RESEARCH ARTICLE

Anti-modularization for both high robustness and efficiency including the optimal case

Jaeho Kim*, Yukio Hayashi

Divison of Transdisciplinary Sciences, Japan Advanced Institute of Science and Technology, Nomi, Ishikawa, Japan

* s2160002@jaist.ac.jp

Abstract

Although robustness of connectivity and modular structures in networks have been attracted much attentions in complex networks, most researches have focused on those two features in Erdos-Renyi random graphs and Scale-Free networks whose degree distributions follow Poisson and power-law, respectively. This paper investigates the effect of modularity on robustness in a modular *d*-regular graphs. Our results reveal that high modularity reduces the robustness even from the optimal robustness of a random *d*-regular graph in the pure effect of degree distributions. Moreover, we find that a low modular *d*-regular graph exhibits small-world property that average path length is $O(logN)$. These results indicate that low modularity on modular structures leads to coexistence of both high robustness and efficiency of paths.

Citation: Kim J, Hayashi Y (2024) Anti-modularization for both high robustness and efficiency including the optimal case. PLoS ONE 19(3): e0301269. https://doi.org/10.1371/journal.pone.0301269

Editor: Mingyang Lu, Northeastern University, UNITED STATES

Received: November 4, 2023

Accepted: March 13, 2024

Published: March 28, 2024

Data Availability Statement: The minimal data set can be accessed at: https://github.com/KJH-JAIST/Modules.

Funding: This research is supported in part by JSPS KAKENHI Grant Number JP.21H03425. The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Competing interests: The authors have declared that no competing interests exist.

Introduction

Energy, transportation, and communication systems provide essential services for supporting human activity and society. However, in these network systems, there is a common topological structure called Scale-Free (SF), which has the extreme vulnerability against malicious attacks to hubs [1]. Therefore, constructing more robust networks is one of the important issues in complex networks. Recently, it has been revealed that enhancing loops is crucial for constructing a robust network in supporting from the asymptotical equivalence of network dismantling and decycling problems when the second moment of degree is not divergent [2]. Here, the dismantling problem is to find the minimum set of nodes which removal makes a network fragmented into at most a given size, while the decycling problem is to find the minimum set of nodes which are necessary to form loops. When all loops are removed from a network, the network becomes a tree which is easily fragmented by any articular-node removals. Thus, enhancing loops is important to make a network hard to become a tree. Actually, several rewiring methods [3] based on enhancing loops generate robust networks with a common phenomena of decreasing the gap between the maximum and minimum degrees. In other words, the network is more robust as the gap becomes smaller. In the extreme case, it is suggested that a random *d*-regular graph with zero gap has the optimal robustness in the pure effect of degree distributions [4, 5]. Regular graphs have been so far studied mainly for not robustness but spectral analysis [6] or graph theory, while there are huge researches [7, 8] for robustness in Erdos-renyi (ER) random graphs and SF networks. Therefore, regular graphs become a blind spot in investigating the robustness of connectivity.

On the other hand, a modular structure is also an important issue in complex networks, because many real-world networks have modular structures. For example, in social networks, modules are corresponding to communities or groups with shared interests or backgrounds. If a network has high modularity, nodes in a same module are densely connected to each other, whereas nodes in different modules are sparsely connected.

Recently, it has been shown that [9, 10] ER random graphs and SF networks with modular structures become weaker against attacks than them without modular structures. Here, the modularity of networks is controlled by rewiring links. Moreover, Module-Based (MB) attacks which are targeting interconnected nodes with high betweenness centrality are highly destructive to modular networks [11]. Thus, we predict that random d-regular graphs with modules become vulnerable against MB attacks, even the original graphs have the optimal robustness [4, 5]. The modularity of the modular network is controlled by rewiring inspired from [9, 10] with preserving degree distributions. In addition, we show that d-regular graphs with low modularity have both high robustness of connectivity and efficiency of paths.

This paper is organized as follows. First, we introduce a modular network of d-regular graphs and an anti-modularization that is rewiring links to decrease the modularity. Second, we show that rewired networks on anti-modularization have high robustness of connectivity and efficiency of paths. Third, we modify the conventional modularization [10] to maintain d-regular graphs and show that modified modularization has the same results with our anti-modularization. Finally, we summarize the obtained results.

Control of modularity

We consider a modular network that consists of random d-regular graphs. Each of random d-regular graphs corresponds to a module. As shown in Fig 1A, m_o modules with size N_m are initially connected as a ring. Here, the total number of nodes and links are constant $N = N_m \times m_o$ and $M = (d \times N)/2$ in the network. The initial configuration of modular network has considerably high modularity, because a ring structure maintains the connectivity of the entire network

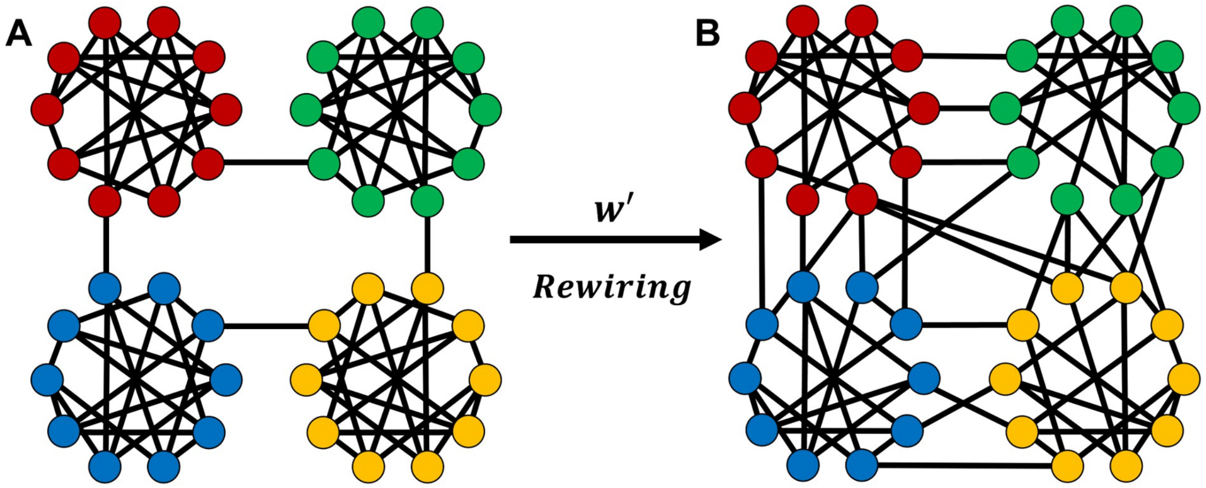

Fig 1. Configuration of a modular network before/after rewirings. (A) Initial configuration of strongly modular network. (B) Rewired modular network to increase the robustness of connectivity. Node colors indicate modules.

https://doi.org/10.1371/journal.pone.0301269.g001 by the minimum number of inter-module links (inter-links) and the maximum number of intra-module links (intra-links). However, this network is extremely vulnerable by removing target nodes which are connecting between modules. As a special case, when each module is set as a clique, such network is called caveman graph [12]. For a caveman graph, small-world (SW) property with the average path length of $O(logN)$ emerges by rewiring from a few intra-links to inter-links. We discuss not only the robustness but also the efficiency with SW property in modular networks of d-regular graphs.

To control the modularity of network, intra-links are rewired to inter-links on anti-modularization as shown in Fig 1B. This is regarded as the inverse process of the conventional modularization [10], although it tends to not make a ring as mentioned later. Table 1 shows the initial number of intra- and inter-links. By rewirings, the number of intra-links is only decreasing on anti-modularization, because the sum of intra- and inter-links is constant M. In contrast, the number of inter-links is only decreasing on modularization [10]. With a rewiring rate w', intra-links are randomly rewired to inter-links on anti-modularization as shown in Fig 1(B), while with a rewiring rate w, inter-links are randomly rewired to intra-links on modularization [10]. Moreover, the relation of w' and w is derived from the following equation

$$m_o + w'(M - m_o)w' = (1 - w)(M - M/m_o), \tag{1}$$

whose left- and right-hand sides are the existing number of inter-links on anti-modularization and the remaining number of them on modularization [10] after both rewirings. Then, we have

$$w' = 1 - \frac{1 + w(m_o - 1)}{m_o(M - m_o)} M. \tag{2}$$

The detail process of anti-modularization is summarized as follows. Through the process, the degree distributions and whole connectivity of rewired networks are maintained, while they are not on the conventional modularization [10]. We will compare such differences in the next section.

