Critical Problem for Matroids and Codes

Keisuke Shiromoto
Department of Mathematics and Engineering, Kumamoto University, Japan

joint work with Thomas Britz (UNSW, Australia)
Tatsuya Maruta (Osaka Pref. Univ, Japan)
Yoshitaka Koga (Kumamoto Univ, Japan)
1. Introduction
Preliminaries

- Let $F_q$ be a finite field of $q$ elements.
- An $[n, k]$ code over $F_q$ is a $k$-dimensional subspace of $F_q^n$.
- The Hamming weight of $\mathbf{x} = (x_1, \ldots, x_n) \in F_q^n$ is defined by
  $\text{wt}(\mathbf{x}) := |\{i : x_i \neq 0\}|$.
- An $[n, k, d]$ code over $F_q$ (for short, $[n, k, d]_q$ code) is an $[n, k]$ code over $F_q$ with
  $d := \min\{\text{wt}(\mathbf{x}) : \mathbf{0} \neq \mathbf{x} \in C\}$.

**Singleton bound** (1964) If $C$ is an $[n, k, d]$ code over $F_q$, then

$$d \leq n - k + 1.$$  

**Griesmer bound** (1960) If $C$ is an $[n, k, d]$ code over $F_q$, then

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil.$$
Critical Problem (Crapo and Rota, 1970)
For given subset \( S \subseteq \mathbb{F}_q^k \), determine the maximum dimension of subspaces of \( \mathbb{F}_q^k \) which do not intersect \( S \).

\[
q = 2
\]

- Four-Color Theorem (Appel and Haken, 1976)
- Hadwiger’s Conjecture (1943)
- 5-Flow Conjecture (Tutte, 1954)
- Problem of correcting a black and white pixel image

For any subset $S \subseteq \mathbb{F}_q^k$, define the critical exponent of $S$ as follows:

$$c(S, q) := k - \max\{r \in \mathbb{Z}^+ : \exists D \subseteq \mathbb{F}_q^k \text{ s.t. dim } D = r \text{ and } D \cap S = \emptyset\}.$$ 

**Example 1.**
- Consider

  $$S = \{(1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1)\} \subseteq \mathbb{F}_2^4.$$ 

  - For instance, if

    $$D = \langle (1, 0, 0, 1), (0, 1, 0, 1), (0, 0, 1, 1) \rangle,$$

    then

    $$D \cap S = \emptyset.$$ 

  - Therefore it follows that

    $$c(S, 2) = 4 - 3 = 1.$$
A definition of matroids

Let $E$ be a finite set and let $\rho : 2^E \to \mathbb{Z}_{\geq 0}$ be a function. $\mathcal{M} = (E, \rho)$ is called a **matroid** if

(R1) If $X \subseteq E$, then $0 \leq \rho(X) \leq |X|$. 

(R2) If $X \subseteq Y \subseteq E$, then $\rho(X) \leq \rho(Y)$. 

(R3) If $X$ and $Y$ are subsets of $E$, then

$$\rho(X \cup Y) + \rho(X \cap Y) \leq \rho(X) + \rho(Y).$$
Matroids from graphs

- For an undirected graph $G = (V, E)$ and a subset $X \subseteq E$, we denote the number of connected components of $G[X]$ by $\omega(G[X])$.

- Set $\rho(X) = |V(G[X])| - \omega(G[X])$, $\forall X \subseteq E$.

- Then $M(G) := (E, \rho)$ is a matroid.

- If $X = \{4, 5, 6, 7, 8\}$, then $\rho(X) = 4 - 1 = 3$.

- If $X = \{1, 3, 7\}$, then $\rho(X) = 4 - 2 = 2$. 
Matroids from codes

- Let $C$ be an $[n, k]$ code over $\mathbb{F}_q$ with $E = \{1, 2, \ldots, n\}$.
- Let $G$ be a generator matrix of $C$, that is, a $k \times n$ matrix over $\mathbb{F}_q$ whose rows form a basis for $C$.
- For each subset $X \subseteq E$, the punctured code $C \setminus X$ is the linear code obtained by deleting the coordinate $X$ from each codeword in $C$.
- Define the function $\rho : 2^E \to \mathbb{Z}_{\geq 0}$ by
  $$\rho(X) := \dim C \setminus (E - X), \quad \forall X \subseteq E.$$
- Then $M_C := (E, \rho)$ is a matroid.
- Consider the binary $[8, 4]$ code having generator matrix
  $$G = \begin{pmatrix}
    1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
    1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
    0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
    0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
    0 & 0 & 0 & 1 & 1 & 1 & 1 & 0
  \end{pmatrix}.$$
- If $X = \{6, 7, 8\}$, then $\rho(X) = 3$. • If $X = \{4, 5, 6, 7, 8\}$, then $\rho(X) = 4$. 
Critical problem for matroids

