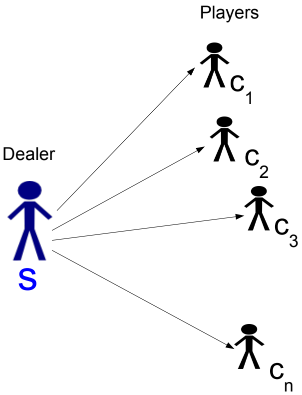
Asymptotics of arithmetic codices and towers of function fields

Ignacio Cascudo

CWI Amsterdam
Joint work with Ronald Cramer (CWI/ULeiden) and Chaoping Xing(NTU)

Algebraic curves over finite fields
Linz, 15 November 2013

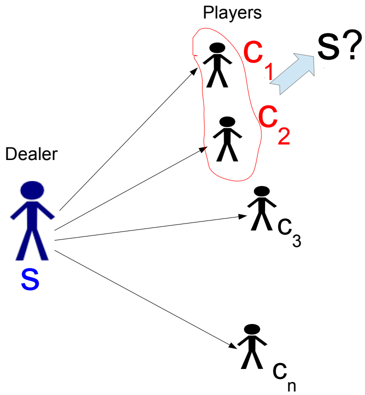
Secret sharing



Setting

- A dealer and n players.
- The dealer knows a secret s in certain (public) set S.
- Sends information (shares) c_i to each player P_i (c_i belong to public sets S_i).

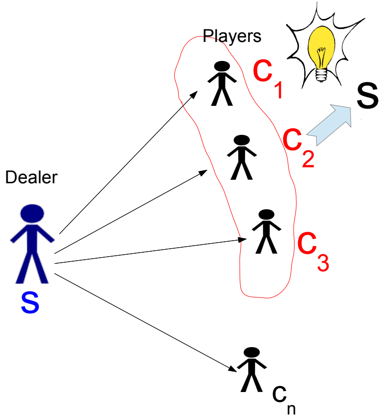
Secret sharing



Setting

- A dealer and n players.
- The dealer knows a secret s in certain (public) set S.
- Sends information (shares) c_i to each player P_i (c_i belong to public sets S_i).
- t-privacy: Any t of shares $\rightarrow$ no information about s.

Secret sharing



Setting

- A dealer and n players.
- The dealer knows a secret s in certain (public) set S.
- Sends information (shares) c_i to each player P_i (c_i belong to public sets S_i).
- t-privacy: Any t of shares $\rightarrow$ no information about s.
- m-reconstruction: Any m shares $\rightarrow$ determines s.

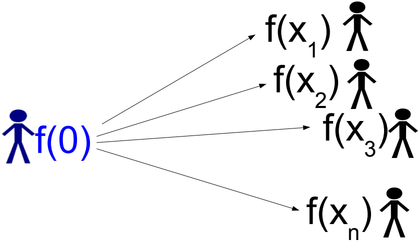
Shamir's secret sharing scheme

$\mathbb{F}_q$ finite field. Space of secrets: $\mathbb{F}_q$. Spaces of shares: $\mathbb{F}_q$.

Let $1 \leq t < n$, with $n < q$. Let $x_1, \ldots, x_n \in \mathbb{F}_q \setminus \{0\}$ distinct.

To deal a secret $s \in \mathbb{F}_q$, the dealer:

1. Selects unif. random $f \in \mathbb{F}_q[X]$ with $\deg f \leq t$, $f(0) = s$.
2. Sends $c_i = f(x_i)$ to player P_i.



Properties

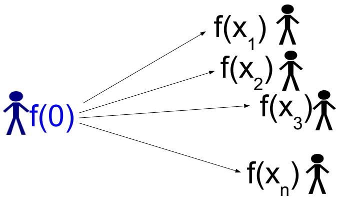
- *t players have no information about the secret.*
- *$t+1$ players can fully determine f, and hence s.*

Proof

For any $y_1, y_2, \ldots, y_{t+1} \in \mathbb{F}_q$ distinct the following is a bijection

$$\{f \in \mathbb{F}_q[X] : \deg f \leq t\} \rightarrow \mathbb{F}_q^{t+1}$$

$$f \mapsto (f(y_1), f(y_2), \ldots, f(y_{t+1}))$$



Properties

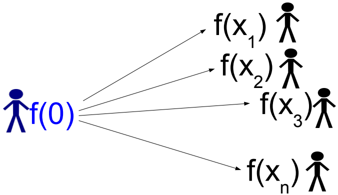
- *t players have no information about the secret.*
- *$t+1$ players can fully determine f, and hence s.*

