On finite geometry codes with locality

Pan Tan [1] Zhengchun Zhou [1]
Vladimir Sidorenko [21] Udaya Parampalli [32]

[1]School of Mathematics
Southwest Jiaotong University, China

[2]Institute for Communications Engineering
Technical University of Munich, Germany

[3]School of Computing and Information Systems
The University of Melbourne, Australia

JWCC, Kühtai, Austria, March, 11-14, 2019

[1]V. Sidorenko is on leave from Institute for Information Transmission Problems, Russian Academy of Sciences. His work is supported by the Russian Government (Contract No 14.W03.31.0019).

[2]U. Parampalli is supported in part by the Australian Research Councils Discovery under Grant DP150104473 and in part by the University of Melbourne's 2014 International Research and Research Training Fund.

Motivation

Codes with locality or Locally Repairable Codes (LRCs) allow to recover one erased code symbol using only a few other symbols.

LRCs can be applied in

- distributed storage systems for repairing multiple disk failures
- and also for management of hot data.

Outline

1. Codes and locality
2. Connection with majority logic decoding
3. Finite geometry
4. New codes

Outline

1. Codes and locality
2. Connection with majority logic decoding
3. Finite geometry
4. New codes

Codes

A code $\mathcal{C}$ is a set of codewords $c = (c_1, c_2, \dots, c_n)$ over a finite field $\mathbb{F}_q$.

Code distance d is the minimum Hamming distance between different codewords.

The code $\mathcal{C}$ is *linear* $[n, k]$-code if it is $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$.

Generator matrix G of a linear $[n, k]$-code is a $k \times n$ matrix over $\mathbb{F}_q$, such that rows of G form a basis of $\mathcal{C}$.

Encoding: $c = uG$, where u is an information vector of length k.

Systematic encoding using systematic $G = (I_k, P)$, then $c = uG = (u, p)$.

A parity check matrix is $H = (-P^T, I_{n-k})$ and for all $c \in \mathcal{C}$ holds $cH^T = 0$.

Codes with locality

A code symbol c_i has *repair locality* r if it can be recovered by accessing at most r other symbols. The set of indexes of those symbols is called repair set $\mathcal{R}$. E.g. for $r = 2$ and $\mathcal{R} = \{2, 3\}$, $i = 1$:

$$c_1 = c_2 + c_3.$$

A linear code has *information locality* r if every information symbol has locality r. A single erasure can be recovered. What if more erasures?

A code symbol c_i has $(r,\ t)$-*locality* if there exist t disjoint repair sets $\mathcal{R}_j$ for c_i, each containing at most r symbols. E.g. for $r = 2$, $t = 2$, and $\mathcal{R}_1 = \{2, 3\}$, $\mathcal{R}_2 = \{4, 5\}$:

$$\begin{aligned} c_1 &= c_2 + c_3, \\ c_1 &= c_4 + c_5. \end{aligned} \tag{1}$$

A linear code has *information locality* (r, t) if every information symbol has locality (r, t). This code can correct up to t erasures and hence

Upper bound for the code distance

Lemma

The distance d of $[n,\ k]$ code with information $(r,\ t)$-locality satisfies

$$d \geq t + 1.$$

Outline

1. Codes and locality
2. Connection with majority logic decoding
3. Finite geometry
4. New codes

Connection with majority logic decoding

Orthogonal parity checks for c_1, $t = 2$ checks:

$$\begin{aligned} c_1 &= c_2 + c_3, \\ c_1 &= c_4 + c_5, \\ c_1 &= c_1. \end{aligned} \tag{2}$$

Symbol can be corrected by *majority logic decoder* if there were up to t erasures or up to $t/2$ errors.

If every (information) symbol has at least t orthogonal parity checks then the code has distance $d \geq t + 1$. The code corrects up to t erasures or up to $t/2$ errors by majority logic decoder.

Some known codes with majority logic decoding: Reed-Muller codes, codes based on finite geometries.

We will use *finite geometries* to design codes with locality.

Upper bound for the code distance

To simplify decoding we require that each repair set contains a single parity symbol only.

Lemma ([RPDV16])

Let $\mathcal{C}$ be an $[n, k]$ code with information (r, t)-locality such that each repair set contains a single parity symbol. Then the code distance is bounded by

$$d \leq n - k - \left\lceil \frac{kt}{r} \right\rceil + t + 1. \tag{3}$$

Can we reach this bound?

[RPDV16] Rawat, A.S., Papailiopoulos, D.S., Dimakis, A.G., Vishwanath, S.: Locality and availability in distributed storage. IEEE Transactions on Information Theory 62(8), 4481–4493, 2016.

