Moments of Autocorrelation Demerit Factors of Binary Sequences

Daniel J. Katz* Miriam E. Ramirez*

Department of Mathematics
California State University, Northridge
Northridge, California, United States

daniel.katz@csun.edu

miriam.ramirez@csun.edu

20 May 2024

Abstract

Sequences with low aperiodic autocorrelation are used in communications and remote sensing for synchronization and ranging. The autocorrelation demerit factor of a sequence is the sum of the squared magnitudes of its autocorrelation values at every nonzero shift when we normalize the sequence to have unit Euclidean length. The merit factor, introduced by Golay, is the reciprocal of the demerit factor. We consider the uniform probability measure on the 2^ℓ binary sequences of length ℓ and investigate the distribution of the demerit factors of these sequences. Sarwate and Jedwab have respectively calculated the mean and variance of this distribution. We develop new combinatorial techniques to calculate the pth central moment of the demerit factor for binary sequences of length ℓ. These techniques prove that for $p \geq 2$ and $\ell \geq 4$, all the central moments are strictly positive. For any given p, one may use the technique to obtain an exact formula for the pth central moment of the demerit factor as a function of the length ℓ. Jedwab's formula for variance is confirmed by our technique with a short calculation, and we go beyond previous results by also deriving an exact formula for the skewness. A computer-assisted application of our method also obtains exact formulas for the kurtosis, which we report here, as well as the fifth central moment.

1 Introduction

A *sequence* is a doubly infinite list $f = (\ldots, f_{-1}, f_0, f_1, f_2, \ldots)$ of complex numbers in which only finitely many of the terms are nonzero. We adopt this definition because

*This paper is based upon work of both authors supported in part by the National Science Foundation under Grants 1500856 and 1815487, and by work of Daniel J. Katz supported in part by the National Science Foundation under Grant 2206454.

we are thinking of our sequences aperiodically. If ℓ is a nonnegative integer, then a *binary sequence of length* ℓ is an $f = (\ldots, f_{-1}, f_0, f_1, f_2, \ldots)$ in which $f_j \in \{-1, 1\}$ for $j \in \{0, 1, \ldots, \ell - 1\}$ and $f_j = 0$ otherwise. Binary sequences are used to modulate signals in telecommunications and remote sensing [7, 8, 13]. Some applications, such as ranging, require very accurate timing. For these applications, it is important that the sequence not resemble any time-delayed version of itself.

Our measure of resemblance is aperiodic autocorrelation. If f is a sequence and $s \in \mathbb{Z}$, then the *aperiodic autocorrelation of* f *at shift* s is

$$C_f(s) = \sum_{j \in \mathbb{Z}} f_{j+s} \overline{f_j}.$$

Since $f_k = 0$ for all but finitely many k, this sum is always defined and is nonzero for only finitely many s. Note that $C_f(0)$ is the squared Euclidean norm of f. For applications, we want $|C_f(s)|$ to be small compared to $C_f(0)$ for every nonzero $s \in \mathbb{Z}$; this distinction is what ensures proper timing.

There are two main measures for evaluating how low the autocorrelation of a sequence f is at nonzero shifts. One measure is the *peak sidelobe level*, which is the maximum of $|C_f(s)|$ over all nonzero $s \in \mathbb{Z}$; this can be regarded as an l^∞ measure. Another important measure is the *demerit factor*, which is an l^2 measure of smallness of autocorrelation. The *(autocorrelation) demerit factor* of a nonzero sequence f is

$$\mathrm{ADF}(f) = \frac{\sum_{\substack{s \in \mathbb{Z} \\ s \neq 0}} |C_f(s)|^2}{C_f(0)^2} = -1 + \frac{\sum_{s \in \mathbb{Z}} |C_f(s)|^2}{C_f(0)^2}, \tag{1}$$

which is the sum of the squared magnitudes of all autocorrelation values at nonzero shifts for the sequence that one obtains from f by normalizing it to have unit Euclidean norm. The *(autocorrelation) merit factor* is the reciprocal of the autocorrelation demerit factor; it was introduced by Golay in [5, p. 450] as the "factor" for a sequence and then as the "merit factor" in [6, p. 460], while "demerit factor" appears later in the work of Sarwate [12, p. 102].

Sequences with low demerit factor (equivalently, high merit factor) are highly desirable for communications and ranging applications. For each given length ℓ, we would like to understand the distribution of the demerit factors of binary sequences of length ℓ, which always have $C_f(0) = \ell$, so the denominator of the last fraction in (1) is always ℓ^2. Thus, it is often convenient to study the numerator of the last fraction in (1), which is the sum of the squares of all the autocorrelation values, so we define

