Synchronization of random walks with reflecting boundaries

2004 J. Phys. A: Math. Gen. 37 8609

(http://iopscience.iop.org/0305-4470/37/36/003)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **37** (2004) 8609–8618 PII: S0305-4470(04)80913-2

Synchronization of random walks with reflecting boundaries

Andreas Ruttor, Georg Reents and Wolfgang Kinzel

Institut für Theoretische Physik, Universität Würzburg, Am Hubland, 97074, Würzburg, Germany

E-mail: andreas.ruttor@physik.uni-wuerzburg.de, georg.reents@physik.uni-wuerzburg.de and wolfgang.kinzel@physik.uni-wuerzburg.de

Received 17 May 2004
Published 24 August 2004
Online at stacks.iop.org/JPhysA/37/8609
doi:10.1088/0305-4470/37/36/003

Abstract

Reflecting boundary conditions cause two one-dimensional random walks to synchronize if a common direction is chosen in each step. The mean synchronization time and its standard deviation are calculated analytically. Both quantities are found to increase proportional to the square of the system size. Additionally, the probability of synchronization in a given step is analysed, which converges to a geometric distribution for long synchronization times. From this asymptotic behaviour the number of steps required to synchronize an ensemble of independent random walk pairs is deduced. Here the synchronization time increases with the logarithm of the ensemble size. The results of this model are compared to those observed in neural synchronization.

PACS numbers: 05.45.Xt, 05.40.Fb, 84.35.+i

1. Introduction

Synchronization of neural networks by mutual learning [1, 2] has recently been applied to cryptography [3]. Two neural networks which are trained by their mutual output bits can synchronize to a state with common time dependent couplings [4]. It has been shown how this phenomenon can be used to generate a secret key over a public channel [5, 6].

The networks used for neural cryptography are tree parity machines [7] consisting of K hidden units, which are discrete perceptrons with independent receptive fields made up of N binary input neurons. The influence of each input value on the output of the neural network is determined by the corresponding weight, which is an integer number in the range between $-L$ and $+L$. Since the synaptic depth of the neural networks is limited by the parameter L, there are only $m = 2L + 1$ possible values for each weight.

In each step a set of common inputs is chosen randomly for all tree parity machines involved in the process of synchronization. Then the weights are updated according to a

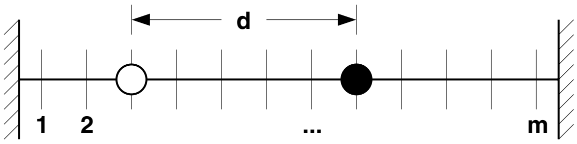

Figure 1. Random walks with reflecting boundaries.

suitable learning rule [8]. Thereby the change of each weight can be either $+1, 0$ or -1 depending on the corresponding input value and the calculated output of the neural networks. If an update is not possible because of the limited synaptic depth, then the affected weight is left unchanged in this step. That is why the process of synchronization is identical to an ensemble of random walks with reflecting boundaries, driven by pairwise identical random signals and controlled by mutual output bits [4, 6].

Therefore, to better understand neural cryptography, it is the aim of this paper to investigate the process of synchronization of random walks in some detail. We neglect the effect of the control bits, which is essential for cryptography [9], but we derive exact solutions for the synchronization times. In addition, since synchronization is an active field of research (for an overview see [10]), synchronization of random walks may be of interest in other contexts, too.

In this paper we analyse the model shown in figure 1. Two random walks can move on a one-dimensional line with m sites. In each step a direction, either left or right, is chosen randomly. Then both random walkers move in this direction. If one random walk hits the boundary, it is reflected, i.e. the random walk remains at its site on the left or on the right. As the other random walker is not affected, the distance d between both decreases by 1 at each reflection. Otherwise d remains constant.

The important quantity in this model is the synchronization time T, which is defined as the number of steps until d reaches zero. In section 2 we calculate the mean value and the standard deviation of this random variable analytically. Because large fluctuations of the synchronization time are observed in simulations, the average value of T does not describe the behaviour of the model sufficiently. Therefore, we estimate the probability distribution of the synchronization time in section 3. Using this result we are able to calculate the number of steps T_N, after which an ensemble of N random walk pairs reaches a synchronized state. This quantity is equal to the maximum of T observed in N independent samples. Therefore, we use methods of extreme order statistics to calculate the distribution of T_N, which is shown in section 4.

