Hermitian-Lifted Codes

Beth Malmskog
Joint work with Hiram H. López, Gretchen Matthews, Fernando Piñero-González, Mary Wootters

COGNAC

February 14, 2023

Goal: Locally Recoverable Codes with Many Recovery Sets

Maybe we want to store our information in the cloud! What could go wrong there?

Photos from telegraph.co.uk and gizmodo.com

Goal: Locally Recoverable Codes with Many Recovery Sets

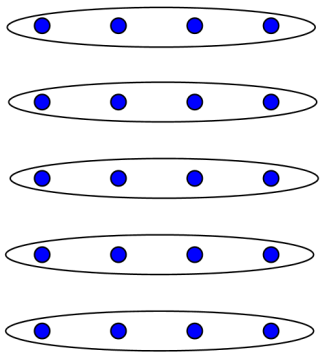
Maybe we want to store our information in the cloud! What could go wrong there?

Photos from telegraph.co.uk and gizmodo.com

- A code C is locally recoverable with *locality* r if any erased codeword symbol can be recovered by accessing at most r other symbols ($1 \leq r \leq k$)
- The set of symbols used to recover c_i is called the *recovery set* for the i^{th} position.

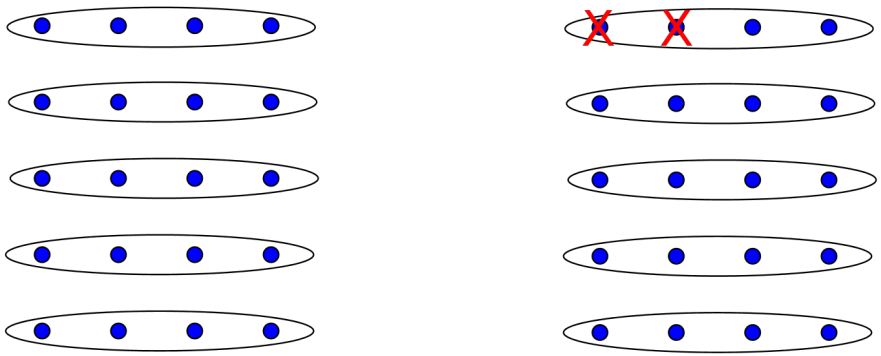
Goal: Locally Recoverable Codes with Many Recovery Sets

- An error correcting code C is locally recoverable with *locality* r if any erased codeword symbol can be recovered by accessing at most r other symbols ($1 \leq r \leq k$)
- The set of symbols used to recover c_i is called the *recovery set* for the i^{th} position.



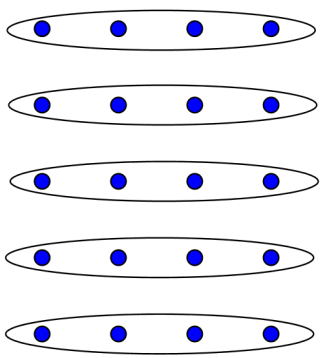
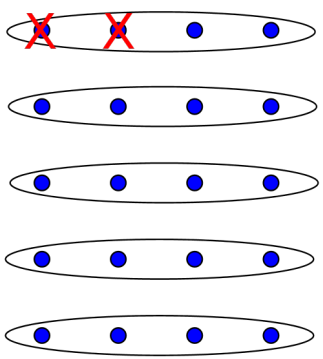
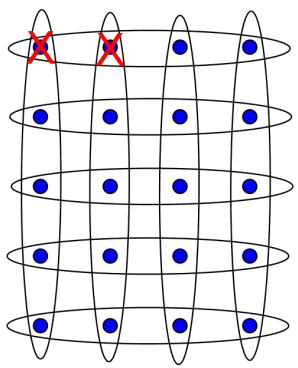
Goal: Locally Recoverable Codes with Many Recovery Sets

- An error correcting code C is locally recoverable with *locality* r if any erased codeword symbol can be recovered by accessing at most r other symbols ($1 \leq r \leq k$)
- The set of symbols used to recover c_i is called the *recovery set* for the i^{th} position.



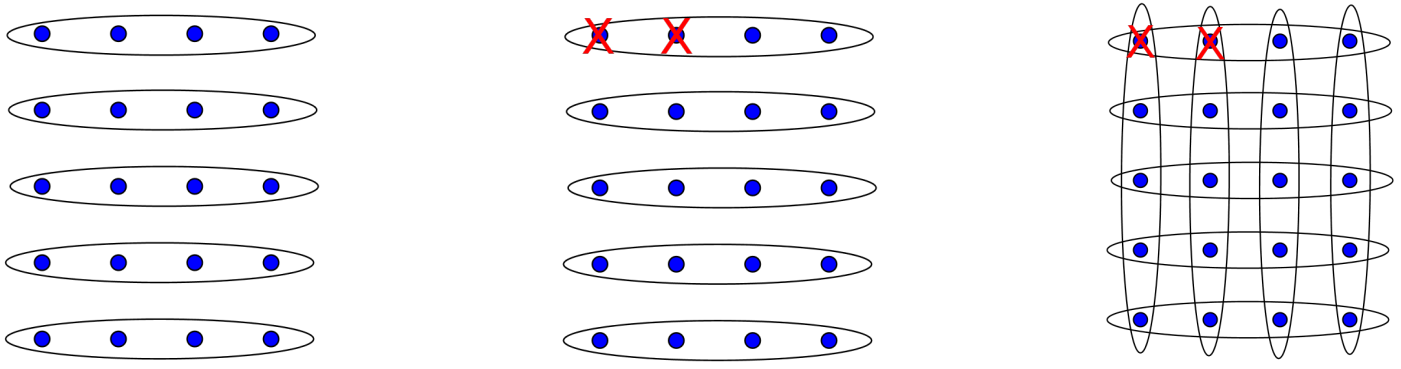
Goal: Locally Recoverable Codes with Many Recovery Sets

- An error correcting code C is locally recoverable with *locality* r if any erased codeword symbol can be recovered by accessing at most r other symbols ($1 \leq r \leq k$)
- The set of symbols used to recover c_i is called the *recovery set* for the i^{th} position.

Goal: Locally Recoverable Codes with Many Recovery Sets

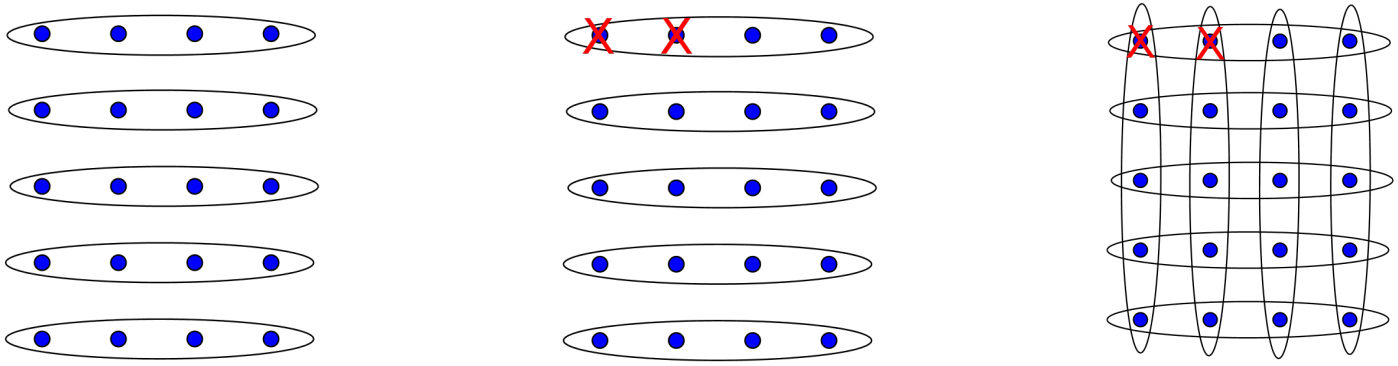
- An error correcting code C is locally recoverable with *locality* r if any erased codeword symbol can be recovered by accessing at most r other symbols ($1 \leq r \leq k$)
- The set of symbols used to recover c_i is called the *recovery set* for the i^{th} position.



