Electronic Colloquium on Computational Complexity, Report No. 100 (2011)

On the Locality of Codeword Symbols

Parikshit Gopalan
Microsoft Research
parik@microsoft.com

Cheng Huang
Microsoft Research
chengh@microsoft.com

Huseyin Simitci
Microsoft Corporation
huseyins@microsoft.com

Sergey Yekhanin
Microsoft Research
yekhanin@microsoft.com

Abstract

Consider a linear $[n, k, d]_q$ code $\mathcal{C}$. We say that that i-th coordinate of $\mathcal{C}$ has locality r, if the value at this coordinate can be recovered from accessing some other r coordinates of $\mathcal{C}$. Data storage applications require codes with small redundancy, low locality for information coordinates, large distance, and low locality for parity coordinates. In this paper we carry out an in-depth study of the relations between these parameters.

We establish a tight bound for the redundancy $n-k$ in terms of the message length, the distance, and the locality of information coordinates. We refer to codes attaining the bound as optimal. We prove some structure theorems about optimal codes, which are particularly strong for small distances. This gives a fairly complete picture of the tradeoffs between codewords length, worst-case distance and locality of information symbols.

We then consider the locality of parity check symbols and erasure correction beyond worst case distance for optimal codes. Using our structure theorem, we obtain a tight bound for the locality of parity symbols possible in such codes for a broad class of parameter settings. We prove that there is a tradeoff between having good locality for parity checks and the ability to correct erasures beyond the minimum distance.

1 Introduction

Modern large scale distributed storage systems such as data centers store data in a redundant form to ensure reliability against node (e.g., individual machine) failures. The simplest solution here is the straightforward replication of data packets across different nodes. Alternative solution involves erasure coding: the data is partitioned into k information packets. Subsequently, using an erasure code, $n-k$ parity packets are generated and all n packets are stored in different nodes.

Using erasures codes instead of replication may lead to dramatic improvements both in terms of redundancy and reliability. However to realize these improvements one has to address the challenge of maintaining an erasure encoded representation. In particular, when a node storing some packet fails, one has to be able to quickly reconstruct the lost packet in order to keep the data readily available for the users and to maintain the same level of redundancy in the system. We say that a certain packet has *locality* r if it can be recovered from accessing only r other packets. One way to ensure fast reconstruction is to use erasure codes where all packets have low locality $r \ll k$. Having small value of locality is particularly important for information packets.

These considerations lead us to introduce the concept of an (r, d)-*code*, i.e., a linear code of distance d, where all information symbols have locality at most r. Storage system based on (r, d)-codes

ISSN 1433-8092

provide fast recovery of information packets from a single node failure (typical scenario), and ensure that no data is lost even if up to $d-1$ nodes fail simultaneously. One specific class of (r, d)-codes called Pyramid Codes has been considered in [5].

Pyramid codes can be obtained from any systematic Maxmimum Distance Seperable (MDS) codes of distance d, such as Reed Solomon codes. Assume for simplicity that the first parity check symbol is the sum $\sum_{i=1}^{k} x_i$ of the information symbols. Replace this with $\lceil \frac{k}{r} \rceil$ parity checks each of size at most r on disjoint information symbols. It is not hard to see that the resulting code $\mathcal{C}$ has information locality r and distance d, while the redundancy of the code $\mathcal{C}$ is given by

$$n - k = \left\lceil \frac{k}{r} \right\rceil + d - 2. \tag{1}$$

1.1 Our results

In this paper we carry out an in-depth study of the relations between redundancy, erasure-correction and symbol locality in linear codes.

Our first result is a tight bound for the redundancy in terms of the message length, the distance, and the information locality. We show that in any $[n, k, d]_q$ code of information locality r,

$$n - k \geqslant \left\lceil \frac{k}{r} \right\rceil + d - 2. \tag{2}$$

We refer to codes attaining the bound above as optimal. Pyramid codes are one such family of codes. The bound (2) is of particular interest in the case when $r \mid k$, since otherwise one can improve the code by increasing the dimension while maintaining the (r, d)-property and redundancy intact. A closer examination of our lower bound gives a structure theorem for optimal codes when $r \mid k$. This theorem is especially strong when $d < r + 3$, it fixes the support of the parity check matrix, the only freedom is in the choice of coefficients. We also show that the condition $r < d + 3$ is in fact necessary for such a strong statement to hold.

We then turn our attention to the locality of parity symbols. We prove tight bounds on the locality of parity symbols in optimal codes assuming $d < r + 3$. In particular we establish the existence of optimal (r, d)-codes that are significantly better than pyramid codes with respect to locality of parity symbols. Our codes are explicit in the case of $d = 4$, and non-explicit otherwise. The lower bound is proved using the structure theorem. Finally, we relax the conditions $d < r + 3$ and $r \mid k$ and exhibit one specific family of optimal codes that gives locality r for all symbols.

Our last result concerns erasure correction beyond the worst case distance of the code. Assume that we are given a bipartite graph which describes the supports of the parity check symbols. What choice of coefficients will maximize the set of erasure patterns that can be corrected by such a code? In [5] the authors gave a necessary condition for an erasure pattern to be correctable, and showed that over sufficiently large fields, this condition is also sufficient. They called such codes Generalized Pyramid codes. We show that such codes cannot have any non-trivial parity locality; thus establishing a tradeoff between parity locality and erasure correction beyond the worst case distance.

1.2 Related work

There are two classes of erasure codes providing fast recovery procedures for individual codeword coordinates (packets) in the literature.

Regenerating codes. These codes were introduced in [2] and developed further in e.g., [8, 1]. See [3] for a survey. One crucial idea behind regenerating codes is that of *sub-packetization*. Each packet is composed of few sub-packets, and when a node storing a packet fails all (or most of) other nodes send in some of their sub-packets for recovery. Efficiency of the recovery procedure is measured in terms of the overall bandwidth consumption, i.e., the total size of sub-packets required to recover from a single failure. Somehow surprisingly regenerating codes can in many cases achieve a rather significant reduction in bandwidth, compared with codes that do not employ sub-packetization. Our experience with data centers however suggests that in practice there is a considerable overhead related to accessing extra storage nodes. Therefore pure bandwidth consumption is not necessarily the right single measure of the recovery time. In particular, coding solutions that do not rely on sub-packetization and thus access less nodes (but download more data) are sometimes more attractive.

Locally decodable codes. These codes were introduced in [6] and developed further in e.g., [10, 4, 7]. See [11] for a survey. An r-query Locally Decodable Code (LDC) encodes messages in such a way that one can recover any message symbol by accessing only r codeword symbols even after some arbitrarily chosen (say) 10% of codeword coordinates are erased. Thus LDCs are in fact very similar to (r, d)-codes addressed in the current paper, with an important distinction that LDCs allow for local recovery even after a very large number of symbols is erased, while (r, d)-codes provide locality only after a single erasure. Not surprisingly locally decodable codes require substantially larger codeword lengths then (r, d)-codes.

1.3 Organization

In section 3 we establish the lower bound for redundancy of (r, d)-codes and obtain a structural characterization of optimal codes, i.e., codes attaining the bound. In section 4 we strengthen the structural characterization for optimal codes with $d < r + 3$ and show that any such code has to be a canonical code. In section 5 we prove matching lower and upper bounds on the locality of parity symbols in canonical codes. Our code construction is not explicit and requires the underlying field to be fairly large. In the special case of codes of distance $d = 4$, we come up with an explicit family that does not need a large field. In section 6 we present one optimal family of non-canonical codes that gives uniform locality for all codeword symbols. Finally, in section 7 we study erasure correction beyond the worst case distance and prove that systematic codes correcting the maximal number of erasure patterns (conditioned on the support structure of the generator matrix) cannot have any non-trivial locality for parity symbols.

2 Preliminaries

We use standard mathematical notation

- For an integer t, $[t] = \{1, \ldots, t\}$;
- For a vector $\mathbf{x}$, $\mathsf{Supp}(\mathbf{x})$ denotes the set $\{i : \mathbf{x}_i \neq 0\}$;
- For a vector $\mathbf{x}$, $\mathsf{wt}(\mathbf{x}) = |\mathsf{Supp}(\mathbf{x})|$ denotes the Hamming weight;
- For a vector $\mathbf{x}$ and an integer i, $\mathbf{x}(i)$ denotes the i-th coordinate of $\mathbf{x}$;
- For sets A and B, $A \sqcup B$ denotes the disjoint union.