2. Average synchronization time

In order to calculate the mean value $\langle T \rangle$ of the synchronization time, the synchronization process is divided into independent parts, each of them with constant distance d. We first compute the average number $\langle S_{d,z} \rangle$ of steps until a reflection occurs, which decreases d by 1. Of course, this value depends on the initial position of the two random walkers. We use the distance d between both walkers and the position z of the left walker to describe these initial conditions.

If the first move is to the right, a reflection only occurs in the case of $z = m - d$. Otherwise the synchronization process continues as if the initial position had been $z + 1$. Under this condition, the average number of steps with distance d is given by $\langle S_{d,z+1} + 1 \rangle$.

Similarly, if the two random walkers move to the left in the first step, this quantity is equal to $\langle S_{d,z-1} + 1\rangle$. Averaging over both possibilities we obtain the following difference equation:

$$\langle S_{d,z}\rangle = \tfrac{1}{2}\langle S_{d,z-1}\rangle + \tfrac{1}{2}\langle S_{d,z+1}\rangle + 1. \tag{1}$$

Reflections are only possible if the current position z is either 1 or $m - d$. In both situations d changes with probability $\frac{1}{2}$ in the next step. In order to take this into account we have to use

$$S_{d,0} = 0 \qquad \text{and} \qquad S_{d,m-d+1} = 0 \tag{2}$$

as boundary conditions.

Equation (1) is identical to the classical ruin problem [11]. Its solution is:

$$\langle S_{d,z}\rangle = (m - d + 1)z - z^2. \tag{3}$$

In a similar manner we obtain a difference equation for $\langle S_{d,z}^2\rangle$, which is used later to calculate the standard deviation of the synchronization time:

$$\langle S_{d,z}^2\rangle = \tfrac{1}{2}\langle (S_{d,z-1} + 1)^2\rangle + \tfrac{1}{2}\langle (S_{d,z+1} + 1)^2\rangle. \tag{4}$$

From (3) and (4) we obtain the following relation for the variance of $S_{d,z}$:

$$\langle S_{d,z}^2\rangle - \langle S_{d,z}\rangle^2 = \frac{\langle S_{d,z-1}^2\rangle - \langle S_{d,z-1}\rangle^2}{2} + \frac{\langle S_{d,z+1}^2\rangle - \langle S_{d,z+1}\rangle^2}{2} + (m - d + 1 - 2z)^2\,. \tag{5}$$

Applying a Z-transformation yields the solution

$$\langle S_{d,z}^2\rangle - \langle S_{d,z}\rangle^2 = \frac{(m - d + 1 - z)^2 + z^2 - 2}{3}\langle S_{d,z}\rangle. \tag{6}$$

With these results we can calculate the average value of the synchronization time $T_{d,z}$ for two random walks starting at distance d and position z. The first reflection occurs after $S_{d,z}$ steps. Then one of the random walkers is located at the boundary. As our model is symmetric, both possibilities $z = 1$ or $z = m - d$ are equal. Hence the second reflection takes place after $S_{d,z} + S_{d-1,1}$ steps. So the total synchronization time is given by

$$T_{d,z} = S_{d,z} + \sum_{j=1}^{d-1} S_{j,1}. \tag{7}$$

Using (3) we obtain

$$\langle T_{d,z}\rangle = (m - d + 1)z - z^2 + \tfrac{1}{2}(d - 1)(2m - d) \tag{8}$$

for the expectation value of this random variable. The variance of $T_{d,z}$ can be calculated in a similar manner, because the parts of the synchronization process are mutually independent.

Finally, we have to average over all possible initial conditions in order to calculate the mean value and the standard deviation of the synchronization time T for randomly chosen starting positions of the two random walkers:

$$\langle T\rangle = \frac{2}{m^2}\sum_{d=1}^{m-1}\sum_{z=1}^{m-d}\langle T_{d,z}\rangle = \frac{(m-1)^2}{3} + \frac{m-1}{3m}, \tag{9}$$

$$\langle T^2\rangle = \frac{2}{m^2}\sum_{d=1}^{m-1}\sum_{z=1}^{m-d}\langle T_{d,z}^2\rangle = \frac{17m^5 - 51m^4 + 65m^3 - 45m^2 + 8m + 6}{90m}. \tag{10}$$

