Multilayer crisscross error and erasure correction

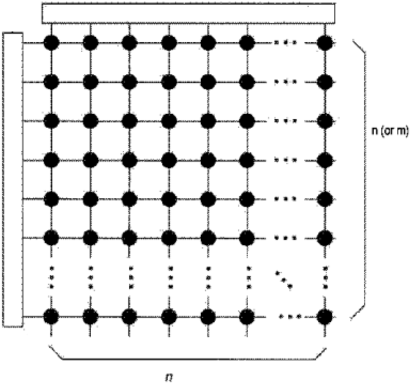
Umberto Martínez-Peñas
University of Valladolid (UVa)

25th MTNS, Network Coding Session,

Universität Bayreuth 2022

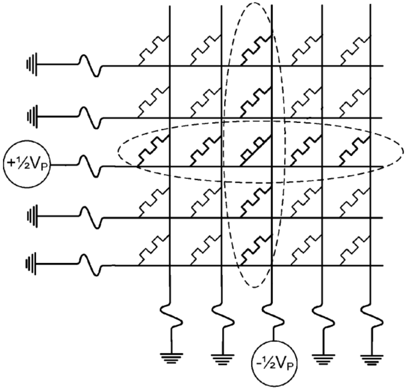
Crisscross Erasure Correction

- Solid state storage devices store data in an $(m \times n)$ matrix of bits.
- Typically, there are multiple devices connected column-wise or row-wise by wires.
- A write or read voltage is applied to a given device through the corresponding column and row wires.



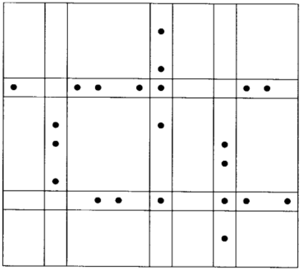
Crisscross Erasure Correction

- A defective device has an even lower resistance than the "on" (or low resistance) state used for storing data.
- As devices in the same row and column are directly connected, a defective device may induce read and write errors in the same row and column.



Crisscross Erasure Correction

- Roth in 1991 showed that the right metric to measure the number of errors/erasures in this case is the cover metric.
- For $C \in \mathbb{F}_q^{m \times n}$, we say $(X, Y) \in [m] \times [n]$ is a cover of C if $C_{i,j} \neq 0$ implies $i \in X$ or $j \in Y$.
- The cover weight $\mathrm{wt}_C(C)$ is the minimum size $|(X, Y)| = |X| + |Y|$ of its covers.
- The cover distance is defined as $\mathrm{d}_C(C, D) = \mathrm{wt}_C(C - D)$, for $C, D \in \mathbb{F}_q^{m \times n}$.



The Multi-Cover Metric

- In this work, we extend the cover metric to the multi-cover metric.
- A multi-cover of $C = (C_1, C_2, \dots, C_\ell) \in \prod_{i=1}^{\ell} \mathbb{F}_q^{m_i \times n_i}$ is $X = (X_i, Y_i)_{i=1}^{\ell} \in \prod_{i=1}^{\ell} [m_i] \times [n_i]$ such that

$$C_{i,a,b} \neq 0 \quad \Longrightarrow a \in X_i \text{ or } b \in Y_i, \quad \forall i \in [\ell].$$

- The multi-cover weight $\mathrm{wt}_{MC}(C)$ is the minimum size

$$|X| = \sum_{i=1}^{\ell} (|X_i| + |Y_i|)$$

  of a multi-cover of C.
- The multi-cover distance between $C, D \in \prod_{i=1}^{\ell} \mathbb{F}_q^{m_i \times n_i}$ is simply defined as

$$\mathrm{d}_{MC}(C, D) = \mathrm{wt}_{MC}(C - D).$$

The Multi-Cover Metric

Example: An encoded tuple

$$C = (C_1, C_2) \in \mathbb{F}_2^{4\times 4} \times \mathbb{F}_2^{4\times 4}$$

with exactly 4 multilayer crisscross errors is of the form

$$Y = C + E \in \mathbb{F}_2^{4\times 4} \times \mathbb{F}_2^{4\times 4},$$

where $\mathrm{wt}_{MC}(E) = 4$.

