v_1 + v_{2s-1}, j_s \cdot v_2 + v_{2s} \rangle, \end{aligned}$$

and we obtain a linear combination of the zero element as follows:

$$\begin{aligned} 0 = {} & \lambda_{1,1}.\Big(v_1 + v_2 + j_1 \cdot \sum_{\ell=2}^{s} v_{2\ell}\Big) + \lambda_{1,2}.\Big(u \cdot v_2 + j_1 \cdot \sum_{\ell=2}^{s} v_{2\ell-1}\Big) \\ & + \lambda_{2,1}.(v_{2i-1} + j_2 v_1) + \lambda_{2,2}.(v_{2i} + j_2 v_2) \\ & + \cdots + \lambda_{s,1}.(v_{2s-1} + j_s v_1) + \lambda_{s,2}.(v_{2s} + j_s v_2). \end{aligned} \tag{7.2}$$

The coefficient matrix M of equation (7.2) has the form

$$M = \begin{pmatrix} 1 & 1 & 0 & j_1 & 0 & j_1 & \cdots & j_1 & 0 & j_1 \\ 0 & u & j_1 & 0 & j_1 & 0 & \cdots & 0 & j_1 & 0 \\ j_2 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & j_2 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ j_3 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & j_3 & 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ j_s & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & j_s & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}.$$

By subtracting j_1 times the rows $4, 6, \ldots, 2s$ from the first row, and j_1 times the rows $3, 5, \ldots, 2s-1$ from the second row of M we obtain the matrix

$$\begin{pmatrix} 1 & 1 - j_1 \cdot \sum_{l=2}^{s} j_l & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ -j_1 \cdot \sum_{l=2}^{s} j_l & u & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ j_2 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & j_2 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ j_3 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & j_3 & 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ j_s & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & j_s & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}$$

with determinant $u + (1 - J)J = -(J^2 - J - u)$ where $J := j_1 \cdot \sum_{\ell=2}^{s} j_\ell$. Since for each given p we can choose a $u \in \mathbb{F}_p \setminus \{0\}$ such that the polynomial $X^2 - X - u \in \mathbb{F}_p[X]$ has no root in $\mathbb{F}_p$, we can conclude that matrix M is invertible and therefore equation (7.2) has a unique solution with $\lambda_{i,j} = 0$ for all $1 \le i \le s$ and $1 \le j \le 2$. So the basis elements of $A_{1,j_1}, A_{2,j_2}, \ldots, A_{s,j_s}$ are linearly independent. Hence $[A_{1,j_1}, A_{2,j_2}, \ldots, A_{s,j_s}]$ forms a logarithmic signature for $\mathcal{H}$.

Thus we have constructed a logarithmic signature β of type $(p^3, \ldots, p^3)$ for $\mathcal{G}$ by the method of Baumeister and de Wiljes. By using Proposition 5.3 and the fact that $A_{i,j} \cap A_{i,k} = \{0\}$ for any $A_{i,j}, A_{i,k} \in \mathcal{L}_i$ with $j \neq k$ and for all $1 \le i \le s$, we conclude that β is aperiodic.

The strong aperiodicity of β will be proved by the following theorem.

Theorem 7.2. *The above constructed logarithmic signature β of type $(p^3, \ldots, p^3)$ is strongly aperiodic.*

Proof. Recall that Lemma 6.7 says that fusing any two blocks of β results in a logarithmic signature, which is again obtained from the BW-construction. By using Lemma 6.8 we need only to consider the fusion of any $(s-1)$ blocks of β. Finally, we use Proposition 5.3 to show that the resulting logarithmic signature derived from each such fusion is aperiodic. This is done by showing that the fusion of any $(s-1)$ collections $\mathcal{L}_i$ yields a collection of subgroups of $\mathcal{G}$ having only the identity element 0 of $\mathcal{G}$ in their intersection.

We consider three cases.

Case (a) Fusing $\mathcal{L}_2, \ldots, \mathcal{L}_s$.

Let $\mathcal{L}_2 + \cdots + \mathcal{L}_s$ denote the collection obtained by fusing $\mathcal{L}_2, \ldots, \mathcal{L}_s$. The subsets of $\mathcal{L}_2 + \cdots + \mathcal{L}_s$ are of the form $(A_{2,j_2} + A_{3,j_3} + \cdots + A_{s,j_s})$ with $(j_2, j_3, \ldots, j_s) \in \{0, 1, \ldots, p-1\}^{s-1}$.

We now prove that

$$\bigcap_{\substack{(j_2,j_3,\ldots,j_s)\\ \in\{0,1,\ldots,p-1\}^{s-1}}} (A_{2,j_2} + A_{3,j_3} + \cdots + A_{s,j_s}) = \{0\}.$$

Observe that

$$\begin{aligned}
&(A_{2,0} + A_{3,0} + \cdots + A_{s,0}) \cap (A_{2,1} + A_{3,0} + \cdots + A_{s,0}) \\
&= \langle v_3, v_4, v_5, v_6, \ldots, v_{2s-1}, v_{2s} \rangle \cap \langle v_1 + v_3, v_2 + v_4, v_5, v_6, \ldots, v_{2s-1}, v_{2s} \rangle \\
&= \langle v_5, v_6, \ldots, v_{2s-1}, v_{2s} \rangle = A_{3,0} + A_{4,0} + \cdots + A_{s,0}.
\end{aligned}$$

Similarly, we have

$$\begin{aligned}
&(A_{2,0} + A_{3,0} + A_{4,0} + \cdots + A_{s,0}) \cap (A_{2,0} + A_{3,1} + A_{4,0} + \cdots + A_{s,0}) \\
&\quad = A_{2,0} + A_{4,0} + \cdots + A_{s,0}, \ \ldots, \\
&(A_{2,0} + \cdots + A_{s-1,0} + A_{s,0}) \cap (A_{2,0} + \cdots + A_{s-2,0} + A_{s-1,1} + A_{s,0}) \\
&\quad = A_{2,0} + A_{3,0} + \cdots + A_{s-2,0} + A_{s,0}, \\
&(A_{2,0} + \cdots + A_{s-1,0} + A_{s,0}) \cap (A_{2,0} + A_{3,0} + \cdots + A_{s-1,0} + A_{s,1}) \\
&\quad = A_{2,0} + A_{3,0} + \cdots + A_{s-1,0}.
\end{aligned}$$

Obviously, the intersection of the elements on the right-hand side of the equalities is trivial.

