NEW EXPLICIT SOLUTION TO THE N-QUEENS PROBLEM AND ITS RELATION TO THE MILLENNIUM PROBLEM

DMITRII MIKHAILOVSKII

Abstract. Using modular arithmetic of the ring $\mathbb{Z}_{n+1}$ we obtain a new short solution to the problem of existence of at least one solution to the N-Queens problem on an $N \times N$ chessboard. It was proved, that these solutions can be represented as the Queen function with the width fewer or equal to 3. It is shown, that this estimate could not be reduced. A necessary and sufficient condition of being a composition of solutions a solution is found. Based on the obtained results we formulate a conjecture about the width of the representation of arbitrary solution. If this conjecture is valid, it entails solvability of the N-Queens completion in polynomial time. The connection between the N-Queens completion and the Millennium $P$ vs $NP$ Problem is found by the group of mathematicians from Scotland in August 2017.

Introduction

The Millennium Problems are seven problems in mathematics that were stated by the Clay Mathematics Institute in 2000. A correct solution to any of these problems results in a US $1000000 prize being awarded by the institute to the discoverer. Currently, the only Problem that has been solved is so-called Poincare conjecture. Another of these 7 Problems is related to the complexity of algorithms. Among these algorithms, polynomial algorithms are highlighted. The class of these algorithms is designated by $P$. Another class of algorithms are the algorithms which are able to check in polynomial number of steps that an answer is indeed a solution to a problem. Class of these algorithms is designated by $NP$. The Millennium Problem is the $P$ versus $NP$ problem. In August 2017 a group of mathematicians from Scotland proved that N-Queens Completion Problem is $NP$-complete. Namely, if this problem can be solved in polynomial time, then $P$ is equal to $NP$.

Our work is devoted to the N-Queens Problem i.e. the well-known problem of placing $N$ chess queens on an $N \times N$ chessboard so that no two queens attack each other.

C.F. Gauss found 72 solutions for $N = 8$. But 24 years later J.W.L. Glaisher proved using a method of determinants that for $N = 8$ there are exactly 92 solutions. The existence of a solution for arbitrary $N$ was proved by different authors using different methods. It was first proved by E. Pauls in 1874. Now the number of different solutions \( Q(N) \) is computed only for $4 \leq N \leq 27$. Calculation of $Q(N)$ is related to the N-Queens Completion Problem (if we have $m < N$ queens on the board, is it possible to complete this board to the solution of the N-Queens Problem?). Existing methods of solving the completion problem stop working for $N \geq 1000$.

In this paper, we try to find such an algorithm.

We introduce the new way of representing the arrangements of queens as a Queen functions with width $k$ which is a map $[1, N] \rightarrow [1, N]$ which is defined on a partition of a segment $[1, N]$ by $k$ segments and on each of them it is linear on subsets of even and odd numbers. A map of positive integers $f : S \subseteq [1, N] \rightarrow [1, N]$ we call linear on $S$, if there exist integers $a \in [1, N], b \in [0, N], f(i) = ai + b \pmod{N + 1}$, where $i \in S$.

Using this construction we prove the next theorem:

The Width Theorem. For any $N > 3$ there exists a solution which can be represented as a Queen function with width fewer or equal to 3.

The width of the function in the theorem cannot be reduced, since for $N = 15$ our program checked that there are no solutions that can be represented as a Queen function with width 1 or 2. All other solutions by different authors have greater width than ours.

Next we introduce the concept of composition of solutions, formulate the criterion of being a composition of solutions a solution and prove this criterion for the generalization of composition. Generalized composition of solutions $(A_1, A_2, \ldots, A_{|B|}) \otimes B$ is an arrangement which is defined by the following rule
\[
C(|B|(i - 1) + j) = B(|A_j|(i) - 1) + B(j),
\]
where $|A_i| = |A_j| (1 \leq i < j \leq |B|), 1 \leq i \leq |A|, 1 \leq j \leq |B|$. Theorem. Generalized composition $(A_1, A_2, \ldots, A_{|B|}) \otimes B$ of the solutions is a solution if and only if both of the following conditions hold:

1. $\{B(i) - i \pmod{|B|} | 1 \leq i \leq |B|\} = \mathbb{Z}_{|B|}$.
2. $\{B(i) + i \pmod{|B|} | 1 \leq i \leq |B|\} = \mathbb{Z}_{|B|}$.

