ELSEVIER

Available online at www.sciencedirect.com
SCIENCE DIRECT®

Theoretical Computer Science 349 (2005) 475–483

Theoretical Computer Science

www.elsevier.com/locate/tcs

On the expected time for Herman's probabilistic self-stabilizing algorithm☆

Toshio Nakata*

Department of Information Education, Fukuoka University of Education, Akama-Bunkyomachi, Munakata, Fukuoka 811-4192, Japan

Received 1 December 2004; received in revised form 8 April 2005; accepted 25 May 2005

Communicated by M. Jerrum

Abstract

In this article we investigate the expected time for Herman's probabilistic self-stabilizing algorithm in distributed systems: suppose that the number of identical processes in a unidirectional ring, say n, is odd and $n \geqslant 3$. If the initial configuration of the ring is not "legitimate", that is, the number of tokens differs from one, then execution of the algorithm made up of synchronous probabilistic procedures with a local parameter $0 < r < 1$ results in convergence to a legitimate configuration with a unique token (Herman's algorithm). We then show that the expected time of the convergence is less than $((\pi^2 - 8)/8r(1-r))n^2$. Note that if $r = \frac{1}{2}$ then it is bounded by $0.936n^2$. Moreover, there exists a configuration whose expected time is $\Theta(n^2)$. The method of the proof is based on the analysis of *coalescing random walks*.

Keywords: Probabilistic self-stabilization; Herman's algorithm; Random walk; Coalescing time

---

1. Introduction

Distributed systems based on self-stabilizing algorithms were introduced by Dijkstra [7]. The algorithms propose an elegant way of solving the problem of fault-tolerance (see also [8,17]). In general, the algorithms have the property that arbitrary configuration reaches "legitimate" configuration satisfying desired property in finite time. Moreover, probabilistic methods are often studied as solutions to problems for distributed computing in order to improve the efficiency of deterministic algorithms. For example, the methods are used in many symmetric distribution to break symmetry (see [8]). So there are some good probabilistic self-stabilizing algorithms [16,14,3]. Especially one of the simple and useful probabilistic self-stabilizing algorithms was proposed by Herman [14]. The basic setting is the following: suppose that the number of identical processes in a unidirectional ring, say n, is odd and $n \geqslant 3$. If the initial configuration of the ring is not *legitimate*, that is, the number of tokens differs from one, then execution of the algorithm made up of synchronous probabilistic procedures with a local parameter $0 < r < 1$ results in convergence to a legitimate configuration with a unique token (Herman's algorithm).

☆ A preliminary version of this paper appeared in the Tenth Annual International Computing and Combinatorics Conference (COCOON 2004).
* Tel.: +81 940 35 1352; fax: +81 940 35 1710.
E-mail address: nakata@fukuoka-edu.ac.jp.

doi:10.1016/j.tcs.2005.05.022

For the algorithm in this article we show that the expected time of the convergence is less than $((\pi^2-8)/8r(1-r))n^2$. Note that if $r=\frac{1}{2}$ then it is bounded by $0.936n^2$. Moreover, we also give a configuration whose expected time is $\Theta(n^2)$. The method of the proof is based on the analysis of the expected time of *coalescing random walks*.

Related works and our method: A model of coalescing random walks was proposed by Aldous and Fill [2, Chapter 14]. They formalized them using continuized chains with 1-exponential distributions. Note that many quantities are unchanged by the passage from the discrete time chain to the continuized chain. Their setting is the following: fix a connected graph G with order n. Consider independent random walks starting from each vertex. When some of them meet, they coalesce into a new random walk. What is the expected time that all walks coalesce into a single random walk? They showed that the time is less than $e(\log n+2)T_G$, where T_G is the maximal (in the meaning of start and goal points) expected *hitting time* of G. On the other hand, Brightwell and Winkler [4] showed that T_G is bounded by $(4/27+\mathrm{o}(1))n^3$, which is attained by some lollipop graphs. Moreover Coppersmith et al. [6], Tetali and Winkler [19] studied the *meeting time*, which is the expected number of steps that two independent random walks collide on a connected graph. They proved that $M_G \leqslant (4/27+\mathrm{o}(1))n^3$, where M_G is the maximal (in the meaning of start points) meeting time on a connected graph G with order n. Furthermore, Hassin and Peleg [13] applied the results of meeting times to an analysis of the expected absorption time in distributed probabilistic polling. In their setting they pointed out that the time is equivalent to the expected time of coalescing random walks. They showed that the time is $\mathrm{O}(M_G \log n)$. Their key idea of the estimate is the following: since M_G is the maximal meeting time, at least $n/2$ random walks have to meet after the time M_G. By repetition, the results can be obtained. Recently, Adler et al. [1] showed good estimates of expected coalescing times for independently and identically distributed random variables without considering graph structures. They noted applications to population biology.