$$\mathrm{SSAC}(f) = \sum_{s \in \mathbb{Z}} |C_f(s)|^2,$$

so that for a binary sequence of length ℓ we have

$$\mathrm{ADF}(f) = -1 + \frac{\mathrm{SSAC}(f)}{\ell^2}. \tag{2}$$

For this entire paper, $\mathrm{Seq}(\ell)$ denotes the set of 2^ℓ binary sequences of length ℓ with the uniform probability distribution, and the expected value of a random variable v with respect to this distribution is denoted by $\mathbb{E}_f^\ell v(f) = \mathbf{E}_{f\in\mathrm{Seq}(\ell)}(v(f))$. The pth central moment of the random variable $v(f)$ as f ranges over the binary sequences of length ℓ is denoted

$$\mu_{p,f}^\ell v(f) = \mathbb{E}_f^\ell \left(v(f) - \mathbb{E}_f^\ell v(f)\right)^p, \tag{3}$$

and the pth standardized moment is denoted by

$$\tilde{\mu}_{p,f}^\ell v(f) = \frac{\mu_{p,f}^\ell v(f)}{\left(\mu_{2,f}^\ell v(f)\right)^{p/2}}.$$

Sarwate [12, eq. (13)] found the mean of the demerit factor for binary sequences of a given length.

Theorem 1 (Sarwate, 1984)**.** *If ℓ is a positive integer, then $\mathbb{E}_f^\ell \mathrm{ADF}(f) = 1 - 1/\ell$.*

Borwein and Lockhart [3, pp. 1469–1470] showed that the variance of the demerit factor for binary sequences of length ℓ tends to 0 as ℓ tends to infinity. Jedwab [9, Theorem 1] gives an exact formula for the variance of the demerit factor for binary sequences of length ℓ. We present a formula involving a quasi-polynomial divided by the fourth power of the length that is equivalent to Jedwab's formula for the variance.

Theorem 2 (Jedwab, 2019)**.** *If ℓ is a positive integer, then*

$$\mu_{2,f}^\ell \mathrm{ADF}(f) = \begin{cases} \frac{16\ell^3-60\ell^2+56\ell}{3\ell^4} & \text{if } \ell \text{ is even,} \\ \frac{16\ell^3-60\ell^2+56\ell-12}{3\ell^4} & \text{if } \ell \text{ is odd.} \end{cases}$$

When one compares the calculation of the variance by Jedwab with that of the mean by Sarwate, one finds the first instance of a general principle: for each p, the determination of the $(p+1)$th moment is always considerably more difficult than that of the pth moment. Jedwab follows the method of Aupetit et al. [1], which involves many multiple summations and is therefore somewhat difficult to execute precisely: Jedwab had to correct the calculation of Aupetit et al. to get the right formula.

In this paper, we devise a new combinatorial method for calculating the moments of the distribution of the demerit factor of binary sequences of length ℓ. For any given p, one may use the technique to obtain an exact formula for the pth central moment of the demerit factor as a function of the length ℓ. For $p = 2$, this entails a short calculation that yields Jedwab's formula for variance. To demonstrate that one can go further, we also use our formula for $p = 3$ to derive an exact formula for the third central moment of $\mathrm{SSAC}(f)$ as a quasi-polynomial function of sequence length, from which we determine the third central moment and third standardized moment (skewness) of $\mathrm{ADF}(f)$.

Theorem 3. *If ℓ is a positive integer, then*

$$\mu_{3,f}^\ell \mathrm{ADF}(f) = \begin{cases} \frac{160\ell^4-1296\ell^3+3296\ell^2-2496\ell}{\ell^6} & \text{if } \ell \equiv 0 \bmod 4, \\ \frac{160\ell^4-1296\ell^3+3296\ell^2-2736\ell+576}{\ell^6} & \text{if } \ell \equiv \pm 1 \bmod 4, \\ \frac{160\ell^4-1296\ell^3+3296\ell^2-2496\ell-384}{\ell^6} & \text{if } \ell \equiv 2 \bmod 4, \end{cases}$$

and

$$\tilde{\mu}^{\ell}_{3,f}\,\mathrm{ADF}(f) = \begin{cases} \frac{6\sqrt{3}(10\ell^4-81\ell^3+206\ell^2-156\ell)}{(4\ell^3-15\ell^2+14\ell)^{3/2}} & \text{if } \ell \equiv 0 \bmod 4, \\ \frac{6\sqrt{3}(10\ell^4-81\ell^3+206\ell^2-171\ell+36)}{(4\ell^3-15\ell^2+14\ell-3)^{3/2}} & \text{if } \ell \equiv \pm 1 \bmod 4, \\ \frac{6\sqrt{3}(10\ell^4-81\ell^3+206\ell^2-156\ell-24)}{(4\ell^3-15\ell^2+14\ell)^{3/2}} & \text{if } \ell \equiv 2 \bmod 4. \end{cases}$$

We also report in Theorem 20 a computer-assisted determination of the fourth central moment of $\mathrm{SSAC}(f)$ as a quasi-polynomial function of sequence length, from which we obtain the fourth central moment and fourth standardized moment (kurtosis) of $\mathrm{ADF}(f)$ (see Corollaries 21 and 22).