Sufficiency in this theorem was proved by Polya in 1918 and we prove more complex part — necessity. If $A_1 = A_2 = \ldots = A_{|B|}$, we obtain The Composition Theorem.

Further we obtain two new corollaries from the Composition Theorem.
And finally, we introduce definition of $Q$-irreducible numbers $N$ for which none of the $N \times N$ solutions can be represented as a composition of smaller boards and definition of a fundamental set of solutions which is a set of arrangements which generate all solutions to the $N$-Queens Problem by the rotation and reflection of the board.

At the end, we formulate the conjecture that solves the $N$-Queens Problem and the $N$-Queens Completion for such $Q$-irreducible $N$ that $N - 1$ is $Q$-irreducible in polynomial time:

**Conjecture.** If numbers $N - 1$ and $N$ are $Q$-irreducible, then there exists a set of fundamental solutions which can be represented as a Queen function with a width less or equal to 4.

Our program has checked this conjecture for $N$ up to 14.

During the research new theoretical problems regarding prime numbers arise:

1. Are there infinitely many primes of form $2^k3^l - 1$ (where $k, l \in \mathbb{N}$)? This is a generalization of Mersenne Primes Problem.
2. Are there infinitely many primes $p$ such that $2^p + 1$ is prime too?

The paper is organized as follows. In the first section we introduce the new way of representation of queens’ arrangements and prove the Width Theorem. In the second section we introduce composition of solutions, consider generalization of composition and prove the Composition Theorem. In the third section we consider connection between the width and composition and introduce a conjecture which solves the $N$-Queens Problem and $N$-Queens Completion in polynomial time.

### 1. Width Theorem

Any arrangement $A$ can be represented as a matrix or a permutation:

![Figure 1. Arrangement $A$, $|A| = 8$](image)

**Notation 1.1.** The size of $A$ is designated by $|A|$.

It is obvious that in any column and any line there must be exactly one queen. It means that the necessary condition of being an arrangement a solution is being a permutation. Now any ascending diagonal can be characterized by constant difference of queen’s line and column. And any descending diagonal can be characterized by constant sum of queen’s line and column.

That is why we can formulate the following well-known statement.

**Statement 1.2.** Permutation $A$ is a solution to the $N$-Queens Problem if and only if

$$
∀ 1 \leq i < j \leq N \quad |i - j| \neq |A(i) - A(j)|.
$$

Now we will introduce the new way of representing solutions.
1. Thus, for any $1 \leq i \leq N$ the value of $A(i)$ is not $0$ since $A(i) = 2i \pmod{N+1}$ for $i \leq \frac{N}{2} \neq 0$. For odd $i > \frac{N}{2}$ suppose opposite. The value $A(i) = 2i + 2 \pmod{N+1} = 2i + 2 - N - 1 = 0$. Then $2i + 2 = N + 1$, but $i > \frac{N}{2}$ hence $2i + 2 > N + 2$. For even $i$ suppose opposite. Then $A(i) = 2i - 2 \pmod{N+1} = 2i - N - 3 = 0$. Then $2i = N + 3 = 12k - 12k - 1$ is odd.

Now we will show that it is a permutation. For $i, j$ which are set by the same formula $A(i) \neq A(j)$. Let $i \leq \frac{N}{2}$, $j > \frac{N}{2}$.

(1) $j$ is odd. Then $2i = 2j + 2 - (N + 1)$. Then $2(j - i - 1) = N + 1$, but $N + 1$ is odd.

(2) $j$ is even. Then $2i = 2j - 2 - (N + 1)$ or $2(j - i - 1) = N + 1$. But $N + 1$ is odd.

Now we will show that $|i - j| \neq |A(i) - A(j)|$. Suppose the opposite.

(1) If for $i < j$ $A(i)$ and $A(j)$ are set by the formula $A(l) = 2l \pmod{N+1}$, then $j - i = 2j - 2i$ or $1 = 2$. If they are set by formula $A(l) = 2l + 2 \pmod{N+1}$, then $j - i = 2j + 2 - (N + 1) = 2(i - j) or 1 = 2$. If they are set by formula $A(l) = 2l - 2 \pmod{N+1}$, then $j - i = 2j - 2 - (N + 1) - 2i + 2 + (N + 1) = 2(j - i)$.

(2) If $i \leq \frac{N}{2}$, $j > \frac{N}{2}$ and $j$ is odd, then $j - i = \pm(2i - 2j - (N + 1))$ or $±(2i - 2j + N - 1)$.