Proof

For any $x_{i_1}, x_{i_2}, \ldots, x_{i_{t+1}} \in \mathbb{F}_q$ distinct the following is a bijection

$$\{f \in \mathbb{F}_q[X] : \deg f \leq t\} \to \mathbb{F}_q^{t+1}$$

$$f \mapsto (f(x_{i_1}), f(x_{i_2}), \ldots, f(x_{i_{t+1}}))$$



Properties

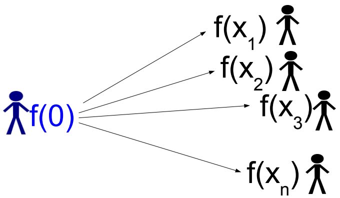
- *t players have no information about the secret.*
- $t+1$ *players can fully determine* f*, and hence* s.

Proof

For any $x_{i_1}, x_{i_2}, \ldots, x_{i_t} \in \mathbb{F}_q$ *distinct the following is a bijection*

$$\{f \in \mathbb{F}_q[X] : \deg f \leq t\} \to \mathbb{F}_q^{t+1}$$

$$f \mapsto (f(0), f(x_{i_1}), \ldots, f(x_{i_t}))$$



Secret sharing with algebraic properties

Secret sharing with **extra algebraic properties** is very interesting for applications.

Space of secrets: $\mathbb{F}_q$-vector space S, and spaces of shares: $\mathbb{F}_q$.

Property (Linearity)

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

Remark

Shamir's secret sharing scheme is linear

since

$$\left.\begin{array}{c} \deg f, \deg g \leq t \\ \lambda \in \mathbb{F}_q \end{array}\right\} \Rightarrow \deg(f + \lambda g) \leq t$$

Space of *secrets*: $\mathbb{F}_q$-algebra (such as $\mathbb{F}_{q^k}$, $\mathbb{F}_q^k$).

Property (r-multiplicativity)

For any $A \subseteq \{1, \ldots, n\}, |A| = r$, the products $\{c_i c_i'\}_{i \in A}$ determine ss'.

Remark

Shamir's scheme has $2t+1$-multiplicativity

since

$$\deg f, \deg g \leq t \Rightarrow \deg fg \leq 2t \text{ and therefore}$$

$2t+1$ evaluations of fg determine fg (and hence $fg(0)$).

- Algebraic properties of secret sharing are important for applications in cryptography, especially to **secure multiparty computation (MPC)**.
- Very useful notion (t-strong multiplication): linearity + t-privacy + $(n-t)$-multiplicativity for “large” t.

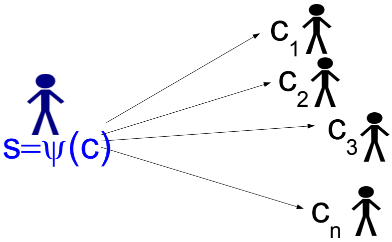
General linear construction

Let S be a $\mathbb{F}_q$-algebra. Suppose $C \subseteq \mathbb{F}_q^n$ vector subspace and $\psi : C \to S$ is a surjective $\mathbb{F}_q$-linear map.

Protocol

To share $s \in S$,

1. *Dealer selects unif. random $c = (c_1, \dots, c_n) \in \psi^{-1}(s) \subseteq C$*
2. *Dealer sends c_i to player P_i, for $i = 1, \dots, n$.*



Arithmetic codex

Question

What properties besides linearity does this construction have (privacy, multiplicativity)?

We will introduce the notion of **arithmetic codex**:

- Captures notion of linear secret sharing with multiplicative properties.
- Also encompasses other concepts: bilinear multiplication algorithm (algebraic complexity).

Arithmetic codex

Definition (d-th power of a linear code)

Let $C \subseteq \mathbb{F}_q^n$ be a vector subspace over $\mathbb{F}_q$, $d > 0$ an integer. Let

$$C^{*d} := \mathbb{F}_q \langle \{ c^{(1)} * c^{(2)} \ldots * c^{(d)} : (c^{(1)}, c^{(2)}, \ldots, c^{(d)}) \in C^d \} \rangle$$

Notation

For $\emptyset \neq A = \{i_1, \ldots, i_\ell\} \subseteq \{1, \ldots, n\}$, let

$$\pi_A : \mathbb{F}_q^n \to \mathbb{F}_q^\ell$$

$$(c_1, \ldots, c_n) \mapsto (c_{i_1}, \ldots, c_{i_\ell})$$

Definition

K (finite) field, S finite dimensional K-algebra,
$n, t, d, r \in \mathbb{Z}$ with $0 \leq t < r \leq n$, $d \geq 1$.

