Combinatorics, Probability and Computing (2006) 15, 663–671.
doi:10.1017/S0963548306007589 Printed in the United Kingdom

Autocorrelations of Random Binary Sequences

IDRIS DAVID MERCER

Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada V5A 1S6
(e-mail: idmercer@math.sfu.ca)

Received 29 October 2003; revised 12 January 2005

We define $\mathscr{B}_n$ to be the set of n-tuples of the form $(a_0, \ldots, a_{n-1})$ where $a_j = \pm 1$. If $A \in \mathscr{B}_n$, then we call A a *binary sequence* and define the *autocorrelations* of A by $c_k := \sum_{j=0}^{n-k-1} a_j a_{j+k}$ for $0 \leqslant k \leqslant n-1$. The problem of finding binary sequences with autocorrelations 'near zero' has arisen in communications engineering and is also relevant to conjectures of Littlewood and Erdős on 'flat' polynomials with ± 1 coefficients. Following Turyn, we define

$$b(n) := \min_{A \in \mathscr{B}_n} \max_{1 \leqslant k \leqslant n-1} |c_k|.$$

The purpose of this article is to show that, using some known techniques from discrete probability, we can improve upon the best upper bound on $b(n)$ appearing in the previous literature, and we can obtain both asymptotic and exact expressions for the expected value of c_k^m if the a_j are independent ± 1 random variables with mean 0. We also include some brief heuristic remarks in support of the unproved conjecture that $b(n) = O(\sqrt{n})$.

1. Introduction and main results

We let $\mathscr{B}_n$ denote the set of all 2^n n-tuples of the form

$$A := (a_0, a_1, \ldots, a_{n-1}), \quad a_j = \pm 1,$$

and we refer to such an n-tuple as a *binary sequence* of *length* n. We define the (acyclic) *autocorrelations* of a binary sequence A by

$$c_k := \sum_{j=0}^{n-k-1} a_j a_{j+k}$$

for $0 \leqslant k \leqslant n-1$. Thus $c_0 = n$, and more generally, c_k is a sum of $n-k$ terms each of which is ± 1, so $c_k \equiv n-k \pmod 2$ and hence

$$0 \leqslant |c_k| \leqslant n-k \quad \text{if } n-k \text{ is even,} \tag{1.1}$$
$$1 \leqslant |c_k| \leqslant n-k \quad \text{if } n-k \text{ is odd.} \tag{1.2}$$

One can regard c_k as measuring how strongly A resembles a version of itself that has been acyclically shifted by k positions. The problem of finding binary sequences with autocorrelations 'near zero' has arisen in applications such as communications engineering [2, 8] and statistical mechanics [3], and has gained notoriety as a difficult problem in combinatorial optimization. For instance, one can ask for which n do there exist $A \in \mathscr{B}_n$ such that $|c_k| \leqslant 1$ for all $k \neq 0$. Such a sequence is called a (binary) *Barker sequence*; they exist for $n \in \{2, 3, 4, 5, 7, 11, 13\}$ and for no other $n \leqslant 4 \cdot 10^{12}$. (See [15] or [17].)

The autocorrelations of a binary sequence $(a_0, \dots, a_{n-1})$ are relevant to the 'flatness' on the unit circle of the polynomial

$$\alpha(z) := a_0 + a_1 z + \cdots + a_{n-1} z^{n-1}.$$

This is because if $|z| = 1$ and α is as above, we have

$$\begin{aligned} |\alpha(z)|^2 &= \alpha(z)\overline{\alpha(z)} \\ &= (a_0 + a_1 z + \cdots + a_{n-1} z^{n-1})\left(a_0 + a_1 \frac{1}{z} + \cdots + a_{n-1} \frac{1}{z^{n-1}}\right) \\ &= c_{n-1} \frac{1}{z^{n-1}} + \cdots + c_1 \frac{1}{z} + c_0 + c_1 z + \cdots + c_{n-1} z^{n-1} \\ &= n + 2(c_1 \Re(z) + \cdots + c_{n-1} \Re(z^{n-1})). \end{aligned}$$

So, for example, if the c_k attain the lower bounds in (1.1) and (1.2), then

$$|\alpha(z)|^2 \leqslant n + 2\left\lceil \frac{n-1}{2} \right\rceil \leqslant 2n$$

if $|z| = 1$, implying $|\alpha(z)| \leqslant \sqrt{2n}$, which would be a better upper bound than the trivial bound $|\alpha(z)| \leqslant n$ given by the triangle inequality. We say nothing more in this paper on the subject of 'flat' polynomials with ± 1 coefficients, other than referring the curious reader to Problem 26 in [7], Problem 19 in [12], or Chapters 4 and 15 of [4].

