

東北大学大学院情報科学研究科  
純粋・応用数学研究センター

情報数理談話会のお知らせ

日 時： 2023年12月13日(水) 15:00 より 16:00 まで

場 所： 東北大学大学院情報科学研究科棟 2階大講義室

講演者： 石塚慶太 (東北大学大学院情報科学研究科)

題 目： Characterization of linear complementary dual codes

備 考： この情報数理談話会は課程博士予備審査会を兼ねています

[概要] Euclidean linear complementary dual codes, Euclidean LCD codes for short, are linear codes whose intersections with their Euclidean dual codes are trivial. Their Hermitian counterparts are Hermitian LCD codes, and these two classes of codes are collectively called LCD codes. Carlet and Guilley proved that a binary Euclidean LCD code can be used as a countermeasure to fault non-invasive attacks and side-channel attacks. Lu, Li, Guo, and Fu showed that a quaternary Hermitian LCD code leads to a maximal entanglement-assisted quantum code. Motivated by these results, constructions of LCD codes over finite fields of small orders have been studied extensively. In particular, Bouyuklieva constructed many optimal binary LCD codes by considering punctured codes and shortened codes of such codes. We show that a similar result to that of Bouyuklieva holds in quaternary Hermitian LCD codes. In addition, we present a construction method for LCD codes over any finite field. As an application, we improve the lower bounds on the minimum weights of many binary Euclidean LCD codes and quaternary Hermitian LCD codes.

ホームページ：<https://www.math.is.tohoku.ac.jp/research/colloquium.html>