Noname manuscript No.
(will be inserted by the editor)

A Nearly Optimal Upper Bound for the Self-Stabilization Time in Herman's Algorithm

Yuan Feng · Lijun Zhang

Received: date / Accepted: date

Abstract Self-stabilization algorithms are very important in designing fault-tolerant distributed systems. In this paper we consider Herman's self-stabilization algorithm and study its expected termination time. McIver and Morgan have conjectured the optimal upper bound being $0.148N^2$, where N denotes the number of processors. We present an elementary proof showing a bound of $0.167N^2$, a sharp improvement compared with the best known bound $0.521N^2$. Our proof is inspired by McIver and Morgan's approach: we find a nearly optimal closed form of the expected stabilization time for any initial configuration, and apply the Lagrange multipliers method to give an upper bound.

Keywords Herman's algorithm · Self-stabilization

1 Introduction

In [2], Dijkstra proposed the influential notion of self-stabilization algorithms for designing fault-tolerant distributed systems. A distributed system is self-stabilizing if it will always reach *legitimate* configurations, no matter where the system starts. The system thus can recover from any transient error such as local corrupted states. The concept has many applications in the network protocol, and thus has received much attention. See for example [15,3] for surveys on this topic.

Dijkstra assumed that all participating processors are identical except for a single processor which is necessary for breaking the symmetry. It was already shown by Dijkstra in 1974 that no deterministic scheduler exists which guarantees self-stabilization if all processors are identical. On the other side, Herman proposed a randomized program in [8] to break the symmetry: he proposed a self-stabilizing mutual exclusion algorithm, today known as Herman's algorithm, which stabilizes within finite steps with probability 1.

The protocol is designed for a *token ring* of N synchronous processors. Each processor may or may not have a token, and in a legitimate configuration only a single token exists. For any finite N, the protocol can be viewed as a finite state Markov chain with a single bottom strongly connected component (SCC) consisting of all legitimate configurations. So a legitimate configuration is reached with probability 1, regardless of the initial configuration. Hence, Herman's protocol is *self-stabilizing*.

Another important performance measure in designing self-stabilization protocols is the stabilization time which is the expected time until a legitimate configuration is reached. In Herman's original work [8], an upper bound $O(N^2\lceil\log N\rceil)$ for stabilization time has been established, while in 2005, several groups of researchers [7,13,14] gave an upper bound of $O(N^2)$, independently. Moreover, McIver and Morgan [13] proved that the stabilization time is actually $\Theta(N^2)$, meaning that the lower bound and the upper bound coincide. They also provided an *exact* formula for the expected stabilization time for configurations with three tokens.

One may expect that the story should end here from the viewpoint of complexity theory, as we already have the asymptotically tight bound for the stabilization time. However, McIver and Morgan [13] conjec-

Y. Feng
Centre for Quantum Computation and Intelligent Systems, University of Technology Sydney, Australia
AMSS-UTS Joint Research Laboratory for Quantum Computation, Chinese Academy of Sciences
E-mail: Yuan.Feng@uts.edu.au

L. Zhang
State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences
E-mail: zhanglj@ios.ac.cn

tured that the optimal upper bound for general configurations is $\frac{4}{27}N^2 \approx 0.148N^2$, which is obtained by equidistant three-token configurations when N is divisible by 3. This conjecture, simple and elegant, is indeed very difficult to prove. In recent years, it has attracted much attention to improve the bound towards this conjecture: Kiefer *et al.* [10] proved a bound of $0.64N^2$, and the authors of this paper further improved it to $0.521N^2$ [5], by simply exploiting the precise solution for the three-token configurations derived in [13].

In this paper, we follow this research line by proving an upper bound of $\frac{1}{6}N^2$, approximately $0.167N^2$, for arbitrary configurations. Our bound is very close to the conjectured optimal bound, with a gap of $0.019N^2$. It is worth noting that our approach is completely elementary: for each initial configuration, we found a closed-form upper bound for the expected stabilization time, inspired by the three-token formula given by McIver and Morgan. This bound, referred to as F, is a homogeneous polynomial of degree 3 over the gap vector of the initial configuration. Our result then follows by obtaining the maximum of the upper bounds over all initial configurations, using the Lagrange multipliers method. Furthermore, we show that our bound can be further improved by subtracting from F a higher-degree polynomial of token gaps. However, it still seems very difficult to finally approach the conjectured bound, as the improved upper bound is complicated, and its maximum value is difficult to determine.

Interestingly, our technique can be used to prove a similar result for a variant of Herman's original algorithm: here the initial configurations have *even* numbers of tokens, and the empty configuration without any token left is referred to as legitimate. In this case we prove that for all initial configurations, the expected stabilization time is bounded by $\frac{1}{2}N^2$, which is obtained by equidistant two-token configurations (provided that N is divisible by 2).

We note that systems of interacting and annihilating particles, either on a circle or on a line, have been heavily studied in areas including physics, combinatorics and neural networks [12]. Most of them focus on exploring the precise solutions, for example Balding [1] gave generating functions for the number of remaining particles at time t, and these results were transferred in [10] to Herman's setting. However, such expressions are in general very complicated and difficult to analyze, see [1,4,10]. In contrast, our proof in this paper exploits mostly elementary concepts, and it is much simpler than previous techniques for analyzing Herman's algorithm [7,10]. Because of this, we are optimistic that our approach might provide alternative ways to improve worst-case analysis of such particle systems.

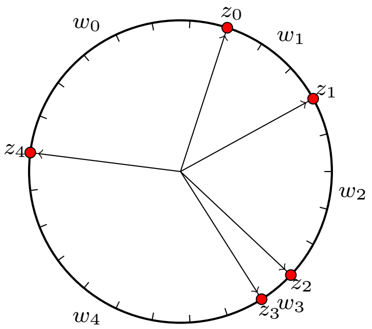

Fig. 1 A configuration with $M = 5$, $N = 25$.

This paper is an extended version of the conference paper [6]. In addition to the conference version, we provide here a better upper bound for any given configuration, and discuss the possibility and difficulty of finally proving the conjecture using our techniques. In addition, we show a tight upper bound of the expected stabilization time for a variant of Herman's algorithm when the initial configuration has an even number of tokens.

Related Work. In [10], an asynchronous variant of Herman's protocol was studied. Recently, [9] has studied the distribution of the self-stabilization time for $M = 3$ and shown that for an arbitrary t the probability of stabilization within time t is minimized under the equidistant configuration with $M = 3$. On the practical side, using the probabilistic model checker PRISM [11], McIver and Morgan's conjecture was validated for all rings with the size $N \leq 21$ that can be exhaustively analyzed.

2 Preliminaries

We assume to have N processors numbered from 0 to $N-1$, clockwise, organized in a ring topology. Each processor may or may not have a token. A configuration with $0 < M \leq N$ tokens, M is odd, is a strictly increasing mapping $z : \{0, \ldots, M-1\} \to \{0, \ldots, N-1\}$ such that $z(0) < \cdots < z(M-1)$. For all $i \in \{0, \ldots, M-1\}$, the processor $z(i)$ has a token. We fix the ring size N throughout this paper. An example configuration with $M = 5$ and $N = 25$ is given in Figure 1.