Case (b) Fusing $\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_{s-1}$.
We prove that

$$\bigcap_{\substack{(j_1,j_2,\ldots,j_{s-1})\\ \in\{0,1,\ldots,p-1\}^{s-1}}} (A_{1,j_1} + A_{2,j_2} + \cdots + A_{s-1,j_{s-1}}) = \{0\}.$$

Recall that

$$\begin{aligned}
&A_{1,0} = \langle v_1, v_2\rangle,\\
&A_{1,j} = \Big\langle v_1 + v_2 + j\cdot\sum_{\ell=2}^{s} v_{2l}, u\cdot v_2 + j\cdot\sum_{\ell=2}^{s} v_{2\ell-1}\Big\rangle, \quad j\in\{1,\ldots,p-1\},\\
&A_{i,j} = \langle v_{2i-1} + jv_1, v_{2i} + jv_2\rangle, \quad i\in\{2,\ldots,s\},\ j\in\{0,\ldots,p-1\}.
\end{aligned}$$

So we have

$$\begin{aligned}
&(A_{1,0} + A_{2,0} + \cdots + A_{s-1,0}) \cap (A_{1,1} + A_{2,0} + \cdots + A_{s-1,0})\\
&\quad = \langle v_1, v_2, v_3, v_4, \ldots, v_{2s-3}, v_{2s-2}\rangle\\
&\qquad \cap \Big\langle v_1 + v_2 + \sum_{\ell=2}^{s} v_{2\ell}, u\cdot v_2 + \sum_{\ell=2}^{s} v_{2\ell-1}, v_3, v_4, \ldots, v_{2s-3}, v_{2s-2}\Big\rangle\\
&\quad = \langle v_3, v_4, \ldots, v_{2s-3}, v_{2s-2}\rangle = A_{2,0} + A_{3,0} + \cdots + A_{s-1,0}.
\end{aligned}$$

Consider further the intersection

$$\begin{aligned}
&(A_{2,0} + A_{3,0} + \cdots + A_{s-1,0}) \cap (A_{1,1} + A_{2,1} + A_{3,0} + \cdots + A_{s-1,0})\\
&\quad = (A_{2,0} + A_{3,0} + \cdots + A_{s-1,0}) \cap (A_{2,1} + A_{3,0} + \cdots + A_{s-1,0})\\
&\quad = \langle v_3, v_4, v_5, \ldots, v_{2s-3}, v_{2s-2}\rangle \cap \langle v_3 + v_1, v_4 + v_2, v_5, \ldots, v_{2s-3}, v_{2s-2}\rangle\\
&\quad = \langle v_5, v_6, \ldots, v_{2s-3}, v_{2s-2}\rangle = (A_{3,0} + \cdots + A_{s-1,0}).
\end{aligned}$$

Similarly,

$$\begin{aligned}
&(A_{3,0} + \cdots + A_{s-1,0}) \cap (A_{1,1} + A_{2,0} + A_{3,1} + A_{4,0} + \cdots + A_{s-1,0})\\
&= (A_{3,0} + \cdots + A_{s-1,0}) \cap (A_{2,0} + A_{3,1} + A_{4,0} + \cdots + A_{s-1,0})\\
&= \langle v_5, v_6, \ldots, v_{2s-3}, v_{2s-2}\rangle \cap \langle v_3, v_4, v_5 + v_1, v_6 + v_2, v_7, \ldots, v_{2s-3}, v_{2s-2}\rangle\\
&= \langle v_7, v_8, \ldots, v_{2s-3}, v_{2s-2}\rangle = A_{4,0} + \cdots + A_{s-1,0}.
\end{aligned}$$

This process can be iterated until we get $\{0\}$ as the intersection.

Case (c) Fusing $\mathcal{L}_1, \ldots, \mathcal{L}_{k-1}, \mathcal{L}_{k+1}, \ldots, \mathcal{L}_{s-1}, \mathcal{L}_s$ for all $k \in \{2, 3, \ldots, s-2, s-1\}$.

We claim that

$$\bigcap_{\substack{(j_1,\ldots,j_{k-1},\\ j_{k+1},\ldots,j_s)\\ \in\{0,1,\ldots,p-1\}^{s-1}}} (A_{1,j_1} + \cdots + A_{k-1,j_{k-1}} + A_{k+1,j_{k+1}} + \cdots + A_{s,j_s}) = \{0\}.$$

We define an isomorphism Φ of $\mathcal{G}$ as follows:

$$\Phi(v_i) = \begin{cases} v_{2s-1} & \text{if } i = 2k-1, \\ v_{2k-1} & \text{if } i = 2s-1, \\ v_{2s} & \text{if } i = 2k, \\ v_{2k} & \text{if } i = 2s, \\ v_i & \text{otherwise.} \end{cases}$$

Thus Φ interchanges v_{2k-1} with v_{2s-1} and v_{2k} with v_{2s}, and fixes the remaining generators. Then we have

$$\begin{aligned}
\Phi(A_{1,j_1}) &= \Phi\Big(\Big\langle v_1 + v_2 + j_1 \sum_{\ell=2}^{s} v_{2\ell}, u \cdot v_2 + j_1 \sum_{\ell=2}^{s} v_{2\ell-1} \Big\rangle\Big) = A_{1,j_1}, \\
\Phi(A_{2,j_2}) &= \Phi(\langle j_2 \cdot v_1 + v_3, j_2 \cdot v_2 + v_4 \rangle) = A_{2,j_2}, \\
&\vdots \\
\Phi(A_{k-1,j_{k-1}}) &= \Phi(\langle j_{k-1} \cdot v_1 + v_{2(k-1)-1}, j_2 \cdot v_2 + v_{2(k-1)} \rangle) = A_{k-1,j_{k-1}}, \\
\Phi(A_{k,j_k}) &= \Phi(\langle j_k \cdot v_1 + v_{2k-1}, j_k \cdot v_2 + v_{2k} \rangle) \\
&= \langle j_k \cdot v_1 + v_{2s-1}, j_k \cdot v_2 + v_{2s} \rangle = A_{s,j_k}, \\
\Phi(A_{k+1,j_{k+1}}) &= \Phi(\langle j_{k+1} \cdot v_1 + v_{2(k+1)-1}, j_2 \cdot v_2 + v_{2(k+1)} \rangle) = A_{k+1,j_{k+1}}, \\
&\vdots \\
\Phi(A_{s-1,j_{s-1}}) &= \Phi(\langle j_{s-1} \cdot v_1 + v_{2(s-1)-1}, j_2 \cdot v_2 + v_{2(s-1)} \rangle) = A_{s-1,j_{s-1}}, \\
\Phi(A_{s,j_s}) &= \Phi(\langle j_s \cdot v_1 + v_{2s-1}, j_s \cdot v_2 + v_{2s} \rangle) \\
&= \langle j_s \cdot v_1 + v_{2k-1}, j_s \cdot v_2 + v_{2k} \rangle = A_{k,j_s}.
\end{aligned}$$

From

$$\bigcap_{\substack{(j_1,j_2,\ldots,j_{s-1})\\ \in\{0,1,\ldots,p-1\}^{s-1}}} (A_{1,j_1} + A_{2,j_2} + \cdots + A_{s-1,j_{s-1}}) = \{0\}$$

we conclude that

$$\bigcap_{\substack{(j_1,j_2,\ldots,j_{s-1})\\ \in\{0,1,\ldots,p-1\}^{s-1}}} (\Phi(A_{1,j_1}) + \Phi(A_{2,j_2}) + \cdots + \Phi(A_{s-1,j_{s-1}})) = \{0\}.$$

This implies that

$$\bigcap_{\substack{(j_1,j_2,\ldots,j_{s-1})\\ \in\{0,1,\ldots,p-1\}^{s-1}}} (A_{1,j_1} + \cdots + A_{k-1,j_{k-1}} + \Phi(A_k, j_k) + A_{k+1,j_{k+1}} + \cdots + A_{s-1,j_{s-1}}) = \{0\}.$$

So we have

$$\bigcap_{\substack{(j_1,j_2,\ldots,j_{s-1})\\ \in\{0,1,\ldots,p-1\}^{s-1}}} (A_{1,j_1} + \cdots + A_{k-1,j_{k-1}} + A_{s,j_k} + A_{k+1,j_{k+1}} + \cdots + A_{s-1,j_{s-1}}) = \{0\},$$

which shows the claim. This completes the proof. □

Remark 7.3. The strongly aperiodic logarithmic signature β of type $(8, 8, 8)$ in Example 6.5 above is constructed by the method in this section.

