Coding for Combined Block-Symbol Error Correction

Pascal O. Vontobel

Talk at WCI 2013, Hong Kong, December 13, 2013

Joint work with Ron M. Roth http://arxiv.org/abs/1302.1931

Overview

- Motivation
- Proposed coding scheme
- Decoding
- Conclusions / open problems

Motivation



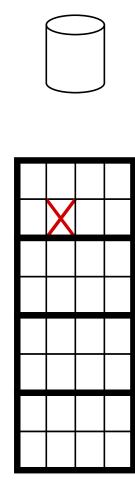






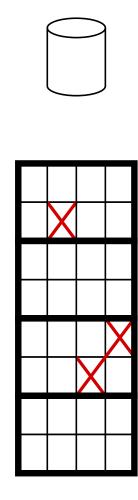






Disk

1 symbol error

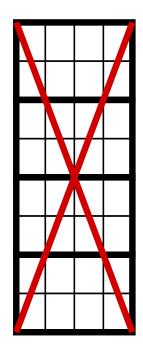


Disk

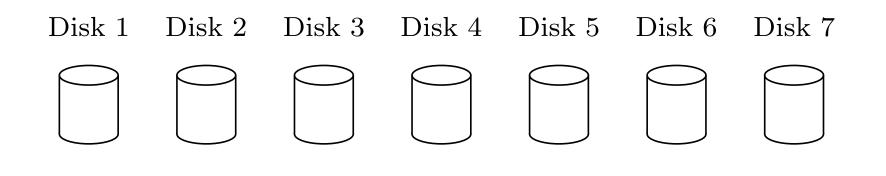
1 symbol error

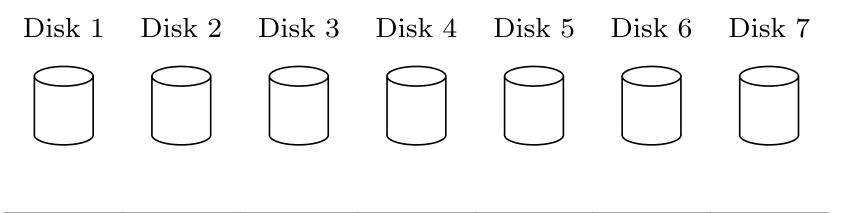
2 symbol errors

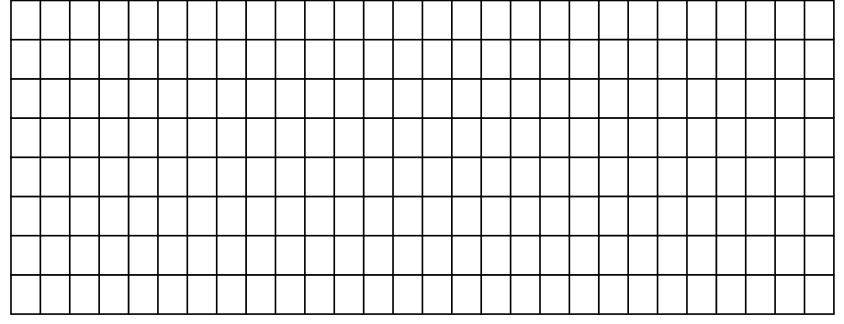


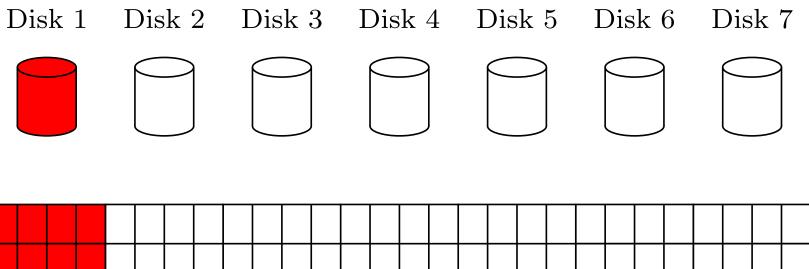


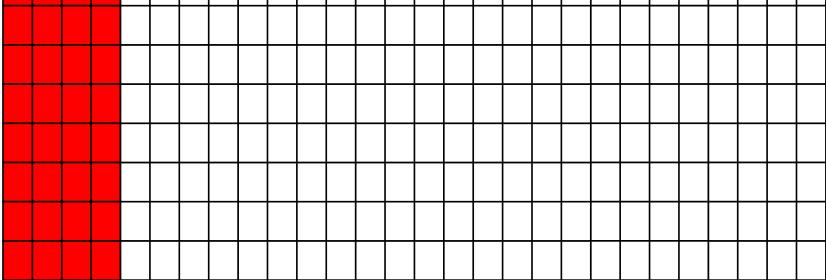
1 burst error

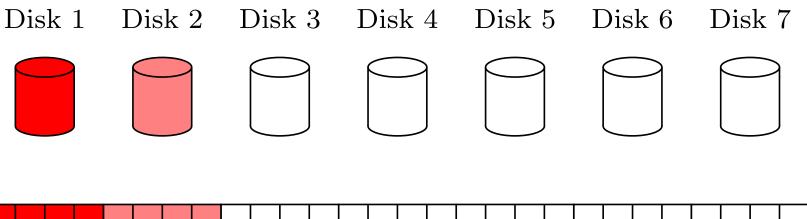


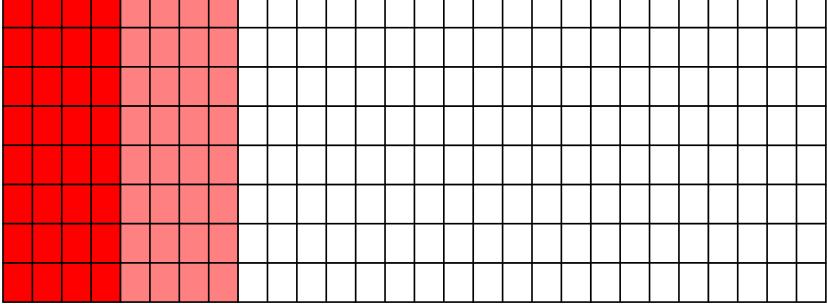


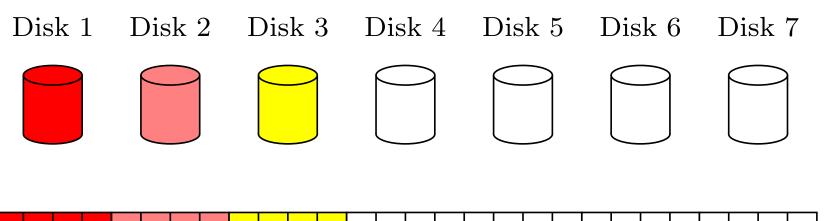


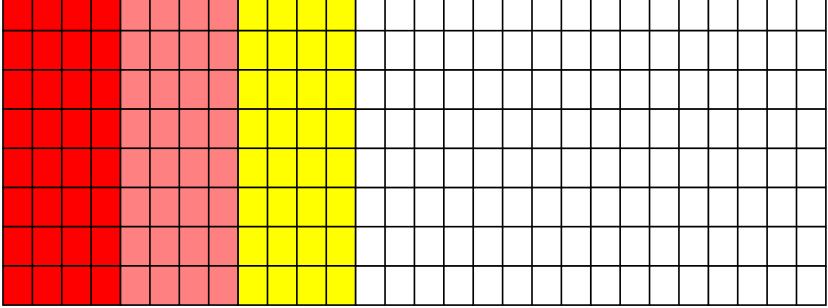


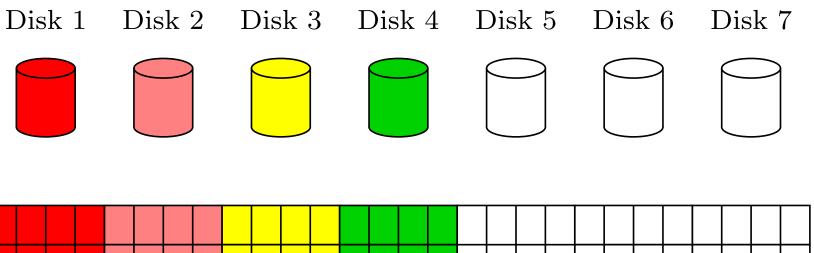


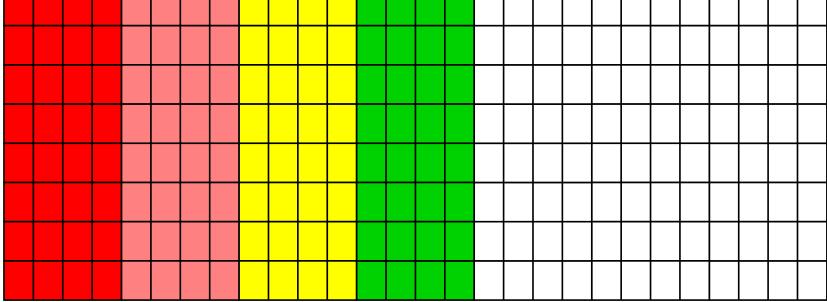


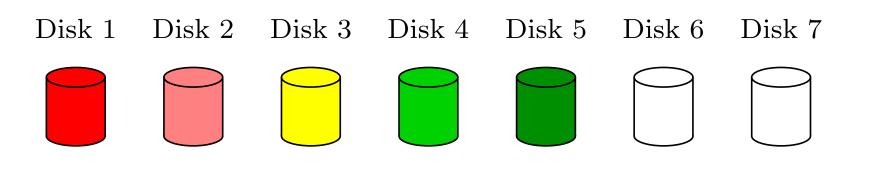


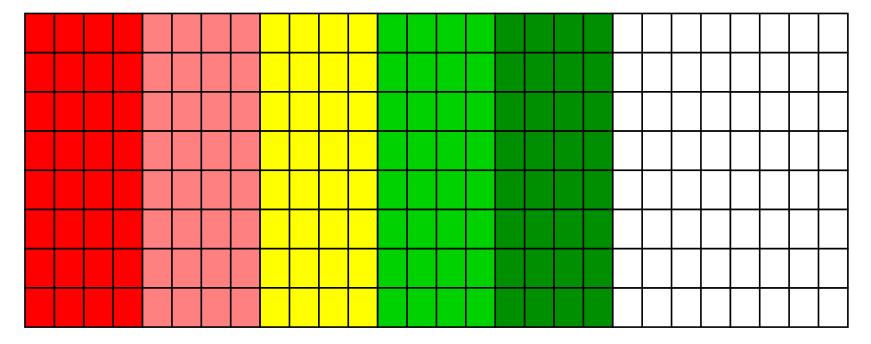


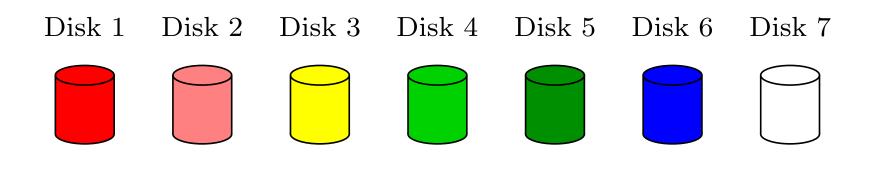


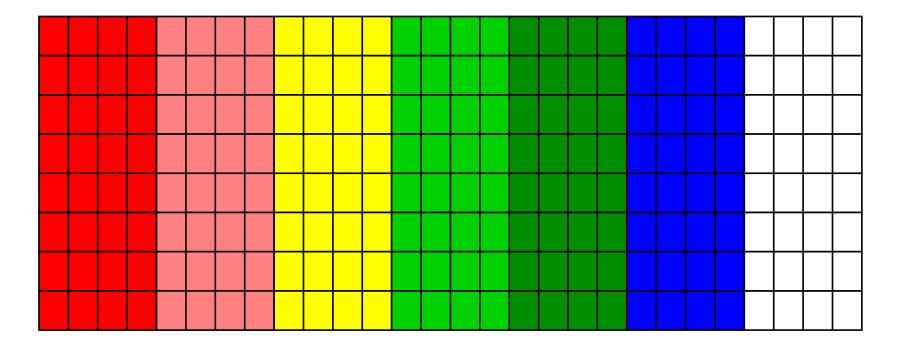


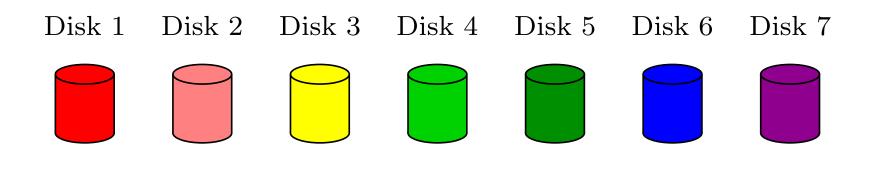


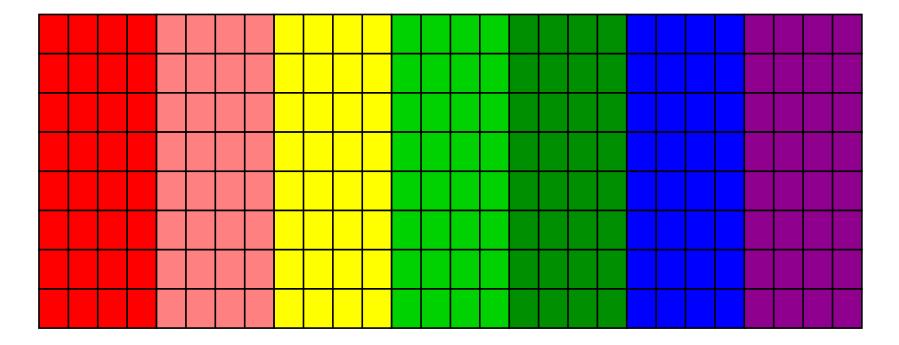