Theorem 4. *If ℓ is a positive integer, then $\mu^{\ell}_{4,f}\,\mathrm{ADF}(f)$ is a quasi-polynomial function of ℓ of degree 6 and period 120 divided by the polynomial ℓ^8 (see Corollary 21 for the precise function), while $\tilde{\mu}^{\ell}_{4,f}\,\mathrm{ADF}(f)$ is a quasi-polynomial function of ℓ of degree 6 and period 120 divided by a quasi-polynomial function of ℓ of degree 6 and period 2 (see Corollary 22 for the precise function).*

Our computer program was also able to find the fifth central moment of ADF as a quasi-polynomial function of ℓ of degree 7 and period 55440 divided by the polynomial ℓ^{10}. Our methods also shed light on interesting aspects of the distribution of demerit factors. For instance, we show that our general theory implies that the odd central moments are always nonnegative, and we can also determine precisely when central moments are zero.

Theorem 5. *Let ℓ and p be positive integers. Then $\mu^{\ell}_{p,f}\,\mathrm{ADF}(f)$ is nonnegative. Moreover, if (i) $p = 1$, (ii) p is odd with $p > 1$ and $\ell \leq 3$, or (iii) p is even and $\ell \leq 2$, then $\mu^{\ell}_{p,f}\,\mathrm{ADF}(f)$ is zero; otherwise it is strictly positive.*

Our method can be developed further to prove that the pth central moment of SSAC for sequences of length ℓ is always a quasi-polynomial function of ℓ with rational coefficients. Further developments of our method also show that in the limit as $\ell \to \infty$, all the standardized moments of the autocorrelation demerit factor tend to those of the standard normal distribution. The additional theoretical tools used to obtain these results are introduced and explored in [10].

The rest of this paper is organized as follows. Section 2 has preliminary conventions and definitions. Section 3 exhibits an exact formula for the central moments of SSAC (cf. Proposition 11). Section 4 describes a group action that yields an easier formula (cf. Proposition 17), and Section 5 discusses an algorithm to assist in the use of this formula. Section 6 discusses the proof of Theorem 5. Section 7 is a brief exposition about how we apply our theory to compute the variance, thus confirming Jedwab's result in Theorem 2. Section 8 follows with a discussion of the exact calculation of skewness reported in Theorem 3. Section 9 then reports on our computer-assisted determination of the kurtosis in reported in Theorem 4.

2 Notation and definitions

In this section, we give the basic conventions, notations, and definitions, mostly concerning particular kinds of partitions and functions, which are used in Section 3 to obtain an exact formula for the central moments (cf. Proposition 11).

We use the convention that $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{Z}_+ = \{1, 2, 3, \ldots\}$. If $\ell \in \mathbb{N}$, we write $[\ell]$ to mean $\{0, 1, \ldots, \ell - 1\}$. If S and T are sets, then T^S denotes the set of all functions from S into T.

A partition of a set A is a collection of nonempty, disjoint subsets of A whose union is A. If $\mathcal{P}$ is a partition of A, then $\mathcal{P}$ induces an equivalence relation on A that is written $a_1 \equiv a_2 \pmod{\mathcal{P}}$, which means that there is some class $P \in \mathcal{P}$ such that $a_1, a_2 \in P$.

Our calculation of the pth central moment of the demerit factor of binary sequences of a given length depends on partitions of $[p] \times [2] \times [2]$.

Definition 6 (**Part(p)**)**.** If p is a nonnegative integer, $\mathrm{Part}(p)$ is the set of all partitions of $[p] \times [2] \times [2]$.

To influence the calculation, a partition must have certain properties. We define the first of these.

Definition 7 (Globally even, locally odd (GELO) partition)**.** Let $p \in \mathbb{N}$. Then $\mathcal{P} \in \mathrm{Part}(p)$ is said to be *globally even, locally odd* (abbreviated *GELO*) if $|P|$ is even for every $P \in \mathcal{P}$ and for every $e \in [p]$ there is some $Q \in \mathcal{P}$ such that $|(\{e\} \times [2] \times [2]) \cap Q|$ is odd.

A certain kind of function, which we shall call an *assignment*, plays a critical role in our probability calculations.

Definition 8 (Assignment)**.** Let $p \in \mathbb{N}$. An *assignment for* $[p]$ is a function from $[p] \times [2] \times [2]$ into $\mathbb{N}$, i.e., an element of $\mathbb{N}^{[p]\times[2]\times[2]}$. The following are notations for the set of all assignments for $[p]$ and some of its important subsets:

- $\mathrm{As}([p]) = \mathbb{N}^{[p]\times[2]\times[2]}$, the set of all assignments for $[p]$,
- $\mathrm{As}([p], \ell) = \{\tau \in \mathrm{As}([p]) : \tau([p] \times [2] \times [2]) \subseteq [\ell]\}$,
- $\mathrm{As}([p], =) = \{\tau \in \mathrm{As}([p]) : \tau(e, 0, 0) + \tau(e, 0, 1) = \tau(e, 1, 0) + \tau(e, 1, 1)$ for every $e \in [p]\}$, and
- $\mathrm{As}([p], =, \ell) = \mathrm{As}([p], =) \cap \mathrm{As}([p], \ell)$.