Let $\mathcal{C}$ be an $[n,k,d]_q$ linear code. Assume that the encoding of $\mathbf{x} \in \mathbb{F}_q^k$ is by the vector

$$\mathcal{C}(\mathbf{x}) = (\mathbf{c}_1 \cdot \mathbf{x}, \mathbf{c}_2 \cdot \mathbf{x}, \ldots, \mathbf{c}_n \cdot \mathbf{x}) \in \mathbb{F}_q^n. \tag{3}$$

Thus the code $\mathcal{C}$ is specified by the set of n points $C = \{\mathbf{c}_1, \ldots, \mathbf{c}_n\} \in \mathbb{F}_q^k$. The set of points must have full rank for $\mathcal{C}$ to have k information symbols. It is well known that the distance property is captured by the following condition (e.g., [9, theorem 1.1.6]).

Fact 1. *The code $\mathcal{C}$ has distance d if and only if for every $S \subseteq C$ such that* $\mathrm{Rank}(S) \leqslant k-1$,

$$|S| \leqslant n - d. \tag{4}$$

In other words, every hyperplane through the origin misses at least d points from C. In this work, we are interested in the recovery cost of each symbol in the code from a single erasure.

Definition 2. *For $\mathbf{c}_i \in C$, we define* $\mathrm{Loc}(\mathbf{c}_i)$ *to be the smallest integer r for which there exists $R \subseteq C$ of cardinality r such that*

$$\mathbf{c}_i = \sum_{j \in R} \lambda_j \mathbf{c}_j.$$

We further define $\mathrm{Loc}(\mathcal{C}) = \max_{i \in [n]} \mathrm{Loc}(\mathbf{c}_i)$.

Note that $\mathrm{Loc}(\mathbf{c}_i) \leqslant k$, provided $d \geqslant 2$, since this guarantees that $C \setminus \{\mathbf{c}_i\}$ has full dimension. We will be interested in (systematic) codes which guarantee locality for the information symbols.

Definition 3. *We say that a code $\mathcal{C}$ has information locality r if there exists $I \subseteq C$ of full rank such that* $\mathrm{Loc}(\mathbf{c}) \leqslant r$ *for all $\mathbf{c} \in I$.*

For such a code we can choose I as our basis for $\mathbb{F}_q^k$ and partition C into $I = \{\mathbf{e}_1, \ldots, \mathbf{e}_k\}$ corresponding to information symbols and $C \setminus I = \{\mathbf{c}_{k+1}, \ldots, \mathbf{c}_n\}$ corresponding to parity check symbols. Thus the code $\mathcal{C}$ can be made systematic.

Definition 4. *A code $\mathcal{C}$ is an (r,d)-code if it has information locality r and distance d.*

For any code $\mathcal{C}$, the set of all linear dependencies of length at most $r+1$ on points in C defines a natural hypergraph $H_r(V,E)$ whose vertex set $V = [n]$ is in one-to-one correspondence to points in C. There is an edge corresponding to set $S \subseteq V$ if $|S| \leqslant r+1$

$$\sum_{i \in S} \lambda_i \mathbf{c}_i = 0, \quad \lambda_i \neq 0.$$

Equivalently $S \subseteq [n]$ is an edge in H if it supports a codeword in $\mathcal{C}^\perp$ of weight at most $r+1$. Since r will usually be clear from the context, we will just say $H(V,E)$. A code $\mathcal{C}$ has locality r if there are no isolated vertices in H. A code $\mathcal{C}$ has information locality r if the set points corresponding to vertices that are incident to some edge in H has full rank.

We conclude this section presenting one specific class of (r,d)-codes has been considered in [5]:

Pyramid codes. In what follows the dot product of vectors $\mathbf{p}$ and $\mathbf{x}$ is denoted by $\mathbf{p} \cdot \mathbf{x}$. To define an (r,d) pyramid code $\mathcal{C}$ encoding messages of dimension k we fix an arbitrary linear systematic $[k+d-1,k,d]_q$ code $\mathcal{E}$. Clearly, $\mathcal{E}$ is MDS. Let

$$\mathcal{E}(\mathbf{x}) = (\mathbf{x}, \mathbf{p}_0 \cdot \mathbf{x}, \mathbf{p}_1 \cdot \mathbf{x}, \ldots, \mathbf{p}_{d-2} \cdot \mathbf{x}).$$

We partition the set $[k]$ into $t = \lceil \frac{k}{r} \rceil$ subsets of size up to r, $[k] = \bigsqcup_{i \in [t]} S_i$. For a k-dimensional vector $\mathbf{x}$ and a set $S \subseteq [k]$ let $\mathbf{x}|_S$ denote the $|S|$-dimensional restriction of $\mathbf{x}$ to coordinates in the set S. We define the systematic code $\mathcal{C}$ by

$$\mathcal{C}(\mathbf{x}) = \left(\mathbf{x}, \left(\mathbf{p}_0|_{S_1} \cdot \mathbf{x}|_{S_1}\right), \ldots, \left(\mathbf{p}_0|_{S_t} \cdot \mathbf{x}|_{S_t}\right), \mathbf{p}_1 \cdot \mathbf{x}, \ldots, \mathbf{p}_{d-2} \cdot \mathbf{x}\right).$$

It is not hard to see that the code $\mathcal{C}$ has distance d. To see that all information symbols and the first $\lceil \frac{k}{r} \rceil$ parity symbols of $\mathcal{C}$ have locality r one needs to observe that (since $\mathcal{E}$ is an MDS code) the vector $\mathbf{p}_0$ has full Hamming weight. The last $d-2$ parity symbols of $\mathcal{C}$ may have locality as large as k.

3 Lower Bound and the Structure Theorem

We are interested in systematic codes with information locality r. Given k, r, d our goal is to minimize the codeword length n. Since the code is systematic, this amounts to minimizing the redundancy $h = n - k$. Pyramid codes have $h = \lceil \frac{k}{r} \rceil + d - 2$. Our goal is to prove a matching lower bound. Lower bounds of k/r and $d-1$ are easy to show, just from the locality and distance constraints respectively. The hard part is to sum them up.

Theorem 5. *For any $[n, k, d]_q$ linear code with information locality r,*

$$n - k \geqslant \left\lceil \frac{k}{r} \right\rceil + d - 2. \tag{5}$$

Proof. Our lower bound proceeds by constructing a large set $S \subseteq C$ where $\mathrm{Rank}(S) \leqslant k-1$ and then applying Fact 1. The set S is constructed by the following algorithm:

1. Let $i = 1, S_0 = \{\}$.
2. While $\mathrm{Rank}(S_{i-1}) \leqslant k-2$:
3. Pick $\mathbf{c}_i \in C \setminus S_{i-1}$ such that there is a hyperedge T_i in H containing $\mathbf{c}_i$.
4. If $\mathrm{Rank}(S_{i-1} \cup T_i) < k$, set $S_i = S_{i-1} \cup T_i$.
5. Else pick $T' \subset T_i$ so that $\mathrm{Rank}(S_{i-1} \cup T') = k-1$ and set $S_i = S_{i-1} \cup T'$.
6. Increment i.

In Line 3, since $\mathrm{Rank}(S_{i-1}) \leqslant k-2$ and $\mathrm{Rank}(I) = k$, there exists $\mathbf{c}_i$ as desired. Let ℓ denote the number of times the set S_i is grown. Observe that the final set S_ℓ has $\mathrm{Rank}(S_\ell) = k-1$. We now lower bound $|S|$. We define s_i, t_i to measure the increase in the size and rank of S_i respectively:

$$s_i = |S_i| - |S_{i-1}|, \quad |S_\ell| = \sum_{i=1}^{\ell} s_i,$$

$$t_i = \mathrm{Rank}(S_i) - \mathrm{Rank}(S_{i-1}), \quad \mathrm{Rank}(S_\ell) = \sum_{i=1}^{\ell} t_i = k-1.$$

We analyze two cases, depending on whether the condition $\mathrm{Rank}(S_{i-1} \cup T_i) = k$ is ever reached. Observe that this condition can only be reached when $i = \ell$.