- A locally recoverable code with t recovery sets for each symbol is said to have *availability* t, and is denoted as an LRC(t).

Goal: Locally Recoverable Codes with Many Recovery Sets

- An error correcting code C is locally recoverable with *locality* r if any erased codeword symbol can be recovered by accessing at most r other symbols ($1 \leq r \leq k$)
- The set of symbols used to recover c_i is called the *recovery set* for the i^{th} position.



- A locally recoverable code with t recovery sets for each symbol is said to have *availability* t, and is denoted as an LRC(t).

Geometry can naturally give rise to the extra structure necessary for LRC(t)s. In this talk, we will discuss a way to construct these codes using curves over finite fields, how to determine the exact minimum distance in many cases, and example parameters.

What Parameters are Possible? Good?

Possible: Tamo, Barg, and Frolov (2016):

$$d \leq n - \sum_{i=0}^{t} \left\lfloor \frac{k-1}{r^i} \right\rfloor, \qquad \frac{k}{n} \leq \frac{1}{\prod_{j=1}^{t} \left(1 + \frac{1}{jr}\right)}.$$

Not known to be sharp for all primes, localities, and availabilities.

What Parameters are Possible? Good?

Possible: Tamo, Barg, and Frolov (2016):

$$d \leq n - \sum_{i=0}^{t} \left\lfloor \frac{k-1}{r^i} \right\rfloor, \qquad \frac{k}{n} \leq \frac{1}{\prod_{j=1}^{t} \left(1 + \frac{1}{jr}\right)}.$$

Not known to be sharp for all primes, localities, and availabilities.
Good: It depends:

- Cloud storage: fairly small availability $t = O(1)$. Minimum distance is still of interest.
- Very large availability $t = \Omega(n)$ are equivalent to locally decodable codes, of interest in theoretical computer science, complexity theory, for private information retrieval. Global minimum distance may not matter much but rate does.
- Intermediate: bridge between two settings.

The Hermitian Curve

Finite field geometric candy:

$$\mathcal{H}_q : x^{q+1} = y^q + y$$

$$X^{q+1} = Y^q Z + Y Z^q$$

- Smooth, Irreducible, one point at infinity $[0 : 1 : 0]$.
- $g = \frac{q(q-1)}{2}$.
- $q^3 + 1$ points over $\mathbb{F}_{q^2}$, maximal over this field.
- Maximal genus for $\mathbb{F}_{q^2}$-maximal curve.
- Maximum symmetry: $|Aut(\mathcal{H}_q)| > 16g^4$.
- Every line in $\mathbb{P}^2$ intersects $\mathcal{H}_q$ in 1 or $q + 1$ points.

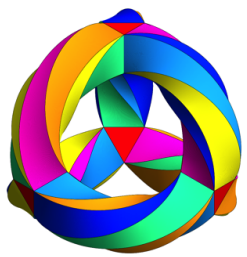
The Hermitian Curve

Finite field geometric candy:

$$\mathcal{H}_q : x^{q+1} = y^q + y$$

$$X^{q+1} = Y^q Z + Y Z^q$$

- Smooth, Irreducible, one point at infinity $[0 : 1 : 0]$.
- $g = \frac{q(q-1)}{2}$.
- $q^3 + 1$ points over $\mathbb{F}_{q^2}$, maximal over this field.
- Maximal genus for $\mathbb{F}_{q^2}$-maximal curve.
- Maximum symmetry: $|Aut(\mathcal{H}_q)| > 16g^4$.
- Every line in $\mathbb{P}^2$ intersects $\mathcal{H}_q$ in 1 or $q + 1$ points.



$$x^4 = y^3 + y$$

images of Klein Quartic from Greg Egan, via website of John Baez

Evaluation Codes

Could also use points on a higher dimensional variety. Given a projective variety $\mathcal{V}$ defined over a field $K = \mathbb{F}_q$:

- Let $A = \{P_1, P_2, \ldots, P_n\} \subset \mathcal{V}(\mathbb{F}_q) \setminus \{P_s\}$.
- For $f \in \mathbb{F}_q(\mathcal{V})$, let $f(A) = (f(P_1), f(P_2), \ldots, f(P_n))$.
- Let $\mathcal{L}$ be a linear space of functions on $\mathcal{V}$ with no poles in A.
- Define the evaluation code $C(A, \mathcal{L}) = \{f(A) : f \in \mathcal{L}\}$.

Evaluation Codes

Could also use points on a higher dimensional variety. Given a projective variety $\mathcal{V}$ defined over a field $K = \mathbb{F}_q$:

- Let $A = \{P_1, P_2, \ldots, P_n\} \subset \mathcal{V}(\mathbb{F}_q) \setminus \{P_s\}$.
- For $f \in \mathbb{F}_q(\mathcal{V})$, let $f(A) = (f(P_1), f(P_2), \ldots, f(P_n))$.
- Let $\mathcal{L}$ be a linear space of functions on $\mathcal{V}$ with no poles in A.
- Define the evaluation code $C(A, \mathcal{L}) = \{f(A) : f \in \mathcal{L}\}$.

If $\mathcal{V} = \mathbb{P}^1$, $P_s = P_\infty$, $A = \{a : a \in \mathbb{F}_q\}$, $\mathcal{L}$ is polynomials of degree $< k$, then $C(\mathcal{L}, A) = RS(q, k)$.

Evaluation Codes

Could also use points on a higher dimensional variety. Given a projective variety $\mathcal{V}$ defined over a field $K = \mathbb{F}_q$:

- Let $A = \{P_1, P_2, \ldots, P_n\} \subset \mathcal{V}(\mathbb{F}_q) \setminus \{P_s\}$.
- For $f \in \mathbb{F}_q(\mathcal{V})$, let $f(A) = (f(P_1), f(P_2), \ldots, f(P_n))$.
- Let $\mathcal{L}$ be a linear space of functions on $\mathcal{V}$ with no poles in A.
- Define the evaluation code $C(A, \mathcal{L}) = \{f(A) : f \in \mathcal{L}\}$.

If $\mathcal{V} = \mathbb{P}^1$, $P_s = P_\infty$, $A = \{a : a \in \mathbb{F}_q\}$, $\mathcal{L}$ is polynomials of degree $< k$, then $C(\mathcal{L}, A) = RS(q, k)$.

If $\mathcal{V} = \mathcal{H}_q$, $K = \mathbb{F}_{q^2}$, $0 < m \leq q^3$, and $A = \mathcal{V}(\mathbb{F}_{q^2}) \setminus P_\infty$,
$\mathcal{L} = \mathcal{L}(mP_\infty) = \langle x^i y^j : 0 \leq j \leq q-1, iq + j(q+1) \leq m \rangle$,then
$C(\mathcal{L}, A) = C_{q,m}$ is the **one-point** Goppa code on the Hermitian curve, with length $n = q^3$, dimension $k \geq m - g + 1$, and minimum distance $d \geq n - m$.