• For a matroid $M = (E, \rho)$, the characteristic polynomial $p(M; \lambda)$ of $M$ is defined by

$$p(M; \lambda) = \sum_{X \subseteq E} (-1)^{|X|} \lambda^{\rho(E) - \rho(X)}.$$

• Let $M$ be a representable matroid over $\mathbb{F}_q$, that is, a matroid obtained from a linear code over $\mathbb{F}_q$.

• It is well known that $p(M; q^r) \geq 0$, for all $r \in \mathbb{Z}^+$.

• The critical exponent $c(M; q)$ of $M$ is defined by

$$c(M; q) = \begin{cases} \infty, & \text{if } M \text{ has a loop;} \\ \min\{j \in \mathbb{Z}^+ : p(M; q^j) > 0\}, & \text{otherwise.} \end{cases}$$
Relation with graph theory

• A *vertex colouring* of a graph $G = (V, E)$ is a map $f : V \to S$ such that $f(v) \neq f(w)$ whenever $v$ and $w$ are adjacent.

• The *chromatic number* of $G$, denoted by $\chi(G)$, is the minimum cardinality of $S$ necessary such that a map $f$ exists.

• For any loopless graph $G$,

$$\chi(G) = \min\{j \in \mathbb{Z}^+ : p(M(G); j) > 0\}.$$ 

• Thus, for $M = M(G)$,

$$q^{c(M; q) - 1} < \chi(G) \leq q^{c(M; q)}.$$
2. Main Results I
The \textit{supports} of each vector $\bm{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ and each subset $B \subseteq \mathbb{F}_q^n$ are defined respectively as:

$$\text{supp}(\bm{x}) := \{ i : x_i \neq 0 \};$$

$$\text{Supp}(B) := \bigcup_{\bm{x} \in B} \text{supp}(\bm{x}).$$

For instance, if

$$B = \{(1, 1, 0, 1, 0, 1), (1, 1, 1, 0, 0, 1)\} \subseteq \mathbb{F}_2^6,$$

then

$$\text{Supp}(B) = \{1, 2, 3, 4, 6\}.$$

For any $r, 1 \leq r \leq k$, define $\mathcal{D}_r(C) := \{D \leq C : \dim D = r\}$.

The \textit{covering dimension} of $C$ is defined by

$$\gamma(C) := \begin{cases} \min\{r : \exists D \in \mathcal{D}_r(C) \text{ s.t. } \text{Supp}(D) = E\}, & \text{if } \text{Supp}(C) \neq E; \\ \infty, & \text{otherwise.} \end{cases}$$
\[ \gamma(C) := \min\{ r \in \mathbb{Z}^+ : \dim D = r, \ D \subseteq C, \ \text{Supp}(D) = E \}. \]

**Example 2.**

- Let \( C \) be a binary \([6, 3]\) code with \( G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \).
- Then we have that

\[
C = \{(0,0,0,0,0,0), (1,0,0,0,1,1), (0,1,0,1,0,1), (0,0,1,1,1,0), (1,1,0,1,1,0), (1,0,1,1,0,1), (0,1,1,0,1,1), (1,1,1,0,0,0)\}.
\]

- For instance, if

\[
B = \langle (1,1,0,1,1,0), (1,0,1,1,0,1) \rangle,
\]

then

\[ \text{Supp}(B) = \{1, 2, 3, 4, 5, 6\}. \]

- Therefore it follows that

\[ \gamma(C) = \dim B = 2 \]
The equivalence

**Problem:** For a given \([n, k]\) code \(C\) over \(\mathbb{F}_q\), determine the covering dimension

\[\gamma(C) = \min \{ r : \exists D \in \mathcal{D}_r(C) \text{ s.t. } \text{Supp}(D) = E \} .\]

