Interactive Communication, Diagnosis and Error Control in Networks

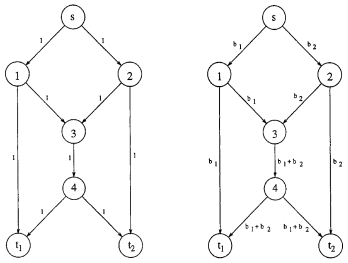
Rudolf Ahlswede[1] and Harout Aydinian[2] ⋆

[1] University of Bielefeld, Department of Mathematics, POB 100131, D-33501 Bielefeld, Germany,
ahlswede@math.uni-bielefeld.de,
[2] ayd@math.uni-bielefeld.de

Abstracts of the work of our research group are given in the following poster of the final meeting.

Network Coding

Network Coding has emerged as a new paradigm that has influenced Information and Coding Theory, Networking, Wireless Communications, Computer Science, Graph Theory etc. (see Network Coding Homepage http://www.ifp.uiuc.edu/ koetter/NWC/) The basic idea of Network Coding (stated by Ahlswede, Cai, Li and Yeung, 2000) is to allow the intermediate nodes to process the received information before forwarding them.



Ahlswede et al. showed that by Network Coding one can achieve the multicast capacity in information networks with a single source. Cai et al. (2002) showed that Linear Coding suffices to achieve the min-cut bound. Sanders et al. (2003) gave a polynomial time algorithm to construct linear codes for single source multicast. The existence of such algorithms is remarkable since the maximum rate without coding can be much smaller and finding the maximum rate routing solution is NP-hard.
Network coding is believed to be highly applicable to communication through real networks, the primary example being the Internet (the most widely known application is the Avalanche program by Microsoft for file distribution protocols). In addition to **throughput gain**, many other benefits such as minimization of **delay**, minimization of **energy per bit**, **robustness, adaptability etc.** of Network Coding have been discovered during the last years.
Research in Network Coding is growing fast (more than 250 papers appeared since 2002). Microsoft, IBM and other companies have research teams who are investigating this new field. A few American universities (Princeton, MIT, Caltech and Berkeley) have also established research groups in Network Coding.
The holy grail in Network Coding is to plan and organize (in an automated fashion) network flow (that is to allow to utilize network coding) in a feasible manner.
Our main contribution is to provide new links between Network Coding and Combinatorics. We showed that the task of designing efficient strategies for information network flow (Network Coding) is closely linked to designing error correcting codes. This link is surprising since it appears even in networks where transmission mistakes never happen! Recall that traditionally error correction is mainly used to reconstruct messages that have been scrambled due to unknown (random) errors. We use error correcting codes when channels are assumed to be error-free. Thus error correcting codes can be used to solve network flow problems even in a setting where errors are assumed to be insignificant or irrelevant.

Identification Entropy

Classical transmission concerns the question "How many messages can we transmit over a noisy channel?" One tries to give an answer to the question "What is the actual message from $\mathcal{M} = \{1, \ldots, M\}$?" On the other hand in *Identification* it is asked "How many possible messages can the receiver of a noisy channel identify?" One tries to give an answer to the question "Is the actual message i?". Here i can be any member of the set of possible messages $\mathcal{N} = \{1, 2, \ldots, N\}$.
On the Source Coding side we introduced the concept of identification entropy, namely the function

$$H_{I,q}(P) = \frac{q}{q-1}\left(1 - \sum_{u \in \mathcal{U}} P_u^2\right).$$

⋆ The author supported by DFG-Schwerpunkt Nr.1126 "Algorithmik großer und komplexer Netzwerke".

We proved that $L_{\mathcal{C}}(P,P) = \sum_{u\in\mathcal{U}} P_u \; L_{\mathcal{C}}(P,u) \geq H_{I,q}(P)$ and thus also that

$$L(P) = \min_{\mathcal{C}} \max_{u\in\mathcal{U}} L_{\mathcal{C}}(P,u) \geq H_{I,q}(P)$$

and related upper bounds, which demonstrate the operational significance of identification entropy in Noiseless **Source Coding similar as Boltzmann/Shannon entropy does in Noiseless Data Compression.**

This theory initiated other research areas like Common Randomness, Authentication in Cryptology, and Alarm Systems. It also led to the discovery of new methods which became fruitful also for the classical theory of transmission, for instance in studies of robustness like arbitrarily varying channels, optimal coding procedures in case o f complete feedback, novel approximation problems for output statistics and generation of common randomness, the key issue in Cryptology.

Connectors in Communication Networks

The study of connectors started with pioneering works by Shannon (1950), Slepian (1952), and Clos (1953), in connection with practical problems in designing switching networks for telephone traffic. Later they were also studied as useful architectures for parallel machines.

An (n, N, d)–connector is an acyclic digraph with n inputs and N outputs in which for any injective mapping of input vertices into output vertices there exist n vertex-disjoint paths of length d joining each input to its corresponding output.

Problem: Construction of sparse $(n, N, 2)$-is lower bounded by $t+1$, for all possible syndromes, in presence of t (or less) faults. Then the degree of sequential diagnosability of the system $t(G) \geq t$.

-connectors (depth 2 connectors) when $n \ll N$.

Such connectors are of particular interest in the design of sparse electronic switches. Also they may be useful as building blocks in multistage connectors.

The probabilistic argument (Baltz, Jäger, and Srivastav 2003) shows the existence of $(n, N, 2)$–connectors of size (number of edges) $O(N)$, if $n \leq N^{1/2-\varepsilon}$, $\varepsilon > 0$.

Our main results are

Explicit constructions: For integers $t > 2$, $n \geq t^t$, $N = \Omega(n^t)$ construction of $(n, N, 2)$-connectors of size $Nn^{\frac{1}{t}(1+o(1))}$. In particular, for all n and $N > N(n)$ construction of connectors of size $2N \log n/(1 + o(1)) \log\log n$.

Existence results: Given $n \geq 2$ and $N \geq N(n)$ there exist $(n, N, 2)$–connectors of size $2N(1 + o(1))$ and this is asymptotically optimal.

For the size of an $(N^\alpha, N, 2)$–connector with $1/2 \leq \alpha < 1$ we have lower and upper bounds: $\Omega(N^{\alpha+1/2})$ and $\mathrm{O}(N^{\alpha+1/2} \log N)$ respectively.

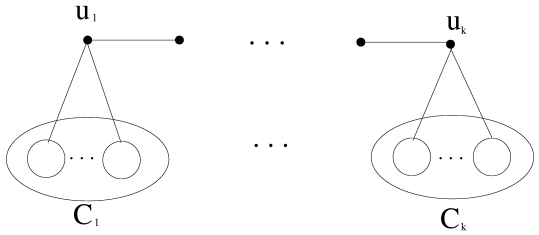
Fault Diagnosis in Large Multiprocessor Networks

Preparata, Metze, and Chien (1967) introduced a graph theoretical model for system-level(see a survey [29]) diagnosis, in which processors perform tests on one another via links in the system. Fault-free processors correctly identify the status of tested processors, while the faulty processors can give arbitrary test results. The goal is to identify faulty processors based on the test results. A system is said to be t-diagnosable if faulty units can be identified, provided the number of faulty units present does not exceed t.

We described an efficient *Diagnosis Algorithm* (DA) for fault identification in large interconnection networks. The algorithm has best known performance: it is linear in time and can be used for sequential diagnosis strategy, as well as for incomplete diagnosis in one step. The algorithm applied to arbitrary topology based interconnection systems G with N processors has sequential diagnosability $t_{\mathbf{DA}}(G) \geq \lceil 2N^{\frac{1}{2}} \rceil - 3$, which is optimal in the worst case.

For any integer N there are connected graphs on N vertices and maximal degree $k \leq N^{\frac{1}{2}}$ with diagnosability $\lceil 2N^{\frac{1}{2}} \rceil - 3$. In particular there are such k–trees.

Example: Let $k = N^{\frac{1}{2}}$ be an integer and let G be a diagnostic graph on N vertices



Each set of vertices C_i with $|C_i| = k - 1$, $(i = 1, \ldots, k)$ represents a union of some connected components (denoted by circles). G is not sequentially $(2N^{\frac{1}{2}} - 2)$–diagnosable. However, using DA any $t \leq 2N^{\frac{1}{2}} - 3$ faulty nodes can be sequentially identified.

Unconventional Error-Correcting Codes

When using amplitude modulation for error-correcting block codes, in several communication systems the magnitude of an error signal is small while the range of error signals can be large. In this case it is impractical to use known classical error-correcting codes. This is a motivation for the development of **codes correcting errors of a limited magnitude** (introduced by Ahlswede et al, 2002).

We studied q-ary codes correcting all unidirectional errors (UEC-codes) of a given magnitude. Tight upper and lower bounds for the cardinality of those codes are obtained and their asymptotic growth rate is determined. For arbitrary code length and alphabet size q, near optimal constructions for UEC-codes capable of correcting all errors of a given magnitude are obtained. An infinite class of perfect codes, for arbitrary code length, is constructed. Recently these codes have been shown to be applicable for design of

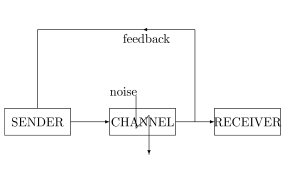
reliable Multilevel Flash memories. Several physical effects that limit the reliability and performance of Multilevel Flash memories induce errors that have low magnitude and are dominantly unidirectional.

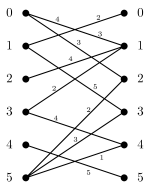
Parallel Error-Correcting Codes

In 2002 Ahlswede, Balkenhol, and Cai introduced a new code concept for multiple-access channels (MAC) with a special error control mechanism. A communication channel consists of several sub-channels transmitting simultaneously and synchronously. The senders encode their messages into codewords of the same length over the same alphabet and transmit them in parallel. When an error occurs in a line at time T, then with a relatively high probability, an error also occurs in its neighbor lines. A parallel t-error-correcting code is a code capable of correcting all t or less errors of this type.
Our main results are constructions of optimal parallel codes with simple decoding schemes. Nontrivial bounds and efficient constructions for such codes for Z–channels have been obtained. The model of parallel error-correcting codes described above is useful for the design of network error-correcting codes in real networks.