Case 1: Assume $\mathrm{Rank}(S_{i-1} \cup T_i) \leqslant k-1$ throughout. In each step we add $s_i \leqslant r+1$ vectors. Note that these vectors are always such that some nontrivial linear combination of them yields a (possibly zero) vector in $\mathsf{Span}(S_{i-1})$. Therefore we have $t_i \leqslant s_i - 1 \leqslant r$. So there are $\ell \geqslant \lceil \frac{k-1}{r} \rceil$ steps in all. Thus

$$|S| = \sum_{i=1}^{\ell} s_i \geqslant \sum_{i=1}^{\ell} (t_i + 1) \geqslant k - 1 + \left\lceil \frac{k-1}{r} \right\rceil \tag{6}$$

Note that $k-1+\left\lceil\frac{k-1}{r}\right\rceil \geqslant k+\left\lceil\frac{k}{r}\right\rceil-2$ with equality holding whenever $r=1$ or $k\equiv 1 \bmod r$.

Case 2: In the last step, we hit the condition $\mathrm{Rank}(S_{\ell-1}\cup T_\ell)=k$. Since the rank only increases by r per step, $\ell \geqslant \left\lceil\frac{k}{r}\right\rceil$. For $i\leqslant \ell-1$, we add a set T_i of $s_i \leqslant r+1$ vectors. Again note that these vectors are always such that some nontrivial linear combination of them yields a (possibly zero) vector in $\mathsf{Span}(S_{i-1})$. Therefore $\mathrm{Rank}(S_i)$ grows by t_i where $t_i \leqslant s_i-1$. In Step ℓ, we add $T'\subset T_\ell$ to S. This increases $\mathrm{Rank}(S)$ by $t_\ell \geqslant 1$ (since $\mathrm{Rank}(S)\leqslant k-2$ at the start) and $|S|$ by $s_\ell \geqslant t_\ell$. Thus

$$|S|=\sum_{i=1}^{\ell} s_i \geqslant \sum_{i=1}^{\ell-1}(t_i+1)+t_\ell = k+\left\lceil\frac{k}{r}\right\rceil-2. \tag{7}$$

The conclusion now follows from Fact 1 which implies that $|S|\leqslant n-d$. □

Definition 6. *We say that an (r,d)-code $\mathcal{C}$ is optimal if its parameters satisfy (5) with equality.*

Pyramid codes [5] yield optimal (r,d)-codes for all values of r,d, and k when the alphabet q is sufficiently large.

The proof of theorem 5 reveals information about the structure of optimal (r,d)-codes. We think of the algorithm as attempting to maximize

$$\frac{|S|}{\mathrm{Rank}(S)}=\frac{\sum_{i=1}^{\ell} s_i}{\sum_{i=1}^{\ell} t_i}.$$

With this in mind, at step i we can choose $\mathbf{c}_i$ such that $\frac{s_i}{t_i}$ is maximized. An optimal length code should yield the same value for $|S|$ for this (or any) choice of $\mathbf{c}_i$. This observation yields an insight into the structure of local dependencies in optimal codes, as given by the following structure theorem.

Theorem 7. *Let $\mathcal{C}$ be an $[n,k,d]_q$ code with information locality r. Suppose $r \mid k$, $r<k$, and*

$$n=k+\frac{k}{r}+d-2; \tag{8}$$

then hyperedges in the hypergraph $H(V,E)$ are disjoint and each has size exactly $r+1$.

Proof. We execute the algorithm presented in the proof of theorem 5 to obtain a set S and sequences $\{s_i\}$ and $\{t_i\}$. We consider the case of $r=1$ separately. Since all $t_i\leqslant 1$ we fall into Case 1. Combining formulas (6), (4) and (8) we get

$$|S|=\sum_{i=1}^{\ell} s_i=\sum_{i=1}^{\ell} t_i+\ell=2k-2.$$

Combining this with $\sum_{i=1}^{\ell} t_i=k-1$ we conclude that $\ell=k-1$, all s_i equal 2, and all t_i equal 1. The latter two conditions preclude the existence of hyperedges of size 1 or intersecting edges in H.

We now proceed to the case of $r>1$. When $r\mid k$, the bound in equation (6) is larger than that in equation (7). Thus, we must be in Case 2. Combining formulas (7), (4) and (8) we get

$$|S|=\sum_{i=1}^{\ell} s_i=\sum_{i=1}^{\ell} t_i+\ell-1=k+\frac{k}{r}-2.$$

Observe that $\sum_{i=1}^{\ell} t_i = k-1$ and thus $\ell = \frac{k}{r}$. Together with the constraint $t_i \leqslant r$, this implies that $t_j = r-1$ for some $j \in [\ell]$ and $t_i = r$ for $i \neq j$. We claim that in fact $j = \ell$. Indeed, if $j < \ell$, we would have $\sum_{i \leqslant \ell-1} t_i = k-r-1$ and $t_\ell = r$, hence we would be in Case 1.

Now assume that there is an edge T with $|T| \leqslant r$. By adding this edge to S at the first step, we would get $t_1 \leqslant r-1$. Next assume that $T_1 \cap T_2$ is non-empty. Observe that this implies $\mathrm{Rank}(T_1 \cup T_2) < 2r$. So if we add edges T_1 and T_2 to S, we have $t_1 + t_2 \leqslant 2r-1$. Clearly these conditions lead to contradiction if $\ell = \frac{k}{r} \geqslant 3$. In fact, they also give a contradiction for $\frac{k}{r} = 2$, since they put us in Case 1. □

4 Canonical Codes

The structure theorem implies then when d is sufficiently small (which in our experience is the setting of interest in most data storage applications), optimal (r,d)-codes have rather rigid structure. We formalize this by defining the notion of a *canonical* code.

Definition 8. *Let $\mathcal{C}$ be a systematic $[n,k,d]_q$ code with information locality r where $r \mid k$, $r < k$, and $n = k + \frac{k}{r} + d - 2$. We say that $\mathcal{C}$ is canonical if the set C can partitioned into three groups $C = I \cup C' \cup C''$ such that:*

1. *Points $I = \{\mathbf{e}_1, \ldots, \mathbf{e}_k\}$.*
2. *Points $C' = \{\mathbf{c}'_1, \ldots, \mathbf{c}'_{k/r}\}$ where $\mathsf{wt}(\mathbf{c}'_i) = r$. The supports of these vectors are disjoint sets which partition $[k]$.*
3. *Points $C'' = \{\mathbf{c}''_1, \ldots, \mathbf{c}''_{d-2}\}$ where $\mathsf{wt}(\mathbf{c}''_i) = k$.*

Clearly any canonical code is systematic and has information locality r. The distance property requires a suitable choice of vectors $\{\mathbf{c}'\}$ and $\{\mathbf{c}''\}$. Pyramid codes [5] are an example of canonical codes. We note that since $r < k$, there is always a distinction between symbols $\{\mathbf{c}'\}$ and $\{\mathbf{c}''\}$.

Theorem 9. *Assume that $d < r+3$, $r < k$, and $r \mid k$. Let $n = k + \frac{k}{r} + d - 2$. Every systematic $[n,k,d]_q$ code with information locality r is a canonical code.*

Proof. Let $\mathcal{C}$ be a systematic $[n,k,d]$ code with information locality r. We start by showing that the hypergraph $H(V,E)$ has $\frac{k}{r}$ edges.

Since $\mathcal{C}$ is systematic, we know that $I = \{\mathbf{e}_1, \ldots, \mathbf{e}_k\} \subset C$. By theorem 7, $H(V,E)$ consists of m disjoint, $(r+1)$-regular edges and every vertex in I appears in some edge. But since the points in I are linearly independent, every edges involves at least one vertex from $C \setminus I$ and at most r from I. So we have $m \geqslant \frac{k}{r}$. We show that equality holds.

Assume for contradiction that $m \geqslant \frac{k}{r} + 1$. Since the edges are regular and disjoint, we have

$$n \geqslant m(r+1) = k + \frac{k}{r} + r + 1 > k + \frac{k}{r} + d - 2$$

which contradicts the choice of n. Thus $m = \frac{k}{r}$. This means that every edge T_i is incident on exactly r vertices $\mathbf{e}_{i_1} \ldots, \mathbf{e}_{i_r}$ from I and one vertex $\mathbf{c}'_i$ outside it. Hence

$$\mathbf{c}'_i = \sum_{j=1}^{r} \lambda_{i_j} \mathbf{e}_{i_j}.$$

Since the T_is are disjoint, the vectors $\mathbf{c}'_1, \ldots, \mathbf{c}'_{k/r}$ have disjoint supports which partition $[k]$.

