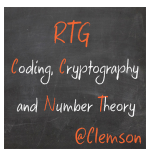
Batch Codes from Hamming and Reed-Müller Codes

Felice Manganiello

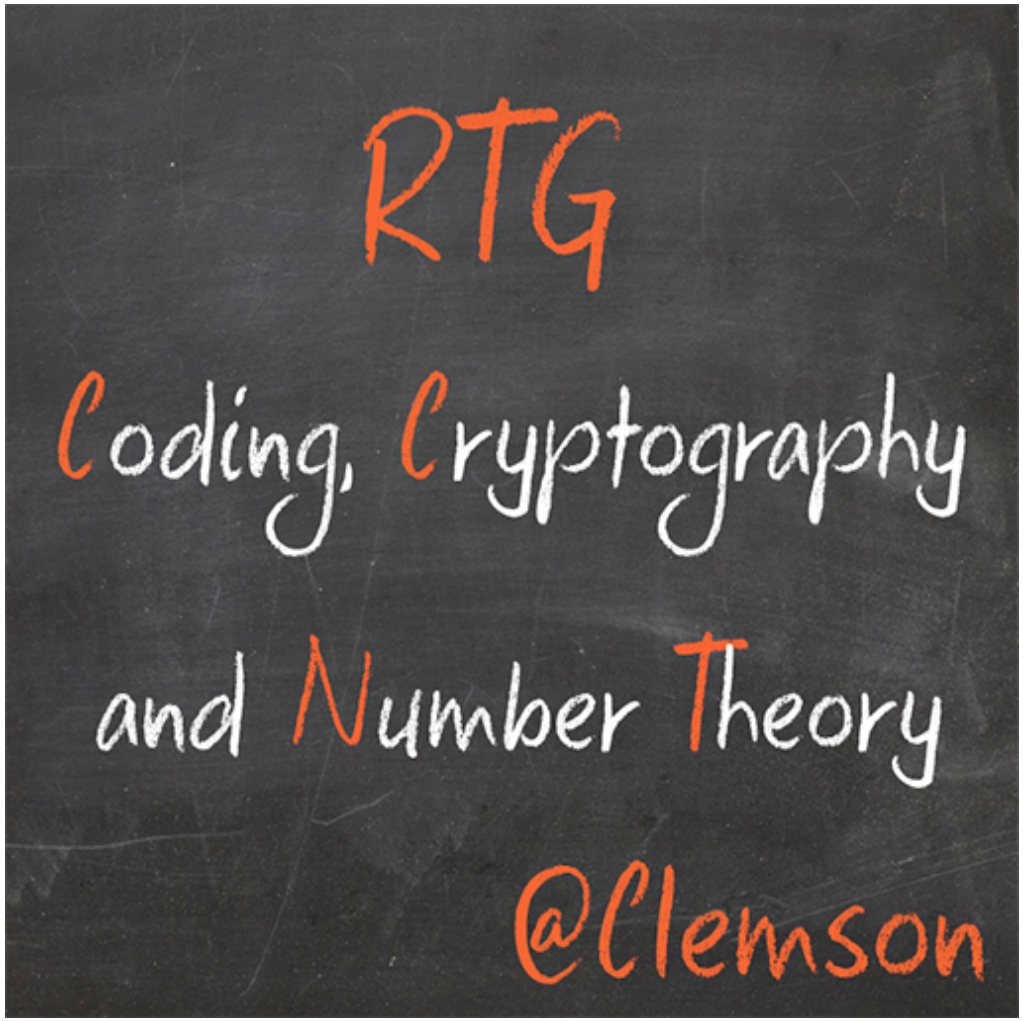
The Sixth Code-Based Cryptography Workshop
April 6, 2018

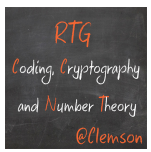
with T. Baumbaugh, Y. Diaz, S. Friesenhahn and A. Vetter.
Research financed by the NSF RTG grant (DMS #1547399).



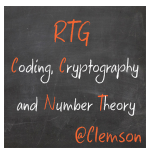
CLEMSON UNIVERSITY

RTG: Coding Theory, Cryptography and Number Theory





CLEMSON UNIVERSITY

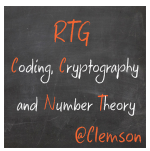


CLEMSON UNIVERSITY

Previously on ...

Codes for Queueing Theory.

Suppose the new episode of Game of Thrones is available for downloads at time X. It is to be expected that at time X+epsilon an incredible amount of fan of the show would be requesting the episode. If the video is stored in only one server working on a first come first serve policy, then the waiting time for completing the download tasks becomes unbearable. How is it possible to decrease download times? This is a question of queueing theory, meaning the mathematical study of waiting lines, or queues. A better strategy is to store the episode in multiple servers. Some recent works show that lower download times are achievable perhaps using redundancy and coding theory.



