ELSEVIER

Discrete Applied Mathematics 102 (2000) 3–36

DISCRETE APPLIED MATHEMATICS

Asymptotically optimal erasure-resilient codes for large disk arrays

Yeow Meng Chee[a], Charles J. Colbourn[b,*], Alan C.H. Ling[c]

[a] *Information Technology Institute, National Computer Board, Science Park Drive, Singapore 0511*
[b] *Department of Computer Science, University of Vermont, Burlington, VT 05405, USA*
[c] *Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1*

Received 2 October 1998; revised 15 June 1999; accepted 21 June 1999

Abstract

Reliability is a major concern in the design of large disk arrays. Hellerstein et al. pioneered the study of erasure-resilient codes that allow one to reconstruct the original data even in the presence of disk failures. In this paper, we take a set systems view of the problem of constructing erasure-resilient codes. This leads to interesting extremal problems in finite set theory. Solutions to some of these problems are characterized by well-known combinatorial designs. In other instances, combinatorial designs are shown to give asymptotically exact solutions to these problems. As a result, we improve, extend and generalize previous results of Hellerstein et al.

1. Introduction

Over the last decade, there has been a sustained exponential advance in the density and performance of semiconductor technology. With this progress came faster microprocessors as well as larger and faster primary memory devices. Improvements in secondary storage systems, on the other hand, have not kept pace. While the performance of RISC microprocessors has been increasing by more than 50% per year [25], disk transfer rates, which depend on the speed of mechanical movements and magnetic media densities, have only improved by about 20% each year [6]. This phenomenon has transformed many computationally bound applications to being I/O-bound. Indeed, Amdahl [3] already predicted about three decades ago that unless accompanied by corresponding increases in secondary storage performance, big increases in microprocessor performance can only bring about marginal improvements in overall system performance. This disparity has led to the consideration of parallelism as a means to speed

* Corresponding author.
E-mail address: Colbourn@uvm-gen.emba.uvm.edu (C.J. Colbourn)

0166-218X/00/$ - see front matter
PII: S0166-218X(99)00228-0

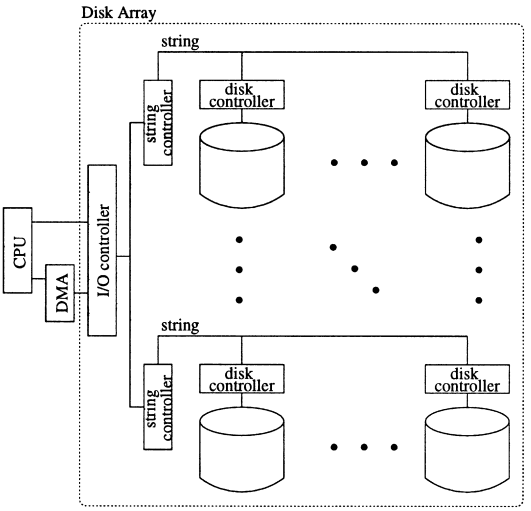


Fig. 1. Disk array architecture.

up secondary storage systems. Several ideas have been proposed as to how parallelism can be exploited. The most important and successful is the *disk array architecture*.

The *disk array architecture* organizes many independent small disks into one large logical disk, as illustrated in Fig. 1. Small disks are preferable to large ones because they have a lower cost and consume less power. For improved performance, disk arrays employ the concept of *data striping* [31], which spreads data to multiple disks. This allows both single and multiple I/O requests to be processed in parallel by separate disks, thus improving effective transfer rates. A further advantage of disk striping is uniform load balance.

The more disks we have in a disk array, the higher the performance we obtain. Unfortunately, large disk arrays have low reliability. Failures in disk arrays are often assumed to satisfy the memoryless property, that is, the life expectancy of a disk is dependent only upon the condition that the disk is working now. Under this assumption, the reliability of a disk array is modeled by the exponential distribution [13]. As a consequence, for low disk failure rates, the failure rate of a disk array is directly proportional to the number of disks it contains. Many applications, notably database and transaction processing systems, require both high throughput and high data availability of their storage systems. The most demanding of these applications require continuous operation, which in terms of a storage system requires

(i) the ability to satisfy all requests for data even in the presence of disk failures, and
(ii) the ability to reconstruct the content of a failed disk onto a replacement disk, thereby restoring itself to a fault-free state.

These requirements strongly encourage the introduction of redundancy to tolerate disk failures. Disk arrays which incorporate redundancy have come to be known as *redundant arrays of inexpensive disks* (RAID).

There are three primary types of disk failures. The first, called *transient errors*, arise from noise corruption and are dealt with by repeating the requests. The second, called *media defects*, are caused by permanent defects in material, and are detected and masked by the manufacturer. The last are *catastrophic failures*, such as head crashes and failures of the disk controller electronics. When a disk suffers a catastrophic failure, its data is rendered unreadable, and is effectively erased. We therefore call such a disk failure *an erasure*. For convenience, we also call a set of k disk failures *a k-erasure*. Error-correcting codes can be used to tolerate erasures. However, components in disk arrays allow us to determine exactly where erasures have occurred. It is possible to take advantage of this additional information to derive codes that are better than those based on error-correcting codes.

Hellerstein et al. [16] pioneered the study of erasure-resilient codes for large disk arrays. Earlier, Rabin [26] had investigated erasure-resilient codes for information dispersal, but his codes are not particularly suited for disk array applications. Very recently, Alon et al. [2] have also studied erasure-resilient codes to combat bursty losses in packet-switched networks. The parameters of interest there are also different from those for disk arrays.

In this paper, we address the problem of designing erasure-resilient codes for large disk arrays along the theme of [16]. By interpreting the coding problem in the context of extremal set theory, we obtain new classes of optimal and asymptotically optimal erasure-resilient codes. These codes improve and extend previous results in the literature. Our treatment also reveals interesting and surprising connections to combinatorial design theory.

2. Preliminaries

Let $\mathbf{x}=(x_1,\ldots,x_n)\in\{0,1\}^n$. The *weight* of $\mathbf{x}$, denoted $\mathrm{wt}(\mathbf{x})$, is the number $\sum_{i=1}^{n} x_i$. The *support* of $\mathbf{x}$, denoted $\mathrm{supp}(\mathbf{x})$, is the set $\{i \mid x_i = 1\}$.

A *data stripe*, or simply *stripe*, is the minimum amount of contiguous user data allocated to one disk before any data is allocated to any other disk. The size of a stripe must be an integral number of sectors, and is often the minimum unit of update used by system software. Because of this, we can view each disk as a collection of (disjoint) stripes.

Definition 2.1. An $[n,c,k]$-*erasure-resilient code*, or briefly an $[n,c,k]$-ERC, consists of an encoding algorithm $\mathscr{E}$ and a decoding algorithm $\mathscr{D}$ with the following properties. Given an n-tuple S of stripes, $\mathscr{E}$ produces an $(n+c)$-tuple $\mathscr{E}(S)=(\mathscr{E}_1(S),\ldots,\mathscr{E}_{n+c}(S))$ of stripes, called a *codeword*, such that for any $I\subseteq\{1,\ldots,n\}$, where $|I|=n+c-k$, the decoding algorithm $\mathscr{D}$ is able to recover S from $(I,\{\mathscr{E}_i(S)\mid i\in I\})$.

We often call an $[n,c,k]$-ERC a k-ERC when the parameters n and c are not important in the context.

To see the relevance of an $[n,c,k]$-ERC to the protection of data loss in a RAID, suppose that we have a piece of data which is partitioned into an n-tuple S of stripes. Given an $[n,c,k]$-ERC, we encode S into a codeword $(\mathscr{E}_1(S),\ldots,\mathscr{E}_{n+c}(S))$, and for $1\leqslant i\leqslant n+c$, store $\mathscr{E}_i(S)$ on disk i of a disk array with $n+c$ disks. The definition of an $[n,c,k]$-ERC ensures that we can reconstruct the original data in the presence of up to k erasures.

For performance reasons, the erasure-resilient codes we study throughout this paper are assumed to satisfy the following two conditions, as in [16].

(i) We restrict ourselves to *systematic* codes. An $[n,c,k]$-ERC is *systematic* if $\mathscr{E}_i(S)=S_i$, for $1\leqslant i\leqslant n$, where $S=(S_1,\ldots,S_n)$. The stripes $\mathscr{E}_i(S)$, for $n<i\leqslant n+c$, are called *checks*. This means that the encoding function leaves the data unmodified on some disks. This property is desirable to avoid read penalties associated with decoding when there are no disk failures.

(ii) We restrict ourselves to *linear* codes over the field $\mathbb{F}_{2^L}$, where L is the bit-size of a stripe. In this case, we interpret a stripe as an L-dimensional vector over $\mathbb{F}_2$, and $\mathscr{E}$ is a linear function. Hence, computations used to encode a stripe are restricted to component-wise modulo two arithmetic, that is, the parity operation $\oplus$. This restriction ensures that encodings and manipulations can be performed efficiently.

Restriction (i) above allows us to separate disks into *information disks*, which contain the original data, and *check disks*, which contain the checks. In fact, restrictions (i) and (ii) imply that an $[n,c,k]$-ERC can be described in terms of a $c\times(n+c)$ matrix $H=[C\,|\,I]$ over $\mathbb{F}_2$, where I is the $c\times c$ identity matrix and C is a $c\times n$ matrix that determines the equations for the checks. This is a well-known result in the theory of error-correcting codes [18]. The matrix H is called the *parity-check matrix* of the code. Given the parity-check matrix $H=[C\,|\,I]$ of a k-ERC, we can think of the rows of C (as well as the rows and columns of I) as being indexed by the check disks of a disk array, and the columns of C as being indexed by the information disks. The content of check disk i is the modulo two sum of the content of those information disks, whose columns they index in C have a one in row i.

The following are some metrics of an erasure-resilient code that are important for disk arrays.

Check disk overhead: This is the ratio of the number of check disks to information disks. An $[n,c,k]$-ERC has a check disk overhead of c/n.

Update penalty: This is the number of check disks whose content must be changed when an update is made in the content of a given information disk. We call these disks the *disks associated with the information disk*. If m check disks need to be involved in every write, then the parallelism of the disk array is reduced by a factor of $m+1$. Since parallelism is the reason behind using disk arrays, update penalties should be kept as small as possible. The update penalties of an erasure- resilient code with parity-check matrix $H=[C\,|\,I]$ are the column sums of C.

Group size: This is the number of disks that must be accessed during the reconstruction of a single failed disk. The cost of reconstruction makes small group size

desirable, while for load balancing reasons, uniform group size is desirable. The group sizes of an erasure-resilient code are the row sums of its parity-check matrix.

Since updates of data are usually much more frequent than the reconstruction of data due to erasures, the update penalties are typically of more concern than the group sizes.

3. Properties of parity-check matrices

Suppose $H = [C \mid I]$ has a set of k or fewer linearly dependent columns (over $\mathbb{F}_2$). The failure of the corresponding disks makes reconstruction of data impossible. In fact, this is the only situation in which disk failures are irrecoverable.

Lemma 3.1 (Hellerstein et al. [16]). *A set of disk failures is recoverable if and only if the corresponding set of columns in its parity-check matrix is linearly independent.*

It follows that H is the parity-check matrix of a k-ERC if and only if every set of k columns of H contains no nonempty set of linearly dependent columns. Precisely the same condition determines when H is the parity-check matrix of a k-error-detecting code [18].

Corollary 3.2. *A* k-ERC *is equivalent to a* k*-error-detecting code.*

This equivalence between k-ERC and k-error-detecting codes means that results on error-detecting codes can be brought to bear. However, the study of codes for error detection has not focused on the metrics discussed in the previous section. Indeed, as observed in [16], many of these codes are not suitable for disk array applications because they have large update penalties.

Corollary 3.3. $H = [C \mid I]$ *is the parity-check matrix of a* k-ERC *if and only if for every* $t \leqslant k$ *columns,* $\mathbf{c}_1, \ldots, \mathbf{c}_t$ *of* C*, the vector* $\mathbf{x} = \oplus_{i=1}^{t} \mathbf{c}_i$ *has weight at least* $k+1-t$.

Proof. The condition is exactly what is needed for every set of at most k columns of H to be linearly independent. □

If an erasure-resilient code is able to tolerate all k-erasures, then every update must affect the content of at least $k+1$ disks (one information disk and k check disks). Thus, the update penalties of a k-ERC are at least k. In view of the importance of minimizing update penalties, we consider from here on only those k-ERC for which the update penalties are all equal to k, the minimum possible. We speak, therefore, of the update *penalty*, instead of the update *penalties* of an erasure-resilient code. The corresponding parity-check matrix $H = [C \mid I]$ has column sums for C all equal to k.

A $(k+1)$-erasure is irrecoverable if it corresponds to the failure of an information disk and its k associated check disks. We call such $(k+1)$-erasures *bad*. With update

penalty k, one can nonetheless hope to tolerate *all* $(k+1)$-erasures, except for bad ones [16]. In fact, it can happen that all t-erasures for some $t > k$ are recoverable except for those that contain bad $(k+1)$-erasures.

Definition 3.4. A t-erasure, $t \geqslant k+1$, is *bad* if it includes the failure of an information disk and all of its k associated check disks.

With this in mind, we extend Definition 2.1 to encompass this notion of higher resilience.