Weighted Constrained Error-Correction

The Rényi-Berlekamp-Ulam game is a model for determining the minimum number of queries to find an unknown member in a finite set when up to a finite number of the answers may be erroneous. Questions with q many possible answers are allowed. Errors in the answer are constrained by a bipartite graph with edges weighted by $0, 1, 2, \ldots$ (the "channel").

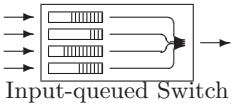




The channel Γ is an arbitrary, though fixed, assignment stipulating the cost of the different possible errors, i.e., of each answer $j \neq i$ when the correct answer is i by $\Gamma(i, j)$. It is also assumed that a maximum cost e (sum of the cost of all wrong answers) can be afforded by the responder. We provided a tight asymptotic estimate for the number of questions needed to solve this problem.

Buffer Management Strategies

We consider the model of an input-queued network switch (m input ports with a buffer of B each; one output port). Data packets have unit length and value. We equip an online algorithm with a lookahead of φ.


Input-queued Switch

We define a class $SFOD_\varphi$ of work-conserving algorithms, which always transmit a packet from a non-empty buffer which would overflow next if not served. If the next overflow is unknown, i.e., it does not fall within the lookahead, $SFOD_\varphi$-algorithms behave arbitrarily.

We proved an upper bound on the competitive ratio of algorithms in $SFOD_\varphi$ that implies optimality ($c = 1$) for $\varphi = B \cdot (m - 1)$ and the known bound of $c \leq 2 - \frac{1}{m}$ for all work-conserving algorithms without lookahead.

If the lookahead grows linearly with B and m with factor $0 \leq p \leq 1$, the bound $c \leq \frac{2}{1+p}$ follows.

We report now about the subjects: **Connectors in communication networks, Diagnosis in multiprocessor networks, Unconventional error-correcting codes, Parallel error-correcting codes** studied jointly with H. Aydinian, the main collaborator in all "Förderzeiträume des Schwerpunktprogramm."

1 Connectors in communication networks

An (n, N)– communication network is defined here as a directed acyclic graph with n distinguished vertices called *inputs* and N other distinguished vertices called *outputs*. All other vertices are called *links*. A *route* in a network is a directed path from an input to an output. The *size* of a network is the number of edges, and the *depth* is the length of the longest route in it. An (n, N, d)–*connector*, also called a *rearrangeable network*, is a network of depth d ($n \leq N$), such that for every injective mapping of the set of input vertices into a set of output vertices there exist n vertex disjoint

paths joining each input to its corresponding output. Usually the size, in some approximate sense, corresponds to the cost and the depth corresponds to the delay of a communication network. Therefore ,for the networks intended for a certain communication task it is preferable to have small size and small depth.

The study of connectors started in the n1950s with works [44], [45], [22], [17], in connection with practical problems in designing switching networks for telephone traffic. Later they were also studied as useful architectures for parallel machines (see [30] for a survey). Connectors are also related to *expander graphs*, a rapidly developing subject in the last three decades, which have found extensive applications (see [29]) in computer science, error correcting codes, cryptography etc.

Symmetric connectors, i.e. connectors with $n = N$, are well studied. Shannon [44] showed that the size of an (n, n, ∞)–connector (unlimited depth) is lower bounded by $\Omega(n \log n)$. Later Beneš [17] gave constructions of $(n, n, \log n)$–connectors of size $O(n \log n)$. In applications it is important to have connectors of a limited depth. Pippenger and Yao [39] obtained lower and upper bounds for the size of an (n, n, d)–connector: $\Omega(n^{1+1/d})$ and $\mathrm{O}(n^{1+1/d}(\log n)^{1/d})$, respectively. The best known explicit construction for odd depth $2i+1$ has size $\mathrm{O}(n^{1+1/(i+1)})$ and is due to Pippenger [38]. Hwang and Richards [30] and Feldman, Friedman, and Pippenger [25] gave explicit constructions for depth 2 connectors of size $\mathrm{O}(n^{5/3})$. The latter can be used for construction of connectors of depth $2i$ and size $\mathrm{O}(n^{1+2/(3i-1)})$.

For asymmetric connectors Oruc [37] gave constructions for depth $\Omega(\log_2 N + \log_2^2 n)$ of size $\mathrm{O}(N + n \log_2 n)$.

Explicit constructions for $(n, N, 2)$–connectors of size $(1 + o(1))N\sqrt{n}$ for $n \leq \sqrt{N}$ (and $N=$ square of a prime) are given in [30] (see also [40]).

Asymmetric connectors of depth two are of particular interest in the design of sparse electronic switches. They are also useful as building blocks in multistage connectors.

Baltz, Jäger, and Srivastav [15] gave construction of $(1 + o(1))N\sqrt{3n/4}$ size connectors for all $n \leq \sqrt{N}$, and have shown, by a probabilistic argument, the existence of $(n, N, 2)$–connectors of size $\mathrm{O}(N)$, if $n \leq N^{1/2-\varepsilon},\ \varepsilon > 0$.

A challenging problem is to construct linear–sized $(n, N, 2)$–connectors (even for some restricted values of n and N).

Construction of asymmetric connectors

We describe here a simple combinatorial construction in [2] of sparse asymmetric connectors. But first we need some preliminaries.

For integers $a < b$ we denote $[a, b] = \{a, a + 1, \ldots, b\}$ and for $[1, b]$ we use the abbreviation $[b]$. We denote $S(k, q) := \{(x_1, \ldots, x_k) :\ x_i \in [0, q]\}$ and for $q = \infty$ we use the notation $[0, \infty] := \{0\} \cup \mathbb{N}$ and $S(k, \infty)$.

We define now a partial ordering on elements of $S(k, q)$ as follows.

For $x, y \in S(k, q)$ we say that $x \leq y$ if either $x_i = y_i$ or $x_i = 0$ for all $i = 1, \ldots, k$. Define also $r(x) =$ the number of nonzero coordinates of $x \in S(k, q)$ (note that $r(x)$ is usually called the Hamming weight of x).

Thus $S(k, q)$ is a partially ordered set ordered by $\leq$ with the rank function $r(x)$ defined for each element $x \in S(k, q)$. In the literature $S(k, q)$ is usually called the product of stars (see e.g. [24]). By $S_r(k, q)$ we denote the elements of rank r, that is $S_r(k, q) = \{x \in S(k, q) :\ r(x) = r\}$. Thus $S(k, q) = S_0(k, q) \dot\cup S_1(k, q) \dot\cup \cdots \dot\cup S_k(k, q)$, where $|S_i(k, q)| = \binom{k}{i} q^i,\ i = 0, 1,\ \ldots, k$.

Given integers $1 \leq l < r \leq k$ and q (or $q = \infty$), the l-th shadow of $x \in S_r(k, q)$ is defined by $\partial_l x = \{y \in S_{r-l} :\ x \geq y\}$. Correspondingly for $X \subset S_r(k, q)$, $\partial_l X = \{\partial_l x :\ x \in X\}$.

Next we define a linear order on $S(k, q)$. Define first $x(t) = \{i \in [k] :\ x_i = t\},\ x \in S(k, q)$. Recall also the colexicographic order on the subsets of $[k]$. For $A, B \subset [k]$ we say $A \prec_{col} B$ iff $\max((A \setminus B) \cup (B \setminus A)) \in B$. Now for $x, y \in S(k, q)$ we define the linear ordering $\prec_L$ as follows: $x \prec_L y$ iff $x(t) \prec_{col} y(t)$, where t is the greatest number such that $x(t) \neq y(t)$.

For a subset $X \subset S(k, q)$ let $\mathcal{C}(m, X)$ denote the set of the first m elements of X with respect to the ordering $\prec_L$.

In our construction we use the following

Lemma 1 *For integers $1 \le l < r \le k$, q and a subset $A \subset S_r(k,\infty)$ with $|A| \le q^r \binom{k}{r}$ we have*

$$|\partial_l A| \ge \frac{|A|\binom{r}{l}}{\binom{k-r+l}{l} q^l}. \tag{1.1}$$

In particular, for $A \subset S_k(k,\infty)$ with $|A| \le \lfloor k/l \rfloor^k$ we have

$$|\partial_l A| \ge |A|. \tag{1.2}$$

The lemma is a consequence of the following result due to Leeb.