Furthermore, if $\mathcal{P} \in \mathrm{Part}(p)$, then

- $\mathrm{As}(\mathcal{P}) = \{\tau \in \mathrm{As}([p]) : \tau(\beta) = \tau(\gamma)$ iff $\beta \equiv \gamma \bmod \mathcal{P}\}$,
- $\mathrm{As}(\mathcal{P}, \ell) = \mathrm{As}(\mathcal{P}) \cap \mathrm{As}([p], \ell)$,
- $\mathrm{As}(\mathcal{P}, =) = \mathrm{As}(\mathcal{P}) \cap \mathrm{As}([p], =)$, and
- $\mathrm{As}(\mathcal{P}, =, \ell) = \mathrm{As}(\mathcal{P}) \cap \mathrm{As}([p], =) \cap \mathrm{As}([p], \ell)$.

We now define another kind of partition that is significant in our calculation of moments.

Definition 9 (Satisfiable partition)**.** Let $p \in \mathbb{N}$. A partition $\mathcal{P}$ of $[p] \times [2] \times [2]$ is said to be *satisfiable* if $\mathrm{As}(\mathcal{P}, =)$ is nonempty. (Equivalently, there is some $\ell \in \mathbb{N}$ such that $\mathrm{As}(\mathcal{P}, =, \ell)$ is nonempty.) We denote the set of satisfiable partitions of $[p] \times [2] \times [2]$ as $\mathrm{Sat}(p)$.

When we calculate the moments of the distribution of demerit factors, it turns out that every nonzero term in our calculation corresponds to some partition combining the attributes of both Definitions 7 and 9, so we name such partitions accordingly.

Definition 10 (Contributory partition)**.** Let $p \in \mathbb{N}$. Then a partition $\mathcal{P}$ of $[p] \times [2] \times [2]$ is said to be *contributory* if it is globally even, locally odd and satisfiable. We denote the set of contributory partitions of $[p] \times [2] \times [2]$ as $\mathrm{Con}(p)$. That is, $\mathrm{Con}(p) = \mathrm{GELO}(p) \cap \mathrm{Sat}(p)$.

3 Moments from partitions

In this section, we exhibit an exact formula for central moments of $\mathrm{SSAC}(f)$, the sum of the squares of the autocorrelation values for a sequence f, where the moments are computed with f ranging over the set $\mathrm{Seq}(\ell)$ of all binary sequences of a given length ℓ (equipped with uniform probability measure). Recall from the Introduction that we use $\mathbb{E}_f^\ell v(f) = \mathbf{E}_{f \in \mathrm{Seq}(\ell)}(v(f))$ to denote the expected value of a random variable v depending on f as f ranges over $\mathrm{Seq}(\ell)$. Also, recall from (3) that the pth central moment of the random variable $v(f)$ as f ranges over $\mathrm{Seq}(\ell)$ is denoted

$$\mu_{p,f}^\ell v(f) = \mathbb{E}_f^\ell \left(v(f) - \mathbb{E}_f^\ell v(f) \right)^p .$$

Since (2) shows that the demerit factor of a binary sequence f of length ℓ is $\mathrm{ADF}(f) = -1 + \mathrm{SSAC}(f)/\ell^2$, it is easy to determine the pth central moment of the demerit factor from that of SSAC. Proposition 11 provides a way of calculating central moments of the sum of squares of the autocorrelation in terms of contributory partitions and assignments.

Proposition 11. *For $p, \ell \in \mathbb{N}$, we have*

$$\mu_{p,f}^\ell \mathrm{SSAC}(f) = \sum_{\mathcal{P} \in \mathrm{Con}(p)} |\mathrm{As}(\mathcal{P}, =, \ell)|.$$

The proof of this proposition is too long to include here, but it is a combinatorial proof involving a binomial-type expansion of a product of multiple summations. See [11, Sec. 3] for details.

4 Moments from isomorphism classes of partitions

In this section, we exhibit a new formula (in Proposition 17 below) that makes the moment calculations much easier than those performed using Proposition 11. The exact formula

for central moments in Proposition 11 typically involves many similar partitions $\mathcal{P}$ that produce the same value for $|\operatorname{As}(\mathcal{P}, =, \ell)|$, so we devise an equivalence relation (via a group action) to organize these partitions into classes.

