Squares of codes and applications to cryptography

Ignacio Cascudo

June 30, 2014
Aarhus University

Powers of a linear code

Let:

- $\mathbb{F}_q$ be a finite field of q elements.
- $C \subseteq \mathbb{F}_q^n$ be an $\mathbb{F}_q$-linear code of length n.
- d be an integer.
- $\mathbf{v} * \mathbf{w}$ the coordinate-wise (Schur) product of $\mathbf{v}, \mathbf{w} \in \mathbb{F}_q^n$.

Definition (d-th power of C)

The d-th power of C is defined as

$$C^{*d} = \mathbb{F}_q\langle\{\mathbf{c}_1 * \cdots * \mathbf{c}_d : \mathbf{c}_1, \ldots, \mathbf{c}_d \in C\}\rangle$$

In this talk: focus on $d = 2$ (square of C)

Some questions

In general:
How are the parameters of C^{*2} (minimum distance, dimension) related to those of C?

Asymptotic questions, for example:

Question

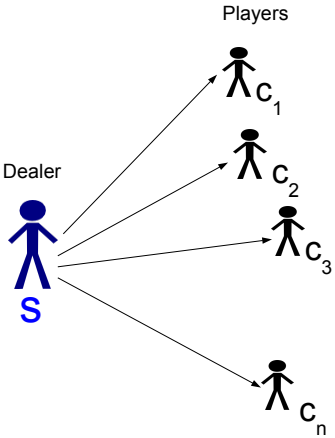
For every finite field $\mathbb{F}_q$, is there a family of $\mathbb{F}_q$-linear codes $\{C_i\}$ such that both $\{C_i\}$ and $\{C_i^{*2}\}$ are asymptotically good?

Applications

Squares of a code are an important notion in:

- **Multiplicative secret sharing** (applications to secure multiparty computation and two-party cryptography)
- Cryptanalysis (McEliece public key encryption).
- Other applications:
  Algebraic complexity (bilinear multiplication algorithms), frameproof codes, some lattice constructions...

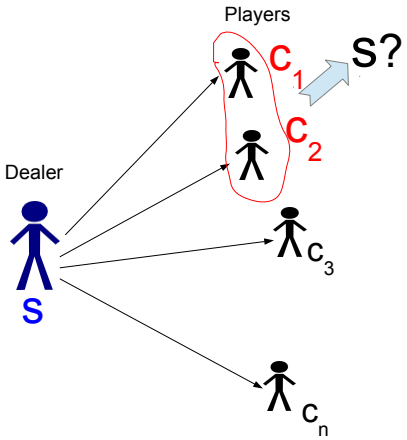
Secret sharing



Setting

- A dealer and n players.
- The dealer knows a secret s.
- Sends information (a share) c_i to each player P_i.

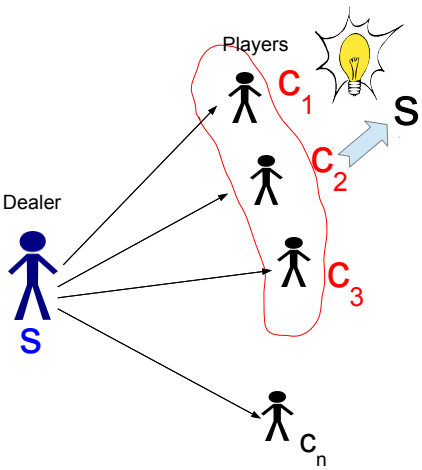
Secret sharing



Properties

- t-privacy: Any set of t shares $\rightarrow$ no info about s.

Secret sharing



Properties

- t-privacy: Any set of t shares $\rightarrow$ no info about s.
- r-reconstruction: Any set of r shares $\rightarrow$ determines s.

