BACHELOR

Secure communication schemes

Aerts, N.K.M.

Award date:
2009

Secure communication schemes

2J008 - bachelors project

Author: Nieke Aerts
Supervisor: Prof. dr. ir. Henk van Tilborg
Technische Universiteit Eindhoven

November 30, 2009

Abstract

To allow all participants in a network to communicate in a secure way, a different secret key may be assigned to all pairs. This method is not very efficient since for n participants $n(n-1)/2$ different keys are needed. In this report we assume that there are at most t adversaries in the network. In many cases it is possible to assign $t+1$ keys to every participant and maintain secure communication between all participants.
Desmedt e.o. has shown that Harary graphs are very useful for this problem [1]. However if there is an odd number of participants n and an even number of adversaries t there are complications. In this report it is shown that for an odd number of participants there are only two cases for which the Harary graphs are still useful, this is for $t = 2$ and $t = n-3$. If t is even and in between those two cases it is proven that the Harary graphs can not be used.
For the special cases where n is odd and $t = n-5$ or $t = n-7$ an algorithm is given to construct a secure communication scheme where $t+1$ different keys are assigned to each participant.
For n odd and $t = n-9$ or $t = 4$ a number of graphs are given in the appendix. No closed formula for these series were found. The graphs in the appendix were checked with a JAVA program written for this project.

Contents

1 Introduction

This report concerns secure communication in a connected network.
For example if two persons in a group want to gossip about the others, they whisper to make sure the others will not hear the content. If no other person is able to hear the conversation the method of whispering was secure. But a third person may eavesdrop and be able to find out the contents of the conversation. To make sure the third person is not able to find out the contents, the two gossipers encrypt the message with a certain key only known to them.
In a network with n participants, the participants are denoted by 0 to $n-1$. If two participants i and j share a secret key $k_{i,j}$ they are able to communicate safely if the encryption method is secure. In this report we will assume a secure encryption method is being used.
If every two participants share a secret key, they are all able to communicate in a secure way. The network with n participants then needs $\binom{n}{2} = \frac{n(n-1)}{2}$ different keys. This is not a very efficient method.

If we make the assumption that there are at most t adversaries among the n participants, who may work together to intercept and decrypt the message, it is possible to use less keys and still allow all participants to communicate safely. This report describes networks where only $\lfloor \frac{1}{2}n(t+1) \rfloor$ different keys are used and all participants are able to communicate safely.

First some definitions are given in the next section of this chapter.
Chapter 2 introduces Harary graphs, which give a safe communication scheme if either the number of participants is even or the number of adversaries is odd. In Chapter 3 non-Harary solutions are given for some problems were the number of participants is odd and the number of adversaries is even.
To test network graphs for some properties we have written a JAVA program, an explanation of this program can be found in Chapter 4.

1.1 Definitions

The network consists of n participants, not every couple will share a secret key, but all couples should be able to communicate in secure way. Each participant is able to intercept every message. All messages are encrypted with a secure method, thus an intercepted message can only be read if one has the key to decrypt the message. In this report we assume that:

- At most t of the n participants are trying to acces messages that are not intended for them
- Each intermediate[1] will forward the message
- None of the intermediates will change the message such that the receiver will not obtain the original message

Safe Communication Scheme

Given the network in Figure 1 with 5 participants and up to 2 adversaries.

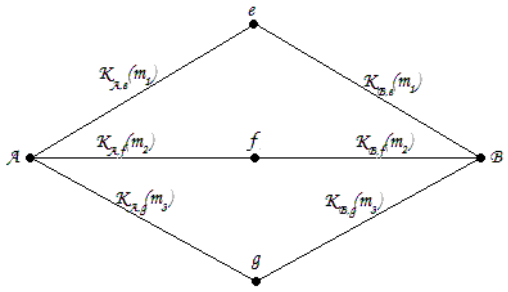


Figure 1: Communication between A and B

It is trivial that A has a secure path to e, f and g since each pair shares a secret key. Also B has a secure path to e, f and g.
Now assume that A wants to send a message M to B. Since they do not share a secret key they have to use intermediates.
There are at most 2 adversaries, which may work together. If A sends three different parts to e, f and g and they send their part to B, the adversaries will possess at most two decrypted parts. So A has to make sure that no two parts will give any information on the original message.
We assume that the message consists of bits. Then A can split the message M into different parts, which give no information on the original message, using bitwise addition modulo 2. First A chooses two random words of the same length as M, say m_1 and m_2. Now A computes m_3: $m_3 = M \oplus m_1 \oplus m_2$ where "$\oplus$" is the bitwise addition modulo 2. Only if one participant has all three parts,

[1] An intermediate is a participant on the path from the sender to the receiver

it is able to find the original message M (again by bitwise addition modulo 2). Now A encrypts m_1 with the key $K_{A,e}$, m_2 with $K_{A,f}$ and m_3 with $K_{A,g}$ and sends the encrypted parts to respectively e, f and g. Now e, f and g can decrypt the part they received from A but no two of them will have enough information to gain M. Now e, f and g encrypt their part with the key they share with B and send the encrypted part to B. B is able to encrypt the three parts and recover the original message M from $M = m_1 \oplus m_2 \oplus m_3$.

Two participants are able to communicate safely if they share a secret key. If all participants in a group have to be able to communicate safely, we may assign a secret key to every couple.
In order to make this scheme more efficient we want to minimize the number of keys per participant. If now two persons want to communicate and they do not share a key, they have to send their message via intermediates as described above.
If there are t adversaries among the n persons, then every person has to have at least $t+1$ keys to be able to communicate safely with all others, since otherwise the t adversaries may be able to intercept and decrypt all parts and find the original message.
Now we are able to define a safe communication scheme.

Definition 1.1. *A communication scheme is a set S of combinations (i, j), where i and j are participants and $(i, j) \in S$ if i and j share a secret key.*
A communication scheme among n participants of which t are adversaries is said to be safe if for every i, j, $i \neq j$ among the n participants at least one of the following holds:

1. *i and j share a secret key*
2. *there are $t + 1$ disjunct paths from i to j such that no t participants are able to intercept and decrypt all message parts*

For a safe communication scheme on a network among n participants and at most t adversaries, at least $n(t + 1)/2$ keys are needed (as every participant has at least $t + 1$ keys and shares each key with at least one other participant). If n is odd and t is even, $n(t + 1)/2$ is not an integer.
During this project we tried to find graphs which represent a safe communication scheme for odd n and even t. The total number of keys is less or equal $\lfloor \frac{1}{2} n(t+1) \rfloor$ and the number of keys is minimized per participant.
Further on we will represent the key that two participants a and b share as (a, b). We will use graphs to represent the network. In those graphs two participants are connected if they share a key.

2 Harary graphs

2.1 Properties of a Harary graph

Harary [4] concentrated on solving a problem given by Claude Berge: 'What is the maximum connectivity[2] of a graph with n vertices and m lines'. The answer is $2 \cdot m/n$. Harary proved this by showing that the connectivity of a graph cannot exceed this number and showing that there exists a graph with n vertices, m lines and connectivity $2 \cdot m/n$. These graphs satisfy Definition 2.1 and are nowadays called Harary graphs.

Definition 2.1. *The Harary graph $H_{(n,k)}$, $n \geq k+1$, is the graph on n vertices, numbered $0, 1, \ldots, n-1$, with calculations modulo n, where two vertices i and j $(i \neq j)$ are connected if and only if*

$$\begin{aligned} |j-i|_{mod\ n} \leq l \quad & if \quad k = 2l, \\ |j-i|_{mod\ n} \leq l \ or\ |j-i|_{mod\ n} = m \quad & if \quad k = 2l+1 \ and \ n = 2m, \\ |j-i|_{mod\ n} \leq l \ or\ j = m+1,\ i \in \{0,1,\ldots,m\} \quad & if \quad k = 2l+1 \ and \ n = 2m+1 \end{aligned}$$

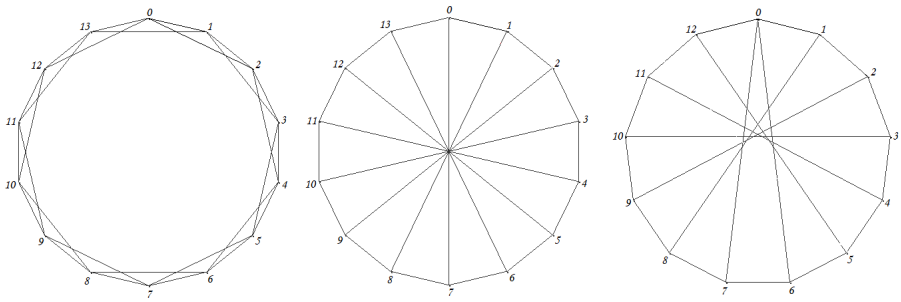


Figure 2: Harary graphs $H_{(14,4)}$, $H_{(14,3)}$ and $H_{(13,3)}$

The objective is to find graphs that represent a safe communication scheme among n persons, of which t are adversaries and at most $\lfloor \frac{1}{2}n(t+1) \rfloor$ different keys are used.
If n is even or t is odd, the Harary graph gives a safe communication scheme with n vertices and $n(t+1)/2 = \lfloor \frac{1}{2}n(t+1) \rfloor$ keys since 2 divides n or $t+1$ or both[3].
If either n is even, t is odd or both conditions hold, every vertex is connected to $t+1$ other vertices.
However if n is odd and t is even, then there is one vertex which is connected to

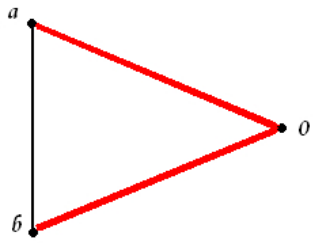
[2] Connectivity is the minimal degree of a vertex
[3] This is not proven in this report, but it is done in [1]

$t+2$ other vertices. The number of edges in this graph is $\lceil n(t+1)/2 \rceil$, if every edge is assigned a different key this graph has $\lceil n(t+1)/2 \rceil$ keys. It is possible to lower the number of keys by assigning the same key to two edges. In particular if two edges that are connected to the vertex who has $t+2$ connections are chosen, this might resolve in a safe communication scheme with no more than $\lfloor \frac{1}{2} n(t+1) \rfloor$ keys and up to t adversaries.