Step 1 At first, remove an intra-link randomly in a module. Then, randomly select one end-node of the removed link.

Step 2 Remove another intra-link randomly in a different module from that in Step1. Then, randomly select one end-node from the removed link.

Step 3 Create a new inter-link between two selected nodes by rewiring.

Step 4 Remove another intra-link randomly in a different module from that in Step 2 or the previous Step 4. Then, randomly select one end-node from the removed link.

Step 5 To preserve the degree at a node, the unselected end-node in Step 2 or the previous Step 4 is selected again. Create a new inter-link between two selected nodes by rewiring.

Step 6 Steps 4 and 5 are repeated until $w'(M - m_o)$ inter-links are created for a given $0 < w' < 1$. If connected components or nodes are isolated by rewiring, select other end-node or

Table 1. Initial numbers of intra- and inter- links.

	Intra-links	rewirings	Inter-links
anti-modularization	$M - m_o$	$\underset{\rightarrow}{w'}$	m_o
modularization [10]	M/m_o	$\underset{\leftarrow}{w}$	$M - M/m_o$

https://doi.org/10.1371/journal.pone.0301269.t001 intra-link again. At the end of repeated process, the last inter-link is connected to the node which is unselected in Step 1.

To investigate the robustness of connectivity, the following three types of attacks RF, IB, and MB are considered. In RF (Random Failures), nodes are randomly selected for removal. In IB (Initial Betweenness) attacks, nodes are selected in decreasing order of betweenness centrality. In MB (Module-Based) attacks [11], nodes are basically selected in decreasing order of betweenness centrality, however the nodes belong to the Largest Connected Component (LCC) and end-nodes of inter-links have the order of priority. MB and IB attacks are highly distructive especially for modular networks [11], while RF gives well-known typical damages and is considered to compare the robustness with them.

Coexistance of robustness and efficiency

We investigate the robustness of connectivity and efficiency of paths in rewired networks on anti-modularization. In addition, we compare the robustness in rewired networks on both anti-modularization and modified modularization to maintain degree distribution, and show that the results for both modularization are almost coincidence. Here, the degree and the size of modular network are $d = 4, 9, 19$ and $N = 10^4$. Since N is constant, the size of each module N_m is also constant for a given number m_o of modules which is a control parameter. When m_o is maximum, the module becomes a clique K_{d+1} in a caveman graph [12]. Modularity Q and following eight measures are investigated and are averaged over 100 realizations for the networks in varying a rewiring rate w'.

- Modularity [13] $Q = \frac{1}{2M}\sum_{i,j}\left(A_{ij} - \frac{k_i k_j}{2M}\right)\delta_{i,j}$, where A is adjacency matrix, k_i is degree of node i, and $\delta_{i,j}$ is 1 if nodes i and j belong to a same module or 0 otherwirse.
- Ratio $S^{1st}(q)/N$ of the 1st LCC size, where $S^{1st}(q)$ denotes the number of nodes in the 1st LCC after attacks to qN nodes. $0 < q \leq 1$ is a fraction of attacks.
- Robustness

  1. Robustnes index [14] $R = \frac{1}{N}\sum_{q=\frac{1}{N}}^{1}\frac{S(q)}{N}$ after attacks to qN nodes. The summation means $q = \frac{1}{N}, \frac{2}{N}, \ldots \frac{N-1}{N}$, and $\frac{N}{N} = 1$.
     Except for R, there are other following measures of robustness [15] in the viewpoints of shortest paths and graph spectrum.
  2. Reciprocal of network efficiency $H = \frac{1}{\frac{2}{N(N-1)}\sum_{i\in V}\sum_{j\in V, i\neq j}\frac{1}{d_{ij}}}$, where d_{ij} denotes the shortest path length between nodes i and j. H is called harmonic mean.
  3. Average path length $L = \frac{1}{N(N-1)}\sum_{i,j} d_{ij}$, where d_{ij} denotes the shortest path length between nodes i and j. L is called arithmetic mean.
  4. Diameter $D = max\{d_{ij}\}$, where d_{ij} is the shortest path length between node i and j. Small values of H, L and D mean that a network is robust.
  5. Average betweenness centrality $b = \frac{1}{N}\sum_{k\in V}\sum_{i\in V}\sum_{j\in V, i\neq j\neq k}\frac{n_{ij}(k)}{n_{ij}}$, where $n_{ij}(k)$ is the number of shortest paths between node i and j through node k. A small value of b indicates that lots of nodes are connected by the shortest path without relying on specific nodes like hubs.

6. Spectral gap $\lambda_d = \lambda_1 - \lambda_2$, which is the difference between the largest and second largest eigenvalues λ_1 and λ_2 of the adjacency matrix of a network. Since a small value of λ_d is related to network bottlenecks and bridges, a larger value of λ_d indicates better robustness.

7. Algebraic connectivity μ_2, which is the second smallest eigenvalue of the Laplacian matrix of a network. A larger value of μ_2 means more rapid diffusion.

Increasing robustness by anti-modularization

Mainly, we explain the results for $d = 9$. See figures from S3 to S8 Figs as similar results obtained for $d = 4$ and $d = 19$. We investigate the ratio $S^{1st}(q)/N$ of the 1st LCC size against MB attacks in rewired networks on anti-modularization. Fig 2A–2F are corresponding to 9-regular graphs with $m_o = 1000, 500, 100, 50, 20$, and 5, respectively. As shown in Fig 2A, the curve for $w' = 0$ (gray line) decreases very rapidly because of initial ring structure. However, as the rewiring rate w' increases on anti-modularization, the curves are shifting to right. At $w' = 0.9$, the curve is approaching purple lines for non-modular random d-regular graphs. Such curve-shifting are also observed in the results for different size of modules $m_o = 500, 100, 50, 20$, and 5 in each of Fig 2B–2F. In comparing with same color lines in Fig 2A–2E, curves are more shifting to right as smaller m_o.

On the other hand, in Fig 2A–2F, curves for $w' \geq 0.5$ (blue and purple lines) are almost identical. Moreover, as shown in Fig 2F, for $w' = 0$ and 0.1 (gray and red lines), the curves rapidly decrease to $S^{1st}(q)/N \approx N_m/N = 2000/10000 = 0.2$ at first. Then, the curves gradually decrease from around 0.2. Note that MB attacks destroy a network in two steps. First, MB attacks are targeting the end-nodes of inter-links, and divide into several isolated modules. Next, each of isolated modules is collapsed gradually. See S1 and S2 Figs in cases of IB attacks and RF.

Table 2 shows a critical fraction q_c denoted by q_c^{MB}, q_c^{IB}, and q_c^{RF} at the maximum size of the 2nd LCC against MB, IB attacks and RF in rewired networks with $d = 9$ and $m_o = 200$. Since the 1st LCC is fragmented at the critical fraction q_c, the whole connectivity is broken considerably. Values of q_c^{MB}, q_c^{IB}, and q_c^{RF} increase as larger w'. Especially, q_c^{MB}, q_c^{IB} are rapidly increasing between the case of $w' = 0.1$ and $w' = 0.3$. When $w' \leq 0.3$, q_c^{RF} is higher than q_c^{MB} and q_c^{IB}. However, when $w' \geq 0.5$, q_c^{RF} becomes lower than q_c^{MB} and q_c^{IB}. In particular, for $w' = 0.9$, q_c^{IB} is approaching 0.875, which is the percolation threshold $1 - 1/(d - 1) = 1 - 0.125$ for $d = 9$ in random d-regular graphs [4]. From Table 2, we find that random d-regular graphs with low modularity ($w' \geq 0.5$) have stronger robustness with high q_c against selected IB attacks than that against unintended RF. This phenomena is unusual in ER random graphs or SF networks [16]. As a considerable reason, IB attacks remove only the core part which is frequently passed by the shortest paths, while the remaining nodes maintain the connectivity on the peripheral in d-regular graphs.

