Constructions of Frameproof Codes

Xiande Zhang

Joint work with Yeow Meng Chee

November 2012, Singapore

Outline

- Introduction
- Upper Bounds of Frameproof Codes
- Constructions of Frameproof Codes
- Concluding Remarks

Outline

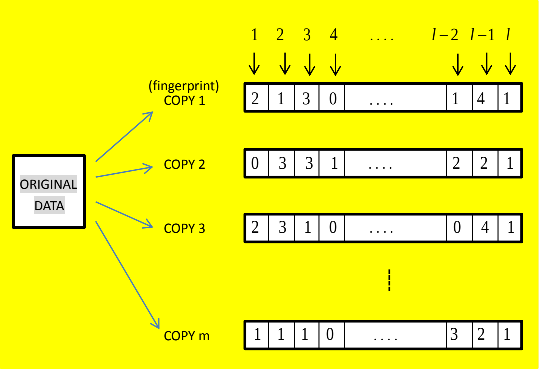
Motivations

- Frameproof codes were first introduced by Boneh and Shaw in 1998 to protect copyrighted materials.
- The study of related objects in the literature goes back to 1960s, as Rényi first introduced the concept of a separating system when concerning certain information-theoretic problems.
- It is applicable for different scenarios such as in broadcast encryption scheme and variants of pay-per-view movies.

(D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inform. Theory*, vol. 44, no. 5, pp. 1897–1905, 1998.)

Fingerprints

A distributor wants to sell copies of a digital product. He randomly chooses l fixed positions in the digital data. For each copy, he marks each position with one of q different states.



Coalitions

Notation:

- Let F be a finite set of cardinality q.
- $[l] = \{1, \ldots, l\}$, where l is a positive integer.
- $\forall x \in F^l$ and $\forall i \in [l]$, let x_i denote the ith component of x.
- Let $P \subset F^l$. The set of *descendants* of P, $desc(P)$, is defined as

$$desc(P) = \{x \in F^l : x_i \in \{y_i : y \in P\}, i \in [l]\}.$$

Example

$C = \{011, 012, 211, 222\}$, $P = \{012, 211\} \subset C$, then $desc(P) = \{012, 011, 212, 211\}$. The coalition of users with fingerprints in P can frame the user with fingerprint 011.

Frameproof codes

Definition

Let $c(\geq 2)$ be an integer. A *c-frameproof code* (FP) is a subset $C \subset F^l$ s.t. $\forall P \subset C$ with $|P| \leq c$, we have $desc(P) \cap C = P$ ($\Leftrightarrow x \in desc(P) \cap C$ implies $x \in P \Leftrightarrow \forall |P| = c$ and $x \in C \setminus P$, $x \notin desc(P)$).

Example

Let $F = \{\infty\} \cup \mathbb{Z}_2$ and $C = \cup_{i=1}^{4} X_i$, where

$$\begin{aligned} X_1 &= \{(\infty, i, i, i) : i \in \mathbb{Z}_2\}, \\ X_2 &= \{(i, \infty, i, i+1) : i \in \mathbb{Z}_2\}, \\ X_3 &= \{(i, i+1, \infty, i) : i \in \mathbb{Z}_2\}, \\ X_4 &= \{(i, i, i+1, \infty) : i \in \mathbb{Z}_2\}. \end{aligned}$$

Then C is a 3-frameproof code of size 8. Further, let $I_0 = (\infty, \infty, \infty, \infty)$, then $C \cup \{I_0\}$ is also 3-frameproof.

Frameproof codes

Definition

Let $c(\geq 2)$ be an integer. A *c-frameproof code* (FP) is a subset $C \subset F^l$ s.t. $\forall P \subset C$ with $|P| \leq c$, we have $desc(P) \cap C = P$ ($\Leftrightarrow x \in desc(P) \cap C$ implies $x \in P \Leftrightarrow \forall |P| = c$ and $x \in C \setminus P$, $x \notin desc(P)$).

Example

Let $F = \{\infty\} \cup \mathbb{Z}_2$ and $C = \cup_{i=1}^{4} X_i$, where

$$\begin{aligned} X_1 &= \{(\infty, i, i, i) : i \in \mathbb{Z}_2\}, \\ X_2 &= \{(i, \infty, i, i+1) : i \in \mathbb{Z}_2\}, \\ X_3 &= \{(i, i+1, \infty, i) : i \in \mathbb{Z}_2\}, \\ X_4 &= \{(i, i, i+1, \infty) : i \in \mathbb{Z}_2\}. \end{aligned}$$

Then C is a 3-frameproof code of size 8. Further, let $I_0 = (\infty, \infty, \infty, \infty)$, then $C \cup \{I_0\}$ is also 3-frameproof.