Evaluation Codes

Could also use points on a higher dimensional variety. Given a projective variety $\mathcal{V}$ defined over a field $K = \mathbb{F}_q$:

- Let $A = \{P_1, P_2, \ldots, P_n\} \subset \mathcal{V}(\mathbb{F}_q) \setminus \{P_s\}$.
- For $f \in \mathbb{F}_q(\mathcal{V})$, let $f(A) = (f(P_1), f(P_2), \ldots, f(P_n))$.
- Let $\mathcal{L}$ be a linear space of functions on $\mathcal{V}$ with no poles in A.
- Define the evaluation code $C(A, \mathcal{L}) = \{f(A) : f \in \mathcal{L}\}$.

If $\mathcal{V} = \mathbb{P}^1$, $P_s = P_\infty$, $A = \{a : a \in \mathbb{F}_q\}$, $\mathcal{L}$ is polynomials of degree $< k$, then $C(\mathcal{L}, A) = RS(q, k)$.

If $\mathcal{V} = \mathcal{H}_q$, $K = \mathbb{F}_{q^2}$, $0 < m \leq q^3$, and $A = \mathcal{V}(\mathbb{F}_{q^2}) \setminus P_\infty$, $\mathcal{L} = \mathcal{L}(mP_\infty) = \langle x^i y^j : 0 \leq j \leq q-1, iq + j(q+1) \leq m \rangle$,then $C(\mathcal{L}, A) = C_{q,m}$ is the **one-point** Goppa code on the Hermitian curve, with length $n = q^3$, dimension $k \geq m - g + 1$, and minimum distance $d \geq n - m$.

If $\mathcal{V} = \mathbb{P}^m$, A is the set of affine points, $\mathcal{L}$ is the space of m-variate polynomials over $\mathbb{F}_q$ of total degree at most v, then $C(\mathcal{L}, A)$ is the q-ary Reed-Muller code $RM_q(v, m)$.

AG Local Recovery Simplest Case: Local Recovery of Reed-Muller Codes

Reed-Muller codes with $v < q - 1$ are locally recoverable as follows:

- Each codeword corresponds to a multivariate polynomial f, which restricts on any fixed line in $(\mathbb{F}_q)^m$ to a univariate polynomial $\tilde{f}$ of degree at most v.
- Since each line in $(\mathbb{F}_q)^m$ has q points, the value of $\tilde{f}$ at any point P can be interpolated from its value on the remaining $q - 1$ points on the line.

AG Local Recovery Simplest Case: Local Recovery of Reed-Muller Codes

Reed-Muller codes with $v < q - 1$ are locally recoverable as follows:

- Each codeword corresponds to a multivariate polynomial f, which restricts on any fixed line in $(\mathbb{F}_q)^m$ to a univariate polynomial $\tilde{f}$ of degree at most v.
- Since each line in $(\mathbb{F}_q)^m$ has q points, the value of $\tilde{f}$ at any point P can be interpolated from its value on the remaining $q - 1$ points on the line.
- Pro: MANY recovery sets for each position!

AG Local Recovery Simplest Case: Local Recovery of Reed-Muller Codes

Reed-Muller codes with $v < q - 1$ are locally recoverable as follows:

- Each codeword corresponds to a multivariate polynomial f, which restricts on any fixed line in $(\mathbb{F}_q)^m$ to a univariate polynomial $\tilde{f}$ of degree at most v.
- Since each line in $(\mathbb{F}_q)^m$ has q points, the value of $\tilde{f}$ at any point P can be interpolated from its value on the remaining $q - 1$ points on the line.
- Pro: MANY recovery sets for each position!
- Con: VERY low rate.

Connecting with Curves: Local Recovery of Hermitian Codes by Lines

One-point Hermitian codes can be thought of as punctured subcodes of Reed-Muller codes, and can be locally recovered by the same idea.

Observation: the one-point code $C_{q,m}$ is locally recoverable with locality q and availability $q^2 - 1$ for all $m \leq q^2 - 1$.

Connecting with Curves: Local Recovery of Hermitian Codes by Lines

One-point Hermitian codes can be thought of as punctured subcodes of Reed-Muller codes, and can be locally recovered by the same idea.

Observation: the one-point code $C_{q,m}$ is locally recoverable with locality q and availability $q^2 - 1$ for all $m \leq q^2 - 1$.

- There are $q^2 - 1$ $\mathbb{F}_{q^2}$-rational non-horizontal, non-tangent lines $L_{\alpha,\beta}(t) = (\alpha t + \beta, t)$ through each point of $\mathcal{H}_q(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$, each intersecting the curve in exactly $q + 1$ non-infinite points.

Connecting with Curves: Local Recovery of Hermitian Codes by Lines

One-point Hermitian codes can be thought of as punctured subcodes of Reed-Muller codes, and can be locally recovered by the same idea.

Observation: the one-point code $C_{q,m}$ is locally recoverable with locality q and availability $q^2 - 1$ for all $m \leq q^2 - 1$.

- There are $q^2 - 1$ $\mathbb{F}_{q^2}$-rational non-horizontal, non-tangent lines $L_{\alpha,\beta}(t) = (\alpha t + \beta, t)$ through each point of $\mathcal{H}_q(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$, each intersecting the curve in exactly $q + 1$ non-infinite points.
- If the position corresponding to point P is erased in the codeword arising from $f \in \mathcal{L} = \langle x^i y^j : 0 \leq j \leq q - 1, iq + j(q + 1) \leq m \rangle$, we can check that f has total degree at most $q - 1$, so $f(P)$ can be interpolated from the value of f on the other q points on $\mathcal{H}_q(\mathbb{F}_{q^2}) \cap \mathrm{Im}(L_{\alpha,\beta}(t))$.

AG Local Recovery Improvement: Lifted Codes

- Lifted Codes were introduced by Guo, Kopparty and Sudan in 2013 to boost the rate of Reed-Muller codes for local decoding.
- Idea: Take a code of short block length and lift to a long code by requiring that each codeword of the long code restricts to a codeword of the short code on every subspace of the original dimension.
- Can lift Reed-Solomon code of length q to length q^m, obtaining a code that contains the largest corresponding Reed-Muller code.

AG Local Recovery Improvement: Lifted Codes

- Lifted Codes were introduced by Guo, Kopparty and Sudan in 2013 to boost the rate of Reed-Muller codes for local decoding.
- Idea: Take a code of short block length and lift to a long code by requiring that each codeword of the long code restricts to a codeword of the short code on every subspace of the original dimension.
- Can lift Reed-Solomon code of length q to length q^m, obtaining a code that contains the largest corresponding Reed-Muller code.
- Key idea-some multivariate polynomials of high total degree reduce to low-degree polynomials on $\mathbb{F}_q$-points of rational lines in $(\mathbb{F}_q)^m$. Observed earlier by Friedl and Sudan, but Guo, Kopparty, and Sudan showed that there are in fact many such polynomials!

Lifted Reed Solomon Code Example

Let $M_{a,b}(x, y) = x^a y^b$, and let $L_{\alpha,\beta}(t) = (\alpha t + \beta, t)$ be the parameterization of a non-horizontal $\mathbb{F}_q$-rational line in $(\mathbb{F}_q)^2$.

Lifted Reed Solomon Code Example

Let $M_{a,b}(x, y) = x^a y^b$, and let $L_{\alpha,\beta}(t) = (\alpha t + \beta, t)$ be the parameterization of a non-horizontal $\mathbb{F}_q$-rational line in $(\mathbb{F}_q)^2$.

