Large deviations for code division multiple access systems

SIAM J. APPL. MATH.
Vol. 62, No. 3, pp. 1044–1065

LARGE DEVIATIONS FOR CODE DIVISION MULTIPLE ACCESS SYSTEMS*

REMCO VAN DER HOFSTAD†, GERARD HOOGHIEMSTRA†, AND MARTEN J. KLOK‡

Abstract. We derive approximations for the probability of a bit error for a code division multiple access (CDMA) system with one-stage soft decision parallel interference cancellation. More precisely, we derive the exponential rates, J_k with cancellation and I_k without cancellation, of a CDMA system with k users and processing gain equal to n as $n \to \infty$.

Whereas the rates I_k follow explicitly from Cramér's theorem, the rates J_k are given in terms of an optimization problem that can be evaluated numerically. We prove that $J_k > I_k$ for $k \geq 3$, which shows that interference cancellation is effective. For the case without interference cancellation, we investigate the second order (Bahadur–Rao) asymptotics. For the case with interference cancellation, we can obtain second order asymptotics only for $k = 3$. Together the limits provide excellent approximations for the probability of a bit error in a wide range of interest.

Key words. large deviation theory, code division multiple access, soft decision parallel interference cancellation, Bahadur–Rao asymptotics

AMS subject classifications. Primary, 60F10, 94A05; Secondary, 60F17, 11K06, 94A11, 94A12

PII. S003613999936372X

1. Introduction.

We consider a problem from telecommunications. Suppose that a system has k users and that all users transmit data simultaneously. In order to do so, each user multiplies his data signal by an individual coding sequence. At the receiver, the signal of the mth ($1 \leq m \leq k$) user can be retrieved by taking the inner product of the transformed total signal and the mth coding sequence. In the case in which the coding sequences are orthogonal, all data that does not originate from the mth user will be annihilated. This technique is known as *code division multiple access* (CDMA); cf. [7].

More precisely, we define the data signal $b_m(t)$ of the mth user as

$$b_m(t) = \sum_{i=-\infty}^{\infty} b_{mi}\, p_T(t - iT), \quad 1 \leq m \leq k, \tag{1}$$

where $b_m = (\ldots, b_{m,-1}, b_{m0}, b_{m1}, \ldots) \in \{-1, +1\}^{\mathbb{Z}}$ and where for $T > 0$,

$$p_T(t) = \begin{cases} 1, & 0 \leq t < T, \\ 0, & \text{elsewhere.} \end{cases}$$

Note that $b_m(t) = b_{m,\lfloor t/T \rfloor}$, where for $x \in \mathbb{R}$, $\lfloor x \rfloor$ denotes the largest integer smaller than or equal to x. For each m, $1 \leq m \leq k$, a sequence $a_m = (\ldots, a_{m,-1}, a_{m0}, a_{m1}, \ldots) \in \{-1, +1\}^{\mathbb{Z}}$ is generated, and we put

$$a_m(t) = \sum_{i=-\infty}^{\infty} a_{mi}\, p_{T_c}(t - iT_c),$$

*Received by the editors November 3, 1999; accepted for publication (in revised form) July 16, 2001; published electronically February 6, 2002.
http://www.siam.org/journals/siap/62-3/36372.html

†Department of Mathematics, Faculty ITS, Delft University of Technology, Mekelweg 4, 2628 CD Delft, the Netherlands (R.W.vanderHofstad@its.tudelft.nl, G.Hooghiemstra@its.tudelft.nl).

‡IRCTR, Delft University of Technology, Mekelweg 4, 2628 CD Delft, the Netherlands (m.j.klok@its.tudelft.nl).

where $T_c = T/n$ for some integer n. In practice, the value of n ranges from 30–180. The transmitted coded signal of the mth user is then

$$s_m(t) = \sqrt{2P}\, b_m(t) a_m(t) \cos(\omega_c t), \quad 1 \le m \le k, \tag{2}$$

where P is the power and ω_c is the carrier frequency. The total transmitted signal is given by

$$r(t) = \sum_{j=1}^{k} s_j(t). \tag{3}$$

To retrieve the data bit b_{m0}, the signal $r(t)$ is multiplied by $a_m(t)\cos(\omega_c t)$ and then averaged over $[0, T]$:

$$\begin{aligned}\frac{1}{T}\int_0^T r(t) a_m(t)\cos(\omega_c t)\, dt &= b_{m0}\frac{\sqrt{2P}}{T}\int_0^T \left\{\frac{1}{2} + \frac{1}{2}\cos(2\omega_c t)\right\} dt \\ &\quad + \frac{1}{n}\sum_{\substack{j=1 \\ j\neq m}}^{k} b_{j0} \sum_{i=0}^{n-1} a_{ji} a_{mi} \frac{\sqrt{2P}}{T_c}\int_{iT_c}^{(i+1)T_c} \left\{\frac{1}{2} + \frac{1}{2}\cos(2\omega_c t)\right\} dt.\end{aligned}$$

In practice, we take $\omega_c T_c$ large. For simplicity, we pick $\omega_c T_c = \pi f_c$, where $f_c \in \mathbb{N}$, to get

$$\frac{1}{T}\int_0^T r(t) a_m(t)\cos(\omega_c t)\, dt = \frac{1}{2}\sqrt{2P} b_{m0} + \frac{1}{2}\sqrt{2P}\sum_{\substack{j=1 \\ j\neq m}}^{k} b_{j0}\frac{1}{n}\sum_{i=0}^{n-1} a_{ji} a_{mi}. \tag{4}$$

The decoded signal consists of the desired bit and interference due to the other users.

In an ideal situation the vectors $(a_{m0}, \ldots, a_{m,n-1})$ and $(a_{j0}, \ldots, a_{j,n-1})$, $j \neq m$, would be orthogonal, so that $\sum_{i=0}^{n-1} a_{ji} a_{mi} = 0$. In practice, however, the a-sequences are generated by a random number generator.

To model the pseudorandom sequence a, let A_{mi}, $m = 1, 2, \ldots, k$, $i = 1, 2, \ldots, n$, be an array of independent and identically distributed (i.i.d.) random variables with distribution

$$\mathbb{P}(A_{11} = +1) = \mathbb{P}(A_{11} = -1) = 1/2. \tag{5}$$

Assuming the coding sequences to be random, we model the signal in (4) as

$$\frac{1}{2}\sqrt{2P} b_{m0} + \frac{1}{2}\sqrt{2P}\sum_{\substack{j=1 \\ j\neq m}}^{k} b_{j0}\frac{1}{n}\sum_{i=1}^{n} A_{ji} A_{mi},$$

where we have replaced $i = 0, \ldots, n-1$ by $i = 1, \ldots, n$, for notational convenience. Note that for each m and j, the sequence $A_{ji}A_{mi}$, $i = 1, \ldots, n$, is an i.i.d. sequence with mean 0, and so by the strong law of large numbers, $\frac{1}{n}\sum_{i=1}^{n} A_{ji}A_{mi} \to 0$ almost surely as n increases to ∞. We shall see that the performance of the system increases with n; for this reason n is called the *processing gain*. An estimator for b_{m0} is given by

$$\hat{b}_{m0} = \operatorname{sign}\left(\frac{1}{2}\sqrt{2P} b_{m0} + \frac{1}{2}\sqrt{2P}\sum_{\substack{j=1 \\ j\neq m}}^{k} b_{j0}\frac{1}{n}\sum_{i=1}^{n} A_{ji} A_{mi}\right),$$

where, for $x \in \mathbb{R}$,

$$\operatorname{sign}(x) = \begin{cases} +1, & x > 0, \\ 0, & x = 0, \\ -1, & x < 0. \end{cases}$$

We are interested in the probability of a bit error, i.e., $\mathbb{P}(\hat{b}_{m0} \neq b_{m0})$. If we define

$$Z_m^{(1)} = 1 + \sum_{\substack{j=1 \\ j \neq m}}^{k} \frac{1}{n} \sum_{i=1}^{n} A_{ji} A_{mi}, \tag{6}$$

then

$$\frac{\hat{b}_{m0}}{b_{m0}} \stackrel{d}{=} \operatorname{sign}(Z_m^{(1)}),$$

since $A_{ji} \stackrel{d}{=} b_{j0} A_{ji}$ and

$$b_{m0} + \sum_{\substack{j=1 \\ j \neq m}}^{k} b_{j0} \frac{1}{n} \sum_{i=1}^{n} A_{ji} A_{mi} = b_{m0} \left(1 + \sum_{\substack{j=1 \\ j \neq m}}^{k} \frac{1}{n} \sum_{i=1}^{n} b_{j0} A_{ji} b_{m0} A_{mi} \right). \tag{7}$$

Hence

$$\mathbb{P}(\hat{b}_{m0} \neq b_{m0}) = \mathbb{P}\left(\frac{\hat{b}_{m0}}{b_{m0}} \neq 1 \right) = \mathbb{P}(Z_m^{(1)} \leq 0).$$

If the probability of the event $\{\hat{b}_{m0} \neq b_{m0}\}$ is too large, we try to cancel the interference of the other users (i.e., the users with subscript $j \neq m$). We estimate the data signal $s_j(t)$ for $t \in [0, T]$ by (recall (2) and (4))

$$\begin{aligned} \hat{s}_j(t) &= 2 \left(\frac{1}{T} \int_0^T r(\tau) a_j(\tau) \cos(\omega_c \tau) \, d\tau \right) (a_j(t) \cos(\omega_c t)) \\ &= \left(\sqrt{2P} b_{j0} + \sqrt{2P} \sum_{\substack{l=1 \\ l \neq j}}^{k} b_{l0} \frac{1}{n} \sum_{i=1}^{n} A_{li} A_{ji} \right) (a_j(t) \cos(\omega_c t)). \end{aligned}$$

