

Quasi-Twisted codes and their applications to code-based cryptography

Rutuja Kshirsagar

Fujitsu Research of America, Inc.

Quasi-twisted (QT) codes generalize several important families of linear codes, including cyclic, constacyclic, and quasi-cyclic codes. Despite their potential, to the best of our knowledge, there exists no efficient decoding algorithm for QT codes. In this work, we propose a syndrome-based decoding method capable of efficiently correcting up to $\frac{d^*-1}{2}$ errors, where d^* denotes an HT-like lower bound on the minimum distance of QT codes, which we formalize here. Additionally, we introduce a Niederreiter-like cryptosystem constructed from QT codes. This cryptosystem is resistant to some classical attacks as well as some quantum attacks based on Quantum Fourier Sampling.

In Special Session 47 on Mathematical Tools with Applications in Quantum and Genetic Coding at the Mathematical Congress of the Americas 2025.