Research direction: Impact of linear code in queuing theory.

CLEMSON UNIVERSITY

RTG
Coding, Cryptography and Number Theory
@Clemson

CLEMSON UNIVERSITY

Coding Theory Application to Queueing and Download

PICTURE

EVENODD Codes [Blaum *et al.* '95]

Let $\mathcal{C}$ be a $[8, 4, 3]_q$ linear code with

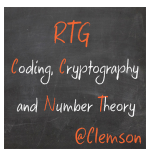
$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

EVENODD Codes [Blaum *et al.* '95]

Encode the word $m = (a_1, a_2, b_1, b_2) \in \mathbb{F}_q^4$ and obtain

$$mG = (a_1, a_2, b_1, b_2, a_1 + b_1, a_2 + b_2, a_2 + b_1, a_1 + a_2 + b_2) \in \mathbb{F}_q^8.$$

a_1	b_1	$a_1 + b_1$	$a_2 + b_1$
a_2	b_2	$a_2 + b_2$	$a_1 + a_2 + b_2$



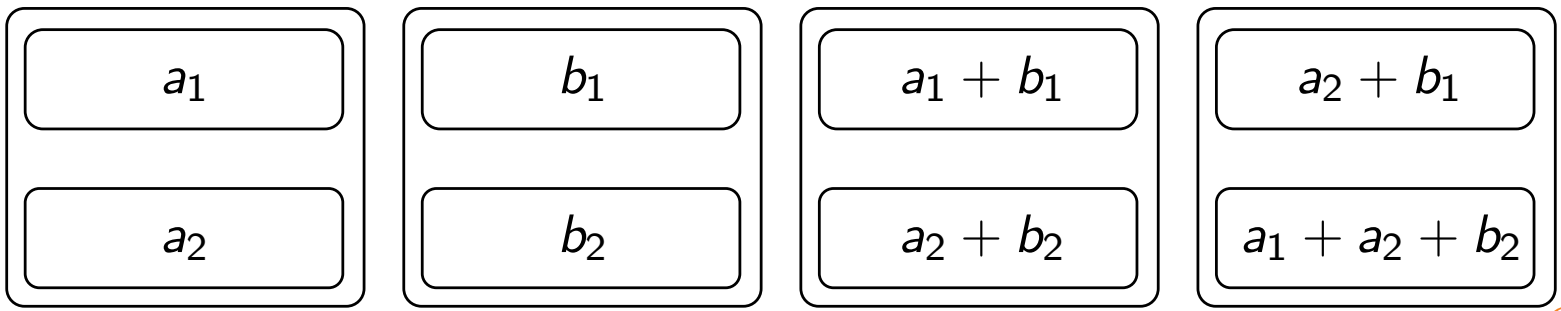
CLEMSON UNIVERSITY

EVENODD Codes [Blaum *et al.* '95]

Encode the word $m = (a_1, a_2, b_1, b_2) \in \mathbb{F}_q^4$ and obtain

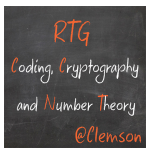
$$mG = (a_1, a_2, b_1, b_2, a_1 + b_1, a_2 + b_2, a_2 + b_1, a_1 + a_2 + b_2) \in \mathbb{F}_q^8.$$

Store the information in different disks.



GOAL

- We have k chunks of data
- Encode as n chunks of data



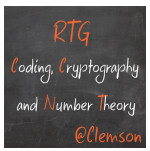
CLEMSON UNIVERSITY

GOAL

- We have k chunks of data
- Encode as n chunks of data
- Spread across m devices/servers

GOAL

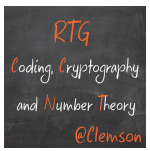
- We have k chunks of data
- Encode as n chunks of data
- Spread across m devices/servers
- There are t users downloading data



CLEMSON UNIVERSITY

GOAL

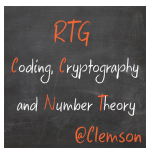
- We have k chunks of data
- Encode as n chunks of data
- Spread across m devices/servers
- There are t users downloading data
  - Could be distinct
  - Could allow repetitions
  - Could all be the same



CLEMSON UNIVERSITY

GOAL

- We have k chunks of data
- Encode as n chunks of data
- Spread across m devices/servers
- There are t users downloading data
  - Could be distinct
  - Could allow repetitions
  - Could all be the same
- Each device has limited bandwidth τ

