Pliable Index Coding Problem

BY

TANG LIU
B.E., University of Electronic Science and Technology of China, 2010
M.S., Korean Advanced Institute of Science and Technology, 2013
M.S., University of Illinois at Chicago, 2019

THESIS

Submitted as partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Electrical and Computer Engineering
in the Graduate College of the
University of Illinois at Chicago, 2020

Chicago, Illinois

Defense Committee:
Daniela Tuninetti, Chair and Advisor
Natasha Devroye
Besma Smida
György Turán, MCS UIC
Christina Fragouli, UCLA

ACKNOWLEDGMENTS

I would first like to thank my Ph.D. advisor Professor Daniela Tuninetti for her hearty guide and support. Her enthusiasm and perfectionism in academic research provided me the direction in pursuing my Ph.D. degree. I find myself lucky to have such a wonderful supervisor to work with during my study.

I would also thank Professor György Turán, from him I learned a lot in combinatorics. The knowledge I got from his class and the discussion with him eventually led me to the solution for the consecutive complete–S PICOD$(\mathtt{t})$ problem. The solution could be much messier without his teaching and help.

Last but not least, I would like to thank all my friendly labmates, especially Dr. Kai Wan. Their help, both in academic research and private life, made my life much more productive and enjoyable during the past years.

TL

TABLE OF CONTENTS

CHAPTER		PAGE
1	**INTRODUCTION**	1
1.1	Pliable Index Coding	1
1.1.1	From Index Coding to Pliable Index Coding	3
1.1.2	Decentralized Pliable Index Coding	5
1.1.3	Secure Pliable Index Coding	6
1.2	Past Work	7
1.2.1	Pliable Index Coding	7
1.3	Decentralized Pliable Index Coding	9
1.3.1	Security in Index Coding	10
1.4	Contributions	10
1.4.1	Achievability	11
1.4.1.1	Pliable Index Coding	11
1.4.1.2	Decentralized Pliable Index Coding	11
1.4.1.3	Secure Pliable Index Coding	12
1.4.2	Converse	13
1.4.2.1	Pliable Index Coding	13
1.4.2.2	Decentralized Pliable Index Coding	15
1.4.2.3	Secure Pliable Index Coding	16
1.4.3	Corresponding Publications	16
2	**CONSTANT FRACTION OF SATISFIED USERS IN PLIABLE INDEX CODING PROBLEM**	18
2.1	System Model	18
2.2	Greedy Set Cover Achievability	20
2.2.1	Problem Representation	20
2.2.2	Performance Analysis	22
2.2.3	Randomly Generated Side Information Sets	29
2.3	Comparison to Known Results	30
3	**COMPLETE–S PICOD(T) AND PICOD(1) WITH CIRCULAR-ARC NETWORK TOPOLOGY HYPERGRAPH**	33
3.1	Main Results and Discussion	33
3.1.1	Achievability	33
3.1.2	Converse for some complete–S PICOD(t) problems	34
3.1.3	Converse for PICOD(1) with circular-arc network topology hypergraph	38
3.2	Achievability: proof of Proposition 1	39

TABLE OF CONTENTS (Continued)

CHAPTER **PAGE**

3.3	Layer Counting Converse: Proof of Theorem 2	40
3.4	Critical Case: complete–$\{s\}$ the PICOD(t) with $m = 2s + t$ messages	47
3.4.1	Converse Main Ingredient 1: Block Cover	48
3.4.2	Converse Main Ingredient 2: Maximum Acyclic Induced Subgraph (MAIS) Bound	51
3.4.3	Proof of Proposition 6	54
3.4.4	Complete–S where $\|S\| = 1$	57
3.4.4.1	Complete–$\{s\}$ PICOD(t) where $m < 2s + t$	57
3.4.4.2	Complete–$\{s\}$ PICOD(t) where $m > 2s + 1$	58
3.5	Complete–S PICOD(t) where S is consecutive: Proof of Theorem 3	59
3.5.1	Case $s_{max} \leq \lceil m/2 \rceil - 1$: $\ell^* = s_{max} + 1$	59
3.5.2	Case $s_{min} \geq \lfloor m/2 \rfloor$: $\ell^* = m - s_{min}$	59
3.5.3	Case $s_{min} \leq \lceil m/2 \rceil - 1 \leq \lfloor m/2 \rfloor \leq s_{max}$	59
3.6	Some other complete–S PICOD(t) problems	61
3.6.1	Proof of Proposition 2	61
3.6.2	Proof of Proposition 3	61
3.6.3	Proof of Proposition 4	61
3.6.4	Proof of Proposition 5	62
3.7	Proof of Theorem 4	65
3.7.1	Graph Preliminary	65
3.7.2	On the Optimality of a Single Transmission	67
3.7.3	Proof of Theorem 4	68
3.8	Proof of Lemma 3	71

4 DECENTRALIZED COMPLETE–S PICOD(T) AND PICOD(1) WITH CIRCULAR-ARC NETWORK TOPOLOGY HYPERGRAPH 73

4.1	System Model	73
4.2	Main Results and Discussions	74
4.2.1	Complete–S d-PICOD(t) problems	75
4.2.2	Converse for d-PICOD(1) with circular-arc network topology hypergraph	79
4.3	Decentralized Complete–S PICOD(t) Problems	80
4.3.1	Proof for Theorem 5	80
4.3.1.1	Case $s_{max} + t \leq m - s_{min}$	80
4.3.1.2	Case $t < m - s_{min} < s_{max} + t$	81
4.3.1.3	Case $s_{min} = s_{max} = m - t$	84
4.3.1.3.1	Converse	84
4.3.1.3.2	Achievability	86
4.3.2	Proof for Theorem 6	90
4.3.2.1	Case $s_{min} - 1 + t < s_{max} + 1 = m - t$	91
4.3.2.2	Other Case	91
4.3.3	Extensions of Theorem 5	92

TABLE OF CONTENTS (Continued)

CHAPTER **PAGE**

4.3.3.1 Proof of Proposition 9 92
4.3.3.2 Proof of Proposition 10 92
4.3.3.3 Proof of Proposition 11 93
4.3.4 Proof of Proposition 12 93
4.4 Circular-arc PICOD(1) 94
4.4.1 Case 1: a 1-factor does not exist 95
4.4.1.1 First transmission 96
4.4.1.2 Second transmission 98
4.4.2 Case 2: a 1-factor exists 98
4.4.2.1 Converse 99
4.4.2.2 Achievability 99

5 INDIVIDUALLY SECURE PICOD(1) WITH CIRCULAR-ARC NETWORK TOPOLOGY HYPERGRAPH 102
5.1 Individual Security and Circular Shift Side Information 103
5.1.1 Individual Security 103
5.1.2 Size-s circular-h shift Side Information 104
5.2 Main Result 104
5.3 Proof of Theorem 8 106
5.3.1 Impossible Cases 106
5.3.1.1 Case m is odd, $s = m-2$, and $g = 1$ 106
5.3.1.2 Case m is odd, $s = 1$, and $g = 1$ 107
5.3.2 Case $s < m/2$ and $g = 1$ (here $m = n$) 107
5.3.2.1 Achievability 107
5.3.2.2 Converse 109
5.3.2.2.1 Proof of Proposition 13 111
5.3.2.2.2 Proof of Proposition 14 112
5.3.3 Case $s < m/2$ and $g = s = 2$ (here $n = m/2$) 113
5.3.3.1 Achievability 113
5.3.3.2 Converse 113
5.3.3.2.1 Proof of Proposition 13 113
5.3.4 Remaining Cases 114
5.3.4.1 Converse for all three cases 115
5.3.4.2 Achievability for case $s < m/2$, $g = 2$, and $s \neq 2$ 115
5.3.4.3 Achievability for case $s < m/2$, $g \geq 3$ 115
5.3.4.4 Achievability for case $s \geq m/2$ 116

6 CONCLUSION AND FUTURE WORK 117
6.1 Conclusion 117
6.1.1 Pliable Index Coding 117
6.1.2 Decentralize Pliable Index Coding 119
6.1.3 Secure Pliable Index Coding 119

TABLE OF CONTENTS (Continued)

CHAPTER **PAGE**

6.2 Future Work 120

CITED LITERATURE 124

VITA 126

LIST OF TABLES

TABLE		PAGE
I	COMPLETE–S PICOD(T) THAT ARE NOT COVERED BY THEOREM 2 AND PROPOSITIONS 2, 3, 4. ©IEEE 2019.	62
II	FIRST 6 TRANSMISSIONS FOR $M = 4, S = T = 2$.©IEEE 2019.	88
III	LAST 6 TRANSMISSIONS FOR $M = 4, S = T = 2$, CODEWORDS AND DECODING MESSAGES AT USERS U_1, U_2, U_3. ©IEEE 2019.	89
IV	LAST 6 TRANSMISSIONS FOR $M = 4, S = T = 2$, CODEWORDS AND DECODING MESSAGES AT USERS U_4, U_5, U_6.©IEEE 2019.	89
V	OPTIMAL CODES FOR THE OTHER CASES OF COMPLETE–S D-PICOD(T) WITH $M \leq 5$ MESSAGES. ©IEEE 2019.	94
VI	COMPLETE-S PICOD	117
VII	CIRCULAR SHIFT PICOD	118

LIST OF FIGURES

FIGURE		PAGE
1	Bipartite graph representing the satisfaction relationship between possible transmitted codewords (left side nodes) and clients (right side nodes). ©IEEE 2016.	21
2	Lower bound on the fraction of satisfied clients by one transmission for different request set sizes. ©IEEE 2016.	31
3	Lower bounds comparison for different message sizes. ©IEEE 2016.	32
4	Layer representation of the complete–$[0 : m - 1]$ PICOD(1) problem. ©IEEE 2019.	44
5	Two transmissions scheme for circular-arc network topology hypergraph PICOD(t). ©IEEE 2019.	69
6	Zero pattern matrix $\mathbf{Z}$. ©IEEE 2019.	83

LIST OF ABBREVIATIONS

IC	Index Coding
NC	Network Coding
PICOD	Pliable Index Coding
d-PICOD	Decentralized Pliable Index Coding.

SUMMARY

The Pliable Index Coding (PICOD) problem is a variant of the Index Coding (IC) problem. The IC consists of one transmitter/server and several users/clients. The transmitter and users are connected by a shared noiseless broadcast channel. Each user has a subset of the messages as its side information set and requests some messages that are not in its side information set. The transmitter has all the messages and knows the side information sets of all users. The transmitter serves all users by sending a codeword through the noiseless broadcast channel. The codeword is encoded by the transmitter based on the message set and the side information sets at all users. The goal for the transmitter is to send a codeword such that all users are able to decode their desired messages. For the IC we seek to determine the minimum number of transmissions needed for the transmitter to achieve this goal. In many practical scenarios, such as network streaming or Internet advertising, the desired messages are not always fixed. The transmitter is thus able to leverage this pliability to reduce the communication cost. The PICOD is a variant of the IC model which captures this idea. In the PICOD users do not request specific messages. Instead, they are satisfied by receiving messages that are not in their side information sets. This pliability provides more encoding opportunities, thus can potentially reduce the number of transmissions.

For the general PICOD problem, we show that at least a constant fraction of users can be satisfied by one transmission. We provide a constructive way to find the codeword and the users that can be satisfied by one transmission. This shows that the number of transmissions for any PICOD is upper bounded by $O(\log^2(n))$, where n is the number of users in the system. We also derive information theoretic converse bounds for some cases of PICOD, shows that these bounds can be achieved by the

linear codes. The converse bounds are derived by novel techniques based on combinatorics and are the first non-trivial information theoretical converse results that are tight for a large class of the PICOD problems.

We then study the decentralized PICOD problem, where the codewords are generated by the users based on their own side information set. This model is motivated by decentralized networks such as distributed computation system and Internet of Things networks. In these networks communication occurs in a decentralized fashion without a central controller. For the cases with information theoretical optimality in the centralized setting, we surprisingly find that the optimal number of transmissions remains the same in the decentralized, except when the problem loses its pliability. When the problem is no long pliable, we show that the cut-set bound is tight and can be achieved using decentralized vector linear index codes.

Lastly, we put the security constraints into the PICOD problem. Security and privacy are some of the major concerns in today's communication networks. Information theoretical security guarantees of security and privacy in the situations where information can be leaked to undesired parties. Different from computational security, which replies on the fact that certain problems are considered hard to solve, information theoretical security is robust against all possible attacks, regardless of the computation capability of the attacker. For the PICOD with security constraint, we look at the problem where all users are allowed to decode one and only one message and the side information structure is a circular-arc hypergraph where all users have the same size of the side information sets. We show that the optimal number of transmissions does not change when the size of side information set is large compared to the number of messages in the system. However, it changes dramatically when the size of side information

set is small. Specifically, when $s < m/2$ (where s is the size of side information set and m is the number of messages), the optimal number of transmissions for a linear code is about $m/2s$, in contrast to the problem without security constraint that requires no more than two transmissions.

CHAPTER 1

INTRODUCTION

1.1 Pliable Index Coding

Information Theory is the fundamental mathematical theory for the problem of communication . The development of communication techniques started at the beginning of the civilizations. However, a rigorous study of information flow came only in the middle of the last century. The groundbreaking work of Claude Shannon [1] laid the foundation of a new field we call today *Information Theory*. In information theory, the amount of information is measured by the "information entropy", which, loosely speaking, is a function of the amount of randomness in the source to be compresal probability distribution. Shannon showed that the "capacity" of the channel, which solely depends on the channel's conditional probability distribution, is the maximum amount of information that can be transfered reliably. sed or communicated. Any "channel" through which the information is sent is modeled as a condition This result provides a guideline to design practical communication systems: for a given channel we know that there exists a family of codes with the maximum possible rate and the probability of unsuccessful decoding can be made as small as desired.

In [1] Shannon considered the channel where one transmitter communicates to one receiver through a noisy channel, which is the so called the point-to-point (p2p) channel model. Shannon showed that the capacity of the p2p channel is the largest mutual information between the input and output.

Based on the result established by Shannon and motivated by practical networks, more sophisticated channel models have been proposed and studied in the field of information theory, such as multiple access channel [2], broadcast channel [3], and interference channel [4]. In this thesis we are concerned with a type of broadcast channels. A broadcast channel is a channel with one input and many outputs, motivated by the downlink of the wireless channels. Different from wired communications, in wireless scenarios the signal is broadcasted over the air. The channel media is thus "shared" by all users in the system. The transmitter can leverage this broadcast nature of the broadcast channel for transmissions. Doing so is generally much better than serving each receiver one at a time, which makes the broadcast channel to be multiple parallel p2p channels by time sharing.

In practical systems, receivers usually have some local storages where results of past communications can be stored. This is modeled as the "broadcast channel with side information at the users". One example can be the satellite communication systems, where the transmitter is the satellite in orbit and the receivers are the receiving stations on earth. All stations within a certain area can receive the signals sent by the satellite. One station can also receive the signals intended for other stations sent by the satellite. By storing them as side information, the previous transmitted signals can be leveraged in future transmissions.

The "broadcast channel with side information at the users" model can also be applied to other wireless communication systems. The broadcast channel with side information at the users model is a critical model to fully understand the potential of wireless communications. However, the general broadcast channel remains open in terms of capacity, let alone the more sophisticated model of the broadcast

channel with side information at the users. Therefore, more reasonably constrained and simpler models become interesting for the study of the wireless communications.

1.1.1 From Index Coding to Pliable Index Coding

The Index Coding (IC) is one of such simpler models for the broadcast channel with side information at the users. First proposed in [5], when considering satellite communications, the IC consists of one transmitter with $\mathfrak{m}$ independent messages to be delivered to $\mathfrak{n}$ users through an error-free broadcast link shared by all users. Each user has some messages as the side information (i.e., a subset of the message set) set available and needs to reliably decode some messages that are not in its side information set; the desired messages for each user are pre-determined. In the IC, one asks what is the minimum number of transmissions (i.e., minimum code length) such that every user is able to decode its desired messages successfully [6]. Compared to the broadcast channel with side information at the users, the IC appears simpler because: 1) the broadcast channel is noiseless; 2) the side information set at each user is a proper subset of the whole message set. The IC focuses on the benefits of the transmitter encoding opportunities brought by the different side information sets at the users. However, despite its simple form, the general IC is still open.

When one restricts attention to only linear codes, the optimal code length is fully characterized by the so-called minrank problem. Unfortunately, the minrank problem is NP-complete [6]. In [7] it is proved that the IC, which is a special case of the general network coding problem, is in fact equivalent to the general network coding problem. Therefore, some properties of the general network coding problems also apply to the IC and vice versa, e.g., in [8] it is shown that linear schemes are not sufficient

for the IC in general; [9] shows that non-Shannon type of inequalities are necessary to characterize the capacity region for the general IC.

The IC problem models the scenario where the transmitter can encode based on the side information sets and the desired messages of all the users. In practical systems, the transmitter may have more freedoms in encoding. For example, in a music radio streaming service, e.g., Spotify, users do not request the next song that will be played. They are usually only guaranteed that it will be one from a certain group and not repeated. Another example could be online advertisement systems. The clients do not request a specific advertisement to be shown, it is the distributor who chooses what will be put on the clients' screens. However, the distributor might want to avoid repeating the same advertisement at the client's end, as it might decrease the client's satisfaction. Put these scenarios into the framework of the IC, we have a variant of the IC where the users can be satisfied by any messages that are not in their side information sets, instead of specific ones as in the original IC setting. The transmitter thus has the freedom to choose the desired messages of the users in order to minimize the transmission duration.

In this thesis, we study this variant of the IC where each user needs to decode $\mathtt{t}$ messages, known as the Pliable Index CODing (PICOD($\mathtt{t}$)), first proposed in [10]. The PICOD($\mathtt{t}$) and the IC share many attributes. In the PICOD($\mathtt{t}$), there is still a single transmitter with $\mathfrak{m}$ message and there are $\mathfrak{n}$ users with message side information sets. The transmitter and the users are connected with a shared noiseless capacity-bounded broadcast channel. The goal is to find the minimal number of transmissions by the transmitter such that all users can decode their desired messages reliably. The only difference is the definition of the "desired messages". For the IC each user has some pre-determined desired messages outside its side information set. For the PICOD($\mathtt{t}$) the desired messages of the users are not

pre-determined. The desired messages for the users can be chosen based on their side information sets. Specifically, each user can decode *any* $\mathtt{t}$ messages that are not in its side information set. By knowing the side information at each user, the transmitter can now encode based on the optimal choice of the desired messages of the users.

The rigorous definition of the PICOD$(\mathtt{t})$ can be found in Chapter 2 and 3. The past work on PICOD$(\mathtt{t})$ is in Section 1.2.1. Our contributions on PICOD$(\mathtt{t})$ in this thesis are shown in Section 1.4.1.1 and 1.4.2.1.

1.1.2 Decentralized Pliable Index Coding

In the decentralized model of network communications, a central transmitter with knowledge of all messages is not present. Instead, in order to decode their desired messages, the users share among themselves coded massages that depend only on their local side information sets. This decentralized model is motivated by ad-hoc communication systems such as ad-hoc networks, peer-to-peer networks, Internet of Things systems, as well as distributed systems such as distributed computation structures and distributed storage systems. In these systems, there is no central controller/transmitter and the communications are done in a decentralized way – the users generate codewords based on their own limited knowledge of the message sets and communicate among themselves.

In the IC framework, the decentralized IC problem is the setting where the users generate the codewords based on their own side information sets and broadcast the codewords to all the rest of the users using a shared channel. The channel is noiseless, capacity limited, and can only be used by one user at a single time.

In this thesis we propose the *d-PICOD*, which is a decentralized IC with pliable desired messages at the users. Specifically, the d-PICOD is a decentralized IC where each user can choose their desired message sets based on the side information sets of all other users. All users need to reliably decode the desired messages by exchanging the fewest possible number of coded symbols among the users. The d-PICOD inherits the freedom of choosing the desired message sets from the PICOD, and the decentralized network structure from the decentralized IC. Thus, the d-PICOD is a model for those practical scenarios where the choice of the desired messages is flexible and the network structure is without central control, such as coded the cooperative data exchange [11] and the distributed storage [12].

The rigorous definition of d-PICOD can be found in Chapter 4. The past work on the decentralized IC is in Section 1.3. Our contribution on the d-PICOD is summarized in Section 1.4.1.2 and 1.4.2.2.

1.1.3 Secure Pliable Index Coding

Security and privacy are of concern to today's communication systems. Besides receiving the messages with highest possible rate and lowest possible error probability, the users also care about the security and privacy of their desired information. The transmitted information should not be accessible without permission by any untrusted 3rd parties. In the broadcast channel, the information aimed for one user can be overheard by another user since all users shared the same channel. The situation is no different in PICOD as the channel is noiseless. For instance, in an Internet streaming service like Spotify, users should get the content they have paid for. However, in PICOD model, the user might be able to get some songs that are transmitted to another user in the same network without paying for them. This brings the security problems in the PICOD. We address this problem by introducing the information theoretical security into the PICOD problem formulation.

The conventional information theoretical security constraint is the so-called strong security constraint [13]. That is, zero information leakage of all the messages that are not supposed to be decoded. This is possible only if certain common randomness is available in the systems. The common randomness works as a one-time-pad to guarantee information theoretical security. In this thesis, we use a weaker version of information theoretical security, i.e., individual message security. The individual message security allows for some leakage of information about the message set, but keeps each individual message secure. In other words, a user may be able to estimate some statistics of the set of the messages that are not allowed to be decoded. However, it can not recover any piece of any individual message that it is not suppose to decode. The individual security constraint is thus weaker but more practical, since it does not require common randomness, which might not be available in practical systems.

1.2 Past Work

1.2.1 Pliable Index Coding

As one would expect, the extra freedom of choosing the desired messages in the PICOD(t) reduces the number of transmissions / code length compared to the classical IC with the same parameters: the number of message, the number of users, and message side information sets.

When we restrict the coding scheme to be linear, [10, Lemma 2] showed finding the optimal code is equivalent to solving a minrank problem similar to the IC, therefore is still NP-complete. The optimal linear code for PICOD(1) offers an exponential reduction in the number of transmissions compared to the IC problem of the same size/number of clients. In particular, [10, discussion after Theorem 4] proved that $O(\log^2(n))$ transmissions suffice for the PICOD. In [14] a deterministic polynomial time algorithm was proposed that requires at most $O(\log^2(n))$ transmissions. A key result in this line of

work is [10, Lemma 3]: for a PICOD problem with n clients, such that each client misses at least d_{min} messages and at most d_{max} messages in its side information set, a single transmission satisfies at least a fraction $d_{min}/(ed_{max})$ of the clients. This result implies that if the cardinalities of the side information sets of the clients are all equal, a linear code of size $O(\log(n))$ is sufficient to satisfy all the clients. If the cardinalities of the side information sets are different, by grouping of the clients and applying [10, Lemma 3] to each group, a linear code of size $O(\log^2(n))$ is sufficient to satisfy all the clients if the number of messages m is polynomially related to the number of clients n [10, Theorem 4].

For PICOD(t), when all users' side information sets are of size $s \leq m - t$, [10] showed that there exits a code of length $O(\min\{t\log(n), t + \log^2(n)\})$ for the PICOD(t). When there is no constraint on the size of side information, and $m = O(n^\delta)$ for some constant positive δ, code length $O(\min\{t\log^2(n), t\log(n) + \log^3(n)\})$ is achievable. Compare it to the IC where there is one desired message pre-determined for each user and desired message and the side information sets are randomly generated for all users, the outer bound is $\Omega(\sqrt{n})$ [15]. Therefore, the proposed achievability showed a dramatic reduction in terms of the code length for the PICOD(t) when compared to the IC .

The code length of a heuristic achievable scheme for the PICOD(t) based on greedy covering proposed in [10] is shown close to $O(\min\{t\log(n), t + \log^2(n)\})$ in numerical analysis. Recently in [16], a deterministic algorithm, which runs in polynomial time, was proposed to achieve the $O(\log^2(n))$ for $t = 1$ and $O(t\log(n) + \log^2(n))$ in general.

Another interesting model proposed in [10] is the oblivious PICOD(t). In the oblivious PICOD(t), the transmitter does not know the side information sets at the users. The transmitter only knows the size of the side information sets of each user. In [10, 17] the authors proved that, for the oblivious PICOD(t)

at least a fraction $1/e$ of the remained unsatisfied users can be satisfied at each new transmission. This shows that there exists an achievable scheme where the code length is the logarithm of the number of users in the system, which is an exponential improvement in the number of transmissions compared to the IC.

1.3 Decentralized Pliable Index Coding

The decentralized IC can be seen as a special case of the *distributed IC*, which is a generalization on the IC to the case of multiple intermediate relays, or servers, with the message side information sets at the users. In the distributed IC with m messages, there are $2^m - 1$ servers; each server has knowledge of a unique subset of the message set (and can thus only encode based on the messages in this message set) and is connected to all the users through a separated error-free rate-limited link. The objective in the decentralized IC is to determine the shortest code length such that all users are able to decoded their desired messages. The decentralized IC is thus a distributed IC where there are as many servers as users, and each server has the same message knowledge as one of the users.

In [18] the *single uniprior* decentralized IC case was studied, where there are multiple senders and each user has only one message in its side information. In [19] a general converse bound for the distributed IC was derived by leveraging the submodularity of entropy, and a general achievable scheme was proposed based on the IC composite coding scheme. For all distributed IC with no more than four messages, the inner and outer bounds were numerically verified to match for the special case of symmetric message rates and of symmetric server-link capacities [19]. However, applying the methods in [19] to the settings with more than four messages becomes intractable since the number of variables involved is the numerical evaluations is exponential in the number of servers (thus is double exponential

in the number of messages). Recently, in [20] it was shown that knowing the length of linear code for the classical (centralized) IC allows one to construct a linear code for the corresponding embedded (decentralized) IC with at most a doubled codeword length. Therefore, for the decentralized IC, the codeword length is within a multiplicative gap 2 to the optimal codeword length of the centralized IC.

1.3.1 Security in Index Coding

The problem of security and privacy in IC has been studied from different perspectives. In [21], the authors proposed an IC model where an eavesdropper has a limited access to the side information sets of the users and the transmitted codewords; the goal here is to prevent the eavesdropper from obtaining any new information. In [22], the authors considered an IC model where the sender must design a code that allows each user to decode its desired message, at the same time prevent each user from obtaining any information of the side information and the desired messages of all other users. The latter model has the flavor of the private information retrieval problem [23], where a user wants to hide its desired message and/or side information set from the other users and/or the server. Similar to the private information retrieval problem, the authors of [24] formulated the *private IC* problem, where a user in the IC problem can only decode its own desired messages but no others. Recently, in [25], the authors extended the private IC problem in [24] to the PICOD framework, where the side information structure is "circular" and each user can decode one and only one message. Several schemes were given in [25] and shown to provide the desired level of privacy, but the optimality is discussed under the linear encoding constraint for some cases.

1.4 Contributions

We list our contributions in both achievability and converse for the three models discussed above.

1.4.1 Achievability

1.4.1.1 Pliable Index Coding

For the achievability perspective, our contribution is a refined analysis of the fraction of clients that can be satisfied by a single transmission in the PICOD(1). We provide a non-probabilistic argument to show a lower bound on the largest fraction of clients that can be satisfied by one transmission as a function of the cardinality of the message set and the side information set, for the case where the cardinalities of the side information sets of the users are all equal. The worst case of our lower bound is still $1/e$ as in [10, Lemma 3, with $\mathrm{d}_{\min} = \mathrm{d}_{\max}$]. However, with our analysis we are able to determine the worst case given the cardinality of the message set and of the side information set. Moreover, we can also show how many messages should be involved in the (network coded) transmission that satisfies the largest fraction of clients in this case. In general, our lower bound is strictly better than $1/e$. The improvement is quite pronounced in the case where the cardinality of the side information set is relatively small comparable to the number of messages. This points to the phenomenon that the largest fraction of clients can be satisfied with one transmission when the cardinality of the side information set is close to zero or close to the number of messages in the system. Our result can be applied to the case where a messages is in the side information of a client with a fixed probability independent of every other message and client, and refines the result in [10, Theorem 8, with $\mathrm{t} = 1$].

1.4.1.2 Decentralized Pliable Index Coding

Our achievability scheme users both scalar and vector linear index coding. Our results show that the optimal code-length for the d-PICOD is the same as the one for the classical (centralized) PICOD counterpart, except when the problem is no longer pliable. That is, when the d-PICOD reduces to an IC

problem where every user needs to decode all the messages not in its side information set (a problem also known as the data exchange problem.) For those cases where the optimal code-length may be the same in both centralized and decentralized settings, the actual optimal codes are not necessarily the same. For the d-PICOD, our results show that the sparse Maximum Distance Separable (MDS) codes and vector linear index codes are required for optimal performance, while the scale linear code is sufficient for the centralized PICOD. Our achievable scheme is based on the recent result on MDS-condition [26]. Our result also provides the required finite filed size for the codewords. The size is known to be the smallest for this problem. The proposed scheme matches the converse bounds for the centralized PICOD for the cases where there are still pliabilities of choosing the desired messages at the users. Therefore, the proposed scheme is optimal for these cases.

1.4.1.3 Secure Pliable Index Coding

We extend the achievability scheme proposed in [25] to a more general setting of the problem. Specifically, we consider the case with a circular shift side information sets of the users and the side information sets of the users are of the same size. However, the shift is not necessarily 1, which is the setting considered in [25]. For our generalized model, we proposed new achievable scheme based on the idea of "grouping" users. Each transmission is able to satisfy two groups of the users while keeping the message secure to all the other users. When $s > m/2$, our scheme is the same as the scheme proposed in [25]. When $s < m/2$, our scheme groups the users and satisfies at most two groups with one transmission and can do strictly better than the scheme proposed in [25]. The individual security is maintained by the regular structure of the circular shift side information structure.

1.4.2 Converse

Known achievable schemes for the PICOD(t) are based on linear code only. Few converse results are available for the PICOD(t). All existing converse proofs are under the "linear constraint", which restrict the codes to be linear. In other words, an information theoretical converse does not exist. For the oblivious PICOD(t), the optimal code length under the linear encoding restriction is shown [10, Theorem 9]. In [16], the authors provide a worst case instance, which needs $\Omega(\log(n))$ code length for the linear code. Our main goal is to prove information theoretic converse results for the PICOD(t) that matches the achievability.

1.4.2.1 Pliable Index Coding

From the converse perspective, we derive information theoretic converse bounds for some the PICOD(t)s based on their side information structure, namely (i) the Complete-S PICOD(t), and (ii) the PICOD(t) whose network topology hypergraph is a circular-arc.

