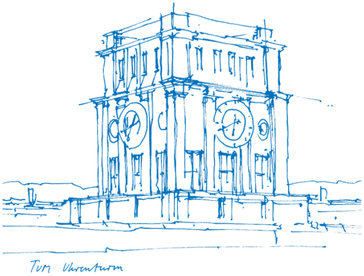
Weighted-Hamming Metric: Codes and Bounds

Sebastian Bitzer
TUM

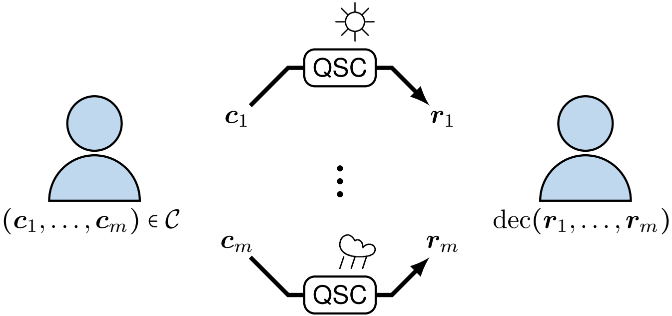
Alberto Ravagnani
TU\e

Violetta Weger
TUM

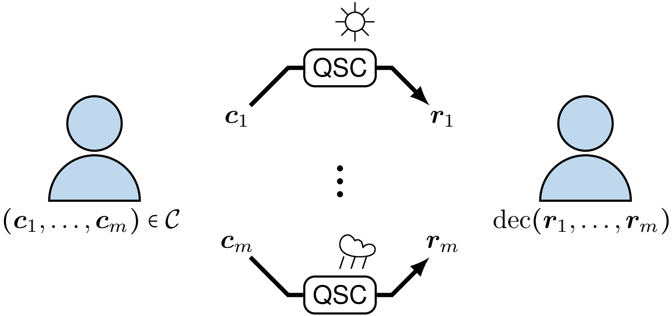
JMM 2025
Seattle



A Tale of Two Channels



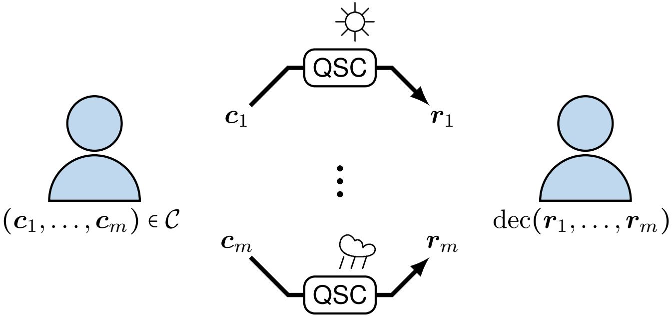
A Tale of Two Channels



Standard solutions:

- Raptor
- Turbo
- LDPC
- Polar
- ...

A Tale of Two Channels



Standard solutions:

- Raptor
- Turbo
- LDPC
- Polar
- ...

Goal of this Work

Analyze codes that uniquely decode *all* errors with $P(e) \geq \theta$

From Probability to Metric

Matching a Channel ♡

A distance matches a channel if

$$d(\boldsymbol{c}, \boldsymbol{r}) \leq d(\boldsymbol{c}', \boldsymbol{r}) \iff P(\boldsymbol{c} \mid \boldsymbol{r}) \geq P(\boldsymbol{c}' \mid \boldsymbol{r})$$

From Probability to Metric

Deza, Deza (2009). Encyclopedia of Distances.

Matching a Channel ♡

A distance matches a channel if

$$d(\boldsymbol{c},\boldsymbol{r}) \leq d(\boldsymbol{c}',\boldsymbol{r}) \iff P(\boldsymbol{c} \mid \boldsymbol{r}) \geq P(\boldsymbol{c}' \mid \boldsymbol{r})$$

Weighted-Hamming Weight

Fix $(\lambda_1,\ldots,\lambda_m) \in \mathbb{N}^m$.

$$\mathsf{wt}(\boldsymbol{c}_1,\ldots,\boldsymbol{c}_m) = \sum_{\ell=1}^{m} \lambda_\ell \cdot \mathsf{wt}_\mathsf{H}(\boldsymbol{c}_\ell)$$

From Probability to Metric

Deza, Deza (2009). Encyclopedia of Distances.