For expected time of Herman's self-stabilizing algorithm we also apply the method of coalescing random walks. We regard tokens in the ring as independent random walks. Though in our case random walks do not coalesce but disappear when two random walks collide, we can see that the expected times do not change essentially. Noting that both $M_{n\text{-ring}}$ and $T_{n\text{-ring}}$ are $\Theta(n^2)$, we can drop $\log n$ term for Aldous and Fill's/Hassin and Peleg's results. Moreover, Aldous and Fill [2, Chapter 14, Section 3] conjectured that there exists an absolute constant K such that for any graph G the expected time of coalescing random walks is bounded by KT_G. Hence our estimate would be one of the positive example for their conjecture. To estimate the expected time of coalescing random walks, we are aiming at not the *maximal* meeting time but the *minimal* meeting time on the ring. It was used by Herman himself to prove the probabilistic self-stabilization with probability 1.

On the other hand, very recently, Fribourg et al. [12] also studied the expected times for Herman's algorithm independent of this article. They used the refined method of *path coupling* introduced by Bubley and Dyer [5]. Actually, they used the convenient version of it studied by Dyer and Greenhill [10]. They showed that the expected times are bounded by $2n^2$ if $r=\frac{1}{2}$ in our setting. Moreover, they gave general good results between coupling and self-stabilization. Indeed, they applied their arguments to self-stabilizing algorithms including *Iterated Prisoner's Dilemma problems* studied by Dyer et al. [9] as well as Herman's one.

Plan of the paper: After some preliminary about Herman's algorithm (Section 2), we state an estimate of the expected time of Herman's algorithm in Section 3.1. The proof is given in Section 3.2. Moreover, showing future works, we conclude in Section 4. The rough scenario of the estimate in Section 3.2 is the following:

(i) We formalize tokens in the ring as independent random walks (Lemma 3.2).
(ii) Noting the minimal meeting time of random walks of Item (i), we investigate correspondent one-dimensional random walks (Lemma 3.3).
(iii) To estimate hitting times of one-dimensional random walks of Item (ii), we use the *dominating random walk* whose expected time can be gotten by some difference equations (Lemmas 3.4 and 3.5).
(iv) Using the hitting time of Item (iii), we estimate the desirable expected time. Moreover, we give a simple example satisfying Eq. (9).

2. Herman's algorithm

Let $L=\{0,\ldots,n-1\}\simeq \mathbf{Z}/n\mathbf{Z}$ be a process ring, where n is an integer satisfying $n\geqslant 3$. Henceforth any index is defined for any integer subscript with modulo n. The state of each process is a single bit in $\{0,1\}$, so that we denote by $\mathcal{X}_n=\{0,1\}^n$ the configuration space whose element is represented by a vector of n bits $x=(x_0,\ldots,x_{n-1})\in\mathcal{X}_n$. For a given $0 < r < 1$, a random procedure $f : \mathcal{X}_n \to \mathcal{X}_n$ is defined by

$$f(x) = f_r(x) = y = (y_0, \ldots, y_{n-1}) \in \mathcal{X}_n, \quad y_i = \begin{cases} x_{i-1} & \text{if } x_i \neq x_{i-1}, \\ \gamma_i & \text{if } x_i = x_{i-1}, \end{cases} \tag{1}$$

where γ_i, $(i = 0, \ldots, n-1)$ are $\{0, 1\}$-valued independent random variables with each distribution

$$\Pr(\gamma_i = x_i) = 1 - \Pr(\gamma_i = 1 - x_i) = r \quad \text{for } i = 0, \ldots, n-1. \tag{2}$$

For a given $x = (x_0, \ldots, x_{n-1}) \in \mathcal{X}_n$, we define a local state to be any consecutive pair (x_{i-1}, x_i):

- if $x_i = x_{i-1}$, then there is a *token* at process i. (We will also say that x_i is a token.)
- if $x_i \neq x_{i-1}$, then there is a *shift* at process i. (We will also say that x_i is a shift.)