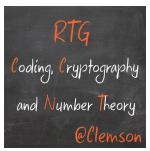


CLEMSON UNIVERSITY

GOAL

- We have k chunks of data
- Encode as n chunks of data
- Spread across m devices/servers
- There are t users downloading data
  - Could be distinct
  - Could allow repetitions
  - Could all be the same
- Each device has limited bandwidth τ

We want to be able to satisfy user demands regardless of what the data is



CLEMSON UNIVERSITY

Papers

- Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai. *Batch codes and their applications*. 2004
- M.B. Paterson, D.R. Stinson, and R. Wei. *Combinatorial Batch Codes*. 2008
- Helger Lipmaa, Vitaly Skachek. *Linear Batch Codes*. 2015
- Hui Zhang and Vitaly Skachek. *Bounds for Batch Codes with Restricted Query Size*. 2016
- N. Silberstein and A. Gál. *Optimal combinatorial batch codes based on block designs*. 2016
- Eldho K. Thomas and Vitaly Skachek. *Constructions and Bounds for Batch Codes with Small Parameters*. 2017
- Hui Zhang, Eitan Yaakobi, and Natalia Silberstein. *Multiset combinatorial batch codes*. 2018

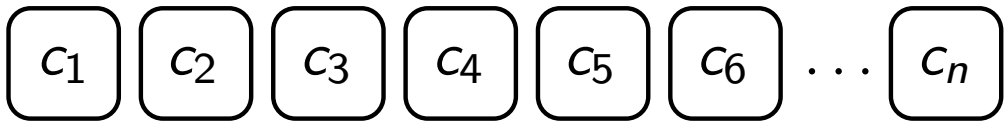
RTG Coding, Cryptography and Number Theory @Clemson

CLEMSON UNIVERSITY

Batch Codes [Ishai *et al.* '04]

A code $\mathcal{C}$ is an $[n, k, t, m, \tau]_q$ linear batch code if:

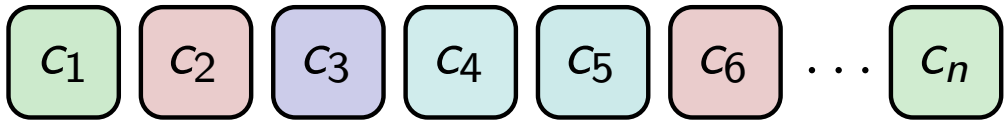
- it is an $[n, k]$ linear code over $\mathbb{F}_q$,



Batch Codes [Ishai *et al.* '04]

A code $\mathcal{C}$ is an $[n, k, t, m, \tau]_q$ linear batch code if:

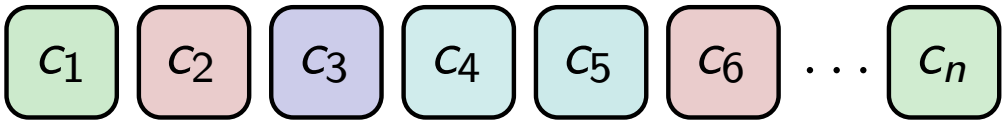
- it is an $[n, k]$ linear code over $\mathbb{F}_q$,
- $\exists$ a partition of $[n] = \{1, \ldots, n\}$ into *buckets* $B_\ell \subset [n]$ for $\ell \in [m]$ such that:



Batch Codes [Ishai *et al.* '04]

A code $\mathcal{C}$ is an $[n, k, t, m, \tau]_q$ linear batch code if:

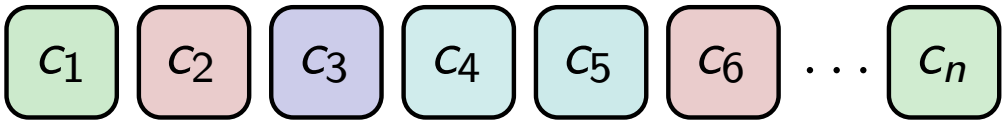
- it is an $[n, k]$ linear code over $\mathbb{F}_q$,
- $\exists$ a partition of $[n] = \{1, \ldots, n\}$ into *buckets* $B_\ell \subset [n]$ for $\ell \in [m]$ such that:
- for each t-tuple of indices, $(i_1, \ldots, i_t) \in [n]^t$, there exist subsets $A_{i_1}, \ldots, A_{i_t} \subset [n]$ such that:



Batch Codes [Ishai *et al.* '04]

A code $\mathcal{C}$ is an $[n, k, t, m, \tau]_q$ linear batch code if:

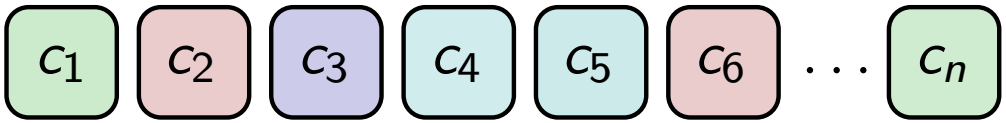
- it is an $[n, k]$ linear code over $\mathbb{F}_q$,
- $\exists$ a partition of $[n] = \{1, \ldots, n\}$ into *buckets* $B_\ell \subset [n]$ for $\ell \in [m]$ such that:
- for each t-tuple of indices, $(i_1, \ldots, i_t) \in [n]^t$, there exist subsets $A_{i_1}, \ldots, A_{i_t} \subset [n]$ such that:
  - For any $c \in \mathcal{C}$, c_{i_s} can be recovered elements with $c|_{A_{i_s}}$



Batch Codes [Ishai *et al.* '04]

A code $\mathcal{C}$ is an $[n, k, t, m, \tau]_q$ linear batch code if:

- it is an $[n, k]$ linear code over $\mathbb{F}_q$,
- $\exists$ a partition of $[n] = \{1, \ldots, n\}$ into *buckets* $B_\ell \subset [n]$ for $\ell \in [m]$ such that:
- for each t-tuple of indices, $(i_1, \ldots, i_t) \in [n]^t$, there exist subsets $A_{i_1}, \ldots, A_{i_t} \subset [n]$ such that:
  - For any $c \in \mathcal{C}$, c_{i_s} can be recovered elements with $c|_{A_{i_s}}$
  - The subsets do not overlap



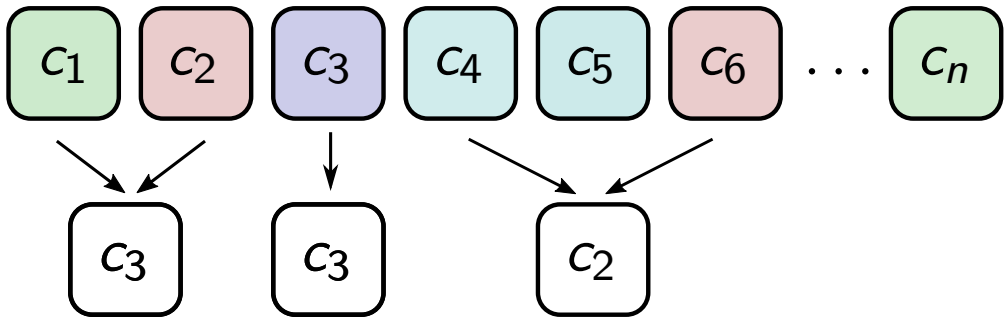
RTG Coding, Cryptography and Number Theory @Clemson

CLEMSON UNIVERSITY

Batch Codes [Ishai *et al.* '04]

A code $\mathcal{C}$ is an $[n, k, t, m, \tau]_q$ linear batch code if:

- it is an $[n, k]$ linear code over $\mathbb{F}_q$,
- $\exists$ a partition of $[n] = \{1, \ldots, n\}$ into *buckets* $B_\ell \subset [n]$ for $\ell \in [m]$ such that:
- for each t-tuple of indices, $(i_1, \ldots, i_t) \in [n]^t$, there exist subsets $A_{i_1}, \ldots, A_{i_t} \subset [n]$ such that:
  - For any $c \in \mathcal{C}$, c_{i_s} can be recovered elements with $c|_{A_{i_s}}$
  - The subsets do not overlap
  - $\left|(\bigcup_{s=1}^{t} A_{i_s}) \cap B_\ell\right| \leq \tau$ for $\ell \in [m]$



RTG Coding, Cryptography and Number Theory @Clemson

CLEMSON UNIVERSITY

Simple Example

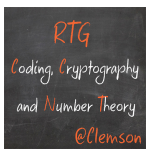
Consider a $[5, 3]$ code over $\mathbb{F}_2$ with parity check matrix

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

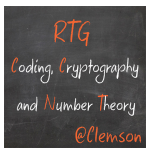
and buckets

$$\{1, 2\}, \{3, 4\}, \{5\}.$$

- This gives us the equations:
  - $c_1 + c_3 + c_5 = 0$
  - $c_2 + c_4 + c_5 = 0$
- If we want to recover $(1, 2)$, we can take
  - $A_1 = \{1\}$
  - $A_2 = \{4, 5\}$



CLEMSON UNIVERSITY



CLEMSON UNIVERSITY

A bound on the download bandwidth

Theorem (Bandwidth bound)

Let $\mathcal{C}$ be an $[n, k, t, m, \tau]$ linear batch code with minimal locality r. Then it holds that

$$m\tau \geq (t-1)r + 1.$$

A bound on the download bandwidth

Theorem (Bandwidth bound)