Definition 3.5. An $[n,c,k,l]$-ERC is an $[n,c,k]$-ERC which can tolerate all t-erasures, for $k+1 \leqslant t \leqslant l$, except for bad t-erasures.

An alternative view of an $[n,c,k,l]$-ERC is that it is an erasure-resilient code with update penalty k that is able to tolerate all t-erasures, $t \leqslant l$, except bad ones. We often write (k,l)-ERC for $[n,c,k,l]$-ERC when the parameters n and c are not important in the context. Requirements for higher reliability of disk arrays make (k,l)-ERC attractive. A (k,k)-ERC is simply a k-ERC. Corollary 3.3 can be extended to handle the more general (k,l)-ERC.

Lemma 3.6. *$H = [C \mid I]$ is the parity-check matrix of a (k,l)-ERC if and only if for every t columns, $\mathbf{c}_1, \ldots, \mathbf{c}_t$ of C, where $2 \leqslant t \leqslant l$, the vector $\mathbf{x} = \oplus_{i=1}^{t} \mathbf{c}_i$ has weight at least $l+1-t$.*

Proof. First we prove necessity. Suppose there exists $\mathbf{x} = \oplus_{i=1}^{t} \mathbf{c}_i$, for some columns $\mathbf{c}_1, \ldots, \mathbf{c}_t$ of C, such that $\mathrm{wt}(\mathbf{x}) \leqslant l-t$. Then there exists $\mathrm{wt}(\mathbf{x})$ columns of I whose sum together with $\mathbf{x}$ gives the zero vector. Hence, the corresponding s-erasure, where $s = \mathrm{wt}(\mathbf{x}) + t \leqslant l$, cannot be recovered. We may assume that this s-erasure is not bad, for otherwise we may discard information disks and their k associated check disks and obtain an s'-erasure, for some $0 < s' < s$, which is still irrecoverable.

For sufficiency, suppose to the contrary that there exists an r-erasure, $r \leqslant l$, which is irrecoverable. Then there exist columns $\mathbf{c}_1, \ldots, \mathbf{c}_t$ of C and columns $\mathbf{e}_1, \ldots, \mathbf{e}_{r-t}$ of I, such that $\left(\bigoplus_{i=1}^{t} \mathbf{c}_i\right) \oplus \left(\bigoplus_{i=1}^{r-t} \mathbf{e}_i\right) = \mathbf{0}$. This is possible if and only if the weight of $\mathbf{x} = \bigoplus_{i=1}^{t} \mathbf{c}_i$ is exactly $r-t$. Hence, $\mathrm{wt}(\mathbf{x}) = r-t \leqslant l-t$, a contradiction. □

Before we leave this section, let us make the following definition.

Definition 3.7. Given c, k, and l, define $F(c,k,l)$ to be the maximum n such that there exists an $[n,c,k,l]$-ERC.

The maximum number of information disks that can be supported by c check disks is $F(c,k,l)$, if one desires an update penalty of k and wants to tolerate all t-erasures, $t \leqslant l$, except bad ones. The important problem is: For given k and l, determine the behavior of $F(c,k,l)$ with respect to c; and construct $[n,c,k,l]$-ERC having n as close

to $F(c,k,l)$ as possible. An $[n,c,k,l]$-ERC with $n=F(c,k,l)$ is said to have *optimal check disk overhead*. We also abbreviate $F(c,k,k)$ to $F(c,k)$.

4. Turán-type problems

If X is a finite set, we denote by $\binom{X}{k}$ the set of all k-subsets of X, that is, $\binom{X}{k}=\{K\subseteq X \mid |K|=k\}$.

Definition 4.1. Let X be a finite set. A *set system*, or *configuration*, is a pair $(X,\mathscr{A})$, where $\mathscr{A}\subseteq 2^X$. The order of the set system is $|X|$. The elements of X are called *points* and the elements of $\mathscr{A}$ are called *blocks*.

A set system $(X,\mathscr{A})$ for which $\mathscr{A}\subseteq\binom{X}{k}$ is said to be *k-uniform*. The *replication number* of a point $x\in X$ is $r_x=|\{A\in\mathscr{A}\mid x\in A\}|$.

Two set systems $(X,\mathscr{A})$ and $(Y,\mathscr{B})$ are *isomorphic* if there exists a bijection $\pi: X\to Y$ such that $A\in\mathscr{A}$ if and only if $\{\pi(a)\mid a\in A\}\in\mathscr{B}$. A set system $(X,\mathscr{A})$ is said to *contain* a configuration $(Y,\mathscr{B})$ if there exists $Z\subseteq X$ and $\mathscr{C}\subseteq\mathscr{A}$ such that $(Z,\mathscr{C})$ is isomorphic to $(Y,\mathscr{B})$. If $(X,\mathscr{A})$ does not contain $(Y,\mathscr{B})$, then $(X,\mathscr{A})$ is said to *avoid* $(Y,\mathscr{B})$. In this case, we also call $(Y,\mathscr{B})$ a *forbidden configuration* of $(X,\mathscr{A})$.

The *symmetric difference* of two sets A and B is denoted $A\Delta B$.

A *Turán-type problem* takes the form: Given a family $\mathscr{F}$ of configurations, determine the maximum number of blocks in a (k-uniform) set system of order n that avoids all the configurations in $\mathscr{F}$. We now explain the role of Turán-type problems in the design of erasure-resilient codes.

Given any matrix $M\in\{0,1\}^{m\times n}$, one can define a set system $(X,\mathscr{A})$, where $X=\{1,\ldots,m\}$ and $\mathscr{A}$ contains precisely the supports of the columns of M. We call $(X,\mathscr{A})$ *the set system of M*.

Let $H=[C\mid I]$ be the parity-check matrix of an erasure-resilient code. We also call the set system of C *the set system of the erasure-resilient code*. If $(X,\mathscr{A})$ is the set system of an $[n,c,k,l]$-ERC, then with our foregoing discussion, $(X,\mathscr{A})$ is k-uniform, $|X|=c$, and $|\mathscr{A}|=n$. Therefore, the check disk overhead is $|X|/|\mathscr{A}|$, and the group sizes are one more than the replication numbers. This correspondence between set systems and parity-check matrices gives rise to Turán-type problems in erasure-resilient codes.

Lemma 4.2. *$(X,\mathscr{A})$ is the set system of a (k,l)-ERC if and only if for any $2\leqslant t\leqslant l$, there do not exist t blocks $A_1,\ldots,A_t\in\mathscr{A}$ such that $|\Delta_{i=1}^{t}A_i|\leqslant l-t$.*

Proof. Translate Lemma 3.6 into the language of set systems and observe that $\mathrm{supp}(\mathbf{u}\oplus\mathbf{v})=\mathrm{supp}(\mathbf{u})\Delta\mathrm{supp}(\mathbf{v})$ for any two vectors $\mathbf{u},\mathbf{v}\in\{0,1\}^n$. □

It follows that the construction of a (k,l)-ERC with optimal check disk overhead is precisely the Turán-type problem of determining the maximum number of blocks in a set system satisfying the condition of Lemma 4.2.

When considering (k,l)-ERC, we may assume $l \leqslant 2k-1$ for the following reason. Let $(X,\mathscr{A})$ be the set system of a (k,l)-ERC. If $\mathscr{A}$ contains at least two blocks A and A' with nonempty intersection, then $|A \Delta A'| \leqslant 2k-2$. It follows from Lemma 4.2 that $l-2 < 2k-2$, which implies $l \leqslant 2k-1$. Hence if $l \geqslant 2k$, then $\mathscr{A}$ must consist of pairwise disjoint blocks. This corresponds to the scheme where the content of each information disk is replicated on k different check disks. This scheme is able to tolerate all t-erasures, for any t, except for bad ones. For fixed update penalty, this scheme has the highest reliability, but suffers from a huge check disk overhead of k. Henceforth, we restrict our attention to $k \leqslant l \leqslant 2k-1$.

In the next section, we give a general construction for (k,l)-ERC and establish a limit on how good a (k,l)-ERC can be.

5. Expander-based construction and an upper bound

Given a set system $(X,\mathscr{A})$, one can construct a bipartite graph $G=(X \cup \mathscr{A}, E)$ as follows. The vertex sets of the bipartition are X and $\mathscr{A}$. Two vertices $x \in X$ and $A \in \mathscr{A}$ are incident if and only if $x \in A$. This graph is called the *point-block incidence graph* of $(X,\mathscr{A})$. The set system $(X,\mathscr{A})$ can be reconstructed from its point-block incidence graph.

Let S be a subset of vertices in a graph. The *neighborhood* of S, denoted $\partial(S)$, is the set of all vertices not in S that are adjacent to some vertex in S. The elements of $\partial(S)$ are called the *neighbors* of S. A vertex v is an *odd neighbor* of S if v is adjacent to an odd number of vertices in S.

Lemma 5.1. *Let $1 \leqslant k \leqslant l$ and $2 \leqslant t \leqslant l$. Let $G=(U \cup V, E)$ be a bipartite graph where each vertex in U has degree k, and such that for any subset $T \in \binom{V}{t}$,*

$$|\partial(T)| \geqslant \frac{t(k-1)+l+1}{2}.$$

Then G is the point-block incidence graph of a (k,l)-ERC.

Proof. From Lemma 4.2, it suffices to show that any $T \in \binom{V}{t}$ has at least $l+1-t$ odd neighbors. Suppose that there are only $s \leqslant l-t$ odd neighbors of T. Then there are $|\partial(T)|-s$ neighbors of T, each of which is adjacent to at least two vertices of T. Hence,

$$2(|\partial(T)|-s)+s \leqslant tk,$$

which gives

$$\begin{aligned} |\partial(T)| &\leqslant \frac{tk+s}{2} \\ &\leqslant \frac{tk+l-t}{2} \end{aligned}$$

$$= \frac{t(k-1)+l}{2}.$$

This is a contradiction. □

Lemma 5.1 shows that bipartite graphs for which the neighborhood of any set of vertices S is large relative to the size of S give erasure-resilient codes. This neighborhood property is exactly what defines an important class of graphs known as *expanders*. Unfortunately, the study of bipartite expanders have focused on the case when the sizes of the two partitions are linearly related, making them unsuitable for our application. The probabilistic construction we give next yields bipartite expanders where the sizes of the two partitions are polynomially related. The construction is a modification of the usual probabilistic construction for expanders (see [22]).

Theorem 5.2. *Let k and l be constants such that $1 \leqslant k \leqslant l$, and define $\alpha = (2k+1-l)/4$. Let $2 \leqslant t \leqslant l$. There is an integer n_0 such that for all $n > n_0$, there exists a bipartite graph $G = (U \cup V, E)$ with $|U| = n$ and $|V| = \Omega(n^\alpha)$ satisfying the following two conditions*:

(i) *each vertex in V has degree k*;

(ii) *for every $T \in \binom{V}{t}$, we have $|\partial(T)| \geqslant (t(k-1)+l+1)/2$.*

Proof. Let $|V| = dn^\alpha$ for some positive constant d. Consider a random bipartite graph on the vertices in U and V, in which each vertex of V chooses its k neighbors by sampling a k-subset of vertices from U independently and uniformly from $\binom{U}{k}$. The bipartite graph so constructed satisfies condition (i).

Let $\mathbb{E}_t$ denote the event that a subset of t vertices from V has fewer than $s = (t(k-1)+l+1)/2$ neighbors in U. Fix any $T \in \binom{V}{t}$ and any $S \in \binom{U}{s}$. There are $\binom{dn^\alpha}{t}$ ways of choosing T and $\binom{n}{s}$ ways of choosing S. The probability that S contains $\partial(T)$ is $\left(\binom{s}{k} / \binom{n}{k}\right)^t$. Thus, the probability of the event that all the edges emanating from some t vertices of V fall within any s vertices of U is bounded as follows:

$$\mathbf{Pr}[\mathbb{E}_t] \leqslant \binom{dn^\alpha}{t} \binom{n}{s} \left[\frac{\binom{s}{k}}{\binom{n}{k}}\right]^t.$$

Using the inequalities $\binom{n}{k} \leqslant (ne/k)^k$ and $\binom{n}{k} \geqslant (n/k)^k$, we obtain

$$\mathbf{Pr}[\mathbb{E}_t] \leqslant O(n^{-(t-2)(l+1)/4}).$$

The probability that the bipartite graph fails to satisfy (ii) is at most $\sum_{t=2}^{l} \mathbf{Pr}[\mathbb{E}_t]$, which can be made to be less than one for n large enough by an appropriate choice of d. The desired result follows. □

Next, we establish an upper bound on $F(c,k,l)$. First, let us recall some definitions from design theory.

Definition 5.3. A t-$(v,k,1)$ *packing* is a k-uniform set system, $(X, \mathscr{A})$, of order v, such that every t-subset of X is contained in at most one block of $\mathscr{A}$.

Definition 5.4. A t-$(v,k,1)$ *design* is a k-uniform set system, $(X,\mathscr{A})$, of order v, such that every t-subset of X is contained in precisely one block of $\mathscr{A}$.

A 2-$(v,3,1)$ design is known as a *Steiner triple system* of order v, denoted STS(v). A 3-$(v,4,1)$ design is known as a *Steiner quadruple system* of order v, denoted SQS(v). A t-$(v,k,1)$ design is *cyclic* if its element set is $\mathbb{Z}_v$, and whenever $\{x_1,\ldots,x_k\}$ is a block, so also is $\{x_1+1,\ldots,x_k+1\}$ (with arithmetic modulo v). A set of representatives of the orbits under the action of $\mathbb{Z}_v$ is called a set of *base* blocks.