Herman's protocol [8] works as follows: in each time step, each processor with a token either passes its token to its clockwise neighbor with probability $\frac{1}{2}$, or keeps it with probability $\frac{1}{2}$. If a processor keeps its token and receives another one from its counterclockwise neighbor, then both of those tokens are annihilated. We refer to configurations with only one token as *legitimate* configurations. The protocol can also be viewed as a finite state Markov chain. It is easy to see that in this Markov chain there is a single bottom SCC consisting of all legitimate configurations. Thus this SCC is reached with probability 1, regardless of the initial configuration. It follows then that Herman's protocol is *self-stabilizing.*

Let S_M be the set of configurations with the number of tokens not exceeding M. Let $P_M : S_M \times S_M \to [0,1]$ be the probabilistic transition matrix between configurations in S_M, and $\mathbb{E}_M : S_M \to [0,\infty)$ the function of expected stabilization time. The following lemma from [13], slightly modified with respect to our notations, is crucial for our discussion.

Lemma 1 *[13, Lemmas 1 and 5] Let $M \geq 1$ and $v : S_M \to [0,\infty)$ be a mapping such that $v(z) = 0$ whenever $z \in S_1$ is a legitimate configuration. Suppose*

$$(P_M \cdot v)(z) \leq v(z) - 1 \tag{1}$$

for any illegitimate configuration z, where $P_M \cdot v$ is the mapping from S_M to $[0,\infty)$ such that

$$(P_M \cdot v)(z) = \sum_{y \in S_M} P_M(z,y)v(y).$$

Then $\mathbb{E}_M(z) \leq v(z)$ for all $z \in S_M$. In particular, if the equality holds in Eqn.(1), then $\mathbb{E}_M(z) = v(z)$ for all $z \in S_M$.

Note that Lemma 1 essentially follows from the fact that the least fixed point of a monotone function is the supremum of the pre-fixed points. Employing Lemma 1, McIver and Morgan were able to find a closed form for $\mathbb{E}_M$ when $M = 3$. To present their result, we need a further definition.

Definition 1 (Gap Vector) Let $M \geq 3$ and $z \in S_M \backslash S_{M-2}$, i.e., z has exactly M tokens. We define the associated *gap vector* $w = \langle w_0, w_1, \ldots, w_{M-1}\rangle$ of z, where w_i is the gap between the tokens $z(i-1)$ and $z(i)$; that is, $w_i := z(i) - z(i-1)$ for $i = 1, \ldots, M-1$, and $w_0 = N - \sum_{i=1}^{M-1} w_i$. We denote by $\mathcal{G}_M$, $M \geq 3$, the set of gap vectors corresponding to configurations from S_M, and set $\mathcal{G}_1 = \{\langle N \rangle\}$.

Obviously, configurations with the same gap vector have the same expected stabilization time. In other words, the value $\mathbb{E}_M(z)$ depends only on the gap vector w associated with z.

Lemma 2 *[13, Lemma 7] For any $z \in S_3$, let $w = \langle w_0, w_1, w_2\rangle$ be the gap vector of z. Then*

$$\mathbb{E}_3(z) = 4w_0w_1w_2/N.$$

In this paper, we will exploit the potential of Lemma 1 to give a (nearly optimal) bound on $\mathbb{E}_M$ for the general case $M \geq 3$.

3 Our Main Result

To simplify notation, we sometimes extend gap vectors, which have finite dimension, to infinite ones by appending 0 entries. That is, we let $w_i = 0$ for all $i \geq M$ if w is a gap vector of dimension M. The following definition is crucial.

Definition 2 Let $\mathcal{G} = \bigcup_{M=1, M \text{ is odd}}^{N} \mathcal{G}_M$ and $F : \mathcal{G} \to [0,\infty)$ be a mapping defined by

$$F(\langle w_0, w_1, \cdots, w_{M-1}\rangle) = \sum_{i=0}^{\infty} w_i \cdot \left[\sum_{j=0}^{\infty} w_{i+2j+1} \cdot \left(\sum_{k=0}^{\infty} w_{i+2j+2k+2}\right)\right]. \tag{2}$$

With this definition, we can now state the main result of this paper.

Theorem 1 *For any odd number $M \geq 3$ and any $z \in S_M$ with the associated gap vector w,*

$$\mathbb{E}_M(z) \leq \frac{4}{N} F(w). \tag{3}$$

We can further apply the Lagrange multipliers method to compute the maximal value of $F(w)$ for each $M \leq N$, which provides a better upper bound $\frac{1}{6}N^2 = 0.167N^2$, compared to the previous best bound $0.521N^2$ [5], of the expected self-stabilization time for arbitrary initial configurations (cf. Theorem 2).

The proof of Theorem 1 will be presented in the next section. But first, we apply it for some small values of M.

- $M = 3$. In this case, $F(\langle w_0, w_1, w_2\rangle) = w_0w_1w_2$, and Eqn. (3) agrees with the precise bound in Lemma 2.
- $M = 5$. Then $F(w)$ equals the sum of all the products of three *neighboring gaps*:

$$F(\langle w_0, w_1, w_2, w_3, w_4\rangle) = w_0w_1w_2 + w_1w_2w_3 + w_2w_3w_4 + w_3w_4w_0 + w_4w_0w_1. \tag{4}$$

- $M = 7$. In this case, $F(w)$ is slightly involved: It contains the sum of all the products of three neighboring gaps, and in addition it contains products of gaps of the form $w_iw_{i+3}w_{i+4}$. Here if we assume all arithmetic operations over the index set $\{0, \ldots, 6\}$ are understood as modulo 7, then

$$F(\langle w_0, w_1, w_2, w_3, w_4, w_5, w_6\rangle) = \sum_{i=0}^{6} w_iw_{i+1}w_{i+2} + \sum_{i=0}^{6} w_iw_{i+3}w_{i+4}.$$

- The explicit expression for $M > 7$ is more involved. It is still the sum of some products of three (not necessarily neighboring) gaps, but the pattern becomes more and more complicated. For example, products of the form $w_i w_{i+\frac{N}{3}} w_{i+\frac{2N}{3}}$ will be needed for those N which are multiples of 3.

To conclude this section, we introduce some notations.

Definition 3 For any configuration $z \in S_M$, we denote by $O(z)$ the *bag* of next-step configurations obtained from z; that is,

$$O(z) = \{y \in S_M : P_M(z, y) > 0\}.$$

Let $O_g(z)$ be the bag of gap vectors for $O(z)$; that is

$$O_g(z) = \{w : w \text{ is the gap vector for some } y \in O(z)\}.$$

Here by bag we mean a multiset where an element can appear more than once. For simplicity, we use the set notation $\{\cdot\}$ to denote bags as well.

Actually, $O_g(z)$ is almost an ordinary set except that the gap vector associated to z occurs twice, one corresponding to the case where all tokens move, and the other where no token moves.

Note that in our setting, for each $z \in S_M \backslash S_{M-2}$, $M \geq 3$, and $y \in O(z)$, the probability $P_M(z, y)$ is always $\frac{1}{2^M}$. Let F^g_M be the function obtained by composing F with the gap function, restricting on the set of M-token configurations; that is, for any $z \in S_M \backslash S_{M-2}$, $F^g_M(z) = F(w)$ where w is the gap vector of z. Then

$$\begin{aligned}(P_M \cdot \frac{4}{N} F^g_M)(z) &= \frac{4}{2^M N} \sum_{y \in O(z)} F^g_M(y) \\ &= \frac{4}{2^M N} \sum_{v \in O_g(z)} F(v).\end{aligned}$$

The proof of our main theorem will exploit the form of F to derive a closed form for the sum $\sum_{v \in O_g(z)} F(v)$, which is the most challenging part. With that we will be able to show

$$(P_M \cdot \frac{4}{N} F^g_M)(z) \leq \frac{4}{N} F^g_M(z) - 1$$

for all illegitimate configuration z, and the main theorem follows from Lemma 1.