Then we estimate the total interference in $r(t)$ by (recall (3))

$$\hat{r}_m(t) = \sum_{\substack{j=1 \\ j \neq m}}^{k} \hat{s}_j(t).$$

We use the above to estimate the data bit b_{m0} by the sign of

$$\begin{aligned} &\frac{1}{T} \int_0^T (r(t) - \hat{r}_m(t)) a_m(t) \cos(\omega_c t) dt \\ &= \frac{1}{2} \sqrt{2P} b_{m0} - \frac{1}{2} \sqrt{2P} \sum_{\substack{j=1 \\ j \neq m}}^{k} \left(\frac{1}{n} \sum_{i=1}^{n} A_{ji} A_{mi} \right) \left(\frac{1}{n} \sum_{\substack{l=1 \\ l \neq j}}^{k} b_{l0} \sum_{i=1}^{n} A_{li} A_{ji} \right). \end{aligned} \tag{8}$$

This procedure is called *soft decision interference cancellation*; cf. [2]. Let $\hat{b}_{m0}^{(2)}$ be the sign of the quantity in (8). We are now interested in the probability that $\hat{b}_{m0}^{(2)} \neq b_{m0}$. Defining

$$Z_m^{(2)} = 1 + \sum_{\substack{j=1 \\ j \neq m}}^{k} \left(\frac{1}{n} \sum_{i=1}^{n} A_{ji} A_{mi} \right) [1 - Z_j^{(1)}], \tag{9}$$

we obtain, similarly as before,

$$\mathbb{P}(\hat{b}_{m0}^{(2)} \neq b_{m0}) = \mathbb{P}(Z_m^{(2)} \leq 0).$$

In this paper we describe the asymptotic behavior for the processing gain $n \to \infty$ of $\mathbb{P}(Z_m^{(s)} \leq 0)$, for $s = 1$ and $s = 2$, using large deviation theory; cf. [3, 6]. To date, the probability of a bit error has only been investigated using the central limit theorem or simulations (cf. Chapter 4 of [8] and the references therein). To our knowledge, the only paper on CDMA in which large deviation theory was involved is [9]. In that paper, rare event simulation was applied to obtain results for the bit error probability when $s = 1$.

Note that the random variables $Z_1^{(s)}, Z_2^{(s)}, \ldots, Z_k^{(s)}$ are exchangeable, so that it suffices to consider the case in which $m = 1$. Also, it is clear that for $k = 1$ there is no interference due to other users, and therefore $\mathbb{P}(Z_1^{(s)} \leq 0) = 0$, $s = 1, 2$. For $k = 2$, i.e., for *two* users, something peculiar happens. It is readily seen that for $k = 2$

$$\hat{b}_{10} = \operatorname{sign}\left(b_{10} + \frac{b_{20}}{n} \sum_{i=1}^{n} A_{1i} A_{2i} \right), \qquad \hat{b}_{10}^{(2)} = \operatorname{sign}\left(b_{10} - \frac{b_{10}}{n^2} \left(\sum_{i=1}^{n} A_{1i} A_{2i} \right)^2 \right).$$

Hence

$$\mathbb{P}(\hat{b}_{10}^{(2)} \neq b_{10}) = \mathbb{P}\left(\left(\sum_{i=1}^{n} A_{1i} A_{2i} \right)^2 = n^2 \right) = 2^{-n+1} = 2\mathbb{P}(\hat{b}_{10} \neq b_{10}),$$

so that after interference cancellation the probability of a bit error is twice as large as the probability of a bit error without cancellation. This is due to the fact that the same term, i.e.,

$$\frac{1}{n} \sum_{i=1}^{n} A_{1i} A_{2i}, \tag{10}$$

is used in estimating both b_{10} and b_{20}. If the absolute error $|\hat{b}_{10} - b_{10}|$ is large, then the absolute error $|\hat{b}_{20} - b_{20}|$ is also large (they are both equal to the absolute value of the expression (10)), and interference cancellation reinforces the probability of a bit error.

For $k \geq 3$, which we assume from now on, interference cancellation is superior. Observe from (6) that

$$\mathbb{P}(Z_1^{(1)} \leq 0) = \mathbb{P}\left(\sum_{j=2}^{k} \sum_{i=1}^{n} A_{1i} A_{ji} \geq n \right),$$

which by Lemma 2.1 is the same as the probability that a sum of $n(k-1)$ independent random variables, each with probability $\frac{1}{2}$ on $+1$ and on -1, is equal to or exceeds n. The large deviation properties are well known and follow from Cramér's theorem (cf. [3]). This behavior will be briefly sketched in section 2 for later use in comparison with the behavior of $\mathbb{P}(Z_1^{(2)} \leq 0)$. In section 2, we also describe the refined asymptotic behavior of

$$\sqrt{n}e^{nI_k}\mathbb{P}(Z_1^{(1)} \leq 0),$$

where I_k is given in (13). We note that this behavior depends on the parity of n.

The results with interference cancellation appear in the sections 3 and 4. In section 3, we prove the rate result:

$$\lim_{n\to\infty} \frac{1}{n} \log \mathbb{P}(Z_1^{(2)} \leq 0) = -J_k,$$

where the value of J_k is the minimum of the variational problem described in Theorem 3.2, which can be evaluated numerically. Here we also show that for $k \geq 3$,

$$J_k > I_k,$$

so that the probability of a bit error with interference cancellation is indeed of smaller order than that without cancellation.

Concerning the second order asymptotics of $\mathbb{P}(Z_1^{(2)} \leq 0)$, we could obtain a complete result only for $k = 3$. This result is Theorem 4.1. The paper closes with a section on conclusions and open problems. In an appendix we prove three technical results.

2. Bit error probabilities without cancellation. In formula (13) below we give the rate of $\mathbb{P}(Z_1^{(1)} \leq 0)$, and in Theorem 2.2 we present the second order (Bahadur–Rao) asymptotics for the quoted probability.

Let

$$\mathcal{X} = \{-1, +1\}^{k-1}. \tag{11}$$

Furthermore, we define the random vectors $X_j \in \mathcal{X}$:

$$X_j = A_{1j}(A_{2j}, A_{3j}, \ldots, A_{kj})^T, \qquad 1 \leq j \leq n, \tag{12}$$

where the distribution of A_{ij}, for $1 \leq i \leq k$, $1 \leq j \leq n$, is defined in (5). The following lemma is straightforward and the proof is omitted.

LEMMA 2.1. *The vectors $X_1, \ldots, X_n$ are i.i.d. Their common distribution μ_0 is the uniform distribution on the finite set $\mathcal{X}$, i.e.,*

$$\mu_0(a) = \mathbb{P}(X_1 = a) = \frac{1}{2^{k-1}} \quad \forall a \in \mathcal{X}.$$

Throughout this paper, $M(\mathcal{X})$ will denote the set of all probability measures (laws) on $\mathcal{X}$. Combining (6) and (12) gives

$$Z_1^{(1)} = 1 + \sum_{j=1}^{k-1} \frac{1}{n} \sum_{i=1}^{n} (X_i)_j.$$

It is clear that $n(Z_1^{(1)} - 1)$ is the sum of $(k-1)n$ i.i.d. random variables that assume values $+1$ or -1 with probability $1/2$. The rate of $\mathbb{P}(Z_1^{(1)} \le 0)$ follows from Cramér's theorem [3]. For $k \ge 3$,

$$\lim_{n\to\infty} \frac{1}{n} \log \mathbb{P}(Z_1^{(1)} \le 0) = -I_k, \tag{13}$$

where

$$I_k = \frac{k-2}{2} \log\left(\frac{k-2}{k-1}\right) + \frac{k}{2} \log\left(\frac{k}{k-1}\right).$$

The next step is to consider the second order asymptotics of $\mathbb{P}(Z_1^{(1)} \le 0)$. Since we deal with lattice random variables, we have, according to Theorem 1 of [1], the following.

THEOREM 2.2. *For $k \ge 3$,*

$$\mathbb{P}(Z_1^{(1)} \le 0) = \frac{A_n}{\sqrt{n}} e^{-nI_k}(1 + o(1)),$$

where

$$A_n = \sqrt{\frac{k-1}{2\pi}} \left(\frac{k-2}{k}\right)^{\lfloor \frac{nk+1}{2} \rfloor - \frac{nk+1}{2}}.$$

3. Exponential rate with interference cancellation. The main result of this section is Theorem 3.2, which specifies the exponential rate for $\mathbb{P}(Z_1^{(2)} \le 0)$ as $n \to \infty$, for arbitrary values of $k \ge 3$. Furthermore, we present a theorem which states that the exponential rate for $s = 2$ is strictly larger than the exponential rate for $s = 1$. We close the section with uniqueness of the variational problem for $k = 3$.

The empirical measure (law) L_n^X is defined by

$$L_n^X(a) = \frac{1}{n} \sum_{i=1}^{n} \mathbb{I}_{\{a\}}(X_i), \quad a \in \mathcal{X}, \tag{14}$$

i.e., $L_n^X(a)$ is the fraction of occurrences of a in the sequence $X_1, \ldots, X_n$. Let $\mathcal{L}_n$ denote the set of all empirical measures. Thus, with $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$,

$$\mathcal{L}_n = \{\rho \in M(\mathcal{X}) : n\rho \in \mathbb{N}_0^{|\mathcal{X}|}\}.$$

Note that the empirical measure L_n^X is a *random* element of the set $\mathcal{L}_n$. We often abbreviate $L_n^X(a)$ by $(L_n)_a$.

We define

$$I_k(\rho) = (k-1)\log 2 + \sum_{a\in\mathcal{X}} \rho_a \log \rho_a. \tag{15}$$

The function $\rho \mapsto I_k(\rho)$ is called the *rate function*. It is nonnegative and convex; cf. [3]. Furthermore, $I_k(\mu_0) = 0$.

LEMMA 3.1. *For $k \ge 3$,*

$$Z_1^{(2)} = F_k(L_n),$$

where for $\rho \in M(\mathcal{X})$

$$F_k(\rho) = 1 - \sum_{i=2}^{k} \sum_{\substack{j=1 \\ j \neq i}}^{k} \left(\sum_{a \in \mathcal{X}} a_{i-1} \rho_a \right) \left(\sum_{a \in \mathcal{X}} a_{i-1} a_{j-1} \rho_a \right), \tag{16}$$

where $a_0 = 1$ *for all* $a \in \mathcal{X}$.