8 Strongly aperiodic logarithmic signatures of type $(2^3, 2^2, \ldots, 2^2)$

In this section we will construct strongly aperiodic logarithmic signatures of type $(2^3, 2^2, \ldots, 2^2)$ for an elementary abelian 2-group $\mathcal{G}$ of order 2^{2s-1} with $s \geq 4$. Let $v_1, v_2, \ldots, v_s, v_{s+1}, \ldots, v_{2s-1}$ be a generator set of $\mathcal{G}$. Using the BW-construction, we define

(i) $\mathcal{T} = \langle v_{s+1}, \ldots, v_{2s-1}\rangle$ and $\theta = [T_1, T_3, T_4, \ldots, T_s]$ with $T_1 = \{0, v_{s+1}\}$ and $T_i = \{0, v_{s+(i-1)}\}$ for $i = 3, 4, \ldots, 2s$;

(ii) $\mathcal{H} = \langle v_1, \ldots, v_s\rangle$.

Note that for the reason of simplicity we have omitted $i = 2$ in indexing the collections $\mathcal{L}_i$ and also the blocks T_i so that we only have $s - 1$ blocks.

For $i = 1, 3, 4, \ldots, s$ define the collection

$$\mathcal{L}_i = \{A_{i,0}, A_{i,1}\}$$

as follows:

$$A_{1,0} = \langle v_1, v_2\rangle, \quad A_{1,1} = \Big\langle v_1 + \sum_{\ell=2}^{\lceil s/2\rceil} v_{2\ell-1}, v_2 + \sum_{\ell=2}^{\lfloor s/2\rfloor} v_{2\ell}\Big\rangle,$$

and, for $i = 3, \ldots, s$,

$$A_{i,0} = \langle v_i \rangle, \quad A_{i,1} = \Big\langle v_i + \sum_{\ell=1}^{\lfloor i/2 \rfloor} v_{2\ell} \Big\rangle, \qquad \text{if } i \text{ is odd,}$$

$$A_{i,0} = \langle v_i \rangle, \quad A_{i,1} = \Big\langle v_i + \sum_{\ell=1}^{i/2} v_{2\ell-1} \Big\rangle, \quad \text{if } i \text{ is even.}$$

Remark 8.1. In the same manner as in Remark 7.1, we may choose θ as a logarithmic signature for a certain transversal $\mathcal{TR}$ of $\mathcal{H}$ in $\mathcal{G}$.

At first we prove that for any choice of $(j_1, j_3, j_4, \ldots, j_s) \in \{0,1\}^{s-1}$ the corresponding collection $[A_{1,j_1}, A_{3,j_3}, \ldots, A_{s,j_s}]$ forms a logarithmic signature for $\mathcal{H}$. This is equivalent to show that the linear combination of the zero element of $\mathcal{G}$ with respect to the basis elements of $A_{1,j_1}, A_{3,j_3}, A_{4,j_4}, \ldots, A_{s,j_s}$, i.e.,

$$\begin{aligned} 0 = {} & \lambda_1 . \Big(v_1 + j_1 \sum_{\ell=2}^{\lceil s/2 \rceil} v_{2\ell-1} \Big) + \lambda_2 . \Big(v_2 + j_1 \sum_{\ell=2}^{\lfloor s/2 \rfloor} v_{2\ell} \Big) \\ & + \sum_{i=1}^{\lfloor (s-1)/2 \rfloor} \lambda_{2i+1} . \Big(v_{2i+1} + j_{2i+1} \sum_{\ell=1}^{i} v_{2\ell} \Big) \\ & + \sum_{i=2}^{\lceil (s-1)/2 \rceil} \lambda_{2i} . \Big(v_{2i} + j_{2i} \sum_{\ell=1}^{i} v_{2\ell-1} \Big) \end{aligned} \tag{8.1}$$

only has the trivial solution $\lambda_i = 0$ for all $i = 1, 3, \ldots, s$. This means that the $(s \times s)$ coefficient matrix $M_s(j_1, j_3, j_4, \ldots, j_s)$ for all λ_i of equation (8.1) is invertible.

If s is even, we have

$$M_s(j_1, j_3, j_4, \ldots, j_s) = \begin{pmatrix} 1 & 0 & j_1 & 0 & j_1 & 0 & \cdots & j_1 & 0 & j_1 & 0 \\ 0 & 1 & 0 & j_1 & 0 & j_1 & \cdots & 0 & j_1 & 0 & j_1 \\ 0 & j_3 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ j_4 & 0 & j_4 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & j_5 & 0 & j_5 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ j_6 & 0 & j_6 & 0 & j_6 & 1 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots \\ 0 & j_{s-3} & 0 & j_{s-3} & 0 & j_{s-3} & \cdots & 1 & 0 & 0 & 0 \\ j_{s-2} & 0 & j_{s-2} & 0 & j_{s-2} & 0 & \cdots & j_{s-2} & 1 & 0 & 0 \\ 0 & j_{s-1} & 0 & j_{s-1} & 0 & j_{s-1} & \cdots & 0 & j_{s-1} & 1 & 0 \\ j_s & 0 & j_s & 0 & j_s & 0 & \cdots & j_s & 0 & j_s & 1 \end{pmatrix}.$$

If s is odd, we have

$$M_s(j_1, j_3, j_4, \ldots, j_s) = \begin{pmatrix} 1 & 0 & j_1 & 0 & j_1 & 0 & \cdots & 0 & j_1 & 0 & j_1 \\ 0 & 1 & 0 & j_1 & 0 & j_1 & \cdots & j_1 & 0 & j_1 & 0 \\ 0 & j_3 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ j_4 & 0 & j_4 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & j_5 & 0 & j_5 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ j_6 & 0 & j_6 & 0 & j_6 & 1 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots \\ j_{s-3} & 0 & j_{s-3} & 0 & j_{s-3} & 0 & \cdots & 1 & 0 & 0 & 0 \\ 0 & j_{s-2} & 0 & j_{s-2} & 0 & j_{s-2} & \cdots & j_{s-2} & 1 & 0 & 0 \\ j_{s-1} & 0 & j_{s-1} & 0 & j_{s-1} & 0 & \cdots & 0 & j_{s-1} & 1 & 0 \\ 0 & j_s & 0 & j_s & 0 & j_s & \cdots & j_s & 0 & j_s & 1 \end{pmatrix}.$$

In both cases the matrix is invertible if $j_1 = 0$. Hence we assume that $j_1 = 1$.

We show by induction on s that the determinant of $M_s(j_1, j_3, j_4, \ldots, j_s)$ is 1 in both cases.

To begin with, if $s = 3$, we have

$$\det(M_3(j_1, j_3)) = \det \begin{pmatrix} 1 & 0 & j_1 \\ 0 & 1 & 0 \\ 0 & j_3 & 1 \end{pmatrix} = 1.$$

Now, let $s > 3$.