The complete–S PICOD(t), where S is a subset of $[0 : m - t]$ (where m is the number of message at the transmitter), is a system where all side information sets/users with size indexed by S are present. We say that S is "consecutive" if $S = [s_{\min} : s_{\max}]$ for some $0 \leq s_{\min} \leq s_{\max} \leq m - t$. The complete–S PICOD$(t)$ with consecutive S is also known as the oblivious PICOD(t) in [10, Section VI]. In [10] the authors proposed optimal converse bounds for the oblivious PICOD(t) when the encoding scheme is restricted to be linear. We provide tight information theoretic converse bounds, i.e., without any restriction on the encoding scheme been used, on some classes of the PICOD(t). Our setting of the complete–S PICOD(t) includes and expands the oblivious PICOD(t) setting in [10] and show the unrestricted optimality of linear codes.

Our converse is based on showing the existence of at least one "special user" who can decode a certain number of messages outside its side information set; the stumbling block in previous approaches was how to find such a "special user." The problem of finding the "special user" can be approached in two ways: 1) *constructively finding* such a "special user" for each choices of the desired messages, or 2) implicitly proving its existence. We show the existence of this "special user" regardless of the choice of desired messages using both methods. For the "complement-consecutive complete–S PICOD(t)", which is the complete–$[0 : m - t] \setminus [s_{\min} : s_{\max}]$ PICOD(t) where $0 \leq s_{\min} \leq s_{\max} \leq m - t$, we constructively find the "special user" that can decode $|S| + t - 1$ messages. The constructively way is not amenable for the "consecutive complete–S PICOD(t)", which is the complete–$[s_{\min} : s_{\max}]$ the PICOD(t) where $0 \leq s_{\min} \leq s_{\max} \leq m - t$. This is because the constructive proof has a high complexity due to the number of sub-cases /different message assignments that must be considered separately. Therefore, we propose a novel combinatorial proof to show the existence of the "special user" regardless of the choices of the desired messages. By not simply focusing on the desired messages, but on all the messages that a user will eventually be able to decode, we consider the messages that a user can eventually know as a "block cover" for this user. The "block cover" for a user must includes the side information sets and the desired message of this user. This is similar to the combinatorial design structure, e.g. Steiner system. We then argue that the absence of the special user leads to a contradiction in this "block cover". Therefore we show the existence of the special user. This new technique greatly reduces the complexity of the proof compared to the constructive method and enables us to obtain a converse bound for a very general class of the complete–S PICOD(t). The keystone of the proof is to show that, for the "critical case" of $S = \{s\}$ and $m = 2s + t$, there exists at least one user who can

decode $s+t$ messages. From this, the extension to the "consecutive complete–S" PICOD(t) follows by enhancing the system to a "critical case" one.

The converse idea based on showing the existence of the"special user" can also be used for the other PICOD(t) cases. For the case $t = 1$ we show a tight converse for those PICOD(1) whose network topology hypergraph is circular-arc (for a detailed definition of network topology hypergraph please refers to Section 3.7.1). For this setting, when a 1-factor does not exist (for a detailed definition please refers to Section 3.7.1) we show that the code length is at least 2 by finding a user that can decode 2 messages. The converse is tight by showing an achievable scheme that satisfies all users with just 2 transmissions.

1.4.2.2 Decentralized Pliable Index Coding

Converse bounds of the centralized PICOD is also valid for d-PICOD as well. Therefore, we use the converse bounds of the corresponding centralized PICOD for d-PICOD. For the cases where we still have pliabilities of choosing the desired messages at the users, we propose achievable schemes that can achieve the converse bounds of the centralized PICOD. Therefore, we show the tightness of the bounds for such cases. The only exceptional case is where pliabilities of choosing the desired message no longer exist, i.e., the d-PICOD problem becomes a data exchange problem where all users need to decode all message they do not have in their side information sets. For this case, we prove that the centralized converse bound is strictly suboptimal. We provide a new converse bound based on the cut-set bound. The new converse bound matches the proposed achievable scheme based on the sparse MDS code and thus is tight.

1.4.2.3 Secure Pliable Index Coding

For the cases where $s \geq m/2$ or the shift is greater than 1, where m is the number of messages and s is the size of the side information, our proposed achievable scheme takes no more than 2 transmissions. We use the converse bound for the PICOD problem with the circular-arc side information structure and show that our proposed scheme is information theoretical optimal for these cases. For the other cases, specifically, the case where $s < m/2$ and the shift is 1, we propose a converse bound under the linear encoding constraint, that is, the encoding function is a linear function of the messages. The linear encoding constrained IC has been well studied and we know the optimality is the minrank problem, which is NP-hard. Our proposed linear encoding constraint converse differs from our proposed achievable scheme by at most one transmission. Therefore, we show that our scheme is almost linearly for this case. Our results shows that when $s < m/2$ and under the linear encoding constraint, the converse bound changes dramatically when applying the security constraint. The optimal number of transmissions is always 1 or 2 when there is no security constraint. However, when security constraint is imposed, the converse bound is about $m/2s$ when $s < m/2$. The bound is thus linear with m/s, in contrast to the constant bound for the problem without the security constraint.

1.4.3 Corresponding Publications

We list our corresponding publications in the following.

- Conference papers

1. Liu, T. and Tuninetti, D.: “Pliable index coding: Novel lower bound on the fraction of satisfied clients with a single transmission and its application.” Information Theory Workshop, ©IEEE 2016.
2. Liu, T. and Tuninetti, D.: “Information theoretic converse proofs for some PICOD problems.” Information Theory Workshop, ©IEEE 2017.
3. Liu, T. and Tuninetti, D.: “An information theoretic converse for the ‘consecutive complete–S’ PICOD problem.” Information Theory Workshop, ©IEEE 2018.
4. Liu, T. and Tuninetti, D.: “Decentralized pliable index coding.” Information Theory Proceedings (ISIT), International Symposium on, ©IEEE 2019.
5. Liu, T. and Tuninetti, D.: “Private pliable index coding.” Information Theory Workshop, ©IEEE 2019.

- Journal papers

1. Liu, T. and Tuninetti, D.: “Tight Information Theoretic Converse Results for Some Pliable Index Coding Problems.” Trans. on Information Theory, ©IEEE 2019.
2. Liu, T. and Tuninetti, D.: “Decentralized Pliable Index Coding.” submitted to Trans. on Information Theory, ©IEEE.
3. Liu, T. and Tuninetti, D.: “Individually Secure Pliable Index Coding.” working in progress.

CHAPTER 2

CONSTANT FRACTION OF SATISFIED USERS IN PLIABLE INDEX CODING PROBLEM

In this chapter we show that for any PICOD(1) (to be defined in Section 2.1), there exists an achievability scheme that can satisfy at least a constant fraction of users that are not satisfied yet. This result shows the upper bound on the optimal code length for PICOD(1) is $\log(n)$, where n is the number of users in the system.

The result of this chapter has been published in [17].

2.1 System Model

In a PICOD(t) system there is one server and $n \in \mathbb{N}$ users; the user set is denoted as $\mathcal{U} := \{u_1, u_2, \ldots, u_n\}$. The server is connected to all users by a rate-limited noiseless broadcast channel. There are $m \in \mathbb{N}$ independent and uniformly distributed binary messages of $\kappa \in \mathbb{N}$ bits; the message set is denoted as $\mathcal{W} := \{w_1, w_2, \ldots, w_m\}$. The transmitter has all m messages known, while user u_i has a subset of the message set as its side information set $\mathcal{A}_i \subset [m]$, $i \in [n]$. The collection of all the side information sets $\mathcal{A} := \{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n\}$ is assumed globally known at the server and all users.

The code the server broadcasts to the users has length $\ell\kappa$ bits, and is a function of the message set $\mathcal{W}$ and the collection of all side information sets $\mathcal{A}$, i.e., for some function ENC we have

$$x^{\ell\kappa} = \mathsf{ENC}(\mathcal{W}, \mathcal{A}). \tag{2.1}$$

Each user decodes based on the code $x^{\ell\kappa}$ and its own side information set; for user $u_j, j \in [n]$, the decoding function is

$$\{\widehat{w}_1^{(j)}, \ldots, \widehat{w}_t^{(j)}\} = \mathsf{DEC}_j(W_{A_j}, x^{\ell\kappa}). \tag{2.2}$$

A code is said to be *valid* if and only if every user can successfully decode at least t messages not in its side information set, i.e., the decoding functions DEC_j, for all $j \in [n]$, is such that

$$\Pr[\exists\{d_{j1}, \ldots, d_{jt}\} \cap A_j = \emptyset : \{\widehat{w}_1^{(j)}, \ldots, \widehat{w}_t^{(j)}\} \neq \{w_{d_{j1}}, \ldots, w_{d_{jt}}\}] \leq \epsilon, \tag{2.3}$$

for some $\epsilon \in (0, 1)$. For a valid code, $\{\widehat{w}_1^{(j)}, \ldots, \widehat{w}_t^{(j)}\} = \{w_{d_{j1}}, \ldots, w_{d_{jt}}\}$ is called the *desired messages set* for user u_j, $j \in [n]$, and the indices of the desired message are denoted as $D_j := \{d_{j1}, \ldots, d_{jt}\}$. For a valid code, the choice of desired messages for the users is $\mathcal{D} = \{D_1, D_2, \ldots D_n\}$ where $D_j \cap A_j = \emptyset, \forall j \in [n]$. The goal is to find a valid code with minimum length

$$\ell^* := \min\{\ell : \exists \text{ a valid code of length } \ell\kappa, \text{ for some } \kappa\}. \tag{2.4}$$

In the following we shall usually focus on the *complete–S PICOD*(t), for a given set $S \subseteq [0 : m-t]$. In this system, there are $n := \sum_{s\in S} \binom{m}{s}$ users, where no two users have the same side information set. In other words, all possible users with distinct side information that are subsets of size s of the m messages, for all $s \in S$, are present in the complete–S PICOD(t).

2.2 Greedy Set Cover Achievability

2.2.1 Problem Representation

In this paper we restrict the encoding and decoding functions to be linear on the binary field, which is motivated by practical reasons but may be suboptimal in general [14]. A client is said to be *satisfied* by a single transmission if there is only one message in the broadcasted binary linear combination that is *not* in its side information. In this paper we are interested in the number of clients satisfied by a single transmission. Therefore it is enough for us to only consider *binary linear encoding* where every transmission is a linear combination of a subset of the messages with coefficient either 0 or 1. There are $2^m - 1$ such binary linear combinations of m messages. We can represent this satisfaction relationship between clients and all possible binary linear combinations of messages as a bipartite graph. Let $\mathcal{Z} := \{z_j,\ j \in [1 : 2^m - 1]\}$ denote the set of all binary linear combinations of m messages (with the exception of the one with all zero coefficients). The set $\mathcal{Z}$ represents the 'left side/code' nodes. The set of 'right side/client' node is the set $\mathcal{A}$ of the n clients. An edge exists between $a_i \in \mathcal{A}$ and $z_j \in \mathcal{Z}$ if client a_i can decode one message in $\mathcal{R}_i$ from z_j, in which case we say the 'client a_i is *covered* by z_j'. For example, for the PICOD($m = 3, n = 4, \mathcal{R}_1 = \{b_1, b_2, b_3\}, \mathcal{R}_2 = \{b_2, b_3\}, \mathcal{R}_3 = \{b_3\}, \mathcal{R}_4 = \{b_1\}$) such a bipartite graph is shown in in Fig. Figure 1.

It is easy to see that for $\mathcal{Z}' \subseteq \mathcal{Z}$ such that its neighbor $N(\mathcal{Z}') = \mathcal{A}$, all clients are satisfied by $|\mathcal{Z}'|$ transmissions. Thus $\min\{|\mathcal{Z}'| : N(\mathcal{Z}') = \mathcal{A}\}$ is an upper bound to the optimal PICOD solution. For the example in Fig. Figure 1, we have $\min |\mathcal{Z}'| = 2$ attained by $\mathcal{Z}' = \{\{b_1\}, \{b_3\}\}$.

The problem of minimizing $|\mathcal{Z}'|$ is the well-known *set cover problem* [27]. The set cover problem is NP-hard and the best polynomial time algorithm is the greedy covering algorithm [28, 29], which

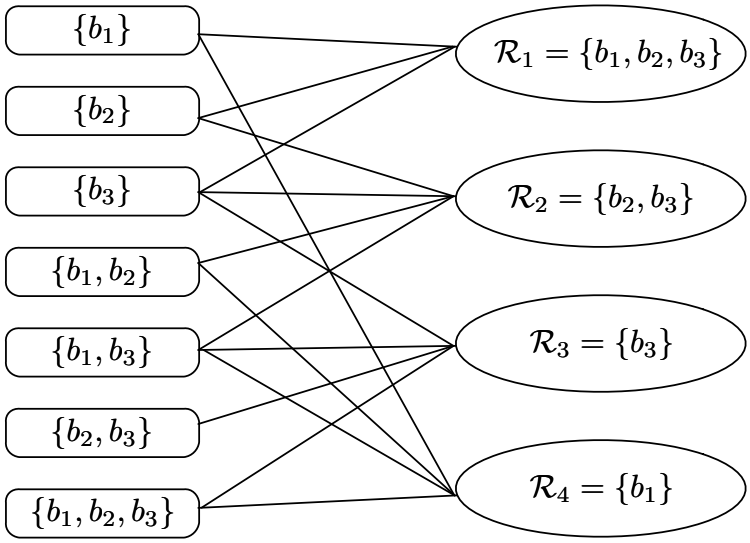

Figure 1. Bipartite graph representing the satisfaction relationship between possible transmitted codewords (left side nodes) and clients (right side nodes). ©IEEE 2016.

approximate the optimal solution to within a factor $\mathrm{H}(\mathrm{n})$, where $\mathrm{H}(\mathrm{n})$ is the n-th harmonic number. $\mathrm{H}(\mathrm{n})$ is known to be the best possible approximation factor for polynomial time algorithms.

The greedy covering algorithm works as follows: in every step, find the 'left side/code' vertex that covers the largest number of 'right side/client' vertices; remove those 'right side/client' vertices that have been covered by the found 'left side/code' vertex, and repeat until all 'right side/client' vertices have been removed.

2.2.2 Performance Analysis

We now analyze the performance of greedy covering approach. We start by considering the case where the side information sets of all clients have the same cardinality and show that the greedy covering approach can satisfy a constant fraction of clients for every transmission.

Theorem 1. *For a PICOD instance with* m *messages and where the request set of all* n *clients has cardinality* l*, the fraction of unsatisfied clients that can be satisfied by one transmission is lower bounded by* $\max\left\{\left(1-\frac{l}{m}\right)^{\frac{m}{l}-1}\left(1-\frac{1}{l}\right)^{l-1}e, \frac{l}{m}\right\}$*, which is at least* $1/e$*.*

To prove the theorem, we introduce a grouping of the clients based on the cardinality of their request set (see step *a)* next). We then provide a lower bound on the fraction of satisfied clients by one transmission for the case where the request sets have the same cardinality; this lower bound is valid for any m, n, l (see step *b)* next). Finally we show that this fraction is no less than $1/e$, as in [10, Lemma 3, with $d_{\min} = d_{\max}$] (see step *c)* next).

Client grouping

We divide the n clients into m groups, where m is the number of messages, based on the cardinality of their request set. Group $\mathcal{S}_l = \{a_i \in \mathcal{A} : |\mathcal{R}_i| = l\}, l \in [1 : m]$. We denote the cardinality of group $\mathcal{S}_l$ as $C_l := |\mathcal{S}_l|$. Note that the sets $\mathcal{S}_l$ are disjoint and $\sum_{l=1}^{m} C_l = n$. For the example in Fig. Figure 1, we have $\mathcal{S}_1 = \{a_3, a_4\}, \mathcal{S}_2 = \{a_2\}, \mathcal{S}_3 = \{a_1\}$.

Number of satisfied clients by one transmission

Every transmission in our model is a binary linear combination of a number of messages, say $k \in [1 : m]$. A client is satisfied by such a transmission if it has $k-1$ messages involved in the linear

combination as its side information. There are $2^m - 1$ such binary linear combinations. Explicitly, there are $\binom{m}{k}$ different choices of transmission for a binary linear combination with k messages. Let $D_{kj}, k \in [1 : m], j \in [1 : \binom{m}{k}]$ denote the number of clients that can be satisfied by jth choices of messages when the linear combination contains k messages. Based on the number of messages in a binary linear combination we have the following:

- $k = 1$ (we send a single message within the message set). A client in $\mathcal{S}_1$ is satisfied by the transmission of the only message that is not in its side information; there is one choice of messages for such transmission. Thus will be counted once for all possible transmissions.

  A client in $\mathcal{S}_2$ is satisfied by the transmission of either of the two messages not in its side information; there are two choices of messages for such transmission. Thus will be

  In general, there are l choices of messages for transmission to satisfy a client in $\mathcal{S}_l, l \in [1 : m]$.

  We count the number of clients that are satisfied by the all possible $\binom{m}{1}$ choices of messages. The total number of satisfied clients is

$$\sum_{j=1}^{\binom{m}{1}} D_{1j} = C_1 + 2C_2 + \cdots + mC_m.$$

  Thus the maximum number of clients that can be satisfied by one transmission containing a single message is lower bounded as

$$\max_j D_{1j} \geq \frac{C_1 + 2C_2 + \cdots + mC_m}{\binom{m}{1}} = \sum_{i=1}^{m} \frac{i}{m} C_i.$$

- $k = 2$ (we send a linear combination of two messages within the message set).

  A client in $\mathcal{S}_1$ can be satisfied if only one of the two messages involved in the linear combination is not in its side information. There are $\binom{m-1}{1}$ possible choices in this case.

  A client in $\mathcal{S}_2$ can be satisfied if only one of the two messages involved in the linear combination is not in its side information, and the other one is. There are $2\binom{m-2}{1}$ choices of two messages that satisfy such condition.

  In general, the number of choices that can satisfy a client in $\mathcal{S}_l$ is $l\binom{m-l}{1}, l \in [1 : m]$.

  In this case we have

$$\sum_{j=1}^{\binom{m}{2}} D_{2j} = \binom{m-1}{1} C_1 + \cdots + (m-1)\binom{1}{1} C_{m-1},$$

  and the maximum number of satisfied clients per transmission is

$$\max_j D_{2j} \geq \frac{\binom{m-1}{2} C_1 + 2\binom{m-2}{2} C_2 + \cdots + (m-1) C_{m-1}}{\binom{m}{2}}.$$

- General k (we send a linear combination of k messages within the message set, with $k \in [1 : m]$).

  The total number clients that can be satisfied these choices is

$$\sum_{j=1}^{\binom{m}{k}} D_{kj} = \sum_{l=1}^{m-1} l\binom{m-l}{k-1} C_l,$$

and the maximum number of satisfied clients by a single transmission is

$$\max_{j} D_{kj} \geq \sum_{l=1}^{m} R_{l,m,k}\, C_l,$$

where

$$R_{l,m,k} := \frac{l\binom{m-l}{k-1}}{\binom{m}{k}} \tag{2.5}$$

and the binomial coefficient is taken to be zero in (Equation 2.5) if $m - l < k - 1$.

Lower bound of maximum covering

We now consider the case where the cardinality of the request size of the clients in the same, say l for some $l \in [1 : m]$. This implies that in the analysis done in the previous paragraph we set $C_i = 0, \forall i \neq l$. The goal is to show a lower bound for every pair of (l, m)

$$\max_{k\in[1:m]} R_{l,m,k} \geq r_{l,m}, \tag{2.6}$$

for some positive $r_{l,m}$ (which can be a function of the size of request set l and the number of messages m), and where $R_{l,m,k}$ was defined in (Equation 2.5).

For $k = 1$ (we send a single message), $R_{l,m,k=1} = \frac{l}{m}$ and therefore we can always satisfy a fraction $\frac{l}{m}$ of the clients; for $k = 2$ (we send a linear combination of two messages), $R_{l,m,k=2} = 2\frac{l}{m}\left(1 - \frac{l}{m}\right)\frac{m}{m-1}$ and therefore we can always satisfy this fraction of the clients; but sending a single

$$\max_{k\in[1:m]} R_{l,m,k} = \max_{k\in[1:m]} \frac{l\binom{m-l}{k-1}}{\binom{m}{k}} = \max_{k\in[1:m]} \frac{l\,(m-l)\,!k!\,(m-k)\,!}{(k-1)\,!\,(m-l-k+1)\,!m!} = \max_{k\in[1:m]} lk\frac{(m-l)\,!\,(m-k)\,!}{m!\,(m-l-k+1)\,!} \tag{2.7}$$

$$> \max_{k\in[1:m]} lk\frac{\sqrt{2\pi\,(m-l)}\left(\frac{m-l}{e}\right)^{m-l} e^{\frac{1}{12(m-l)+1}}}{\sqrt{2\pi m}\left(\frac{m}{e}\right)^{m} e^{\frac{1}{12m}}} \frac{\sqrt{2\pi\,(m-k)}\left(\frac{m-k}{e}\right)^{m-k} e^{\frac{1}{12(m-k)+1}}}{\sqrt{2\pi\,(m-l-k+1)}\left(\frac{m-l-k+1}{e}\right)^{m-l-k+1} e^{\frac{1}{12(m-l-k+1)}}} \tag{2.8}$$

$$= \max_{k\in[1:m]} \frac{l}{m}\left(1-\frac{l}{m}\right)^{m-l+\frac{1}{2}} \left(\frac{m-k}{m-l-k+1}\right)^{m-l-k+\frac{3}{2}} \frac{k(m-k)^{l-1}}{m^{l}}\, e^{\beta} \tag{2.9}$$

$$\geq \left(\frac{m-l-k+\frac{kl}{m}}{m-l-k+1}\right)^{m-l-k+\frac{3}{2}} \frac{lk}{m}\left(1-\frac{l}{m}\right)^{k-1}\left(1-\frac{k}{m}\right)^{l-1} e^{\beta} \quad | \quad k=\lfloor\frac{m}{l}\rfloor = \frac{m}{l}-\alpha \tag{2.10}$$

$$> \left(\frac{m-l-\frac{m}{l}+\alpha+1-\alpha\frac{l}{m}}{m-l-\frac{m}{l}+\alpha+1}\right)^{m-l-\frac{m}{l}+\alpha+\frac{3}{2}} \frac{1-\alpha\frac{l}{m}}{\left(1-\frac{l}{m}\right)^{\alpha}}\left(1-\frac{l}{m}\right)^{\frac{m}{l}-1}\left(1-\frac{1}{l}\right)^{l-1} e^{\beta} \tag{2.11}$$

$$= \frac{1-\alpha\frac{l}{m}}{\left(1-\frac{l}{m}\right)^{\alpha}}\left(1-\frac{l}{m}\right)^{\frac{m}{l}-1}\left(1-\frac{1}{l}\right)^{l-1} e > \left(1-\frac{l}{m}\right)^{\frac{m}{l}-1}\left(1-\frac{1}{l}\right)^{l-1} e \tag{2.12}$$

message or a a linear combination of two message may not be the best strategy, so next we investigate the case of general $k \in [1:m]$ by understanding the behavior of $R_{l,m,k}$.

The bounding steps are reported at the top of the next page; next we give a justification for the various (in)equalities:

- step (Equation 2.7) is by definition of the binomial coefficient;
- step (Equation 2.8) follows by the Stirling's approximation formula [30]

$$\sqrt{2\pi n}\left(\frac{n}{e}\right)^{n} e^{\frac{1}{12n+1}} < n! < \sqrt{2\pi n}\left(\frac{n}{e}\right)^{n} e^{\frac{1}{12n}};$$

- step (Equation 2.9) is simple algebra and where we defined

$$\beta := 1 + \frac{1}{12(m-l)+1} + \frac{1}{12(m-k)+1} - \frac{1}{12m} - \frac{1}{12\,(m-l-k+1)};$$

- in step (Equation 2.10) we choose $k = \lfloor m/l \rfloor$ since the function $k(m-k)^{l-1}$ is maximized by $x = m/l$ and the number of messages in a linear combination needs to be an integer, and where we indicate the flooring $\lfloor m/l \rfloor = m/l - \alpha$ for some $0 \leq \alpha < 1$;

- step (Equation 2.11) by replacing k with $\frac{m}{l} - \alpha$; and

- step (Equation 2.12) follows since

$$\left(\frac{m-l-\lfloor \frac{m}{l} \rfloor + \frac{\lfloor \frac{m}{l} \rfloor l}{m}}{m-l-\lfloor \frac{m}{l} \rfloor + 1} \right)^{m-l-\lfloor \frac{m}{l} \rfloor + \frac{3}{2}} = 1 - o(1/m),$$

$$e^{\beta} = e - o(1 - e^{-1/m^2}),$$

for sufficiently large m, and $\frac{1-\alpha\frac{l}{m}}{(1-\frac{l}{m})^{\alpha}} \geq 1$ for $0 \leq \alpha < 1$.

Since by choosing $k = 1$ we can satisfy a fraction $R_{l,m,k=1} = \frac{l}{m}$ of the clients, together with the bound derived at the top of the page, we arrived at

$$\begin{aligned}\max_k R_{l,m,k} &\geq \max\left\{\left(1-\frac{l}{m}\right)^{\frac{m}{l}-1}\left(1-\frac{1}{l}\right)^{l-1}e, \frac{l}{m}\right\} \\ &\geq \left(1-\frac{1}{\sqrt{m}}\right)^{2\sqrt{m}-2}e \qquad (2.13) \\ &> 1/e. \qquad (2.14)\end{aligned}$$

where the inequality in (Equation 2.13) follows since the function $\left(1-\frac{l}{m}\right)^{\frac{m}{l}-1}\left(1-\frac{1}{l}\right)^{l-1}$ is minimized by $l = \sqrt{m}$, and since the function in (Equation 2.14) is monotonically decreasing and converging to $1/e^2$. This shows that at least a fraction $1/e$ of the unsatisfied clients can be satisfied by one transmission. This concludes the proof.

To illustrate our bounds, in Fig. Figure 2 we plot our bound and the bound in [10, Lemma 3] for $m = 100, 400, 900$ as a function of l, the size of request set. Compared to the known bound, our bound better characterizes the fraction of satisfied clients by a single transmission when m is finite. Our lower bound is minimized when $l = \sqrt{m}$. When $1 \leq l \leq \sqrt{m}$, our result shows that having more messages in the side information set results in a larger fraction of satisfied clients with a single transmission. However, in the range $\sqrt{m} \leq l \leq m/2$, the opposite is true. This phenomenon becomes more apparent in the region $m/2 \leq l \leq m$ and is in contrast to the bound in [10, Lemma 3], which is a strictly decreasing function of l.

In Fig. Figure 3 we compare our result to the known lower bound in [10, Lemma 3] as a function of m, the number of messages at the server. Our new bound improves on the known bound when m is not very large.

2.2.3 Randomly Generated Side Information Sets

Consider a PICOD instance with n clients and m messages represented by a $n \times m$ binary matrix W, where every entry w_{ij} is i.i.d. according to a Bernoulli distribution with parameter $p \in (0,1)$. Message $b_j \in I_i$ if and only if $w_{ij} = 1$. This setting is usually used for generating PICOD instances and testing the performance of achievable algorithms in numerical evaluations [10].

By applying our result, we can show the lower bound on the largest fraction of satisfied clients with a single transmission showed previously in Thm 1 holds for the case where the side information sets are generated in an i.i.d. fashion. In particular, we have:

Lemma 1. *For a PICOD instance with $m \gg 1$ messages and n clients where each message is in the side information set of a client according to an i.i.d. Bernoulli distribution with parameter $p \in (0,1)$, the maximum number of clients that can be satisfied by a single transmission is at least $r_{m,p} = \max\{1-p, p^{\frac{1}{1-p}}(1-\frac{1}{m(1-p)})^{m(1-p)-1}e\} > 1/e$, and the number of required transmissions to satisfy all the clients is upper bounded by $1 + \frac{\log(n)}{-\log(1-r_{m,p})}$.*

Proof. The detailed proof is omitted for the sake of space. The main idea is to define the set of typical clients as

$$\mathcal{T}_\epsilon^{(m)} = \left\{ a_i, \left| \frac{|\mathcal{R}_i|}{m} - (1-p) \right| \leq \varepsilon(1-p) \right\}$$

where $\varepsilon = m^{\delta-\frac{1}{2}}$, $0 < \delta < \frac{1}{2}$. Then by similar steps as done previously, we can show that one transmission satisfies at least $r_{m,p}$ clients in $\mathcal{T}_\epsilon^m$. Thus the number of required transmissions to satisfy all the clients is at most $1 + \frac{\log(n)}{-\log(1-r_{m,p})}$. □

2.3 Comparison to Known Results

We now compare the complexity of our proposed greedy cover approach. Our achievability needs to check all possible choices of messages for a linear combination in order to find the one that gives maximum coverage. However, in the scenarios where all clients have the side information set of approximately the same cardinality, we can limit the search to the choices with $k = \lfloor \frac{m}{l} \rfloor$ messages, which has cardinality $\binom{m}{k} \leq \binom{m}{\lfloor m/2 \rfloor} \approx \frac{2^m}{\sqrt{\frac{\pi m}{2}}}$. Thus the running time of our algorithm is at most $O(\frac{2^m}{\sqrt{m}})$, and only depends only on the number of messages m. The greedy cover algorithm proposed in [10, GRCOV] has running time $O\left(mn^2\right)$. The deterministic algorithm in [14] has running time $O(nm^2 \log(n))$. Note that the running times of the last two algorithms depend on the number of clients n also. For a PICOD instance $1 \leq n \leq 2^m - 1$ (i.e., we only consider clients those that have distinct side information sets). Thus the upper bounds of running time for the last two algorithms are $O(m2^{2m})$ and $O(m^3 2^m)$, respectively, in the worst case. Compared to the achievability proposed in this paper, the last two algorithms are faster when n is small, but slower when n approaching its upper bound.

