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

Yuan Feng[1,2] and Lijun Zhang[3]

[1] Centre for Quantum Computation and Intelligent Systems,
University of Technology Sydney, Australia
[2] AMSS-UTS Joint Research Laboratory for Quantum Computation,
Chinese Academy of Sciences
[3] State Key Laboratory of Computer Science, Institute of Software,
Chinese Academy of Sciences

**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 self-stabilization 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 of it.

## 1 Introduction

In [2], Dijkstra proposed the influential notion of self-stabilization algorithms for designing fault-tolerant distributed systems. A distributed system is self-stabilizable 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 received much attention. See for example [14,3] 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 is 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 [7] 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 $N$, $N$ is odd, 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 [7], an upper bound $O(N^2\lceil \log N \rceil)$ for stabilization time has been established, while in 2005, several groups of researchers [6,12,13] gave an upper bound of $O(N^2)$, independently. Moreover, McIver and Morgan [12] proved that the stabilization time is actually $\Theta(N^2)$, meaning that the lower bound and upper bound coincide. They also provided a *precise* expected stabilization time for configurations with exactly 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 [12] conjectured 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. 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.* [9] 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 [12].

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 is a function of the gap vector of the initial configuration, thus a multivariate function. Our result then follows by obtaining the maximum of the upper bounds over all initial configurations, using the Lagrange multipliers method.

Note that systems of interacting and annihilating particles, either on a circle or on a line, are heavily studied in areas including physics, combinatorics and neural networks [11]. Most of them focus on exploring the precise solutions, for example Balding [1] gives generating functions for the number of remaining particles at time $t$, and this results is transferred in [9] to Herman's setting. However, such expressions are in general very complex and difficult to analyze, see [1,4,9]. In contrast, our proof in this paper exploits mostly elementary concepts, and it is much simpler than previous techniques for analyzing Herman's algorithm [6,9]. Because of this, we are optimistic that our approach might provide alternative ways to improve worst-case analysis of such particle systems.

*Related Work.* In [9], an asynchronous variant of Herman's protocol is studied as well. Recently, [8] has studied the distribution of the self-stabilization time and shown that for an arbitrary $t$ the probability of stabilization within time $t$ is minimized under this configuration with $M = 3$. On the practical side, using the probabilistic model checker PRISM [10], McIver and Morgan's conjecture is 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, with $N$ odd, 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.

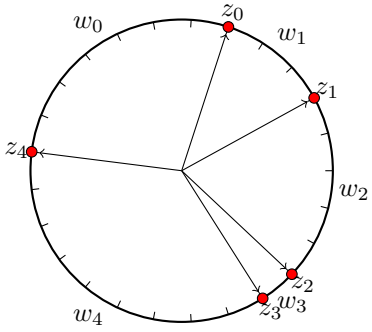


**Fig. 1.** A configuration with $M = 5$, $N = 25$.

Herman's protocol [7] 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 implies 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 [12], slightly modified with respect to our notations, is crucial for our discussion.

**Lemma 1.** *[12, Lemma 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 $(P_M \cdot v)(z) \leq v(z) - 1$ for any non-legitimate 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 $z \in S_M$.*

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., it 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 $z(i)$ defined by $w_i := z(i) - z(i-1)$ for $i = 1, \ldots, M-1$, and $w_0 = N - \sum_{i=1}^{M-1} w_i$. We denote by $G_M$, $M \geq 3$, the set of gap vectors corresponding to configurations from $S_M$, and set $G_1 = \{\langle N \rangle\}$.*

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.** *[12, 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 further dig 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 notations, 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 $G = \bigcup_{M=1,M \text{ is odd}}^{N} G_M$ and $F : G \to [0, \infty)$ be a mapping defined by*

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

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

**Theorem 1.** *For any $z \in S_M$ with the associated gap vector $w$,*

$$\mathbb{E}_M(z) \leq \frac{4}{N} F(w). \quad (2)$$

We can further apply the Lagrange multipliers method to compute the maximal value of $\mathbb{E}_M(z)$ for each $M \leq N$, which provides a better upper bound $\frac{1}{6}N^2 = 0.167N^2$, over the previous known 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 $M$.

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

$$F(\langle w_0, w_1, w_2, w_3, w_4 \rangle) = w_0w_1w_2 + w_1w_2w_3 + w_2w_3w_4 + w_3w_4w_0 + w_4w_0w_1 \quad (3)$$

- $M = 7$. In this case, $F(w)$ is already 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 $\{0, \ldots, M-1\}$ are understood as modulo 7, then it can be written as:

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

– The explicit expressions for $M > 7$ are even 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 prove the main theorem, we first need to introduce some notation.