We note that the rewired networks for high w' on anti-modularization have low modularity. Fig 3 shows that robustness index R against each of three types of attacks is monotonically decreasing function of modularity Q even for varying m_o shown by color lines. In Fig 3A and 3B, when $Q < 0.2$, all colored curves are approaching cyan lines, which indicates the robustness index R_{IB} against IB attacks for non-modular random 9-regular graphs. All colored curves in Fig 3C are also approaching cyan lines when $Q < 0.5$. In addition, there are two behaviors among curves in Fig 3A and 3B. One is that, from $m_o = 1000$ to $m_o = 50$, red curves are shifting to green curves. The other is that, from $m_o = 50$ to $m_o = 5$, green curves are shifting to purple

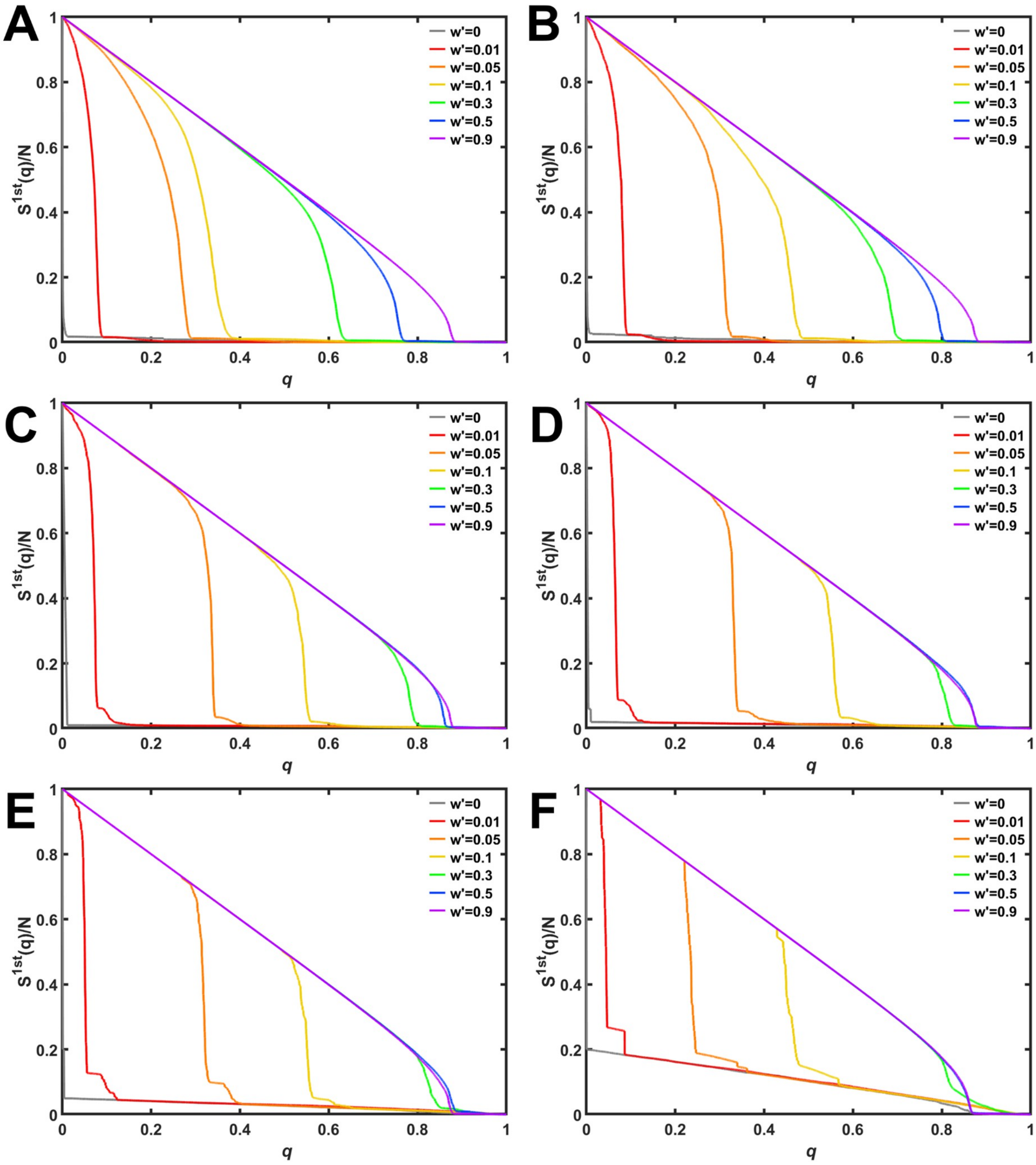

Fig 2. The 1st LCC size against MB attacks in rewired networks with $d = 9$ and the number m_o of modules. (A) $m_o = 1000$, (B) $m_o = 500$, (C) $m_o = 100$, (D) $m_o = 50$, (E) $m_o = 20$, and (F) $m_o = 5$. Color lines represent the rewiring rates w' on anti-modularization.

https://doi.org/10.1371/journal.pone.0301269.g002

Table 2. Values of the critical fraction q_c against three types of attacks in rewired networks with $d = 9$ and $m_o = 200$.

	w'=0.01	w'=0.05	w'=0.1	w'=0.3	w'=0.5	w'=0.9
MB	0.075	0.340	0.546	0.786	0.858	0.874
IB	0.092	0.353	0.559	0.803	0.886	0.911
RF	0.592	0.775	0.809	0.848	0.850	0.861

https://doi.org/10.1371/journal.pone.0301269.t002

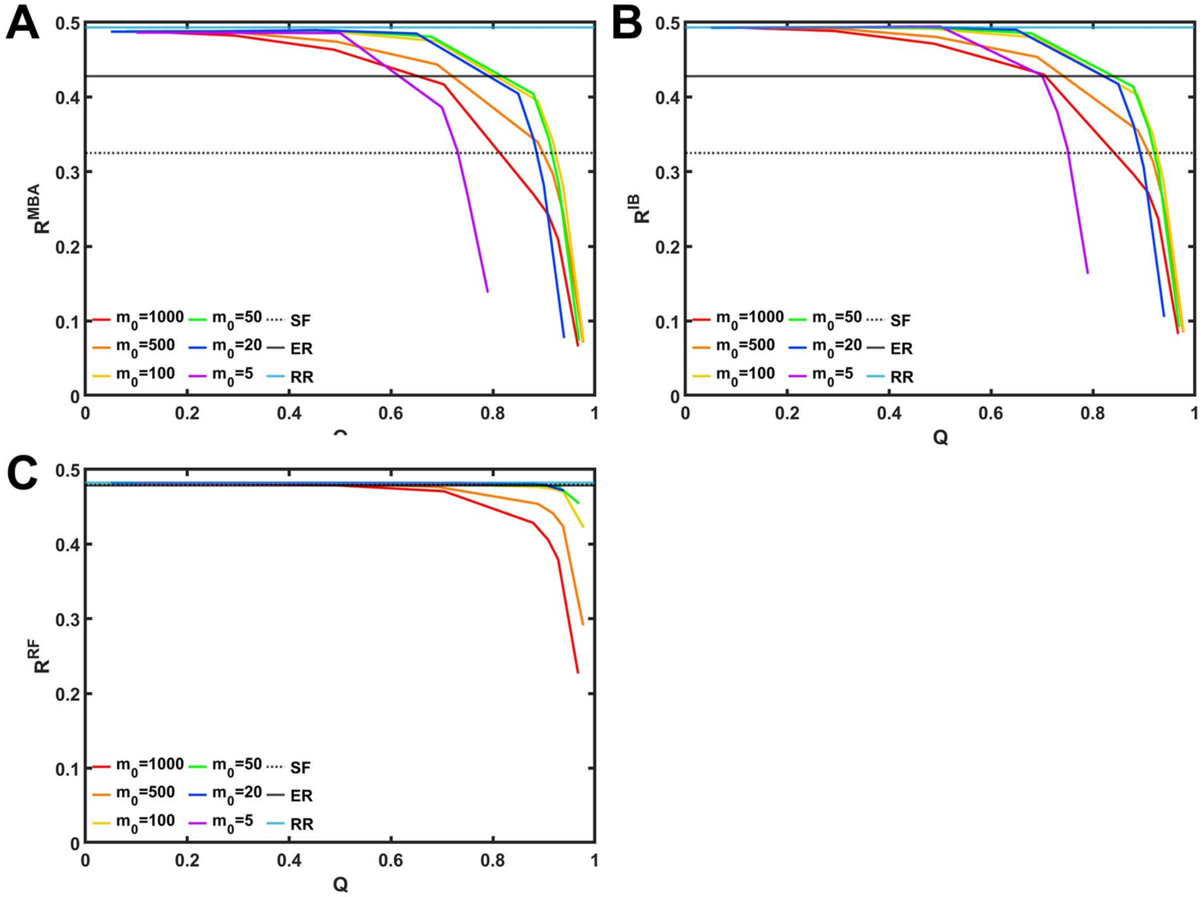

Fig 3. Relation between modularity *Q* and robustness index *R* against three types of attacks. (A) R_{MB} against MB, (B) R_{IB} against IB, and (C) R_{RF} against RF. Color lines represent the results for the number m_o of modules. Black solid, dotted, and cyan lines represent the robustness after these attacks in non-modular ER, SF networks and random *d*-regular graphs.

https://doi.org/10.1371/journal.pone.0301269.g003

curves. However, these behaviors are not observed in in Fig 3C. The reasons for such behaviors are unknown in the current stage, and will be investigated in future works.