Note that if n is odd, the number of tokens is also odd, that is,

$$\|x\| \bmod 2 \equiv n \bmod 2 \quad \text{for } x \in \mathcal{X}_n, \tag{3}$$

where $\|\cdot\|$ is the number of tokens in the ring. For each $x = (x_0, \ldots, x_{n-1}) \in \mathcal{X}_n$ define the set of tokens/shifts as follows:

$$L_T = L_T(x) = \{1 \leqslant i \leqslant n : x_i = x_{i-1}\},$$

$$L_S = L_S(x) = L \setminus L_T = \{1 \leqslant i \leqslant n : x_i \neq x_{i-1}\}. \tag{4}$$

Moreover, we also define $\mathcal{X}_n^k = \{x \in \mathcal{X}_n : |L_T(x)| = k\} = \{x \in \mathcal{X}_n : \|x\| = k\}$. We call the element of $\mathcal{X}_n^1$ a *legitimate* configuration. Use notation $f^t(x) = f(f^{t-1}(x))$ for $t \geqslant 1$, where $f^0(x) = x$. Herman proved the following theorem:

Theorem 2.1 (*Herman*). *For the random procedure f defined by Eq.* (1), *the following statements hold*:

(i) *The number of tokens does not increase*:

$$\Pr(\|x\| \geqslant \|f(x)\|) = 1. \tag{5}$$

(ii) *If there exists a unique token at i*, *then the token is eventually at* $i + 1$: *for each* $x \in \mathcal{X}_n^1$ *with* $x_i = x_{i-1}$

$$\Pr(\exists k > 0 \ s.t. \ y = f^k(x) \in \mathcal{X}_n^1, y_i = y_{i+1}) = 1. \tag{6}$$

(iii) *If there are more than two tokens*, *the number of tokens is eventually strictly decreasing*:

$$\Pr(\exists k > 0 \ s.t. \ \|f^k(x)\| < \|x\|) = 1 \quad \textit{for } \|x\| \geqslant 2. \tag{7}$$

Remark 2.1. (i) Suppose that n is odd. Then by Eq. (3), the number of tokens is also odd. Moreover, by Eqs. (5) and (7) we see that the number of decreasing tokens is even (including 0) for an arbitrary configuration, and at last there will hereafter become a unique token.

(ii) By Eq. (6), the algorithm progresses in a legitimate configuration, that is, the token circulates in the ring.

3. Expected times for Herman's algorithm

3.1. Main results

Fix an odd integer $n \geqslant 3$. Then by Item (i) in Remark 2.1, we see that for $x \in \mathcal{X}_n$ there exists $t = t(x) < \infty$ with probability 1 such that

$$\|x\| \geqslant \|f(x)\| \geqslant \cdots \geqslant \|f^{t-1}(x)\| > \|f^t(x)\| = \|f^{t+1}(x)\| = \cdots = 1.$$

Now we analyze the above random time t for any $x \in \mathcal{X}_n$.

Theorem 3.1. *Let $n \geqslant 3$ be an odd integer. Then for any parameter $0 < r < 1$ of Eq. (2), the expected time to become a legitimate configuration on the n-ring is less than $((\pi^2 - 8)/8r(1-r))n^2$, that is,*

$$\max_{x \in \mathcal{X}_n} \mathbf{E}\left[\inf\{t \geqslant 0 : f^t(x) \in \mathcal{X}_n^1\}\right] < \frac{\pi^2 - 8}{8r(1-r)} n^2. \tag{8}$$

Moreover, there exists $x \in \mathcal{X}_n$ such that

$$\mathbf{E}\left[\inf\{t \geqslant 0 : f^t(x) \in \mathcal{X}_n^1\}\right] = \Theta(n^2). \tag{9}$$

The notation $a_n = \Theta(b_n)$ denotes that there exist $c, C > 0$ and n_0 such that $cb_n \leqslant a_n \leqslant Cb_n$ for $n \geqslant n_0$.

3.2. Proof of Theorem 3.1

Now we consider a configuration with k tokens $x^k \in \mathcal{X}_n^k$ for $k \leqslant n$. Then we define the *first decreasing time* for $x^k \in \mathcal{X}_n^k$:

$$T(x^k) = \inf\{t > 0 : f^t(x^k) \notin \mathcal{X}_n^k\}. \tag{10}$$

To investigate the time, we define the minimum token distance: for $x^k \in {\mathcal{X}_n}^k$, remembering Eq. (4),

$$D(x^k) = \begin{cases} \min\{d(i, j) : i \neq j \in L_T(x^k)\} & \text{if } k \geqslant 2, \\ 0 & \text{if } k = 1, \end{cases}$$

where $d(i, j)$ denotes the minimum distance between i and j, that is,

$$d(i, j) = \min\{(i - j) \bmod n, (j - i) \bmod n\}. \tag{11}$$

Then it is easy to see that

$$D(x^k) \leqslant \lfloor n/k \rfloor \quad \text{for } x^k \in \mathcal{X}_n^k. \tag{12}$$

