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 $B_n$ to be the set of $n$-tuples of the form $(a_0, \ldots, a_{n-1})$ where $a_j = \pm 1$. If $A \in B_n$, 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 $0 \leq k \leq n-1$. 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 $\pm 1$ coefficients. Following Turyn, we define $b(n) := \min_{A \in B_n} \max_{1 \leq k \leq n-1} |c_k|$. 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 $\pm 1$ 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 $B_n$ denote the set of all $2^n$ $n$-tuples of the form $A := (a_0, a_1, \ldots, a_{n-1})$, $a_j = \pm 1$, 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 $0 \leq k \leq n-1$. Thus $c_0 = n$, and more generally, $c_k$ is a sum of $n-k$ terms each of which is $\pm 1$, so $c_k \equiv n-k \pmod{2}$ and hence

1. $0 \leq |c_k| \leq n-k$ if $n-k$ is even, \hspace{1cm} (1.1)
2. $1 \leq |c_k| \leq n-k$ if $n-k$ is odd. \hspace{1cm} (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 \cite{2, 8} and statistical mechanics \cite{3}, and has gained notoriety as a difficult problem in combinatorial optimization. For instance, one can ask for which $n$ do there exist $A \in B_n$ such that $|c_k| \leq 1$ 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 $n \leq 4 \cdot 10^{12}$. (See \cite{15} or \cite{17}.)

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

$$z(z) := \frac{a_0}{z} + \frac{a_1}{z^2} + \cdots + \frac{a_{n-1}}{zn^{n-1}}.$$ 

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

$$|z(z)|^2 = |z(z)\bar{z}| = (a_0 + a_1z + \cdots + a_{n-1}zn^{n-1})(a_0 + a_1\frac{1}{z} + \cdots + a_{n-1}\frac{1}{zn-1})$$

$$= c_{n-1}\frac{1}{zn-1} + \cdots + c_1\frac{1}{z} + c_0 + c_1z + \cdots + c_{n-1}zn^{n-1}$$

$$= n + 2(c_1\Re(z) + \cdots + c_{n-1}\Re(z^{n-1})).$$

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

$$|z(z)|^2 \leq n + 2\left(\frac{n-1}{2}\right) \leq 2n$$

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

For $A \in B_n$, we define the autocorrelation vector by

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

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 $\ell_p$ 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 $p \geq 1$. Recall that $p \leq q$ implies $\|C\|_p \geq \|C\|_q$, and that

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

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

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

Following \cite{16}, we adopt the notation

$$b(n) := \min_{A \in B_n} \|C\|_{\infty} = \min_{A \in B_n} \max_{1 \leq k \leq n-1} |c_k|,$$
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{align*}
    b(n) &\leq 2 \quad \text{for all } n \leq 21, \\
    b(n) &\leq 3 \quad \text{for all } n \leq 48, \text{ and} \\
    b(n) &\leq 4 \quad \text{for all } n \leq 69.
\end{align*}

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

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

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

$$b(n) \leq (\sqrt{2} + \varepsilon)\sqrt{n \log n}.$$
where each \( s_r \) is either +1 or −1. We must show that among the binary sequences in \( B_n \) 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 \( X_1, \ldots, X_m \). Using the fact that the components of \( G' \) are paths, it is straightforward to see that the number of binary sequences in \( B_n \) satisfying (1.3) is equal to \( 2^\lambda \), where \( \lambda \) 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 \( \mathbb{E}(Y_r^k) = 0 \) if \( r \) is odd. We also see that for general \( r \), \( \mathbb{E}(Y_r^k) \) is given by the non-closed-form expression

\[
\sum_{j=0}^{k} \left( \begin{array}{c}
k \\
2j\end{array} \right) (k - 2j)^r.
\]

(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 \( \mathbb{E}(Y_r^k) \) 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 \( \mathbb{E}(Y_r^k) \) 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 \( r \)th 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 \( Y_r^k \). 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 $B_n$ that satisfies

$$|c_k| \leq (\sqrt{2} + \varepsilon)\sqrt{n \log n} \quad (1.5)$$

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

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

which, by Proposition 1.2, is bounded above by

$$\sum_{k=1}^{n-1} 2 \exp(-\lambda^2/2k) < \sum_{k=1}^{n-1} 2 \exp(-\lambda^2/2n)$$

$$< 2n \exp(-\lambda^2/2n)$$

$$= 2n \exp(-(2 + \varepsilon')(n \log n)/2n)$$

$$= 2n \exp(-(1 + \varepsilon'') \log n)$$

$$= 2/n^{\varepsilon''}$$

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 $B_n$ satisfies (1.5) for all $k \in \{1, \ldots, n-1\}$.