We should remark that R_{MB}, R_{IB} and R_{RF} in rewired networks with high Q become lower than those in non-modular ER networks (black line) and SF networks known as the extremely vulnerable structure (black dotted line). This means that modular random d-regular graphs become more vulnerable than SF networks by increasing the modularity, even if non-modular random d-regular graphs have the optimal robustness against malicious attacks [4, 5]. Note that robustness against IB and Initial Degree (ID) attacks also decrease as increasing the modualarity Q in SF networks and real-world networks [10].

As shown in Fig 4A–4F, we investigate other measures of robustness: average betweenness centrality, the reciprocal of network efficiency, average path length, diameter, spectral gap, and algebraic connectivity. Consequently, when modularity Q increase, the values of average betweenness centrality, the reciprocal of network efficiency, average path length, and diameter also increase (Fig 4A–4D), while the values of spectral gap and algebraic connectivity decrease (Fig 4E and 4F). These results indicate that networks with low modularity have good robustness. Similar results are obtained for other networks with varying d as shown in S9 and S10 Figs.

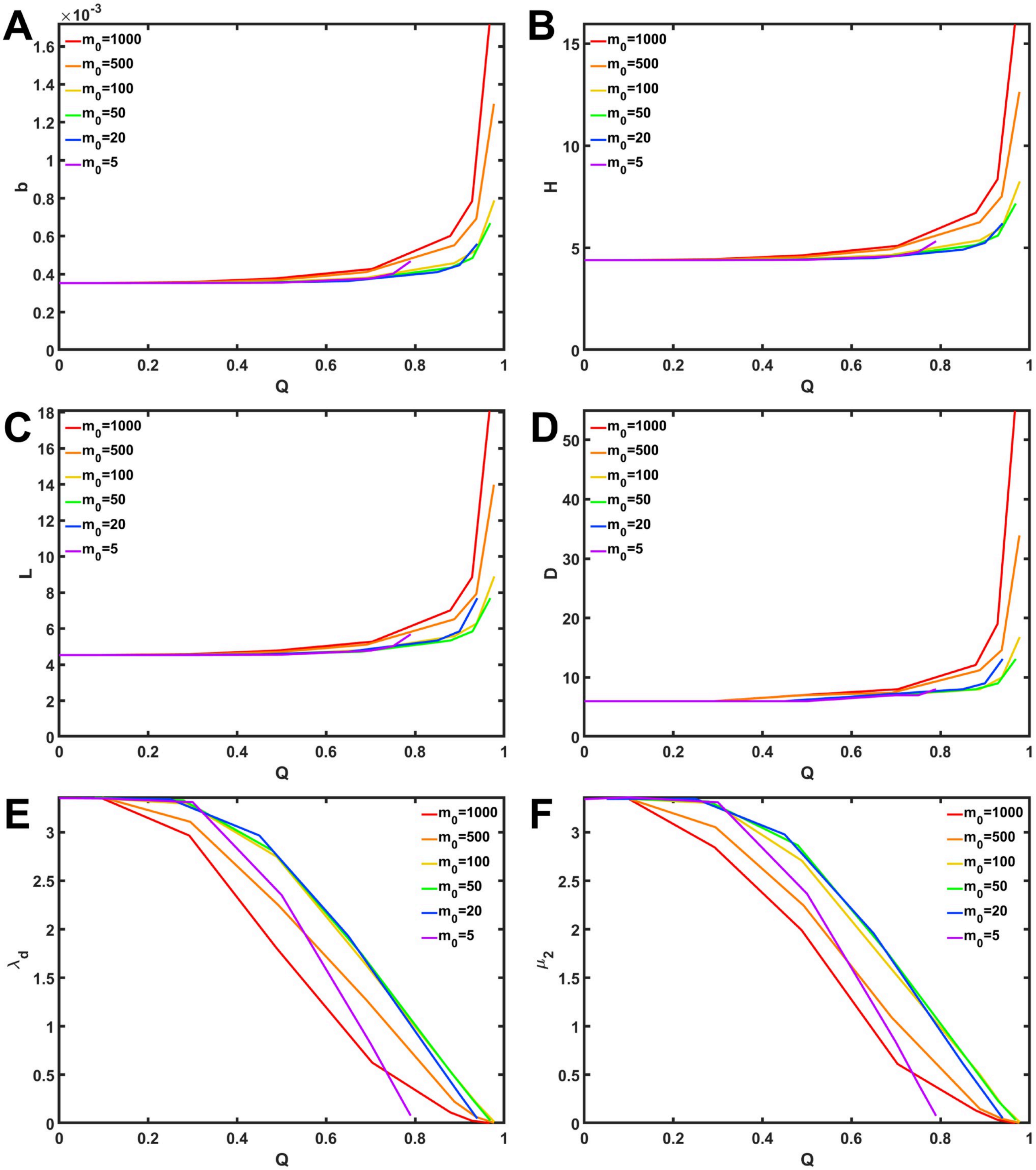

Fig 4. Relation between modularity Q and six measures of robustness in rewired networks with $d = 9$. (A) Average betweenness centrality, (B) reciprocal of network efficiency, (C) average path length, (D) diameter, (E) spectral gap, (F) algebraic connectivity. Color lines represent the results for the numbers m_o of modules.

https://doi.org/10.1371/journal.pone.0301269.g004

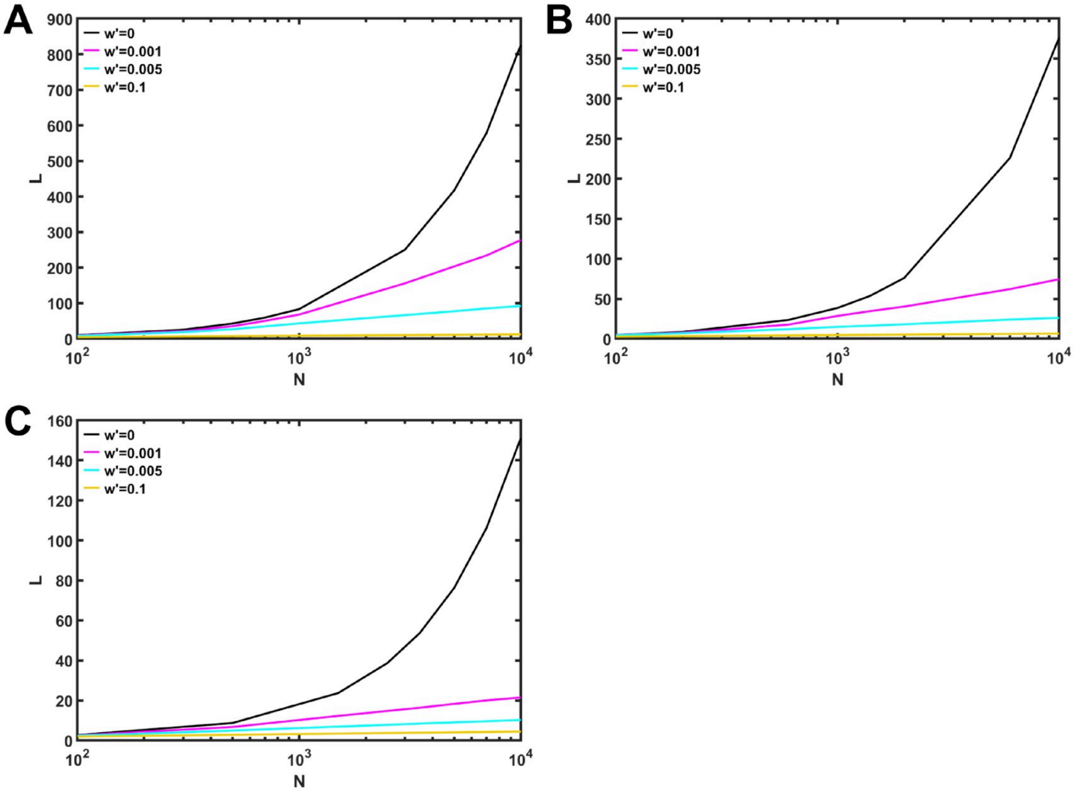

Fig 5. Average path length *L* in rewired networks for varying the network size *N*. Rewired networks with (A) $d = 4$, $N_m = 10$, (B) $d = 9$, $N_m = 20$, and (C) $d = 19$, $N_m = 50$. Color lines represent a rewiring rate w' on anti-modularization.