For $A \in \mathscr{B}_n$, we define the *autocorrelation vector* by

$$C := (c_1, c_2, \dots, c_{n-1}),$$

so C is simply an $(n-1)$-tuple containing the 'nontrivial' autocorrelations. Then the question of the 'closeness to zero' of the autocorrelations motivates the introduction of the usual ℓ_p norms of C. Recall their definitions:

$$\|C\|_p := (|c_1|^p + |c_2|^p + \cdots + |c_{n-1}|^p)^{1/p},$$

where $p \in \mathbb{R}$ and $p \geqslant 1$. Recall that $p \leqslant q$ implies $\|C\|_p \geqslant \|C\|_q$, and that

$$\lim_{p \to \infty} \|C\|_p = \|C\|_\infty := \max_{1 \leqslant k \leqslant n-1} |c_k|.$$

Note that if $p = 2m$ where $m \in \mathbb{Z}^+$, then

$$\|C\|_{2m} = \left(c_1^{2m} + c_2^{2m} + \cdots + c_{n-1}^{2m}\right)^{1/2m}.$$

Following [16], we adopt the notation

$$b(n) := \min_{A \in \mathscr{B}_n} \|C\|_\infty = \min_{A \in \mathscr{B}_n} \max_{1 \leqslant k \leqslant n-1} |c_k|,$$

so $b(n) = 1$ if and only if there is a Barker sequence of length n. Some exact values of $b(n)$ have been found by exhaustive search; for example, computations in [5] and [6] reveal that we have

$$\begin{aligned} b(n) &\leqslant 2 \quad \text{for all } n \leqslant 21, \\ b(n) &\leqslant 3 \quad \text{for all } n \leqslant 48, \text{ and} \\ b(n) &\leqslant 4 \quad \text{for all } n \leqslant 69. \end{aligned}$$

The exact growth rate of the function $b(n)$ remains unknown. Moon and Moser [13] proved in 1968 that for every $\varepsilon > 0$, there exists $N \in \mathbb{Z}^+$ such that

$$b(n) \leqslant (2 + \varepsilon)\sqrt{n \log n}$$

for all $n \geqslant N$. One purpose of this paper is to show (Theorem 1.3) that this can be improved to

$$b(n) \leqslant (\sqrt{2} + \varepsilon)\sqrt{n \log n}.$$

In [16], Turyn conjectured in passing that perhaps $b(n)$ grows like $\log n$. However, any result of the form $b(n) = o(\sqrt{n})$ would violate the 'merit factor conjecture' credited to Golay, which says that for all n and for all $A \in \mathscr{B}_n$, we have $\|C\|_2^2 \geqslant Kn^2$, where K is a positive constant independent of n. See [9] or Chapter 15 of [4]. It would be interesting to know whether or not $b(n) = O(\sqrt{n})$; this question does not seem to be answered in the available literature on autocorrelation of binary sequences.

Throughout the remainder of this paper, we suppose the a_j are independent random variables, each equally likely to be $+1$ or -1. This is equivalent to turning $\mathscr{B}_n$ into a sample space whose 2^n elements each have the same probability of occurring.

If n and k are fixed positive integers with $k < n$, we define $Y_k := c_{n-k}$, so Y_k is the autocorrelation which is a sum of k terms. (Here we are reverting to the common convention of using capital letters to denote random variables.) We also define $X_j := a_j a_{j+n-k}$ for $0 \leqslant j \leqslant k-1$, so we have

$$\begin{aligned} Y_k &= a_0 a_{n-k} + a_1 a_{n-k+1} + \cdots + a_{k-1} a_{n-1} \\ &= X_0 + X_1 + \cdots + X_{k-1}. \end{aligned}$$

The following is the crucial observation that allows us to prove the results of this paper.

Proposition 1.1. *The X_j are mutually independent.*

I have been told that Proposition 1.1 is folklore, but since I have not been able to find it in the literature, I include a short proof below.