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 $k < n$, $E(c_{n-k}^{2m})$ is a polynomial in $k$ of degree $m$, and hence $E(\|C\|_{2m}^2)$ is a polynomial in $n$ of degree $m+1$. If we define

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

then we can generate the polynomials $P_m$ recursively via

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

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

$$M_X(t) := E(e^{tx}),$$

then we have

$$E(c_{n-k}^{2m}) = E(e^{tx}) = \left[E(e^{tx})\right]^{2m} = P_m(k).$$

The recursion follows from

$$E(e^{tx}) = E([E(e^{tx})]^{2m}) = E(E(e^{tx})E(e^{tx})^{2m-2}) = E(E(e^{tx})E(e^{tx})^{2m-2}) = E(E(e^{tx})^{2m-1}).$$

Therefore, $P_m(k)$ is a polynomial in $k$ of degree $m$, and hence $E(\|C\|_{2m}^2)$ is a polynomial in $n$ of degree $m+1$. If we define

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

then we can generate the polynomials $P_m$ recursively via

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

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

$$M_X(t) := E(e^{tx}),$$

then we have

$$E(c_{n-k}^{2m}) = E(e^{tx}) = \left[E(e^{tx})\right]^{2m} = P_m(k).$$

The recursion follows from

$$E(e^{tx}) = E([E(e^{tx})]^{2m}) = E(E(e^{tx})E(e^{tx})^{2m-2}) = E(E(e^{tx})E(e^{tx})^{2m-2}) = E(E(e^{tx})^{2m-1}).$$

Therefore, $P_m(k)$ is a polynomial in $k$ of degree $m$, and hence $E(\|C\|_{2m}^2)$ is a polynomial in $n$ of degree $m+1$. If we define

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

then we can generate the polynomials $P_m$ recursively via

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

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

$$M_X(t) := E(e^{tx}),$$

then we have

$$E(c_{n-k}^{2m}) = E(e^{tx}) = \left[E(e^{tx})\right]^{2m} = P_m(k).$$

The recursion follows from

$$E(e^{tx}) = E([E(e^{tx})]^{2m}) = E(E(e^{tx})E(e^{tx})^{2m-2}) = E(E(e^{tx})E(e^{tx})^{2m-2}) = E(E(e^{tx})^{2m-1}).$$

Therefore, $P_m(k)$ is a polynomial in $k$ of degree $m$, and hence $E(\|C\|_{2m}^2)$ is a polynomial in $n$ of degree $m+1$. If we define

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

then we can generate the polynomials $P_m$ recursively via

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

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

$$M_X(t) := E(e^{tx}),$$

then we have

$$E(c_{n-k}^{2m}) = E(e^{tx}) = \left[E(e^{tx})\right]^{2m} = P_m(k).$$

The recursion follows from

$$E(e^{tx}) = E([E(e^{tx})]^{2m}) = E(E(e^{tx})E(e^{tx})^{2m-2}) = E(E(e^{tx})E(e^{tx})^{2m-2}) = E(E(e^{tx})^{2m-1}).$$

Therefore, $P_m(k)$ is a polynomial in $k$ of degree $m$, and hence $E(\|C\|_{2m}^2)$ is a polynomial in $n$ of degree $m+1$. If we define

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

then we can generate the polynomials $P_m$ recursively via

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

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

$$M_X(t) := E(e^{tx}),$$

then we have

$$E(c_{n-k}^{2m}) = E(e^{tx}) = \left[E(e^{tx})\right]^{2m} = P_m(k).$$

The recursion follows from

$$E(e^{tx}) = E([E(e^{tx})]^{2m}) = E(E(e^{tx})E(e^{tx})^{2m-2}) = E(E(e^{tx})E(e^{tx})^{2m-2}) = E(E(e^{tx})^{2m-1}).$$

Therefore, $P_m(k)$ is a polynomial in $k$ of degree $m$, and hence $E(\|C\|_{2m}^2)$ is a polynomial in $n$ of degree $m+1$. If we define