We now show that the remaining vectors $\mathbf{c}''_1, \ldots, \mathbf{c}''_{d-2}$ must all have $\mathsf{wt}(\mathbf{c}'') = k$. For this, we consider the encoding of $\mathbf{e}_j$. We note $\mathbf{e}_i \cdot \mathbf{e}_j \neq 0$ iff $i = j$ and $\mathbf{c}'_i \cdot \mathbf{e}_j \neq 0$ iff $j \in \mathsf{Supp}(\mathbf{c}_i)$. Thus only 2 of these inner products are non-zero. Since the code has distance d, all the $d-2$ inner products $\mathbf{c}''_i \cdot \mathbf{e}_j$ are non-zero. This shows that $\mathsf{wt}(\mathbf{c}''_i) = k$ for all i. □

The above bound is strong enough to separate having locality of r from having just information locality of r. The following corollary follows from the observation that the hypergraph $H(V, E)$ must contain $n - \frac{k}{r}(r+1) = d-2$ isolated vertices, which do not participate in any linear relations of size $r+1$.

Corollary 10. *Assume that $2 < d < r+3$ and $r \mid k$. Let $n = k + \frac{k}{r} + d - 2$. There are no $[n, k, d]_q$ linear codes with locality r.*

5 Canonical codes: parity locality

Theorem 9 gives a very good understanding optimal (r, d)-codes in the case $r < d+3$ and $r \mid k$. For any such code the coordinate set $C = \{\mathbf{c}_i\}_{i \in [n]}$ can be partitioned into sets I, C', C'' where for all $\mathbf{c} \in I \cup C'$, $\mathrm{Loc}(\mathbf{c}) = r$, and for all $\mathbf{c}'' \in C''$, $\mathrm{Loc}(\mathbf{c}'') > r$. It is natural to ask how low can the locality of symbols $\mathbf{c}'' \in C''$ be. In this section we address and resolve this question.

5.1 Parity locality lower bound

We begin with a lower bound.

Theorem 11. *Let $\mathcal{C}$ be a systematic optimal (r, d)-code with parameters $[n, k, d]_q$. Suppose $d < r+3$, $r < k$, and $r \mid k$. Then some $\frac{k}{r}$ parity symbols of $\mathcal{C}$ have locality exactly r, and $d-2$ other parity symbols of $\mathcal{C}$ have locality no less than*

$$k - \left(\frac{k}{r} - 1\right)(d-3). \tag{9}$$

Proof. Theorem 9 implies that $\mathcal{C}$ is a canonical code. Let $C = I \cup C' \cup C''$ be the canonical partition of the coordinates of $\mathcal{C}$. Clearly, for all $\frac{k}{r}$ symbols $\mathbf{c}' \in C'$ we have $\mathrm{Loc}(\mathbf{c}') \leqslant r$. We now prove lower bounds on the locality of symbols in $C' \cup C''$.

We start with symbols $\mathbf{c}'' \in C''$. For every $j \in [k/r]$ we define a subset $R_j \subseteq C$ that we call a *row*. Let $S_j = \mathsf{Supp}\left(\mathbf{c}'_j\right)$. The j-th row contains the vector $\mathbf{c}'_j$, all r unit vectors in the support of $\mathbf{c}'_j$ and the set C''.

$$R_j = \{\mathbf{c}'_j\} \cup \left(\bigcup_{i \in S_j} \mathbf{e}_i\right) \cup C''.$$

Observe that restricted to $I \cup C'$ rows $\{R_j\}_{j \in [k/r]}$ form a partition. Consider an arbitrary symbol $\mathbf{c}'' \in C''$. Let $\ell = \mathrm{Loc}(\mathbf{c}'')$. We have

$$\mathbf{c}'' = \sum_{i \in L} \mathbf{c}_i, \tag{10}$$

where $|L| = \ell$. In what follows we show that for each row R_j,

$$|R_j \cap L| \geqslant r \tag{11}$$

needs to hold. It is not hard to see that this together with the structure of the sets $\{R_j\}$ implies inequality (9). To prove (11) we consider the code

$$\mathcal{C}_j = \{\mathcal{C}(\mathbf{x}) \mid \mathbf{x} \in \mathbb{F}_q^k \text{ such that } \mathsf{Supp}(\mathbf{x}) \subseteq S_j\}. \tag{12}$$

It is not hard to see that $\mathsf{Supp}(\mathcal{C}_j) = R_j$ and $\dim \mathcal{C}_j = r$. Observing that the distance of the code $\mathcal{C}_j$ is at least d and $|R_j| = r + d - 1$ we conclude that (restricted to its support) $\mathcal{C}_j$ is an MDS code. Thus any r symbols of $\mathcal{C}_j$ are independent. It remains to note that (10) restricted to coordinates in S_j yields a non-trivial dependency of length at most $|R_j \cap L| + 1$ between the symbols of $\mathcal{C}_j$.

We proceed to the lower bound on the locality of symbols in C'. Fix an arbitrary $\mathbf{c}'_j \in C'$. A reasoning similar to the one above implies that if $\mathrm{Loc}(\mathbf{c}_j) < r$; then there is a dependency of length below $r + 1$ between the coordinates of the $[r + d - 1, r, d]_q$ code $\mathcal{C}_j$ (defined by (12)) restricted to its support. □

Observe that the bound (9) is close to k only when r is large and d is small. In other cases theorem 11 does not rule out existence of canonical codes with low locality for all symbols (including those in C''). In the next section we show that such codes indeed exist. In particular we show that the bound (9) can be always met with equality.

5.2 Parity locality upper bounds

Our main results in this section are given by theorems 15 and 16. Theorem 15 gives a general upper bound matching the lower bound of theorem 11. The proof is not explicit. Theorem 16 gives an explicit family of codes in the narrow case of $d = 4$. We start by introducing some concepts we need for the proof of theorem 15.

Definition 12. *Let $L \subseteq \mathbb{F}_q^n$ be a linear space and $S \subseteq [n]$ be a set, $|S| = k$. We say that S is a k-core for L if for all vectors $\mathbf{v} \in L$, $\mathsf{Supp}(\mathbf{v}) \not\subseteq S$.*

It is not hard to verify that S is a k-core for L, if and only if S is a subset of some set of information coordinates in the space $L^\perp$. In other words S is a k-core for L, if and only k columns in the $(n - \dim L)$-by-n generator matrix of $L^\perp$ that correspond to elements of S are linearly independent.

Definition 13. *Let $L \subseteq \mathbb{F}_q^n$ be a linear space. Let $\{\mathbf{c}_1, \ldots, \mathbf{c}_n\}$ be a sequence of n vectors in $\mathbb{F}_q^k$. We say that vectors $\{\mathbf{c}_i\}$ are in general position subject to L if the following conditions hold:*

1. *For all vectors $\mathbf{v} \in L$ we have $\sum_{i=1}^n \mathbf{v}(i)\mathbf{c}_i = 0$;*
2. *For all k-cores S of L we have $\mathrm{Rank}\,(\{\mathbf{c}_i\}_{i \in S}) = k$.*

The next lemma asserts existence of vectors that are in general position subject to an arbitrary linear space provided the underlying field is large enough.

Lemma 14. *Let $L \subseteq \mathbb{F}_q^n$ be a linear space and k be a positive integer. Suppose $q > kn^k$; then there exists a family of vectors $\{\mathbf{c}_i\}_{i \in [n]}$ in $\mathbb{F}_q^k$ that are in general position subject to L.*

Proof. We obtain a matrix $M \in \mathbb{F}_q^{k \times n}$ picking the rows of M at random (uniformly and independently) from the linear space $L^\perp$. We choose vectors $\{\mathbf{c}_i\}$ to be the columns of M. Observe that the first condition in definition 13 is always satisfied. Further observe that our choice of M induces a uniform distribution on every set of k columns of M that form a k-core. The second condition in definition 13

is satisfied as long as all k-by-k minors of M that correspond to k-cores are invertible. This happens with probability at least

$$1 - \binom{n}{k} \cdot \left(1 - \prod_{i=1}^{k} \left(1 - \frac{1}{q^i}\right)\right) \geqslant 1 - \binom{n}{k} \cdot \left(1 - \left(1 - \frac{1}{q}\right)^k\right) \geqslant 1 - n^k \cdot \frac{k}{q} > 0.$$

This concludes the proof. □

We proceed to the main result of this section.