An (n, t, d, r)-codex (C, ψ) for S over K consists of:

- A vector subspace $C \subseteq K^n$
- A linear map $\psi : C \to S$

satisfying 3 properties:

1. ψ is surjective.
2. (t-disconnection): If $t \geq 1$, for any $A \subseteq \{1, \dots, n\}$ with $|A| = t$ the map

$$C \to S \times \pi_A(C)$$

$$c \mapsto (\psi(c), \pi_A(c))$$

is surjective.

Arithmetic codex

Definition (cont.)

3. $((d,r)$-multiplicativity):
   There exists a function $\overline{\psi} : C^{*d} \rightarrow S$ such that
   - $\overline{\psi}$ is linear.
   - For all $c^{(1)}, \ldots, c^{(d)} \in C$,

$$\overline{\psi}(c^{(1)} * \cdots * c^{(d)}) = \prod_{i=1}^{d} \psi(c^{(j)}).$$

   - $\overline{\psi}$ is "r-wise determined": for all $B \subseteq \{1, \ldots, n\}$, $|B| = r$,

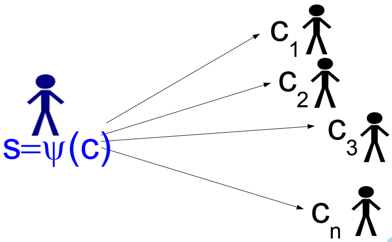
$$C^{*d} \cap \mathrm{Ker}\, \pi_B \subseteq \mathrm{Ker}\, \overline{\psi}.$$

Using codices for linear multiplicative secret sharing

Given (C, ψ) a (n, t, d, r)-codex used for secret sharing.

Properties

- *t shares c_i give no info about s (by t-disconnection)*
- *Linearity (by C being a v.space, and linearity of ψ)*
- *If $s^{(1)}, \ldots, s^{(d)} \in S$ are shared,*
  $\Pi_{j=1}^{d} s^{(j)}$ is determined by products of shares of r players (by (d, r)-multiplicativity)



Associated linear code

Now consider $S = \mathbb{F}_q^k$.
For a (n, t, d, r)-codex (C, ψ) for S over $\mathbb{F}_q$, we define the associated linear code

$$\widetilde{C} := \{(\psi(c), c) : c \in C\} \subseteq \mathbb{F}_q^{n+k}$$

Proposition

Given a linear code $\widetilde{C} \subseteq \mathbb{F}_q^{n+k}$, if the unit vectors $e_1, \ldots, e_k \notin \widetilde{C}^{*d} \cup \widetilde{C}^{\perp}$ then $\widetilde{C}$ is the associated code of an $(n, 0, d, n)$-codex.

Proposition

If in addition $d_{min}(\widetilde{C}^{\perp}) \geq t + k + 1$ and $d_{min}(\widetilde{C}^{*d}) \geq n - r + k + 1$, then $\widetilde{C}$ is the associated code of an (n, t, d, r)-codex.

- Drawback of Shamir's scheme: $n < q$.
- Asymptotics: q fixed, $n \to \infty$, and asymptotic requirements on other parameters.
- Example: Do there exists families of $(n, t, 2, n-t)$-codex for $\mathbb{F}_q^k$ over $\mathbb{F}_q$, where $t = \Omega(n)$?
- "Random codices do not seem to work" (C., Cramer, Mirandola, Zémor, 2013).
- **Only** known tool: **algebraic geometric secret sharing** (Chen, Cramer, 2006).

AG-codices

Let:
$F/\mathbb{F}_q$ be a function field.
$Q_1, \ldots, Q_k, P_1, \ldots, P_n \in \mathbb{P}^{(1)}(F)$.
$G \in \mathrm{Div}(F)$.
$\mathcal{L}(G)$ Riemann-Roch space of G.

