1

Matrix Code Equivalence

Attacks using isometry-invariant substructures

Example*: find low-rank codewords in both codes and match them up, construct isometry from this.*
or*, find peculiar subcodes on both sids, match them up, and construct the isometry between the subcodes*

· Graph-based algorithm

· Leon's like algorithm

$$\tilde{\mathcal{O}}(q^{\min(n,m,k)})$$

1

Matrix Code Equivalence

Attacks using isometry-invariant substructures

Example: *find low-rank codewords in both codes and match them up, construct isometry from this.*
or, *find peculiar subcodes on both sids, match them up, and construct the isometry between the subcodes*

· Graph-based algorithm

· Leon's like algorithm

$$\tilde{\mathcal{O}}(q^{\min(n,m,k)})$$

Attacks reducing MCE to solving a system of polynomial equations

Example: *write down both generator matrices and add rows in variables of A and B*
or, *use the formulation as tensor isomorphism to get a bilinear system, apply Gröbner techniques*

· direct modelling

· minor's modelling

· *improved* modelling

$$\mathcal{O}\left(n^{\omega\frac{n}{4}}\right)$$