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

then we can generate the polynomials $P_m$ recursively via

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

Proof. If $X$ is any random variable, we define the usual (ordinary) moment-generating function, or $MGF$,
where \( t \) is a formal variable. We have
\[
\frac{d^r}{dt^r} M_X(t) \bigg|_{t=0} = \mathbb{E}(X'^r) \quad (r \in \mathbb{Z}^+),
\]
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
\[
M(t) := \left( \frac{e^{+t} + e^{-t}}{2} \right)^k = \cosh^k t = 1 + \mathbb{E}(Y_k^2) \frac{t^2}{2!} + \mathbb{E}(Y_k^4) \frac{t^4}{4!} + \cdots
\]
(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
\[
\frac{d^2}{dt^2} M(t) = \frac{d}{dt} (k \cosh^{k-1} t \sinh t)
= k(k-1) \cosh^{k-2} t \sinh^2 t + k \cosh^k t
= k(k-1) \cosh^{k-2} t (\cosh^2 t - 1) + k \cosh^k t
= k^2 \cosh^k t - k(k-1) \cosh^{k-2} t,
\]
but also
\[
\frac{d^2}{dt^2} M(t) = \frac{d^2}{dt^2} \left( 1 + \mathbb{E}(Y_k^2) \frac{t^2}{2!} + \mathbb{E}(Y_k^4) \frac{t^4}{4!} + \cdots \right)
= \mathbb{E}(Y_k^2) + \mathbb{E}(Y_k^4) \frac{t^2}{2!} + \mathbb{E}(Y_k^6) \frac{t^4}{4!} + \cdots. \tag{1.8}
\]
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
\[
\mathbb{E}(Y_k^{2m+2}) = k^2 \mathbb{E}(Y_k^{2m}) - k(k-1) \mathbb{E}(Y_k^{2m-2}),
\]
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):
\[
P_1(k) = k = \mathbb{E}(Y_k^2),
\]
\[
P_2(k) = 3k^2 - 2k = \mathbb{E}(Y_k^4),
\]
\[
P_3(k) = 15k^3 - 30k^2 + 16k = \mathbb{E}(Y_k^6),
\]
\[
P_4(k) = 105k^4 - 420k^3 + 588k^2 - 272k = \mathbb{E}(Y_k^8).
\]
In general, $P_m(k)$ has the form
\[ P_m(k) = (2m - 1)!! k^m + O(k^{m-1}), \]  
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
\[ \mathbb{E}(Y_k^{2m}) \leq (2m - 1)!! k^m \]  
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
\[ A_p \left( \sum_{j=0}^{k-1} r_j^2 \right)^{1/2} \leq \left[ \mathbb{E} \left( \left| \sum_{j=0}^{k-1} r_j X_j \right|^p \right) \right]^{1/p} \leq B_p \left( \sum_{j=0}^{k-1} r_j^2 \right)^{1/2}, \]  
where $A_p$ and $B_p$ are constants depending only on $p$. If $p > 2$, we can take $A_p = 1$ and
\[ B_p = 2^{1/2} \left( \frac{\Gamma\left(\frac{p+1}{2}\right)}{\sqrt{\pi}} \right)^{1/p}. \]  
If $p = 2m$ where $m \in \mathbb{Z}^+$, and $r_j = 1$ for all $j$, then the rightmost inequality in (2.3) gives
\[ \mathbb{E}(Y_k^{2m}) = \mathbb{E} \left( \left| \sum_{j=0}^{k-1} X_j \right|^{2m} \right) \leq B_{2m}^2 \left( \sum_{j=0}^{k-1} 1 \right)^m = B_{2m}^2 k^m, \]  
and we then observe that
\[ B_{2m}^2 = 2^m \frac{\Gamma\left(\frac{2m+1}{2}\right)}{\sqrt{\pi}} = 2^m \frac{(2m-1)!! \sqrt{\pi}}{\sqrt{\pi}} = (2m - 1)!!, \]  
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
\[ \mathbb{E}(\|C\|_{2m}^{2m}) = \mathbb{E} \left( \sum_{k=1}^{n-1} c_{n-k}^{2m} \right) = \sum_{k=1}^{n-1} \mathbb{E}(Y_k^{2m}) = \sum_{k=1}^{n-1} P_m(k) \]
\[ = \sum_{k=1}^{n-1} ((2m - 1)!! k^m + O(k^{m-1})) \]
\[ = (2m - 1)!! \frac{n^{m+1}}{m+1} + O(n^m). \]
It follows that there is at least one binary sequence in $B_n$ that satisfies

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

and hence also satisfies

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

For example, we have

$$E(\|C\|_{10}^{10}) = \sum_{k=1}^{n-1} P_{5}(k) = \sum_{k=1}^{n-1} (945k^5 - 6300k^4 + 16380k^3 - 18960k^2 + 7936k)$$

$$= \frac{315}{2} n^6 - \frac{3465}{2} n^5 + \frac{30555}{4} n^4 - 16610n^3 + \frac{69857}{4} n^2 - 6918n$$

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

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

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 $B_n$ satisfy

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

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 $B_n$ that is merely ‘better than average’ will satisfy

$$\|C\|_{\infty} \leq K_m n^{(m+1)/2m} + o\left(n^{(m+1)/2m}\right)$$

(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

Autocorrelations of Random Binary Sequences


