CSS-T Codes from Reed-Muller Codes for Quantum Fault-Tolerance

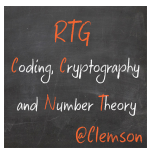
Felice Manganiello

Coding theory and cryptography

July 14, 2022

Joint work with Jessalyn Bolkema.

Supported by the NF DMS grant 1547399



CLEMSON UNIVERSITY

1. Quantum Computing and Quantum Correction
2. Asymptotic properties of Reed-Muller codes
3. Reed-Muller codes as CSS-T codes

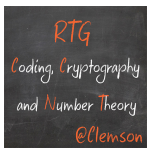
CSS codes

Definition ("CSS codes")

Given C_1 is a binary $[n, k_1, d_1]$ code and C_2 is a binary $[n, k_2, d_2]$ code, then $CSS(C_1, C_2)$ is a $[\![n, k_1 - k_2, \geq \min\{d_1, d_2^{\perp}\}]\!]$ quantum error correcting code.

CSS codes:

- are stabilizer codes generally not optimal;
- correct X and Z errors and their combinations;
- are not fault-tolerance "friendly" because, when considering the universal gates $\{H, S, CX, T\}$, they don't always support the T gate.



CLEMSON UNIVERSITY

CSS-T codes [Rengaswamy et al., 2020]

Definition

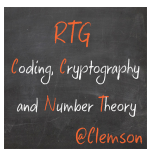
Given C_1 is $[n, k_1, d_1]$ and C_2 is $[n, k_2, d_2]$, the stabilizer code $CSS(C_1, C_2)$ is a CSS-T code if for every $x \in C_2$, $C_1^{\perp}|_x$ contains a self-dual code.

CSS-T codes [Rengaswamy et al., 2020]

Definition

Given C_1 is $[n, k_1, d_1]$ and C_2 is $[n, k_2, d_2]$, the stabilizer code $CSS(C_1, C_2)$ is a CSS-T code if for every $x \in C_2$, $C_1^{\perp}|_x$ contains a self-dual code.

Open Problem: A $[\![n, k_1 - k_2, \min(d_1, d_2^{\perp})]\!]$ family of CSS-T codes such that $\frac{(k_1 - k_2)}{n} = \Omega(1)$ and (ideally) $\frac{\min(d_1, d_2^{\perp})}{n} = \Omega(1)$, where $d_2^{\perp}$ is the minimum distance of $C_2^{\perp}$.



CLEMSON UNIVERSITY

Reed-Muller Codes

Definition

Let $\mathbb{F}_2[x_1, \ldots, x_m]$, $\mathbb{F}_2^m = \{P_1, \ldots, P_{2^m}\}$. The RM$(r, m)$ is defined as:

$$\mathrm{RM}(r, m) = \{(f(P_1), \ldots, f(P_{2^m})) \mid f \in \mathbb{F}_2[x_1, \ldots, x_m]^r\},$$

where $\mathbb{F}_2[x_1, \ldots, x_m]^r$ is the set of polynomials of total degree at most r.

- A RM(r, m) code is a $[2^m, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r}]$ linear code.
- For $0 \leq r_2 \leq r_1 \leq m$, we have $\mathrm{RM}(r_2, m) \subseteq \mathrm{RM}(r_1, m)$.
- $\mathrm{RM}(r, m)^{\perp} = \mathrm{RM}(m - r - 1, m)$

RM codes and non-vanishing distance

Proposition

Let $C(s) = RM(r(s), m(s))$ *for* $s \in \mathbb{N}$ *with* $\lim_{s\to\infty} m(s) = \infty$. *The sequence of codes* $(C(s))_{s\in\mathbb{N}}$ *has non-vanishing relative distance if and only if* $\lim_{s\to\infty} r(s) = c$.

Corollary

Let $C_1(s) = RM(r_1(s), m(s))$ *and* $C_2(s) = RM(r_2(s), m(s))$ *for* $s \in \mathbb{N}$ *with* $\lim_{s\to\infty} m(s) = \infty$. *The sequence of CSS codes*

$$(CSS(C_1(s), C_2(s)))_{s\in\mathbb{N}}$$

has always vanishing relative distance.