Proof. According to the definitions (6) and (9),

$$A_{il} A_{jl} = A_{1l} A_{il} A_{1l} A_{jl} = (X_l)_{i-1} (X_l)_{j-1}, \quad i, j \geq 1,\ 1 \leq l \leq n,$$

where by convention $(X_l)_0 = 1$. Switching over to empirical measures,

$$\frac{1}{n} \sum_{l=1}^{n} (X_l)_i (X_l)_j = \sum_{a \in \mathcal{X}} a_i a_j (L_n)_a$$

yields the lemma. □

Remark. For $k = 3$, we write $\rho_+ = \rho(+1, +1)$, $\rho_\pm = \rho(+1, -1)$, $\rho_\mp = \rho(-1, +1)$, and $\rho_- = \rho(-1, -1)$. Then it is straightforward that for $\rho \in M(\mathcal{X})$ we have

$$F_3(\rho) = 1 - 2(\rho_+ - \rho_-)(2\rho_+ - \rho_\pm - \rho_\mp) - 2(\rho_\pm - \rho_\mp)^2.$$

For $k \geq 3$, we obtain the following from Sanov's theorem (cf. [3]) and the contraction principle.

THEOREM 3.2. *For* $k \geq 3$,

$$\lim_{n \to \infty} \frac{1}{n} \log \mathbb{P}(Z_1^{(2)} \leq 0) = -J_k,$$

where

$$J_k = \inf_{\rho \in M(\mathcal{X}):\, F_k(\rho) = 0} I_k(\rho).$$

We now prove that, for $k \geq 3$, interference cancellation reduces the bit error rate if n is significantly large, i.e., $J_k > I_k$.

THEOREM 3.3. *For* $k \geq 3$,

$$J_k > I_k.$$

Proof. We will show that $J_k \geq I_k$ here. The proof that $J_k > I_k$ is similar but is more involved and is therefore deferred to Appendix A.

$$\begin{aligned}
\mathbb{P}(Z_1^{(2)} \leq 0) &= \mathbb{P}\left(\bigcap_{j=2}^{k} \left\{ Z_j^{(1)} \in [0, 2] \right\} \bigcap \left\{ Z_1^{(2)} \leq 0 \right\} \right) \\
&\quad + \mathbb{P}\left(\bigcup_{j=2}^{k} \left\{ Z_j^{(1)} \notin [0, 2] \right\} \bigcap \left\{ Z_1^{(2)} \leq 0 \right\} \right) \\
&\leq \mathbb{P}\left(\bigcap_{j=2}^{k} \left\{ Z_j^{(1)} \in [0, 2] \right\} \right\} \bigcap \left\{ Z_1^{(2)} \leq 0 \right\} \right) + 2(k-1) \mathbb{P}(Z_1^{(1)} \leq 0).
\end{aligned}$$

In the last step we used Boole's inequality and the fact that $\mathbb{P}(Z_1^{(1)} \notin [0,2]) \leq 2\mathbb{P}(Z_1^{(1)} \leq 0)$.

Furthermore,

$$\begin{aligned}
&\mathbb{P}\left(\bigcap_{j=2}^{k}\left\{Z_j^{(1)} \in [0,2]\right\}\bigcap\left\{Z_1^{(2)} \leq 0\right\}\right)\\
&= \mathbb{P}\left(\bigcap_{j=2}^{k}\left\{Z_j^{(1)} \in [0,2]\right\}\bigcap\left\{1+\frac{1}{n}\sum_{j=2}^{k}\sum_{i=1}^{n}A_{1i}A_{ji}(1-Z_j^{(1)}) \leq 0\right\}\right)\\
&\leq \mathbb{P}\left(1-\frac{1}{n}\sum_{j=2}^{k}\left|\sum_{i=1}^{n}A_{1i}A_{ji}\right| \leq 0\right) \leq 2^{k-1}\mathbb{P}\left(1+\frac{1}{n}\sum_{j=2}^{k}\sum_{i=1}^{n}A_{1i}A_{ji} \leq 0\right)\\
&= 2^{k-1}\mathbb{P}(Z_1^{(1)} \leq 0).
\end{aligned}$$

Hence, $\mathbb{P}(Z_1^{(2)} \leq 0) \leq (2^{k-1}+2(k-1))\mathbb{P}(Z_1^{(1)} \leq 0)$. This proves that $J_k \geq I_k$, since k is fixed. □

For $k=3$, we can prove that the minimizer in Theorem 3.2 is unique and symmetric in the second and third coordinate. This theorem is important for the calculation of the second order asymptotics in the next section. Unfortunately, the proof is rather technical and therefore it is deferred to Appendix B.

THEOREM 3.4. *For $k=3$, the minimizer ν of the variational problem of Theorem 3.2 is unique. Furthermore, $\nu_+ = \nu_\mp$.*

4. Bahadur–Rao asymptotics. The second order asymptotics of $\mathbb{P}(Z_1^{(2)} \leq 0)$ depend on the uniqueness of the minimizer and on irrationality of the partial derivatives of the rate function. For $k=3$, our results are complete and formulated in Theorem 4.1.

THEOREM 4.1. *For $k=3$,*

$$\lim_{n\to\infty}\sqrt{n}e^{nJ_3}\mathbb{P}(Z_1^{(2)} \leq 0) = A,$$

where $A \approx 0.5946$ (see (23)), and where $J_3 \approx 0.3094$ is defined in Theorem 3.2.

Proof. The proof will be divided into 5 steps. We need some additional notation. Denote by $+$ the vector of $\mathcal{X}$ consisting of only $+1$'s, and by $-$ the vector consisting of only -1's.

Step 1: Multinomial probabilities. Using Stirling's formula we approximate the multinomial distribution of L_n by

$$\mathbb{P}(L_n = \rho) = \frac{(2\pi n)^{-3/2}}{\prod_{a\in\mathcal{X}}\rho_a^{1/2}}e^{-nI_3(\rho)}\left(1+\mathcal{O}\left(\left[n\min_{a\in\mathcal{X}}\rho_a\right]^{-1}\right)\right),$$

where

$$I_3(\rho) = \log 4 + \sum_{a\in\mathcal{X}}\rho_a\log\rho_a.$$

As before, we denote by ν the unique minimizer of the variational problem. Then for every $\epsilon > 0$ there exists a $\delta > 0$ such that for n large enough

$$\mathbb{P}(F_3(L_n) \leq 0, ||L_n - \nu||_1 > \epsilon) \leq e^{-n[I_3(\nu)+\delta]},$$

where $||\cdot||_1$ is the ℓ_1-norm. Hence, since ν is strictly positive (see Appendix B),

$$\mathbb{P}(F_3(L_n) \le 0) = \frac{(2\pi n)^{-3/2}}{\prod_{a\in\mathcal{X}} {\nu_a}^{1/2}} \sum_{\rho: F_3(\rho)\le 0} e^{-nI_3(\rho)}(1+o(1)).$$

Step 2*: The sum over* ρ_+. To obtain compact notation, we define $\tilde{\rho} = (\rho_\pm, \rho_\mp)^T$ and

$$r(\tilde{\rho}) = \frac{1}{4} + \frac{1}{4}\sqrt{(4\tilde{\rho}_1 - 1)(4\tilde{\rho}_2 - 1) + 2}, \tag{17}$$
$$J(\tilde{\rho}) = I_3(r(\tilde{\rho}), \tilde{\rho}_1, \tilde{\rho}_2, 1 - r(\tilde{\rho}) - \tilde{\rho}_1 - \tilde{\rho}_2).$$

Write $\rho_- = 1 - \sum_{a\in\mathcal{X}\setminus -} \rho_a$, fix $\rho_\pm$ and $\rho_\mp$, and invoke the notation $\tilde{\rho}$. For $||\rho - \nu||_1 < \epsilon$, the condition $F_3(\rho) \le 0$ is now equivalent to $\rho_+ \ge r(\tilde{\rho})$.

If we make a Taylor expansion in $\rho_+ = r(\tilde{\rho})$, we obtain

$$I_3(\rho) = J(\tilde{\rho}) + (\rho_+ - r(\tilde{\rho}))\frac{\partial}{\partial \rho_+} I_3(\rho)\big|_{\rho_+ = \xi},$$

where ξ is between $r(\tilde{\rho})$ and ρ_+. Since $||\rho - \nu||_1 < \epsilon$, we have that $\xi - r(\tilde{\rho}) = \mathcal{O}(\epsilon)$. Define

$$\alpha_{\tilde{\rho}} = e^{-\frac{\partial}{\partial \rho_+} I_3(\rho)|_{\rho_+ = r(\tilde{\rho})}}.$$

Then

$$\sum_{\rho:\rho_+\ge r(\tilde{\rho})} e^{-nI_3(\rho)} = \sum_{\tilde{\rho}} e^{-nJ(\tilde{\rho})} \sum_{\rho: n\rho_+ \ge nr(\tilde{\rho})} \alpha_{\tilde{\rho}}^{n(\rho_+ - r(\tilde{\rho}))}(1+o(1)).$$

Furthermore, since $||\rho - \nu||_1 < \epsilon$, we have that $\alpha_{\tilde{\rho}} = \alpha_{\tilde{\nu}} + \mathcal{O}(\epsilon) = \frac{\nu_-}{\nu_+} + \mathcal{O}(\epsilon) < 1$ (see Appendix B). This proves that with $\alpha = \alpha_{\tilde{\nu}}$,

$$\sum_{\rho:\rho_+\ge r(\tilde{\rho})} e^{-nI_3(\rho)} = \sum_{\tilde{\rho}} e^{-nJ(\tilde{\rho})} \frac{\alpha^{\lceil nr(\tilde{\rho})\rceil - nr(\tilde{\rho})}}{1-\alpha}(1+o(1)),$$

where $\lceil x \rceil$ is the smallest integer larger than or equal to x. Hence, using that $I_3(\nu) = J_3$, we arrive at

$$\sqrt{n}e^{nJ_3}\mathbb{P}(F_3(L_n) \le 0) \tag{18}$$
$$= \frac{(2\pi)^{-3/2}}{\prod_{a\in\mathcal{X}} {\nu_a}^{1/2}} \frac{1}{n} \sum_{\tilde{\rho}} \frac{\alpha^{\lceil nr(\tilde{\rho})\rceil - nr(\tilde{\rho})}}{1-\alpha} e^{-n(J(\tilde{\rho}) - J(\tilde{\nu}))}(1+o(1)).$$