If s is even, we subtract j_s times the first row from the last row and obtain

$$\begin{aligned}
&\det(M_s(j_1, j_3, j_4, \ldots, j_s)) \\
&= \det \begin{pmatrix}
1 & 0 & j_1 & 0 & j_1 & 0 & \cdots & j_1 & 0 & j_1 & 0 \\
0 & 1 & 0 & j_1 & 0 & j_1 & \cdots & 0 & j_1 & 0 & j_1 \\
0 & j_3 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\
j_4 & 0 & j_4 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\
0 & j_5 & 0 & j_5 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\
j_6 & 0 & j_6 & 0 & j_6 & 1 & \cdots & 0 & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots \\
0 & j_{s-3} & 0 & j_{s-3} & 0 & j_{s-3} & \cdots & 1 & 0 & 0 & 0 \\
j_{s-2} & 0 & j_{s-2} & 0 & j_{s-2} & 0 & \cdots & j_{s-2} & 1 & 0 & 0 \\
0 & j_{s-1} & 0 & j_{s-1} & 0 & j_{s-1} & \cdots & 0 & j_{s-1} & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1
\end{pmatrix} \\
&= \det \begin{pmatrix}
1 & 0 & j_1 & 0 & j_1 & 0 & \cdots & j_1 & 0 & j_1 \\
0 & 1 & 0 & j_1 & 0 & j_1 & \cdots & 0 & j_1 & 0 \\
0 & j_3 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
j_4 & 0 & j_4 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & j_5 & 0 & j_5 & 1 & 0 & \cdots & 0 & 0 & 0 \\
j_6 & 0 & j_6 & 0 & j_6 & 1 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
0 & j_{s-3} & 0 & j_{s-3} & 0 & j_{s-3} & \cdots & 1 & 0 & 0 \\
j_{s-2} & 0 & j_{s-2} & 0 & j_{s-2} & 0 & \cdots & j_{s-2} & 1 & 0 \\
0 & j_{s-1} & 0 & j_{s-1} & 0 & j_{s-1} & \cdots & 0 & j_{s-1} & 1
\end{pmatrix} \\
&= \det(M_{s-1}(j_1, j_3, j_4, \ldots, j_{s-1})).
\end{aligned}$$

If s is odd, we subtract j_s times the second row from the last row and obtain

$$\det(M_s(j_1, j_3, j_4, \ldots, j_s))$$

$$= \det \begin{pmatrix} 1 & 0 & j_1 & 0 & j_1 & 0 & \cdots & 0 & j_1 & 0 & j_1 \\ 0 & 1 & 0 & j_1 & 0 & j_1 & \cdots & j_1 & 0 & j_1 & 0 \\ 0 & j_3 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ j_4 & 0 & j_4 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & j_5 & 0 & j_5 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ j_6 & 0 & j_6 & 0 & j_6 & 1 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots \\ j_{s-3} & 0 & j_{s-3} & 0 & j_{s-3} & 0 & \cdots & 1 & 0 & 0 & 0 \\ 0 & j_{s-2} & 0 & j_{s-2} & 0 & j_{s-2} & \cdots & j_{s-2} & 1 & 0 & 0 \\ j_{s-1} & 0 & j_{s-1} & 0 & j_{s-1} & 0 & \cdots & 0 & j_{s-1} & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \det \begin{pmatrix} 1 & 0 & j_1 & 0 & j_1 & 0 & \cdots & 0 & j_1 & 0 \\ 0 & 1 & 0 & j_1 & 0 & j_1 & \cdots & j_1 & 0 & j_1 \\ 0 & j_3 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ j_4 & 0 & j_4 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & j_5 & 0 & j_5 & 1 & 0 & \cdots & 0 & 0 & 0 \\ j_6 & 0 & j_6 & 0 & j_6 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ j_{s-3} & 0 & j_{s-3} & 0 & j_{s-3} & 0 & \cdots & 1 & 0 & 0 \\ 0 & j_{s-2} & 0 & j_{s-2} & 0 & j_{s-2} & \cdots & j_{s-2} & 1 & 0 \\ j_{s-1} & 0 & j_{s-1} & 0 & j_{s-1} & 0 & \cdots & 0 & j_{s-1} & 1 \end{pmatrix}$$

$$= \det(M_{s-1}(j_1, j_3, j_4, \ldots, j_{s-1})).$$

In both cases induction shows us that the determinant is 1. Hence

$$[A_{1,j_1}, A_{3,j_3}, \ldots, A_{s,j_s}]$$

forms a logarithmic signature for $\mathcal{H}$.

Thus we have constructed a logarithmic signature β of type $(2^3, 2^2, \ldots, 2^2)$ for $\mathcal{G}$ from the method of Baumeister and de Wiljes. By using Proposition 5.3 and the fact that $A_{i,1} \cap A_{i,2} = \{0\}$ for any $i = 1, 3, 4, \ldots, s$, we conclude that β is aperiodic.

Next we prove the following theorem.

Theorem 8.2. *The above constructed logarithmic signature β of type* $(2^3, 2^2, \ldots, 2^2)$ *is strongly aperiodic.*

The proof of the strong aperiodicity for β is given by a number of lemmas.

In view of Theorem 6.1, we have to consider two types of fusions for β: (a) fusing all $(s-1)$ blocks of size 2^2 each; (b) fusing any $(s-2)$ blocks, where one block is of size 2^3. By Lemmas 6.7, 6.8 and Proposition 5.3 we have to show that for type (a) the fusion of $\mathcal{L}_3, \mathcal{L}_4, \ldots, \mathcal{L}_s$ and for type (b) the fusion of $\mathcal{L}_1$ with any $(s-3)$ other collections $\mathcal{L}_i$ each yields a collection of subgroups of $\mathcal{G}$ having only the identity element 0 in their intersection.

Case (a) Fusing $\mathcal{L}_3, \mathcal{L}_4, \ldots, \mathcal{L}_s$.

Lemma 8.3.

$$\bigcap_{\substack{(j_3, j_4, \ldots, j_{s-1}, j_s) \\ \in \{0,1\}^{s-2}}} (A_{3,j_3} + A_{4,j_4} + \cdots + A_{s-1,j_{s-1}} + A_{s,j_s}) = \{0\}.$$

Proof. We consider the two sums

$$A_{3,0} + A_{4,0} + A_{5,0} + \cdots + A_{s-2,0} + A_{s-1,0} + A_{s,0} = \langle v_3, v_4, \ldots, v_{s-1}, v_s \rangle,$$
$$A_{3,0} + A_{4,0} + A_{5,0} + \cdots + A_{s-2,0} + A_{s-1,0} + A_{s,1}$$
$$= \langle v_3, v_4, \ldots, v_{s-2}, v_{s-1}, v_s + v_{s-1} + v_{s-3} + \cdots \rangle.$$

Their intersection is

$$\langle v_3, v_4, \ldots, v_{s-2}, v_{s-1} \rangle$$

because either v_1 or v_2 occurs as a summand in the last term of the second sum.

When intersecting $\langle v_3, v_4, \ldots, v_{s-2}, v_{s-1} \rangle$ further with the sum

$$A_{3,0} + A_{4,0} + A_{5,0} + \cdots + A_{s-3,0} + A_{s-2,0} + A_{s-1,1} + A_{s,0}$$
$$= \langle v_3, v_4, \ldots, v_{s-3}, v_{s-2}, v_s, (v_{s-1} + v_{s-2} + v_{s-4} + \cdots) \rangle,$$

we obtain

$$\langle v_3, v_4, \ldots, v_{s-3}, v_{s-2} \rangle$$

because either v_1 or v_2 occurs as a summand in the last two terms of the sum. By doing further iterations, we eventually get $\{0\}$ as intersection, as claimed. □

Case (b) Fusing $\mathcal{L}_1$ with $(s-3)$ other $\mathcal{L}_i$.