2.2 Forbidden subgraphs

If a graph of a communication scheme among n participants and t adversaries is constructed, such that n is odd and t is even, then there is at least one vertex with degree $t+2$. Let this vertex be denoted as 0. To keep the number of keys less or equal to $\lfloor \frac{1}{2} n(t+1) \rfloor$ we need to assign the same key to two edges ending in 0.
If the same key k is assigned to two edges, say $(0, a)$ and $(0, b)$, there are some restrictions to the paths two vertices may use to communicate.
If $(0, a)$ is used, then b may not be used unless they lie on the same path. If both are used and say a and 0 are trusted but b is an adversary, then b is also able to decrypt the partial message sent over the path $(0, a)$. Then b might be able to construct the original message if all other paths contain an adversary and they cooperate with b. If b lies on the same path, it is only able to find the same partial message twice, which will not cause a problem.
This restriction leads to three subgraphs that are not allowed in a safe communication scheme. In these graphs a and b are chosen to be the vertices which share the same key with the vertex 0.

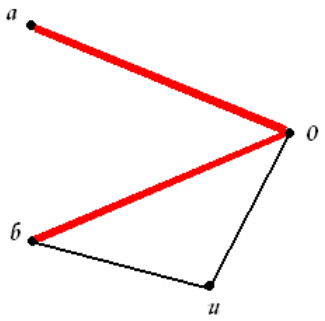
Forbidden subgraph 1



Choose two neighbors of 0, say a and b, which are directly connected. If a wants to send a message to a vertex $u \neq 0, b$ and a and u do not share a secret key. Since a has degree $t+1$ and $t+1$ disjunct paths are needed, it needs to send a partial message over both $(a, 0)$ and (a, b). Since b knows the key for both paths, b is able to recover two partial message. If b is one of the adversaries, the t adversaries might be able to find $t+1$ partial messages and thus recover

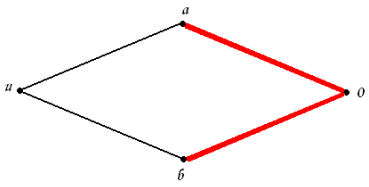
the original message. Thus in this case a and u are not able to communicate in a secure way.
Thus the two vertices which will share the same key with 0 may not be directly connected.

Forbidden subgraph 2



Choose two neighbors of 0, say a and b, which are not directly connected. Let u be connected to b and 0 but not to a.
Now a and u do not share a key, so to communicate they need $t+1$ disjunct paths. Since both a and u are only connected to $t+1$ other vertices, all these connections need to be used. Thus both $(u,0)$ and (u,b) need to be used. The vertex 0 can only be used once, thus $(u,0),(0,a)$ is a path. Now b can eavesdrop on this path, thus b may not be used in another path, which is a contradiction since (u,b) should be used too. Thus a and u can not communicate safely in this situation.
Thus there may not be a third vertex which is connected to 0 and to only one of the two vertices which share the same key with 0.

Forbidden subgraph 3

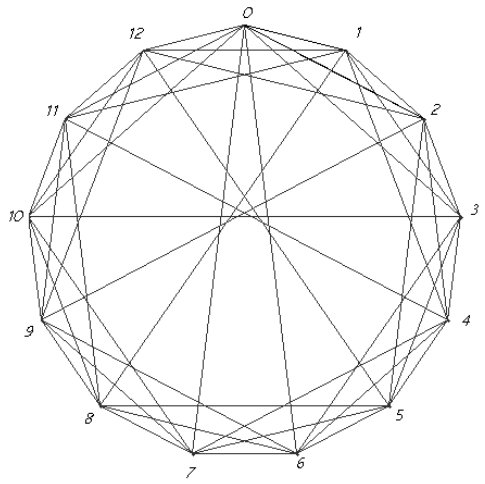


Choose two neighbors of 0, say a and b, which are not directly connected. Let u be connected to both a and b and not connected to 0. Now for 0 and u to

communicate safely they need $t+1$ disjunct paths. Since u is only connected to $t+1$ vertices, all of these need to be used. Thus we need to use both (u,a) and (u,b). Since 0 has $t+2$ paths and we need to use $t+1$ of those, at least one of $(0,a)$ or $(0,b)$ needs to be used. If we choose the first, we may not use the vertex b which leads to a contradiction, if we choose the latter, we may not use vertex a which also leads to a contradiction. In this situation u and 0 are not able to communicate safely.
Thus there may not be a third vertex connected to both the vertices which share the same key with 0 and not to 0.

2.3 Consequences of the forbidden subgraphs

Harary graphs give solutions if either the number of participants is even, the number of adversaries is odd or both. Otherwise the Harary graph contains one vertex, denoted as 0, with degree one more than all others. To minimize the number of keys, we assign the same key to two edges ending in 0. For 13 participants and 6 adversaries, Harary gives the following graph:



We need to find two vertices, were one may assign the same key to the edges between them and zero. In this case, every possible combination of two vertices, connected to zero, leads to a forbidden subgraph. In the table 1 you can find to which forbidden subgraph every combination leads.

first point	second point	forbidden subgraph
1	2, 3, 11, 12	1
2	3, 12	
3	6, 10	
6	7	
7	10	
10	11, 12	
11	12	
1	10	2 (look at vertex 2)
2	10	(1)
3	11	(12)
3	12	(11)
6	1, 2, 11, 12	(7)
7	1, 2, 11, 12	(6)
6	10	3 (look at vertex 9)
7	3	(5)

Table 1: Vertices which share the same key with 0 and the forbidden subgraphs that they cause

We have now seen that if n is odd and t is even, the Harary graph might not give a safe communication scheme. The three forbidden subgraphs are sufficient to show that this graph does not give a safe communication scheme.

The following theorem is proved using the three forbidden subgraphs.

Theorem 2.2. *Consider the Harary graph $H_{(2m+1,t+1)}$ were $m \geq 4$, $4 \leq t \leq 2m-4$ and t even. Suppose that all edges have their own unique key, except for two edges ending in 0, which are assigned the same key. Then this graph will not be a safe communication scheme if there are up to t adversaries.*

Proof. There are several possibilities to choose the pair of vertices for which the edge ending in zero is given the same key.
First define three subsets on the set of vertices connected to zero (not all vertices are in these subsets since in none of these graphs 0 is connected to all other vertices):

$$\begin{aligned} A &= \{1, 2, \ldots, \frac{t}{2}\} \\ B &= \{2m, 2m-1, \ldots, 2m-(\frac{t}{2}-1)\} \\ C &= \{m, m+1\} \end{aligned}$$

One can choose the pair of vertices in the following ways:

i) 2 vertices of the same subset

ii) a vertex of A and a vertex of C (which is the same as choosing one vertex of B and one of C by symmetry)

iii) a vertex of A and a vertex of B

All vertices within a subset are connected since every vertex is connected to $t/2$ neighbors on both sides and no subset contains more than $t/2$ vertices. Choosing two edges from 0 to a pair of vertices of the same subset results in forbidden subgraph 1. So option *i*) does not produce a safe communication scheme.
Now look at three cases and in every case prove that *ii*) and *iii*) lead to a forbidden subgraph:

Case 1: $4 \leq t < m$

Option ii)
The vertex with the highest number less then or equal to m, which is connected to at least one of the vertices of A is $\frac{t}{2} + \frac{t}{2} = t$, which is not in $\{m, m+1\}$ since $t < m$. For $m+2, m+3, \ldots m+\frac{t}{2}$ it is trivial that they are not in $\{m, m+1\}$. The same holds for B by symmetry.
Thus in this case none of the vertices in A or B is connected to a vertex in C. Every pair in the same subset forms a triangle with 0. Now say we choose $a \in A$ and $c \in C$. Then there is an $a' \in A$ such that a and a' are connected, a, a' and c are connected to 0 and a' is not connected to c. Now we have found forbidden subgraph 2. Thus one cannot assign the same key to the edges from 0 to a vertex of A and a vertex of C. So option *ii*) does not produce a safe communication scheme in this case.