One interesting observation regarding our results is that a larger side information set does not always bring benefits in terms of number of required number of transmissions in PICOD. This is in contrast to the classical IC, where more messages in the side information can not degrade performance. This is because in PICOD all messages which are not in the side information are potentially desired messages. Thus more messages in the side information means less choices for messages to decode / to satisfy a

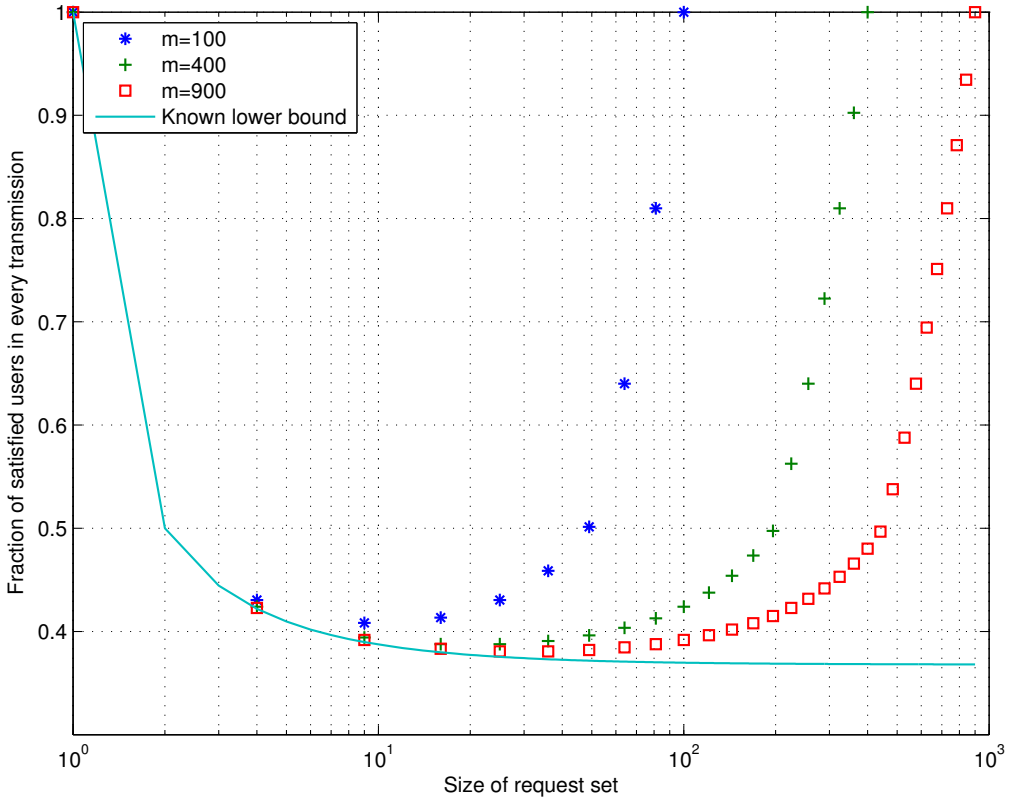

Figure 2. Lower bound on the fraction of satisfied clients by one transmission for different request set sizes. ©IEEE 2016.

client. At the other extreme, like for IC, more messages in the side information set give more network coding opportunities. There are scenarios where more messages in the side information actually reduce the fraction of clients satisfied by one transmission. The phenomenon is shown as the U-shaped curve in Fig. Figure 2. This shows that PICOD is not a generalization, but rather a variation of the classical IC.

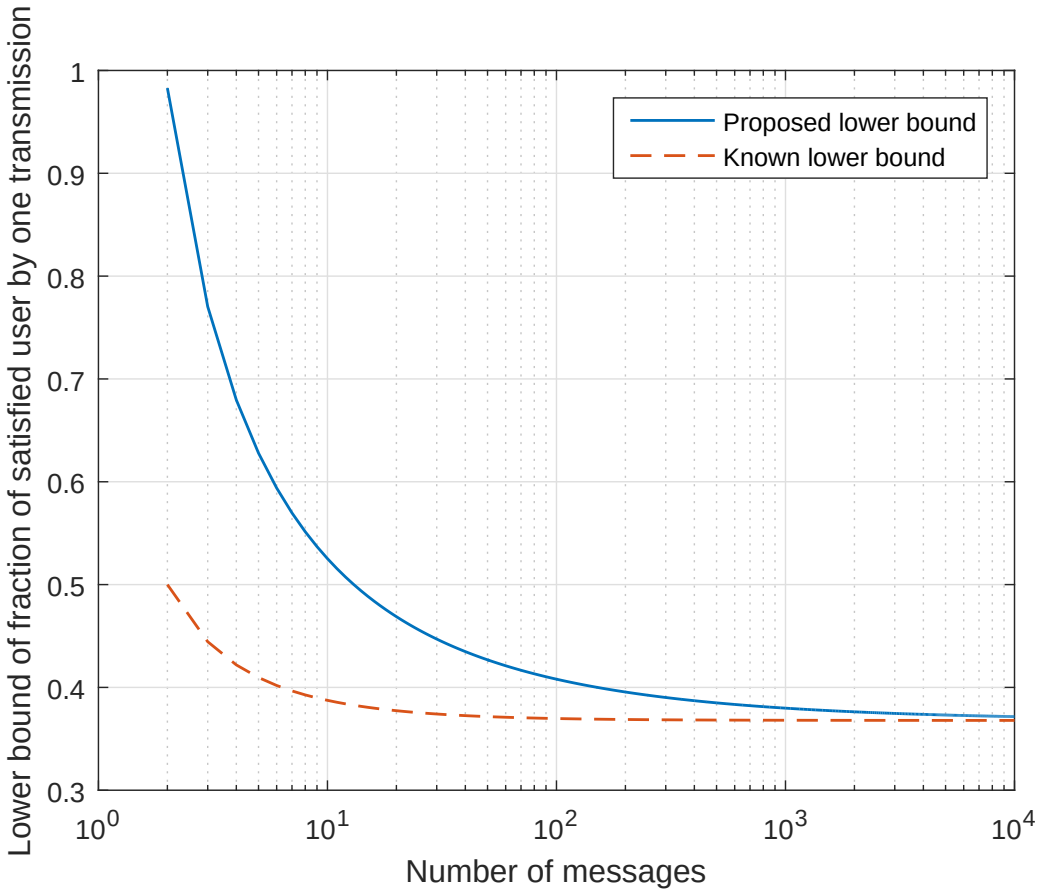

Figure 3. Lower bounds comparison for different message sizes. ©IEEE 2016.

CHAPTER 3

COMPLETE–S PICOD(T) AND PICOD(1) WITH CIRCULAR-ARC NETWORK TOPOLOGY HYPERGRAPH

3.1 Main Results and Discussion

This section summarizes our main results and comments on their proof techniques, their relationship with past work and their implications. We start with a simple achievable scheme based on linear codes. The main contribution of the paper is converse bounds on the optimal code length for the two broad families of the PICOD(t): (i) the Complete-S PICOD(t), where S is nonempty subset of $[0 : m - t]$, in Section 3.1.2, and (ii) the PICOD(1) with network topology hypergraph which are circular-arc in Section 3.1.3.

The results of this chapter have appeared in [31] and [32].

3.1.1 Achievability

We give next an achievable scheme for the general complete–S PICOD(t) based on linear codes.

Proposition 1 (Achievable Scheme)**.** *Let $\mathcal{S}$ by a partition of S, i.e., $S = \cup_{S_i \in \mathcal{S}} S_i$ and $S_i \cap S_j = \emptyset$ for all $i, j \in [|\mathcal{S}|]$ such that $i \neq j$. The optimal number of transmission for the complete–S PICOD(t) with m messages is upper bounded by*

$$\ell^* \leq \sum_{i \in [|\mathcal{S}|]} \min \left\{ m - \min_{s \in S_i}\{s\}, \max_{s \in S_i}\{s\} + t \right\}. \tag{3.1}$$

By minimizing over all possible partitions $\mathcal{S}$, we have

$$\ell^* \leq \min_{\mathcal{S}} \sum_{i \in [|\mathcal{S}|]} \min \left\{ m - \min_{s \in S_i} \{s\}, \max_{s \in S_i} \{s\} + t \right\}. \tag{3.2}$$

The proof can be found in Section 3.2.

Remark 1. *Proposition 1 is a generalization of the scheme proposed in [10] whose main idea is as follows. Let $s_{\min}$ and $s_{\max}$ denote the smallest and largest size of the side information sets, respectively. Transmitting $s_{\max} + t$ messages one by one can satisfy all users since each user has at most $s_{\max}$ of the messages in its side information. Transmitting $m - s_{\min}$ linearly independent linear combinations of the m messages also satisfies all users, as each user has at least $s_{\min}$ messages in its side information. Therefore by choosing the best of above two linear codes, we have $\ell^* \leq \min\{s_{\max} + t, m - s_{\min}\}$.*

We generalize this idea for the complete–S PICOD(t) by partitioning S into the collection $\mathcal{S}$ and by satisfying the users in each $S_i \in \mathcal{S}$ by using the above scheme. The total code length is the sum of the code length for each partition. Finally, the shortest code length this scheme can achieve is given by searching the best possible partition of S.

3.1.2 Converse for some complete–S PICOD(t) problems

We show that for two choices of S the achievability in Proposition 1 is information theoretic optimal. In the following, if $s_{\min} = 0$ or $s_{\max} = m - 1$ we set $[0 : s_{\min} - 1] = \emptyset$ or $[s_{\max} + 1 : m - 1] = \emptyset$, respectively.

Theorem 2 (Converse for the "complement of the consecutive" complete–S PICOD$(\mathtt{t})$)**.** *For the complete–S PICOD*$(\mathtt{t})$ *with* $\mathtt{m}$ *messages and* $\mathtt{S} = [0 : \mathtt{m} - \mathtt{t}] \backslash [\mathtt{s}_{\min} : \mathtt{s}_{\max}] = [0 : \mathtt{s}_{\min} - 1] \cup [\mathtt{s}_{\max} + 1 : \mathtt{m} - \mathtt{t}]$ *for some* $0 \leq \mathtt{s}_{\min} \leq \mathtt{s}_{\max} \leq \mathtt{m} - \mathtt{t}$*, the optimal code length is*

$$\ell^* = \min\{\mathtt{m}, \mathtt{m} + \mathtt{t} + \mathtt{s}_{\min} - \mathtt{s}_{\max} - 2\}. \tag{3.3}$$

The proof can be found in Section 3.3.

Theorem 3 (Converse for the "consecutive" complete–S PICOD$(\mathtt{t})$)**.** *For the complete–S PICOD*$(\mathtt{t})$ *with* $\mathtt{m}$ *messages and* $\mathtt{S} = [\mathtt{s}_{\min} : \mathtt{s}_{\max}]$ *for some* $0 \leq \mathtt{s}_{\min} \leq \mathtt{s}_{\max} \leq \mathtt{m} - \mathtt{t}$ *(*$\mathtt{S}$ *contains consecutive integers, from* $\mathtt{s}_{\min}$ *to* $\mathtt{s}_{\max}$*), where* $\mathtt{t}$ *is the number of messages each user needs to decode, the optimal code length is*

$$\ell^* = \min\{\mathtt{s}_{\max} + \mathtt{t}, \mathtt{m} - \mathtt{s}_{\min}\}. \tag{3.4}$$

The proof for critical case where $\mathtt{m} = 2\mathtt{s} + \mathtt{t}$ can be found in Section 3.4. The general proof is in Section 3.5.

Remark 2. *Theorems 2 and 3 show that the simple achievable scheme in Proposition 1 can be information theoretical optimal for a class of PICOD*$(\mathtt{t})$*. Specifically, the consecutive complete–S PICOD*$(\mathtt{t})$ *is the oblivious PICOD*$(\mathtt{t})$ *studied in [10]. Our Theorem 3 provides the tight information theoretic converse for the achievability proposed in [10].*

The basic idea in the proof of Theorem 2 is to prove the existence of a user who can decode $|\mathtt{S}|$ *messages by a method referred to as "layer counting". We partition all users in the complete–S PICOD*$(\mathtt{t})$

into $|S|$ *layers. Each layer consists the users with the same size of the side information set. A layer is said to be "lower" than another if the size of the side information set of the users is smaller. The intuition is that a user in a lower layer, after having decoded its desired messages, can mimic users in higher layers and thus decode also the desired messages of those higher layer users.*

In the "complement of the consecutive" complete–S PICOD(t) *where* $S = [0 : s_{\min} - 1] \cup [s_{\max} + 1 : m - t]$ *for some* $0 \leq s_{\min} \leq s_{\max} \leq m - t$*, we show the user in the lowest layer (without any side information) can mimic a user in each higher layers and eventually decodes* $|S| + t$ *messages.*

However, this layer counting *converse is not tight in general, as explained in Remark 6 for the complete–S PICOD*(1) *with* $S = [1 : q]$ *or* $S = [q : m - 2]$ *for some* $2 \leq q \leq m - 2$*.*

To improve on the layer counting *converse, we propose a novel converse technique for the "consecutive" complete–S PICOD*(t)*, where* $S = [s_{\min} : s_{\max}]$ *for some* $0 \leq s_{\min} \leq s_{\max} \leq m - t$*. The "critical case" for this proof is the complete–S PICOD*(t) *for*

$$m = 2s + t \text{ messages and } S = \{s\} \quad \text{("critical case").} \tag{3.5}$$

In Section 3.4 Proposition 6, we show that for this critical case, regardless of the choice of desired messages and valid code, there always exists at least one user who can decode $s + t$ *messages. While the proof of Theorem 2 is constructive, that is, we explicitly identify the user who can always decode* $|S| + t - 1$ *messages (the one with no side information), the proof of Proposition 6 is not. The problem with a "constructive argument" the critical case is that, for every specific user, it is possible for every user to decode only* t *messages. Specifically, as our result shows, for any specific user, there exists*

an information theoretic optimal choice of desired messages and a corresponding code such that this user can decode only its desired $\mathtt{t}$ *messages. In other words, showing that a certain user can always decode more than* $\mathtt{t}$ *messages is impossible. Therefore, in the proof of Proposition 6, we propose a combinatorial method to show the existence of at a least a user with some desired property, namely, the ability to decode a certain number of messages. The new method involves the Maximum Acyclic Induced Subgraph (MAIS) converse idea for the classic index coding problem [6] as well as a combinatorial design technique inspired by Steiner system [33]. The existence proof does not indicate which user has the desired property, but only shows its existence regardless of the choice of desired messages at the users. In this way we avoid the tedious case-by-case study for the various different choices of desired messages.*

Theorem 3 can be further extended to cover other complete–S PICOD$(\mathtt{t})$. We have the following results.

Proposition 2 (Not a complete–S, but all users are below the "critical case" users)**.** *For the complete–*S *PICOD*$(\mathtt{t})$ *with* $\mathtt{m}$ *messages and* $\mathtt{s}_{\max} := \max_{\mathtt{s}\in\mathtt{S}}\{\mathtt{s}\} \leq \lfloor \frac{\mathtt{m}-\mathtt{t}}{2} \rfloor$*, the optimal code length is* $\ell^* = \mathtt{s}_{\max} + \mathtt{t}$.

The proof can be found in Section 3.6

Proposition 3 (Not a complete–S, but all users are above the "critical case" users)**.** *For the complete–*S *PICOD*$(\mathtt{t})$ *with* $\mathtt{m}$ *messages and* $\mathtt{s}_{\min} := \min_{\mathtt{s}\in\mathtt{S}}\{\mathtt{s}\} \geq \lceil \frac{\mathtt{m}-\mathtt{t}}{2} \rceil$*, the optimal code length is* $\ell^* = \mathtt{m} - \mathtt{s}_{\min}$.

The proofs can be found in Section 3.6

Proposition 4 (Not a complete–S, but all users in a band around the "critical case" users are present)**.** *For the complete–*S *PICOD*$(\mathtt{t})$ *with* $\mathtt{m}$ *messages, let* $\delta := \min\{\mathtt{s}_{\max} - \lceil \frac{\mathtt{m}-\mathtt{t}}{2} \rceil, \lfloor \frac{\mathtt{m}-\mathtt{t}}{2} \rfloor - \mathtt{s}_{\min}\}$*, where*

$s_{\max} = \max_{s\in S}\{s\}$ *and* $s_{\min} = \min_{s\in S}\{s\}$. *If* $\left[\lfloor \frac{m-t}{2} \rfloor - \delta : \lceil \frac{m-t}{2} \rceil + \delta\right] \subseteq S$ *then the optimal code length is* $\ell^* = \min\{s_{\max} + t, m - s_{\min}\}$.

The proof can be found in Section 3.6

Remark 3. *Propositions 2, 3 and 4 show an interesting fact: for these settings the only relevant layer in the layer representation are the ones closest to the "critical" middle layer* $\frac{m-t}{2}$*, or the layers in a band* $\left[\lfloor \frac{m-t}{2} \rfloor - \delta : \lceil \frac{m-t}{2} \rceil + \delta\right]$ *that is around the "critical" middle layer. The optimal code for the users in these layers satisfies all the remaining users.*

Finally, for the PICOD(t) cases that are not covered by Propositions 2, 3, 4 and Theorem 2, up to $m = 5$ we have the following:

Proposition 5. *For all complete–S PICOD*(t) *with* $m \leq 5$ *and non-empty* $S \subseteq [0 : m-1]$*, the achievable scheme in Proposition 1 is information theoretic optimal.*

The proof can be found in Section 3.6.

Remark 4. *Proposition 5 is proved by checking all cases of the complete–S PICOD*(t) *with* $m \leq 5$*. In Section 3.6, some new techniques are developed for the converse proof. However, these techniques are not generalizable for the complete–S PICOD*(t) *of general* m*.*

3.1.3 Converse for PICOD(1) with circular-arc network topology hypergraph

We refer the reader to an introduction on graph theory terminology in Section 3.7.1. The complete–$\{s\}$ PICOD(t) has a network topology hypergraph which is the dual hypergraph of the complete $(m-s)$–uniform hypergraph. For this case, we prove the converse by finding a user that can decode a certain

number of messages, as what we do for the complete–S PICOD$(\mathtt{t})$. Specifically, we show a tight converse for the PICOD(1) whose network topology hypergraph is circular-arc.

Theorem 4. *For a PICOD(1) with $\mathtt{m}$ messages and the network topology hypergraph is a circular-arc, the optimal number of transmissions satisfies $\ell^* \leq 2$. In particular, the optimal number of transmissions is $\ell^* = 2$ unless network topology hypergraph is a 1-factor hypergraph.*

The proof can be found in Section 3.7.

Remark 5. *The achievability part of Theorem 4 is based on the following property of circular-arc hypergraph: if two vertices belong to one edge, then all vertices (cyclic) between these two vertices must belong to the same edge. The converse part of Theorem 4, which is in Proposition 8, is proved by showing that there exists one user that can decode one more message other than its desired message if a 1-factor does not exist. By showing the existence of such a user, regardless of the choices of desired messages and code sent by the transmitter, we obtain a tight lower bound on the optimal code length.*

The proofs of the main results summarized in this section will be given in the following sections.

3.2 Achievability: proof of Proposition 1

We consider the following two types of linear codes for any PICOD$(\mathtt{t})$, as originally considered in [10]:

1. Let $\mathtt{s}_{\max}$ be the maximum size of the side information set at the users. Transmit $\mathtt{s}_{\max}+\mathtt{t}$ messages, one by one. With this, every user can decode at least $\mathtt{t}$ message not in its side information set.
2. Let $\mathtt{s}_{\min}$ be the minimum size of the side information set at the users. Transmit $\mathtt{m}-\mathtt{s}_{\min}$ linearly independent linear combinations of all messages, e.g., an MDS code that allows to recover from

any $s_{\min}$ erasures of m symbols. Since each user has at least $s_{\min}$ messages in its side information set, by receiving $m - s_{\min}$ linear combinations each user is able to decode all the messages not in its side information set.

We can generalize this achievable scheme for the complete–S PICOD(t) as follows. Consider the collection $\mathcal{S}$ that is a partition S. We say that u_j belongs to the i-th group if $|A_j| \in S_i$. Our achievable scheme considers each group individually, i.e., satisfy every group by using one of the two above schemes. The code length is then the sum of code length used for each group. This proves the bound (Equation 3.1). The bound in (Equation 3.2) is simply proved by taking the best partition, as explained earlier in Remark 1.

3.3 Layer Counting Converse: Proof of Theorem 2

Recall that the complete–S PICOD(t), for a given set $S \subseteq [0 : m - t]$, comprises $n = \sum_{s \in S} \binom{m}{s}$ users where the side information sets are all possible distinct subsets of size s of m messages, for all $s \in S$. Before getting into the proof of Theorem 2, we show a general converse for any PICOD(t) based on idea of "decoding chain."

To begin with, let us consider $t = 1$ and $S = \{s\}$. In this system consider user u_j, who has side information A_j, and desires message d_j. After decoding w_{d_j}, user u_j knows messages $W_{A_j \cup \{d_j\}}$. Besides user u_j, there are s other users whose side information sets are subsets of size s of $A_j \cup \{d_j\}$. If any of these other users decode a message w_k such that $k \notin A_j \cup \{d_j\}$, then user u_j can decode message w_k as well (because it has the same side information $A_k \subset A_j \cup \{d_j\}$ as u_k). This reasoning can be repeated until user u_j can not longer mimic any other users / decode extra messages. Therefore, we have

identified a "decoding chain" for user u_j. This idea can be extended to show the following Lemma for any PICOD(t).

Lemma 2. *In a PICOD(t), for any ordering of the n users, we have*

$$\ell^* \geq \sum_{i=1}^{n} \left| D_i \setminus \cup_{j=1}^{i-1} (A_j \cup D_j) \right|. \tag{3.6}$$

Proof of Lemma 2. Since we have a working system, all users are satisfied by the transmission of the code $x^{\ell\kappa}$ of length ℓ. For user u_1 we have

$$H\left(W_{D_1} | x^{\ell\kappa}, W_{A_1}\right) \leq \ell\epsilon_\ell, \tag{3.7}$$

where $\lim_{\ell\to\infty} \epsilon_\ell = 0$ by Fano's inequality. Similarly, for user u_2 we have

$$H\left(W_{D_2} | x^{\ell\kappa}, W_{A_2}\right) \leq \ell\epsilon_\ell. \tag{3.8}$$

Therefore, by "condition reduces entropy," we have

$$\begin{aligned}
&\mathrm{H}\left(W_{D_1}, W_{D_2}|x^{\ell\kappa}, W_{A_1}, W_{A_2\setminus D_1}\right)\\
&= \mathrm{H}\left(W_{D_1}|x^{\ell\kappa}, W_{A_1}, W_{A_2\setminus D_1}\right) + \mathrm{H}\left(W_{D_2}|x^{\ell\kappa}, W_{A_1}, W_{A_2\setminus D_1}, W_{D_1}\right)\\
&= \mathrm{H}\left(W_{D_1}|x^{\ell\kappa}, W_{A_1}, W_{A_2\setminus D_1}\right) + \mathrm{H}\left(W_{D_2}|x^{\ell\kappa}, W_{A_2}, W_{A_1\cup D_1}\right)\\
&\leq \mathrm{H}\left(W_{D_1}|x^{\ell\kappa}, W_{A_1}\right) + \mathrm{H}\left(W_{D_2\setminus(A_1\cup D_1)}|x^{\ell\kappa}, W_{A_2}\right)\\
&\leq 2\ell\epsilon_\ell.
\end{aligned}$$

Therefore we have

$$\mathrm{H}\left(W_{\cup_{i=1}^{n} D_i}|x^{\ell\kappa}, W_{\cup_{i=1}^{n}(A_i\setminus\cup_{j=1}^{i-1} D_j)}\right) \leq n\ell\epsilon_\ell. \tag{3.9}$$

Since the messages are independent and uniformly distributed with entropy κ bits, and since the code is binary, we conclude

$$\sum_{i=1}^{n} \left| D_i \setminus \cup_{j=1}^{i-1} (A_j \cup D_j) \right| \tag{3.10}$$

$$= \left| \cup_{i=1}^{n} \left(D_i \setminus \cup_{j=1}^{i-1} (A_j \cup D_j) \right) \right| \kappa \tag{3.11}$$

$$= H\left(W_{\cup_{i=1}^{n} \left(D_i \setminus \cup_{j=1}^{i-1} (A_j \cup D_j) \right)} \right) \tag{3.12}$$

$$= H\left(W_{\cup_{i=1}^{n} \left(D_i \setminus \cup_{j=1}^{i-1} (A_j \cup D_j) \right)} | W_{\cup_{i=1}^{n} (A_i \setminus \cup_{j=1}^{i-1} D_j)} \right) \tag{3.13}$$

$$\leq I\left(W_{\cup_{i=1}^{n} \left(D_i \setminus \cup_{j=1}^{i-1} (A_j \cup D_j) \right)}; x^{\ell\kappa} \middle| W_{\cup_{i=1}^{n} (A_i \setminus \cup_{j=1}^{i-1} D_j)} \right) + n\ell\epsilon_\ell \tag{3.14}$$

$$\leq H\left(x^{\ell\kappa} | W_{\cup_{i=1}^{n} (A_i \setminus \cup_{j=1}^{i-1} D_j)} \right) + n\ell\epsilon_\ell \tag{3.15}$$

$$\leq H(x^{\ell\kappa}) + n\ell\epsilon_\ell \tag{3.16}$$

$$\leq \ell\kappa + n\ell\epsilon_\ell, \tag{3.17}$$

which implies that for all valid code

$$\ell \geq \sum_{i=1}^{n} \left| D_i \setminus \cup_{j=1}^{i-1} (A_j \cup D_j) \right| \tag{3.18}$$

for constant (n, κ), sufficiently large ℓ, and any valid codes. Thus this holds for the optimal code length. □

The sequence of users $u_1, u_2, \ldots, u_n$ in Lemma 2 is the "decoding chain" mentioned at the beginning of this section. In fact, the converse in Lemma 2 can also be thought of as the "acyclic induced subgraph converse" for all unicast IC [6], where each user desired multiple messages, as opposed to

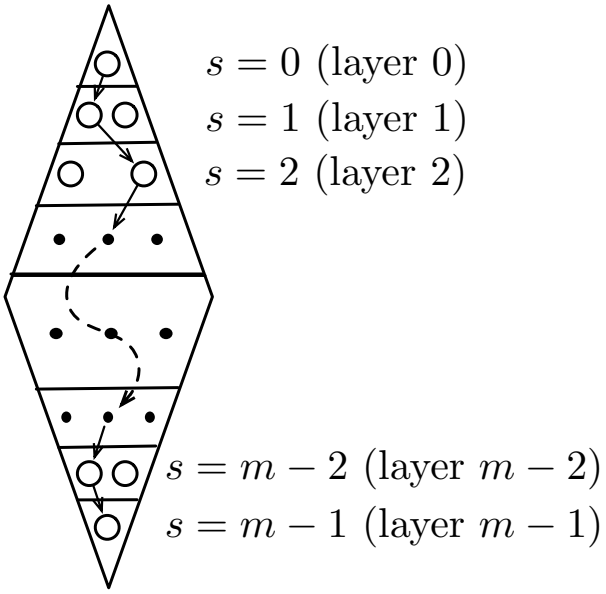

Figure 4. Layer representation of the complete–$[0 : m - 1]$ PICOD(1) problem. ©IEEE 2019.

a single message. The users with $\left|D_i \setminus \cup_{j=1}^{i-1}(A_j \cup D_j)\right| \neq 0$ form an acyclic induced subgraph in the graph representation of the IC. Therefore, in Lemma 2 the value of $\left|\cup_{i=1}^{n}\left(D_i \setminus \cup_{j=1}^{i-1}(A_j \cup D_j)\right)\right|$ depends on the choice of the order for the users, that is, we can re-lable the users in order to find the best bound provided by Lemma 2. Finding such an order for Lemma 2 illustrates the intuition for the converse proof of Theorem 2: finding the user that can decode the largest number of messages.

To illustrate the method of finding the user who can decode the largest number of messages, we introduce the "layer representation" of the complete–S PICOD(t). As an example, the "layer representation" of the complete–$[0 : m - 1]$ PICOD(1) problem is given in Fig. Figure 4 in order to facilitate the understanding of the converse proof later on: all the users with the same size of the side information set are said to form a layer; there are in total m layers; the i-th layer contains the users whose side

information set has size $i \in [0 : m-1]$, and the number of users in the i-th layer is $\binom{m}{i}$. The key observation is that, in a working system, a user u_i in i-th layer can decode a message w_{d_i} it does not have in its side information set A_i. After that, user u_i is equivalent to a user u_{i+1} in the $(i+1)$-th layer whose side information is $A_{i+1} = A_i \cup \{d_i\}$. User u_i will thus be able to decode the message $w_{d_{i+1}}$ that is desired by user $u_{d_{i+1}}$, in addition to its own desired message w_{d_i}. But now user u_i will have $A_{i+2} = A_i \cup \{w_{d_i}, w_{d_{i+1}}\}$, which is the side information of a user u_{i+2} in the $(i+2)$-th layer. By continuing with the same reasoning, user u_i will be able to mimic one user per layer until the last layer. We apply this argument to the user in the 0-th layer (there is only one such user). We see that the user in the 0-th layer is able to decode one message "per layer" without loss of generality (wlog), that is, m messages in total. This provides a "decoding chain" of length m. In this decoding chain each user's side information set and the desired message set form the side information set of the next user. By having such a decoding chain, we can use Lemma 2 to show that $\ell^* \geq m$. We use this observation, and similar ones, to provide a lower bound on ℓ^* in terms of number of messages a user can decode.

The proof of Theorem 2 directly follows this idea. The key for the proof is the fact that each layer in the "layer representation" for the complement complete–S, where $S = [0 : m-t] \setminus [s_{\min} : s_{\max}]$, contains all users with side information set of the same size. After the user decode its desired message, we can "map" this user another user in the next layer. Such a mapping forms a decoding chain started from a user in the 0-th layer, which provides a lower bound on ℓ^*.

We are now ready to prove Theorem 2 for the complement complete–S with m messages and $S = [0 : m-t] \setminus [s_{\min} : s_{\max}]$.

Proof of Theorem 2. Consider the PICOD(t) where $S = [0 : m-t] \backslash [s_{\min} : s_{\max}] = [0 : s_{\min} - 1] \cup [s_{\max} + 1 : m - t]$ for some $0 \leq s_{\min} \leq s_{\max} + 1 \leq m - t$. Assume all users are satisfied by the transmission of x^{ℓ_K}. Let u_1 be the user with empty set information, i.e., $A_1 = \emptyset$. Since all users are satisfied, u_1 can decode a message not in its side information set, with index d_{11}. Layer 1 contains the users with side information set of size 1. There exists a user in layer 1, say u_2, with side information $A_2 = \{d_{11}\}$ and desired message $d_{21} \notin A_2$. By continuing with this reasoning we can find users $u_1, \ldots, u_{s_{\min}}, u_{s_{\min}+1}, \ldots, u_{m+1-\max\{s_{\max}+1, s_{\min}-1+t\}}$ such that $A_j = A_{j-1} \cup \{d_{(j-1)1}\}$, $j \in [2 : m + 1 - \max\{s_{\max} + 1, s_{\min} - 1 + t\}] \setminus \{s_{\min} + 1\}$ and $A_{s_{\min}+1} \supseteq A_{s_{\min}} \cup D_{s_{\min}}$.

We have thus constructed a chain of $n' := m + 1 - \max\{s_{\max} + 1, s_{\min} - 1 + t\}$ users. These users satisfy $A_j \supset A_{j-1}$, for all $j \in [2 : n']$, therefore $\left| D_i \setminus \cup_{j=1}^{i-1} (A_j \cup D_j) \right| \geq 1$ for all $i \in [n']$. By Lemma 2 we have

$$\begin{aligned}
\ell^* &\geq \sum_{i=1}^{n'} \left| D_i \setminus \cup_{j=1}^{i-1} (A_j \cup D_j) \right| \\
&\geq s_{\min} - 1 + t + m - \max\{s_{\min} - 1 + t, s_{\max} + 1\} \\
&= \min\{m, m + t + s_{\min} - s_{\max} - 2\}.
\end{aligned}$$

The value $\ell^* = \min\{m, m + t + s_{\min} - s_{\max} - 2\}$ can be achieved by the scheme in Proposition 1 by using the following partition. Partition S into two groups as $S = S_1 \cup S_2$ with $S_1 := [0 : s_{\min} - 1]$ and $S_2 := [s_{\max} + 1 : m - t]$. All users in group S_1 are satisfied with $s_{\min} + t - 1$ transmissions. All users in group S_2 are satisfied with $m - s_{\max} - 1$ transmissions. Therefore, we have an achievability with code

length $m + s_{\min} + t - s_{\max} - 2$. By (Equation 3.3) we have $\ell^* \leq \min\{m, m + s_{\min} + t - s_{\max} - 2\}$, which coincides the converse.