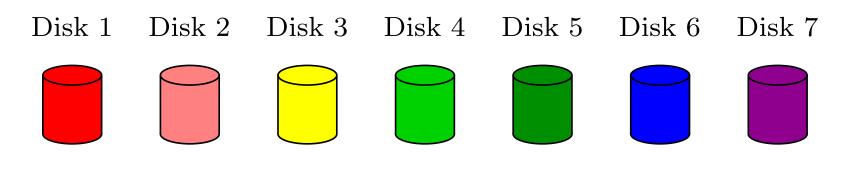


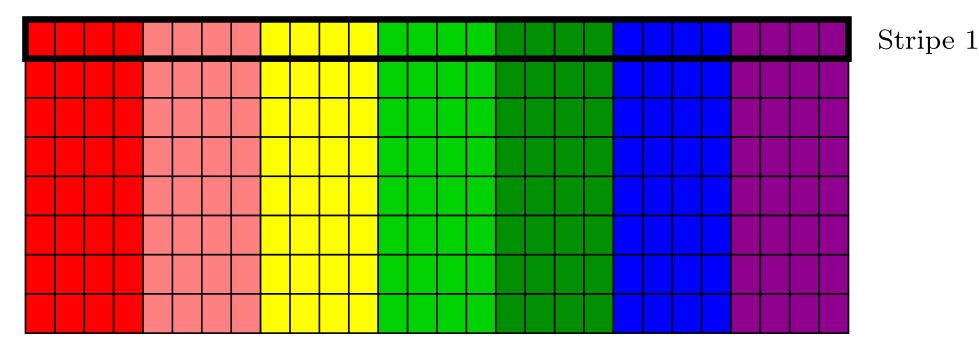


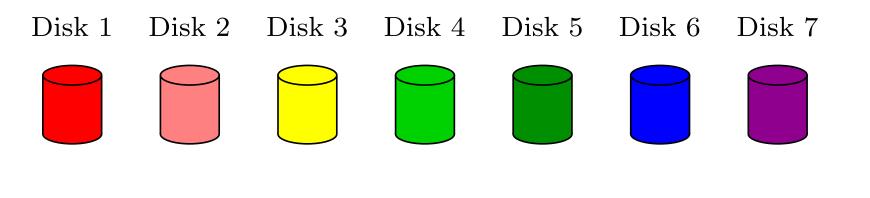


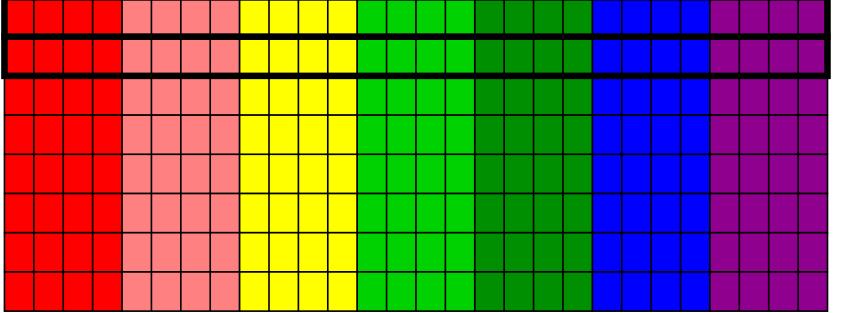




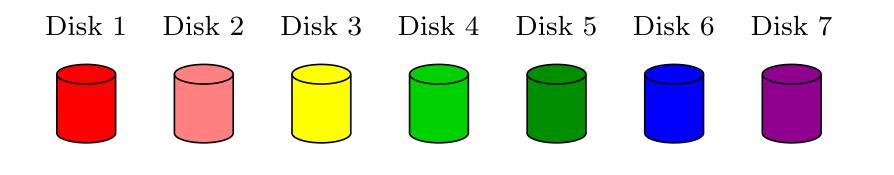


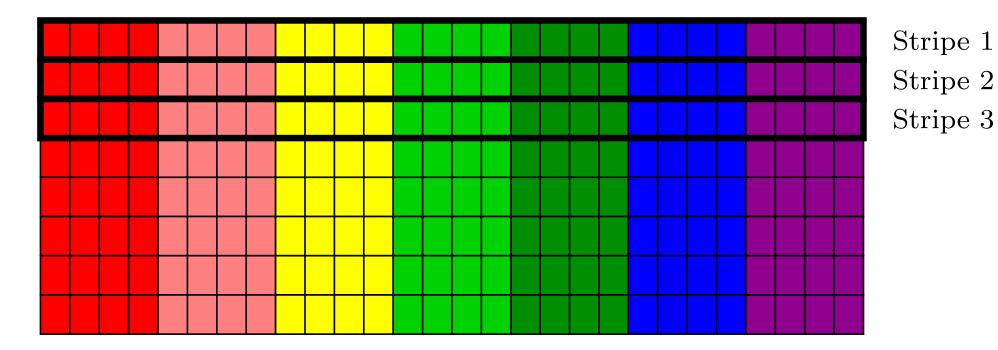


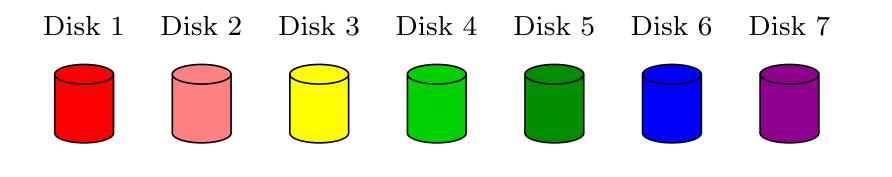


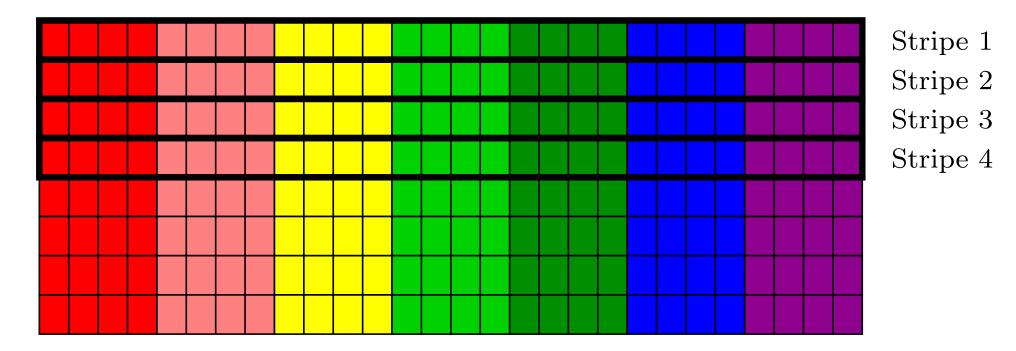


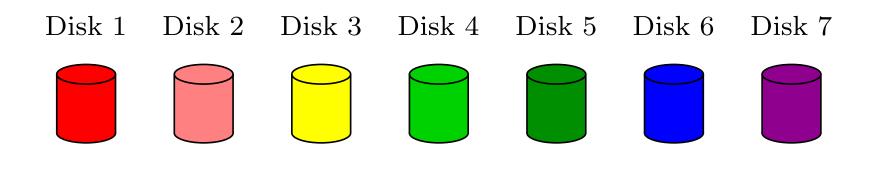
Stripe 1 Stripe 2

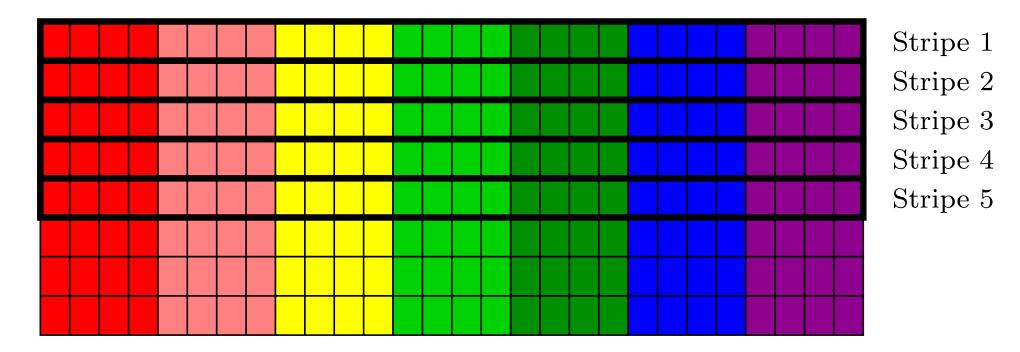


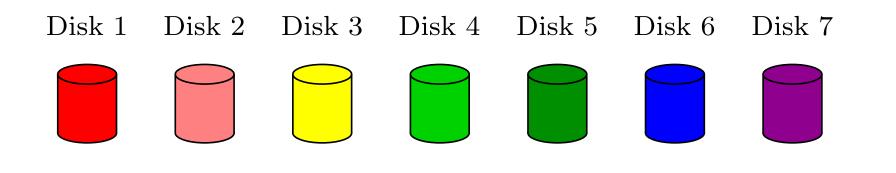


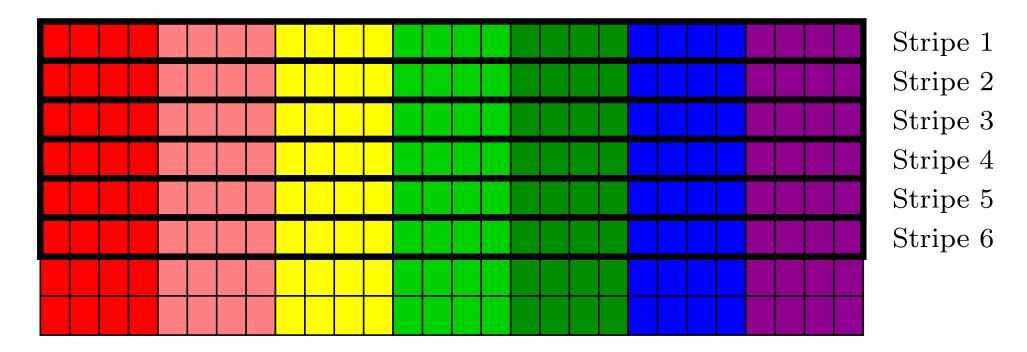


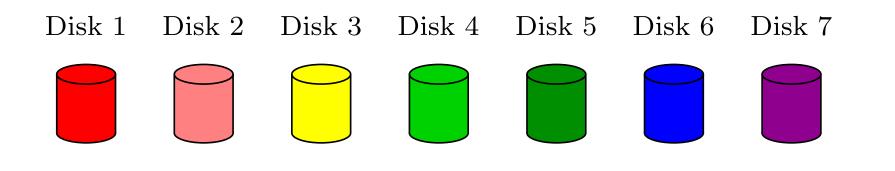


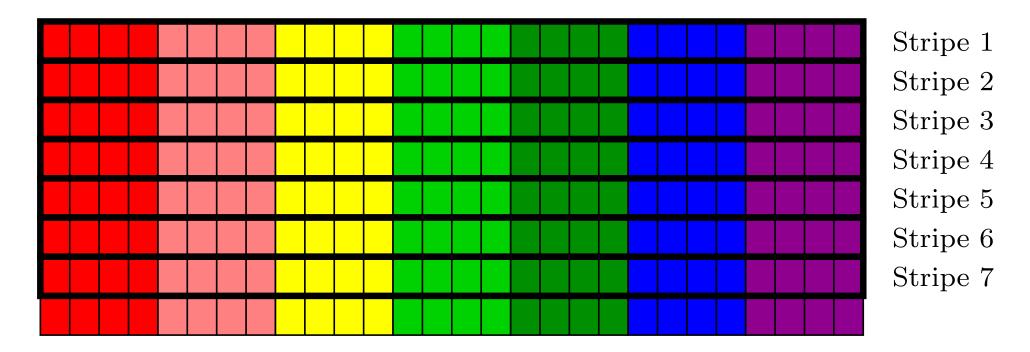


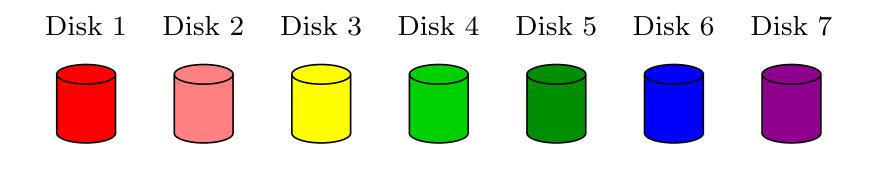


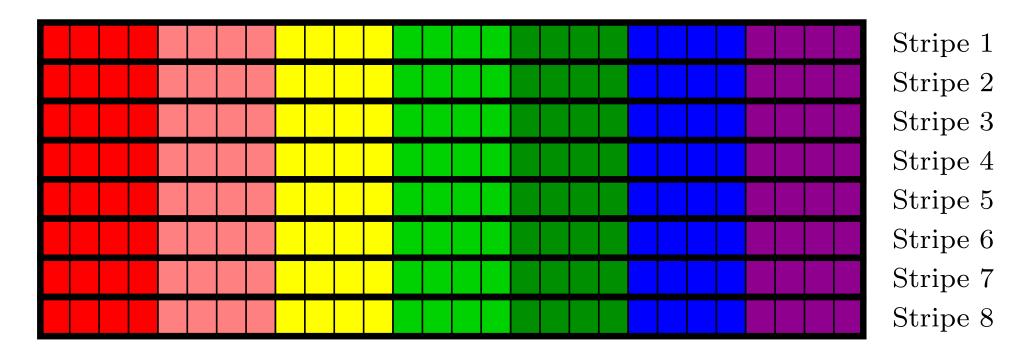


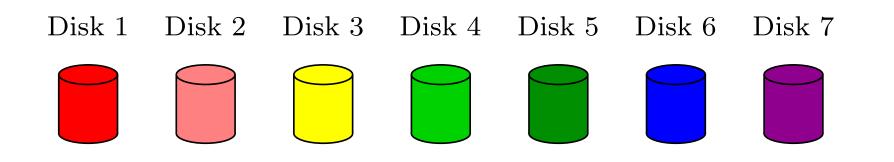


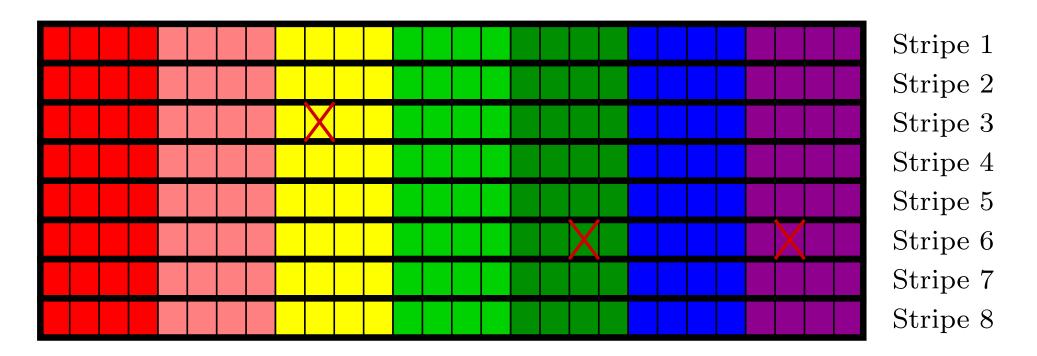


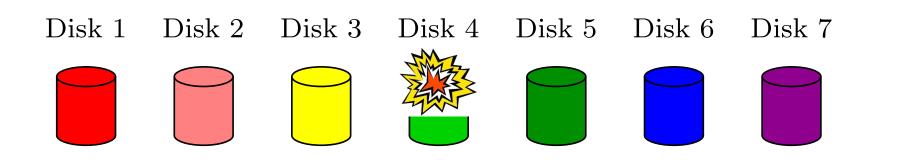


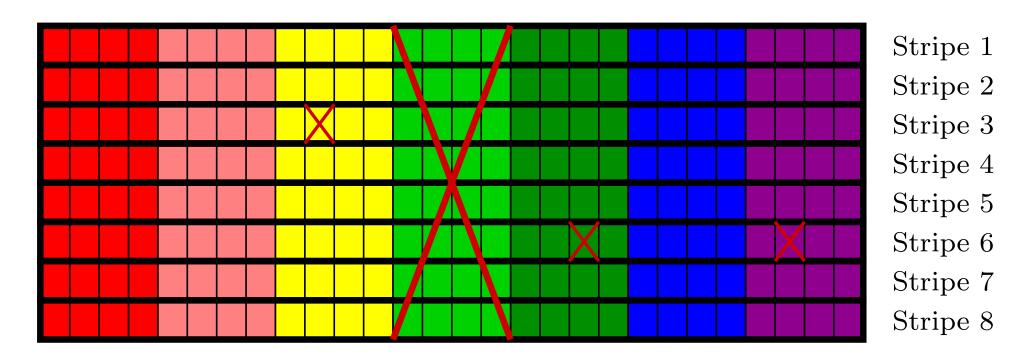


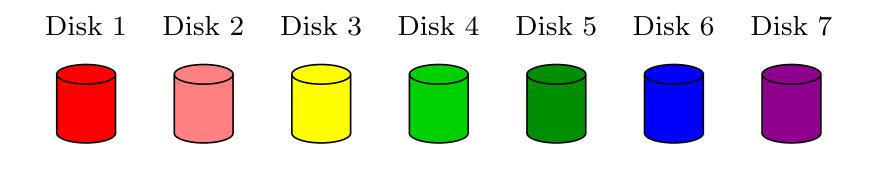


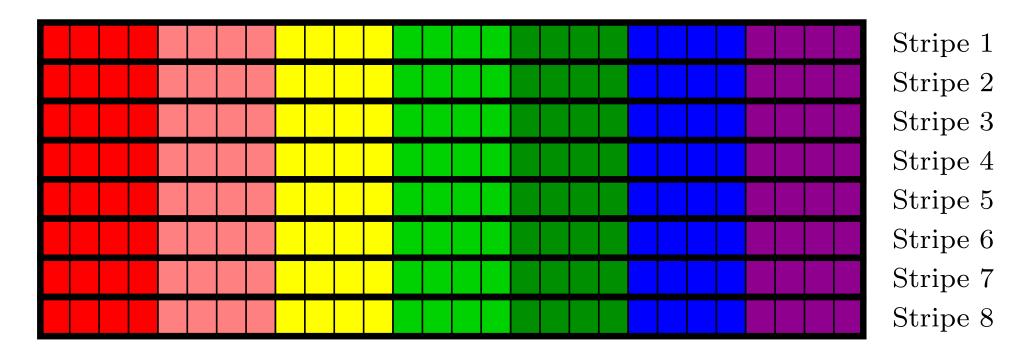






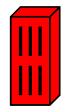


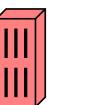


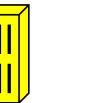


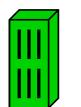
Similar Principle with DRAMs

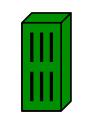
DRAM 1 DRAM 2 DRAM 3 DRAM 4 DRAM 5 DRAM 6 DRAM 7