Option iii)
Let $a \in A$ and $b \in B$ not be connected.
If there is an a^* connected to a and not to b we find forbidden subgraph 2. Assume there is no a^*, then b is connected to all $a_i \in A$ except a, to all $b_i \in B$ and to 0. The definition of Harary Graphs gives that b is connected to $\frac{t}{2}$ consecutive vertices on his right and on his left. Now there are $\frac{t}{2}-1+\frac{t}{2}-1+1 = t-2$ vertices defined to which b is connected, since b should be in the middle of these, $b = -1$. In Figure 3 if we choose $b = 11$, then b is not connected to 1 and 2, thus $b = 12$.
Since b is not connected to a, $a = \frac{t}{2}$. Now the vertex -2 is not connected to a, but it is connected to b and 0. Thus now we have found a b^* which is connected to b and 0 and not to a, which leads to forbidden subgraph 2.

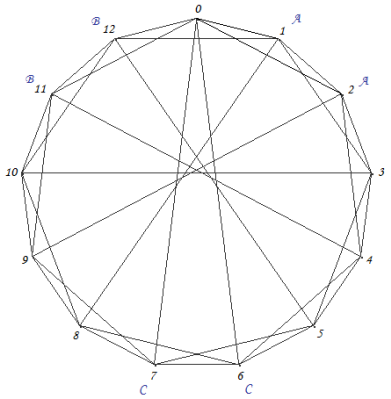


Figure 3: $H_{(13,5)}$

Now assume that there is no b^*, by the same reasons as above we find $a = 1$ and $b = -\frac{t}{2}$. Now 2 is connected to a and 0 and not to b thus we have found

an a^* which leads to forbidden subgraph 2.
Thus at least one of the following holds:

- either there is a vertex $a^* \in A$, connected to a and not to b, and one finds forbidden subgraph 2
- or there is a vertex $b^* \in A$, connected to b and not to a, and one finds forbidden subgraph 2.

It is not possible to assign the same key to two edges and not achieving a forbidden subgraph in this case. Thus none of the options $i), ii)$ and $iii)$ lead to a safe communication scheme for $4 \leq t < m$, t even.

Case 2: $4 < t = m$

Option ii)
In this case precisely one vertex in A, namely $\frac{t}{2}$ and one vertex in B, namely $2m - \frac{t}{2}$ is connected to m respectively $m + 1$.

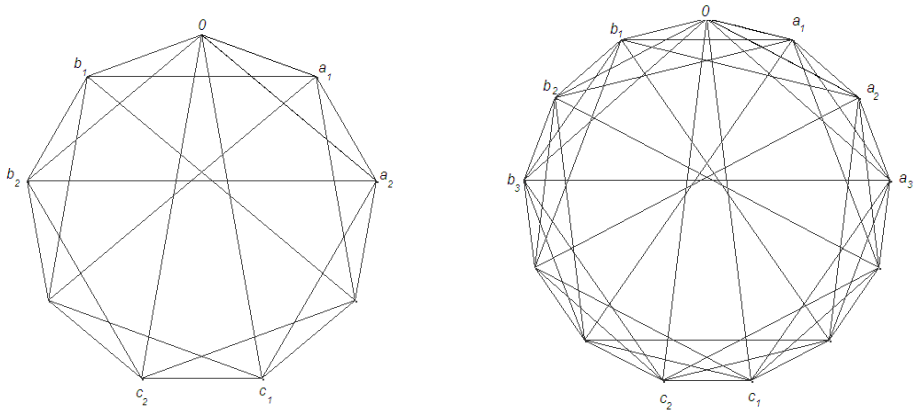


Figure 4: Harary graphs $H_{(9,5)}$ and $H_{(13,7)}$

We may not assign the same key to $(0, t/2)$ and $(0, m)$ since they are connected. Now let $a \in A$ and $c \in C$ not be connected. If $t \geq 6$ then A contains at least three vertices which are all connected and only one of them is connected to a vertex in C. Thus then there will be a vertex in A not equal to a, which is connected to a and 0 but not connected to c. This leads to forbidden subgraph 2. If $t = 5$ there will not always be such vertex (take a_1 and c_1 in $H_{(9,5)}$), but b_1 is connected to a_1 and 0 and not to c_1 by definition, thus here we also find forbidden subgraph 2. By symmetry the same holds if a vertex of B and one of C are chosen.
Thus option $ii)$ does not produce a safe communication scheme in this case.

Option iii) and $t = m = 4$
Let $a \in A$ and $b \in B$ not be connected.
If there is either an a^* or a b^* as before[4] then one finds forbidden subgraph 2.
Assume there is no such a^* and no such b^*. First look at $t = 4$ and $m = 4$ (left graph in Figure 4). If the edges $(a_1, 0)$ and $(b_2, 0)$ are assigned the same key, then there is no a^* nor a b^*. But now we find forbidden subgraph 3 since both a_1 and b_2 are connected to the vertex between b_2 and c_2. For a_2 and b_1 we find forbidden subgraph 3 by taking the vertex between a_2 and c_1. And since a_1 is connected to b_1 and a_2 is connected to b_2 (both forbidden subgraph 1) it is not possible to find an $a \in A$ and a $b \in B$ for which we may assign the same key to both edges $(0, a)$ and $(0, b)$. Thus option *iii)* does not produce a safe communication scheme for $t = m = 4$.

Option iii) and $t = m > 4$
For bigger m we will always find an a^* or a b^* by the same reasoning as in the case $4 \leq t < m$.
Assume there is no a^*. Then b is connected to all $a_i \in A$ except a. Also b is connected to all $b_i \in B$ except itself. Thus we find $\frac{t}{2} + \frac{t}{2} = t$ vertices which share an edge with b. By the definition of Harary graphs we know that b is connected to $\frac{t}{2}$ consecutive vertices on the left and $\frac{t}{2}$ consecutive vertices on the right. This implies that $b = b_1$ and $a = a_{t/2}$. But now a is not connected to b_2, thus we find a b^*.
In the same way, if we assume there is no b^*, we find $a = a_1$ and $b = b_{t/2}$ and $a_2 = a^*$.
Thus option *iii)* does not produce a safe communication scheme for $4 \leq t = m$.

None of the options $i), ii)$ and *iii)* lead to a safe communication scheme for $4 \leq t = m$, t even.

Case 3: $m < t < 2m - 3$

Option ii)
Let $a \in A$ and $c \in C$ not be connected. It is known that a is connected to vertex $t/2 + 1$, which is not connected to 0. Since c is connected to $t/2$ consecutive vertices, it is connected to $m - 1, m - 2, \ldots, m - \frac{t}{2} + 1$. Now $m - \frac{t}{2} + 1 < t - \frac{t}{2} + 1 = \frac{t}{2} + 1 \leq m - 1$, thus $t/2 + 1$ is connected to c. Now $t/2 + 1$ is connected to a and c and not to 0. This leads to forbidden subgraph 3. By symmetry the same holds if we choose $b \in B$ and $c \in C$.
Thus option *ii)* leads to forbidden subgraph 3.

[4] Thus a^* is connected to a and 0, but not to b and b^* is connected to b and 0, but not to a

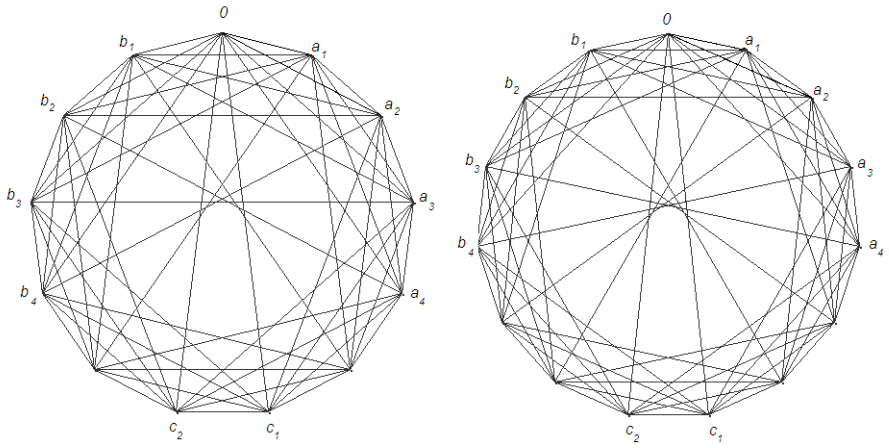


Figure 5: Harary graphs $H_{(13,9)}$ and $H_{(15,9)}$

Option iii)
Let $a \in A$ and $b \in B$ not be connected.
Again if there is either an a^* or a b^* as before[5] then one finds forbidden subgraph 2.
Assume there is no a^*. Then b is connected to all $a_i \in A$ except a. Also b is connected to all $b_i \in B$ except itself. Thus we find $\frac{t}{2} + \frac{t}{2} = t$ vertices which share an edge with b. By the definition of Harary graphs we know that b is connected to $\frac{t}{2}$ consecutive vertices on the left and $\frac{t}{2}$ consecutive vertices on the right. All vertices in $B \backslash b_1$ are not connected to at least two vertices in A. Only b_1 is connected to all $a \in A$ except one. This implies that $b = b_1$ and $a = a_{t/2}$. But now a is not connected to b_2, thus we find a b^*.
In the same way, if we assume there is no b^*, we find $a = a_1$ and $b = b_{t/2}$ and $a_2 = a^*$.
Thus in the case $m < t < 2m-3$ one cannot find two vertices a and b for which we may assign the same key to the edges $(a, 0)$ and $(b, 0)$. Thus option *iii*) does not produce a safe communication scheme for $m < t < 2m - 3$.
None of the options $i), ii)$ and *iii*) lead to a safe communication scheme for $m < t < 2m - 3$, t even.