https://doi.org/10.1371/journal.pone.0301269.g005

Emerging SW property by anti-modularization

Moreover, we have investigated efficiency of paths in two ways. First, as similar to the result of SW property for a caveman graph [12], we show that SW property emerges in regular graphs. Then, we compare the numerical values of average path length with newly proposed estimation [17].

Fig 5A shows the average path length L as function of network size N, when $d = 4$ and $N_m = 10$ are fixed. In a ring structure (when $w' = 0$), L is $O(N)$ (black line). However, even only rewiring a few intra-links, L becomes $O(logN)$ for $w' = 0.1$ (yellow line). This indicates that a network has SW property [12]. Similar results are obtained for other networks in Fig 5B with $d = 9$, $N_m = 20$ and in Fig 5C with $d = 19$, $N_m = 50$. It is common that L is $O(logN)$ in these networks for $w' = 0.1$. In addition, figures from S11 to S13 Figs show that SW property emerges in rewired networks even for varying d and N_m. Remember the result in caveman graphs [12], which consist of cliques initially connected as a ring. Our obtained results include the robustness for the caveman graphs in Fig 2A, because cliques are the most densely case of regular graphs.

In general for a sparse network with any degree distribution, the average path length

$$L \approx \frac{log(N/\langle k \rangle)}{log((\langle k^2 \rangle - \langle k \rangle)/\langle k \rangle)} + 1$$

is derived through the analysis of generating functions [18]. From $\langle k \rangle = d$ and $\langle k^2 \rangle = d^2$ for a

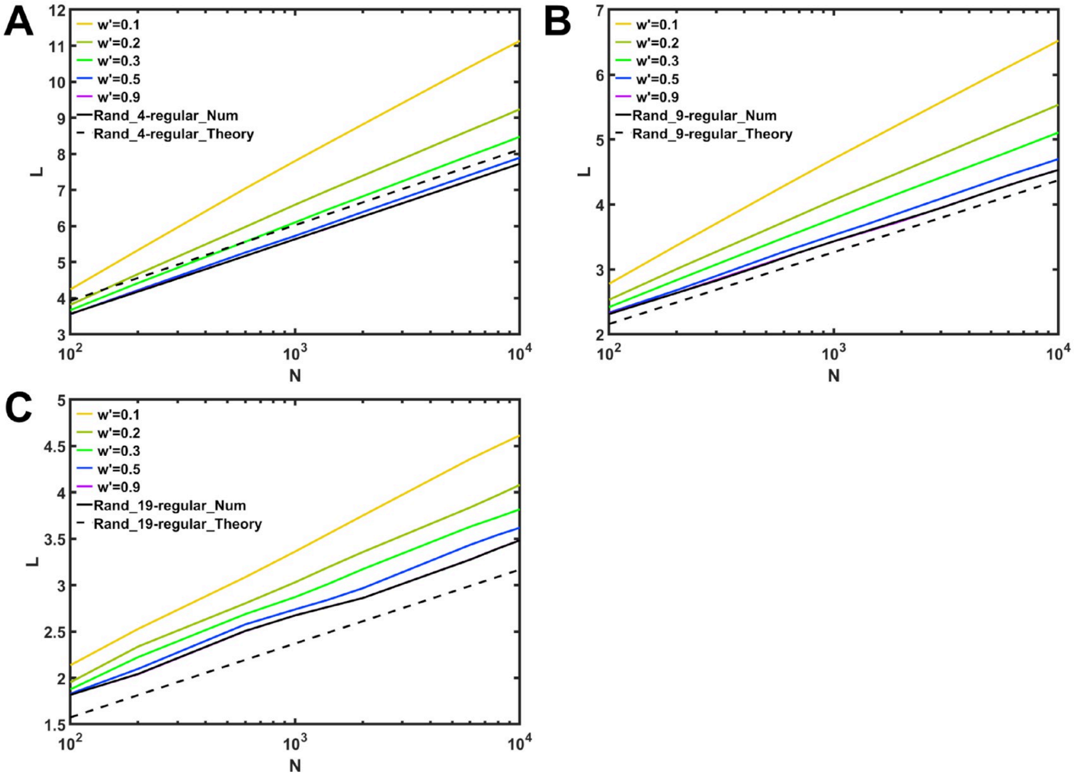

Fig 6. Disparities of average path length *L* between the values for rewired modular networks and theoretical value. Rewired networks with (A) $d = 4$, $N_m = 20$, (B) $d = 9$, $N_m = 20$, and (C) $d = 19$, $N_m = 20$. Color lines represent a rewiring rate w' on anti-modularization. Black solid and dashed lines indicate numerical and theoretical values for random d-regular graphs without modular structures.

https://doi.org/10.1371/journal.pone.0301269.g006

d-regular graph, the estimation

$$L \approx \frac{log(N/d)}{log(d-1)} + 1 \tag{2}$$

is obtained approximately as SW property. Thus, we compare Eq (2) with our results for the modular networks after rewirings. Fig 6 shows that the color lines of $O(logN)$ with slightly different slops approach black solid line for random d-regular graphs. In particular, purple line for the case with $w' = 0.9$ almost coincides with black solid line, while there is a small gap between black solid and dashed lines. Note that dashed line corresponds to Eq (2). However, it has been pointed out that there exist disparities between numerically obtained average path length and more rigorous estimation than Eq (2) for random regular graphs, when they are dense [17]. Our study for $d = 4$, 9 and $19 \ll N$ is classified as sparse graphs, the derivation of more rigorous estimation is intractable for the modular networks. Therefore, it will be a future work to investigate the existing such disparities.

Comparing with modified modularization as the inverse process of anti-modularization

Since the conventional modularization [10] does not maintain a degree distribution and whole connectivity, we propose modified process of it. Fig 7A–7C show that the degree distributions