The maximum number of blocks in a t-$(v,k,1)$ packing is denoted $D(v,k,t)$. Then $D(v,k,t)\leqslant \binom{v}{t} / \binom{k}{t}$ with equality if and only if there exists a t-$(v,k,1)$ design.

Theorem 5.5. *Let k and l be constants such that $1\leqslant k\leqslant l$. Then $F(c,k,l) = \mathrm{O}(c^{k+1-\lfloor l/2\rfloor})$.*

Proof. Consider all configurations of two blocks of size k intersecting in at least $k+1-\lfloor l/2\rfloor$ points. Any set system $(X,\mathscr{A})$ of an $[n,c,k,l]$-ERC must avoid all such configurations, for otherwise it would violate the condition of Lemma 4.2. Hence, any two blocks of $(X,\mathscr{A})$ intersect in at most $k-\lfloor l/2\rfloor$ points. It follows that $(X,\mathscr{A})$ is a $(k+1-\lfloor l/2\rfloor)$-$(c,k,1)$ packing. Hence,

$$|\mathscr{A}|\leqslant \frac{\binom{c}{k+1-\lfloor l/2\rfloor}}{\binom{k}{k+1-\lfloor l/2\rfloor}} = \mathrm{O}(c^{k+1-\lfloor l/2\rfloor}). \qquad \square$$

Theorems 5.2 and 5.5 give the following.

Corollary 5.6. *For any fixed k and l such that $1\leqslant k\leqslant l$, there exist positive constants a_1 and a_2 such that*

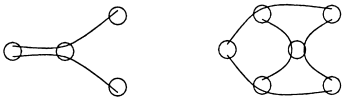
$$a_1 c^{(2k+1-l)/4}\leqslant F(c,k,l)\leqslant a_2 c^{k+1-\lfloor l/2\rfloor},$$

for all positive integer c.

For general k, the only previously known lower bound on $F(c,k,l)$ is due to Hellerstein et al. [16] and applies when $l=k$.

Theorem 5.7 (Hellerstein et al. [16])**.** *For any positive integer k, $F(c,k)\geqslant(1-\mathrm{o}(1))\binom{c}{2}/\binom{k}{2}$.*

For $k\leqslant l\leqslant 2k-8$ (hence $k\geqslant 8$), the (k,l)-ERC we built from expanders are at least as reliable and have asymptotically better check disk overheads than those provided by Theorem 5.7. The theorem is proved by establishing that every 2-$(v,k,1)$ packing with b blocks is a $[b,v,k]$-ERC. One might hope that, when k is large enough, a 3-$(v,k,1)$ packing might also give a $[b,v,k]$-ERC. However, this condition does not suffice. When $k=2s$, for instance, form a complete bipartite graph $K_{s,s}$ and add a second copy of each



(a) P_1 (b) P_2

Fig. 2. Forbidden configurations for $(3,4)$-ERC.

edge. Now label each of the $2s^2$ edges with distinct symbols, and form $2s$ sets each of size $2s$ by listing, for each vertex, the labels of the edges incident with the vertex. No two of these share more than two symbols, but by Lemma 4.2 it corresponds to an irrecoverable k-erasure.

The exponent in the upper bound of Corollary 5.6 is about twice that for the lower bound. We believe the upper bound to be the true asymptotic behavior of $F(c,k,l)$, but tightening the lower bound in general appears difficult. In Sections 6 and 7, we give exact and asymptotically exact bounds for several cases when k is small.

6. Optimal $(3,l)$-ERC and anti-Pasch Steiner triple systems

An extensive treatment of $(3,l)$-ERC was given by Hellerstein et al. [16] for $l=3$ and 4. We summarize their results next.

Lemma 6.1 (Hellerstein et al. [16]). *$(X,\binom{X}{3})$ is the set system of a* 3-ERC. *Hence*, $F(c,3)=\binom{c}{3}$.

Lemma 6.2 (Hellerstein et al. [16]). *For any positive integer c, $F(c,3,4)\leqslant c(c-1)/6$, with equality if c is a power of* 3. *If $c\equiv 3 \pmod 6$, then $F(c,3,4)\geqslant c(c-3)/6$.*

We can improve on Lemma 6.2 by examining the set system of a $(3,4)$-ERC. The only 3-uniform configurations $(Y,\mathscr{B})$, $2\leqslant|\mathscr{B}|\leqslant 4$, for which $|\Delta_{B\in\mathscr{B}}B|\geqslant 4-t$, are those shown in Fig. 2. By Lemma 4.2, these configurations must be avoided by the set system of any $(3,4)$-ERC.

Forbidding P_1 from the set system $(X,\mathscr{A})$ of an $[n,c,3,4]$-ERC is equivalent to saying that $(X,\mathscr{A})$ is a 2-$(c,3,1)$ packing. The configuration P_2 is known in the design theory literature under various names: *quadrilateral*, *Pasch configuration*, *fragment*, or *arrow* (see [9]). A 2-$(v,3,1)$ packing that does not contain a Pasch configuration is called *anti-Pasch* or *quadrilateral-free* (QF). The construction of $(3,4)$-ERC with optimal check disk overhead is therefore equivalent to the following problem.

Problem 6.3. Determine the maximum number of blocks in an anti-Pasch 2-$(v,3,1)$ packing.

The maximum number of blocks in a 2-$(v,3,1)$ packing has been determined a long time ago [32]:

$$D(v,3,2)=\begin{cases}\lfloor\frac{v}{3}\lfloor\frac{v-1}{2}\rfloor\rfloor-1, & \text{if } v\equiv 5\,(\mathrm{mod}\,6),\\ \lfloor\frac{v}{3}\lfloor\frac{v-1}{2}\rfloor\rfloor, & \text{otherwise.}\end{cases}$$

However, a complete solution to Problem 6.3 is not known. An anti-Pasch 2-$(v,3,1)$ packing with $D(v,3,2)$ blocks is said to be *optimal*. We believe that for all sufficiently large v, there exists an optimal anti-Pasch 2-$(v,3,1)$ packing. It is sufficient to treat the cases $v\equiv 1,\ 3,$ or $5\,(\mathrm{mod}\,6)$:

Lemma 6.4. *Let* $v\equiv 1,\ 3,$ *or* $5\,(\mathrm{mod}\,6)$. *If there exists an optimal anti-Pasch* 2-$(v,3,1)$ *packing, then there exists an optimal anti-Pasch* 2-$(v-1,3,1)$ *packing.*

Proof. Schönheim [32] has shown that for $v\equiv 1,\ 3,$ or $5\,(\mathrm{mod}\,6)$, every 2-$(v,3,1)$ packing with $D(v,3,2)$ blocks contains a 2-$(v-1,3,1)$ packing with $D(v-1,3,2)$ blocks. □

Already 20 years ago, Erdös [10] made the conjecture that there exists an anti-Pasch STS(v) for all $v\equiv 1$ or $3\,(\mathrm{mod}\,6)$ whenever v is sufficiently large. The unique STS(7) and the two nonisomorphic STS(13) contain Pasch configurations. Brouwer [5] refined Erdös' conjecture as follows.

Conjecture 6.5 (Brouwer [5])**.** *There exists an anti-Pasch* STS(v) *for all* $v\equiv 1$ *or* $3\,(\mathrm{mod}\,6)$, except when $v=7$ or 13.

Conjecture 6.5 is known to be true for $v\equiv 3\,(\mathrm{mod}\,6)$.

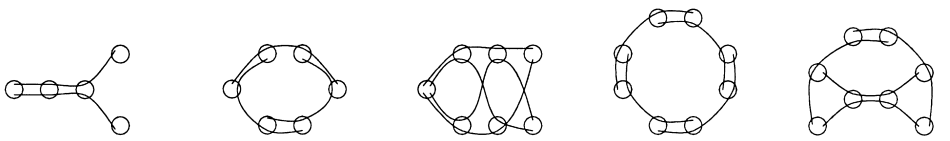
Theorem 6.6 (Brouwer [5])**.** *There exists an anti-Pasch* STS(v) *for all* $v\equiv 3\,(\mathrm{mod}\,6)$.

The results for anti-Pasch STS(v), $v\equiv 1\,(\mathrm{mod}\,6)$ are more fragmented; see [9] for a survey, and [17] for recent results. So by observing the equivalence between $[n,c,3,4]$-ERC with optimal check disk overhead and optimal anti-Pasch 2-$(c,3,1)$ packings, we can improve Lemma 6.2 as follows.

Lemma 6.7. *For each positive integer* c, *we have* $F(c,3,4)\leqslant D(c,3,2)$, *with equality if* $c\equiv 2$ *or* $3\,(\mathrm{mod}\,6)$.

Proof. Follows from Theorem 6.6 and Lemma 6.4. □

We now turn our attention to $(3,5)$-ERC. It turns out that there are no configurations in addition to P_1 and P_2 which need to be avoided by the set system of a $(3,5)$-ERC. Consequently, every $(3,4)$-ERC is also a $(3,5)$-ERC.



(a) Q_1 (b) Q_2 (c) Q_3 (d) Q_4 (e) Q_5

Fig. 3. Forbidden configurations for 4-ERC.

Lemma 6.8. *For each positive integer c, we have $F(c,3,5) = F(c,3,4)$.*

7. Asymptotically optimal $(4, l)$-ERC

The only previously known result concerning $(4, l)$-ERC is the lower bound $F(c,4) \geqslant (1 - o(1))c(c-1)/12$ given by Theorem 5.7. Hellerstein et al. [16] posed the open problem of determining $F(c,4)$.

7.1. Finite field construction for $l \in \{4,5\}$

Lemma 4.2 implies that for $(X, \mathscr{A})$ to be the set system of an $[n,c,4]$-ERC, it is necessary and sufficient to avoid the five configurations in Fig. 3. Avoiding Q_1 means that $(X, \mathscr{A})$ is a 3-$(c,4,1)$ packing. Therefore, $F(c,4) \leqslant D(c,4,3)$. It follows that $F(c,4) = c(c-1)(c-2)/24$ if and only if there exists an SQS(c) that avoids all the configurations Q_2, Q_3, Q_4, and Q_5. At present, we do not know of any example of an SQS(c), $c > 4$, that avoids all these configurations. For a comprehensive survey on Steiner quadruple systems, we refer the reader to [15].

Here, we address the more difficult problem of constructing $(4,5)$-ERC, and in the process, obtain asymptotically exact bounds on both $F(c,4)$ and $F(c,4,5)$. A short computation demonstrates that in order for $(X, \mathscr{A})$ to be the set system of an $[n,c,4,5]$-ERC, it is necessary and sufficient to avoid Q_i, $1 \leqslant i \leqslant 5$, and the nine configurations shown in Fig. 4. The remainder of this section describes a finite field construction for $(4,5)$-ERC.

Definition 7.1. A set system $(X, \mathscr{A})$ is k-partite if there is a partition of X into k parts, $X = X_1 \cup \cdots \cup X_k$, such that for every block $A \in \mathscr{A}$, we have $|A \cap X_i| \leqslant 1$, for $1 \leqslant i \leqslant k$.

One idea we use to simplify our construction is to restrict our attention to set systems of $(4,5)$-ERC that are 4-partite. It is known [11] that for every k-uniform set system $(X, \mathscr{A})$, one can find a k-partite set system $(X, \mathscr{B})$, where $\mathscr{B} \subseteq \mathscr{A}$, such that $|\mathscr{B}| \geqslant (k!/k^k)|\mathscr{A}|$. So our restriction to 4-partite set systems is not a severe one, and affects $F(c,4,l)$ by at most a constant factor of $32/3$. The configurations Q_i, $i \in \{2,6,7,8,9,10,11,12,13,14\}$, are not 4-partite. Hence, they are avoided by any 4-partite

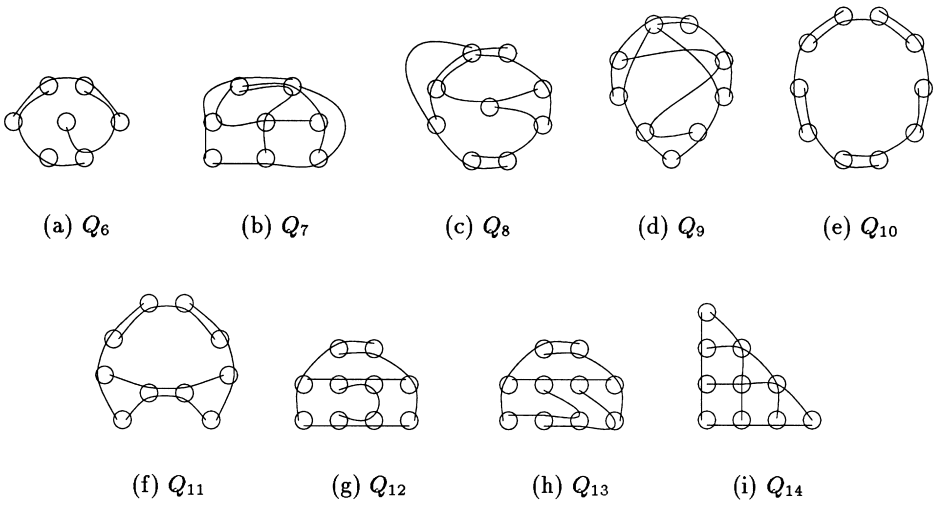


Fig. 4. Forbidden configurations in $(4,5)$-ERC.

set system. It therefore suffices to construct 4-partite set systems that avoid Q_i for $i \in \{1,3,4,5\}$.