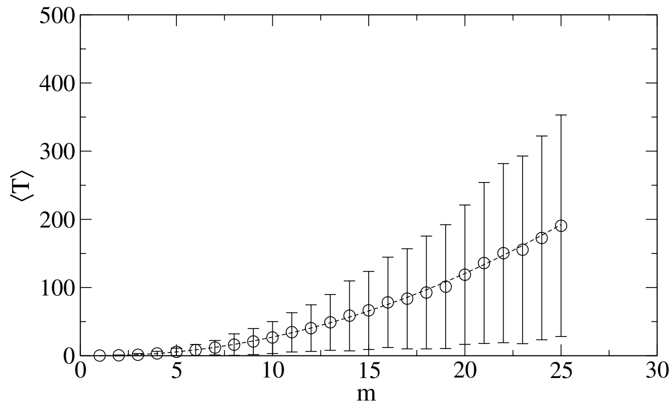

Figure 2. Synchronization time of two random walks as a function of the system size m. Error bars denote the standard deviation observed in 1000 simulations. The analytical solution from (9) is plotted as a dashed curve.

So the average number of steps required to reach a synchronized state, which is shown in figure 2, increases nearly proportional to m^2. In particular for large system sizes m, we obtain the asymptotic relation

$$\langle T\rangle \sim \tfrac{1}{3}m^2 \sim \tfrac{4}{3}L^2. \tag{11}$$

This result is consistent with the scaling behaviour $\langle T\rangle \propto L^2$ observed in neural synchronization [5].

Numerical simulations, both for random walks and neural networks, show large fluctuations of the synchronization time. The reason for this observation is that not only the mean value, but also the standard deviation

$$\sigma_T = \sqrt{\frac{7m^6 - 11m^5 - 15m^4 + 55m^3 - 72m^2 + 46m - 10}{90m^2}} \tag{12}$$

of the synchronization time increases with the extension m of the random walks. Here we find that σ_T is asymptotically proportional to $\langle T\rangle$:

$$\sigma_T \sim \sqrt{\frac{7}{10}}\langle T\rangle. \tag{13}$$

Therefore, the relative fluctuations $\sigma_T/\langle T\rangle$ are nearly independent of m and not negligible.

3. Probability distribution

The synchronization of two random walks is a Markov chain, because the next step only depends on the current state of the system. We can, therefore, derive an equation for the distribution of the total synchronization time T.

For this purpose we introduce $\frac{1}{2}m(m+1)$ variables $p_{d,z}(t)$, which are defined as the probability to find the two random walkers at the positions z and $z+d$ in time step t. In the initial ensemble the positions are chosen randomly, hence all variables are set to

$$p_{d,z}(0) = \frac{2-\delta_{d,0}}{m^2}. \tag{14}$$

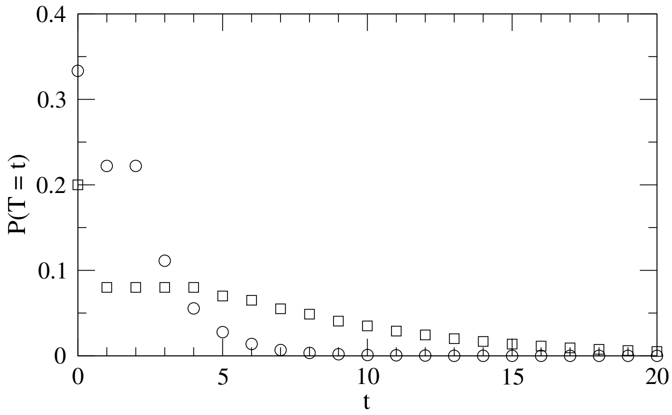

Figure 3. Probability of synchronization $\mathrm{P}(T = t)$ as a function of the number of steps. The symbols show the result of the numerical calculation for $m = 3$ (○) and $m = 5$ (□).