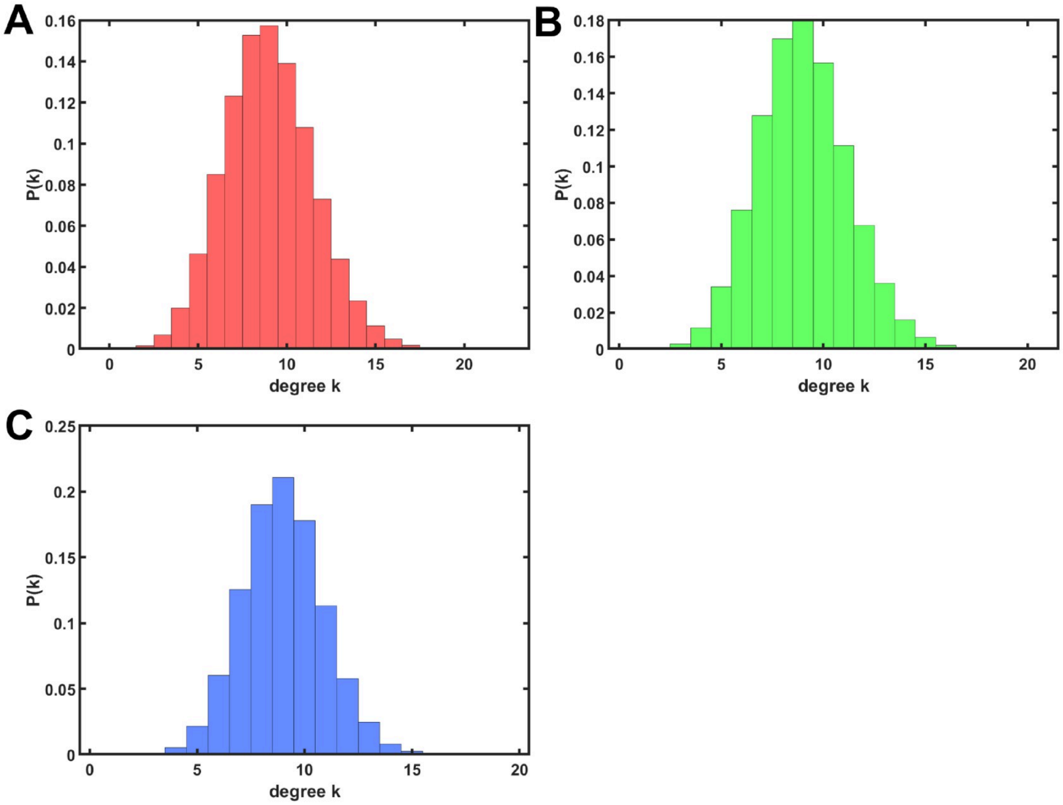

Fig 7. Degree distribution in rewired networks with d = 9 and m_o = 100. For rewiring rates (A) w = 0.988, (B) w = 0.695, and (C) w = 0.494. The values of w are corresponding to w' = 0.01, 0.3, 0.5 from Eq (1).

https://doi.org/10.1371/journal.pone.0301269.g007

have widths in rewired networks with d = 9 and m_o = 100 on the conventional modularization [10]. We confirm that degree distributions also have widths in rewired networks for varying d and m_o. This means that rewired networks are no longer random d-regular graphs on the conventional modularization [10].

Thus, we modify the process of modularization [10] to maintain connected d-regular graphs. The basic idea is similar to our anti-modularization. Fig 8 illustrates the modified process. Initially, module numbers 1, 2, . . ., m_o are assigned to nodes randomly, while a size of each module N_m is constant. (1) An inter-link (i, j) is randomly removed. Then, one end-node j of the removed link is selected randomly. (2) A node k is randomly selected, which belongs to a same module with node j and does not connected to node j. Then, a new intra-link is created between nodes j and k. (3) To preserve a node degree, an inter-link (k, l) is randomly removed. (4) Select node m in a same module with node l randomly. Then, create a new intra-link between nodes l and m. (5) An inter-link (m, n) is randomly removed. After (5), node n is the next target for rewiring. Such process is repeated until $w(M - M/m_o)$ intra-links are created without isolation of connected components and nodes. However, at the end of repeated process, the degree of first selected node i is decreased by one at (1), while the degree of last selected p is increased by one.

As shown in Fig 9A for the robustness, curves of each colors on modified modularization (dotted lines) and anti-modularization (solid lines) are almost identical in rewired networks with m_o = 100. However, as smaller number m_o of modules, the gaps between solid and dotted

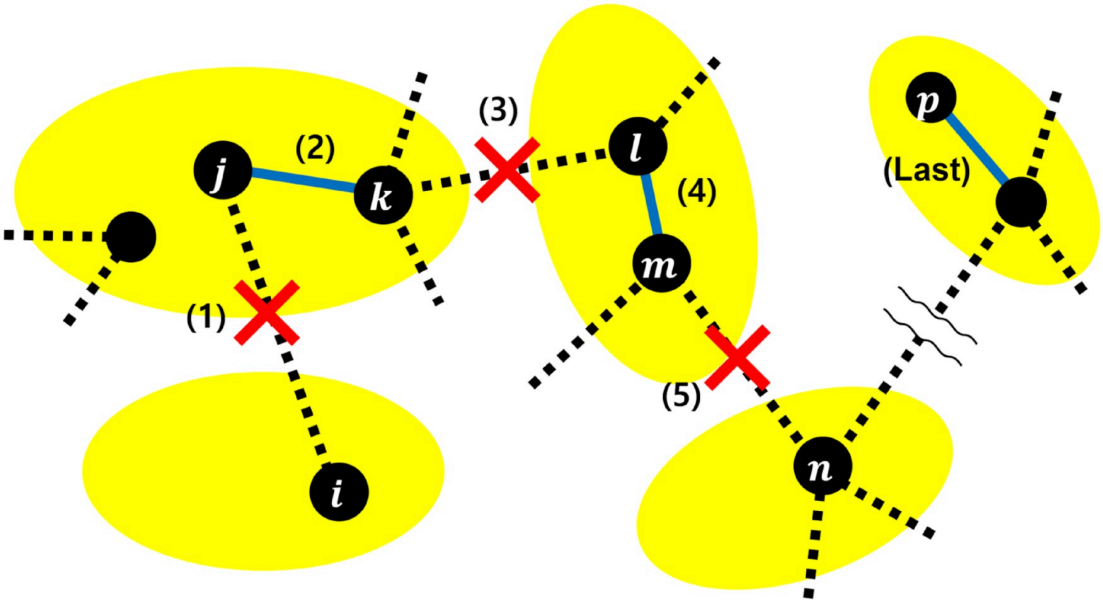

Fig 8. Process of the modified modularization. The numbers in brackets denote a sequence of the process. Yellow circles represent modules. Black dotted and Blue solid lines are inter- and intra-links by rewirings, respectively.

https://doi.org/10.1371/journal.pone.0301269.g008

lines are larger. Especially, in rewired networks with $m_o = 5$, such gaps are remarkable for orange and yellow lines in Fig 9C. Red lines in Fig 9A–9C are almost identical, although rewired networks for high rewiring rate w on modified modularization tend to not have a ring structure. See S15 and S16 Figs in cases of IB attacks and RF.

Conclusion

We have numerically investigated the robustness of connectivity in modular d-regular graphs which have the optimal tolerance in the non-modular random case. The robustness against MB, IB attacks and RF increases, when more intra-links are rewiring on anti-modularization. In particular, our results have shown that the robustness decreases rapidly against MB attacks than IB attacks as the modularity increases. When the modularity Q is above 0.8, the robustness of modular d-regular graphs becomes lower than the robustness of very fragile SF networks. Moreover, we have shown that both high robustness and efficiency coexist in rewired networks on anti-modularization. In fact, like caveman graphs [12], modular d-regular graphs exhibit SW property by rewiring only a few intra-links for $w' = 0.1$, whereas the numerical values of L for modular networks are slightly different from the well-known theoretical values [18] for random regular graphs. At $w' = 0.1$, modular d-regular graphs still have low robustness. Thus, in order to be both high robust and efficient, more intra-links at least with $0.1 < w' < 0.3$ are needed in modular d-regular graphs.

Unlike our results for regular graphs with $N = 10^4$, the previous study [9] shows that there exists a critical number m_o^* of modules below which ER random graphs are completely broken into modules by attacks on interconnected nodes. In particular, for ER random graphs with $N = 6 \times 10^5$, discontinuous jump of the 1st LCC size occurs for a critical number m^* of modules. Although the study [9] also considers a modular network that consist of m_o modules, it additionally defines the ratio α between the probabilities for an intra- and inter-links. With constant average degree $\langle k \rangle$ and ratio α, the percolation threshold is shown as a function of m_o