**Critical Problem** (Crapo and Rota, 1970)
For given subset \(S \subseteq \mathbb{F}_q^k\), determine the maximum dimension of subspaces of \(\mathbb{F}_q^k\) which do not intersect \(S\).
Kung’s bound (1996). If $M = (E, \rho)$ is a simple representable matroid over $\mathbb{F}_q$ with girth $g$, then

$$c(M; q) \leq \rho(E) - g + 3.$$


- Let $C$ be a binary $[n, n - 1]$ code which is (permutation) equivalent to the binary code having generator matrix $G = \begin{pmatrix} 1 & \ddots & \ddots & \ddots \\ \vdots & \ddots & \ddots & \ddots \\ \vdots & & \ddots & \ddots \\ 1 & & & \ddots \end{pmatrix}$.

- Then $C^\perp = \{0 = (0, 0, \ldots, 0), 1 = (1, 1, \ldots, 1)\}$ and so $d^\perp = n$.

- If $n$ is odd, then $1 \notin C$ and so

$$\gamma(C) = 2(= (n - 1) - n + 3).$$
Let $G$ be $k \times n$ matrix over $\mathbb{F}_q$ which contains as columns exactly one multiple of each nonzero vector in $\mathbb{F}_q^k$.

Then the $[n = (q^k - 1)/(q - 1), k]$ code $C$ having generator matrix $G$ is a dual Hamming code (or a simplex code) and $d^\perp = 3$.

It finds easily that

$$c(\text{PG}(k - 1, q), q) = k - 0 = k.$$ 

Thus we have that

$$\gamma(C) = k (= k - 3 + 3).$$
Proposition 2. Let $C$ be an $[n, k]$ code over $\mathbb{F}_q$ with $d^\perp = 3$.

$$\gamma(C') = k - d^\perp + 3 (= k - 3 + 3 = k),$$

if and only if $C$ is isomorphic to a dual Hamming code.

Proposition 3. Let $C$ be a binary $[n, n-1]$ MDS code.

$$\gamma(C) = k - d^\perp + 3 (= (n-1) - n + 3 = 2),$$

if and only if $n$ is odd.

Theorem 4. Let $C$ be a binary $[n, k]$ code with $3 < d^\perp < k + 1$. Then

$$\gamma(C') \leq k - d^\perp + 2.$$
Theorem 5. Let $C$ be an $[n, k]$ code over $\mathbb{F}_q$ with $d^\perp > 3$. If $q$ is odd, then

$$\gamma(C) \leq k - d^\perp + 2.$$ 

Sketch of Proof

$$\gamma(C) = k - d^\perp + 3$$

$$t = d^\perp - 1$$

$$\exists [t + q - 1, t, q] \text{ MDS code } C'$$


If $C$ is a nontrivial $[n, k \geq 3, n - k + 1]$ MDS code over $\mathbb{F}_q$, $q$ odd, then $n \leq q + k - 2$.

... contradiction.
**Theorem 6.** Let $C$ be an $[n, k]$ code over $\mathbb{F}_q$ with $d^\perp > 3$. If $q = 2^m$ and $m \geq 2$, then

$$\gamma(C) \leq k - d^\perp + 2.$$

**Sketch of Proof**

$$\gamma(C) = k - d^\perp + 3$$

$$t = d^\perp - 1$$

$$\exists [t + q - 1, t, q] \text{ MDS code } C'$$

**Lemma.** (Segre (1955) and Casse (1969))

The maximum value of $n$ for which there exists an $[n, 4, n - 3]$ MDS code over $\mathbb{F}_q$ is $q + 1$ for $q \geq 4$.

$$\exists [q + 3, 4, q] \text{ MDS code } C''$$

... contradiction.
**Theorem** (Britz and S, 2016)

If $C$ is an $[n, k]_q$ code with $d^\perp := d(C^\perp)$, then

$$\gamma(C) \leq k - d^\perp + 2$$

unless $C$ is isomorphic to a dual Hamming code or $C$ is a binary $[n, n - 1]$ code such that $d^\perp = n$ is odd, in either which case $\gamma(C) = k - d^\perp + 3$.

