

The mean and variance of the reciprocal merit factor of four classes of binary sequences

Jonathan Jedwab

16 March 2024

Abstract

The merit factor of a $\{-1, 1\}$ binary sequence measures the collective smallness of its non-trivial aperiodic autocorrelations. Binary sequences with large merit factor are important in digital communications because they allow the efficient separation of signals from noise. It is a longstanding open question whether the maximum merit factor is asymptotically unbounded and, if so, what is its limiting value. Attempts to answer this question over almost sixty years have identified certain classes of binary sequences as particularly important: skew-symmetric sequences, symmetric sequences, and anti-symmetric sequences. Using only elementary methods, we find an exact formula for the mean and variance of the reciprocal merit factor of sequences in each of these classes, and in the class of all binary sequences. This provides a much deeper understanding of the distribution of the merit factor in these four classes than was previously available. A consequence is that, for each of the four classes, the merit factor of a sequence drawn uniformly at random from the class converges in probability to a constant as the sequence length increases.

1 Introduction

We consider the class of *length n binary sequences* \mathcal{A}_n , namely n -tuples $(a_0, a_1, \dots, a_{n-1})$ (where $n > 1$) having all entries a_j in $\{-1, 1\}$. The *aperiodic autocorrelation* of the binary sequence A at shift u is given by

$$C_A(u) := \sum_{j=0}^{n-u-1} a_j a_{j+u} \quad \text{for } 0 \leq u < n,$$

which measures the extent to which the sequence A resembles itself when shifted by u positions. Binary sequences whose aperiodic autocorrelations for $u \neq 0$ are collectively small have played a prominent role in digital communications engineering since the 1950s, because such sequences allow the efficient separation of signals from noise; see [11] and [20] for surveys. One of the principal measures of this collective smallness is how small the *peak sidelobe level* $\max_{0 < u < n} |C_A(u)|$ can be

J. Jedwab is with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC V5A 1S6, Canada. He is supported by NSERC. Email: jed@sfu.ca

for $A \in \mathcal{A}_n$. Our interest in this paper is the other principal measure of collective smallness, namely how large the *merit factor*

$$F(A) := \frac{n^2}{2 \sum_{u=1}^{n-1} C_A(u)^2} \quad (1.1)$$

(defined by Golay [6] in 1972) can be for $A \in \mathcal{A}_n$. See [10] for a survey of the merit factor and its importance in practical digital communications, and for an equivalent formulation in terms of the L_4 norm of complex-valued polynomials with ± 1 coefficients on the unit circle.

Let $F_n = \max_{A \in \mathcal{A}_n} F(A)$ be the maximum value of the merit factor over all binary sequences of length n . The overall goal in the study of the merit factor is to understand the asymptotic optimal behaviour by determining the value of $\limsup_{n \rightarrow \infty} F_n$. In 1966, Littlewood [16, §6] conjectured (using the L_4 norm formulation) that $\limsup_{n \rightarrow \infty} F_n$ is infinite, whereas in 1982 Golay [7] (apparently without being aware of Littlewood's prior study) conjectured to the contrary that $\limsup_{n \rightarrow \infty} F_n$ is finite. This remains unresolved.

Several studies have identified an important subset of \mathcal{A}_n : the class of *skew-symmetric* length n binary sequences

$$\mathcal{SS}_n := \left\{ (a_0, a_1, \dots, a_{n-1}) \in \mathcal{A}_n : n \text{ is odd and } a_j = (-1)^{j+\frac{n-1}{2}} a_{n-1-j} \text{ for } 0 \leq j < n \right\}. \quad (1.2)$$

Indeed, Golay [7] conjectured that

$$\limsup_{n \rightarrow \infty} \max_{A \in \mathcal{SS}_n} F(A) = \limsup_{n \rightarrow \infty} \max_{A \in \mathcal{A}_n} F(A),$$

which would imply that to determine the asymptotic largest merit factor it is sufficient to restrict attention from \mathcal{A}_n to the class \mathcal{SS}_n . For twenty-five years from 1988, the best known asymptotic result was the construction of an infinite family of binary sequences having asymptotic merit factor 6; the same value of 6 is also attained asymptotically by certain families of skew-symmetric sequences of length $2p + 1$ or $4p + 1$, where p is a prime congruent to 1 modulo 4 [21, Corollaries 6 and 9]. Then, in 2013, the asymptotic value 6 was improved to the value $\frac{1}{c-1} > 6.34$, where c is the smallest root of $27x^3 - 498x^2 + 1164x - 722$ [14]. It was subsequently shown that this larger value can also be attained asymptotically by skew-symmetric sequences [13].

This provides clear motivation to understand the distribution of the merit factor as a function of length n , in both the classes \mathcal{A}_n and \mathcal{SS}_n . In this paper, we shall show how to determine the exact mean and variance of $\frac{1}{F(A)}$ for a sequence A drawn uniformly at random from \mathcal{A}_n and \mathcal{SS}_n , as set out in Theorems 1 and 2.

Theorem 1. *Let A be drawn uniformly at random from \mathcal{A}_n . Then*

$$\begin{aligned} n^2 \mathbb{E}\left(\frac{1}{F(A)}\right) &= n^2 - n, \\ n^4 \text{Var}\left(\frac{1}{F(A)}\right) &= \frac{16}{3}n^3 - 20n^2 + \frac{56}{3}n - 2 + 2(-1)^n. \end{aligned}$$

Theorem 2. *Let n be odd and let A be drawn uniformly at random from \mathcal{SS}_n . Then*

$$\begin{aligned} n^2 \mathbb{E}\left(\frac{1}{F(A)}\right) &= n^2 - 3n + 2, \\ n^4 \text{Var}\left(\frac{1}{F(A)}\right) &= \frac{32}{3}n^3 - 88n^2 + \frac{592}{3}n - 512 \left\lfloor \frac{n-1}{8} \right\rfloor - 512 \left\lfloor \frac{n-1}{12} \right\rfloor - 88 + 16(-1)^{\frac{n-1}{2}}(n-3). \end{aligned}$$

Two other subsets of \mathcal{A}_n arise naturally in the study of the merit factor: the class of *symmetric* length n binary sequences

$$\mathcal{S}_n := \{(a_0, a_1, \dots, a_{n-1}) \in \mathcal{A}_n : a_j = a_{n-1-j} \text{ for } 0 \leq j < n\}, \quad (1.3)$$

and the class of *anti-symmetric* length n binary sequences

$$\mathcal{AS}_n := \{(a_0, a_1, \dots, a_{n-1}) \in \mathcal{A}_n : n \text{ is even and } a_j = -a_{n-1-j} \text{ for } 0 \leq j < n\}. \quad (1.4)$$

For example, the asymptotic value 6 for $F(A)$ is attained not only by skew-symmetric sequences but also by binary sequences formed by prepending the element 1 to a sequence g of length $n-1$ and then cyclically rotating by $\lfloor n/4 \rfloor$ positions, for certain symmetric g when n is a prime congruent to 1 modulo 4 and for certain anti-symmetric g when n is a prime congruent to 3 modulo 4 [9]. Furthermore, every skew-symmetric binary sequence can be written as the interleaving of sequences f and g , where one of f, g is symmetric and the other is anti-symmetric. By choosing such sequences f and g each to have large merit factor, Golay and Harris [8] constructed examples of sequences in \mathcal{SS}_n with large merit factor for each odd n in the range $71 \leq n \leq 117$; these values of the merit factor were later shown to attain the actual maximum over \mathcal{SS}_n for all but two values of n in this range [18]. In contrast to the class \mathcal{A}_n , the merit factor of sequences in \mathcal{S}_n is known to be bounded above: Fredman, Saffari and Smith [5] proved that $F(A) \leq 0.1048^{-1} < 10$ for all $A \in \mathcal{S}_n$.

We shall provide a counterpart to Theorems 1 and 2 by determining the exact mean and variance of $\frac{1}{F(A)}$ for a sequence A drawn uniformly at random from either of the classes \mathcal{S}_n and \mathcal{AS}_n , as set out in Theorem 3 (in which $I[\cdot]$ denotes the indicator function of an event).

Theorem 3. *Let f be drawn uniformly at random from \mathcal{S}_n , or (for even n) from \mathcal{AS}_n . Then*

$$\begin{aligned} n^2 \mathbb{E}\left(\frac{1}{F(A)}\right) &= 2n^2 - 3n + \frac{1 - (-1)^n}{2}, \\ n^4 \text{Var}\left(\frac{1}{F(A)}\right) &= \begin{cases} 32n^3 - 216n^2 + 304n + 256 \left\lfloor \frac{n}{6} \right\rfloor + 256 \cdot I[n \bmod 6 = 4] & \text{for } n \text{ even,} \\ 32n^3 - 144n^2 + 160n - 576 \left\lfloor \frac{n-1}{4} \right\rfloor - 512 \left\lfloor \frac{n-1}{6} \right\rfloor - 48 & \text{for } n \text{ odd.} \end{cases} \end{aligned}$$

The expected value of $\frac{1}{F(A)}$, as given in Theorems 1, 2, and 3, was previously calculated for \mathcal{A}_n [19] (often attributed instead to [17]), for \mathcal{SS}_n [2], and for \mathcal{S}_n and \mathcal{AS}_n [3]. An expression for $\text{Var}(\frac{1}{F(A)})$ for the class \mathcal{A}_n was stated in [1], but was incorrectly calculated (see the discussion following the proof of Theorem 1). Katz and Ramirez [15], with reference to a preprint version [12] of the current paper, recently calculated $\mathbb{E}(\frac{1}{F(A)} - \mathbb{E}(\frac{1}{F(A)}))^p$ for $p = 2, 3, 4$, where A is drawn uniformly at random from \mathcal{A}_n , and in the case $p = 2$ obtained the same variance expression as in Theorem 1. None of the variance expressions for the classes \mathcal{SS}_n , \mathcal{S}_n , and \mathcal{AS}_n was previously known, and their derivation is considerably more difficult than that for \mathcal{A}_n . We find it surprising and remarkable that these exact closed form expressions exist, and that they can be determined precisely using only elementary methods. These expressions provide a much deeper understanding of the distribution of the merit factor in the four classes \mathcal{A}_n , \mathcal{SS}_n , \mathcal{S}_n , \mathcal{AS}_n than was previously available. The expressions in Theorem 1 have been verified numerically for $n \leq 40$, and those in Theorems 2 and 3 for $n \leq 75$.