Proof of Proposition 1.1. We just need to show that if the values of some of the X_j are specified, then any one of the remaining X_j is equally likely to be $+1$ or -1. So suppose $0 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k-1$ and $j \notin \{i_1, i_2, \ldots, i_m\}$, and suppose we are given that

$$X_{i_\ell} = s_\ell \quad \text{for } 1 \leqslant \ell \leqslant m, \tag{1.3}$$

where each s_ℓ is either $+1$ or -1. We must show that among the binary sequences in $\mathscr{B}_n$ that satisfy (1.3), half of them satisfy $X_j = +1$ and half satisfy $X_j = -1$.

Consider a graph G whose vertices are the a_j and whose edges are precisely the pairs of the form (a_j, a_{j+n-k}), so the edges correspond to the X_j. Note that the components of G are paths. Let G' be the graph obtained from G by deleting all edges except $X_{i_1}, \ldots, X_{i_m}$. Using the fact that the components of G' are paths, it is straightforward to see that the number of binary sequences in $\mathscr{B}_n$ satisfying (1.3) is equal to 2^λ, where λ is the number of components of G'. Observing that the endvertices of edge X_j lie in different components of G', we see that the conditional distribution of X_j is as claimed. □

The mutual independence of the X_j has several immediate consequences. First, it is obvious by symmetry that $\mathbb{E}(Y_k^r) = 0$ if r is odd. We also see that for general r, $\mathbb{E}(Y_k^r)$ is given by the non-closed-form expression

$$\sum_{j=0}^{k} \frac{\binom{k}{j}}{2^k}(k-2j)^r. \tag{1.4}$$

It is not immediately apparent that, for fixed even r, the sum (1.4) is a polynomial in k of degree $r/2$. It does, however, follow immediately from Proposition 1.1 that Y_k is a linearly transformed binomial random variable. More specifically, we have

$$Y_k = 2\left(U - \frac{k}{2}\right) = 2(U - \mathbb{E}(U)),$$

where U is binomial with parameters k and $1/2$. Thus, evaluating $\mathbb{E}(Y_k^r)$ reduces to evaluating the central moments of a binomial random variable, but as there is no simple closed-form expression for those central moments, this does not make the evaluation of $\mathbb{E}(Y_k^r)$ trivial.

A 1923 recurrence due to Romanovsky [14], which also appears in Chapter 3 of [11], shows that if U is binomial with parameters k and p, then the rth central moment of U, considered as a polynomial in k, has degree at most $\lfloor r/2 \rfloor$. Romanovsky's recurrence, however, involves differentiation with respect to p, and if we care only about the special case $p = 1/2$, then a variant of Romanovsky's technique yields a more efficient way to generate the expected values of Y_k^r. This is the content of Theorem 1.4 of this paper.

Another immediate consequence of the mutual independence of the X_j is that we can apply Chernoff-type bounds for 'tails' of sums of independent ± 1 random variables. One such Chernoff-type bound is given by the following proposition, which appears, for example, in Appendix A of [1].

Proposition 1.2. *If $Y_k = X_0 + X_1 + \cdots + X_{k-1}$, where the X_j are independent random variables equally likely to be $+1$ or -1, then for any $\lambda > 0$, we have*

$$\mathbb{P}[|Y_k| > \lambda] < 2\exp(-\lambda^2/2k).$$

This yields an improvement of the result of Moon and Moser mentioned previously.

Theorem 1.3. *For all $\varepsilon > 0$, there exists $N \in \mathbb{Z}^+$ such that if $n > N$, then there exists a binary sequence in $\mathcal{B}_n$ that satisfies*

$$|c_k| \leqslant (\sqrt{2} + \varepsilon)\sqrt{n \log n} \tag{1.5}$$

for all $k \in \{1, 2, \ldots, n-1\}$.

Proof. Suppose $\varepsilon > 0$, and define

$$\lambda := (\sqrt{2} + \varepsilon)\sqrt{n \log n}.$$

A crude overestimate for the probability that $|c_k| > \lambda$ for some $k \in \{1, \ldots, n-1\}$ is given by

$$\sum_{k=1}^{n-1} \mathbb{P}[|c_{n-k}| > \lambda] = \sum_{k=1}^{n-1} \mathbb{P}[|Y_k| > \lambda]$$

which, by Proposition 1.2, is bounded above by

$$\begin{aligned}\sum_{k=1}^{n-1} 2\exp(-\lambda^2/2k) &< \sum_{k=1}^{n-1} 2\exp(-\lambda^2/2n) \\ &< 2n\exp(-\lambda^2/2n) \\ &= 2n\exp(-(2+\varepsilon')(n\log n)/2n) \\ &= 2n\exp(-(1+\varepsilon'')\log n) \\ &= 2/n^{\varepsilon''}\end{aligned}$$

which, since it approaches 0, is certainly less than $1 - 1/2^n$ for n large enough. Therefore there exists $N \in \mathbb{Z}^+$ such that for $n > N$, at least one binary sequence in $\mathcal{B}_n$ satisfies (1.5) for all $k \in \{1, \ldots, n-1\}$. $\square$