Matching a Channel ♡

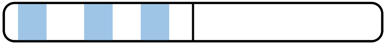
A distance matches a channel if

$$d(\boldsymbol{c}, \boldsymbol{r}) \leq d(\boldsymbol{c}', \boldsymbol{r}) \iff P(\boldsymbol{c} \mid \boldsymbol{r}) \geq P(\boldsymbol{c}' \mid \boldsymbol{r})$$

Weighted-Hamming Weight

Fix $(\lambda_1, \ldots, \lambda_m) \in \mathbb{N}^m$.

$$\mathrm{wt}(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_m) = \sum_{\ell=1}^{m} \lambda_\ell \cdot \mathrm{wt}_\mathrm{H}(\boldsymbol{c}_\ell)$$



$\lambda_1 = 1$ $\lambda_2 = 2$

$\mathrm{wt}_\mathrm{H}(\boldsymbol{c}_1, \boldsymbol{c}_2) = 3$

$\mathrm{wt}(\boldsymbol{c}_1, \boldsymbol{c}_2) = 3$

From Probability to Metric

Deza, Deza (2009). Encyclopedia of Distances.

Matching a Channel ♡

A distance matches a channel if

$$d(\boldsymbol{c}, \boldsymbol{r}) \le d(\boldsymbol{c}', \boldsymbol{r}) \iff P(\boldsymbol{c} \mid \boldsymbol{r}) \ge P(\boldsymbol{c}' \mid \boldsymbol{r})$$

Weighted-Hamming Weight

Fix $(\lambda_1, \ldots, \lambda_m) \in \mathbb{N}^m$.

$$\mathrm{wt}(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_m) = \sum_{\ell=1}^{m} \lambda_\ell \cdot \mathrm{wt}_\mathrm{H}(\boldsymbol{c}_\ell)$$

$\lambda_1 = 1$ $\lambda_2 = 2$

$\mathrm{wt}_\mathrm{H}(\boldsymbol{c}_1, \boldsymbol{c}_2) = 3$

$\mathrm{wt}(\boldsymbol{c}_1, \boldsymbol{c}_2) = 6$

Codes in the Weighted-Hamming Metric

Trivial constructions: → Hamming-metric code
→ Independent codes for subchannels

suboptimal

Codes in the Weighted-Hamming Metric

Trivial constructions: ➔ Hamming-metric code
➔ Independent codes for subchannels

suboptimal

Previous work:

- Bezzateev, Shekhunova (2013). Class of Generalized Goppa Codes Perfect in Weighted Hamming Metric.
- Moon (2018). Weighted Hamming Metric Structures.

} perfect codes for certain parameters

Codes in the Weighted-Hamming Metric

Trivial constructions: → Hamming-metric code
→ Independent codes for subchannels

suboptimal

Previous work:

- Bezzateev, Shekhunova (2013). Class of Generalized Goppa Codes Perfect in Weighted Hamming Metric.
- Moon (2018). Weighted Hamming Metric Structures.

} perfect codes for certain parameters

Open: General bounds and constructions

Error-Correction Capability

- Silva, Kschischang (2009). On Metrics for Error Correction in Network Coding.
- → General framework for adversarial error correction

Error-Correction Capability

Silva, Kschischang (2009). On Metrics for Error Correction in Network Coding.

→ General framework for adversarial error correction

Error-Correction Capability

Let $\tau(\boldsymbol{c}) = \min_{\boldsymbol{r}\in\mathbb{F}_q^n} \max\{\mathsf{wt}(\boldsymbol{r}), \mathsf{wt}(\boldsymbol{c}-\boldsymbol{r})\} - 1$

Linear $\mathcal{C}$ t-error-correcting $\iff t \leq \tau(\mathcal{C}) = \min_{\boldsymbol{c}\in\mathcal{C}\setminus\{0\}} \tau(\boldsymbol{c})$

Error-Correction Capability

Silva, Kschischang (2009). On Metrics for Error Correction in Network Coding.

→ General framework for adversarial error correction

Error-Correction Capability

Let $\tau(\boldsymbol{c}) = \min_{\boldsymbol{r}\in\mathbb{F}_q^n} \max\{\mathsf{wt}(\boldsymbol{r}), \mathsf{wt}(\boldsymbol{c}-\boldsymbol{r})\} - 1$

Linear $\mathcal{C}$ t-error-correcting $\iff t \leq \tau(\mathcal{C}) = \min_{\boldsymbol{c}\in\mathcal{C}\setminus\{0\}} \tau(\boldsymbol{c})$

Minimum Distance

$$\tau(\mathcal{C}) \geq \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor$$

Equality for *normal* metrics

Error-Correction Capability

Silva, Kschischang (2009). On Metrics for Error Correction in Network Coding.