Thus in the case $4 \leq t < m + 1$, t even, it is not possible to choose two neighbors of 0 which share the same key with 0. The Harary graphs $H_{(2m+1,t+1)}$, t even, do not give a safe communication scheme with at most $\lfloor \frac{1}{2} n(t+1) \rfloor$ keys. □

There are two series of Harary graphs which are not taken into account in the proof above. In these cases the Harary graph, with a key assigned to two edges ending in zero, does give a safe communication scheme.

[5] Thus a^* is connected to a and 0, but not to b and b^* is connected to b and 0, but not to a

Theorem 2.3. *Consider the Harary graph $H_{(2m+1,3)}$ were $m \geq 4$. Suppose that all edges have their own unique key, except for two edges ending in 0. The edges $(0,1)$ and $(0,2m)$ represent the same key. Then safe communication between any two vertices is always possible if there are up to 2 adversaries.*

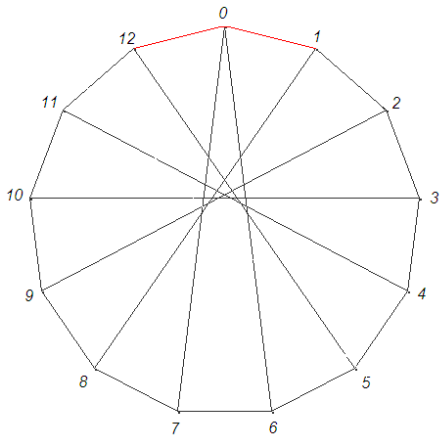


Figure 6: The Harary graph $H_{(13,3)}$

Proof. The vertex 0 is connected to $1, m, m+1$ and $2m$. Let the edges $(0,1)$ and $(0,2m)$ represent the same key.
Because we do not have to consider communication between two vertices that share a unique key, we only have to find three disjunct paths for the following couples.

$$0 \leftrightarrow 1 \begin{cases} 0 \rightarrow 1 \\ 0 \rightarrow m \rightarrow m-1 \rightarrow \ldots \rightarrow 1 \\ 0 \rightarrow m+1 \rightarrow m+2 \rightarrow 1 \end{cases}$$

$$0 \leftrightarrow 2m \begin{cases} 0 \rightarrow 2m \\ 0 \rightarrow m+1 \rightarrow m+2 \rightarrow \ldots \rightarrow 2m \\ 0 \rightarrow m \rightarrow m-1 \rightarrow 1 \end{cases}$$

For $i : 1 < i < m$

$$0 \leftrightarrow i \begin{cases} 0 \rightarrow 1 \rightarrow \ldots \rightarrow i \\ 0 \rightarrow m \rightarrow m-1 \rightarrow \ldots \rightarrow i \\ 0 \rightarrow m+1 \rightarrow m+2 \rightarrow \ldots \rightarrow m+1+i \rightarrow i \end{cases}$$

For $i : m+1 < i < 2m$

$$0 \leftrightarrow i \begin{cases} 0 \rightarrow 2m \rightarrow \ldots \rightarrow i \\ 0 \rightarrow m+1 \rightarrow m+2 \rightarrow \ldots \rightarrow i \\ 0 \rightarrow m \rightarrow m-1 \rightarrow \ldots \rightarrow m+i \rightarrow i \end{cases}$$

$$1 \leftrightarrow 2m \begin{cases} 1 \to 0 \to 2m \\ 1 \to 2 \to 3 \to \ldots \to m-1 \to 2m \\ 1 \to m+2 \to m+3 \to \ldots \to 2m-1 \to 2m \end{cases}$$

For $i : 1 < i < m+2$

$$1 \leftrightarrow i \begin{cases} 1 \to 2 \to \ldots \to i-1 \to i \\ 1 \to 0 \to 2m \to \ldots \to i+m+1 \to i \\ 1 \to m+2 \to m+1 \to \ldots \to i+1 \to i \end{cases}$$

For $i : m+1 < i < 2m$

$$1 \leftrightarrow i \begin{cases} 1 \to 2 \to \ldots \to i+m \to i \\ 1 \to 0 \to 2m \to \ldots \to i+1 \to i \\ 1 \to m+2 \to m+3 \to \ldots \to i-1 \to i \end{cases}$$

By symmetry we do not need to show $2m \leftrightarrow i$.
Let $m(i) = m+1$ if $1 \leq i \leq m$ and $m(i) = m$ if $m+1 \leq i \leq 2m$.
For $i, j \notin \{0, 1, 2m\}$, $i < j$ and $j - i < m+1$:

$$i \leftrightarrow j \begin{cases} i \to i+m(i) \to \ldots \to j+1 \to j \\ i \to i+1 \to \ldots \to j-1 \to j \\ i \to i-1 \to \ldots \to j+m(j) \to j \end{cases}$$

For $i, j \notin \{0, 1, 2m\}$, $i < j$ and $j - i > m$:

$$i \leftrightarrow j \begin{cases} i \to i+m(i) \to \ldots \to j-1 \to j \\ i \to i+1 \to \ldots \to j+m(j) \to j \\ i \to i-1 \to \ldots \to j+1 \to j \end{cases}$$

Thus all vertices can communicate safely with all other vertices. Harary graphs give a safe communication scheme for this case with only $\lfloor \frac{1}{2} \cdot 3n \rfloor$ keys.

□

Theorem 2.4. *Consider the Harary graph $H_{(2m+1,2m-1)}$ were $m \geq 4$. Suppose that all edges have their own unique key, except for two edges ending in 0. The edges $(0,1)$ and $(0, m+1)$ represent the same key. Then safe communication between any two vertices is always possible if there are up to $2m-2$ adversaries.*

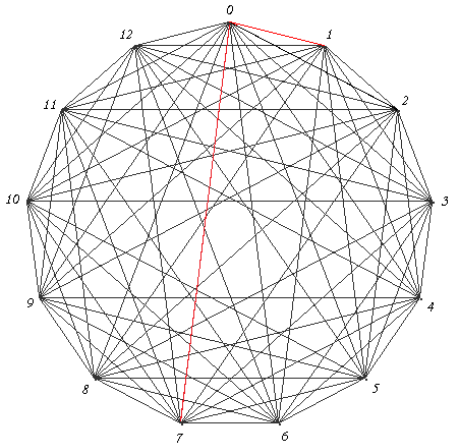


Figure 7: The Harary graph $H_{(13,11)}$

Proof. Assign the same key to the edges $(0,1)$ and $(0,m+1)$.
Vertex 0 is connected to every other vertex, for 1 and $m+1$ use the paths $0 \to i \to 1$ respectively $m+1$ for all i except 1 and $m+1$.
Now each vertex $i \neq 0$ is connected to all other vertices but one, say $j \neq 0$. Now j is connected to all vertices except i. So the $2m-1$ vertices connected to i are also connected to j, thus there are $2m-1$ disjunct paths from i to j.
The two paths with the same key are only used if either 1 or $m+1$ is one of the vertices that want to communicate. This is only the case if 1 and $m+1$ want to communicate (since they are not connected and every vertex is connected to all other but one). And in this case the whole path $1 \to 0 \to m+1$ is used.
Thus every couple is able to communicate in a secure way.
Thus the Harary graph $H_{(2m+1,2m-1)}$ were $m \geq 4$ where the edges $(0,1)$ and $(0,m+1)$ represent the same key allow safe communication if there are up to $2m-2$ adversaries. □

Now we have seen that there are two types of Harary graphs that give a safe communication scheme, but in between it is not possible to assign the same key to two edges without implying a forbidden subgraph.

The forbidden subgraphs are not allowed in a graph. For a graph to represent a safe communication scheme were two edges represent the same key, it is a necessary condition that is does not contain a forbidden subgraph. But this is not sufficient, a graph without forbidden subgraphs does not automatically represent a safe communication scheme.
Consider graph in Figure 8. This is a scheme for 13 participants and up to 6 adversaries. If we assign the same key to the edges $(0,1)$ and $(0,2)$ and a unique key to all other edges, there is no forbidden subgraph. But not all couples are able to communicate in a secure way.

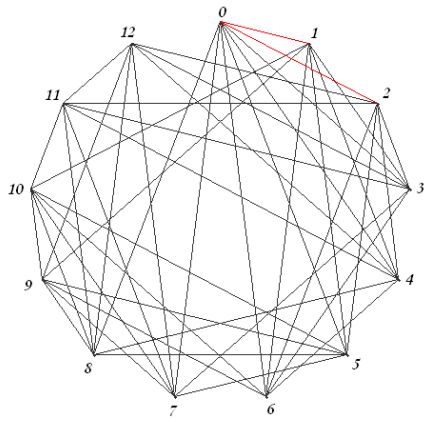


Figure 8: A graph with 13 vertices without forbidden subgraphs

For example communication between vertex 1 and vertex 7 may use the paths:
$1 \to 10 \to 7$
$1 \to 9 \to 7$
$1 \to 5 \to 7$
$1 \to 3 \to 7$
$1 \to 0 \to 7$
$1 \to 4 \to 12 \to 7$
Thus we find 6 disjunct paths, the last path will contain the vertex 2. But we may not use vertex 2 since it is able to recover another partial message (the one on path $1 \to 0 \to 7$).