A 4-FP code

Example

Let $F = \{\infty\} \cup \mathbb{Z}_3$. Define

$$\begin{aligned}
X_1 &= \{(\infty, i, i, i, i) : i \in \mathbb{Z}_3\},\\
X_2 &= \{(i, \infty, i, i+1, i+2) : i \in \mathbb{Z}_3\},\\
X_3 &= \{(i, i, \infty, i+2, i+1) : i \in \mathbb{Z}_3\},\\
X_4 &= \{(i, i+1, i+2, \infty, i) : i \in \mathbb{Z}_3\},\\
X_5 &= \{(i, i+2, i+1, i, \infty) : i \in \mathbb{Z}_3\}.
\end{aligned}$$

Let $C = \cup_{i=1}^{5} X_i$, which forms a 4-ary 4-frameproof code of size 15. Furthermore, $C \cup \{(\infty, \infty, \infty, \infty, \infty)\}$ is also 4-frameproof.

c-SFP codes

Definition

Secure frameproof codes (SFP) are defined to demand that no coalition of at most c users can frame another disjoint coalition of at most c users; i.e., for any two disjoint subsets P and P' of size at most c, we have $desc(P) \cap desc(P') = \emptyset$.

Example

$C = \{011, 120, 101, 210\}$ is a 2-frameproof code. But $\{110\} \in desc(\{011, 120\}) \cap desc(\{101, 210\})$, i.e., C is not a 2-SFP code.

c-SFP codes

Definition

Secure frameproof codes (SFP) are defined to demand that no coalition of at most c users can frame another disjoint coalition of at most c users; i.e., for any two disjoint subsets P and P' of size at most c, we have $desc(P) \cap desc(P') = \emptyset$.

Example

$C = \{011, 120, 101, 210\}$ is a 2-frameproof code. But $\{110\} \in desc(\{011, 120\}) \cap desc(\{101, 210\})$, i.e., C is not a 2-SFP code.

c-IPP codes

Definition

Codes with *identifiable parent property* (IPP) require that no coalition of at most c users can produce a copy that cannot be traced back to at least one member of the coalition; i.e., if $x \in desc(P)$ for some $P \subset C$ of size at most c, then

$$\bigcap_{\{Q: x \in desc(Q), |Q| \leq c\}} Q \neq \emptyset.$$

Example

$C = \{011, 123, 211, 332\}$ is a 4-IPP code.
$D = \{011, 113, 121\}$ is not a 2-IPP code, since $x = 111$ is a descendent of any two codewords.

c-IPP codes

Definition

Codes with *identifiable parent property* (IPP) require that no coalition of at most c users can produce a copy that cannot be traced back to at least one member of the coalition; i.e., if $x \in desc(P)$ for some $P \subset C$ of size at most c, then

$$\bigcap_{\{Q: x \in desc(Q), |Q| \leq c\}} Q \neq \emptyset.$$

Example

$C = \{011, 123, 211, 332\}$ is a 4-IPP code.
$D = \{011, 113, 121\}$ is not a 2-IPP code, since $x = 111$ is a descendent of any two codewords.

c-TA codes

Definition

Traceability codes (TA) have much stronger identifiable parent property which allows an efficient (i.e., linear-time in the size of the code) algorithm to determine one member of the coalition. For any $x, y \in C$, let $I(x, y) = \{i : x_i = y_i\}$. For any $|P| \leq c$ and any $x \in desc(P)$, there exist $y \in P$ such that $|I(x, y)| > |I(x, z)|$ for all $z \in C \setminus P$.

Example

$C = \{011, 123, 211, 332\}$ is a 4-IPP code. But it is not a 2-TA code. For example, let $x = 111 \in desc(\{011, 123\})$. However, $|I(x, 123)| = 1$ and $|I(x, 011)| = 2$, and $|I(x, 211)| = 2$.

c-TA codes

Definition

Traceability codes (TA) have much stronger identifiable parent property which allows an efficient (i.e., linear-time in the size of the code) algorithm to determine one member of the coalition. For any $x, y \in C$, let $I(x, y) = \{i : x_i = y_i\}$. For any $|P| \leq c$ and any $x \in desc(P)$, there exist $y \in P$ such that $|I(x, y)| > |I(x, z)|$ for all $z \in C \setminus P$.

Example

$C = \{011, 123, 211, 332\}$ is a 4-IPP code. But it is not a 2-TA code. For example, let $x = 111 \in desc(\{011, 123\})$. However, $|I(x, 123)| = 1$ and $|I(x, 011)| = 2$, and $|I(x, 211)| = 2$.

Hash families

Definition

An (n, q)-*hash function* is a function $h : A \to F$ with $|A| = n$ and $|F| = q$. An (n, q)-*hash family* is a set $\mathcal{H}$ of (n, q)-hash functions from A to F. Denoted by $\mathrm{HF}(l; n, q)$ if $|\mathcal{H}| = l$.

- $c \geq 2$. $\mathcal{H}$ is an (n, q, c)-*perfect hash family* if $\forall X \subset A$ with $|X| = c$, there exists at least one $h \in \mathcal{H}$ s.t. $h|_X$ is injective. Denoted by $\mathrm{PHF}(l; n, q, c)$ if $|\mathcal{H}| = l$;
- $\mathcal{H}$ is an (n, q, c_1, c_2)-*separating hash family* if for any disjoint $X_1, X_2 \subset A$ with $|X_1| = c_1$ and $|X_2| = c_2$, there exists at least one $h \in \mathcal{H}$ s.t. $|h(X_1) \cap h(X_2)| = \emptyset$. Denoted by $\mathrm{SHF}(l; n, q, c_1, c_2)$ if $|\mathcal{H}| = l$;

Hash families

Definition

An (n, q)-*hash function* is a function $h : A \to F$ with $|A| = n$ and $|F| = q$. An (n, q)-*hash family* is a set $\mathcal{H}$ of (n, q)-hash functions from A to F. Denoted by $\mathrm{HF}(l; n, q)$ if $|\mathcal{H}| = l$.