**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 $F_M^g$ be the function obtained by composing $F$ with the gap function, restricting on the set of $M$-token configurations; that is, for any $z \in S_M \backslash S_{M-2}$, $F_M^g(z) = F(w)$ where $w$ is the gap vector of $z$. Then

$$(P_M \cdot \frac{4}{N} F_M^g)(z) = \frac{4}{2^M N} \sum_{y \in O(z)} F_M^g(y) = \frac{4}{2^M N} \sum_{v \in O_g(z)} F(v).$$

The proof of our main theorem will exploit the definition 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

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

for all non-legitimate 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.(3), which has obviously the following properties:

– $F$ is *rotationally symmetric*, i.e., $F(\langle w_0, \ldots, w_4\rangle) = F(\langle w_1, w_2, w_3, w_4, w_0\rangle)$.
– $F$ 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, and 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.

These two properties will be extended for arbitrary $M$, and they will be exploited to prove our main theorem.

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 remaining. Obviously, the cases where a single token passes while the others remain can be obtained by applying $Per^i$ to $\Delta_1^T$, 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 $\Delta_{2,1} = \langle 1, 0, -1, 0, 0\rangle$, corresponding to the first two tokens passing while the others remaining, and $\Delta_{2,2} = \langle 1, -1, 1, -1, 0\rangle$, corresponding to the first and the third tokens passing while the others remaining. Other cases where exactly 2 tokens passing can be obtained by applying the cyclic permutation matrices to either $\Delta_{2,1}$ or $\Delta_{2,2}$.
3. Let $\Delta_0 = \langle 0, 0, 0, 0, 0\rangle$, corresponding to the case that no token, or all, moves.

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

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

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

$$\square_1^i := F(w + Per^i\Delta_1^T) + F(w - Per^i\Delta_1^T)$$

for $i = 0, 1, 2, 3, 4$, and $\square_{2,1}^i$ and $\square_{2,2}^i$ be defined similarly. Note that

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

We have $\square_1^0 = 2F(w) - 2w_2 - 2w_4$. Moreover, as $F(w)$ is rotationally symmetric, and $\sum_{i=0}^4 w_i = N$, we derive $\sum_{i=0}^4 \square_1^i = 10F(w) - 4N$. In a similar way, we have $\square_{2,1}^0 = 2F(w) - 2w_1$ and $\sum_{i=0}^4 \square_{2,1}^i = 10F(w) - 2N$. The case for $\Delta_{2,2}$ is slightly complicated: the sum $\square_{2,2}^0$ can be first simplified to

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

Thus $\square_{2,2}^0 = 2F(w) - 2(w_0 + w_3) - 6w_4$, and $\sum_{i=0}^4 \square_{2,2}^i = 10F(w) - 10N$. Finally, noting $F(w + \Delta_0) = F(w - \Delta_0) = F(w)$, we have $\sum_{v \in O_g(z)} F(v) = 32F(w) - 16N$. Thus

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

and Lemma 1 implies $\mathbb{E}_5(z) \leq \frac{4}{N} \cdot F_5^g(z)$. Using Lagrange multipliers method (cf. Theorem 2), we have then $\mathbb{E}_5(z) \leq \frac{4}{N} \cdot \frac{1}{25}N^3 = \frac{4}{25}N^2 = 0.16N^2$.

### 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 Symmetricity] The function $F$ is rotationally symmetric. That is, for any odd number $M \geq 3$,*

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

*Proof.* 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.(1),

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

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

$$\Sigma_1(w) := \sum_{n=1}^{(M-3)/2} w_{2n-1} \sum_{j=0}^{(M-3-2n)/2} w_{2n+2j} \sum_{k=0}^{(M-3-2n-2j)/2} w_{2n+2j+2k+1} \quad (4)$$

$$\Sigma_2(w) := \sum_{n=0}^{(M-3)/2} w_{2n} \sum_{j=0}^{(M-3-2n)/2} w_{2n+2j+1} \sum_{k=0}^{(M-3-2n-2j)/2} w_{2n+2j+2k+2}. \quad (5)$$

Then $F(w) = \Sigma_1(w) + \Sigma_2(w)$. 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