We first describe the group in our action. If $p \in \mathbb{N}$, then we use S_p to denote the group of all permutations of $[p]$. The group in our action is the following wreath product of wreath products: $\mathcal{W}^{(p)} = (S_2 \operatorname{Wr}_{[2]} S_2) \operatorname{Wr}_{[p]} S_p$. Each element $\pi \in \mathcal{W}^{(p)}$ permutes $[p] \times [2] \times [2]$ in a certain way; see [11, pp. 7–8] for details. If $\pi \in \mathcal{W}^{(p)}$ and $P \subseteq [p] \times [2] \times [2]$ and $\mathcal{Q}$ is a set of subsets of $[p] \times [2] \times [2]$, then we let π act on P by setting $\pi(P) = \{\pi(e, s, v) : (e, s, v) \in P\}$ and we let π act on $\mathcal{Q}$ by setting $\pi(\mathcal{Q}) = \{\pi(Q) : Q \in \mathcal{Q}\}$. This gives an action of π on $\operatorname{Part}(p)$. If τ is an assignment from $\operatorname{As}([p])$, we define $\pi^*(\tau) = \tau \circ \pi$, so that $\mathcal{W}^{(p)}$ acts on $\operatorname{As}([p])$ by $\tau \mapsto \pi^*(\tau)$. Then we have the following result concerning the assignment counts of interest in Proposition 11.

Lemma 12. *Let $p, \ell \in \mathbb{N}$ and suppose that $\pi \in \mathcal{W}^{(p)}$ and $\mathcal{P} \in \operatorname{Part}(p)$. Then we have $\pi^*(\operatorname{As}(\pi(\mathcal{P}), =, \ell)) = \operatorname{As}(\mathcal{P}, =, \ell)$.*

This shows that partitions within the same orbit of the action of our group $\mathcal{W}^{(p)}$ make the same contribution to the summation in Proposition 11.

Definition 13 (Isomorphic partitions, isomorphism class)**.** Let $p \in \mathbb{N}$ and $\mathcal{P}, \mathcal{Q} \in \operatorname{Part}(p)$. Then we say that $\mathcal{P}$ and $\mathcal{Q}$ are *isomorphic* and write $\mathcal{P} \cong \mathcal{Q}$ to mean that there exists $\pi \in \mathcal{W}^{(p)}$ such that $\mathcal{Q} = \pi(\mathcal{P})$. The *isomorphism class* of $\mathcal{P}$ is the set of all partitions that are isomorphic to $\mathcal{P}$.

Since $\mathcal{W}^{(p)}$ is a group, the isomorphism relation is clearly an equivalence relation. It turns out that all partitions isomorphic to a contributory partition are also contributory.

Lemma 14. *Let $p, \ell \in \mathbb{N}$. If $\mathcal{P}, \mathcal{Q} \in \operatorname{Part}(p)$ with $\mathcal{P} \cong \mathcal{Q}$, then $\mathcal{P} \in \operatorname{Con}(p)$ if and only if $\mathcal{Q} \in \operatorname{Con}(p)$, and furthermore $|\operatorname{As}(\mathcal{P}, =, \ell)| = |\operatorname{As}(\mathcal{Q}, =, \ell)|$.*

This last result shows that each orbit in $\operatorname{Part}(p)$ under the action of $\mathcal{W}^{(p)}$ either contains only contributory partitions or no contributory partitions at all. Since we are primarily interested in the contributory partitions and their equivalence classes, we make a name for the set of all such classes.

Definition 15 (**Isom(p)**)**.** Let $p \in \mathbb{N}$. We use $\operatorname{Isom}(p)$ to denote the set of isomorphism classes of partitions in $\operatorname{Con}(p)$.

In view of Lemma 14, it is helpful to have a notation for the common value of $|\operatorname{As}(\mathcal{P}, =, \ell)|$ for all partitions $\mathcal{P}$ in an isomorphism class of contributory partitions.

Definition 16 (**Sols($\mathfrak{P}, \ell$)**)**.** Let $p, \ell \in \mathbb{N}$. If $\mathfrak{P}$ is any subset of $\operatorname{Part}(p)$ such that all partitions in $\mathfrak{P}$ are isomorphic to each other, we let $\operatorname{Sols}(\mathfrak{P}, \ell)$ be the common value (by Lemma 14) of $|\operatorname{As}(\mathcal{P}, =, \ell)|$ for $\mathcal{P} \in \mathfrak{P}$.

We most commonly use this definition when $\mathfrak{P} \in \operatorname{Isom}(p)$. Now our formula in Proposition 11 for central moments of the sum of squares of autocorrelation can be made much less unwieldy by grouping terms according to isomorphisms classes.

Proposition 17. *If $p, \ell \in \mathbb{N}$, then*

$$\mu^{\ell}_{p,f}\,\mathrm{SSAC}(f) = \sum_{\mathfrak{P}\in\mathrm{Isom}(p)} |\mathfrak{P}|\,\mathrm{Sols}(\mathfrak{P},\ell).$$

5 Finding contributory partitions

In order to use Proposition 17 to compute the pth central moment of SSAC, we need to find all the isomorphism classes of contributory partitions of $[p] \times [2] \times [2]$. It turns out that a matrix algorithm can be devised to make this search straightforward. This is described in detail at the end of [11, Section 5].