Definition 7.2. An extension of a set system $(X,\mathscr{A})$ by a point $\infty \notin X$ is the set system $(X \cup \{\infty\},\mathscr{B})$, where $\mathscr{B} = \{A \cup \{\infty\} \mid A \in \mathscr{A}\}$.

We now describe the finite field construction. Let q be an odd prime power and let ω be a primitive element of $\mathbb{F}_q$. For each i, $1 \leqslant i \leqslant (q-1)/2$, define a set system $(X_i,\mathscr{B}_i)$, where

$$X_i = \mathbb{F}_q \times \{0,1,2\}$$

and

$$\mathscr{B}_i = \{\{(a,0),(b,1),(a+\omega^i b,2)\} \mid a,b \in \mathbb{F}_q,\ b \neq 0\}.$$

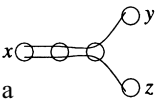
Now let $(Y_i,\mathscr{C}_i)$ be the extension of $(X_i,\mathscr{B}_i)$ by the point ∞_i, $1 \leqslant i \leqslant (q-1)/2$. Finally, define $(Y,\mathscr{C})$ so that

$$Y = \bigcup_{i=1}^{(q-1)/2} Y_i \quad \text{and} \quad \mathscr{C} = \bigcup_{i=1}^{(q-1)/2} \mathscr{C}_i.$$

For $1 \leqslant i \leqslant (q-1)/2$, $(X_i,\mathscr{B}_i)$ is a 2-$(3q,3,1)$ packing, and $(Y,\mathscr{C})$ is a 4-uniform set system. Since each block in $\mathscr{C}$ intersects each of the sets $\mathbb{F}_q \times \{0\}$, $\mathbb{F}_q \times \{1\}$, $\mathbb{F}_q \times \{2\}$, and $\{\infty_1,\ldots,\infty_{(q-1)/2}\}$ in exactly one point, and these sets partition Y, $(Y,\mathscr{C})$ is also 4-partite. The lemmas that follow show that $(Y,\mathscr{C})$ avoids several configurations.

Lemma 7.3. *The set system $(Y,\mathscr{C})$ avoids Q_1.*

Proof. Suppose $(Y, \mathscr{C})$ contains the configuration below:



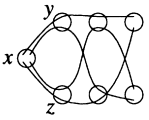
Without loss of generality, either $x = \infty_i$, or $y = \infty_i$ and $z = \infty_j$, for some $i \neq j$.

If $x = \infty_i$, then some $(X_i, \mathscr{B}_i)$ must contain P_1, which contradicts the fact that $(X_i, \mathscr{B}_i)$ is a 2-$(3q, 3, 1)$ packing.

If $y = \infty_i$ and $z = \infty_j$, then there exists $\{(a,0),(b,1),(c,2)\} \in \mathscr{B}_i \cap \mathscr{B}_j$. This is only possible if $b = 0$, a contradiction. □

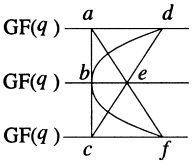
Lemma 7.4. *The set system* $(Y, \mathscr{C})$ *avoids* Q_3.

Proof. Suppose $(Y, \mathscr{C})$ contains the configuration below:



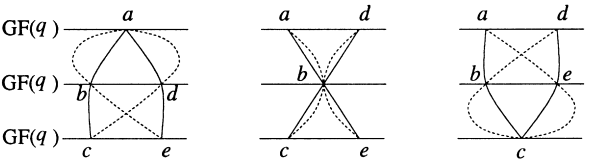
Without loss of generality, either $x = \infty_i$, or $y = \infty_i$ and $z = \infty_j$, for some $i \neq j$.

If $x = \infty_i$, then $(X_i, \mathscr{B}_i)$ contains P_2. The only way P_2 can occur in $(X_i, \mathscr{B}_i)$ is as follows.



But this implies $c = a + \omega^i b = d + \omega^i e$ and $f = a + \omega^i e = d + \omega^i b$, which can only be satisfied if $b = e$. This is a contradiction.

If $y = \infty_i$ and $z = \infty_j$, then $(X_i, \mathscr{B}_i)$ and $(X_j, \mathscr{B}_j)$ must contain four blocks (two from each of $\mathscr{B}_i, \mathscr{B}_j$) that occur in one of the following three ways:

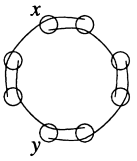


The blocks in $\mathscr{B}_i$ are shown in solid lines and those in $\mathscr{B}_j$ are shown in dashed lines. In the first situation, we have $c = a + \omega^i b = a + \omega^j d$ and $e = a + \omega^i d = a + \omega^j b$, which can only be satisfied if $b = d$. In the second situation, we have $c = d + \omega^i b = a + \omega^j b$ and $e = a + \omega^i b = d + \omega^j b$, which can only be satisfied if $a = d$. For the last situation,

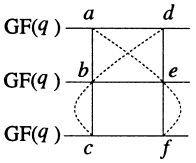
we have $c = a + \omega^i b = d + \omega^j e = a + \omega^i e = d + \omega^j b$, which can only be satisfied if $b = e$. All these lead to contradictions. □

Lemma 7.5. *The set system* $(Y, \mathscr{C})$ *avoids* Q_4.

Proof. Suppose $(Y, \mathscr{C})$ contains the configuration below:



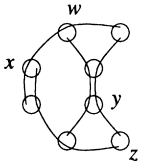
Without loss of generality, we may assume $x = \infty_i$ and $y = \infty_j$, for some $i \neq j$. Then $(X_i, \mathscr{B}_i)$ and $(X_j, \mathscr{B}_j)$ must contain four blocks (two from each of $\mathscr{B}_i, \mathscr{B}_j$) that occur as shown here:



The blocks in $\mathscr{B}_i$ are shown in solid lines and those in $\mathscr{B}_j$ are shown in dashed lines. But this implies that $c = a + \omega^i b = d + \omega^j b$ and $f = a + \omega^i e = d + \omega^j e$, which can only be satisfied if $b = e$. This is a contradiction. □

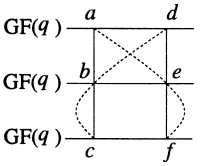
Lemma 7.6. *The set system* $(Y, \mathscr{C})$ *avoids* Q_5.

Proof. Suppose $(Y, \mathscr{C})$ contains the configuration below:



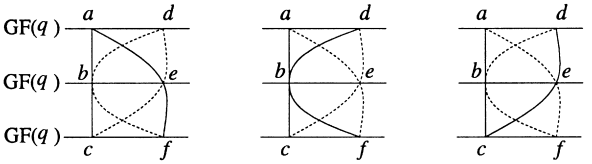
Without loss of generality, either $w = \infty_i$ and $z = \infty_j$, or $x = \infty_i$ and $y = \infty_j$, for some $i \neq j$.

If $w = \infty_i$ and $z = \infty_j$, then $(X_i, \mathscr{B}_i)$ and $(X_j, \mathscr{B}_j)$ must contain four blocks (two from each of $\mathscr{B}_i, \mathscr{B}_j$) that occur as shown here:



This, as we have seen in the proof of Lemma 7.5, is impossible.

If $x = \infty_i$ and $y = \infty_j$, then $(X_i, \mathscr{B}_i)$ and $(X_j, \mathscr{B}_j)$ must contain four blocks (two from each of $\mathscr{B}_i, \mathscr{B}_j$) that occur in one of the following three ways.



The blocks in $\mathscr{B}_i$ are shown in solid lines and the blocks in $\mathscr{B}_j$ are shown in dashed lines. The first situation gives $c = a + \omega^i b = d + \omega^j e$ and $f = a + \omega^i e = d + \omega^j b$, which can only be satisfied if $b = e$ or $\omega^i = -\omega^j$. But $-\omega^j = \omega^{j+(q-1)/2}$ since q is odd, and $i \not\equiv j \pmod{(q-1)/2}$, because $1 \leqslant i,\ j \leqslant (q-1)/2$. The second situation gives $c = a + \omega^i b = d + \omega^j e$ and $f = d + \omega^i b = a + \omega^j e$, which can only be satisfied if $d = a$. For the last situation, we have $c = a + \omega^i b = d + \omega^j e$ and $f = a + \omega^j e = d + \omega^j b$, which can only be satisfied if $b = e$ or $\omega^i = -\omega^j$. As before $\omega^i = -\omega^j$ is impossible. All these lead to contradictions. □

We now state the main result of this section.

Theorem 7.7. *Let q be an odd prime power, and let λ be an integer such that $1 \leqslant \lambda \leqslant (q-1)/2$. Then there exists an $[n, c, 4, 5]$-ERC, where $c = 3q - 1 + \lambda$ and $n = \lambda q(q-1)$.*

Proof. The set system $(\bigcup_{i=1}^{\lambda} Y_i, \bigcup_{i=1}^{\lambda} \mathscr{C}_i)$ is a 4-uniform 4-partite set system of order $3q - 1 + \lambda$ having $\lambda q(q-1)$ blocks, which avoids Q_i, $i \in \{1, 3, 4, 5\}$, by the previous lemmas. Hence, it is the set system of a $(4, 5)$-ERC. □

The asymptotic behavior of $F(c, 4)$ and $F(c, 4, 5)$ can now be determined.

Corollary 7.8. *$F(c, 4) = \Theta(c^3)$ and $F(c, 4, 5) = \Theta(c^3)$.*

Proof. Let q be the largest odd prime power at most $(2c+3)/7$. Taking $\lambda = (q-1)/2$ in Theorem 7.7 gives a $[q(q-1)^2/2, (7q-3)/2, 4, 5]$-ERC. Hence,

$$\begin{aligned} F(c, 4, 5) &\geqslant F((7q-3)/2, 4, 5) \\ &\geqslant \frac{q(q-1)^2}{2} \\ &\geqslant (1 - o(1))\, \frac{4}{343}\, c^3. \end{aligned}$$

The last inequality follows from bounds on the gap between consecutive primes (see, for example, [23]). This, together with the inequalities

$$F(c, 4, 5) \leqslant F(c, 4) \leqslant D(c, 4, 3) \leqslant \tfrac{1}{24} c^3,$$

gives the required result. □

The bound on $F(c,4,5)$ in Corollary 7.8 improves upon the results of Hellerstein et al. [16]. It is an order of magnitude better than the bound on $F(c,4)$ obtained in [16].

One drawback of the $(4,5)$-ERC constructed in Theorem 7.7 is that the group sizes are large and nonuniform. Among the $3q-1+\lambda$ points, $2q$ have replication number $\lambda(q-1)$, $q-1$ have replication number λq, and the remaining λ have replication number $q(q-1)$. When $\lambda=(q-1)/2$, all groups have size $\Theta(q^2)$, but the largest group remains about twice as big as the smallest. However, the following *splitting* process can be used to make the group sizes more uniform.

Definition 7.9. Suppose $(X,\mathscr{A})$ is a set system and $x\in X$. Let $\mathscr{A}_x=\{A\in\mathscr{A}\mid x\in A\}$ and $\mathscr{B}\subseteq\mathscr{A}_x$ such that $|\mathscr{B}|=\lfloor|\mathscr{A}_x|/2\rfloor$. Define $W=X\cup\{x'\}$ and $\mathscr{D}=(\mathscr{A}\backslash\mathscr{B})\cup\{(A\backslash\{x\})\cup\{x'\}\mid A\in\mathscr{B}\}$. Then $(W,\mathscr{D})$ is the set system obtained by splitting x in $(X,\mathscr{A})$, and is denoted $\mathrm{split}_x(X,\mathscr{A})$.

We can extend this definition to *splitting a subset* $S\subseteq X$ in $(X,\mathscr{A})$ as follows:

$$\mathrm{split}_S(X,\mathscr{A})=\begin{cases}\mathrm{split}_x(X,\mathscr{A}) & \text{if } S=\{x\},\\ \mathrm{split}_{S\backslash\{x\}}(\mathrm{split}_x(X,\mathscr{A})) & \text{if } x\in S \text{ and } |S|\geqslant 2.\end{cases}$$

Next, we show that splitting preserves erasure-resilience.