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

The most involved part is the sum $\Sigma_2(w')$. Note $k = (M-3-2n-2j)/2$ implies $w'_{2n+2j+2k+2} = w'_{M-1}$. Isolating the term of $w'_{M-1}$ from the last part of $\Sigma_2(w')$, we derive:

$$\begin{aligned}\Sigma_2(w') = &\sum_{n=0}^{(M-5)/2} w'_{2n} \sum_{j=0}^{(M-5-2n)/2} w'_{2n+2j+1} \sum_{k=0}^{(M-5-2n-2j)/2} w'_{2n+2j+2k+2} \\ &+ \sum_{n=0}^{(M-3)/2} w'_{2n} \sum_{j=0}^{(M-3-2n)/2} w'_{2n+2j+1} \cdot w'_{M-1}.\end{aligned}$$

Some subtle simplifications have been used above: the case $n = (M-3)/2$ implies $(M-3-2n)/2 = 0$ and $(M-3-2n-2j)/2 = 0$ as well, thus the corresponding term $w'_{M-3}w'_{M-2}w'_{M-1}$ appears in the sum in the last line. Similar with the case $j = (M-3-2n)/2$. Now we can further rewrite $\Sigma_2(w')$ by:

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

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 harmony 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*

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

*Proof.* The equality is obtained by directly expanding both sides according to Eqn.(1), by noting that $w_1 = 0$:

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

□

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

### 4.3 Gap Increment Vector

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 increment vector $\Delta$ for $z$, both $w + \Delta$ and $w - \Delta$ are in $O_g(z)$.*

*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. □

Let $C(M)$ be a subset of gap increment vectors for $M$ tokens such that for each non-legitimate $z \in S_M \backslash S_{M-2}$,

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

Without loss of generality, we assume every vector in $C(M)$ has the first entry being either 0 or 1. We would like to construct $C(M)$ in an inductive way.

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 $v' = w' + \Delta'$ and $\Delta' \in C(M-2)$, we need to consider two cases:

1. $v'_0 = w'_0$. That is, the first gap of $w'$ does not change. Come back to 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 $\Delta' \in C(M-2)$ with $\Delta'_0 = 0$, there are four increment vectors $\Delta \in C(M)$ obtained from $\Delta'$ by replacing $\Delta'_0$ 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 $\Delta' \in C(M-2)$ with $\Delta'_0 = 1$, there are four increment vectors $\Delta \in C(M)$ obtained from $\Delta'$ by replacing $\Delta'_0$ 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 above. 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,*

$$C^i(M-2) = \{\langle \Delta_1, \ldots, \Delta_{M-3} \rangle : \langle i, \Delta_1, \ldots, \Delta_{M-3} \rangle \in C(M-2)\}$$

*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:

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

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 $\Delta_i = 0$ for all $i \geq M$ if $w = (w_0, \cdots, w_{M-1})$ and $\Delta = (\Delta_0, \cdots, \Delta_{M-1})$. 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 $M \geq 3$,*

$$\sum_{\Delta \in C(M)} \Delta_1 \sum_{k=0}^{\infty} \Delta_{2k+2} = -2^{M-3}. \tag{6}$$

*Proof.* The lemma is proved by dividing the sum according to the recursive definition of the gap increment vector. Precisely, $\sum_{\Delta \in C(M)} \Delta_1 \sum_{k=0}^{\infty} \Delta_{2k+2}$ equals

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

□

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

$$\sum_{\Delta \in C(M)} \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} \Delta_{2j+1} \Delta_{2j+2k+2} = -(M-1)2^{M-4}. \tag{7}$$

*Proof.* Let $T(M)$ be the LHS of Eqn.(7).We prove by induction that $T(M) = -(M-1)2^{M-4}$. The result is obvious for $M = 1$. Suppose now that Eqn.(7) holds for $M-2$, $M \geq 3$. Then we have from Lemma 6 that

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

□

### 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.** *For any non-legitimate configuration $z \in S_M \backslash S_{M-2}$ with gap vector $w$,*

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

*Proof.* First note that

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

On the other hand, a simple calculation shows that for any $a, b, c$ and $x, y, z$,

$$(a+x)(b+y)(c+z) + (a-x)(b-y)(c-z) = 2abc + 2xyc + 2xzb + 2yza$$

Thus we have

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

where $A_{w_i}$ is the coefficient of $w_i$. Using Lemma 7 we compute the coefficient $A_{w_0}$ of $w_0$ as

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

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 non-legitimate configuration $z \in S_M \backslash S_{M-2}$ with gap vector $w$,

$$(P_M \cdot \frac{4}{N}F_M^g)(z) = \frac{4}{2^M N}\sum_{v\in O_g(z)} F(v) = \frac{4}{N}F(w) - \frac{M-1}{2} \le \frac{4}{N}F_M^g(z) - 1. \tag{8}$$

