Twisted Hermitian Codes and the McEliece Cryptosystem

Bethany Matsick

Liberty University

January 26, 2018

Joint work with Austin Allen, Keller Blackwell, Olivia Fiol, Rutuja Kshirsagar, and Zoe Nelson, supervised by Gretchen Matthews.

Coding Theory

What is coding theory?

Coding theory studies the properties of codes and their various applications. Its goal is to provide reliable communication or reliable storage of data.

What are codes used for?

- Data transmission
- Data storage
- Error/correction
- Cryptography

The Hermitian code

Definition

Fix a prime power q, and let $\mathbb{F}_q$ be the finite field with q elements. A *Hermitian code* by the set

$$\mathcal{C}(\alpha P_\infty) := \{(f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(\alpha \mathcal{P}_\infty)\} \subseteq (\mathbb{F}_q)^n,$$

where

$$\mathcal{L}(\alpha P_\infty) = \langle 1, x, y, x^2, xy, y^2, x^3, x^2 y, \ldots, x^m y^n \rangle,$$

and m and n are the largest integers such that $mq + n(q+1) \leq \alpha$.

Example

A Hermitian code

Let $q = 5$ and $\alpha = 12$.

For every $x^i y^j$, we require that i and j satisfy the equation $5i + 6j \leq 12$. Thus,

$$\mathcal{L}(12P_\infty) = \langle 1, x, y, x^2, xy, y^2 \rangle.$$

Introduction to McEliece

The McEliece cryptosystem

- Public key cryptosystem
- Security based on code indistinguishability
- Candidate for use in the post-quantum era

The McEliece cryptosystem

Method of Encryption and Decryption

Let

- $S \in \mathbb{F}_q^{k \times k}$ be an invertible matrix.
- $P \in \mathbb{F}_q^{n \times n}$ be a permutation matrix.
- $G \in \mathbb{F}_q^{k \times n}$ be a generator matrix for a t-error correcting code.

Set $G^{pub} = SGP \in \mathbb{F}_q^{k \times n}$.

- Release (G^{pub}, t) as the public key.
- Keep $(S, D_{\mathcal{C}}, P)$ as the private key where $D_{\mathcal{C}}$ is an efficient decoding algorithm.

Encryption and Decryption

To send a private message $m = (m_1, m_2, ..., m_k) \in \mathbb{F}_q^k$,

- Multiply on the right by G^{pub} and add an error vector e of weight $\leq t$ to obtain

$$w = mG^{pub} + e = mSGP + e.$$

When w is received by the user holding the private key,

- Multiply by P^{-1} on the right to obtain $wP^{-1} = mSG + eP^{-1}$.
- Apply $D_{\mathcal{C}}$ to wP^{-1} to get mS.
- Multiply by S^{-1} on the right to obtain m.

Schur square

Definition

The *Schur square* of $\mathcal{C} \subseteq \mathbb{F}^n$ is

$$\mathcal{C}^2 = \langle \mathbf{a} * \mathbf{b} : \mathbf{a}, \mathbf{b} \in \mathcal{C} \rangle.$$

If $\mathcal{C}_k \subseteq \mathbb{F}^n$ has basis $\{b_1, b_2, ..., b_k\}$, then

$$\mathcal{C}_k^2 = \langle b_i * b_j : 1 \leq i, j \leq k \rangle.$$

Schur square dimension

How large can the Schur square be for a given code $\mathcal{C}$ of dimension k?

- The largest possible dimension of is $\binom{k+1}{2} = \frac{k(k+1)}{2}$.
- Since $\mathcal{C}^2 \subseteq \mathbb{F}^n$, its dimension cannot exceed n.
- Consequently, dim $\mathcal{C}^2 \leq min\{n, \binom{k+1}{2}\}$.

Schur squares and McEliece

Lemma

If $\mathcal{C} \subseteq \mathbb{F}^n$ is a code chosen at random from the set of all k-dimensional codes with $\binom{k+1}{2} < n$, then

$$Pr\left(dim\, \mathcal{C}_k^2 = \binom{k+1}{2}\right) = 1.$$

Goal: Choose families of codes such that G^{pub} behaves as the generator matrix of a random code. Given the above lemma, we seek codes with $\dim \mathcal{C}^2 = \binom{k+1}{2}$.