Theorem L [34] *For integers $1 \le r \le k$, m and a subset $A \subset S_r(k,\infty)$ with $|A| = m$ holds*

$$\partial_l \mathcal{C}(m, S_r(k,\infty)) \subseteq \mathcal{C}(|\partial_l A|, S_{r-1}(k,\infty)). \tag{1.3}$$

One of standard approaches for construction of connectors is the concatenation of a connector with a *concentrator*. An (N, L, c)–concentrator is an (N, L)–network such that for every set of $j \le c$ inputs there exist j disjoint routes containing these inputs. For concentrators of depth one (that is for bipartite graphs) this is equivalent to the property that every $j \le c$ input vertices have at least j neighbors, that is Hall's matching condition is satisfied for every set of $j \le c$ input vertices.
Depth-one concentrators, also called *crossbar concentrators*, are useful devices in designing of communication networks.
We are prepared now to describe our construction. Let the vertex set $V = \mathcal{I} \cup \mathcal{L} \cup \mathcal{O}$ of a graph $G = (V, E)$ be partitioned into input vertices $\mathcal{I}$ with $|\mathcal{I}| = n$, link vertices $\mathcal{L}$ with $|\mathcal{L}| = L$ and output vertices $\mathcal{O}$ with $|\mathcal{O}| = N$. Consider a network satisfying the following two conditions.
C1: $\mathcal{I}$ and $\mathcal{L}$ form a depth one connector which clearly is a complete bipartite graph.
C2: $\mathcal{O}$ and $\mathcal{L}$ form an (N, L, n)-concentrator.
It is easy to see that G is an $(n, N, 2)$–connector.
Given $t > 2$ and $n \ge t^t$, let k be the minimum integer such that $n \le t^k$. Suppose $k = tl + r$ where $0 \le r < t$. Thus $t^{k-1} < n \le t^k$. Let also, for ease of calculations, $N = q^k$ (in general, $N = \Omega(q^k)$) for some integer $q > \binom{k}{l}^{1/l}$.
We construct the following network satisfying conditions C1, C2:
$\mathcal{O} := \mathcal{C}(N, S_k(k,q))$, $\mathcal{L} := \partial_l \mathcal{C}(N, S_k(k,q))$, $L := |\mathcal{L}|$, and $n := |\mathcal{I}| = \Theta(t^k)$.
The edge set E is defined in a natural way: for $x \in \mathcal{O}$ and $y \in \mathcal{L}$ we have an edge $(x, y) \in E$ iff $y \in \partial_l(x)$. In view of Lemma 1, for any subset $X \subset \mathcal{O}$ with $|X| \le n$ we have $|\Gamma(X)| \ge |X|$. Hence $\mathcal{O}$ and $\mathcal{L}$ form an (N, L, n)-concentrator.
The size of the connector

$$|E| = Ln + N\binom{k}{l} = q^{k-l}\binom{k}{l}\Theta(t^k) + q^k\binom{k}{l}.$$

We choose any $q \ge t^t$. Easy calculations show that we have a $(\Theta(t^k), t^{tk})$–connector with

$$|E| \le 2N\binom{k}{l} = 2Nn^{\frac{1}{t}(1+o(1))}.$$

In particular, for $l = 1$, $n \le k^k \le q$ we get $|E| \le 2N \log n/(1 + o(1)) \log\log n$.
Thus we have

Theorem 1 *[2] For all integers $t > 2$, $n \ge t^t$, and $N = \Omega(n^t)$ the construction above gives $(n, N, 2)$-connectors of size $Nn^{\frac{1}{t}(1+o(1))}$. In particular, for all n and $N > N(n)$ we get connectors of size $2N \log n/(1 + o(1)) \log\log n$.*

Fault–Tolerant Connectors

An important task in designing of communication networks is reliability. Therefore it is natural to consider connectors which are robust under edge or node failures. An $(n, N, 2)$–connector is called

t–edge fault–tolerant if in spite of deletion of any t or less edges (edge failures) the resulting graph is an $(n, N, 2)$–connector. Correspondingly, it is called t– fault–tolerant if this property holds after deletion of any t or less link vertices (vertex failures), which also implies t–edge fault–tolerance.
Note also that for any t–edge fault–tolerant connector, t is less than its minimum degree of input/output vertices.
Constructions of sparse fault-tolerant $(n, N, 2)$–connectors of size $(1+o(1))N \log_2 n$ are given in [1]. The construction is similar to the construction described above. Here we use the Boolean lattice of finite subsets of $[N]$, $N \subset \mathbb{N}$, and output vertices are associated with the k–sets of $[N]$.

Theorem 2 *[1] For all N and $n = O\big(N^{1/\sqrt{\log_2 N}}\big)$ there exist explicitly constructible $(n, N, 2)$–connectors of size $(1 + o(1))N \log_2 n$ which are $(k-1)$– fault–tolerant, where $k = \Theta(\log_2 n)$ is the degree of output vertices.*

Existence results

As we mentioned above the existence of linear sized $(n, N, 2)$–connectors for $n \leq N^{1/2-\varepsilon}$, with $\varepsilon > 0$ is shown in [15]. A simple probabilistic argument gives also exact upper bound for the size of an $(n, N, 2)$-connector.

Theorem 3 *[2] For all $n \geq 2$ and $N \geq N(n)$ there exist $(n, N, 2)$–connectors of size $2N(1 + o(1))$ and this is asymptotically optimal.*

It is natural to ask for the size of $(n, N, 2)$–connectors with $N^{1/2} \leq n < N$. Construction of such connectors of size $O(N^{3/4}n)$ are given in [30], [15].

Theorem 4 *[2] For the size of an $(N^\alpha, N, 2)$–connector with $1/2 \leq \alpha < 1$ we have lower and upper bounds: $\Omega(N^{\alpha+1/2})$ and $O(N^{\alpha+1/2} \log N)$ respectively.*

The proof follows from the following observation. Let G_1 and G_2 be $(n_1, N, 2)$ and $(n_2, N, 2)$–connectors respectively and let $G_1 * G_2$ be the $(n_1 + n_2, N, 2)$–network obtained by identifying the outputs of G_1 and G_2 by any one-to-one mapping. It is easy to see that $G_1 * G_2$ is an $(n_1 + n_2, N, 2)$–connector and the size of the resulting connector equals to the sum of sizes of G_1 and G_2.
Suppose there exists an $(N^\alpha, N, 2)$–connector G of size $\Omega(N^x)$ with $1/2 \leq \alpha \leq 1$. We construct an $(N, N, 2)$–connector from $G * \ldots * G$, taking sufficiently many copies of G and then deleting all but N input vertices of the resulting network. The constructed connector has size $\Omega(N^{1-\alpha}N^x)$. This, together with the lower bound $\Omega(N^{3/2})$ in [25] for an $(N, N, 2)$-connector, implies that G has size $\Omega(N^{1/2+\alpha})$. Similarly the existence of linear-sized $(N^\delta, N, 2)$–connectors for any $0 < \delta < 1/2$ implies also the existence of $(N^\alpha, N, 2)$– connectors of size $\mathrm{O}(N^{1+\alpha-\delta})$ with $1/2 \leq \alpha \leq 1$. This can be used to obtain upper bounds for the size of $(N^\alpha, N, 2)$ in particular, connectors of size $\mathrm{O}(N^{\alpha+1/2} \log N)$.

Open problems

A challenging open problem is an explicit construction of linear-sized depth two (or at least limited depth) asymmetric connectors.
In our construction we used posets of star products. Can we improve the construction using other posets?
In fact, our approach above reduces to construction of sparse concentrators of depth one. In general, we have the following combinatorial optimization problem which has been extensively studied in various settings (see [29],[53], [41]) : Given N, l, c determine
$E(N, l, c)$:= the minimum possible size of a depth-one (N, l, c) –concentrator.
This, however seems to be a difficult problem.
Note that in terms of the adjacency matrix A of a bipartite graph $G = (V, E)$ $E(N, l, c)$ is the minimum number of 1's of an $l \times N$ (0,1)–matrix A such that the boolean sum of every j columns, $j = 1, ..., c$, has at least j ones. Equivalently, no set of j columns, $j = 1, ..., c$, contains an $(l - j + 1) \times j$ all zero submatrix.

A weakened version of the problem is as follows: Minimize the number of 1's of an $l \times N$ (0,1)–matrix A such that it does not contain an $(l - n + 1) \times n$ all zero submatrix.
This problem (exchanging $0 \leftrightarrows 1$) is equivalent to *Zarankiewicz's problem* (1951):
Given integers $k, m, a, b;\ 0 \leq a \leq k,\ 0 \leq b \leq m,$ determine
$Z_{a,b}(k, m) :=$ maximum number of 1's in an $k \times m$ (0,1)– matrix which does not contain an $a \times b$ all one submatrix.
The problem is widely open, even for the case $a = b = 2$. Kövari, Sós, and Turán (see [19], pp. 309-326) obtained the following upper bound: $Z_{a,b}(k, m) \leq (a-1)^{1/b}(m-b+1)k^{1-1/b} + (b-1)k$.

2 Fault diagnosis in large multiprocessor networks

With the continuing development of semiconductor technologies, large multiprocessor systems such as VLSI have been of growing concern. A multiprocessor system may contain a huge number of processors proceeding simultaneously at very high speed. The uninterrupted processing is an important task in designing of reliable multiprocessors systems. An integral part of reliability is the identification of faulty processors.
The concept of *system–level* diagnosis was introduced by Preparata, Metze, and Chien [42] to perform automatic fault diagnosis in multiprocessor systems. In their graph theoretical model, called PMC model, a system S is composed of independent units $u_1, \ldots, u_n$ connected by communication links. The system is represented as an undirected graph $G = (V, E)$, where the vertices are units and edges are interconnection links. In the PMC model diagnosis is based on a suitable set of tests between units. A unit u_i can test u_j iff the vertices corresponding to u_i and u_j in the graph $G = (V, E)$ of the system S are adjacent. The outcome of a test in which u_i tests u_j is denoted by a_{ij}, where $a_{ij} = 1$ if u_i finds u_j to be faulty and $a_{ij} = 0$ if u_i finds u_j to be fault-free.
The basic conditions of the PMC model are the following:

- The fault-free units give correct test outcomes.
- The answers of faulty units are unreliable.
- The number of faulty units t is bounded.