Thus, Lemma 1 implies that $\mathbb{E}_M(z) \le \frac{4}{N}F_M^g(z) = \frac{4}{N}F(w)$. □

## 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 $3 \le M \le N$, we have*

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

*2. For all $N$ and for all initial configurations, we have $\mathbb{E}\mathbf{T} \le \frac{1}{6}N^2$.*

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

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

First, we use the method of Lagrange multipliers to find the critical point of $F(w)$ with the constraints $w_i \ge 0$ for each $i$, and $\sum_{i=0}^{M-1} w_i = N$. Here we do not require values of $w_i$ being integers any more; they can be any nonnegative real numbers. 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:

$$w_2 + w_4 + \cdots + w_{M-1} = \frac{N - w_1}{2} \tag{9}$$
$$w_1 + w_3 + \cdots + w_{M-2} = \frac{N + w_1}{2} - w_0. \tag{10}$$

Since $F$ is rotationally symmetric, we can derive from Eqn.(10) that

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

Thus $w_1 = w_2$ from Eqs.(9) and (11). 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.(4) and (5).

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 in $G(M)$). Then the theorem follows.

We now argue that $w'$ is indeed an interior point of $R(M)$. Otherwise, $w'$ must have some zero elements. By deleting all zero elements from $w'$, we get a vector $w''$ which lies in the interior of $R(M')$ for some $M' < M$. Thus $F(w'') = F(w')$ is the global maximum of $F(w)$ in $R(M')$, so $w''$ is a critical point, and $F(w'') = u(M')$. From the fact that $u(M)$ is a strictly increasing function, we have

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

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

## 6 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.(8) for $M \geq 5$. To make the inequality tighter, and derive a better bound is one of our further works. Our technique takes large advantage of the uniform distribution of the next-step configurations. This is not true for the asynchronous variant of Herman's protocol [9], as well as for the asymmetric case for token passing. The generalization to these cases will 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

Yuan Feng was partially supported by Australian Research Council (Grant Nos. DP130102764 and FT100100218). Lijun Zhang is the corresponding author (zhanglj@ios.ac.cn), and has received support from the National Natural Science Foundation of China (NSFC) under grant No. 61361136002, and the CAS/SAFEA International Partnership Program for Creative Research Teams.

## References

1. D. Balding. Diffusion-reaction in one dimension. *J. Appl. Prob.*, 25:733–743, 1988.
2. E. Dijkstra. Self-stabilizing systems in spite of distributed control. *Communications of the ACM*, 17(11):643–644, 1974.
3. S. Dolev. *Self-Stabilization.* MIT Press, 2000.
4. W. Feller. *An introduction to probability theory and its applications, volume 1.* John Wiley & Sons, 1968.
5. Y. Feng and L. Zhang. A tighter bound for the self-stabilization time in Herman's algorithm. *Inf. Process. Lett.*, 113(13):486–488, 2013.
6. L. Fribourg, S. Messika, and C. Picaronny. Coupling and self-stabilization. *Distributed Computing*, 18(3):221–232, 2006.
7. T. Herman. Probabilistic self-stabilization. *Information Processing Letters*, 35(2):63–67, 1990. Report at `ftp://ftp.math.uiowa.edu/pub/selfstab/H90.html`.
8. S. Kiefer, A. S. Murawski, J. Ouaknine, B. Wachter, and J. Worrell. Three tokens in Herman's algorithm. *Formal Asp. Comput.*, 24(4-6):671–678, 2012.
9. S. Kiefer, A. S. Murawski, J. Ouaknine, J. Worrell, and L. Zhang. On Stabilization in Herman's Algorithm. In *ICALP (2)*, pages 466–477, 2011.
10. M. Z. Kwiatkowska, G. Norman, and D. Parker. Probabilistic verification of Herman's self-stabilisation algorithm. *Formal Asp. Comput.*, 24(4-6):661–670, 2012.
11. T. Liggett. *Interacting particle systems.* Springer, 2005.
12. A. McIver and C. Morgan. An elementary proof that Herman's ring is $\Theta(N^2)$. *Inf. Process. Lett.*, 94(2):79–84, 2005.
13. T. Nakata. On the expected time for Herman's probabilistic self-stabilizing algorithm. *Theoretical Computer Science*, 349(3):475–483, 2005.
14. M. Schneider. Self-stabilization. *ACM Comput. Surv.*, 25(1):4567, 1993.