Theorem 15. *Let $2 < d < r + 3$, $r < k$, $r \mid k$. Let $q > kn^k$ be a prime power. Let $n = k + \frac{k}{r} + d - 2$. There exists a systematic $[n, k, d]_q$ code $\mathcal{C}$ of information locality r, where $\frac{k}{r}$ parity symbols have locality r, and $d - 2$ other parity symbols have locality $k - \left(\frac{k}{r} - 1\right)(d - 3)$.*

Proof. Let $t = \frac{k}{r}$. Fix some $t + 1$ subsets $P_0, P_1, \ldots, P_t$ of $[n]$ subject to the following constraints:

1. $|P_0| = k - (t - 1)(d - 3) + 1$;
2. For all $i \in [t]$, $|P_i| = r + 1$;
3. For all $i, j \in [t]$ such that $i \neq j$, $P_i \cap P_j = \emptyset$;
4. For all $i \in [t]$, $|P_0 \cap P_i| = r - d + 3$.

For every set P_i, $0 \leqslant i \leqslant t$ we fix a vector $\mathbf{v}_i \in \mathbb{F}_q^n$, such that $\mathsf{Supp}(\mathbf{v}_i) = P_i$. We ensure that non-zero coordinates of $\mathbf{v}_0$ contain the same value. We also ensure that for all $i \in [t]$ non-zero coordinates of $\mathbf{v}_i$ contain distinct values. The lower bound on q implies that these conditions can be met. For a finite set A let A° denote a set that is obtained from A by dropping *at most* one element. Note that for all $i \in [t]$ and all non-zero α, β in $\mathbb{F}_q$ we have

$$\mathsf{Supp}(\alpha\mathbf{v}_0 + \beta\mathbf{v}_i) = (P_0 \setminus P_i) \sqcup (P_0 \cap P_i)^\circ \sqcup (P_i \setminus P_0). \tag{13}$$

Consider the space $L = \mathsf{Span}\left(\{\mathbf{v}_i\}_{0 \leqslant i \leqslant t}\right)$. Let $M = P_0 \setminus \bigsqcup_{i=1}^{t} P_i$. Observe that

$$|M| = k - (t-1)(d-3) + 1 - t(r - d + 3) = d - 2.$$

By (13) for any $\mathbf{v} \in L$ we have

$$\mathsf{Supp}(\mathbf{v}) = \begin{cases} \bigsqcup\limits_{i \in T} P_i, & \text{for some } T \subseteq [t] \text{ OR} \\ M \bigsqcup\limits_{i \in [n] \setminus T} (P_0 \cap P_i) \bigsqcup\limits_{i \in T} (P_0 \cap P_i)^\circ \bigsqcup\limits_{i \in T} (P_i \setminus P_0) & \text{for some } T \subseteq [t]. \end{cases} \tag{14}$$

Observe that a set $K \subseteq [n]$, $|K| = k$ is a k-core for L if and only if for all $i \in [t]$, $P_i \not\subseteq K$ and

$$\begin{cases} M \not\subseteq K; \text{ OR} \\ M \subseteq K \text{ and } \exists i \in [t] \text{ such that } \begin{cases} |P_i \cap P_0 \cap K| < r - d + 2; \text{ OR} \\ |P_i \cap P_0 \cap K| = r - d + 2 \text{ and } P_i \setminus P_0 \not\subseteq K. \end{cases} \end{cases} \tag{15}$$

Let $I \subseteq [n]$ be such that $M \cap I = \emptyset$ and for all $i \in [t]$, $|I \cap P_i| = r$. By (15) I is a k-core for L. We use lemma 14 to obtain vectors $\{\mathbf{c}_i\}_{i \in [n]} \in \mathbb{F}_q^k$ that are in general position subject to the space L. We choose vectors $\{\mathbf{c}_i\}_{i \in I}$ as our basis for $\mathbb{F}_q^k$ and consider the code $\mathcal{C}$ defined as in (3).

In it not hard to see that $\mathcal{C}$ is a systematic code of information locality r. All t parity symbols in the set $\left(\bigsqcup_{i\in[t]} P_i\right) \setminus I$ also have locality r. Furthermore all $d-2$ parity symbols in the set M have locality $k-(t-1)(d-3)$. It remains to prove that the code $\mathcal{C}$ has distance

$$d = n - k - t + 2. \tag{16}$$

According to Fact 1 the distance of $\mathcal{C}$ equals $n - |S|$ where $S \subseteq [n]$ is the largest set such that vectors $\{\mathbf{c}_i\}_{i\in S}$ do not have full rank. By definition 13 for any k-core K of L we have $\mathrm{Rank}\{\mathbf{c}_i\}_{i\in K} = k$. Thus in order to establish (16) it suffices to show that every set $S \subseteq [n]$ of size $k+t-1$ contains a k-core of L. Our proof involves case analysis. Let $S \subseteq [n]$, $|S| = k+t-1$ be an arbitrary set. Set

$$b = \#\{i \in [t] \mid P_i \subseteq S\}.$$

Note that since $t(r+1) > |S|$ we have $b \leqslant t-1$.

Case 1: $M \not\subseteq S$. We drop $t-1$ elements from S to obtain a set $K \subseteq S$, $|K| = k$ such that for all $i \in [t]$, $P_i \not\subseteq K$. By (15) K is a k-core.

Case 2: $M \subseteq S$ and $b \leqslant t-2$. We drop $t-1$ elements from S to obtain a set $K \subseteq S$, $|K| = k$ such that $M \not\subseteq K$ and for all $i \in [t]$, $P_i \not\subseteq K$. By (15) K is a k-core.

Case 3: $M \subseteq S$ and $b = t-1$. Let $i \in [t]$ be such that $P_i \not\subseteq S$. Such i is unique. Observe that

$$|P_i \cap S| = k + t - 1 - (d-2) - (t-1)(r+1) = r - d + 2.$$

Also observe that $|P_i \setminus P_0| = r + 1 - (r - d + 3) = d - 2 \geqslant 1$. Combining the last two observations we conclude that either

$$\left[\begin{array}{l} |P_i \cap P_0 \cap S| < r - d + 2; \text{ OR} \\ |P_i \cap P_0 \cap S| = r - d + 2 \text{ and } P_i \setminus P_0 \not\subseteq S. \end{array}\right. \tag{17}$$

Finally, we drop $t-1$ elements from S to obtain a set $K \subseteq S$, $|K| = k$ such that for all $i \in [t]$, $P_i \not\subseteq K$. By (15) and (17) K is a k-core. □

Theorem 15 gave a general construction of (r,d)-codes that are optimal not only with respect to information locality and redundancy but also with respect to locality of parity symbols. That theorem however is weak in two respects. Firstly, the construction is not explicit. Secondly, the construction requires a large underlying field. The next theorem gives an explicit construction that works even over small fields in the narrow case of codes of distance 4.