In fact if $D(x^k) > \lfloor n/k \rfloor$ then any distance of two tokens is greater than n/k then the sum of these distance is greater than n. Now the repetition of a random procedure f implies a stochastic chain $D(f^t(x^k))$ for $t = 0, 1, 2, \ldots$ on $\{0, 1, \ldots, \lfloor n/k \rfloor\}$. Lemma 3.3 will claim the statistical property of $D(f(x^k))$. Defining

$$\tau_k = \max_{x^k \in \mathcal{X}_n^k} \mathbf{E}[T(x^k)], \tag{13}$$

we investigate the expected time that configuration x^k will be legitimate, which is defined by

$$\mathtt{T}_k = \max_{x^k \in \mathcal{X}_n^k} \mathbf{E}\left[\inf\{t \geqslant 0 : f^t(x^k) \in \mathcal{X}_n^1\}\right] = \max_{x^k \in \mathcal{X}_n^k} \mathbf{E}\left[\inf\{t \geqslant 0 : D(f^t(x^k)) = 0\}\right].$$

Noting Item (i) in Remark 2.1, we see that $\mathtt{T}_k$ can be bounded by $\{\tau_k\}_{k=1}^n$ as follows:

Lemma 3.1. *For an odd integer $n \geqslant 3$, assume that there exist $3 \leqslant k \leqslant n$ tokens in an n-ring. Then we have*

$$\mathtt{T}_k \leqslant \sum_{l=1}^{(k-1)/2} \tau_{2l+1}. \tag{14}$$

Proof. Since n is odd, k is also odd by Theorem 2.1. Now suppose that the number of tokens will be k_1 at the first decreasing time $T(x^k)$. Putting $k = k_0$, similarly we suppose that the number of k_i tokens will be k_{i+1} at $T(x^{k_i})$ for $i = 0, \ldots, l$, and $k_{l+1} = 1$. Note that $k = k_0 > k_1 > \cdots > k_l > k_{l+1} = 1$ are well-defined by Item (i) in Remark 2.1. It is clear that k_i depends on x^k for $i = 1, \ldots, l$. By the definition of $\mathtt{T}_k$, we have

$\mathrm{T}_k = \max_{x^k \in \mathcal{X}_n^k} \mathbf{E}[T(x^{k_0}) + T(x^{k_1}) + \cdots + T(x^{k_l})]$. Since k_i is odd for $i = 0, 1, \ldots, l$ and $k_l \geqslant 3$, we obtain

$$\begin{aligned}\mathrm{T}_k &\leqslant \max_{x^k \in \mathcal{X}_n^k} \mathbf{E}[T(x^k)] + \max_{x^{k-2} \in \mathcal{X}_n^{k-2}} \mathbf{E}[T(x^{k-2})] + \cdots + \max_{x^3 \in \mathcal{X}_n^3} \mathbf{E}[T(x^3)] \\ &= \tau_k + \tau_{k-2} + \cdots + \tau_3. \qquad \square\end{aligned}$$

Computing local probability of the position of each token, we will estimate τ_i for $i = 3, 5, \ldots, k$. The movement of each token in the ring is characterized by the following random walks:

Lemma 3.2. *For an odd integer $n \geqslant 3$, assume that there exist $3 \leqslant k \leqslant n$ tokens in an n-ring. Putting each position of k tokens of x^k as*

$$S_0^1, \ldots, S_0^k \in L_T(x^k) \text{ sequentially}, \tag{15}$$

we consider independent k random walks $S_t^1, \ldots, S_t^k$ defined by Eq. (15) *and*

$$\Pr(S_t^l = i + 1 | S_{t-1}^l = i) = 1 - \Pr(S_t^l = i | S_{t-1}^l = i) = r \quad \text{for } l = 1, \ldots, k, \quad 1 \leqslant t \leqslant t^*, \tag{16}$$

where t^* is the first coalescing time of $\{S_t^l\}_{i=1}^k$, that is,

$$t^* = t^*(x^k) = \inf\{t > 0 : S_t^i = S_t^j \quad \text{for some } 1 \leqslant i < j \leqslant k\}. \tag{17}$$

Then the process of the position of tokens is equivalent to the process of $S_t^1, \ldots, S_t^k$ for $0 \leqslant t \leqslant t^* - 1$. Moreover, the distribution for t^* is equivalent to the one of $T(x^k)$ defined by Eq. (10).

Proof. For $x^k = x = (x_0, \ldots, x_{n-1}) \in \mathcal{X}_n^k$, we will show this lemma with either $D(x) \geqslant 2$ or $D(x) = 1$.

Assume that $D(x) \geqslant 2$, that is, if $i \in L_T(x)$ then $i - 1, i + 1 \in L_S(x)$. By the definition of the shift/token, we have that $x_{i-1} = x_i,\ x_{i-2} \neq x_{i-1}$ and $x_i \neq x_{i+1}$. Therefore, we obtain that

$$\begin{aligned}&\Pr(\{i \in L_S(f(x))\} \cap \{i + 1 \in L_T(f(x))\}) \\ &\quad = 1 - \Pr(\{i \in L_T(f(x))\} \cap \{i + 1 \in L_S(f(x))\}) = r\end{aligned}$$

by Eqs. (1) and (2). Hence we see that

$$\Pr(\|f(x)\| = \|x\|) = 1 \quad \text{for } D(x) \geqslant 2, \tag{18}$$

and the local transition probability of the position of the token is equivalent to Eq. (16) for $D(x) \geqslant 2$.