6 Positivity of moments

Proposition 11 gives the pth central moment of SSAC as a sum of cardinalities, which means that all the central moments are nonnegative. In fact, the pth central moment for $p \geq 2$ is strictly positive for almost all lengths of binary sequences, with the exceptions noted in Theorem 5 of the Introduction. The proof of this amounts to showing that there does exist at least one partition $\mathcal{P} \in \mathrm{Con}(p)$ for all $p \geq 2$ and that the number $|\,\mathrm{As}(\mathcal{P}, =, \ell)|$ of associated assignments is strictly positive for ℓ sufficiently large. See [11, Section 6] for details.

7 Explicit calculation of variance

The calculation of the variance of SSAC (and then of ADF) is detailed in [11, Section 7]. Since we use Proposition 17, the first challenge is finding all the isomorphism classes contributory partitions. We present the results of the search here; see [11, Lemma 7.1] for details.

Lemma 18. *There are precisely two equivalence classes, $\mathfrak{C}_1$ and $\mathfrak{C}_2$, in* Isom(2)*, which are represented respectively by partitions*

$$\mathcal{P}_1 = \Big\{\{(0,0,0),(0,0,1),(1,0,0),(1,0,1)\},\{(0,1,0),(1,1,0)\},\{(0,1,1),(1,1,1)\}\Big\} \text{ and}$$
$$\mathcal{P}_2 = \Big\{\{(0,0,0),(1,0,0)\},\{(0,0,1),(1,0,1)\},\{(0,1,0),(1,1,0)\},\{(0,1,1),(1,1,1)\}\Big\}.$$

To apply Proposition 17, we now need to find $|\mathfrak{P}|$ and $\mathrm{Sols}(\mathfrak{P})$ for each isomorphism class $\mathfrak{P}$. We compute these in [11, Lemmas 7.2–7.3] to obtain the variance of SSAC, and then use (2) to obtain the variance of ADF, which is reported Theorem 2 of the Introduction.

8 Explicit calculation of skewness

The calculation of the skewness of SSAC (and then of ADF) is detailed in [11, Section 8]. Since we use Proposition 17, the first challenge is finding all the isomorphism classes contributory partitions. We present the results of the search here; see [11, Lemma 8.1] for details.

Lemma 19. *There are precisely eight equivalence classes,* $\mathfrak{C}_1, \ldots, \mathfrak{C}_8$*, in* Isom(3)*, which are represented respectively by partitions*

$$\mathcal{P}_1 = \Big\{\big\{(0,0,0),(0,0,1),(1,1,0),(2,0,0)\big\},\big\{(1,0,0),(1,0,1),(0,1,0),(2,0,1)\big\},\big\{(0,1,1),(2,1,0)\big\},\big\{(1,1,1),(2,1,1)\big\}\Big\};$$

$$\mathcal{P}_2 = \Big\{\big\{(0,0,0),(0,0,1),(1,0,0),(1,0,1)\big\},\big\{(0,1,0),(2,0,0)\big\},\big\{(0,1,1),(2,0,1)\big\},\big\{(1,1,0),(2,1,0)\big\},\big\{(1,1,1),(2,1,1)\big\}\Big\};$$

$$\mathcal{P}_3 = \Big\{\big\{(0,0,0),(0,0,1),(1,1,0),(2,1,0)\big\},\big\{(1,0,0),(1,0,1)\big\},\big\{(2,0,0),(2,0,1)\big\},\big\{(0,1,0),(1,1,1)\big\},\big\{(0,1,1),(2,1,1)\big\}\Big\};$$

$$\mathcal{P}_4 = \Big\{\big\{(0,0,0),(0,0,1),(1,0,0),(2,0,0)\big\},\big\{(0,1,0),(1,1,0)\big\},\big\{(0,1,1),(2,1,0)\big\},\big\{(1,0,1),(2,1,1)\big\},\big\{(1,1,1),(2,0,1)\big\}\Big\};$$

$$\mathcal{P}_5 = \Big\{\big\{(0,0,0),(0,0,1)\big\},\big\{(1,0,0),(1,0,1)\big\},\big\{(2,0,0),(2,0,1)\big\},\big\{(1,1,0),(2,1,1)\big\},\big\{(2,1,0),(0,1,1)\big\},\big\{(0,1,0),(1,1,1)\big\}\Big\};$$

$$\mathcal{P}_6 = \Big\{\big\{(0,0,0),(0,0,1)\big\},\big\{(1,0,0),(1,0,1)\big\},\big\{(0,1,0),(2,0,0)\big\},\big\{(0,1,1),(2,1,0)\big\},\big\{(1,1,0),(2,0,1)\big\},\big\{(1,1,1),(2,1,1)\big\}\Big\};$$

$$\mathcal{P}_7 = \Big\{\big\{(0,0,0),(1,1,0)\big\},\big\{(0,0,1),(1,1,1)\big\},\big\{(1,0,0),(2,1,0)\big\},\big\{(1,0,1),(2,1,1)\big\},\big\{(2,0,0),(0,1,0)\big\},\big\{(2,0,1),(0,1,1)\big\}\Big\};\ \textit{and}$$

$$\mathcal{P}_8 = \Big\{\big\{(0,0,0),(1,1,1)\big\},\big\{(0,1,0),(1,0,1)\big\},\big\{(1,0,0),(2,1,1)\big\},\big\{(1,1,0),(2,0,1)\big\},\big\{(2,0,0),(0,1,1)\big\},\big\{(2,1,0),(0,0,1)\big\}\Big\}.$$