Theorem 16. *Let $r < k$, $r \mid k$ be positive integers. Let $q \geqslant r+2$ be a prime power. Let $n = k + \frac{k}{r} + 2$. There exists a systematic $[n,k,4]_q$ code $\mathcal{C}$ of information locality r, where $\frac{k}{r}$ parity symbols have locality r, and 2 other parity symbols have locality $k - \frac{k}{r} + 1$.*

Proof. Fix an arbitrary systematic $[r+3, r, 4]_q$ code $\mathcal{E}$. For instance, one can choose $\mathcal{E}$ to be a Reed Solomon code. Let

$$\mathcal{E}(\mathbf{y}) = (\mathbf{y}, \mathbf{p}_0 \cdot \mathbf{y}, \mathbf{p}_1 \cdot \mathbf{y}, \mathbf{p}_2 \cdot \mathbf{y}).$$

Since $\mathcal{E}$ is a MDS code all vectors $\{\mathbf{p}_i\}$ have weight r. Thus for some non-zero $\{\alpha_j\}_{j\in[r]}$ we have

$$\mathbf{p}_1 = \sum_{j=1}^{r-1} \alpha_j \mathbf{e}_j + \alpha_r \mathbf{p}_2, \tag{18}$$

where $\{\mathbf{e}_j\}_{j\in[r]}$ are the r-dimensional unit vectors. To define a systematic code $\mathcal{C}$ we partition the input vector $\mathbf{x} \in \mathbb{F}_q^n$ into $t = \frac{k}{r}$ vectors $\mathbf{y}_1, \ldots, \mathbf{y}_t \in \mathbb{F}_q^r$. We set

$$\mathcal{C}(\mathbf{x}) = \left(\mathbf{y}_1, \ldots, \mathbf{y}_t, \mathbf{p}_0 \cdot \mathbf{y}_1, \ldots, \mathbf{p}_0 \cdot \mathbf{y}_t, \left(\mathbf{p}_1 \cdot \sum \mathbf{y}_i\right), \left(\mathbf{p}_2 \cdot \sum \mathbf{y}_i\right)\right), \tag{19}$$

where the summation is over all $i \in [t]$. It is not hard to see that the first $k + t$ coordinates of $\mathcal{C}$ have locality r. We argue that the last two coordinates have locality $k - t + 1$. From (18) we have

$$\left(\mathbf{p}_1 \cdot \sum \mathbf{y}_i\right) = \sum_{j=1}^{r-1} \alpha_j \left(\mathbf{e}_j \cdot \sum \mathbf{y}_i\right) + \alpha_r \left(\mathbf{p}_2 \cdot \sum \mathbf{y}_i\right),$$

where the summation is over all $i \in [t]$. Equivalently,

$$\left(\mathbf{p}_1 \cdot \sum \mathbf{y}_i\right) = \sum_{j=1}^{r-1} \sum_{i\in[t]} \alpha_j \mathbf{y}_i(j) + \alpha_r \left(\mathbf{p}_2 \cdot \sum \mathbf{y}_i\right).$$

Thus the next-to-last coordinate of $\mathcal{C}$ can be recovered from accessing $(r-1)t$ information coordinates and the last coordinate. Similarly, the last coordinate can be recovered from $k - t$ information coordinates and the next-to-last coordinate. To prove that the code $\mathcal{C}$ has distance 4 we give an algorithm to correct 3 erasures in $\mathcal{C}$. The algorithm has two steps.

Step 1: For every $i \in [t]$, we refer to a subset $(\mathbf{y}_i, \mathbf{p}_0 \cdot \mathbf{y}_i)$ of $r + 1$ coordinates of $\mathcal{C}$ as a block. We go over all t blocks. If we encounter a block where one symbol is erased, we recover this symbol from other symbols in the block.

Step 2: Observe that after the execution of Step 1 there can be at most one block that has erasures. If no such block exists; then on Step 1 we have successfully recovered all information symbols and thus we are done. Otherwise, let the unique block with erasures be $(\mathbf{y}_j, \mathbf{p}_0 \cdot \mathbf{y}_j)$ for some $j \in [t]$. Since we know all vectors $\{\mathbf{y}_i\}_{i\neq j,\ i\in[t]}$, from $\left(\mathbf{p}_1 \cdot \sum_{i\in[t]} \mathbf{y}_i\right)$ and $\left(\mathbf{p}_2 \cdot \sum_{i\in[t]} \mathbf{y}_i\right)$ (if these symbols are not erased) we recover symbols $\mathbf{p}_1 \cdot \mathbf{y}_j$ and $\mathbf{p}_2 \cdot \mathbf{y}_j$. Finally, we invoke the decoding procedure for the code $\mathcal{E}$ to recover $\mathbf{y}_j$ form at most 3 erasures in $\mathcal{E}(\mathbf{y}_j) = (\mathbf{y}_j, \mathbf{p}_0 \cdot \mathbf{y}_j, \mathbf{p}_1 \cdot \mathbf{y}_j, \mathbf{p}_2 \cdot \mathbf{y}_j)$. □

6 Non-Canonical Codes

In this section we observe that canonical codes detailed in sections 4 and 5 are not the only family of optimal (r, d)-codes. If one relaxes conditions of theorem 9 one can get other families. One such family that yields uniform locality for all symbols is given below. The (non-explicit) proof resembles the proof of theorem 15 albeit is much simpler.

Theorem 17. *Let n, k, r, and $d \geqslant 2$ be positive integers. Let $q > kn^k$ be a prime power. Suppose $(r + 1) \mid n$ and*

$$n - k = \left\lceil \frac{k}{r} \right\rceil + d - 2;$$

then there exists an $[n, k, d]_q$ code where all symbols have locality r.

Proof. Let $t = \frac{n}{r+1}$. We partition the set $[n]$ into t subsets $P_1, \ldots, P_t$ each of size $r+1$. For every $i \in [t]$ we fix a vector $\mathbf{v}_i \in \mathbb{F}_q^n$, such that $\mathsf{Supp}(\mathbf{v}_i) = P_i$. We set all non-zero coordinates in vectors $\{\mathbf{v}_i\}_{i\in[t]}$

to be equal to 1. We consider the linear space $L = \mathsf{Span}\left(\{\mathbf{v}_i\}_{i\in[t]}\right)$. For every any $\mathbf{v} \in L$ we have

$$\mathsf{Supp}(\mathbf{v}) = \bigsqcup_{i\in T} P_i \quad \text{for some for some } T \subseteq [t].$$

Observe that a set $K \subseteq [n]$, $|K| = k$ is a k-core for L if and only if for all $i \in [t]$, $P_i \not\subseteq K$. Also observe that conditions of the theorem imply $k \leqslant n - t$. Therefore k-cores for L exist. We use lemma 14 to obtain vectors $\{\mathbf{c}_i\}_{i\in[n]} \in \mathbb{F}_q^k$ that are in general position subject to the space L. We consider the code $\mathcal{C}$ defined as in (3). In it not hard to see that $\mathcal{C}$ has dimension k and locality r for all symbols. It remains to prove that the code $\mathcal{C}$ has distance

$$d = n - k - \left\lceil \frac{k}{r} \right\rceil + 2. \tag{20}$$

Our proof relies on Fact 1. Let $S \subseteq [n]$ be an arbitrary subset such that $\mathrm{Rank}\{\mathbf{c}_i\}_{i\in S} < k$. Clearly, no k-core of L is in S. Let

$$b = \#\{i \in [t] \mid P_i \subseteq S\}.$$

We have $|S| - b \leqslant k - 1$ since dropping b elements from S (one from each $P_i \subseteq S$) turns $|S|$ into an $(|S| - b)$-core. We also have $br \leqslant k - 1$ since dropping one element from each $P_i \subseteq S$ gives us a br-core in S. Combining the last two inequalities we conclude that

$$|S| \leqslant k + \left\lfloor \frac{k-1}{r} \right\rfloor - 1.$$

Combining this inequality with the identity $\left\lfloor \frac{k-1}{r} \right\rfloor = \left\lceil \frac{k}{r} \right\rceil - 1$ and Fact 1 we obtain (20). □

7 Beyond Worst-Case Distance

In this section, codes are assumed to be systematic unless otherwise stated. They will have k information symbols and $h = n - k$ parity check symbols.

7.1 Generalized Pyramid Codes

The supports of the parity check symbols in a code can be described using a bipartite graph. More generally, we define the notion of a set of points with supports matching a graph G.

Definition 18. *Let $G([k], [h], E)$ be a bipartite graph. We say that $\mathbf{c}_1, \ldots, \mathbf{c}_h \in \mathbb{F}_q^k$ have supports matching G if $\mathsf{Supp}(\mathbf{c}_j) = \Gamma(j)$ for all $j \in [h]$ where $\Gamma(j)$ denotes the neighborhood of j in G.*

Given points $\mathbf{c}_1, \ldots, \mathbf{c}_h$, consider the $k \times h$ matrix C with columns $\mathbf{c}_1, \ldots, \mathbf{c}_h$. For $I \subseteq [k]$ and $J \subseteq [h]$, let $C_{I,J}$ denote the sub-matrix of C with rows indexed by I and columns indexed by J.