Lemma 7.10. *If $(X,\mathscr{A})$ is the set system of a (k,l)-ERC and $x\in X$, then $\mathrm{split}_x(X,\mathscr{A})$ is also the set system of a (k,l)-ERC.*

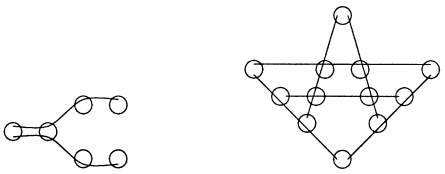
Proof. Suppose not. Then by Lemma 4.2, there exist t blocks $A_1,\ldots,A_t$ in $\mathrm{split}_x(X,\mathscr{A})$, where $2\leqslant t\leqslant l$, such that $|\Delta_{i=1}^t A_i|\leqslant l-t$. For each of the blocks $A_1,\ldots,A_t$ that contains x', replace x' by x. This does not increase the size of their symmetric difference. But now, all these blocks are in $\mathscr{A}$, contradicting the assumption that $(X,\mathscr{A})$ is the set system of a (k,l)-ERC. □

Then $\mathrm{split}_x(Y,\mathscr{C})$ is a set system of order $4q-2$ with $q(q-1)^2/2$ blocks and all replication numbers are $q^2/2$ or $q(q-1)/2$. By Lemma 7.10, this is the set system of a $(4,5)$-ERC:

Lemma 7.11. *Let q be an odd prime power. Then there exists a $[q(q-1)^2/2, 4q-2, 4, 5]$-ERC, where the group sizes are $q^2/2$ and $q(q-1)/2$.*

7.2. Transversal design construction for $l\in\{6,7\}$

Let $(X,\mathscr{A})$ be the set system of a $(4,6)$-ERC. Lemma 4.2 implies that $(X,\mathscr{A})$ must avoid the configuration Q_{15} shown in Fig. 5. Hence, $(X,\mathscr{A})$ is a 2-$(c,4,1)$ packing and $F(c,4,6)\leqslant D(c,4,2)$. This obviates the need to consider many of the configurations treated for the case when $l=5$. The only configurations that a 2-$(c,4,1)$ packing must



(a) Q_{15} (b) Q_{16}

Fig. 5. Forbidden configurations for $(4,6)$-ERC.

avoid in order for it to be the set system of a $(4,6)$-ERC is Q_{14} and Q_{16} (shown in Fig. 5).

Definition 7.12. A *transversal design*, TD(k,n), is a triple $(X,\mathscr{G},\mathscr{B})$, where X is a set of kn points, $\mathscr{G}$ is a partition of X into k parts (called *groups*), each of size n, and $(X,\mathscr{B})$ is a k-uniform set system such that every 2-subset of X is contained in exactly one group (of $\mathscr{G}$) or one block (of $\mathscr{B}$), but not both.

Definition 7.13. Let $(X,\mathscr{G},\mathscr{B})$ be a TD(k,n). The design obtained by *removing a group* $G\in\mathscr{G}$ is the triple $(X\backslash G,\mathscr{G}\backslash\{G\},\{B\backslash G\,|\,B\in\mathscr{B}\})$.

Removing a group in a TD(k,n) gives a TD$(k-1,n)$. Consider the *standard* construction of a transversal design TD$(4,q)$, where q is a prime power (see, for example, [4]). Let

$$X=\mathbb{F}_q\times\{0,1,2,3\},$$
$$\mathscr{G}=\{\mathbb{F}_q\times\{i\}\,|\,i\in\{0,1,2,3\}\}$$

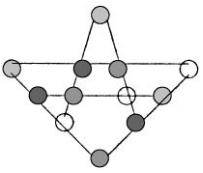
and

$$\mathscr{B}=\{\{(a,0),(b,1),(a+b,2),(a+2b,3)\}\,|\,a,b\in\mathbb{F}_q\}.$$

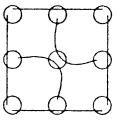
Then $(X,\mathscr{G},\mathscr{B})$ is a TD$(4,q)$. The set system $(X,\mathscr{B})$ is a 4-partite 2-$(4q,4,1)$ packing. Let $(X',\mathscr{G}',\mathscr{B}')$ be the TD$(3,q)$ obtained by removing the group $\mathbb{F}_q\times\{3\}$ in $(X,\mathscr{B},\mathscr{G})$.

Lemma 7.14. *The set system* $(X,\mathscr{B})$ *avoids* Q_{16}.

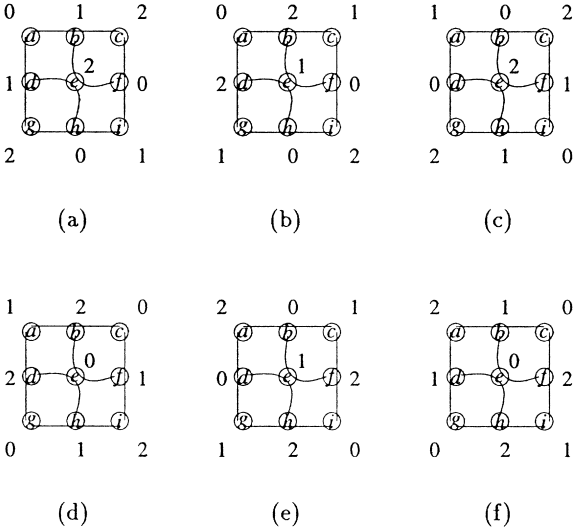
Proof. Suppose $(X,\mathscr{B})$ contains the configuration



This configuration has a unique (up to isomorphism) partition of its points into four parts so that each block contains exactly one point from each part. This partition is indicated by different shadings in the figure. Hence, the points of one of the parts must belong to $\mathbb{F}_q \times \{3\}$. Deleting all the points in any part gives the following configuration:



So $(X', \mathscr{B}')$ must contain the configuration above. There are six possibilities to consider, as shown below.



Each point is an element of $\mathbb{F}_q \times \{0,1,2\}$. The label inside a point shows its first coordinate, and the label outside a point shows its second coordinate.

Consider case (a). We have $c = a + b = f + i$, $e = b + f = d + h$, and $g = a + d = h + i$, which is only satisfied if $b = d$. This is a contradiction.

The other five cases can be disposed of similarly. □

Corollary 7.15. *$(X, \mathscr{B})$ is the set system of a* $(4,6)$-ERC.

The set system of a $(4,7)$-ERC must avoid the four configurations in Fig. 6 in addition to all the forbidden configurations for set systems of $(4,6)$-ERC.

Theorem 7.16. *Let q be a prime power. Then there exists a* $[q^2, 4q, 4, 7]$-ERC. *Moreover, this code has uniform group size q.*

Proof. We claim that $(X, \mathscr{B})$ is the set system of a $[q^2, 4q, 4, 7]$-ERC. By Corollary 7.15, we only need to show that $(X, \mathscr{B})$ avoids all the configurations in Fig. 6. None of the

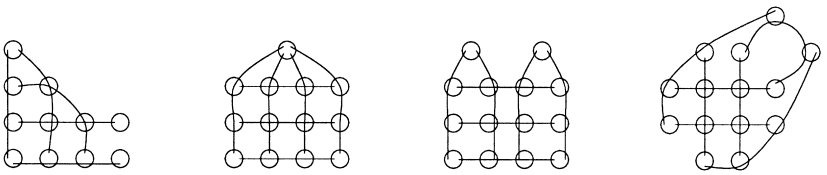


Fig. 6. Forbidden configurations for $(4,7)$-ERC.

configurations in Fig. 6 is 4-partite. Since $(X,\mathscr{B})$ is 4-partite, these configurations are all avoided. The replication number of every point in X is q. □

Corollary 7.17. *$F(c,4,6)=\Theta(c^2)$ and $F(c,4,7)=\Theta(c^2)$.*

Proof. Let q be the largest prime power at most $c/4$. Theorem 7.16 gives a $[q^2,4q,4,7]$-ERC. Hence,

$$\begin{aligned} F(c,4,7) &\geqslant F(4q,4,7)\\ &\geqslant q^2\\ &\geqslant (1-\mathrm{o}(1))\tfrac{1}{16}c^2. \end{aligned}$$

This, together with the inequalities

$$F(c,4,7)\leqslant F(c,4,6)\leqslant D(c,4,2)\leqslant \tfrac{1}{12}c^2,$$

gives the required result. □

When $c\equiv 1,4\,(\mathrm{mod}\,12)$ and c is sufficiently large, we expect that $F(c,4,7)=c(c-1)/12$. Equality occurs when $c=(3^\alpha-1)/2$ for $\alpha\geqslant y3$, using the projective spaces $\mathrm{PG}(\alpha,3)$ (see [4] for the definition and basic properties). In addition, we have found a number of sporadic small examples where equality holds. Following are base blocks for $[c(c-1)/12,c,4,7]$-ERCs (i.e., cyclic 2-$(c,4,1)$ designs) with $c\in\{40,49,52,61,64\}$:

40: $\{0,10,20,30\},\{0,1,4,13\},\{0,2,17,24\},\{0,5,26,34\}$.
49: $\{0,1,3,9\},\{0,4,18,37\},\{0,5,25,32\},\{0,10,21,36\}$.
52: $\{0,13,26,39\},\{0,1,3,11\},\{0,4,16,37\},\{0,5,14,32\},\{0,6,23,30\}$.
61: $\{0,1,3,8\},\{0,4,13,36\},\{0,6,28,49\},\{0,10,27,47\},\{0,11,30,46\}$.
64: $\{0,16,32,48\},\{0,1,3,9\},\{0,4,18,39\},\{0,5,15,41\},\{0,7,20,47\},\{0,11,30,42\}$.

It is a tedious verification that the set systems produced are $[c(c-1)/12,c,4,7]$-ERCs.

Theorem 7.18. *If a $[c(c-1)/12,c,4,7]$-ERC exists, then a $[(3c+1)3c/12,3c+1,4,7]$-ERC exists.*

Proof. Let $(V,\mathscr{B})$ be a $[c(c-1)/12,c,4,7]$-ERC. On $(V\times\{0,1,2\})\cup\{\infty\}$, place blocks as follows:

1. if $\{u,v,w,x\} \in \mathscr{B}$, include $\{(v,i_v),(w,i_w),(x,i_x),(y,i_y)\}$ for $(i_v,i_w,i_x,i_y) \in \{(0,0,0,0), (0,1,1,2),(0,2,2,1),(1,0,1,1),(1,1,2,0),(1,2,0,2),(2,0,2,2),(2,1,0,1),(2,2,1,0)\}$.
2. for $x \in V$, include $\{\infty,(x,0),(x,1),(x,2)\}$.

The verification is tedious but straightforward. □

8. Controlling group sizes by balanced orderings

Let $g_1,\ldots,g_c$ be the group sizes of an $[n,c,k,l]$-ERC. Then, $\sum_{i=1}^{c} g_i = kn + c$. So the average group size is $kn/c + 1$. Since the check disk overhead is c/n, the smaller the check disk overhead, the larger the average group size. In the previous sections, our focus has been on the construction of erasure-resilient codes with optimal and asymptotically optimal check disk overheads. Therefore, inevitably, our codes have large average group size.

It is, however, possible to trade check disk overhead for a smaller average group size. Given the parity-check matrix $[C\,|\,I]$ of an erasure-resilient code, one can simply delete the appropriate number of columns of C so that the desired average group size is obtained. However, this process does not guarantee that the maximum group size is lowered. We have indicated in Section 2 that for load-balancing reasons, uniform group size is desirable. This raises the issue of whether it is possible to construct erasure-resilient codes in which there is a way of deleting columns from its parity-check matrix so that every group size is close to the average. We now discuss this problem more formally. The terminology we use here generalizes that in [16].

Definition 8.1. Let α be a positive integer. An erasure-resilient code is said to have *α-balanced group size* if the following conditions hold:

(i) when the average group size is $1 \pmod{\alpha}$, all groups are the same size;
(ii) when the average group size is not $1 \pmod{\alpha}$, the maximum group size is at most α greater than the minimum group size.

Let M be an $m \times n$ matrix. For any i, $1 \leqslant i \leqslant n$, $M(i)$ denotes the $m \times i$ matrix comprising the first i columns of M.

Definition 8.2. Let $[C\,|\,I]$ be the parity-check matrix of an $[n,c,k,l]$-ERC, and α a positive integer. We say that the columns of C are arranged in an *α-balanced ordering* if, for any i, $1 \leqslant i \leqslant n$, $[C(i)\,|\,I]$ is the parity-check matrix of an $[i,c,k,l]$-ERC with α-balanced group size.

The existence of an α-balanced ordering for a (k,l)-ERC allows us to derive from it other (k,l)-ERC with higher check disk overhead but smaller group sizes, and whose group sizes differ from one another by at most α. Another use of balanced orderings observed by Hellerstein et al. [16] is in the design of extendible disk array systems. If we have chosen a code whose parity-check matrix has more columns

than we need, then as more disks are added to the system, the extra columns are put to use. The existence of an α-balanced ordering for the original parity-check matrix ensures that we have α-balanced group size at all times if disks are associated with columns according to this ordering. The case $\alpha = 1$ was considered in [16].

Definition 8.3. Let α be a positive integer and $(X, \mathscr{A})$ a set system. Let $\mathscr{B} \subseteq \mathscr{A}$. Then,
(i) $\mathscr{B}$ is an *α-resolution class* if every point of X is contained in precisely α blocks of $\mathscr{B}$;
(ii) $\mathscr{B}$ is a *partial α-resolution class* if every point of X is contained in at most α blocks of $\mathscr{B}$.

Definition 8.4. Let α be a positive integer. A set system $(X, \mathscr{A})$ is *α-resolvable* if $\mathscr{A}$ can be partitioned into parts, each of which is an α-resolution class.

Definition 8.5. Let α be a positive integer. A set system $(X, \mathscr{A})$ is *almost α-resolvable* if $\mathscr{A}$ can be partitioned into parts, each of which is an α-resolution class, except perhaps for one part, which is a partial α-resolution class.

If $(X, \mathscr{A})$ is k-uniform, then it is α-resolvable or almost α-resolvable only if $\alpha|X| \equiv 0 \pmod{k}$. The following lemma relates the existence of balanced orderings of parity-check matrices to resolution properties of their set systems.