The set of tests for the purpose of diagnosis is represented by a set of directed edges where the presence of oriented edge (u_i, u_j) means that u_i tests u_j. Given a faulty set of units $F \subset V$ the set of all test outcomes $\{a_{ij}\}$ is called *syndrome*. The task is to identify the faulty units based on a syndrome produced by the system. In [42] two different kinds of strategies were introduced for implementing the diagnosis approach.
One-step diagnosis (or diagnosis without repair): a system is called t-fault diagnosable (or shortly t-diagnosable) in one step, if all faulty units can be uniquely identified from any syndrome, provided the number of faulty units does not exceed t.
Sequential diagnosis (or diagnosis with repair): a system is called sequentially t-diagnosable if it can identify at least one faulty unit from any syndrome, provided the number of faulty units does not exceed t. Under a sequential diagnosis strategy a system can locate a faulty unit, repair it and then repeat the process until all faulty units are repaired.
The *degree of diagnosability*, or simply diagnosability, of a system graph G is defined (for both kinds of strategies) as the maximum t such that the system is t-diagnosable.
The PMC model has been widely studied (see [16] for a good survey). It is known that the maximum degree of diagnosability of a one-step diagnosis algorithm for any system is bounded from above by the minimum vertex degree of the interconnection graph. However, the real commercial multiprocessor systems are based on topologies of graphs with small average vertex degree (like grids, hypercubes, cube-connected cycles, trees etc).
Sequential diagnosis is a much more powerful strategy than one-step t-fault diagnosis. On the other hand the sequential diagnosis has the disadvantage of repeated execution of diagnosis and repair phases and may be time consuming for large systems.
That was the motivation for developing diagnosis algorithms (see [20]) which are able to diagnose in one step the status of a large fraction of the system units (i.e. if a "large" subset F' of the actual fault set F can be identified from any syndrome, provided $|F| \leq t$). This approach is referred to as *incomplete diagnosis in one step.*

Further we concern with sequential diagnosis problems. In fact there are two main problems (for both strategies). Theoretical: determination of diagnosability of a given system and Algorithmic: development of algorithms for fault identification.
Note that the problem of determining the sequential diagnosability of a system is shown to be co-NP complete [46].
The *diagnostic graph DG* of a system graph $G = (V, E)$, corresponding to a given syndrome, consists of bidirectional arcs, between every two neighbors of the original graph G, labelled by 0 or 1. Let $\{u, v\} \in E(G)$, then the presence of oriented edges (u, v) and (v, u) with $a_{uv} = 1$ and $a_{vu} = 0$ implies that v is faulty. Thus, in the worst case analysis, we assume that the outcomes of any two neighbors coincide. Therefore, a diagnostic graph is represented as an undirected graph where each edge is labelled by a 0 or a 1.
Given a syndrome, a subset F of the vertex set V is called a *consistent fault set* if the assumption that the vertices in F are faulty and those in $V \setminus F$ are fault–free is consistent with the syndrome. The following simple facts are useful for obtaining upper and lower bounds for the diagnosability of a system graph.

Proposition 1 *Given a syndrome, let $F_1, \ldots, F_k$ be a collection of consistent fault sets with $|F_i| \leq t$ for $i = 1, \ldots, k$. Then G is not sequentially t-diagnosable if $\bigcap_{i=1}^{k} F_i = \varnothing$ and $\bigcup_{i=1}^{k} F_i = V$.*

Given a diagnostic graph DG, define the subgraph G_0 consisting of edges labelled only by 0 (0-edges). The connected components of the graph G_0 are called 0-components of DG.

Proposition 2 *(i) All vertices of a 0-component in a diagnostic graph DG have the same status: "faulty" or "fault-free".*
(ii) Suppose the size of a largest 0-component $K \subset$ in G_0 is greater than the fault bound t. Then all vertices of K can be identified as fault-free.

Two extremal problems on graphs

Motivated by a problem (Dijkstra's critical section problem) arising in parallel computation for unreliable networks, Ahlswede and Koschnick [13] considered the following extremal problems for graphs.

Problem 1 *Given a connected graph $G = (V, E)$, let $\lambda(G, c)$ denote the maximal number such that removal of any $\lambda(G, c)$ or less vertices results in a graph with a connected component of size at least c. Determine or estimate $\lambda(G, c)$.*

Problem 2 *Removing edges instead of vertices, define analogously the function $\mu(G, c)$ and determine or estimate $\mu(G, c)$.*

Define also the function $\lambda^*(G, c)$ (resp. $\mu^*(G, c)$) = minimal number with the property that there exist $\lambda^*(G, c)$ vertices (resp. $\mu^*(G, c)$ edges) whose removal results in a graph with a maximal connected component of size $\leq c$. Observe that $\lambda^*(G, c)$=$\lambda(G, c+1)+1$ and $\mu^*(G, c)$= $\mu(G, c+1)+1$.
In fact, these functions are measures of connectivity in a graph, which generalize the known notion of edge/vertex connectivity in graphs.
It is not hard to show that both problems are NP-hard.
We note that both functions $\lambda(G, c)$ and $\mu(G, c)$ are useful for diagnosis problems in multiprocessor systems. In fact the following derived quantity is essential. For a graph G define $m(G) = \max\{x : \lambda(G, x + 1) \geq x\}$.
Now Proposition 2 implies

Proposition 3 *For every interconnection graph G, the diagnosability $t(G) \geq m(G)$.*

Note, however, that in general $m(G)$ can be much smaller than the degree of sequential diagnosability. Consider, for example, a star graph G on $N = 2k + 1$ vertices. It is not hard to observe that the sequential diagnosability of this graph $t(G) = k$ while $m(G) = 0$.

Khanna and Fuchs [32], and also Caruso *et al.* [20], studied the function $m(G)$ and gave algorithms for fault identification for some regular structures. In [32] a sequential diagnosis algorithm (referred to as PARTITION) applied to arbitrary interconnection graph on N vertices has diagnosability $\Omega(N^{\frac{1}{3}})$. Yamada *et al* [54] described a sequential diagnosis algorithm (referred to as HYBRID) for an interconnection graph G on N vertices with diagnosability $t_{HYBRID}(G) \geq \lceil \sqrt{N-1} \rceil - 1$.
Next we describe an efficient diagnosis algorithm DA [4] which can be used for sequential diagnosis as well as for incomplete diagnosis in one step. In particular, the algorithm applied to arbitrary topology based interconnection systems has the best performance.

Diagnosis Algorithm DA

Given a connected graph $G = (V, E)$ and a syndrome, that is, a diagnostic graph $DG = (V, E')$, where each edge of E is labelled by a 0 or 1.
Step 1 Partition the vertices of DG into 0-components $K_1, \ldots, K_\ell$; $\mathcal{K} := \{K_1, \ldots, K_\ell\}$.
Step 2 Construct the contracted graph $G_c = (V_c, E_c)$ as follows.
Each component K_i contracts to vertex $a_i \in V_c$ and $\{a_i, a_j\} \in E_c$ iff there is an edge $\{u, v\}$ (labelled with 1) in E with $u \in K_i$ and $v \in K_j$. To each vertex a_i of V_c assign the weight $wt(a_i) = |K_i|$. Thus G_c is an undirected graph with weights on vertices. Clearly $\sum\limits_{a \in V_c} wt(a) = |V|$. The weight of a subgraph $G' \subset G_c$ is defined by $wt(G') = \sum\limits_{b \in V'} wt(b)$, where V' is the vertex set of G'.
Step 3 Find a spanning tree TG_c of G_c.
Step 4 Partition the vertex set of TG_c into subsets $T_1, \ldots, T_p$, each containing at least two vertices, such that the induced subgraph of each subset T_i forms a star S_i, $i = 1, \ldots, p$. Denote by z_i the center of S_i, $i = 1, \ldots, p$ and put

$$w_i := \min\big\{wt(z_i),\ wt(S_i \setminus \{z_i\})\big\}, \quad \alpha_i := \max\big\{wt(z_i),\ wt(S_i \setminus \{z_i\})\big\}, \quad i = 1, \ldots, p,$$
$$\bar{w} := w_1 + \cdots + w_p, \quad \bar{\alpha} := \alpha_1 + \cdots + \alpha_p.$$

Step 5 Determine $\Delta = \max_{1 \leq i \leq p}\{\alpha_i + \bar{w} - w_i\}$. Suppose $\Delta = \alpha_r + \bar{w} - w_r$; $r \in [1, p]$. Suppose also the number of actual faults $t \leq \Delta - 1$.
Step 6 If $wt(z_r) = w_r$, then the vertex z_r is labelled as "faulty". The component $K_{i_r} \subset \mathcal{K}$ corresponding to z_r is diagnosed as faulty set.
If $wt(z_r) = \alpha_r$, then z_r is labelled as "non-faulty" and the remaining vertices of S_r are labelled as "faulty". The components corresponding to vertices $S \setminus \{z_i\}$ are diagnosed as faulty sets.

The described algorithm allows to identify the status of at least one vertex if the number of faulty units $t < \min \Delta(t, G)$, where the minimum is taken over all syndromes produced by all faulty sets $F \subset V$ with $|F| \leq t$.
The status of remaining vertices is identified iteratively applying the "diagnosis and repair" procedure.

Theorem 5 *[4] Given interconnection graph $G = (V, E)$,*
(i) the overall running time of the diagnosis algorithm DA is $O(|E|)$,
(ii) it requires at most $d(G)$ (diameter of G) iterations, to identify all faults,
(iii) and given a lower bound $m^*(G)$ for $m(G)$, the diagnosability of the algorithm $t_{DA}(G) \geq \max\{m^*(G), 2|V|^{\frac{1}{2}} - 3\}$.

Corollary 1 *For an arbitrary interconnection graph G on N vertices the diagnosability of the algorithm $t_{DA}(G) \geq \lceil 2N^{\frac{1}{2}} \rceil - 3$.*

In fact, the algorithm is optimal for "bad graphs": there exist infinitely many interconnection graphs $G = (V, E)$ with sequential diagnosability $\lceil 2|V|^{\frac{1}{2}} \rceil - 3$. In particular there are such k–trees.

Example Let $k = N^{\frac{1}{2}}$ be an integer and let DG be a diagnostic graph on N vertices shown in Figure 1.
DG: each set of vertices C_i with $|C_i| = k-1$, $(i = 1, \ldots, k)$ represents a union of some 0–components (denoted by circles), where the edges incident with vertices $u_1, \ldots, u_k$ are labelled by 1's. We denote

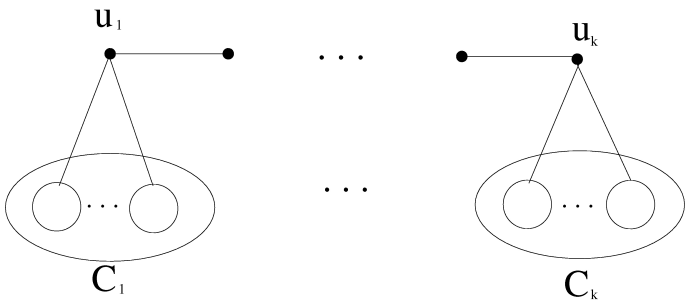


Fig. 1.