Definition 19. *Points $\mathbf{c}_1, \ldots, \mathbf{c}_h \in \mathbb{F}_q^k$ with supports matching G are in general position if for every $I \subseteq [h]$ and $J \subseteq [k]$ such that there is a perfect matching from I to J in G, the sub-matrix $C_{I,J}$ is invertible.*

Standard arguments show that over sufficiently large fields $\mathbb{F}_q$, choosing $\mathbf{c}_1, \ldots, \mathbf{c}_h$ randomly from the set of vectors with support matching G gives points in general position.

Coming back to codes, the supports of the parity checks define a bipartite graph which we will call the support graph. This is closely related to but distinct from the Tanner graph.

Definition 20. *Let $\mathcal{C}$ be a systematic code with point set $C = \{\mathbf{e}_1, \ldots, \mathbf{e}_k, \mathbf{c}_1, \ldots, \mathbf{c}_h\}$. The support graph $G([k], [h], E)$ of $\mathcal{C}$ is a bipartite graph where $(i, j) \in E$ if $\mathbf{e}_i \in \mathsf{Supp}(\mathbf{c}_j)$.*

For instance in any canonical (r, d)-code, the support graph is specified up to relabeling. There are $\frac{k}{r}$ vertices in V of degree r corresponding to $C' \subseteq C$, whose neighborhood partitions the set U and $d-2$ vertices of degree k corresponding to $C'' \subseteq C$. The minimum distance of such a code is exactly d, and hence there are some patterns of d erasures that the code cannot correct. However it is possible that the code could correct many patterns of erasures of weight d and higher, for a suitable choice of $\mathbf{c}_i$s. In general one could ask: among all codes with a support graph G, which codes can correct the most erasure patterns? *A Priori*, it is unclear that there should be a single code that is optimal in the sense that it corrects the maximal possible set of patterns. As shown by [5] such codes do exist over sufficiently large fields.

Consider a systematic code $\mathcal{C}$ with support graph $G([k], [h], E)$. Given $I \subseteq [k]$ and $J \subseteq [h]$, let $\Gamma_J(I)$ denote $\Gamma(I) \cap J$ (define $\Gamma_I(J)$ similarly). Consider a set of erasures $S \cup T$ where $S \subseteq [k]$ and $T \subseteq [h]$ are the sets of information and parity check symbols respectively that are erased. To correct these erasures, we need to recover the symbols corresponding to $\{\mathbf{e}_i : i \in S\}$ from the parity checks corresponding to $\{\mathbf{c}_j : j \in \bar{T} = [h] \setminus T\}$. For this to be possible, a necessary condition is that for every $S' \subseteq S, |\Gamma_{\bar{T}}(S')| \geqslant |S'|$. By Hall's theorem, this is equivalent to the existance of a matching in G from S to $\bar{T}$. We say that such a set of erasures satisfies Hall's condition.

Definition 21. *A systematic code $\mathcal{C}$ with support graph G is a generalized pyramid code if every set of erasures satisfying Hall's condition can be corrected.*

We can rephrase this definition in algebraic terms using the notion of points with specified supports in general position.

Theorem 22. *[5] Let $\mathcal{C}$ be a systematic code with support graph G. $\mathcal{C}$ is a generalized pyramid code iff $\mathbf{c}_1, \ldots, \mathbf{c}_h$ are in general position with supports matching G.*

7.2 The Tradeoff between Locality and Erasure Correction

For any parity check symbol $\mathbf{c}_j$, it is clear that $\mathrm{Loc}(\mathbf{c}_j) \leqslant \mathsf{wt}(\mathbf{c}_j) = \deg(j)$. We will show that no better locality is possible for a generalized pyramid code. This result relies on a characterization of the support of the vectors in the space $\mathcal{V}$ spanned by $\{\mathbf{c}_1, \ldots, \mathbf{c}_h\}$ in terms of the graph G.

Let $\mathcal{V}$ denote the space spanned by $\{\mathbf{c}_1, \ldots, \mathbf{c}_h\}$ which are in general position with supports matching G. Let $\mathsf{Supp}(\mathcal{V}) \subseteq 2^{[k]}$ denote the set of supports of vectors in $\mathcal{V}$. We give a necessary condition for membership in $\mathsf{Supp}(\mathcal{V})$. Our condition is in terms of sets of coordinates that can be eliminated by combination of certain $\mathbf{c}_j$s.

Definition 23. *Let $\mathbf{c} = \sum_{j \in J} \mu_j \mathbf{c}_j$ where $\mu_j \neq 0$. Let $I = \cup_{j \in J} \Gamma(j) \setminus \mathsf{Supp}(\mathbf{c})$. We say that the set I has been eliminated from $\cup_{j \in J} \Gamma(j)$.*

Theorem 24. *Let $\{\mathbf{c}_1, \ldots, \mathbf{c}_h\}$ be vectors with supports matching G in general position. The set I can be eliminated from $\cup_{j \in J} \Gamma(j)$ only if $|\Gamma_J(I')| > |I'|$ for every $I' \subseteq I$.*

Proof. Let $\mathbf{c} = \sum_{j \in J} \mu_j \mathbf{c}_j$ where $\mu_j \neq 0$. Let $I = \cup_{j \in J} \Gamma(j) \setminus \mathsf{Supp}(\mathbf{c})$. Assume for contradiction that there exists $\tilde{I} \subseteq I$ where $\Gamma_J(\tilde{I}) \leqslant |\tilde{I}|$. We will show that there exists $I' \subseteq \tilde{I}$ so that $\Gamma_J(I') = |I'|$ and that $\Gamma_J(I'') > |I''|$ for every non-empty subset $I'' \subsetneq I'$.

It suffices to prove the existence of $I' \subseteq \tilde{I}$ where $|\Gamma_J(I')| = |I'|$; the claim about subsets of I' will then follow by taking a minimal such I'. Observe that every $i \in I$ must have $|\Gamma_J(i)| \geqslant 2$, since if i occurs in exactly one S_j, then it cannot be eliminated. Hence we must have $|\tilde{I}| \geqslant 2$.

One can construct the set I starting from a singleton and adding elements one at a time, giving a sequence $I_1, \ldots, I_\ell = I$. We claim that for any $l \leqslant \ell$,

$$|\Gamma_J(I_l)| - |I_l| \geqslant |\Gamma_J(I_{l-1})| - |I_{l-1}| - 1.$$

This holds since $\Gamma_J(I_l)$ can only increase on adding i to I_{l-1} while $|I_l|$ increases by 1. Since $|\Gamma_J(I_1)| - |I_1| \geqslant 1$ whereas $|\Gamma(I_\ell)| - |I_\ell| \leqslant 0$, we must have $|\Gamma_J(I_l)| - |I_l| = 0$ for some $l \leqslant \ell$. Thus we have a set where $|\Gamma_J(I_l) = |I_l|$ as desired.

Since the set I' satisfies Hall's matching condition, there is a perfect matching from I' to $J' = \Gamma_J(I')$ in G. But this means that the sub-matrix $C_{I',J'}$ has full rank. On the other hand, $\mathbf{c} = \sum_j \mu_j \mathbf{c}_j$ and $I' \subseteq I = \cup_j \Gamma(j) \setminus \mathsf{Supp}(\mathbf{c})$. Let $\pi(\mathbf{c})$ denote the restriction of $\mathbf{c}$ onto the co-ordinates in I'. Then we have

$$\sum_{j \in J} \mu_j \pi(\mathbf{c}_j) = \sum_{j \in J'} \mu_j \pi(\mathbf{c}_j) = \pi(\mathbf{c}) = 0.$$

The first equality holds because $\pi(\mathbf{c}_j) = 0$ for $j \notin \Gamma(I')$, the second by linearity of π and the last since $\pi(\mathbf{c}) = 0$. Hence the vector $\mu'_J = \{\mu_j\}_{j \in J'}$ lies in the kernel of $C_{I',J'}$ which contradicts the assumption that it has full rank.

This shows that the condition $|\Gamma_J(I')| > |I'|$ for all $I' \subseteq I$ is necessary. □

Corollary 25. *If the set I can be eliminated from $\cup_{j \in J} \Gamma(j)$, then $|I| \leqslant |J| - 1$.*

If the field size q is sufficiently large, the necessary condition given by theorem 24 is also sufficient. We defer the proof of this statement to Appendix A and prove our lower bound on the locality of generalized pyramid codes.