Secret sharing schemes from linear codes

A $[\ell + n, \geq \ell]$ $\mathbb{F}_q$-linear code C yields a secret sharing scheme $\Sigma_\ell(C)$ with

- n players
- Every share in $\mathbb{F}_q$.
- Secret in $\mathbb{F}_q^\ell$.

Let C be in systematic form in first ℓ coordinates.

Definition (Sharing algorithm)

To share $\mathbf{s} \in \mathbb{F}_q^\ell$.

- Select word $\mathbf{c} = (\mathbf{s}, c_1, \ldots, c_n) \in C$ uniformly at random.
- Send c_i to player i, $i = 1, \ldots, n$.

Example

$q = 2$, $\ell = 1$ (secrets in $\mathbb{F}_2$), $n = 4$ (4 players).
Let C be the $[5, 3, 2]$ $\mathbb{F}_2$-linear code with the following codewords.

$$
\begin{array}{ccccc}
0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1
\end{array}
$$

$$
\begin{array}{ccccc}
1 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 1
\end{array}
$$

Example

$q = 2$, $\ell = 1$ (secrets in $\mathbb{F}_2$), $n = 4$ (4 players).
Let C be the $[5, 3, 2]$ $\mathbb{F}_2$-linear code with the following codewords.

$$
\begin{array}{ccccc}
\mathbf{0} & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 \\
\mathbf{0} & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 \\
 & & & & \\
\mathbf{1} & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 \\
\mathbf{1} & 0 & 1 & 0 & 1
\end{array}
$$

1-privacy:
Each share gives no info about the secret.

Example

$q = 2$, $\ell = 1$ (secrets in $\mathbb{F}_2$), $n = 4$ (4 players).
Let C be the $[5, 3, 2]$ $\mathbb{F}_2$-linear code with the following codewords.

$$
\begin{array}{ccccc}
0 & 0 & 0 & 0 & 0 \\
\mathbf{0} & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 \\
\mathbf{0} & 1 & 0 & 0 & 1 \\
 & & & & \\
1 & 0 & 0 & 1 & 1 \\
\mathbf{1} & 1 & 1 & 0 & 0 \\
\mathbf{1} & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 1
\end{array}
$$

1-privacy:
Each share gives no info about the secret.

Example

$q = 2$, $\ell = 1$ (secrets in $\mathbb{F}_2$), $n = 4$ (4 players).
Let C be the $[5, 3, 2]$ $\mathbb{F}_2$-linear code with the following codewords.

$$
\begin{array}{ccccc}
0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 \\
\mathbf{0} & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 \\
 & & & & \\
1 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 1
\end{array}
$$

3-reconstruction:
Every 3 shares determine the secret.

Example

$q = 2$, $\ell = 1$ (secrets in $\mathbb{F}_2$), $n = 4$ (4 players).
Let C be the $[5, 3, 2]$ $\mathbb{F}_2$-linear code with the following codewords.

$$
\begin{array}{ccccc}
0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 \\
 & & & & \\
1 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 \\
\mathbf{1} & 0 & 1 & 0 & 1
\end{array}
$$

3-reconstruction:
Every 3 shares determine the secret.

Example

$q = 2$, $\ell = 1$ (secrets in $\mathbb{F}_2$), $n = 4$ (4 players).
Let C be the $[5, 3, 2]$ $\mathbb{F}_2$-linear code with the following codewords.

$$
\begin{array}{ccccc}
0 & 0 & 0 & 0 & 0 \\
\mathbf{0} & 1 & 1 & 1 & 1 \\
\mathbf{0} & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 \\
\\
1 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 1
\end{array}
$$

Neither 2-privacy nor 2-reconstruction:
The shares of $\{c_1, c_4\}$ and the shares of $\{c_2, c_3\}$ determine the secret.