(a) $j - i = 2i - 2j + N - 1$. Then $3(j - i) = N - 1 = 12k - 5$, but $12k - 5$ is not divisible by $3$.

(b) $j - i = 2j - 2i - N + 1$. Then $j - i = N - 1$. It is possible only for $j = N$, $i = 1$, but then $j$ is even, which is another case.

(3) If $i \leq \frac{N}{2}$, $j > \frac{N}{2}$, $j$ is even, then $j - i = ±(2i - 2j - (N - 1)) = ±(2i - 2j + N + 3)$.

(a) $j - i = 2i - 2j + N + 3$. Then $3(j - i) = N + 3 = 12k - 1$, but $12k - 1$ is not divisible by $3$.

(b) $j - i = 2j - 2i - N - 3$. Then $j - i = N + 3$, which is impossible since $j \leq n$.

Thus, $|i - j| \neq |A(i) - A(j)|$ and $A$ is a solution and for $N = 12k - 4$ there exists a solution with width $2$. \[\Box\]

Lemma 1.7. Let $N = 6k$ or $N = 6k + 4$. Then the following Queen function gives a solution

$$A(i) = 2i \pmod{N+1}.$$ 

Proof. For any $1 \leq i \leq N$ the value of $A(i)$ is not $0$ since $N + 1$ is not divisible by $2$. So all function values will be in range from $1$ to $N$.

It will be a permutation: let $i \leq \frac{N}{2}$, $j > \frac{N}{2}$, suppose that $A(i) = A(j)$. Then $2i = 2j - (N + 1)$ or $2(i - j) = N + 1$, but $N + 1$ is odd.

Now let’s show that this permutation is a solution. Suppose the opposite. Let $i > j$. Then $i - j = |(2i \pmod{N+1}) - 2j \pmod{N+1}|$.

(1) $i, j \leq \frac{N}{2}$, Then $i - j = 2i(j - j)$ or $1 = 2$.

(2) $i, j > \frac{N}{2}$, Then $i - j = 2i - (N + 1) - (2j - (N + 1)) = 2(i - j)$ or $1 = 2$.

(3) $j \leq \frac{N}{2}$, $i > \frac{N}{2}$. Then

(a) $i - j = 2i - (N + 1) - 2j$. Then $i - j = N + 1$ which is impossible.

(b) $i - j = 2j - (2i - (N + 1)) = 2j - 2i + N + 1$ or $3(i - j) = N + 1$, but $N$ is not divisible by $3$.

Thus, $|i - j| \neq |A(i) - A(j)|$ and $A$ is a solution and for $N = 6k$ and $N = 6k + 4$ there exists a solution with width $1$. \[\Box\]
Lemma 1.8. Let \( N = 6k + 1 \) or \( N = 6k + 5 \). Then the following Queen function gives a solution

\[
A(i) = \begin{cases} 
2i \pmod{N+1}, & i < \frac{N}{2} \\
2i + 1 \pmod{N+1}, & i > \frac{N}{2} 
\end{cases}
\]

Proof. Obviously, it will be a permutation. Let \( i < \frac{N}{2} \), \( j > \frac{N}{2} \). Suppose that \( A(i) = A(j) \) or \( 2i = 2j + 1 - N - 1 \).

Then \( 2i - 2j = -N \) or \( j - i = \frac{N}{2} \), contradiction (\( \frac{N}{2} \) is not integer).

Now we will show that \(|i - j| \neq |A(i) - A(j)|\). Suppose the opposite.

\begin{enumerate}
\item \( j < i < \frac{N}{2} \). Then \( i - j = (2i \mod{N+1}) - (2j \mod{N+1}) = 2i - 2j = 2i - 2j - 1 = 2 \).
\item \( i > j > \frac{N}{2} \). Then \( i - j = (2i+1 \mod{N+1}) - (2j + 1 \mod{N+1}) = 2i+1 - (N+1) - (2j+1 - (N+1)) = 2i - 2j + 1 = 2 \).
\item \( j < \frac{N}{2}, i > \frac{N}{2} \). Then
\begin{enumerate}
\item \( i - j = (2i + 1 \mod{N+1}) - (2j \mod{N+1}) = 2i + 1 - (N+1) - 2j = 2i - 2j - N \). Then \( i - j = N \), contradiction.
\item \( i - j = (2j \mod{N+1}) - (2i + 1 \mod{N+1}) = 2j - (2i + 1 - (N+1)) = 2j - 2i + 1 \). Then \( 3(i - j) = N \), contradiction because \( N \) is not divisible by 3.
\end{enumerate}
\end{enumerate}

Thus, \(|i - j| \neq |A(i) - A(j)|\) and \( A \) is a solution and for \( N = 6k + 1 \) and \( N = 6k + 5 \) there exists a solution with width 2.