Now, let $I = \{i_1, \ldots, i_{s-3}\} \subseteq \{3, 4, \ldots, s\}$ be arbitrary with $|I| = s-3$. Let $\{3, 4, \ldots, s\} \setminus I = \{k_1, k_2\}$, where we assume that $k_1 < k_2$.

We have to prove that

$$\bigcap_{\substack{(j_1,j_3,j_4,\ldots,j_{k_1-1},j_{k_1+1},\ldots,\\ j_{k_2-1},j_{k_2+1},\ldots,j_s)\in\{0,1\}^{s-3}}} \Big(\sum_{i\in I\cup\{1\}} A_{i,j_i}\Big) = \{0\}. \tag{8.2}$$

Here we have

$$A_{1,0} + \sum_{i\in I} A_{i,0} = \langle v_1, v_2, v_{i_1}, v_{i_2}, \ldots, v_{k_1-1}, v_{k_1+1}, \ldots, v_{k_2-1}, v_{k_2+1}, \ldots, v_{i_{s-3}}\rangle.$$

There are three subcases which we have to handle separately.

(i) $k_1 \equiv k_2 \equiv 1 \bmod 2$,

(ii) $k_1 \equiv k_2 \equiv 0 \bmod 2$,

(iii) $k_1 + k_2 \equiv 1 \bmod 2$.

Lemma 8.4. *Suppose that* $k_1 \equiv k_2 \equiv 1 \bmod 2$. *Then equation* (8.2) *is satisfied.*

Proof. First consider

$$A_{1,1} + \sum_{i\in I} A_{i,0} = \langle v_1 + v_3 + v_5 + \cdots, v_2 + v_4 + v_6 + \cdots, v_{i_1}, v_{i_2}, \ldots, v_{k_1-1}, v_{k_1+1}, \ldots, v_{k_2-1}, v_{k_2+1}, \ldots, v_{i_{s-3}}\rangle.$$

Since $v_1 \notin A_{1,1} + \sum_{i\in I} A_{i,0}$ and $v_2 \in A_{1,1} + \sum_{i\in I} A_{i,0}$, we have

$$C := \Big(A_{1,0} + \sum_{i\in I} A_{i,0}\Big) \cap \Big(A_{1,1} + \sum_{i\in I} A_{i,0}\Big) = \langle \{v_2\} \cup \{v_i \mid i \in I\}\rangle.$$

To compute further intersections we need to introduce some notation.
For $i \in I$ let $\mathcal{A}_i$ be defined by

$$\mathcal{A}_i := A_{i,1} + \sum_{j\in I, j\neq i} A_{j,0}.$$

Then

$$\mathcal{A}_i = \big\langle \{v_j \mid j \in I \setminus \{i\}\} \cup \{v_i + v_{i-1} + v_{i-3} + \cdots\}\big\rangle.$$

For $i, j \in I$ let $\mathcal{A}_{i,j}$ be defined by

$$\mathcal{A}_{i,j} := A_{i,1} + A_{j,1} + \sum_{\ell\in I, \ell\neq i,j} A_{\ell,0}.$$

Then

$$\mathcal{A}_{i,j} = \big\langle \{v_\ell \mid \ell \in I \setminus \{i,j\}\} \cup \{v_i + v_{i-1} + v_{i-3} + \cdots, v_j + v_{j-1} + v_{j-3} + \cdots\}\big\rangle.$$

To prove (8.2) we proceed with a number of steps.

Step 1. k even and $k > k_1$.
We prove that

$$C \cap (A_{1,0} + \mathcal{A}_k) = \big\langle \{v_2\} \cup \{v_j \mid j \in I \setminus \{k\}\}\big\rangle.$$

Since we have

$$\begin{aligned} A_{1,0} + \mathcal{A}_k &= A_{1,0} + \big\langle \{v_j \mid j \in I \setminus \{k\}\} \cup \{v_k + v_{k-1} + v_{k-3} + \cdots\}\big\rangle \\ &= \big\langle \{v_j \mid j \in I \setminus \{k\}\} \cup \{v_1, v_2, v_k + v_{k-1} + v_{k-3} + \cdots\}\big\rangle, \end{aligned}$$

it is obvious that

$$\big\langle \{v_2\} \cup \{v_j \mid j \in I \setminus \{k\}\}\big\rangle \subseteq C \cap (A_{1,0} + \mathcal{A}_k).$$

Moreover, since $\langle \{v_2\} \cup \{v_j \mid j \in I \setminus \{k\}\}\rangle$ has codimension 1 in C, it suffices to show that $v_k \notin A_{1,0} + \mathcal{A}_k$. Suppose, by contradiction, that $v_k \in A_{1,0} + \mathcal{A}_k$. Then there exist $\lambda_1, \lambda_2, \ldots \in \{0,1\}$ with

$$v_k = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_k (v_k + v_{k-1} + v_{k-3} + \cdots) + \sum_{j \in I \setminus \{k\}} \lambda_j v_j.$$

But v_{k_1} occurs exactly once on the right-hand side of this equation (note that k is even, k_1 is odd and $k > k_1$), and we conclude $\lambda_k = 0$. But then

$$v_k = \lambda_1 v_1 + \lambda_2 v_2 + \sum_{j \in I \setminus \{k\}} \lambda_j v_j,$$

a contradiction. Hence, for all $k > k_1$ with k even, we have

$$C \cap (A_{1,0} + \mathcal{A}_k) = \big\langle \{v_2\} \cup \{v_j \mid j \in I \setminus \{k\}\}\big\rangle.$$

Let $I' := \{k \in I \mid k > k_1, k \text{ even}\}$. We conclude

$$\begin{aligned} C' := C \cap \Big(\bigcap_{k \in I'} (A_{1,0} + \mathcal{A}_k)\Big) &= \bigcap_{k \in I'} (C \cap (A_{1,0} + \mathcal{A}_k)) \\ &= \bigcap_{k \in I'} \big(\big\langle \{v_2\} \cup \{v_j \mid j \in I \setminus \{k\}\}\big\rangle\big) = \big\langle \{v_2\} \cup \{v_j \mid j \in I \setminus I'\}\big\rangle. \end{aligned}$$

Next, we prove that

$$C'' := C' \cap (A_{1,1} + \mathcal{A}_{k_1+1}) = \langle \{v_j \mid j \in I \setminus I'\} \rangle.$$

We have

$$\begin{aligned} &A_{1,1} + \mathcal{A}_{k_1+1} \\ &\quad = A_{1,1} + \langle \{v_j \mid j \in I \setminus \{k_1+1\}\} \cup \{v_{k_1+1} + v_{k_1} + v_{k_1-2} + \cdots\} \rangle \\ &\quad = \langle \{v_j \mid j \in I \setminus \{k_1+1\}\} \cup \{v_1 + v_3 + v_5 + \cdots, v_2 + v_4 + v_6 + \cdots, \\ &\qquad v_{k_1+1} + v_{k_1} + v_{k_1-2} + \cdots\} \rangle. \end{aligned}$$

Since $k_1 + 1 \in I'$, we clearly have $\langle \{v_j \mid j \in I \setminus I'\} \rangle \subseteq C''$.