Example

$q = 2$, $\ell = 1$ (secrets in $\mathbb{F}_2$), $n = 4$ (4 players).
Let C be the $[5, 3, 2]$ $\mathbb{F}_2$-linear code with the following codewords.

$$
\begin{array}{ccccc}
\mathbf{0} & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 \\
 & & & & \\
1 & 0 & 0 & 1 & 1 \\
\mathbf{1} & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 1
\end{array}
$$

Neither 2-privacy nor 2-reconstruction:
The shares of $\{c_1, c_4\}$ and the shares of $\{c_2, c_3\}$ determine the secret.
None of $\{c_1, c_2\}$, $\{c_1, c_3\}$, $\{c_2, c_4\}$, $\{c_3, c_4\}$ give info about the secret.

Example

$q = 2$, $\ell = 1$ (secrets in $\mathbb{F}_2$), $n = 4$ (4 players).
Let C be the $[5, 3, 2]$ $\mathbb{F}_2$-linear code with the following codewords.

$$
\begin{array}{ccccc}
0 & 0 & 0 & 0 & 0 \\
\mathbf{0} & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 \\
 & & & & \\
\mathbf{1} & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 1
\end{array}
$$

Neither 2-privacy nor 2-reconstruction:
The shares of $\{c_1, c_4\}$ and the shares of $\{c_2, c_3\}$ determine the secret.
None of $\{c_1, c_2\}$, $\{c_1, c_3\}$, $\{c_2, c_4\}$, $\{c_3, c_4\}$ give info about the secret.

Relations between parameters(I)

From now on we focus on the case $\ell = 1$.

Proposition

$$d(C^{\perp}) \geq t + 2 \Rightarrow t - privacy$$

$$d(C) \geq n - r + 2 \Rightarrow r - reconstruction$$

Implications in the other direction not necessarily true!

Relations between parameters(II)

If we want an “if and only if”...

Definition

Let $w_0(C) := min\{w_H(c) : c \in C, c_0 \neq 0\}$

Remark

Obviously $d(C) \leq w_0(C)$.

Then

Proposition

$$w_0(C^{\perp}) \geq t + 2 \Leftrightarrow t - privacy$$

$$w_0(C) \geq n - r + 2 \Leftrightarrow r - reconstruction$$

Generalization for $\ell > 1$ is also possible.

Linear secret sharing schemes (LSSS)

$\Sigma_\ell(C)$ is a **linear** secret sharing scheme (LSSS).

- The secret- and all share-spaces are $\mathbb{F}_q$-vector spaces.
- And we have the property:

Property (Linearity)

$$\left.\begin{array}{c} c_1, \ldots, c_n \text{ shares for } s \\ c'_1, \ldots, c'_n \text{ shares for } s' \\ \lambda \in \mathbb{F}_q \end{array}\right\} \Rightarrow \begin{array}{l} c_1 + \lambda c'_1, \ldots, c_n + \lambda c'_n \\ \text{are shares for } s + \lambda s' \\ \text{in the same scheme.} \end{array}$$

Very useful property: allows secure multi-party computation of linear functions!!

Multiplicative secret sharing

We would like a similar property for multiplication. However,

$$\left.\begin{array}{l}\mathbf{w} = (\mathbf{s}, c_1, \ldots, c_n) \in C \\ \mathbf{w}' = (\mathbf{s}', c'_1, \ldots, c'_n) \in C\end{array}\right\} \not\Rightarrow \mathbf{w} * \mathbf{w}' = (\mathbf{s} * \mathbf{s}', c_1 c'_1, \ldots, c_n c'_n) \in C \ldots$$

... but $\mathbf{w} * \mathbf{w}' \in C^{*2}$!!

Definition

A LSSS $\Sigma(C)$ has $\hat{r}$-product reconstruction iff $\Sigma(C^{*2})$ has $\hat{r}$-reconstruction.

Remark

A LSSS $\Sigma(C)$ has $\hat{r}$-product reconstruction iff
For every set $A \subseteq \{1, \ldots, n\}$ of size $\hat{r}$, there exists a linear function

$$\psi_A : \mathbb{F}_q^{\hat{r}} \to \mathbb{F}_q$$

such that

$$ss' = \psi_A((c_i c_i')_{i \in A}).$$

Key property in MPC protocols!!