Thus 1 and 7 are not able to communicate in a secure way. Thus the absence of the forbidden subgraphs does not imply that the communication scheme is safe.

3 Non-Harary solutions

So Harary graphs do not give a full solution to this problem, but another type of graphs might work. Now we try to find graphs where:

- every vertex has $t+1$ neighbors, except 0 which has $t+2$
- the same key is assigned to two edges ending in 0, all other edges represent a unique key
- every vertex can communicate safely with every other vertex

After finding a few we might be able to generalize these.
The case $n, t = n-3$ is solved, the Harary graphs give a safe communication scheme. Now we will first look at the case $n = 2m+1, t = n-5$, since the restrictions given by the forbidden subgraphs might lead to a solution immediately.
From now on we will use the incidence matrix to represent the graphs and we will assign the same key to the paths (0,1) and (0,2) unless stated otherwise. The vertex with one connection more will be numbered 0 in all examples.

3.1 Case $n = 2m+1$, $t = n-5$

After finding some graphs for small n, one can try to generalize this form such that it will work for all n. As the case $t+1 = 1$ will not give a connected graph as $n > 2$ and for the case $t+1 = 3$ the Harary graph gives a safe communication scheme, we will start with $t+1 = 5$.

Case $n = 9$, $t = 4$

Since we know three forbidden subgraphs we can construct a graph for the case $n = 9$, $t+1 = 5$. It is known that the diagonal consists only of zeros. Now use the fact that the first row contains three zeros and vertices 1 and 2 are not connected (forbidden subgraph 1). This gives:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & * & * & * & * & * & * \\ 1 & 0 & 0 & * & * & * & * & * & * \\ 1 & * & * & 0 & * & * & * & * & * \\ 1 & * & * & * & 0 & * & * & * & * \\ 1 & * & * & * & * & 0 & * & * & * \\ 1 & * & * & * & * & * & 0 & * & * \\ 0 & * & * & * & * & * & * & 0 & * \\ 0 & * & * & * & * & * & * & * & 0 \end{pmatrix}$$

If vertex 1 is connected to a point a which is also connected to vertex 0, than a should also be connected to vertex 2 (forbidden subgraph 2). If vertex 1 is connected to a point a which is not connected to vertex 0, than a should not

be connected to vertex 2 (forbidden subgraph 3). These two rules and the fact that the second and third row both contain four zeros gives:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & * & * & * & * & * \\ 1 & 1 & 1 & * & 0 & * & * & * & * \\ 1 & 1 & 1 & * & * & 0 & * & * & * \\ 1 & 0 & 0 & * & * & * & 0 & * & * \\ 0 & 1 & 0 & * & * & * & * & 0 & * \\ 0 & 0 & 1 & * & * & * & * & * & 0 \end{pmatrix}$$

The fourth, fifth and sixth row need three more zeros to be filled in. The last three columns only allow one more zero since all three already have three zeros. It is then obvious that (4,5), (4,6), (5,4), (5,6), (6,4) and (6,5) should all be zero. The last three columns get a zero in row 4, 5 or 6, thus (7,8), (7,9), (8,7), (8,9), (9,7) and (9,8) should not be zero.

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & * & * & * \\ 1 & 1 & 1 & 0 & 0 & 0 & * & * & * \\ 1 & 1 & 1 & 0 & 0 & 0 & * & * & * \\ 1 & 0 & 0 & * & * & * & 0 & 1 & 1 \\ 0 & 1 & 0 & * & * & * & 1 & 0 & 1 \\ 0 & 0 & 1 & * & * & * & 1 & 1 & 0 \end{pmatrix}$$

The last eighteen places can be filled in different ways, but these all give isomorphic graphs. This graph is a safe communication scheme for 9 participants and up to 4 adversaries.

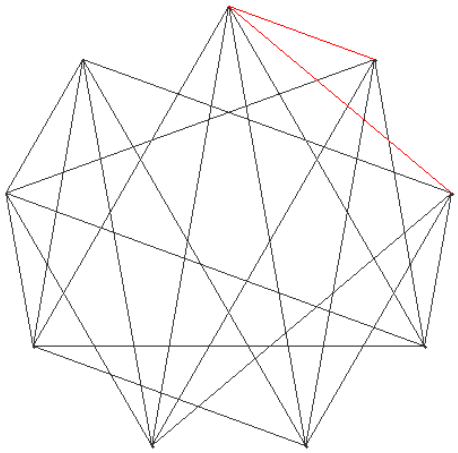


Figure 9: The graph for $n = 9$ and $t + 1 = 5$

Case $n = 11$, $t = 6$

The first three rows of the matrix can be filled the same way as in the $n = 9$, $t = 4$ case and the diagonal only contains zeros. For the others places there are restrictions, but not enough to define the whole matrix. Since there are not so many options left, a correct matrix for this problem can be found easily by trial and error. The next matrix gives a safe communication scheme for $n = 11$, $t = 6$.

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Larger n

The first three rows of every matrix of this type can be filled by using the three forbidden subgraphs and the diagonal only contains zeros. The freedom to fill in the other places gets larger as n gets larger.
Since a graph of this type contains *sum of the degrees of the vertices divided by 2* $= (n \cdot (t+1) + 1)/2 = (n^2 - 4n + 1)/2$ lines, the complement graph contains only $((n-t-1) \cdot (t+1) - 1)/2 = (4n - 17)/2$ lines (which is more than a factor $\frac{1}{4}n$ less as $4n - 17 < \frac{1}{4}n(4n - 17) < n^2 - 4n + 1$).

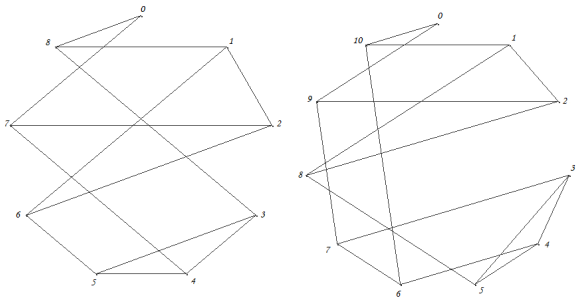


Figure 10: The complement graphs for $n = 9$ and $n = 11$

By changing the positions of the vertices one gets a more simple shape, as can be seen in Figure 11

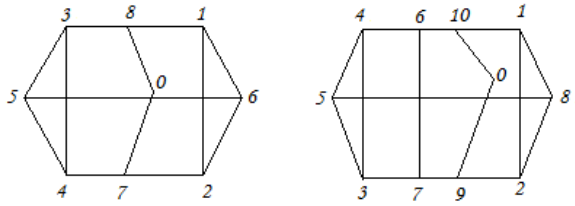


Figure 11: The complement graphs for $n = 9$ and $n = 11$

For the construction we do not use the same numbering as above. The construction of a graph of this type consists of three steps:

1. Start with a cycle of length $n-1$, name the vertices $0, \ldots, n-2$. Connect 0 with $(n-1)/2$ and i with $n-1-i$ for $i = 1, \ldots, (n-1)/2-1$.
2. Remove the edge $2 \leftrightarrow n-3$, add the vertex $n-1$ and connect $n-1$ with 2 and $n-3$.
3. Now take the complement of this graph. And assign the same key to the edges $n-1 \leftrightarrow 1$ and $n-1 \leftrightarrow n-2$.

Proof of the series $n = 2m+1, t = n-5$

We need to prove that this construction gives a safe communication scheme for every odd n and up to $n-5$ adversaries.

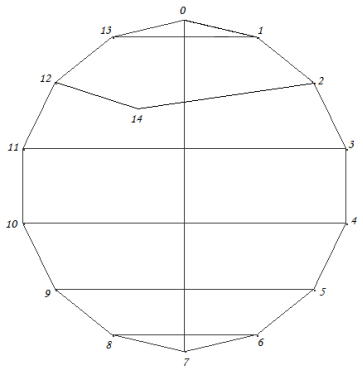


Figure 12: The complement graph for $n = 15$ and $t = 10$

The same key is assigned to the edges $(n-1, 1)$ and $(n-1, n-2)$.

Proof. The proof is a case analysis.