Example

Schur square of a Hermitian code

Let $q = 5$ and $\alpha = 12$. Then $\mathcal{L}(12P_\infty) = \langle 1, x, y, x^2, xy, y^2 \rangle$.

- Counting the basis elements, observe $k = 6$.
- Thus, we have $\binom{k+1}{2} = 21$.

Computing the Schur square, we find
$\mathcal{L}(12P_\infty)^2 = \langle 1, x, y, x^2, xy, y^2, \ldots, x^2y^2, xy^3, y^4 \rangle$.

- Counting the basis elements, we find $15 < 21$ basis elements.
- While not extremely low, this dimension is clearly less than the desired Schur square dimension.

Example

Three twists

Let $q = 5$ and $\alpha = 12$. Recall $\mathcal{L}(12P_\infty) = \langle 1, x, y, x^2, xy, y^2 \rangle$.

- To implement three "twists," let $\boldsymbol{h} = ((2,0),(1,1),(0,2))$ and $\boldsymbol{t} = ((4,-1),(7,0),(10,1))$.
- "Hooking" and "twisting" elements appropriately,

$$\mathcal{L}_{\boldsymbol{k},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}(12P_\infty) = \langle 1, x, y, x^2 + x^4 y, xy + x^7 y^2, y^2 + x^{10} y^3 \rangle.$$

Example

Three twists (continued)

- From the previous slide, recall

$$\mathcal{L}_{\boldsymbol{k},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}(12P_\infty) = \langle 1, x, y, x^2 + x^4 y, xy + x^7 y^2, y^2 + x^{10} y^3 \rangle.$$

  - Counting the basis elements, we find $k = 6$.
  - Thus, we desire a Schur square dimension of $\binom{6+1}{2} = \frac{6 \cdot 7}{2} = 21$.
- We indeed find that $dim\ \mathcal{L}_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}(12P_\infty)^2 = 21$.

Why did the twists raise the dimension so effectively?

Main ideas

- Hook elements with powers equal to the sums of other powers.
- Space out twists so that multiplied elements land in "gaps."
- Maintain linear independence of basis elements.

ℓ-Twisted Hermitian codes

Definition

We define an ℓ-twist Hermitian code to be

$$C_{\boldsymbol{k},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}(\alpha P_\infty) = ev(\langle f : f \in \mathcal{L}_{\boldsymbol{k},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}(\alpha P_\infty)\rangle), \text{ where}$$

$$\mathcal{L}_{\boldsymbol{k},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}(\alpha P_\infty) := \langle \{x^i y^j : 0 \leq i,\ 0 \leq j \leq q-1,\ iq + j(q+1) \leq \alpha,$$
$$(i,j) \neq (a_k, b_k), \forall k = 1, \ldots, \ell\} \cup \bigcup_{k=1}^{\ell} \left\{ x^{a_k} y^{b_k} + \eta_k x^{u+r_k} y^{v+s_k} \right\} \rangle.$$

General Twisted Hermitian codes

Then, if $\dim C_{\mathbf{k},\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = k$, we find that

$$\dim C_{\mathbf{k},\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)^2 \geq \binom{k+1}{2} - g.$$

References

P. Beelen, M. Bossert, S. Puchinger, J. Rosenkilde. Structural Properties of Twisted Reed-Solomon Codes with Applications to Cryptography, IEEE International Symposium on Information Theory, 2018.

P. Beelen, J.S.R. Nielsen. Sub-quadratic Decoding of One-Point Hermitian Codes, IEEE Transactions on Information Theory, 2015.

P. Beelen, S. Puchinger, J. Rosenkilde. Twisted Reed-Solomon Codes, IEEE International Symposium on Information Theory, 2017.

J. Walker. Codes and Curves, 2000.

Acknowledgements

Work completed collectively with Austin Allen, Keller Blackwell, Olivia Fiol, Rutuja Kshirsagar, and Zoe Nelson, supervised by Gretchen Matthews.

The twisted construction is a variant of that considered by Peter Beelen, Martin Bossert, Sven Puchinger, and Johan Rosenkilde.

Special thanks to Liberty University for providing assistance with the cost of travel.