- $c \geq 2$. $\mathcal{H}$ is an (n, q, c)-*perfect hash family* if $\forall X \subset A$ with $|X| = c$, there exists at least one $h \in \mathcal{H}$ s.t. $h|_X$ is injective. Denoted by $\mathrm{PHF}(l; n, q, c)$ if $|\mathcal{H}| = l$;
- $\mathcal{H}$ is an (n, q, c_1, c_2)-*separating hash family* if for any disjoint $X_1, X_2 \subset A$ with $|X_1| = c_1$ and $|X_2| = c_2$, there exists at least one $h \in \mathcal{H}$ s.t. $|h(X_1) \cap h(X_2)| = \emptyset$. Denoted by $\mathrm{SHF}(l; n, q, c_1, c_2)$ if $|\mathcal{H}| = l$;

Hash families

Definition

An (n,q)-*hash function* is a function $h : A \to F$ with $|A| = n$ and $|F| = q$. An (n,q)-*hash family* is a set $\mathcal{H}$ of (n,q)-hash functions from A to F. Denoted by $\mathrm{HF}(l; n, q)$ if $|\mathcal{H}| = l$.

- $c \geq 2$. $\mathcal{H}$ is an (n,q,c)-*perfect hash family* if $\forall X \subset A$ with $|X| = c$, there exists at least one $h \in \mathcal{H}$ s.t. $h|_X$ is injective. Denoted by $\mathrm{PHF}(l; n, q, c)$ if $|\mathcal{H}| = l$;
- $\mathcal{H}$ is an (n,q,c_1,c_2)-*separating hash family* if for any disjoint $X_1, X_2 \subset A$ with $|X_1| = c_1$ and $|X_2| = c_2$, there exists at least one $h \in \mathcal{H}$ s.t. $|h(X_1) \cap h(X_2)| = \emptyset$. Denoted by $\mathrm{SHF}(l; n, q, c_1, c_2)$ if $|\mathcal{H}| = l$;

HFs and codes (Staddon, Stinson and Wei, 2001, IT IEEE)

A code $C \subset F^l$ with $|C| = n \Leftrightarrow$ an HF$(l; n, q)$ when depicted by a $n \times l$ matrix.

$$\mathcal{H}(C) = \begin{array}{c|c} & \begin{array}{cccc} h_1 & h_2 & \cdots & h_l \end{array} \\ \begin{array}{c} c_1 \\ c_2 \\ \vdots \\ c_n \end{array} & \left(\begin{array}{cccc} & & & \\ & & & \\ & & & \\ & & & \end{array} \right)_{n \times l} \end{array}$$

C is a c-FP code iff $\mathcal{H}(C)$ is an SHF$(l; n, q, c, 1)$;
C is a c-SFP code iff $\mathcal{H}(C)$ is an SHF$(l; n, q, c, c)$;
C is a 2-IPP code iff $\mathcal{H}(C)$ is simultaneously a PHF$(l; n, q, 3)$ and an SHF$(l; n, q, 2, 2)$.

Outline

$M_{c,l}(q)$

- Let $M_{c,l}(q)$ be the largest cardinality of a q-ary c-frameproof code of length l.
- Staddon, Stinson and Wei(2001) proved
$$M_{c,l}(q) \leq c\left(q^{\lceil l/c \rceil} - 1\right).$$
for all $q \geq 2$.
- (Blackburn, 2003) Let $r \equiv l \pmod{c}$. Then
$$M_{c,l}(q) \leq max\left\{q^{\lceil l/c \rceil}, r(q^{\lceil l/c \rceil} - 1) + (c-r)(q^{\lfloor l/c \rfloor} - 1)\right\}.$$

$M_{c,l}(q)$

- Let $M_{c,l}(q)$ be the largest cardinality of a q-ary c-frameproof code of length l.
- Staddon, Stinson and Wei(2001) proved

$$M_{c,l}(q) \leq c\left(q^{\lceil l/c \rceil} - 1\right).$$

for all $q \geq 2$.

- (Blackburn, 2003) Let $r \equiv l \pmod{c}$. Then

$$M_{c,l}(q) \leq max\left\{q^{\lceil l/c \rceil}, r(q^{\lceil l/c \rceil} - 1) + (c-r)(q^{\lfloor l/c \rfloor} - 1)\right\}.$$

$M_{c,l}(q)$

- Let $M_{c,l}(q)$ be the largest cardinality of a q-ary c-frameproof code of length l.
- Staddon, Stinson and Wei(2001) proved

$$M_{c,l}(q) \leq c\left(q^{\lceil l/c \rceil} - 1\right).$$

  for all $q \geq 2$.
- (Blackburn, 2003) Let $r \equiv l \pmod{c}$. Then

$$M_{c,l}(q) \leq max\left\{q^{\lceil l/c \rceil}, r(q^{\lceil l/c \rceil} - 1) + (c-r)(q^{\lfloor l/c \rfloor} - 1)\right\}.$$