Application of Chebyshev's inequality to Theorems 1, 2 and 3 gives the following corollary.

Corollary 4. *Let A be drawn uniformly at random from \mathcal{A}_n or (for odd n) from \mathcal{SS}_n , and let B be drawn uniformly at random from \mathcal{S}_n or (for even n) from \mathcal{AS}_n . Then, as $n \rightarrow \infty$,*

$$F(A) \rightarrow 1 \text{ in probability, and } F(B) \rightarrow \frac{1}{2} \text{ in probability.}$$

Of the asymptotic results given in Corollary 4, only that for \mathcal{A}_n was previously known [4]; our techniques are very different. Corollary 4 highlights the difficulty of trying to determine which sequences of length n attain the largest merit factor: they have zero density within their respective class as $n \rightarrow \infty$. Indeed, a value of $\limsup_{n \rightarrow \infty} F(A)$ larger than 6.34 can be attained for A in \mathcal{A}_n and \mathcal{SS}_n [14, 13] (as already noted), and a value of $\limsup_{n \rightarrow \infty} F(B)$ equal to 1.5 can be attained for B in \mathcal{S}_n and \mathcal{AS}_n (by taking the offset fraction in the main result of [9] to be 0).

In Section 2 we give some preliminary results for use in later calculations. In Sections 3, 4, and 5 we prove Theorems 1, 3, and 2, respectively.

2 Summation and calculation identities

Throughout the paper, we denote the indicator function of the event X by $I[X]$, and write $I_u := I[u \text{ odd}]$. We shall make use of the following summation identities, of which (2.1) to (2.5) can readily be verified by considering the cases n even and n odd separately; (2.6) follows from (2.4); (2.7) can be verified by substituting $u = 2U + 1$ and considering the cases $n \bmod 4 = 1$ and $n \bmod 4 = 3$ separately; (2.8) follows from (2.7) by substituting $v = 2V + 1$; (2.9) can be verified by considering the cases $n \bmod 8 = 1, 3, 5, 7$ separately; and (2.10) can be verified by considering each of the congruence classes of n modulo 6 separately:

$$\sum_{u=1}^{n-1} \left\lfloor \frac{u}{2} \right\rfloor = \left\lfloor \frac{n}{2} \right\rfloor \left\lfloor \frac{n-1}{2} \right\rfloor, \quad (2.1)$$

$$3 \sum_{u=1}^{n-1} \left\lfloor \frac{u}{2} \right\rfloor \left\lfloor \frac{u-2}{2} \right\rfloor = 2 \left\lfloor \frac{n}{2} \right\rfloor \binom{n-2}{2} \left\lfloor \frac{n-4}{2} \right\rfloor, \quad (2.2)$$

$$\sum_{u=1}^{n-1} I_u = \left\lfloor \frac{n}{2} \right\rfloor, \quad (2.3)$$

$$2 \sum_{u=1}^{n-1} I_u \binom{u-1}{2} = \left\lfloor \frac{n}{2} \right\rfloor \left\lfloor \frac{n-2}{2} \right\rfloor, \quad (2.4)$$

$$3 \sum_{u=1}^{n-1} I_u \binom{u-1}{2} \binom{u-3}{2} = \left\lfloor \frac{n}{2} \right\rfloor \left\lfloor \frac{n-2}{2} \right\rfloor \left\lfloor \frac{n-4}{2} \right\rfloor, \quad (2.5)$$

$$2 \sum_{u,v=1}^{n-1} I_u I[u+2v > 2n] = \left\lfloor \frac{n}{2} \right\rfloor \left\lfloor \frac{n-2}{2} \right\rfloor, \quad (2.6)$$

$$\sum_{u=\frac{n+1}{2}}^{n-1} I_u \binom{2u-n-1}{2} = \left\lfloor \frac{n-1}{4} \right\rfloor \left\lfloor \frac{n-3}{4} \right\rfloor \quad \text{for } n \text{ odd,} \quad (2.7)$$

$$\sum_{u,v=1}^{n-1} I_u I_v I[2u+v > 2n] = \left\lfloor \frac{n-1}{4} \right\rfloor \left\lfloor \frac{n-3}{4} \right\rfloor \quad \text{for } n \text{ odd,} \quad (2.8)$$

$$\sum_{u=\lceil \frac{3n+1}{4} \rceil}^{n-1} I_u = \left\lfloor \frac{n-1}{8} \right\rfloor \quad \text{for } n \text{ odd}, \quad (2.9)$$

$$\sum_{u=\lceil \frac{2n+1}{3} \rceil}^{n-1} I_u = \left\lfloor \frac{n}{6} \right\rfloor + I[n \bmod 6 = 4]. \quad (2.10)$$

We next obtain expressions for $n^2 \mathbb{E}(\frac{1}{F(A)})$ and $n^4 \text{Var}(\frac{1}{F(A)})$ for $A = (a_0, a_1, \dots, a_{n-1}) \in \mathcal{A}_n$. We write

$$C_u := \sum_{j=0}^{u-1} a_j a_{j+n-u} \quad \text{for } 0 < u < n, \quad (2.11)$$

regarding the sequence entries a_j as random variables each taking values in $\{1, -1\}$.

Proposition 5. *Let $A = (a_0, a_1, \dots, a_{n-1}) \in \mathcal{A}_n$ be drawn at random according to an arbitrary distribution on the sequence entries a_j . Then*

$$n^2 \mathbb{E}\left(\frac{1}{F(A)}\right) = 2E, \quad (2.12)$$

$$n^4 \text{Var}\left(\frac{1}{F(A)}\right) = 4(V - E^2), \quad (2.13)$$

where

$$E = \sum_{u=1}^{n-1} \mathbb{E} C_u^2, \quad (2.14)$$

$$V = \sum_{u,v=1}^{n-1} \mathbb{E}(C_u^2 C_v^2). \quad (2.15)$$

Proof. Since $C_u = C_A(n-u)$, by the definition (1.1) of $F(A)$ we have

$$\frac{n^2}{F(A)} = 2 \sum_{u=1}^{n-1} C_u^2. \quad (2.16)$$

Take the expectation to obtain (2.12). Take the variance and substitute from (2.14) to obtain (2.13). \square

3 The class \mathcal{A}_n

In this section, we use Proposition 5 to prove Theorem 1 for the class \mathcal{A}_n of binary sequences.

Proof of Theorem 1. Let $A = (a_0, a_1, \dots, a_{n-1}) \in \mathcal{A}_n$, and regard the sequence entries a_j as independent random variables that each take the values 1 and -1 with probability $\frac{1}{2}$. Substitute the definition (2.11) of C_u into expression (2.14) for E to give

$$E = \sum_{u=1}^{n-1} \sum_{j,k=0}^{u-1} \mathbb{E}(a_j a_{j+n-u} a_k a_{k+n-u}).$$

Since the a_i are independent, the expectation term in the triple sum is nonzero exactly when $\{j, j+n-u, k, k+n-u\} = \{i, i, i', i'\}$ for some indices i, i' , or equivalently when $j = k$. Therefore $E = \sum_{u=1}^{n-1} \sum_{j=0}^{u-1} \mathbb{E}(1) = n(n-1)/2$, and then (2.12) gives

$$n^2 \mathbb{E}\left(\frac{1}{F(A)}\right) = n^2 - n,$$

as required.

Substitute the definition (2.11) of C_u into expression (2.15) for V to give

$$V = \sum_{u,v=1}^{n-1} \sum_{j,k=0}^{u-1} \sum_{\ell,m=0}^{v-1} \mathbb{E}(a_j a_{j+n-u} a_k a_{k+n-u} a_\ell a_{\ell+n-v} a_m a_{m+n-v}).$$

There are four mutually disjoint cases for which the expectation term in the sum V is nonzero.

Case 1: $u = v$ and $j = k = \ell = m$. The contribution to V is $\sum_{u=1}^{n-1} \sum_{j=0}^{u-1} 1 = \sum_{u=1}^{n-1} u$.

Case 2: $u = v$ and $\{j, k, \ell, m\} = \{i, i, i', i'\}$ for some indices $i \neq i'$. The contribution to V (from 3 symmetrical cases) is

$$3 \sum_{u=1}^{n-1} \sum_{j=0}^{u-1} \sum_{\substack{k=0 \\ k \neq j}}^{u-1} 1 = 3 \sum_{u=1}^{n-1} u(u-1).$$

Case 3: $u \neq v$ and $j = k$ and $\ell = m$. The contribution to V is

$$\sum_{\substack{u=1 \\ v \neq u}}^{n-1} \sum_{v=1}^{n-1} \sum_{j=0}^{u-1} \sum_{\ell=0}^{v-1} 1 = \sum_{u=1}^{n-1} \sum_{\substack{v=1 \\ v \neq u}}^{n-1} uv = \left(\sum_{u=1}^{n-1} u\right)^2 - \sum_{u=1}^{n-1} u^2.$$

Case 4: $u \neq v$ and $\{j, k\} = \{i, i+n-v\}$ and $\{\ell, m\} = \{i, i+n-u\}$ for some index i satisfying $0 \leq i < u+v-n$. The contribution to V (from 4 symmetrical cases) is

$$4 \sum_{\substack{u=1 \\ v \neq u}}^{n-1} \sum_{v=1}^{n-1} \sum_{j=0}^{u+v-n-1} 1 = 4 \sum_{u=1}^{n-1} \sum_{\substack{v=n-u+1 \\ v \neq u}}^{n-1} (u+v-n) = 4 \sum_{u=1}^{n-1} \sum_{\substack{w=1 \\ w \neq 2u-n}}^{u-1} w,$$

putting $w = u+v-n$. The condition $w \neq 2u-n$ in the inner sum takes effect only when $2u-n \geq 1$, so the contribution for this case equals

$$4 \sum_{u=1}^{n-1} \sum_{w=1}^{u-1} w - 4 \sum_{u=\lceil \frac{n+1}{2} \rceil}^{n-1} (2u-n) = 2 \sum_{u=1}^{n-1} u(u-1) - (n^2 - 2n + I_n)$$

by evaluating the sum involving $2u-n$ separately according to whether n is even or odd.