The next result gives a particularly elegant recurrence that generates the expected values of Y_k^r (and hence also generates the central moments of a binomial random variable in the special case $p = 1/2$).

Theorem 1.4. *If the a_j, c_k, and C are as previously described, then, for $k < n$, $\mathbb{E}(c_{n-k}^{2m})$ is a polynomial in k of degree m, and hence $\mathbb{E}(\|C\|_{2m}^{2m})$ is a polynomial in n of degree $m+1$. If we define*

$$P_m(k) := \mathbb{E}\big(c_{n-k}^{2m}\big),$$

then we can generate the polynomials P_m recursively via

$$P_{m+1}(k) = k^2 P_m(k) - k(k-1)P_m(k-2). \tag{1.6}$$

Proof. If X is any random variable, we define the usual (ordinary) moment-generating function, or *MGF*,

$$M_X(t) := \mathbb{E}(e^{tX}),$$

where t is a formal variable. We have

$$\left.\frac{d^r}{dt^r} M_X(t)\right|_{t=0} = \mathbb{E}(X^r) \quad (r \in \mathbb{Z}^+),$$

or equivalently,

$$M_X(t) = 1 + \mathbb{E}(X)\frac{t}{1!} + \mathbb{E}(X^2)\frac{t^2}{2!} + \cdots .$$

Recall that if Y is a sum of k independent identically distributed random variables, each with MGF $M_X(t)$, then the MGF of Y is

$$M_Y(t) = (M_X(t))^k.$$

Thus, the MGF of the previously defined $Y_k = c_{n-k}$ is

$$M(t) := \left(\frac{e^{+t} + e^{-t}}{2}\right)^k = \cosh^k t = 1 + \mathbb{E}(Y_k^2)\frac{t^2}{2!} + \mathbb{E}\big(Y_k^4\big)\frac{t^4}{4!} + \cdots$$

(note that the MGF of Y_k contains only even powers of t since $\mathbb{E}(Y_k^r) = 0$ when r is odd).

We now observe that

$$\begin{aligned}\frac{d^2}{dt^2} M(t) &= \frac{d}{dt}(k \cosh^{k-1} t \sinh t)\\ &= k(k-1)\cosh^{k-2} t \sinh^2 t + k \cosh^k t\\ &= k(k-1)\cosh^{k-2} t(\cosh^2 t - 1) + k\cosh^k t\\ &= k^2 \cosh^k t - k(k-1)\cosh^{k-2} t, \end{aligned} \tag{1.7}$$

but also

$$\begin{aligned}\frac{d^2}{dt^2} M(t) &= \frac{d^2}{dt^2}\left(1 + \mathbb{E}\big(Y_k^2\big)\frac{t^2}{2!} + \mathbb{E}\big(Y_k^4\big)\frac{t^4}{4!} + \cdots\right)\\ &= \mathbb{E}\big(Y_k^2\big) + \mathbb{E}\big(Y_k^4\big)\frac{t^2}{2!} + \mathbb{E}\big(Y_k^6\big)\frac{t^4}{4!} + \cdots . \end{aligned} \tag{1.8}$$

If we now equate the coefficient of $t^{2m}/(2m)!$ in (1.8) and the coefficient of $t^{2m}/(2m)!$ in (1.7), we get

$$\mathbb{E}\big(Y_k^{2m+2}\big) = k^2\mathbb{E}\big(Y_k^{2m}\big) - k(k-1)\mathbb{E}\big(Y_{k-2}^{2m}\big),$$

or equivalently,

$$P_{m+1}(k) = k^2 P_m(k) - k(k-1)P_m(k-2),$$

establishing (1.6), as required. □

2. Further comments

For illustration, we give the first few polynomials $P_m(k)$ generated by the recurrence (1.6):

$$\begin{aligned} P_1(k) &= k = \mathbb{E}\big(Y_k^2\big),\\ P_2(k) &= 3k^2 - 2k = \mathbb{E}\big(Y_k^4\big),\\ P_3(k) &= 15k^3 - 30k^2 + 16k = \mathbb{E}\big(Y_k^6\big),\\ P_4(k) &= 105k^4 - 420k^3 + 588k^2 - 272k = \mathbb{E}\big(Y_k^8\big). \end{aligned}$$