This concludes the proof of Theorem 2. □

Remark 6. *The above proof constructively builds a "decoding chain". The "decoding chain" starts from the user in the lowest layer. The next user in the chain is chosen in the next layer, based on the side information and desired message of the previous one. The chain ends at the highest layer. However, this construction, where each layer contributes at most one user to the decoding chain, does not always work.*

As shown in [31], for the complete–S *PICOD*(1) *where* $S = [1 : q]$ *or* $S = [q : m-2]$, $1 \leq q \leq m-2$, *the optimal number of transmission is* $\ell^* = |S| - 1$. *In other words, there exists a decoding chain which includes two users with the same size of side information, where one of the users can mimic the other one.*

However, the proofs in [31] use a "case-by-case" reasoning, where the different cases are for different choices of desired messages of the users. For the complete–S *PICOD*(1) *for general* $S = [s_{\min} : s_{\max}]$, *the number of cases becomes too many to be tractable. Thus the method is not easily generalizable. The two cases considered in [31] are covered by Theorem 3.*

3.4 Critical Case: complete–$\{s\}$ the PICOD(t) with $m = 2s + t$ messages

To overcome the limitation of the "case-by-case" reasoning highlighted in Remark 6, we shall use the "existence proof" technique for Theorem 3. Loosely speaking, when dealing with general $S = [s_{\min} : s_{\max}]$, to avoid the numerous sub-cases need to be considered in [31], we treat all users and all the various desired message choices at once. Before we prove Theorem 3 in full generality, we consider the

"critical case" in (Equation 3.5). We shall see that all other cases can be deduced from the critical one. Therefore this section contains the proof of the major result for the consecutive complete–S PICOD$(\mathtt{t})$, which is largely based on combinatorics.

Specifically, in the rest of this section we prove the following result:

Proposition 6. *For the complete–*$\{\mathtt{s}\}$ *PICOD*$(\mathtt{t})$ *with* $\mathtt{m} = 2\mathtt{s} + \mathtt{t}$ *messages, the optimal code length is* $\ell^* = \mathtt{s} + \mathtt{t}$. *Specifically, given a valid code, there always exists a user that can decode* $\mathtt{s} + \mathtt{t}$ *messages.*

The fundamental part of the proof idea is similar to the layer counting converse used in Theorem 2: we show that under the assumption that all users can decode at least one message outside their side information, there must exist a user that can mimic the other users thus decodes ℓ^* messages regardless of the desired messages of all the users. Note that in the complete–S PICOD$(\mathtt{t})$ where $|\mathsf{S}| = 1$, only one layer exists. Thus by the constructive method in Theorem 2, we only obtain the trivial bound $\ell^* \geq 1$. However, we really need is not to find the specific user that can decode $\mathtt{s} + \mathtt{t}$ messages, but only show its existence. So we turn to an existence proof. Specifically, for all possible desired message choices for the users, given a valid code that satisfies all users, we show that there exists a user that can decode $\mathtt{s} + \mathtt{t}$ messages. We start by introducing the two main ingredients needed in the converse proof of Proposition 6.

3.4.1 Converse Main Ingredient 1: Block Cover

So far we used the idea of decoding chain to show that a user can decode more than its desired messages. The decoding chain depends on the choice of desired messages at the users. Once the desired messages change, the decoding chain may change as well. Here we are only interested in the existence

of such a decoding chain. In other words, we show the existence of the decoding chain of certain length regardless of the choice of desired messages at the users.

Example 1. *Consider the complete–*$\{1\}$ *PICOD*(1)*, i.e.,* $s = t = 1$*,* $m = 2s + 1 = 3$*,* $n = \binom{m}{s} = 3$ *and* $\ell^\star = s + 1 = 2$*. Say that* u_1 *knows* $A_1 = \{1\}$ *and desires* $d_1 = 2$*;* u_2 *knows* $A_2 = \{2\}$ *and desires* $d_2 = 1$*; and* u_3 *knows* $A_3 = \{3\}$ *and desires* $d_3 = 1$*. By sending* w_1*, users* u_2 *and* u_3 *are satisfied; by sending* w_2*, user* u_1 *is satisfied. By the "decoding chain" argument, user* u_3 *is able to mimic* u_1 *(because he decodes the message that is the side information set of user* u_1*) and therefore can also decode* w_2*; on the contrary, users* u_2 *and* u_3 *can not decode any more messages other than the desired one. However, another choice of desired messages can be* $d_1 = 3, d_2 = 1, d_3 = 1$*. By this choice of desired message, users* u_1 *and user* u_3 *can only decode their desired messages while user* u_2 *can mimic user* u_1 *thus is able to decode two messages.*

As in Example 1 shows for $t = 1$, for a specific user, there is always a choice of desired messages such that this user cannot decode any message other the desired one. However, we also note that for any choice of desired message, there always exists one user that can decode one more message. Then in the critical case setting, we shall prove that regardless of the choice of desired messages, there always exists a user who can decode $s + t$ messages. Since there are $\binom{s+t}{t}^{\binom{2s+t}{s}}$ (doubly exponential in s) possible choices of desired messages, finding explicitly such a user for every case is intractable. Therefore, our converse is an existence proof of such a user. The main idea of the existence proof is as follows.

Instead of checking all possible different possible choices of desired messages at a user, we reason on the size of the decoding chain for that user. By condition every user can decode t messages outside its side information. Some users may be able to decode more by mimicking other users. After receiving

a valid code, every user eventually knows at least $s + t$ messages, including the s messages in its side information set. Let user u_j, with side information A_j, eventually can decode the messages indexed by $B_j \supseteq D_j$. One can think of the set $C_j := A_j \cup B_j$ as a "block" that "covers" the side information set A_j, by which we mean that the set C_j is a proper superset of A_j. User u_j can also mimic any users u_k whose side information $A_k \subset C_j$. Therefore the desired message set for all the users u_k whose side information $A_k \subset C_j$ is $D_k \subset C_j$. For any subset of users we can find a collection $\mathcal{C}$ such that, for every side information set A_j, there is a cover $C_j \in \mathcal{C}$ such that $C_j = A_j \cup B_j$ where B_j is the set of the messages that user u_j can decode. By this definition, when consider all $\binom{m}{s}$ users, this collection $\mathcal{C}$ satisfies the following conditions:

1. For every s-element subset of $[m]$, there exists at least one $C \in \mathcal{C}$ that contains this subset.
2. $s < |C| \leq m$ for all $C \in \mathcal{C}$.
3. For all $P \subseteq [|\mathcal{C}|]$, we have $|\cap_{i \in P} C_i| \neq s$.

1 and 2 follow by the definition of block cover $\mathbb{C}$. While 3 holds because if we have $|\cap_{i \in P} C_i| = s$ for some $P \subseteq [|\mathcal{C}|]$, we have some $j \in P$ and $A_i = \cap_{i \in P} C_i$ such that $A_i \subset C_j$ and $D_i \nsubseteq C_j$, which contradicts to the definition of $\mathcal{C}$.

This "block cover" idea was inspired by the called generalized Steiner system in combinatorial design [33]. An $\mathcal{S}(s, *, m)$ generalized Steiner system consists of blocks/sets such that each subset of size s from the ground set of size m is covered exactly once. In a critical PICOD(t) setting, the collection of "blocks" $\mathcal{C}$ also cover all s-element subsets of $[m]$ (i.e., all users' side information sets). But our problem is not exactly a generalized Steiner system because an s-element subset may be contained

in more than one block as long as it is not an exact intersection of the blocks. Therefore, our "block cover" can be seen as a relaxed generalized Steiner system.

For the "critical case" we aim to show that there is a user who can decode $s + t$ messages (as in Example 1). We argue it by contradiction. Assume no user can decode $s + t$ messages, that is, every user can decode at least t and at most $s + t - 1$ messages by mimicking other users. In terms of block cover, this indicates that we can have a block cover $\mathcal{C}$ with $\max_{C\in\mathcal{C}}\{|C|\} < m$. Our argument of showing that there always exists one user that can decode $t + s$ messages for the "critical case" is equivalent to showing that a "block cover" with size at most $2s + t - 1$ cannot exist. Our combinatorial proof shows that the existence of a choice of desired messages such that $s + t \leq |C_j| \leq 2s + t - 1, \forall j \in [|\mathcal{C}|]$ leads to the existence of a user that can decode $t + s$ messages, thus $\max |C_j| = 2s + t$, which is a contradiction. Therefore must exists a user whose block cover has size $m = 2s + t$.

3.4.2 Converse Main Ingredient 2: Maximum Acyclic Induced Subgraph (MAIS) Bound

Recall that for a PICOD(t), each user chooses t desired messages outside its side information set. The indices of the desired messages for all users users is denoted as $\mathcal{D} = \{D_1, \ldots, D_n\}$, where $n = \binom{2s+t}{s}$. Once D is chosen, the PICOD(t) reduces to a *multi-cast IC* where each user requests t messages. We can make one user to be t users with the same side information but each has a distinct desired message. The IC with n users becomes a multi-cast IC with tn users, each requesting one message.

Similarly to the classic all-unicast IC, we can represent the side information sets and the desired messages in a digraph [6]. Pick a subset $U \subseteq [tn]$ of users who desire different messages and create a digraph $G(U)$ as follows. The vertices $V(G) \subseteq W$ represent the desired messages by the users in U. A directed arc $(w_i, w_j) \in E(G)$ exists if and only if the user who desires w_i has w_j in its side information

set. G is called acyclic if it does not contain a directed cycle. The size of G is the number of the vertices in, i.e. $|\mathsf{V}(\mathsf{G})| = |\mathsf{U}|$. For the all-unicast IC, the maximum size of U such that the corresponding digraph $\mathsf{G}(\mathsf{U})$ is acyclic serves as a converse bound on the optimal code length. This converse is known as "maximum acyclic induced subgraph" (MAIS) bound [6]. For the PICOD$(\mathtt{t})$, the same MAIS bound exists, which is the maximum size of the acyclic digraph $\mathsf{G}(\mathsf{U})$ created by the choice of users $\mathsf{U} \subseteq [\mathtt{tn}]$ such that they all desire different messages. Since MAIS depends on the desired message set $\mathcal{D}$, we denote its size as $|\text{MAIS}(\mathcal{D})|$.

For the PICOD$(\mathtt{t})$, as for multi-cast IC, the size of MAIS is a converse bound on ℓ [6], i.e., $\ell \geq |\text{MAIS}(\mathcal{D})|$. Finding MAIS fpr the all-unicast IC is an NP-hard problem [34] in general. Finding MAIS for the multi-cast IC will be more difficult since one needs to check every possible choice of users with distinct desired messages. For the PICOD$(\mathtt{t})$ problem it is even more complicated since each choice of $\mathcal{D}$ in the PICOD$(\mathtt{t})$ corresponds to a multi-cast IC. To find the MAIS for the PICOD$(\mathtt{t})$ we need to find the best $\mathcal{D}$ in terms of code length. Finding the MAIS for the PICOD$(\mathtt{t})$ appears intractable. Therefore, our existence proof does not find the exact MAIS for the PICOD$(\mathtt{t})$, but only its size, i.e., $\max_{\mathcal{D}} |\text{MAIS}(\mathcal{D})|$. Towards this goal, we have the following observations on MAIS for the "critical case".

Claim 1. *For the complete–*$\{\mathtt{s}\}$ *PICOD*$(\mathtt{t})$ *with* $\mathtt{m} = 2\mathtt{s} + \mathtt{t}$ *messages,* $|\mathit{MAIS}(\mathcal{D})| = \mathtt{s} + \mathtt{t}$ *for certain* $\mathcal{D}$ *if and only if there exists a user who decodes* $\mathtt{s} + \mathtt{t}$ *messages.*

Proof of Claim 1. On the one hand, if $|\text{MAIS}(\mathcal{D})| = \mathtt{s} + \mathtt{t}$, there are $\mathtt{s} + \mathtt{t}$ users who desire different messages. These users form an acyclic induced subgraph. We can obtain a decoding chain from the acyclic induced subgraph, in which the first user has side information of all $\mathtt{s}$ messages that are not

desired by these $s + t$ users. The first user, by decoding its desired message, can mimic all the other users and eventually decode $s + t$ messages.

On the other hand, if there is one user who can decode $s + t$ messages, there are $s + t - 1$ users that can be mimicked by it with different desired messages. These $s + t$ users form an acyclic induced subgraph of size $s + t$. Then $|\text{MAIS}(D)| = s + t$. □

Claim 2. *For the complete–{s} PICOD(t) with $m = 2s + t$ messages, if there exists a $\mathcal{D}$ such that $|MAIS(\mathcal{D})| < s + t$, there exists a $\mathcal{D}'$ where $|MAIS(\mathcal{D}')| = s + t - 1$.*

Proof of Claim 2. Let the choice of desired message for the complete–{s} PICOD(t) to be $\mathcal{D} = \{D_1, \ldots, D_n\}$. Consider it as a PICOD(1) with tn users. Let there be an order of the m messages, starting from 1 to m. For user u_j, we let the index of the desired message d_j represents the order of the message in the set of messages not in its side information, instead of the whole message set. Therefore, $d_j \in [s+t]$, for all $j \in [tn]$. We use $\hat{D} = \{d_1, d_2, \ldots, d_{tn}\}$ as the representation of $\mathcal{D}$, where $d_i < d_i + 1$ for $i \in [1 : t-1] \pmod t$. We can see that $|\text{MAIS}(\mathcal{D})| = |\text{MAIS}(\hat{D})|$.

Let $\hat{D}_1 = \{d_1^1, \ldots, d_{tn}^1\} = \{1, 2, \ldots, t\}$. For the choice of desired message $\hat{D}_1$, the original PICOD(t) becomes a complete–$[0 : s]$ PICOD(t) with $m = s + t$, therefore $|\text{MAIS}(\hat{D}_1)| = s + t$. Assume there is $\hat{D}_k$ with $|\text{MAIS}(\hat{D}_k)| \leq s + t - 1$. $\hat{D}_k$ can be obtained from $\hat{D}_1$ by checking each d_i^j using the following rules:

1. Start from d_1^1. For $i \in [tn]$ and $j \in [k]$, if $d_i^j = d_i^k$, skip d_i^j and move to d_{i+1}^j.
2. Else, let d_i^{j+1} to be d_i^k, i.e., create $\hat{D}_{j+1} = \{d_1^{j+1}, \ldots, d_{tn}^{j+1}\}$ such that $d_p^{j+1} = d_p^j$ for all $p \neq i$ and $d_i^{j+1} = d_i^k$. Then move to d_{i+1}^{j+1}.

3. Iterate until the last.

The iteration eventually obtains $\hat{D}_k$. By these steps we create an order of desired messages $\hat{D}_1, \hat{D}_2, \ldots, \hat{D}_k$. In this order, the adjacent $\hat{D}_j, \hat{D}_{j+1}, j \in [k-1]$ differ only in one desired message index, i.e., all users but one desire the same messages.

Recall that $|\text{MAIS}(\hat{D}_i)|$ is the maximum size of the subgraph by choosing some users U_i in the system such that the subgraph is acyclic. From $\hat{D}_i$ to $\hat{D}_{i+1}$ only one user changes its desired message. Only one vertex changes in the digraph representation. As a result, for any induced acyclic subgraph, at most one vertex changes. Therefore the size of the maximum acyclic subgraph is changed by at most 1. We have $|\text{MAIS}(D_{i+1})| \in [\text{MAIS}(D_i) - 1 : \text{MAIS}(D_i) + 1]$, i.e., the MAIS bounds of two adjacent choice of desired messages in the order differ by at most one. Since we have $|\text{MAIS}(\hat{D}_1)| = s + t$ and $|\text{MAIS}(\hat{D}_k)| \leq s + t - 1$, there exists $\hat{D}'$ such that $|\text{MAIS}(\hat{D}')| = s + t - 1$, i.e., we have $|\text{MAIS}(\mathcal{D}')| = s + t - 1$. □

3.4.3 Proof of Proposition 6

Our proof is by contradiction. Specifically, we prove that under the assumption that there exists $\mathcal{D}'$ such that $|\text{MAIS}(\mathcal{D}')| = s + t - 1$, given a valid code there must exist one user that can decode $s + t$ messages. This contradicts the Claim 1. Therefore $\mathcal{D}'$ does not exist, which implies that there must exists one user that can decode $s + t$ messages and $|\text{MAIS}(\mathcal{D})| = s + t$ for all $\mathcal{D}$. This proves that for the critical case where $S = \{s\}$ and $m = 2s + t$, the optimal number of transmission is $\ell^* = s + t$.

Specifically, the assumption that $|\text{MAIS}(D')| = s + t - 1$ implies that one can find a set of $s + t - 1$ users, denoted by V, who desire different messages and with a strict partial order on V given by: for distinct $i, j \in V$, if $i < j$ then $d_j \notin A_i$. Without loss of generality, let the desired messages by the users

V be $[s+2:2s+t]$. It is easy to see (by the definition of MAIS) that with side information $[s+1]$, one is able to decode all the remaining messages in $[s+2:2s+t]$. Consider the following $s+1$ users: for $i \in [s+1]$ user u_i has side information $A_i = [s+1] \setminus \{i\}$. We have two cases.

Case a)

Assume that for some $k \in [s+1]$ we have $B_k \cap [s+1] = [s+1] \setminus A_k$ (recall B_k is the set of messages that user u_k can decode and A_k its side information). Since this user knows all messages $W_{[s+1]}$, it can decode all the remaining messages $W_{[s+2:2s+t]}$. Eventually this user decodes $s+t$ messages, therefore $C_k = [2s+t]$.

Case b)

For every user $u_i, i \in [s+1]$, we have $B_i \subseteq [s+2:2s+t]$. We have the following claims:

Claim 3. *For the setting in Case b, for any* $P \subseteq [s+1]$*, we have* $|\cap_{i\in P} B_i| \notin [|P|-1 : |P|+t-2]$.

Proof of Claim 3. We assume that $B_i \subseteq [s+2:2s+t]$. Note B_i is the set of indices of the messages decoded by user u_i; by the "decoding chain," for any user u_k with $A_k \subset C_i = A_i \cup B_i$, we have $D_k \subset C_i$. By definition of "decoding chain," we have $|\cap_{i\in P} C_i| \notin [s : s+t-1]$ for any $P \subseteq [s+1]$. This is so because if $|\cap_{i\in P} C_i| \in [s : s+t-1]$, we have $A_k \subseteq \cap_{i\in P} C_i$ for some $k \in [n]$. Then $(D_k \cup A_k) \subset C_i, \forall i \in P$ since all users indexed by P can mimic user u_k. However, $|B_k \cup A_k| \geq s+t$ since user u_k can decode at least t messages outside its side information. This implies $|\cap_{i\in P} C_i| \geq s+t$. While we have $|\cap_{i\in P} C_i| \leq s+t-1$. We have a contradiction.

Therefore $|\cap_{i\in P} C_i| \notin [s : s+t-1]$ for all $P \subseteq [s+1]$. Note that $|\cap_{i\in P} A_i| = s+1-|P|$ and $A_i \cap B_i = \emptyset$, thus we have $|\cap_{i\in P} B_i| \notin [|P|-1 : |P|+t-2]$. □

Claim 4. *For* $s+1$ *arbitrary subsets* B_i *from a ground set of size* s*, there exists a set* $P \subseteq [s+1]$ *such that* $|\cap_{i\in P} B_i| = |P| - 1$.

To prove Claim 4 we need the following Lemma.

Lemma 3. *Let* $B_1, B_2, \ldots, B_x$ *are non-empty subsets of set* $\{v_1, v_2, \ldots, v_y\}$*, for some positive integers* x, y*. Let* C_j *be the collection of subsets that contain* v_j*, i.e.,* $v_j \in B_i$ *if and only if* $i \in C_j$*. Let* $c_j = |C_j|$*. There always exists a pair* (i, j) *such that* $\frac{c_j}{|B_i|} \geq \frac{x}{y}$ *and* $v_j \in B_i$.

The proof can be found at the end of this chapter in Section 3.8.

Proof of Claim 4. When $|B_i| = 0$ for some i, take $P = \{i\}$, we have $|\cap_{i\in P} B_i| = 0 = |P| - 1$. Claim 4 is proven. Therefore we just need to consider the case where all B_i are non-empty.

For the initial case $s = 1$ the statement in Claim 4 is true. It can be easily seen since $B_1 = B_2 = \{1\}$. Take $P = [2]$ we have $|\cap_{i\in[2]} B_i| = 1 = 2 - 1$.

Assume the statement in Claim 4 is true for all $s \leq t - 1$. We construct a P such that $|\cap_{i\in P} B_i| = |P| - 1$ for $s = t$. In Lemma 3, substitute x by $s+1$ and y by s, we have a pair (i, j) such that $j \in B_i$ and $\frac{c_j}{|B_i|} \geq \frac{s+1}{s}$, where $c_j = |C_j|$ and $C_j \subseteq [s+1]$ is the collection of subsets that contain j. By reordering the label, without loss of generality, let $i = 1$ and $B_i = B_1 = [j]$. Since $\frac{c_j}{|B_1|} \geq \frac{s+1}{s} > 1$, we have $c_j > j$, $|C_j \setminus \{1\}| > j - 1$. Consider $B'_{i'} := B_{i'} \cap [j-1]$, $i' \in C_j \setminus \{1\}$ where $B'_{i'}$ are subsets of $[j-1]$. Since $j - 1 < s$, by the inductive hypothesis there exists P' such that $|\cap_{i'\in P'} B'_{i'}| = |P'| - 1$. Let $P = P' \cup \{1\}$. Note that $j \in B_q$ for all $q \in P$ and $k \notin \cap_{q\in P} B_q$ for all $k \in [j+1 : s]$. We have $\cap_{q\in P} B_q = \cap_{j' P'} \cup \{j\}$. Then $|\cap_{q\in P} B_q| = |P'| - 1 + 1 = |P| - 1$ as $|P| = |P'| + 1$.

Therefore we can always find a P such that $|\cap_{i\in P} B_i| = |P| - 1$ for all positive integer s. □

In Case b $B_i, i \in [s+1]$ are non-empty subsets of a ground set $[s+2 : 2s+t]$. By Claim 4 it is guaranteed that there is a P such that $|[s+2 : 2s+1] \cap (\cap_{i\in P} B_i)| = |P| - 1$. Therefore we have $|\cap_{i\in P} B_i| \in [|P| - 1 : |P| + t - 2]$ for some $P \subseteq [s+1]$. However this contradicts Claims 3. Case b is thus impossible.

Therefore only Case a is possible. It shows the existence of a user whose block cover is $[m] = [2s+t]$. This user can decode $s+t$ messages. It contradicts the assumption that the MAIS bound is $|\text{MAIS}(\mathcal{D}')| = 2s+t-1$. Overall, this shows that for all possible choices of $\mathcal{D}$ one must have the MAIS bound $|\text{MAIS}(\mathcal{D})| = 2s+t$, which implies $\ell^* \geq s+t$. This, with the achievability in Section 3.2, concludes the proof of Proposition 6.

3.4.4 Complete–S where $|S| = 1$

With Proposition 6, we can prove a more general case.

Proposition 7. *For the complete–$\{s\}$ PICOD(t), the optimal code length is* $\ell^* = m - \min\{s+t, m-s\}$.

Proof of Proposition 7. Proposition 6 solves the case where $S = \{s\}$ and $m = 2s+t$. Therefore, in the following we study the remaining two cases: $m < 2s+t$ and $m > 2s+t$.

3.4.4.1 Complete–$\{s\}$ PICOD(t) where $m < 2s+t$

Consider the complete–$\{s\}$ PICOD(t) with $m < 2s+t$ and an integer $\alpha \leq s$. The $n = \binom{m}{s}$ users in the system can be split into two categories: users u_i with $[\alpha] \subset A_i$, and the other users. The users in the first category do not decode any message in $[\alpha]$ (since they have all these messages in their side information set); these users together form a complete–$\{s-\alpha\}$ PICOD(t) with $m - \alpha$ messages. Since this complete–$\{s-\alpha\}$ PICOD(t) is a subset of the original complete–$\{s\}$ PICOD, its optimal number

of transmissions is a lower bound on the number of transmissions in the original system. If we take $m - \alpha = 2(s - \alpha) + t \iff \alpha = 2s + t - m > 0$ then, by Proposition 6, the optimal number of transmissions for the complete–$\{s - \alpha\}$ PICOD(t) with $m - \alpha$ messages is $(s - \alpha) + t = m - s$.

Therefore the original complete–$\{s\}$ PICOD(t) requires at least $m - s$ transmissions, i.e., $\ell^* \geq m - s = \min\{m - s, s + t\}$.

3.4.4.2 Complete–$\{s\}$ PICOD(t) where $m > 2s + 1$

The proof is by contradiction.

Assume there exists a D' such that $|\text{MAIS}(D')| = s + t - 1$ and, without loss of generality, that the maximum acyclic induced subgraph is formed by users with desired messages $[s + t - 1]$. Specifically, we have users $u_i, i \in [s + t - 1]$ such that $d_i = i$ and $d_j \notin A_i$ for any $j, i \in [s], j > i$ (by the definition of MAIS and its induced partial order).

Let U' index the users whose side information is a subset of $[s+t : m]$, i.e., $i \in U'$ if $A_i \subset [s+t : m]$. Apparently $1 \in U'$. We distinguish two cases.

Case c) If there is a user $u_t \in U'$ with desired message $d_t \in [s + t : m]$, we have $d_j \notin A_t$ for all $j \in [s]$. Thus users $u_t, u_1, u_2, \ldots, u_{s+t-1}$ form an acyclic induced subgraph of length $s + t$. This contradicts to the assumption that $|\text{MAIS}(D')| = s + t - 1$.

Case d) For all $t \in U'$ we have $d_t \in [s]$. By a similar reasoning as in proof of Proposition 6, we can show that there exists a user who can decode $s + t$ messages. This again contradicts the assumption that $|\text{MAIS}(D)| = s + t - 1$.

By combining the two above cases, we conclude that $|\text{MAIS}(D)| > s$. By Claims 1 and 2 we thus have $\ell^* \geq s + 1$.

The achievability follows directly the schemes in Proposition 1. Since $|S| = 1$, no partition is needed. □

3.5 Complete–S PICOD(t) where S is consecutive: Proof of Theorem 3

With Proposition 7, we are ready to prove Theorem 3 in full generality. We consider the following three cases.

3.5.1 Case $s_{max} \leq \lceil m/2 \rceil - 1$: $\ell^* = s_{max} + 1$

Drop all the users except those with side information set of size s_{max}, thereby obtaining a compete-$\{s_{max}\}$ PICOD(t) with m messages. For this system the optimal number of transmissions is $\min\{m - s_{max}, s_{max} + 1\} = s_{max} + 1$ (because $s_{max} + 1 \leq \lceil m/2 \rceil$ in this case), which is a lower bound on the number of transmissions in the original system. By Proposition 1, we have $\ell^* = s_{max} + 1$.

3.5.2 Case $s_{min} \geq \lfloor m/2 \rfloor$: $\ell^* = m - s_{min}$

As for the case in Section 3.5.1, drop all the users except those with side information of size s_{min}, thereby obtaining a compete-$\{s_{min}\}$ PICOD(t) with m messages and optimal number of transmissions is $\min\{m - s_{min}, s_{min} + 1\} = m - s_{min}$ (because $s_{min} \geq \lfloor m/2 \rfloor$ in this case). This lower bound on the number of transmissions in the original systems is attained by our second type of achievability in Proposition 1.

3.5.3 Case $s_{min} \leq \lceil m/2 \rceil - 1 \leq \lfloor m/2 \rfloor \leq s_{max}$

Define $\delta := \min\{s_{max} - \lceil \frac{m-t}{2} \rceil, \lfloor \frac{m-t}{2} - s_{min} \rfloor\}$, drop all users except those with side information of size $s \in [\lfloor \frac{m-t}{2} \rfloor - \delta : \lceil \frac{m-t}{2} \rceil + \delta]$, thereby obtaining a complete–$[\lfloor \frac{m-t}{2} \rfloor - \delta : \lceil \frac{m-t}{2} \rceil + \delta]$ PICOD(t) with m messages. Create dummy messages $W_{[m+1:m']}$, where $m' = m + 2\delta + \lfloor m/2 \rfloor - \lceil m/2 \rceil + 1$.

Dummy messages will not be desired by any user. To every user, with side information of size s, who was not dropped and has size information set of size $s \in [\lfloor \frac{m-t}{2} \rfloor - \delta : \lceil \frac{m-t}{2} \rceil + \delta]$ give, as extra side information, an $(\lceil \frac{m-t}{2} \rceil + \delta - s)$-subset of $[m+1 : m']$; each such user generates $\binom{2\delta+\lfloor m/2 \rfloor - \lceil m/2 \rceil + 1}{\lceil \frac{m-t}{2} \rceil + \delta - s}$ new users. The new users created by this procedure form a complete–$\{\lceil \frac{m-t}{2} \rceil + \delta\}$ PICOD(t) with m' messages, whose optimal number of transmissions is

$$
\begin{aligned}
&\min \left\{ \lceil \frac{m-t}{2} \rceil + \delta + t, m' - (\lceil \frac{m-t}{2} \rceil + \delta) \right\} \\
&= \min \left\{ \lceil \frac{m-t}{2} \rceil + \delta + t, m + 2\delta + \lfloor m/2 \rfloor - \lceil m/2 \rceil + 1 - \lceil \frac{m-t}{2} \rceil - \delta \right\} \\
&= \delta + t + \min \left\{ \lceil \frac{m-t}{2} \rceil, \lfloor \frac{m-t}{2} \rfloor + t + \lfloor m/2 \rfloor - \lceil m/2 \rceil + 1 \right\} \\
&= \delta + t + \lceil \frac{m-t}{2} \rceil \\
&= \min \left\{ \lfloor \frac{m-t}{2} \rfloor - s_{\min}, s_{\max} - \lceil \frac{m-t}{2} \rceil \right\} + t + \lceil \frac{m-t}{2} \rceil \\
&= \min \{ s_{\max} + t, m - s_{\min} \} \\
&= \ell'.
\end{aligned}
$$

Although the new system contains more users, any valid code for the original system works for the new one. Therefore the optimal code length ℓ' is a lower bound on the optimal code length for the original system. This lower bound can be attained by the scheme described in Proposition 1.

This concludes Theorem 3.

3.6 Some other complete–S PICOD(t) problems

Note that in Section 3.4.4, the proof starts with dropping some users in the system. This shows that there exists "non-critical" users that do not affect the optimal code length. Therefore, by adding non-critical users, we can obtain a "non-consecutive complete–S" PICOD(t) where the proof used for Theorem 3 can still provide a tight converse.