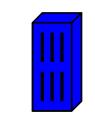




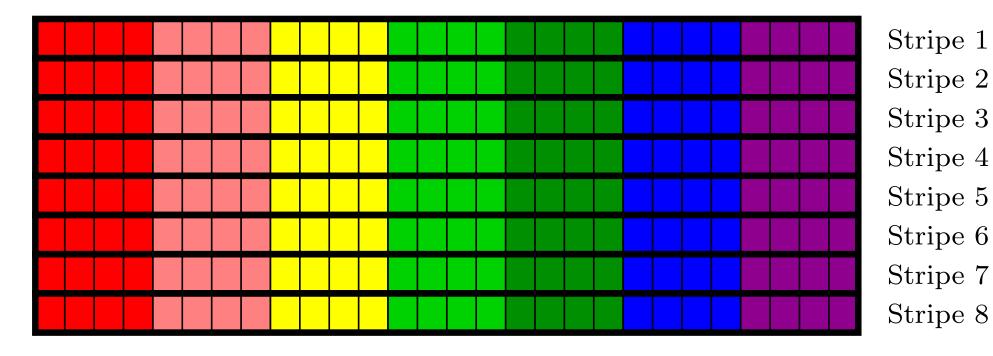


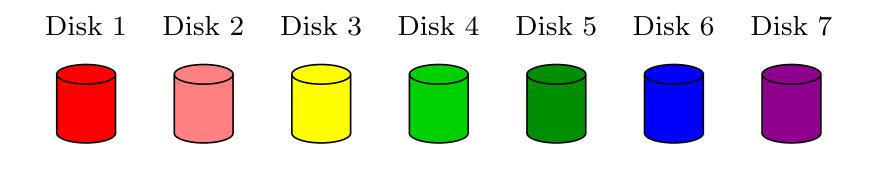


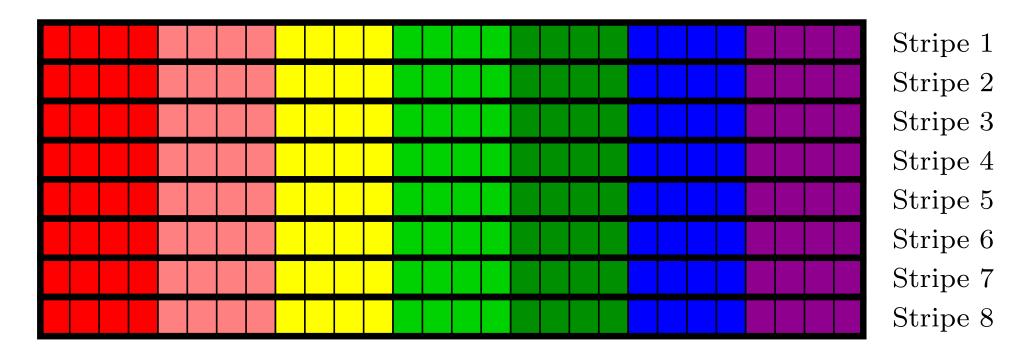






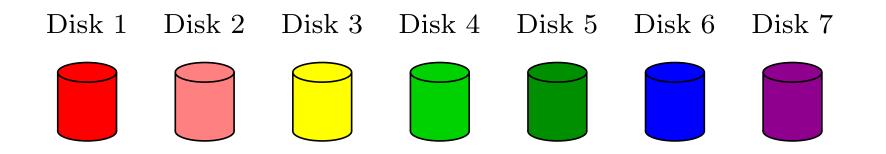


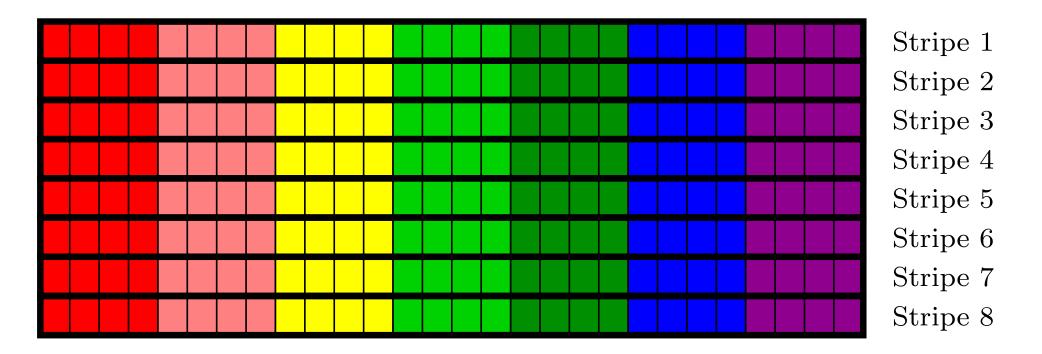


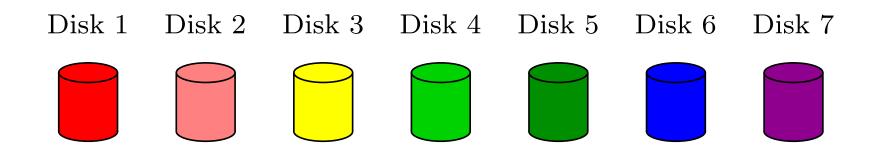


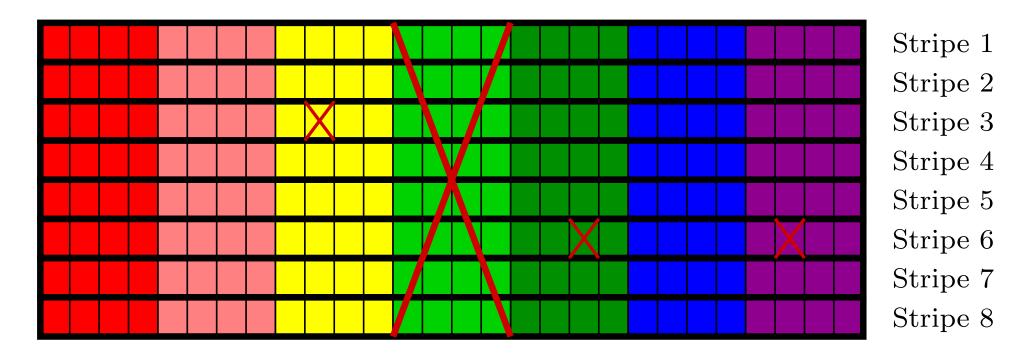
Error / erasure model

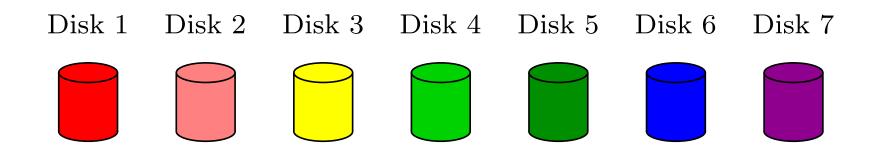
Error / Erasure Model

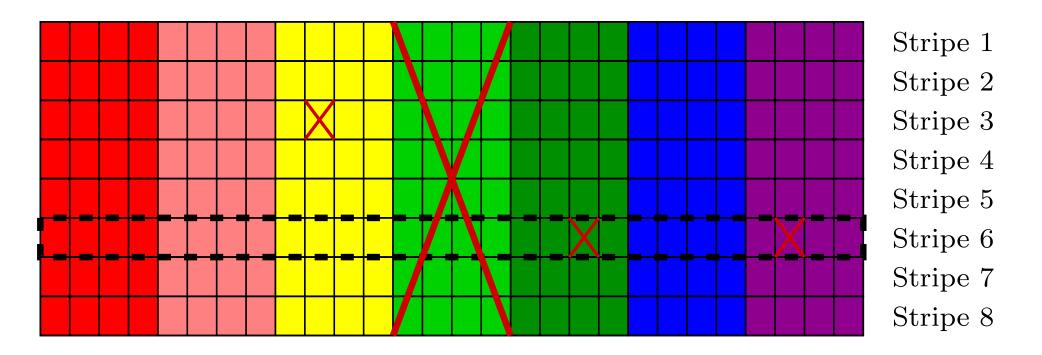


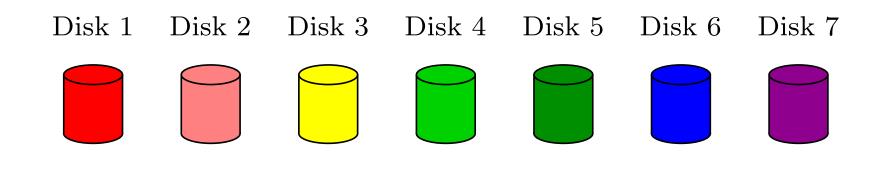


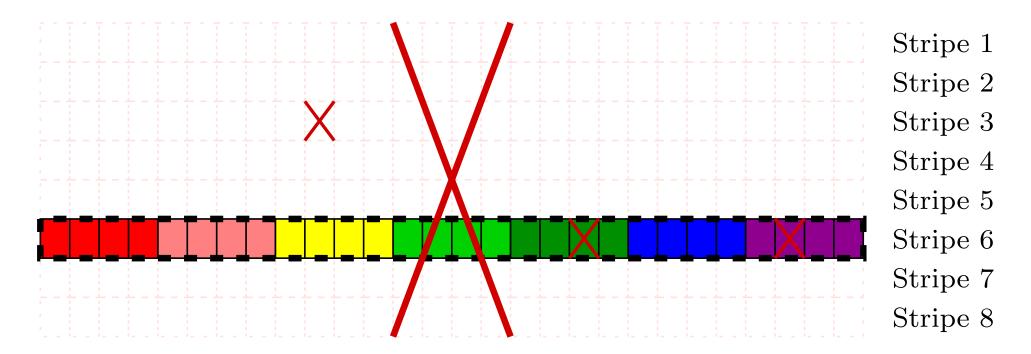


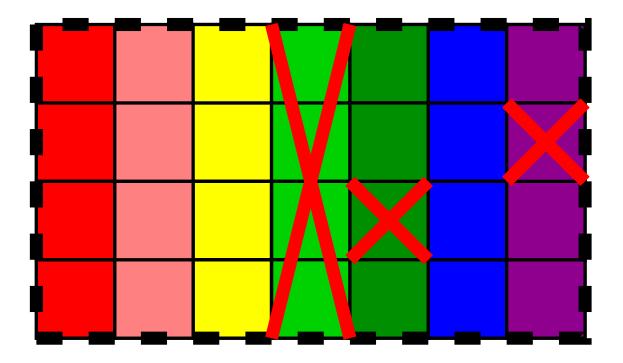


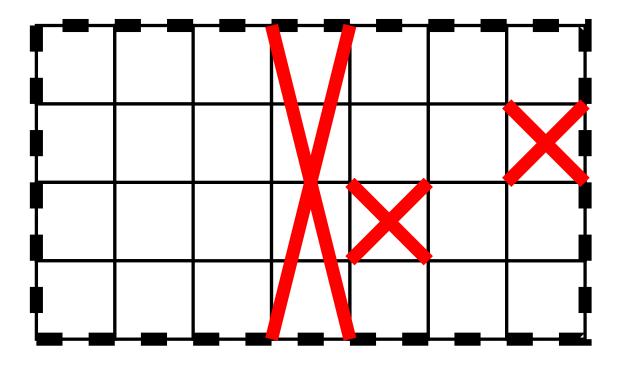


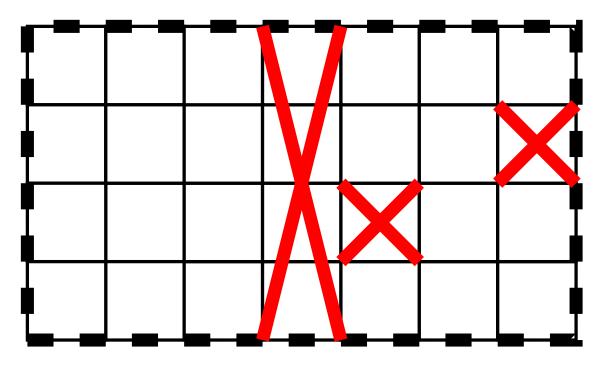












 $m \times n$

Wish List for ECC Scheme

We want ECC schemes that can jointly handle

- burst errors,
- symbol errors.

Wish List for ECC Scheme

We want ECC schemes that can jointly handle

- burst errors,
- symbol errors.

Moreover, the ECC scheme schould also be able to handle

- burst erasures,
- symbol erasures.

Wish List for ECC Scheme

We want ECC schemes that can jointly handle

- burst errors,
- symbol errors.

Moreover, the ECC scheme schould also be able to handle

- burst erasures,
- symbol erasures.

Finally, the ECC scheme should have

- low encoding complexity,
- low decoding complexity.

Overview

Example of previous coding schemes for related setups.

[Blokh, Zyablov, 1974]
[Kasahara, Hirasawa, Sugiyama, Namekawa, 1976]
[Zinov'ev, Zyablov, 1979]
[Zinov'ev, 1981]
[Abdel-Ghaffar, Hassner, 1991]
[Feng, Tzeng, 1991]
[Dumer, 1998]
[Metzner, Kapturowski, 1990]
[Sakata, 1991]
[Krachkovsky, Lee, 1998]
[Roth, Seroussi, 1998]

[Haslach, Vinck, 1999, 2000]
[Brown, Minder, Shokrollahi, 2004]
[Justesen, Thommesen, Høholdt, 2004]
[Bleichenbacher, Kiayas, Yung, 2007]
[Wu, 2008]
[Schmidt, Sidorenko, Bossert, 2009]
[Kurzweil, Seidl, Huber, 2011]
[Blaum, Hafner, Hetzler, 2012]
[Wachter–Zeh, Zeh, Bossert, 2013]

Overview

Example of previous coding schemes for related setups.