$U = \{u_1, \ldots, u_k\}$. and define then the faulty sets $F_1, \ldots, F_k$ as $F_i = (U \setminus \{u_i\}) \cup C_i,\ \ i = 1, \ldots, k$. Note that $|F_i| = 2k - 2$. All these sets are consistent fault sets (their intersection is empty and the union is the vertex set of G). Therefore, G is not sequentially $(2N^{\frac{1}{2}} - 2)$–diagnosable.

Bounds for $\lambda(\mathcal{H}_n, c)$ in Hamming graphs $\mathcal{H}_n$

Lower bound
Let $\mathcal{H}_n = \{0,1\}^n$ denote the binary Hamming space and let $d(x,y)$ denote the Hamming distance between any two vectors $x, y \in \mathcal{H}_n$, defined as the number of coordinates in which they differ. We associate $\mathcal{H}_n$ with the Hamming graph $G(\mathcal{H}_n)$ where two vertices $x, y \in \mathcal{H}_n$ are adjacent iff $d(x,y) = 1$. Let us denote $N_{n,k+1} = \binom{n}{n} + \cdots + \binom{n}{k+1}$,

Theorem 6 *(i) For $n \geq 2k$ we have*

$$\lambda^*(n, N_{n,k+1}) = \binom{n}{k}$$

(ii)

$$\lambda(n, N_{n,k+1}) = \begin{cases} \binom{n}{k} & ,if \quad n > 2k \\ \binom{n}{k} + 1 & ,if \quad n = 2k,\ \ k \geq 3. \end{cases}$$

The proof is based on Harpers vertex isoperimetric theorem [28].

Upper bound
We describe a regular separation of the vertices of the Hamming graph $G(\mathcal{H}_n)$. For convenience of the description, we identify $\mathcal{H}_n$ with the set of vectors $\mathcal{H}_n^* := \{-1, 1\}^n \subset \mathbb{R}^n$ using $1 \to -1$ and $0 \to 1$ exchange of the coordinates. Thus we can speak about an identical graph $G(\mathcal{H}_n^*)$. Note that the Hamming distance between any $x, y \in \mathcal{H}_n^*$ can be evaluated by their inner product $\langle x, y \rangle$, that is, $d(x,y) = \frac{1}{2}(n - \langle x, y \rangle)$.
The idea is to separate the elements of $\mathcal{H}_n^*$ into equal sized parts by mutually orthogonal hyperplanes of $\mathbb{R}^n$. It is known that for any $n = 2^k$ there exist Hadamard matrices of order n. Recall that a $(+1, -1)$–matrix H of size $n \times n$ is called a Hadamard matrix of order n, if $HH^T = nI_n$. Hadamard matrices H_n of order $n = 2^k$ can be constructed as k-th Kronecker power of matrix $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.
Note that the corresponding (0,1)-matrix without all-zero column can be viewed as the simplex code of length $2^k - 1$ (well known in Coding Theory [36]) with a generator matrix of size $k \times 2^k - 1$ consisting of all-nonzero column vectors.
Given a set of n vectors $v_1, \ldots, v_n \in \mathcal{H}_n^*$, let $\langle v_1 \rangle, \ldots, \langle v_n \rangle$ be the hyperplanes defined by $\langle v_i \rangle = \{x \in \mathbb{R}^n : \langle v_i, x \rangle = 0\}$, $i = 1, \ldots, n$.
Given an integer $1 \leq r \leq n$ let us define the set of *sign sequences* $\Sigma := \{+, -\}^r$. Let $x \in \mathcal{H}_n^*$ and let $(\sigma_1, \ldots, \sigma_r) \in \Sigma$. We say that $Sign(x) = (\sigma_1, \ldots, \sigma_r)$ if $Sign\langle x, v_i \rangle = \sigma_i$, $i = 1, \ldots, r$, (where for a real number a, like $\langle x, v_i \rangle$, $Sign\ a$ is defined in the natural way). Let $\Sigma_1, \ldots, \Sigma_{2^r}$ be the elements of Σ in some fixed order. Define the sets $B_i = \{x \in \mathcal{H}_n^* : Sign(x) = \Sigma_i\}$; $i = 1, \ldots, 2^r$. Clearly these sets are disjoint. Denote the set of remaining elements of $\mathcal{H}_n^*$ by S_r, that is, $S_r = \{x \in \langle v_i \rangle \cap \mathcal{H}_n^*$:

$1 \leq i \leq r\}$. The hyperplanes $\langle v_1\rangle, \ldots, \langle v_r\rangle$ separate the points of $\mathbb{R}^n$ into classes which have different signs. Therefore we have the following.

Lemma 2 *S_r is a vertex separating set for $B_1, \ldots, B_{2^r}$, that is, any path between the vertices of two distinct classes B_i and B_j contains a vertex of S_r.*

Theorem 7 *Given integers $n = 2^k$ and $1 \leq r \leq k$, we have*

$$\lambda(n, 2^{n-r} - |S_r|/2^r) \leq |S_r|. \tag{2.12}$$

Corollary 2 *For positive integers n and $r \leq \lfloor \log n \rfloor$.*

$$\lambda(n, 2^{n-r}) = O(r2^n/\sqrt{n}). \tag{2.13}$$

Conjecture *For $n = 2^k$ and $1 \leq r \leq k$*

$$\lambda(n, 2^{n-r} - |S_r|/2^r) = |S_r|. \tag{2.14}$$

Note that (in view of Theorem 6) the conjecture holds for $r = 1$.

Diagnosability of the n-cube

Theorem 6 has several consequences. Suppose the number of faulty sets $\binom{n}{k-1} < t \leq \binom{n}{k}$, $(k \leq n/2)$, then there exists a set of vertices $A \subset \mathcal{H}_n$ with $|A| \geq N_{n,k+1}$ that can be identified as "fault-free" and the vertices ΓA can be identified as "faulty". Thus the status of at least $|\sigma(A)|=|A \cup \Gamma A|$ elements can be identified in one step.

Corollary 3 *(i) Let t be the number of faulty vertices and let $\binom{n}{k-1} < t \leq \binom{n}{k}$, $k \leq n/2$. Then the status of at least $N_{n,k}$ vertices can be identified in one step. In particular, for $k = n/2$, the status of at least $N_{n,n/2} = 2^{n-1} + \binom{n-1}{\frac{n}{2}-1}$ vertices can be identified.*
(ii) Given integer $n \geq 3$ we have $m(\mathcal{H}_n) \geq \binom{n}{\lfloor \frac{n}{2} \rfloor}$ and hence the degree of sequential diagnosability of the n-cube $t(\mathcal{H}_n) > \binom{n}{\lfloor \frac{n}{2} \rfloor}$

An important parameter in sequential diagnosis is the number of test and repair iterations needed to locate all the faulty units within the system (see [20], [48]). Thus, reducing the number of iterations is an important task in implementation of a diagnosis scheme. It was shown in [48] that this number for n-cubes is upper bounded by $\Theta(n)$. As a direct consequence of Theorem 6 we also get

Corollary 4 *Let $\binom{n}{k-1} < t \leq \binom{n}{k}$, $k \leq n/2$, then the number of iterations needed for sequential diagnosis is at most k.*

Theorem 7, in turn, can be used to obtain an upper bound for the sequential diagnosability of the n-cube. The following upper bound obtained by Yamada et al. [54] can be easily derived from (2.13).

Theorem 8 *[54] $t(\mathcal{H}_n) = O(2^n \log n/\sqrt{n})$.*

Diagnosis under pessimistic strategy: $t|s$-diagnosis

In both, one-step and sequential diagnosis strategies, it is assumed that only those processors that where truly faulty were replaced. Therefore, the strategy may be called *precise diagnosis strategy.* Friedman [26] proposed a strategy under which up to s or less processors containing all (t or less faulty processors) and possibly some processors of unknown status were identified and replaced. This strategy is called *pessimistic diagnosis strategy* or shortly *$t|s$–diagnosis.* A system is called $t|s$–diagnosable if for a given syndrome all faulty units can be isolated within a set of at most s units, provided the number of faulty units does not exceed t.

The motivation for the study of such strategy is to increase the "diagnosability" of a given multiprocessor networks. Suppose all $t-1$ neighbors of a processor are faulty. Then under precise diagnosis strategy the status of this isolated processor cannot be determined. Under the pessimistic strategy such an isolated processor is treated as potentially faulty and replaced. Therefore the diagnosability under pessimistic strategy can be much higher.

Definition 1 *Given integer $r \geq 0$ the degree of $t|t+r$–diagnosability of a system is defined as the maximum t for which the system is $t|t+r$ diagnosiable.*

Kavianpour and Kim [31] showed that $t|t$– diagnosability of the n-cube is $2n-2$ for $n \geq 4$ (Note that the diagnosability of the n–cube under one-step strategy is n.). The next theorem gives exact answer for all $0 \leq r \leq 2n-4$.

Theorem 9 *The degree of $t|t+r$ diagnosability of the n–cube is*
$\binom{n}{2} - \binom{n-r-2}{2} + 1$ *for* $0 \leq r \leq n-2$; $n \geq 4$, *and is*
$\binom{n}{2} + \binom{n-2}{2} - \binom{2n-r-4}{2} + 1$ *for* $n-1 \leq r \leq 2n-4$; $n \geq 6$.

Open problems

Close the gap between upper and lower bounds (or give better estimates) for the sequential diagnosability of n–cube systems.
A closely related problem is to give good estimates for $m(\mathcal{H}_n)$ and $\lambda(\mathcal{H}_n, c)$.
Consider these problems (and the $t|s$–diagnosis problem) for other popular topology based systems.