Step 3*: Taylor expansion of the exponential rate.* Since $F_3(\nu) = 0$, $\tilde{\nu}$ minimizes $\tilde{\rho} \mapsto J(\tilde{\rho})$. Therefore, we have that $\nabla J(\tilde{\nu}) = 0$, and Taylor expansion of J leads to

$$J(\tilde{\rho}) - J(\tilde{\nu}) = (\tilde{\rho} - \tilde{\nu})^T \nabla^2 J(\tau)(\tilde{\rho} - \tilde{\nu})/2,$$

where τ is some interpolation point between $\tilde{\rho}$ and $\tilde{\nu}$. Since we can restrict ourselves to ρ's with $||\rho - \nu||_1 < \epsilon$, we also have that $\nabla^2 J(\tau) = M + \mathcal{O}(\epsilon)$, where $M = \nabla^2 J(\tilde{\nu})$. This gives

$$\sqrt{n}e^{nJ_3}\mathbb{P}(F_3(L_n) \le 0) \tag{19}$$
$$= \frac{(2\pi)^{-3/2}}{\prod_{a\in\mathcal{X}} {\nu_a}^{1/2}} \frac{1}{n} \sum_{\tilde{\rho}} \frac{\alpha^{\lceil nr(\tilde{\rho})\rceil - nr(\tilde{\rho})}}{1-\alpha} e^{-n(\tilde{\rho} - \tilde{\nu})^T M(\tilde{\rho} - \tilde{\nu})/2}(1+o(1)).$$

Step 4: Strategy of the proof. It is time to reveal how we intend to prove the theorem. Introduce a sequence of distribution functions G_n on $[0,1]$,

$$G_n(x) = \frac{1}{Z_n} \sum_{\tilde{\rho}} \mathbb{I}_{\{[0,x]\}}(\lceil nr(\tilde{\rho}) \rceil - nr(\tilde{\rho})) e^{-n(\tilde{\rho}-\tilde{\nu})^T M(\tilde{\rho}-\tilde{\nu})/2},$$

where Z_n is defined by $G_n(1) = 1$:

$$Z_n = \sum_{\tilde{\rho}} e^{-n(\tilde{\rho}-\tilde{\nu})^T M(\tilde{\rho}-\tilde{\nu})/2}. \tag{20}$$

Observe that

$$\frac{1}{n} \sum_{\tilde{\rho}} \alpha^{\lceil nr(\tilde{\rho}) \rceil - nr(\tilde{\rho})} e^{-n(\tilde{\rho}-\tilde{\nu})^T M(\tilde{\rho}-\tilde{\nu})/2} = \frac{Z_n}{n} \int_0^1 \alpha^x \, dG_n(x),$$

and hence, according to (19),

$$\sqrt{n} e^{nJ_3} \mathbb{P}(F_3(L_n) \le 0) = \frac{(2\pi)^{-3/2}}{(1-\alpha) \prod \nu_a^{1/2}} \frac{Z_n}{n} \int_0^1 \alpha^x \, dG_n(x)(1 + o(1)). \tag{21}$$

We will show that for $m = 1, 2, \ldots$

$$\lim_{n\to\infty} \int_0^1 e^{2\pi i m x} \, dG_n(x) = \int_0^1 e^{2\pi i m x} \, dx = 0. \tag{22}$$

By the selection principle [4, p. 267], each subsequence $\{n'\}$ has a further subsequence $\{n''\}$ such that $G_{n''}$ converges weakly to a proper distribution function G on $[0,1]$. This implies, in particular, that every continuous function u on $[0,1]$ which is periodic ($u(0) = u(1)$) satisfies

$$\lim_{n''\to\infty} \int_0^1 u(x) \, dG_{n''}(x) = \int_0^1 u(x) \, dG(x).$$

In turn, (22) will then imply that the Fourier coefficients $\int_0^1 e^{2\pi i m x} \, dG(x)$ are those of the *uniform* distribution, and this pinpoints the limit G, so that in fact each convergent subsequence has the same weak limit, which is the uniform distribution function, if (22) holds. This implies that the sequence G_n converges weakly to the uniform distribution on $[0,1]$.

Since $u(x) = \alpha^x$, $x \in [0,1]$, is continuous, we conclude that

$$\lim_{n\to\infty} \int_0^1 \alpha^x \, dG_n(x) = \int_0^1 \alpha^x \, dx = \frac{1-\alpha}{\log(1/\alpha)},$$

and hence this implies that for $n \to \infty$

$$\sqrt{n} e^{nJ_3} \mathbb{P}(F_3(L_n) \le 0) \to A = |\log \alpha|^{-1} \left(2\pi |M| \prod_{a \in \mathcal{X}} \nu_a \right)^{-1/2}, \tag{23}$$

because obviously

$$\frac{Z_n}{n} \to \int \int e^{-(s,t)M(s,t)^T/2} \, ds dt = \frac{2\pi}{\sqrt{|M|}}.$$

The determinant $|M|$ is strictly positive by Lemma B.6. In the final step we will show (22).

Step 5*: The Fourier coefficients.* The last step, in which we deal with the Fourier coefficients for $m > 0$, is the most delicate one. Fix $m > 0$. By a Taylor expansion of $r(\tilde{\rho})$ around $\tilde{\rho} = \tilde{\nu}$, we get that

$$\begin{aligned} r(\tilde{\rho}) &= r(\tilde{\nu}) + (\tilde{\rho} - \tilde{\nu})^T \nabla r(\tilde{\nu}) + (\tilde{\rho} - \tilde{\nu})^T \nabla^2 r(\tilde{\tau})(\tilde{\rho} - \tilde{\nu})/2 \\ &= \nu_+ + (\tilde{\rho}_1 - \tilde{\nu}_1 + \tilde{\rho}_2 - \tilde{\nu}_2) r'(\tilde{\nu}) + (\tilde{\rho} - \tilde{\nu})^T \nabla^2 r(\tilde{\tau})(\tilde{\rho} - \tilde{\nu})/2, \end{aligned}$$

where $\tilde{\tau}$ is between $\tilde{\rho}$ and $\tilde{\nu}$ and where $r'(\tilde{\nu})$ is defined as

$$\frac{\partial r}{\partial \tilde{\rho}_1}(\tilde{\nu}) = \frac{\partial r}{\partial \tilde{\rho}_2}(\tilde{\nu}),$$

which are equal by symmetry of the minimizer. Hence, with $j = (n\tilde{\rho}_1 - \lceil n\tilde{\nu}_1 \rceil, n\tilde{\rho}_2 - \lceil n\tilde{\nu}_2 \rceil)^T \in \mathbb{Z}^2$ and using that $\tilde{\nu}_1 = \tilde{\nu}_2$, we can write

$$\begin{aligned} nr(\tilde{\rho}) &= n\nu_+ + r'(\tilde{\nu})(j_1 + j_2) \\ &\quad + 2r'(\tilde{\nu})(\lceil n\tilde{\nu}_1 \rceil - n\tilde{\nu}_1) + \frac{j^T \nabla^2 r(\tilde{\nu}) j}{(2n)} + \mathcal{O}\left(\frac{\|j\|^3}{n^2} \right). \end{aligned} \tag{24}$$

Using (24) gives, since M is strictly positive definite,

$$\begin{aligned} \sum_{\tilde{\rho}} e^{-2\pi i m n r(\tilde{\rho})} e^{-n(\tilde{\rho}-\tilde{\nu})^T M(\tilde{\rho}-\tilde{\nu})/2} &= e^{-2\pi i m [n\nu_+ + 2r'(\tilde{\nu})(\lceil n\tilde{\nu}_1 \rceil - n\tilde{\nu}_1)]} \\ &\quad \times \sum_{j \in \mathbb{Z}^2} e^{-2\pi i m (j_1+j_2) r'(\tilde{\nu})} e^{-j^T (M + 2\pi i m \nabla^2 r(\tilde{\nu})) j/(2n)} (1 + o(1)). \end{aligned} \tag{25}$$

Because $mr'(\tilde{\nu})$ is not an integer (which we know from Lemma C.1 of Appendix C), we have

$$e^{-2\pi i r'(\tilde{\nu}) m \ell} = c_m \int_\ell^{\ell+1} e^{-2\pi i r'(\tilde{\nu}) m x} dx \qquad \text{with} \qquad c_m = \frac{2\pi i m r'(\tilde{\nu})}{1 - e^{-2\pi i m r'(\tilde{\nu})}}.$$

Use this result and the fact that for $\|x - j\|_1 \le 2$

$$e^{-j^T (M + 2\pi i m \nabla^2 r(\tilde{\nu})) j/(2n)} = e^{-x^T (M + 2\pi i m \nabla^2 r(\tilde{\nu})) x/(2n)} \left(1 + \mathcal{O}\left(\frac{\|x\|}{n} \right) \right)$$

to obtain

$$\begin{aligned} &\frac{1}{n} \sum_{j \in \mathbb{Z}^2} e^{-2\pi i m (j_1+j_2) r'(\tilde{\nu})} e^{-j'(M + 2\pi i m \nabla^2 r(\tilde{\nu})) j/(2n)} \\ &= c_m^2 \frac{1}{n} \int_{\mathbb{R}^2} e^{-2\pi i m (x_1+x_2) r'(\tilde{\nu})} e^{-x^T (M + 2\pi i m \nabla^2 r(\tilde{\nu})) x/(2n)} dx (1 + o(1)) \\ &= c_m^2 \int_{\mathbb{R}^2} e^{-2\pi i m \sqrt{n} (x_1+x_2) r'(\tilde{\nu})} e^{-x^T (M + 2\pi i m \nabla^2 r(\tilde{\nu})) x/2} dx (1 + o(1)). \end{aligned}$$