$$\begin{array}{|c|c|c|c|} \hline 1 & 0 & 0 & 1 \\ \hline 0 & 1 & 0 & 1 \\ \hline 1 & 1 & 1 & 0 \\ \hline 1 & 0 & 0 & 1 \\ \hline \end{array} \quad \begin{array}{|c|c|c|c|} \hline 1 & 1 & 1 & 0 \\ \hline 1 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & 1 \\ \hline 0 & 1 & 1 & 0 \\ \hline \end{array} \quad \mapsto \quad \begin{array}{|c|c|c|c|} \hline 1 & 0 & 0 & 1 \\ \hline 1 & 0 & 1 & 0 \\ \hline 1 & 1 & 1 & 0 \\ \hline 0 & 1 & 1 & 1 \\ \hline \end{array} \quad \begin{array}{|c|c|c|c|} \hline 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 \\ \hline 0 & 1 & 1 & 1 \\ \hline 0 & 1 & 0 & 0 \\ \hline \end{array}$$

Crisscross Erasure Correction

- Correction characterization: $\mathcal{C} \subseteq \prod_{i=1}^{\ell} \mathbb{F}_q^{m_i \times n_i}$ can correct t errors and ρ erasures if, and only if,

$$2t + \rho < \mathrm{d}_{MC}(\mathcal{C}).$$

- Bounds by other metrics:

$$\mathrm{wt}_{SR}(C) \leq \mathrm{wt}_{MC}(C) \leq \mathrm{wt}_{H}(C),$$

where $\mathrm{wt}_{SR}(C) = \sum_{i=1}^{\ell} \mathrm{rk}(C_i)$ and $C = (C_1, \ldots, C_\ell) \in \prod_{i=1}^{\ell} \mathbb{F}_q^{m_i \times n_i}$.

- Bounds for the multi-cover metric: Every upper bound valid for the Hamming metric is also valid for the multi-cover metric.
- Singleton bound: Set $m = m_1 = \ldots = m_\ell$ and $n = n_1 + \cdots + n_\ell$. Given $\mathcal{C} \subseteq \prod_{i=1}^{\ell} \mathbb{F}_q^{m \times n_i}$, we have

$$|\mathcal{C}| \leq q^{m(n - \mathrm{d}_{MC}(\mathcal{C}) + 1)}.$$

MMCD Codes

- MMCD codes: $\mathcal{C} \subseteq \prod_{i=1}^{\ell} \mathbb{F}_q^{m_i \times n_i}$ is a maximum multi-cover distance (MMCD) code if it attains the Singleton bound.
- If there is an MMCD code $\mathcal{C} \subseteq (\mathbb{F}_q^{m \times n})^{\ell}$, and δ is the remainder of $d-3$ divided by n,

$$\ell \leq \left\lfloor \frac{q^{2m} - 1 - m(q^{n-\delta} - 1) - (n-\delta)(q^m - 1) + m(n-\delta)(q-1)}{m(q^n - 1) + n(q^m - 1) - mn(q-1)} \right\rfloor + \left\lfloor \frac{d-3}{n} \right\rfloor + 1. \tag{1}$$

- Set $m = n$. If $q \geq 4$ and $n \geq 2$, or if $q = 3$ and $n \geq 3$, or if $q = 2$ and $n \geq 4$, then the upper bound (1) is tighter than

$$\ell \leq \left\lfloor \frac{2q^n}{3n} \right\rfloor + \left\lfloor \frac{d-3}{n} \right\rfloor + 1. \tag{2}$$

Duality

- Consider the product

$$\langle C, D\rangle = \sum_{i=1}^{\ell} \mathrm{Tr}(C_i D_i),$$

where $C = (C_1, \ldots, C_\ell), D = (D_1, \ldots, D_\ell) \in \prod_{i=1}^{\ell} \mathbb{F}_q^{m_i \times n_i}$, and where $\mathrm{Tr}(\cdot)$ denotes the matrix trace.