To apply Proposition 17, we now need to find $|\mathfrak{P}|$ and $\mathrm{Sols}(\mathfrak{P})$ for each isomorphism class $\mathfrak{P}$. We compute these in [11, Lemmas 8.2–8.3] to obtain the third central moment of SSAC, and then use (2) to obtain the third central moment of ADF, which is reported Theorem 3 of the Introduction. Dividing the third central moment of ADF by the 3/2 power of the variance produces the skewness, which is also reported in Theorem 3 of the Introduction.

9 Computer-assisted calculation of kurtosis and fifth moment

A computer program was used to find the fourth central moment of SSAC. The program first finds representatives for each isomorphism class $\mathfrak{C}$ in Isom(4). This is done by the matrix algorithm alluded to in Section 5, and the program finds 97 isomorphism classes. For each class $\mathfrak{C}$ in Isom(4), the program determines $|\mathfrak{C}|$ using an orbit-stabilizer technique and determines $\mathrm{Sols}(\mathfrak{C}, \ell)$ using Ehrhart theory and inclusion-exclusion, since finding $\mathrm{Sols}(\mathfrak{C}, \ell)$ requires one to count the number of integer solutions of a homogeneous linear system that lie in a hypercube as a function of the size of the hypercube (see [2, Ch. 3]) and to then deduct the number of solutions whose coordinates do not have distinct values. The program uses these calculations to compute the sum in Proposition 17 with $p = 4$, and thereby determines the fourth central moment of SSAC. The result is given below as Theorem 20. The program was written in C++ and employing the GNU Multiple Precision Arithmetic Library (GMP) [4], and obtained the fourth central moment of SSAC in about 5 seconds on a personal computer. The same program also obtained the second a third moments of SSAC, and its results agree with our hand calculations in Sections 7 and 8. With a few hours of computation time, the program was also able to find that Isom(5) has 2581 isomorphism classes and then to compute an exact formula for the fifth central moment of SSAC as a quasi-polynomial of degree 7 and period 55440.

Theorem 20. *For $\ell \in \mathbb{N}$, the quantity $\mu^{\ell}_{4,f}\,\mathrm{SSAC}(f)$ is a quasi-polynomial function of ℓ of degree* 6 *and period* 120 *given by*

$$\mu^{\ell}_{4,f}\,\mathrm{SSAC}(f) = \frac{1}{45}\sum_{j=0}^{6} a_j(\ell)\ell^j,$$

where for every ℓ we have $a_6(\ell) = 3840$; $a_5(\ell) = 501120$; $a_4(\ell) = -6786480$;

$$a_3(\ell) = \begin{cases} \textit{27078080} & \textit{if } \ell \equiv 0 \pmod 2, \\ \textit{27072320} & \textit{if } \ell \equiv 1 \pmod 2; \end{cases}$$

$$a_2(\ell) = \begin{cases} \textit{-17638464} & \textit{if } \ell \equiv 0 \pmod 2, \\ \textit{-18213024} & \textit{if } \ell \equiv 1 \pmod 2; \end{cases}$$

$$a_1(\ell) = \begin{cases} \textit{-69561600} & \textit{if } \ell \equiv 0 \pmod{12}, \\ \textit{-71342400} & \textit{if } \ell \equiv \pm 1, \pm 5 \pmod{12}, \\ \textit{-75982080} & \textit{if } \ell \equiv \pm 2 \pmod{12}, \\ \textit{-68516160} & \textit{if } \ell \equiv \pm 3 \pmod{12}, \\ \textit{-72387840} & \textit{if } \ell \equiv \pm 4 \pmod{12}, \\ \textit{-73155840} & \textit{if } \ell \equiv 6 \pmod{12}; \end{cases}$$

and $a_0(\ell)$ is a function of period 120 *whose values are given on Table 1.*

Since $\mathrm{ADF}(f) = -1 + \mathrm{SSAC}(f)/\ell^2$, we can divide this result by ℓ^8 to obtain the fourth central moment of the demerit factor.