4 Proof of the Main Theorem

4.1 The 5-token Case

To illustrate our basic ideas, let us first consider the case of 5 tokens. The function F is given in Eqn.(4), which has the following obvious properties:

- F is *rotationally symmetric*, i.e.,

  $$F(\langle w_0, w_1, w_2, w_3, w_4 \rangle) = F(\langle w_1, w_2, w_3, w_4, w_0 \rangle).$$

- F is in *harmony* for smaller $M < 5$, i.e., assuming $w_1 = 0$,

  $$F(\langle w_0, w_1, w_2, w_3, w_4 \rangle) = F(\langle w_0 + w_2, w_3, w_4 \rangle).$$

  Thus, we can freely use the 5-token formula for all 3-token configurations as well. For this reason, we will not distinguish a 5-dimensional integer vector with some of the elements being 0 with the 3-token or 1-token configuration it really represents.

We define the one-step *gap increment vectors* for a 5-token configuration as follows.

1. Let $\Delta_1 = \langle 1, -1, 0, 0, 0 \rangle$, which corresponds to the first token passing while the others remain. Obviously, the cases where a single token passes while the others remain can be obtained by post-multiplying Per^i to Δ_1, where $i \in \{0, 1, 2, 3, 4\}$ and

   $$Per = \begin{pmatrix} 0\,0\,0\,0\,1 \\ 1\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0 \\ 0\,0\,1\,0\,0 \\ 0\,0\,0\,1\,0 \end{pmatrix}$$

   is the basic cyclic permutation matrix.
2. Let $\Delta_{2,1} = \langle 1, 0, -1, 0, 0 \rangle$ correspond to the first two tokens passing while the others remain, and $\Delta_{2,2} = \langle 1, -1, 1, -1, 0 \rangle$, corresponding to the first and the third tokens passing while the others remain. Other cases where exactly 2 tokens passing can be obtained by post-multiplying the cyclic permutation matrices to either $\Delta_{2,1}$ or $\Delta_{2,2}$.
3. Let $\Delta_0 = \langle 0, 0, 0, 0, 0 \rangle$ correspond to the cases where no token moves or all tokens move.

Observe that the case of exactly 3 tokens passing is equivalent to exactly 2 passing, but in the opposite direction. Similar correspondences hold for exactly 1 or 4 tokens passing. Thus all the possible outcomes of a single step starting from an illegitimate configuration $z \in S_5$ with the gap vector $w = (w_0, \cdots, w_4)$ constitute the set

$$\begin{aligned}O_g(z) = \{w \pm \Delta_0, w \pm \Delta_1 \cdot Per^i, w \pm \Delta_{2,1} \cdot Per^i,& \\ w \pm \Delta_{2,2} \cdot Per^i : i = 0, 1, 2, 3, 4\}&\end{aligned}$$

where each element occurs with probability 1/32 (here we recall $O_g(z)$ is a bag, and $w + \Delta_0 = w - \Delta_0$). Since $F(v)$ is in harmony, in case some gaps in $v \in O_g(z)$ are equal to 0, which corresponds to a 3- or 1-token configuration, we can still use the 5-token formula.

To calculate the value $\sum_{v\in O_g(z)} F(v)$, we let

$$\Box_1^i := F(w+\mathit{\Delta}_1\cdot Per^i)+F(w-\mathit{\Delta}_1\cdot Per^i)$$

for $i=0,1,2,3,4$, and $\Box_{2,1}^i$ and $\Box_{2,2}^i$ be defined similarly. Using the identity

$$(w_0+1)(w_1-1)w_2+(w_0-1)(w_1+1)w_2 = 2w_0w_1w_2-2w_2,$$

we derive that $\Box_1^0 = 2F(w)-2w_2-2w_4$. Moreover, as $F(w)$ is rotationally symmetric, and $\sum_{i=0}^4 w_i = N$, we derive $\sum_{i=0}^4 \Box_1^i = 10F(w)-4N$. In a similar way, we have $\Box_{2,1}^0 = 2F(w)-2w_1$ and $\sum_{i=0}^4 \Box_{2,1}^i = 10F(w)-2N$. The case for $\mathit{\Delta}_{2,2}$ is slightly complicated: the sum $\Box_{2,2}^0$ can be first simplified to

$$\begin{aligned}&(w_1-1)(w_2+1)(w_0+w_3)+(w_2+1)(w_3-1)w_4\\ &\qquad+(w_3-1)w_4(w_0+1)+w_4(w_0+1)(w_1-1)+\\ &(w_1+1)(w_2-1)(w_0+w_3)+(w_2-1)(w_3+1)w_4\\ &\qquad+(w_3+1)w_4(w_0-1)+w_4(w_0-1)(w_1+1)\end{aligned}$$

Thus $\Box_{2,2}^0 = 2F(w)-2(w_0+w_3)-6w_4$, and $\sum_{i=0}^4 \Box_{2,2}^i = 10F(w)-10N$. Finally, noting $F(w+\mathit{\Delta}_0) = F(w-\mathit{\Delta}_0) = F(w)$, we have $\sum_{v\in O_g(z)} F(v) = 32F(w)-16N$. Thus

$$\begin{aligned}(P_5\cdot\frac{4}{N}F_5^g)(z) &= \frac{4}{32N}(32F(w)-16N)\\ &= \frac{4}{N}F(w)-2 \le \frac{4}{N}F_5^g(z)-1,\end{aligned}$$

and Lemma 1 implies $\mathbb{E}_5(z) \le \frac{4}{N}\cdot F_5^g(z)$. Using Lagrange multipliers method (cf. Theorem 2), we have then

$$\mathbb{E}_5(z) \le \frac{4}{N}\cdot\frac{1}{25}N^3 = \frac{4}{25}N^2 = 0.16N^2.$$

4.2 Properties of the Function F

For $M=5$, we have seen that F is rotationally symmetric and in harmony for smaller values of M. Below we generalize these two properties for arbitrary M.

Lemma 3 *[Rotational Symmetry] The function F is rotationally symmetric. That is, for any odd number $M\ge 3$,*

$$F(\langle w_0,w_1,\cdots,w_{M-1}\rangle) = F(\langle w_1,\cdots,w_{M-1},w_0\rangle).$$

Proof To simplify notation, let $w=\langle w_0,w_1,\cdots,w_{M-1}\rangle$ and $w'=\langle w_1,w_2,\cdots,w_{M-1},w_0\rangle$. We need to prove $F(w)=F(w')$. Note that by Eqn.(2),

$$\begin{aligned}F(w) &= \sum_{i=0}^{M-3} w_i \sum_{j=0}^{\infty} w_{i+2j+1} \sum_{k=0}^{\infty} w_{i+2j+2k+2}\\ &= \sum_{i=0}^{M-3} w_i \sum_{j=0}^{\lfloor (M-3-i)/2\rfloor} w_{i+2j+1}\cdot\\ &\qquad \sum_{k=0}^{\lfloor (M-3-i-2j)/2\rfloor} w_{i+2j+2k+2}.\end{aligned}$$

The proof idea is to divide the sum above into two parts, for even and odd indices, respectively. Then we can see the relation of $F(w)$ and $F(w')$ by shifting the indices. For this purpose, we denote by

$$\begin{aligned}\mathit{\Sigma}_1(w) := \sum_{n=1}^{(M-3)/2} w_{2n-1} \sum_{j=0}^{(M-3-2n)/2} w_{2n+2j}\cdot\\ \sum_{k=0}^{(M-3-2n-2j)/2} w_{2n+2j+2k+1}\end{aligned}\qquad(5)$$

$$\begin{aligned}\mathit{\Sigma}_2(w) := \sum_{n=0}^{(M-3)/2} w_{2n} \sum_{j=0}^{(M-3-2n)/2} w_{2n+2j+1}\cdot\\ \sum_{k=0}^{(M-3-2n-2j)/2} w_{2n+2j+2k+2}.\end{aligned}\qquad(6)$$