Sketch of the proof

Proof of $M_{c,l}(q) \leq max\{q^{\lceil l/c \rceil}, r(q^{\lceil l/c \rceil} - 1) + (c-r)(q^{\lfloor l/c \rfloor} - 1)\}$:

- $S \subset [l]$, $|S| = s$, $U_S = \{x \in C : \nexists y \in C \; s.t. \; x_i = y_i, \forall i \in S\}$, $|U_S| \leq q^{|S|}$. If $|C| > q^{|S|}$, then $|U_S| \leq q^{|S|} - 1$.
- $[l] = S_1|S_2|\ldots|S_c$, $|S_j| = \lceil l/c \rceil$ or $\lfloor l/c \rfloor$. If $C = \cup_{j=1}^{c} U_{S_j}$ then the upper bound is obvious.
- Otherwise, $\exists x \in C \setminus \cup_{j=1}^{c} U_{S_j}$.
  $x \notin U_{S_j} \Leftrightarrow \exists y^j \in C \setminus \{x\}$ s.t. $y^j|_{S_j} = x|_{S_j}$.
- It is true for each $j = 1, 2, \ldots, c$, so there exist $y^1, y^2, \ldots, y^c \in C \setminus \{x\}$ such that $x \in desc(\{y^1, y^2, \ldots, y^c\})$.

Sketch of the proof

Proof of $M_{c,l}(q) \leq max\{q^{\lceil l/c \rceil}, r(q^{\lceil l/c \rceil} - 1) + (c - r)(q^{\lfloor l/c \rfloor} - 1)\}$:

- $S \subset [l]$, $|S| = s$, $U_S = \{x \in C : \nexists y \in C \ s.t.\ x_i = y_i, \forall i \in S\}$, $|U_S| \leq q^{|S|}$. If $|C| > q^{|S|}$, then $|U_S| \leq q^{|S|} - 1$.
- $[l] = S_1|S_2|\ldots|S_c$, $|S_j| = \lceil l/c \rceil$ or $\lfloor l/c \rfloor$. If $C = \cup_{j=1}^{c} U_{S_j}$ then the upper bound is obvious.
- Otherwise, $\exists x \in C \setminus \cup_{j=1}^{c} U_{S_j}$.
  $x \notin U_{S_j} \Leftrightarrow \exists y^j \in C \setminus \{x\}$ s.t. $y^j|_{S_j} = x|_{S_j}$.
- It is true for each $j = 1, 2, \ldots, c$, so there exist $y^1, y^2, \ldots, y^c \in C \setminus \{x\}$ such that $x \in desc(\{y^1, y^2, \ldots, y^c\})$.

Sketch of the proof

Proof of $M_{c,l}(q) \leq max\{q^{\lceil l/c \rceil}, r(q^{\lceil l/c \rceil} - 1) + (c - r)(q^{\lfloor l/c \rfloor} - 1)\}$:

- $S \subset [l]$, $|S| = s$, $U_S = \{x \in C : \nexists y \in C \ s.t. \ x_i = y_i, \forall i \in S\}$, $|U_S| \leq q^{|S|}$. If $|C| > q^{|S|}$, then $|U_S| \leq q^{|S|} - 1$.
- $[l] = S_1|S_2|\ldots|S_c$, $|S_j| = \lceil l/c \rceil$ or $\lfloor l/c \rfloor$. If $C = \cup_{j=1}^{c} U_{S_j}$ then the upper bound is obvious.
- Otherwise, $\exists x \in C \setminus \cup_{j=1}^{c} U_{S_j}$.
  $x \notin U_{S_j} \Leftrightarrow \exists y^j \in C \setminus \{x\}$ s.t. $y^j|_{S_j} = x|_{S_j}$.
- It is true for each $j = 1, 2, \ldots, c$, so there exist $y^1, y^2, \ldots, y^c \in C \setminus \{x\}$ such that $x \in desc(\{y^1, y^2, \ldots, y^c\})$. $\square$

Sketch of the proof

Proof of $M_{c,l}(q) \leq max\{q^{\lceil l/c \rceil}, r(q^{\lceil l/c \rceil} - 1) + (c-r)(q^{\lfloor l/c \rfloor} - 1)\}$:

- $S \subset [l]$, $|S| = s$, $U_S = \{x \in C : \nexists y \in C \ s.t. \ x_i = y_i, \forall i \in S\}$, $|U_S| \leq q^{|S|}$. If $|C| > q^{|S|}$, then $|U_S| \leq q^{|S|} - 1$.
- $[l] = S_1|S_2|\ldots|S_c$, $|S_j| = \lceil l/c \rceil$ or $\lfloor l/c \rfloor$. If $C = \cup_{j=1}^{c} U_{S_j}$ then the upper bound is obvious.
- Otherwise, $\exists x \in C \setminus \cup_{j=1}^{c} U_{S_j}$.
  $x \notin U_{S_j} \Leftrightarrow \exists y^j \in C \setminus \{x\}$ s.t. $y^j|_{S_j} = x|_{S_j}$.
- It is true for each $j = 1, 2, \ldots, c$, so there exist $y^1, y^2, \ldots, y^c \in C \setminus \{x\}$ such that $x \in desc(\{y^1, y^2, \ldots, y^c\})$. $\square$

Small Optimal Cases ($l \leq c$)

Lemma

If $2 \leq l \leq c$, $M_{c,l}(q) = l(q-1)$.