3 Unconventional error–correcting codes

In the binary symmetric channel it is assumed that for both symbols of the alphabet the probability of an error is the same. However in many digital systems such as fiber optical communications and optical disks the ratio between probability of errors of type $1 \to 0$ and $0 \to 1$ can be large. Practically one can assume that only one type of errors, called asymmetric, can occur in those systems. This binary channel is referred to as Z–channel. Similarly, asymmetric errors are defined for a q-ary alphabet $Q = \{0, \ldots, q-1\}$. For every input symbol i the receiver gets a symbol only from $\{i, \ldots, q-1\}$. Thus for any transmitted vector $(x_1, \ldots, x_n)$ the received vector is of the form $(x_1 + e_1, \ldots, x_n + e_n)$ where $e_i \in Q$ and $x_i + e_i \leq q-1$, $i = 1, \ldots, n$. For more information on asymmetric/unidirectional error correcting codes and their applications see [18], [33], [51].
When using amplitude modulation (in multilevel transmission) for error correcting block codes, in several communication systems the magnitude of an error signal (i.e. the correlation between an input and the output signal) is small while the range of error signals (i.e. the number of errors occurred in a block) can be large (even close to the block length). In this case it is impractical to use known classical error correcting codes. This is a motivation for the development of *codes correcting /detecting asymmetric errors of a limited magnitude*. These codes were first introduced and studied in Ahlswede et al [5],[8].
Recently these codes have been shown to be applicable for design of reliable Multilevel Flash memories [21]. Several physical effects that limit the reliability and performance of Multilevel Flash memories induce errors that have low magnitude and are dominantly asymmetric. Flash Memory is a NonVolatile Memory (NVM) technology that is both electrically programmable and electrically erasable. This property, together with high storage densities and high speed programming, has made Flash Memory the dominant NVM technology and a prominent enabler for many portable applications and technologies. It is a technology that is primarily used in memory cards and USB flash drives, which are used for general storage and transfer of data between computers and other digital products.
We consider *a special type of asymmetric errors in a q-ary channel*, where the magnitude of each component of $\mathbf{e}$ satisfies $0 \leq e_i \leq \ell$ for $i = 1, \ldots, n$. We refer to ℓ as level. Correspondingly we say that *a unidirectional error of level ℓ has occurred*, if the output is either $\mathbf{x} + \mathbf{e}$ or $\mathbf{x} - \mathbf{e}$ (in the latter case, it is of course required that $x_i \geq e_i$ for all i).

If the error vector $\mathbf{e}$ has Hamming weight t, then we say that t errors of level ℓ have occurred. Thus the general coding problem can be formulated as follows.
Given n, ℓ, t, q construct q-ary codes of length n capable of correcting t errors of level ℓ. Of course we wish the size of a code to be as big as possible. We consider q-ary codes correcting all asymmetric errors of given level ℓ, (that is $t = n$) for which we use the abbreviation ℓ-AEC code, and ℓ-UEC codes that correct all unidirectional errors of level ℓ.
For given ℓ, let $A_a(n,\ell)_q$ and $A_u(n,\ell)_q$ denote the maximum number of words in a q-ary AEC code, or UEC code respectively, of length n. Clearly $A_u(n,\ell)_q \leq A_a(n,\ell)_q$.

Distances and error-correcting capabilities

Definition 2 *For* $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in Q^n$ *and* $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in Q^n$,

$$d_{\max}(\mathbf{x},\mathbf{y}) = \max\{|x_i - y_i| : i = 1, 2, \ldots, n\}$$
$$d_u(\mathbf{x},\mathbf{y}) = \begin{cases} d_{\max}(\mathbf{x},\mathbf{y}) & \text{if } \mathbf{x} \geq \mathbf{y} \text{ or } \mathbf{y} \geq \mathbf{x}, \\ 2d_{\max}(\mathbf{x},\mathbf{y}) & \text{if } \mathbf{x} \text{ and } \mathbf{y} \text{ are incomparable}, \end{cases}$$

where $\mathbf{x} \geq \mathbf{y}$ *means that* $x_i \geq y_i$ *for all* i.

Later on for short we will write $d(\mathbf{x},\mathbf{y})$ for $d_{\max}(\mathbf{x},\mathbf{y})$.
Note that d_u does not define a metric: take $\mathbf{x}$=(0,2), $\mathbf{y}$=(1,0) and $\mathbf{z}$=(1,2). Then $d_u(\mathbf{x},\mathbf{y}) = 4 > 1 + 2 = d_u(\mathbf{x},\mathbf{z}) + d_u(\mathbf{z},\mathbf{y})$.

Proposition 4 *A code* $\mathcal{C} \subset Q^n$ *is an* ℓ*-AEC code iff* $d(\mathbf{x},\mathbf{y}) \geq \ell + 1$ *for all distinct* $\mathbf{x}$,$\mathbf{y}$ *in* $\mathcal{C}$.

Proposition 5 *A code* $\mathcal{C} \subset Q^n$ *is an* ℓ*-UEC code if and only if* $d_u(\mathbf{x},\mathbf{y}) \geq 2\ell + 1$ *for all distinct* $\mathbf{x}$, $\mathbf{y}$ *in* $\mathcal{C}$.

ℓ-AEC and ℓ-AUC codes

Theorem 10 *For all integers* n *and each* $\ell \in Q$, $A_a(n,\ell)_q = \left\lceil \frac{q}{\ell+1} \right\rceil^n$.

The code $\mathcal{C} = \left\{(x_1, x_2, \ldots, x_n) \in Q^n : x_i \equiv 0 \mod (\ell+1) \text{ for } i = 1, 2, \ldots, n\right\}$ obviously is an ℓ-AEC code that achieves equality in Theorem 10. A received vector can be decoded by component-wise rounding downwards to the nearest multiple of ℓ+1.
We study $A_u(n,\ell)_q$, the maximum number of words in a q-ary ℓ-UEC code of length n. As any ℓ-UEC code is an ℓ-AEC code, Theorem 10 implies that

$$A_u(n,\ell)_q \leq A_a(n,\ell)_q = \left\lceil \frac{q}{\ell+1} \right\rceil^n. \tag{3.1}$$

We give two constructions for q-ary ℓ-UEC codes valid for all pairs (q,ℓ). We denote by $Q_{\ell+1}$ all integers in $Q = [0, q-1]$ that are multiples of $\ell + 1$, that is

$$Q_{\ell+1} = \{m \in \{0, 1, \ldots, q-1\} : m \equiv 0 \pmod{\ell+1}\} = \{a(\ell+1) : 0 \leq a \leq b-1\}, \tag{3.2}$$

where

$$b = |Q_{\ell+1}| = \left\lceil \frac{q}{\ell+1} \right\rceil.$$

It is clear that $d(\mathbf{x},\mathbf{y}) \geq \ell + 1$ for any two distinct words $\mathbf{x}, \mathbf{y}$ in $Q^n_{\ell+1}$.

Construction 1 "Taking a subset of $Q^n_{\ell+1}$"
For each j let

$$C(j) = \{(x_1, x_2, \ldots, x_n) \in Q^n_{\ell+1} : \sum_{i=1}^{n} \frac{x_i}{\ell+1} = j\}.$$

Any two distinct words from $C(j)$ clearly are incomparable and so $C(j)$ is an ℓ-UEC code. It is clear that

$$|C(j)| = |\{(y_1, y_2, \ldots, y_n) \in \{0, 1, \ldots, b-1\}^n : \sum_{i=1}^{n} y_i = j\}|.$$

This construction leads to the following

Theorem 11 *For each integer q and $\ell \in Q$, there is a constant $c > 0$ such that for each n,*

$$A_u(n,\ell)_q \geq c\frac{1}{\sqrt{n}}\lceil\frac{q}{\ell+1}\rceil^n .$$

Construction 2 "Adding tails to words from $Q^n_{\ell+1}$"

Proposition 6 *Let $X \subset Q^n$ be an ℓ-AEC code. For $\mathbf{x} \in X$, let $S(\mathbf{x})$ denote the sum of its entries, and let s_1, s_2 be such that for each $\mathbf{x} \in X$, $s_1 \leq S(x) \leq s_2$. Let $\phi : [s_1, s_2] \to Q^m$ be such that for all $a, b \in [s_1, s_2]$ with $a > b$, there is an $i \in \{1, 2, \ldots, m\}$ such that $(\phi(a))_i < (\phi(b))_i$. Then $\mathcal{C} = \{(\mathbf{x}, \phi(S(x)) : \mathbf{x} \in X\} \subset Q^{n+m}$ is an ℓ-UEC code.*

Theorem 12 *For each q and ℓ, there exists a positive constant K such that for each n,*

$$A_u(n,\ell)_q \geq Kb^n n^{-\frac{1}{2}\log_q b}, \text{ where } b = \lceil\frac{q}{\ell+1}\rceil .$$

ℓ-UEC codes of Varshamov-Tennengolts type

In [49] Varshamov and Tennengolts gave the first construction of nonlinear codes correcting asymmetric errors. Given $n \in \mathbb{N}$ and an integer a, the Varshamov–Tennengolts code (VT code) $C(n, a)$ is defined by

$$C(n,a) = \{x^n \in \{0,1\}^n : \sum_{i=1}^{n} ix_i \equiv a \mod (n+1)\}. \tag{3.3}$$

Code $C(n, a)$ is capable of correcting all single asymmetric errors. Moreover it was shown that $|C(n, 0)| \geq |C(n, a)|$ and

$$|C(n,0)| \geq \frac{2^n}{n+1}, \tag{3.4}$$

thus exceeding the Hamming upper bound for the size of binary single symmetric error correcting codes.
We study VT-type ℓ-UEC codes. Note, however, that unlike the VT-codes, the codes we introduce here are defined by means of some linear equation (rather than a congruence) over the real field. Namely given $Q = [0, q-1] \subset \mathbb{R}$ and $a_0, \ldots, a_{n-1}, a \in \mathbb{Z}$ let

$$X = \{(x_0, \ldots, x_{n-1}) \in Q^n : \sum_{i=0}^{n-1} a_i x_i = a\}. \tag{3.5}$$

Note that X defines an ℓ-UEC code iff for each distinct $\mathbf{x}, \mathbf{y} \in X$ holds $\mathbf{x} - \mathbf{y} \notin [-\ell, \ell]^n$ and $\mathbf{x} - \mathbf{y} \notin [0, 2\ell]^n$.
Thus an obvious sufficient condition for the set of vectors $X \subset Q^n$ to be an ℓ-UEC code is that the hyperplane H defined by

$$H = \left\{(x_0, \ldots, x_{n-1}) \in \mathbb{R}^n : \sum_{i=0}^{n-1} a_i x_i = 0\right\}$$

does not contain vectors from $[-\ell, \ell]^n \cup [0, 2\ell]^n$, except for the zero vector.