Let $\mathcal{C}$ be an $[n, k, t, m, \tau]$ linear batch code with minimal locality r. Then it holds that

$$m\tau \geq (t-1)r + 1.$$

- Pick symbol with all recovery sets of size at least r

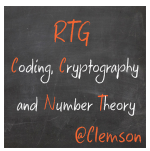
A bound on the download bandwidth

Theorem (Bandwidth bound)

Let $\mathcal{C}$ be an $[n, k, t, m, \tau]$ linear batch code with minimal locality r. Then it holds that

$$m\tau \geq (t-1)r + 1.$$

- Pick symbol with all recovery sets of size at least r
- Try to recover t copies of it
  - One direct download
  - The remaining $t-1$ copies require at least r downloads



CLEMSON UNIVERSITY

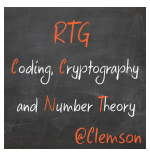
A bound on the download bandwidth

Theorem (Bandwidth bound)

Let $\mathcal{C}$ be an $[n, k, t, m, \tau]$ linear batch code with minimal locality r. Then it holds that

$$m\tau \geq (t-1)r + 1.$$

- Pick symbol with all recovery sets of size at least r
- Try to recover t copies of it
  - One direct download
  - The remaining $t-1$ copies require at least r downloads
- This gives at least $(t-1)r + 1$ total downloads required



CLEMSON UNIVERSITY

A bound on the download bandwidth

Theorem (Bandwidth bound)

Let $\mathcal{C}$ be an $[n, k, t, m, \tau]$ linear batch code with minimal locality r. Then it holds that

$$m\tau \geq (t-1)r + 1.$$

- Pick symbol with all recovery sets of size at least r
- Try to recover t copies of it
  - One direct download
  - The remaining $t-1$ copies require at least r downloads
- This gives at least $(t-1)r + 1$ total downloads required

Definition

A n $[n, k, t, m, \tau]$ linear batch code $\mathcal{C}$ with minimal locality r is optimal if it satisfies the Bandwidth bound with equality.

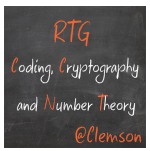
Locality based on the dual code

Lemma

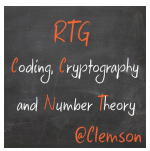
Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear code and $d^\perp$ be the minimum distance of $\mathcal{C}^\perp$. If $\mathcal{C}^\perp$ is generated by its minimum weight codewords and

$$\bigcup_{\lambda \in \mathcal{C}^\perp} \text{supp}(\lambda) = [n],$$

then $\mathcal{C}$ is a locally recoverable code with locality $d^\perp - 1$.



CLEMSON UNIVERSITY



CLEMSON UNIVERSITY

Definition

Definition

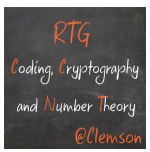
Let $s \geq 2$, $n = 2^s - 1$ and $H \in \mathbb{F}_2^{2^s-1 \times s}$ be a matrix whose columns are all of the nonzero vectors of $\mathbb{F}_2^s$. The binary Hamming code is

$$\mathcal{H}_s = \ker(H^t).$$

$\mathcal{H}_s$ is a $[2^s - 1, 2^s - 1 - s, 3]$ linear code.

If $s = 3$, then the parity check matrix H is as follows:

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$



Then $\mathcal{H}_s$ is a $[7, 4, 3]$ linear code.

CLEMSON UNIVERSITY

Locality and Availability

Lemma

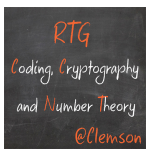
The Hamming code $\mathcal{H}_s$ has locality $2^{s-1}-1$ and availability 1.

It is well known that $\mathcal{H}_s^{\perp}$ is a $[2^s-1, s, 2^{s-1}]$ linear code that satisfies the *Dual minimum codewords condition.* then $\mathcal{H}_s$ has locality $2^{s-1}-1$.

Suppose $\mu = 3$ wlog for $i = 1$, then there are two minimum weight codewords $\lambda_1, \lambda_2 \in \mathcal{C}^{\perp}$ such that

$$\text{supp}(\lambda_1) \cap \text{supp}(\lambda_2) = \{1\}$$

Since $\mathcal{C}^{\perp}$ is linear and $\mathbf{1} \in \mathcal{C}^{\perp}$, then $1 + \lambda_1 + \lambda_2 \in \mathcal{C}^{\perp}$.

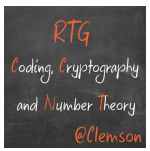


CLEMSON UNIVERSITY

Batch Properties

Theorem

A binary $[n, k]$ Hamming code is an optimal batch code with properties $[n, k, 2, m, \tau]$, for any $m, \tau \in \mathbb{N}$ such that $m\tau = 2^{s-1}$.