Sum the contributions to V from the four cases and substitute into (2.13), together with the relation $E = n(n-1)/2$ already calculated, to give

$$\begin{aligned} n^4 \text{Var}\left(\frac{1}{F(A)}\right) &= 16 \sum_{u=1}^{n-1} u^2 - 16 \sum_{u=1}^{n-1} u + 4 \left(\sum_{u=1}^{n-1} u\right)^2 - 4(n^2 - 2n + I_n) - n^2(n-1)^2 \\ &= \frac{16}{3}n^3 - 20n^2 + \frac{56}{3}n - 2 + 2(-1)^n, \end{aligned}$$

as required. □

The calculations in the proof of Theorem 1 follow the general method of Aupetit, Liardet and Slimane [1, §2], but correct the mistaken conclusion of [1, p.44, l.6] that (in our notation) $n^4 \text{Var}(\frac{1}{F(A)}) = \frac{8}{3}n(n-1)(n+4)$. The mistake arises from failing to apply the condition $r+s < N$ in computing the summation of [1, p.44, l.2], which corresponds in our notation to neglecting the condition $u+v > n$ in the analysis of Case 4.

4 The classes \mathcal{S}_n and \mathcal{AS}_n

In this section, we use Proposition 5 to prove Theorem 3 for the class \mathcal{S}_n of symmetric binary sequences and for the class \mathcal{AS}_n of anti-symmetric binary sequences.

Proof of Theorem 3. By (1.3) and (1.4), the map sending the sequence $A = (a_j)$ to the sequence $B = ((-1)^j a_j)$ is an involution between \mathcal{S}_{2m} and \mathcal{AS}_{2m} satisfying $F(A) = F(B)$. It is therefore sufficient to consider the class \mathcal{S}_n .

Let $(a_0, a_1, \dots, a_{n-1}) \in \mathcal{S}_n$. By the definition (1.3) of \mathcal{S}_n , the a_j satisfy the symmetry condition

$$a_j = a_{n-1-j} \quad \text{for } 0 \leq j < n. \quad (4.1)$$

We regard the sequence entries $a_0, a_1, \dots, a_{\lfloor \frac{n-1}{2} \rfloor}$ as independent random variables that each take the values 1 and -1 with probability $\frac{1}{2}$, and the remaining sequence entries as being determined by (4.1).

Set

$$D_u := 2 \sum_{0 \leq j < \frac{u-1}{2}} a_j a_{j+n-u}, \quad (4.2)$$

and use condition (4.1) to rewrite (2.11) as

$$C_u = I_u + D_u,$$

where the term I_u arises from the product $a_{(u-1)/2}^2$ when u is odd. Substitute for C_u in (2.14) and expand to give

$$E = \left\lfloor \frac{n}{2} \right\rfloor + 2 \sum_{u=1}^{n-1} I_u \mathbb{E} D_u + \sum_{u=1}^{n-1} \mathbb{E} D_u^2, \quad (4.3)$$

using the summation identity (2.3). Similarly substitute for C_u and C_v in (2.15) and expand; using symmetry in u and v , and the summation identity (2.3), we obtain

$$\begin{aligned} V &= \left\lfloor \frac{n}{2} \right\rfloor^2 + 4 \left\lfloor \frac{n}{2} \right\rfloor \sum_{u=1}^{n-1} I_u \mathbb{E} D_u + 4 \sum_{u,v=1}^{n-1} I_u I_v \mathbb{E}(D_u D_v) + 2 \left\lfloor \frac{n}{2} \right\rfloor \sum_{u=1}^{n-1} \mathbb{E} D_u^2 \\ &\quad + 4 \sum_{u,v=1}^{n-1} I_u \mathbb{E}(D_u D_v^2) + \sum_{u,v=1}^{n-1} \mathbb{E}(D_u^2 D_v^2). \end{aligned} \quad (4.4)$$

We shall use (4.2) to express each of $\mathbb{E} D_u$, $\mathbb{E}(D_u D_v)$, $\mathbb{E} D_u^2$, $\mathbb{E}(D_u D_v^2)$, and $\mathbb{E}(D_u^2 D_v^2)$ as a sum of expectation terms of the form $\mathbb{E}(a_{j_1} a_{j_2} \dots a_{j_{2r}})$, where $1 \leq r \leq 4$. In view of the symmetry condition (4.1), such a term is nonzero exactly when the indices j_1, j_2, \dots, j_{2r} admit a *matching decomposition*, namely a partition into r pairs $\{j, k\}$ such that those pairs which are not *equal*

($j = k$) are *symmetric* ($j + k = n - 1$, written as $j \sim k$). We shall identify the index sets admitting a matching decomposition, multiply the resulting expressions by I_u or I_v and sum over u or v in the range $1 \leq u, v \leq n - 1$ as appropriate, and then substitute into the forms (4.3) and (4.4) for E and V to calculate $n^2 \mathbb{E}(\frac{1}{F(A)})$ and $n^4 \text{Var}(\frac{1}{F(A)})$ from Proposition 5.

We shall use the observations that, for $1 \leq u, v \leq n - 1$,

$$\text{a pair (equal or symmetric) cannot be formed from indices } j, j + n - u \text{ satisfying } 0 \leq j < \frac{u-1}{2}, \quad (4.5)$$

$$j \not\sim k \text{ for indices } j, k \text{ satisfying } 0 \leq j < \frac{u-1}{2} \text{ and } 0 \leq k < \frac{v-1}{2}, \quad (4.6)$$

and

$$\begin{aligned} &\text{the only pairs that can be formed from indices } j, j + n - u, k, k + n - u \text{ satisfying} \\ &0 \leq j < k < \frac{u-1}{2} \text{ are } k = j + n - u \text{ (equal) and } j + n - u \sim k + n - u \text{ (symmetric)}. \end{aligned} \quad (4.7)$$

The sum $\sum_{u=1}^{n-1} I_u \mathbb{E} D_u$. From (4.2) and (4.5), this sum is

$$\sum_{u=1}^{n-1} I_u \mathbb{E} D_u = 2 \sum_{u=1}^{n-1} I_u \sum_{0 \leq j < \frac{u-1}{2}} \mathbb{E}(a_j a_{j+n-u}) = 0. \quad (4.8)$$

The sum $\sum_{u,v=1}^{n-1} I_u I_v \mathbb{E}(D_u D_v)$. From (4.2), this sum equals

$$4 \sum_{u,v=1}^{n-1} I_u I_v \sum_{0 \leq j < \frac{u-1}{2}} \sum_{0 \leq k < \frac{v-1}{2}} \mathbb{E}(a_j a_{j+n-u} a_k a_{k+n-v}).$$

The indices $j, j + n - u, k, k + n - v$ admit a matching decomposition in two ways, represented in Cases 1 and 2 below. All other possible arrangements of these four indices into two pairs are inconsistent with the given ranges for u, v, j, k , either because of a single pairing excluded by (4.5) or (4.6), or else by combination of two pairings as summarized in Table 1.

Case 1: $j = k$ and $j + n - u = k + n - v$. This gives $j = k$ and $u = v$, and the contribution to the sum is

$$4 \sum_{u=1}^{n-1} I_u \sum_{0 \leq j < \frac{u-1}{2}} 1 = 4 \sum_{u=1}^{n-1} I_u \left(\frac{u-1}{2} \right) = 2 \left\lfloor \frac{n}{2} \right\rfloor \left\lfloor \frac{n-2}{2} \right\rfloor$$

using the summation identity (2.4).

Case 2: $j = k$ and $j + n - u \sim k + n - v$. This gives $j = k = \frac{u+v-n-1}{2}$. These values of j, k have already been counted as part of Case 1 when $u = v$, so we impose the constraint $u \neq v$ and calculate the additional contribution to the sum from Case 2 as

$$4 I_n \sum_{\substack{u,v=1 \\ u \neq v}}^{n-1} I_u I_v I[u + v > n].$$

Substitute $u = 2U + 1$ and $2V + 1$ to evaluate this additional contribution as

$$\begin{aligned} 4 I_n \sum_{\substack{U, V=0 \\ U \neq V}}^{\frac{n-3}{2}} I[U + V > \frac{n-2}{2}] &= 4 I_n \sum_{U, V=0}^{\frac{n-3}{2}} I[U + V > \frac{n-2}{2}] - 4 I_n \sum_{U=0}^{\frac{n-3}{2}} I[U > \frac{n-2}{4}] \\ &= 4 I_n \frac{(n-1)(n-3)}{8} - 4 I_n \left\lfloor \frac{n-1}{4} \right\rfloor. \end{aligned}$$

Table 1: Inconsistent index pairings for the sum $\sum_{u,v=1}^{n-1} I_u I_v \mathbb{E}(D_u D_v)$

Index pairings	Inconsistency from
$j = k + n - v, \quad k = j + n - u$	$u + v = 2n$
$j = k + n - v, \quad k \sim j + n - u$	$j = \frac{u-1}{2} + \frac{n-v}{2} > \frac{u-1}{2}$
$j \sim k + n - v, \quad k = j + n - u$	$k = \frac{v-1}{2} + \frac{n-u}{2} > \frac{v-1}{2}$
$j \sim k + n - v, \quad k \sim j + n - u$	$j + k = \frac{u-1}{2} + \frac{v-1}{2}$

Combine Cases 1 and 2 to give

$$\sum_{u,v=1}^{n-1} I_u I_v \mathbb{E}(D_u D_v) = 2 \left\lfloor \frac{n}{2} \right\rfloor \left\lfloor \frac{n-2}{2} \right\rfloor + 2 I_n \left(\frac{n-1}{2} \right) \left(\frac{n-3}{2} \right) - 4 I_n \left\lfloor \frac{n-1}{4} \right\rfloor. \quad (4.9)$$

The sum $\sum_{u=1}^{n-1} \mathbb{E} D_u^2$. This sum arises by restricting to $u = v$ in the analysis of the previous sum (with the $I_u I_v$ term absent), and so is

$$\sum_{u=1}^{n-1} \mathbb{E} D_u^2 = 4 \sum_{u=1}^{n-1} \sum_{0 \leq j < \frac{u-1}{2}} 1 = 4 \sum_{u=1}^{n-1} \left\lfloor \frac{u}{2} \right\rfloor = 4 \left\lfloor \frac{n}{2} \right\rfloor \left\lfloor \frac{n-1}{2} \right\rfloor \quad (4.10)$$

using the summation identity (2.1).