→ General framework for adversarial error correction

Error-Correction Capability

Let $\tau(\boldsymbol{c}) = \min_{\boldsymbol{r} \in \mathbb{F}_q^n} \max\{\mathrm{wt}(\boldsymbol{r}), \mathrm{wt}(\boldsymbol{c} - \boldsymbol{r})\} - 1$

Linear $\mathcal{C}$ t-error-correcting $\iff t \leq \tau(\mathcal{C}) = \min_{\boldsymbol{c} \in \mathcal{C} \setminus \{0\}} \tau(\boldsymbol{c})$

Minimum Distance

$$\tau(\mathcal{C}) \geq \left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor$$

Equality for *normal* metrics

Hamming metric, rank metric, . . . are normal.

Error-Correction Capability

Silva, Kschischang (2009). On Metrics for Error Correction in Network Coding.

→ General framework for adversarial error correction

Error-Correction Capability

Let $\tau(\boldsymbol{c}) = \min_{\boldsymbol{r}\in\mathbb{F}_q^n} \max\{\mathrm{wt}(\boldsymbol{r}), \mathrm{wt}(\boldsymbol{c}-\boldsymbol{r})\} - 1$

Linear $\mathcal{C}$ t-error-correcting $\iff t \leq \tau(\mathcal{C}) = \min_{\boldsymbol{c}\in\mathcal{C}\setminus\{0\}} \tau(\boldsymbol{c})$

Minimum Distance

$$\tau(\mathcal{C}) \geq \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor$$

Equality for *normal* metrics

Hamming metric, rank metric, ... are normal.

What about the weighted-Hamming metric?

Being Normal is Boring!

$$\lambda_1 = 1 \qquad \lambda_2 = 2$$

$$\boldsymbol{c}_0 = (0, 0, 0 \mid 0, 0, 0)$$

$$\boldsymbol{c}_1 = (0, 0, 0 \mid 1, 1, 1)$$

Being Normal is Boring!

$$\lambda_1 = 1 \qquad \lambda_2 = 2$$

$$d = 6 \left(\begin{array}{l} \boldsymbol{c}_0 = (0, 0, 0 \mid 0, 0, 0) \\ \\ \boldsymbol{c}_1 = (0, 0, 0 \mid 1, 1, 1) \end{array} \right.$$

Being Normal is Boring!

$$\lambda_1 = 1 \qquad \lambda_2 = 2$$

$$\boldsymbol{c}_0 = (0, 0, 0 \mid 0, 0, 0)$$

$$d = 6 \qquad \tau = 3$$

$$\boldsymbol{c}_1 = (0, 0, 0 \mid 1, 1, 1)$$

Being Normal is Boring!

$$\lambda_1 = 1 \qquad \lambda_2 = 2$$

$$\boldsymbol{c}_0 = (0, 0, 0 \mid 0, 0, 0)$$

$$d = 6 \qquad \tau = 3$$

$$\boldsymbol{c}_1 = (0, 0, 0 \mid 1, 1, 1)$$

➔ corrects all errors beyond $\left\lfloor \frac{d-1}{2} \right\rfloor$

Being Normal is Boring!

$\lambda_1 = 1 \qquad \lambda_2 = 2$

$$d = 6 \left(\begin{array}{c} \boldsymbol{c}_0 = (0, 0, 0 \mid 0, 0, 0) \\ \\ \boldsymbol{c}_1 = (0, 0, 0 \mid 1, 1, 1) \end{array} \right) \tau = 3$$

➔ corrects all errors beyond $\left\lfloor \frac{d-1}{2} \right\rfloor$

Bound on τ via d

Let $\lambda_1 \leq \ldots \leq \lambda_m$.

$$\left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor \leq \tau(\mathcal{C}) \leq \left\lfloor \frac{d(\mathcal{C}) + \lambda_m}{2} \right\rfloor - 1$$

Being Normal is Boring!