Since

- By the previous upper bound, $M_{c,l}(q) \leq l(q-1)$.
- Let $F = 0, 1, \ldots, q-1$. The set C of all words of length l and weight exactly 1 (i.e., the elements of F^l with exactly one nonzero component) forms a c-frameproof code of cardinality $l(q-1)$. □

Small Optimal Cases ($l \leq c$)

Lemma

If $2 \leq l \leq c$, $M_{c,l}(q) = l(q-1)$.

Since

- By the previous upper bound, $M_{c,l}(q) \leq l(q-1)$.
- Let $F = 0, 1, \ldots, q-1$. The set C of all words of length l and weight exactly 1 (i.e., the elements of F^l with exactly one nonzero component) forms a c-frameproof code of cardinality $l(q-1)$. $\square$

Small Optimal Cases ($l \leq c$)

Lemma

If $2 \leq l \leq c$, $M_{c,l}(q) = l(q-1)$.

Since

- By the previous upper bound, $M_{c,l}(q) \leq l(q-1)$.
- Let $F = 0, 1, \ldots, q-1$. The set C of all words of length l and weight exactly 1 (i.e., the elements of F^l with exactly one nonzero component) forms a c-frameproof code of cardinality $l(q-1)$. $\square$

Blackburn, 2003

Theorem

Let c, l and q be positive integers greater than 1. Let $t \in \{1, 2, \ldots, c\}$ be an integer such that $t \equiv l \pmod{c}$. Then

$$M_{c,l}(q) \leq \left(\frac{l}{l-(t-1)\lceil l/c \rceil}\right) q^{\lceil l/c \rceil} + O(q^{\lceil l/c \rceil - 1}).$$

Reed-Solomn codes are c-FP codes: Let $q \geq l$ be a prime power. Let $\alpha_1, \alpha_2, \ldots, \alpha_l$ be distinct elements in $\mathbb{F}_q$. Define

$$C = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_l)) : f \in \mathbb{F}_q[X], \deg f < \lceil l/c \rceil\}.$$

Then C is a c-frameproof code of cardinality $q^{\lceil l/c \rceil}$ $(\forall c, l)$. If $q = l - 1$, allow a polynomial f to be evaluated at a "point at infinity": $f(\infty)$ is defined to be the coefficient of $X^{\lceil l/c \rceil}$ in f.

$R_{c,l}$

Definition

Let $R_{c,l}(q) := M_{c,l}(q)/q^{\lceil l/c \rceil}$ and $R_{c,l} := \lim_{q\to\infty} R_{c,l}(q)$.

Corollary

Let c and l be positive integers greater than 1. Let $t \in [c]$ be an integer such that $t \equiv l \pmod{c}$. Then

$$R_{c,l} \leq \frac{l}{l-(t-1)\lceil l/c \rceil}.$$

Theorem

(1) $R_{c,l} = 1$ *when* $l \equiv 1 \pmod{c}$;

(2) $R_{c,l} = 2$ *when* $c = 2$ *and* l *is even (Blackburn, 2003);*

Question

Blackburn (2003) asked the following question: Is there a q-ary c-frameproof code of length l with cardinality approximately $l/(l-\lceil l/c \rceil)q^{\lceil l/c \rceil}$ when $l \equiv 2 \pmod c$?
i.e., $R_{c,l} = l/(l - \lceil l/c \rceil)$?
When $l = c+2$, $R_{c,c+2} \leq \frac{c+2}{c}$. Blackburn proved that $R_{3,5} = 5/3$.
Our work is to prove that $R_{c,c+2} = \frac{c+2}{c}$ for a large amount of integers c.

Outline

From high distance codes

Lemma

Let C be a code of minimum distance d and length l. Then C is a c-frameproof code for any $c \geq 2$ satisfying $l > c(l-d)$.

Example

(1)(RS codes) Let $q \geq l$ be a prime power. Let $\alpha_1, \alpha_2, \ldots, \alpha_l$ be distinct elements in $\mathbb{F}_q$.

$$C = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_l)) : f \in F[X], \deg f < \lceil l/c \rceil\}.$$

Then C is of minimum distance $d = l - (\lceil l/c \rceil - 1)$. Obviously, $l > c(l-d)$. So C is a c-frameproof code of cardinality $q^{\lceil l/c \rceil}$.
(2) The converse is not true. $C = \{112, 212, 312\}$ is a 2-FP code. Let $d = 2$, then $l > c(l-d)$, but C is not of minimum distance 2.

From high distance codes

Lemma

Let C be a code of minimum distance d and length l. Then C is a c-frameproof code for any $c \geq 2$ satisfying $l > c(l-d)$.