The sum $\sum_{u,v=1}^{n-1} I_u \mathbb{E}(D_u D_v^2)$. From (4.2), this sum equals

$$8 \sum_{u,v=1}^{n-1} I_u \sum_{0 \leq j < \frac{u-1}{2}} \sum_{0 \leq k, \ell < \frac{v-1}{2}} \mathbb{E}(a_j a_{j+n-u} a_k a_{k+n-v} a_\ell a_{\ell+n-v}).$$

The contributions from indices $k = \ell$ involve terms in $\mathbb{E}(a_j a_{j+n-u})$, which by (4.5) is zero. By symmetry in k and ℓ , it is therefore sufficient to take twice the contributions from indices $k < \ell$, namely

$$16 \sum_{u,v=1}^{n-1} I_u \sum_{0 \leq j < \frac{u-1}{2}} \sum_{0 \leq k < \ell < \frac{v-1}{2}} \mathbb{E}(a_j a_{j+n-u} a_k a_{k+n-v} a_\ell a_{\ell+n-v}).$$

In order for the indices $j, j + n - u, k, k + n - v, \ell, \ell + n - v$ to admit a matching decomposition, at least one equal pair or one symmetric pair must be formed from the four indices

$k, k + n - v, \ell, \ell + n - v$. In the given range $k < \ell < \frac{v-1}{2}$, from observation (4.7) either $\ell = k + n - v$ (represented in Cases 2 and 3 below) or $k + n - v \sim \ell + n - v$ (represented in Cases 1 and 4 below). We can now determine all matching decompositions by starting with each of these two pairs in turn, and identifying all possible arrangements of the four remaining unpaired indices into two further pairs consistent with the given ranges for u, v, j, k, ℓ . These arrangements are listed in Cases 1 to 4 below; all other arrangements are inconsistent, either because of a single pairing excluded by (4.5) or (4.6), or else by combination of two or more pairings as summarized in Table 2.

Case 1: $k + n - v \sim \ell + n - v$ and $j = k$ and $j + n - u \sim \ell$. This gives $2v - u = n$ and $j = k$ and $\ell = 2v - n - 1 - j$, and the contribution to the sum is

$$16 I_n \sum_{v=\frac{n+1}{2}}^{n-1} \sum_{\substack{0 \leq j < \frac{2v-n-1}{2} \\ j > \frac{3v-2n-1}{2}}} 1.$$

Case 2: $\ell = k + n - v$ and $j = k$ and $j + n - u = \ell + n - v$. This gives $2v - u = n$ and $j = k$ and $\ell = j + n - v$, and the contribution to the sum is

$$16 I_n \sum_{v=\frac{n+1}{2}}^{n-1} \sum_{0 \leq j < \frac{3v-2n-1}{2}} 1.$$

Case 3: $\ell = k + n - v$ and $j = k$ and $j + n - u \sim \ell + n - v$. This gives $j = k = \frac{u+2v-2n-1}{2}$ and $\ell = \frac{u-1}{2}$. These values of j, k, ℓ have already been counted as part of Case 2 when $2v - u = n$, so we impose the constraint $2v - u \neq n$ and evaluate the additional contribution to the sum from Case 3 as

$$16 \sum_{\substack{u, v=1 \\ 2v-u \neq n}}^{n-1} I_u I[u + 2v > 2n] I[u < v].$$

Case 4: $k + n - v \sim \ell + n - v$ and $j = k$ and $j + n - u = \ell$. This gives $j = k = \frac{u+2v-2n-1}{2}$ and $\ell = \frac{2v-u-1}{2}$, and the contribution to the sum is

$$16 \sum_{u, v=1}^{n-1} I_u I[u + 2v > 2n] I[u > v].$$

The combined contribution to the sum from Cases 1 and 2 is

$$16 I_n \sum_{v=\frac{n+1}{2}}^{n-1} \sum_{\substack{0 \leq j < \frac{2v-n-1}{2} \\ j \neq \frac{3v-2n-1}{2}}} 1,$$

in which the condition $j \neq \frac{3v-2n-1}{2}$ in the inner sum takes effect only when $\frac{3v-2n-1}{2}$ is a non-negative integer. The combined contribution from Cases 1 and 2 therefore equals

$$16 I_n \sum_{v=\frac{n+1}{2}}^{n-1} \frac{2v-n-1}{2} - 16 I_n \sum_{v=\lceil \frac{2n+1}{3} \rceil}^{n-1} I_v = 8 I_n \left(\frac{n-1}{2} \right) \left(\frac{n-3}{2} \right) - 16 I_n \left\lfloor \frac{n-1}{6} \right\rfloor$$

Table 2: Inconsistent index pairings for the sum $\sum_{u,v=1}^{n-1} I_u \mathbb{E}(D_u D_v^2)$

Index pairings	Inconsistency from
$\ell = k + n - v, \quad j = \ell + n - v, \quad k = j + n - u$	$u + 2v = 3n$
$\ell = k + n - v, \quad j = \ell + n - v, \quad k \sim j + n - u$	$j = \frac{u-1}{2} + n - v > \frac{u-1}{2}$
$\ell = k + n - v, \quad j \sim \ell + n - v, \quad k = j + n - u$	$\ell = \frac{v-1}{2} + \frac{2n-u-v}{2} > \frac{v-1}{2}$
$\ell = k + n - v, \quad j \sim \ell + n - v, \quad k \sim j + n - u$	$j + \ell = \frac{u+n-2}{2} > \frac{u-1}{2} + \frac{v-1}{2}$
$k + n - v \sim \ell + n - v, \quad j = \ell, \quad k = j + n - u$	$k = \ell + n - u > \ell$
$k + n - v \sim \ell + n - v, \quad j = \ell, \quad k \sim j + n - u$	$k + \ell = u - 1$

using the summation identity (2.10).

The combined additional contribution to the sum from Cases 3 and 4 is

$$\begin{aligned}
16 \sum_{\substack{u,v=1 \\ u \neq v \\ 2v-u \neq n}}^{n-1} I_u I[u+2v > 2n] &= 16 \sum_{u,v=1}^{n-1} I_u I[u+2v > 2n] - 16 \sum_{u=\lceil \frac{2n+1}{3} \rceil}^{n-1} I_u - 16 I_n \sum_{v=\lceil \frac{3n+1}{4} \rceil}^{n-1} 1 \\
&= 16 \cdot \frac{1}{2} \left\lfloor \frac{n}{2} \right\rfloor \left\lfloor \frac{n-2}{2} \right\rfloor - 16 \left(\left\lfloor \frac{n}{6} \right\rfloor + I[n \bmod 6 = 4] \right) - 16 I_n \left\lfloor \frac{n-1}{4} \right\rfloor,
\end{aligned}$$

where the first summation is evaluated using the identity (2.6), the second using the identity (2.10), and the third by considering the cases $n \bmod 4 = 1$ and $n \bmod 4 = 3$ separately.

Add the contribution from Cases 1 and 2 to the additional contribution from Cases 3 and 4 to obtain

$$\begin{aligned}
\sum_{u,v=1}^{n-1} I_u \mathbb{E}(D_u D_v^2) &= 8 I_n \binom{n-1}{2} \binom{n-3}{2} + 8 \left\lfloor \frac{n}{2} \right\rfloor \left\lfloor \frac{n-2}{2} \right\rfloor \\
&\quad - 16 \left\lfloor \frac{n}{6} \right\rfloor - 16 I_n \left\lfloor \frac{n-1}{6} \right\rfloor - 16 I_n \left\lfloor \frac{n-1}{4} \right\rfloor - 16 \cdot I[n \bmod 6 = 4]. \tag{4.11}
\end{aligned}$$

The sum $\sum_{u,v=1}^{n-1} \mathbb{E}(D_u^2 D_v^2)$. From (4.2), this sum equals

$$16 \sum_{u,v=1}^{n-1} \sum_{0 \leq j, k < \frac{u-1}{2}} \sum_{0 \leq \ell, m < \frac{v-1}{2}} \mathbb{E}(a_j a_{j+n-u} a_k a_{k+n-u} a_\ell a_{\ell+n-v} a_m a_{m+n-v}).$$

We distinguish five mutually disjoint cases.

Case 1: $j = k$ and $\ell = m$. The contribution to the sum is

$$16 \sum_{u,v=1}^{n-1} \sum_{0 \leq j < \frac{u-1}{2}} \sum_{0 \leq \ell < \frac{v-1}{2}} 1 = 16 \left(\sum_{u=1}^{n-1} \left\lfloor \frac{u}{2} \right\rfloor \right)^2 = 16 \left\lfloor \frac{n}{2} \right\rfloor^2 \left\lfloor \frac{n-1}{2} \right\rfloor^2$$

using the summation identity (2.1).

Case 2: $j = k$ and $\ell \neq m$. By symmetry in ℓ and m , the contribution to the sum is

$$2 \cdot 16 \sum_{u,v=1}^{n-1} \sum_{0 \leq j < \frac{u-1}{2}} \sum_{0 \leq \ell < m < \frac{v-1}{2}} \mathbb{E}(a_\ell a_{\ell+n-v} a_m a_{m+n-v}),$$

and the inner sum over $\ell < m$ is zero because by (4.7) the index ℓ cannot form an equal or symmetric pair with any of the other three indices $\ell + n - v$, m , $m + n - v$ in the given range $\ell < m < \frac{v-1}{2}$.

Case 3: $j \neq k$ and $\ell = m$. Similarly to Case 2, the contribution to the sum is zero.