Moreover, since $\langle \{v_j \mid j \in I \setminus I'\} \rangle$ has codimension 1 in C', it suffices to show that $v_2 \notin A_{1,1} + \mathcal{A}_{k_1+1}$. Suppose, by contradiction, that $v_2 \in A_{1,1} + \mathcal{A}_{k_1+1}$. Then there exist $\lambda_1, \lambda_2, \ldots \in \{0, 1\}$ with

$$\begin{aligned} v_2 = {} & \lambda_1(v_1 + v_3 + v_5 + \cdots) + \lambda_2(v_2 + v_4 + v_6 + \cdots) \\ & + \lambda_{k_1+1}(v_{k_1+1} + v_{k_1} + v_{k_1-2} + \cdots) + \sum_{j \in I \setminus \{k_1+1\}} \lambda_j v_j. \end{aligned}$$

But since v_{k_2} occurs exactly once on the right-hand side of this equation, we conclude that $\lambda_1 = 0$; also, since v_{k_1} occurs only once on the right-hand side of this equation, we conclude that $\lambda_{k_1+1} = 0$; further, since v_{k_1+1} occurs only once, we conclude that $\lambda_2 = 0$. But this is a contradiction.

Step 2. k even and $k < k_1$.

We prove that

$$C'' \cap (A_{1,1} + \mathcal{A}_{k,k_1+1}) = \langle \{v_j \mid j \in (I \setminus I') \setminus \{k\}\} \rangle.$$

We have

$$\begin{aligned} &A_{1,1} + \mathcal{A}_{k,k_1+1} \\ &\quad = A_{1,1} + \langle \{v_j \mid j \in I \setminus \{k, k_1+1\}\} \cup \{v_k + v_{k-1} + v_{k-3} + \cdots, \\ &\qquad v_{k_1+1} + v_{k_1} + v_{k_1-2} + \cdots\} \rangle \\ &\quad = \langle \{v_j \mid j \in I \setminus \{k, k_1+1\}\} \cup \{v_1 + v_3 + v_5 + \cdots, v_2 + v_4 + v_6 + \cdots, \\ &\qquad v_k + v_{k-1} + v_{k-3} + \cdots, v_{k_1+1} + v_{k_1} + v_{k_1-2} + \cdots\} \rangle. \end{aligned}$$

It is clear that

$$\langle \{v_j \mid j \in (I \setminus I') \setminus \{k\}\} \rangle \subseteq C'' \cap (A_{1,1} + \mathcal{A}_{k,k_1+1}).$$

Moreover, since $\langle\{v_j \mid j \in (I \setminus I') \setminus \{k\}\}\rangle$ has codimension 1 in C'', it suffices to show that $v_k \notin A_{1,1} + \mathcal{A}_{k,k_1+1}$. Suppose, by contradiction, that $v_k \in A_{1,1} + \mathcal{A}_{k,k_1+1}$. Then there exist $\lambda_1, \lambda_2, \ldots \in \{0, 1\}$ with

$$\begin{aligned} v_k = {} & \lambda_1(v_1 + v_3 + v_5 + \cdots) + \lambda_2(v_2 + v_4 + v_6 + \cdots) \\ & + \lambda_k(v_k + v_{k-1} + v_{k-3} + \cdots) \\ & + \lambda_{k_1+1}(v_{k_1+1} + v_{k_1} + v_{k_1-2} + \cdots) + \sum_{j \in I \setminus \{k, k_1+1\}} \lambda_j v_j. \end{aligned}$$

This implies that on the right-hand side of this equation the coefficient of v_k is equal to 1 and all other coefficients of v_j, $j \neq k$, are equal to 0. The set of respective coefficients of $\{v_{k_1+1}, v_{k_1}, v_1, v_2\}$ is

$$\{\lambda_2 + \lambda_{k_1+1} = 0, \lambda_1 + \lambda_{k_1+1} = 0, \lambda_1 + \lambda_k + \lambda_{k_1+1} = 0, \lambda_2 = 0\}.$$

It follows that $\lambda_2 = \lambda_1 = \lambda_k = \lambda_{k_1+1} = 0$. So $\lambda_2 + \lambda_k = 0$, but this is a contradiction because $\lambda_2 + \lambda_k$ is the coefficient of v_k and should be equal to 1.

Hence, for all $k < k_1$ with k even, we have

$$C'' \cap (A_{1,1} + \mathcal{A}_{k,k_1+1}) = \langle\{v_2\} \cup \{v_j \mid j \in (I \setminus I') \setminus \{k\}\}\rangle.$$

Let $I'' := \{k \in I \mid k < k_1, k \text{ even}\}$. We conclude

$$\begin{aligned} D := C'' \cap \Big(\bigcap_{k \in I''} (A_{1,1} + \mathcal{A}_{k,k_1+1})\Big) &= \bigcap_{k \in I''} (C'' \cap (A_{1,1} + \mathcal{A}_{k,k_1+1})) \\ &= \bigcap_{k \in I''} \big(\langle\{v_j \mid j \in (I \setminus I') \setminus \{k\}\}\rangle\big) \\ &= \langle\{v_j \mid j \in I \setminus (I' \cup I'')\}\rangle = \langle\{v_j \mid j \in I, j \text{ odd}\}\rangle. \end{aligned}$$

Step 3. k odd and $k < k_1$.

Let us write $I = I_o \cup I_e$, where I_o and I_e are the subsets of odd and even numbers in I, respectively. We prove that

$$D \cap (A_{1,1} + \mathcal{A}_{k,k+1}) = \langle\{v_j \mid j \in I_o \setminus \{k\}\}\rangle.$$

We have

$$\begin{aligned} & A_{1,1} + \mathcal{A}_{k,k+1} \\ & \quad = A_{1,1} + \langle\{v_j \mid j \in I \setminus \{k, k+1\}\} \cup \{v_k + v_{k-1} + v_{k-3} + \cdots, \\ & \qquad v_{k+1} + v_k + v_{k-2} + \cdots\}\rangle \end{aligned}$$

$$= \big\langle \{v_j \mid j \in I \setminus \{k, k+1\}\} \cup \{v_1 + v_3 + v_5 + \cdots, v_2 + v_4 + v_6 + \cdots, v_k + v_{k-1} + v_{k-3} + \cdots, v_{k+1} + v_k + v_{k-2} + \cdots\}\big\rangle.$$

Observe that

$$\big\langle \{v_j \mid j \in I_o \setminus \{k\}\}\big\rangle \subseteq D \cap (A_{1,1} + \mathcal{A}_{k,k+1}).$$

Moreover, since $\langle \{v_j \mid j \in I_o \setminus \{k\}\}\rangle$ has codimension 1 in D, it suffices to show that $v_k \notin A_{1,1} + \mathcal{A}_{k,k+1}$. Suppose, by contradiction, that $v_k \in A_{1,1} + \mathcal{A}_{k,k+1}$. Then there exist $\lambda_1, \lambda_2, \ldots \in \{0, 1\}$ with

$$\begin{aligned} v_k &= \lambda_1(v_1 + v_3 + v_5 + \cdots) + \lambda_2(v_2 + v_4 + v_6 + \cdots) \\ &\quad + \lambda_k(v_k + v_{k-1} + v_{k-3} + \cdots) + \lambda_{k+1}(v_{k+1} + v_k + v_{k-2} + \cdots) \\ &\quad + \sum_{j \in I \setminus \{k, k+1\}} \lambda_j v_j. \end{aligned}$$

This says that on the right-hand side of this equation the coefficient of v_k is equal to 1 and all other coefficients of v_j, $j \neq k$, are equal to 0. The set of respective coefficients of $\{v_{k+1}, v_1, v_2, v_{k_1}\}$ is

$$\big\{\lambda_2 + \lambda_{k+1} = 0, \lambda_1 + \lambda_{k+1} = 0, \lambda_2 + \lambda_k = 0, \lambda_1 = 0\big\}.$$

It follows that $\lambda_1 = \lambda_{k+1} = \lambda_2 = \lambda_k = 0$. So $\lambda_1 + \lambda_k + \lambda_{k+1} = 0$, but this is a contradiction because $\lambda_1 + \lambda_k + \lambda_{k+1}$ is the coefficient of v_k and should be equal to 1.