**Corollary** (Britz and S, 2016)

If $S$ is a subset of $\mathbb{F}_q^k$ and $M[S] = (E, I)$ is the matroid obtained from the matrix $[S]$, then

$$c(S, q) \leq \rho(E) - g + 2$$

unless $S = \text{PG}(k - 1, q)$ or $S = \{e_1, e_2, \ldots, e_k, \sum_{i=1}^k e_i\} \subseteq \mathbb{F}_2^k$ and $k$ is even, in either which case $\gamma(C) = \rho(E) - g + 3$. 
3. Main Results II
**Critical Problem** (Crapo and Rota, 1970)
For given subset $S \subseteq \mathbb{F}^n_q$, determine the maximum dimension of subspaces of $\mathbb{F}^n_q$ which do not intersect $S$.

$$S = B_{n,t}(q) := \{ \mathbf{x} \in \mathbb{F}^n_q : \text{wt}(\mathbf{x}) \leq t \}$$

**Problem in Coding Theory:**
For given $n, t$, and $q$ ($n, t \in \mathbb{Z}^+, q : a$ prime power), determine the maximum dimension $k$ such that there exists an $[n, k, t + 1]_q$ code.
• For any subset $S \subseteq \mathbb{F}_q^n$, define the *critical exponent* of $S$ as follows:

$$c(S, q) := n - \max\{r \in \mathbb{Z}^+ : \exists D \leq \mathbb{F}_q^n \text{ s.t. } \dim D = r \text{ and } D \cap S = \emptyset\}.$$ 

**Example 3.**

• Consider

$$S = B_{4,2}(2) = \{\mathbf{x} \in \mathbb{F}_2^4 : \text{wt}(\mathbf{x}) \leq 2\}.$$ 

• Assume that there exists a $[4, 2, 3]_2$ code $C$ and let

$$G = \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \end{pmatrix}$$

be a generator matrix of $C$.

• Then there does not exist such $a, b, c, d \in \mathbb{F}_2$.

• On the other hand, $D = \{(0, 0, 0, 0), (1, 1, 1, 0)\}$ is a $[4, 1, 3]_2$ code.

• Therefore it follows that

$$c(B_{4,2}(2), 2) = 4 - 1 = 3.$$
Kung’s results

Theorem 7. (Kung, 1996)

\[ c(B_{n,t}(q), q) = n - 1 \iff n - 1 \geq t \geq n - \left\lceil \frac{n}{q + 1} \right\rceil. \]

Theorem 8. (Kung, 1996) Let

\[ e = \left\lfloor \frac{1}{q + 1 + \frac{1}{q}} \left\lceil \frac{n}{q + 1} \right\rceil \right\rfloor. \]

Suppose that \( e \geq 1 \) and

\[ n - \left\lceil \frac{n}{q + 1} \right\rceil - 1 \geq t \geq n - \left\lceil \frac{n}{q + 1} \right\rceil - e. \]

Then \( B_{n,t}(q) \) has critical exponent \( n - 2 \).
**Theorem** (Koga, Maruta, and S, 2017) Suppose that $n \geq q^2 + q + 1$. If $n = (q^2 + q + 1)m + aq + b$ for $m \geq 1$, $0 \leq a \leq q - 1$, and $0 \leq b \leq q - 1$ such that (1) $a < b$ with $b - a \neq 1$, or (2) $a > b = 0$ holds, then $B_{n,t}(q)$ has critical exponent $n - 2$ if and only if

$$n - \left\lfloor \frac{n}{q + 1} \right\rfloor - 1 \geq t \geq n - \left\lfloor \frac{(q + 1)n}{q^2 + q + 1} \right\rfloor - 1.$$ 

Otherwise $B_{n,t}(q)$ has critical exponent $n - 2$ if and only if

$$n - \left\lfloor \frac{n}{q + 1} \right\rfloor - 1 \geq t \geq n - \left\lfloor \frac{(q + 1)n}{q^2 + q + 1} \right\rfloor.$$
**Sketch of Proof**

- We shall prove that

\[ \exists [n, 3, t + 1]_q \text{ code with } t \geq n - \left\lfloor \frac{n(q + 1)}{(q^2 + q + 1)} \right\rfloor \]

and

\[ \exists [n, 3, s + 1]_q \text{ code with } s \leq n - \left\lfloor \frac{n(q + 1)}{(q^2 + q + 1)} \right\rfloor - 1 \]

**or**

\[ \exists [n, 3, t + 1]_q \text{ code with } t \geq n - \left\lfloor \frac{n(q + 1)}{(q^2 + q + 1)} \right\rfloor - 1 \]

and

\[ \exists [n, 3, s + 1]_q \text{ code with } s \leq n - \left\lfloor \frac{n(q + 1)}{(q^2 + q + 1)} \right\rfloor - 2 \]