Table 1: Values of $a_0(\ell)$ as a function of $\ell \pmod{120}$

$\ell \pmod{120}$	$a_0(\ell)$	$\ell \pmod{120}$	$a_0(\ell)$	$\ell \pmod{120}$	$a_0(\ell)$
0	0	21, 69	53732304	51, 99	57464784
1, 49	68764624	22, 58, 82, 118	100980736	53, 77	76964816
2, 38, 62, 98	98195456	23, 47	79591376	55	60110800
3, 27	63657936	24, 96	12386304	56, 104	43065344
4, 76	48062464	25	56378320	60	2211840
5	58385360	28, 52	54255616	61, 109	69870544
6, 54, 66, 114	61323264	29, 101	70771664	63, 87	62552016
7, 103	78690256	30, 90	48936960	65	57279440
8, 32	49258496	31, 79	72497104	68, 92	51470336
9, 81	52626384	33, 57	58819536	71, 119	73398224
10, 70	82401280	34, 46, 94, 106	94787584	73, 97	74957776
11, 59	74504144	35	62117840	75	45078480
12, 108	20791296	36, 84	14598144	80	30679040
13, 37	76063696	39, 111	56358864	83, 107	80697296
14, 26, 74, 86	92002304	40	33464320	85	57484240
15	43972560	41, 89	69665744	88, 112	52043776
16, 64	45850624	43, 67	79796176	93, 117	59925456
17, 113	75858896	44, 116	45277184	95	61011920
18, 42, 78, 102	67516416	45	41346000	100	35676160
19, 91	73603024	48, 72	18579456	105	40240080
20	32890880	50, 110	79616000	115	61216720

Corollary 21. *If $\ell \in \mathbb{Z}_+$, then*

$$\mu_{4,f}^{\ell}\,\mathrm{ADF}(f) = \frac{\mu_{4,f}^{\ell}\,\mathrm{SSAC}(f)}{\ell^8},$$

where $\mu_{4,f}^{\ell}\,\mathrm{SSAC}(f)$ is the quasi-polynomial function of degree 6 and period 120 described in Theorem 20.

We can normalize the fourth central moment using the variance from Theorem 2 to obtain the kurtosis of $\mathrm{SSAC}(f)$, which is the same as the kurtosis of $\mathrm{ADF}(f) = -1 + \mathrm{SSAC}(f)/\ell^2$.

Corollary 22. *If $\ell \in \mathbb{Z}_+$, then*

$$\tilde{\mu}_{4,f}^{\ell}\,\mathrm{ADF}(f) = \tilde{\mu}_{4,f}^{\ell}\,\mathrm{SSAC}(f) = \frac{\mu_{4,f}^{\ell}\,\mathrm{SSAC}(f)}{\left(\mu_{2,f}^{\ell}\,\mathrm{SSAC}(f)\right)^2},$$

where $\mu_{4,f}^{\ell}\,\mathrm{SSAC}(f)$ is the quasi-polynomial function of degree 6 and period 120 described in Theorem 20 and $\mu_{2,f}^{\ell}\,\mathrm{SSAC}(f)$ is the quasi-polynomial function of degree 3 and period 2 described in Theorem 2.

Acknowledgements

The authors thank Bernardo Ábrego and Silvia Fernández-Merchant for helpful discussions and suggestions.

References

[1] S. Aupetit, P. Liardet, and M. Slimane. Evolutionary search for binary strings with low aperiodic auto-correlations. In P. Liardet, P. Collet, C. Fonlupt, E. Lutton, and M. Schoenauer, editors, *Artificial Evolution*, volume 2936 of *Lecture Notes in Computer Science*, pages 39–50, 2004.

[2] M. Beck and S. Robins. *Computing the continuous discretely*. Undergraduate Texts in Mathematics. Springer, New York, second edition, 2015.

[3] P. Borwein and R. Lockhart. The expected L_p norm of random polynomials. *Proc. Amer. Math. Soc.*, 129(5):1463–1472, 2001.

[4] Free Software Foundation, Inc. *GNU MP version* `6.2.1`, 2020. Available at `https://gmplib.org/`.

[5] M. J. E. Golay. A class of finite binary sequences with alternate autocorrelation values equal to zero. *IEEE Trans. Inform. Theory*, 18:449–450, 1972.

[6] M. J. E. Golay. Hybrid low autocorrelation sequences. *IEEE Trans. Inform. Theory*, 21:460–462, 1975.

[7] S. W. Golomb. *Shift register sequences*. With portions co-authored by Lloyd R. Welch, Richard M. Goldstein, and Alfred W. Hales. Holden-Day, Inc., San Francisco, Calif.-Cambridge-Amsterdam, 1967.

[8] S. W. Golomb and G. Gong. *Signal design for good correlation*. Cambridge University Press, Cambridge, 2005.

[9] J. Jedwab. The distribution of the L_4 norm of Littlewood polynomials. arXiv:1911.11246, 2019.

[10] D. J. Katz and M. E. Ramirez. Limiting moments of autocorrelation demerit factors of binary sequences. arXiv:2307.14566, 2023.

[11] D. J. Katz and M. E. Ramirez. Moments of autocorrelation demerit factors of binary sequences. arXiv:2307.14281, 2024.

[12] D. V. Sarwate. Mean-square correlation of shift-register sequences. *Communications, Radar and Signal Processing, IEE Proceedings F*, 131(2):101–106, 1984.

[13] M. R. Schroeder. *Number theory in science and communication*, volume 7 of *Springer Series in Information Sciences*. Springer-Verlag, Berlin, fourth edition, 2006.