3.6.1 Proof of Proposition 2

The converse depends only on the users with side information of size $s_{\max}$. Therefore adding any users with smaller size of side information does not change the converse. The optimal transmission that satisfies the complete–$\{s_{\max}\}$ PICOD(t), i.e., transmit $s_{\max}+t$ messages one at a time, also satisfies all the users with smaller size of side information.

3.6.2 Proof of Proposition 3

The converse depends only on the users with side information of size $s_{\min}$. Therefore adding any users with larger size of side information does not change the converse. The optimal transmission that satisfies the complete–$\{s_{\min}\}$ PICOD(t), i.e., transmit $m-s_{\min}$ linearly independent linear combinations of all messages, also satisfies all the users with larger size of side information.

3.6.3 Proof of Proposition 4

The converse depends only on the users with side information of size in $[\lfloor\frac{m-t}{2}\rfloor-\delta:\lceil\frac{m-t}{2}\rceil+\delta]$. Therefore adding any users with either larger or smaller size of side information does not change the converse. The optimal transmission that satisfies the complete–$[\lfloor\frac{m-t}{2}\rfloor-\delta:\lceil\frac{m-t}{2}\rceil+\delta]$ PICOD(t) also satisfies all the users with larger size of side information. That is, either transmit $s_{\max}+t$ messages one at a time, or $m-s_{\min}$ linearly independent linear combinations of all messages.

3.6.4 Proof of Proposition 5

Proposition 5 states that the achievable scheme in Proposition 1 is information theoretically optimal for the complete–S PICOD(t) with $m \leq 5$. The main idea behind these proofs follows the one in converse proof of Theorem 2: construct a decoding chain by providing proper messages to the user as genie, in a way that the user can mimic other users and decode the desired number of messages.

Table Table I lists the optimal code length ℓ^* of all complete–S PICOD(t) instances that are not covered by Theorem 2 and Propositions 2, 3, 4.

TABLE I

COMPLETE–S PICOD(t) THAT ARE NOT COVERED BY THEOREM 2 AND PROPOSITIONS 2, 3, 4. ©IEEE 2019.

$m = 4$	$S = \{0, 2\}$	$t = 1, 2$	$\ell^* = t + 2$
	$S = \{1, 3\}$	$t = 1$	$\ell^* = 3$
$m = 5$	$S = \{0, 3\}$	$t = 1, 2$	$\ell^* = t + 2$
	$S = \{1, 4\}$	$t = 1$	$\ell^* = 3$
	$S = \{1, 3\}$	$t = 1, 2$	$\ell^* = 4$
	$S = \{0, 1, 3\}$	$t = 1, 2$	$\ell^* = t + 3$
	$S = \{1, 3, 4\}$	$t = 1$	$\ell^* = 4$
	$S = \{0, 2, 3\}$	$t = 1, 2$	$\ell^* = t + 3$
	$S = \{0, 2, 4\}$	$t = 1$	$\ell^* = 4$
	$S = \{1, 2, 4\}$	$t = 1$	$\ell^* = 4$

Unfortunately, the converse proofs are based on a "case-by-case" reasoning, i.e., constructively find a user that can decode a certain number of messages. They can not be straightforwardly extended to

the complete–S PICOD(t) for general m. Here we show proofs of two cases. The other cases can be proved using the similar methods.

Corollary 1. *For the complete–S PICOD*(1) *where* $S = \{1, 3\}$ *and* $m = 5$*, the optimal code has length* $\ell^* = 4$.

Proof of Corollary 1. We show that there exists one user with a message in its side information set who can decode the remaining 4 messages.

By Proposition 7 we claim there exists a user u_1 with side information set of size 1, say $A_1 = \{1\}$, can decode 2 messages, say $B_1 \supseteq \{2, 3\}$. User u_1 thus can mimic user u_2 with side information $A_2 = \{1, 2, 3\}$ and decode its desired message. Therefore user u_1 can decode at least 3 messages, $|B_1| \geq 3$. Denote the last message that has not been decoded by user u_1 as w_5. Now, if w_5 is desired by some users, i.e., we have a user u_3 with $d_3 = 5$, user u_1 can mimic user u_3 and decode w_5 since $A_3 \subset [4]$. Therefore user u_1 can decode 4 messages and $\ell^* \geq 4$

Otherwise, w_5 is not desired by any users in the system. Since the message that is not desired by any users does not have any effects, by deleting it, the system becomes the complete–$\{0, 1, 2, 3\}$ PICOD(1) with $m = 4$. By Theorem 2 we have the user with $A = \{5\}$ can decode 4 messages and $\ell^* \geq 4$.

We apply the achievability for the complete–$\{1, 2, 3\}$ PICOD(1). This achievability works since $\{1, 3\} \subset \{1, 2, 3\}$. By Theorem 3 we have $\ell^* \leq 4$. This achievability is optimal. □

Corollary 2. *For the complete–S PICOD*(1) *problem where* $S = \{0, 2, 4\}$ *and* $m = 5$*, the optimal code has length* $\ell^* = 4$.

The following lemma, which is a refined version of Proposition 7, is used in the proof of Corollary 2.

Lemma 4. *For a complete–*$\{s\}$ *PICOD*(t)*, let* $A' \subset [m], |A'| \leq s$*,* $U_{A'}$ *be the group of users who have* A' *in their side information, i.e.,* $u_i \in U_{A'}$ *if and only if* $A' \subseteq A_i$*. For any* A'*, there exists a user in* $U_{A'}$ *that can decode at least* $\min\{m - s, s + t - |A'|\}$ *messages. Note that it recovers Proposition 7 when* $A' = \emptyset$*.*

Proof of Lemma 4. The users in $U_{A'}$ alone can be seen as the users in a new complete–S' PICOD(t), where $S' = \{s - |A'|\}$, $m' = m - |A'|$. By Proposition 7 we have that there exists a user in this system that can decode $\min\{s' + t, m' - s'\} = \min\{s + t - |A'|, m - s\}$ messages. The above argument holds for all $A' \subset [m], |A'| \leq s$. □

Proof of Corollary 2. We show that by giving one message as a genie, the user with no side information can decode the other 4 messages.

Since every user can decode one message, user u_1 with $A_1 = \emptyset$ can decode message w_{d_1}. By Lemma 4, we see that there exists a user $u_2 \in U_{\{d_1\}}$ that can decode 2 messages, where $U_{\{d_1\}}$ is the group of users who have side information sets of size 2 and w_{d_1} in their side information sets. Without loss of generality let $A_2 = \{d_1, 2\}$ and the two messages that u_2 can decode be w_3, w_4, $d_1 \notin \{2, 3, 4\}$. Therefore, giving message w_2 to user u_1 allows it to decode w_3, w_4. Also, there exists a user with side information $\{d_1, 2, 3, 4\}$ and decodes $w_{d_5} \notin \{d_1, 2, 3, 4\}$. So user u_1 can decode w_{d_5} as well. Overall, user u_1 can decode 4 messages with the proper genie w_2. The code length is therefore lower bounded by $\ell^* \geq 4$.

For the achievability, we split the users into two groups: $S_{\{0,2\}}$ where users have side information of size 0 or 2; $S_{\{4\}}$ where users have side information of size 4. By Proposition 2 we can satisfy all users

in $S_{\{0,2\}}$ with 3 transmission; by Proposition 7 we can satisfy all users in $S_{\{4\}}$ with one transmission. In total we use 4 transmissions to satisfy all users. □

Remark 7. *In fact the existence proof based on block cover used for Proposition 6 is also workable for Proposition 5 as well. For instance, for the complete–*$\{1,3\}$ *PICOD*(1)*, we can define the block cover* $\mathcal{C} = \{C_i, i \in [5]\}$ *for each user with side information* $A_i = \{i\}, i \in [5]$*. The block cover satisfies*

1. $i \in C_i$ *for all* $i \in [5]$.
2. $\forall P \subseteq [5]$, $|\cap_{i\in P} C_i| \neq 1, 3$.

By a similar reasoning used in the proof of Proposition 6, we can show that these two conditions lead to the block cover with $\max_{\mathcal{C}} |C_i| = 5$*, meaning that there always exists one user that can decode* 4 *messages. However, this existence proof can not be generalized as an universal converse proof for all cases. It is also more complex compared to the constructive proofs we showed in Corollary 1 and Corollary 2.*

3.7 Proof of Theorem 4

In this section, we prove a tight converse bound on ℓ^* for the PICOD(1) whose network topology hypergraph is circular-arc. We start by introducing some graph theory terminologies.

3.7.1 Graph Preliminary

Let $H = (V, \mathcal{E})$ denote a *hypergraph* with vertex set V and edge set $\mathcal{E}$, where an edge $E \in \mathcal{E}$ is a subset of V, i.e., $E \subseteq V$. The hypergraph is called r-*uniform* if all edges have cardinality r, i.e., $|E| = r$, $\forall E \in \mathcal{E}$. For $R \subseteq [|V|]$, the hypergraph is called R-*uniform* if all edges have cardinality of some $r \in R$, i.e., $|E| \in R$, $\forall E \in \mathcal{E}$. The hypergraph is called *complete* r-*uniform* if all edges with

cardinality r exit, i.e., for all E such that $|E| = r, E \subseteq V$, we have $E \in \mathcal{E}$. The hypergraph is called complete R-*uniform* if all edges with cardinality $r \in R$ exist. The dual hypergraph $H^* = (V^*, \mathcal{E}^*)$ of H is a hypergraph where the vertices and edges are interchanged, i.e., $\mathcal{E}^* = V$, $V^* = \mathcal{E}$.

The degree of a vertex $v \in V$ is the number of its incident edges, i.e., $\delta(v) = |\{E : v \in E, E \in \mathcal{E}\}|$. The hypergraph is called k-*regular* if the degree of all vertices is k. A *factor* of H is a spanning edge induced subgraph of H, i.e., an edge induced subgraph of H with the same vertex set of V. A k-*factor* is a factor which is k-regular. A hypergraph H is called an *circular-arc hypergraph* if there exists an ordering of the vertices $v_1, v_2, \ldots, v_n$ such that if $v_i, v_j, i \leq j$, then the v_q for either all $i \leq q \leq j$ or all $q \leq i$ and $a \geq j$ are incident to an edge E,

For a PICOD(t), its network topology hypergraph is a hypergraph $H = (V, \mathcal{E})$ such that: i) $V = \{u_1, \ldots, u_n\}$, i.e., vertices represent the users; ii) $\mathcal{E} = \{E_1, \ldots, E_m\}$, i.e., edges represent the messages; iii) $u_i \in E_j$ if $w_j \notin A_i$, i.e., a vertex is incident to an edge if the user does not have the message in the side information. This definition of network topology hypergraph is a generalization of the network topology graph in [35].

Note that the network topology hypergraph is defined solely on user set U, message set W, and side information set $\mathcal{A}$. For the IC, the network topology hypergraph does not uniquely define an instance of the problem, since it does not contain the information about desired messages of the users. However, the network topology hypergraph uniquely defines a PICOD(t) for a given t, due to the property that the PICOD(t) does not specify the desired messages for the users.

3.7.2 On the Optimality of a Single Transmission

We give the necessary and sufficient condition on the network topology hypergraph of a PICOD(1) problem for which one transmission is optimal. This result applies to all PICOD(1) instances, thus serves as a general converse bound for the PICOD(1).

Proposition 8. *A PICOD*(1) *has* $\ell^* = 1$ *if and only if its network topology hypergraph has a* 1*-factor. Otherwise* $\ell^* \geq 2$*.*

Proof of Proposition 8. Achievability: The network topology hypergraph H has a 1-factor if it has an edge induced sub-hypergraph whose vertices are the same as the vertices of H and all have degree one. In other words, in this induced sub-hypergraph, all vertices are adjacent to one and only one edge. Since H is the network topology hypergraph , its vertices represent users and edges represent messages. A vertex is adjacent to an edge if and only if the user does not have that message in its side information. For the PICOD(1), that message can be a desired message by the incident users. Therefore, among all the messages corresponding to the edges in the 1-factor, every user has one and only one message that is not in its side information. Transmitting the sum of all these messages satisfies all users. By this transmission we achieve $\ell^* = 1$.

Converse: We aim to show that if the network topology hypergraph does not have a 1-factor hypergraph, then we can create a user that can decode two messages by any valid code, thus two transmissions are needed. For any valid code, consider the sub-hypergraph induced by the edges corresponding to all the desired messages by all users, i.e., the edge induced sub-hypergraph of H where the edges correspond to the messages that are decoded by at least one user. This sub-hypergraph is always a factor, i.e., spanning sub-hypergraph, since all users can decode at least one message. Assume no 1-factor exists

in H. There exists a vertex whose degree is at least 2 in the sub-hypergraph. In other word, there is a user with an undesired message that is not in its side information. This message is desired by some other users. Let this user to be u_1 and the undesired message to be w_{d_2}. That is, user u_1 desires w_{d_1}, user u_2 desires message w_{d_2}. By the condition that 1-factor does not exist, we have $d_2 \notin A_1$ and $A_1 \subseteq [m] \setminus \{d_1, d_2\}$. Therefore, we can construct a user u' with $A' = [m] \setminus \{d_1, d_2\}$. Given any valid code, user u' can mimic user u_1 then user u_2, thus can decode w_{d_1}, w_{d_2}. By Lemma 2, we conclude that $\ell^* \geq 2$. □

3.7.3 Proof of Theorem 4

We show a case where the converse proposed in Proposition 8 is tight. To do that we propose an achievable scheme based on the properties of circular-arc hypergraph.

First we show the following claim, which will be used in the proof.

Claim 5. *For a circular-arc hypergraph H without isolated vertex and the vertices are in a cyclic order $\{v_1, v_2, \ldots, v_n\}$, if there exist two edges $E_i = \{v_{i_1}, \ldots, v_{i_p}\}$, $E_j = \{v_{j_1}, \ldots, v_{j_q}\}$, such that*

1. $i_p + 1 < j_1$,
2. *every edge in $\mathcal{E}$ that contains v^{j_1} contains v_{i_p},*

then there exists an edge $E_k \in \mathcal{E} : \{v_{i_p+1}, \ldots, v_{j_1-1}\} \subseteq E_k$.

Proof of Claim 5. Since H does not have any isolated vertices, there exists $E_k \in \mathcal{E}$ such that $v_{j_1-1} \in E_k$. By the condition $v_{i_p} \in E_k$, the property of circular-arc hypergraph that if v_{i_p} and v_{j_1-1} are contained in E_k, all the vertices between are contained in E_k as well. We have $\{v_{i_p+1}, \ldots, v_{j_1-1}\} \subseteq E_k$. □

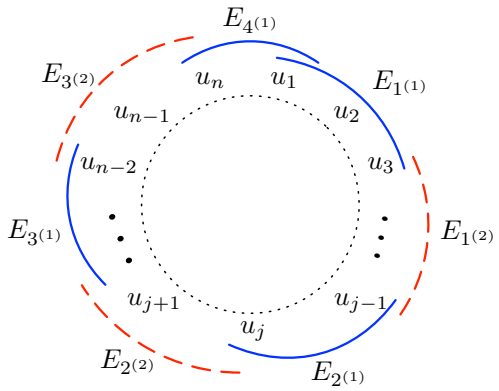

Figure 5. Two transmissions scheme for circular-arc network topology hypergraph PICOD$(\mathtt{t})$. ©IEEE 2019.

Proof of Theorem 4. We propose an achievability scheme that uses two transmissions to satisfy all users for all PICOD(1) instances whose network topology is a circular-arc hypergraph. The scheme consists two steps.

Step 1

In a PICOD(1), the side information set for any user is a proper subset of the message set, i.e, there exists at least one message not in the side information set. Therefore the network topology hypergraph does not have isolated vertex for any PICOD(1). We only consider the edges that are not a subset of the union of rest of the edges, i.e., for the set of edges $\mathcal{E}$ we consider, $E_i \nsubseteq \cup_{E_j \in \mathcal{E}, j \neq i} E_j$ for any $E_i \in \mathcal{E}$. That is to say, every edge has at least one vertex that is not in all the other edges. The message that does not satisfy this condition is not going to be considered in this achievability scheme. After applying the condition, the remaining edges $\mathcal{E}$ still span all vertices, i.e., $|\cup_{E_j \in \mathcal{E}} E_j| = n$.

Recall that in circular-arc hypergraph there exists a cyclic order on the vertices $u_1, u_2, \ldots, u_n$. Let $E_{1^{(1)}}$ be the edge with largest cardinality that is incident to u_1. Assume without loss of generality, $E_{1^{(1)}} = \{u_1, \ldots, u_i\}$ for some $i \geq 1$. The algorithm runs as follows:

1. Check if there exists an edge E incident to u_{i+1} such that $E_{1^{(1)}} \cap E = \emptyset$.

   (a) If so, choose it to be $E_{2^{(1)}}$. Note that E will be unique since no E is a subset of the others.

   (b) Otherwise, check the edges incident on next vertex u_{i+2}.

2. After find $E_{j^{(1)}}$, get back to 1) to check each vertex after $E_{j^{(1)}}$ to find $E_{(j+1)^{(1)}}$.

3. Iterate until u_n has been checked.

The result of this step is a set of k edges $\mathcal{E}^{(1)} = \{E_{1^{(1)}}, \ldots, E_{k^{(1)}}\}$. (see Fig. Figure 5). By sending the sum of the corresponding messages, the users that are "spanned" by these edges are satisfied, excluding the users whose vertices are in $E_{1^{(1)}} \cap E_{k^{(1)}}$ when $E_{1^{(1)}} \cap E_{k^{(1)}} \neq \emptyset$. This is because all edges in $\mathcal{E}^{(1)}$ are pairwise disjoint except $E_{1^{(1)}}$ and $E_{k^{(1)}}$. We then are left with the users whose corresponding vertices are contained in $(U \setminus (\cup_{\mathcal{E}^{(1)}} E_{i^{(1)}})) \cup (E_{1^{(1)}} \cap E_{k^{(1)}})$.

Step 2

The users who are not satisfied by the first transmission are users whose side information contain either all the chosen messages in Step 1, or both $W_{1^{(1)}}$ and $W_{k^{(1)}}$. In other words, they are the users who lie "between" the edges, or in the intersection of the first and last edges, in $\mathcal{E}^{(1)}$ chosen in Step 1.

For the unsatisfied users between $E_{i^{(1)}} \in \mathcal{E}^{(1)}$ and $E_{(i-1)^{(1)}} \in \mathcal{E}^{(1)}$, there exists an edge $E_{j^{(2)}}$ that includes all those users because $|\cup_{E_j \in \mathcal{E}} E_j| = n$. We find a set of edges $\mathcal{E}^{(2)} = \{E_{1^{(2)}}, \ldots, E_{(k-1)^{(2)}}\}$ such that $U \setminus (\cup_{\mathcal{E}^{(1)}} E_{i^{(1)}}) \subseteq \cup_{E_j \in \mathcal{E}^{(2)}} E_j$ (see Fig. Figure 5). Note that all edges in $\mathcal{E}^{(2)}$ are pairwise disjoint, since if $E_{j^{(2)}} \cap E_{j+1^{(2)}} \neq \emptyset$ then we have $E_{j+1^{(1)}} \subseteq E_{j^{(2)}} \cup E_{j+1^{(2)}}$.

We send the sum $\left(\sum_{j=1}^{k-1} W_{j^{(2)}}\right) + W_{1^{(1)}}$ as the second transmission. The users that are not satisfied yet by the first transmission have all but one of the messages in $\{W_{1^{(2)}}, \ldots, W_{k-1^{(2)}}, W_{1^{(1)}}\}$ in their side information sets. Therefore all the unsatisfied user after Step 1 can be satisfied by the second transmission. All the users are satisfied with two transmissions.

This, together with the converse in Proposition 8, conclude Theorem 4. □

3.8 Proof of Lemma 3

Proof of Lemma 3. Construct a $x \times y$ matrix W. $w_{ij} = 1/|B_i|$ if $v_j \in B_i$, otherwise $w_{ij} = 0$. Since $|B_i| \neq 0$ for all i, matrix W can be constructed. Note that the sum of each row is one. We have the

summation of all elements in W is $\sum_{i\in[x],j\in[y]} w_{ij} = \sum_{i\in[x]}(\sum_{j\in[y]} w_{ij}) = x$, which is the number of rows. The summation of all elements in W can also be obtained by adding up the summation of the columns. Since there are y columns, there exists a column whose summation is no less than the average, i.e., exists j such that

$$\sum_{k\in[x]} w_{kj} = \sum_{k:v_j\in B_k} \frac{1}{|B_k|} \geq \frac{x}{y}. \tag{3.19}$$

Let B_i be the smallest subset that contains v_j. We have

$$\sum_{k:v_j\in B_k} \frac{1}{|B_k|} \leq \sum_{k:v_j\in B_k} \frac{1}{|B_i|} = \frac{c_j}{|B_i|}. \tag{3.20}$$

Therefore, for the pair (i,j) we have $v_j \in B_i$ and

$$\frac{c_j}{|B_i|} \geq \frac{x}{y}. \tag{3.21}$$

□

CHAPTER 4

DECENTRALIZED COMPLETE–S PICOD(T) AND PICOD(1) WITH CIRCULAR-ARC NETWORK TOPOLOGY HYPERGRAPH

This chapter studies the decentralized setting of the PICOD which have been studied in Chapter 3. We show that when there are still pliability of choosing the desired message at some users, the centralized bound can be achieved. Otherwise, strictly more number of transmissions are needed to satisfy all users in the decentralized setting. The achievable scheme is also more complex, as we need vector index code in order to achieve the optimality in d-PICOD.

This chapter has appeared in [36].

4.1 System Model

The difference between PICOD and d-PICOD systems is the absence of the centralized transmitter. Due to this change, the encoding function will be different since it is now the function of the messages that are in the side information of a particular user. We here list the difference to the centralized PICOD channel model introducted in Chapter 3.

1. There are $n \in \mathbb{N}$ users but no central transmitter.
2. User u_i knows the messages indexed by its side information set $A_i \subset [m]$, $i \in [n]$. The collection of all side information sets is denoted as $\mathcal{A} := (A_1, A_2, \ldots, A_n)$, which is assumed globally known at all users.

Note that for a d-PICOD problem to have a solution, one must have $\cup_{i=1}^{n} A_i \neq A_j, \forall j \in [n]$, that is, every user must have at least one unknown message in the side information set of another user (so that the transmission of that message can satisfy said user).

3. The codeword $x^{\kappa\ell} := \left(x^{\kappa\ell_1}, x^{\kappa\ell_2}, \ldots, x^{\kappa\ell_n}\right)$ is eventually received by all users, where $\ell := \sum_{j\in[n]} \ell_j$ is the total (normalized by the message length) code length and where

$$x^{\kappa\ell_j} := \mathsf{ENC}_j(W_{A_j}, \mathcal{A}),\ \forall j \in [n], \tag{4.1}$$

is the encoding function at user u_j.

Note that ℓ_j are not necessarily integers when $f \neq 1$, i.e., messages are split before encoding. Also, the code is referred to a 'scalar index code' if the number of sub-message split $f = 1$, and it is called 'vector index code' otherwise.

The goal is still to find the shortest code-length with vanishing-error, that is,

$$\ell^* := \inf\{\ell : \exists \text{ a reliable code such that } \lim_{\kappa\to\infty} \epsilon_\kappa = 0\}. \tag{4.2}$$

4.2 Main Results and Discussions

In the rest of the chapter we focus on two classes of d-PICOD: the *complete*–S d-PICOD(t), for a given set $S \subseteq [0 : m - t]$, and the *circular-arc* d-PICOD(1). These two classes have been studied in the centralized setting in Chapter 3, their information theoretical optimalities are known.

4.2.1 Complete–S d-PICOD(t) problems

Theorem 5 (Converse for the *consecutive* complete–S d-PICOD(t))**.** *For the complete–S d-PICOD*(t) *with* m *messages and* $\mathsf{S} = [\mathsf{s}_{\min} : \mathsf{s}_{\max}]$ *for some* $0 \le \mathsf{s}_{\min} \le \mathsf{s}_{\max} \le \mathsf{m} - \mathsf{t}$*, the optimal code-length is*

$$\ell^* = \begin{cases} \frac{\binom{\mathsf{m}}{\mathsf{m}-\mathsf{t}}}{\binom{\mathsf{m}}{\mathsf{m}-\mathsf{t}}-1}\mathsf{t}, & \mathsf{s}_{\max} = \mathsf{s}_{\min} = \mathsf{m} - \mathsf{t}, \\ \min\{\mathsf{s}_{\max} + \mathsf{t}, \mathsf{m} - \mathsf{s}_{\min}\}, & \textit{otherwise.} \end{cases} \tag{4.3}$$

Theorem 6 (Converse for the *complement-consecutive* complete–S d-PICOD(t))**.** *For the complete–S d-PICOD*(t) *with* m *messages and* $\mathsf{S} = [0 : \mathsf{m} - \mathsf{t}] \backslash [\mathsf{s}_{\min} : \mathsf{s}_{\max}] = [0 : \mathsf{s}_{\min} - 1] \cup [\mathsf{s}_{\max} + 1 : \mathsf{m} - \mathsf{t}]$ *for some* $0 < \mathsf{s}_{\min} \le \mathsf{s}_{\max} < \mathsf{m} - \mathsf{t}$*, the optimal code-length is*

$$\ell^* = \min\{\mathsf{m}, |\mathsf{S}| + 2\mathsf{t} - 2\}. \tag{4.4}$$

Remark 8. *The detailed proofs for Theorem 5 and 6 are in Sections 4.3.1 and 4.3.2, respectively. Here are some interesting observations when we compare Theorem 5 and 6 with their centralized counterparts in [37].*

1. *Surprisingly, Theorem 6 says that, for the same* $(\mathsf{m}, \mathsf{S}, \mathsf{t})$ *the centralized and the decentralized settings have the same optimal code-length; similarly for Theorem 5, except for the case* $\mathsf{s}_{\max} = \mathsf{s}_{\min} = \mathsf{m} - \mathsf{t}$*. In other words, for most cases the d-PICOD*(t) *has the same optimal code-length as the centralized PICOD*(t) *with the same parameters of* $(\mathsf{m}, \mathsf{S}, \mathsf{t})$*. In other words, lacking a powerful centralized transmitter does not reduce the code-length is these cases.*

2. *Having the same optimal code-length does not necessarily imply that the same code is optimal in both cases. In [37], we showed that for the centralized setting simple* scalar linear *codes are optimal; in particular, the central transmitter either sends ℓ^* distinct messages one by one, or ℓ^* random linear combinations of all the messages. Clearly, the former strategy can be implemented in a decentralized setting, but not the latter. In this latter case we show that we need more sophisticated coding scheme. In particular, our achievable scheme uses* sparse Maximum Distance Separable (MDS) codes. *We also show that* vector linear *codes are necessary for optimality.*

3. *When compare the classical (centralized) PICOD and d-PICOD*$(\mathtt{t})$ *with the same parameters* $(\mathtt{m}, \mathtt{S}, \mathtt{t})$*, we shall use the notation $\ell^{*,cen}$ and $\ell^{*,dec}$, respectively, to distinguish the optimal code lengths of the centralized and decentralized setting when necessary. For the situation without ambiguity, we use ℓ^* to notate the optimal number of transmission of the d-PICOD*$(\mathtt{t})$*, which is the objective of this paper.*

   Among all d-PICOD$(\mathtt{t})$ *cases studied in this paper, the only case where the decentralized optimal code-length $\ell^{*,dec}$ is strictly larger than the corresponding centralized optimal code-length $\ell^{*,cen}$ is when*

$$\mathtt{s}_{\min} = \mathtt{s}_{\max} = \mathtt{m} - \mathtt{t}.$$

   This is the only studied case in centralized PICOD$(\mathtt{t})$ *where $\ell^{*,cen} = \mathtt{t}$, which is a trivial converse bound for the optimal number of transmissions. Since $\ell^{*,dec} > \mathtt{t}$ for all d-PICOD*$(\mathtt{t})$ *(as what is*

*sent by a user is not useful for that user), our results show that for the consecutive and complete consecutive complete–*S *d-PICOD*$(\mathtt{t})$

$$\ell^{*,dec} \neq \ell^{*,cen} \text{ if only if } \ell^{*,cen} = \mathtt{t}.$$

Interestingly, when $\ell^{*,cen} = \mathtt{t}$*, the d-PICOD problem looses its pliability. That is, it reduces to a decentralized IC problem where every user needs to decode all messages not in its side information set – a setting knows as data exchange problem. Our result recovers the previously result from [11]. However, by using the recent result on the "MDS condition" in [26], we provide a sufficient condition on the field size of the MDS code used by our achievable scheme, which was not known before.*

By Proposition 12 next we show that for $\mathtt{m} \leq 5$*, the optimal number of transmissions for d-PICOD*$(\mathtt{t})$ *is different from the centralized PICOD*$(\mathtt{t})$ *with the same parameter* $(\mathtt{m}, \mathsf{S}, \mathtt{t})$ *if and only if* $\mathsf{S} = \{\mathtt{s}\}$ *and* $\mathtt{m} = \mathtt{s}+\mathtt{t}$*. An intriguing open question is whether it is true for all complete–*S *PICOD*$(\mathtt{t})$ *that* $\ell^{*,dec} \neq \ell^{*,cen}$ *if and only if* $\mathsf{S} = \{\mathtt{s}\}$ *and* $\mathtt{m} = \mathtt{s} + \mathtt{t}$*.*

We can extend Theorem 5 to some non-consecutive complete–S d-PICOD$(\mathtt{t})$. The following cases are some complete–S d-PICOD$(\mathtt{t})$ that are not covered by either Theorem 5 or Theorem 6.

Proposition 9 (All users have side information size less or equal to $\lfloor \frac{\mathtt{m}-\mathtt{t}}{2} \rfloor$)**.** *For the complete–*S *d-PICOD*$(\mathtt{t})$ *with* $\mathtt{m}$ *messages and* $\mathtt{s}_{\max} := \max_{\mathtt{s}\in\mathsf{S}}\{\mathtt{s}\} \leq \lfloor \frac{\mathtt{m}-\mathtt{t}}{2} \rfloor$*, the optimal code length is* $\ell^* = \mathtt{s}_{\max} + \mathtt{t}$*.*

The proof can be found in Section 4.3.3.1.

Proposition 10 (All users have side information size greater or equal to $\lceil \frac{m-t}{2} \rceil$)**.** *For the complete–*S *d-PICOD*(t) *with* m *messages,* $s_{\min} := \min_{s \in S}\{s\} \geq \lceil \frac{m-t}{2} \rceil$ *and* $s_{\min} \neq m - t$*, the optimal code length is* $\ell^* = m - s_{\min}$.

The proofs can be found in Section 4.3.3.2.