- The dual of $\mathcal{C} \subseteq \prod_{i=1}^{\ell} \mathbb{F}_q^{m_i \times n_i}$ is defined as

$$\mathcal{C}^\perp = \left\{ D \in \prod_{i=1} \mathbb{F}_q^{m_i \times n_i} \middle| \langle C, D\rangle = 0, \text{ for all } C \in \mathcal{C} \right\}.$$

Duality

- Consider $\mathcal{C} \subseteq \mathbb{F}_2^{3\times 3}$ generated by

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

- $\mathcal{C}$ is MDS by columns and rows since $|\mathcal{C}| = 8$ ($\dim(\mathcal{C}) = 3$) and $\mathrm{d}_H^R(\mathcal{C}) = \mathrm{d}_H^C(\mathcal{C}) = 3$.
- $\mathcal{C}$ is not MMCD, since $\mathrm{d}_{MC}(\mathcal{C}) = 2$.
- $\mathcal{C}^\perp$ has $\dim(\mathcal{C}^\perp) = 6$ and $\mathrm{d}_{MC}(\mathcal{C}^\perp) = 2$, hence it is MMCD.
- Thus the dual of a linear MMCD code may not be MMCD.
- A linear code that is MDS by rows and columns may not be MMCD.

Dually MMCD Codes

- Dually MMCD codes: A linear $\mathcal{C} \subseteq \prod_{i=1}^{\ell} \mathbb{F}_q^{m_i \times n_i}$ is dually MMCD if both $\mathcal{C}$ and $\mathcal{C}^\perp$ are MMCD.
- Let $\mathcal{C} \subseteq (\mathbb{F}_q^{2\times 2})^\ell$ be a linear code. The following are equivalent:
  1. $\mathcal{C}^{\mathbf{t}}$ is MDS by columns for all $\mathbf{t} \in \{0,1\}^\ell$.
  2. $\mathcal{C}$ is MMCD.
  3. $\mathcal{C}$ is dually MMCD.
- If $\mathcal{C} \subseteq \prod_{i=1}^{\ell} \mathbb{F}_q^{m_i \times n_i}$ is a maximum sum-rank distance (MSRD) code, then it is also an MMCD code.
- If $\mathcal{C}$ is a linear MSRD code and $m_1 = m_2 = \ldots = m_\ell$, then $\mathcal{C}$ is a dually MMCD code.

Nested Construction

- Let $n = rs$ and $t = r\ell$. Given $\mathcal{C} \subseteq (\mathbb{F}_q^{s \times s})^t$, define $\varphi(\mathcal{C}) \subseteq (\mathbb{F}_q^{n \times n})^\ell$, where $\varphi\left(C^1, C^2, \ldots, C^r\right) =$

$$\left(\begin{array}{cccc|cccc|c|cccc} C_1^1 & C_1^2 & \ldots & C_1^r & C_{r+1}^1 & C_{r+1}^2 & \ldots & C_{r+1}^r & \ldots & C_{(\ell-1)r+1}^1 & C_{(\ell-1)r+1}^2 & \ldots & C_{(\ell-1)r+1}^r \\ C_2^r & C_2^1 & \ldots & C_2^{r-1} & C_{r+2}^r & C_{r+2}^1 & \ldots & C_{r+2}^{r-1} & \ldots & C_{(\ell-1)r+2}^r & C_{(\ell-1)r+2}^1 & \ldots & C_{(\ell-1)r+2}^{r-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ C_r^2 & C_r^3 & \ldots & C_r^1 & C_{2r}^2 & C_{2r}^3 & \ldots & C_{2r}^1 & \ldots & C_t^2 & C_t^3 & \ldots & C_t^1 \end{array} \right),$$

  for $C^i = (C_1^i, C_2^i, \ldots, C_t^i) \in (\mathbb{F}_q^{s \times s})^t$, for $i = 1, 2, \ldots, r$.