The resulting integral equals zero by the Riemann–Lebesgue lemma, which shows that for $m > 0$

$$\lim_{n \to \infty} \int_0^1 e^{2\pi i m x} \, dG_n(x) = \lim_{n \to \infty} \frac{1}{Z_n} \sum_{\tilde{\rho}} e^{-2\pi i m n r(\tilde{\rho})} e^{-n(\tilde{\rho}-\tilde{\nu})^T M(\tilde{\rho}-\tilde{\nu})/2} = 0,$$

because $Z_n/n \to \frac{2\pi}{\sqrt{|M|}}$. □

5. Discussion. In the preceding sections we have used large deviation theory to analyze the probability of a bit error in CDMA, with and without one stage of interference cancellation. We have been able to prove that the rate for $s = 2$, i.e., with interference cancellation, is larger than for $s = 1$, the case without cancellation, implying that the bit error probability is significantly smaller through interference cancellation. Below we display a table with the numerical values of the exponential rate for $s = 1, s = 2$, and $k = 3, 4, \ldots, 10$. Note that both rates are monotone in k. This empirical fact is easy to prove.

s	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$	$k=9$	$k=10$
1	0.2616	0.1699	0.1263	0.1007	0.0837	0.0717	0.0627	0.0557
2	0.3094	0.2398	0.2058	0.1845	0.1696	0.1582	0.1492	0.1418

An even sharper result has been obtained for $k = 3$. We have been able to prove that the minimizer of the variational problem is unique, which we have used to prove the second order asymptotics of section 4.

In Figure 1 we display, for $k = 3$ and for the processing gain n running from 1 to 160, the large deviation approximation without interference cancellation, $s = 1$, the large deviation approximation after interference cancellation, $s = 2$ (almost a straight line), and the absolute difference of the latter approximation with the exact values. The exact values of the error probabilities have been obtained from extensive numerical calculations.

The analysis in this paper answers various questions; nevertheless, many other questions remain unanswered. We summarize the most important ones:

1. Is the minimizer for $k \geq 4$ unique? We think that the answer to this question is affirmative. This problem becomes more difficult with increasing k.

2. Can we describe the second order asymptotics for $k \geq 4$? The answer to this question is tied up with an affirmative answer to the first question and the question of irrationality of expressions that describe the boundaries of regions to which the empirical measure is constrained (see the proof of Theorem 4.1).

3. What happens when one applies *multi*stage interference cancellation? In the paper, we defined $Z_1^{(s)}$ for $s = 1, 2$. We can recursively define

$$Z_m^{(s+1)} = 1 + \sum_{\substack{j=1 \\ j \neq m}}^{k} \left(\frac{1}{n} \sum_{i=1}^{n} A_{ji} A_{mi} \left[1 - Z_j^{(s)} \right] \right), \quad s = 2, 3, \ldots.$$

The probabilities $\mathbb{P}(Z_1^{(s+1)} \leq 0)$, for $s \geq 1$, correspond with bit error probabilities after s stages of interference cancellation. It is interesting to see how these error probabilities behave for increasing s, $s \geq 3$.

4. In *hard decision* interference cancellation, one studies

$$1 + \sum_{j=2}^{k} \left(\frac{1}{n} \sum_{i=1}^{n} A_{ji} A_{1i} \right) \left[1 - \operatorname{sign}(Z_j^{(1)}) \right],$$

instead of the statistic $Z_1^{(2)}$ (compare (8)). Results for this case will appear in [5]. Another practical problem is that of a noisy channel, meaning that the received signal is corrupted by Gaussian noise.

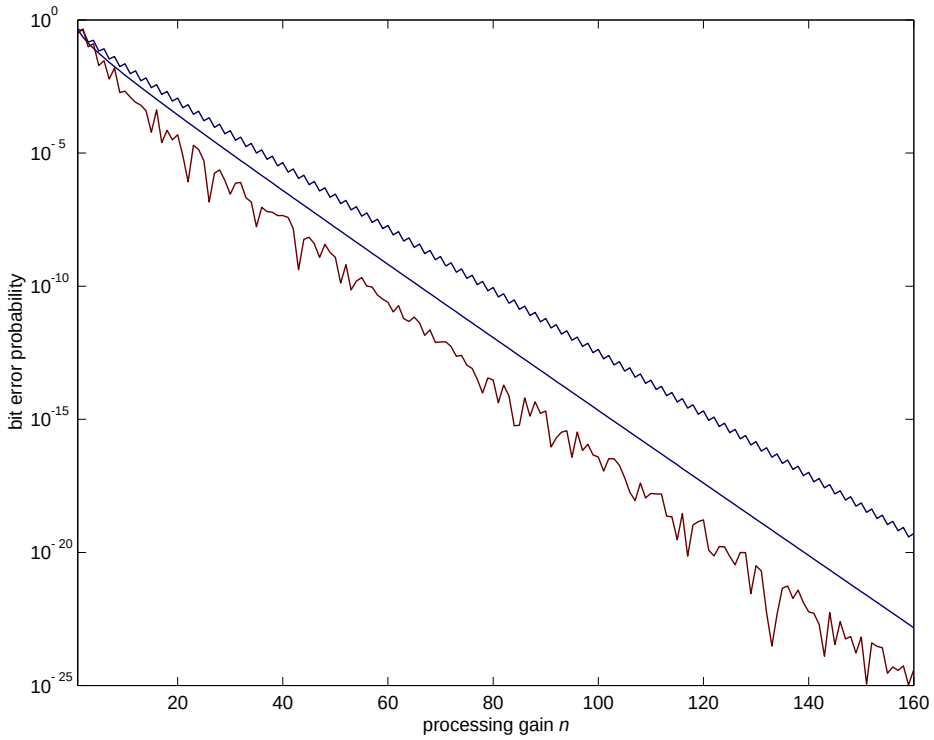

FIG. 1. *L.D. approximations for $k = 3$. The top curve is $s = 1$; the center curve is $s = 2$, the curve of Theorem 4.1; and the bottom curve is the absolute error between the exact value and the approximation for $s = 2$.*

Appendix. The appendix is split into three parts A, B, and C. In A we will present the proof of Theorem 3.3, that is, the proof that $J_k > I_k$. In B we will give the proof of Theorem 3.4, which states that for $k = 3$ the minimizer is unique and symmetric. Finally, in C we will show that for $k = 3$ the derivative $r'(\tilde{\nu})$ is irrational.

Appendix A. Proof of Theorem 3.3. For the proof of this theorem the following lemma is helpful. The lemma shows that the exponential rate of the rare event

$$\{Z_1^{(1)} \le 0, Z_2^{(1)} \notin [7/10, 1)\}$$

is strictly larger than I_k for $k \ge 3$.

LEMMA A.1. *For $k \ge 3$*

$$\lim_{n\to\infty} \frac{1}{n} \log \mathbb{P}(Z_1^{(1)} \le 0, Z_2^{(1)} \notin [7/10, 1)) < \lim_{n\to\infty} \frac{1}{n} \log \mathbb{P}(Z_1^{(1)} \le 0) = -I_k.$$

Proof. The rate of a rare event can be obtained as the infimum of the rate function $\rho \mapsto I_k(\rho)$, where $\rho \in M(\mathcal{X})$ is restricted to some specified region (compare section 3). More precisely, we have that

$$Z_1^{(1)} = E_k(L_n), \quad Z_2^{(1)} = D_k(L_n),$$

where, for $\rho \in M(\mathcal{X})$,

$$E_k(\rho) = 1 + \sum_{j=2}^{k} \sum_{a \in \mathcal{X}} a_{j-1} \rho_a, \qquad D_k(\rho) = 1 + \sum_{a \in \mathcal{X}} a_1 \rho_a + \sum_{j=3}^{k} \sum_{a \in \mathcal{X}} a_1 a_{j-1} \rho_a.$$

Let μ be the (unique) minimizer of $\rho \mapsto I_k(\rho)$, subject to $\rho \in M(\mathcal{X})$ and $E_k(\rho) \le 0$, i.e., $I_k(\mu) = I_k$, the rate without interference cancellation. It is not hard to verify that μ is the product measure:

$$\mu_a = \otimes_{j=1}^{k-1} \left[\frac{k}{2(k-1)} \delta_{-1}(a_j) + \frac{k-2}{2(k-1)} \delta_{+1}(a_j) \right], \qquad a \in \mathcal{X}.$$

Hence

$$\begin{aligned} D_k(\mu) &= 1 - \frac{k}{2(k-1)} + \frac{k-2}{2(k-1)} + (k-2) \left(-\frac{k}{2(k-1)} + \frac{k-2}{2(k-1)} \right)^2 \\ &= 1 - \frac{1}{k-1} + \frac{k-2}{(k-1)^2} = 1 - \frac{1}{(k-1)^2}. \end{aligned}$$

This implies that $D_k(\mu) \in [3/4, 1)$ for $k \ge 3$. Since $D_k(L_n) = Z_2^{(1)}$ and $7/10 < 3/4$, the conclusion of the lemma follows. □

We proceed with the proof of Theorem 3.3. For $\varepsilon > 0$ and $0 < \delta < 1$, we define

$$\begin{aligned} S &= \text{card}\{2 \le j \le k : Z_j^{(1)} \in (-\infty, -\varepsilon) \cup (2 + \varepsilon, \infty)\}, \\ T &= \text{card}\{2 \le j \le k : Z_j^{(1)} \in [\delta, 2 - \delta]\}, \\ R &= \text{card}\{2 \le j \le k : Z_j^{(1)} \in [-\varepsilon, \delta) \cup (2 - \delta, 2 + \varepsilon]\}. \end{aligned}$$

Then

$$\begin{aligned} \mathbb{P}(Z_1^{(2)} \le 0) &= \mathbb{P}(Z_1^{(2)} \le 0, S \ge 1) + \mathbb{P}(Z_1^{(2)} \le 0, T = k-1) \\ &\quad + \mathbb{P}(Z_1^{(2)} \le 0, R = 1, T = k-2) + \sum_{l=2}^{k-1} \mathbb{P}(Z_1^{(2)} \le 0, R = l, T = k-l-1), \end{aligned} \tag{26}$$

since $S + T + R = k - 1$. We will show that for some fixed $\varepsilon > 0$ and for some fixed δ, $0 < \delta < 1$, each of the four terms on the right-hand side of (26) has exponential rate strictly larger than I_k.