Definition

- Multiplicative LSSS: LSSS with n-product reconstruction.
- t-strongly multiplicative LSSS: LSSS with t-privacy and $(n-t)$-product reconstruction.

Specially useful: t-strong multiplicative LSSS where t/n is large.

Example: Shamir's scheme

Assume $n < q$. Consider a $[n+1, t+1]$-Reed-Solomon code

$$C_{n,t} := \{(f(x_0), f(x_1), \ldots, f(x_n)) : f \in \mathbb{F}_q[X], \deg f \leq t\},$$

where $x_0, x_1, \ldots, x_n \in \mathbb{F}_q$, pairwise distinct.

Proposition

$\Sigma(C_{n,t})$ *(Shamir's secret sharing scheme)*

- *Has t-privacy,*
- *Has $(t+1)$-reconstruction.*

Proposition

Suppose $n \geq 2t+1$. Then $C_{n,t}^{*2} = C_{n,2t}$ and

- *$\Sigma(C_{n,t})$ has $(2t+1)$-product reconstruction.*
- *$\Sigma(C_{n,t})$ is t-strongly multiplicative if $3t < n$ (optimal!!!).*

Asymptotics

Drawback of Shamir: Number of players n bounded by q.

Why does it matter?

For recent applications: we want t-strong multiplicative LSSS (t-privacy, $(n-t)$-product reconstruction), where

- $n \to \infty$.
- q constant.
- $t = \Theta(n)$.

Also $\ell = \Theta(n)$ is useful.

In other words, we need a family of $\mathbb{F}_q$-linear codes C_n of length $n+1 \to \infty$ with:

1. $w_0(C_n^{*2}) \geq t$,
2. $w_0(C_n^{\perp}) \geq t$.

where $t = \Theta(n)$.
(2) implies $\dim(C_n) \geq t+1$.

Remark

It is sufficient (but not necessary) to have a family of $\mathbb{F}_q$-linear codes C_n of length $n+1 \to \infty$ with

1. $d(C_n^{*2}) = \Theta(n)$,
2. $d(C_n^{\perp}) = \Theta(n)$.

Algebraic geometric codes

Let:

- F a function field with full field of constants $\mathbb{F}_q$.
- $P_0, P_1, \ldots, P_n$ distinct rational places of F.
- $D = \sum P_i$.
- G a divisor, $\operatorname{supp} G \cap \operatorname{supp} D = \emptyset$.
- $\mathcal{L}(G)$ Riemann-Roch space of G.

Define the AG code:

$$C_{\mathcal{L}}(D, G) := \{(f(P_0), f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G)\}$$

Proposition

We have: $d(C_{\mathcal{L}}(D, G)) \geq n + 1 - \deg G$.

In general it is not true that $C_{\mathcal{L}}(D,G)^{*2} = C_{\mathcal{L}}(D,2G)$, however

Remark

$C_{\mathcal{L}}(D,G)^{*2} \subseteq C_{\mathcal{L}}(D,2G)$.

and this means

$$d(C_{\mathcal{L}}(D,G)^{*2}) \geq d(C_{\mathcal{L}}(D,2G)).$$

So it is enough to lower bound $d(C_{\mathcal{L}}(D,2G))$!

On the other hand it is well known that:

Lemma

$(C_{\mathcal{L}}(D,G))^{\perp} \sim C_{\mathcal{L}}(D,K-G+D)$, K canonical divisor.

We need families of function fields with

- genus: $g \to \infty$
- number of rational places: $n + 1 > (4 + \epsilon)g$

Using Ihara's results (Garcia-Stichtenoth towers).