Note that \( \{6k + 2 \mid k \in \mathbb{N}\} = \{12k - 4 \mid k \in \mathbb{N}\} \cup \{12k + 2 \mid k \in \mathbb{N}\} \).

Lemma 1.9. Let \( N = 12k + 2 \). Then the following Queen function gives a solution

\[
A(i) = \begin{cases} 
2i + 4 \pmod{N+1}, & i < \frac{N}{2} \text{ and } i \text{ is odd or } i = N \\
2i \pmod{N+1}, & i < \frac{N}{2} \text{ and } i \text{ is even} \\
2i + 2 \pmod{N+1}, & \frac{N}{2} \leq i < N 
\end{cases}
\]

Proof. For any \( 1 \leq i \leq N \) the value of \( A(i) \) is not 0 since in the first part of the formula \( i <= \frac{N}{2} \) (or \( A(N) = 2 \)) and odd \( i \) by the formula \( 2i + 4 \leq N < N + 1 \) or \( A(i) \neq 0 \). In the second part \( i \leq \frac{N}{2} - 1 \) we have \( 2i \leq N - 2 < N + 1 \). In the third part \( N + 2 \leq 2i + 2 < 2N + 2 \) or \( 2i + 2 \pmod{N+1} \neq 0 \).

Now we will show that it is a permutation. For \( i, j \) which are set by the same formula \( A(i) \neq A(j) \). In other cases

\begin{enumerate}
\item \( i < \frac{N}{2} \) and \( \frac{N}{2} \leq j < N \). Suppose the opposite \( A(i) = A(j) \).
\begin{enumerate}
\item \( i \) is odd or \( i = N \). Then \( 2i + 4 \pmod{N+1} = 2j + 2 \pmod{N+1} \) which is \( 2i + 4 = 2j + 2 - (N + 1) \) or \( 2i + 2 - (N + 1) = 2 \). Then we get \( 2(j - i + 1) = N + 1 \) or \( 2j = N + 1 \) which is impossible because \( N + 1 = 12k + 3 \) is odd.
\item \( i \) is even. Then \( 2i \pmod{N + 1} = 2j + 2 \pmod{N + 1} \) or \( 2i = 2j + 2 - (N + 1) \). And now we get \( 2(j - i + 1) = N + 1 = 12k + 3 \) contradiction.
\end{enumerate}
\item \( i, j < \frac{N}{2} \) and \( i \) is even, \( j \) is odd. Then \( 2i \pmod{N + 1} = 2j + 4 \pmod{N + 1} \) or \( i - j = 2 \), but \( i \) and \( j \) have different parity.
\end{enumerate}
\end{enumerate}

Now we will show that \(|i - j| \neq |A(i) - A(j)|\). Suppose the opposite. If for \( i \) and \( j \) \( A \) is set by the same formula it is obvious. In other cases

\begin{enumerate}
\item \( j < i < \frac{N}{2} \), \( j \) is odd, \( i \) is even. Then
\begin{enumerate}
\item \( i - j = (2i \pmod{N + 1}) - (2j + 4 \pmod{N + 1}) = 2i - 2j - 4 \) or \( i - j = 4 \), but they have different parity.
\item \( j < \frac{N}{2} \), \( j \) is odd and \( \frac{N}{2} \leq i < N \). Then
\begin{enumerate}
\item \( i - j = (2i + 2 \pmod{N + 1}) - (2j \pmod{N + 1}) = 2i + 2 - (N + 1) - 2j + 4 \), but they have different parity.
\item \( i - j = (2j + 4 \pmod{N + 1}) - (2i + 2 \pmod{N + 1}) = 2j + 4 - (2i + 2 - N - 1) \). Then \( 3(i - j) = 12k + 5 \), impossible.
\end{enumerate}
\item \( j < \frac{N}{2} \), \( j \) is even and \( \frac{N}{2} \leq i < N \). Then
\begin{enumerate}
\item \( i - j = (2i \pmod{N + 1}) - (2j \pmod{N + 1}) = 2i - 2j + 1 - N - 1 \) or \( i - j = 12k + 1 \), impossible.
\item \( i - j = (2j \pmod{N + 1}) - (2i + 2 \pmod{N + 1}) = 2j - 2i + N + 1 \) or \( 3(i - j) = N - 1 \) or \( 3(i - j) = 12k + 1 \), impossible.
\end{enumerate}
\end{enumerate}
\end{enumerate}