Then $F(w) = \mathit{\Sigma}_1(w)+\mathit{\Sigma}_2(w)$. Note that $M-1$ is an even number, and w'_i equals w_{i+1} if $i<M-1$, and equals w_0 if $i=M-1$. For the gap vector w', we calculate that

$$\begin{aligned}\mathit{\Sigma}_1(w') &= \sum_{n=1}^{(M-3)/2} w_{2n} \sum_{j=0}^{(M-3-2n)/2} w_{2n+2j+1}\cdot\\ &\qquad \sum_{k=0}^{(M-3-2n-2j)/2} w_{2n+2j+2k+2}\\ &= \mathit{\Sigma}_2(w) - w_0 \sum_{j=0}^{(M-3)/2} w_{2j+1} \sum_{k=0}^{(M-3-2j)/2} w_{2j+2k+2}\ .\end{aligned}$$

The most involved part is the sum $\mathit{\Sigma}_2(w')$. Note that $k=(M-3-2n-2j)/2$ implies $w'_{2n+2j+2k+2}=w'_{M-1}$. Isolating the term of w'_{M-1} from the last part of $\mathit{\Sigma}_2(w')$, we derive:

$$\begin{aligned}\mathit{\Sigma}_2(w') &= \sum_{n=0}^{(M-5)/2} w'_{2n} \sum_{j=0}^{(M-5-2n)/2} w'_{2n+2j+1}\cdot\\ &\qquad \sum_{k=0}^{(M-5-2n-2j)/2} w'_{2n+2j+2k+2}\\ &\quad+ \sum_{n=0}^{(M-3)/2} w'_{2n} \sum_{j=0}^{(M-3-2n)/2} w'_{2n+2j+1}\cdot w'_{M-1}.\end{aligned}$$

Some subtle simplifications have been used above: when $n = (M-3)/2$, it holds that $(M-3-2n)/2 = 0$; while when $j = (M-3-2n)/2$, $(M-3-2n-2j)/2 = 0$. Thus the corresponding term $w'_{M-3}w'_{M-2}w'_{M-1}$ appears in the sum at the last line. Now we can further rewrite $\Sigma_2(w')$ by:

$$\begin{aligned}\Sigma_2(w') = &\sum_{n=1}^{(M-3)/2} w_{2n-1} \sum_{j=0}^{(M-3-2n)/2} w_{2n+2j} \cdot \\ &\qquad \sum_{k=0}^{(M-3-2n-2j)/2} w_{2n+2j+2k+1} \\ &+ \; w_0 \sum_{n=0}^{(M-3)/2} w_{2n+1} \sum_{j=0}^{(M-3-2n)/2} w_{2n+2j+2} \\ &= \Sigma_1(w) + w_0 \sum_{j=0}^{(M-3)/2} w_{2j+1} \sum_{k=0}^{(M-3-2j)/2} w_{2j+2k+2}.\end{aligned}$$

Thus we have $F(w') = \Sigma_1(w') + \Sigma_2(w') = \Sigma_1(w) + \Sigma_2(w) = F(w)$. □

Remark 1 We could also define the function F in Definition 2 in a rotationally symmetric way directly by, say, letting the arithmetic operations over indices be modulo M. This would save our efforts to prove Lemma 3. However, we decided to adopt the current definition for the following two reasons:

1. This definition makes the proof of Lemma 4 easier to follow;
2. The generating set $C(M)$ of the gap increment vectors in the next section is constructed inductively (Proposition 1), which is in accordance with the current definition of F, and makes the proof of the main theorem easy to follow as well.

The following lemma shows that the definition of F is in harmony for arbitrary M.

Lemma 4 *For any odd number $M \geq 3$, if $w_1 = 0$ then*

$$F(\langle w_0, w_1, w_2, \cdots, w_{M-1}\rangle) = F(\langle w_0 + w_2, \cdots, w_{M-1}\rangle).$$

Proof The equality is obtained by directly expanding both sides according to Eqn.(2), by noting that $w_1 = 0$:

$$\begin{aligned}&F(\langle w_0, w_1, w_2, \cdots, w_{M-1}\rangle) \\ &= \sum_{i=0}^{\infty} w_i \cdot \left[\sum_{j=0}^{\infty} w_{i+2j+1} \cdot \left(\sum_{k=0}^{\infty} w_{i+2j+2k+2}\right)\right] \\ &= w_0 \cdot \left[\sum_{j=0}^{\infty} w_{2j+1} \cdot \left(\sum_{k=0}^{\infty} w_{2j+2k+2}\right)\right] \\ &\qquad + w_2 \cdot \left[\sum_{j=0}^{\infty} w_{2j+3} \cdot \left(\sum_{k=0}^{\infty} w_{2j+2k+4}\right)\right] \\ &\qquad + \sum_{i=3}^{\infty} w_i \cdot \left[\sum_{j=0}^{\infty} w_{i+2j+1} \cdot \left(\sum_{k=0}^{\infty} w_{i+2j+2k+2}\right)\right] \\ &= (w_0 + w_2) \cdot \left[\sum_{j=0}^{\infty} w_{2j+3} \cdot \left(\sum_{k=0}^{\infty} w_{2j+2k+4}\right)\right] \\ &\qquad + \sum_{i=3}^{\infty} w_i \cdot \left[\sum_{j=0}^{\infty} w_{i+2j+1} \cdot \left(\sum_{k=0}^{\infty} w_{i+2j+2k+2}\right)\right] \\ &= F(\langle w_0 + w_2, w_3, \cdots, w_{M-1}\rangle).\end{aligned}$$

□

As the function F is rotationally symmetric, the above lemma indeed shows that *any* 0 entry in the gap vector can be absorbed, without affecting the value of the F function.

4.3 Gap Increment Vectors

In this section, we characterize the vectors in $O_g(z)$ with the help of gap increment vectors.

Definition 4 (Gap Increment Vector) Let z be a configuration with w its associated gap vector. The vectors $\Delta := w' - w$, where $w' \in O_g(z)$, are called the *gap increment vector* for z.

Moreover, as seen in the 5-token case, the set of gap increment vectors consists of pairs of *symmetric* ones:

Lemma 5 *For any gap vector w, Δ is a gap increment vector if and only if $-\Delta$ is a gap increment vector.*

Proof By definition, $w' := w + \Delta \in O_g(z)$. The gap vector w' is obtained from w by moving a set A of tokens forward. By symmetry, the vector $w - \Delta$ is obtained if all tokens in A stay, but other tokens move forward. □

In virtue of Lemma 5, we can find a set $C(M)$, in which every vector has first entry either 0 or 1, such that for each $z \in S_M \backslash S_{M-2}$,

$$O_g(z) = \{w \pm \varDelta : \varDelta \in C(M)\}. \tag{7}$$

We now show how to construct $C(M)$.