Next suppose that $D(x) = 1$, that is, there exists $2 \leqslant m \leqslant k$ satisfying that

$$i, i + 1, \ldots, i + m - 1 \in L_T(x), i - 1, i + m \in L_S(x).$$

Then we see that $x_{i-1} = x_i = x_{i+1} = \cdots = x_{i+m-1}$ and $x_{i-2} \neq x_{i-1}, x_{i+m-1} \neq x_{i+m}$. Putting $y = (y_0, \ldots, y_{n-1}) = f(x)$, we have that $y_{i-1} \neq y_{i+m}$. On the other hand, assume that continual m particles at time $t - 1$, that is, $S_{t-1}^1 = i, S_{t-1}^2 = i + 1, \ldots, S_{t-1}^m = i + m - 1$, so that we regard these particles as tokens. At the next step, consider that there is a token (resp. shift) if the number of particles of $\{S_t^l\}_{l=1,\ldots,m}$ on each position $i \leqslant j \leqslant i + m$ is one (resp. zero or two). Noting that y_j is a token if $y_{j-1} = y_j$ for $j = i, \ldots, i + m$, we have that the distribution of process for continual m are equivalent to the distribution of $S_t^1, \ldots, S_t^m$ for $0 \leqslant t \leqslant t^* - 1$. It is clear that the equivalence of the law of $T(x)$ and the first collision time $t^*(x)$. $\square$

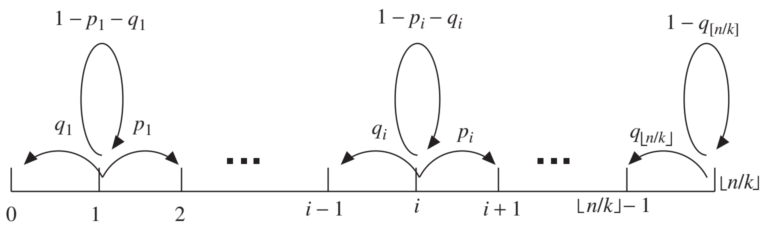

Fig. 1. Illustration of the transition probabilities of $D(f^t(x))$ in Lemma 3.3. Each suffix of the axis denotes not $f^t(x) \in \mathcal{X}_n$ but $D(f^t(x)) \in \{0, 1, \ldots, \lfloor n/k \rfloor\}$. Therefore, for example the probability p_i presents p_x in Lemma 3.3 for some $D(x) = i$. Hence we see that $0 < p_i \leqslant r(1-r) \leqslant q_i < 1$ for $i = 1, \ldots, \lfloor n/k \rfloor$.

By Lemma 3.2 we see that the process of each token is simulated by the random walk defined by Eq. (16). We will give some estimate of the transition probability for $D(f(x))$ as the following lemma:

Lemma 3.3. *For an odd integer $n \geqslant 3$, assume that there exist $3 \leqslant k \leqslant n$ tokens in an n-ring. Then the following statements hold*:

(i) *If a configuration $x \in \mathcal{X}_n^k$ satisfies $D(x) = 1$ then there exist p_x, q_x such that $p_x \leqslant r(1-r) \leqslant q_x < 1 - p_x$ and*

$$\Pr(\{D(f(x)) = 2\} \cap \{\|f(x)\| = k\}) = p_x, \quad \Pr(\|f(x)\| < k) = q_x,$$
$$\Pr(\{D(f(x)) = 1\} \cap \{\|f(x)\| = k\}) = 1 - p_x - q_x.$$

(ii) *If a configuration $x \in \mathcal{X}_n^k$ satisfies $D(x) \geqslant 2$, then $f(x) \in \mathcal{X}_n^k$.*

(a) *If $2 \leqslant D(x) \leqslant \lfloor n/k \rfloor - 1$ then there exist p_x, q_x such that $p_x \leqslant r(1-r) \leqslant q_x < 1 - p_x$ and*

$$\Pr(D(f(x)) = D(x) + 1) = p_x, \ \Pr(D(f(x)) = D(x) - 1) = q_x,$$
$$\Pr(D(f(x)) = D(x)) = 1 - p_x - q_x.$$

(b) *If $D(x) = \lfloor n/k \rfloor \geqslant 2$ then there exists $r(1-r) \leqslant q_x < 1$ such that*

$$\Pr(D(f(x)) = \lfloor n/k \rfloor - 1) = q_x, \quad \Pr(D(f(x)) = \lfloor n/k \rfloor) = 1 - q_x.$$

The rough sketch of estimating transition probabilities in Lemma 3.3 is in Fig. 1.