Proposition 11 (Users with side information size in a band around $\frac{m-t}{2}$)**.** *For the complete–*S *d-PICOD*(t) *with* m *messages, let*

$$\delta := \min \left\{ s_{\max} - \lceil \frac{m-t}{2} \rceil, \lfloor \frac{m-t}{2} \rfloor - s_{\min} \right\}, \tag{4.5}$$

where $s_{\max} := \max_{s \in S}\{s\}$ *and* $s_{\min} := \min_{s \in S}\{s\}$*. If* $\left[\lfloor \frac{m-t}{2} \rfloor - \delta : \lceil \frac{m-t}{2} \rceil + \delta \right] \subseteq S$ *then the optimal code length is* $\ell^* = \min\{s_{\max} + t, m - s_{\min}\}$.

The proof can be found in Section 4.3.3.3.

Remark 9. *Propositions 9, 10 and 11 show an interesting fact: for these settings the only relevant users are those with side information sets of size closest to the "critical" middle one* $\frac{m-t}{2}$*, or the ones in a band* $\left[\lfloor \frac{m-t}{2} \rfloor - \delta : \lceil \frac{m-t}{2} \rceil + \delta \right]$ *around the "critical" middle one. The optimal code for the users in these layers satisfies all the remaining users.*

For the complete–S d-PICOD(t) problems with $m \leq 5$ messages, we have the following:

Proposition 12. *With* $m \leq 5$*, if* $S = \{s\}$ *and* $s = m - t$*, the optimal number of transmissions for the complete–*S *d-PICOD*(t) *is* $\ell^* = \frac{m}{m-1}$*. Otherwise it is the same as the centralized complete–*S *PICOD*(t) *with the same parameters* (m, S, t) *as derived in [37].*

The proof can be found in Section 4.3.4.

Remark 10. *Proposition 12 is proved by checking all complete–*S *d-PICOD*$(\mathtt{t})$ *problems. Some cases have been covered by Theorem 6 and Propositions 9, 10, 11. Therefore, we only need to check the rest of the cases that have not been covered. Unfortunately we have not been able to find a systematic way to prove the converse for general* $\mathtt{m}$*. So even our method can be applied to some cases where* $\mathtt{m} > 5$*, since the method is a case-by-case study, at this point we can not generalize our results to the general complete–*S *d-PICOD*$(\mathtt{t})$*.*

4.2.2 Converse for d-PICOD(1) with circular-arc network topology hypergraph

Theorem 7. *For a d-PICOD*(1) *with* $\mathtt{m}$ *messages and with circular-arc network topology hypergraph, the optimal number of transmissions is* $\ell^* = 2$ *if the network topology hypergraph does not contain a* 1*-factor sub-hypergraph; otherwise,* $\ell^* = \frac{\gamma}{\gamma-1}$*, where* γ *is the size of the largest 1-factor of the network topology hypergraph.*

The proof can be found in Section 4.4.

Remark 11. *Similar to the centralized case, we show that for all d-PICOD*(1) *with* $\mathtt{m}$ *messages and with circular-arc network topology hypergraph, the number of transmissions is at most 2. The difference in the decentralized setting is that the optimal number of transmissions is always strictly greater than* $\mathtt{t} = 1$*. Therefore, for the case where the 1-factor exists, the optimal number of transmissions is a rational number between* 1 *and* 2*. This is in contrast to the centralized setting, where the* ℓ^* *can only be either* 1 *or* 2*.*

4.3 Decentralized Complete–S PICOD(t) Problems

In this section we show tight bounds for those complete–S d-PICOD(t) problems whose centralized version was solved in Chapter 3.

4.3.1 Proof for Theorem 5

We proof the theorem by splitting it into various sub-cases:

1. $s_{max} + t \leq m - s_{min}$;
2. $t < m - s_{min} < s_{max} + t$; and
3. $s_{min} = s_{max} = m - t$.

For the first two cases we have $\ell^{*,cen} = \min\{s_{max} + t, m - s_{min}\} < t$. We study separately the cases $s_{max} + t \leq m - s_{min}$ (Section 4.3.1.1) and $t < m - s_{min} < s_{max} + t$ (Section 4.3.1.2). The third case we have $\ell^{*,cen} = t$; in Section 4.3.1.3 we show that in such a case we have $\ell^{*,cen} < \ell^{*,dec} = \ell^* = \frac{\binom{m}{m-t}}{\binom{m}{m-t}-1} t$, where the trivial centralized converse bound is not tight anymore for the decentralized setting.

4.3.1.1 Case $s_{max} + t \leq m - s_{min}$

For the achievable scheme we send $s_{max} + t$ messages, one at a time. This can be done in a decentralized setting since each message is in the side information set of at least one user. Therefore, such a user can transmit the message to the rest of the users in one channel use. This achievable scheme is optimal since $s_{max} + t$ is the optimal code-length for the corresponding centralized setting. We thus conclude $\ell^* = s_{max} + t$ for $s_{max} + t \leq m - s_{min}$.

4.3.1.2 Case $t < m - s_{min} < s_{max} + t$

We show that in this case a decentralized scheme with $m - s_{min}$ transmissions can satisfy all users; being $m - s_{min}$ the optimal code-length for the corresponding centralized setting, such a scheme is thus optimal. In the centralized case, the optimal code involves $m - s_{min}$ linearly independent linear combinations of *all* the messages, or alternatively a scalar linear MDS code; this is not possible in a decentralized setting as no user knows all messages.

When describing achievable schemes, we treat each message as a symbol of κ bits in the finite field $\mathbb{F}_{2^\kappa}$. In other words, we use κ channel extensions. With an abuse of notation, we also let x^ℓ denote the codeword of length ℓ symbols from the finite field $\mathbb{F}_{2^\kappa}$, and where each symbol corresponds to a transmission by a user. Therefore ℓ^* is the optimal number of transmitted symbol per message. Once normalized by the channel extension number κ, it is equivalent to the optimal number of transmission in the bit-pipe per bit in the definition of Section 2.1. A linear code for the decentralized system is thus $x^\ell = \mathbf{G}w^m$, where $\mathbf{G}$ is the code generator matrix of size $\ell \times m$ and w^m of length m is the messages vector over $\mathbb{F}_{2^\kappa}$.

For a decentralized linear code, we look for a code generator matrix $\mathbf{G} = [\mathbf{C}, \mathbf{0}]$, where $\mathbf{0}$ is a zero matrix of size $\ell^* \times (m - s_{max} - t)$ with $\ell^* = m - s_{min}$, and $\mathbf{C}$ is a matrix of size $\ell^* \times (s_{max} + t)$ that satisfies two conditions:

1. [Condition 1] each row has at most s_{max} non-zero elements, and
2. [Condition 2] all submatrices formed by any p columns, with $t \leq p \leq \ell^*$, have rank p / are full rank.

Since the encoding is done in a decentralized fashion, each row of $\mathbf{G}$ is the encoding vector used by a user. Condition 1 holds because a user knows at most s_{max} messages (in its side information set). Condition 2 is for successful decoding at the users; once the contribution of the messages in the side information set has been subtracted off from the received code, each user sees a subset of the remaining messages encoded by a full rank submatrix of p columns; the range of p is because each user must decode at least t messages, thus $t \leq p$, and at most all messages in the code that are not in the side information, thus $p \leq \ell^*$.

Note that Condition 2 is equivalent to require all $\ell^* \times \ell^*$ submatrices of $\mathbf{G}$ to be full rank. This is because any submatrix obtained by taking a subset of columns of a full rank square matrix is full rank. We therefore only look at all submatrices of size $\ell^* \times \ell^*$ and require all of them to be full rank. This condition is the so-called the *MDS-property* of a linear code of dimension ℓ^*.

In an MDS code of dimension a, every a codewords are separable, i.e., linear independent. Thus the code generation matrix of an MDS code of dimension ℓ^* satisfies the requirements we imposed here. We now show that such an MDS code generation matrix exists for our problem setting. Specifically, we show that the desired matrix $\mathbf{G}$ exists as a sparse MDS code generator matrix for sufficiently large κ, which is the field size of the elements in matrix $\mathbf{G}$.

For better explanation, we introduce the "zero pattern" matrix for the sparse MDS code generator matrix. The zero pattern matrix $\mathbf{Z} \in \{0,1\}^{(m-s_{min})\times(s_{max}+t)}$ of $\mathbf{C}$ is a matrix whose entry is 1 if the corresponding entry in $\mathbf{C}$ is 0, and 0 otherwise. Therefore, the ones in the zero pattern matrix indicate the zero pattern in the corresponding matrix $\mathbf{C}$. Consider the zero pattern matrix $\mathbf{Z}$ in Fig. Figure 6

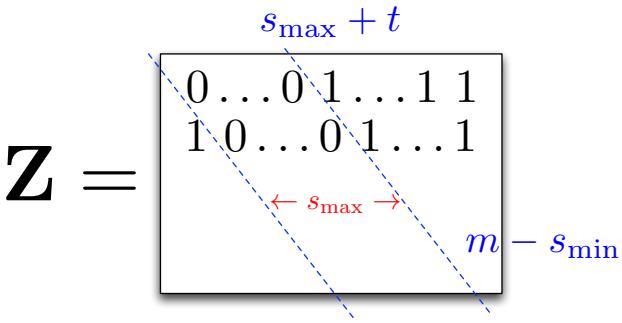

Figure 6. Zero pattern matrix **Z**. ©IEEE 2019.

constructed as following

$$z_{ij} = \begin{cases} 0, & \text{for } 2 \leq (i+j) \pmod{(s_{max}+t)} \leq s_{max}+1, \\ 1, & \text{otherwise.} \end{cases}$$

Let $Z_i := \{j \in [s_{max}+t] : z_{ij} = 1\}$ be the set of the one entries in the ith row, $|Z_i| = t, \forall i \in [m - s_{min}]$. Since $s_{max} + t > m - s_{min}$, we have $Z_i \neq Z_j$, $i \neq j$. Therefore, all Z_i can be seen as different "shifted" versions of Z_1.

For a set $P \subseteq [m - s_{min}]$, there are $|P|-1$ "shifts" in $\cap_{i\in P} Z_i$, which reduce the size of the intersection by at least $|P| - 1$. We then have the inequality

$$|P| + |\cap_{i\in P} Z_i| \leq |P| + t - (|P| - 1) = t + 1 \leq \ell^*,$$

which is known as the "MDS condition" (which is sufficient for the existence of an MDS generator matrix over some finite field [26, Eq. $*$]). Therefore, there exists a matrix $\mathbf{C}$ that satisfies conditions C1 and C2 with the specified zero pattern $\mathbf{Z}$. By [26, Thm. 1.2], a finite field of size $m - s_{\min} + s_{\max} + t - 1$ suffices. Since $\mathbf{G}$ satisfies condition C1, this code thus can be generated in a distributed way when the message size $\kappa \geq m - s_{\min} + s_{\max} + t - 1$.

After receiving the codeword of length $\ell^* = m - s_{\min}$, user u_i subtracts off the messages in its side information set A_i and is left with a linear code for the messages $W_{[s_{\max}+t]\setminus A_i}$. Condition C2 guarantees that all user can decode at least t messages that are not in their side information. Therefore all users can be satisfied by this code of length $m - s_{\min}$. This concludes the proof for this case.

4.3.1.3 Case $s_{\min} = s_{\max} = m - t$

Let $s := s_{\min} = s_{\max} = m - t$. This is the case where the trivial centralized converse bound $\ell^{*,\text{cen}} = \min\{m-s, s+t\} = t \leq \ell^*$ is not tight, and for which we want to show $\ell^* = \frac{\binom{m}{s}}{\binom{m}{s}-1} t > t = \ell^{*,\text{cen}}$.

4.3.1.3.1 Converse

An intuitive explanation for the converse proof is as follows. The $n := \binom{m}{s}$ users in the system are symmetric, i.e., by relabeling the messages we can swap any pair of users. Therefore all users have the same "chance" $1/n$ to be the one who sends part of the overall codeword x^ℓ. In the decentralized setting, the part of x^ℓ sent by a user is generated based on its own side information set, and such a transmission cannot benefit the transmitting user. Therefore, at most a fraction $\frac{n-1}{n}$ of x^ℓ can be useful for each user. Since each transmission can convey at most one message, in order to let each user decode at least t messages, the total number of transmissions satisfies $\frac{n-1}{n}\ell \geq t$.

We next provide the formal proof for the converse. Let $\ell_i\kappa$ be the number of bits sent by user $u_i, i \in [n]$, and $x^{\kappa\ell} := (x^{\kappa\ell_1}, x^{\kappa\ell_2}, \ldots, x^{\kappa\ell_n})$ be the overall codeword used for decoding by the users, with $\ell := \sum_{i\in[n]} \ell_i$. With an abuse of notation, let $x^{(\ell-\ell_i)\kappa}$ indicate the bits in the transmit codeword $x^{\ell\kappa}$ that were not sent by user $u_i, i \in [n]$.

By Fano's inequality, with $\lim_{\kappa\to\infty} \epsilon_\kappa = 0$, we have

$$\begin{aligned}
\ell\kappa\epsilon_\kappa &\geq H(W_{D_i}|x^{\ell\kappa}, W_{A_i}) = H(W_{D_i}|x^{(\ell-\ell_i)\kappa}, W_{A_i}) \\
&= H(W_{D_i}|W_{A_i}) - I(W_{D_i}; x^{(\ell-\ell_i)\kappa}|W_{A_i}) \\
&= H(W_{D_i}) - I(W_{D_i}; x^{(\ell-\ell_i)\kappa}|W_{A_i}).
\end{aligned}$$

Therefore, for $\forall i \in [n]$, we have

$$\begin{aligned}
(\ell-\ell_i)\kappa &\geq H(x^{(\ell-\ell_i)\kappa}) \geq H(x^{(\ell-\ell_i)\kappa}|W_{D_i}) \\
&\geq I(W_{D_i}; x^{(\ell-\ell_i)\kappa}|W_{A_i}) \\
&\geq H(W_{D_i}) - \ell\kappa\epsilon_\kappa \\
&\geq t\kappa - \ell\kappa\epsilon_\kappa,
\end{aligned}$$

and therefore, for large enough κ, by summing the above inequalities we obtain the converse bound

$$\ell \geq \frac{nt}{n-1} = \frac{\binom{m}{s}}{\binom{m}{s}-1} t. \tag{4.6}$$

4.3.1.3.2 Achievability

The achievability involves message splitting and random linear coding. i.e., we use a vector linear code, in contrast to the scalar linear code used in Section 4.3.1.2.

We split each message into f sub-messages, $w_i = (w_{i,1}, w_{i,2}, \ldots, w_{i,f}), i \in [m]$. The size of the sub-message is κ/f bits, which is assumed to be an integer. The parameter f will be appropriately chosen later. Each sub-message is thus on the finite field $\mathbb{F}_{2^{\kappa/f}}$. Each user uses $\ell' = \frac{f\ell}{n}$ sub-timeslots (as the messages are split into f pieces, the time slots are split into f pieces as well) to transmit. In each sub-timeslot the user transmits a linear combination of all the sub-messages it has in its side information set, i.e., at sub-timeslot h, user u_i transmits $\sum_{g \in A_i, j \in [f]} a_{gj}(h) w_{g,j}$, where the coefficients $a_{gj}(h)$ are on $\mathbb{F}_{2^{\kappa/f}}$. The linear code has generator matrix $\mathbf{G}$, which consists of $a_{gj}(h)$ for $g \in [m], j \in [f], h \in [f\ell]$, is of size $n\ell' \times mf$. Each row of $\mathbf{G}$ has at most sf nonzero entries.

For each user, among all $n\ell'$ sub-timeslots, only $(n-1)\ell'$ are useful for its decoding since the other ℓ' sub-timeslots are used for transmission by itself. Therefore, we choose ℓ' and f such that

$$(n-1)\ell' = (m-s)f,\ n = \binom{m}{s},\ \ell' = \frac{f\ell}{n}.$$

For each user, the submatrix of $\mathbf{G}$ corresponding to what all other users have sent needs to be a full rank square matrix of size $(n-1)\ell' = (m-s)f$ so that each user can successfully decode. In other

words, every submatrix of $\mathbf{G}$ formed by $(m-s)f$ columns must be full rank. Similarly to the proof in Section 4.3.1.2, the "MDS condition" on its zero-pattern matrix is as follows

$$\begin{aligned}|P| + |\cap_{i\in P} Z_i| &\leq |P| + \left((m-s) - (\lceil \frac{|P|}{\ell'} \rceil - 1)\right) f \\ &\leq n\ell' + |P| - \ell' - \frac{|P|-\ell'}{\ell'} f \\ &\leq n\ell'.\end{aligned}$$

Therefore the proposed code generator matrix $\mathbf{G}$ exists for some large enough κ. By this scheme each user decodes all the $(m-s)f$ sub-messages that are not in its side information set.

The total number of transmissions by this scheme is

$$\ell = \frac{\ell'}{f} n = \frac{1}{f} \frac{f(m-s)}{n-1} n = t \frac{n}{n-1}, \tag{4.7}$$

which coincides with the converse bound in (Equation 4.6). Therefore the achievability scheme is information theoretically optimal.

Remark 12. *Note that in this case, the d-PICOD(t) becomes a multicast decentralized IC problem, which is a special case of the data exchange problem [11]. Our results recover the results of the data exchange problem for this specific setting. The converse proof we have in Section 4.3.1.3.1 follows the same idea of the converse bounds in Section [11] (i.e., cut-set bound). Our achievability proof in Section 4.3.1.3.2, however, uses the "MDS condition" idea in Section 4.3.1.2. By the result on the "MDS*

TABLE II

FIRST 6 TRANSMISSIONS FOR $M = 4, S = t = 2$.*©IEEE 2019.*

#	*Tx*	*Code*	u_1 *decodes*	u_2 *decodes*	u_3 *decodes*	u_4 *decodes*	u_5 *decodes*	u_6 *decodes*
1	u_1	$w^1_{11} \oplus w^1_{21}$	$\emptyset$	w^1_{21}	w^1_{21}	w^1_{11}	w^1_{11}	$w^1_{11} + w^1_{21}$
2	u_2	$w^1_{12} \oplus w^1_{32}$	w^1_{32}	$\emptyset$	w^1_{32}	w^1_{12}	$w^1_{12} + w^1_{32}$	w^1_{12}
3	u_3	$w^1_{13} \oplus w^1_{43}$	w^1_{43}	w^1_{43}	$\emptyset$	$w^1_{13} + w^1_{43}$	w^1_{13}	w^1_{13}
4	u_4	$w^1_{22} \oplus w^1_{31}$	w^1_{31}	w^1_{22}	$w^1_{22} + w^1_{31}$	$\emptyset$	w^1_{31}	w^1_{22}
5	u_5	$w^1_{23} \oplus w^1_{41}$	w^1_{41}	$w^1_{23} + w^1_{41}$	w^1_{23}	w^1_{41}	$\emptyset$	w^1_{23}
6	u_6	$w^1_{33} \oplus w^1_{42}$	$w^1_{33} + w^1_{42}$	w^1_{42}	w^1_{33}	w^1_{42}	w^1_{33}	$\emptyset$

condition" in [26], we can provide a sufficient condition on field size of the code and message size κ*, which was not studied in [11].*

However, the scheme proposed in Section 4.3.1.3.2 can be suboptimal in terms the required κ*. Consider the case* $m = 4, s = t = 2$ *as an example. The proposed scheme in Section 4.3.1.3.2 splits each message into* 5 *sub-messages and the sufficient field size for the sub-message is* 31*. In other words, we have* $\kappa \geq 5\lceil \log 31 \rceil = 25$*. However, we show that there is an optimal linear code requiring smaller* κ*.*

Let us label the users as $A_1 = \{1, 2\}, A_2 = \{1, 3\}, A_3 = \{1, 4\}, A_4 = \{2, 3\}, A_5 = \{2, 4\}, A_6 = \{3, 4\}$*. Split the messages as* $w_i = \{w^h_{ij} : i \in [4], j \in [3], h \in [5]\}$ *and* $w^h_{ij} \in \{0, 1\}$*. Therefore each message* $w_i, i \in [m]$ *is* 15 *bits.*

We list the first 6 *(i.e., for* $h = 1$*; the same can be done for all* $h \in [5]$*) transmissions in Table II. After the first* 30 *transmissions (for all* $h \in [5]$*), we have the last* 6 *transmissions shown in Table III and Table IV. In total this scheme uses* 36 *transmissions. Note for the first* 30 *transmissions, after each group of* 6 *transmissions, each user can decode* 4 *sub-messages and obtain a sum of* 2 *sub-messages that it will still need to decode. Among the last 6 transmissions, each transmission allows 5 users, which are*

TABLE III

LAST 6 TRANSMISSIONS FOR $M = 4, S = t = 2$*, CODEWORDS AND DECODING MESSAGES AT USERS* U_1, U_2, U_3*.* ©*IEEE 2019.*

#	*Tx*	*Code*	u_1 *decodes*	u_2 *decodes*	u_3 *decodes*
31	u_1	$w^1_{11} \oplus w^1_{12} \oplus w^1_{13} \oplus w^1_{22} \oplus w^1_{23}$	$\emptyset$	w^1_{23}, w^1_{41}	w^1_{22}, w^1_{31}
32	u_2	$w^2_{11} \oplus w^2_{12} \oplus w^2_{13} \oplus w^2_{31} \oplus w^2_{33}$	w^2_{33}, w^2_{42}	$\emptyset$	w^2_{22}, w^2_{31}
33	u_3	$w^3_{11} \oplus w^3_{12} \oplus w^3_{13} \oplus w^3_{41} \oplus w^3_{42}$	w^3_{33}, w^3_{42}	w^3_{23}, w^3_{41}	$\emptyset$
34	u_4	$w^4_{21} \oplus w^4_{22} \oplus w^4_{23} \oplus w^4_{32} \oplus w^4_{33}$	w^4_{33}, w^4_{42}	w^4_{23}, w^4_{41}	w^4_{22}, w^4_{31}
35	u_5	$w^5_{21} \oplus w^5_{22} \oplus w^5_{23} \oplus w^5_{42} \oplus w^5_{43}$	w^5_{33}, w^5_{42}	w^5_{23}, w^5_{41}	w^5_{22}, w^5_{31}
36	u_6	$w^1_{42} \oplus w^2_{41} \oplus w^3_{31} \oplus w^4_{43} \oplus w^5_{32}$	w^1_{33}, w^1_{42}	w^2_{23}, w^2_{41}	w^3_{22}, w^3_{31}

TABLE IV

LAST 6 TRANSMISSIONS FOR $M = 4, S = t = 2$*, CODEWORDS AND DECODING MESSAGES AT USERS* U_4, U_5, U_6*.*©*IEEE 2019.*

#	*Tx*	*Code*	u_4 *decodes*	u_5 *decodes*	u_6 *decodes*
31	u_1	$w^1_{11} \oplus w^1_{12} \oplus w^1_{13} \oplus w^1_{22} \oplus w^1_{23}$	w^1_{13}, w^1_{43}	w^1_{12}, w^1_{32}	w^1_{11}, w^1_{21}
32	u_2	$w^2_{11} \oplus w^2_{12} \oplus w^2_{13} \oplus w^2_{31} \oplus w^2_{33}$	w^2_{13}, w^2_{43}	w^2_{12}, w^2_{32}	w^2_{11}, w^2_{21}
33	u_3	$w^3_{11} \oplus w^3_{12} \oplus w^3_{13} \oplus w^3_{41} \oplus w^3_{42}$	w^3_{13}, w^3_{43}	w^3_{12}, w^3_{32}	w^3_{11}, w^3_{21}
34	u_4	$w^4_{21} \oplus w^4_{22} \oplus w^4_{23} \oplus w^4_{32} \oplus w^4_{33}$	$\emptyset$	w^4_{12}, w^4_{32}	w^4_{11}, w^4_{21}
35	u_5	$w^5_{21} \oplus w^5_{22} \oplus w^5_{23} \oplus w^5_{42} \oplus w^5_{43}$	w^5_{13}, w^5_{43}	$\emptyset$	w^5_{11}, w^5_{21}
36	u_6	$w^1_{42} \oplus w^2_{41} \oplus w^3_{31} \oplus w^4_{43} \oplus w^5_{32}$	w^4_{13}, w^4_{43}	w^5_{12}, w^5_{32}	$\emptyset$

all users except the user who generates the code, to resolve one sum of two sub-messages that still needs to be decoded. Therefore, 6 *transmissions let all* 6 *users decode the 5 sum of two sub-messages that they got from the first 30 transmissions. In total we use 36 transmissions to convey 2 messages for each user, with each message of size* 15 *bits. The number of transmissions, in multiple of the message size, is* $\ell = \frac{36}{15} = \frac{\binom{4}{2}}{\binom{4}{2}-1}2 = \frac{n}{n-1}t = \ell^*$*, thus proposed scheme is optimal in terms of number of transmissions.*

Note that this scheme only needs message size to be $\kappa = 15$*, which is less than the one proposed in Section 4.3.1.3.2. Indeed, the MDS condition only provides a sufficient condition of the minimum field size and not a necessary one. Deriving a lower bound on the field size such that a linear code with vanishing error exists is an interesting open question for further study.*

4.3.2 Proof for Theorem 6

Also for this complement-consecutive complete–S d-PICOD(t), where $S = [0 : m-1] \setminus [s_{\min} : s_{\max}]$ for some $0 < s_{\min} \leq s_{\max} < m - t$, we need to show a decentralized achievable scheme that meet the trivial centralized converse bound.

In the centralized case, the achievable scheme consists of two scalar linear codes: one to serve all the users with side information of size in $[0 : s_{\min} - 1]$, and the other to serve all the users with side information of size in $[s_{\max} + 1 : m - t]$. Also for the decentralized scheme, we separate the users into these two groups: $\mathcal{U}_1 = \{u_i : |\mathcal{A}_i| \in [0 : s_{\min} - 1]\}$ and $\mathcal{U}_2 = \{u_i : |\mathcal{A}_i| \in [s_{\max} + 1 : m - t]\}$. The analysis of the achievability scheme is divided into two parts: $s_{\min} - 1 + t < s_{\max} + 1 = m - t$, and the remaining case.

4.3.2.1 Case $s_{\min} - 1 + t < s_{\max} + 1 = m - t$

In this case the decentralized scheme is different from the centralized one proposed in [19]. This is because the users in $\mathcal{U}_2$ are a consecutive complete–S case as discussed in Section 4.3.1.3, where the trivial centralized converse bound is not tight. Therefore, we can not treat the problem of serving the users in $\mathcal{U}_1$ and $\mathcal{U}_2$ as two independent subproblems, as the centralized scheme does.

The decentralized achievability scheme takes two steps:

- Step 1: Send messages $W_{[s_{\min}-1+t]}$ one by one. All users in $\mathcal{U}_1$ are satisfied with $s_{\min} - 1 + t \geq t$ (since $s_{\min} > 0$) messages are sent in this step. Since all users in $\mathcal{U}_2$ have side information sets of size $s_{\max} + 1 = m - t$, there exists at least one user in $\mathcal{U}_2$ that has been satisfied in the first step. This step takes $s_{\min} - 1 + t$ transmissions.
- Step 2: The user in $\mathcal{U}_2$ that was satisfied in Step 1 has knowledge of all messages and can thus act as the centralized transmitter of the corresponding centralized PICOD(t) [37], sending t linearly independent linear combinations of all messages. Since all users in $\mathcal{U}_2$ have t messages not in the side information, by having t linear independent linear combinations of all messages, all remaining users in $\mathcal{U}_2$ are satisfied. This step takes t transmissions.

It thus takes in total $s_{\min} - 1 + t + t = |S| + 2t - 2$ number of transmissions to satisfy all users.

4.3.2.2 Other Case

The achievable scheme in Section 4.3.1.1 satisfies the users in $\mathcal{U}_1$ with $s_{\min} - 1 + t$ transmissions. The achievable scheme in Section 4.3.1.2 satisfies the users in $\mathcal{U}_2$ with $m - (s_{\max} + 1)$ transmissions. Therefore, the total number of transmissions is $s_{\min} - 1 + t + m - s_{\max} - 1 = |S| + 2t - 2$.

Note that $\ell = m$ is a trivially achievable number of transmissions for the decentralized setting as well, we conclude for complement-consecutive complete–S d-PICOD(t) the optimal number of transmissions is $\ell^* = \min\{m, |S| + 2t - 2\}$, which is the same as the corresponding centralized setting.

4.3.3 Extensions of Theorem 5

Similar to the centralized case, there are cases where we can drop some users from the system while maintain the optimality of the original bounds. As we did in the centralized case, these users are called *non-critical users*, which do not affect the optimal code length. Therefore, we can add or drop these non-critical users without changing the optimal code-length. This allow us to extend Theorem 5 to some *non-consecutive* or *non-complement-consecutive* complete–S d-PICOD(t) cases.

4.3.3.1 Proof of Proposition 9

The converse for the centralized setting is $s_{max} + t$. The decentralized achievable scheme transmits $s_{max} + t$ messages, one at a time. This is a feasible decentralized scheme since all messages are in the side information of at least one user. Therefore we have $\ell^* = s_{max} + t$ for this case.

4.3.3.2 Proof of Proposition 10

The converse for the centralized setting is $m - s_{min}$. The achievable scheme in Section 4.3.1.1 only needs the users with side information of size s_{max}. Thus the achievable scheme is applicable in the non-consecutive case here as well. Moreover, note that the set users of the consecutive case studied in Section 4.3.1.1 is a superset of the set of the users in this case, the achievable scheme can satisfy all users here as well. Therefore, we have $\ell^* = m - s_{min}$.

4.3.3.3 Proof of Proposition 11

The converse depends only on the users with side information of size in $[\lfloor \frac{m-t}{2} \rfloor - \delta : \lceil \frac{m-t}{2} \rceil + \delta]$. The code that satisfies the complete–$[\lfloor \frac{m-t}{2} \rfloor - \delta : \lceil \frac{m-t}{2} \rceil + \delta]$ PICOD(t) also satisfies all the users with the larger size of side information set. If $s_{\min} \leq \lfloor \frac{m-t}{2} \rfloor - \delta$, we have $s_{\max} = \lceil \frac{m-t}{2} \rceil + \delta$. This case is similar to the one in Proposition 9. We transmit $s_{\max} + t$ messages one at a time. If $s_{\max} \geq \lceil \frac{m-t}{2} \rceil + \delta$, we have $s_{\min} = \lfloor \frac{m-t}{2} \rfloor - \delta$. This case is similar to the one in Proposition 10. We adopt the achievable scheme in Section 4.3.1.1, which uses $m - s_{\min}$ transmissions.

4.3.4 Proof of Proposition 12

Proposition 12 states that for the complete–S d-PICOD(t) cases not covered by the results in the previous sections and with $m \leq 5$ messages, the trivial centralized converse bound is information theoretically optimal for the decentralized setting as well. If the optimal centralized achievable scheme is also feasible in the decentralized setting, then the trivial centralized converse bound is then obviously tight. This is the case for those cases where the centralized achievability scheme involves sending messages one by one, i.e., when optimal number of transmissions is $\ell^* = \ell^{*,\text{cen}} = \min\{m, s_{\max} + t\}$ (which corresponds the cases: (a) $m = 4, S = \{0, 2\}, t = 2$, (b) $m = 5, S = \{0, 1, 3\}, t = 2$, and (c) $m = 5, S = \{0, 2, 3\}, t = 2$). Thus, we only need to consider the cases where $\ell^{*,\text{cen}} < \min\{m, s_{\max} + t\}$; Table Table V lists the optimal codes for those cases.