The development of the probabilities in each step is given by the following equations for $0 \leqslant d < m - 1$ and $1 < z < m - d$:

$$p_{d,z}(t+1) = \tfrac{1}{2} p_{d,z-1}(t) + \tfrac{1}{2} p_{d,z+1}(t), \tag{15}$$

$$p_{d,1}(t+1) = \tfrac{1}{2} p_{d,2}(t) + \tfrac{1}{2} p_{d+1,1}(t) + \tfrac{1}{2}\delta_{d,0} p_{0,1}, \tag{16}$$

$$p_{d,m-d}(t+1) = \tfrac{1}{2} p_{d,m-d-1}(t) + \tfrac{1}{2} p_{d+1,m-d-1}(t) + \tfrac{1}{2}\delta_{d,0} p_{0,m}, \tag{17}$$

$$p_{m-1,1}(t+1) = 0. \tag{18}$$

The probability $\mathrm{P}(T = t)$, that the two random walks synchronize in the time step $t > 0$, is given by

$$\mathrm{P}(T = t) = \sum_{z=1}^{m} (p_{0,z}(t) - p_{0,z}(t-1)). \tag{19}$$

Using (15)–(18) we deduce the expression

$$\mathrm{P}(T = t) = \tfrac{1}{2} p_{1,1}(t-1) + \tfrac{1}{2} p_{1,m-1}(t-1). \tag{20}$$

These equations can easily be iterated numerically.

Figure 3 shows the results of these calculations for $m = 3$ and $m = 5$. Because of the randomly chosen initial conditions there is a probability of $\mathrm{P}(T = 0) = 1/m$ that the two random walkers even start synchronized. Furthermore, one notices that $\mathrm{P}(T = t)$ is constant and equal to $2/m^2$ in the range $0 < t < m$.

In principle, it is also possible to calculate the probability distribution $\mathrm{P}(T = t)$ analytically. We use this method to estimate an approximation of $\mathrm{P}(T = t)$, which is asymptotically exact for very long synchronization times $t \gg m$. For that purpose we start with a result known from the solution of the classical ruin problem [11]: the probability that a fair game ends with the ruin of one player in time step t is given by

$$u(t) = \frac{1}{a} \sum_{k=1}^{a-1} \sin\left(\frac{k\pi z}{a}\right) \left[\sin\left(\frac{k\pi}{a}\right) + \sin\left(k\pi - \frac{k\pi}{a}\right)\right] \left[\cos\left(\frac{k\pi}{a}\right)\right]^{t-1}. \tag{21}$$

In our model $a - 1 = m - d$ denotes the number of possible positions for two random walkers with distance d. And $u(t)$ is the probability distribution of the random variable $S_{d,z}$, which we introduced in section 2. As before, z is the initial position of the left random walker.

According to (7) the synchronization time $T_{d,z}$ for fixed initial conditions is the sum over $S_{i,j}$ for each distance i from d to 1. Therefore, its probability distribution $\mathrm{P}(T_{d,z} = t)$ is a convolution of d functions $u(t)$ defined in (21). The convolution of two different geometric sequences $b_n = b^n$ and $c_n = c^n$ is itself a linear combination of these sequences:

$$b_n * c_n = \sum_{j=1}^{n-1} b^j c^{n-j} = \frac{c}{b-c} b_n + \frac{b}{c-b} c_n. \tag{22}$$

Therefore, $\mathrm{P}(T_{d,z} = t)$ can be written as a sum over geometric sequences, too:

$$\mathrm{P}(T_{d,z} = t) = \sum_{a=m-d+1}^{m} \sum_{k=1}^{a-1} q_{a,k}^{d,z} \left[\cos\left(\frac{k\pi}{a}\right)\right]^{t-1}. \tag{23}$$

In order to obtain $\mathrm{P}(T = t)$ for random initial conditions, we have to average over all possible starting positions of the random walkers:

$$\mathrm{P}(T = t) = \frac{2}{m^2} \sum_{d=1}^{m-1} \sum_{z=1}^{m-d} \mathrm{P}(T_{d,z} = t). \tag{24}$$

So we can even write

$$\mathrm{P}(T = t) = \sum_{a=2}^{m} \sum_{k=1}^{a-1} q_{a,k} \left[\cos\left(\frac{k\pi}{a}\right)\right]^{t-1} \tag{25}$$

as a sum over many geometric sequences.