Example

(1)(RS codes) Let $q \geq l$ be a prime power. Let $\alpha_1, \alpha_2, \ldots, \alpha_l$ be distinct elements in $\mathbb{F}_q$.

$$C = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_l)) : f \in F[X], \deg f < \lceil l/c \rceil\}.$$

Then C is of minimum distance $d = l - (\lceil l/c \rceil - 1)$. Obviously, $l > c(l-d)$. So C is a c-frameproof code of cardinality $q^{\lceil l/c \rceil}$.
(2) The converse is not true. $C = \{112, 212, 312\}$ is a 2-FP code. Let $d = 2$, then $l > c(l-d)$, but C is not of minimum distance 2.

Product Construction (PC)

Lemma

If

(1) *C: an s-ary code, length l over an alphabet S, $d \geq l-(t-1)$ (i.e. each codeword is uniquely determined by specifying t of its components), and*

(2) *D: an m-ary code, length l over an alphabet F, $d \geq l-(t-1)$.*

Then

$C' = \{(x, y) : x \in C, y \in D\}$ is an sm-ary code, length l over $S \times F$, $d \geq l-(t-1)$, $|C'| = |C||D|$, where

$$(x, y) = ((x_1, y_1), (x_2, y_2), \ldots, (x_l, y_l)).$$

If $c(t-1) < l$, then C' is a c-FP code.

Modified Product Construction (MPC)

Lemma

If: $c \geq t \geq 2$, $l \geq 2t-1$ *and* $l = c(t-1)+r$, *where* $t \leq r \leq c$.

(1) C: *an* s*-ary code, length* l *over an alphabet* S, $d \geq l-(t-1)$. C *satisfies Property* $P(t)$, *i.e.,* $\exists$ *a special element say* $\infty \in S$, *s.t. each codeword contains* $\leq t-1$ ∞*'s.*

(2) D: *an* m*-ary code, length* l *over an alphabet* F, $d \geq l-(t-1)$.

Then

$C' = \{[x,y] : x \in C, y \in D\}$ *is an* $((s-1)m+1)$*-ary code, length* l *over* $((S \setminus \{\infty\}) \times F) \cup \{\infty\}$, c*-FP code,* $|C'| = |C||D|$, *where* $[x,y]$ *is defined as*

$$[x,y]_i = \begin{cases} \infty, & \text{if } x_i = \infty; \\ (x_i, y_i), & \text{otherwise.} \end{cases}$$

Modified Product Construction (MPC)

Proof.

(1) Aim: $\forall [x, y] \in C'$ and $P \subset C'$, $|P| = c$ such that $[x, y] \in desc(P) \Rightarrow [x, y] \in P$.
Since $l = c(t-1) + r$, where $r > t$ and $[x, y]$ has $\leq t - 1$ ∞'s, there exist $[x', y'] \in P$ that agrees with $[x, y]$ more than t components that are not equal to ∞.
Thus x, x' have more than t identical components, $x = x'$.
Similarly, $y = y'$.
(2)$|C'| = |C||D|$ since $l \geq 2t - 1$.

$\square$

Comparison of two constructions

PC: $C' = \{(x, y) : x \in C, y \in D\}$ is an sm-ary code, length l over $S \times F$, $d \geq l - (t-1)$, $|C'| = |C||D|$;

MPC: $C' = \{[x, y] : x \in C, y \in D\}$ is an $((s-1)m+1)$-ary code, length l over $((S \setminus \{\infty\}) \times F) \cup \{\infty\}$, $d \geq l - (t-1)$ (i.e., c-FP code), $|C'| = |C||D|$.

Comm: c, l and $|C'|$.

Diff: PC: sm-ary, but MPC: $((s-1)m+1)$-ary. MPC needs a little stronger C.

Example: C and D are both RS codes. By PC, $\frac{|C|}{s^{\lceil l/c \rceil}} \cdot \frac{|D|}{m^{\lceil l/c \rceil}} = \frac{|C||D|}{(sm)^{\lceil l/c \rceil}} = 1$.

Comparison of two constructions

PC: $C' = \{(x, y) : x \in C, y \in D\}$ is an sm-ary code, length l over $S \times F$, $d \geq l - (t-1)$, $|C'| = |C||D|$;

MPC: $C' = \{[x, y] : x \in C, y \in D\}$ is an $((s-1)m+1)$-ary code, length l over $((S \setminus \{\infty\}) \times F) \cup \{\infty\}$, $d \geq l - (t-1)$ (i.e., c-FP code), $|C'| = |C||D|$.

Comm: c, l and $|C'|$.

Diff: PC: sm-ary, but MPC: $((s-1)m+1)$-ary. MPC needs a little stronger C.

Example: C and D are both RS codes. By PC, $\frac{|C|}{s^{\lceil l/c \rceil}} \cdot \frac{|D|}{m^{\lceil l/c \rceil}} = \frac{|C||D|}{(sm)^{\lceil l/c \rceil}} = 1.$

Comparison of two constructions

PC: $C' = \{(x, y) : x \in C, y \in D\}$ is an sm-ary code, length l over $S \times F$, $d \geq l - (t-1)$, $|C'| = |C||D|$;

MPC: $C' = \{[x, y] : x \in C, y \in D\}$ is an $((s-1)m+1)$-ary code, length l over $((S \setminus \{\infty\}) \times F) \cup \{\infty\}$, $d \geq l - (t-1)$ (i.e., c-FP code), $|C'| = |C||D|$.