Lemma 8.6. *Let $[C \mid I]$ and $(X, \mathscr{A})$ be the parity-check matrix and set system of an $[n, c, k, l]$-ERC, respectively. Then C has an α-balanced ordering if and only if $(X, \mathscr{A})$ is almost α-resolvable.*

Proof. Suppose $(X, \mathscr{A})$ is almost α-resolvable with α-resolution classes $\mathscr{A}_1, \ldots, \mathscr{A}_{r-1}$ and a partial α-resolution class $\mathscr{A}_r$ (which can be empty). Order the matrix C so that $C = [C_1 \mid \cdots \mid C_r]$, where each C_i contains precisely those columns whose supports are in $\mathscr{A}_i$. The ordering of the columns within each C_i can be arbitrary. This is an α-balanced ordering for C.

Now suppose C has an α-balanced ordering. Consider the first $\alpha c/k$ columns of C and the set of their supports $\mathscr{A}_1$. The erasure-resilient code formed by these columns has average group size $\alpha + 1$, and hence each group has size $\alpha + 1$. It follows that every point is contained in exactly α blocks in $\mathscr{A}_i$. Now consider the first $i(\alpha c/k)$ columns of C, $2 \leqslant i \leqslant \lfloor nk/\alpha c \rfloor$, and the set of their supports $\mathscr{B} \cup \mathscr{A}_i$, where $\mathscr{A}_i$ is the set of supports of columns $(i-1)\alpha c/k + 1$ to $i(\alpha c/k)$ of C. The average group size of the code formed by the first $i(\alpha c/k)$ columns of C is $i\alpha + 1$. Hence, every point appears in exactly $i\alpha$ blocks of $\mathscr{B} \cup \mathscr{A}_i$. By the induction hypothesis, every point appears in exactly $(i-1)\alpha$ blocks of $\mathscr{B}$. It follows that every point must appear in precisely α blocks of $\mathscr{A}_i$. Consequently, $\mathscr{A}_i$ is an α-resolution class. The supports of the remaining columns of C constitute a partial α-resolution class. □

Hellerstein et al. [16] construct $[3^m(3^m-1)/6, 3^m, 3, 4]$-ERCs with a 1-balanced ordering. In fact, the set system of their $(3,4)$-ERC is the *affine geometry* $\mathrm{AG}_1(m,3)$ (see, for example, [4]), whose 1-resolvability is a classical result in design theory. An $\mathrm{STS}(v)$ that is 1-resolvable is known as a *Kirkman triple system of order* v, or $\mathrm{KTS}(v)$. Our discussion shows that the problem of constructing $[n,c,3,4]$-ERC, $c \equiv 3 \pmod 6$, with optimal check disk overhead, having a 1-balanced ordering is equivalent to the following problem.

Problem 8.7. Determine those v for which there exists an anti-Pasch $\mathrm{KTS}(v)$.

The existence of $\mathrm{KTS}(v)$ has long been settled [27]; the condition $v \equiv 3 \pmod 6$ is both necessary and sufficient. Work on the existence problem for anti-Pasch $\mathrm{STS}(v)$ is also well under way. However, Problem 8.7 appears not to have been studied, perhaps due to the lack in motivation. This is not the case now. We settle here the existence of anti-Pasch $\mathrm{KTS}(v)$ for a third of the admissible values of v. In particular, we prove that there exists an anti-Pasch $\mathrm{KTS}(v)$ for all $v \equiv 9 \pmod{18}$. The proof is somewhat technical and uses more complex design-theoretic machinery than we have required thus far. In order to conserve space, we refer the reader to [4,7] for definitions and results in design theory not explicitly stated here.

A *group divisible design* (GDD) is a triple $(X, \mathscr{G}, \mathscr{B})$ which satisfies the following properties:

(1) $\mathscr{G}$ is a partition of a set X (of *points*) into subsets called *groups*,
(2) $\mathscr{B}$ is a set of subsets of X (called *blocks*) such that a group and a block contain at most one common point,
(3) every pair of points from distinct groups occurs in a unique block.

The *group-type* (*type*) of the GDD is the multiset $[|G|: G \in \mathscr{G}]$. We usually use an "exponential" notation to describe group-type: a group-type $g_1^{u_1} \cdots g_s^{u_s}$ denotes u_i occurrences of g_i for $1 \leqslant i \leqslant s$. Groups of size 0 are permitted as a notational convenience. The type is *uniform* when all groups have the same size, in which case the type is of the form g^u.

If K is a set of positive integers, each of which is not less than 2, then we say that a GDD $(X, \mathscr{G}, \mathscr{B})$ is a K-GDD if $|B| \in K$ for every block B in $\mathscr{B}$. When $K = \{k\}$, we simply write k for K. A *balanced incomplete block design* $\mathrm{BIBD}(v,k,1)$ is a k-GDD of type 1^v. A *transversal design* $\mathrm{TD}(k,n)$ is a k-GDD of type n^k.

We need the following notion of resolvability. A set of blocks is an *α-parallel class* if every point x is contained in exactly α blocks. A $\mathrm{GDD}(X, \mathscr{G}, \mathscr{B})$ is called *A-resolvable* where A is a multiset of positive integers of r elements and if its block set $\mathscr{B}$ admits a partition into subsets $B_1, B_2, \ldots, B_r$ where for each $i = 1, 2, \ldots, r$, there is an $\alpha \in A$ such that B_i is an α-parallel class. The case when $A = [1^r]$ corresponds to the case of the usual notion of resolvability.

A 3-GDD is anti-Pasch, and called a QFGDD, when it contains no Pasch configurations. In fact, we enforce the stronger condition that there is no way to place a single triple on the points within one group and thereby introduce a Pasch configuration. In

effect, since the Pasch configuration does not have two disjoint blocks, the consequence is that no matter how triples are placed within groups, a Pasch configuration would lie (if at all) entirely on the points of a single group. A TD(3,n) which is a QFGDD is denoted by QFTD(n). It is an easy exercise to see that a QFTD(n) is precisely the same as a latin square of order n which has no subsquare of order two (see [21] for related results).

8.1. Direct constructions

In this subsection, we present some direct constructions of anti-Pasch KTS.

The basic necessary condition for the existence of anti-Pasch KTS(v) is $v \equiv 3 \pmod 6$. There does not exist an anti-Pasch KTS(15) as the only anti-Pasch STS(15) is number 80 of [20], and it is not resolvable. Hence, the smallest open case is when $v=21$. In [19], 30 nonisomorphic Kirkman triple systems of order 21 are found. However, each of them contains a subsystem of order 7. Hence, none can be anti-Pasch.

Lemma 8.8. *There exists an anti-Pasch* KTS(33).

Proof. Consider the following KTS(33) from [33]. Let $V = \mathbb{Z}_{33}$.

$$\{1,3,6\},\{17,19,32\},\{9,11,24\},\{22,25,13\},\{5,8,29\},\{27,30,18\},$$

$$\{31,4,23\},\{14,20,6\},\{15,21,7\},\{28,2,12\},\{26,0,10\},$$

$$\{3,10,20\},\{1,2,6\},\{2,3,7\},\{3,4,8\},\{1,12,23\}.$$

Let $\pi(x) = x + 3$. The design is generated by letting π act on the set of blocks. The first 11 blocks form a parallel class; the action of π gives 11 parallel classes. Each of the remaining base blocks generates a parallel class under the action of π. □

Lemma 8.9. *There exists an anti-Pasch* KTS(39), *an anti-Pasch* KTS(45), *and an anti-Pasch* KTS(63).

Proof. Let $V = \mathbb{Z}_{39}$. Consider

$$\{0,7,16\},\{4,10,25\},\{1,6,18\},\{8,9,11\}$$

$$\{0,8,19\},\{0,4,14\},\{2,15,28\}.$$

These form the base blocks of an anti-Pasch STS(39) over $\mathbb{Z}_{39}$. The 12 points in the first four base blocks are distinct (mod 13). Adding 13 and 26 to each block and appending the block $\{2,15,28\}$ gives a parallel class. Develop to obtain 13 parallel classes. Each of the two remaining base blocks generates three parallel classes, as the points in each block are distinct (mod 3).

Similarly, let $V = \mathbb{Z}_{45}$. Consider

$$\{0,1,3\},\{2,7,13\},\{12,19,39\},\{5,14,26\},\{6,10,23\},$$

$$\{0,8,31\},\{0,10,29\}.$$

The first five blocks contain elements that are all distinct modulo 15, and hence generate 15 parallel classes. The last two blocks each generate three parallel classes, as the points in each block are distinct (mod 3). Finally, the base block $\{0,15,30\}$ generates a single parallel class.

Let $V=\mathbb{Z}_{63}$. Consider

$$\{0,1,3\},\{4,8,13\},\{6,12,19\},\{15,23,39\},\{5,17,49\},\{16,30,52\},\{20,35,53\},$$
$$\{0,10,38\},\{0,11,34\},\{0,17,43\}.$$

These generate an anti-Pasch KTS(63) in the same manner as the anti-Pasch KTS(45). □

Next we present a general construction for anti-Pasch KTSs.

Theorem 8.10. *Suppose that* $v \equiv 1 \pmod 6$, *and there exists a cyclic anti-Pasch* STS(v) *over* V *with mutually disjoint base blocks. Then there exists an anti-Pasch* KTS($3v$).

Proof. This construction is a simple modification of one in [12]. Let $V'=V\times\{0,1,2\}$. We construct the following set of blocks.

(i) For every block $\{a,b,c\}$ in the STS(v), include blocks $\{(a,0),(b,0),(c,0)\}$, $\{(2a,1),(2b,1),(2c,1)\}$ and $\{(3a,2),(3b,2),(3c,2)\}$.

(ii) $\{(i,0),(i+2j,1),(i+3j,2)\}$ for $i,j\in V$.

This results in a KTS($3v$) [12], and the verification that it is anti-Pasch is routine. □

It is therefore of interest to determine when a cyclic anti-Pasch STS exists whose base blocks can be made mutually disjoint. A conjecture of Novák [24] asserts that when $v\equiv 1\pmod 6$, every cyclic STS(v) can be made to have disjoint base blocks by suitable addition of different values (modulo v) to each base block. This is widely believed to be true but not much progress has been made.

The only known infinite class of cyclic anti-Pasch STS(v) when $v\equiv 1\pmod 6$ is the Netto triple systems. Let $q=p^n$ where p is a prime such that $p\equiv 7\pmod{12}$. Take two primitive sixth roots of unity ε_1 and ε_2 in $\mathbb{F}_q$; they both are non-squares and satisfy the equation $x^2-x+1=0$. It follows that $\varepsilon_1+\varepsilon_2=\varepsilon_1\varepsilon_2=1$, $\varepsilon_1^2=-\varepsilon_2$ and $\varepsilon_2^2=-\varepsilon_1$. For any two distinct elements $a,b\in\mathbb{F}_q$ define $a\to b$ if and only if $b-a$ is a non-zero square in $\mathbb{F}_q$. This relation has the property that exactly one of $a\to b$ and $b\to a$ is true for $a\neq b$, since -1 is not a square in $\mathbb{F}_q$. On the set of all ordered pairs (a,b) such that $a\to b$, define a function f by $f(a,b)=a\varepsilon_1+b\varepsilon_2$. If $c=f(a,b)$, then also $b\to c$ with $f(b,c)=a$ and $c\to a$ with $f(c,a)=b$. The *Netto system* $N(q)$ is the STS $(V,\mathscr{B})$ where $V=\mathbb{F}_q$ and $\mathscr{B}=\{\{a,b,c\}: a\to b \text{ and } c=f(a,b)\}$.

Theorem 8.11 (Robinson [30]). *If* $p\equiv 19\pmod{24}$, *then* $N(q)$ *is anti-Pasch and transitive over* $\mathbb{F}_q$. *If* $\{a,b,c\}$ *is a block in* $N(q)$, *so is* $\{\omega^2a,\omega^2b,\omega^2c\}$ *for any* $\omega\in\mathbb{F}_q$.

Theorem 8.12 (Abel [1]). *If q is a prime power congruent to* $1 \pmod 6$, *ω is a primitive root over $\mathbb{F}_q$, and A is a block of size three so that $\{\omega^{6i}A\colon i = 0, 1, \ldots, (q-1)/6\}$ is the set of base blocks for the cyclic* STS(q), *then the* STS(q) *can be made to have disjoint base blocks.*

Combining Theorems 8.10 and 8.12 with Netto triple systems, we obtain:

Corollary 8.13. *If $v = 3q$, $q = p^\alpha$ and $p \equiv 19 \pmod{24}$ a prime, then there exists an anti-Pasch* KTS(v).

Next, we present some further base block disjoint anti-Pasch STS(v) where $v \equiv 1 \pmod 6$.