Thus, \(|i - j| \neq |A(i) - A(j)|\) and \( A \) is a solution and for \( N = 12k + 2 \) there exists a solution with width 3. \( \square \)
Lemma 1.10. Let \( N = 6k + 3 \). Then the following Queen function gives a solution

\[
A(i) = \begin{cases}
2i + 2 \pmod{N + 1}, & i < \frac{N - 1}{2} \\
2i + 4 \pmod{N + 1}, & i = \frac{N - 1}{2} \\
2i + 5 \pmod{N + 1}, & i > \frac{N - 1}{2}.
\end{cases}
\]

Proof. For any \( 1 \leq i \leq N \) the value of \( A(i) \) is not 0 since \( i \neq \frac{N - 1}{2} \), \( A(i) = 2i \pmod{N + 1} = 2i \neq 0 \). For \( i = \frac{N - 1}{2} \), \( A(i) = 2 \). For \( \frac{N - 1}{2} < i < N - 1 \), \( A(i) = 2i + 5 \pmod{N + 1} = 2i - N + 4 \neq 0 \) and \( A(N - 1) = 1 \), \( A(n) = 3 \). Now we will show that \( |i - j| \neq |A(i) - A(j)| \). Suppose the opposite.

(1) \( i < \frac{N - 1}{2}, j = \frac{N - 1}{2} \). Then \( j - i = \pm(2 - 2i - 2) = \pm 2i \).
   (a) \( j - i = 2i \). Then \( 2i = j = \frac{N - 1}{2} = \frac{6k + 2}{2} = 3k + 1 \).
   (b) \( j - i = -2i \). Then \( i + j = 0 \).

(2) \( i < \frac{N - 1}{2}, \frac{N - 1}{2} < j < N - 1 \). Then \( j - i = \pm(2i + 5 - N - 1 - 2i - 2) = \pm(2j - i) + N - 2 \).
   (a) \( j - i = 2(j - i) - N + 2 \). Then \( j - i = N - 2 \).
   (b) \( j - i = -2(j - i) + N - 2 \). Then \( 3(j - i) = N - 2 = 6k + 1 \).

(3) \( i < \frac{N - 1}{2}, j \geq N - 1 \). Then \( j - i = \pm(2j + 5 - 2N - 2 - 2i - 2) = \pm(2j - i) - 2N + 1 \).
   (a) \( j - i = 2(j - i) - 2N + 1 \). Then \( j - i = 2N - 1 \).
   (b) \( j - i = -2(j - i) + 2N - 1 \). Then \( 3(j - i) = 2N - 1 = 12k + 5 \).

(4) \( i = \frac{N - 1}{2}, \frac{N - 1}{2} < j < N - 1 \). Then \( j - i = \pm(2j + 5 - N - 1 - 2) = \pm(2j - N + 2) \).
   (a) \( j - i = 2j - N + 2 \). Then \( j = N - 2 - i = \frac{2N - 4 - N + 1}{2} = \frac{N - 3}{2} < \frac{N - 1}{2} \).
   (b) \( j - i = N - 2 - 2j \). Then \( 3j = N - 2 + i = \frac{2N - 4 + N - 1}{2} = \frac{3N - 5}{2} < \frac{3(N - 1)}{2} \).

(5) \( i = \frac{N - 1}{2}, j \geq N - 1 \). Then \( j - i = \pm(2j + 5 - 2N - 2 - 2) = \pm(2j - 2N + 1) \).
   (a) \( j - i = 2j - 2N + 1 \). Then \( j = 2N - 1 - i = \frac{3N - 1}{2} > N \).
   (b) \( j - i = 2N - 2j - 1 \). Then \( 3j = 2N + 1 + i = \frac{5N - 3}{2} < 3(N - 1) \).

(6) \( \frac{N - 1}{2} < i < N - 1, j \geq N - 1 \). Then \( j - i = \pm(2j + 5 - 2N - 2 - 2i - 2 + 5 + N + 1) = \pm(2j - i) - N - 1 \).
   (a) \( j - i = 2(j - i) - N - 1 \). Then \( j - i = N + 1 \).
   (b) \( j - i = -2(j - i) + N + 1 \). Then \( 3(j - i) = n + 1 = 6k + 4 \).