Comm: c, l and $|C'|$.

Diff: PC: sm-ary, but MPC: $((s-1)m+1)$-ary. MPC needs a little stronger C.

Example: C and D are both RS codes. By PC, $\frac{|C|}{s^{\lceil l/c \rceil}} \cdot \frac{|D|}{m^{\lceil l/c \rceil}} = \frac{|C||D|}{(sm)^{\lceil l/c \rceil}} = 1$.

Comparison of two constructions

PC: $C' = \{(x, y) : x \in C, y \in D\}$ is an sm-ary code, length l over $S \times F$, $d \geq l - (t-1)$, $|C'| = |C||D|$;

MPC: $C' = \{[x, y] : x \in C, y \in D\}$ is an $((s-1)m+1)$-ary code, length l over $((S \setminus \{\infty\}) \times F) \cup \{\infty\}$, $d \geq l - (t-1)$ (i.e., c-FP code), $|C'| = |C||D|$.

Comm: c, l and $|C'|$.

Diff: PC: sm-ary, but MPC: $((s-1)m+1)$-ary. MPC needs a little stronger C.

Example: C and D are both RS codes. By PC, $\frac{|C|}{s^{\lceil l/c \rceil}} \cdot \frac{|D|}{m^{\lceil l/c \rceil}} = \frac{|C||D|}{(sm)^{\lceil l/c \rceil}} = 1.$

Comparison of two constructions

PC: $C' = \{(x, y) : x \in C, y \in D\}$ is an sm-ary code, length l over $S \times F$, $d \geq l - (t-1)$, $|C'| = |C||D|$;

MPC: $C' = \{[x, y] : x \in C, y \in D\}$ is an $((s-1)m+1)$-ary code, length l over $((S \setminus \{\infty\}) \times F) \cup \{\infty\}$, $d \geq l - (t-1)$ (i.e., c-FP code), $|C'| = |C||D|$.

Comm: c, l and $|C'|$.

Diff: PC: sm-ary, but MPC: $((s-1)m+1)$-ary. MPC needs a little stronger C.

Example: C and D are both RS codes. By PC, $\frac{|C|}{s^{\lceil l/c \rceil}} \cdot \frac{|D|}{m^{\lceil l/c \rceil}} = \frac{|C||D|}{(sm)^{\lceil l/c \rceil}} = 1$.

Corollary

An application of the Modified Product Construction:

C: Let $s = c + 1$ be a prime power and $l = c + 2$, $t = r = 2$. Let C be the RS code defined by all nonzero $f \in \mathbb{F}_s[X], \deg f < 2$. Then $|C| = s^2 - 1$ satisfying Property $P(2)$ with 0 as the special element.

D: Let m be a prime power and l, c, t, r as above. Let D be the RS code defined by all $f \in \mathbb{F}_m[X], \deg f < 2$. Then $|D| = m^2$.

Result: Applying the modified product construction to C and D, we have C' is a q-ary c-frameproof code, where $q = (s-1)m + 1 = cm + 1$ and

$$|C'| = (s^2-1)m^2 = \frac{(s^2-1)}{(s-1)^2}(q-1)^2$$

$$= \frac{(s+1)}{(s-1)}(q-1)^2 = \frac{c+2}{c}(q-1)^2. \quad \square$$

Corollary

An application of the Modified Product Construction:

C: Let $s = c + 1$ be a prime power and $l = c + 2$, $t = r = 2$. Let C be the RS code defined by all nonzero $f \in \mathbb{F}_s[X], \deg f < 2$. Then $|C| = s^2 - 1$ satisfying Property $P(2)$ with 0 as the special element.

D: Let m be a prime power and l, c, t, r as above. Let D be the RS code defined by all $f \in \mathbb{F}_m[X], \deg f < 2$. Then $|D| = m^2$.

Result: Applying the modified product construction to C and D, we have C' is a q-ary c-frameproof code, where $q = (s-1)m + 1 = cm + 1$ and

$$|C'| = (s^2-1)m^2 = \frac{(s^2-1)}{(s-1)^2}(q-1)^2$$

$$= \frac{(s+1)}{(s-1)}(q-1)^2 = \frac{c+2}{c}(q-1)^2. \quad \square$$

Corollary

An application of the Modified Product Construction:

C: Let $s = c + 1$ be a prime power and $l = c + 2$, $t = r = 2$. Let C be the RS code defined by all nonzero $f \in \mathbb{F}_s[X], \deg f < 2$. Then $|C| = s^2 - 1$ satisfying Property $P(2)$ with 0 as the special element.

D: Let m be a prime power and l, c, t, r as above. Let D be the RS code defined by all $f \in \mathbb{F}_m[X], \deg f < 2$. Then $|D| = m^2$.

Result: Applying the modified product construction to C and D, we have C' is a q-ary c-frameproof code, where $q = (s-1)m + 1 = cm + 1$ and

$$|C'| = (s^2-1)m^2 = \frac{(s^2-1)}{(s-1)^2}(q-1)^2$$

$$= \frac{(s+1)}{(s-1)}(q-1)^2 = \frac{c+2}{c}(q-1)^2. \quad \square$$

$R_{c,c+2}$

Corollary

Let $c \geq 2$ be an integer such that $c+1$ is a prime power, and let $m \geq c+1$ be any prime power. Then there exists a q-ary c-frameproof code of length $c+2$ with cardinality $\frac{c+2}{c}(q-1)^2$, where $q = cm+1$.