25: $\{1,2,4\}, \{3,7,14\}, \{6,12,21\}$

31: $\{1,2,4\}, \{3,7,14\}, \{5,10,18\}, \{6,12,24\}, \{8,16,25\}$

37: $\{1,2,4\}, \{3,7,29\}, \{5,10,19\}, \{6,12,31\}, \{8,15,25\}, \{9,17,30\}$

49: $\{1,2,4\}, \{3,7,12\}, \{5,11,22\}, \{6,13,29\}, \{8,16,38\}, \{9,19,40\}, \{10,23,35\}, \{14,38,48\}$

55: $\{1,2,4\}, \{3,7,12\}, \{5,11,21\}, \{6,13,38\}, \{8,16,37\}, \{9,20,51\}, \{14,26,41\}, \{10,24,46\}, \{15,32,52\}$

61: $\{1,2,4\}, \{3,7,12\}, \{5,11,18\}, \{6,14,31\}, \{9,19,42\}, \{10,21,40\}, \{13,25,45\}, \{8,22,48\}, \{15,30,52\}, \{16,32,50\}$

73: $\{3,7,13\}, \{5,10,40\}, \{9,16,41\}, \{6,14,30\}, \{8,17,63\}, \{11,22,64\}, \{15,27,67\}, \{18,32,47\}, \{0,19,36\}, \{20,42,65\}, \{1,2,4\}$

79: $\{9,15,31\}, \{12,19,64\}, \{11,20,66\}, \{14,24,67\}, \{16,28,75\}, \{17,32,71\}, \{25,43,73\}, \{0,23,44\}, \{1,2,30\}, \{3,5,22\}, \{4,7,18\}, \{6,10,48\}, \{8,13,21\}$

85: $\{1,2,60\}, \{3,5,52\}, \{4,7,50\}, \{6,10,67\}, \{8,13,27\}, \{9,15,77\}, \{11,18,29\}, \{12,20,68\}, \{14,23,83\}, \{16,26,48\}, \{19,31,64\}, \{17,30,61\}, \{21,36,56\}, \{24,45,79\}$

91: $\{1,2,4\}, \{22,43,62\}, \{23,46,72\}, \{3,7,14\}, \{5,10,39\}, \{6,12,65\}, \{8,16,44\}, \{9,18,36\}, \{11,21,82\}, \{13,25,71\}, \{15,28,63\}, \{17,31,56\}, \{19,34,88\}, \{24,40,84\}, \{20,37,87\}$

97: $\{1,2,4\}, \{10,21,82\}, \{14,26,56\}, \{17,30,74\}, \{15,29,62\}, \{18,33,50\}, \{3,7,12\}, \{5,11,31\}, \{6,13,72\}, \{8,16,43\}, \{9,19,67\}, \{25,48,77\}, \{20,36,57\}, \{22,40,91\}, \{23,42,96\}, \{24,46,80\}$.

These designs are from [8] and made base block disjoint here.

Lemma 8.14. *If n is odd, then there exists a resolvable* QFTD($3, n$).

Proof. Construct the TD($3, n$) by taking $V = \mathbb{Z}_n \times \{0,1,2\}$. The block set is $\{\{(a,0), (b,1), (a+b,2)\}\colon a, b \in \mathbb{Z}_n\}$. □

Theorem 8.15. *If there exists an anti-Pasch* KTS($2v+1$), *an anti-Pasch* KTS($2n+1$) *and a resolvable* QFTD($3, n$), *then there exists an anti-Pasch* KTS($2vn+1$).

Proof. Delete a point from the anti-Pasch KTS($2v+1$) to form a 3-GDD of type 2^v. Give weight n using a resolvable QFTD($3,n$) to produce a 3-GDD of type $(2n)^v$. Add one infinite point ∞, and on each group together with ∞, place a copy of the QFSTS($2n+1$) so that when $\{\infty,a,b\}$ is a triple, a and b arise from different points of the 3-GDD of type 2^v. Call the triples of the 3-GDD of type $(2n)^v$ *vertical*, and the triples of the STS($2n+1$)s *horizontal*. The result is an STS($2vn+1$) [4], which we prove is anti-Pasch.

Suppose to the contrary that a Pasch configuration is present. If it contains ∞, it contains two horizontal and two vertical triples, since the STS($2n+1$) used is anti-Pasch. The placement of the blocks containing ∞, and the fact that the STS($2v+1$) is anti-Pasch, ensures that the two vertical blocks are disjoint and hence not in a Pasch configuration. Hence any Pasch configuration must involve six points other than ∞. Then there cannot be two horizontal triples (since they are either disjoint or from the same QFSTS($2n+1$). If there is one horizontal triple, the three vertical triples cannot involve only three further points. So all triples are vertical. However, at most one can arise from each QFTD($3,n$) used, and hence any Pasch configuration would correspond to a Pasch configuration in the QFSTS($2v+1$), which is a contradiction. □

We have established existence of resolvable QFTD(3,n)s here only when n is odd. Obtaining such TDs when n is even is more involved and not needed for the main result we present, and so we omit it here.

8.2. Rees's construction

In this section, we employ Rees's construction [28] on resolvable group divisible designs to obtain some new anti-Pasch KTSs.

A *partial transversal design* PlTD(k,n) is a triple $(X,\mathscr{C},\mathscr{B})$ where X is a kn-set, $\mathscr{B}$ is a collection of k-subsets of X (blocks) so that any pair of distinct points from X is contained in at most one block, and $\mathscr{C}$ is a strong k-vertex-coloring of X (i.e., each block receives k different colors) so that $|C|=n$ for each $C\in\mathscr{C}$. Any transversal design is a PlTD (just take each group as a color class). Similarly, a *partial group divisible design* K-PlGD of type T is a triple $(X,\mathscr{C},\mathscr{B})$ where X is a v-set, $\mathscr{B}$ is a collection of subsets of C (blocks) each having same size from the set K so that any pair of distinct points from X is contained in at most one block, and $\mathscr{C}$ is a strong coloring of X.

A group $\mathscr{H}$ of automorphisms on a set V acts *sharply transitively* on V if for every two elements $x,y\in V$, there exists $h\in\mathscr{H}$ so that $xh=y$ where the group action is written as left multiplication.

A *block-partition* of a transversal design $(X,\mathscr{G},\mathscr{B})$ is a partition P of its block set $\mathscr{B}$; we refer to the members of P as *aggregates*. If each member of P is a clear set (i.e., composed of mutually disjoint blocks) then we refer to P by the usual term *block-coloring*.

Theorem 8.16 (Rees [28]). *Let $(X,G,\mathscr{B})$ be an A-resolvable K-PlGD of type T in which for each $\alpha_i \in A$, there are r_i α_i-parallel classes of blocks. Suppose that there is a* TD(u,h) *admitting $\mathscr{H}$ as a group of automorphism acting transitively on the points of each group where $u=|G|$. Let H_j be a collection of subsets of $\mathscr{H}$, with r_i such subsets of size α_i for each $\alpha_i \in A$, and suppose that the collection $\{H_i * r\colon r \in \mathscr{H},\ j=1,2,\ldots,\sum_i r_i\}$ is Γ-resolvable on $\mathscr{H}$. Then there is a Γ-resolvable K-PlGD of type hT.*

Theorem 8.17 (Rees [28]). *Let $(X,G,\mathscr{B})$ be a K-PlGD of type T whose block set $\mathscr{B}$ forms an α-parallel class, and let $u=|G|$. Suppose that there is a* TD(u,h) *each of whose groups $J_1,J_2,\ldots,J_u$ is written on the symbols of a group $\mathscr{H}$, and let $H^1,H^2,\ldots,H^u$ be a sequence of subsets of $\mathscr{H}$ each of size α. Let $\mathscr{C}$ be a block-partition of the TD with the following property: for each aggregate $C \in \mathscr{C}$ and each $i=1,2,\ldots,u$, the set $\{H^i * r\colon r \in J_i \cap (\bigcup_{b\in C} b)\}$ forms a γ-parallel class on J_i. Then there is a K-PlGD of type hT whose block set is γ-resolvable.*

These two constructions are complicated and very powerful. In our case, if we begin with an anti-Pasch GDD, we can inflate to get an anti-Pasch resolvable GDD. The proof of this theorem is lengthy and similar to the proof in [28], so we do not include it here. Briefly, we inflate the GDD so that for every block of size k, we put the TD(k,h) that corresponds to the groups of the k points. Hence, when all blocks have size three, if the TD(u,h) has the extra property that any three groups induce an anti-Pasch TD, then we produce an anti-Pasch GDD. Therefore, it is important to know if such TD(u,h)s exist.

Lemma 8.18. *If $h=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_n^{\alpha_n}$, where p_i are odd prime powers and α_i are positive integers, and $m=\min_i(p_i^{\alpha_i})$, then there exists a* TD$(m-1,h)$ *admitting $\mathscr{H}=\mathbb{F}_{p_1}^{\alpha_1}\times\mathbb{F}_{p_2}^{\alpha_2}\times\cdots\times\mathbb{F}_{p_n}^{\alpha_n}$ acting sharply transitively on the points of each group. In addition, the* TD$(3,h)$ *induced by any three groups is anti-Pasch.*

Proof. Let $V=\mathbb{F}_{p_1}^{\alpha_1}\times\mathbb{F}_{p_2}^{\alpha_2}\times\cdots\times\mathbb{F}_{p_n}^{\alpha_n}$. There exist $m-1$ elements $t_1,t_2,\ldots,t_{m-1}\in V$ so that the difference between any two of them is invertible over the ring V. We can construct a TD$(m-1,h)$ over $V\times\{0,\ldots,m-2\}$ by taking the blocks $\{(at_1+b,1),(at_2+b,2),\ldots,(at_{m-1}+b,m-1)\}$ for $a,b\in V$. This is a TD$(m-1,h)$ for which V acts sharply transitively on the points of each group. To see that the TD$(3,h)$ induced by any three groups is anti-Pasch, the presence of a Pasch configuration implies that the desarguesian projective plane of order p contains a projective subplane of order two, which it does not when p is odd [4]. □

In order to apply Rees's technique, we begin with an anti-Pasch GDD which admits a certain resolution. Many examples come from Bose's construction.

Theorem 8.19 (Griggs et al. [14]). *If $v=3n$ where n is odd and $(n,7)=1$, then there exists an anti-Pasch* STS(v). *Indeed, there exists a 3-resolvable anti-Pasch* GDD *of type 3^n.*

Proof. We state the construction; see [14] for a proof. The anti-Pasch STS($3n$) is constructed over $V = \mathbb{Z}_n \times \mathbb{Z}_3$. For every $a, b, c \in \mathbb{Z}_n$, we construct a block of form $\{(a,i),(b,i),(c,i+1)\}$ if $a + b = 2c$ and $i \in \mathbb{Z}_3$. Also, we take n blocks of form $\{(x,0),(x,1),(x,2)\}$ for $x \in \mathbb{Z}_n$.

In this construction, if $\{(a,i),(b,i),(c,i+1)\}$ is a block then so are $\{(a+1,i),(b+1,i),(c+1,i+1)\}$ and $\{(a,i+1),(b,i+1),(c,i+2)\}$. Hence, this design is transitive over $\mathbb{Z}_n \times \mathbb{Z}_3$. In fact, the base blocks are $\{(0,0),(2,0),(1,1)\}$, $\{(0,0),(4,0),(2,1)\},\ldots,\{(0,0),(n-1,0),((n-1)/2,1)\}$ together with a short orbit $\{(0,0),(0,1),(0,2)\}$. Each base block forms a 3-parallel class, and the short orbit gives a 1-parallel class. □

Lemma 8.20. *Let $V = \mathbb{Z}_v$, $v \geqslant 3$ odd and $\mathscr{B} = \{\{0,1,2\} + a\}: a \in \mathbb{Z}_v\}$. If $v \neq 5$, then there exists a strong vertex coloring on V with at most four color classes.*

Proof. If $v = 3m$, then let $C_1 = \{3i: i = 0,1,\ldots,m-1\}$, $C_2 = C_1 + 1$ and $C_3 = C_1 + 2$. If $v = 6m+1$, then let $C_1 = \{3i: i = 0,1,\ldots,2m-1\}$, $C_2 = C_1 + 1$, $C_3 = C_1 + 2$ and $C_4 = \{6m\}$. If $v = 6m+5$, let $C_1 = \{3i: i = 0,1,2,\ldots,2m-1\} \cup \{6m+1\}$, $C_2 = C_1 + 1$, $C_3 = C_1 + 2$ and $C_4 = \{6m, 6m+4\}$. For any block $\{a, a+1, a+2\}$, the three points are in three different color classes. □

Lemma 8.21. *Let $V = \mathbb{Z}_{2n+1} \times \mathbb{Z}_3$, $n \neq 2$ and $\mathscr{B} = \{\{(0,0),(2a,0),(a,1)\} + b: b \in V\}$ for $a = 1,2,\ldots,n$. There exists a strong vertex coloring on V with at most four color classes for every $a = 1,2,\ldots,n$.*

Proof. First of all, use Lemma 8.20 by taking $v = 2n+1$ to obtain C_i for $i = 1,2,3,4$. If $(a, 2n+1) = 1$, then we can construct $D_i = aC_i \times \mathbb{Z}_3$ which is the appropriate vertex-coloring. If $(a, 2n+1) = c$, let $(a/c, (2n+1)/c) = 1$ and apply Lemma 8.20 by taking $v = (2n+1)/c$ to obtain C_i for $i = 1,2,3,4$. Then define $T_i = (a/c)C_i$ for $i = 1,2,3,4$. For every $x = 0,1,\ldots,2n$, define $T_i^* = \{x: x = qc + r, q \in T_i\}$. Finally, define $D_i = T_i^* \times \mathbb{Z}_3$, which is a strong vertex coloring. □

We now apply Rees's Theorem.

Theorem 8.22. *If $v = 9n$ where n is odd, $v \neq 45$ and $(n,7) = 1$, then there exists an anti-Pasch* KTS(v).