When $M = 1$, obviously $C(M) = \{\langle 0 \rangle\}$. Let $z \in S_M \backslash S_{M-2}$ be a configuration with $M \geq 3$ tokens, and $w = \langle w_0, w_1, \cdots, w_{M-1} \rangle$ the associated gap vector. We first ignore the first two tokens and consider the $M-2$ token configuration z' with gap vector $w' = \langle w_0 + w_1 + w_2, w_3, \cdots, w_{M-1} \rangle$. For each $v' \in O_g(z')$ with $v' = w' + \varDelta'$ and $\varDelta' \in C(M-2)$, we need to consider two cases:

1. $v'_0 = w'_0$. That is, the first gap of w' does not change. Consider again the original vector w. There are four gap vectors $v \in O_g(z)$ corresponding to this case: (i) $v_i = w_i$ for each $i = 0, 1, 2$; (ii) $v_0 = w_0$, $v_1 = w_1 + 1$, and $v_2 = w_2 - 1$; (iii) $v_0 = w_0 + 1$, $v_1 = w_1 - 1$, and $v_2 = w_2$; (iv) $v_0 = w_0 + 1$, $v_1 = w_1$, and $v_2 = w_2 - 1$. That is, corresponding to each increment vector $\varDelta' \in C(M-2)$ with $\varDelta'_0 = 0$, there are four increment vectors $\varDelta \in C(M)$ obtained from $\varDelta'$ by replacing $\varDelta'_0$ with the three-element vectors $\langle 0,0,0 \rangle$, $\langle 0,1,-1 \rangle$, $\langle 1,-1,0 \rangle$, and $\langle 1,0,-1 \rangle$, respectively.
2. $v'_0 = w'_0 + 1$. That is, the first gap of w' increases by 1. Similar to the first case, we have for each increment vector $\varDelta' \in C(M-2)$ with $\varDelta'_0 = 1$, there are four increment vectors $\varDelta \in C(M)$ obtained from $\varDelta'$ by replacing $\varDelta'_0$ by the three-element vectors $\langle 0,0,1 \rangle$, $\langle 0,1,0 \rangle$, $\langle 1,-1,1 \rangle$, and $\langle 1,0,0 \rangle$, respectively.

The items 1 and 2 above actually give us an inductive way to construct $C(M)$, $M \geq 3$, from $C(M-2)$:

Proposition 1 *Let $C(M)$ be defined in Eqn.(7). Then $C(1) = \{\langle 0 \rangle\}$, and for any odd number $M \geq 3$,*

$$C(M) = A^\frown C^0(M-2) \cup B^\frown C^1(M-2)$$

where the operation $^\frown$ means the element-wise concatenation of vectors,

$$C^i(M-2) = \{\langle \varDelta_1, \ldots, \varDelta_{M-3} \rangle : \\ \langle i, \varDelta_1, \ldots, \varDelta_{M-3} \rangle \in C(M-2)\}$$

for $i = 0, 1$, and

$$A := \{\langle 0,0,0 \rangle, \langle 0,1,-1 \rangle, \langle 1,-1,0 \rangle, \langle 1,0,-1 \rangle\}$$
$$B := \{\langle 0,0,1 \rangle, \langle 0,1,0 \rangle, \langle 1,-1,1 \rangle, \langle 1,0,0 \rangle\}.$$

For example, applying the above proposition, we have $C(3) = A$, and $C(5)$ is the union of the following two sets:

$$A^\frown C^0(3) = \left\{ \begin{array}{l} \langle 0,\ 0,\ 0, 0,\ 0 \rangle, \\ \langle 0,\ 1, -1, 0,\ 0 \rangle, \\ \langle 1, -1,\ 0, 0,\ 0 \rangle, \\ \langle 1,\ 0, -1, 0,\ 0 \rangle, \\ \langle 0,\ 0,\ 0, 1, -1 \rangle, \\ \langle 0,\ 1, -1, 1, -1 \rangle, \\ \langle 1, -1,\ 0, 1, -1 \rangle, \\ \langle 1,\ 0, -1, 1, -1 \rangle \end{array} \right\}$$

and

$$B^\frown C^1(3) = \left\{ \begin{array}{l} \langle 0,\ 0, 1, -1,\ 0 \rangle, \\ \langle 0,\ 1, 0, -1,\ 0 \rangle, \\ \langle 1, -1, 1, -1,\ 0 \rangle, \\ \langle 1,\ 0, 0, -1,\ 0 \rangle, \\ \langle 0,\ 0, 1,\ 0, -1 \rangle, \\ \langle 0,\ 1, 0,\ 0, -1 \rangle, \\ \langle 1, -1, 1,\ 0, -1 \rangle, \\ \langle 1,\ 0, 0,\ 0, -1 \rangle \end{array} \right\}.$$

Obviously, the cardinality of $C(M)$ is 2^{M-1}.

4.4 Properties of Gap Increment Vectors

As for the gap vectors, in the following, when the index exceeds $M-1$, we always assume 0 entries for the gap increment vectors. That is, we let $w_i = 0$ and $\varDelta_i = 0$ for all $i \geq M$ if $w = (w_0, \cdots, w_{M-1})$ and $\varDelta = (\varDelta_0, \cdots, \varDelta_{M-1})$. The following two lemmas state properties about sums of increment vectors that will be used to simplify the sum $\sum_{v \in O_g(z)} F(v)$ later.

Lemma 6 *For any odd number $M \geq 3$,*

$$\sum_{\varDelta \in C(M)} \varDelta_1 \sum_{k=0}^{\infty} \varDelta_{2k+2} = -2^{M-3}. \tag{8}$$

Proof The lemma is proved by dividing the sum according to the recursive definition of the gap increment vector. Precisely,

$$\begin{aligned}
&\sum_{\Delta\in C(M)} \Delta_1 \sum_{k=0}^{\infty} \Delta_{2k+2} \\
&= \sum_{\Delta'\in C^0(M-2)} 1\cdot\left(\sum_{k=0}^{\infty}\Delta'_{2k+1}-1\right) \\
&\qquad\qquad + \sum_{\Delta'\in C^0(M-2)} (-1)\cdot\sum_{k=0}^{\infty}\Delta'_{2k+1} \\
&+ \sum_{\Delta'\in C^1(M-2)} (-1)\cdot\left(\sum_{k=0}^{\infty}\Delta'_{2k+1}+1\right) \\
&\qquad\qquad + \sum_{\Delta'\in C^1(M-2)} \sum_{k=0}^{\infty}\Delta'_{2k+1} \\
&= -|C^0(M-2)| - |C^1(M-2)| \\
&= -|C(M-2)| = -2^{M-3}.
\end{aligned}$$

□

Lemma 7 *For any odd number $M \geq 1$,*

$$\sum_{\Delta\in C(M)} \sum_{j=0}^{\infty}\sum_{k=0}^{\infty} \Delta_{2j+1}\Delta_{2j+2k+2} = -(M-1)2^{M-4}. \quad (9)$$

Proof Let $T(M)$ be the LHS of Eqn.(9).We prove by induction that $T(M) = -(M-1)2^{M-4}$. The result is obvious for $M = 1$. Suppose now that Eqn.(9) holds for $M-2$, $M \geq 3$. Then we have from Lemma 6 that

$$\begin{aligned}
T(M) &= \sum_{\Delta\in C(M)} \Delta_1 \sum_{k=0}^{\infty}\Delta_{2k+2} \\
&\qquad + \sum_{\Delta\in C(M)} \sum_{j=1}^{\infty}\sum_{k=0}^{\infty}\Delta_{2j+1}\Delta_{2j+2k+2} \\
&= -2^{M-3} + 4\cdot \sum_{\Delta\in C(M-2)} \sum_{j=0}^{\infty}\sum_{k=0}^{\infty}\Delta_{2j+1}\Delta_{2j+2k+2} \\
&= -2^{M-3} - 4(M-3)2^{M-6} = -(M-1)2^{M-4}.
\end{aligned}$$

□

4.5 Proof of the Main Theorem

We are now ready to prove the main theorem. First we give a closed form for the sum $\sum_{v\in O_g(z)} F(v)$.

