Duality for Simple Multiple Access Networks

Iwan Duursma

Department of Mathematics and Coordinated Science Laboratory
U of Illinois at Urbana-Champaign

DIMACS Workshop on Network Coding
December 15-17, 2015

Outline

1 - Reliability and Security

2 - Efficient repair

3 - Constrained codes and Duality

- Tail-biting trellises
- Simple multiple access networks

1 - Reliability and Security

High rank submatrices protect against erasures and eavesdroppers

Details

Erasure channel

Encoding using G_C yields a vector with entropy $H(C)$.
For vectors observed outside the erased positions $\mathcal{E} \subset [n]$,

$$H(C) \;=\; H(C|\mathcal{E}) \;\text{(information gain)}\; + I(C;\mathcal{E}) \;\text{(equivocation)}$$

Wiretep channel II

Decoding using G_D^T distinguishes vectors with entropy $H(D)$.
For vectors observed in the eavesdropped positions $\mathcal{E} \subset [n]$,

$$H(D) \;=\; I(D;\mathcal{E}) \;\text{(information gain)}\; + H(D|\mathcal{E}) \;\text{(equivocation)}$$

$H(C|\mathcal{E}), H(D|\mathcal{E}) = \text{rank}\Big($  $\Big)$, for $\mathcal{E} =$ 

Protection against erasures AND eavesdroppers

Nested codes

Combine encoding via G_C with decoding via G_D^T

- Transmission rate reduces from $H(C)$ to $H(C|D^\perp)$ in return for a higher threshold for the eavesdropper.
- We may assume wlog that $D^\perp \subset C$ (nested codes)

For vectors observed outside $\mathcal{E} \subset [n]$ (legitimate receiver),

$$\begin{aligned} H(C|D^\perp) &= H(C) - H(D^\perp) \\ &= H(C|\mathcal{E}) - H(D^\perp|\mathcal{E}) \text{ (information gain)} \\ &\quad + I(C;\mathcal{E}) - I(D^\perp;\mathcal{E}) \text{ (equivocation)} \end{aligned}$$

Main example (Reed-Solomon)

$$G_{RS} = \left[\begin{array}{c|c|c|c|c|c|ccc} 1 & 1 & 1 & 1 & 1 & 1 & \cdots & \cdots & \cdots \\ x & y & z & u & v & w & & & \\ x^2 & y^2 & z^2 & u^2 & v^2 & w^2 & & & \\ x^3 & y^3 & z^3 & u^3 & v^3 & w^3 & & & \\ x^4 & y^4 & z^4 & u^4 & v^4 & w^4 & & & \\ x^5 & y^5 & z^5 & u^5 & v^5 & w^5 & \cdots & \cdots & \cdots \end{array}\right]$$

$B = \text{rank}\left(\right.$  $\left. \right) = 6.$

2 - Efficient repair

Reed-Solomon codes provide maximum protection of a message against erasures.

() is full rank

However repair using RS-codes is inefficient. For RS-codes,

repair bandwith $=$ rank ( .)

Other codes are more suitable when erasure repair is important (e.g. in distributed storage).

MSR construction (Rashmi-Shah-Kumar 2010)

$$G_{MSR} = \left[\begin{array}{cc|cc|cc|ccc} 1 & 0 & 1 & 0 & 1 & 0 & \cdots & \cdots & \cdots \\ x & 1 & y & 1 & z & 1 & & & \\ 0 & x & 0 & y & 0 & z & & & \\ x^2 & 0 & y^2 & 0 & z^2 & 0 & & & \\ x^3 & x^2 & y^3 & y^2 & z^3 & z^2 & & & \\ 0 & x^3 & 0 & y^3 & 0 & z^3 & \cdots & \cdots & \cdots \end{array}\right]$$

$B = \text{rank}\Big($  $\Big) = 6. \qquad (k = 3, \alpha = 2)$

$$\gamma = \text{repair bandwith} = 4 \qquad (d = 4, \beta = 1)$$

(modify if char $\neq 2$)

MBR construction (Rashmi-Shah-Kumar 2010)

$$G_{MBR} = \left[\begin{array}{ccc|ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 & \cdots & \cdots & \cdots \\ x & 1 & 0 & y & 1 & 0 & & & \\ 0 & x & 0 & 0 & y & 0 & & & \\ x & 1 & 0 & y & 1 & 0 & & & \\ x^2 & 2x & 1 & y^2 & 2y & 1 & & & \\ 0 & x^2 & x & 0 & y^2 & y & \cdots & \cdots & \cdots \end{array}\right]$$