Case 4: $j \neq k$ and $\ell \neq m$ and $u = v$. By symmetry in j, k and in ℓ, m , the contribution to the sum is

$$4 \cdot 16 \sum_{u=1}^{n-1} \sum_{0 \leq j < k < \frac{u-1}{2}} \sum_{0 \leq \ell < m < \frac{u-1}{2}} \mathbb{E}(a_j a_{j+n-u} a_k a_{k+n-u} a_\ell a_{\ell+n-u} a_m a_{m+n-u}).$$

If $j \neq \ell$, then by (4.7) the expectation term is zero because the smaller of j, ℓ cannot form a pair with any of the other seven indices. We may therefore take $j = \ell$, and then by similar reasoning take $k = m$, so that the contribution to the sum is

$$64 \sum_{u=1}^{n-1} \sum_{0 \leq j < k < \frac{u-1}{2}} 1 = 32 \sum_{u=1}^{n-1} \left\lfloor \frac{u}{2} \right\rfloor \left\lfloor \frac{u-2}{2} \right\rfloor = \frac{64}{3} \left\lfloor \frac{n}{2} \right\rfloor \binom{n-2}{2} \left\lfloor \frac{n-4}{2} \right\rfloor$$

using the summation identity (2.2).

Case 5: $j \neq k$ and $\ell \neq m$ and $u \neq v$. By symmetry in u, v and in j, k , the contribution to the sum is

$$4 \cdot 16 \sum_{\substack{u,v=1 \\ u < v}}^{n-1} \sum_{0 \leq j < k < \frac{u-1}{2}} \sum_{\substack{0 \leq \ell, m < \frac{v-1}{2} \\ \ell \neq m}} \mathbb{E}(a_j a_{j+n-u} a_k a_{k+n-u} a_\ell a_{\ell+n-v} a_m a_{m+n-v}).$$

By (4.7), the index j cannot form an equal or symmetric pair with any of the indices $j + n - u, k, k + n - u$ in the given range $j < k < \frac{u-1}{2}$. Furthermore, j cannot form a symmetric pair with any of the indices $\ell, \ell + n - v, m, m + n - v$ in the given ranges $\ell, m < \frac{v-1}{2}$ and $j < \frac{u-1}{2}$ and $u < v$. A matching decomposition for the eight indices of the expectation term therefore requires that j form an equal pair with one of the four indices $\ell, \ell + n - v, m, m + n - v$. By symmetry in ℓ, m , we may replace the resulting four contributions to the sum by twice the contribution from $j = \ell$ and twice the contribution from $j = \ell + n - v$.

We claim that the contribution from $j = \ell + n - v$ is zero. To prove the claim, set $j = \ell + n - v$, so that ℓ and k are now constrained via $\ell + n - v < k < \frac{u-1}{2}$ and the remaining six unpaired indices are $\ell + 2n - u - v, k, k + n - u, \ell, m, m + n - v$. It is straightforward to check that ℓ cannot form an equal or symmetric pair with any of the three indices $\ell + 2n - u - v, k, k + n - u$ subject to the given constraint $\ell + n - v < k < \frac{u-1}{2}$, and therefore by (4.7) the only possible pairing involving ℓ is $\ell = m + n - v$. We therefore

set $\ell = m + n - v$, so that m and k are now constrained via $m + 2n - 2v < k < \frac{u-1}{2}$ and the remaining four unpaired indices are $m + 3n - u - 2v, k, k + n - u, m$. By (4.5), the indices $k, k + n - u$ cannot form an equal or symmetric pair and so, for a matching decomposition, m must form an equal or symmetric pair with k or $k + n - u$. This is not possible subject to the given constraint $m + 2n - 2v < k < \frac{u-1}{2}$, proving the claim. The contribution to the sum from Case 5 is therefore twice the contribution from $j = \ell$, namely

$$128 \sum_{\substack{u,v=1 \\ u < v}}^{n-1} \sum_{0 \leq j < k < \frac{u-1}{2}} \sum_{\substack{0 \leq m < \frac{v-1}{2} \\ m \neq j}} \mathbb{E}(a_k a_{k+n-u} a_{j+n-u} a_{j+n-v} a_m a_{m+n-v}).$$

The index k cannot form a symmetric pair with any of the indices $k + n - u, j + n - u, j + n - v, m, m + n - v$ in the given ranges $j < k < \frac{u-1}{2}$ and $m < \frac{v-1}{2}$ and $u < v$. A matching decomposition for the six indices of the expectation term therefore requires that k form an equal pair with one of the four indices $j + n - u, j + n - v, m, m + n - v$. We now determine all matching decompositions by starting with each of these four equal pairs in turn, identifying all possible arrangements of the four remaining unpaired indices into two further pairs consistent with the given ranges for u, v, j, k, m . These arrangements are listed in Cases 5a to 5e below. Inconsistent arrangements of indices arising from combinations of two or more pairings are summarized in Table 3.

Case 5a: $k = j + n - u$ and $m = j + n - v$ and $k + n - u \sim m + n - v$. This gives $j = \frac{2u+2v-3n-1}{2}$ and $k = \frac{2v-n-1}{2}$ and $m = \frac{2u-n-1}{2}$, and the contribution to the sum is

$$128 I_n \sum_{\substack{u,v=1 \\ u < v}}^{n-1} I[2u + 2v > 3n] I[2v - u < n].$$

Case 5b: $k = m + n - v$ and $k + n - u \sim j + n - u$ and $j + n - v = m$. This gives $j = \frac{2u+2v-3n-1}{2}$ and $k = \frac{2u-2v+n-1}{2}$ and $m = \frac{2u-n-1}{2}$, and the contribution to the sum is

$$128 I_n \sum_{\substack{u,v=1 \\ u < v}}^{n-1} I[2u + 2v > 3n] I[2v - u > n].$$

Case 5c: $k = j + n - v$ and $m = j + n - u$ and $k + n - u, m + n - v$ form an equal or symmetric pair. This gives $k = j + n - v$ and $m = j + n - u$ when the third pair (formed by $k + n - u, m + n - v$) is equal; the special case $j = \frac{2u+2v-3n-1}{2}$, $k = \frac{2u-n-1}{2}$, $m = \frac{2v-n-1}{2}$ is obtained when this pair is symmetric, and so is not counted again. The contribution to the sum is

$$128 \sum_{\substack{u,v=1 \\ u < v}}^{n-1} \sum_{j \geq 0} I[j < \frac{2u+v-2n-1}{2}].$$

Case 5d: $k = j + n - v$ and $m \sim k + n - u$ and $j + n - u, m + n - v$ form an equal or symmetric pair. This gives $k = j + n - v$ and $m = u + v - n - 1 - j$ when the

third pair is symmetric; the special case $j = \frac{2u-n-1}{2}$, $k = \frac{2u-2v+n-1}{2}$, $m = \frac{2v-n-1}{2}$ is obtained when this pair is equal, and is not counted again. The contribution to the sum is

$$128 \sum_{\substack{u,v=1 \\ u < v}}^{n-1} \sum_{j \geq 0} I\left[\frac{2u+v-2n-1}{2} < j < \frac{u+2v-2n-1}{2}\right].$$

Case 5e: $k = m$ and $k + n - u \sim j + n - v$ and $j + n - u, m + n - v$ form an equal or symmetric pair. This gives $k = m = u + v - n - 1 - j$ when the third pair is symmetric; the special case $j = \frac{2u-n-1}{2}$, $k = m = \frac{2v-n-1}{2}$ is obtained when this pair is equal, and is not counted again. The contribution to the sum is

$$128 \sum_{\substack{u,v=1 \\ u < v}}^{n-1} \sum_{j \geq 0} I\left[\frac{u+2v-2n-1}{2} < j < \frac{u+v-n-1}{2}\right].$$

Table 3: Inconsistent index pairings for Case 5 of the sum $\sum_{u,v=1}^{n-1} \mathbb{E}(D_u^2 D_v^2)$

Index pairings	Inconsistency from
$k = j + n - u, \quad m = k + n - u, \quad j + n - v \sim m + n - v$	$m = \frac{v-1}{2} + \frac{v-u}{2} + \frac{n-u}{2} > \frac{v-1}{2}$
$k = j + n - u, \quad m \sim k + n - u, \quad j + n - v \sim m + n - v$	$u = v$
$k = j + n - u, \quad m = j + n - v, \quad k + n - u = m + n - v$	$u = v$
$k = j + n - u, \quad m \sim j + n - v, \quad k + n - u = m + n - v$	$k = \frac{n-1}{2}$
$k = j + n - u, \quad m \sim j + n - v, \quad k + n - u \sim m + n - v$	$u = n$
$k = m + n - v, \quad k + n - u \sim j + n - u, \quad j + n - v \sim m$	$u = n$
$k = m + n - v, \quad k + n - u \sim j + n - v, \quad j + n - u = m$	$k = \frac{n-1}{2}$
$k = m + n - v, \quad k + n - u \sim j + n - v, \quad j + n - u \sim m$	$v = n$
$k = m + n - v, \quad k + n - u = m$	$u + v = 2n$
$k = m + n - v, \quad k + n - u \sim m$	$k = \frac{u-1}{2} + \frac{n-v}{2} > \frac{u-1}{2}$
$k = j + n - v, \quad m \sim j + n - u, \quad k + n - u = m + n - v$	$m = \frac{n-1}{2}$
$k = j + n - v, \quad m \sim j + n - u, \quad k + n - u \sim m + n - v$	$v = n$
$k = j + n - v, \quad m = k + n - u, \quad j + n - u = m + n - v$	$v = n$
$k = j + n - v, \quad m = k + n - u, \quad j + n - u \sim m + n - v$	$m = \frac{n-1}{2}$
$k = m, \quad k + n - u \sim j + n - u, \quad j + n - v \sim m + n - v$	$u = v$
$k = m, \quad k + n - u = m + n - v$	$u = v$
$k = m, \quad k + n - u \sim m + n - v, \quad j + n - u \sim j + n - v$	$j = k$

We now calculate the total contribution to the sum from Cases 1 to 5. The combined contribution from Cases 5a and 5b is

$$128 I_n \sum_{\substack{u,v=1 \\ u < v}}^{n-1} I[2u + 2v > 3n] I[2v - u \neq n] = 128 I_n \sum_{\substack{u,v=1 \\ u < v}}^{n-1} I[2u + 2v > 3n] - 128 I_n \sum_{v=\lceil \frac{5n+1}{6} \rceil}^{n-1} 1.$$