$\lambda_1 = 1 \qquad \lambda_2 = 2$

$$\boldsymbol{c}_0 = (0, 0, 0 \mid 0, 0, 0)$$

$$d = 6 \left(\qquad \right) \tau = 3$$

$$\boldsymbol{c}_1 = (0, 0, 0 \mid 1, 1, 1)$$

→ corrects all errors beyond $\left\lfloor \frac{d-1}{2} \right\rfloor$

Bound on τ via d

Let $\lambda_1 \leq \ldots \leq \lambda_m$.

$$\left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor \leq \tau(\mathcal{C}) \leq \left\lfloor \frac{d(\mathcal{C}) + \lambda_m}{2} \right\rfloor - 1$$

→ Build on known bounds for the Hamming metric

Being Normal is Boring!

$$\lambda_1 = 1 \qquad \lambda_2 = 2$$

$$d = 6 \left(\begin{array}{c} \boldsymbol{c}_0 = (0, 0, 0 \mid 0, 0, 0) \\ \\ \boldsymbol{c}_1 = (0, 0, 0 \mid 1, 1, 1) \end{array} \right) \tau = 3$$

→ corrects all errors beyond $\left\lfloor \frac{d-1}{2} \right\rfloor$

Bound on τ via d

Let $\lambda_1 \leq \ldots \leq \lambda_m$.

$$\left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor \leq \tau(\mathcal{C}) \leq \left\lfloor \frac{d(\mathcal{C}) + \lambda_m}{2} \right\rfloor - 1$$

→ Build on known bounds for the Hamming metric

Hamming Singleton Plotkin Linear Programming Gilbert-Varshamov

Being Normal is Boring!

$\lambda_1 = 1 \qquad \lambda_2 = 2$

$\boldsymbol{c}_0 = (0, 0, 0 \mid 0, 0, 0)$

$d = 6 \qquad \tau = 3$

$\boldsymbol{c}_1 = (0, 0, 0 \mid 1, 1, 1)$

→ corrects all errors beyond $\left\lfloor \frac{d-1}{2} \right\rfloor$

Bound on τ via d

Let $\lambda_1 \leq \ldots \leq \lambda_m$.

$$\left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor \leq \tau(\mathcal{C}) \leq \left\lfloor \frac{d(\mathcal{C}) + \lambda_m}{2} \right\rfloor - 1$$

→ Build on known bounds for the Hamming metric

Hamming Singleton Plotkin Linear Programming Gilbert-Varshamov

Singleton-Like Bound on d

Singleton-like Bound

Let $\lambda_1 \leq \ldots \leq \lambda_m$, $\dim(\mathcal{C}) = k$.

$$d \leq d_{\mathrm{SB}} = \sum_{\ell=1}^{\ell'} n_\ell \lambda_\ell + \left(\sum_{\ell=\ell'+1}^{m} n_\ell - k + 1 \right) \cdot \lambda_{\ell'+1},$$

where ℓ' maximal s.t. $\sum_{\ell=1}^{\ell'} n_\ell \leq n - k + 1$.

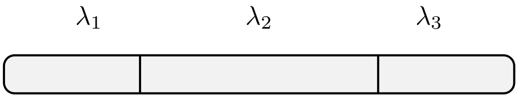
Singleton-Like Bound on d

Singleton-like Bound

Let $\lambda_1 \leq \ldots \leq \lambda_m$, $\dim(\mathcal{C}) = k$.

$$d \leq d_{\mathrm{SB}} = \sum_{\ell=1}^{\ell'} n_\ell \lambda_\ell + \left(\sum_{\ell=\ell'+1}^{m} n_\ell - k + 1 \right) \cdot \lambda_{\ell'+1},$$

where ℓ' maximal s.t. $\sum_{\ell=1}^{\ell'} n_\ell \leq n - k + 1$.



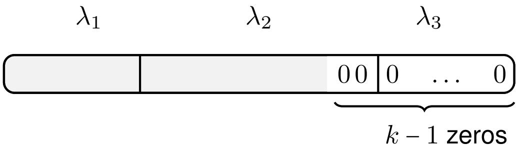
Singleton-Like Bound on d

Singleton-like Bound

Let $\lambda_1 \leq \ldots \leq \lambda_m$, $\dim(\mathcal{C}) = k$.

$$d \leq d_{\mathrm{SB}} = \sum_{\ell=1}^{\ell'} n_\ell \lambda_\ell + \left(\sum_{\ell=\ell'+1}^{m} n_\ell - k + 1 \right) \cdot \lambda_{\ell'+1},$$

where ℓ' maximal s.t. $\sum_{\ell=1}^{\ell'} n_\ell \leq n - k + 1$.