In general, $P_m(k)$ has the form

$$P_m(k) = (2m-1)!!\,k^m + O(k^{m-1}), \tag{2.1}$$

where the notation $(2m-1)!!$ means $(2m-1)(2m-3)\cdots 3\cdot 1$. This does not seem to follow immediately from (1.6), but can be proved by a counting argument, which we consider too much of a digression to include here.

If we care only about the asymptotic behaviour of $\mathbb{E}(Y_k^{2m})$, then it is worth noting that we can prove

$$\mathbb{E}(Y_k^{2m}) \leqslant (2m-1)!!\,k^m \tag{2.2}$$

by using the following version of the Khinchin inequalities, due to Haagerup [10].

Proposition 2.1. *Let $X_0,\ldots,X_{k-1}$ be independent random variables, each equally likely to be $+1$ or -1, and let $r_0,\ldots,r_{k-1}$ be real constants. For positive real p, we have*

$$A_p\left(\sum_{j=0}^{k-1} r_j^2\right)^{1/2} \leqslant \left[\mathbb{E}\left(\left|\sum_{j=0}^{k-1} r_j X_j\right|^p\right)\right]^{1/p} \leqslant B_p\left(\sum_{j=0}^{k-1} r_j^2\right)^{1/2}, \tag{2.3}$$

where A_p and B_p are constants depending only on p. If $p>2$, we can take $A_p = 1$ and

$$B_p = 2^{1/2}\left(\frac{\Gamma(\frac{p+1}{2})}{\sqrt{\pi}}\right)^{1/p}.$$

If $p = 2m$ where $m\in\mathbb{Z}^+$, and $r_j = 1$ for all j, then the rightmost inequality in (2.3) gives

$$\mathbb{E}\big(Y_k^{2m}\big) = \mathbb{E}\left(\left|\sum_{j=0}^{k-1} X_j\right|^{2m}\right) \leqslant B_{2m}^{2m}\left(\sum_{j=0}^{k-1} 1\right)^m = B_{2m}^{2m}k^m,$$

and we then observe that

$$B_{2m}^{2m} = 2^m\frac{\Gamma(\frac{2m+1}{2})}{\sqrt{\pi}} = 2^m\frac{\frac{(2m-1)!!}{2^m}\sqrt{\pi}}{\sqrt{\pi}} = (2m-1)!!,$$

which establishes that (2.2) holds as claimed.

We now observe that (2.1), together with the elementary fact that a random variable cannot always exceed its expected value, yields upper bounds on $b(n)$ that, roughly speaking, are 'slightly greater' than $\sqrt{n}$, as is true of the bound given by Theorem 1.3.

If the c_k and C are as defined previously, observe that

$$\begin{aligned}\mathbb{E}\big(\|C\|_{2m}^{2m}\big) &= \mathbb{E}\left(\sum_{k=1}^{n-1} c_{n-k}^{2m}\right) = \sum_{k=1}^{n-1}\mathbb{E}\big(Y_k^{2m}\big) = \sum_{k=1}^{n-1} P_m(k)\\ &= \sum_{k=1}^{n-1}((2m-1)!!\,k^m + O(k^{m-1}))\\ &= (2m-1)!!\frac{n^{m+1}}{m+1} + O(n^m).\end{aligned}$$

It follows that there is at least one binary sequence in $\mathscr{B}_n$ that satisfies

$$\|C\|_{2m}^{2m} \leqslant \frac{(2m-1)!!}{m+1} n^{m+1} + O(n^m)$$

and hence also satisfies

$$\|C\|_\infty \leqslant \|C\|_{2m} \leqslant \left(\frac{(2m-1)!!}{m+1}\right)^{1/2m} n^{(m+1)/2m} + o\big(n^{(m+1)/2m}\big). \tag{2.4}$$