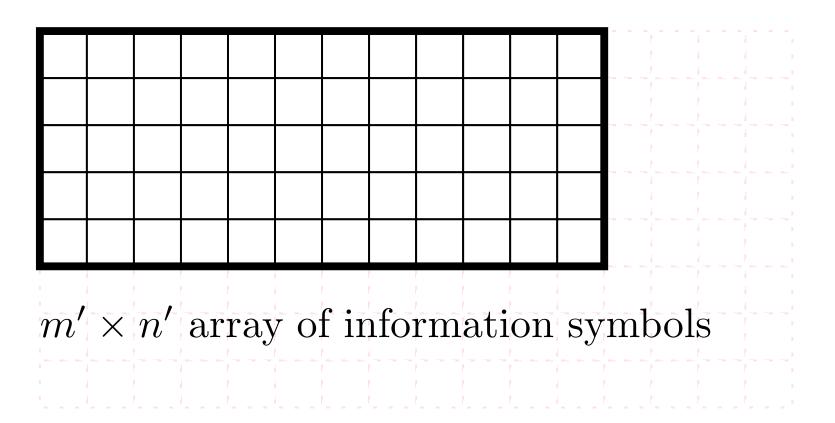
[Blokh, Zyablov, 1974]
[Kasahara, Hirasawa, Sugiyama, Namekawa, 1976]
[Zinov'ev, Zyablov, 1979]
[Zinov'ev, 1981]
[Abdel-Ghaffar, Hassner, 1991]
[Feng, Tzeng, 1991]
[Dumer, 1998]
[Metzner, Kapturowski, 1990]
[Sakata, 1991]
[Krachkovsky, Lee, 1998]
[Roth, Seroussi, 1998]

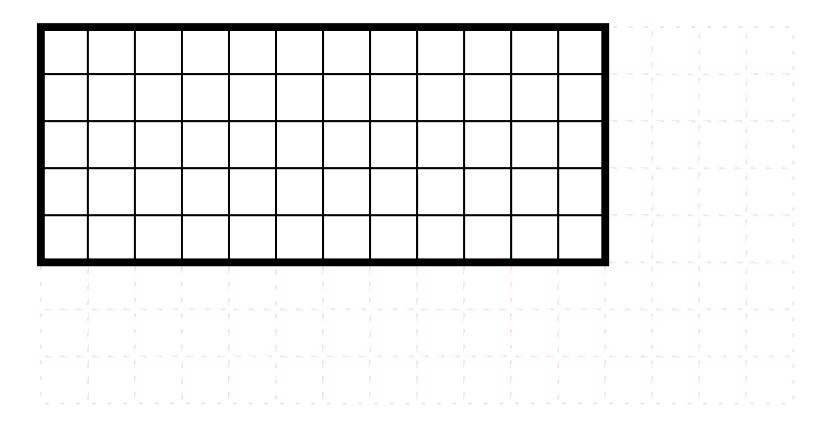
[Haslach, Vinck, 1999, 2000]
[Brown, Minder, Shokrollahi, 2004]
[Justesen, Thommesen, Høholdt, 2004]
[Bleichenbacher, Kiayas, Yung, 2007]
[Wu, 2008]
[Schmidt, Sidorenko, Bossert, 2009]
[Kurzweil, Seidl, Huber, 2011]
[Blaum, Hafner, Hetzler, 2012]
[Wachter–Zeh, Zeh, Bossert, 2013]

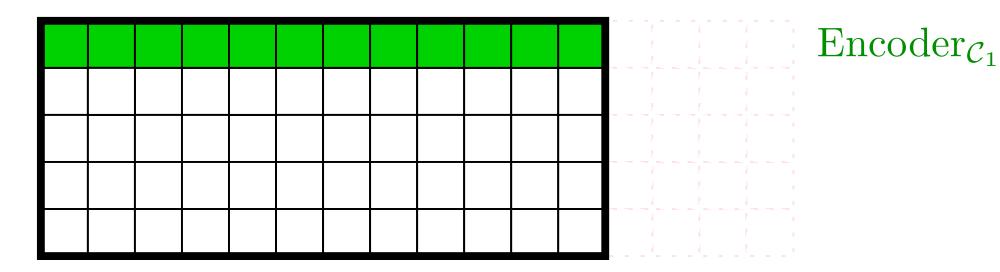
Our proposed coding scheme:

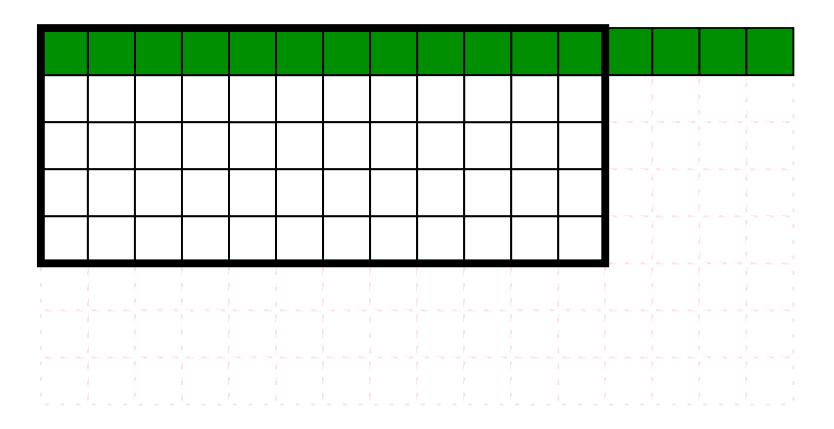
- Code construction
- Code properties
- Decoding algorithms

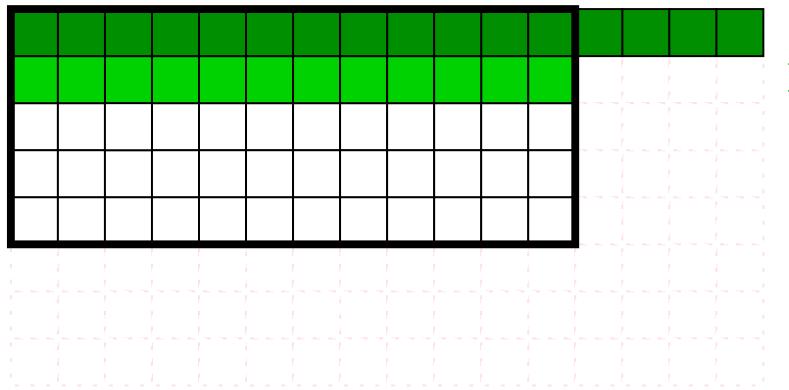
Example of a more "traditional" coding scheme