- It is sufficient to prove that

\[ [t + 1] + \left\lfloor \frac{(t + 1)}{q} \right\rfloor + \left\lfloor \frac{(t + 1)}{q^2} \right\rfloor = \cdots > n, \]

and

\[ [s + 1] + \left\lfloor \frac{(s + 1)}{q} \right\rfloor + \left\lfloor \frac{(s + 1)}{q^2} \right\rfloor = \cdots \leq n, \]

and the existences of such Griesmer codes.
• Set $\theta_i := q^i + q^{i-1} + \cdots + q + 1$, for any non-negative integer $i$, and set $\theta_{-1} := 0$.

• Let $s_0, s_1, \ldots, s_{r-1}$ be integers s.t. $0 \leq s_i \leq q$ for $0 \leq i \leq r - 1$.

• We consider the following cases:

\textbf{Cases } $\mathcal{B}_r$:

1. $n = \theta_r m$ for some $m \geq 1$,
2. $n = \theta_r m + \theta_r - \theta_l$ for some $m \geq 0$ and some $l$ with $0 \leq l \leq r - 1$,
3. $n = \theta_r m + \sum_{i=0}^{r-1} s_i q^i$ for some $m \geq r - 1$ and some $s_0, \ldots, s_{r-1}$ with $1 \leq s_0 \leq s_1 \leq \cdots \leq s_{r-1}$,
4. $n = \theta_r m + \beta \theta_{r-1} + 1$ for some $m \geq r - 1$ and some $\beta$ with $0 \leq \beta \leq q - 1$,
5. $n = \theta_r m + \theta_r - \theta_l + 1$ for some $m \geq 0$ and some $l$ with $0 \leq l \leq r - 1$.

\textbf{Theorem} (Koga, Maruta, and S, 2017) \textit{For given } $n$ \textit{and } $r$, \textit{suppose that both one of the cases } $\mathcal{B}_r$ \textit{and one of the cases } $\mathcal{B}_{r-1}$ \textit{hold. Then } $B_{n,t}(q)$ \textit{has critical exponent } $n - r$ \textit{if and only if}

\[ n - \left\lceil \frac{n\theta_{r-2}}{\theta_{r-1}} \right\rceil - 1 \geq t \geq n - \left\lceil \frac{n\theta_{r-1}}{\theta_r} \right\rceil. \]
**Corollary** (Britz and S, 2016)
If $S$ is a subset of $\mathbb{F}_q^k$ and $M[S] = (E, \mathcal{I})$ is the matroid obtained from the matrix $[S]$, then

$$c(S, q) \leq \rho(E) - g + 2$$

unless $S = \text{PG}(k - 1, q)$ or $S = \{e_1, e_2, \ldots, e_k, \sum_{i=1}^k e_i\} \subseteq \mathbb{F}_2^k$ and $k$ is even, in either which case $\gamma(C) = \rho(E) - g + 3$.

*Britz and Shiromoto, On the covering dimension of linear codes, IEEE IT 62 (2016)*

**Theorem** (Brooks, 1941)
For any connected undirected graph $G$ with maximum degree $\Delta$,

$$\chi(G) \leq \Delta,$$

unless $G$ is a complete graph or an odd cycle, in which case $\chi(G) \leq \Delta + 1$. 
Critical Problem (Crapo and Rota, 1970)
For given subset $S \subseteq \mathbb{F}_q^n$, determine the maximum dimension of subspaces of $\mathbb{F}_q^n$ which do not intersect $S$.

$S = B_{n,t}(q) := \{ \mathbf{x} \in \mathbb{F}_q^n : \text{wt}(\mathbf{x}) \leq t \}$

Theorem (Koga, Maruta, and S, 2017) For given $n$ and $r$, suppose that both one of the cases $B_r$ and one of the cases $B_{r-1}$ hold. Then $B_{n,t}(q)$ has critical exponent $n - r$ if and only if

$$n - \left\lfloor \frac{n\theta_{r-2}}{\theta_{r-1}} \right\rfloor - 1 \geq t \geq n - \left\lfloor \frac{n\theta_{r-1}}{\theta_r} \right\rfloor .$$

Problem: What is the next $S$?