Since each summand of the sum over u, v is symmetric in u and v , this combined contribution is

$$\begin{aligned} & 128 \cdot \frac{1}{2} I_n \sum_{u,v=1}^{n-1} I[2u + 2v > 3n] - 64 I_n \sum_{u=\lceil \frac{3n+1}{4} \rceil}^{n-1} 1 - 128 I_n \sum_{v=\lceil \frac{5n+1}{6} \rceil}^{n-1} 1 \\ & = 32 I_n \left(\frac{n-1}{2} \right) \left(\frac{n-3}{2} \right) - 64 I_n \left\lfloor \frac{n-1}{4} \right\rfloor - 128 I_n \left\lfloor \frac{n-1}{6} \right\rfloor. \end{aligned}$$

The combined contribution to the sum from Cases 5c, 5d, and 5e is

$$\begin{aligned} & 128 \sum_{\substack{u,v=1 \\ u < v}}^{n-1} \sum_{j \geq 0} I[j < \frac{u+v-n-1}{2}, j \neq \frac{2u+v-2n-1}{2}, j \neq \frac{u+2v-2n-1}{2}] \\ & = 128 \sum_{\substack{u,v=1 \\ u < v}}^{n-1} \left(\left\lfloor \frac{u+v-n}{2} \right\rfloor I[u+v > n] - I_v I[2u+v > 2n] - I_u I[u+2v > 2n] \right), \end{aligned}$$

which is of the form $128 \sum_{\substack{u,v=1 \\ u < v}}^{n-1} s_{u,v}$ where $s_{u,v}$ is symmetric in u and v . We calculate this

combined contribution as $64 \sum_{u,v=1}^{n-1} s_{u,v} - 64 \sum_{u=1}^{n-1} s_{u,u}$. We have

$$\begin{aligned} 64 \sum_{u,v=1}^{n-1} s_{u,v} &= 64 \sum_{u,v=1}^{n-1} \left\lfloor \frac{u+v-n}{2} \right\rfloor I[u+v > n] - 128 \sum_{u,v=1}^{n-1} I_u I[u+2v > 2n] \\ &= 64 \left(\frac{2}{3} \left\lfloor \frac{n}{2} \right\rfloor \left(\frac{n-2}{2} \right) \left\lfloor \frac{n-4}{2} \right\rfloor + \frac{1}{2} \left\lfloor \frac{n}{2} \right\rfloor \left\lfloor \frac{n-2}{2} \right\rfloor \right) - 128 \cdot \frac{1}{2} \left\lfloor \frac{n}{2} \right\rfloor \left\lfloor \frac{n-2}{2} \right\rfloor, \end{aligned}$$

where the second summation is evaluated using the identity (2.6), and the first by substituting $w = u + v - n$ to obtain $64 \sum_{u=1}^{n-1} \sum_{w=1}^{u-1} \left\lfloor \frac{w}{2} \right\rfloor = 64 \sum_{u=1}^{n-1} \left\lfloor \frac{u}{2} \right\rfloor \left\lfloor \frac{u-1}{2} \right\rfloor$ from the identity (2.1), then applying the identity

$$\left\lfloor \frac{u}{2} \right\rfloor \left\lfloor \frac{u-1}{2} \right\rfloor = \left\lfloor \frac{u}{2} \right\rfloor \left\lfloor \frac{u-2}{2} \right\rfloor + I_u \left(\frac{u-1}{2} \right),$$

and finally using the identities (2.2) and (2.4). We also have

$$\begin{aligned} 64 \sum_{u=1}^{n-1} s_{u,u} &= 64 \sum_{u=\lceil \frac{n+1}{2} \rceil}^{n-1} \left\lfloor \frac{2u-n}{2} \right\rfloor - 128 \sum_{u=\lceil \frac{2n+1}{3} \rceil}^{n-1} I_u \\ &= 32 \left\lfloor \frac{n}{2} \right\rfloor \left\lfloor \frac{n-2}{2} \right\rfloor - 128 \left(\left\lfloor \frac{n}{6} \right\rfloor + I[n \bmod 6 = 4] \right), \end{aligned}$$

where the first summation is evaluated by considering the cases n even and n odd separately, and the second using the identity (2.10).

The combined contribution to the sum from Cases 5c, 5d, and 5e is therefore

$$\begin{aligned} & 64 \sum_{u,v=1}^{n-1} s_{u,v} - 64 \sum_{u=1}^{n-1} s_{u,u} \\ &= \frac{128}{3} \left\lfloor \frac{n}{2} \right\rfloor \binom{n-2}{2} \left\lceil \frac{n-4}{2} \right\rceil - 64 \left\lfloor \frac{n}{2} \right\rfloor \left\lceil \frac{n-2}{2} \right\rceil + 128 \left\lfloor \frac{n}{6} \right\rfloor + 128 \cdot I[n \bmod 6 = 4]. \end{aligned}$$

Add the contributions from Case 1, Case 4, Cases 5a/5b, and Cases 5c/5d/5e to obtain

$$\begin{aligned} \sum_{u,v=1}^{n-1} \mathbb{E}(D_u^2 D_v^2) &= 16 \left\lfloor \frac{n}{2} \right\rfloor^2 \left\lceil \frac{n-1}{2} \right\rceil^2 + 64 \left\lfloor \frac{n}{2} \right\rfloor \binom{n-2}{2} \left\lceil \frac{n-4}{2} \right\rceil - 64 \left\lfloor \frac{n}{2} \right\rfloor \left\lceil \frac{n-2}{2} \right\rceil \\ &+ 32 I_n \left(\frac{n-1}{2} \right) \binom{n-3}{2} - 64 I_n \left\lfloor \frac{n-1}{4} \right\rfloor - 128 I_n \left\lfloor \frac{n-1}{6} \right\rfloor + 128 \left\lfloor \frac{n}{6} \right\rfloor + 128 \cdot I[n \bmod 6 = 4]. \end{aligned} \tag{4.12}$$

We are now ready to determine $n^2 \mathbb{E}\left(\frac{1}{F(A)}\right)$ and $n^4 \text{Var}\left(\frac{1}{F(A)}\right)$ using Proposition 5, separating the calculation according to whether n is even or odd. Substitution of (4.8) and (4.10) into (4.3) gives

$$E = \frac{1}{2}(2n^2 - 3n + I_n), \tag{4.13}$$

and then from (2.12) we obtain

$$n^2 \mathbb{E}\left(\frac{1}{F(A)}\right) = 2n^2 - 3n + \frac{1 - (-1)^n}{2},$$

as required. Substitution of (4.8), (4.9), (4.10), (4.11), and (4.12) into (4.4) gives, after simplification,

$$V = \begin{cases} n^4 + 5n^3 - \frac{207}{4}n^2 + 76n + 64 \left\lfloor \frac{n}{6} \right\rfloor + 64 \cdot I[n \bmod 6 = 4] & \text{for } n \text{ even,} \\ n^4 + 5n^3 - \frac{131}{4}n^2 + \frac{77}{2}n - 128 \left\lfloor \frac{n-1}{6} \right\rfloor - 144 \left\lfloor \frac{n-1}{4} \right\rfloor - \frac{47}{4} & \text{for } n \text{ odd,} \end{cases}$$

and then from (2.13) and (4.13) we find that

$$n^4 \text{Var}\left(\frac{1}{F(A)}\right) = \begin{cases} 32n^3 - 216n^2 + 304n + 256 \left\lfloor \frac{n}{6} \right\rfloor + 256 \cdot I[n \bmod 6 = 4] & \text{for } n \text{ even,} \\ 32n^3 - 144n^2 + 160n - 576 \left\lfloor \frac{n-1}{4} \right\rfloor - 512 \left\lfloor \frac{n-1}{6} \right\rfloor - 48 & \text{for } n \text{ odd,} \end{cases}$$

as required. \square

5 The class \mathcal{SS}_n

In this section, we use Proposition 5 to prove Theorem 2 for the class \mathcal{SS}_n of skew-symmetric binary sequences.

Proof of Theorem 2. We modify the proof of Theorem 3 to obtain the result. Let $(a_0, a_1, \dots, a_{n-1}) \in \mathcal{SS}_n$. By the definition (1.2) of \mathcal{SS}_n , the a_j satisfy the skew-symmetry condition

$$a_j = (-1)^{j+\frac{n-1}{2}} a_{n-1-j} \quad \text{for } 0 \leq j < n. \quad (5.1)$$

We regard the sequence entries $a_0, a_1, \dots, a_{\frac{n-1}{2}}$ as independent random variables that each take the values 1 and -1 with probability $\frac{1}{2}$, and the remaining sequence entries as being determined by (5.1). Use condition (5.1) to rewrite (2.11) as

$$C_u = I_u \left((-1)^{\frac{n-u}{2}} + D_u \right).$$

Substitute for C_u in (2.14), and for C_u and C_v in (2.15), to obtain the expressions

$$E = \frac{n-1}{2} + 2 \sum_{u=1}^{n-1} (-1)^{\frac{n-u}{2}} I_u \mathbb{E} D_u + \sum_{u=1}^{n-1} I_u \mathbb{E} D_u^2, \quad (5.2)$$

$$\begin{aligned} V &= \left(\frac{n-1}{2} \right)^2 + 4 \left(\frac{n-1}{2} \right) \sum_{u=1}^{n-1} (-1)^{\frac{n-u}{2}} I_u \mathbb{E} D_u + 4 \sum_{u,v=1}^{n-1} (-1)^{\frac{2n-u-v}{2}} I_u I_v \mathbb{E}(D_u D_v) \\ &\quad + 2 \left(\frac{n-1}{2} \right) \sum_{u=1}^{n-1} I_u \mathbb{E} D_u^2 + 4 \sum_{u,v=1}^{n-1} (-1)^{\frac{n-u}{2}} I_u I_v \mathbb{E}(D_u D_v^2) + \sum_{u,v=1}^{n-1} I_u I_v \mathbb{E}(D_u^2 D_v^2), \end{aligned} \quad (5.3)$$

noting that $(-1)^{n-u} I_u = I_u$ because n is odd here.