RTG Coding, Cryptography and Number Theory @Clemson

CLEMSON UNIVERSITY

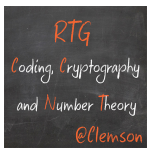
RM codes with non-vanishing rate [Kudekar et al., 2017]

Proposition

Let $C(s) = RM(r(s), m(s))$ *for* $s \in \mathbb{N}$ *such that* $\lim_{s\to\infty} m(s) = \infty$. *Let* $R(C(s))$ *be the rate of code* $C(s)$, *then the asymptotic rate of the sequence* $(C(s))_{s\in\mathbb{N}}$ *is*

$$\lim_{s\to\infty} R(C(s)) = \Phi\left(\lim_{s\to\infty}\left(\frac{2r(s) - m(s)}{\sqrt{m(s)}}\right)\right)$$

where Φ *is the standard normal Gaussian CDF.*



CLEMSON UNIVERSITY

RM codes with non-vanishing rate - cont'd

Corollary

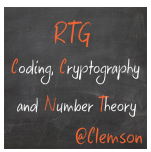
Let $C(m) = RM(\lfloor \frac{m-1}{2} \rfloor + t(m), m)$ *for* $m \in \mathbb{N}$ *with* $t(m)$ *positive. Then the sequence* $(C(m))_{m\in\mathbb{N}}$ *has nonvanishing rate if and only if*

$$\lim_{m\to\infty} \frac{t(m)}{\sqrt{m}} \neq -\infty$$

$$\lim_{m\to\infty} R(C(m)) = \begin{cases} 0 & \lim_{m\to\infty} \frac{t(m)}{\sqrt{m}} = -\infty \\ \frac{1}{2} & \lim_{m\to\infty} \frac{t(m)}{\sqrt{m}} = 0 \\ 1 & \lim_{m\to\infty} \frac{t(m)}{\sqrt{m}} = \infty \end{cases}$$

and

$$\lim_{m\to\infty} R(C(m)) \in \begin{cases} (0, \frac{1}{2}) & \lim_{m\to\infty} \frac{t(m)}{\sqrt{m}} \in (-\infty, 0) \\ (\frac{1}{2}, 1) & \lim_{m\to\infty} \frac{t(m)}{\sqrt{m}} \in (0, \infty) \end{cases}$$



CLEMSON UNIVERSITY

CSS-T codes

Definition (CSS-T)

Let C_1 and C_2 be a $[n, k_1, d_1]$ and a $[n, k_2, d_2]$ binary linear codes respectively. Then $CSS(C_1, C_2)$ is a $[\![n, k_1 - k_2, \geq \min\{d_1, d_2^{\perp}\}]\!]$ quantum stabilizer code. The code $CSS(C_1, C_2)$ is a CSS-T code if for every $x \in C_2$, $C_1^{\perp}|_x$ contains a self-dual code.

Restriction of a code

Definition

We say a codeword, $c \in C$, is supported by some vector $x \in \mathbb{F}_2^n$ if $c \times x = c$, where $\times$ is element-wise multiplication.

Example

$x = (1,1,1,0,0,0)$, $c_1 = (1,1,0,0,0,0)$, $c_2 = (0,0,1,1,0,0)$.
$c_1 \times x = (1,1,0,0,0,0) = c_1$, so c_1 is supported on x.
$c_2 \times x = (0,0,1,0,0,0) \neq c_2$, so c_2 is not supported on x.

Restriction of a code - cont'd

Definition

For some $[n, k]$ binary linear code C and $x \in \mathbb{F}_2^n$, the **restriction of C to (the support of) x**, $C|_x$, is the code created by removing from C all codewords not supported on x followed by removing the entris with coord. where x has zeros.