For long times only the terms with the largest absolute value of the coefficient $\cos(k\pi/a)$ are relevant, because the others decline exponentially faster and can be neglected for $t \to \infty$. Hence the asymptotic behaviour of the probability distribution is given by

$$\mathrm{P}(T = t) \sim [q_{m,1} + (-1)^{t-1} q_{m,m-1}] \left[\cos\left(\frac{\pi}{m}\right)\right]^{t-1}. \tag{26}$$

The two coefficients $q_{m,1}$ and $q_{m,m-1}$ in this equation can be calculated using (22). This leads to the following result:

$$\begin{aligned} q_{m,1} = {} & \frac{\sin^2(\pi/m)}{m^2 m!} \sum_{d=1}^{m-1} \frac{2^{d+1}(m-d)!}{1 - \delta_{d,1}\cos(\pi/m)} \\ & \times \prod_{a=m-d+1}^{m-1} \sum_{k=1}^{a-1} \frac{\sin^2(k\pi/2)}{\cos(\pi/m) - \cos(k\pi/a)} \frac{\sin^2(k\pi/a)}{1 - \delta_{a,m-d+1}\cos(k\pi/a)}, \end{aligned} \tag{27}$$

$$\begin{aligned} q_{m,m-1} = {} & \frac{\sin^2(\pi/m)\cos^2(m\pi/2)}{m^2 m!} \sum_{d=1}^{m-1} (-1)^{d-1} \frac{2^{d+1}(m-d)!}{1 + \delta_{d,1}\cos(\pi/m)} \\ & \times \prod_{a=m-d+1}^{m-1} \sum_{k=1}^{a-1} \frac{\sin^2(k\pi/2)}{\cos(\pi/m) + \cos(k\pi/a)} \frac{\sin^2(k\pi/a)}{1 - \delta_{a,m-d+1}\cos(k\pi/a)}, \end{aligned} \tag{28}$$

which is also shown in figure 4.

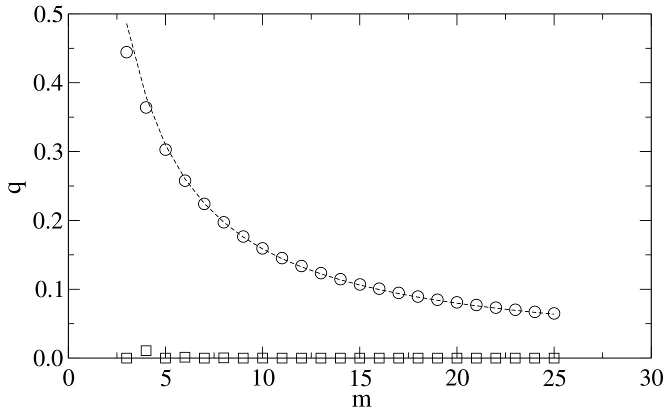

Figure 4. Value of the coefficients $q_{m,1}$ (○) and $q_{m,m-1}$ (□) as a function of m. The parameter $q_{m,1}$ can be approximately calculated using the function $q_{m,1} \approx 0.324m[1 - \cos(\pi/m)]$, which is shown as a dashed curve.

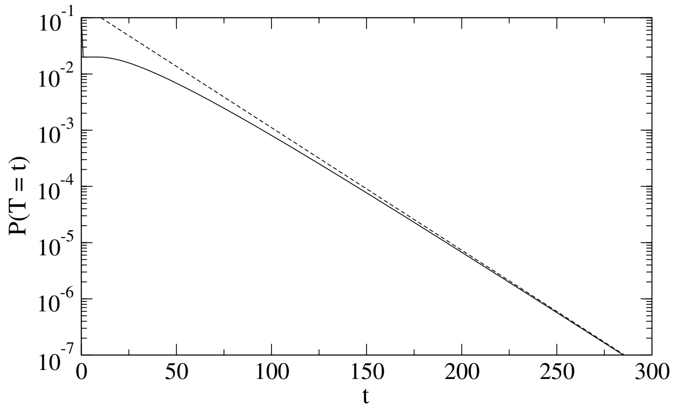

Figure 5. Probability distribution $\mathrm{P}(T = t)$ of the synchronization time for $m = 10$. The numerical result is plotted as a full curve. The dashed line denotes the asymptotic function defined in (29).

For odd values of m, the coefficient $q_{m,m-1} = 0$. In this case $\mathrm{P}(T = t)$ asymptotically converges to a geometric probability distribution for long synchronization times:

$$\mathrm{P}(T = t) \sim q_{m,1} \left[\cos\left(\frac{\pi}{m}\right)\right]^{t-1}. \tag{29}$$

If m is even, we have to consider oscillations of $\mathrm{P}(t)$ around the function given by (29), because $q_{m,m-1} \neq 0$. But for $m > 8$, the coefficient $q_{m,m-1}$, which determines the amplitude of these oscillations, is smaller than $10^{-3}q_{m,1}$. As shown in figure 5, (29) is a good approximation of the asymptotic behaviour for even values of m, too.