We express each of $\mathbb{E} D_u$, $\mathbb{E}(D_u D_v)$, $\mathbb{E} D_u^2$, $\mathbb{E}(D_u D_v^2)$, and $\mathbb{E}(D_u^2 D_v^2)$ as a sum of expectation terms of the form $\mathbb{E}(a_{j_1} a_{j_2} \dots a_{j_{2r}})$, where $1 \leq r \leq 4$, and then calculate $n^2 \mathbb{E}(\frac{1}{F(A)})$ and $n^4 \text{Var}(\frac{1}{F(A)})$ from Proposition 5 by substitution into the forms (5.2) and (5.3). In view of the skew-symmetry condition (5.1), the expectation term $\mathbb{E}(a_{j_1} a_{j_2} \dots a_{j_{2r}})$ is nonzero exactly when the indices j_1, j_2, \dots, j_{2r} admit a matching decomposition. The index sets admitting a matching decomposition are identical to those in the proof of Theorem 3; each symmetric index pair $\{j, k\}$ in the resulting expectation term introduces an additional multiplicative factor $(-1)^{j+\frac{n-1}{2}}$, by (5.1).

We use the same case analyses in the following calculations as in the proof of Theorem 3, inserting additional factors I_u , I_v , $(-1)^{\frac{n-u}{2}}$, and $(-1)^{\frac{2n-u-v}{2}}$ as appropriate.

The sum $\sum_{u=1}^{n-1} (-1)^{\frac{n-u}{2}} I_u \mathbb{E} D_u$. Similarly to (4.8), this sum is zero.

The sum $\sum_{u,v=1}^{n-1} (-1)^{\frac{2n-u-v}{2}} I_u I_v \mathbb{E}(D_u D_v)$. We modify the calculation of $\sum_{u,v=1}^{n-1} I_u I_v \mathbb{E}(D_u D_v)$ in the proof of Theorem 3. Cases 1 and 2 both receive a multiplicative factor $(-1)^{\frac{2n-u-v}{2}} I_u I_v$ in place of $I_u I_v$. Case 2 receives a further multiplicative factor $(-1)^{j+n-u+\frac{n-1}{2}} = (-1)^{\frac{v-u}{2}}$ because of the symmetric index pair $\{j+n-u, k+n-v\}$ with $j = \frac{u+v-n-1}{2}$. The resulting multiplicative factor in both cases is $I_u I_v$ (using the relation $u = v$ for Case 1), and the sum is therefore unchanged from (4.9). Since n is odd, expression (4.9) simplifies to give

$$\sum_{u,v=1}^{n-1} (-1)^{\frac{2n-u-v}{2}} I_u I_v \mathbb{E}(D_u D_v) = 4 \left(\frac{n-1}{2} \right) \left(\frac{n-3}{2} \right) - 4 \left\lfloor \frac{n-1}{4} \right\rfloor.$$

The sum $\sum_{u=1}^{n-1} I_u \mathbb{E} D_u^2$. We modify the calculation of $\sum_{u=1}^{n-1} \mathbb{E} D_u^2$ in the proof of Theorem 3 by introducing an additional factor I_u , giving

$$\sum_{u=1}^{n-1} I_u \mathbb{E} D_u^2 = 4 \sum_{u=1}^{n-1} I_u \left(\frac{u-1}{2} \right) = 2 \binom{n-1}{2} \binom{n-3}{2}$$

using the summation identity (2.4).

The sum $\sum_{u,v=1}^{n-1} (-1)^{\frac{n-u}{2}} I_u I_v \mathbb{E}(D_u D_v^2)$. We modify the calculation of $\sum_{u,v=1}^{n-1} I_u \mathbb{E}(D_u D_v^2)$ in the proof of Theorem 3. Cases 1 to 4 all receive a multiplicative factor $(-1)^{\frac{n-u}{2}} I_u I_v$ in place of I_u . The presence of symmetric index pairs introduces further multiplicative factors: in Case 1, a factor of $(-1)^{(k+n-v)+\frac{n-1}{2}} (-1)^{(j+n-u)+\frac{n-1}{2}} = (-1)^{\frac{n-u}{2}}$ because of index pairs $\{k+n-v, \ell+n-v\}$ and $\{j+n-u, \ell\}$ with $j=k$ and $2v-u=n$; in Case 3, a factor of $(-1)^{(j+n-u)+\frac{n-1}{2}} = (-1)^{\frac{2v-u+n-2}{2}}$ because of index pair $\{j+n-u, \ell+n-v\}$ with $j = \frac{u+2v-2n-1}{2}$; and in Case 4, a factor of $(-1)^{(k+n-v)+\frac{n-1}{2}} = (-1)^{\frac{u+n-2}{2}}$ because of index pair $\{k+n-v, \ell+n-v\}$ with $k = \frac{u+2v-2n-1}{2}$.

The resulting multiplicative factors are given in Table 4 (using the relation $2v-u=n$ to evaluate Case 2). We see that the calculation differs from that of $\sum_{u,v=1}^{n-1} I_u \mathbb{E}(D_u D_v^2)$ in the proof of Theorem 3 only via the introduction of a factor I_v in all four cases.

Table 4: Multiplicative factors in calculation of $\sum_{u,v=1}^{n-1} (-1)^{\frac{n-u}{2}} I_u I_v \mathbb{E}(D_u D_v^2)$

Case	Multiplicative factor	Evaluates to
1	$(-1)^{\frac{n-u}{2}} I_u I_v \cdot (-1)^{\frac{n-u}{2}}$	$I_u I_v$
2	$(-1)^{\frac{n-u}{2}} I_u I_v$	$I_u I_v$
3	$(-1)^{\frac{n-u}{2}} I_u I_v \cdot (-1)^{\frac{2v-u+n-2}{2}}$	$I_u I_v$
4	$(-1)^{\frac{n-u}{2}} I_u I_v \cdot (-1)^{\frac{u+n-2}{2}}$	$I_u I_v$

The combined contribution from Cases 1 and 2 is therefore

$$16 \sum_{v=\frac{n+1}{2}}^{n-1} I_v \binom{2v-n-1}{2} - 16 \sum_{v=\lceil \frac{2n+1}{3} \rceil}^{n-1} I_v = 16 \left\lfloor \frac{n-1}{4} \right\rfloor \left\lfloor \frac{n-3}{4} \right\rfloor - 16 \left\lfloor \frac{n-1}{6} \right\rfloor$$

using the summation identities (2.7) and (2.10). The combined additional contribution from Cases 3 and 4 is

$$\begin{aligned} 16 \sum_{\substack{u,v=1 \\ u \neq v \\ 2v-u \neq n}}^{n-1} I_u I_v I[u+2v > 2n] &= 16 \sum_{u,v=1}^{n-1} I_u I_v I[u+2v > 2n] - 16 \sum_{u=\lceil \frac{2n+1}{3} \rceil}^{n-1} I_u - 16 \sum_{v=\lceil \frac{3n+1}{4} \rceil}^{n-1} I_v \\ &= 16 \left\lfloor \frac{n-1}{4} \right\rfloor \left\lfloor \frac{n-3}{4} \right\rfloor - 16 \left\lfloor \frac{n-1}{6} \right\rfloor - 16 \left\lfloor \frac{n-1}{8} \right\rfloor \end{aligned}$$

using the summation identities (2.8), (2.10), and (2.9).

Add the contributions from Cases 1 and 2 to the additional contribution from Cases 3 and 4 to obtain

$$\sum_{u,v=1}^{n-1} (-1)^{\frac{n-u}{2}} I_u I_v \mathbb{E}(D_u D_v^2) = 32 \left\lfloor \frac{n-1}{4} \right\rfloor \left\lfloor \frac{n-3}{4} \right\rfloor - 32 \left\lfloor \frac{n-1}{6} \right\rfloor - 16 \left\lfloor \frac{n-1}{8} \right\rfloor.$$

The sum $\sum_{u,v=1}^{n-1} I_u I_v \mathbb{E}(D_u^2 D_v^2)$. We modify the calculation of $\sum_{u,v=1}^{n-1} \mathbb{E}(D_u^2 D_v^2)$ in the proof of Theorem 3. All cases receive a multiplicative factor $I_u I_v$ in place of 1. The presence of symmetric index pairs introduces further multiplicative factors: in Case 5a, a factor of $(-1)^{(k+n-u)+\frac{n-1}{2}} = 1$ because of index pair $\{k+n-u, m+n-v\}$ with $k = \frac{2v-n-1}{2}$; in Case 5b, a factor of $(-1)^{(k+n-u)+\frac{n-1}{2}} = 1$ because of index pair $\{k+n-u, j+n-u\}$ with $k = \frac{2u-2v+n-1}{2}$; in Case 5d, a factor of $(-1)^m (-1)^{j+n-u} = 1$ because of index pairs $\{m, k+n-u\}$ and $\{j+n-u, m+n-v\}$ with $m = u+v-n-1-j$; and in Case 5e, a factor of $(-1)^{k+n-u} (-1)^{j+n-u} = 1$ because of index pairs $\{k+n-u, j+n-v\}$ and $\{j+n-u, m+n-v\}$ with $k = u+v-n-1-j$. Since these further factors all equal 1, we see that the calculation differs from that of $\sum_{u,v=1}^{n-1} \mathbb{E}(D_u D_v^2)$ in the proof of Theorem 3 only via the introduction of a factor $I_u I_v$ in all cases.