Proof of Lemma 3.3. Fix $x \in \mathcal{X}_n^k$. By Lemma 3.2, we can regard the process of k tokens as k independent random walks defined by Eqs. (15) and (16). For convenience, we define $L_T^{\min} = L_T^{\min}(x) = \{i \in L_T(x) : i, i+D(x) \in L_T(x)\}$, which is not empty. Noting that $S_0^1, \ldots, S_0^k$ are defined by Eq. (15), we have that

$$\Pr(d(S_0^i, S_0^{i+1}) = D(x)) = 1 \quad \text{for any } i \in L_T^{\min}. \tag{19}$$

By Eq. (16), we see that

$$\Pr(d(S_1^i, S_1^{i+1}) = D(x) - 1) = r(1-r), \quad \Pr(d(S_1^i, S_1^{i+1}) = D(x)) = r^2 + (1-r)^2,$$
$$\Pr(d(S_1^i, S_1^{i+1}) = D(x) + 1) = r(1-r) \quad \text{for any } i \in L_T^{\min}. \tag{20}$$

(i) If $D(x) = 1$, then using Eq. (20) we obtain that

$$p_x = \Pr(\{D(f(x)) = 2\} \cap \{\|f(x)\| = \|x\|\})$$
$$\leqslant \Pr\left(\bigcap_{i \in L_T^{\min}(x)} \{d(S_1^i, S_1^{i+1}) = 2\}\right) \leqslant r(1-r). \tag{21}$$

Moreover, we also have that

$$1 > q_x = \Pr(\|f(x)\| < k) = \Pr\left(\bigcup_{i \in L_T^{\min}(x)} \{d(S_1^i, S_1^{i+1}) = 0\}\right)$$
$$\geqslant r(1-r). \tag{22}$$

The first inequality of Eq. (22) holds, because $\Pr(\|f(x)\| = k) \geqslant \Pr(f(x) = x) > 0$. Hence Item (i) has been proved.

(ii) Since $D(x) \geqslant 2$, Eq. (18) holds. Using Lemma 3.2,

$$\Pr(D(f(x)) = D(x)) + \Pr(D(f(x)) = D(x) + 1) + \Pr(D(f(x)) = D(x) - 1) = 1. \tag{23}$$

(a) $2 \leqslant D(x) \leqslant \lfloor n/k \rfloor - 1$: then we can prove that

$$\Pr(D(f(x)) = D(x) + 1) \leqslant r(1-r) \leqslant \Pr(D(f(x)) = D(x) - 1) < 1, \tag{24}$$

by the same method of Eqs. (21) and (22). Hence by Eq. (23), Item (a) has been proved.

(b) $D(x) = \lfloor n/k \rfloor$: using the same method of Eq. (22), we see that

$$\Pr(D(f(x)) = \lfloor n/k \rfloor - 1) \geqslant r(1-r).$$

Since $D(x) \leqslant \lfloor n/k \rfloor$ for $x \in \mathcal{X}_n$, we have that $\Pr(D(f(x)) = \lfloor n/k \rfloor + 1) = 0$. Hence by Eq. (23), Item (b) has been proved. □

Remark 3.1. There exist an n-ring and a configuration $x \in \mathcal{X}_n$ satisfying that the equality holds in Eqs. (21), (22) and (24), respectively.

We will compare $D(f^t(x^k))$ to the following random walks:

Lemma 3.4. *Consider the following Markov chain X_t on state space $\{0, 1, \ldots, m\}$ with absorbing barrier 0: for $t \geqslant 0$ and $i = 1, \ldots, m-1$*

$$\begin{aligned}&\Pr(X_{t+1} = i \mid X_t = i) = r^2 + (1-r)^2,\\&\Pr(X_{t+1} = i+1 \mid X_t = i) = \Pr(X_{t+1} = i-1 \mid X_t = i) = r(1-r)\end{aligned} \tag{25}$$

and for $t \geqslant 0$

$$\begin{aligned}&\Pr(X_{t+1} = 0 \mid X_t = 0) = 1, \quad \Pr(X_{t+1} = m \mid X_t = m) = 1 - r(1-r),\\&\Pr(X_{t+1} = m-1 \mid X_t = m) = r(1-r).\end{aligned} \tag{26}$$

Then the expected hitting time of the absorbing barrier 0 is

$$\max_{1 \leqslant i \leqslant m} \mathbf{E}[\inf\{t \geqslant 0 : X_t = 0\} \mid X_0 = i] = \mathbf{E}[\inf\{t \geqslant 0 : X_t = 0\} \mid X_0 = m] = \frac{m(m+1)}{2r(1-r)}.$$