$B = \text{rank}\Bigg($  $\Bigg) = 5. \qquad (k = 2, \alpha = 3)$

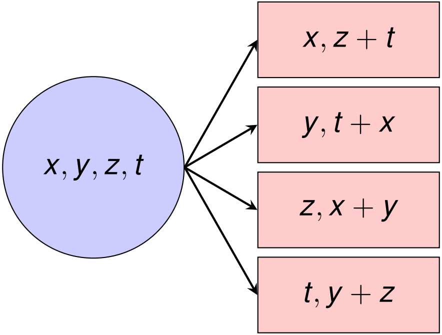
$\gamma = \text{repair bandwith} = 3 \qquad (d = 3, \beta = 1)$

Storage vs bandwith trade-off

- MSR minimizes storage per disk.
- MBR minimizes repair bandwith.
- For exact repair solutions in between MBR and MSR, the optimal trade-offs are an open problem.
- Case $n = k + 1 = d + 1$ is solved

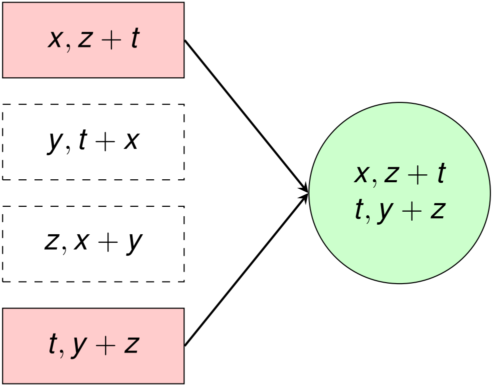
  Tian; Sasidharan, Senthoor, Kumar; D;
  Tian, Sasidharan, Aggarwal, Vaishampayan, Kumar;
  Mohajer, Tandon; Prakash, Krishnan; D'

Storing four bits on four disks



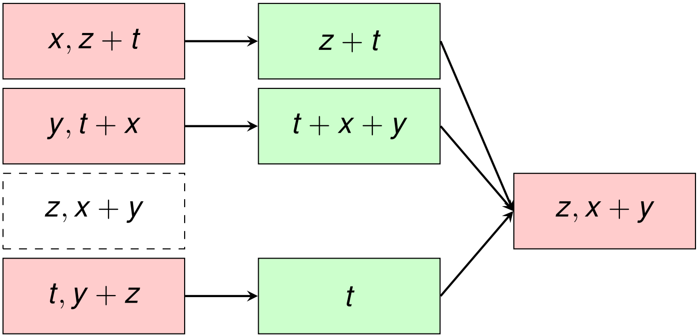
$B = 4 \qquad n = 4$

Reading four bits from any two disks



$\alpha = 2 \qquad k = 2$

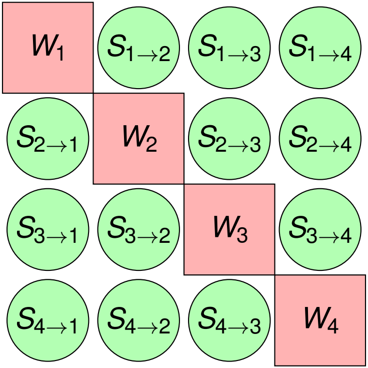
Disk repair with help form any three disks



$\beta = 1 \qquad d = 3$

Repair matrix

The repair matrix summarizes storage and repair for a regenerating code.



$$
\begin{aligned}
W_i &= \text{data stored at node } i \\
S_{i\to j} &= \text{helper information from node } i \text{ to node } j
\end{aligned}
$$

[D - arxiv 2014]

Theorem 1

Let $B_q = H(W_1) + \cdots + H(W_q) + \sum H(S_{i \to j})$, such that $B \leq B_q$.

Let $q, q_1, \ldots, q_{m-2}, r, s > 0$ such that (explicit condition). Then

$$mB \leq B_q + \sum_{i=1}^{m-2} B_{q_i} + B_{r+s} - rs\beta.$$

Theorem 2

Let $B_q = H(W_1) + \cdots + H(W_q) + \sum H(S_{M \to L})$, such that $B \leq B_q$.

For each (M, L), let $\ell = |L|$, $m = |M|$, and let $r \geq \ell$. Then

$$B + \sum_{(M,L)} \ell B \leq B_q + \sum_{(M,L)} (B_{r+m-1} + (\ell - 1)(B_{r+m-2} - \beta)).$$

[D arXiv 2015]

Theorem 3

For any set of parameters (n, k, d), and for $0 \leq \ell \leq k$, $0 \leq v$,

$$\binom{v+2}{2} B \leq \binom{v+1}{2} B_k + (v+1) B_{k-\ell} - v \binom{\ell}{2} \beta.$$

Independently (special cases)

Prakash-Krishnan, arXiv 2015
Mohajer-Tandon, ITA/ISIT 2015a, ISIT2015b.