Example

If $x = (1, 1, 1, 0, 1, 0) \in C_2 \subseteq \mathbb{F}_2^6$ and $C_1^\perp$ has generator matrix

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

Restriction of a code - cont'd

Definition

For some $[n, k]$ binary linear code C and $x \in \mathbb{F}_2^n$, the **restriction of C to (the support of) x**, $C|_x$, is the code created by removing from C all codewords not supported on x followed by removing the entris with coord. where x has zeros.

Example

If $x = (1, 1, 1, 0, 1, 0) \in C_2 \subseteq \mathbb{F}_2^6$ and $C_1^\perp$ has generator matrix

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

$$(0,0,0,0,0,0), (1,1,0,0,0,0), (1,1,1,0,1,0), (0,0,1,0,1,0)$$

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

Notes on duality

- C is self-dual if $C^{\perp} = C \Rightarrow n$ is even and $\dim C = \frac{n}{2}$
- C is self-orthogonal if $C \subseteq C^{\perp}$

Remark

The maximum rate of a CSS-T code defined by RM codes is $\frac{1}{2}$.

Notes on duality

- C is self-dual if $C^{\perp} = C \Rightarrow n$ is even and $\dim C = \frac{n}{2}$
- C is self-orthogonal if $C \subseteq C^{\perp}$

Remark

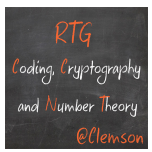
The maximum rate of a CSS-T code defined by RM codes is $\frac{1}{2}$.

Let $C(m) = RM(\lfloor \frac{m}{2} \rfloor + t(m), m)$ with $m \in \mathbb{N}$

$$\lim_{m\to\infty} R(C(m)) = \begin{cases} 0 & \lim_{m\to\infty} \frac{t(m)}{\sqrt{m}} = -\infty \\ \frac{1}{2} & \lim_{m\to\infty} \frac{t(m)}{\sqrt{m}} = 0 \\ 1 & \lim_{m\to\infty} \frac{t(m)}{\sqrt{m}} = \infty \end{cases}$$

and

$$\lim_{m\to\infty} R(C(m)) \in \begin{cases} (0, \frac{1}{2}) & \lim_{m\to\infty} \frac{t(m)}{\sqrt{m}} \in (-\infty, 0) \\ (\frac{1}{2}, 1) & \lim_{m\to\infty} \frac{t(m)}{\sqrt{m}} \in (0, \infty) \end{cases}$$



CLEMSON UNIVERSITY

Notes on duality - again

Proposition

An $[n, k]$ binary linear code C contains a self-dual code if and only if n is even and $C^{\perp}$ is self-orthogonal, meaning that $C^{\perp} \subseteq C$.

Notes on duality - again

Proposition

An $[n, k]$ binary linear code C contains a self-dual code if and only if n is even and $C^{\perp}$ is self-orthogonal, meaning that $C^{\perp} \subseteq C$.

Definition (CSS-T)

$\cdots$ The code $CSS(C_1, C_2)$ is a CSS-T code if for every $x \in C_2$, $C_1^{\perp}|_x$ contains a self-dual code.

Notes on duality - again

Proposition

An $[n, k]$ binary linear code C contains a self-dual code if and only if n is even and $C^{\perp}$ is self-orthogonal, meaning that $C^{\perp} \subseteq C$.

Definition (CSS-T)

$\cdots$ The code $CSS(C_1, C_2)$ is a CSS-T code if for every $x \in C_2$, $(C_1^{\perp}|_x)^{\perp} \subseteq C_1^{\perp}|_x$.

Notes on shortening and puncturing

Let $C \subseteq \mathbb{F}_2^n$ be a code and $I \subseteq \{1, \dots, n\}$

- $\text{short}(C, I) = C|_x$ where $\text{supp}(x) = \{1, \dots, n\} \setminus I$.
- $\text{punct}(C, I)$: remove from any $x \in C$ the coordinates in I.

Notes on shortening and puncturing

Let $C \subseteq \mathbb{F}_2^n$ be a code and $I \subseteq \{1, \dots, n\}$

- $\text{short}(C, I) = C|_x$ where $\text{supp}(x) = \{1, \dots, n\} \setminus I$.
- $\text{punct}(C, I)$: remove from any $x \in C$ the coordinates in I.