Proof. Putting $a_j = \mathbf{E}[\inf\{t \geqslant 0 : X_t = 0\} \mid X_0 = j]$, we have that

$$\begin{cases} a_{j+1} - 2a_j + a_{j-1} = -\dfrac{1}{r(1-r)} & \text{for } j = 1, \ldots, m-1 \\ a_0 = 0, & a_m = a_{m-1} + \dfrac{1}{r(1-r)}. \end{cases}$$

Hence $a_j = a_{j-1} + (m - j + 1)/r(1-r)$ for $j = 1, \ldots, m$. Noting $a_0 = 0$, sum up the equations. We then obtain $a_m = m(m+1)/2r(1-r)$. □

To estimate τ_k, we use the dominating chain X_t in Lemma 3.4 which is defined in the same probability space for $D(f^t(x^k))$.

Lemma 3.5. *For an odd integer $n \geqslant 3$, assume that there exist k tokens for $3 \leqslant k \leqslant n$ in an n-ring. Then we have $\tau_k \leqslant n^2/r(1-r)k^2$.*

Proof. Putting $m = \lfloor n/k \rfloor$ in Lemma 3.4, we define the stochastic process X_t satisfying $X_0 = D(f^0(x^k))$ and Eqs. (25), (26), which is defined on the state space $\{0, \ldots, \lfloor n/k \rfloor\}$. Then we see that $D(f^t(x^k))$ is stochastically smaller than X_t, that is, $\Pr(D(f^t(x^k)) > a) \leqslant \Pr(X_t > a)$ for any real number a (see [18, Chapter IV]). Therefore, putting $T_X = \inf\{t > 0 : X_t = 0\}$, we have

$$\tau_k \leqslant \mathbf{E}[T_X | X_0 = \lfloor n/k \rfloor] = \frac{\lfloor n/k \rfloor(\lfloor n/k \rfloor + 1)}{2r(1-r)} \leqslant \frac{1}{r(1-r)} \left(\frac{n}{k}\right)^2,$$

since $\lfloor n/k \rfloor \geqslant 1$. $\square$

Proof of Theorem 3.1. By Eq. (14) and Lemma 3.5

$$\mathrm{T}_k \leqslant \frac{n^2}{r(1-r)} \left(\frac{1}{3^2} + \frac{1}{5^2} + \cdots + \frac{1}{k^2}\right) < \frac{\pi^2 - 8}{8r(1-r)} n^2 \quad \text{for any } k = 3, 5, \ldots, n. \tag{27}$$

In fact the last inequality of Eq. (27) holds because it is well-known that

$$\sum_{j=0}^{\infty} \frac{1}{(2j+1)^2} = \frac{\pi^2}{8}$$

(see e.g. [15]).

On the other hand, for a sufficiently large n, consider the token $x = (x_0, \ldots, x_{n-1}) \in \mathcal{X}_n^3$ with $\{0, \lfloor n/6 \rfloor, \lfloor n/2 \rfloor\} = L_T(x)$. Now set random walks S_t^1, S_t^2, S_t^3 with initial positions $S_0^1 = x_0,\ S_0^2 = x_{\lfloor n/6 \rfloor},\ S_0^3 = x_{\lfloor n/2 \rfloor}$, and transition probabilities satisfying Eq. (16), respectively. We see that $D(x) = d(S_0^1, S_0^2) = \lfloor n/6 \rfloor$. Moreover, $D(f^t(x)) = d(S_t^1, S_t^2)$ for $t \in \{t : d(S_t^1, S_t^2) \leqslant \lfloor n/3 \rfloor\}$. Until the time, we have

$$\Pr(D(f^t(x)) = D(f^{t-1}(x)) + 1) = \Pr(D(f^t(x)) = D(f^{t-1}(x)) - 1) = r(1-r),$$
$$\Pr(D(f^t(x)) = D(f^{t-1}(x))) = r^2 + (1-r)^2.$$

Remembering $T(x)$ as Eq. (10), we have $\mathbf{E}[T(x)] \geqslant \mathbf{E}[T_* | D(x) = \lfloor n/6 \rfloor]$, where $T_* = \inf\{t > 0 : D(f^t(x)) \in \{0, \lfloor n/3 \rfloor\}\}$. Now put $b_i = \mathbf{E}[T_* | D(x) = i]$, $(i = 0, \ldots, \lfloor n/3 \rfloor)$. Then the following difference equation holds: $b_i = \{r^2 + (1-r)^2\} b_i + r(1-r) b_{i+1} + r(1-r) b_{i-1} + 1$ for $i = 1, \ldots, \lfloor n/3 \rfloor - 1$ with boundary conditions $b_0 = b_{\lfloor n/3 \rfloor} = 0$. It is easy to get the solution $b_i = i(\lfloor n/3 \rfloor - i)/\{2r(1-r)\}$ for $i = 0, \ldots, \lfloor n/3 \rfloor$. Therefore, we see that $b_{\lfloor n/6 \rfloor} \geqslant n^2/\{100r(1-r)\}$, so that $\mathrm{T}_3 \geqslant \mathbf{E}[T(x)] \geqslant n^2/\{100r(1-r)\}$. Hence we have Eq. (9). $\square$

Remark 3.2. By the proof of Eq. (9), we see that a few tokens with long distances make the expected time large.