Lemma 8 *Let $z \in S_M\backslash S_{M-2}$ be an illegitimate configuration with gap vector w. Then*

$$\sum_{v\in O_g(z)} F(v) = 2^M F(w) - (M-1)2^{M-3}N.$$

Proof First note that

$$\begin{aligned}
\sum_{v\in O_g(z)} F(v) &= \sum_{\Delta\in C(M)} [F(w+\Delta)+F(w-\Delta)] \\
&= \sum_{\Delta\in C(M)} \sum_{i=0}^{M-3}\sum_{j=0}^{\infty}\sum_{k=0}^{\infty}[(w_i+\Delta_i)(w_{i+2j+1}+\Delta_{i+2j+1})\cdot \\
&\qquad (w_{i+2j+2k+2}+\Delta_{i+2j+2k+2}) \\
&\quad + (w_i-\Delta_i)(w_{i+2j+1}-\Delta_{i+2j+1})\cdot \\
&\qquad (w_{i+2j+2k+2}-\Delta_{i+2j+2k+2})].
\end{aligned}$$

On the other hand, a simple calculation shows that for any real numbers a, b, c and x, y, z, we have the following identity:

$$\begin{aligned}
&(a+x)(b+y)(c+z) + (a-x)(b-y)(c-z) \\
&\qquad = 2abc + 2xyc + 2xzb + 2yza
\end{aligned}$$

Thus we can write

$$\sum_{v\in O_g(z)} F(v) = \sum_{\Delta\in C(M)} 2F(w) + \sum_{i=0}^{M-1} A_{w_i}w_i$$

for some coefficient A_{w_i} of w_i. Using Lemma 7 we compute the coefficient A_{w_0} of w_0 as

$$\begin{aligned}
A_{w_0} &= \sum_{\Delta\in C(M)} 2\cdot\sum_{j=0}^{\infty}\sum_{k=0}^{\infty}\Delta_{2j+1}\Delta_{2j+2k+2} \\
&= -(M-1)2^{M-3}.
\end{aligned}$$

As the function F is rotationally symmetric, we derive that

$$\begin{aligned}
\sum_{v\in O_g(z)} F(v) &= \sum_{\Delta\in C(M)} 2F(w) - (M-1)2^{M-3}\sum_{i=0}^{M-1} w_i \\
&= 2^M F(w) - (M-1)2^{M-3}N.
\end{aligned}$$

□

Proof of the Main Theorem. From Lemma 8, we have that for any illegitimate configuration $z \in S_M\backslash S_{M-2}$ with gap vector w,

$$\begin{aligned}
(P_M\cdot\frac{4}{N}F_M^g)(z) &= \frac{4}{2^M N}\sum_{v\in O_g(z)} F(v) \qquad (10)\\
&= \frac{4}{N}F(w) - \frac{M-1}{2} \leq \frac{4}{N}F_M^g(z) - 1.
\end{aligned}$$

Thus, Lemma 1 implies that

$$\mathbb{E}_M(z) \leq \frac{4}{N}F_M^g(z) = \frac{4}{N}F(w).$$

□

5 A Nearly Optimal Upper Bound

In our main theorem, we derived an upper bound for the stabilization time $\mathbb{E}_M(z)$, which is given in terms of the function $F(w)$. Furthermore, using the method of Lagrange multipliers, we can derive a nearly optimal upper bound which is independent of the initial configurations.

Theorem 2 *1. For all N and odd number $3 \leq M \leq N$, we have*

$$\max_{z \in S_M} \mathbb{E}_M(z) \leq \frac{N^2}{6} \cdot \left(1 - \frac{1}{M^2}\right).$$

2. For all N and for all initial configurations, the expected stabilization time of Herman's algorithm is upper bounded by $\frac{1}{6}N^2$.

Proof Item 2 is obvious from Item 1. For Item 1, it suffices to show that for any $z \in S_M$ with gap vector w,

$$F(w) \leq u(M) := \frac{N^3}{24} \cdot \left(1 - \frac{1}{M^2}\right).$$

First, we use the method of Lagrange multipliers to find the critical point of $F(w)$ with the constraints $w_i \geq 0$ for each i, and $\sum_{i=0}^{M-1} w_i = N$. Here we consider w_i's as ranging over the nonnegative reals. Let

$$f(w) = F(w) + \lambda \left(\sum_{i=0}^{M-1} w_i - N \right).$$

We calculate the gradient equations for w_0 and w_2 as

$$\frac{\partial f}{\partial w_0} = \sum_{j=0}^{\infty} w_{2j+1} \sum_{k=0}^{\infty} w_{2j+2k+2} + \lambda$$

$$\frac{\partial f}{\partial w_2} = \sum_{j=0}^{\infty} w_{2j+3} \sum_{k=0}^{\infty} w_{2j+2k+4} + w_0 w_1 + w_1 \sum_{k=0}^{\infty} w_{2k+3} + \lambda.$$

By letting $\frac{\partial f}{\partial w_0} = \frac{\partial f}{\partial w_2} = 0$ and noting that $\sum_{i=0}^{M-1} w_i = N$, we derive directly:

$$w_2 + w_4 + \cdots + w_{M-1} = \frac{N - w_1}{2} \tag{11}$$

$$w_1 + w_3 + \cdots + w_{M-2} = \frac{N + w_1}{2} - w_0. \tag{12}$$

Since F is rotationally symmetric, we can derive from Eqn.(12) that

$$w_2 + w_4 + \cdots + w_{M-1} = \frac{N + w_2}{2} - w_1. \tag{13}$$

Thus $w_1 = w_2$ from Eqs.(11) and (13). By the rotational symmetry of F again, we have $w_0 = w_1 = \cdots = w_{M-1} = N/M$. Denote by w^* this (unique) critical point. Then $F(w^*) = u(M) = \frac{N^3}{24} \cdot \left(1 - \frac{1}{M^2}\right)$ from Eqs.(5) and (6).

On the other hand, note that $F(w)$ is a continous multivariate function and

$$R(M) := \{w \in \mathbf{R}^M \mid w_i \geq 0, \sum_{i=0}^{M-1} w_i = N\}$$

is a compact set. It follows that $F(w)$ has a global maximum in $R(M)$. For any $w' \in R(M)$ which achieves this global maximum, if w' is an interior point of $R(M)$, then it must be a critical point. Thus $w^* = w'$, and as a result, $F(w^*) = u(M)$ is the global maximum of $F(w)$ in $R(M)$ (and so an upper bound in $\mathcal{G}_M$). Then the theorem follows.

We now argue that w' is indeed an interior point of $R(M)$. Otherwise, w' must have some zero elements. Let w'' be the vector obtained from w' by recursively deleting all zero elements and merging the surrounding nonzero ones. Then w'' lies in the interior of $R(M')$ for some $M' < M$. As F is in harmony, we have $F(w'') = F(w')$ being the global maximum of $F(w)$ in $R(M')$. Thus w'' is a critical point, and $F(w'') = u(M')$. From the fact that $u(M)$ is a strictly increasing function, we have

$$F(w') = F(w'') = u(M') < u(M),$$

contradicting the assumption that w' achieves the global maximum of F in $R(M)$. □

6 Extensions

In this section, we first discuss how our approach may lead to closing the gap of the obtained upper bound with respect to the conjecture. Second, we show how our techniques can be applied in solving a variant of Herman's original algorithm with an initially *even* number of tokens.

6.1 Conjecture

Theorem 2 provides us an upper bound that is very close to the conjectured one. The gap between these two bounds is partially due to the inequality in Eqn.(10): for $M = 3$, $\frac{M-1}{2} = 1$, but for $M > 3$, $\frac{M-1}{2} > 1$. Thus, our upper bound is tight for $M = 3$, and is only an over approximation for the case $M > 3$. In the proof of Theorem 2, the Lagrange multipliers method is used to show that our bound has a unique global maximum value, obtained by equally distributed configurations. Interestingly, as observed from numerical results for small M, whereas the equally distributed configuration achieves maximum stabilization time for 3-token case, it is only a local maximum for configurations with 5 or more tokens. This subsection is devoted to exploiting a better upper bound to avoid such local maximums.