Theorem

Let C be a $[n, k]$ binary linear code and $I \subseteq \{1, \dots, n\}$, then

$$\text{short}(C, I)^\perp = \text{punct}(C^\perp, I)$$

Notes on shortening and puncturing

Let $C \subseteq \mathbb{F}_2^n$ be a code and $I \subseteq \{1, \dots, n\}$

- $\text{short}(C, I) = C|_x$ where $\text{supp}(x) = \{1, \dots, n\} \setminus I$.
- $\text{punct}(C, I)$: remove from any $x \in C$ the coordinates in I.

Theorem

Let C be a $[n, k]$ binary linear code and $I \subseteq \{1, \dots, n\}$, then

$$\text{short}(C, I)^\perp = \text{punct}(C^\perp, I)$$

Definition (CSS-T)

$\cdots$ The code $CSS(C_1, C_2)$ is a CSS-T code if for every $x \in C_2$, $(C_1^\perp|_x)^\perp \subseteq C_1^\perp|_x$

Notes on shortening and puncturing

Let $C \subseteq \mathbb{F}_2^n$ be a code and $I \subseteq \{1, \dots, n\}$

- $\text{short}(C, I) = C|_x$ where $\text{supp}(x) = \{1, \dots, n\} \setminus I$.
- $\text{punct}(C, I)$: remove from any $x \in C$ the coordinates in I.

Theorem

Let C be a $[n, k]$ binary linear code and $I \subseteq \{1, \dots, n\}$, then

$$\text{short}(C, I)^\perp = \text{punct}(C^\perp, I)$$

Definition (CSS-T)

$\cdots$ The code $CSS(C_1, C_2)$ is a CSS-T code if for every $x \in C_2$, $(C_1^\perp|_x)^\perp = \text{short}(C_1^\perp, [n] \setminus x)^\perp$

Notes on shortening and puncturing

Let $C \subseteq \mathbb{F}_2^n$ be a code and $I \subseteq \{1, \dots, n\}$

- $\text{short}(C, I) = C|_x$ where $\text{supp}(x) = \{1, \dots, n\} \setminus I$.
- $\text{punct}(C, I)$: remove from any $x \in C$ the coordinates in I.

Theorem

Let C be a $[n, k]$ binary linear code and $I \subseteq \{1, \dots, n\}$, then

$$\text{short}(C, I)^\perp = \text{punct}(C^\perp, I)$$

Definition (CSS-T)

$\cdots$ The code $CSS(C_1, C_2)$ is a CSS-T code if for every $x \in C_2$, $(C_1^\perp|_x)^\perp = \text{short}(C_1^\perp, [n] \setminus x)^\perp$

$$\text{punct}(C_1, [n] \setminus x) \subseteq \text{short}(C_1^\perp, [n] \setminus x)$$

CSS-T with RM codes

Theorem

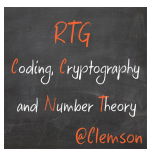
Define $C_1 = RM(\lfloor \frac{m-1}{2} \rfloor - t, m)$ *and* $C_2 = RM(r_2, m)$. *If*

- $r_2 \leq 2t + 1$ *for* m *even, or*
- $r_2 \leq 2t$ *for* m *odd*

then $CSS(C_1, C_2)$ *is a CSS-T code.*

$x = \mathrm{ev}_{\mathbb{F}_2^m}(p) \in C_1$ and $y = \mathrm{ev}_{\mathbb{F}_2^m}(q) \in C_2$

$$\begin{aligned}\mathrm{punct}(y, \mathbb{F}_2^m \setminus \mathrm{supp}(x)) &= \mathrm{punct}(\mathrm{ev}_{\mathbb{F}_2^m}(q), \mathbb{F}_2^m \setminus \mathrm{supp}(x)) \\ &= \mathrm{punct}(\mathrm{ev}_{\mathbb{F}_2^m}((1-p)q) + \mathrm{ev}_{\mathbb{F}_2^m}(pq), \mathbb{F}_2^m \setminus \mathrm{supp}(x)) \\ &= \mathrm{punct}(\mathrm{ev}_{\mathbb{F}_2^m}(pq), \mathbb{F}_2^m \setminus \mathrm{supp}(x)) \\ &= \mathrm{short}(\mathrm{ev}_{\mathbb{F}_2^m}(pq), \mathbb{F}_2^m \setminus \mathrm{supp}(x))\end{aligned}$$