Remark 13. *Our achievable schemes in Section 4.3.1.3 use vector linear index code (while the corresponding centralized setting used a scalar linear index code). An interesting question is whether vector index codes are necessary to achieve optimality in the decentralized setting. From the definition of scalar index code in Section 2.1, a code is scalar if it operates over $\mathbb{F}_{2^\kappa}$, in other words, $f = 1$. Therefore, for*

TABLE V

OPTIMAL CODES FOR THE OTHER CASES OF COMPLETE–S d-PICOD(t) WITH $M \leq 5$ MESSAGES. ©IEEE 2019.

$m = 4$	$S = \{1, 3\}$	$t = 1$	$w_1 \oplus w_2$, $w_2 \oplus w_3$, $w_3 \oplus w_4$
$m = 5$	$S = \{0, 3\}$	$t = 1$	w_1, $w_2 \oplus w_3$, $w_3 \oplus w_4$
	$S = \{0, 3\}$	$t = 2$	w_1, $w_2 \oplus w_3$, $w_3 \oplus w_4$, w_5
	$S = \{1, 4\}$	$t = 1$	w_1, w_2, $w_3 \oplus w_4 \oplus w_5$
	$S = \{1, 3\}$	$t = 2$	$w_1 \oplus w_2$, $w_2 \oplus w_3$, $w_3 \oplus w_4$, $w_4 \oplus w_5$
	$S = \{1, 3, 4\}$	$t = 1$	$w_1 \oplus w_2$, $w_2 \oplus w_3$, $w_3 \oplus w_4$, $w_4 \oplus w_5$
	$S = \{0, 2, 4\}$	$t = 1$	w_1, $w_2 \oplus w_3$, $w_3 \oplus w_4$, $w_4 \oplus w_5$
	$S = \{1, 2, 4\}$	$t = 1$	$w_1 \oplus w_2$, $w_2 \oplus w_3$, $w_3 \oplus w_4$, $w_4 \oplus w_5$

a scalar index code, the number of transmissions is always an integer. The number of transmissions by each user defined in (Equation 4.1) *are integers and the overall codeword length ℓ is also an integer. In the case $s_{\min} = s_{\max} = m - t$, the converse bound gives $\ell^* \geq \frac{nt}{n-1}$, which is not an integer in general. Thus a scalar index code can not achieve $\frac{nt}{n-1}$ in general. For the case $s_{\min} = s_{\max} = m - t$, a vector index code is thus necessary to achieve optimality.*

4.4 Circular-arc PICOD(1)

Theorem 7 provides the information theoretical optimality of the d-PICOD(1) with circular-arc network topology hypergraph. We split the problem into two cases: 1) the circular-arc does not have a 1-factor, analyzed in in Section 4.4.1, in which case we show that the optimal number of transmissions is 2; and 2) the circular-arc has a 1-factor, analyzed in in Section 4.4.2, in which case we show that the optimal number of transmissions is $\frac{\gamma}{\gamma-1}$, where γ is the size of the largest 1-factor. For each case we propose schemes of achievability and converse and show that they coincide.

4.4.1 Case 1: a 1-factor does not exist

In the centralized setting, $\ell^{*,\text{cen}} = 2$ when the 1-factor does not exist. We show that this is still optimal in the decentralized setting. Specifically, we show that the proposed achievable scheme in Section 3.7 for the centralized circular-arc PICOD(1) is still feasible in the corresponding decentralized setting with a small modification.

Remark 14 (Example when a 1-factor does not exist)**.** *To highlight the idea of the proof, we provide here a toy example. The general achievable scheme is the same as [19, Algorithm 1]. The extra work we need to do here is to show that this scheme is also feasible in the circular-arc d-PICOD*(1).

Consider the case with $n = 5$ *users and* $m = 5$ *messages, with* $A_i = [i : (i+2) \pmod 5], i \in [5]$, *(each user has* 3 *messages in its side information set).*

In the centralized case, following [19, Algorithm 1] the centralized transmitter sends $w_5 \oplus w_2$ *as the first transmission, and* w_4 *as the second transmission. This centralized scheme is feasible in the decentralized case, i.e., user* u_5 *can do the first transmission, and user* u_4 *the second transmission.*

In general, in order to show that the centralized scheme is feasible in the corresponding decentralized setting, we must find a set of messages such that the following holds:

1. *[Condition 1] no two messages in the set are in the side information set of the same user, and*
2. *[Condition 2] the sum of the messages in the set satisfies the maximal number of users.*

Condition 1 guarantees that there exists one user whose side information set contains all the messages in the set; the summation of all the messages in such a set is the first transmission. The second transmission is a summation of another set of messages that can satisfy the remaining users who were not satisfied

by the first transmission; its existence is guaranteed by the circular-arc network topology hypergraph structure.

For our specific example we have:

- *First we find the first message that can satisfy user* u_1 *but not* u_5*; we find it to be* w_5.
- *We then determine the users that* w_5 *can satisfy; these users are* u_1 *and* u_2.
- *Next we try to find a message that can satisfy* u_3*; we realize that* w_2 *can satisfy* u_3 *and* u_4.
- *Note that there are no more messages that can be added into the set such that Condition 1 still holds; we set the first transmission to be* $w_5 + w_2$ *(which can be sent by user* u_5 *as* $\{2,5\} \subset A_5$*).*
- *The remaining unsatisfied user is* u_5*, who can be satisfied by receiving* w_4 *(which can be sent by* u_4*, for example).*

For completeness, we briefly show the achievable scheme proposed as [19, Algorithm 1] in the following.

4.4.1.1 First transmission

The first step of the achievable scheme is shown as Algorithm 1 next. Recall that the hyperedges in the network topology hypergraph represent the messages in the system. We drop those edges that are proper subsets of the union of other edges, obtaining the edge set $\mathcal{E}$. These are the messages we are going to use in the achievable schemes. Note that every vertex is incident to at least one of the remaining edges. The remaining messages are sufficient to satisfy all users. We relabel the users such that the first edge E_1 in $\mathcal{E}$ starts at v_1, i.e., $E_1 = \{v_1, v_2, \ldots, v_{|E_1|}\}$.

Algorithm 1: Algorithm for finding $\mathcal{E}^{(1)}$ in the first transmission.

Data: User set: $V = \{v_1, \ldots, v_n\}$, message set: $\mathcal{E} = \{E_1, \ldots, E_m\}$ where $E_1 = \{v_1, v_2, \ldots, v_{|E_1|}\}$.
Result: Message set: $\mathcal{E}^{(1)} = \{E_{1^{(1)}}, \ldots E_{e^{(1)}}\}$.
Initialization: set $i = |E_1| + 1$, $\mathcal{E}^{(1)} = \{E_1\}$.
while $i \leq n$ **do**
  Seek an edge that starts at v_i and does not contain v_1, i.e., an edge $\{v_i, \ldots, v_j\}$, for some $j \leq n$;
  if *Such an edge is found* **then**
    Let $\mathcal{E}^{(1)}$ include the edge found;
    i becomes the index of the vertex right after the found edge, that is, $i = j + 1$;
  else
    $i = i + 1$;
  end
end

We find a set of messages $\mathcal{E}^{(1)} \subseteq \mathcal{E}$ for the first transmission by using Algorithm 1. Let $\mathcal{E}^{(1)} = \{E_1, E_2, \ldots, E_e\}$ and $E_i = \{v_{i1}, v_{i2}, \ldots, v_{i|E_i|}\}$. In the first transmission we send the sum of the messages in $\mathcal{E}^{(1)}$, i.e., $\sum_{i=1}^{e} w_i$. By Algorithm 1, all edges in $\mathcal{E}^{(1)}$ are disjoint, i.e., they pairwise do not have common incident vertex. Therefore, the users either have all of these messages in the side information, or all but one of the messages in the side information.

The users who have all but one of these messages in their side information are shown as the vertices in $\cup_{E_i \in \mathcal{E}^{(1)}} E_i \setminus (E_{1^{(1)}} \cap E_e)$. They are the users that will be satisfied by the first transmission.

The users that were not satisfied by the first transmission have the corresponding vertices contained in $G := U \setminus (\cup_{\mathcal{E}^{(1)}} E_{i^{(1)}}) = \cup_{i=1}^{|\mathcal{E}^{(1)}|} G_i$, where $G_i = \{v_{i|E_i|+1}, \ldots, v_{(i+1)1-1}\}$. Since a 1-factor does not exist, there must exists a user who has all of these messages in its side information, that is, $G \neq \emptyset$. That user can perform the summation and the first transmission.

4.4.1.2 Second transmission

The unsatisfied users after the first transmission can be seen as the users that are in the "gap" between the edges $\mathcal{E}^{(1)}$ chosen by Algorithm 1. We show that one transmission can satisfy all the remaining unsatisfied users and it can be generated by a user in the system.

By Algorithm 1, for all $i \in [e]$, there exists $E_{i'}$ such that $G_i \subset E_{i'}$. This is because all vertices in G_i are incident to at least one $E \in \mathcal{E}$. If no such $E_{i'}$ exists then there exists $E_{i'} \notin \mathcal{E}^{(1)}$ such that $E_{i'} \cap E_i = \emptyset$ and $E_{i'} \cap G_i \neq \emptyset$. However, by Algorithm 1, such $E_{i'} \in \mathcal{E}^{(1)}$, which is a contradiction.

Moreover, since in $\mathcal{E}$ all edges are not proper subsets of the union of the other edges, we have $E_{i'} \cap E_{j'} = \emptyset$, $\forall i \neq j$. Therefore, we find a set of edges $\mathcal{E}^{(2)} = \{E_{1'}, \ldots, E_{1'}\}$ such that $G \subseteq \cup_{E_i \in \mathcal{E}^{(2)}} E_i$.

In the second transmission, we send the sum $\sum_{j=1}^{e} w_{j'}$. All users in G have all but one messages in the sum in their side information. Thus all the remaining users are satisfied by the second transmission. Also, since there is not 1-factor, $G \subset V$. There exists one user who has all the messages in $\mathcal{E}^{(2)}$ in its side information. The proposed summation can be computed in the decentralized setting. All the users are satisfied with two transmissions.

We conclude $\ell^* = 2$ for the d-PICOD(1) with circular-arc network topology hypergraph that has no 1-factor, as in the corresponding centralized case.

4.4.2 Case 2: a 1-factor exists

In the centralized setting when 1-factor exists we have $\ell^{*,\text{cen}} = t = 1$, which is clearly not feasible in a decentralized case. We show next that $2 \geq \ell^* = \ell^{*,\text{dec}} > 1$, by developing both converse and achievability bounds that differ from their centralized counterparts.

4.4.2.1 Converse

For the PICOD(1) whose network topology hypergraph has a 1-factor, let $\hat{\mathcal{E}} \subset \mathcal{E}$ be the subset of the edges of the network topology hypergraph that represent the messages that are desired by at least one user. In other words, hyperedge $\mathsf{E}_\mathfrak{i} \in \hat{\mathcal{E}}$ if and only if $w_\mathfrak{i}$ is the desired message of a user. $\hat{\mathcal{E}}$ is a spanning sub-hypergraph of the network topology hypergraph, since every user has at least one message known in $\hat{\mathcal{E}}$.

If $\hat{\mathcal{E}}$ is not 1-regular, i.e., there exists one user who has two messages in $\hat{\mathcal{E}}$ that are not in its side information, by the converse argument for the case where 1-factor does not exist, $\ell^* \geq 2$.

If $\hat{\mathcal{E}}$ is 1-regular, i.e., $\hat{\mathcal{E}}$ is a 1-factor, the converse argument is as follows: choose $|\hat{\mathcal{E}}|$ users with different desired messages; for all $|\hat{\mathcal{E}}|$ messages that are desired in the system, each user has all but one message in its side information. For these $|\hat{\mathcal{E}}|$ users, the converse bound for the decentralized complete–$\{\mathfrak{m}-1\}$ PICOD(1), where $\mathfrak{m} = |\hat{\mathcal{E}}|$, applies. To satisfy these $|\hat{\mathcal{E}}|$ users, $\frac{|\hat{\mathcal{E}}|}{|\hat{\mathcal{E}}|-1}$ transmissions are needed. Therefore, to satisfy all users in the system, we have $\ell^* \geq \frac{|\hat{\mathcal{E}}|}{|\hat{\mathcal{E}}|-1}$. $|\hat{\mathcal{E}}|$ is an integer greater than 1. $\frac{|\hat{\mathcal{E}}|}{|\hat{\mathcal{E}}|-1}$ is a decreasing function on $|\hat{\mathcal{E}}|$. Recall that γ is the size of the largest 1-factor in network topology hypergraph . We have $\ell^* \geq \frac{\gamma}{\gamma-1}$.

4.4.2.2 Achievability

To highlight the idea of the proposed scheme, we provide here a toy example.

Remark 15 (Example when a 1-factor exists)**.** *Consider the case with* $\mathfrak{n} = 6$ *users and* $\mathfrak{m} = 6$ *messages, with* $\mathsf{A}_\mathfrak{i} = [\mathfrak{i} : (\mathfrak{i}+3) \pmod 6]$*, (each user has* 4 *messages in its side information set). In the centralized setting, one transmission, for example* $w_1 + w_3 + w_5$*, is sufficient to satisfies all users. However, this is not feasible in the decentralized setting as no users knows all three messages* w_1, w_3, w_5*. Note that in*

this case we have a 1-factor of size $\gamma = 3$; the converse bound is $\ell^* \geq 3/2$; we show next an achievable scheme that uses 3 transmissions to convey 2 messages to each user.

Let us split the messages as $w_i = (w_{i1}, w_{i2}), w_{ij} \in \mathbb{F}_{2^\kappa}, i \in [6], j \in [2]$. As desired message assignments, let $d_1 = d_6 = 5$, $d_2 = d_3 = 1$, $d_4 = d_5 = 3$. The 3 transmissions (each involving sub-messages that are half the size of a message) are:

$$x_1 = \alpha_{11}w_{11} + \alpha_{12}w_{12} + \alpha_{13}w_{31} + \alpha_{14}w_{32}, \text{ generated by } u_1,$$

$$x_2 = \alpha_{21}w_{31} + \alpha_{22}w_{32} + \alpha_{23}w_{51} + \alpha_{24}w_{52}, \text{ generated by } u_3,$$

$$x_3 = \alpha_{31}w_{11} + \alpha_{32}w_{12} + \alpha_{33}w_{51} + \alpha_{34}w_{52}, \text{ generated by } u_5,$$

where $\alpha_{ij}, i \in [3], j \in [4]$ are drawn independently uniformly at random over $\mathbb{F}_{2^\kappa}$. For each user, there are two unknown sub-messages as the desired messages that are involved in a random linear combinations, while the other 4 sub-messages are already in the side information sets (thus can be subtracted off). Eventually, each user gets two random linear combinations of two desired messages. With probability that can be made as close to one as desired for sufficiently large κ, these two random linear combinations are linearly independent. The users are thus able to decode two sub-messages.

This achievable scheme allows all users to recover the two sub-messages that compose the desired message by using three transmissions (each of size of a sub-message), thus achieves $\ell = \frac{3}{2}$.

Let the number of desired messages be m'. If the edges of the desired messages is a 1-factor of the network topology hypergraph, all users have all but one of these messages in their side information. Following the achievability of the complete–$\{m' - 1\}$ d-PICOD(1) with $m = m'$, we have $\ell^* \leq \frac{m'}{m'-1}$.

Therefore, by choosing the desired messages of the users such that the corresponding hyperedges are the largest 1-factor of the network topology hypergraph , we can achieve $\ell = \frac{\gamma}{\gamma-1}$ using the achievable scheme of the complete–$\{\gamma-1\}$ d-PICOD(1) with $\mathfrak{m} = \gamma$.

We conclude $\ell^* = \frac{\gamma}{\gamma-1}$, where γ is the size of the largest 1-factor, for the d-PICOD(1) with circular-arc network topology hypergraph that has 1-factor. Together with the result in Section 4.4.1, we conclude the proof of Theorem 7.

CHAPTER 5

INDIVIDUALLY SECURE PICOD(1) WITH CIRCULAR-ARC NETWORK TOPOLOGY HYPERGRAPH

This chapter we study the individual information theoretical security problem for a special class of PICOD(1) problem with circular-arc network topology hypergraph.

This chapter studies the PICOD problem where users are subject to a *individual security constraint*. In particular, the following spacial class of private PICODs is investigated: 1) the side information structure is circular, and 2) each user can decode one and only one message. The first condition is a special case of the PICOD(1) with circular-arc network topology hypergraph studied in Chapter 3, for which an optimal solution was given without the privacy constraint. The second condition was first studied in [25] and was motivated by the need to keep content privacy is some distribution networks.

We propose both converse and achievable bounds. The proposed achievable scheme not only strictly outperforms the one in [25] for some values of the system parameters, but it is also information theoretically optimal in some settings. For the remaining cases, the proposed linear code is shown to require at most one more transmission than the converse bound derived by restricting the sender to only use linear codes.

This chapter has appeared in [38].

5.1 Individual Security and Circular Shift Side Information

5.1.1 Individual Security

The model follows the general PICOD model with m messages, n users, and t number of desired messages for each user. Each user has side information set, indexed by A. We do not repeat the channel model here as it is stated in Chapter 3. The extra individual information theoretical security constraint is defined as the following: The individual security is modeled here as follows: user u_j can not decode any particular message other than the t messages indexed by D_j. Specifically, we impose that for all $j \in [n]$,

$$\begin{aligned} &H(w_i|x^{\kappa\ell}, W_{A_j}, \mathcal{A}) \\ \geq &H(w_i) - \kappa\epsilon, \forall i \in [m] \setminus (D_j \cup A_j). \end{aligned} \tag{5.1}$$

A code is called *valid* for the individual secure $(n, m, \mathcal{A})$ PICOD(t) if it allows each user to decode its desired messages listed in D and satisfies the condition in (Equation 5.1). The goal is to find a valid code and a desired message assignment that result in the smallest possible codelength, i.e.,

$$\ell^\star := \min\{\ell : \exists \text{ a valid } x^{\kappa\ell} \text{ for some } \kappa\}. \tag{5.2}$$

Finally, if the encoding function at the sender is restricted to be a linear map from the message set, the length of shortest possible such valid codewords is denoted as $\ell^\star_{\text{lin}}$.

5.1.2 Size-s circular-h shift Side Information

We shall consider the $(n, m, \mathcal{A})$ individual secure PICOD(1) with a special side information set structure: the sets in $\mathcal{A}$ are size-s circular-h shift of the message set. More precisely, The side information set of user u_i is of the form

$$A_i = \{(i-1)h + 1, \ldots, (i-1)h + s\}, \tag{5.3}$$

for $i \in [n]$ where all indices are intended modulo the size of the message set, i.e., denoted as $(\text{mod } m)$ when needed, where $0 \leq s \leq m - t$ and $h \geq 1$, here $t = 1$.

Let $g := \gcd(m, h)$. In this private PICOD(1) there are $n = m/g$ users, since all users have distinct side information sets. Note that the size-s circular-h shift side information setup is a special case of the side information structure with *circular-arc*. Also, the model studied in [25] is the special case when $g = 1$ (and thus $n = m$).

5.2 Main Result

For the size-s circular-h shift side information private PICOD(1) problem, we have the following main result.

Theorem 8. *For the private PICOD(1) where the side information sets are as in* (Equation 5.3) *we have the following.*

Impossibility: when m is odd, $g = 1$, and either $s = m - 2$ or $s = 1$, a valid code does not exists (i.e., it is not possible to satisfy the privacy constraint).

For the remaining possible cases, we have:

- *For* $s \geq m/2$*, and either* $1 \leq s < m/2, g \geq 3$*, or* $1 \leq s < m/2, s \neq 2, g = 2$

$$\ell^* = \begin{cases} 1, & \textit{if the NTH has a } 1\textit{-factor,} \\ 2, & \textit{otherwise.} \end{cases} \tag{5.4}$$

- *For* $1 \leq s < m/2$*, and either* $g = 1$ *or* $s = g = 2$

$$\lceil \lfloor \frac{m}{s} \rfloor / 2 \rceil \leq \ell^\star_{\text{lin}} \leq \begin{cases} \lceil \lfloor \frac{m}{s} \rfloor / 2 \rceil, & \frac{m}{s} \in \mathbb{Z}, \\ \lceil \lfloor \frac{m}{s} \rfloor / 2 \rceil + 1, & \frac{m}{s} \notin \mathbb{Z}. \end{cases} \tag{5.5}$$

A few observations are in order. When $s \geq m/2$, the achievable scheme provided in [25] is indeed information theoretical optimal given (Equation 5.4), which is our converse bound in Chapter 3 for the case without privacy constraint. Therefore, our main contribution in Theorem 8 is three-fold compared to [25]: 1) for $s \geq m/2$ we provide information theoretic optimality of the scheme in [25]; 2) for $s < m/2$ we provide a new achievable scheme, and show it is almost linear optimal; 3) we generalize the side information structure to any $g > 1$.

In (Equation 5.5), if we fix s and g, $\lfloor \frac{m}{s} \rfloor$ is monotonic in the message set size m. One interesting observation is that, although the lower bound on $\ell^\star_{\text{lin}}$ is monotonic with m, the upper bound is not. For instance, consider the case $s = 2, g = 1$; when $m = 10$ or $m = 12$, we have $\ell^\star_{\text{lin}} \leq 3$, while when $m = 11$ we have $\ell^\star_{\text{lin}} \leq 4$. In other words, from the point of $m = 11$, both increasing and decreasing the message set size may result in an increase of the required number of transmissions. Note that this is the point where the upper and the lower bounds differ. It is not clear at this point whether this means the

achievable scheme here is not optimal, or the optimal private *linear* PICOD solution is not monotonic in m.

5.3 Proof of Theorem 8

We divide the proof of Theorem 8 into various cases. Specifically, the impossibility result is proved in Section 5.3.1, the case $s < m/2, g = 1$ in Section 5.3.2, and the case $s < m/2, g = s = 2$ in Section 5.3.3. The schemes that achieve (Equation 5.4) are in Section 5.3.4.

5.3.1 Impossible Cases

First we show that in some cases the privacy constraint can not be satisfied. The proof of the same under a linear encoding constraint was provided in [25]. Here we provide a simple information theoretic proof of the same. The main idea is to proof the existence of a "decoding chain" (as defined in Chapter 3) regardless of the choices of the desired messages at the users. This "decoding chain" technique was used for the converse proof of so called consecutive complete–S PICOD(t). Since this argument does not rely on any assumption on the encoding function at the server, the resulting bound is truly information theoretical (as opposed to a form of 'restricted converse').

5.3.1.1 Case m is odd, $s = m - 2$, and $g = 1$

User u_i has two possible choices for its desired message (because all the others are in its side information set); these messages are $d_i = (i + s) \pmod m$ or $d_i = (i - 1) \pmod m$. If $d_i = (i + s) \pmod m$, by decoding w_{d_i}, user u_i can mimic $u_{(i-1) \pmod m}$ since $A_{(i-1) \pmod m} \subset \{(i + s) \pmod m\} \cup A_i$. Therefore, user u_i can decode $w_{d_{(i-1) \pmod m}}$. To make sure user u_i can decode only one message, we need $d_{(i-1) \pmod m} \in A_i$ so that user u_i does not decode another message that is not in its side information set. We thus have $d_i \in A_{(i-1) \pmod m}$ and $d_{(i-1) \pmod m} \in A_i$ can mimic

each other. We say that two user mimicking each other form a "loop". The same argument holds for the other choice of d_i as well. To make sure all users can decode one message only, every user must be in a "loop". However, one user can be in only one loop. Thus, there must be one user that is not contained in any loop because here we have taken m to be odd. Therefore, there exists one user that can mimic another user and thus decode two messages, which violates the privacy constraint.

5.3.1.2 Case m is odd, $s = 1$, and $g = 1$

User u_i, by decoding its desired message $d_i = j, j \neq i$, can mimic user u_j and thus also decode d_j. To make sure user u_i can decode only one message, we must have $d_j = i$. Therefore user u_i and u_j form a "loop". Similarly, every user can be in only one loop. We need all users to be in a loop to make sure that every user can decode at most one message. Since m is odd, this is impossible. Thus, there must exists one user that can decode two messages, which violates the privacy constraint.

5.3.2 Case $s < m/2$ and $g = 1$ (here $m = n$)

5.3.2.1 Achievability

Let $m = 2sq + r$ for some $q, r \in \mathbb{Z}$ such that $0 \leq r < 2s$, i.e., r is the remainder of m modulo $2s$, and q is the maximum number of users who can have disjoint side information sets. We can have $2q + \lfloor \frac{r}{s} \rfloor$ groups of s users such that the users in each group have at least one message in common in their side information sets. Also, $r - s\lfloor \frac{r}{s} \rfloor$ is the number of users that are not contained in any of these groups.

The intuition of our achievable scheme is as follows. Under the privacy constraint, we can satisfy the users in two groups with one transmission, therefore $2sq$ users can be satisfied by q transmissions. If $r = 0$, q transmissions suffice; if $0 < r \leq s$, we can satisfy the remaining r users by one transmission;

and if $s < r < 2s$, we can satisfy the remaining r users by two transmissions. Therefore the total number of transmissions is $q + \lceil \frac{r}{s} \rceil$. Based on this intuition, we distinguish three sub-cases: a) $r = 0$; b) $0 < r \leq s$; and c) $s < r < 2s$.

Case $r = 0$

This is the case where m is divisible by $2s$, therefore is divisible by s. We partition the users into groups $G_1, G_2, \ldots, G_{2q}$, such that all users in G_i have message w_{is} in their side information. Set the desired message of the users in $G_{2i}, i \in [q]$, to be $w_{(2i-1)s}$, and the desired message of the users in $G_{2i-1}, i \in [q]$ to be w_{2is} There are q transmissions, each of them is $w_{2is} + w_{(2i-1)s}, i \in [q]$, that satisfies the users in G_i and G_{i+1} while it does not provide any useful information for the users in other groups. Therefore, $q = \frac{m}{2s}$ transmissions suffice to satisfy all the m users.

Case $0 < r \leq s$

We partition the users into $2q + 1$ groups. As for to the case $r = 0$, the first $2q$ groups contain s users. The users in $G_i, i \in [2q]$, all have w_{is} in their side information. Group G_{2q+1} has r users. The first q transmissions are $w_{2is} + w_{(2i-1)s}, i \in [q]$, and satisfy the users in groups $G_i, i \in [2q]$. We next satisfy the users in G_{2q+1}.

If $r = 1$, we have $G_{2q+1} = \{u_m\}$. Let $d_m = s + 1$ and the $(q + 1)$-th transmission be $w_{s+1} + \sum_{j \in A_m} w_j$. Note that $s \geq r + 1 = 2$, therefore user u_m can decode w_{s+1} while the other users can not decode any new messages one they receive the last transmission.

If $r \geq 2$, the users in G_{2q+1} all have $W_{[1:s-r] \cup \{m\}}$ in their side information. Let $d_{2sq+1} = s - r + 1$ and $d_j = 2sq + 1, j \in [2sq + 2 : m]$. The $(q + 1)$-th transmission is $w_{2sq+1} + w_m + \sum_{j=1}^{s-r+1} w_j$. Since user u_{2sq+1} can compute $w_{2sq+1} + w_m + \sum_{j=1}^{s-r} w_j$ and users $u_j, j \in [2sq + 2 : m]$, can compute $w_m +$

$\sum_{j=1}^{s-r+1} w_j$, these users have the message that is not in their side information set as their desired message. All the other users who are not in G_{2q+1} have at least two messages unknown in the transmission and thus cannot decode it. Therefore, each user can decode only one message by the achievable scheme with $q+1$ transmissions. If m is divisible by s, then $r = s$ and $q+1 = \lceil \frac{m}{2s} \rceil$; if m is not divisible by s, $q+1 = \lceil \lfloor \frac{m}{s} \rfloor /2 \rceil + 1$.

Case $s < r < 2s$

We partition the users into $2q+2$ groups. The users in group $G_i, i \in [2q+1]$, all have message $w_{(is)}$, while the users in group G_{2q+2} all have $W_{[1:2s-r] \cup \{m\}}$. We satisfy the first $2q$ groups by sending $w_{2is} + w_{(2i-1)s}, i \in [q]$. We satisfy all users in G_{2q+1} by sending $w_{2sq+1} + w_{2sq+s} + w_{2sq+s+1}$. If $r = s+1$, $G_{2q+2} = \{u_m\}$ and we let $d_m = s+1$ and send as last transmission $w_{s+1} + \sum_{j \in A_m}$; otherwise, we let $d_{2sq+s+1} = 2s - r + 1$ and $d_j = 2sq + s + 1, j \in [2sq + s + 1 : m]$ and send $w_{2sq+s+1} + w_m + \sum_{i=1}^{2s-r+1} w_i$. One can verify that all users can decode one and only one message by using a code of length $q + 2 = \lceil \lfloor \frac{m}{s} \rfloor /2 \rceil + 1$.

5.3.2.2 Converse

Messages are bit vectors of length κ, for some κ; we thus see each message as an element in $\mathbb{F}_{2^\kappa}$. When the sender uses a linear code (on $\mathbb{F}_{2^\kappa}$), we can write the transmitted codeword as $x^\ell = E w^m$, where $w^m = (w_1, w_2, \ldots, w_m)^T$ is the vector containing all the messages, and where $E \in \mathbb{F}_{2^\kappa}^{\ell \times m}$ is the generator matrix of the code. We denote the linear span of the row vectors of E as $\text{Span}(E)$. Recall that in this setting, user $u_i, i \in [n]$, must to be able to decode one and only one message outside its side information set A_i; the index of the decoded message is d_i. Let $v_{i,j}$ be a vector whose j-th element is non-zero and all elements with index not in A_i are zeros.

A valid generator matrix E must satisfy the following two conditions:

1. *Decodability*: $v_{i,d_i} \in \text{Span}(\mathsf{E})$, for all $i \in [m]$;
2. *Privacy*: $v_{i,j} \notin \text{Span}(\mathsf{E})$ for all $i \in [m], j \in [m] \setminus (A_i \cup \{d_i\})$.

The decodability condition guarantees successful decoding of the desired message w_{d_i} by user u_i as argued in [6]. The privacy condition must hold because the existence of a vector $v_{i,j} \in \text{Span}(\mathsf{E})$ for some $j \in [m] \setminus (A_i \cup \{d_i\})$ implies that user u_i is able to decode message w_j in addition to its desired message w_{d_i}.