We bound the first term in (26) as

$$\mathbb{P}(Z_1^{(2)} \le 0, S \ge 1) \le 2(k-1) \mathbb{P}(Z_1^{(1)} < -\varepsilon), \tag{27}$$

which has rate larger than I_k, for each $\varepsilon > 0$.

For the second term in (26), we obtain

$$\begin{aligned} &\mathbb{P}(Z_1^{(2)} \le 0, T = k-1) \\ &\quad = \mathbb{P}\left(\bigcap_{j=2}^{k} \left\{ Z_j^{(1)} \in [\delta, 2-\delta] \right\} \bigcap \left\{ 1 + \frac{1}{n} \sum_{j=2}^{k} \sum_{i=1}^{n} A_{1i} A_{ji} \left(1 - Z_j^{(1)} \right) \le 0 \right\} \right) \\ &\quad \le \mathbb{P}\left(1 - (1-\delta) \frac{1}{n} \sum_{j=2}^{k} \left| \sum_{i=1}^{n} A_{1i} A_{ji} \right| \le 0 \right) \end{aligned} \tag{28}$$

$$\le \mathbb{P}\left(\bigcup_{(\varepsilon_2,\dots,\varepsilon_k)\in\{-1,1\}^{k-1}}\left\{1-(1-\delta)\frac{1}{n}\sum_{j=2}^{k}\varepsilon_j\sum_{i=1}^{n}A_{1i}A_{ji}\le 0\right\}\right)$$

$$\le 2^{k-1}\mathbb{P}\left(\delta+(1-\delta)+(1-\delta)\frac{1}{n}\sum_{j=2}^{k}\sum_{i=1}^{n}A_{1i}A_{ji}\le 0\right)$$

$$= 2^{k-1}\mathbb{P}(Z_1^{(1)}\le -\delta/(1-\delta)),$$

which has rate larger than I_k, because $\delta/(1-\delta)>0$.

For the third term in (26), a similar calculation gives

$$\begin{aligned}(29)\quad &\mathbb{P}(Z_1^{(2)}\le 0, R=1, T=k-2)\\ &\le (k-1)\mathbb{P}\left(\left\{1+\frac{1}{n}\sum_{j=2}^{k}\sum_{i=1}^{n}A_{1i}A_{ji}(1-Z_j^{(1)})\le 0\right\}\right.\\ &\qquad\left.\bigcap\left\{Z_2^{(1)}\in[-\varepsilon,\delta)\cup(2-\delta,2+\varepsilon]\right\}\bigcap_{j=3}^{k}\left\{Z_j^{(1)}\in[\delta,2-\delta]\right\}\right)\\ &\le (k-1)\mathbb{P}\left(1-(1+\varepsilon)\frac{1}{n}\left|\sum_{i=1}^{n}A_{1i}A_{2i}\right|-(1-\delta)\frac{1}{n}\sum_{j=3}^{k}\left|\sum_{i=1}^{n}A_{1i}A_{ji}\right|\le 0\right)\\ &\le (k-1)2^{k-1}\mathbb{P}\left(1+\frac{1}{n}\sum_{j=2}^{k}\sum_{i=1}^{n}A_{1i}A_{ji}\le\frac{-\delta-(\delta+\varepsilon)\frac{1}{n}\sum_{i=1}^{n}A_{1i}A_{2i}}{1-\delta}\right)\\ &\le (k-1)2^{k-1}\left[\mathbb{P}\left(Z_1^{(1)}<\frac{-\delta+\alpha(\delta+\varepsilon)}{1-\delta}\right)+\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^{n}A_{1i}A_{2i}\le-\alpha\right)\right]\end{aligned}$$

by intersecting with $(\sum A_{1i}A_{2i})/n>-\alpha$ and its complement. Take $\alpha=7/10$ and $\varepsilon=\delta/4$. Clearly, the first term of the right-hand side in (29) has rate larger than I_k. The second probability has rate larger than I_k, because the exponential rate satisfies

$$\frac{1+7/10}{2}\log(1+7/10)+\frac{1-7/10}{2}\log(1-7/10)>\frac{3}{2}\log 3-2\log 2=I_3\ge I_k$$

for $k\ge 3$.

Finally,

$$\begin{aligned}&\sum_{l=2}^{k-1}\mathbb{P}(Z_1^{(2)}\le 0, R=l, T=k-l-1)\ \le\ \mathbb{P}(R\ge 2)\\ &\quad\le\binom{k-1}{2}\mathbb{P}\Big(Z_1^{(1)}\in[-\varepsilon,\delta)\cup(2-\delta,2+\varepsilon], Z_2^{(1)}\in[-\varepsilon,\delta)\cup(2-\delta,2+\varepsilon]\Big)\\ &\quad\le(k-1)^2\mathbb{P}(Z_1^{(1)}<\delta, Z_2^{(1)}\notin[7/10,13/10])\\ &\quad\le(k-1)^2\mathbb{P}(Z_1^{(1)}<\delta, Z_2^{(1)}\notin[7/10,1))\end{aligned}$$

by choosing $\delta\le 7/10$. Observe from Lemma A.1 and the continuity of the rate function that for δ small enough

$$\lim_{n\to\infty}\frac{1}{n}\log\mathbb{P}\left(Z_1^{(1)}\le\delta, Z_2^{(1)}\notin[7/10,1)\right)<-I_k.$$

Hence for some $\delta \in (0, 7/10]$ the rate of $\mathbb{P}(R \geq 2)$ is larger than I_k.

Appendix B. Proof of Theorem 3.4. We start with three lemmas concerning unconstrained minima of $I_3(\rho)$, for $\rho = (\rho_+, \rho_\pm, \rho_\mp, \rho_-) \in M(\mathcal{X})$. Denote by

$$e = \rho_\pm + \rho_\mp, \quad e \in [0,1], \qquad d = \rho_\mp - \rho_\pm, \quad d \in [-1,1].$$

LEMMA B.1. *For $|d| \geq d_0 \in (0,1)$,*

$$I_3(\rho) \geq I_3\left(\frac{1-d_0^2}{4}, \frac{(1-d_0)^2}{4}, \frac{(1+d_0)^2}{4}, \frac{1-d_0^2}{4}\right).$$

Proof. Minimize $I_3(\rho)$ over all ρ with $d \geq d_0$ (which suffices by symmetry). The infimum is attained at a ρ for which $d = d_0$. Hence, we have to compute

$$\inf_{\rho_+, \rho_\mp} I_3(\rho_+, \rho_\mp - d_0, \rho_\mp, 1 - \rho_+ - 2\rho_\mp + d_0).$$

Setting the partial derivatives with respect to ρ_+ and $\rho_\mp$ equal to zero, we obtain

$$\begin{aligned} &\log \rho_+ - \log(1 - \rho_+ - 2\rho_\mp + d_0) = 0, \\ &\log \rho_\mp + \log(\rho_\mp - d_0) - 2\log(1 - \rho_+ - 2\rho_\mp + d_0) = 0. \end{aligned}$$

Solving for ρ_+ and $\rho_\mp$ gives $\rho_+ = \frac{1-d_0^2}{4}$ and $\rho_\mp = \frac{(1+d_0)^2}{4}$. ∎

LEMMA B.2. *For $|d| \geq d_0 \in (0,1)$ and $\rho_+ \geq m \in ((1-d_0^2)/4, 1-d_0)$,*

$$I_3(\rho) \geq I_3\left(m, D - d_0/2, D + d_0/2, 1 - m - 2D\right),$$

where

$$D = \frac{2(1-m)}{3} - \frac{1}{6}\sqrt{4(1-m)^2 - 3d_0^2}.$$

Proof. The approach is similar to that of the above proof. Minimize $I_3(\rho)$ over all ρ with $d \geq d_0$ and $\rho_+ \geq m$. Since $m \in ((1-d_0^2)/4, 1-d_0)$, the infimum is attained at a ρ for which $d = d_0$ and $\rho_+ = m$. Hence, we have to compute

$$\inf_{\rho_\mp} I_3(m, \rho_\mp - d_0, \rho_\mp, 1 - m - 2\rho_\mp + d_0).$$

Setting the derivative with respect to $\rho_\mp$ equal to zero, we obtain

$$\log \rho_\mp + \log(\rho_\mp - d_0) - 2\log(1 - m - 2\rho_\mp + d_0) = 0.$$

Solving for $\rho_\mp$ gives $\rho_\mp = \frac{2(1-m)}{3} \pm \frac{1}{6}\sqrt{4(1-m)^2 - 3d_0^2} + d_0/2$. For the minus root, $\rho_\mp - d_0$ is negative, and hence only the plus root remains. ∎

LEMMA B.3. *For $|d| \geq d_0 \in (0,1)$ and $\rho_+ \leq m \leq (1-d_0^2)/4$,*

$$I_3(\rho) \geq I_3\left(m, D - d_0/2, D + d_0/2, 1 - m - 2D\right).$$

Proof. Minimize $I_3(\rho)$ over all ρ with $d \geq d_0$ and $\rho_+ \leq m$. Since $m \leq \min((1-d_0^2)/4, 1-d_0)$, the infimum is attained at a ρ for which $d = d_0$ and $\rho_+ = m$. This gives precisely the same minimization problem as in the proof of Lemma B.2. ∎

Besides these lemmas we use the following (trivial) inequality for $x, y \in \mathbb{R}$:

$$-4d^2 \le (4\rho_\pm - 1)(4\rho_\mp - 1) \le (2e-1)^2. \tag{30}$$

Also note that the solution of the minimization problem is attained at the boundary $F_3(\rho) = 0$ (cf. Theorem 3.2). Since $\rho = [0.6213, 0.137, 0.137, 0.1047]$ satisfies $F_3(\rho) < 0$ and $I_3(\rho) = 0.30967 < 0.31$, we can exclude areas where the minimal value of the rate function satisfies $I_3(\rho) \ge 0.31$.