CLEMSON UNIVERSITY

Conclusion

- CSS-T codes can be used for quantum fault-tolerance.
- CSS-T from Reed-Muller codes first family of CSS-T codes with non-vanishing asymptotic rate up to $\frac{1}{2}$.
- Missing CSS-T families with higher asymptotic rates and non-vanishing relative distance.

Conclusion

- CSS-T codes can be used for quantum fault-tolerance.
- CSS-T from Reed-Muller codes first family of CSS-T codes with non-vanishing asymptotic rate up to $\frac{1}{2}$.
- Missing CSS-T families with higher asymptotic rates and non-vanishing relative distance.

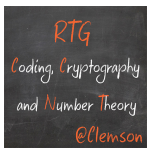
Thank you.

References

Andrade, E., Bolkema, J., Dexter, T., Eggers, H., Manganiello, F., and Luongo, V.
CSS-T codes from Reed-Muller codes for quantum fault-tolerance.
TBD.

Kudekar, S., Kumar, S., Mondelli, M., Pfister, H. D., Şaşoğlu, E., and Urbanke, R. L. (2017).
Reed–muller codes achieve capacity on erasure channels.
IEEE Transactions on Information Theory, 63(7):4298–4316.

Rengaswamy, N., Calderbank, R., Newman, M., and Pfister, H. D. (2020).
Classical coding problem from transversal T gates.
In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 1891–1896.



CLEMSON UNIVERSITY

Single Qubit

The **state** of a qubit can be described as a normalized vector in $\mathbb{C}^2$.

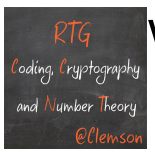
In quantum computing, we define the **standard** or **computational basis** of $\mathbb{C}^2$ to be

$$\left\{ |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$$

General form for the state of a qubit (superposition):

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

with $|\alpha|^2 + |\beta|^2 = 1$.



CLEMSON UNIVERSITY

n Qubits

- n qubits use $\mathbb{C}^{2^n}$, since $\mathbb{C}^{2^n} = \bigotimes_{i=1}^{n} \mathbb{C}^2$.

Example

Consider a state consisting of 2 qubits:

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

The probability mass function of this state is given by

$$p_{|\psi\rangle}(x) = \begin{cases} |\alpha|^2 & \text{if } x = |00\rangle \\ |\beta|^2 & \text{if } x = |01\rangle \\ |\gamma|^2 & \text{if } x = |10\rangle \\ |\delta|^2 & \text{if } x = |11\rangle \end{cases}.$$

Quantum Errors and Quantum Error Correction

Definition ("Errors")

$\boxed{X}$	$\boxed{Z}$
$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Definition ("CSS codes")

Given C_1 is $[n, k_1, d_1]$ and C_2 is $[n, k_2, d_2]$, then $CSS(C_1, C_2)$ is a $[\![n, k_1 - k_2, \geq \min\{d_1, d_2^{\perp}\}]\!]$ quantum stabilizer code.

Operations

Definition

We say a linear operator U is **unitary** if $UU^\dagger = U^\dagger U = I$.

- All operations in quantum computing are unitary.
- The group of unitary operations on 1 qubit under composition is denoted $\mathbb{U}$.
- The group of unitary operations on n qubits, $\mathbb{U}^n$, is the n-fold tensor product of $\mathbb{U}$

Universality

Example

Some popular Clifford gates are

H	S	X	T
$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$	$\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$	$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$	$\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$

The set of gates $\{H, S, CX, T\}$ is universal.