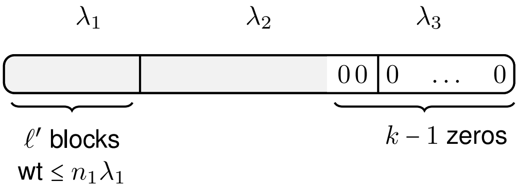
Singleton-Like Bound on d

Singleton-like Bound

Let $\lambda_1 \leq \ldots \leq \lambda_m$, $\dim(\mathcal{C}) = k$.

$$d \leq d_{\mathrm{SB}} = \sum_{\ell=1}^{\ell'} n_\ell \lambda_\ell + \left(\sum_{\ell=\ell'+1}^{m} n_\ell - k + 1 \right) \cdot \lambda_{\ell'+1},$$

where ℓ' maximal s.t. $\sum_{\ell=1}^{\ell'} n_\ell \leq n - k + 1$.



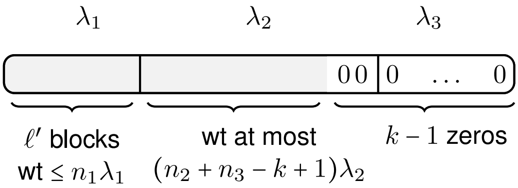
Singleton-Like Bound on d

Singleton-like Bound

Let $\lambda_1 \leq \ldots \leq \lambda_m$, $\dim(\mathcal{C}) = k$.

$$d \leq d_{\mathrm{SB}} = \sum_{\ell=1}^{\ell'} n_\ell \lambda_\ell + \left(\sum_{\ell=\ell'+1}^{m} n_\ell - k + 1 \right) \cdot \lambda_{\ell'+1},$$

where ℓ' maximal s.t. $\sum_{\ell=1}^{\ell'} n_\ell \leq n - k + 1$.



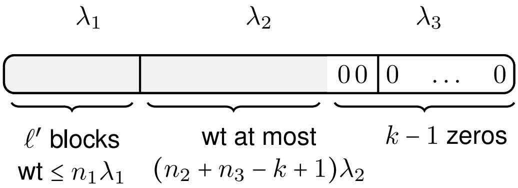
Singleton-Like Bound on d

Singleton-like Bound

Let $\lambda_1 \leq \ldots \leq \lambda_m$, $\dim(\mathcal{C}) = k$.

$$d \leq d_{\mathrm{SB}} = \sum_{\ell=1}^{\ell'} n_\ell \lambda_\ell + \left(\sum_{\ell=\ell'+1}^{m} n_\ell - k + 1 \right) \cdot \lambda_{\ell'+1},$$

where ℓ' maximal s.t. $\sum_{\ell=1}^{\ell'} n_\ell \leq n - k + 1$.



Observation: → MDS codes optimal
→ But smaller field size possible

Singleton-Like Bound on τ

Denote $d_{\mathrm{SB}} = \sum_{\ell=1}^{\ell'} n_\ell \lambda_\ell + (\sum_{\ell=\ell'+1}^{m} n_\ell - k + 1) \cdot \lambda_{\ell'+1}$, where ℓ' maximal s.t. $\sum_{\ell=1}^{\ell'} n_\ell \leq n - k + 1$

Singleton-like Bound on τ

Let $\lambda_1 \leq \ldots \leq \lambda_m$.

$$\tau(\mathcal{C}) \leq \left\lfloor \frac{d_{\mathrm{SB}} + \lambda_m}{2} \right\rfloor - 1$$

Singleton-Like Bound on τ

Denote $d_{\mathrm{SB}} = \sum_{\ell=1}^{\ell'} n_\ell \lambda_\ell + (\sum_{\ell=\ell'+1}^{m} n_\ell - k + 1) \cdot \lambda_{\ell'+1}$, where ℓ' maximal s.t. $\sum_{\ell=1}^{\ell'} n_\ell \leq n - k + 1$

Singleton-like Bound on τ

Let $\lambda_1 \leq \ldots \leq \lambda_m$.

$$\tau(\mathcal{C}) \leq \left\lfloor \frac{d_{\mathrm{SB}} + \lambda_m}{2} \right\rfloor - 1$$

Can be tightened to

$$\tau(\mathcal{C}) \leq \left\lfloor \frac{d_{\mathrm{SB}} + \lambda_j}{2} \right\rfloor - 1$$

with $j = \ell'$ or $j = \ell' + 1$.