Note that the function F defined in Definition 2 is a homogeneous polynomial of degree 3 over token gaps. To get a better (that is, smaller) upper bound of the expected stabilization time for a given initial configuration, a reasonable candidate would be one obtained by subtracting from F a higher-degree polynomial of token gaps. For this purpose, we define a family of homogeneous polynomials g_k of degree k, where $k \geq 3$ is odd, as follows:

$$\begin{aligned} & g_k(w_0, w_1, \cdots, w_{M-1}) \\ & = \sum_{i_1,\cdots,i_k=0}^{\infty} w_{i_1} w_{i_1+2i_2+1} \cdots w_{i_1+2(i_2+\cdots+i_k)+k-1}. \end{aligned} \tag{14}$$

Observe that when $k = 3$, the function g_3 reduces to F defined in Definition 2, while for $k = M = 5$, $g_5(\langle w_0, w_1, \cdots, w_4\rangle) = w_0 w_1 w_2 w_3 w_4$. The next theorem shows that higher-degree polynomials indeed give better upper bound for any given initial configuration.

Theorem 3 *For any odd number $M \geq 3$ and any $z \in S_M$ with the associated gap vector w,*

$$\mathbb{E}_M(z) \leq \frac{4}{N} g(w) \tag{15}$$

where $g(w) = g_3(w) - c \cdot g_5(w)$, and

$$c = \frac{48M^2}{(M-1)(2N^2M + 2N^2 - 3M^2)}.$$

Proof The proof is similar to the proof of Theorem 1. We sketch the main steps here. The function g_k can be proven to be rotationally symmetric, and in harmony in M. With some further properties of the gap vectors, we can derive that for any illegitimate configuration $z \in S_M \backslash S_{M-2}$ with gap vector w,

$$\begin{aligned} \sum_{v \in O_g(z)} g_5(v) = 2^M g_5(w) - (M-3)2^{M-3} g_3(w) \\ + (M-3)(M-1)2^{M-7} N. \end{aligned} \tag{16}$$

Noting that $g_3(w) \leq \frac{N^3}{24}(1 - \frac{1}{M^2})$, we have

$$\begin{aligned} & (P_M \cdot \frac{4}{N} g)(w) = \frac{4}{2^M N} \sum_{v \in O_g(z)} [g_3(v) - c \cdot g_5(v)] \\ & = \frac{4}{N} g(w) - \frac{1}{2N}[(M-1)N - c(M-3)g_3(w) \\ & \qquad + c(M-3)(M-1)2^{-4}N)] \\ & \leq \frac{4}{N} g(w) - \frac{1}{2N}[(M-1)N - (M-3)N] \\ & = \frac{4}{N} g(w) - 1. \end{aligned}$$

Thus, Lemma 1 implies $\mathbb{E}_M(z) \leq \frac{4}{N} g(w)$. □

Obviously, $g(w) < F(w)$ for any configuration with more than 3 tokens, thus Theorem 3 provides a strictly better upper bound on the stabilization time for any *given* configuration. We also expect that $g(w)$ admits a better *universal* upper bound, compared with $\frac{1}{6}N^2$ obtained in the previous section, when the initial configuration varies. However, as the gradient function of $g(w)$ is of degree 4, it seems difficult to calculate the maximum value of $g(w)$ using Lagrange multipliers method, as we did in Theorem 2 for $F(w)$. Anyway, numerical results indicate that the maximum value of $g(w)$ is not obtained at the (non-degenerate) equidistant configurations, thus avoiding the local maximum problem of $F(w)$ pointed out at the beginning of this subsection.

For the purpose of illustration, we only consider g_3 and g_5 in Theorem 3. However, to prove the conjectured upper bound, if our technique works at all, we might have to consider higher-degree polynomials such as g_7, g_9, etc. We have proven that for any odd number k, g_k is both rotationally symmetric and in harmony in M, but it becomes more and more difficult to obtain a closed form for the sum $\sum_{v \in O_g(z)} g_k(v)$, as shown in Lemma 8 for $k = 3$ and Eqn.(16) for $k = 5$, when k increases. In addition, finding the maximum value of a function involving higher-degree g_k is also a difficult task. We leave these topics for further investigation.

6.2 Herman's algorithm with an even number of tokens

As an application of the techniques employed in this paper, we now consider a variant of Herman's original algorithm in which the initial configurations have *even* number of tokens. Obviously, from any such initial configuration, all tokens will eventually (with probability 1) be annihilated. If we refer to the empty configuration without any tokens as legitimate, then all the notions such as S_M, P_M, $\mathbb{E}_M$, $\mathcal{G}_M$, O, O_g defined for odd number M can be extended to even M. Surprisingly, when M is even, it is relatively straightforward to show a $\frac{1}{2}N^2$ upper bound on the expected stabilization time for all initial configurations, and this bound is obtained by equidistant two-token configurations. In particular, for the simplest case of $M = 2$, we are able to give a closed form for the expected stabilization time, just like McIver and Morgan did for three-token case.

First we note that Lemma 1, which was given for odd numbers of tokens in [13], actually holds for even number cases as well. Now we present the key function for even number tokens, which plays a similar role to F in Definition 2 for odd number tokens.

Definition 5 Let $\mathcal{G}_e = \bigcup_{M=2, M \text{ is even}}^{N} \mathcal{G}_M$ and $F_e : \mathcal{G}_e \to [0, \infty)$ be a mapping defined by

$$F_e(w) = \Sigma_w^e \cdot \Sigma_w^o \tag{17}$$

where $w = \langle w_0, w_1, \cdots, w_{M-1} \rangle$, and

$$\Sigma_w^e = \sum_{i=0}^{\infty} w_{2i} \qquad \text{and} \qquad \Sigma_w^o = \sum_{i=0}^{\infty} w_{2i+1}$$

are the sums of even-index elements and odd-index elements in w, respectively.

Again, we can prove that the function defined in Definition 5 is both rotationally symmetric and in harmony for different even Ms.

Lemma 9 *1. For any even number $M \geq 2$,*

$$F_e(\langle w_0, w_1, \cdots, w_{M-1} \rangle) = F_e(\langle w_1, \cdots, w_{M-1}, w_0 \rangle).$$

2. For any even number $M \geq 2$, if $w_1 = 0$ then

$$F_e(\langle w_0, w_1, w_2, \cdots, w_{M-1} \rangle) = F_e(\langle w_0 + w_2, w_3, \cdots, w_{M-1} \rangle).$$

Proof Easy from the definition. □

Furthermore, it is easy to see that the set $C(M)$ of generating vectors for even number gaps can be constructed inductively in the same way as shown in Proposition 1, except that the base case is $M = 2$ for which $C(2) = \{\langle 0, 0 \rangle, \langle 1, -1 \rangle\}$. Again, the cardinality of $C(M)$ is 2^{M-1}. The following is the corresponding version of Lemma 7 when M is even.