Thus, \( |i - j| \neq |A(i) - A(j)| \) and \( A \) is a solution and for \( N = 6k + 3 \) there exists a solution with width 3.

Thus, the width theorem is proved by building the examples of Queen functions for arbitrary values of \( N \).

\[ \square \]

Remark 1.11. The width of the function in the theorem cannot be reduced, since for \( N = 15 \) our program checked that there are no solutions that can be represented as a Queen function with width 1 or 2.

Also, all known solutions (1874 — Glaisher, 1969 — Hoffman, Loessi, Moore, 1991 — Bernhardsson) have a greater width.

Here is the example of our solution and the easiest known solution for \( N = 20 \).

\[ \text{Figure 2. Author’s solution with width 2} \hspace{1cm} \text{Figure 3. Bernhardsson’s solution with width 4} \]
2. Composition Theorem

Definition 2.1. Given to arbitrary solutions $A$ and $B$. Then we can obtain new arrangement by insertion of one arrangement into queens’ positions of another arrangement. The obtained arrangement is called composition $A \otimes B$.

For example consider two solutions $A$ and $B$:

By we definition of composition we can obtain two new arrangements:

It is easy to see that composition of solutions is not always a solution. Thus we found necessary and sufficient condition of being a composition of solutions a solution:

The Composition Theorem. Composition $A \otimes B$ of the solutions $A$ and $B$ is a solution if and only if both of the following conditions hold:

1. $\{B(i) - i \ (\text{mod} \ |B|) \mid 1 \leq i \leq |B|\} = \mathbb{Z}_{|B|}$.
2. $\{B(i) + i \ (\text{mod} \ |B|) \mid 1 \leq i \leq |B|\} = \mathbb{Z}_{|B|}$.

To prove this theorem we will consider more general construction and prove the same criterion for it.

Definition 2.2. Generalized composition of solutions $(A_1, A_2, \ldots, A_{|B|}) \otimes B$ is an arrangement which is defined by the following rule

$$C(|B|(i - 1) + j) = |B|(A_j(i) - 1) + B(j),$$

where $|A_i| = |A_j| \ (1 \leq i < j \leq |B|), \ 1 \leq i \leq |A|, \ 1 \leq j \leq |B|$.

This construction is taken from [2] and firstly introduced by Polya in [7].

Obviously, if arrangements $(A_1, A_2, \ldots, A_{|B|})$ are the same, then we get usual composition of solutions.

Theorem 2.3. Generalized composition $(A_1, A_2, \ldots, A_{|B|}) \otimes B$ of the solutions is a solution if and only if both of the following conditions hold:

1. $\{B(i) - i \ (\text{mod} \ |B|) \mid 1 \leq i \leq |B|\} = \mathbb{Z}_{|B|}$.
2. $\{B(i) + i \ (\text{mod} \ |B|) \mid 1 \leq i \leq |B|\} = \mathbb{Z}_{|B|}$.
Proof. Sufficiency was proved in 1918 by Polya in [7].

We will prove it again and also prove more complex part of this statement — necessity.

Note that any integer \(1 \leq m \leq |A||B|\) can be uniquely represented as \(m = |B|(i - 1) + j\), \((1 \leq i \leq |A|, 1 \leq j \leq |B|)\). Then for the chessboard \(|A||B| \times |A||B|\) we will set the queens’ arrangements by the formula

\[
C(|B|(i - 1) + j) = |B|(A_s(i) - 1) + B(j).
\]

Firstly, we will prove that this arrangement is a permutation. It is obvious since for different numbers their maps are either in different intervals or in one interval but with different values because \(A_s, B\) are solutions.

Secondly, we will prove that this permutation is a solution. Let \(1 \leq s < r \leq |A||B|\). We have to prove \(s - r \neq \pm(C(s) - C(r)) \neq \pm(C(|B|(i_1 - 1) + j_1) - C(|B|(i_2 - 1) + j_2)) \neq \pm(|B|(A_s(i_1) - 1) + B(j_1) - |B|(A_s(i_2) - 1) - B(j_2)) \neq \pm(|B|(A_s(i_1) - A_s(i_2)) + (B(j_1) - B(j_2))). We get that

\[
\text{(1)} \quad |B|(|i_1 - i_2| \pm (A_s(i_2) - A_s(i_1))) \neq |B|(j_1) - B(j_2) - (j_1 - j_2).
\]

First, we will prove sufficiency. Suppose the opposite: inequality \(\text{(1)}\) doesn’t hold. The conditions of the theorem are satisfied. Specifically, integers \(B(i) - i\) are different modulo \(|B|\) and integers \(B(i) + i\) are different modulo \(|B|\). Then the right-hand part of \(\text{(1)}\) (now it is equality) is not divisible by \(|B|\) and the required equality doesn’t hold.