$n-1 \to 1$ Use the paths $n-1 \to 1$, $n-1 \to 0 \to n-3 \to 1$ and for $3 \leq i \leq n-4$ use $n-1 \to i \to 1$, by symmetry there is also a secure communication path between $n-1$ and $n-2$

$n-1 \to 2$ Use the paths $n-1 \to 0 \to 2$, $n-1 \to n-2 \to 2$, $n-1 \to 3 \to n-3 \to 2$ and for $4 \leq i \leq n-4$ use $n-1 \to i \to 2$, by symmetry there is also a secure communication path between $n-1$ and $n-3$

$0 \to 1$ Use the paths $0 \to n-1 \to 1$, $0 \to 2 \to m \to 1$ and for $3 \leq i \leq m-1$ and $m+1 \leq i \leq n-3$ use $0 \to i \to 1$

$0 \to m$ Use the paths $0 \to n-1 \to m$, $0 \to m-1 \to 1 \to m$, $0 \to m+1 \to n-2 \to m$ and for $2 \leq i \leq m-22$ and $m+2 \leq i \leq n-3$ use $0 \to i \to m$

$1 \to 2$ Use the paths $1 \to 3 \to 0 \to 2$, $1 \to n-1 \to n-2 \to 2$ and for $4 \leq i \leq n-3$ use $1 \to i \to 2$

$2 \to 3$ Use the paths $2 \to 4 \to 1 \to 3$, $2 \to n-1 \to 3$ and for $i = 0, 5 \leq i \leq n-5, i = n-3, n-2$ use $2 \to i \to 3$

$k \to k+1$ $(k = 3, 4, \ldots, m-2)$ Use the paths $k \to n-1 \to k+1$, $k \to n-1-k-1 \to k+1$, $k \to k+2 \to n-1-k \to k+1$ and for $i = 0, \ldots, k-2, k+3, \ldots, n-1-k-2, n-1-k+1, \ldots, n-2$ use $k \to i \to k+1$

$m-1 \to m$ Use the paths $m-1 \to n-1 \to m$ and for $i = 0, \ldots, m-3, m+2, \ldots, n-2$ use $m-1 \to i \to m$

$k \to n-1-k$ $(k = 3, 4, \ldots, m-1)$ Use the paths $k \to n-1 \to n-1-k$, $k \to n-1-k-1 \to k-1 \to n-1-k$, $k \to n-1-k+1 \to k+1 \to n-1-k$ and for $i = 0, \ldots, k-2, k+2, \ldots, n-1-k-2, n-1-k+2, \ldots, n-2$ use $k \to i \to n-1-k$

□

3.2 Case $n = 2m + 1$, $t = n - 7$

Again the first three rows can be filled using the forbidden subgraphs. The next step is not as trivial as for the $t = n - 5$-series.

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & * & * & * & * & * & * & * & * \\ 1 & 1 & 1 & * & * & * & * & * & * & * & * \\ 1 & 1 & 1 & * & * & * & * & * & * & * & * \\ 1 & 0 & 0 & * & * & * & * & * & * & * & * \\ 0 & 1 & 0 & * & * & * & * & * & * & * & * \\ 0 & 0 & 1 & * & * & * & * & * & * & * & * \\ 0 & 0 & 0 & * & * & * & * & * & * & * & * \\ 0 & 0 & 0 & * & * & * & * & * & * & * & * \end{pmatrix}$$

With trial and error matrices for $n = 11, 13, 15, 17$ and 19 were found. From these it was again possible to find a structure that seems to work for every n.

The construction of a graph of this type, for $n \geq 13$ consists of the following steps[6]: First draw a subgraph as in Figure 14.

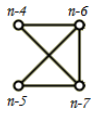


Figure 13: Subgraph 2

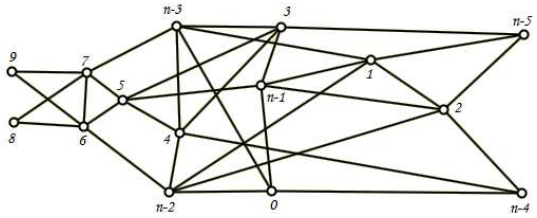


Figure 14: Subgraph 1

Then draw a subgraph as in Figure 13 starting from the left, repeat until the vertices 6 and 7 are reached.
Now connect the graphs and take the complement.

Proof of the series $n = 2m + 1, t = n - 7$

We need to proof that this construction gives a safe communication scheme for every odd n and up to $n - 7$ adversaries.

[6]The graph for $n = 11$, $t = 4$ can be found in appendix A

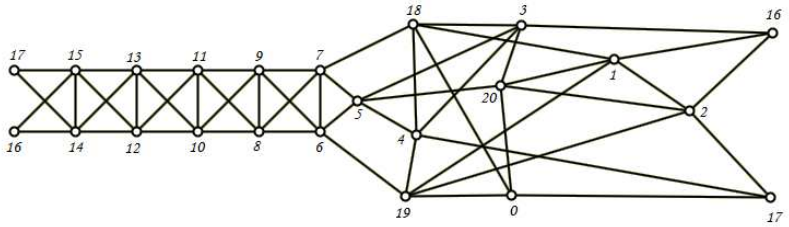


Figure 15: The complement graph for $n = 21$, $t = 14$

For this proof the incidence matrix is used, it gives a more structural view on this graph.

$$\begin{pmatrix}
0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&0&0&0\\
1&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&1&0&0&0\\
1&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&0&1&0&0\\
1&1&1&0&0&0&1&1&1&1&1&1&1&1&1&1&1&0&1&0&1&0\\
1&1&1&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&0&0&0&1\\
1&1&1&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&0\\
1&1&1&1&1&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&0&1\\
1&1&1&1&1&0&0&0&0&0&1&1&1&1&1&1&1&1&1&0&1&1\\
1&1&1&1&1&1&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&1&1&1&1&1\\
1&0&0&0&1&1&1&1&1&1&1&1&1&1&0&0&0&1&1&1&1&1\\
0&1&0&1&0&1&1&1&1&1&1&1&1&1&0&0&1&0&1&1&1&1\\
0&0&1&0&0&1&1&0&1&1&1&1&1&1&1&1&1&1&0&1&1&1\\
0&0&0&1&0&1&0&1&1&1&1&1&1&1&1&1&1&1&1&0&1&1\\
0&0&0&0&1&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&1\\
0&0&0&0&1&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0
\end{pmatrix}$$

Proof. The proof is a case analysis. Let $n > 13$. For $n = 11$ and $n = 13$ the proofs are quite similar and are left for the reader.

$0 \to 1$ Use the paths $0 \to 1$, $0 \to n-5 \to n-4 \to 1$ and for $3 \leq i \leq n-6$ use $0 \to i \to 1$

$0 \to 2$ Use the paths $0 \to 2$, $0 \to n-5 \to n-3 \to 2$ and for $3 \leq i \leq n-6$ use $0 \to i \to 2$

$0 \to n-4$ Use the paths $0 \to i \to n-4$ for $i \in \{1, 3, 5, \ldots, n-8, n-5\}$, $0 \to n-6 \to n-3 \to n-4$, $0 \to n-7 \to n-2 \to n-4$ and $0 \to 4 \to n-1 \to n-4$

$0 \to n-3$ Use the paths $0 \to i \to n-3$ for $i \in \{2, 5, 6, 8, \ldots, n-5\}$, $0 \to 3 \to n-4 \to n-3$, $0 \to 7 \to n-2 \to n-3$ and $0 \to 4 \to n-1 \to n-3$

$0 \to n-2$ Use the paths $0 \to i \to n-2$ for $i \in \{3, 5, 7, \ldots, n-5\}$, $0 \to 1 \to n-4 \to n-2$, $0 \to 6 \to n-3 \to n-2$ and $0 \to 4 \to n-1 \to n-2$

$0 \to n-1$ Use the paths $0 \to i \to n-1$ for $i \in \{4, 6, \ldots, n-5\}$, $0 \to 5 \to n-4 \to n-1$, $0 \to 2 \to n-3 \to n-1$ and $0 \to 3 \to n-2 \to n-1$

$1 \to 2$ Use the paths $1 \to 0 \to 2$, $1 \to n-4 \to n-3 \to 2$ and for $3 \leq i \leq n-6$ use $1 \to i \to 2$

$1 \to n-5$ Use the paths $1 \to i \to n-5$ for $i \in \{0, 4, \ldots, n-8, n-4\}$, $1 \to 3 \to n-2 \to n-5$, $1 \to n-6 \to n-1 \to n-5$ and $1 \to n-7 \to n-3 \to n-5$

$1 \to n-3$ Use the paths $1 \to i \to n-3$ for $i \in \{5, 6, 8, \ldots, n-6, n-4\}$, $1 \to 0 \to 2 \to n-3$, $1 \to 3 \to n-2 \to n-3$, $1 \to 4 \to n-1 \to n-3$ and $1 \to 7 \to n-5 \to n-3$

$1 \to n-2$ Use the paths $1 \to i \to n-2$ for $i \in \{3, 5, 7, \ldots, n-6, n-4\}$, $1 \to 0 \to n-5 \to n-2$, $1 \to 4 \to n-1 \to n-2$ and $1 \to 6 \to n-3 \to n-2$

$1 \to n-1$ Use the paths $1 \to i \to n-2$ for $i \in \{4, 6, \ldots, n-6, n-4\}$, $1 \to 0 \to n-5 \to n-1$, $1 \to 3 \to n-2 \to n-1$ and $1 \to 5 \to n-3 \to n-1$

$2 \to n-5$ Use the paths $2 \to i \to n-5$ for $i \in \{0, 4, \ldots, n-8, n-3\}$, $2 \to 3 \to n-2 \to n-5$, $2 \to n-6 \to n-1 \to n-5$ and $2 \to n-7 \to n-4 \to n-5$

$2 \to n-4$ Use the paths $2 \to i \to n-4$ for $i \in \{3, 5, \ldots, n-8, n-3\}$, $2 \to 0 \to 1 \to n-4$, $2 \to 4 \to n-1 \to n-4$, $2 \to n-6 \to n-2 \to n-4$ and $2 \to n-7 \to n-1 \to n-4$

$2 \to n-2$ Use the paths $2 \to i \to n-2$ for $i \in \{3, 5, 7, \ldots, n-6, n-3\}$, $2 \to 0 \to n-5 \to n-2$, $2 \to 4 \to n-1 \to n-2$ and $2 \to 6 \to n-4 \to n-2$

