1

Matrix Code Equivalence

combinatorial

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

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

algebraic

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

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

1

Matrix Code Equivalence

equations

$$\mathscr{C}(Ax, By, z) = \mathscr{D}(x, y, T^{-1}z)$$
$$\mathscr{C}(Ax, y, Tz) = \mathscr{D}(x, B^{-1}y, z)$$
$$\mathscr{C}(x, By, Tz) = \mathscr{D}(A^{-1}x, y, z)$$

bilinear system of

- $k(nm - k)$ equations
- $n^2 + m^2$ variables

combinatorial

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

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

algebraic

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

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