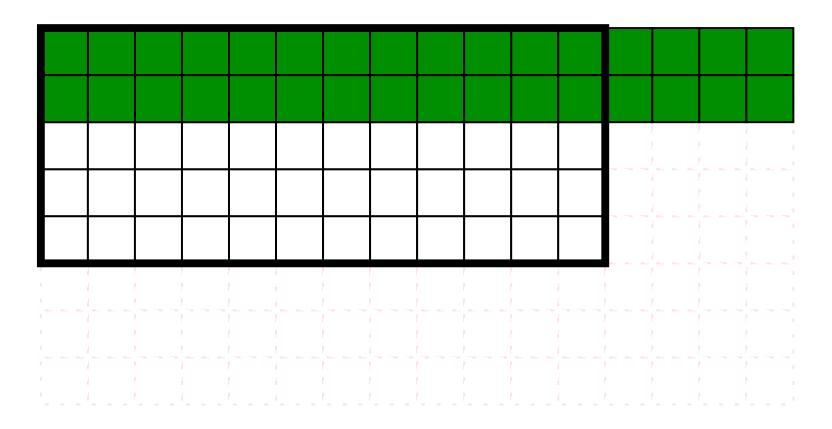




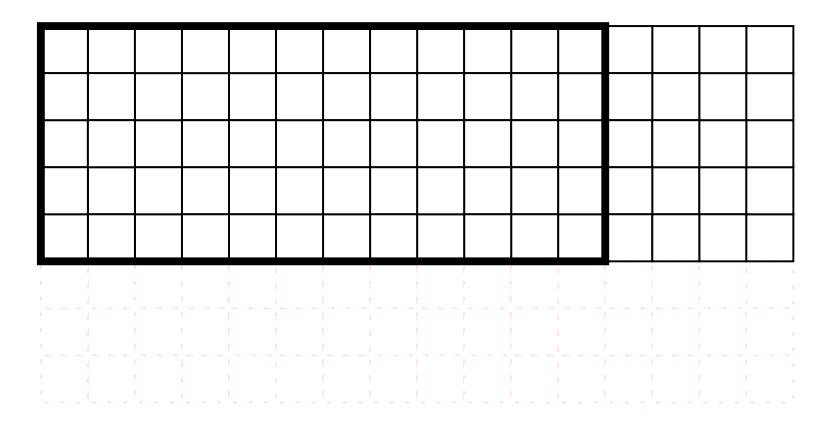


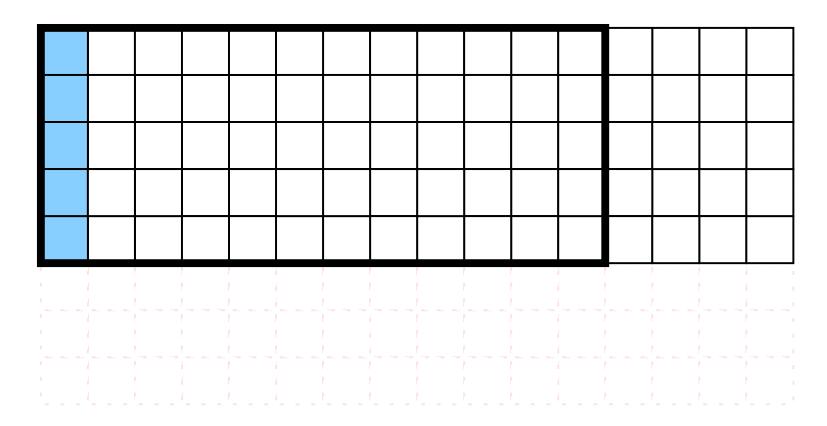


 $\mathrm{Encoder}_{\mathcal{C}_1}$

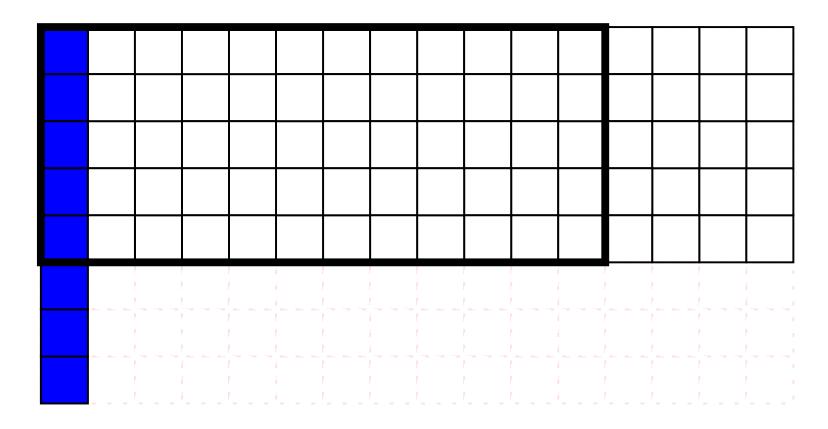


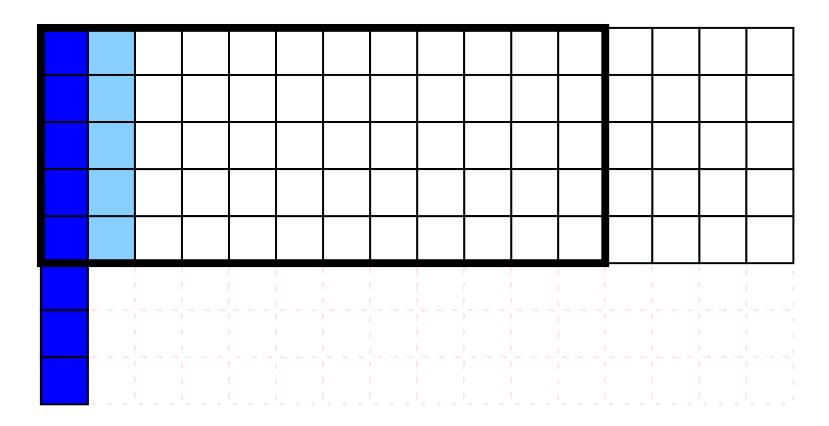
							1



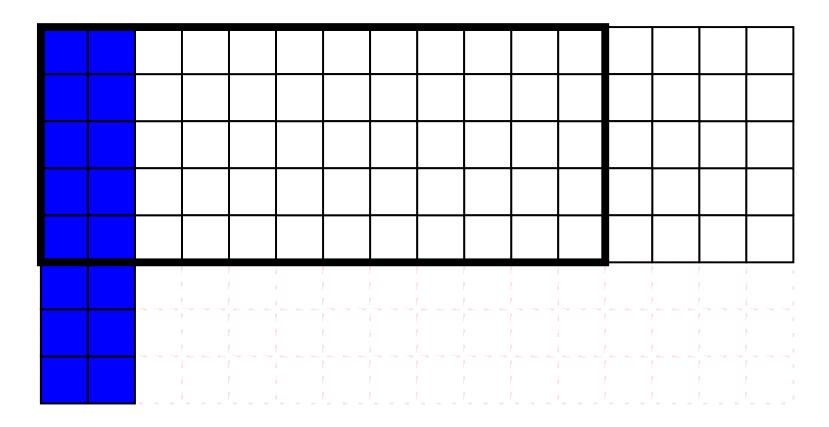


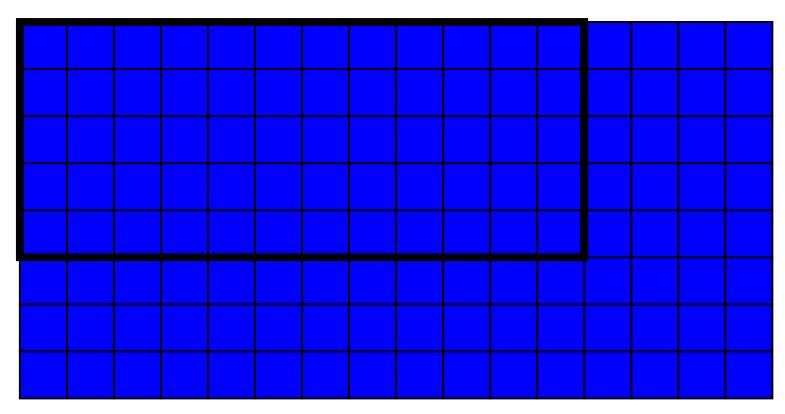
Encoder $_{\mathcal{C}_2}$



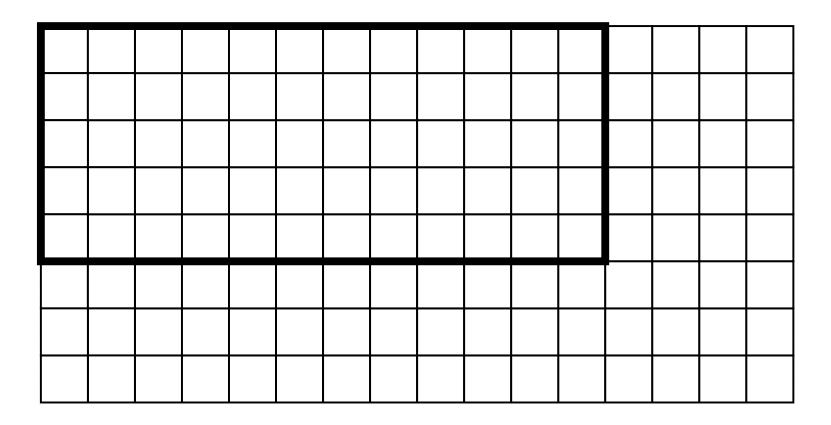


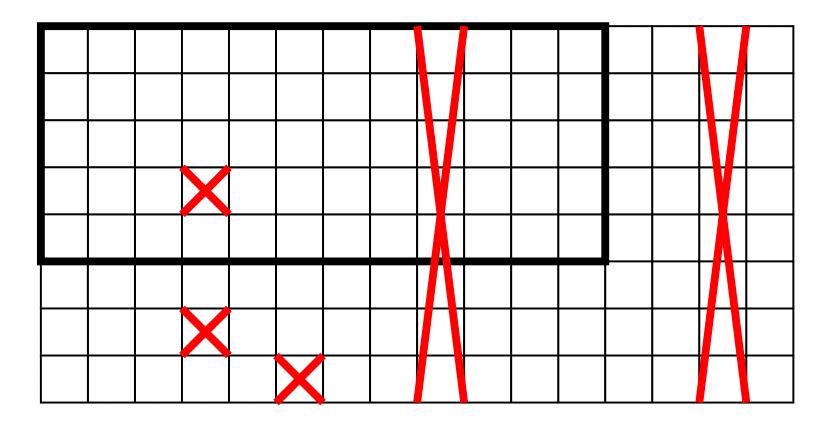
Encoder $_{\mathcal{C}_2}$

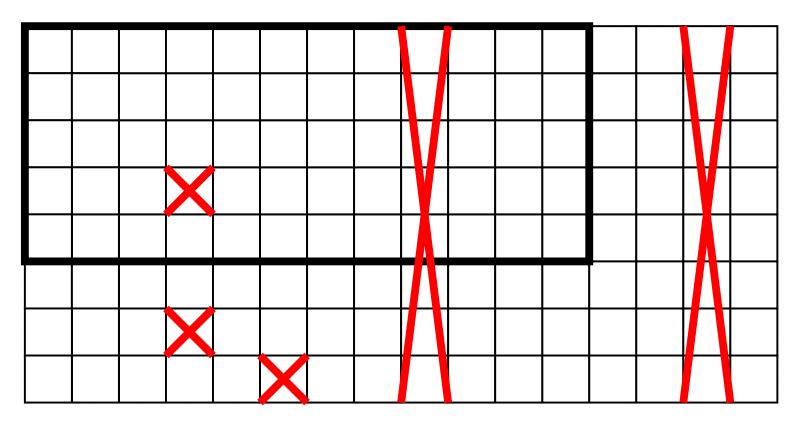




 $m \times n$ array of codeword symbols

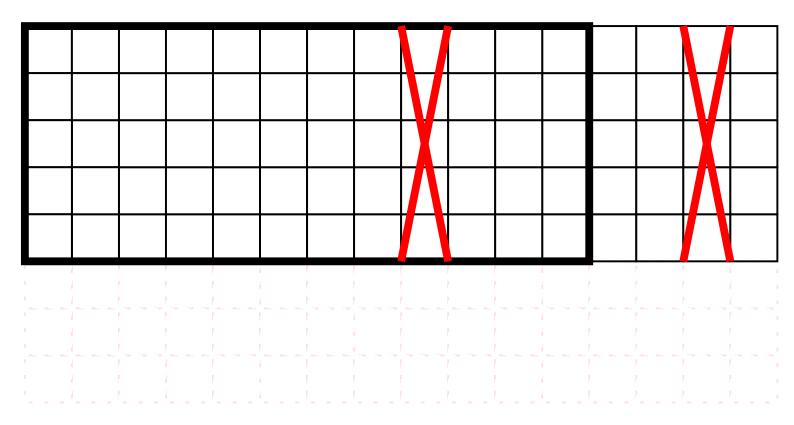






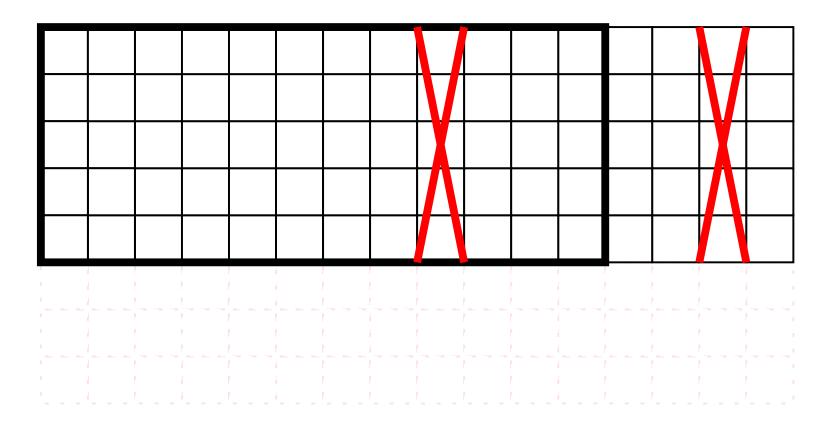
Decoding of columns based on C_2 :

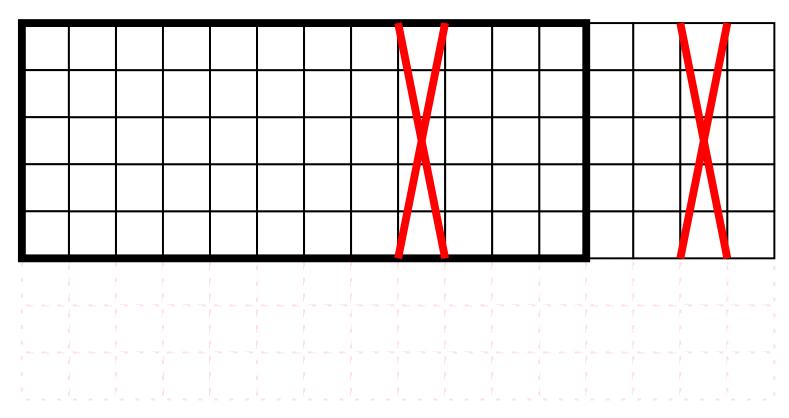
- corrects symbol errors (as far as possible),
- leaves or modifies block errors.



Decoding of columns based on C_2 :

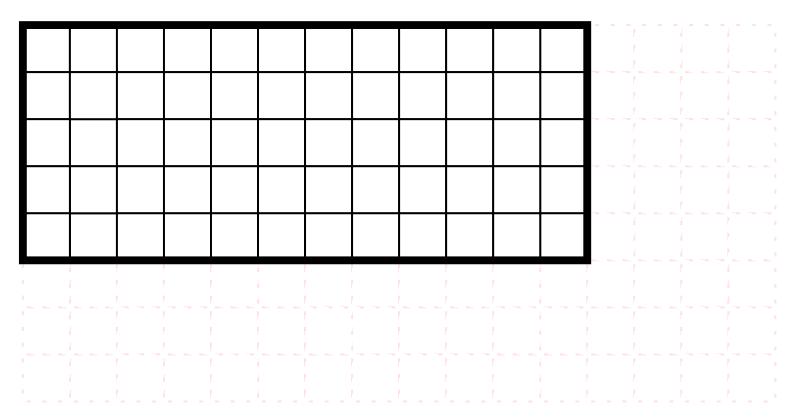
- corrects symbol errors (as far as possible),
- leaves or modifies block errors.





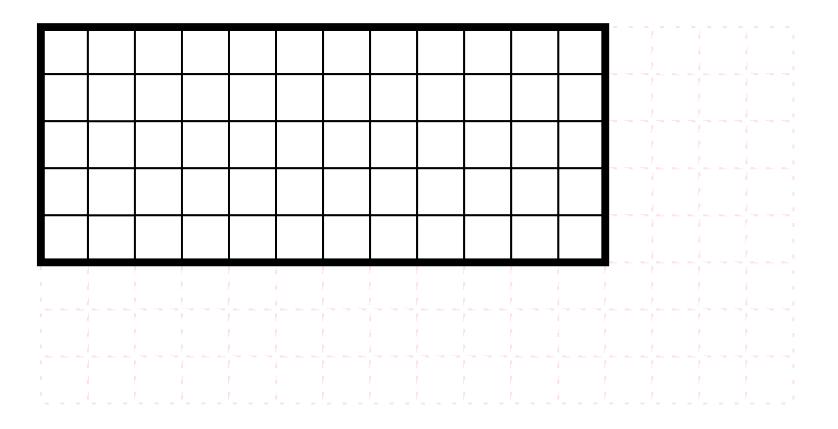
Decoding of rows based on C_1 :

corrects block errors (as far as possible).

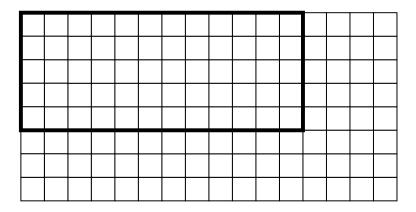


Decoding of rows based on C_1 :

corrects block errors (as far as possible).

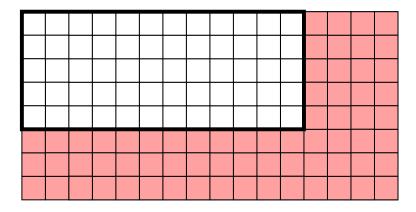


Disadvantages of Product Coding Scheme



Product coding schemes have many favorable aspects.

Disadvantages of Product Coding Scheme



Product coding schemes have many favorable aspects.

However:

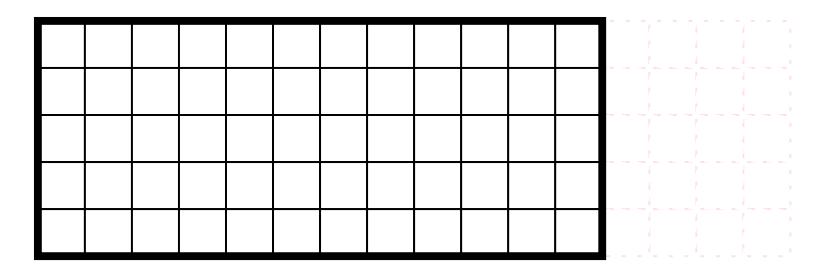
• $\operatorname{Rate}(\mathcal{C}_1) < 1.$

 \Rightarrow The redundancy of the coding scheme is at least linear in m.

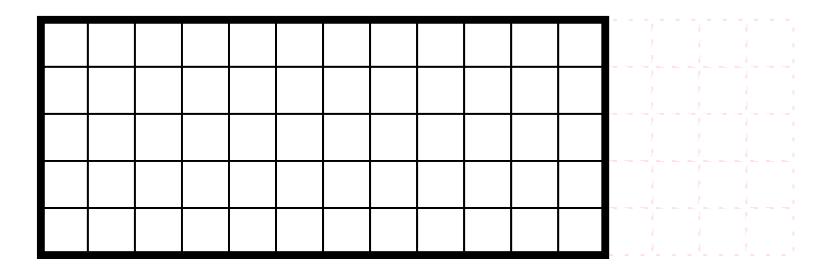
• $\operatorname{Rate}(\mathcal{C}_2) < 1.$

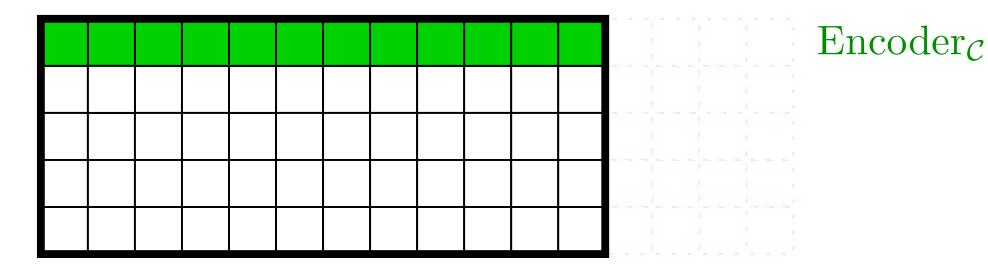
 \Rightarrow The redundancy of the coding scheme is at least linear in n.

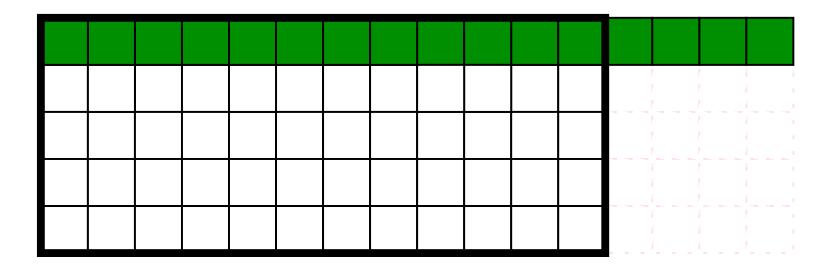
Proposed coding scheme: Overview

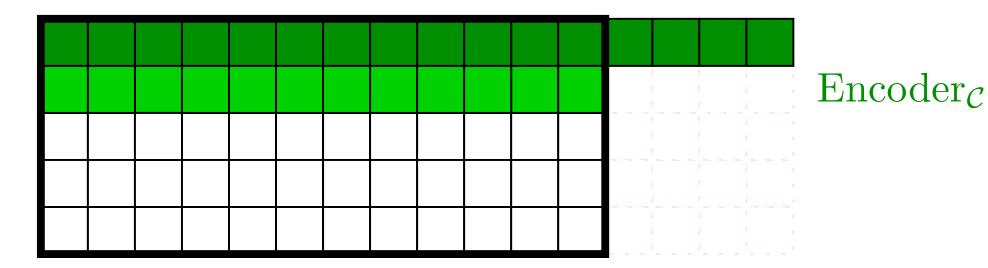


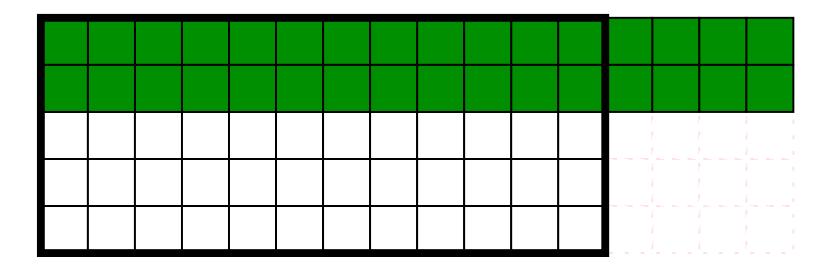
 $m \times n'$ array of information symbols