For example, we have

$$\begin{aligned}\mathbb{E}\big(\|C\|_{10}^{10}\big) &= \sum_{k=1}^{n-1} P_5(k) = \sum_{k=1}^{n-1}(945k^5 - 6300k^4 + 16380k^3 - 18960k^2 + 7936k) \\ &= \frac{315}{2}n^6 - \frac{3465}{2}n^5 + \frac{30555}{4}n^4 - 16610n^3 + \frac{69857}{4}n^2 - 6918n\end{aligned}$$

which, a computation reveals, is less than $(315/2)n^6$ for $n \geqslant 1$. It follows that for $n \geqslant 1$ there is always at least one binary sequence in $\mathscr{B}_n$ satisfying

$$\|C\|_\infty \leqslant \|C\|_{10} \leqslant \left(\frac{315}{2}n^6\right)^{1/10} \approx 1.658n^{6/10}.$$

We thus get an upper bound on $b(n)$ that is worse than Theorem 1.3 in a big O sense, but better than Theorem 1.3 in the sense that it holds for all n.

Notice that in the proof of Theorem 1.3 we were able to show that, eventually, 'most' binary sequences in $\mathscr{B}_n$ satisfy

$$\|C\|_\infty \leqslant (\sqrt{2} + \varepsilon)\sqrt{n \log n},$$

by using the trivial fact that the probability of a union of events is bounded above by the sum of the probabilities of the events. Notice also that (2.4) says, roughly speaking, that any binary sequence in $\mathscr{B}_n$ that is merely 'better than average' will satisfy

$$\|C\|_\infty \leqslant K_m n^{(m+1)/2m} + o\big(n^{(m+1)/2m}\big)$$

(where the constant K_m of course depends on m). For these reasons, it is the author's opinion that in the near future, more sophisticated techniques will establish the (as yet unproved) statement that we have $b(n) = O(\sqrt{n})$.

Acknowledgements

The author would like to thank the referee of the first version of this paper for pointing out the connection with the Khinchin inequalities.

References

[1] Alon, N. and Spencer, J. H. (2000) *The Probabilistic Method*, 2nd edn, Wiley, New York.

[2] Barker, R. H. (1953) Group synchronising of binary digital systems. In *Communication Theory* (W. Jackson, ed.), Butterworth, London, pp. 273–287.

[3] Bernasconi, J. (1988) Statistical physics and optimization: Binary sequences with small autocorrelations. In *Stochastic Processes in Physics and Engineering* (S. Albeverio *et al.*, eds), Reidel, Dordrecht, Germany, pp. 1–16.
[4] Borwein, P. (2002) *Computational Excursions in Analysis and Number Theory*, Springer, New York.
[5] Cohen, M. N., Fox, M. R. and Baden, J. M. (1990) Minimum peak sidelobe compression codes. In *IEEE International Radar Conference*, IEEE, pp. 633–638.
[6] Coxson, G. E., Hirschel, A. and Cohen, M. N. (2001) New results on minimum-PSL binary codes. In *IEEE Radar Conference*, IEEE, pp. 153–156.
[7] Erdős, P. (1957) Some unsolved problems. *Michigan Math. J.* **4** 291–300.
[8] Fan, P. and Darnell, M. (1996) *Sequence Design for Communications Applications*, Research Studies Press, Taunton, UK.
[9] Golay, M. J. (1972) A class of finite binary sequences with alternate autocorrelation values equal to zero. *IEEE Trans. Inform. Theory* **18** 449–450.
[10] Haagerup, U. (1981) The best constants in the Khintchine inequality. *Studia. Math.* **70** 231–283.
[11] Johnson, N. L., Kotz, S. and Kemp, A. W. (1992) *Univariate Discrete Distributions*, Wiley, New York.
[12] Littlewood, J. E. (1968) *Some Problems in Real and Complex Analysis*, D. C. Heath and Co., Lexington, MA.
[13] Moon, J. W. and Moser, L. (1968) On the correlation function of random binary sequences. *SIAM J. Appl. Math.* **16** 340–343.
[14] Romanovsky, V. (1923) Note on the moments of a binomial $(p+q)^n$ about its mean. *Biometrika* **15** 410–412.
[15] Schmidt, B. (1999) Cyclotomic integers and finite geometry. *J. Amer. Math. Soc.* **12** 929–952.
[16] Turyn, R. J. (1968) Sequences with small correlation. In *Error Correcting Codes: Proceedings of a Symposium* (H. B. Mann, ed.), Wiley, New York, pp. 195–228.
[17] Turyn, R. J. and Storer, J. (1961) On binary sequences. *Proc. Amer. Math. Soc.* **12** 394–399.