CLEMSON UNIVERSITY

Batch Properties

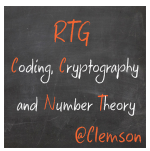
Theorem

A binary $[n, k]$ Hamming code is an optimal batch code with properties $[n, k, 2, m, \tau]$, for any $m, \tau \in \mathbb{N}$ such that $m\tau = 2^{s-1}$.

Buckets construction.

Let $h_j \in \mathbb{F}_2^s \setminus \{0\}$ for $1 \leq j \leq n$.

- If $h_a + h_b = \mathbf{1}$, $a\&b$ same bucket.
- Since $h_n = \mathbf{1}$ in H, n own bucket.



CLEMSON UNIVERSITY

Batch Properties

Theorem

A binary $[n, k]$ Hamming code is an optimal batch code with properties $[n, k, 2, m, \tau]$, for any $m, \tau \in \mathbb{N}$ such that $m\tau = 2^{s-1}$.

Buckets construction.

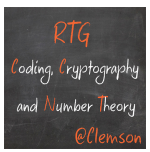
Let $h_j \in \mathbb{F}_2^s \setminus \{0\}$ for $1 \leq j \leq n$.

- If $h_a + h_b = \mathbf{1}$, $a\&b$ same bucket.
- Since $h_n = \mathbf{1}$ in H, n own bucket.

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Buckets:

$\{1, 6\}, \{2, 5\}, \{3, 4\}, \{7\}$



CLEMSON UNIVERSITY

Batch Properties

Theorem

A binary $[n, k]$ Hamming code is an optimal batch code with properties $[n, k, 2, m, \tau]$, for any $m, \tau \in \mathbb{N}$ such that $m\tau = 2^{s-1}$.

Buckets construction.

Let $h_j \in \mathbb{F}_2^s \setminus \{0\}$ for $1 \leq j \leq n$.

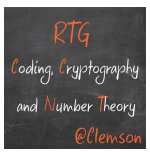
- If $h_a + h_b = \mathbf{1}$, $a\&b$ same bucket.
- Since $h_n = \mathbf{1}$ in H, n own bucket.

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Buckets:

$\{1, 6\}, \{2, 5\}, \{3, 4\}, \{7\}$

The support of any $\lambda \in \mathcal{C}^{\perp}$ intersects each bucket in a singleton.



CLEMSON UNIVERSITY

Batch Properties

Theorem

A binary $[n, k]$ Hamming code is an optimal batch code with properties $[n, k, 2, m, \tau]$, for any $m, \tau \in \mathbb{N}$ such that $m\tau = 2^{s-1}$.

Buckets construction.

Let $h_j \in \mathbb{F}_2^s \setminus \{0\}$ for $1 \leq j \leq n$.

- If $h_a + h_b = \mathbf{1}$, $a\&b$ same bucket.
- Since $h_n = \mathbf{1}$ in H, n own bucket.

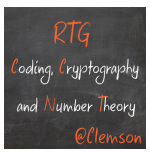
$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Buckets:

$\{1, 6\}, \{2, 5\}, \{3, 4\}, \{7\}$

The support of any $\lambda \in \mathcal{C}^{\perp}$ intersects each bucket in a singleton.

$(1, 1) \to \{1\}, \{1, 3, 5, 7\}$



CLEMSON UNIVERSITY

Batch Properties

Theorem

A binary $[n, k]$ Hamming code is an optimal batch code with properties $[n, k, 2, m, \tau]$, for any $m, \tau \in \mathbb{N}$ such that $m\tau = 2^{s-1}$.

Buckets construction.

Let $h_j \in \mathbb{F}_2^s \setminus \{0\}$ for $1 \leq j \leq n$.

- If $h_a + h_b = \mathbf{1}$, $a\&b$ same bucket.
- Since $h_n = \mathbf{1}$ in H, n own bucket.

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

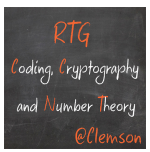
Buckets:

$\{1, 6\}, \{2, 5\}, \{3, 4\}, \{7\}$

The support of any $\lambda \in \mathcal{C}^{\perp}$ intersects each bucket in a singleton.

$(1, 1) \rightarrow \{1\}, \{1, 3, 5, 7\}$

$(1, 2) \rightarrow \{1\}, \{2\}$



CLEMSON UNIVERSITY

Batch Properties

Theorem

A binary $[n, k]$ Hamming code is an optimal batch code with properties $[n, k, 2, m, \tau]$, for any $m, \tau \in \mathbb{N}$ such that $m\tau = 2^{s-1}$.