Hence, for all $k < k_1$ with k odd, we have

$$D \cap (A_{1,1} + \mathcal{A}_{k,k+1}) = \big\langle \{v_j \mid j \in I_o \setminus \{k\}\}\big\rangle.$$

Let $J := \{k \in I_o \mid k < k_1, k \text{ odd}\}$. We conclude

$$\begin{aligned} D' &:= D \cap \Big(\bigcap_{k \in J} (A_{1,1} + \mathcal{A}_{k,k+1})\Big) = \bigcap_{k \in J} (D \cap (A_{1,1} + \mathcal{A}_{k,k+1})) \\ &= \bigcap_{k \in J} \big(\big\langle \{v_j \mid j \in I_o \setminus \{k\}\}\big\rangle\big) = \big\langle \{v_j \mid j \in I_o \setminus J\}\big\rangle. \end{aligned}$$

Step 4. k odd and $k > k_1$.

By considering further intersections of D' with $A_{1,0} + \mathcal{A}_{k-1,k}$ for all odd $k > k_1$ we show in this step that equation (8.2) is satisfied.

First we prove that

$$D' \cap (A_{1,0} + \mathcal{A}_{k-1,k}) = \big\langle \{v_j \mid j \in I_o \setminus (J \cup \{k\})\}\big\rangle.$$

We have

$$\begin{aligned} A_{1,0} + \mathcal{A}_{k-1,k} &= A_{1,0} + \big\langle \{v_j \mid j \in I \setminus \{k-1,k\}\} \cup \{v_{k-1} + v_{k-2} + v_{k-4} + \cdots\}, \\ &\qquad \{v_k + v_{k-1} + v_{k-3} + \cdots\} \big\rangle \\ &= \big\langle \{v_j \mid j \in I \setminus \{k-1,k\}\} \cup \{v_1, v_2, v_{k-1} + v_{k-2} + v_{k-4} + \cdots, \\ &\qquad v_k + v_{k-1} + v_{k-3} + \cdots\} \big\rangle. \end{aligned}$$

Observe that

$$\big\langle \{v_j \mid j \in I_o \setminus (J \cup \{k\})\} \big\rangle \subseteq D' \cap (A_{1,0} + \mathcal{A}_{k-1,k}).$$

Moreover, since $\langle \{v_j \mid j \in I_o \setminus (J \cup \{k\})\} \rangle$ has codimension 1 in D', it suffices to show that $v_k \notin A_{1,0} + \mathcal{A}_{k-1,k}$. Suppose, by contradiction, that $v_k \in A_{1,0} + \mathcal{A}_{k-1,k}$. Then there exist $\lambda_1, \lambda_2, \ldots \in \{0, 1\}$ with

$$\begin{aligned} v_k = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_{k-1}(v_{k-1} + v_{k-2} + v_{k-4} + \cdots) \\ + \lambda_k (v_k + v_{k-1} + v_{k-3} + \cdots) + \sum_{j \in I \setminus \{k-1,k\}} \lambda_j v_j. \end{aligned}$$

On the right-hand side of this equation the coefficient of v_k is equal to 1 and all other coefficients of v_j, $j \neq k$, are equal to 0. Now the coefficient of v_{k-1} is $\lambda_{k-1} + \lambda_k = 0$. Note that v_{k_1} appears once in the summand $v_{k-1} + v_{k-2} + v_{k-4} + \cdots$. So the coefficient of v_{k_1} is $\lambda_{k-1} = 0$. This implies that $\lambda_k = 0$, a contradiction to the fact that $\lambda_k = 1$, because the coefficient of v_k is λ_k.

Hence for all $k > k_1$ with k odd, we have

$$D' \cap (A_{1,0} + \mathcal{A}_{k-1,k}) = \big\langle \{v_j \mid j \in I_o \setminus (J \cup \{k\})\} \big\rangle.$$

Let $J' := \{k \in I_o \mid k > k_1, k \text{ odd}\}$. We conclude

$$\begin{aligned} D'' := D' \cap \Big(\bigcap_{k \in J'} (A_{1,0} + \mathcal{A}_{k-1,k}) \Big) &= \bigcap_{k \in J'} (D' \cap (A_{1,0} + \mathcal{A}_{k-1,k})) \\ = \bigcap_{k \in J'} \big(\big\langle \{v_j \mid j \in I_o \setminus (J \cup \{k\})\} \big\rangle \big) &= \big\langle \{v_j \mid j \in I_o \setminus (J \cup J')\} \big\rangle = \{0\}. \end{aligned}$$

This completes the proof of Lemma 8.4. □

Lemma 8.5. *Suppose that* $k_1 \equiv k_2 \equiv 0 \bmod 2$. *Then equation* (8.2) *is satisfied.*

We omit the proof of Lemma 8.5 since it is similar to that of Lemma 8.4.
The next lemma deals with the last subcase.

Lemma 8.6. *Suppose that* $k_1 + k_2 \equiv 1 \bmod 2$. *Then equation* (8.2) *is satisfied.*

Proof. Without loss of generality, we assume $k_1 \equiv 1 \bmod 2$ and $k_2 \equiv 0 \bmod 2$.
We give a brief description of the steps that need to be carried out to prove (8.2) without showing the details.

Step 1. Prove that

$$C := \Big(A_{1,0} + \sum_{i\in I} A_{i,0}\Big) \cap \Big(A_{1,1} + \sum_{i\in I} A_{i,0}\Big) = \big\langle \{v_j \mid j \in I\}\big\rangle.$$

Step 2. k odd and $k < k_2$. Prove

$$C \cap (A_{1,1} + \mathcal{A}_k) = \big\langle \{v_j \mid j \in I \setminus \{k\}\}\big\rangle$$

by showing $v_k \notin (A_{1,1} + \mathcal{A}_k)$. Let $I' := \{k \in I \mid k < k_2, k \text{ odd}\}$. Then we have

$$\begin{aligned} C' := C \cap \Big(\bigcap_{k\in I'} (A_{1,0} + \mathcal{A}_k)\Big) &= \bigcap_{k\in I'} (C \cap (A_{1,0} + \mathcal{A}_k)) \\ &= \bigcap_{k\in I'} \big(\big\langle \{v_j \mid j \in I \setminus \{k\}\}\big\rangle\big) = \big\langle \{v_j \mid j \in I \setminus I'\}\big\rangle. \end{aligned}$$

Step 3. k odd and $k > k_2$. Prove

$$C \cap (A_{1,0} + \mathcal{A}_k) = \big\langle \{v_j \mid j \in I \setminus \{k\}\}\big\rangle$$

by showing $v_k \notin (A_{1,0} + \mathcal{A}_k)$. Let $I'' := \{k \in I \mid k > k_2, k \text{ odd}\}$. Then we have

$$\begin{aligned} C'' := C' \cap \Big(\bigcap_{k\in I''} (A_{1,0} + \mathcal{A}_k)\Big) &= \bigcap_{k\in I''} (C' \cap (A_{1,0} + \mathcal{A}_k)) \\ &= \bigcap_{k\in I''} \big(\big\langle \{v_j \mid j \in I \setminus \{I' \cup k\}\}\big\rangle\big) \\ &= \big\langle \{v_j \mid j \in I \setminus (I' \cup I'')\}\big\rangle = \big\langle \{v_j \mid j \in I_e\}\big\rangle, \end{aligned}$$

where I_e is the subset of all even numbers in I.