3 - Constrained codes

David Forney (Talk at Allerton '97)

Does the Golay code have a generator matrix of the form

$$
\begin{bmatrix}
\ast\ast & \ast\ast & \ast\ast & \ast\ast & \ast\ast & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\
00 & \ast\ast & \ast\ast & \ast\ast & \ast\ast & \ast\ast & 00 & 00 & 00 & 00 & 00 & 00 \\
00 & 00 & \ast\ast & \ast\ast & \ast\ast & \ast\ast & \ast\ast & 00 & 00 & 00 & 00 & 00 \\
00 & 00 & 00 & \ast\ast & \ast\ast & \ast\ast & \ast\ast & \ast\ast & 00 & 00 & 00 & 00 \\
00 & 00 & 00 & 00 & \ast\ast & \ast\ast & \ast\ast & \ast\ast & \ast\ast & 00 & 00 & 00 \\
00 & 00 & 00 & 00 & 00 & \ast\ast & \ast\ast & \ast\ast & \ast\ast & \ast\ast & 00 & 00 \\
00 & 00 & 00 & 00 & 00 & 00 & \ast\ast & \ast\ast & \ast\ast & \ast\ast & \ast\ast & 00 \\
00 & 00 & 00 & 00 & 00 & 00 & 00 & \ast\ast & \ast\ast & \ast\ast & \ast\ast & \ast\ast \\
\ast\ast & 00 & 00 & 00 & 00 & 00 & 00 & 00 & \ast\ast & \ast\ast & \ast\ast & \ast\ast \\
\ast\ast & \ast\ast & 00 & 00 & 00 & 00 & 00 & 00 & 00 & \ast\ast & \ast\ast & \ast\ast \\
\ast\ast & \ast\ast & \ast\ast & 00 & 00 & 00 & 00 & 00 & 00 & 00 & \ast\ast & \ast\ast \\
\ast\ast & \ast\ast & \ast\ast & \ast\ast & 00 & 00 & 00 & 00 & 00 & 00 & 00 & \ast\ast
\end{bmatrix}
$$

Answer: Yes (Calderbank-Forney-Vardy 1999)

Characteristic matrices (Koetter-Vardy 2003)

A set of characteristic generators for the row space row G is a subset of n vectors such that

1) Spans of vectors start and end in distinct positions, and
2) The sum of the spanlengths of the vectors is minimal.

A square matrix is called a characteristic matrix for G if its rows form a set of characteristic generators.

Example

$$X = \left[\begin{array}{ccccc} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ \hline 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{array}\right] \qquad Y = \left[\begin{array}{ccccc} 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ \hline 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{array}\right]$$

Dual characteristic matrices

Question

Under what conditions is a pair of characteristic matrices in duality, i.e. when does a pair define dual trellises?

Conjecture (KV 2003)

For a choice of lexicographically first characteristic generators for G and for a matching choice of lexicographically first characteristic generators for H, the obtained tail-biting trellises are in duality.

(Gleussen-Larssing and Weaver 2011)

Counterexample to the conjecture.

Characterization of dual characteristic matrices in terms of local duality of trellises

(GLW 2011)

Example

$$X = \left[\begin{array}{cccc} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{array}\right] \qquad Y = \left[\begin{array}{cccc} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ \hline 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{array}\right]$$

$$X' = \left[\begin{array}{cccc} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{array}\right] \qquad Y' = \left[\begin{array}{cccc} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ \hline 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{array}\right]$$

Conjecture: $X \sim Y$. Local duality: $X \sim Y'$ and $X' \sim Y$.

-Adjusted- Conjecture holds (D 2015)

We define unique reduced characteristic matrices and show

Theorem

Reduced characteristic matrices are in duality.

Corollary

The KV conjecture holds if the characteristic generators for G are lexicographically ordered in a forward direction and the characteristic generators for H are lexicographically ordered in a reverse direction.

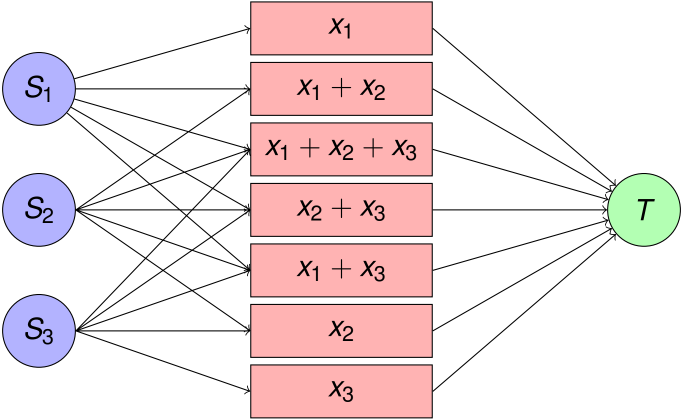
Furthermore, an explicit duality is given by

Theorem

A pair of characteristic matrices X and Y, with maximal orthogonal row spaces, is in duality if and only if X and Y have orthogonal column spaces.