Then $M_{a,b} \circ L_{\alpha,\beta} = (\alpha t + \beta)^a t^b$ is a univariate polynomial of degree at most $q - 1$ after reducing.

Lifted Reed Solomon Code Example

Let $M_{a,b}(x, y) = x^a y^b$, and let $L_{\alpha,\beta}(t) = (\alpha t + \beta, t)$ be the parameterization of a non-horizontal $\mathbb{F}_q$-rational line in $(\mathbb{F}_q)^2$.

Then $M_{a,b} \circ L_{\alpha,\beta} = (\alpha t + \beta)^a t^b$ is a univariate polynomial of degree at most $q - 1$ after reducing.

Say $M_{a,b}$ is *good* if the degree of $M_{a,b} \circ L_{\alpha,\beta}$ is at most $q - 2$ after reduction for all $\alpha, \beta \in \mathbb{F}_q$.

Lifted Reed Solomon Code Example

Let $M_{a,b}(x, y) = x^a y^b$, and let $L_{\alpha,\beta}(t) = (\alpha t + \beta, t)$ be the parameterization of a non-horizontal $\mathbb{F}_q$-rational line in $(\mathbb{F}_q)^2$.

Then $M_{a,b} \circ L_{\alpha,\beta} = (\alpha t + \beta)^a t^b$ is a univariate polynomial of degree at most $q - 1$ after reducing.

Say $M_{a,b}$ is *good* if the degree of $M_{a,b} \circ L_{\alpha,\beta}$ is at most $q - 2$ after reduction for all $\alpha, \beta \in \mathbb{F}_q$.

- Let $q = 8$, $m = 2$. Then the monomial $M_{6,6} = x^6 y^6$ has total degree 12, but on the line $x = t, y = t$, we have $M_{6,6} \circ L_{1,0} = t^{12} = t^5$ when $t \in \mathbb{F}_8$.

Lifted Reed Solomon Code Example

Let $M_{a,b}(x,y) = x^a y^b$, and let $L_{\alpha,\beta}(t) = (\alpha t + \beta, t)$ be the parameterization of a non-horizontal $\mathbb{F}_q$-rational line in $(\mathbb{F}_q)^2$.

Then $M_{a,b} \circ L_{\alpha,\beta} = (\alpha t + \beta)^a t^b$ is a univariate polynomial of degree at most $q-1$ after reducing.

Say $M_{a,b}$ is *good* if the degree of $M_{a,b} \circ L_{\alpha,\beta}$ is at most $q-2$ after reduction for all $\alpha, \beta \in \mathbb{F}_q$.

- Let $q = 8$, $m = 2$. Then the monomial $M_{6,6} = x^6 y^6$ has total degree 12, but on the line $x = t, y = t$, we have $M_{6,6} \circ L_{1,0} = t^{12} = t^5$ when $t \in \mathbb{F}_8$.
- More generally,

$$M_{6,6} \circ L_{\alpha,\beta} = (\alpha t + \beta)^6 t^6 = \alpha^6 t^{12} + 3\alpha^4 \beta^2 t^{10} + 3\alpha^2 \beta^4 t^8 + \beta^6 t^6$$
$$= \beta^6 t^6 + \alpha^6 t^5 + \alpha^4 \beta^2 t^3 + \alpha^2 \beta^4 t.$$

Lifted Reed Solomon Code Example

Let $M_{a,b}(x,y) = x^a y^b$, and let $L_{\alpha,\beta}(t) = (\alpha t + \beta, t)$ be the parameterization of a non-horizontal $\mathbb{F}_q$-rational line in $(\mathbb{F}_q)^2$.

Then $M_{a,b} \circ L_{\alpha,\beta} = (\alpha t + \beta)^a t^b$ is a univariate polynomial of degree at most $q-1$ after reducing.

Say $M_{a,b}$ is *good* if the degree of $M_{a,b} \circ L_{\alpha,\beta}$ is at most $q-2$ after reduction for all $\alpha, \beta \in \mathbb{F}_q$.

- Let $q = 8$, $m = 2$. Then the monomial $M_{6,6} = x^6 y^6$ has total degree 12, but on the line $x = t, y = t$, we have $M_{6,6} \circ L_{1,0} = t^{12} = t^5$ when $t \in \mathbb{F}_8$.
- More generally,

$$M_{6,6} \circ L_{\alpha,\beta} = (\alpha t + \beta)^6 t^6 = \alpha^6 t^{12} + 3\alpha^4 \beta^2 t^{10} + 3\alpha^2 \beta^4 t^8 + \beta^6 t^6$$
$$= \beta^6 t^6 + \alpha^6 t^5 + \alpha^4 \beta^2 t^3 + \alpha^2 \beta^4 t.$$

- In this case, there are 28 monomials $M_{a,b}$ with total degree at most 6, but there are 37 good monomials.

Lifted Reed Solomon Code Example

Let $M_{a,b}(x,y) = x^a y^b$, and let $L_{\alpha,\beta}(t) = (\alpha t + \beta, t)$ be the parameterization of a non-horizontal $\mathbb{F}_q$-rational line in $(\mathbb{F}_q)^2$.

Then $M_{a,b} \circ L_{\alpha,\beta} = (\alpha t + \beta)^a t^b$ is a univariate polynomial of degree at most $q-1$ after reducing.

Say $M_{a,b}$ is *good* if the degree of $M_{a,b} \circ L_{\alpha,\beta}$ is at most $q-2$ after reduction for all $\alpha, \beta \in \mathbb{F}_q$.

- Let $q = 8$, $m = 2$. Then the monomial $M_{6,6} = x^6 y^6$ has total degree 12, but on the line $x = t, y = t$, we have $M_{6,6} \circ L_{1,0} = t^{12} = t^5$ when $t \in \mathbb{F}_8$.
- More generally,

$$M_{6,6} \circ L_{\alpha,\beta} = (\alpha t + \beta)^6 t^6 = \alpha^6 t^{12} + 3\alpha^4 \beta^2 t^{10} + 3\alpha^2 \beta^4 t^8 + \beta^6 t^6$$
$$= \beta^6 t^6 + \alpha^6 t^5 + \alpha^4 \beta^2 t^3 + \alpha^2 \beta^4 t.$$

- In this case, there are 28 monomials $M_{a,b}$ with total degree at most 6, but there are 37 good monomials. When $q = 16$, have 120 monomials of small total degree but 155 good monomials.

Who's Good?

Let $q = 2^h$.

$$M_{a,b} \circ L_{\alpha,\beta} = (\alpha t + \beta)^a t^b = \sum_{i=0}^{a} \binom{a}{i} \alpha^i \beta^{a-i} t^{i+b} = \sum_{i=0}^{q-1} c_i t^i,$$

for some $c_i \in \mathbb{F}_{q^2}$.

Who's Good?

Let $q = 2^h$.

$$M_{a,b} \circ L_{\alpha,\beta} = (\alpha t + \beta)^a t^b = \sum_{i=0}^{a} \binom{a}{i} \alpha^i \beta^{a-i} t^{i+b} = \sum_{i=0}^{q-1} c_i t^i,$$

for some $c_i \in \mathbb{F}_{q^2}$.

Since $a + b \leq 2(q-1)$, we know

$$c_{q-1} = \binom{a}{q-1-b} \alpha^{q-1-b} \beta^{a+b-(q-1)}.$$

$M_{a,b}$ is good if $c_{q-1} = 0$, which will occur if $2 | \binom{a}{q-1-b}$.