Now assume that $\nu \in M(\mathcal{X})$ minimizes $\rho \mapsto I_3(\rho)$ under the constraint $F_3(\rho) = 0$. We will show that ν is unique by proving that ν lies in a set that makes convex the rate function constrained to $F_3(\rho) = 0$. This will be done in the following 13 steps:

1. Observe from Lemma B.1 that for $|d| \ge 0.55$ the minimum of $I_3(\rho)$ exceeds 0.31. Hence $|\nu_\mp - \nu_\pm| < 0.55$.
2. The condition $F_3(\nu) = 0$ can be written as

$$\nu_+ = \frac{1}{4} \pm \frac{1}{4}\sqrt{(4\nu_\pm - 1)(4\nu_\mp - 1) + 2}. \tag{31}$$

It follows from (30) that $|d| < 0.55$ implies that either $\nu_+ \le 0.03 < 0.05$ or $\nu_+ \ge 0.47 > 0.45$.

3. For $\nu_+ > 0.45$, Lemma B.2 applied with $d_0 = 0.5$ and $m = 0.45$ implies that $|\nu_\mp - \nu_\pm| < 0.5$.
4. Similarly, for $\nu_+ < 0.05$, Lemma B.3 implies that $|\nu_\mp - \nu_\pm| < 0.5$.
5. $|d| < 0.5$ implies that either $\nu_+ < 0$ or $\nu_+ > 0.5$. Therefore the minus root can be excluded and $\nu_+ = r(\nu_\pm, \nu_\mp)$, where

$$r(\rho_\pm, \rho_\mp) = \frac{1}{4} + \frac{1}{4}\sqrt{(4\rho_\pm - 1)(4\rho_\mp - 1) + 2}.$$

6. For $\nu_+ > 0.5$, Lemma B.2 implies that $|\nu_\mp - \nu_\pm| < 0.32$.
7. From (30), $|\nu_\mp - \nu_\pm| < 0.32$ implies that $\nu_+ > 0.56$.
8. For $\nu_+ > 0.56$, Lemma B.2 implies that $|\nu_\mp - \nu_\pm| < 0.23$.
9. From (30), $|\nu_\mp - \nu_\pm| < 0.23$ implies that $\nu_+ > 0.58$.
10. For $\nu_+ > 0.58$, Lemma B.2 implies that $|\nu_\mp - \nu_\pm| < 0.19$.
11. From (30), $|\nu_\mp - \nu_\pm| < 0.19$ implies that $\nu_+ > 0.59$.
12. Lemma B.2 also implies that $|\nu_+ - \nu_-| < 0.55$. However, $\nu_+ > 0.59$ then implies $\nu_- > 0.04$.
13. The latter statement implies that $\nu_\mp + \nu_\pm \le 1 - 0.59 - 0.04 = 0.37$.

The following two lemmas now show that ν is unique. Let

$$J(\rho_\pm, \rho_\mp) = I_3\left(r(\rho_\pm, \rho_\mp), \rho_\pm, \rho_\mp, 1 - r(\rho_\pm, \rho_\mp) - \rho_\pm - \rho_\mp\right).$$

LEMMA B.4. *For $|d| \le 0.19$ and $0 \le e \le 0.37$,*

$$\rho_\pm \mapsto J(\rho_\pm, e - \rho_\pm), \quad \rho_\pm \in [\max(0, (e-0.19)/2), (e+0.19)/2]$$

is convex and attains its minimal value at $\rho_\pm = e/2$.

Proof. Observe that

$$\max_{0\le e\le 0.37} \frac{1}{4} + \frac{1}{4}\sqrt{(2e-1)^2 + 2} = \frac{1}{4} + \frac{1}{4}\sqrt{3} \le 0.69,$$

$$\min_{|d|\le 0.19} \frac{1}{4} + \frac{1}{4}\sqrt{2 - 4d^2} \ge 0.59,$$

$$\min_{0\le e\le 0.37} \frac{3}{4} - e - \frac{1}{4}\sqrt{(2e-1)^2 + 2} \ge 0.02.$$

From the first two inequalities and (30), we obtain that for all $\rho_\pm$, with $|d| \le 0.19$ and $0 \le e \le 0.37$,

$$0.59 \le r(\rho_\pm, e-\rho_\pm) \le 0.69.$$

Using the above inequalities, we will now show that

$$\frac{\partial^2 J(\rho_\pm, e-\rho_\pm)}{\partial \rho_\pm^2} > 0,$$

and thus the function is strictly convex.

Observe that

$$\frac{\partial r}{\partial \rho_\pm} = \frac{2(e-2\rho_\pm)}{4r-1}, \qquad \frac{\partial^2 r}{\partial \rho_\pm^2} = -\frac{4}{4r-1} - \frac{16(e-2\rho_\pm)^2}{(4r-1)^3},$$

where we abbreviate $r = r(\rho_\pm, e-\rho_\pm)$.

Hence,

$$\begin{aligned}\frac{\partial^2 J(\rho_\pm, e-\rho_\pm)}{\partial \rho_\pm^2} &= -\frac{4}{4r-1}\log\left(\frac{r}{\rho_-}\right) \\ &\quad + \frac{4(e-2\rho_\pm)^2}{(4r-1)^2}\left[\left(\frac{1}{r}+\frac{1}{\rho_-}\right) - \frac{4}{4r-1}\log\left(\frac{r}{\rho_-}\right)\right] + \frac{1}{\rho_\pm} + \frac{1}{e-\rho_\pm},\end{aligned}$$

where $\rho_- = 1-e-r$. The inequalities $3\log x \le 1+x$ for $x>0$ and $\frac{4}{4r-1} \le 3$ (which follows from $r \ge 0.59 \ge 7/12$) together imply

$$\left(\frac{1}{r}+\frac{1}{\rho_-}\right) - \frac{4}{4r-1}\log\left(\frac{r}{\rho_-}\right) \ge \left(\frac{1}{r}+\frac{1}{\rho_-}\right)\left(1 - \frac{4r}{3(4r-1)}\right) \ge 0.$$

Furthermore, we use that $1/\rho_\pm + 1/(e-\rho_\pm) = e/\{\rho_\pm(e-\rho_\pm)\} \ge 4/e$ and the obtained bounds for r and ρ_- to arrive at

$$\frac{\partial^2 J}{\partial \rho_\pm^2} \ge \frac{4}{e} - 3\log\left(\frac{0.69}{0.02}\right) > 0$$

for $0 \le e \le 0.37$. Since

$$\frac{\partial J}{\partial \rho_\pm}(e/2, e/2) = 0,$$

the minimum of J over $\rho_\pm$ for fixed $e \in [0, 0.37]$ is attained in $e/2$. □

LEMMA B.5. *The function*

$$e \mapsto J(e/2, e/2)$$

is convex and therefore has a unique minimum.

Proof. We have

$$J(e/2, e/2) = I_3(\rho_+, e/2, e/2, \rho_-),$$

where

$$\rho_+ = \frac{1}{4} + \frac{1}{4}\sqrt{(2e-1)^2+2}, \qquad \rho_- = 1-e-\rho_+.$$

Then

$$\frac{d^2J(e/2,e/2)}{de^2} = \frac{2}{4\rho_+ - 1}\log\left(\frac{\rho_+}{\rho_-}\right) + \frac{(2e-1)^2}{(4\rho_+-1)^2}\left[\left(\frac{1}{\rho_+}+\frac{1}{\rho_-}\right) - \frac{2}{4\rho_+-1}\log\left(\frac{\rho_+}{\rho_-}\right)\right] + \frac{1}{e}.$$

From $\rho_+ > 1/2$ and $3\log x < 1 + x$ for $x > 0$, we obtain that $\frac{d^2J}{de^2} > 0$. □

LEMMA B.6. *For $0 \le e \le 0.37$, the 2×2 matrix*

$$Q = \nabla^2 J(e/2, e/2)$$

is strictly positive definite.

Proof. We have

$$\begin{aligned} \tfrac{\partial^2 J(e/2,e/2)}{\partial e^2} &= Q_{11} + 2Q_{12} + Q_{22}, \\ \left.\tfrac{\partial^2 J(\rho_\pm, e-\rho_\pm)}{\partial \rho_\pm^2}\right|_{\rho_\pm = e/2} &= Q_{11} - 2Q_{12} + Q_{22}, \end{aligned}$$

and by Lemmas B.4–B.5 both quantities are positive. By symmetry, we have that $Q_{11} = Q_{22}$, so that $Q_{11} > |Q_{12}|$. This proves that Q is positive definite. □

Appendix C. Irrationality for $k = 3$. In this appendix we will prove the following lemma.

LEMMA C.1. *For $k = 3$ and for $a = \pm$ or $\mp$, $\frac{\partial r_{\tilde\rho}}{\partial \rho_a}(\tilde\nu)$ is irrational.*

Proof. Verify that $\frac{\partial r}{\partial \rho_a}(\tilde\nu) = \frac{4\nu_a - 1}{2(4\nu_+ - 1)}$ for $a = \pm$ and $a = \mp$. We will prove that for $a = \pm$ or $\mp$, $\frac{4\nu_a - 1}{2(4\nu_+ - 1)}$ is irrational.