$2 \to n-1$ Use the paths $2 \to i \to n-2$ for $i \in \{4, 6, \ldots, n-6, n-3\}$, $2 \to 0 \to n-5 \to n-1$, $2 \to 3 \to n-2 \to n-1$ and $2 \to 5 \to n-4 \to n-1$

$3 \to 4$ Use the paths $3 \to i \to 4$ for $i \in \{0, 1, 2, 6, \ldots, n-6\}$, $3 \to n-4 \to n-5 \to 4$ and $3 \to n-2 \to n-1 \to 4$

$3 \to 5$ Use the paths $3 \to i \to 5$ for $i \in \{0, 1, 2, 8, \ldots, n-6, n-4, n-2\}$, $3 \to 6 \to n-3 \to 5$ and $3 \to 7 \to n-5 \to 5$

$3 \to n-5$ Use the paths $3 \to i \to n-5$ for $i \in \{0, 6, \ldots, n-8, n-4, n-2\}$, $3 \to 1 \to 4 \to n-5$, $3 \to 2 \to 5 \to n-5$, $3 \to n-6 \to n-3 \to n-5$ and $3 \to n-7 \to n-1 \to n-5$

$3 \to n-3$ Use the paths $3 \to i \to n-3$ for $i \in \{2, 6, 8, \ldots, n-6, n-4, n-2\}$, $3 \to 0 \to n-5 \to n-3$, $3 \to 1 \to 5 \to n-3$ and $3 \to 7 \to n-1 \to n-3$

$3 \to n-1$ Use the paths $3 \to i \to n-1$ for $i \in \{6, \ldots, n-6, n-4, n-2\}$, $3 \to 0 \to n-5 \to n-1$, $3 \to 1 \to 4 \to n-1$ and $3 \to 2 \to n-3 \to n-1$

$4 \to 5$ Use the paths $4 \to i \to 5$ for $i \in \{0, 1, 2, 8, \ldots, n-5\}$, $4 \to 6 \to n-3 \to 5$, $4 \to 7 \to n-2 \to 5$ and $4 \to n-1 \to n-4 \to 5$

$4 \to n-4$ Use the paths $4 \to i \to n-4$ for $i \in \{1, 6, \ldots, n-8, n-5, n-1\}$, $4 \to 0 \to n-5 \to n-4$, $4 \to 2 \to 3 \to n-4$, $4 \to n-7 \to n-2 \to n-4$ and $4 \to n-6 \to n-3 \to n-4$

$4 \to n-3$ Use the paths $4 \to i \to n-3$ for $i \in \{2, 6, 8, \ldots, n-5, n-1\}$, $4 \to 0 \to 5 \to n-3$, $4 \to 1 \to n-4 \to n-3$ and $4 \to 7 \to n-2 \to n-3$

$4 \to n-2$ Use the paths $4 \to i \to n-2$ for $i \in \{7, \ldots, n-5, n-1\}$, $4 \to 0 \to 5 \to n-2$, $4 \to 1 \to n-4 \to n-2$, $4 \to 2 \to n-3 \to n-2$ and $4 \to 6 \to 3 \to n-2$

$5 \to 6$ Use the paths $5 \to i \to 6$ for $i \in \{0, 1, 2, 10, \ldots, n-3\}$, $5 \to 8 \to 3 \to 6$, $5 \to 9 \to 4 \to 6$ and $5 \to n-2 \to n-1 \to 6$

$5 \to 7$ Use the paths $5 \to i \to 7$ for $i \in \{0, 1, 2, 10, \ldots, n-4, n-2\}$, $5 \to 8 \to 3 \to 7$, $5 \to 9 \to 4 \to 7$ and $5 \to n-3 \to n-1 \to 7$

$5 \to n-1$ Use the paths $5 \to i \to n-1$ for $i \in \{8, \ldots, n-2\}$, $5 \to 0 \to 4 \to n-1$, $5 \to 1 \to 6 \to n-1$ and $5 \to 2 \to 7 \to n-1$

$6 \to 7$ Use the paths $6 \to i \to 7$ for $i \in \{0, \ldots, 4, 10, \ldots, n-4, n-1\}$ and $6 \to n-3 \to n-2 \to 7$

$6 \to 8$ Use the paths $6 \to i \to 8$ for $i \in \{0, \ldots, 4, 12, \ldots, n-3, n-1\}$, $6 \to 9 \to n-2 \to 8$ and $6 \to 10 \to 5 \to 8$

$6 \to 9$ Use the paths $6 \to i \to 9$ for $i \in \{0, \ldots, 4, 12, \ldots, n-3, n-1\}$, $6 \to 9 \to n-2 \to 9$ and $6 \to 10 \to 5 \to 9$

$6 \to n-2$ Use the paths $6 \to i \to n-2$ for $i \in \{3, 10, \ldots n-3, n-1\}$, $6 \to 0 \to 5 \to n-2$, $6 \to 1 \to 7 \to n-2$, $6 \to 2 \to 8 \to n-2$ and $6 \to 4 \to 9 \to n-2$

$7 \to 8$ Use the paths $7 \to i \to 8$ for $i \in \{0, \ldots, 4, 12, \ldots, n-4, n-2, n-1\}$, $7 \to n-11 \to 5 \to 8$ and $7 \to n-10 \to n-3 \to 8$

$7 \to 9$ Use the paths $7 \to i \to 9$ for $i \in \{0, \ldots, 4, 12, \ldots, n-4, n-2, n-1\}$, $7 \to n-11 \to 5 \to 9$ and $7 \to n-10 \to n-3 \to 9$

$7 \to n-3$ Use the paths $7 \to i \to n-3$ for $i \in \{2, 10, \ldots n-4, n-2, n-1\}$, $7 \to 0 \to 5 \to n-3$, $7 \to 1 \to 6 \to n-3$, $7 \to 3 \to 8 \to n-3$ and $7 \to 4 \to 9 \to n-3$

$n-5 \to n-7$ Use the paths $n-5 \to i \to n-7$ for $i \in \{0, 4, \ldots, n-10, n-3, \ldots, n-1\}$, $n-5 \to n-9 \to 1 \to n-7$, $n-5 \to n-8 \to 2 \to n-7$ and $n-5 \to n-4 \to 3 \to n-7$

$n-5 \to n-7$ Use the same paths as from $n-5$ to $n-7$

$n-4 \to n-7$ Use the paths $n-4 \to i \to n-7$ for $i \in \{1,3,5,\ldots,n-10,n-3,\ldots,n-1\}$, $n-4 \to n-9 \to 0 \to n-7$, $n-4 \to n-8 \to 2 \to n-7$ and $n-4 \to n-5 \to 4 \to n-7$

$n-4 \to n-6$ Use the paths $n-4 \to i \to n-6$ for $i \in \{1,3,5,\ldots,n-10,n-3,\ldots,n-1\}$, $n-4 \to n-9 \to 0 \to n-6$, $n-4 \to n-8 \to 2 \to n-6$ and $n-4 \to n-5 \to 4 \to n-6$

Now for $j = 8,\ldots,n-6$, if for $j \to i$ holds $i \leq n-6$:
if j is even:

$j \to j+1$ Use the paths $j \to i \to j+1$ for $i \in \{0,\ldots,j-3,j+4,\ldots,n-1\}$

$j \to j+2$ Use the paths $j \to i \to j+1$ for $i \in \{0,\ldots,j-3,j+6,\ldots,n-1\}$, $j \to j-2 \to j+4 \to j+2$ and $j \to j-1 \to j+5 \to j+2$

$j \to j+3$ Use the paths $j \to i \to j+1$ for $i \in \{0,\ldots,j-3,j+6,\ldots,n-1\}$, $j \to j-2 \to j+4 \to j+3$ and $j \to j-1 \to j+5 \to j+3$

if j is odd:

$j \to j+1$ Use the paths $j \to i \to j+1$ for $i \in \{0,\ldots,j-3,j+6,\ldots,n-1\}$, $j \to j-2 \to j+4 \to j+1$ and $j \to j-1 \to j+5 \to j+1$

$j \to j+2$ Use the paths $j \to i \to j+1$ for $i \in \{0,\ldots,j-3,j+6,\ldots,n-1\}$, $j \to j-2 \to j+4 \to j+2$ and $j \to j-1 \to j+5 \to j+2$

□

This proof has a lot more cases than the proof of the $t = n-5$-series and more graphs were needed to find the structure of this series. So probably every following series will be harder to find and to prove than the one before.

3.3 Case $n = 2m+1$, $t = n-9$

For this series the graphs for $n = 13, 15, 17, 19, 21$ and 23 were found by trial and error, but still no structure was found. Knowing these graphs, the graph for $n = 25$ can not be constructed trivially. As expected for each new series more graphs are needed to find the structure and the proof will contain more cases as the non-trivial part of the graph gets larger.
Also there is no trivial path from the series before to the next series. Unfortunately there was no more time to find a construction which would give all graphs.

