A Note on Parity Check Matrix of Private Information Retrieval Code

1st Koki Kazama
Shonan Institute of Technology
Emai : kazama@info.shonan-it.ac.jp

2nd Takahiro Yoshida
Nihon University
yoshida.takahiro@nihon-u.ac.jp

***Abstract*—A private information retrieval (PIR) is a scheme that allows a user to retrieve messages from information databases while keeping secret which one the user wants to retrieve. Sun et al. formulated the download rate and showed that there is an upper limit to it (capacity). Previous construction methods of a capacity-achieving linear PIRs (CAL-PIR) are ad hoc. We propose a systematic construction method for a CAL-PIR using the parity check matrix.**

***Index Terms*—private information retrieval**

I. Introduction

A private information retrieval (PIR) is a scheme that allows a user to retrieve messages from information database (DBs) while keeping secret which one the user wants to retrieve (user's privacy). One scheme is for the user to download all information from all DBs. However, the communication efficiency of this scheme is very low. We construct a PIR with high communication efficiency. Chor et al. first studied a PIR. Since Sun et al. studied a PIR using information theory and coding theory, numerous studies have followed Sun's study.

The scheme of PIR in this study is as follows: Multiple databases store multiple messages. First, the user generates queries and sends them to the DBs. Then, each DB generates responses based on the query and all messages and sends a response to the user. Lastly, the user reconstructs the message that the user wants to retrieve. Each DB independently tries to guess which message the user wants when receiving a query, while each DB cannot obtain any information about it.

Sun et al. formulated the user's privacy and a download rate, which is the communication efficiency when a user receives responses from all DBs, using information theory and showed that there is an upper limit to the download rate (capacity) when we fix the number of the DBs N and the number of messages M.

The representative construction methods of a PIR that achieves the capacity and whose response-generating function (encoder) and reconstruction function (decoder) are linear (capacity-achieving linear PIR, CAL-PIR) are Sun's and Tian's. However, both methods were ad hoc because describing the converse part of the proof of the capacity using entropy did not clarify the properties of the encoder and the decoder in the form of matrices.

We propose a systematic construction method for a CAL-PIR using the parity check matrix. Using the parity check matrix clarifies the conditions for achieving capacity.

II. Ease of Use

A. Some Common Mistakes

B. Authors and Affiliations

C. Identify the Headings

D. Figures and Tables

a) Positioning Figures and Tables:

III. Conclusion

In this paper, we proposed and evaluated a new distributed coded computation scheme called GDCC and, as one example, GDCCG. First, we evaluated the GDCCG with (a) the computation time complexity and showed the parameter condition in which the GDCCG system is superior to the SA system. Next, we evaluated the GDCC and the GDCCG with (b) the error-correcting capability of the overall system and showed that the GDCCG system can correct $\boldsymbol{E}$ which satisfies $\mathrm{rank}(\boldsymbol{E}) \leq t$.

In future works, we would like to improve the proposed schemes. For example, if we use more efficient decoding algorithms such as [1], the GDCCG may be better concerning the CTC. For another example, the GDCCG uses more workers than the DCCG. Thus we would like to propose new DCCs considering not only (a) and (b) but also communication load and the number of workers.

References

[1] H. Bartz, T. Jerkovits, S. Puchinger, and J. Rosenkilde. Fast decoding of codes in the rank, subspace, and sum-rank metric. *IEEE Transactions on Information Theory*, Vol. 67, No. 8, pp. 5026–5050, 2021.

Appendix

A. The Proof of Proposition