The optimal linear code length $\ell^\star_{\text{lin}}$ is the smallest rank of the generator matrix E, which by definition is the maximum number of pairwise linearly independent vectors in $\text{Span}(\mathsf{E})$. We prove the linear converse bound by giving a lowered bound on the maximum number of pairwise linearly independent vectors in $\text{Span}(\mathsf{E})$, i.e., the rank of E. To do so, we need the following two propositions. These propositions are the key technical novelty of this work.

Proposition 13. *In a working system (where every user can decode without violating the privacy condition) with* $g = 1$ *we must have* $e_i \notin \text{Span}(\mathsf{E})$ *for all* $i \in [m]$*, where* e_i *are standard bases of* m*-dimensional linear space.*

Proposition 14. *For a working system with* $g = 1$*, among all* n *users, consider* k *users whose side information sets are pairwise disjoint. The number of transmissions of any linear code that satisfies these* k *users must be* $\ell_{\text{lin}} \geq \lceil k/2 \rceil$.

5.3.2.2.1 Proof of Proposition 13

Recall that, for $g = 1$, the side information sets are $A_i = (i, \ldots, i+s-1 \pmod m)$ for all $i \in [m]$, as here $n = m$. The proof is by contradiction. Assume without loss of generality (wlog) that we have a working systems with $e_1 \in \text{Span}(E)$, that is, every user can decode message w_1 without even using its side information. Then, all users $u_i, i \in [2 : m - s + 1]$ (who do not have w_1 in their side information sets) must have desired message w_1, in order to make sure that privacy constraint is not violated. This implies Fact 1: user u_1 can only have $w_{d_1} = w_{s+1}$ as desired message.

Fact 1 is true because u_2 desires w_1, therefore $A_2 \cup \{d_2\} \supset A_1$. After decoding w_1, user u_2 can mimic user u_1 and thus decode message d_2. Since user u_2 can decode only one message, then $d_1 \in A_2 \setminus A_1 = \{s + 1\}$. Therefore $d_1 = s + 1$. By taking $d_1 = s + 1$, we conclude that there must exist vector $v_{1,d_1} = v_{1,s+1} = c + \alpha_{s+1} e_{s+1}$, where $\alpha \in \mathbb{F}_{2^\kappa}$, $\alpha \neq 0$ and $c \in \text{Span}(A_1)$, where with an abuse of notation we let $\text{Span}(A_i)$ denote $\text{Span}(\{e_j : j \in A_i\})$.

Given that we established Fact 1, let j be the position of the fist non-zero element in the so found $v_{1,s+1}$. Clearly, $j \leq s + 1$ since the $(s + 1)$-th element of $v_{1,s+1}$ is $\alpha_{s+1} \neq 0$. We have the following cases:

1. If $j = s + 1$, all the users who do not have w_{s+1} in their side information sets, can decode w_{s+1}. This is because in this case $v_{1,s+1} = \alpha e_{s+1}$. Thus user u_{s+2}, who has neither w_1 nor w_{s+1} in its side information set, can decode both w_1 and w_{s+1}.

2. If $1 < j < s + 1$, then user u_{j+1} can decode w_j, since $s + 1 \in A_j$. But user u_{j+1} decodes w_1 by assumption. Therefore, user u_j can decode both w_1 and w_j.

3. If $j = 1$, user u_{s+2} can decode both w_{s+1} and w_1. Therefore, u_{s+2} can decode two messages.

In all the three above cases, there exists at least one user who can decode at least two messages, thus violating the privacy constraint. Therefore, the original assumption $e_1 \in \text{Span}(E)$ must be impossible in a working system. The same reasoning applies to any $e_j, j \in [m]$. This proves the claim.

5.3.2.2.2 Proof of Proposition 14

By Proposition 13, for all $i \in [k]$ there exists $v_{i,d_i} = \alpha_i e_{d_i} + c_i \in \text{Span}(E)$, where $c_i \in \text{Span}(A_i)$ and $\alpha_i \neq 0$. Since the side information sets A_i are assumed to be disjoint, the vectors c_i are linearly independent. v_{i,d_i} are linearly dependent only if $d_i \in A_j$ and $d_j \in A_i$ for some $i \neq j$. In other words, there exists a "loop" between u_i and u_j. Note that since the side information sets are disjoint, one user can be in at most one "loop", and the number of "loops" is at most $\lfloor k/2 \rfloor$. Therefore the number of v_{i,d_i} that are linearly dependent is at most $\lfloor k/2 \rfloor$, and thus the number of *linearly independent* v_{i,d_i} is at least $k - \lfloor k/2 \rfloor = \lceil k/2 \rceil$. Therefore, the number of transmissions that is needed to satisfy k users with disjoint side information sets must satisfy $\ell = \text{rk}(E) \geq \lceil k/2 \rceil$.

Proposition 13 states that in this case, a trivial 'uncoded scheme' (that consists of sending $\ell^\star_{\text{lin}}$ messages one by one) always violates the privacy constraint. In other words, no user is allowed to decode without using its side information.

Proposition 14 provides a lower bound on the code-length of a linear code for a subset of the users in the system (those with pairwise disjoint side information sets), thus for all users. Therefore, among all m users in the system, there are $\lfloor \frac{m}{s} \rfloor$ users with pairwise disjoint side information sets. By Proposition 14, we need at least $\lceil \lfloor \frac{m}{s} \rfloor /2 \rceil$ transmissions to satisfy these users. Therefore, in order to satisfy all the users in the system, we must have $\ell^\star_{\text{lin}} \geq \lceil \lfloor \frac{m}{s} \rfloor /2 \rceil$. This provides the claimed lower bound.

5.3.3 Case $s < m/2$ and $g = s = 2$ (here $n = m/2$)

5.3.3.1 Achievability

In this case we show $\ell^{\star}_{\text{lin}} = \lceil m/4 \rceil$. We use the achievable scheme for case $s = 2 < m/2$ and $g = 1$ from Section 5.3.2.1, where we need $\lceil m/4 \rceil$ transmissions to satisfy all $n = m$ users. We users we have in this case are a proper subset of the users in the case $g = 1$. The achievable scheme for $g = 1$ still satisfies all users and meets the privacy constraint. We have $\ell \leq \lceil m/4 \rceil$ in this case.

5.3.3.2 Converse

The converse proof in Section 5.3.2.2 does not directly apply in this case, mainly because the proof of Proposition 13 requires $g = 1$. Therefore we show that the same result holds for $g = 2$, stated as Proposition 15.

Proposition 15. *In a working system (where every user can decode without violating the privacy condition) with* $g = s = 2$ *we must have* $e_i \notin \mathit{Span}(E)$ *for all* $i \in [m]$*, where* e_i *are standard bases of* m*-dimensional linear space.*

5.3.3.2.1 Proof of Proposition 13

Similar to the proof of Proposition 13, Wlog assume e_1 is in Span(E). All users $u_i, i \in [2 : m-s+1]$ in this case need to desire message w_1. Let $d_1 \in A_j$, for some $j \neq 1$ For the decoding at u_1, there exists a vector $v_{1,d_1} \in$ Span(E) such that: 1) the d_1-th element is non-zero; 2) all elements with indices that are not $1, 2$ or d_1 are zeros. We check the first and second element of v_{1,d_1} and have the following cases:

1. Both the first and second elements of v_{1,d_1} are zeros, $v_{1,d_1} = e_{d_i}$. Therefore all users without w_{d_i} in their side information sets can decode w_{d_i}.

2. The first element is zero while the second element is non-zero. By v_{1,d_1} the user u_j is able decode w_2 since u_j already decodes w_1 and has w_{d_1} in its side information sets. u_j can decodes two messages.

3. The first element is non-zero while the second element is zero. Since all users that do not have w_1 can decode w_1, all users can decode w_{d_1} if they do not have it in their side information sets.

4. Both the first and second elements of v_{1,d_1} are non-zeros. u_j decodes w_1 by assumption. It also has w_{d_i} in its side information set. Therefore u_j can decode w_2.

All possible cases show that there exists at least one user that can decode at least two messages. The assumption that e_1 is in Span(E) is impossible. The reasoning applies to all $e_j, j \in [m]$. Therefore we conclude that $e_i \notin$ Span(E) for all $i \in [m]$.

Hence the converse follows the same argument in Section 5.3.2.2 by replacing Proposition 13 with Proposition 15. We show that for k user with pairwise disjoint side information sets, $\lceil k/2 \rceil$ transmissions are needed for this case under the linear encoding restriction. Note that in this case all $n = m/2$ users are with pairwise disjoint side information sets. Therefore, the total number of transmissions that satisfy all users is at least $\lceil m/4 \rceil$.

5.3.4 Remaining Cases

For the following three cases: $s < m/2$, $g = 2$, $s \neq 2$; $s < m/2$, $g \geq 3$; $s \geq m/2$, we aim to prove

$$\ell^* = \begin{cases} 1, & \text{if the NTH has 1-factor,} \\ 2, & \text{otherwise.} \end{cases}$$

5.3.4.1 Converse for all three cases

By the converse bound for circular-arc PICOD without the privacy constraint, $\ell* \geq 1$ when the NTH has 1-factor, and $\ell^* \geq 2$ when the NTH has no 1-factor.

5.3.4.2 Achievability for case $s < m/2$, $g = 2$, and $s \neq 2$

If $s = 1$, the NTH has 1-factor. Thus $\ell^* = 1$, in which case we send the sum of all messages. If $2 < s < m/2$, we send w_{s+1} as the first transmission. This transmission satisfies all users but $u_i, i = 2, \ldots, \lfloor s/2 \rfloor + 1$, since they all have w_{s+1} in their side information set. When s is even, they have common side information set $\{s+1, s+2\}$. We send the second transmission as $w_3 + w_{s+1} + w_{s+2} + w_{s+3}$. u_2 can decode w_{s+3}, $u_i, i = 3, \ldots, \lfloor s/2 \rfloor + 1$ can decode w_3. All the other users, after decoding w_{s+1}, still have at least two messages known in the summation, therefore can not decode any more messages. When s is odd, we send the second transmission as $w_3 + w_s + w_{s+1} + w_{s+2} + w_{s+3}$. By similar argument we can show that $u_i, i = 2, \ldots, \lfloor s/2 \rfloor + 1$ can decode one messages from the second transmission while the other users can not.

5.3.4.3 Achievability for case $s < m/2$, $g \geq 3$

It is trivial that if the NTH has 1-factor we have $\ell^* = 1$, in which case we send the sum of all messages. Therefore, we show that if the NTH does not have 1-factor we can satisfy all users with two transmissions while satisfying the privacy constraint. Send w_{s+1} as the first transmission. All users who do not have w_{s+1} in the side information sets are satisfied. The users that have w_{s+1} in the side information sets are $u_i, i = 2, \ldots, \lfloor s/g \rfloor, \lfloor s/g \rfloor + 1$. They have common side information set $[\lfloor s/g \rfloor g + 1 : s + g]$. $|[s + 2 : s + g]| \geq 2$ since $g \geq 3$. For the second transmission we send $w_m + \sum_{i=s+2}^{s+g} w_i$. By the condition $s < m/2$, all users $u_i, i = 2, \ldots, \lfloor s/g \rfloor, \lfloor s/g \rfloor + 1$ do not have

w_m in the side information sets. Therefore these users can decode w_m as the desired message. For the second transmission, all the other users have at least two messages known in the summation, therefore can not decode any information from the second transmission. The privacy constraint is satisfied.

5.3.4.4 Achievability for case $s \geq m/2$

We use the proposed achievable scheme in [25] for this case. When $g = 1$, [25] showed one can achieve $\ell = 1$ if the NTH has 1-factor, and $\ell = 2$ otherwise. When $g > 1$, the users are in a proper subset of the users of $g = 1$. Therefore the users can still be satisfied by the scheme that can satisfy strictly more users. The privacy constraint is still satisfied as less users can not decode more messages. Therefore, the achievable scheme can achieve $\ell = 1$ when NTH has 1-factor, and $\ell = 2$ when NTH does not have 1-factor.

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Conclusion

The main results of this work are summarized in Table VI and Table VII.

6.1.1 Pliable Index Coding

We provided information theoretic converse bounds for some cases of the PICOD$(\mathtt{t})$.

Because the only difference between the IC and the PICOD is the pliablity of choosing the desired messages at users, the converse of the PICOD$(\mathtt{t})$ can be obtained by solving all the IC instances with the same users in the PICOD$(\mathtt{t})$ while choosing all possible desired messages at the users. Obviously, solving the converse for the PICOD$(\mathtt{t})$ in this way becomes intractable when there are more users/messages in the system. In this thesis we show that there are alternative ways to find tight lower bounds. The key idea for the converse is to show that for the PICOD$(\mathtt{t})$ with some certain structures of side information set, regardless of the choice of desired message at the users, there exists a user that

TABLE VI

COMPLETE-S PICOD

	centralized	decentralized
without security	$\ell^* = \min\{\mathtt{m} - \mathtt{s}_{\min}, \mathtt{s}_{\max} + \mathtt{t}\}$	$\ell^* = \min\{\mathtt{m} - \mathtt{s}_{\min}, \mathtt{s}_{\max} + \mathtt{t}\}$ when pliable; $\ell^* = \frac{\binom{\mathtt{m}}{\mathtt{s}}}{\binom{\mathtt{m}}{\mathtt{s}}-1}\mathtt{t}$ when non-pliable
individual security	unknown	unknown

TABLE VII

CIRCULAR SHIFT PICOD

	centralized	decentralized
without security	$\ell^* = 1$ when $m/(m-s)$ is an integer; $\ell^* = 2$ otherwise	$\ell^* = \gamma/(\gamma-1)$ when $m/(m-s)$ is an integer; $\ell^* = 2$ otherwise
individual security	$\ell^* = 1$ when $m/(m-s)$ is an integer; otherwise $\ell^* = 2$ if $s > m/2$; $\ell^* = m/2s$ if $s < m/2$	not yet studied

can decode a certain number of messages beside its desired ones by receiving any valid code that allows every user to decode its desired message. We showed two methods to prove the existence of such a user: constructive proof and existence proof. The constructive proof works for the PICOD(t) where network topology hypergraph is a circular-arc hypergraph and the complete–S PICOD(t) with m messages where $S = [0 : m-t] \setminus [s_{\min} : s_{\max}], 0 \leq s_{\min} \leq s_{\max} \leq m-1$. However, the constructive proof in [31] becomes intractable for general complete–S PICOD(t) with m messages, even for $S = \{s\}$, $0 < s < m-t$.

To circumvent the difficulty, we turn to the existence proof: implicitly showing the existence of a user by proving its nonexistence leads to a contradiction. Inspired by the similarity of the side information set structure of the complete–$\{s\}$ PICOD(t) to the Steiner system, we brought the idea of "block cover" in combinatorial design as the tool for the proof. Combinatorial design studies the properties of a family of subsets, called blocks, that "cover" all s-element subsets of the same ground set. The results are usually established on the high symmetry of the structure of all s-element subsets. In the complete–$\{s\}$ PICOD(t), we consider the union of decoded messages and side information set of a user

as the "block" that cover this user. Therefore, we show that there exists a user who can decode $s + t$ messages in the complete–$\{s\}$ PICOD(t) with $2s + t$ messages by showing that the "block cover" with maximum block size strictly less than $2s + t$ does not exist.

For the other cases, we prove the converse by showing that they can be enhanced to the critical case: the complete–$\{s\}$ PICOD(t) with $m = 2s + t$ messages. Therefore the converse bound we obtained for the critical case extends to all the consecutive complete–S PICOD(t) and some other cases.

6.1.2 Decentralize Pliable Index Coding

We solved the d-PICODproblems whose corresponding centralized versions have been solved. One of the purpose is to study the decentralization impact on the PICOD. Recently, [20] showed that optimality of a decentralized IC problem has a multiplicative gap at most 2 to its centralized IC instance. For the PICOD cases we have studied the optimality, the gap is much smaller. We find the gap at most $\frac{\binom{m}{s}}{\binom{m}{s}-1}$, which is usually much smaller than 2. Also, for most of the cases, the d-PICOD problem has the same number of transmissions to its centralized version. That is, the gap is in fact 1.

Another interesting observation is that although linear code is still optimal, we need the vector linear codes to achieve the optimality in many cases. The scaler linear code is proved to be strictly suboptimal for some cases of the d-PICOD.

6.1.3 Secure Pliable Index Coding

We considered the individual secure PICOD(1) with circular shift side information. Our model is a generalization of the problem modeled in [25]. We proposed a new achievable scheme for our generalized model. Our scheme can recover the existing scheme proposed in [25] and can perform strictly better in some cases. The intuition of the scheme is to satisfy "group" of users one at a time while

maintaining the security of the messages to all the other users that do not desire the messages. Moreover, we provide a linear encoding constrained converse, which is based on the vector space spaning argument. Our linear achievable scheme is information theoretical optimal for some parameters, or is at most one more transmission away from the linear encoding constrainted converse. Therefore, the proposed scheme is almost linearly optimal.

6.2 Future Work

Our results show the fundamental different behavior of PICOD compared to the classical IC where the desired messages at the users are pre-determined. We have several interesting observations and related open problems for the PICOD.

- The main contribution of the converse for the complete–S PICOD$(\mathtt{t})$ in this thesis is a method to prove the existence of a user that can decode the desired number of messages: constructive and existence proofs. While the later shows an advantage over the former on the complexity of the proof, it is based on the strong symmetric structure of the side information set of the users. Like combinatorial design, for the result to hold we need exactly all the s-element subsets of ground set $[\mathtt{m}]$. Therefore, this method suits the complete–$\{\mathtt{s}\}$ PICOD$(\mathtt{t})$. For the other cases, we need some extra tools. We showed the proof for the consecutive complete–S PICOD$(\mathtt{t})$ by a reduction to the critical case. However, not all the PICOD$(\mathtt{t})$, even all complete–S PICOD$(\mathtt{t})$, can be reduced in the same fashion without loss of optimality in terms of the code length. Therefore we still lack an efficient method to obtain a general optimal converse bound for the general PICOD$(\mathtt{t})$. In Section 3.6.4 we showed the optimality of the proposed achievability up to $\mathtt{m} = 5$ for the complete–S PICOD$(\mathtt{t})$. The converse is obtained by checking all the cases that are not

covered by the Theorem 2 and Propositions 2, 3, 4. Therefore the method is not systematic and straightforwardly generalizable to larger m. The information theoretical optimal code length for the general complete–S PICOD(t) with m messages is still open.

- We notice that in the complete–S PICOD(t) considered in this work, removing/adding some users does not change the optimal code length. In fact, in some cases (e.g., $S = [0 : m/2]$) roughly half of the users can be removed without affecting ℓ^*. These users can be considered as "non-critical", in contrast to the other "critical" users who will change the optimal code length if removed/added. The PICOD(t) is called "critical" if all of its users are critical. We can see the "critical" consecutive complete–S PICOD(t) are those with $m \geq s_{\min} + s_{\max} + t$. In other words, the ones with "small" size of side information/number of desired messages. In this case the optimal code length is $s_{\max} + t$. For this setting, removing any single user reduces the optimal code length by 1. If $m < s_{\min} + s_{\max} + 1$, there are $\sum_{s=s_{\min}}^{s_{\max}} \binom{m}{s} - \binom{2m-2s_{\min}-1}{m-s_{\min}-1}$ users non-critical. It is worth to mention that due to the symmetric structure of the complete–S PICOD(t) where $|S| = 1$, all users are essentially the same, i.e., all users are critical if any user is critical. The question about the critical users in the PICOD(t) is interesting because it shows the redundancy embedded in the system structure. The condition for a complete–S PICOD(t) problem to be critical, the number of the non-critical users for a complete–S PICOD(t) problem, and in general, the condition for a general PICOD(t) problem to be critical, are interesting topics of future works for the PICOD(t) problem.

- Our results on the d-PICODproblem shows that there is little difference between the centralized PICOD problem and the d-PICODproblem in terms of the optimal number of transmissions, for

the cases which we have the information theoretical optimality. Since for the IC the difference between centralized and decentralized setting is upper bounded by a multiplicative gap 2, for PICOD we expect a gap no greater than 2. Our result provides one example that the multiplicative gap is indeed 2. This shows that on the extreme, the multiplicative gap 2 between the IC and the decentralized IC can not be further reduced by allowing the pliability of choosing of the desired messages at the user. However, we also notice that the maximum multiplicative gap for the cases that we have studied is $\frac{\binom{m}{s}}{\binom{m}{s}-1}$, which is usually much less than 2. One interesting question to ask is for the PICOD, what is the expected number of transmission when turning it into a d-PICODproblem. Fundamentally, will the pliability of desired message have a impact or not.

- One of the contributions on the secure PICOD is the linear encoding constraint converse bound. The converse bound allows us to show the fundamental difference between the centralized PICOD and the d-PICODwhen the security constraint is taken into consideration. However, the converse is based on the extra assumption that the encoding function is a linear function. We are interested in removing this constraint. Doing so would allow us to have a converse bound without any assumption on the encoding function and provide us the information theoretical converse bound.
- Our converse is combinatorial and based on contradiction. The proof idea is basically extremal combinatorics. Although graph theory has been extensively used to derive achievability schemes in the IC problem, there are few converse proofs purely based on graph theory or combinatorics. Our proposed technique is thus new and different from all the other converse proof techniques that have been developed in the IC. Since the IC can be very much treated as a problem in combinatorics, it is interesting to seek for the applications of our proof techniques to a broader range

of more general IC and network coding problems. Furthermore, the connection between extremal combinatorics and index coding is a very interesting and important question to study for the future direction.

CITED LITERATURE

1. Shannon, C. E.: A mathematical theory of communication. Bell System Technical Journal, 1948.

2. Shannon, C. E.: Two-way communication channels. Proc. 4th Berkeley Symp. Math. Statist. Probab., I(611-644), 1961.

3. Cover, T.: Broadcast channels. IEEE Trans. on Information Theory, 18(1):2–14, 1972.

4. Ahlswede, R.: The capacity region of a channel with two senders and two receivers. Ann. Probability, 2(5):805–814, 1974.

5. Birk, Y. and Kol, T.: Informed-source coding-on-demand (ISCOD) over broadcast channels. Proc. IEEE 17th INFOCOM, pages 1257–1264, 1998.

6. Bar-Yossef, Z., Birk, Y., Jayram, T. S., and Kol, T.: Index coding with side information. IEEE Trans. on Information Theory, 57(3):1479–1494, Mar 2011.

7. Rouayheb, S. E., Sprintson, A., and Georghiades, C.: On the index coding problem and its relation to netowrk coding and matroid theory. IEEE Trans. on Information Theory, 56(7):3187–3195, July 2010.

8. Lubetzky, E. and Stav, U.: Nonlinear index coding outperforming the linear optimum. IEEE Trans. on Information Theory, 2009.

9. Sun, H. and Jafar, S. A.: Index coding capacity: How far can one go with only shannon inequalities? IEEE Trans. on Information Theory, 61(6):3041–3055, June 2015.

10. Brahma, S. and Fragouli, C.: Pliable index coding. IEEE Trans. on Information Theory, 61(11):6192–6203, Nov 2015.

11. Milosavljevic, N., Pawar, S., Rouayheb, S. E., Gastpar, M., and Ramchandran, K.: Efficient algorithms for the data exchange problem. IEEE Trans. on Information Theory, 62(4):1878 – 1896, April 2016.

12. Ji, M., Caire, G., and Molisch, A. F.: Fundamental limits of caching in wireless d2d networks. IEEE Trans. on Information Theory, 2016.

13. Shannon, C. E.: Communication Theory of Secrecy Systems. Bell System Technical Journal, 28 (4):656–715, October 1949.

14. Song, L. and Fragouli, C.: A deterministic algorithm for pliable index coding. In Information Theory Proceedings (ISIT), 2016 IEEE International Symposium on, July 2016.

15. Haviv, I. and Langberg, M.: On linear index coding for random graphs. Information Theory Proceedings (ISIT), IEEE International Symposium on, pages 2231 – 2235, July 2012.

16. Song, L. and Fragouli, C.: A polynomial-time algorithm for pliable index coding. IEEE Trans. on Information Theory, 64(2):979 – 999, Feb 2018.

17. Liu, T. and Tuninetti, D.: Pliable index coding: Novel lower bound on the fraction of satisfied clients with a single transmission and its application. Information Theory Workshop, ©IEEE 2016.

18. Ong, L., Ho, C. K., and Lim, F.: The single-uniprior index-coding problem: The single-sender case and the multi-sender extension. IEEE Trans. on Information Theory, 62(6):3165 – 3182, June 2016.

19. Liu, Y., Sadeghi, P., Arbabjolfaei, F., and Kim, Y.-H.: Capacity theorems for distributed index coding. arXiv:1801.09063, 2018.

20. Alexandra Porter, M. W.: Embedded index coding. arXiv:1904.02179, 2019.

21. Dau, S. H., Skachek, V., and Chee, Y. M.: On the security of index coding with side information. IEEE Trans. on Information Theory, 58(6):3975 – 3988, June 2012.

22. Karmoose, M., Song, L., Cardone, M., and Fragouli, C.: Private broadcasting: An index coding approach. Information Theory Proceedings (ISIT), IEEE International Symposium on, 2017. [Online]. Available: https://arxiv.org/abs/1701.04958.

23. Sun, H. and Jafar, S. A.: The capacity of private information retrieval. IEEE Trans. on Information Theory, 63(7):4075 – 4088, July 2017.

24. Narayanan, V., Ravi, J., Mishra, V. K., Dey, B. K., Karamchandani, N., and Prabhakaran, V. M.: Private index coding. Information Theory Proceedings (ISIT), IEEE International Symposium on, 2018.

25. Sasi, S. and Rajan, B. S.: On pliable index coding. arXiv:1901.05809, 2019.

26. Lovett, S.: MDS matrices over small fields: A proof of the gm-mds conjecture. arXiv:1803.02523v2, 2018.

27. Garfinkel, R. and Nemhauser, G. L.: Integer Programming. John Wiley & Sons Inc, 1973.

28. Lovász, L.: On the ratio of optimal integral and fractional covers. Discrete Mathematics, 13:383–390, Jan. 1975.

29. Chvatal, V.: A greedy heuristic for the set-covering problem. Mathematics of Operations Research, 4(3):233–235, Aug 1979.

30. Robbins, H.: A remark on stirling's formula. Amer. Math. Monthly, 62(1):26–29, 1955.

31. Liu, T. and Tuninetti, D.: Information theoretic converse proofs for some picod problems. Information Theory Workshop, ©IEEE 2017.

32. Liu, T. and Tuninetti, D.: An information theoretic converse for the "consecutive complete–s" picod problem. Information Theory Workshop, ©IEEE 2018.

33. van Lint, J. H.: On the number of blocks in a generalized steiner system. Journal of Combinatorial Theory, A(80):353 – 355, 1997.

34. Karp, R. M.: Reducibility among combinatorial problems. Complexity of Computer Computations, pages 85–103, 1972.

35. Yi, X., Sun, H., Jafar, S. A., and Gesbert, D.: TDMA is optimal for all-unicast dof region of TIM if and only if topology is chordal bipartite. IEEE Trans. on Information Theory, 64(3):2065 – 2076, Mar 2018.

36. Liu, T. and Tuninetti, D.: Decentralized pliable index coding. Information Theory Proceedings (ISIT), International Symposium on, ©IEEE 2019.

37. Liu, T. and Tuninetti, D.: Tight information theoretic converse results for some pliable index coding problems. Information Theory Workshop, ©IEEE 2018. [Online]. Available: https://arxiv.org/abs/1810.02451.

38. Liu, T. and Tuninetti, D.: Private pliable index coding. Information Theory Workshop, ©IEEE 2019.

VITA

Name: Tang Liu

Education Background

- Ph.D. in electrical engineering at University of Illinois at Chicago, Chicago, United States, 2020.
- M.S. in mathematical computer science at University of Illinois at Chicago, United States, 2019.
- M.S. in electrical engineering at Korean Advanced Institute of Science and Technology, Daejeon, South Korea, 2013.
- B.S. in telecommunication engineering at University of Electronic Science and Technology of China, Chengdu, China, 2010.

Publications

- T. Liu and D. Tuninetti, "Secure Decentralized Pliable Index Coding," Accepted at IEEE International Symposium on Information Theory (ISIT), 2020.
- T. Liu and D. Tuninetti, "Private Pliable Index Coding," presented at IEEE Information Theory Workshop (ITW), 2019.
- T. Liu and D. Tuninetti, "Decentralized Pliable Index Coding," presented at IEEE International Symposium on Information Theory (ISIT), 2019.
- T. Liu and D. Tuninetti, "Tight Information Theoretic Converse Results for some Pliable Index Coding Problems," submitted to IEEE Transactions on Information Theory.
- T. Liu and D. Tuninetti, "An Information Theoretic Converse for the 'Consecutive Complete– S' PICOD Problem," presented at IEEE Information Theory Workshop (ITW), 2018.

- T. Liu, D. Tuninetti, and S. Y. Chung, "On the DoF Region of the MIMO Gaussian Two-User Interference Channel with an Instantaneous Relay," IEEE Transactions on Information Theory, July 2017.

- T. Liu and D. Tuninetti, "Information Theoretic Converse Proofs for some PICOD Problems," presented at IEEE Information Theory Workshop (ITW), 2017.

- T. Liu and D. Tuninetti, "Pliable Index Coding: Novel Lower bound on the Fraction of Satisfied Clients with a Single Transmission and its Application," presented at IEEE Information Theory Workshop (ITW), 2016.

- T. Liu, D. Tuninetti, and S. Y. Chung, "On the DoF of Two-User Interference Channel with an Instantaneous Relay," presented at IEEE International Symposium on Information Theory (ISIT), 2015.

- T. Liu, D. Tuninetti, and S. A. Jafar, "The DoF of the Asymmetric MIMO Interference Channel with Square Direct Link Channel Matrices," presented at 52nd Allerton Conference, 2014.

- Z. Cheng, N. Devroye, and T. Liu, "The Degrees of Freedom of Full-Duplex Bi-directional Interference Networks with and without a MIMO Relay," IEEE Transactions on Wireless Communication, Dec 2015.

Awards

- *Korean Government Scholarship*: 2010-2013, by South Korea government.

IEEE Copyright Permission

journals.ieeeauthorcenter.ieee.org/choose-a-publishing-agreement/avoid-infringement-upon-ieee-copyright/

Can I reuse my published article in my thesis?

You may reuse your published article in your thesis or dissertation without requesting permission, provided that you fulfill the following requirements depending on which aspects of the article you wish to reuse.

- **Text excerpts:** Provide the full citation of the original published article followed by the IEEE copyright line: © 20XX IEEE. If you are reusing a substantial portion of your article and you are not the senior author, obtain the senior author's approval before reusing the text.
- **Graphics and tables:** The IEEE copyright line (© 20XX IEEE) should appear with each reprinted graphic and table.
- **Full text article:** Include the following copyright notice in the references: "© 20XX IEEE. Reprinted, with permission, from [full citation of original published article]."

When posting your thesis on your university website, include the following message:

> "In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [name of university or educational entity]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink. If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation."

Only the accepted version of your article, ***not the final published version***, may be posted online in your thesis.