The contribution from Case 1 is therefore

$$16 \left(\sum_{u=1}^{n-1} I_u \left(\frac{u-1}{2} \right) \right)^2 = 4 \left(\frac{n-1}{2} \right)^2 \left(\frac{n-3}{2} \right)^2$$

using the summation identity (2.4). The contribution from Cases 2 and 3 is zero. The contribution from Case 4 is

$$32 \sum_{u=1}^{n-1} I_u \left(\frac{u-1}{2} \right) \left(\frac{u-3}{2} \right) = \frac{32}{3} \left(\frac{n-1}{2} \right) \left(\frac{n-3}{2} \right) \left(\frac{n-5}{2} \right)$$

using the summation identity (2.5). The contribution from Cases 5a and 5b is

$$\begin{aligned} & 128 \sum_{\substack{u,v=1 \\ u < v}}^{n-1} I_u I_v I[2u+2v > 3n] I[2v-u \neq n] \\ &= 128 \cdot \frac{1}{2} \sum_{u,v=1}^{n-1} I_u I_v I[2u+2v > 3n] - 64 \sum_{u=\lceil \frac{3n+1}{4} \rceil}^{n-1} I_u - 128 \sum_{v=\lceil \frac{5n+1}{6} \rceil}^{n-1} I_v \\ &= 32 \left\lfloor \frac{n-1}{4} \right\rfloor \left\lfloor \frac{n-5}{4} \right\rfloor - 64 \left\lfloor \frac{n-1}{8} \right\rfloor - 128 \left\lfloor \frac{n-1}{12} \right\rfloor, \end{aligned}$$

where the first summation is evaluated by substituting $u = 2U + 1$ and $v = 2V + 1$ and considering the cases $n \bmod 4 = 1$ and $n \bmod 4 = 3$ separately, the second using identity (2.9), and the third using an identity analogous to (2.9). The combined contribution to the sum from Cases 5c, 5d, and 5e is

$$128 \sum_{\substack{u,v=1 \\ u < v}}^{n-1} \left(I_u I_v \left(\frac{u+v-n-1}{2} \right) I[u+v > n] - I_u I_v I[2u+v > 2n] - I_u I_v I[u+2v > 2n] \right),$$

which is of the form $128 \sum_{\substack{u,v=1 \\ u < v}}^{n-1} s'_{u,v}$ where $s'_{u,v}$ is symmetric in u and v . We calculate

$$\begin{aligned} 64 \sum_{u,v=1}^{n-1} s'_{u,v} &= 64 \sum_{u,v=1}^{n-1} I_u I_v \left(\frac{u+v-n-1}{2} \right) I[u+v > n] - 128 \sum_{u,v=1}^{n-1} I_u I_v I[u+2v > 2n] \\ &= 64 \cdot \frac{1}{6} \binom{n-1}{2} \binom{n-3}{2} \binom{n-5}{2} - 128 \left\lfloor \frac{n-1}{4} \right\rfloor \left\lfloor \frac{n-3}{4} \right\rfloor, \end{aligned}$$

where the first summation is evaluated by substituting $w = u + v - n$ to obtain the expression $64 \sum_{u=1}^{n-1} I_u \sum_{w=1}^{u-1} I_w \binom{w-1}{2}$ and then using the identities (2.4) and (2.5), and the second using the identity (2.8); and

$$\begin{aligned} 64 \sum_{u=1}^{n-1} s'_{u,u} &= 64 \sum_{u=\frac{n+1}{2}}^{n-1} I_u \binom{2u-n-1}{2} - 128 \sum_{u=\lceil \frac{2n+1}{3} \rceil}^{n-1} I_u \\ &= 64 \left\lfloor \frac{n-1}{4} \right\rfloor \left\lfloor \frac{n-3}{4} \right\rfloor - 128 \left\lfloor \frac{n-1}{6} \right\rfloor, \end{aligned}$$

using the summation identities (2.7) and (2.10). The combined contribution to the sum from Cases 5c, 5d, and 5e is

$$\begin{aligned} 64 \sum_{u,v=1}^{n-1} s'_{u,v} - 64 \sum_{u=1}^{n-1} s'_{u,u} \\ = \frac{32}{3} \binom{n-1}{2} \binom{n-3}{2} \binom{n-5}{2} - 192 \left\lfloor \frac{n-1}{4} \right\rfloor \left\lfloor \frac{n-3}{4} \right\rfloor + 128 \left\lfloor \frac{n-1}{6} \right\rfloor. \end{aligned}$$

Add the contributions from Case 1, Case 4, Cases 5a/5b, and Cases 5c/5d/5e to obtain

$$\begin{aligned} \sum_{u,v=1}^{n-1} I_u I_v \mathbb{E}(D_u^2 D_v^2) \\ = 4 \binom{n-1}{2}^2 \binom{n-3}{2}^2 + \frac{64}{3} \binom{n-1}{2} \binom{n-3}{2} \binom{n-5}{2} - 192 \left\lfloor \frac{n-1}{4} \right\rfloor \left\lfloor \frac{n-3}{4} \right\rfloor \\ + 32 \left\lfloor \frac{n-1}{4} \right\rfloor \left\lfloor \frac{n-5}{4} \right\rfloor + 128 \left\lfloor \frac{n-1}{6} \right\rfloor - 64 \left\lfloor \frac{n-1}{8} \right\rfloor - 128 \left\lfloor \frac{n-1}{12} \right\rfloor. \end{aligned}$$

We now use the calculated expectation expressions to determine $n^2 \mathbb{E}(\frac{1}{F(A)})$ and $n^4 \text{Var}(\frac{1}{F(A)})$ using Proposition 5. Substitution into (5.2) gives

$$E = \frac{1}{2}(n^2 - 3n + 2), \quad (5.4)$$

and then from (2.12) we obtain

$$n^2 \mathbb{E}\left(\frac{1}{F(A)}\right) = n^2 - 3n + 2,$$

as required. Substitution into (5.3), after separation according to whether $n \bmod 4 = 1$ or $n \bmod 4 = 3$, gives

$$V = \begin{cases} \frac{1}{4}n^4 + \frac{7}{6}n^3 - \frac{75}{4}n^2 + \frac{151}{3}n - 128 \left\lfloor \frac{n-1}{8} \right\rfloor - 128 \left\lfloor \frac{n-1}{12} \right\rfloor - 33 & \text{for } n \bmod 4 = 1, \\ \frac{1}{4}n^4 + \frac{7}{6}n^3 - \frac{75}{4}n^2 + \frac{127}{3}n - 128 \left\lfloor \frac{n-1}{8} \right\rfloor - 128 \left\lfloor \frac{n-1}{12} \right\rfloor - 9 & \text{for } n \bmod 4 = 3, \end{cases}$$

and then from (2.13) and (5.4) we find that

$$n^4 \operatorname{Var}\left(\frac{1}{F(A)}\right) = \frac{32}{3}n^3 - 88n^2 + \frac{592}{3}n - 512 \left\lfloor \frac{n-1}{8} \right\rfloor - 512 \left\lfloor \frac{n-1}{12} \right\rfloor - 88 + 16(-1)^{\frac{n-1}{2}}(n-3),$$

as required. □

Acknowledgements

I am most grateful to Kai-Uwe Schmidt for many helpful discussions, which significantly improved this paper. I was deeply saddened both personally and professionally by his untimely passing in August 2023 and I respectfully dedicate this paper to his memory.

References

- [1] S. Aupetit, P. Liardet, and M. Slimane. Evolutionary search for binary strings with low aperiodic auto-correlations. In P. Liardet et al., editors, *Artificial Evolution*, volume 2936 of *Lecture Notes in Computer Science*, pages 39–50. Springer-Verlag, Berlin Heidelberg, 2004.
- [2] P. Borwein. *Computational Excursions in Analysis and Number Theory*. CMS Books in Mathematics. Springer-Verlag, New York, NY, 2002.
- [3] P. Borwein and K.-K.S. Choi. The average norm of polynomials of fixed height. *Trans. Amer. Math. Soc.*, **359**:923–936, 2007.
- [4] P. Borwein and R. Lockhart. The expected L_p norm of random polynomials. *Proc. Amer. Math. Soc.*, **129**:1463–1472, 2001.
- [5] M.L. Fredman, B. Saffari, and B. Smith. Polynômes réciproques: conjecture d’Erdős en norme L^4 , taille des autocorrélations et inexistence des codes de Barker. *C.R. Acad. Sci. Paris*, **308**:461–464, 1989.
- [6] M.J.E. Golay. A class of finite binary sequences with alternate autocorrelation values equal to zero. *IEEE Trans. Inf. Theory*, **IT-18**:449–450, 1972.
- [7] M.J.E. Golay. The merit factor of long low autocorrelation binary sequences. *IEEE Trans. Inf. Theory*, **IT-28**:543–549, 1982.
- [8] M.J.E. Golay and D.B. Harris. A new search for skewsymmetric binary sequences with optimal merit factors. *IEEE Trans. Inf. Theory*, **36**:1163–1166, 1990.

- [9] T. Høholdt and H.E. Jensen. Determination of the merit factor of Legendre sequences. *IEEE Trans. Inf. Theory*, **34**:161–164, 1988.
- [10] J. Jedwab. A survey of the merit factor problem for binary sequences. In T. Helleseth et al., editors, *Sequences and Their Applications — Proceedings of SETA 2004*, volume 3486 of *Lecture Notes in Computer Science*, pages 30–55. Springer-Verlag, Berlin Heidelberg, 2005.
- [11] J. Jedwab. What can be used instead of a Barker sequence? *Contemp. Math.*, **461**:153–178, 2008.
- [12] J. Jedwab. The distribution of the L_4 norm of Littlewood polynomials. [arXiv:1911.11246v1](https://arxiv.org/abs/1911.11246v1), November 2019.
- [13] J. Jedwab, D.J. Katz, and K.-U. Schmidt. Advances in the merit factor problem for binary sequences. *J. Comb. Theory A*, **120**:882–906, 2013.
- [14] J. Jedwab, D.J. Katz, and K.-U. Schmidt. Littlewood polynomials with small L^4 norm. *Adv. Math.*, **241**:127–136, 2013.
- [15] D.J. Katz and M.E. Ramirez. Moments of autocorrelation demerit factors of binary sequences. [arXiv:2307.14281v2](https://arxiv.org/abs/2307.14281v2), February 2024.
- [16] J.E. Littlewood. On polynomials $\sum^n \pm z^m$, $\sum^n e^{\alpha_m i} z^m$, $z = e^{\theta i}$. *J. London Math. Soc.*, **41**:367–376, 1966.
- [17] D.J. Newman and J.S. Byrnes. The L^4 norm of a polynomial with coefficients ± 1 . *Amer. Math. Monthly*, **97**:42–45, 1990.
- [18] T. Packebusch and S. Mertens. Low autocorrelation binary sequences. *J. Phys. A: Math. Theor.*, **49**:165001, 2016. (18 pages).
- [19] D.V. Sarwate. Mean-square correlation of shift-register sequences. *IEE Proceedings Part F*, **131**:101–106, 1984.
- [20] K.-U. Schmidt. Sequences with small correlation. *Des. Codes Cryptogr.*, **78**:237–267, 2016.
- [21] K.-U. Schmidt, J. Jedwab, and M.G. Parker. Two binary sequence families with large merit factor. *Adv. Math. Commun.*, **3**:135–156, 2009.