4. Extreme order statistics

In this section we extend our model to ensembles of random walks. We consider N independent pairs of random walkers driven pairwise by identical random noise. Each pair is finally synchronized by the effect of the reflecting boundary conditions. From the results discussed

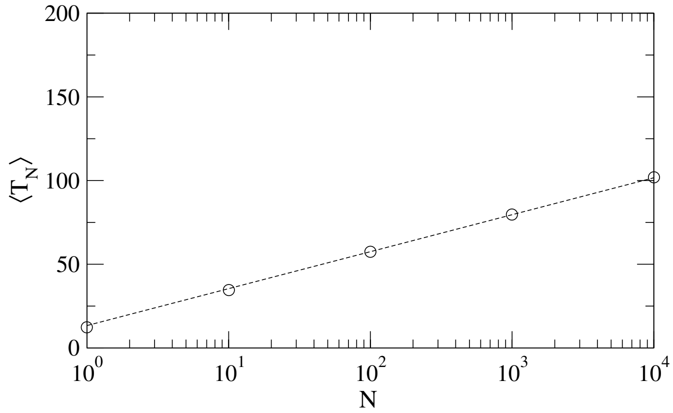

Figure 6. Average synchronization time $\langle T_N \rangle$ as a function of N for $m = 7$. Results of the numerical calculation using (30) are represented by circles. The dashed line shows the expectation value of T_N calculated in (35).

above we know the expected average synchronization time. But the important quantity in this case is the number of steps T_N until all random walks are synchronized. Of course, this random variable is equal to the maximum value of T observed in N independent samples.

From the distribution function $\mathrm{P}(T \leqslant t)$ we can easily deduce the probability distribution of T_N:

$$\mathrm{P}(T_N \leqslant t) = \mathrm{P}(T \leqslant t)^N. \tag{30}$$

Therefore, we can calculate the average value $\langle T_N \rangle$ using the numerically computed distribution. The result, which is shown in figure 6, indicates that $\langle T_N \rangle$ increases proportional to $\ln N$:

$$\langle T_N \rangle - \langle T \rangle \propto \ln N. \tag{31}$$

Similar behaviour has been observed in neural synchronization [4, 6].

For large N only the asymptotic behaviour of $\mathrm{P}(T \leqslant t)$ is relevant for the distribution of T_N. The exponential decay of $\mathrm{P}(T = t)$ in (26) yields a Gumbel distribution for $\mathrm{P}(T_N \leqslant t)$ [12],

$$G(x) = \exp\left(-\mathrm{e}^{\frac{\alpha - x}{\beta}}\right), \tag{32}$$

for $N \gg m$ with the parameters

$$\alpha = \beta \ln \frac{N q_{m,1}}{1 - \cos(\pi/m)} \qquad \text{and} \qquad \beta = -\frac{1}{\ln\cos(\pi/m)}. \tag{33}$$

Substituting (33) into (32) we get

$$\mathrm{P}(T_N \leqslant t) = \exp\left(-\frac{N q_{m,1} \cos^t(\pi/m)}{1 - \cos(\pi/m)}\right) \tag{34}$$

as the distribution function for the total synchronization time of N pairs of random walks ($N \gg m$). The expectation value of this probability distribution is given by [12]

$$\langle T_N \rangle = \alpha + \beta\gamma = -\frac{1}{\ln\cos(\pi/m)} \left(\gamma + \ln N + \ln \frac{q_{m,1}}{1 - \cos(\pi/m)}\right). \tag{35}$$

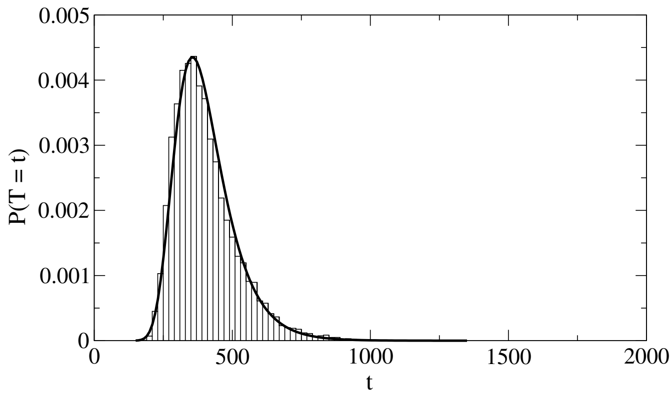

Figure 7. Probability distribution of the synchronization time for two tree parity machines with the parameters $K = 3, L = 3$ and $N = 1000$. The histogram shows the relative frequency of occurrence observed in 10 000 simulations. The thick curve represents a Gumbel distribution for $\alpha = 355.8$ and $\beta = 84.5$.