An ℓ-UEC code of VT type may have the advantage of a simple **Encoding and Decoding** procedure. In particular, let $\mathcal{C}$ be a code given by (3.5) where for $i = 0, 1, \ldots, n-1$, $a_i = (\ell+1)^i$. Suppose for the received vector $\mathbf{y} = (y_0, \ldots, y_{n-1})$ we have

$$\sum_{i=0}^{n-1} (\ell+1)^i y_i = a'$$

with $a' \geq a$. Then the transmitted vector $(x_0, \ldots, x_{n-1}) = (y_0 - e_0, \ldots, y_{n-1} - e_{n-1})$, where the error vector $(e_0, \ldots, e_{n-1})$ is just the $(\ell+1)$-ary representation of the number $a' - a$. Similarly, if

$a' \le a$, then $(x_0, \ldots, x_{n-1}) = (y_0 - e_0, \ldots, y_{n-1} - e_{n-1})$, where $(e_0, e_1, \ldots, e_{n-1})$ is the $(\ell+1)$-ary representation of $a - a'$.
For given ℓ, q and n, we define $LA_u(n,\ell)_q$ = the maximum size of an ℓ-UEC code, over the alphabet $[0, q-1]$, defined by a linear equation (3.5).
Correspondingly we use $LA_a(n,\ell)_q$ for ℓ-AEC codes.

Theorem 13 *(i) For all n, q and ℓ, $LA_a(n,\ell)_q = LA_u(n,\ell)_q$.*
(ii) For all integers q, n and ℓ satisfying $q > \ell + 1$ we have

$$\frac{\ell}{q-1}\left(\frac{q}{\ell+1}\right)^n \le LA_u(n,\ell)_q \le \lceil \frac{q}{\ell+1} \rceil^{n-1}.$$

Construction of optimal codes

We call a VT-type ℓ-UEC code VT-type optimal (or shortly optimal) if it attains the upper bound in Theorem 20.

Given integers $\ell \in [1, q-1],\ n,\ r$ we define

$$\mathcal{C}_n(r) = \left\{ (x_0, \ldots, x_{n-1}) \in Q^n : \sum_{i=0}^{n-1} (\ell+1)^i x_i = \alpha S_n + r \right\}, \tag{3.6}$$

$$\text{where } S_n := \sum_{i=0}^{n-1} (\ell+1)^i = \frac{(\ell+1)^n - 1}{\ell}, \text{ and } \alpha := \lfloor \frac{q-1}{2} \rfloor. \tag{3.7}$$

It can be seen that $\mathcal{C}_n(r)$ is an ℓ-UEC code for all n and r.

We use the notation $\langle x \rangle_y$ to denote the integer in $[0, y-1]$ that is equivalent to x modulo y.

Theorem 14 *Let $u_1, u_2, \ldots$ and $v_1, v_2, \ldots$ be sequences of integers such that:*
(i) $0 \le u_1 + \alpha \le v_1 + \alpha \le q - 1$,
and for each $n \ge 2$
(ii) $\lceil \frac{1}{\ell+1}(u_n + \alpha - (q-1)) \rceil \ge u_{n-1}$,
(iii) $\lfloor \frac{1}{\ell+1}(v_n + \alpha) \rfloor \le v_{n-1}$, and
(iv) $\ell + 1$ divides q, or for each $r \in [u_n, v_n]$, $\langle \alpha + r \rangle_{\ell+1} < \langle q \rangle_{\ell+1}$.
Then for each $n \ge 1$ and $r \in [u_n, v_n]$ we have $|\mathcal{C}_n(r)| = \lceil \frac{q}{\ell+1} \rceil^{n-1}$.

Theorem 15 *Let ℓ and q be such that $\ell + 1$ divides q. Let $u_1 = -\alpha$, $v_1 = \alpha$, and for $n \ge 2$, $u_n = (\ell+1)u_{n-1} + \alpha$ and $v_n = (\ell+1)v_{n-1} - \alpha$. In other words, for $n \ge 1, v_n = -u_n = \frac{\alpha}{\ell}\left[(\ell-1)(\ell+1)^{n-1} + 1\right]$.*
Then for each $n \ge 1$ and $r \in [u_n, v_n]$, we have

$$|\mathcal{C}_n(r)| = LA_u(n,\ell)_q = \left(\frac{q}{\ell+1}\right)^{n-1}.$$

Theorem 16 *Let $q = (b-1)(\ell+1)+d$, where the integers b, d and ℓ are such that $1 \le b-1 < d \le \ell$. Then for each n*

$$LA_u(n,\ell)_q = \left\lceil \frac{q}{\ell+1} \right\rceil^{n-1}.$$

Open problems

Give constructions for asymmetric/unidirectional codes, capable of correcting/detecting t errors of a given magnitude, with efficient coding and decoding schemes.
For practical application of those codes [21] (e.g. in multi-level flash memories), it is important to have efficient constructions of systematic codes (that is codes having systematic encoders), that are advantageous in high-speed memory architecture.
Give constructions of AEC/UEC-codes of a limited magnitude, correcting bursts of errors.

4 Parallel error–control codes

In [11] Ahlswede, Balkenhol and Cai introduced a new code concept for multiple-access channels (MAC) with a special error control mechanism. A communication channel consists of several sub–channels transmitting simultaneously and synchronously. The senders encode their messages into codewords of the same length over the same alphabet and transmit them in parallel. When an error occurs in a line at time T with a relatively high probability, an error also occurs in its neighbor lines. A parallel t-error correcting code is a code capable of correcting all t or less errors of this type. A parallel code is called independent, if the encoders proceed independently, that is, the code in this case is the Cartesian product of the codes used by the senders. As an example consider a parallel port of a computer device, where the message from the computer to the device is transmitted in parallel over a set of lines. A magnetic influence from outside produces errors during the transmission. However, the time instances when errors occur in the different lines are related. Thus we have a model for a coding problem for a MAC.
The model of parallel error correcting codes described above can be useful for the design of network error correcting codes in real networks. For instance, if we model a large link as several parallel links, an error of a link may cause the error for all associated links.
For blocklength n, messages are encoded by q-ary $r \times n$ matrices. In the channel considered in [11] the errors are of the additive type. To each row-vector in a code matrix M the same error vector e is added, that is, the $r \times n$ matrix E, called error matrix, with identical row vectors e is added.
In [9] we introduce a new model of a one-way channel, which is again based on parallel subchannels and again has the same error vectors, however, the errors are produced by the binary Z-channels (Boolean sums) now. We therefore call it *Parallel Error Z-channel* (PEZ-channel).
Recall that the binary Z-channel, has the property that only $0 \to 1$ (or $1 \to 0$) type of errors can occur during the transmission. This type of errors are called asymmetric. Here we consider errors of type $0 \to 1$.
In case errors are not correlated, but are produced letterwise again by Z-channels, we speak about the *Parallel Z-channel* (PZ-channel). We study it under the constraint: all letterwise errors occur in at most t columns.
A code $\mathcal{C}$, called $(r \times n)$-code, is a set of $r \times n$ $(0,1)$–matrices. We say that t parallel asymmetric errors have occurred in a sent matrix M, also called *code matrix*, if in some t columns of M all zero entries turn into ones. The received word M' can be written as $M' = M \oplus E$, where the *error matrix* E is an $r \times n$ matrix with each column consisting of all ones or all zeros and $\oplus$ means the Boolean sum of $(0,1)$-matrices. The weight $w(E)$ is defined as the number of nonzero columns in E.
We say that an $(r \times n)$–code $\mathcal{C}$ is capable of correcting t (parallel asymmetric) errors if any transmitted code matrix can be uniquely reconstructed at the receiving end in the presence of t or less errors. In other words, for every two codematrices M_1, M_2 and error matrices E_1, E_2 of weight not greater than t we have

$$M_1 \oplus E_1 \neq M_2 \oplus E_2. \tag{4.1}$$

We also say that $\mathcal{C}$ is capable of detecting t errors if

$$M_1 \oplus E \neq M_2 \tag{4.2}$$

holds for all E with $w(E) \leq t$. Such a code is called *t–parallel asymmetric error correcting/detecting code* (shortly $(r \times n, t)$ *PEZ-code*).
Similarly we define error correcting/detecting codes for the PZ-channel. The $0 \to 1$ errors can occur now in at most t columns. That is, an error E now is an $r \times n$ matrix of weight $w(E) \leq t$ (the weight of E is defined as above). Codes capable of correcting/detecting such type of errors are called here $(r \times n, t)$ *PZ-codes*. More precisely, a t error correcting (resp. detecting) $(r \times n)$ PZ-code is a code that satisfies the condition (3.1) (resp. condition (3.2)).

Construction of error correcting/detecting codes for PEZ-channel

For an $r \times n$ $(0,1)$-matrix M the columns of M can be viewed as elements of the alphabet $Q = \{0, 1, \ldots, q-1\}$ $(q = 2^r)$ using an arbitrary one-to-one mapping $\varphi : \{0,1\}^r \to Q$. Thus any matrix

M can be represented as an n-tuple $(a_1, \ldots, a_n) \in Q^n$. A natural way is to consider each column as the binary expansion of the corresponding number from Q. Our PEZ-channel can be illustrated now as a q-ary channel (with $q = 2^r$) called here q-ary Z-channel (shortly Z_q-channel) shown in Figure 1. In case $q = 2$ this is simply the Z-channel.