Outline

1. Codes and locality
2. Connection with majority logic decoding
3. Finite geometry
4. New codes

Partial geometry

Definition ([CD96])

A (finite) *partial geometry* is an incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{L}, I)$ in which $\mathcal{P}$ is a set of *points* p, $\mathcal{L}$ is a set of *lines* ℓ and I is a symmetric point-line incidence relation satisfying the following axioms:

1. Each point p is incident with $u+1$ lines$(u \geq 1)$, and two distinct points are incident with at most one line.
2. Each line ℓ is incident with $s+1$ points$(s \geq 1)$, and two distinct lines are incident with at most one point.
3. Given a point p not incident with a line ℓ, there are exactly α lines incident with p and also with some point of ℓ.

Such a partial geometry will be denoted by $\mathrm{PG}(s+1,\ u+1,\ \alpha)$. Parameter α is called *connection number*.

[CD96] Colbourn, C.J., Dinitz, J.H.: Handbook of combinatorial designs. CRC Press (1996).

Fano plane

Well known examples of partial geometries are Euclidean and projective geometries over finite fields.
The Fano plane [F1892] is the finite projective geometry with the smallest number of points and lines: 7 points and 7 lines, with 3 points on every line and 3 lines through every point.

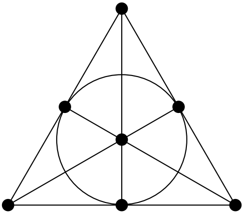


Figure 1: Partial geometry PG(3,3,3)

[F1892] Gino Fano, (1892), "Sui postulati fondamentali della geometria proiettiva", Giornale di Matematiche, 30: 106–132.

New partial geometry [DLLB2015]

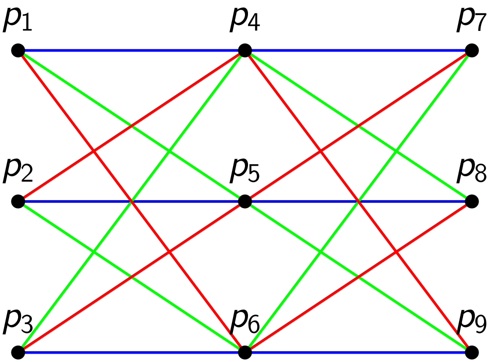


Figure 2: Partial geometry PG(3,3,2)

[DLLB2015] Qiuju Diao,Juane Li, Shu Lin, Ian Blake, New Classes of Partial Geometries and Their Associated LDPC Codes, arXiv: 1503.06900v1 [cs.IT] 24 Mar 2015

Number of points and lines

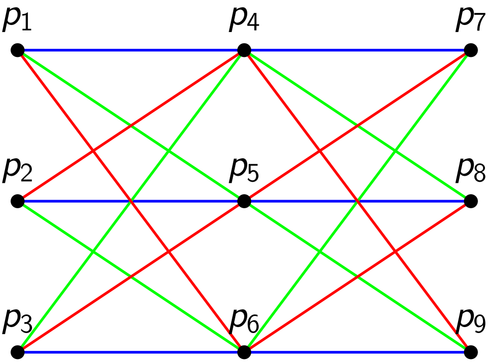
Let $P = |\mathcal{P}|$ and $L = |\mathcal{L}|$, then [CD96]

$$P = \frac{(s+1)(su+\alpha)}{\alpha}, \quad L = \frac{(u+1)(su+\alpha)}{\alpha}. \tag{4}$$

[CD96] Colbourn, C.J., Dinitz, J.H.: Handbook of combinatorial designs. CRC Press (1996).

Incidence matrix N of PG(3,3,2)

$$
N = \begin{array}{c} \\ \ell_1 \\ \ell_2 \\ \ell_3 \\ \ell_4 \\ \ell_5 \\ \ell_6 \\ \ell_7 \\ \ell_8 \\ \ell_9 \end{array}
\begin{array}{c}
\begin{array}{ccccccccc} p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 & p_9 \end{array} \\
\begin{pmatrix}
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0
\end{pmatrix}
\end{array}. \qquad (5)
$$



N was used as parity check matrix H.

Dual geometry. Some known geometries.

The dual of a partial geometry $\mathrm{PG}(s+1,\ u+1,\ \alpha)$ is obtained by exchanging the set of points and the set of lines, which is also a partial geometry $\mathrm{PG}(u+1,\ s+1,\ \alpha)$ with incidence matrix $N^{\perp} = N^T$.