Theorem

Let $c \geq 2$ be an integer such that $c+1$ is a prime power, then $R_{c,c+2} = (c+2)/c$.

$R_{c,c+2}$

Corollary

Let $c \geq 2$ be an integer such that $c+1$ is a prime power, and let $m \geq c+1$ be any prime power. Then there exists a q-ary c-frameproof code of length $c+2$ with cardinality $\frac{c+2}{c}(q-1)^2$, where $q = cm+1$.

Theorem

Let $c \geq 2$ be an integer such that $c+1$ is a prime power, then $R_{c,c+2} = (c+2)/c$.

Proof of Theorem

Proof.

(1) $R_{c,c+2} \leq (c+2)/c$ (Upper bound).

(2) $\forall q$, denote q_l the largest prime power s.t. $cq_l + 1 \leq q$, and q_u the smallest integer s.t. $cq_u + 1 \geq q$. Then $\frac{q_l}{q_u} = 1 - o(1)$.

$$M_{c,c+2}(q)/q^2 \geq M_{c,c+2}(cq_l + 1)/q^2$$

$$\geq \frac{c+2}{c}(cq_l)^2/q^2 \geq \frac{c+2}{c}(cq_l)^2/(cq_u + 1)^2,$$

which shows $R_{c,c+2} \geq (c+2)/c$.

$\square$

Proof of Theorem

Proof.

(1) $R_{c,c+2} \leq (c+2)/c$ (Upper bound).

(2) $\forall q$, denote q_l the largest prime power s.t. $cq_l + 1 \leq q$, and q_u the smallest integer s.t. $cq_u + 1 \geq q$. Then $\frac{q_l}{q_u} = 1 - o(1)$.

$$M_{c,c+2}(q)/q^2 \geq M_{c,c+2}(cq_l + 1)/q^2$$

$$\geq \frac{c+2}{c}(cq_l)^2/q^2 \geq \frac{c+2}{c}(cq_l)^2/(cq_u + 1)^2,$$

which shows $R_{c,c+2} \geq (c+2)/c$.

□

Proof of Theorem

Proof.

(1) $R_{c,c+2} \leq (c+2)/c$ (Upper bound).

(2) $\forall q$, denote q_l the largest prime power s.t. $cq_l + 1 \leq q$, and q_u the smallest integer s.t. $cq_u + 1 \geq q$. Then $\frac{q_l}{q_u} = 1 - o(1)$.

$$M_{c,c+2}(q)/q^2 \geq M_{c,c+2}(cq_l + 1)/q^2$$

$$\geq \frac{c+2}{c}(cq_l)^2/q^2 \geq \frac{c+2}{c}(cq_l)^2/(cq_u + 1)^2,$$

which shows $R_{c,c+2} \geq (c+2)/c$.

$\square$

Other results

Theorem

There exists a q-ary 2-frameproof code with length 4 of cardinality $2(q-1)^2+1$ *for any odd* $q > 1$.

Theorem

There exists a q-ary 3-frameproof code with length 5 of cardinality $\frac{5}{3}(q-1)^2+1$ *for any integer* $q \equiv 4 \pmod 6$.

Other results

Theorem

There exists a q-ary 2-frameproof code with length 4 of cardinality $2(q-1)^2+1$ *for any odd* $q>1$.

Theorem

There exists a q-ary 3-frameproof code with length 5 of cardinality $\frac{5}{3}(q-1)^2+1$ *for any integer* $q \equiv 4 \pmod 6$.

Outline

Concluding Remarks

Theorem

(1) $R_{c,l} = 1$ *when* $l \equiv 1 \pmod{c}$*;*
(2) $R_{c,l} = 2$ *when* $c = 2$ *and* l *is even;*
(3) $R_{c,c+2} = \frac{c+2}{c}$ *for all* c *s.t.* $c + 1$ *is a prime power.*

Question

(1) What is $R_{c,c+2}$ *for other values of* c*?*
(2) What is $R_{c,l}$ *in general?*

Concluding Remarks

Theorem

(1) $R_{c,l} = 1$ when $l \equiv 1 \pmod{c}$;
(2) $R_{c,l} = 2$ when $c = 2$ and l is even;
(3) $R_{c,c+2} = \frac{c+2}{c}$ for all c s.t. $c + 1$ is a prime power.

Question

(1) What is $R_{c,c+2}$ for other values of c?
(2) What is $R_{c,l}$ in general?

References

[1] S. R. Blackburn, "Frameproof codes," *SIAM J. Discrete Math.*, vol. 16, no. 3, pp. 499–510, 2003.

[2] Y. M. Chee and X. Zhang, "Improved constructions of frameproof codes," *IEEE Transactions on Information Theory*, vol. 58, no. 8, pp. 5449–5453, 2012.

[3] J. N. Staddon, D. R. Stinson, and R. Wei, "Combinatorial properties of frameproof and traceability codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 3, pp. 1042–1049, 2001.

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!