Who's Good?

Who's Good?

If $0 \leq f \leq g$ are integers, we say f is in the **2-shadow** of g if every binary digit of f is less than or equal to the corresponding binary digit of g.

Theorem (Lucas)

The quantity $\binom{g}{f}$ *is even iff* f *is not in the 2-shadow of* g.

Who's Good?

If $0 \leq f \leq g$ are integers, we say f is in the **2-shadow** of g if every binary digit of f is less than or equal to the corresponding binary digit of g.

Theorem (Lucas)

The quantity $\binom{g}{f}$ *is even iff* f *is not in the 2-shadow of* g*.*

So $M_{a,b}$ is good when $q-1-b$ is not in the 2-shadow of a, so b has a 0 in at least one place where a has a 0. By symmetry, this will mean that $q-1-a$ is not in the 2-shadow of b (meaning $M_{a,b}$ is also good on horizontal lines).

Who's Good?

If $0 \leq f \leq g$ are integers, we say f is in the **2-shadow** of g if every binary digit of f is less than or equal to the corresponding binary digit of g.

Theorem (Lucas)

The quantity $\binom{g}{f}$ *is even iff* f *is not in the 2-shadow of* g*.*

So $M_{a,b}$ is good when $q-1-b$ is not in the 2-shadow of a, so b has a 0 in at least one place where a has a 0. By symmetry, this will mean that $q-1-a$ is not in the 2-shadow of b (meaning $M_{a,b}$ is also good on horizontal lines).
This is not uncommon! As $h \to \infty$, $\frac{k}{n} \to 1$.

Hermitian-Lifted Codes

The Hermitian-lifted code over $\mathbb{F}_{q^2}$ combines the local recovery method on the one-point Hermitian code with the notion of lifting. Let:

Hermitian-Lifted Codes

The Hermitian-lifted code over $\mathbb{F}_{q^2}$ combines the local recovery method on the one-point Hermitian code with the notion of lifting. Let:

- A be the set of affine points in $\mathcal{H}_q(\mathbb{F}_{q^2})$

Hermitian-Lifted Codes

The Hermitian-lifted code over $\mathbb{F}_{q^2}$ combines the local recovery method on the one-point Hermitian code with the notion of lifting. Let:

- A be the set of affine points in $\mathcal{H}_q(\mathbb{F}_{q^2})$
- $L = \{L_{\alpha,\beta}(t) = (\alpha t + \beta, t) : \alpha, \beta \in \mathbb{F}_{q^2}, L_{\alpha,\beta} \text{ not tangent to } \mathcal{H}_q\}$.

Hermitian-Lifted Codes

The Hermitian-lifted code over $\mathbb{F}_{q^2}$ combines the local recovery method on the one-point Hermitian code with the notion of lifting. Let:

- A be the set of affine points in $\mathcal{H}_q(\mathbb{F}_{q^2})$
- $L = \{L_{\alpha,\beta}(t) = (\alpha t + \beta, t) : \alpha, \beta \in \mathbb{F}_{q^2}, L_{\alpha,\beta} \text{ not tangent to } \mathcal{H}_q\}$.
- $p_{\alpha,\beta}(t) = t^{q+1} + \alpha^q t^q + \alpha t + (\beta + \beta^q)$

Hermitian-Lifted Codes

The Hermitian-lifted code over $\mathbb{F}_{q^2}$ combines the local recovery method on the one-point Hermitian code with the notion of lifting. Let:

- A be the set of affine points in $\mathcal{H}_q(\mathbb{F}_{q^2})$
- $L = \{L_{\alpha,\beta}(t) = (\alpha t + \beta, t) : \alpha, \beta \in \mathbb{F}_{q^2}, L_{\alpha,\beta} \text{ not tangent to } \mathcal{H}_q\}$.
- $p_{\alpha,\beta}(t) = t^{q+1} + \alpha^q t^q + \alpha t + (\beta + \beta^q)$
- $[g(t)]_{\alpha,\beta} \equiv g(t) \mod p_{\alpha,\beta}$ with $\deg([g(t)]_{\alpha,\beta}) \leq q$ (for $g(t) \in \mathbb{F}_{q^2}[t]$)

Hermitian-Lifted Codes

The Hermitian-lifted code over $\mathbb{F}_{q^2}$ combines the local recovery method on the one-point Hermitian code with the notion of lifting. Let:

- A be the set of affine points in $\mathcal{H}_q(\mathbb{F}_{q^2})$
- $L = \{L_{\alpha,\beta}(t) = (\alpha t + \beta, t) : \alpha, \beta \in \mathbb{F}_{q^2}, L_{\alpha,\beta} \text{ not tangent to } \mathcal{H}_q\}$.
- $p_{\alpha,\beta}(t) = t^{q+1} + \alpha^q t^q + \alpha t + (\beta + \beta^q)$
- $[g(t)]_{\alpha,\beta} \equiv g(t) \mod p_{\alpha,\beta}$ with $\deg([g(t)]_{\alpha,\beta}) \leq q$ (for $g(t) \in \mathbb{F}_{q^2}[t]$)
- $\mathcal{R} = \langle x^i y^j : 0 \leq i \leq q^2, 0 \leq j \geq q \rangle$

Hermitian-Lifted Codes

The Hermitian-lifted code over $\mathbb{F}_{q^2}$ combines the local recovery method on the one-point Hermitian code with the notion of lifting. Let:

- A be the set of affine points in $\mathcal{H}_q(\mathbb{F}_{q^2})$
- $L = \{L_{\alpha,\beta}(t) = (\alpha t + \beta, t) : \alpha, \beta \in \mathbb{F}_{q^2}, L_{\alpha,\beta} \text{ not tangent to } \mathcal{H}_q\}$.
- $p_{\alpha,\beta}(t) = t^{q+1} + \alpha^q t^q + \alpha t + (\beta + \beta^q)$
- $[g(t)]_{\alpha,\beta} \equiv g(t) \mod p_{\alpha,\beta}$ with $\deg([g(t)]_{\alpha,\beta}) \leq q$ (for $g(t) \in \mathbb{F}_{q^2}[t]$)
- $\mathcal{R} = \langle x^i y^j : 0 \leq i \leq q^2, 0 \leq j \geq q \rangle$
- $\mathcal{F} = \{F \in \mathcal{R} : \deg([F \circ L_{\alpha,\beta}(t)]_{\alpha,\beta}) \leq q - 1 \text{ for all } L_{\alpha,\beta} \in L\}$

Hermitian-Lifted Codes

The Hermitian-lifted code over $\mathbb{F}_{q^2}$ combines the local recovery method on the one-point Hermitian code with the notion of lifting. Let:

- A be the set of affine points in $\mathcal{H}_q(\mathbb{F}_{q^2})$
- $L = \{L_{\alpha,\beta}(t) = (\alpha t + \beta, t) : \alpha, \beta \in \mathbb{F}_{q^2}, L_{\alpha,\beta} \text{ not tangent to } \mathcal{H}_q\}$.
- $p_{\alpha,\beta}(t) = t^{q+1} + \alpha^q t^q + \alpha t + (\beta + \beta^q)$
- $[g(t)]_{\alpha,\beta} \equiv g(t) \mod p_{\alpha,\beta}$ with $\deg([g(t)]_{\alpha,\beta}) \leq q$ (for $g(t) \in \mathbb{F}_{q^2}[t]$)
- $\mathcal{R} = \langle x^i y^j : 0 \leq i \leq q^2, 0 \leq j \geq q \rangle$
- $\mathcal{F} = \{F \in \mathcal{R} : \deg([F \circ L_{\alpha,\beta}(t)]_{\alpha,\beta}) \leq q - 1 \text{ for all } L_{\alpha,\beta} \in L\}$

The Hermitian-lifted code is $\mathcal{C} = C(A, \mathcal{F})$.