Question

When is

$$\widetilde{C} := \{(f(Q_1), \ldots, f(Q_k), f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(G)\}$$

an (n, t, d, r)-codex for $\mathbb{F}_q^k$ over $\mathbb{F}_q$?

Sufficient condition

$Q := \sum_{j=1}^{k} Q_j$.
For $A \in \{1, \ldots, n\}$, $P_A := \sum_{i \in A} P_i \in \mathrm{Div}(F)$.
W canonical divisor.
$\ell(G) := \dim \mathcal{L}(G)$.

Proposition (Sufficient condition)

Suppose G satisfies the following equations.

$$\begin{cases} \ell(W - G + P_A + Q) = 0 & \textit{for all } A \subseteq \{1, \ldots, n\},\ |A| = t. \\ \ell(dG - P_B) = 0 & \textit{for all } B \subseteq \{1, \ldots, n\},\ |B| = r. \end{cases}$$

Then

$$\widetilde{C} := \{(f(Q_1), \ldots, f(Q_k), f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(G)\}$$

is an (n, t, d, r)-codex for $\mathbb{F}_q^k$ over $\mathbb{F}_q$.

Key fact: If $d \in \mathbb{Z}, d \geq 1$, then $\widetilde{C}_{\mathcal{L}}(D, G)^{*d} \subseteq \widetilde{C}_{\mathcal{L}}(D, dG)$.

Riemann Roch systems of equations

Definition

Let $s \in \mathbb{Z}_{>0}$ and let $Y_i \in \mathrm{Cl}(F)$, $d_i \in \mathbb{Z} \setminus \{0\}$ for $i = 1, \ldots, s$.
A *Riemann-Roch system of equations* in X is a system

$$\{\ell(d_i X + Y_i) = 0\}_{i=1}^{s}.$$

A solution is some $G \in \mathrm{Cl}(F)$ which satisfies all equations when substituted for X.

We may also state Riemann Roch equations in terms of divisors instead of classes.

Let $\mathcal{J}_F := \mathrm{Cl}_0(F)$, $h := |\mathcal{J}_F|$.
For $d \in \mathbb{Z}_{>0}$, let $\mathcal{J}_F[d] := \{G \in \mathcal{J}_F : dG = 0\}$.
For $d \in \mathbb{Z}_{<0}$, let $\mathcal{J}_F[d] := \mathcal{J}_F[-d]$.
For $r \in \mathbb{Z}_{\geq 0}$, let A_r be the number of positive divisors of deg r.

Theorem

Consider the Riemann-Roch system of equations

$$\{\ell(d_i X + Y_i) = 0\}_{i=1}^{s}.$$

If $\exists m \in \mathbb{Z}$ *such that*

$$h > \sum_{i=1}^{s} A_{r_i} \cdot |\mathcal{J}_F[d_i]|,$$

where $r_i = d_i m + \deg Y_i, i = 1, \ldots, s$,
then the Riemann-Roch system has a solution $[G] \in Cl_m(F)$.

"Solving by degree"

Remark

If $r_i < 0$, then $A_{r_i} = 0$. Hence,

$$r_i < 0 \; \forall \; i = 1, \ldots, s \Rightarrow h > \sum_{i=1}^{s} A_{r_i} \cdot |\mathcal{J}_F[d_i]|$$

and any divisor of a certain degree is a solution.

"Solving by degree"

Remark

If $r_i < 0$, then $A_{r_i} = 0$. Hence,

$$r_i < 0 \; \forall \; i = 1, \ldots, s \Rightarrow h > \sum_{i=1}^{s} A_{r_i} \cdot |\mathcal{J}_F[d_i]|$$

and any divisor of a certain degree is a solution.

Theorem (Chen, Cramer 06)

If $A(q) > 4$, then there is an infinite family of $(n, t, 2, n - t)$-codices for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ where n is unbounded, $t = \Omega(n)$, $k = \Omega(n)$.

If q square, $q \geq 49$, $A(q) > 4$ (attained by Garcia-Stichtenoth towers).
But: If $q \leq 25$, then $A(q) \leq 4$.

More general strategy

More generally we can upper bound the numbers $|\mathcal{J}_F[d_i]|$ asymptotically and A_{r_i} (as follows)

Lemma

Suppose $g \geq 1$. Then, for any r with $0 \leq r \leq g-1$,

$$A_r/h \leq \frac{g}{q^{g-r-1}(\sqrt{q}-1)^2}.$$

Using "Functional Equation" of the L-polynomial, Hasse-Weil theorem.
Similar results by Vladut, Niederreiter, Xing,...