Theorem (Chen, Cramer 06)

For every square q, $q \geq 49$, there exist $\mathbb{F}_q$-linear codes C_n with:

- *length $n + 1 \to \infty$,*
- $d(C_n^{\perp}) = \Omega(n)$,
- $d(C_n^{*2}) = \Omega(n)$.

Improvement using f.f. with small torsion of class groups

In order to have $d(C_{\mathcal{L}}(D, K - G + D)) \geq t$ and $d(C_{\mathcal{L}}(D, 2G)) \geq t$ it is enough that

$$\begin{cases} \mathcal{L}((K - G + D) - \sum_{i \in A} P_i) = 0 & \forall A \subseteq \{0, \ldots, n\}, |A| = n + 1 - t. \\ \mathcal{L}(2G - \sum_{i \in A} P_i) = 0 & \forall A \subseteq \{0, \ldots, n\}, |A| = n + 1 - t. \end{cases}$$

We prove results on towers of function fields with many rational points and small 2-torsion in their class groups to conclude:

Theorem (C., Cramer, Xing 11)

For every q, $q \geq 8$, $q \neq 11, 13$, there exist $\mathbb{F}_q$-linear codes C_n with

- *length $n + 1 \to \infty$,*
- *$d(C_n^{\perp}) = \Omega(n)$,*
- *$d(C_n^{*2}) = \Omega(n)$.*

Improvement using f.f. with small torsion of class groups

In order to have $d(C_{\mathcal{L}}(D, K - G + D)) \geq t$ and $d(C_{\mathcal{L}}(D, 2G)) \geq t$ it is enough that

$$\begin{cases} \mathcal{L}((K - G + D) - \sum_{i \in A} P_i) = 0 & \forall A \subseteq \{0, \ldots, n\}, |A| = n + 1 - t. \\ \mathcal{L}(2G - \sum_{i \in A} P_i) = 0 & \forall A \subseteq \{0, \ldots, n\}, |A| = n + 1 - t. \end{cases}$$

We prove results on towers of function fields with many rational points and small 2-torsion in their class groups to conclude:

Theorem (C., Cramer, Xing 11)

For every q, $q \geq 8$, $q \neq 11, 13$, there exist $\mathbb{F}_q$-linear codes C_n with

- *length $n + 1 \to \infty$,*
- *$d(C_n^{\perp}) = \Omega(n)$,*
- *$d(C_n^{*2}) = \Omega(n)$.*

Concatenation-based construction

From CC06/CCX11 on extension fields+ dedicated field descent (using dedicated code concatenation).

Theorem (C., Chen, Cramer, Xing 09)

For every finite field $\mathbb{F}_q$, there exist $\mathbb{F}_q$-linear codes C_n of length $n+1 \to \infty$, $w_0(C_n^\perp) = \Omega(n)$, $w_0(C_n^{*2}) = \Omega(n)$.

However, in this construction, $d(C_n^\perp)$ necessarily constant, and $d(C_n^{*2})$ may not be $\Omega(n)$.

Other results

Using AG-codes over the extension fields with good higher powers + a more sophisticated concatenation technique

Theorem (Randriam)

For every finite field $\mathbb{F}_q$, there exist $\mathbb{F}_q$-linear codes C_n of length $n \to \infty$, $\dim C_n = \Omega(n)$, $d(C_n^{*2}) = \Omega(n)$.

The search for other constructions

- All asymptotic constructions so far are based on AG-codes.
- Other (simpler) constructions?
- For random codes:

Theorem (C., Cramer, Mirandola, Zemor 13)

Let C be a random linear code of dimension k and length $n(k)$. If $n(k) \leq k(k+1)/2$, then

$$Pr(C^{*2} = \mathbb{F}_q^{n(k)}) = 1 - O(2^{-t(k)})$$

where $t(k) := k(k+1)/2 - n(k) \geq 0$.

Proofs based on results on quadratic forms.

Conclusions

- Studying parameters of squares of codes has important applications.
- Asymptotically, only AG-based constructions are known to be “good enough”.