Singleton-Like Bound on τ

Denote $d_{\mathrm{SB}} = \sum_{\ell=1}^{\ell'} n_\ell \lambda_\ell + \left(\sum_{\ell=\ell'+1}^{m} n_\ell - k + 1\right) \cdot \lambda_{\ell'+1}$, where ℓ' maximal s.t. $\sum_{\ell=1}^{\ell'} n_\ell \leq n - k + 1$

Singleton-like Bound on τ

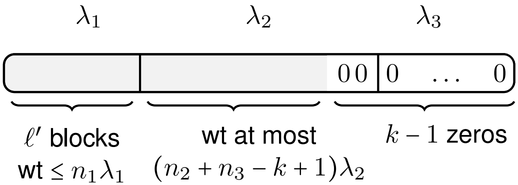
Let $\lambda_1 \leq \ldots \leq \lambda_m$.

$$\tau(\mathcal{C}) \leq \left\lfloor \frac{d_{\mathrm{SB}} + \lambda_m}{2} \right\rfloor - 1$$

Can be tightened to

$$\tau(\mathcal{C}) \leq \left\lfloor \frac{d_{\mathrm{SB}} + \lambda_j}{2} \right\rfloor - 1$$

with $j = \ell'$ or $j = \ell' + 1$.



Singleton-Like Bound on τ

Denote $d_{\text{SB}} = \sum_{\ell=1}^{\ell'} n_\ell \lambda_\ell + (\sum_{\ell=\ell'+1}^{m} n_\ell - k + 1) \cdot \lambda_{\ell'+1}$, where ℓ' maximal s.t. $\sum_{\ell=1}^{\ell'} n_\ell \leq n - k + 1$

Singleton-like Bound on τ

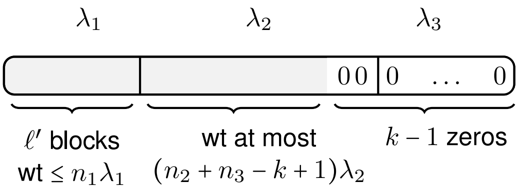
Let $\lambda_1 \leq \ldots \leq \lambda_m$.

$$\tau(\mathcal{C}) \leq \left\lfloor \frac{d_{\text{SB}} + \lambda_m}{2} \right\rfloor - 1$$

Can be tightened to

$$\tau(\mathcal{C}) \leq \left\lfloor \frac{d_{\text{SB}} + \lambda_j}{2} \right\rfloor - 1$$

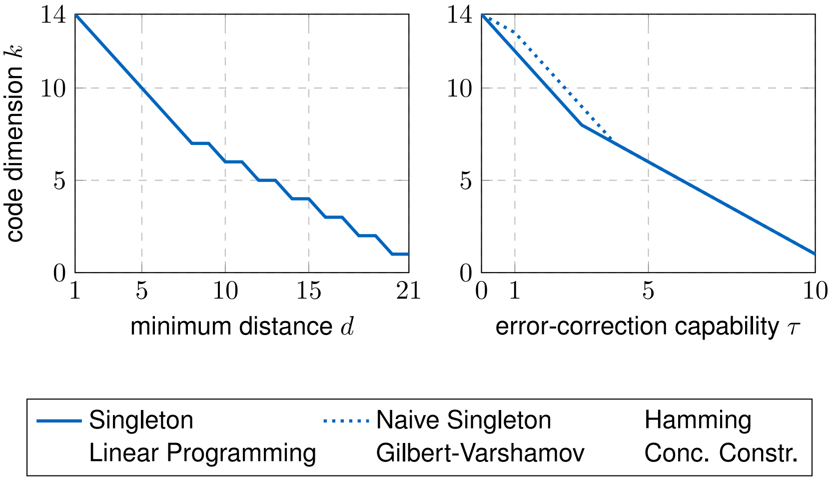
with $j = \ell'$ or $j = \ell' + 1$.