Lemma 10 *For any even number $M \geq 2$,*

$$\sum_{\Delta \in C(M)} F_e(\Delta) = -2^{M-3} M. \tag{18}$$

Proof We prove this lemma by induction. The case when $M = 2$ is obvious by noting $C(2) = \{\langle 0, 0 \rangle, \langle 1, -1 \rangle\}$. Suppose the induction hypothesis holds for $M \geq 2$. Note that $\Sigma_\Delta^e + \Sigma_\Delta^o = 0$. Then $F_e(\Delta) = -(\Sigma_\Delta^e)^2 = -(\Sigma_\Delta^o)^2$, and

$$\begin{aligned}
&\sum_{\Delta \in C(M+2)} F_e(\Delta) = - \sum_{\Delta \in C(M+2)} (\Sigma_\Delta^o)^2 \\
&= - \sum_{\Delta' \in C^0(M)} \left[2(\Sigma_{\Delta'}^e)^2 + (\Sigma_{\Delta'}^e + 1)^2 + (\Sigma_{\Delta'}^e - 1)^2 \right] \\
&- \sum_{\Delta' \in C^1(M)} \left[2(\Sigma_{\Delta'}^e)^2 + (\Sigma_{\Delta'}^e + 1)^2 + (\Sigma_{\Delta'}^e - 1)^2 \right] \\
&= -4 \sum_{\Delta'' \in C(M)} (\Sigma_{\Delta''}^o)^2 - 2|C(M)| \\
&= -2^{M-1} M - 2^M = -2^{M-1}(M+2),
\end{aligned}$$

where the second equality is due to the definition of $C(M+2)$ from $C(M)$, and the third equality from the fact that

$$C(M) = \{\langle 0 \rangle\}^\frown C^0(M) \cup \{\langle 1 \rangle\}^\frown C^1(M).$$

This concludes the proof of the lemma. □

Now we are able to show the main result of this section, which is in contrast with Theorem 1 and Lemma 2.

Theorem 4 *For any even number $M \geq 2$ and any $z \in S_M$ with the associated gap vector w,*

$$\mathbb{E}_M(z) \leq 2F_e(w). \tag{19}$$

In particular, when $M = 2$, $\mathbb{E}_M(z) = 2F_e(w) = 2w_0 w_1$.

Proof First, from Lemma 10 we have

$$\begin{aligned}
&\sum_{v \in O_g(z)} F_e(v) = \sum_{\Delta \in C(M)} [F_e(w + \Delta) + F_e(w - \Delta)] \\
&= \sum_{\Delta \in C(M)} \sum_{i,j=0}^{\infty} [(w_{2i} + \Delta_{2i})(w_{2j+1} + \Delta_{2j+1}) \\
&\qquad + (w_{2i} - \Delta_{2i})(w_{2j+1} - \Delta_{2j+1})] \\
&= \sum_{\Delta \in C(M)} 2(F_e(w) + F_e(\Delta)) = 2^M F_e(w) - 2^{M-2} M.
\end{aligned}$$

Thus for any illegitimate configuration $z \in S_M \backslash S_{M-2}$ with gap vector w,

$$\begin{aligned}
(P_M \cdot 2F_e^g)(z) &= \frac{1}{2^{M-1}} \sum_{v \in O_g(z)} F_e(v) \\
&= 2F_e(w) - \frac{M}{2} \leq 2F_e^g(z) - 1
\end{aligned} \tag{20}$$

where F_e^g is the function obtained by composing F_e with the gap function; that is, $F_e^g(z) = F_e(w)$ and w is the gap vector of z. Thus, Lemma 1 implies that $\mathbb{E}_M(z) \leq 2F_e^g(z) = 2F_e(w)$.

When $M = 2$, the inequality in Eq.(20) becomes an equality. Then $\mathbb{E}_M(z) = 2F_e(w) = 2w_0 w_1$ by Lemma 1. □

A byproduct of Theorem 4 is a tight upper bound of the expected stabilization time for all initial configurations with an even number of tokens.

Theorem 5 *For all N and for all initial configurations with even number of tokens, the expected stabilization time is upper bounded by $\frac{1}{2}N^2$, which can be obtained by equidistant two-token configurations .*

Proof For any initial configuration z with even number tokens, suppose w is the corresponding gap vector. Note that $\Sigma_w^e + \Sigma_w^o = N$. Thus $F_e(w) \leq \frac{1}{4}N^2$, and $\mathbb{E}_M(z) \leq \frac{1}{2}N^2$. Furthermore, when z is an equidistant two-token configuration, i.e., $w_0 = w_1 = N/2$, it holds that $\mathbb{E}_M(z) = \frac{1}{2}N^2$ by Theorem 4, obtaining the upper bound. □

7 Conclusion and future work

It is conjectured that $\frac{4}{27}N^2$ is the tight upper bound of Herman's self-stabilization algorithm. Our paper provides a bound $\frac{1}{6}N^2$, which is very close to the conjectured bound. This gap, which is approximately $0.019N^2$, arises from the strict inequality in Eqn.(10) for $M \geq 5$. To make the inequality tighter, and derive a better bound is one of our further research topics. Our technique takes advantage of the uniform distribution of the next-step configurations. This is not true for the asynchronous variant of Herman's protocol [10], as well as for the asymmetric case for token passing. The generalization to these cases will also be our future work.

Finally, as Herman's protocol is very similar to systems of interacting and annihilating particles proposed and studied in physics, combinatorics, and neural networks, we are also interested in exploiting the possibility of extending our elementary methodology for Herman's protocol to providing approximate upper bound for the worst-case analysis of such particle systems.

Acknowledgement

The authors would like to thank the anonymous reviewers for their insightful and helpful comments.

This work was partially supported by the Australian Research Council (Grant No. DP130102764), the National Natural Science Foundation of China (Grant Nos. 61428208, 61472473, 61472412, and 61361136002), and the CAS/SAFEA International Partnership Program for Creative Research Teams.

References

1. Balding, D.: Diffusion-reaction in one dimension. J. Appl. Prob. **25**, 733–743 (1988)
2. Dijkstra, E.: Self-stabilizing systems in spite of distributed control. Communications of the ACM **17**(11), 643–644 (1974)
3. Dolev, S.: Self-Stabilization. MIT Press (2000)
4. Feller, W.: An introduction to probability theory and its applications, volume 1. John Wiley & Sons (1968)
5. Feng, Y., Zhang, L.: A tighter bound for the self-stabilization time in Herman's algorithm. Inf. Process. Lett. **113**(13), 486–488 (2013)
6. Feng, Y., Zhang, L.: A nearly optimal upper bound for the self-stabilization time in Herman's algorithm. In: CONCUR, vol. 8704, pp. 342–356. Springer (2014)
7. Fribourg, L., Messika, S., Picaronny, C.: Coupling and self-stabilization. Distributed Computing **18**(3), 221–232 (2006)
8. Herman, T.: Probabilistic self-stabilization. Information Processing Letters **35**(2), 63–67 (1990).
9. Kiefer, S., Murawski, A.S., Ouaknine, J., Wachter, B., Worrell, J.: Three tokens in Herman's algorithm. Formal Asp. Comput. **24**(4-6), 671–678 (2012)
10. Kiefer, S., Murawski, A.S., Ouaknine, J., Worrell, J., Zhang, L.: On Stabilization in Herman's Algorithm. In: ICALP (2), pp. 466–477 (2011)
11. Kwiatkowska, M.Z., Norman, G., Parker, D.: Probabilistic verification of Herman's self-stabilisation algorithm. Formal Asp. Comput. **24**(4-6), 661–670 (2012)
12. Liggett, T.: Interacting particle systems. Springer (2005)
13. McIver, A., Morgan, C.: An elementary proof that Herman's ring is $\Theta(N^2)$. Inf. Process. Lett. **94**(2), 79–84 (2005)
14. Nakata, T.: On the expected time for Herman's probabilistic self-stabilizing algorithm. Theoretical Computer Science **349**(3), 475–483 (2005)
15. Schneider, M.: Self-stabilization. ACM Comput. Surv. **25**(1), 45–67 (1993)