4. Concluding remarks

We proved that the maximal expected time of Herman's self-stabilizing algorithm is less than $((\pi^2 - 8)/8r(1-r))n^2$. Especially if $r = \frac{1}{2}$ it is bounded by $0.936n^2$. However, we do not know that whether $r = \frac{1}{2}$ is optimal, which is a future work. It would also be of future interest to apply our argument to general connected graphs.

Moreover, note that recently Fribourg et al. [11] characterized Herman's algorithm with Gibbs fields. We should study the self-stabilization at the viewpoint of statistical physics.

Acknowledgements

The author would like to thank the anonymous referees for helpful comments. This work was supported by Grant-in-Aid for Young Scientists (B) No. 14740077 from MEXT Japan.

References

[1] I. Adler, H. Ahn, R. Karp, S. Ross, Coalescing times for IID random variables with applications to population biology, Random Struct. Alg. 23 (2) (2003) 155–166.

[2] D. Aldous, J.A. Fill, Reversible Markov chains and random walk on graphs, monograph in preparation, <http://www.stat.berkeley.edu/users/aldous/RWG/book.html>.
[3] J. Beauquier, S. Delaët, Probabilistic self-stabilizing mutual exclusion in uniform rings, Proc. of PDOC, Vol. 9 (1994) 378.
[4] R. Brightwell, P. Winkler, Maximal hitting time for random walks on graphs, Random Struct. Alg. 1 (1990) 263–275.
[5] R. Bubley, M. Dyer, Path coupling: a technique for proving rapid mixing in Markov chains, Proc. 38th Annual IEEE Symposium on Foundations of Computer Science, 1997, 223–231.
[6] D. Coppersmith, P. Tetali, P. Winkler, Collisions among random walks on a graph, SIAM J. Discrete Math. 6 (3) (1993) 363–374.
[7] E. Dijkstra, Self-stabilizing system in spite of distributed control, Comm. ACM 17 (11) (1974) 643–644.
[8] S. Dolev, Self-Stabilization, MIT Press, Cambridge, MA, 2000.
[9] M. Dyer, L. Goldberg, C. Greenhill, G. Istrate, M. Jerrum, Convergence of the iterated prisoner's dilemma game, Combinatorics, Probab. Comput. 11 (2002) 135–147.
[10] M. Dyer, C. Greenhill, A more rapidly mixing Markov chain for graph colorings, Random Struct. Alg. 13 (1998) 285–317.
[11] L. Fribourg, S. Messika, C. Picaronny, Trace of randomized distributed algorithms as Gibbs fields, Research Report LSV-02-12, September 2002, Lab. Spéc. et. Vér, CNRS & ENS de Cachan, France.
[12] L. Fribourg, S. Messika, C. Picaronny, Coupling and self-stabilization, in: Proc. 18th Internat Conf. on Distributed Computing (DISC 2004), Amsterdam, NL, October 2004, Lecture Notes in Computer Science, Vol. 3274, Springer, Berlin, 2004, pp. 201–215.
[13] Y. Hassin, D. Peleg, Distributed probabilistic polling and applications to proportionate agreement, Inform. and Comput. 171 (2) (2001) 248–268.
[14] T. Herman, Probabilistic self-stabilization, Inform. Proc. Lett. 35 (1990) 63–67.
[15] J. Hofbauer, A simple proof of $1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}$ and related identities, Amer. Math. Monthly 109 (2002) 196–200.
[16] A. Israeli, M. Jalfon, Token management schemes and random walks yield self stabilizing mutual exclusion, Proc. PDOC, Vol. 9, 1990, pp. 119–130.
[17] L. Lamport, Solved problems, unsolved problems and non-problems in concurrency, Proc. PDOC, 1984, pp. 1–11.
[18] T. Lindvall, Lectures on the Coupling Method, Wiley, New York, 1992.
[19] P. Tetali, P. Winkler, Simultaneous reversible Markov chains, Combinatorics: Paul Erdös is Eighty, Vol. 1, Bolyai Society for Mathematical Studies, 1993, pp. 433–451.