Step 4. k even and $k < k_1$. Prove

$$C'' \cap (A_{1,1} + \mathcal{A}_k) = \big\langle \{v_j \mid j \in I_e \setminus \{k\}\}\big\rangle$$

by showing $v_k \notin (A_{1,1} + \mathcal{A}_k)$. Let $J := \{k \in I_e \mid k < k_1, k \text{ even}\}$. Then we have

$$D := C'' \cap \Big(\bigcap_{k \in J} (A_{1,1} + \mathcal{A}_k) \Big) = \bigcap_{k \in J} (C'' \cap (A_{1,1} + \mathcal{A}_k))$$
$$= \bigcap_{k \in J} \big(\langle \{v_j \mid j \in I_e \setminus \{k\}\} \rangle \big) = \big\langle \{v_j \mid j \in I \setminus J\} \big\rangle.$$

Step 5. k even and $k > k_1$. Prove

$$D \cap (A_{1,0} + \mathcal{A}_k) = \big\langle \{v_j \mid j \in I_e \setminus \{J \cup k\}\} \big\rangle$$

by showing $v_k \notin (A_{1,0} + \mathcal{A}_k)$. Let $J' := \{k \in I_e \mid k > k_1, k \text{ even}\}$. Then we have

$$D' := D \cap \Big(\bigcap_{k \in J'} (A_{1,0} + \mathcal{A}_k) \Big) = \bigcap_{k \in J'} (D \cap (A_{1,0} + \mathcal{A}_k))$$
$$= \bigcap_{k \in J'} \big(\langle \{v_j \mid j \in I_e \setminus \{J \cup k\}\} \rangle \big) = \big\langle \{v_j \mid j \in I \setminus \{J \cup J'\}\} = \{0\} \big\rangle,$$

which proves (8.2). □

9 Some open questions

We have seen from Theorem 5.5 that the logarithmic signature β constructed from the Baumeister–de Wiljes method is tame provided the logarithmic signatures $[A_{1,j_1}, \ldots, A_{s,j_s}]$ and θ are known and tame. Obviously, if θ or/and $[A_{1,j_1}, \ldots, A_{s,j_s}]$ are not tame, even they are known, no efficient method is known regarding the factorization with respect to β. It is worth finding an answer to the following interesting problem.

Question 9.1. Suppose $[A_{1,j_1}, \ldots, A_{s,j_s}]$, $1 \le j_i \le r_i$, and θ are tame but they are not known. Suppose further that β is strongly aperiodic. Can elements of $\mathcal{G}$ be (efficiently) factorized with respect to β?

The result of the cryptanalysis of the enhanced version of MST_3 (see [11]) has shown that the scheme is secure when fused transversal logarithmic signatures are used. More precisely, fused transversal logarithmic signatures withstand the powerful matrix-permutation attack, a type of chosen plaintext attack, against the scheme and moreover one can determine a bound on the complexity of the attack for a given fused transversal logarithmic signature. It turns out that the

complexity is less than the input length of the scheme (see [11]). By virtue of the Baumeister–de Wiljes construction method we would conjecture that the complexity of the matrix-permutation attack against MST_3 is of size of the input length, when strongly aperiodic logarithmic signatures constructed in this paper are used. Hence we put the following challenging and important question.

Question 9.2. Determine the complexity of the matrix-permutation attack of the enhanced version of MST_3, when strongly aperiodic logarithmic signatures constructed in this paper are used.

Recall that fusing blocks of a strongly aperiodic logarithmic signature constructed in this paper remains a logarithmic signature of Baumeister–de Wiljes type. Furthermore, a logarithmic signature $\beta = [B_1, \ldots, B_s]$ used in MST_3 of Question 9.2 should have a reasonable block size, say, $|B_i| \geq 2^6$ for $1 \leq i \leq s$. So, β is obtained by fusing blocks of a logarithmic signature constructed in Sections 7 and 8.

10 Conclusion

We introduced the concept of strongly aperiodic logarithmic signatures, having properties suitable for use in cryptosystem MST_3. We developed an algebraic approach based on the Baumeister–de Wiljes method which enables the construction of such logarithmic signatures for elementary abelian p-groups. The existence of strongly aperiodic logarithmic signatures not only extends the private key space of MST_3 but would significantly contribute to its security. It is therefore worthwhile to investigate further methods for constructing strongly aperiodic logarithmic signatures for abelian groups.

Bibliography

[1] B. Baumeister and J.-H. de Wiljes, Aperiodic logarithmic signatures, *J. Math. Cryptol.* **6** (2012), 21–37.

[2] S. R. Blackburn, C. Cid and C. Mullan, Cryptanalysis of the MST_3 Public Key Cryptosystem, *J. Math. Cryptol.* **3** (2009), 321–338.

[3] B. Huppert and N. Blackburn, *Finite Groups II*, Springer, Berlin, 1982.

[4] D. Janiszczak, Konstruktion aperiodischer logarithmischer Signaturen elementarabelscher p-Gruppen und Untersuchung ihrer Faktorisierungseigenschaft, Diploma thesis, Fakultät für Mathematik der Universität Duisburg-Essen, 2012.

[5] W. Lempken, S. S. Magliveras, Tran van Trung and W. Wei, A public key cryptosystem based on non-abelian finite groups, *J. Cryptology* **22** (2009), 62–74.

[6] S. S. Magliveras and N. D. Memon, The algebraic properties of cryptosystem PGM, *J. Cryptology* **5** (1992), 167–183.

[7] S. S. Magliveras, B. A. Oberg and A. J. Surkan, A new random number generator from permutation groups, Rend. del Sem. Matemat. e Fis. di Milano **LIV** (1984), 203–223.

[8] S. S. Magliveras, D. R. Stinson and Tran van Trung, New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups, *J. Cryptology* **15** (2002), 285–297.

[9] S. S. Magliveras, P. Svaba, Tran van Trung and P. Zajac, On the security of a realization of cryptosystem MST_3, *Tatra Mt. Math. Publ.* **41** (2008), 1–13.

[10] P. Marquardt, P. Svaba and Tran van Trung, Pseudorandom number generators based on random covers for finite groups, *Des. Codes Cryptography* **64** (2012), 209–220.

[11] P. Svaba and Tran van Trung, Public key cryptosystem MST3: Cryptanalysis and realization, *J. Math. Cryptol.* **4** (2010), 271–315.

[12] S. Szabó, *Topics in Factorization of Abelian Groups*, Birkhäuser, Basel, 2004.

Received January 15, 2013; revised May 2, 2013; accepted May 5, 2013.

Author information

Reiner Staszewski, Institut für Experimentelle Mathematik,
Universität Duisburg-Essen, Ellernstr. 29, 45326 Essen, Germany.
E-mail: reiner@iem.uni-due.de

Tran van Trung, Institut für Experimentelle Mathematik,
Universität Duisburg-Essen, Ellernstr. 29, 45326 Essen, Germany.
E-mail: trung@iem.uni-due.de