For $\rho \in [0,1]$, let

$$v_\rho = \frac{1}{4} + \frac{1}{4}\sqrt{(4\rho - 1)^2 + 2}$$

be the symmetric version of (17). We want to minimize with respect to ρ

$$v_\rho \log v_\rho + 2\rho \log \rho + (1 - 2\rho - v_\rho)\log(1 - 2\rho - v_\rho) \tag{32}$$

and show that for the minimizer ρ^* we have that $\frac{4\rho^* - 1}{\sqrt{(4\rho^*-1)^2+2}} \notin \mathbb{Q}$. Since the minimizer ρ^* is equal to $\nu_\pm = \nu_\mp$, this proves the claim. The minimizer ρ^* has to satisfy

$$v'_{\rho^*}(\log v_{\rho^*} - \log(1 - 2\rho^* - v_{\rho^*})) + 2(\log \rho^* - \log(1 - 2\rho^* - v_{\rho^*})) = 0, \tag{33}$$

where

$$v'_\rho = \frac{4\rho - 1}{4v_\rho - 1}.$$

Suppose that $v'_{\rho^*} = -p/q$, with $p, q \in \mathbb{N}$, such that $p < q$. Then

$$\left(\frac{p}{q}\right)^2 = \frac{(4\rho^* - 1)^2}{(4v_{\rho^*} - 1)^2} = \frac{(4\rho^* - 1)^2}{(4\rho^* - 1)^2 + 2},$$

so that

$$\rho^* = \frac{1}{4} - \frac{1}{4}\sqrt{\frac{2p^2}{q^2 - p^2}}.$$

Here we have used that $2\rho^* = \nu_\pm + \nu_\mp \leq (1 - \nu_+) < 1/2$. We can rewrite (33) as

$$\left(\frac{v_{\rho^*}}{1-2\rho^*-v_{\rho^*}}\right)^{-p/q}\left(\frac{\rho^*}{1-2\rho^*-v_{\rho^*}}\right)^2 = 1. \tag{34}$$

From $-p/q = (4\rho^* - 1)/(4v_{\rho^*} - 1)$, it follows that

$$v_{\rho^*} = \frac{1}{4} + \frac{q}{4}\sqrt{\frac{2}{q^2-p^2}}.$$

Hence, (34) is equivalent to

$$\left(\sqrt{2(q^2-p^2)}+2q\right)^p\left(\sqrt{2(q^2-p^2)}+(4p-2q)\right)^{2q-p} = \left(\sqrt{2(q^2-p^2)}-2p\right)^{2q}. \tag{35}$$

In the remainder of the proof we will show that (35) has no integer solutions $p < q$.

Choose p and q having no common factor. There are two cases, depending on whether $2(q^2 - p^2)$ is a square or not.

Case 1*:* $2(q^2 - p^2)$ *is not a square.* From (35) and Newton's binomium we also obtain that

$$\begin{aligned}\left(-\sqrt{2(q^2-p^2)}+2q\right)^p&\left(-\sqrt{2(q^2-p^2)}+(4p-2q)\right)^{2q-p}\\ &= \left(-\sqrt{2(q^2-p^2)}-2p\right)^{2q}.\end{aligned} \tag{36}$$

Combining (35) and (36), we get

$$(p^2+q^2)^p(q^2-8pq+9p^2)^{2q-p} = (3p^2-q^2)^{2q}. \tag{37}$$

Now, $3p^2 - q^2$ must contain a prime factor, because if we suppose that $3p^2 - q^2 = 1$ or -1, then it follows from (37) that $p^2 + q^2 = 1$. This gives $p = 0, q = 1$, which is not a solution of (35).

Let j be a prime factor of $3p^2 - q^2$. Then, from (37), j must be a prime factor of $(p^2 + q^2)^p$, of $(q^2 - 8pq + 9p^2)^{2q-p}$, or of both. We will first show that j cannot be a prime factor of both $(p^2+q^2)^p$ and $(q^2-8pq+9p^2)^{2q-p}$. Indeed, if j is a prime factor of both terms, then it is also a prime factor of $p^2 + q^2$ and of $q^2 - 8pq + 9p^2$. Now, if j is odd, then j cannot be a prime factor of $p^2 + q^2$, since then it would also be a prime factor of $3p^2 - q^2 + p^2 + q^2 = 4p^2$ and of $3(p^2 + q^2) - (3p^2 - q^2) = 4q^2$, which would imply that p and q have a common (odd) factor. However, if $3p^2 - q^2$ is even, then p and q are both odd, since they cannot both be even. Furthermore, $p^2 + q^2$ is 2 modulo 4. Hence, by (37) and the fact that $3p^2 - q^2$ is a power of 2, we have that $p^2 + q^2 = 2$, which contradicts $p < q$.

At this stage, we know that j^{2q} is a prime factor of $(p^2 + q^2)^p$, or of $(q^2 - 8pq + 9p^2)^{2q-p}$, but not of both. From $gcd(p, q) = 1$ it follows that $gcd(2q, p) = 1$ or 2. Hence, j^q is a prime factor of p^2+q^2 or of $q^2-8pq+9p^2$. In the first case, this implies that

$$2^q \leq j^q \leq p^2 + q^2 \leq 2q^2,$$

so that $q \leq 6$. Similarly, in the second case,

$$2^q \leq j^q \leq |q^2 - 8pq + 9p^2| = |(q-3p)^2 - 2pq| \leq 2q^2,$$

so that again $q \leq 6$. We see that there are no solutions of (35) with $p < q$.

Case 2: $2(q^2 - p^2)$ is a square. Let $2(q^2 - p^2) = t^2$. First of all, t is even and p, q are odd. But then $t^2 = 2(q + p)(q - p)$ is an 8-fold, and therefore t is a 4-fold. We arrive at $t = 4 \prod p_i^{\alpha_i}$, where p_i are prime. Now $2(q^2 - p^2) = t^2$ factorizes into

$$\frac{(q+p)}{2}\frac{(q-p)}{2} = 2\prod p_i^{2\alpha_i}.$$

Since $(q+p)/2$ and $(q-p)/2$ are relative prime, it follows that both terms are quadratic and one of them is multiplied by 2; i.e., we have either that $(q - p)/2 = 2a^2$ and $(q+p)/2 = (b-a)^2$, or that $(q-p)/2 = a^2$ and $(q+p)/2 = 2(b-a)^2$. This gives that either

$$q = 2a^2 + (b-a)^2, \quad p = (b-a)^2 - 2a^2, \quad \text{or}$$

$$q = a^2 + 2(b-a)^2, \quad p = 2(b-a)^2 - a^2,$$

where a and b are integers having no common prime factors. Suppose that we are in the first case. Then we have that $2(q^2 - p^2) = 16a^2(b-a)^2$, so that (35) becomes

$$(a^2 + b^2)^p (b^2 - 7a^2)^{2q-p} = (a^2 - 4ab + b^2)^{2q}. \tag{38}$$

Let j be a prime factor of $a^2 - 4ab + b^2$. Then, similarly as above, if j is odd, j cannot be a prime factor of both $(a^2 + b^2)^p$ and $(b^2 - 7a^2)^{2q-p}$, since then it would also be a prime factor of $(a^2 + b^2) - (b^2 - 7a^2) = 8a^2$ and $7(a^2 + b^2) + (b^2 - 7a^2) = 8b^2$, which implies that a and b have common factors. The latter is not possible by construction. Hence, we are left with the case in which $a^2 - 4ab + b^2$ is a power of 2. This again implies that $a^2 + b^2$ is a power of 2, so that $a^2 + b^2$ must be equal to 2. This leads to $a = b = 1$, which is not a solution to (38). Hence, j^{2q} is a prime factor of $(a^2 + b^2)^p$ or of $(b^2 - 7a^2)^{2q-p}$ but not of both. Again, since $gcd(2q, p) = 1$ or 2, we have that j^q is a prime factor of $a^2 + b^2$ or of $b^2 - 7a^2$. In the first case, we estimate

$$2^q \leq r^q \leq a^2 + b^2 = (b-a)^2 + 2a(b-a) + 2a^2 \leq 2(b-a)^2 + 3a^2 \leq 2q.$$

Hence, $q \leq 2$.

Similarly, in the second case,

$$2^q \leq r^q \leq |b^2 - 7a^2| = |(b-a)^2 + 2a(b-a) - 5a^2| \leq (b-a)^2 + a^2 + (b-a)^2 + 5a^2 \leq 4q,$$

so that $q \leq 4$. Again, there are no solutions with $p < q$.

The case in which $q = a^2 + 2(b-a)^2$, $p = 2(b-a)^2 - a^2$ is proved the same way, using in this case that (35) turns into

$$((b-a)^2 + b^2)^p ((b-a)^2 + b^2 - 4a^2)^{2q-p} = (3(b-a)^2 - b^2)^{2q}. \tag{39}$$

We again see that there are no solutions of (35) with $p < q$. □

Acknowledgments. We would like to thank Frank den Hollander for help with the large deviation problem and Frits Beukers for the main ideas in the proof of Lemma C.1. Furthermore, we thank Arie Quist for help with plots of the rate function $\tilde{\rho} \mapsto J(\tilde{\rho})$, and Tero Ojanperä and Ramjee Prasad for proposing the problem.

REFERENCES

[1] R. R. Bahadur and R. Ranga Rao, *On deviations of the sample mean*, Ann. Math. Statist., 31 (1960), pp. 1015–1027.

[2] R. M. Buehrer and B. D. Woerner, *Analysis of adaptive multistage interference cancellation for CDMA using an improved Gaussian approximation*, IEEE Trans. Comm., 44 (1996), pp. 1308–1329.

[3] A. Dembo and O. Zeitouni, *Large Deviations Techniques and Applications*, 2nd ed., Springer, New York, 1998.

[4] W. Feller, *Introduction to Probability Theory*, Vol. 2, 2nd ed., Wiley, New York, 1971.

[5] R. van der Hofstad and M. J. Klok, *Improving the Performance of Third Generation Wireless Communication Systems*, submitted, 2001.

[6] F. den Hollander, *Large Deviations*, Fields Institute Monograph, AMS, Providence, RI, 2000.

[7] R. K. Morrow and J. S. Lehnert, *Bit-to-bit error dependence in slotted DS/SSMA packet systems with random signature sequences*, IEEE Trans. Comm., 37 (1989), pp. 1052–1061.

[8] R. Prasad, *CDMA for Wireless Personal Communications*, Artech House, Boston, 1996.

[9] J. S. Sadowsky and R. K. Bahr, *Direct-sequence spread-spectrum multiple-access communications with random signature sequences: A large deviations analysis*, IEEE Trans. Inform. Theory, 37 (1991), pp. 514–527.