3.4 Case $n = 2m+1$, $t = 4$

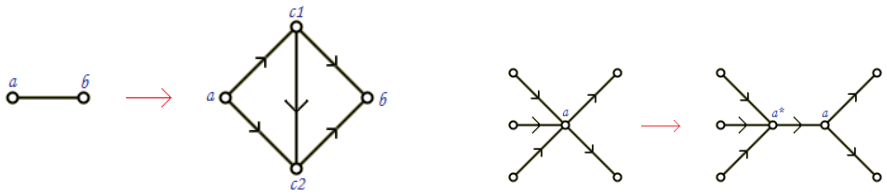
For $n = 9, 11, 13$ these graphs are mentioned before in this paper. Knowing these, the graphs for $n = 15, 17, 19, 21, 23$ were found easily, but every one of these has a few rows that are not resemblant. No structure was found for this series.

4 JAVA Program

I have written a JAVA program that checks whether safe communication is possible in a graph, where the graph has an odd number of vertices and an even number of adversaries and the edges from 0 to 1 and 0 to 2 are assigned the same key.

`Input:`
A matrix M which represents a graph in which every edge is assigned a different key except for the edges (0,1) and (0,2) which share a key.

`Method`
Create four new matrices to make sure that the edges (0,1) and (0,2) are not used in two different paths:
$M1$ remove all edges to 0,1 and 2 (the vertices 0,1,2 are not used)
$M2$ remove all edges to 0, add the edge (1,2) (the path $1 \leftrightarrow 0 \leftrightarrow 2$ is used)
$M3$ remove all edges to 1 (the vertex 1 is not used)
$M3$ remove all edges to 2 (the vertex 2 is not used)
Change these matrices to directed matrices as follows:



Replace each edge by five directed edges (left figure) and replace a vertex with multiple edges coming in and multiple edges going out by two vertices (right figure).
For every two vertices find a max flow by using Ford and Fulkersons max-flow algorithm, Dijkstra's shorthest path algorithm is used to find a path in every step in the Ford and Fulkerson algorithm.

`Output:`
The number of disjunct paths for every two vertices which are not directly connected by an edge with a non-shared key.

Bibliography

[1] Y. Desmedt, H.-X. Wang, and H.C.A. van Tilborg, *Bounds and constructions for key distribution schemes*, Advances in Mathematics of Communications, Vol. 3, 2009, p. 273-293.

[2] Alexander Schrijver, *Grafen: Kleuren en Routeren*, http://www.win.tue.nl/ gwoegi/2WO10/

[3] Alexander Schrijver, *A Course in Combinatorial Optimization*, http://www.win.tue.nl/ gwoegi/2WO10/

[4] Frank Harary, *The Maximum Connectivity of a Graph*, Proceedings of the National Academy of Sciences of the United States of America, Vol. 48, No. 7 (Jul. 15, 1962)

A Matrices

The matrices are named $(n, t+1)$ where n is the number of participants and t is the maximum number of adversaries.

A.1 Case $n = 2m + 1$, $t = n - 5$

(9,5)

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

(11,7)

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

(13,9)

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

(15,11)

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0
\end{pmatrix}$$

(17,13)

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0
\end{pmatrix}$$

(19,15)

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0
\end{pmatrix}$$

A.2 Case $n = 2m + 1$, $t = n - 7$

(11,5)

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0
\end{pmatrix}$$

(13,7)

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

(15,9)

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

(17,11)

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0
\end{pmatrix}$$

(19,13)

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0
\end{pmatrix}$$

(21,15)

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0
\end{pmatrix}$$

A.3 Case $n = 2m + 1$, $t = n - 9$

(13,5)

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0
\end{pmatrix}$$

(15,7)

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0
\end{pmatrix}$$

(17,9)

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0
\end{pmatrix}$$

(19,11)

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0
\end{pmatrix}$$

(21,13)

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0
\end{pmatrix}$$

(23,15)

$$\begin{pmatrix}
0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0\\
1&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&1&0&0&0&0\\
1&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&0&1&0&0&0\\
1&1&1&0&0&0&1&1&1&1&1&1&1&1&1&1&1&0&1&0&1&0&0\\
1&1&1&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&0&0&0&1&0\\
1&1&1&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&0&1&0&1&0\\
1&1&1&1&1&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&0&0&1\\
1&1&1&1&1&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&0&1&1\\
1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&1&1&1&1\\
1&0&0&0&1&1&1&1&1&1&1&1&1&1&0&0&0&0&1&0&1&1&1\\
0&1&0&1&0&1&1&1&1&1&1&1&1&1&0&0&0&0&1&0&1&1&1\\
0&0&1&0&0&0&1&1&1&1&1&1&1&1&0&0&1&1&0&1&1&1&1\\
0&0&0&1&0&1&1&1&1&1&1&1&1&1&1&0&0&0&1&0&1&1&1\\
0&0&0&0&1&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&0&1&1\\
0&0&0&0&0&1&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&0\\
0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&0
\end{pmatrix}$$

A.4 Case $n = 2m + 1 \geq 15$, $t = 4$

(15,5)

$$\begin{pmatrix}
0&1&1&1&1&1&1&0&0&0&0&0&0&0&0\\
1&0&0&1&1&0&0&1&1&0&0&0&0&0&0\\
1&0&0&1&1&0&0&0&0&1&1&0&0&0&0\\
1&1&1&0&0&0&0&0&0&0&0&1&1&0&0\\
1&1&1&0&0&0&0&0&0&0&0&0&0&1&1\\
1&0&0&0&0&0&0&1&1&1&1&0&0&0&0\\
1&0&0&0&0&0&0&1&1&1&1&0&0&0&0\\
0&1&0&0&0&1&1&0&0&0&0&1&1&0&0\\
0&1&0&0&0&1&1&0&0&0&0&1&1&0&0\\
0&0&1&0&0&1&1&0&0&0&0&0&0&1&1\\
0&0&1&0&0&1&1&0&0&0&0&0&0&1&1\\
0&0&0&1&0&0&0&1&1&0&0&0&0&1&1\\
0&0&0&1&0&0&0&1&1&0&0&0&0&1&1\\
0&0&0&0&1&0&0&0&0&1&1&1&1&0&0\\
0&0&0&0&1&0&0&0&0&1&1&1&1&0&0
\end{pmatrix}$$

(17,5)

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0
\end{pmatrix}$$

(19,5)

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0
\end{pmatrix}$$

(21,5)

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0
\end{pmatrix}$$

(23,5)

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0
\end{pmatrix}$$

B Program manual

Make sure you have the program in the same folder as the matrices you want to check. The matrices should be in a .txt file and every row contains only zeros and ones separated by spaces. The program can check whether the matrix you loaded is symmetric and if the zero row has exactly one one more than all other rows.

`Menu items`

- **Check Graph** After you loaded a graph you can make the program find out whether safe communication is possible in the loaded graph, where the edges (0,1) and (0,2) share one key.
- **Load Graph** This asks for the name of the .txt file which contains the file, the input should end with ".txt".
- **Options** Here you can choose whether the program should check if the matrix is symmetric and if the vertex zero has exactly one edge more than all others vertices. This will be executed when the option check graph is activated.
- **Output** Here you can generate different outputs, the complement graph, the adjacency matrix and the adjacency matrix of the complement graph.

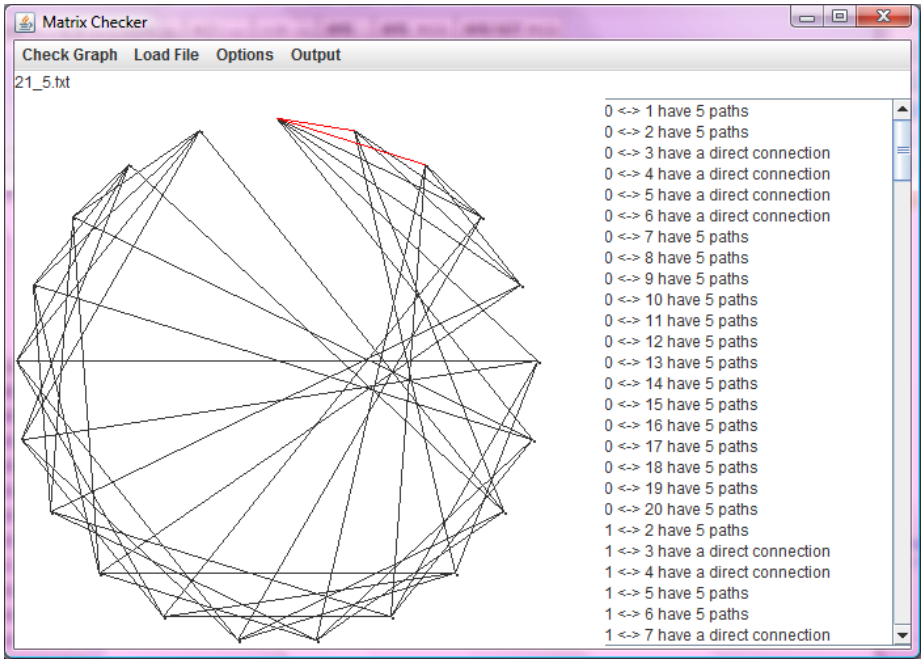


Figure 16: The JAVA Program

The program looks as in Figure 16. The graph is drawn in the center, above the graph is the name of the file you loaded. After you have checked the graph the right textfield will be filled with the number of paths between every pair of vertices.

The JAVA code can be found on the cd attached to this report. All matrices given in appendix A and an executable jar file of the program can also be found on the cd.