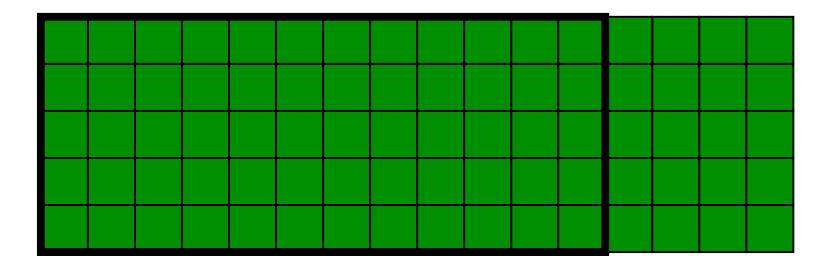


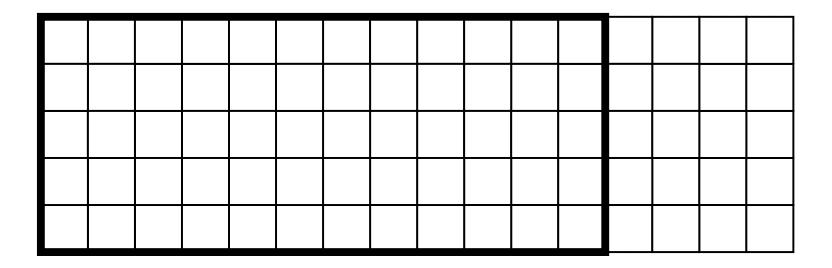


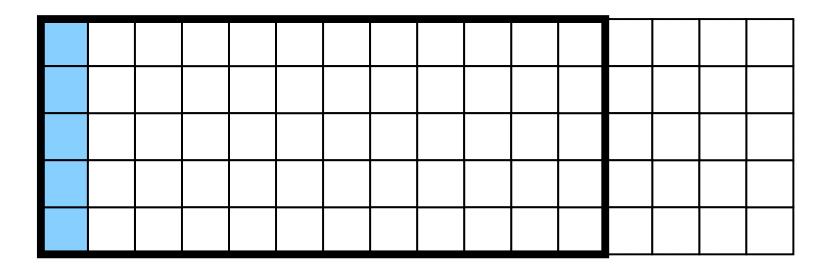




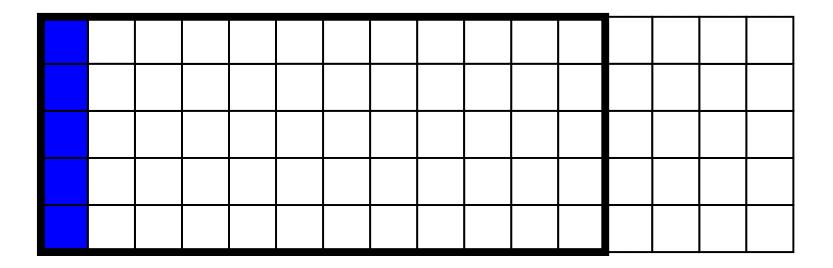


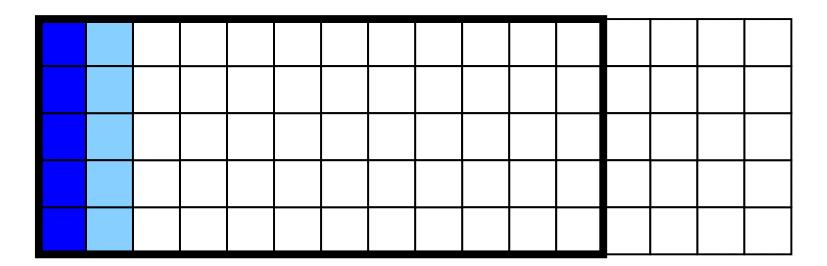




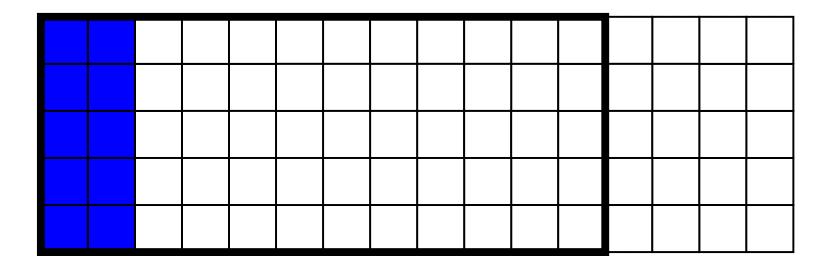


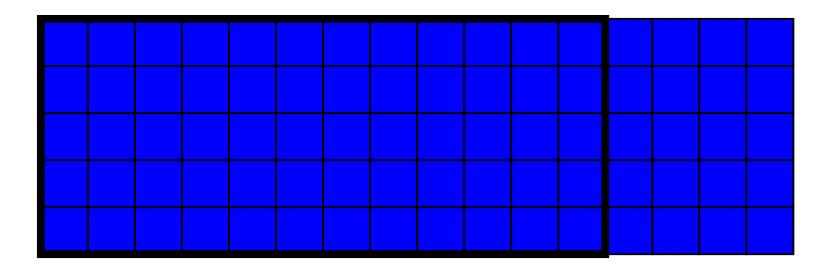
T multiply by square matrix H_0^{-1}



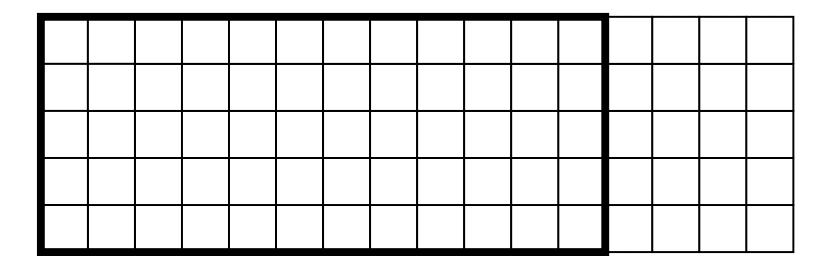


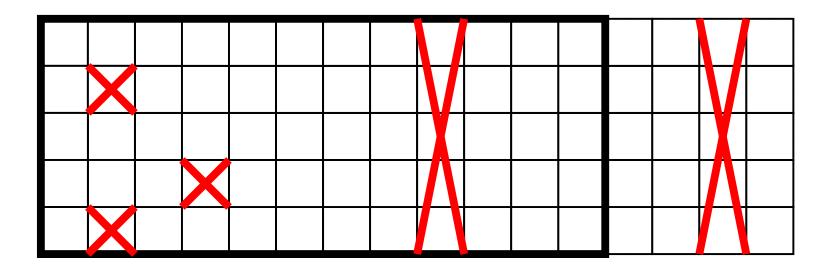
multiply by square matrix H_1^{-1}

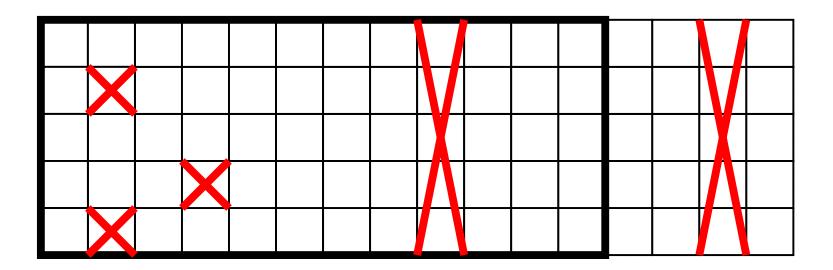




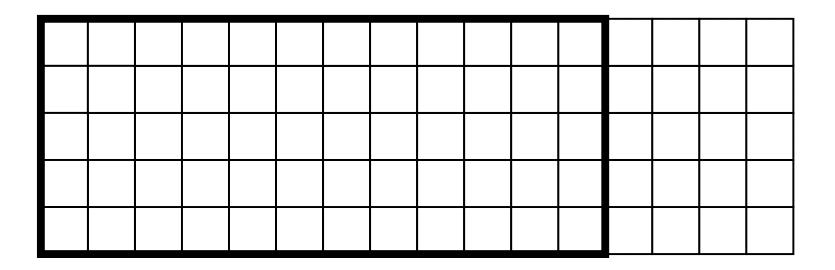
 $m \times n$ array of codeword symbols



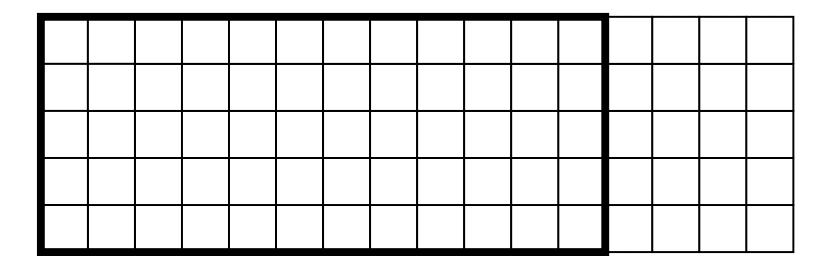


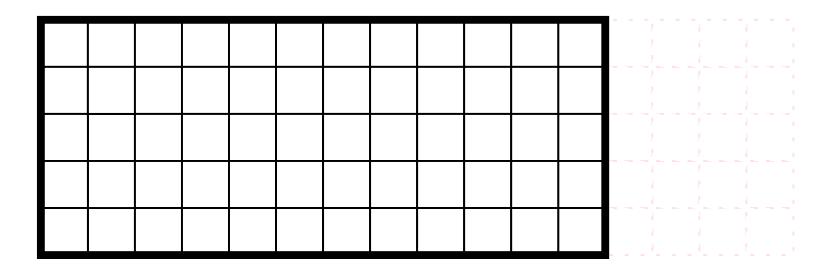


Decoding based on code C and matrices H_0, H_1, \ldots .



Decoding based on code C and matrices H_0, H_1, \ldots .

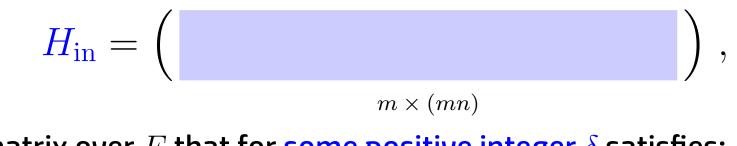




Proposed coding scheme: Code definition

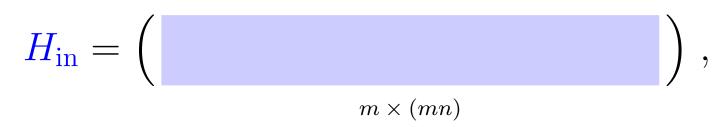
• Let \mathcal{C} be a linear [n, k, d] code over F.

- Let \mathcal{C} be a linear [n, k, d] code over F.
- Let



be a matrix over F that for some positive integer δ satisfies:

- Let \mathcal{C} be a linear [n, k, d] code over F.
- Let



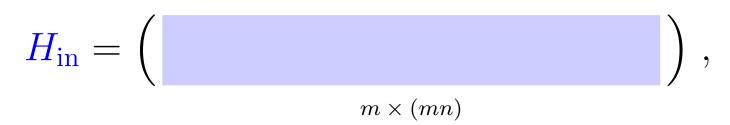
- be a matrix over F that for some positive integer δ satisfies:
 - writing

$$H_{\rm in} = \left(\begin{array}{ccccc} H_0 & H_1 & \dots & & H_{n-1} \end{array}\right),$$

$$m \times m & m \times m & m \times m & m \times m & m \times m \end{array}$$

every submatrix H_j is invertible over F,

- Let \mathcal{C} be a linear [n, k, d] code over F.
- Let



- be a matrix over F that for some positive integer δ satisfies:
 - writing

$$H_{\rm in} = \begin{pmatrix} H_0 & H_1 & \dots & H_{n-1} \end{pmatrix},$$

$$m \times m & m \times m & m \times m & m \times m & m \times m \end{pmatrix},$$

every submatrix H_i is invertible over F,

• every subset of $\delta - 1$ columns in $H_{\rm in}$ is linearly independent.

We define $\mathbb{C} = (\mathcal{C}, H_{in})$ to be

We define $\mathbb{C} = (\mathcal{C}, H_{\mathrm{in}})$ to be

• the linear [mn, mk] code over F

We define $\mathbb{C} = (\mathcal{C}, H_{\mathrm{in}})$ to be

- the linear [mn, mk] code over F
- which consists of all $m \times n$ matrices over F

$$\Gamma = \left(\begin{array}{c|c} \Gamma_0 & \Gamma_1 & \dots & \dots & \Gamma_{n-1} \end{array} \right)_{m \times 1} \quad m \times 1 \quad m \times 1 \quad m \times 1 \quad m \times 1 \quad m \times 1$$

We define $\mathbb{C} = (\mathcal{C}, H_{\mathrm{in}})$ to be

- the linear [mn, mk] code over F
- which consists of all m imes n matrices over F

$$\Gamma = \left(\begin{array}{c|c} \Gamma_0 & \Gamma_1 & \dots & \dots & \Gamma_{n-1} \end{array} \right)$$

$$\xrightarrow{m \times 1} & \xrightarrow{m \times 1} & \xrightarrow{m \times 1} & \xrightarrow{m \times 1} & \xrightarrow{m \times 1} \end{array}$$

such that each row in

$$Z = \begin{pmatrix} H_0 \Gamma_0 & H_1 \Gamma_1 & \dots & M_{n-1} \Gamma_{n-1} \end{pmatrix}$$

$$\xrightarrow{m \times 1} \quad m \times 1 \quad m \times 1 \quad m \times 1 \quad m \times 1 \quad m \times 1$$

is a codeword of $\mathcal{C}.$

Proposed coding scheme: Correction capabilities

Correction Capability of Proposed Code

	error	erasure
block	au columns in error	ho columns erased
symbol	artheta symbols in error	ϱ symbols erased

Correction Capability of Proposed Code

	error	erasure
block	au columns in error	ho columns erased
symbol	artheta symbols in error	ϱ symbols erased

Theorem: There exists a decoder for the code \mathbb{C} that correctly recovers the transmitted array in the presence of the above error and erasure types (which may occur simultaneously), whenever

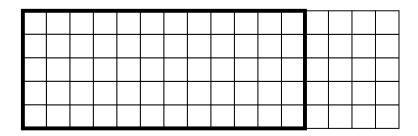
Correction Capability of Proposed Code

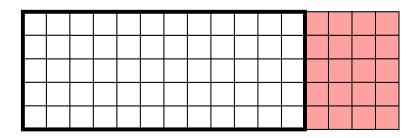
	error	erasure
block	au columns in error	ho columns erased
symbol	artheta symbols in error	ϱ symbols erased

Theorem: There exists a decoder for the code \mathbb{C} that correctly recovers the transmitted array in the presence of the above error and erasure types (which may occur simultaneously), whenever

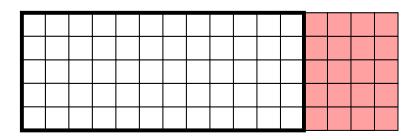
Surprisingly simple conditions!

Proposed coding scheme: Advantages



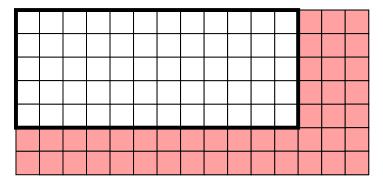


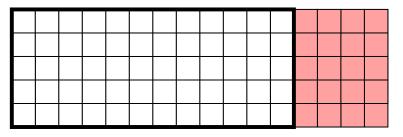
• Multiplication by H_i^{-1} is like a rate-1 inner code.



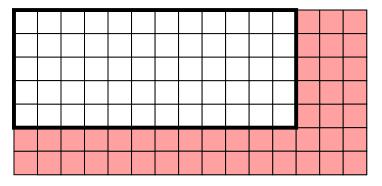
• Multiplication by H_i^{-1} is like a rate-1 inner code.