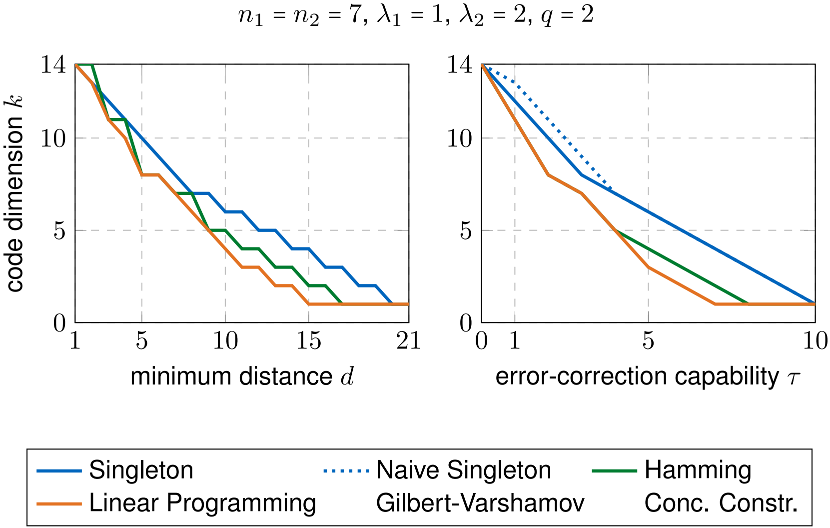
Bounding τ directly gives a tighter bound ☺

Some Curves

$n_1 = n_2 = 7$, $\lambda_1 = 1$, $\lambda_2 = 2$



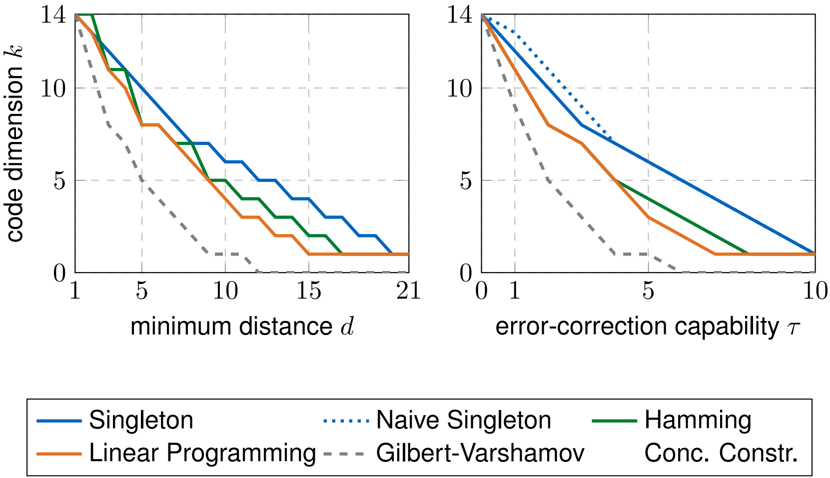
Some Curves



$n_1 = n_2 = 7,\ \lambda_1 = 1,\ \lambda_2 = 2,\ q = 2$
code dimension k
14
10
5
0
1
5
10
15
21
minimum distance d
0
1
5
10
error-correction capability τ
Singleton
Naive Singleton
Hamming
Linear Programming
Gilbert-Varshamov
Conc. Constr.