Buckets construction.

Let $h_j \in \mathbb{F}_2^s \setminus \{0\}$ for $1 \leq j \leq n$.

- If $h_a + h_b = \mathbf{1}$, $a\&b$ same bucket.
- Since $h_n = \mathbf{1}$ in H, n own bucket.

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Buckets:

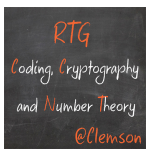
$\{1, 6\}, \{2, 5\}, \{3, 4\}, \{7\}$

The support of any $\lambda \in \mathcal{C}^\perp$ intersects each bucket in a singleton.

$(1, 1) \to \{1\}, \{1, 3, 5, 7\}$

$(1, 2) \to \{1\}, \{2\}$

For a bucket $\{a, b\}$ there exists $\lambda \in \mathcal{C}^\perp$ such that $a \notin \text{supp}(\lambda)$ and $b \in \text{supp}\,\lambda$.



CLEMSON UNIVERSITY

Batch Properties

Theorem

A binary $[n, k]$ Hamming code is an optimal batch code with properties $[n, k, 2, m, \tau]$, for any $m, \tau \in \mathbb{N}$ such that $m\tau = 2^{s-1}$.

Buckets construction.

Let $h_j \in \mathbb{F}_2^s \setminus \{0\}$ for $1 \leq j \leq n$.

- If $h_a + h_b = \mathbf{1}$, $a\&b$ same bucket.
- Since $h_n = \mathbf{1}$ in H, n own bucket.

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Buckets:

$\{1, 6\}, \{2, 5\}, \{3, 4\}, \{7\}$

The support of any $\lambda \in \mathcal{C}^\perp$ intersects each bucket in a singleton.

$(1, 1) \to \{1\}, \{1, 3, 5, 7\}$

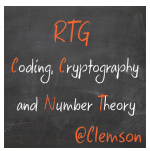
$(1, 2) \to \{1\}, \{2\}$

For a bucket $\{a, b\}$ there exists $\lambda \in \mathcal{C}^\perp$ such that $a \notin \text{supp}(\lambda)$ and $b \in \text{supp}\,\lambda$.

$(1, 6) \to \{1\}, \{2, 3, 6, 7\}$

RTG Coding, Cryptography and Number Theory @Clemson

CLEMSON UNIVERSITY



CLEMSON UNIVERSITY

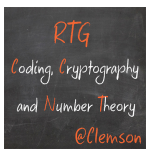
Definition

Definition

Let $\mathbb{F}_2[x_1, \ldots, x_\mu]$, $\mathbb{F}_2^\mu = \{P_1, \ldots, P_n\}$ and $\rho < \mu$.
The binary Reed-Müller code, $\mathcal{RM}(\rho, \mu)$ is defined as:

$$\mathcal{RM}(\rho, \mu) = \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathbb{F}_2[X_1, \ldots, X_\mu]^\rho\},$$

where $\mathbb{F}_2[x_1, \ldots, x_\mu]^\rho$ is the set of polynomials of total degree at most ρ.
$\mathcal{RM}(\rho, \mu)$ is a $[n = 2^\mu, k = \sum_{i=0}^{\rho} \binom{\mu}{i}]$ linear code.



CLEMSON UNIVERSITY

Alternative definition

Definition

Let $\rho < \mu$ and $n = 2^\mu$. A binary Reed-Müller code $\mathcal{RM}(\rho, \mu)$ is

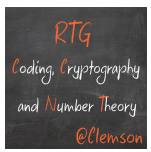
$$\mathcal{RM}(\rho, \mu) = \{(u \mid u+v) \mid u \in \mathcal{RM}(\rho, \mu-1),\ v \in \mathcal{RM}(\rho-1, \mu-1)\}$$

where $\mathcal{RM}(0, \mu) = \{0, \mathbf{1}\} \subset \mathbb{F}_2^n$, and $\mathcal{RM}(\mu, \mu) = \mathbb{F}_2^n$.

As a consequence if $G_{\rho,\mu}$ is a generator matrix of the code $\mathcal{RM}(\rho, \mu)$, then

$$G_{\rho,\mu} = \begin{pmatrix} G_{\rho,\mu-1} & G_{\rho,\mu-1} \\ 0 & G_{\rho-1,\mu-1} \end{pmatrix}$$

where $G_{0,\mu} = \mathbf{1}$ and $G_{\mu,\mu} = I$.



CLEMSON UNIVERSITY

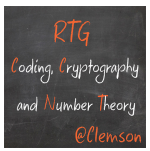
Properties of Reed-Müller codes

Theorem

The dual of a Reed-Müller code $\mathcal{RM}(\rho, \mu)$ is the Reed-Müller code $\mathcal{RM}(\mu - 1 - \rho, \mu)$.