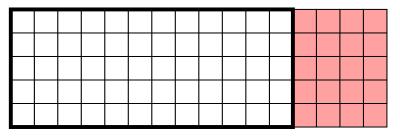
 \Rightarrow The redundancy of the coding scheme can be independent of n.





Overall, we want to handle ϑ symbol errors and ϱ symbol erasures.





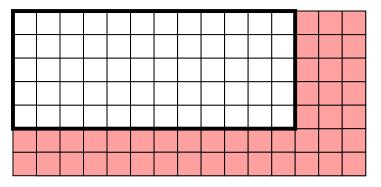
Overall, we want to handle ϑ symbol errors and ϱ symbol erasures.

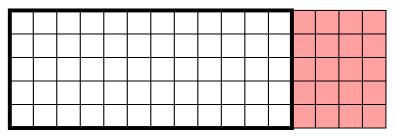
Product code:

code C_2 needs to be designed such that it can handle the worst case where ϑ symbol errors and ϱ symbol erasures appear all in the same column.

Proposed code:

"same redundancy symbols" can be used to handle overall ϑ symbol errors and ϱ symbol erasures.





Overall, we want to handle ϑ symbol errors and ϱ symbol erasures.

Product code:

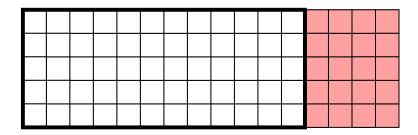
code C_2 needs to be designed such that it can handle the worst case where ϑ symbol errors and ϱ symbol erasures appear all in the same column.

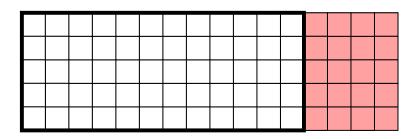
Proposed code:

"same redundancy symbols" can be used to handle overall ϑ symbol errors and ϱ symbol erasures.

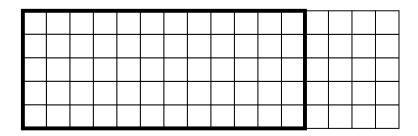
 \Rightarrow "Price" that is paid for this:

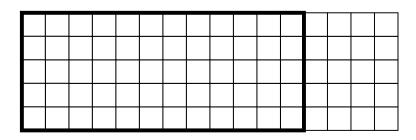
$$2\tau + \rho \le d - 2$$
 vs.
$$2\tau + \rho \le d - 1$$



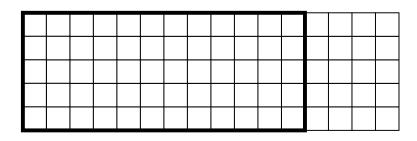


 One can identify a range of code parameters for C for which the resulting redundancy improves upon the best known. (To the best of our knowledge.)

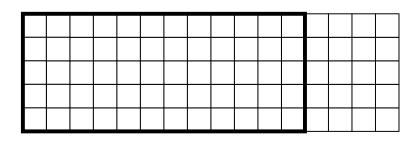




 One can devise efficient decoders for combinations of block and symbol errors and erasures most relevant in practical applications.



- One can devise efficient decoders for combinations of block and symbol errors and erasures most relevant in practical applications.
- In particular, these decoders are more efficient than a corresponding decoder for a suitably chosen Reed–Solomon code of length mn over F, assuming such a Reed–Solomon code exists in the first place.

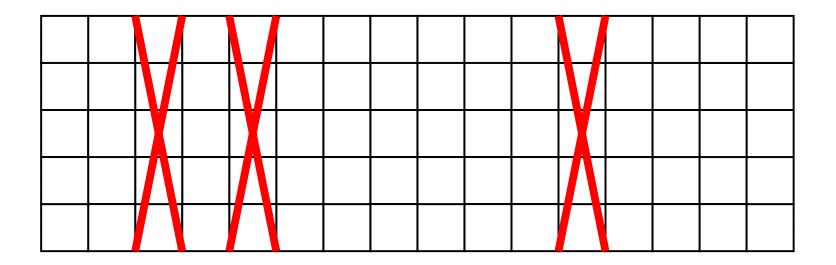


- One can devise efficient decoders for combinations of block and symbol errors and erasures most relevant in practical applications.
- In particular, these decoders are more efficient than a corresponding decoder for a suitably chosen Reed–Solomon code of length mn over F, assuming such a Reed–Solomon code exists in the first place.
- Finding efficient decoders for the general case is still an open problem.

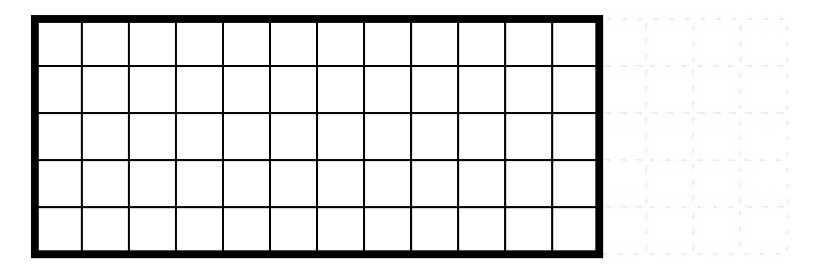
Decoding

A Simplified Setup

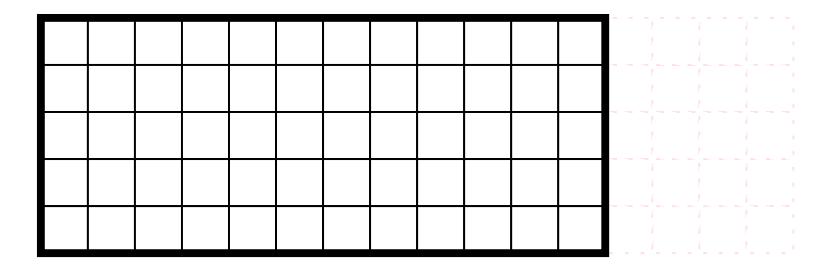
A Simplified Setup: Error Model

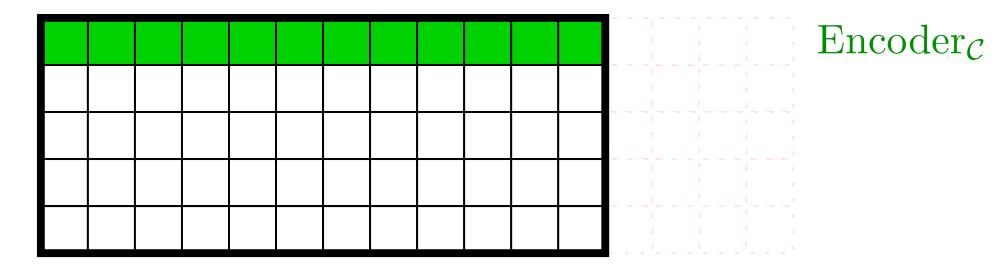


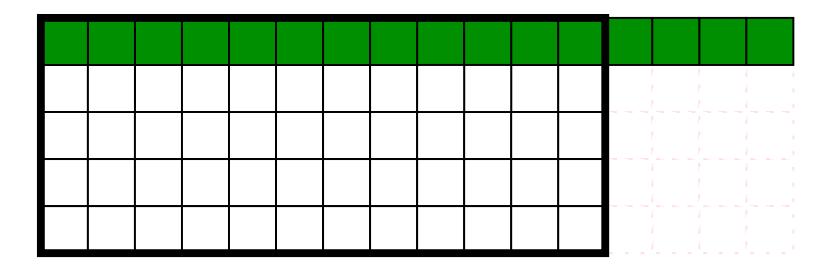
- Encoded array has size $m \times n$.
- Up to *t* burst errors happen.

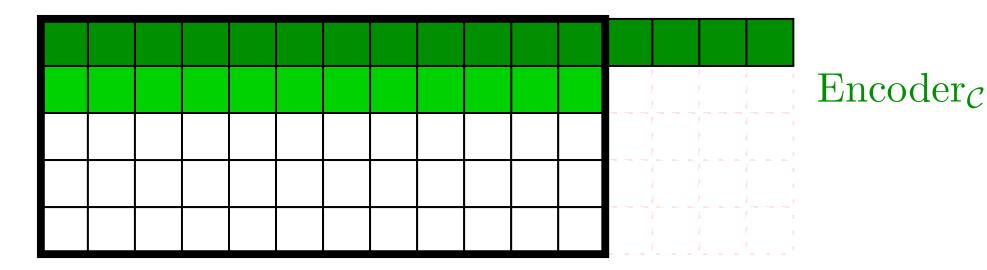


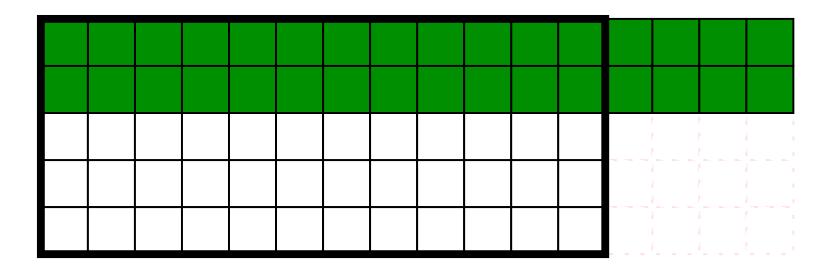
 $m \times n'$ array of information symbols

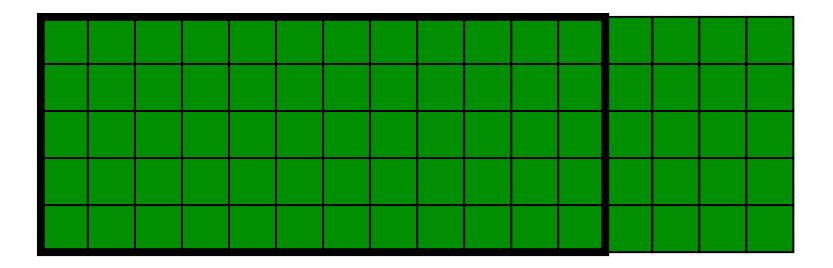


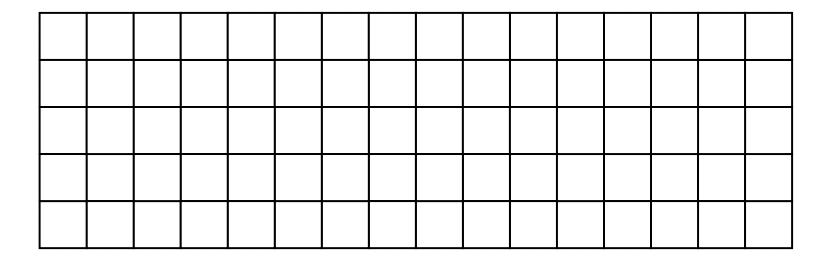


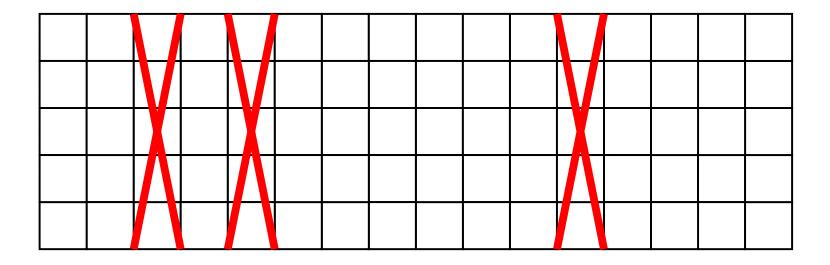


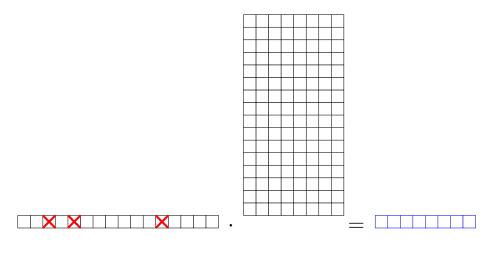






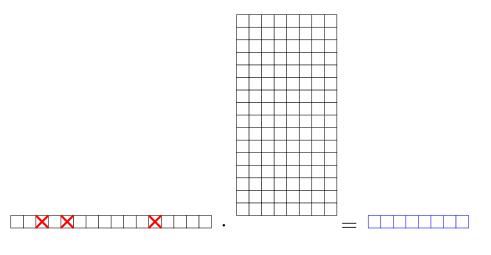






E · $H^{\mathsf{T}} = S$

We consider first the case m = 1.

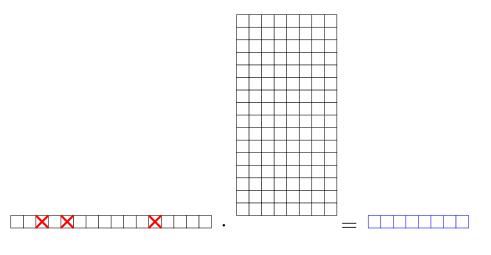


E · $H^{\mathsf{T}} = S$

We consider first the case m = 1.

A necessary condition for being able to correct (up to) t errors:

#error patterns that we want to correct \leq #different syndromes.

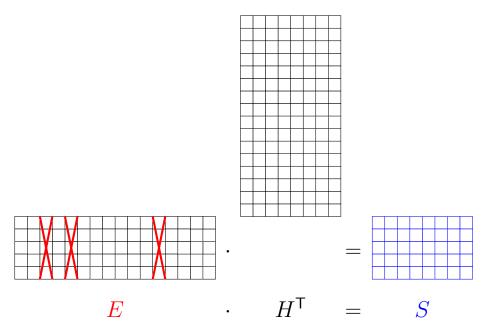


E · $H^{\mathsf{T}} = S$

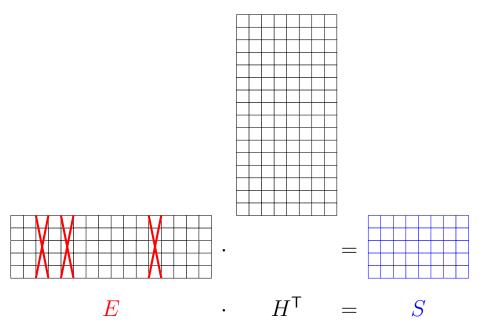
We consider first the case m = 1.

A necessary condition for being able to correct (up to) t errors:

$$\binom{n}{t} \cdot q^t \quad \lesssim \quad q^{n-k}$$



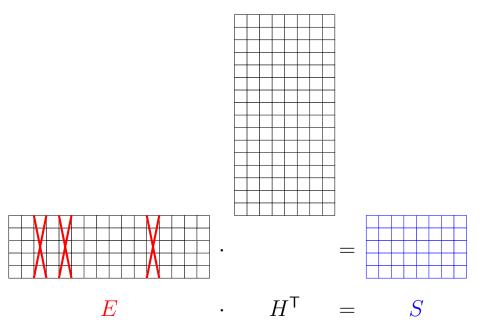
Now we consider the case of general m.



Now we consider the case of general m.

A necessary condition for being able to correct (up to) t burst errors:

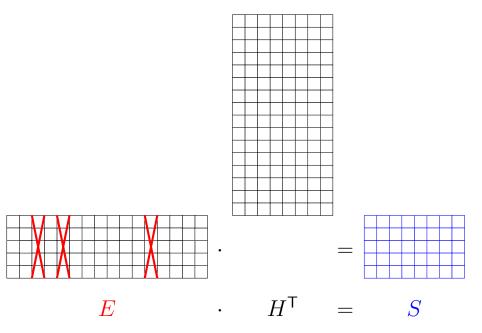
#error patterns that we want to correct \leq #different syndromes.