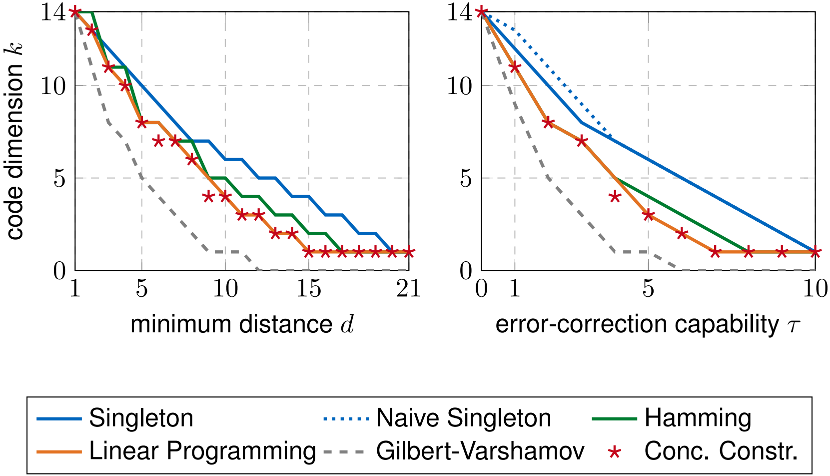
Some Curves

$n_1 = n_2 = 7,\ \lambda_1 = 1,\ \lambda_2 = 2,\ q = 2$

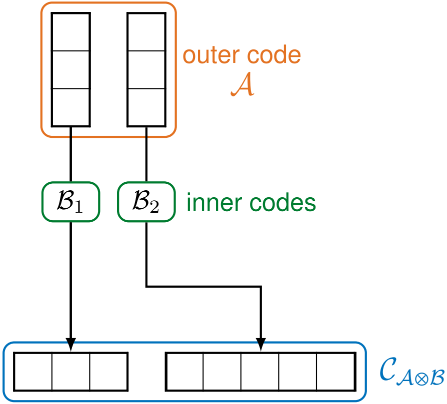


Some Curves

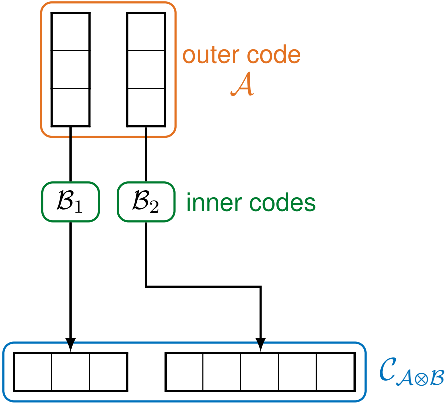
$n_1 = n_2 = 7, \lambda_1 = 1, \lambda_2 = 2, q = 2$



A Concatenated Construction



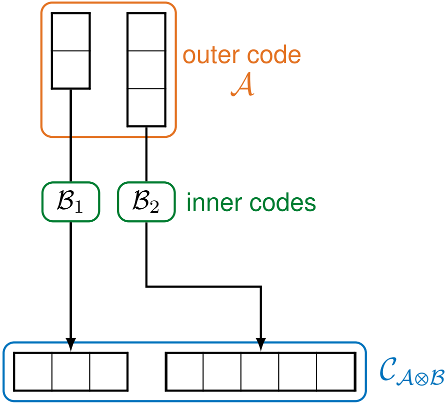
A Concatenated Construction



Error Correction

- Bound on d
- Bound on τ
- Efficient decoding

A Concatenated Construction



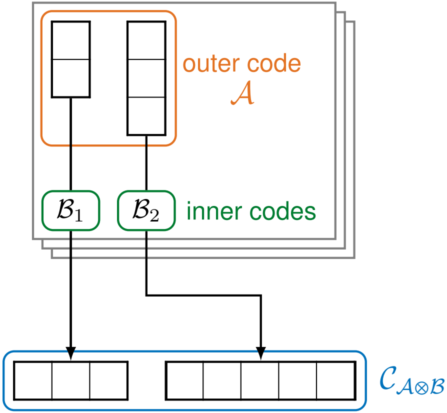
Error Correction

- Bound on d
- Bound on τ
- Efficient decoding

Increase flexibility:

→ Polyaphabetic outer code

A Concatenated Construction



Error Correction

- Bound on d
- Bound on τ
- Efficient decoding

Increase flexibility:

→ Polyaphabetic outer code

→ Multilevel concatentation

Conclusion

arXiv

Weighted-Hamming metric suitable for parallel channels:

- ☺ Error-correction capability can exceed $\left\lfloor \frac{d-1}{2} \right\rfloor$
- ☺ Bounds on d and τ
- ☺ Concatenated code construction

Conclusion

arXiv

Weighted-Hamming metric suitable for parallel channels:

- Error-correction capability can exceed $\left\lfloor \frac{d-1}{2} \right\rfloor$
- Bounds on d and τ
- Concatenated code construction

Future work:

- Calculate or bound $\left|\{\boldsymbol{x} \in \mathbb{F}_q^n \mid \tau(\boldsymbol{x}) \leq t\}\right|$
- More code constructions?

Conclusion

Weighted-Hamming metric suitable for parallel channels:

- ☺ Error-correction capability can exceed $\left\lfloor \frac{d-1}{2} \right\rfloor$
- ☺ Bounds on d and τ
- ☺ Concatenated code construction

Future work:

- ? Calculate or bound $\left|\{\boldsymbol{x} \in \mathbb{F}_q^n \mid \tau(\boldsymbol{x}) \leq t\}\right|$
- ? More code constructions?

arXiv

Thank you!

Questions?