Corollary (Case of Thm by Ding-Key 2000)

Binary Reed-Müller codes are generated by their minimal weight codewords.



CLEMSON UNIVERSITY

Properties of $\mathcal{RM}(1,\mu)$

Theorem

Let $\mathbb{F}_q^\mu = \{P_1, \ldots, P_n\}$ be the set of evaluation points for $\mathcal{RM}(1,\mu)$. Then

$$(\lambda_1, \ldots, \lambda_n) \in \mathcal{RM}(1,\mu)^\perp \iff \sum_{i=1}^{n} \lambda_i P_i = 0 \ \textit{and} \ \sum_{i=1}^{n} \lambda_i = 0.$$

Corollary

The minimum distance of $\mathcal{RM}(1,\mu)^\perp$ is 4.

If $P_1 = 0$, $P_i, P_j \in \mathbb{F}_2^\mu$ and $P_\ell = P_i + P_j$ then

$$P_1 + P_i + P_j + P_\ell = 0.$$

RTG Coding, Cryptography and Number Theory @Clemson

CLEMSON UNIVERSITY

Locality and Availability

Theorem

$\mathcal{RM}(1,\mu)$ is a locally repairable code with locality 3 with availability

- $\frac{2^\mu-1}{3}$ *when* μ *is even, and*
- *at least* $\frac{2^\mu-4}{4}$ *when* μ *is odd.*

Batch properties of $\mathcal{RM}(1, \mu)$

Theorem

Any first order Reed-Müller code, $\mathcal{RM}(1, \mu)$, with $\mu \geq 4$, has batch properties $(n, k, 4, m, \tau)$ for any $m, \tau \in \mathbb{N}$ such that $m\tau = 10$.

Any $\mathcal{RM}(1, \mu)$ is an optimal batch code when $t = 4$.

Theorem

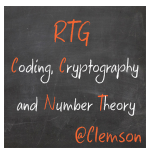
Let $\rho \geq 1$ and $\mu \in \{2\rho + 2, 2\rho + 3\}$. Then, for $\rho' \leq \rho$, $\mathcal{RM}(\rho', \mu)$ is a $(n, k, 4, m, \tau)$ linear batch code for any $m, \tau \in \mathbb{N}$ such that $m\tau = 10 \cdot 2^{2\rho - 2}$.

Conclusions and projects

- Batch codes can be considered as a generalization of codes with locality and availability.
- Hamming codes are optimal batch codes for 2-strings download.
- First order Reed-Müller codes are optimal batch codes for 4-strings download.

Projects

- Find constructions of batch codes for any request from t users.
- Influence of codes with high availability on the McEliece Cryptosystem.



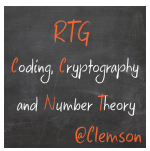
CLEMSON UNIVERSITY

Conclusions and projects

- Batch codes can be considered as a generalization of codes with locality and availability.
- Hamming codes are optimal batch codes for 2-strings download.
- First order Reed-Müller codes are optimal batch codes for 4-strings download.

Projects

- Find constructions of batch codes for any request from t users.
- Influence of codes with high availability on the McEliece Cryptosystem.



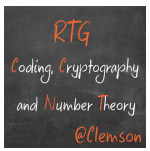
CLEMSON UNIVERSITY

Conclusions and projects

- Batch codes can be considered as a generalization of codes with locality and availability.
- Hamming codes are optimal batch codes for 2-strings download.
- First order Reed-Müller codes are optimal batch codes for 4-strings download.

Projects

- Find constructions of batch codes for any request from t users.
- Influence of codes with high availability on the McEliece Cryptosystem.



CLEMSON UNIVERSITY

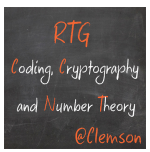
Conclusions and projects

- Batch codes can be considered as a generalization of codes with locality and availability.
- Hamming codes are optimal batch codes for 2-strings download.
- First order Reed-Müller codes are optimal batch codes for 4-strings download.

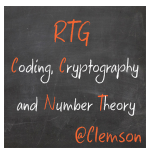
Projects

- Find constructions of batch codes for any request from t users.
- Influence of codes with high availability on the McEliece Cryptosystem.

Thank you.



CLEMSON UNIVERSITY



CLEMSON UNIVERSITY

Muller vs. Müller

Portrait of David E. Muller, professor of mathematics and computer science at the University of Illinois from 1953-92.

Muller vs. Müller

Portrait of David E. Muller, professor of mathematics and computer science at the University of Illinois from 1953-92.