Observations

Observations

- Like $C_{q,m}$, the code $\mathcal{C}$ has local recovery on $q^2 - 1$ non-vertical, non-tangent lines passing through each evaluation point, so is an LRC$(q^2 - 1)$ with locality q.

Observations

- Like $C_{q,m}$, the code $\mathcal{C}$ has local recovery on $q^2 - 1$ non-vertical, non-tangent lines passing through each evaluation point, so is an LRC$(q^2 - 1)$ with locality q.
- The minimum distance of code $\mathcal{C}$ has bounds $q^2 \leq d \leq q^3 - q^2 + 1$.

Observations

- Like $C_{q,m}$, the code $\mathcal{C}$ has local recovery on $q^2 - 1$ non-vertical, non-tangent lines passing through each evaluation point, so is an LRC$(q^2 - 1)$ with locality q.
- The minimum distance of code $\mathcal{C}$ has bounds $q^2 \leq d \leq q^3 - q^2 + 1$.

Theorem (López, M., Matthews,Piñero-González, Wootters, 2021)

Suppose that $q \geq 4$ is a power of 2. Then the rate of $\mathcal{C}$ is bounded below by the constant 0.007.

Good monomials result from both Lucas' theorem and interaction of line and curve equations.
Very recent work by Piñero-González and REU students improves bound to 0.1

Example of a good monomial.

Let $q = 4$. Then $\mathcal{H}_4 : y^4 + y = x^5$ over $\mathbb{F}_{16}$. We saw that $C_{4,15} \subseteq \mathcal{C}$. Consider $f(x, y) := x^8 y^2$

Example of a good monomial.

Let $q = 4$. Then $\mathcal{H}_4 : y^4 + y = x^5$ over $\mathbb{F}_{16}$. We saw that $C_{4,15} \subseteq \mathcal{C}$. Consider $f(x, y) := x^8 y^2 \in \mathcal{L}(42P_\infty) \setminus \mathcal{L}(15P_\infty)$.

Example of a good monomial.

Let $q = 4$. Then $\mathcal{H}_4 : y^4 + y = x^5$ over $\mathbb{F}_{16}$. We saw that $C_{4,15} \subseteq \mathcal{C}$. Consider $f(x, y) := x^8 y^2 \in \mathcal{L}(42P_\infty) \setminus \mathcal{L}(15P_\infty)$.

Claim: $x^8 y^2 \in \mathcal{F}$

Example of a good monomial.

Let $q = 4$. Then $\mathcal{H}_4 : y^4 + y = x^5$ over $\mathbb{F}_{16}$. We saw that $C_{4,15} \subseteq \mathcal{C}$. Consider $f(x, y) := x^8 y^2 \in \mathcal{L}(42P_\infty) \setminus \mathcal{L}(15P_\infty)$.

Claim: $x^8 y^2 \in \mathcal{F}$

Note that

$$x^8 y^2 \circ L_{\alpha,\beta}(t) = t^8(\alpha t + \beta)^2 = \alpha^2 t^{10} + \beta^2 t^8,$$

and

$$p_{\alpha,\beta} = t^5 + \alpha^4 t^4 + \alpha t + (\beta + \beta^4).$$

So:

$t^6 \equiv \alpha^4 t^5 + \alpha t^2 + \text{deg } 1 \equiv \alpha^8 t^4 + \alpha t^2 + \text{deg } 1,$

Example of a good monomial.

Let $q = 4$. Then $\mathcal{H}_4 : y^4 + y = x^5$ over $\mathbb{F}_{16}$. We saw that $C_{4,15} \subseteq \mathcal{C}$. Consider $f(x, y) := x^8 y^2 \in \mathcal{L}(42P_\infty) \setminus \mathcal{L}(15P_\infty)$.

Claim: $x^8 y^2 \in \mathcal{F}$

Note that

$$x^8 y^2 \circ L_{\alpha,\beta}(t) = t^8(\alpha t + \beta)^2 = \alpha^2 t^{10} + \beta^2 t^8,$$

and

$$p_{\alpha,\beta} = t^5 + \alpha^4 t^4 + \alpha t + (\beta + \beta^4).$$

So:

$t^6 \equiv \alpha^4 t^5 + \alpha t^2 + \text{deg } 1 \equiv \alpha^8 t^4 + \alpha t^2 + \text{deg } 1,$

$t^7 \equiv \alpha^8 t^5 + \alpha t^3 + \text{deg } 2 \equiv \alpha^{12} t^4 + \alpha t^3 + \text{deg } 2,$

Example of a good monomial.

Let $q = 4$. Then $\mathcal{H}_4 : y^4 + y = x^5$ over $\mathbb{F}_{16}$. We saw that $C_{4,15} \subseteq \mathcal{C}$. Consider $f(x, y) := x^8 y^2 \in \mathcal{L}(42P_\infty) \setminus \mathcal{L}(15P_\infty)$.

Claim: $x^8 y^2 \in \mathcal{F}$

Note that

$$x^8 y^2 \circ L_{\alpha,\beta}(t) = t^8(\alpha t + \beta)^2 = \alpha^2 t^{10} + \beta^2 t^8,$$

and

$$p_{\alpha,\beta} = t^5 + \alpha^4 t^4 + \alpha t + (\beta + \beta^4).$$

So:

$t^6 \equiv \alpha^4 t^5 + \alpha t^2 + \text{deg } 1 \equiv \alpha^8 t^4 + \alpha t^2 + \text{deg } 1,$

$t^7 \equiv \alpha^8 t^5 + \alpha t^3 + \text{deg } 2 \equiv \alpha^{12} t^4 + \alpha t^3 + \text{deg } 2,$ and

$t^8 \equiv \alpha^{12} t^5 + \alpha t^4 + \text{deg } 3 \equiv \alpha^{16} t^4 + \alpha t^4 + \text{deg } 3$

Example of a good monomial.

Let $q = 4$. Then $\mathcal{H}_4 : y^4 + y = x^5$ over $\mathbb{F}_{16}$. We saw that $C_{4,15} \subseteq \mathcal{C}$. Consider $f(x, y) := x^8 y^2 \in \mathcal{L}(42P_\infty) \setminus \mathcal{L}(15P_\infty)$.

Claim: $x^8 y^2 \in \mathcal{F}$

Note that

$$x^8 y^2 \circ L_{\alpha,\beta}(t) = t^8(\alpha t + \beta)^2 = \alpha^2 t^{10} + \beta^2 t^8,$$

and

$$p_{\alpha,\beta} = t^5 + \alpha^4 t^4 + \alpha t + (\beta + \beta^4).$$

So:
$t^6 \equiv \alpha^4 t^5 + \alpha t^2 + \text{deg } 1 \equiv \alpha^8 t^4 + \alpha t^2 + \text{deg } 1,$
$t^7 \equiv \alpha^8 t^5 + \alpha t^3 + \text{deg } 2 \equiv \alpha^{12} t^4 + \alpha t^3 + \text{deg } 2,$ and
$t^8 \equiv \alpha^{12} t^5 + \alpha t^4 + \text{deg } 3 \equiv \alpha^{16} t^4 + \alpha t^4 + \text{deg } 3 = \text{deg } 3$ as $\alpha^{16} t^4 + \alpha t^4 = 0$.