- $\mathrm{d}_{MC}(\varphi(\mathcal{C})) = \mathrm{d}_{MC}(\mathcal{C})$ and $|\varphi(\mathcal{C})| = |\mathcal{C}|^r$.

- $\varphi(\mathcal{C})$ is MMCD if, and only if, so is $\mathcal{C}$.

- $\varphi(\mathcal{C})$ is linear if, and only if, so is $\mathcal{C}$, and in that case, $\dim(\varphi(\mathcal{C})) = r\dim(\mathcal{C})$ and $\varphi(\mathcal{C})^\perp = \varphi(\mathcal{C}^\perp)$.

- (If $\mathcal{C}$ is linear) $\varphi(\mathcal{C})$ is a dually MMCD code if, and only if, so is $\mathcal{C}$.

Nested Construction

- If $q > t$, there is a linear MSRD code $\mathcal{C} \subseteq (\mathbb{F}_q^{s \times s})^t$ (linearized RS).
- The code $\varphi(\mathcal{C}) \subseteq (\mathbb{F}_q^{n \times n})^\ell$ is a dually MMCD code.
- We may choose $q = t + 1$, and $\varphi(\mathcal{C})$ may be decoded with a complexity $\mathcal{O}(t\ell n^2)$ over a field of size $q^{\ell n/t} = (t+1)^{\ell n/t}$.
- If a product in $\mathbb{F}_{2^b}$ costs $\mathcal{O}(b^2)$ operations in $\mathbb{F}_2$, then the previous complexity over $\mathbb{F}_2$ is

$$\mathcal{O}\left(t^{-1} \log_2(t+1)^2 \ell^3 n^4 \right).$$

- This complexity is lower for larger values of t.
- However, codes for larger t require larger alphabets ($q > t$), whereas codes for smaller t can be used for smaller alphabets.

Nested Construction

- If $\ell = 1$ (but $1 \leq t \leq n$, $t|n$), then the previous code $\varphi(\mathcal{C}) \subseteq \mathbb{F}_q^{n \times n}$ is dually MMCD code for the classical cover metric (MCD code?).
- The case $t = n$ corresponds to the code by Roth (1991), where $\mathbf{c}^i \in \mathcal{C}$, for a Reed–Solomon code $\mathcal{C} \subseteq \mathbb{F}_q^n$ and

$$\varphi\left(\mathbf{c}^1, \mathbf{c}^2, \ldots, \mathbf{c}^n\right) = \left(\begin{array}{cccc} c_1^1 & c_1^2 & \ldots & c_1^n \\ c_2^n & c_2^1 & \ldots & c_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_n^2 & c_n^3 & \ldots & c_n^1 \end{array} \right).$$

- The case $t = 1$ corresponds to the code by Roth (1991) given by a Gabidulin code $\mathcal{C} \subseteq \mathbb{F}_q^{n \times n}$.
- The cases $1 < t < n$, $t|n$, correspond to a new family of dually MMCD codes for the classical cover metric.
- Their advantage is the previous alphabet-complexity trade-off.

Open Problems

- We only considered error-free worst-case deterministic decoding. Probabilistic decoding as considered by Roth (1997) but in the multi-cover metric is open.
- List decoding for the cover metric was studied by Wachter-Zeh (2016). The multi-cover metric case is open.
- Crisscross insertions and deletions were studied recently by Bitar et al. (2021), where several code constructions are given. The multi-cover metric case is open.
- Codes with local crisscross erasure correction was studied by Kadhe et al. (2019). The multi-cover metric case is open.

Conclusion

Thank you for your attention.