In this equation, γ denotes the Euler–Mascheroni constant. For $N \gg m \gg 1$, we obtain the relation

$$\langle T_N \rangle \sim \frac{2}{\pi^2} m^2 \left(\gamma + \ln N + \ln \frac{2m^2 q_{m,1}}{\pi^2} \right), \tag{36}$$

which shows that $\langle T_N \rangle$ increases asymptotically proportional to $m^2 \ln N$. Using the approximation for $q_{m,1}$ shown in figure 4, we find $\langle T_N \rangle \approx (2/\pi^2) m^2 (\ln N + \ln(0.577m))$.

Neural cryptography is somewhat more complex than our model with random walks. Since in this case the movements of the random walks are controlled by learning rules [8], there are also steps without changes of the weights. These are not included in our calculation of the synchronization time. Additionally, repulsive steps destroying synchronization [7] are possible, too. Nevertheless, the synchronization time of neural synchronization scales like $\langle T_N \rangle \propto L^2 \ln N$ [5], in agreement with (36). And its probability distribution, obtained from numerical simulations and shown in figure 7, is described well by a Gumbel distribution where the two parameters α and β are fitted to the data.

5. Conclusion

We have analysed the synchronization of two random walks with reflecting boundary conditions. We calculated the mean value and the standard deviation of the synchronization time T analytically for randomly chosen initial positions of the two random walkers. The average number of steps until synchronization increases with m^2, the square of the system size. Additionally, the standard deviation σ_T also scales with m^2, which shows that fluctuations of T cannot be neglected even if m is large.

The probability $\mathrm{P}(T = t)$ that two random walks synchronize at t steps has been derived. For long synchronization times $t \gg m$, the asymptotic behaviour of $\mathrm{P}(T = t)$ is given by a geometric probability distribution with parameter $p = 1 - \cos(\pi/m)$.

We have also studied the number of steps T_N needed to synchronize N independent pairs of random walks. The average value of this random variable increases with $\ln N$. And, for large values of N, the probability $\mathrm{P}(T_N \leqslant t)$ that t steps are sufficient for synchronization is given by a Gumbel distribution.

Finally, our model is able to reproduce the scaling behaviour observed in neural cryptography. We find that T_N increases nearly proportional to $L^2 \ln N$. Additionally, even for tree parity machines, the distribution of the synchronization times of neural cryptography is described by a Gumbel distribution.

References

[1] Metzler R, Kinzel W and Kanter I 2000 *Phys. Rev.* E **62** 2555–65
[2] Kinzel W, Metzler R and Kanter I 2000 *J. Phys. A: Math. Gen.* **33** L141–7
[3] Kanter I, Kinzel W and Kanter E 2002 *Europhys. Lett.* **57** 141–7
[4] Kinzel W and Kanter I 2002 *Advances in Solid State Physics* vol 42 ed B Kramer (Berlin: Springer) pp 383–91
[5] Mislovaty R, Perchenok Y, Kanter I and Kinzel W 2002 *Phys. Rev.* E **66** 066102
[6] Kinzel W and Kanter I 2003 *J. Phys. A: Math. Gen.* **36** 11173–86
[7] Rosen-Zvi M, Klein E, Kanter I and Kinzel W 2002 *Phys. Rev.* E **66** 066135
[8] Ruttor A, Kinzel W, Shacham L and Kanter I 2004 *Phys. Rev.* E **69** 046110
[9] Klimov A, Mityagin A and Shamir A 2003 *Advances in Cryptology—ASIACRYPT 2002* ed Y Zheng (Heidelberg: Springer) p 288
[10] Pikovsky A, Rosenblum M and Kurths J 2001 *Synchronization* (Cambridge, UK: Cambridge University Press)
[11] Feller W 1968 *An Introduction to Probability Theory and Its Applications* vol 1 3rd edn (New York: Wiley)
[12] Galambos J 1940 *The Asymptotic Theory of Extreme Order Statistics* (New York: Wiley)