Proof. Theorem 8.19 gives a 3-resolvable QFGDD of type 3^n. For every 3-parallel class, there exists a strong 4-vertex coloring. Hence, we can regard this as a P1GD with block size three and four groups. Apply Theorem 8.17 with a TD(4,3), taking each $H^i = \mathbb{Z}_3$ and $\mathscr{C}$ to be the block set of the TD. This gives a 3-resolvable QFGDD of type 9^n. Fill in the holes with anti-Pasch KTS(9)s. □

8.3. Zhu, Du and Zhang's construction

We use a technique introduced by Zhu et al. [34] and later extended by Rees and Stinson [29]. A design $\mathscr{D}$ is *s-block-colorable* if its blocks can be colored with s colors in such a way that any two blocks of the same color do not intersect. Such an assignment of s colors is said to be an *s-coloring*. If $\mathscr{D}$ is *s-block-colorable* but not $(s-1)$-*block-colorable*, we say that the *chromatic index* of $\mathscr{D}$ is s.

Theorem 8.23 (Zhu et al. [34]). *Suppose there exists an resolvable* BIBD$(u,k,1)$, *a* BIBD$(v,k,1)$ *which is s-block-colorable, and a resolvable* TD(k,v). *If* $s \leqslant r_u + r_v$ *where* $r_x = (x-1)/(k-1)$, *then there exists an resolvable* BIBD$(uv,k,1)$.

Theorem 8.24 (Rees and Stinson [29]). *Suppose there exists a resolvable k-GDD of type* g^u, *a k-GDD of type* $(mg)^v$ *with the property that there is an s-coloring of its blocks such that each color class precisely covers some subset of its groups, and a resolvable* TD(k,mv). *If* $s \leqslant r_u + r_v$ *where* $r_u = g(u-1)/(k-1)$ *and* $r_v = mg(v-1)/(k-1)$, *then there exists a resolvable k-GDD of type* $(mg)^{uv}$.

If we replace all ingredients by anti-Pasch KTS, QFGDD and resolvable QFTD, then we can obtain a similar result for the construction of resolvable QFGDD. We need some QFGDDs with few color classes, and can obtain some from Bose's construction.

Lemma 8.25. *Let* $n = 6k+5$ *and* $C_i = \{i, i+1, i+2\}$ *for* $i = 0,1,\ldots,n-1$, *arithmetic over* $\mathbb{Z}_n$. *If* $\mathscr{C} = \{C_i : i = 0,1,\ldots,n-1\}$, *then for any* $a,b \in \mathbb{Z}_n$ $\mathscr{C} \backslash (C_a \cup C_b)$ *can be partitioned into three sets of* $2k+1$ *blocks so that any two blocks in the same set are disjoint.*

Proof. Sort the blocks in increasing order according to smallest element in the block. Then put the jth block in the $j \pmod 3$ set to obtain the required partition. □

Theorem 8.26. *When* $k \equiv 0,2 \pmod 3$ *and and* $(2k+1,7) = 1$, *there exists an anti-Pasch* 3-GDD *of type* 3^{2k+1} *which is* $3k+6$ *colorable so that each color class misses a subset of the groups.*

Proof. We use the QFGDD of type 3^{2k+1} from Theorem 8.19 with groups formed by taking $\{(i,0),(i,1),(i,2)\}$ for $i \in \mathbb{Z}_{2k+1}$. We construct a graph $G = (V,E)$ as follows: $V = \mathbb{Z}_{2k+1} \backslash \{0\}$ and $(a,b) \in E$ if $\{a,2a,3a\} \cap \{b,2b,3b\} \neq \emptyset$. Each vertex has degree at most six so by Brooks's Theorem in vertex coloring, this graph is 6-colorable. If $2k+1 \equiv 1 \pmod 6$, for every color class C, consider the subset of $\{1,2,\ldots,k\}$ in C. Form a partial parallel class missing a subset of groups: Take $\{(c,i),(3c,i),(2c,i+1)\}$ for $i \in \mathbb{Z}_3$ and $c \in C$. In this way, we obtain six partial parallel classes. For each base block $\{(0,0),(2a,0),(a,1)\}$ over $\mathbb{Z}_{2k+1} \times \mathbb{Z}_3$, we have used the translate $\{(a,i),(3a,i),(2a,i+1)\}$. The remaining translates can be partitioned into three partial parallel classes, each missing one group.

In the case when $2k+1 \equiv 5 \pmod 6$, the vertices for a and $-a$ correspond to two distinct translates of $\{0,a,2a\}$. For every base block $\{(0,0),(2a,0),(a,1)\}$ in the QFSTS from Theorem 8.19, two blocks are used to obtain six partial parallel classes. The remaining blocks from each base block form three partial parallel classes by Lemma 8.25. □

Theorem 8.27. *Suppose there exists an anti-Pasch* KTS(v) *where* $v \geqslant 15$, *and* $w \equiv 3, 15 \pmod{18}$, *then there exists an anti-Pasch* KTS($vw/3$).

Proof. Take an anti-Pasch 3-GDD of type $3^{w/3}$ from Theorem 8.26 which is $(w-3)/2+6$ colorable. Apply Theorem 8.24 to obtain the result. □

Lemma 8.28. *There exists a* 14*-colorable anti-Pasch* 3-GDD *of type* 3^7 *so that each color class misses a subset of groups.*

Proof. A QFSTS(21) exists on $V = \mathbb{Z}_7 \times \mathbb{Z}_3$ having base blocks $\{(0,0),(0,1),(0,2)\}$, $\{(0,0),(1,1),(3,0)\}$, $\{(5,0),(2,2),(4,0)\}$ and $\{(0,0),(4,1),(5,0)\}$. The first base block generates a single parallel class. The second and third base blocks generate seven partial parallel classes when developed over $\mathbb{Z}_7 \times \mathbb{Z}_3$ since each mod 7 component is distinct. The last block generates another seven partial parallel classes. □

Corollary 8.29. *For n odd, there exists an anti-Pasch* KTS($9n$).

Proof. If $n \in \{5,7\}$, see Lemma 8.9. Otherwise write $n = 7^a w$ where $(w,7)=1$. If $a=0$, apply Theorem 8.22. If $a=1$, take a 14-colorable anti-Pasch 3-GDD of type 3^7 from Lemma 8.28, a resolvable QFGDD of type 3^{3w}, and apply Theorem 8.24 to obtain a resolvable QFGDD of type 3^{21w}. If $a \geqslant 2$, apply Theorem 8.22 with a resolvable QFGDD of type $3^{7^{a-1}\cdot 3w}$ and a 14-colorable anti-Pasch 3-GDD of type 3^7. □

This settles the existence of anti-Pasch KTS(v)s when $v \equiv 9 \pmod{18}$, along with many of the small orders in the remaining classes. The techniques here do not seem sufficiently powerful to handle the cases in which v is a multiple of 3 but not 9. From a practical standpoint, the solution of a single congruence class modulo 18 already provides a rich source of codes.

9. Conclusion

Disk arrays provide a solution to the disparity in performance between microprocessors and secondary storage systems. There is an increasing popularity in the use of disk arrays. One of the major problems faced by critical applications is the reliability of disk arrays. In this paper, we have provided constructions for erasure-resilient codes that can tolerate failures in disk arrays. Our results improve, extend, and generalize previous results of Hellerstein et al. [16].

One surprise in this work is the role of combinatorial designs. For example, it is shown that $(3,4)$-ERC are equivalent to anti-Pasch Steiner triple systems, which have been studied actively for the past decade by mathematicians without having any particular applications in mind. In exchange, the study of erasure-resilient codes offers new interesting problems in combinatorial design theory such as the existence of anti-Pasch Kirkman triple systems addressed in this paper.

Acknowledgements

Research of the authors is supported by the Army Research Office (USA) under grant number DAAG55-98-1-0272 (Colbourn). This work was begun while the authors were at the University of Waterloo, Waterloo, Ontario N2L 3G1, Canada.

References

[1] R.J.R. Abel, Some new BIBDs with $\lambda = 1$ and $6 \leqslant k \leqslant 10$, J. Combin. Des. 4 (1996) 27–50.
[2] N. Alon, J. Edmonds, M. Luby, Linear time erasure codes with nearly optimal recovery, in Proceedings of the 36th Annual IEEE Symposium on Foundations of Computer Science, IEEE, New York, 1995, pp. 512–519.
[3] G.M. Amdahl, Validity of the single processor approach to achieving large scale computing capabilities, in Proceedings of the AFIPS Spring Joint Computer Conference, Vol. 30, Washington, DC, 1967. AFIPS. pp. 483–485.
[4] T. Beth, D. Jungnickel, H. Lenz, Design Theory, Cambridge University Press, Cambridge, 1993.
[5] A.E. Brouwer, Steiner triple systems without subconfigurations, Technical Report ZW 104/77, Mathematisch Centrum Amsterdam, Amsterdam, 1977.
[6] P.M. Chen, E.K. Lee, G.A. Gibson, R.H. Katz, D.A. Patterson, RAID: high-performance, reliable secondary storage, ACM Comput. Surv. 26 (1994) 145–185.
[7] C.J. Colbourn, J.H. Dinitz (Eds.), CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 1996.
[8] C.J. Colbourn, E. Mendelsohn, A. Rosa, J. Širáň, Anti-mitre Steiner triple systems, Graphs Combin. 10 (1994) 215–224.
[9] C.J. Colbourn, A. Rosa, Leaves, excesses and neighbourhoods in triple systems, Austral. J. Combin. 4 (1991) 143–178.
[10] P. Erdös, Problems and results in combinatorial analysis, Creation Math. 9 (1976) 25.
[11] P. Erdös, D.J. Kleitman, On coloring graphs to maximize the proportion of multicolored k-edges, J. Combin. Theory 5 (1968) 149–164.
[12] S. Furino, J. Yin, Y. Miao, Frames and Resolvable Designs, CRC Press, Boca Raton, FL, 1996.
[13] G.A. Gibson, Redundant Disk Arrays: Reliable, Parallel Secondary Storage, MIT Press, Cambridge, MA, 1992.
[14] T.S. Griggs, J. Murphy, J.S. Phelan, Anti-Pasch Steiner triple systems, J. Combin. Inform. Systems Sci. 15 (1990) 79–84.
[15] A. Hartman, K.T. Phelps, Steiner quadruple systems, in: J.H. Dinitz, D.R. Stinson (Eds.), Contemporary Design Theory: A Collection of Surveys, Wiley, New York, 1992, pp. 205–240 (Chapter 6).
[16] L. Hellerstein, G.A. Gibson, R.M. Karp, R.H. Katz, D.A. Patterson, Coding techniques for handling failures in large disk arrays, Algorithmica 12 (1994) 182–208.
[17] A.C.H. Ling, C.J. Colbourn, M.J. Grannell, T.S. Griggs, Construction techniques for anti-Pasch Steiner triple systems, J. London Math. Soc., to appear.
[18] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.

[19] R. Mathon, K.T. Phelps, A. Rosa, A class of Steiner triple systems of order 21 and associated Kirkman systems, Math. Comput. 3 (1981) 209–222.
[20] R. Mathon, K.T. Phelps, A. Rosa, Small Steiner triple systems and their properties, Ars Combin. 15 (1983) 3–110.
[21] M. McLeish, On the existence of latin squares with no subsquares of order two, Utilitas Math. 8 (1975) 41–53.
[22] R. Motwani, P. Raghavan, Randomized Algorithms, Cambridge University Press, Cambridge, 1995.
[23] J. Mozzochi, On the difference between consecutive primes, J. Number Theory 24 (1986) 181–187.
[24] J. Novák, A note on disjoint cyclic Steiner triple systems, in: Proceedings of Symposium Prague, Academia, Praha, 1974, pp. 439–440.
[25] D.A. Patterson, J.L. Hennessy, Computer Organization and Design: The Hardware/Software Interface, Morgan Kaufmann, San Mateo, CA, 1994.
[26] M.O. Rabin, Efficient dispersal of information for security, load balancing, and fault tolerance, J. Assoc. Comput. Mach. 36 (1989) 335–348.
[27] D.K. Ray-Chaudhuri, R.M. Wilson, Solution of Kirkman's schoolgirl problem, Proc. Symp. Pure Math. Amer. Math. Soc. 19 (1971) 187–204.
[28] R. Rees, Two new direct product-type constructions for resolvable group-divisible designs, J. Combin. Des. 1 (1993) 15–26.
[29] R. Rees, D.R. Stinson, Frames with block size four, Canad. J. Math. 44 (1992) 1030–1049.
[30] R.M. Robinson, The structure of certain triple systems, Math. Comput. 20 (1975) 233–241.
[31] K. Salem, H. Garcia-Molina, Disk striping, in: Proceedings of the 2nd International Conference on Data Engineering, Washington, DC, IEEE, New York, 1986, pp: 336–342.
[32] J. Schönheim, On maximal systems of k-tuples, Stud. Sci. Math. Hungar. 1 (1966) 363–368.
[33] V.D. Tonchev, S.A. Vanstone, On Kirkman triple systems of order 33, Discrete Math. 106/107 (1992) 493–496.
[34] L. Zhu, B. Du, X. Zhang, A few more RBIBDs with $k = 5$ and $\lambda = 1$, Discrete Math. 97 (1991) 409–417.