Example of a good monomial.

Let $q = 4$. Then $\mathcal{H}_4 : y^4 + y = x^5$ over $\mathbb{F}_{16}$. We saw that $C_{4,15} \subseteq \mathcal{C}$. Consider $f(x, y) := x^8 y^2 \in \mathcal{L}(42P_\infty) \setminus \mathcal{L}(15P_\infty)$.

Claim: $x^8 y^2 \in \mathcal{F}$

Note that

$$x^8 y^2 \circ L_{\alpha,\beta}(t) = t^8(\alpha t + \beta)^2 = \alpha^2 t^{10} + \beta^2 t^8,$$

and

$$p_{\alpha,\beta} = t^5 + \alpha^4 t^4 + \alpha t + (\beta + \beta^4).$$

So:
$t^6 \equiv \alpha^4 t^5 + \alpha t^2 + \text{deg } 1 \equiv \alpha^8 t^4 + \alpha t^2 + \text{deg } 1,$
$t^7 \equiv \alpha^8 t^5 + \alpha t^3 + \text{deg } 2 \equiv \alpha^{12} t^4 + \alpha t^3 + \text{deg } 2,$ and
$t^8 \equiv \alpha^{12} t^5 + \alpha t^4 + \text{deg } 3 \equiv \alpha^{16} t^4 + \alpha t^4 + \text{deg } 3 = \text{deg } 3$ as $\alpha^{16} t^4 + \alpha t^4 = 0$.
Also, $t^{10} = (t^5)^2 \equiv \alpha^8 t^8 + \alpha^2 t^2 + \beta^2 + \beta^8$.
Thus, t^{10} and t^8 are of degree at most $q - 1 = 3$

Example of a good monomial.

Let $q = 4$. Then $\mathcal{H}_4 : y^4 + y = x^5$ over $\mathbb{F}_{16}$. We saw that $C_{4,15} \subseteq \mathcal{C}$. Consider $f(x, y) := x^8 y^2 \in \mathcal{L}(42P_\infty) \setminus \mathcal{L}(15P_\infty)$.

Claim: $x^8 y^2 \in \mathcal{F}$

Note that

$$x^8 y^2 \circ L_{\alpha,\beta}(t) = t^8(\alpha t + \beta)^2 = \alpha^2 t^{10} + \beta^2 t^8,$$

and

$$p_{\alpha,\beta} = t^5 + \alpha^4 t^4 + \alpha t + (\beta + \beta^4).$$

So:
$t^6 \equiv \alpha^4 t^5 + \alpha t^2 + \text{deg } 1 \equiv \alpha^8 t^4 + \alpha t^2 + \text{deg } 1,$
$t^7 \equiv \alpha^8 t^5 + \alpha t^3 + \text{deg } 2 \equiv \alpha^{12} t^4 + \alpha t^3 + \text{deg } 2,$ and
$t^8 \equiv \alpha^{12} t^5 + \alpha t^4 + \text{deg } 3 \equiv \alpha^{16} t^4 + \alpha t^4 + \text{deg } 3 = \text{deg } 3$ as $\alpha^{16} t^4 + \alpha t^4 = 0$.
Also, $t^{10} = (t^5)^2 \equiv \alpha^8 t^8 + \alpha^2 t^2 + \beta^2 + \beta^8$.
Thus, t^{10} and t^8 are of degree at most $q - 1 = 3$, and $x^8 y^2 \in \mathcal{F}$.

Example: Hermitian-Lifted Code for $q = 4$

When $q = 4$, we work with the Hermitian curve $x^4 + x = y^5$ over $\mathbb{F}_{16}$, for a code of iength $n = 64$. The code $\mathcal{C}$ has dimension 13. In contrast, the comparable non-lifted one-point Hermitian code $C_{4,15}$ has dimension 10. Thus the rate of $\mathcal{C}$ is at least $\frac{13}{64} \approx 0.20$, while the rate of $C_{4,15}$ is $\frac{10}{64} \approx 0.16$.

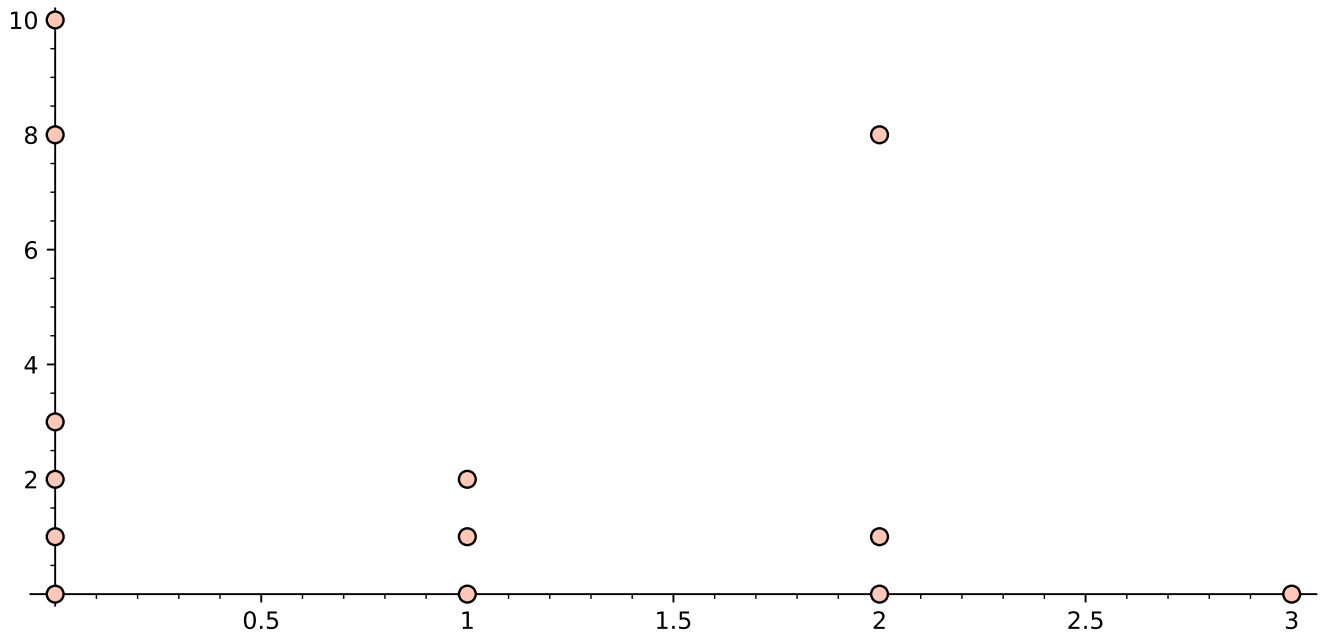


Figure: Exponent pairs (a, b) with $x^a y^b \in \mathcal{C}$ for $q = 4$ (a is on horizontal axis).

Example: Hermitian-Lifted Code for $q = 8$

The code $\mathcal{C}$ has dimension 75. In contrast, the comparable non-lifted one-point Hermitian code $C_{8,63}$ has dimension 36. Thus the rate of $\mathcal{C}$ is at least $\frac{75}{512} \approx 0.15$. The rate of $C_{8,63}$ is $\frac{36}{512} \approx 0.07$.