Now we will prove the necessity. We consider cases of different sign before the expression:

\[
\text{(2)} \quad |B|(|A_s(i_2) - i_2| - |A_s(i_1) - i_1|) \neq (B(j_1) - j_1) - (B(j_2) - j_2).
\]

Suppose the opposite. Such integers \(j_1, j_2\), that \(B(j_1) - j_1 \equiv B(j_2) - j_2 (\text{mod } |B|)\) exist. Then \(|B|\) divides \(B(j_2) - j_2 - B(j_1) - j_1\). Note that \(-2|B| + 3 \leq B(j_2) - j_2 - B(j_1) + j_1) \leq 2|B| - 3\). Then \(B(j_2) - j_2 - B(j_1) - j_1 = \pm|B|\). Then we will divide both parts of the inequality by \(|B|\) and we get \((A_s(i_1) - i_1) - (A_s(i_2) - i_2) \equiv \pm 1\). What is more \(\forall 1 \leq p \leq |B|\) \(2 \leq A_p(i) + i \leq 2|A|\). Then we arrange in non-decreasing order \(|A||B|\) integers \(A_p(i) + i\) so that \((A_s(i_1) + i_1) - (A_s(i_2) + i_2) \equiv \pm 1\). There will be more than \(|A| - 1\) different integers among them. The following inequality \(A_p(i) + i - (A_q(j) + j) \geq 2\) holds for them. Then we will add up all these inequalities and get that the difference between the largest and the least numbers is not fewer than \(2|A| - 2\). But the largest possible difference is \(2|A| - 3\).

Necessity is proved.

\(\square\)

**Proof of The Composition Theorem.** This statement is a special case of the generalized composition theorem 2.3, where \(A_1 = A_2 = \ldots = A_{|B|}\).

The next theorem is proved by Hedayat in [3]:

**Statement 2.4** (Hedayat’s Lemma 2.2 in [3]). A permutation \(B\) such that \(\{B(i) - i \pmod{|B|}\} | 1 \leq i \leq |B|\} = \mathbb{Z}_{|B|}\) and \(\{B(i) + i \pmod{|B|}\} | 1 \leq i \leq |B|\} = \mathbb{Z}_{|B|}\) exists if and only if \(\gcd(|B|, 6) = 1\).

Using this statement we obtain the following two corollaries.

**Corollary 2.5.** If \(A \otimes B\) is a solution, then \(\gcd(|B|, 6) = 1\). The opposite implication does not hold.

**Proof.** If \(A \otimes B\) is a solution, then \(\{B(i) - i \pmod{|B|}\} | 1 \leq i \leq |B|\} = \mathbb{Z}_{|B|}\); \(\{B(i) + i \pmod{|B|}\} | 1 \leq i \leq |B|\} = \mathbb{Z}_{|B|}\) by the composition theorem. And finally by the previous statement \(\gcd(|B|, 6) = 1\).

But the opposite does not hold because for example for \(|B| = 7\) there exists a solution

\[
B = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
4 & 7 & 5 & 2 & 6 & 1 & 3
\end{pmatrix},
\]

which doesn’t satisfy the required condition.

\(\square\)

**Corollary 2.6.** If \(A \otimes B\) is a solution, then \(C \otimes B\) is a solution for any solution \(C\).

**Proof.** Based on the composition theorem, it is easy to see that criterion of being a composition of solutions \(A \otimes B\) doesn’t depend on the first arrangement \(A\).

\(\square\)
3. Connection between width and composition: conjecture

It is easy to see that the width of the composition is quite large and it is impossible to find a constant bound on its width. According to this we introduce the next definition:

Definition 3.1. Number $N$ is called Q-irreducible, if none of the $N \times N$ solutions can be represented as a composition of smaller boards.