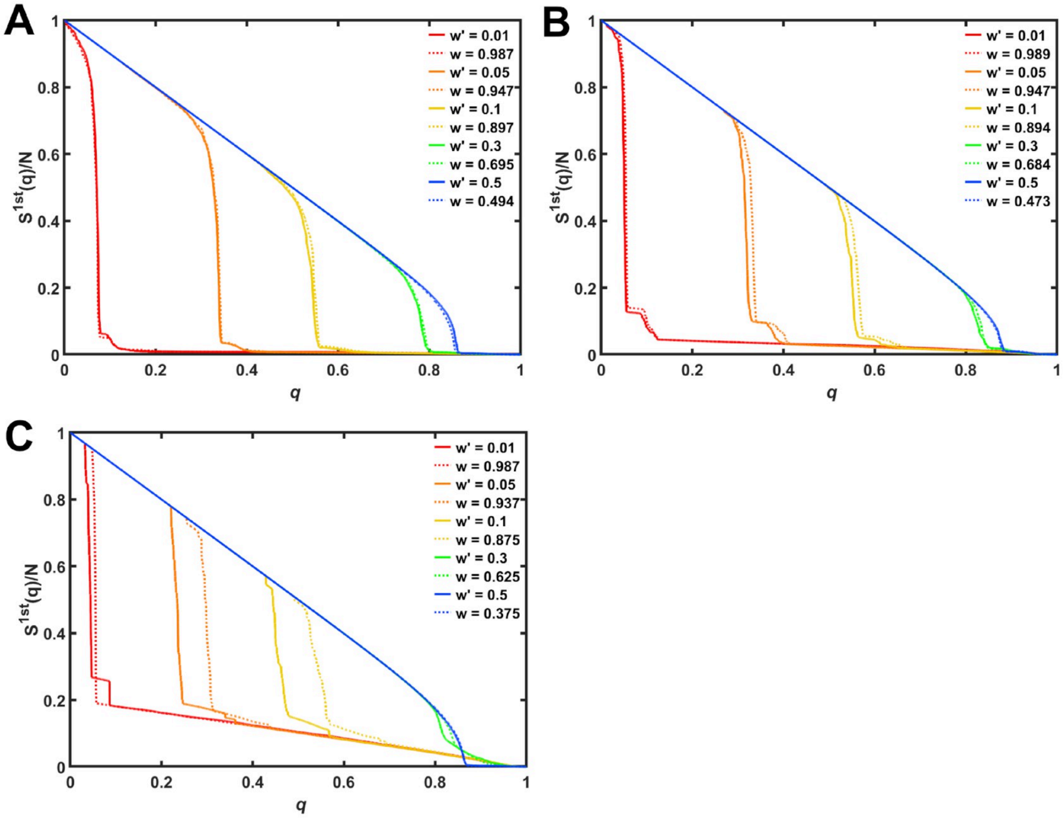

Fig 9. Comparing the robustness against MB attacks in rewired networks on the anti-modularization and modified modularization. The 1st LCC size against MB attacks in rewired networks with $d = 9$ and number m_o of modules. (A) m_o = 100, (B) m_o = 20, and (C) m_o = 5. Solid and dotted color lines represent the results by rewiring with w' on anti-modularization and w on modified modularization.

https://doi.org/10.1371/journal.pone.0301269.g009

modules. However, in varying m_o for constant $N = m_o \times N_m$ and $M = N \times d/2$, if α is fixed, rewiring rate w is also changed simultaneously because of $\alpha = \frac{m_o}{1-w} - (m_o - 1)$ [10]. Hence there exists such differences, it is unknown whether or not the discontinuous jump also appears in our case for very larger N. Thus, it is required to compare the results in this point.

On the other hand, we find that modular d-regular graphs with low modularity are more robust against selected IB attacks than against unintended RF. We also confirm that the robustness of rewired networks on modified modularization is almost identical to that on the anti-modularization which is the inverse process of the modified one. However, there still remains some unclear reasons for our results. For example, as shown in S4A Fig, curves of R_{IB} with $w' = 0.01$ and 0.1 have inverse relationship. In addition, in Fig 2F, S3F and S6F Figs, some curves of the 1st LCC size with $w' = 0.9$ and $w' = 0.1$ are crossing at high attack rates $q \simeq 0.85$, 0.7, and 0.92 of node removals. Thus, further investigations are necessary for such phenomena.

Although huge computation times are required, it will be future works to investigate the robustness of connectivity against various attacks: edge attacks [19], attacks based on other node centrality [20], CoreHD [21], collective influence [22], belief propagation [23], or spatial localized attacks [24]. Moreover, expanding our analytical framework may be meaningful as another direction. For example, since our work mainly deals with malicious attack, it can be considered to investigate an effect of cascading failures [25]. Link addition on modular networks for studying robustness [26] could be considered because SW property emerge by not only random rewiring but also link addition [27].

We obtain similar results for different attacks or values of d and m_o as follows. Figures from S1 to S8 Figs show the 1st LCC size against MB, IB attacks and RF in rewired networks with $d = 4$, 9 and 19. The 1st LCC size against MB attacks with $d = 9$ is already shown in Fig 2. S11–S13 Figs show the average path length in rewired networks with $d = 4$, 9 and 19 for varying N_m from 5, 10, and 20 as cliques to 100. Thus, for each N_m, the network size $N = N_m \times m_o$ is changed by m_o, while the minimum value of m_o is 3. S14 Fig show disparities of L between the values for rewired modular networks with $N_m = 100$ and theoretical value. S15 and S16 Figs show the 1st LCC size against IB attacks and RF to compare the results on anti-modularization and modified modularization. Note that the number m_o of modules becomes the maximum when it is equal to the size of clique K_5, K_{10} or K_{20}. Since network size N is 10^4, the maximum values of m_o are 2000, 1000, and 500 for each of module sizes $N_m = 5$, 10 and 20.

Supporting information

S1 Fig. The 1st LCC size against IB attacks in rewired networks with $d = 9$ and the number m_o of modules. (A) $m_o = 1000$, (B) $m_o = 500$, (C) $m_o = 100$, (D) $m_o = 50$, (E) $m_o = 20$, and (F) $m_o = 5$. Color lines represent the rewiring rates w' on anti-modularization.
(TIF)

S2 Fig. The 1st LCC size against RF in rewired networks with $d = 9$ and the number m_o of modules. (A) $m_o = 1000$, (B) $m_o = 500$, (C) $m_o = 100$, (D) $m_o = 50$, (E) $m_o = 20$, and (F) $m_o = 5$. Color lines represent the rewiring rates w' on anti-modularization.
(TIF)

S3 Fig. The 1st LCC size against MB attacks in rewired networks with $d = 4$ and the number m_o of modules. (A) $m_o = 2000$, (B) $m_o = 1000$, (C) $m_o = 500$, (D) $m_o = 100$, (E) $m_o = 20$, and (F) $m_o = 5$. Color lines represent the rewiring rates w' on anti-modularization.
(TIF)

S4 Fig. The 1st LCC size against IB attacks in rewired networks with $d = 4$ and the number m_o of modules. (A) $m_o = 2000$, (B) $m_o = 1000$, (C) $m_o = 500$, (D) $m_o = 100$, (E) $m_o = 20$, and (F) $m_o = 5$. Color lines represent the rewiring rates w' on anti-modularization.
(TIF)

S5 Fig. The 1st LCC size against RF in rewired networks with $d = 4$ and the number m_o of modules. (A) $m_o = 2000$, (B) $m_o = 1000$, (C) $m_o = 500$, (D) $m_o = 100$, (E) $m_o = 20$, and (F) $m_o = 5$. Color lines represent the rewiring rates w' on anti-modularization.
(TIF)

S6 Fig. The 1st LCC size against MB attacks in rewired networks with $d = 19$ and the number m_o of modules. (A) $m_o = 500$, (B) $m_o = 200$, (C) $m_o = 100$, (D) $m_o = 50$, (E) $m_o = 20$, and (F) $m_o = 5$. Color lines represent the rewiring rates w' on anti-modularization.
(TIF)

S7 Fig. The 1st LCC size against IB attacks in rewired networks with $d = 19$ and the number m_o of modules. (A) $m_o = 500$, (B) $m_o = 200$, (C) $m_o = 100$, (D) $m_o = 50$, (E) $m_o = 20$, and (F) $m_o = 5$. Color lines represent the rewiring rates w' on anti-modularization.
(TIF)

S8 Fig. The 1st LCC size against RF in rewired networks with $d = 19$ and the number m_o of modules. (A) $m_o = 500$, (B) $m_o = 200$, (C) $m_o = 100$, (D) $m_o = 50$, (E) $m_o = 20$, and (F) $m_o = 5$. Color lines represent the rewiring rates w' on anti-modularization.
(TIF)

S9 Fig. Relation between modularity Q and six measures of robustness in rewired networks with $d = 4$. (A) Average betweenness centrality, (B) reciprocal of network efficiency, (C) average path length, (D) diameter, (E) spectral gap, (F) algebraic connectivity. Color lines represent the results for the numbers m_o of modules.
(TIF)

S10 Fig. Relation between modularity Q and six measures of robustness in rewired networks with $d = 19$. (A) Average betweenness centrality, (B) reciprocal of network efficiency, (C) average path length, (D) diameter, (E) spectral gap, (F) algebraic connectivity. Color lines represent the results for the numbers m_o of modules.
(TIF)