Theorem 26. *In a generalized pyramid code,* $\mathrm{Loc}(\mathbf{c}_j) = \deg(j)$ *for all* $j \in [h]$.

Proof. Assume for contradiction that $\mathrm{Loc}(\mathbf{c}_t) \leqslant \deg(t) - 1$ for some $t \in [h]$. Hence there exist $A \subseteq [k]$ and $B \subseteq [h]$ (not containing t) such that

$$\mathbf{c}_t = \sum_{i \in A} \lambda_i \mathbf{e}_i + \sum_{j \in B} \mu_j \mathbf{c}_j.$$

We have $|A| = a$, $|B| = b$ and $a + b \leqslant \deg(t) - 1$. Hence

$$\mathbf{c}_t - \sum_{j \in B} \mu_j \mathbf{c}_j = \sum_{i \in A} \lambda_i \mathbf{e}_i.$$

Thus we have eliminated at least $\deg(t) - a \geqslant b + 1$ indices from $\cup_{j \in B \cup \{t\}} \mathsf{Supp}(\mathbf{c}_j)$ using a linear combination of $b + 1$ vectors. By corollary 25 this is not possible for vectors in general position. □

References

[1] Viveck R. Cadambe, Syed A. Jafar, and Hamed Maleki. Distributed data storage with minimum storage regenerating codes - exact and functional repair are asymptotically equally efficient. Arxiv 1004.4299, 2010.

[2] Alexandros G. Dimakis, Brighten Godfrey, Yunnan Wu, Martin J. Wainwright, and Kannan Ramchandran. Network coding for distributed storage systems. *IEEE Transactions on Information Theory*, 56:4539–4551, 2010.

[3] Alexandros G. Dimakis, Kannan Ramchandran, Yunnan Wu, and Changho Suh. A survey on network codes for distributed storage. *Proceedings of the IEEE*, 99:476–489, 2011.

[4] Klim Efremenko. 3-query locally decodable codes of subexponential length. In *41st ACM Symposium on Theory of Computing (STOC)*, pages 39–44, 2009.

[5] Cheng Huang, Minghua Chen, and Jin Li. Pyramid codes: flexible schemes to trade space for access efficiency in reliable data storage systems. In *6th IEEE International Symposium on Network Computing and Applications (NCA 2007)*, pages 79–86, 2007.

[6] Jonathan Katz and Luca Trevisan. On the efficiency of local decoding procedures for error-correcting codes. In *32nd ACM Symposium on Theory of Computing (STOC)*, pages 80–86, 2000.

[7] Swastik Kopparty, Shubhangi Saraf, and Sergey Yekhanin. High-rate codes with sublinear-time decoding. In *43nd ACM Symposium on Theory of Computing (STOC)*, pages 167–176, 2011.

[8] K. V. Rashmi, Nihar B. Shah, and P. Vijay Kumar. Optimal exact-regenerating codes for distributed storage at the MSR and MBR points via a product-matrix construction. Arxiv 1005.4178, 2010.

[9] Michael Tsfasman, Serge Vladut, and Dmitry Nogin. *Algebraic geometric codes: basic notions.* American Mathematical Society, Providence, Rhode Island, USA, 2007.

[10] Sergey Yekhanin. Towards 3-query locally decodable codes of subexponential length. *Journal of the ACM*, 55:1–16, 2008.

[11] Sergey Yekhanin. Locally decodable codes. *Foundations and trends in theoretical computer science*, 2011. To appear. Preliminary version available for download at http://research.microsoft.com/en-us/um/people/yekhanin/Papers/LDC_now.pdf.

A Spaces spanned by general position vectors

Lemma 27. *Let $q \geqslant n$ be a prime power. The set of supports of vectors in any linear space $\mathcal{V} \subseteq \mathbb{F}_q^n$ is closed under union.*

Proof. Consider two vectors $\mathbf{a}$ and $\mathbf{b}$ in $\mathcal{V}$ with $\mathsf{Supp}(\mathbf{a}) = S$ and $\mathsf{Supp}(\mathbf{b}) = T$. We may assume that $|S|, |T| \leqslant n-1$ and that one set does not contain the other. Now consider $\mathbf{a} + \lambda\mathbf{b}$ for $\lambda \in F_q^*$. It suffices to find λ such that $\mathbf{a}(i) + \lambda\mathbf{b}(i) \neq 0$ for each $i \in S \cap T$. This rules out at most $|S \cap T| \leqslant n-2$ values of λ, so there is a solution provided $q - 1 > n - 2$ or $q \geqslant n$. □

It is easy to see that the condition $q \geqslant n$ is tight by considering the length 3 parity check code over $\mathbb{F}_2$, where the set of supports is not closed under union.

Theorem 28. *Let $q \geqslant n$. Let $\{\mathbf{c}_1, \ldots, \mathbf{c}_h\}$ be vectors with supports matching G in general position which span a space $\mathcal{V}$. $\mathsf{Supp}(\mathcal{V})$ consists of all sets of the form $\cup_{j \in J}\Gamma(j) \setminus I$ where I satisfies the condition $|\Gamma_J(I')| > |I'|$ for every $I' \subseteq I$.*

Proof. Theorem 24 shows that the condition on I is necessary, we now show that it is sufficient. For $j \notin \Gamma(I)$ the sets $\Gamma(j)$ and I are disjoint. Hence we can write

$$\cup_{j\in J}\Gamma(j) \setminus I = (\cup_{j\in J\cap\Gamma(I)}\Gamma(j) \setminus I) \bigcup (\cup_{j\in J\cap\overline{\Gamma(I)}}\Gamma(j)).$$

By the closure under union, it suffices to prove the statement in the case when $J \subseteq \Gamma(I)$. Fix $j_0 \in J$ and let $J' = J \setminus \{j_0\}$. Since $|\Gamma_J(I')| > |I'|$ we have $|\Gamma_{J'}(I')| \geqslant |I'|$ for every $I' \subseteq I$. So there is a matching from I to some subset $J'' \subseteq J'$ where $|J''| = |I|$, and the matrix $C_{I,J''}$ is of full rank since the $\mathbf{c}_j$s are in general position.

Let $\pi(\mathbf{c})$ denote the restriction of a vector $\mathbf{c}$ onto coordinates in I. Since $C_{I,J''}$ is invertible, the row vectors $\{\pi(\mathbf{c}_j)\}_{j\in J''}$ have full rank. Note that $\pi(\mathbf{c}_{j_0})$ is not a zero vector since $j_0 \in \Gamma(I)$. So there exist $\{\mu_j\}$ for $j \in J$ which are not all 0 and

$$\pi(\mathbf{c}_{j_0}) = \sum_{j\in J''} \mu_j \pi(\mathbf{c}_j).$$

Now consider the vector $\mathbf{c}'_{j_0} = \mathbf{c}_{j_0} - \sum_{j\in J''} \mu_j \mathbf{c}_j$. Note that $\pi(\mathbf{c}'_{j_0})$ is a zero vector, which shows that $\mathsf{Supp}(\mathbf{c}'_{j_0}) \subseteq \cup_{j\in J''\cup\{j_0\}}\Gamma(j) \setminus I$. We will show that equality holds by using corollary 25. Since we have eliminated $|I|$ vectors, the linear combination must involve at least $|I|+1$ vectors, which means that $\mu_j \neq 0$ for all j. Further the set of eliminated co-ordinates cannot be larger than I, since this would violate corollary 25. Hence we have

$$\mathsf{Supp}(\mathbf{c}'_{j_0}) = \cup_{j\in J''\cup\{j_0\}}\Gamma(j) \setminus I. \tag{21}$$

By repeating this argument for every $j_0 \in J$, we will be able to find $J(j_0) \subseteq J$ of size $|I|+1$ which contains j_0 and a vector $\mathbf{c}'_{j_0}$ such that

$$\mathsf{Supp}(\mathbf{c}'_{j_0}) = \cup_{j\in J(j_0)}\Gamma(j) \setminus I.$$

Using the closure under union of supports, we conclude that $\mathsf{Supp}(\mathcal{V})$ contains the set

$$\cup_{j_0\in J} \cup_{j\in J(j_0)} \Gamma(j) \setminus I = \cup_{j\in J}\Gamma(j) \setminus I.$$

□

ECCC ISSN 1433-8092
http://eccc.hpi-web.de