Statement 3.2. Number $N$ is Q-irreducible if and only if $N$ equals either $p$, or $2p$, or $3p$, or $2^k3^l$, where $p$ is prime and $k, l \in \mathbb{N}_0$.

Proof. It is easy to see that if $N$ is equal to either $p$, or $2p$, or $3p$, or $2^k3^l$, then it is Q-irreducible.

Now we prove the necessity. Suppose the opposite. $N$ is neither $p$ or $2p$ or $3p$ or $2^k3^l$. Firstly, if $N = np$ (where $n > 3$), then there exists a solution which is a composition of arrangements $A$ and $B$, where $|A| = n$ and $|B| = p$. Secondly, if $N = 2^k3^l s$ (where $s \neq p$), then $s$ is not divisible by 2 and 3 and consequently $\gcd(s, 6) = 1$. Thus, for such $N$ there exists a solution which is composition of smaller boards.

Also operation of rotation of the board doesn’t save the width of representation. Thus, we introduce the next definition:

Definition 3.3. A fundamental set of solutions is a set of arrangements which generate all solutions to the $N$-Queens Problem by the rotation and reflection of the board.

Since generalized composition gives lots of solutions with large width, we consider Q-irreducible $N$. Also a queen can be arranged in the corner of the smaller board and $N \times N$ solution can be obtained. That is way $N – 1$ must be Q-irreducible.

Conjecture 3.4. If numbers $N – 1$ and $N$ are Q-irreducible, then there exists a set of fundamental solutions which can be represented as a Queen function with a width less or equal to 4.

This conjecture is checked by our program for $N$ up to 14. Currently, the number of solutions is known only for values of $N \leq 27$.

For example, numbers 2018 and 2019 satisfy the condition of the conjecture (because 2017 is a prime, 2018 = 2 · 1009 is a doubled prime, 2019 = 3 · 673 is a tripled prime).

If this conjecture is correct, then the N-Queens Problem and, consequently, the N-Queens Completion can be solved in polynomial time. Also then the number of solutions to the N-Queens Problem is bounded by the polynomial for such Q-irreducible $N$ that $N – 1$ is also Q-irreducible.

Based on the conjecture, new problem arise: are there infinitely many integers, satisfying the condition of the conjecture?

Let $N = 2^k3^l$. Then $N – 1$ is not divisible by 2 and 3. Thus $N – 1$ must be prime and the question is the next one: are there infinitely many primes of form $2^k3^l – 1$ (where $k, l \in \mathbb{N}_0$)? This is a generalization of Mersenne Primes Problem, because it is easy to see that for $l = 0$ it is the Mersenne Primes Problem.

And the second problem is the next one: are there infinitely many primes $p$ such that $2p + 1$ is prime too?

Acknowledgments

The author would like to thank Dr. of Science (Habilitation) Stanislav Kublanovsky for problem statement and helpful discussion. Author is also grateful to Nikita Tepelin for assistance in writing programs.

References

[1] I.P. Gent, C. Jefferson, P. Nightingale. Complexity of $n$-Queens Completion, Journal of Artificial Intelligence Research 59 (2017) 815 – 848.

[2] I. Rivin, I. Vardi and P. Zimmerman. The $n$-Queens Problem, The American Mathematical Monthly, Vol. 101, No. 7 (Aug. - Sep., 1994), pp. 629-639.

[3] A. Hedayat. A Complete Solution to the Existence and Nonexistence of Knut Vik Designs and Orthogonal Knut Vik Designs, Journal of Combinatorial Theory (A) 22, 331-337 (1977).

[4] B. Abramson. Divide and Conquer under Global Constraints: A Solution to the $N$-Queens Problem, Journal of Parallel and Distributed Computing, 6, 649-662 (1989).

[5] J. Bell, B. Stevens. A survey of known results and research areas for $n$-queens, Discrete Mathematics 309 (2009) 1–31.

[6] E.J. Hoffman, J.C. Loessi and R.C. Moore. Constructions for the Solution of the $m$ Queens Problem, Mathematics Magazine, Vol. 42, No. 2 (Mar., 1969), pp. 66-72.

[7] G. Polya. Über die “doppelt-periodischen” Lösungen des $n$-Damen-Problems, in: W. Ahrens (Ed.), Mathematische Unterhaltungen und Spiele, vol. 2, 2nd ed., B.G. Teubner, 1918, pp. 364-374

School 564, Saint Petersburg, 190005 Russia
E-mail address: mikhaylovsyki.dmitriy@gmail.com