The torsion limit

Definition

For an infinite family $\mathcal{F}$,

$$J_r(\mathcal{F}) := \inf_{F \in \mathcal{F}} \frac{\log_q |\mathcal{J}_F[r]|}{g(F)}.$$

Definition

For a field $\mathbb{F}_q$, and $0 \leq A \leq A(q)$,

$$J_r(q, A) := \liminf J_r(\mathcal{F}),$$

where inf is taken over families with Ihara's limit A.

Upper bounds for r-torsion limit, r prime

Theorem

Let $\mathbb{F}_q$ be a finite field and let $r > 1$ be a prime.

(i) *If $r \mid (q-1)$, then $J_r(q, A(q)) \leq \frac{2}{\log_r q}$.*

(ii) *If $r \nmid (q-1)$, then $J_r(q, A(q)) \leq \frac{1}{\log_r q}$*

(iii) *If q is square and $r \mid q$, then $J_r(q, \sqrt{q}-1) \leq \frac{1}{(\sqrt{q}+1)\log_r q}$.*

Proof.

Ideas:

(i) (and (ii) when $r = \mathrm{char}\, \mathbb{F}_q$). Direct from Weil's classical result on torsion of abelian varieties.

(ii) (in the rest of the cases): Use of self-orthogonality of $J[r]$ w.r.t. to Weil pairing.

(iii) Apply **Deuring-Shafarevich** theorem for r-rank in a tower of **Garcia and Stichtenoth**.

Application to Strongly Multiplicative Secret Sharing

The general strategy for solving R.R-systems based on torsion limits, allows to improve the results on arithmetic secret sharing.

Theorem

If $A(q) > 1 + J_2(q, A(q))$, then there is an infinite family $\{C_n\}$ of $(n, t, 2, n-t)$-codices for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ where:
n unbounded, $k = \Omega(n)$ and $t = \Omega(n)$.

Remark

In CC06, the condition $A(q) > 4$ was required. Now it is sufficient that $A(q) > 1 + J_2(q, A(q))$!

Drawback: It is not clear how to compute the solutions in general (as opposed to “solving by degree")

When does $A(q) > 1 + J_2(q, A(q))$ hold?

Theorem

For any finite field $\mathbb{F}_q$, with $q = 8, 9$ or $q \geq 16$, we have $A(q) > 1 + J_2(q, A(q))$

Remark

$A(q) > 1 + J_2(q, A(q))$ holds for some q with $A(q) \leq 4$ ($q = 8, 9$, $16 \leq q \leq 25$) and many q where $A(q) > 4$ not known.

Asymptotically good constructions over any finite field

- C., Chen, Cramer, Xing (2009): CC06 + concatenation gives $(n, t, 2, n-t)$-codices for $\mathbb{F}_q^k$ over $\mathbb{F}_q$, n unbounded, $t = \Omega(n)$, $k = \Omega(n)$ **for every finite field $\mathbb{F}_q$.** Torsion limits NOT necessary.
- However, concatenation gives bad dual distance (important for some applications).
- Moreover, torsion limits do give **quantitative** improvements on t/n for small fields.

Open questions

Main problem: Efficiency of construction.

- More "elementary" constructions? (without function fields)
  - Families of codes C with $d_{min}(C^{*2})$, $d_{min}(C^{\perp})$ linear in length?
  - Families of codes C with $d_{min}(C^{\perp})$ linear in length and $d_{min}(C^{*3}) \geq 2$?
- Efficiently solving Riemann-Roch equations when solving by degree not possible?

Open questions

Main problem: Efficiency of construction.

- More "elementary" constructions? (without function fields)
  - Families of codes C with $d_{min}(C^{*2})$, $d_{min}(C^{\perp})$ linear in length?
  - Families of codes C with $d_{min}(C^{\perp})$ linear in length and $d_{min}(C^{*3}) \geq 2$?
- Efficiently solving Riemann-Roch equations when solving by degree not possible?

Torsion limit:

- Better bounds?
- Other towers for which we have good bounds?

Conclusions

- Codices encompass several objects useful in info-theoretically secure crypto and algebraic complexity.
- Asymptotics are important.
- Towers are useful (so far, indispensable) for asymptotics.
- Towers with extra properties of the function fields are gaining importance.