S11 Fig. Average path length L in rewired networks with $d = 4$ for varying the network size N. Rewired networks with (A) $N_m = 5$, (B) $N_m = 20$, (C) $N_m = 50$, and (D) $N_m = 100$. Color lines represent a rewiring rate w' on anti-modularization.
(TIF)

S12 Fig. Average path length L in rewired networks with $d = 9$ for varying the network size N. Rewired networks with (A) $N_m = 10$, (B) $N_m = 50$, and (C) $N_m = 100$. Color lines represent a rewiring rate w' on anti-modularization.
(TIF)

S13 Fig. Average path length L in rewired networks with $d = 19$ for varying the network size N. Rewired networks with (A) $N_m = 20$, (B) $N_m = 100$. Color lines represent a rewiring rate w' on anti-modularization.
(TIF)

S14 Fig. Difference of average path length L between the values for rewired modular networks and theoretical value. Rewired networks with (A) $d = 4$, $N_m = 100$, (B) $d = 9$, $N_m = 100$, and (C) $d = 19$, $N_m = 100$. Color lines represent a rewiring rate w' on anti-modularization. Black solid and dashed lines indicate numerical and theoretical values for random d-regular graphs without modular structures.
(TIF)

S15 Fig. Comparing the robustness against IB attacks in rewired networks on the anti-modularization and modified modularization. The 1st LCC size against MB attacks in rewired networks with $d = 9$ and the number m_o of modules. (A) $m_o = 100$, (B) $m_o = 20$, and (C) $m_o = 5$. Solid and dotted color lines represent the results by rewiring with w' on anti-modularization and w on modified modularization.
(TIF)

S16 Fig. Comparing the robustness against RF in rewired networks on the anti-modularization and modified modularization. The 1st LCC size against MB attacks in rewired networks with $d = 9$ and the number m_o of modules. (A) $m_o = 100$, (B) $m_o = 20$, and (C) $m_o = 5$. Solid and dotted color lines represent the results by rewiring with w' on anti-modularization and w on modified modularization.
(TIF)

Author Contributions

Conceptualization: Yukio Hayashi.

Data curation: Jaeho Kim.

Formal analysis: Jaeho Kim.

Funding acquisition: Yukio Hayashi.

Investigation: Jaeho Kim.

Project administration: Yukio Hayashi.

Supervision: Yukio Hayashi.

Validation: Yukio Hayashi.

Visualization: Jaeho Kim.

Writing – original draft: Jaeho Kim.

Writing – review & editing: Yukio Hayashi.

References

1. Albert R, Jeong H, Barabási AL. Error and attack tolerance of complex networks. nature. 2000; 406 (6794):378–382. https://doi.org/10.1038/35019019 PMID: 10935628
2. Braunstein A, Dall'Asta L, Semerjian G, Zdeborová L. Network dismantling. Proceedings of the National Academy of Sciences. 2016; 113(44):12368–12373. https://doi.org/10.1073/pnas.1605083113 PMID: 27791075
3. Chujyo M, Hayashi Y. A loop enhancement strategy for network robustness. Applied Network Science. 2021; 6(1):1–13. https://doi.org/10.1007/s41109-020-00343-6
4. Chujyo M, Hayashi Y, Hasegawa T. Optimal Network Robustness Against Attacks in Varying Degree Distributions. arXiv preprint arXiv:230106291. 2023;.
5. Ma L, Liu J, Duan B, Zhou M. A theoretical estimation for the optimal network robustness measure R against malicious node attacks. Europhysics Letters. 2015; 111(2):28003. https://doi.org/10.1209/0295-5075/111/28003
6. Stanić Z. Regular graphs: a spectral approach. vol. 4. Walter de Gruyter GmbH & Co KG; 2017.
7. Barabási AL. Network science. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences. 2013; 371(1987):20120375. https://doi.org/10.1098/rsta.2012.0375 PMID: 23419844
8. Newman M. Networks. Oxford university press; 2018.
9. Shai S, Kenett DY, Kenett YN, Faust M, Dobson S, Havlin S. Critical tipping point distinguishing two types of transitions in modular network structures. Physical Review E. 2015; 92(6):062805. https://doi.org/10.1103/PhysRevE.92.062805 PMID: 26764742
10. Nguyen Q, Vu TV, Dinh HD, Cassi D, Scotognella F, Alfieri R, et al. Modularity affects the robustness of scale-free model and real-world social networks under betweenness and degree-based node attack. Applied Network Science. 2021; 6(1):1–21. https://doi.org/10.1007/s41109-021-00426-y
11. Requião da Cunha B, González-Avella JC, Gonçalves S. Fast fragmentation of networks using module-based attacks. PloS one. 2015; 10(11):e0142824. https://doi.org/10.1371/journal.pone.0142824 PMID: 26569610
12. Watts DJ. Small worlds: the dynamics of networks between order and randomness. vol. 36. Princeton university press; 2004.
13. Newman ME. Modularity and community structure in networks. Proceedings of the national academy of sciences. 2006; 103(23):8577–8582. https://doi.org/10.1073/pnas.0601602103
14. Schneider CM, Moreira AA, Andrade JS Jr, Havlin S, Herrmann HJ. Mitigation of malicious attacks on networks. Proceedings of the National Academy of Sciences. 2011; 108(10):3838–3841. https://doi.org/10.1073/pnas.1009440108 PMID: 21368159
15. Freitas S, Yang D, Kumar S, Tong H, Chau DH. Graph Vulnerability and Robustness: A Survey. IEEE Transactions on Knowledge and Data Engineering. 2023; 35(6):5915–5934.

16. Almeira N, Billoni OV, Perotti JI. Scaling of percolation transitions on Erdös-Rényi networks under centrality-based attacks. Physical Review E. 2020; 101(1):012306. https://doi.org/10.1103/PhysRevE.101.012306 PMID: 32069537

17. Tishby I, Biham O, Kühn R, Katzav E. The mean and variance of the distribution of shortest path lengths of random regular graphs. Journal of Physics A: Mathematical and Theoretical. 2022; 55(26):265005. https://doi.org/10.1088/1751-8121/ac6f9a

18. Newman ME, Strogatz SH, Watts DJ. Random graphs with arbitrary degree distributions and their applications. Physical review E. 2001; 64(2):026118. https://doi.org/10.1103/PhysRevE.64.026118 PMID: 11497662

19. Holme P, Kim BJ, Yoon CN, Han SK. Attack vulnerability of complex networks. Physical review E. 2002; 65(5):056109. https://doi.org/10.1103/PhysRevE.65.056109 PMID: 12059649

20. Chen D, Lü L, Shang MS, Zhang YC, Zhou T. Identifying influential nodes in complex networks. Physica a: Statistical mechanics and its applications. 2012; 391(4):1777–1787. https://doi.org/10.1016/j.physa.2011.09.017

21. Zdeborová L, Zhang P, Zhou HJ. Fast and simple decycling and dismantling of networks. Scientific reports. 2016; 6(1):37954. https://doi.org/10.1038/srep37954 PMID: 27897223

22. Morone F, Makse HA. Influence maximization in complex networks through optimal percolation. Nature. 2015; 524(7563):65–68. https://doi.org/10.1038/nature14604 PMID: 26131931

23. Mugisha S, Zhou HJ. Identifying optimal targets of network attack by belief propagation. Physical Review E. 2016; 94(1):012305. https://doi.org/10.1103/PhysRevE.94.012305 PMID: 27575146

24. Shao S, Huang X, Stanley HE, Havlin S. Percolation of localized attack on complex networks. New Journal of Physics. 2015; 17(2):023049. https://doi.org/10.1088/1367-2630/17/2/023049

25. Stephen E. Does Isolating High-modularity Communities Prevent Cascading Failure? In: International Conference on Complex Networks and Their Applications. Springer; 2023.

26. Tian M, Moriano P. Robustness of community structure under edge addition. Phys Rev E. 2023; 108:054302. https://doi.org/10.1103/PhysRevE.108.054302 PMID: 38115408

27. Chujyo M, Hayashi Y. Adding links on minimum degree and longest distance strategies for improving network robustness and efficiency. Plos one. 2022; 17(10):e0276733. https://doi.org/10.1371/journal.pone.0276733 PMID: 36288333