Up to duality, parameters of some known partial geometries are [CD96]:

Type 0: $s = w,\ u = w^{m-1} - 1,\ \alpha = w$, with $m \geq 2$ and w is a power of prime;

Type 1: $s = 2^h - 2^m,\ u = 2^h - 2^{h-m},\ \alpha = (2^{h-m} - 1)(2^m - 1)$, $1 \leq m \leq h$;

Type 2: $s = 2^h - 1,\ u = (2^h + 1)(2^m - 1),\ \alpha = 2^m - 1$, $1 \leq m \leq h$;

Type 3: $s = 2^{2h-1} - 1,\ u = 2^{2h-1},\ \alpha = 2^{2h-2}$, $1 < h$;

Type 4: $s = 3^{2m} - 1,\ u = (3^{4m} - 1)/2,\ \alpha = (3^{2m} - 1)/2,\ m \geq 1$;

[CD96] Colbourn, C.J., Dinitz, J.H.: Handbook of combinatorial designs. CRC Press (1996).

Outline

1. Codes and locality
2. Connection with majority logic decoding
3. Finite geometry
4. New codes

New codes

Given $L \times P$ incidence matrix N of $\mathrm{PG}(s+1,\ u+1,\ \alpha)$, we define a code $\mathcal{C}_{(s+1,\ u+1,\ \alpha)}$ over $\mathbb{F}_q$ by the following binary systematic generator matrix

$$G = [I_L | N]. \tag{6}$$

Theorem

The q-ary linear code $\mathcal{C}_{(s+1,\ u+1,\ \alpha)}$ over $\mathbb{F}_q$ is an $[n,\ k]$ locally repairable code with information $(r,\ t)$-locality, where $n = L + P$, $k = L$, $r = u+1$, $t = s+1$. The code distance $d = s+2$ reaches the upper bound (3).

Remark: The q-ary code over a field $\mathbb{F}_q$ of characteristic 2, $q = 2^m$, is the interleaving of m binary codes, since both G and H are binary matrices.

Example of a new code

Let N be the incidence matrix of $\mathrm{PG}(3,3,2)$ see (5). Then the code $\mathcal{C}_{(3,3,2)}$ has the parity check matrix $H = (N^T, -I_L)$, defined by (6), as follows:

$$H = \left(\begin{array}{ccccccccc|ccccccccc}
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1
\end{array}\right)$$

and we have $[n = 18,\ k = 9]$ locally recoverable code over $\mathbb{F}_q$ with information $(r = 3,\ t = 3)$-locality and distance $d = 4$.

For the first information symbol the repair relations with a single parity symbol are: $c_1 = c_{10} - c_4 - c_7 = c_{13} - c_6 - c_8 = c_{16} - c_5 - c_9$. Every repair set includes only one parity check symbol.

New optimal codes

Theorem

1. *For partial geometry of Type 0 the code* $\mathcal{C}_{(s+1,\ u+1,\ \alpha)}$ *is* $[n = w^{m-1}(w^{m-1} + w + 1),\ k = w^{2(m-1)},\ d = w + 2]$ *with information* $(r = w^{m-1},\ t = w + 1)$*-locality.*
2. *For Type 1 we get* $[n = 2(2^h + 1)(2^h - 2^{m-1} - 2^{h-m-1} + 1),\ k = (2^h + 1)(2^h - 2^{h-m} + 1),\ d = 2^h - 2^m + 2]$ *code with information* $(r = 2^h - 2^{h-m} + 1,\ t = 2^h - 2^m + 1)$*-locality.*
3. *Type 2:* $[n = 2^{m+2h}(2^h + 1),\ k = 2^{m+2h}(2^h - 2^{h-m} + 1),\ d = 2^h + 1]$ *code with information* $(r = 2^m(2^h - 2^{h-m} + 1),\ t = 2^h)$*-locality.*
4. *Type 3: we get* $[n = 2^{4h} - 1,\ k = (2^{2h-1} + 1)(2^{2h} - 1),\ d = 2^{2h-1} + 1]$ *code with information* $(r = 2^{2h-1} + 1,\ t = 2^{2h-1})$*-locality.*
5. *Type 4:* $[n = \frac{3^{4m}(3^{2m}+1)^2}{2},\ k = \frac{3^{4m}(3^{4m}+1)}{2},\ d = 3^{2m} + 1]$ *code with information* $(r = \frac{3^{4m}+1}{2},\ t = 3^{2m})$*-locality.*

All codes reach the bound (3) *and have rates* $k/n = \frac{1}{1+t/r}$.

Conclusions

- From partial geometries, we constructed a class of q-ary locally recoverable codes (LRC) with new parameters, which are optimal with respect to the upper bound (3).
- New geometries will give new codes.
- Future work: Design efficient decoders correcting more than $d/2$ errors (and erasures) using interleaved structure of the codes.

Thank you!