Now we consider the case of general m.

A necessary condition for being able to correct (up to) t burst errors:

$$\binom{n}{t} \cdot q^{mt} \quad \lesssim \quad q^{m(n-k)}$$

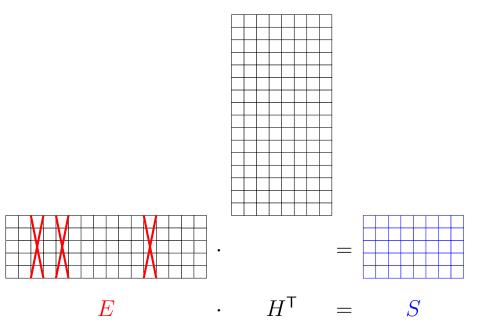


Now we consider the case of general m.

A necessary condition for being able to correct (up to) t burst errors:

$$t \leq \frac{m}{m+1} \cdot (n-k).$$

(Assumption: $n \approx q$ and t small.)

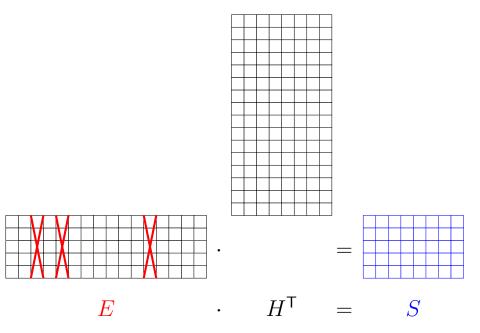


Now we consider the case of general m.

A necessary condition for being able to correct (up to) t burst errors:

$$t \leq \frac{1}{2} \cdot \left(n - k + \operatorname{rank}(E) - 1\right)$$

(Assumption: MDS code.)

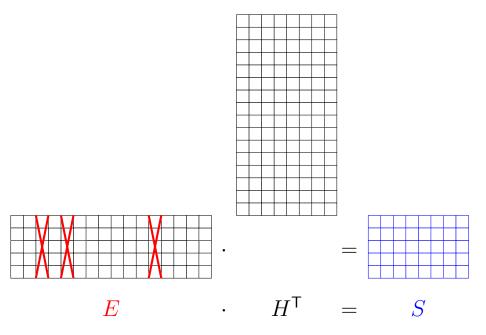


Now we consider the case of general m.

A necessary condition for being able to correct (up to) t burst errors:

$$t \leq \frac{1}{2} \cdot \left(n - k + \operatorname{rank}(E) - 1\right) = \begin{cases} \frac{1}{2} \cdot \left(n - k\right) & (\operatorname{rank}(E) = 1) \\ n - k - 1 & (\operatorname{rank}(E) = t) \end{cases}$$

(Assumption: C is an MDS code.)



Now we consider the case of general m.

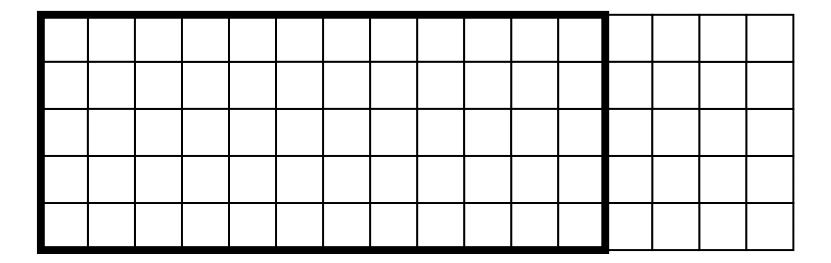
Remarkable:

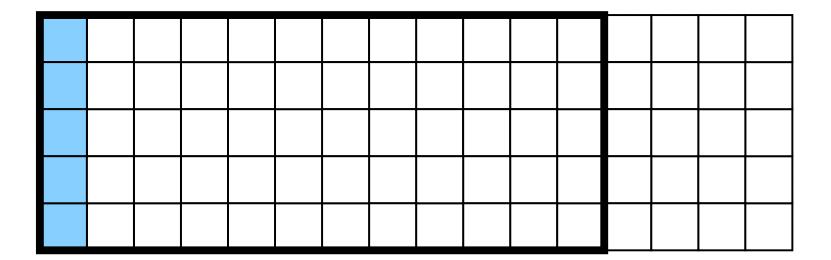
Decoding can be done by Gaussian elimination, independently of the chosen code C.

See [Metzner, Kapturowski, 1990] and [Haslach, Vinck, 2000/2001].

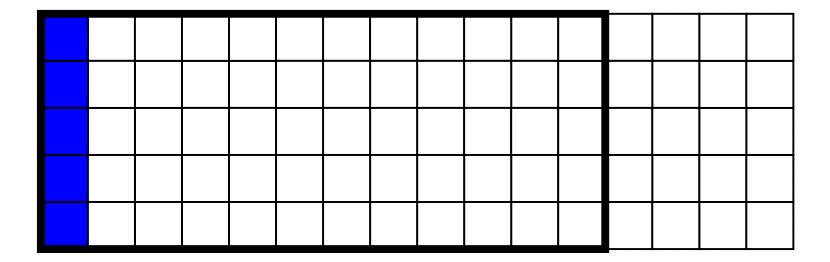
Proposed Coding Scheme: Encoding and Decoding

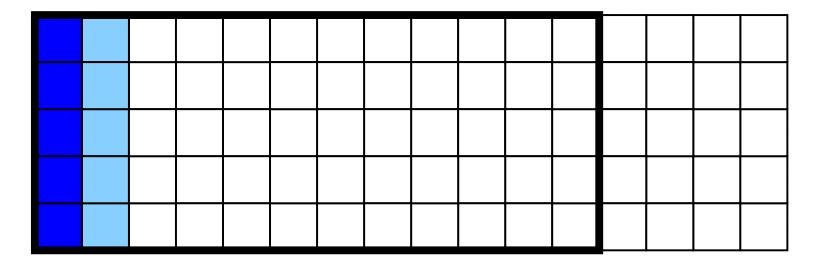
Assume that the rows have already been encoded.



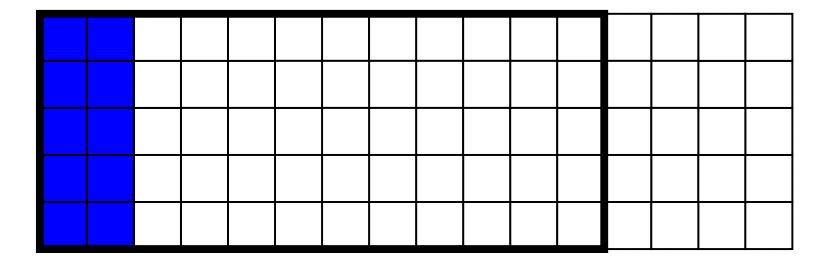


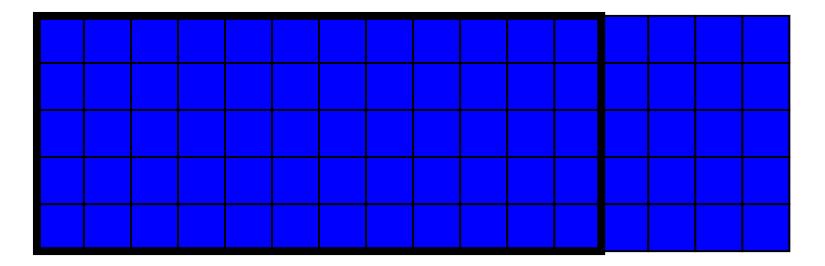
multiply by square matrix H_0^{-1}



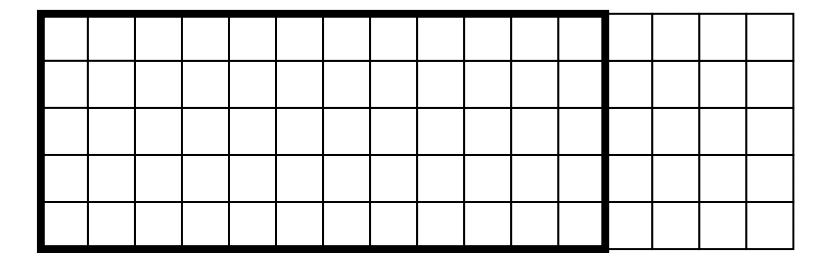


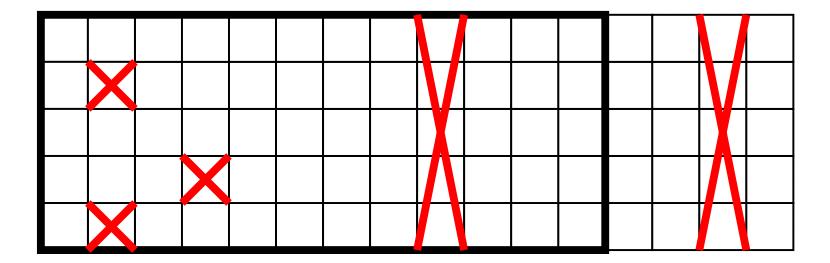
multiply by square matrix H_1^{-1}



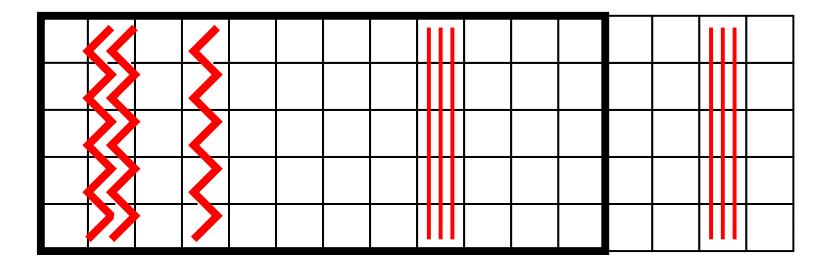


 $m \times n$ array of codeword symbols

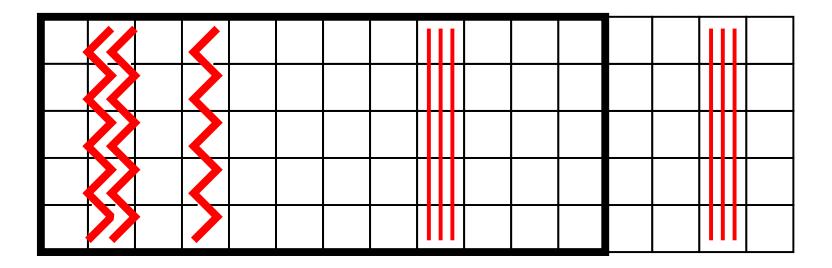




First decoding step: multiply the *i*-th column by H_i .



First decoding step: multiply the *i*-th column by H_i .



Decoder then takes advantage of special structure of burst errors in this modified array.

Conclusions

Conclusions

- Motivation for block and symbol errors / erasures.
- Discussed traditional and novel ECC schemes that can handle such errors / erasures with low complexity and compared their advantages / disadvantages.
- Finding efficient decoders for the general case is still an open problem.
- More details, in particular decoding schemes and comparison with other coding schemes, can be found in the paper available at http://arxiv.org/abs/1302.1931

Original Talk Topic

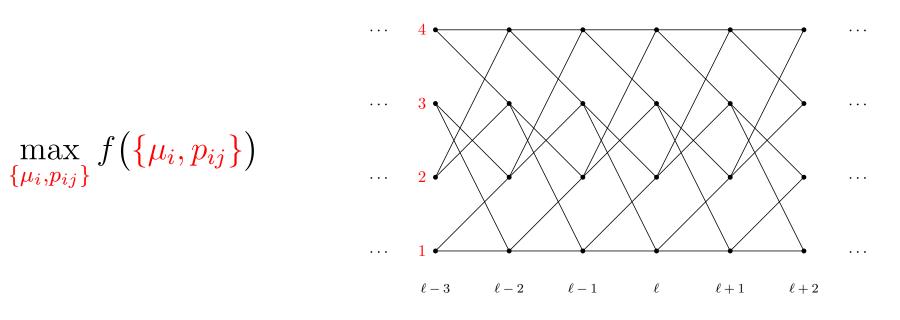
Connections between Techniques for Analyzing Finite State Channels and Techniques for Analyzing Graphical Models

- Theorems 26 and Corollary 27 in
 - P. O. Vontobel, "The Bethe permanent of a non-negative matrix," IEEE Trans. Inf. Theory, vol. 59, no. 3, pp. 1866–1901, Mar. 2013.

Theorem 8 and Corollary 9 in

H. D. Pfister and P. O. Vontobel, "On the relevance of graph covers and zeta functions for the analysis of SPA decoding of cycle codes," Proc. ISIT 2013.

Optimization Problem



$$f(\{\mu_i, p_{ij}\}) = -\sum_{(i,j)\in\mathcal{B}} \mu_i \cdot p_{ij} \cdot \log(p_{ij})$$

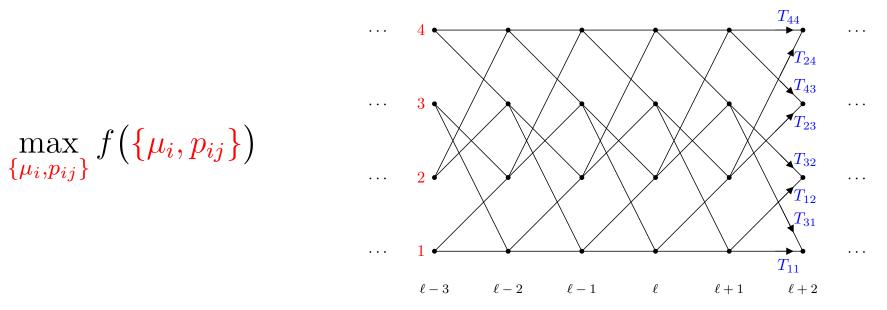
 \mathcal{S} : state alphabet

B : branch alphabet

 $\{\mu_i\}$: stationary state probabilities

 $\{p_{ij}\}$: transition probabilities

Optimization Problem



$$f(\{\mu_i, p_{ij}\}) = -\sum_{(i,j)\in\mathcal{B}} \mu_i \cdot p_{ij} \cdot \log(p_{ij}) + \sum_{(i,j)\in\mathcal{B}} \mu_i \cdot p_{ij} \cdot T_{ij}$$

 \mathcal{S} : state alphabet

B : branch alphabet

 $\{\mu_i\}$: stationary state probabilities

 $\{p_{ij}\}$: transition probabilities

 $\{T_{ij}\}$: branch weights

Solution of this Optimization Problem

Definitions:

• "Noisy adjacency matrix" A with $A_{ij} = \begin{cases} e^{T_{ij}} & \text{if } (i,j) \in \mathcal{B} \\ 0 & \text{otherwise} \end{cases}$.

- Let ρ be the maximal (real) eigenvalue of A.
- Let β^{T} and γ be the corresponding left and right eigenvectors.

Then:

$$p_{ij}^* = \frac{\gamma_j}{\gamma_i} \cdot \frac{A_{ij}}{\rho} \quad (i,j) \in \mathcal{B},$$
$$\mu_i^* \propto \beta_i \cdot \gamma_i \qquad i \in \mathcal{S},$$

$$f\left(\left\{\mu_i^*, p_{ij}^*\right\}\right) = \log\left(\rho\right).$$

This and similar problems were solved in, e.g., [Justesen, Høholdt, 1984], [Khayrallah, Neuhoff, 1996], [V., Kavčić, Arnold, Loeliger, 2008].

http://arxiv.org/abs/1302.1931

Thank you!