Simple Multiple Access Network

Sources S_i transmit at rates r_i to a unique receiver T via a layer of n intermediate nodes. T observes $(c_1, c_2, \ldots, c_n) \in C$.



Shown is $C = [7, 3, 4]$ simplex code.

Related problems

Opportunistic data exchange

El Rouayheb, Sprintson, Sadeghi, ITW 2010
On coding for cooperative data exchange

Sensor networks

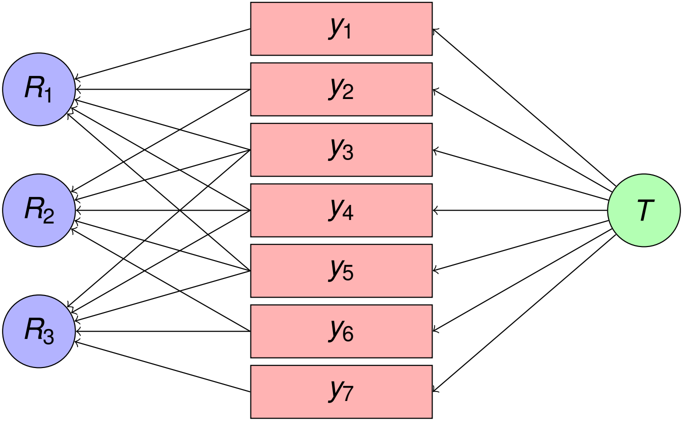
Dau, Song, Dong, Yuen, ISIT 2013
Balanced Sparsest generator matrices for MDS codes

Error-correction in networks

Dikaliotis, Ho, Jaggi, Vyetrenko, Yao, Effros, Kliewer, Erez, IT-2011
Multiple access network information-flow and correction codes

Dual version (same network, arrows reversed)

Receivers R_i request data at rates r_i from a unique source T via a layer of n intermediate nodes. T uploads $(y_1, y_2, \ldots, y_n)$.



e.g. R_1 requests x_1, to be obtained from y_1, y_2, y_3, y_4, y_5.

SMAN (reliable multiple access $(S_1, S_2, S_3) \longrightarrow T$)

$$\begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \begin{bmatrix} x & x & x & x & x & 0 & 0 \\ 0 & x & x & x & x & x & 0 \\ 0 & 0 & x & x & x & x & x \end{bmatrix} = \begin{bmatrix} c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 \end{bmatrix}$$

Dual version (secure broadcast $T \longrightarrow (R_1, R_2, R_3)$)

$$\begin{bmatrix} y_1 & y_2 & y_3 & y_4 & y_5 & y_6 & y_7 \end{bmatrix} \begin{bmatrix} x & x & x & x & x & 0 & 0 \\ 0 & x & x & x & x & x & 0 \\ 0 & 0 & x & x & x & x & x \end{bmatrix}^T = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix}$$

Theorem

For the same three-layer network,

A SMAN can transmit at rates $(r_1, \ldots, r_k)$ tolerating z erasures

if and only if

The dual version can reach receivers at rates $(r_1, \ldots, r_k)$ tolerating z eavesdroppers.

Distributed Reed-Solomon codes

Given a generator matrix of the form

$$\begin{bmatrix} x & 0 & 0 & x & x & x & x & 0 & 0 & x \\ x & 0 & 0 & x & x & x & x & 0 & 0 & x \\ 0 & x & 0 & x & x & 0 & 0 & x & x & x \\ 0 & x & 0 & x & x & 0 & 0 & x & x & x \\ 0 & 0 & x & 0 & 0 & x & x & x & x & x \\ 0 & 0 & x & 0 & 0 & x & x & x & x & x \end{bmatrix}$$

can the nonzero entries be chosen such that the matrix represents a Reed-Solomon code?

Theorem (Halbawi, Ho, Yao, D ISIT 2014)

For any rate vector in the capacity region of a three-source SMAN, we can construct a distributed Reed-Solomon code.

Why is this difficult?

Question (`http://math.stackexchange.com`) 10/31/12

Dimension of Intersection of three vector spaces satisfying specific postulates. Let A, B, C, be subspaces of V such that

$$\dim A = \dim A', \dim B = \dim B', \dim C = \dim C'$$
$$\dim A \cap B = \dim A' \cap B',\ \dim C \cap B = \dim C' \cap B',\ \dim A \cap C = \dim A' \cap C'$$
$$\dim A + B + C = \dim A' + B' + C'$$

Prove that $\dim A \cap B \cap C = \dim A' \cap B' \cap C'$. Thanks.

Answer

The result stated is false, so you need not bother to try and prove it.
MvL

Reply

Thank MvL. This is a great answer.

The next 15 months

Extend SMAN and its dual version to

multiple sources AND multiple receivers

reliability AND security

As well as many other things

distributed storage, matroids, . . .

THANK YOU.