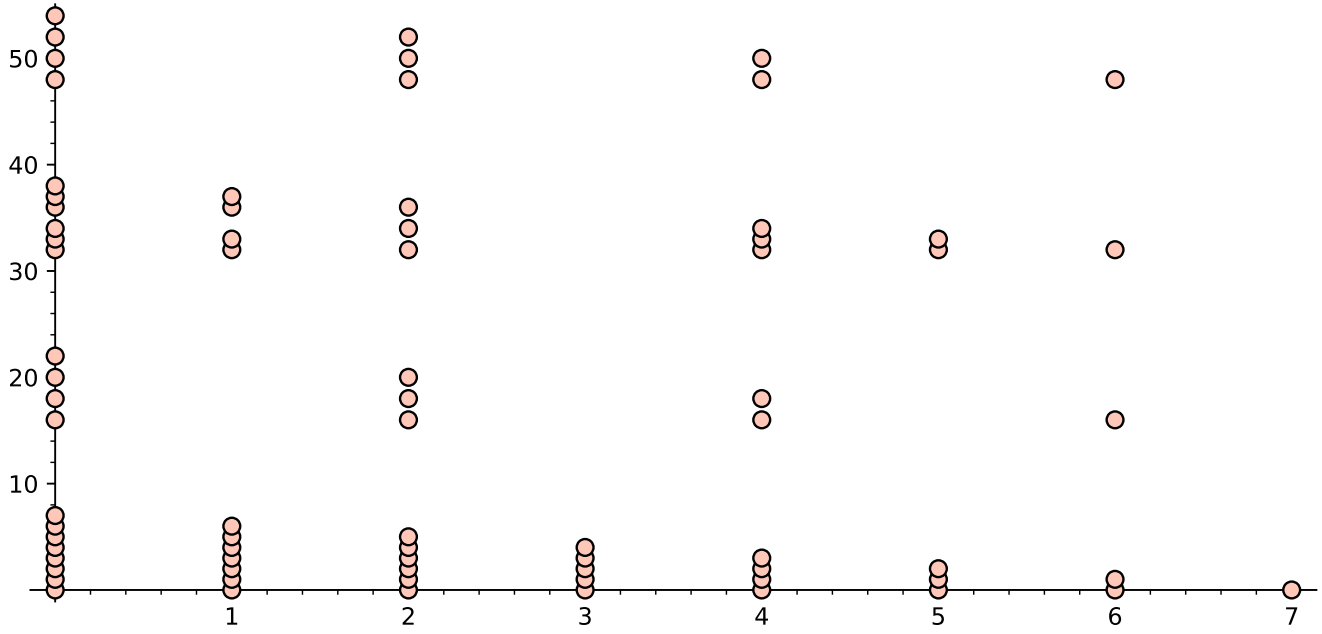


Figure: Exponent pairs (a, b) with $x^a y^b \in \mathcal{C}$ for $q = 8$ (a is on horizontal axis).

Example: Hermitian-Lifted Code for $q = 16$

The code $\mathcal{C}$ has dimension 505. In contrast, the comparable non-lifted one-point Hermitian code $C_{16,255}$ has dimension 136. Thus the rate of $\mathcal{C}$ is at least $\frac{505}{4096} \approx 0.123$. The rate of $C_{16,255}$ is $\frac{136}{4096} \approx 0.033$.

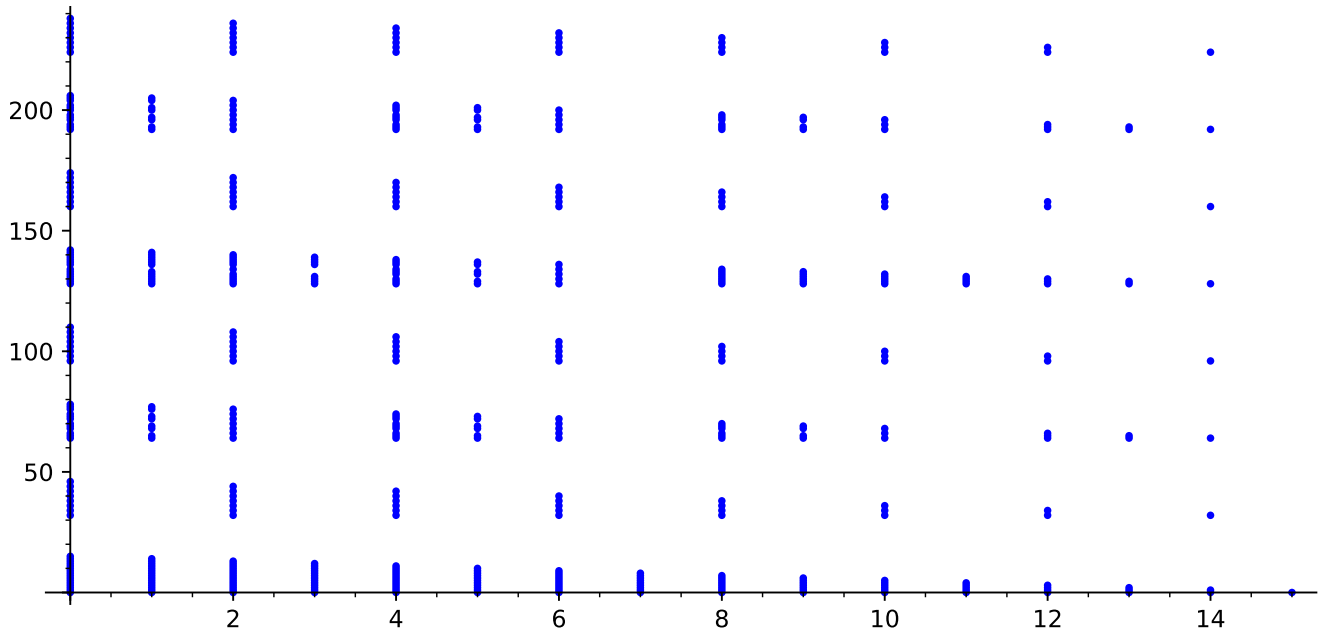


Figure: Exponent pairs (a, b) with $x^a y^b \in \mathcal{C}$ for $q = 16$ (a is on horizontal axis).

Further Work

- Rate bounds for all q–undergraduate student Na'ama Nevo.
- What is exact rate? Minimum distance?
- Curve-lifted codes for other curves? What curves give best parameters? Aiden Murphy did Norm-Trace curves.
- How to think about extra functions?
- Current work with V. Guruswami, H. López, G.Matthews, F. Piñero-González, and M. Wootters: lifted codes with intersecting recovery sets, recovery using curves, and using Hermitian surface for locality and hierarchy.
- General ways to use geometry and especially nice varieties to get lifted codes with good properties?

References

- A. Barg, I. Tamo, and S. Vlăduţ, "Locally recoverable codes on algebraic curves," *Proceedings of the IEEE Int. Symp. Info. Theory*, 1252–1256, 2015.
- S. Luna Frank-Fischer, V. Guruswami, and M. Wootters. "Locality via Partially Lifted Codes," Proceedings of Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2017). Article No. 43; pp. 43:1–43:17, 2017.
- A. Guo, S. Kopparty, and M. Sudan. "New affine-invariant codes from lifting," *ITCS*, 529–540, 2013.
- H. López, B. Malmskog, G.Matthews, F. Piñero-González, M. Wootters. "Hermitian-lifted codes," *Designs, Codes, and Cryptography*, 89, 497–515, 2021.