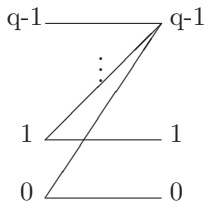


Figure 1: q-ary Z-channel

Thus, the PEZ-channel is a special case of the Z_q-channel when $q = 2^r$. Therefore, in general it makes sense to study this channel for arbitrary q. The notion of t-error correcting/detecting codes is extended to any Z_q-channel in a natural way. Such codes are called here Z_q-code capable of correcting/detecting t errors.

Optimal error-detecting codes. Recall the notion of $S(n, q-1)$ introduced in Section 1 and let $W_i := |S_i(n, q-1)| = \binom{n}{i}(q-1)^{n-i}$, $i = 0, 1, \ldots, n$. $A \subset S(n, q-1)$ is called an antichain if any two distinct members of A are incomparable.

Lemma 3 *Let $A \subset S(n, q)$. Then the following two conditions are equivalent.*
(i) A is a Z_q-code capable of detecting t errors.
(ii) If $a^n, b^n \in A$ are two codewords such that $a^n \succ b^n$ then $w(a^n) - w(b^n) \geq t + 1$.

Note, in particular, that $A \subset S(n, q-1)$ is a Z_q-code capable of detecting all errors iff A is an antichain.

Theorem 17 *Given integers $n, a \geq 1$, and $1 \leq t < n$ we have*
(i) For arbitrary $a \in [0, t]$ the code $\mathcal{C}_a$ defined by

$$\mathcal{C}_a = \{x \in S_i(n, q-1) : i \equiv a \mod (t+1)\} \tag{4.3}$$

is a Z_q-code capable of detecting t errors.
(ii) The code C_{a^*} with $|\mathcal{C}_{a^*}| = \max\{|\mathcal{C}_a| : a \in [0, t]\}$ is an optimal t error detecting code.

Note that

$$|\mathcal{C}_{a^*}| = \max_{a \in [0,t]} \sum_{i \geq 0} W_{a+i(t+1)} > \frac{q^n}{t+1}. \tag{4.4}$$

In particular, for $W_k := \max\{W_i : 0 \leq i \leq n\}$ the theorem says that $S_k(n, q-1)$ is an optimal Z_q-code capable of detecting all errors. Next we consider
Error–correcting Z_q-codes. We define first *asymmetric distance* d_A between elements of Q^n. To this end we define two distances d_0 and d_1 between $a^n, b^n \in Q^n$:
$d_1(a^n, b^n) := \#\{i : a_i \neq b_i \text{ and } a_i, b_i \neq q-1\}$, $d_0(a^n, b^n) := \max\{\delta(a^n, b^n), \delta(b^n, a^n)\}$, where
$\delta(a^n, b^n) := \#\{i : a_i \neq b_i \text{ and } a_i = q-1\}$ and $\delta(b^n, a^n) := \#\{j : a_j \neq b_j \text{ and } b_j = q-1\}$.

Definition 3 *For $a^n, b^n \in Q^n$ the distance $d_A(a^n, b^n)$ is defined by*

$$d_A(a^n, b^n) = d_0(a^n, b^n) + d_1(a^n, b^n). \tag{4.5}$$

We can describe now error correcting capabilities of a Z_q-code via asymmetric distance d_A.

Proposition 7 *A Z_q-code $\mathcal{C} \subset Q^n$ is capable of correcting t errors iff for every distinct $a^n, b^n \in \mathcal{C}$ holds*

$$d_A(a^n, b^n) \geq t + 1.$$

Note that for $q = 2$ we have $d_A = d_0$, and codes with minimum distance $d_A = t + 1$ are simply binary codes capable of correcting t asymmetric errors.
Clearly any code capable of correcting t symmetric errors is a t error correcting Z_q-code. It is also clear that for vectors $a^n, b^n \in Q^n$ the Hamming distance $d_H(a^n, b^n) \geq d_A(a^n, b^n)$. Thus, a t error correcting Z_q-code is capable of detecting t or less symmetric errors. Therefore, an upper bound for a code with the minimum distance $d_H = t + 1$ is a trivial upper bound for a t error correcting Z_q-code.
Let us, in particular, consider the case when $n \leq q+1$ and let $\mathcal{C}$ be a Z_q-code correcting t errors. The minimum Hamming distance of this code $d_H(\mathcal{C}) \geq t + 1$ and the Singleton bound $|\mathcal{C}| \leq q^{n-t}$ (see [36]) is a trivial upper bound for $\mathcal{C}$. Note also that in case of prime power q we can use MDS codes (codes attaining the Singleton bound, see [36], Ch.11), with the minimum distance $d_H = 2t + 1$ and size q^{n-2t}, as t error correcting Z_q-codes. However one can do better.
Consider in particular single-error correcting Z_q-codes. Then an MDS code with the minimum distance $d_H = 3$ has cardinality q^{n-2}. On the other hand the following parity check code has a greater size.

Proposition 8 *Given q the code $\mathcal{C} \subset Q^n$ defined by*

$$\mathcal{C} = \{(x_1, \ldots, x_n) \in S_0(n, q) : \sum_{i=1}^{n} x_i \equiv a \mod q - 1\} \tag{4.6}$$

is a single error correcting Z_q-code of cardinality $|\mathcal{C}| = (q-1)^{n-1}$.

One can extend the construction to t-error correcting Z_q-codes. In view of Proposition 7 it is sufficient to construct a code $\mathcal{C}$ of length n and minimum distance $d_H(\mathcal{C}) = t + 1$ over alphabet $Q^* := [0, q-2]$.

Proposition 9 *For $n \leq q + 1$ one can construct a Z_q-code $\mathcal{C}$ of length n capable of correcting $1 \leq t < n$ errors, with*

$$|\mathcal{C}| \geq \frac{(q-1)^n}{q^t}$$

Note that $|\mathcal{C}|$ is greater than q^{n-2t}, the size of a corresponding MDS code correcting t symmetric errors.

Remark The described codes can be viewed as codes correcting *erasures* with the erasure symbol $q - 1$. The *erasure channel*, in which each alphabet symbol is lost with a fixed probability (that is, turned into an erasure symbol "$*$"), was introduced by P. Elias [23]. Erasure correcting codes (Fountain codes, Lt codes etc) are widely used for reliable networks (see e.g. [52]), and recently in Network Coding problems.
Formally, a t error correcting Z_q- code can be viewed as a *code, capable of correcting t erasures, in which the erasure symbol is also used for the transmission.*
Thus, erasure correcting codes can be used as Z_q-codes. Note however that the size of a t–error correcting Z_q-code can be much larger than the size of a corresponding optimal erasure code over an alphabet of size $q-1$. To show that, we describe a more general construction of t–error correcting Z_q-codes.

Construction: Let C be a binary code of length capable of correcting t asymmetric errors. Let also $\mathcal{D} = \{D_m\}$; $m = 1, \ldots, n$ be a set of codes of length m capable of detecting t symmetric errors (i.e. a code with minimum Hamming distance $t + 1$) over the alphabet Q^*. Note that some of D_m could be trivial codes containing only one codeword (by convention the minimum distance in a trivial code is ∞). Given a codeword $v^n \in C$ of Hamming weight $wt_H(v^n) = r$ let $\{i_1, \ldots, i_r\}$ be nonzero coordinates of v^n and let $\{j_1, \ldots, j_{n-r}\} = [1, n] \setminus \{i_1, \ldots, i_r\}$ where $j_1 < \ldots < j_{n-r}$. Define then
$D(v^n) = \{(x_1, \ldots, x_n) \in Q^n : x_{i_1} = \ldots = x_{i_r} = q - 1$ and $(x_{j_1}, \ldots, x_{j_{n-r}}) \in D_{n-r}\}$.
Define now the code $\mathcal{C} = C \circ \mathcal{D}$ where

$$C \circ \mathcal{D} := \bigcup_{v^n \in \mathcal{C}} D(v^n). \tag{4.7}$$

Proposition 10 *Given integers $1 \le t \le n$ and $q > 2$ the code $\mathcal{C} = C \circ \mathcal{D}$ is a t error correcting Z_q- code of length n over alphabet $Q = [0, q-1]$.*

Notice that given n and q, the size of an optimal Z_q-code $C \circ \mathcal{D}$ capable of correcting t errors is greater than the size of an optimal code $\mathcal{C}'$ of length n, over an alphabet (say Q^*) of size $q-1$, capable of correcting t erasures. Indeed, let C (the code in our construction) contain the all zero vector 0^n. Then clearly $\mathcal{C}' \subset C \circ \mathcal{D}$.
Next we apply the described approach for construction of single error correcting Z_q-codes for arbitrary n and q.
We use Varshamov-Tennengolts codes (VT codes) for construction of q–ary single–error correcting Z_q-codes.
Given integers $n \ge 1$ and $q > 2$ $(Q = [0, q-1],\ Q^* = [0, q-2])$ let $C(n, a)$ be a VT code.
For $m = 1, \ldots, n$ and $\alpha \in Q^*$ we define now $\mathcal{D} = \{D_1(\alpha), \ldots, D_n(\alpha)\}$ with

$$D_m(\alpha) := \{x^m \in Q^{*m} : \sum_{i=1}^{m} x_i \equiv \alpha \mod q-1\}. \tag{4.8}$$

Each code $D_m(\alpha)$ has size $|D_m(\alpha)| = (q-1)^{m-1}$ and minimum Hamming distance 2 ($m \in [1, n]$, $\alpha \in [0, q-2]$). In view of Proposition 7 the code

$$\mathcal{C}(n, a, \alpha) := C(n, a) \circ \mathcal{D}$$

is a single-error correcting Z_q-code.
Let $A_0(n, a), A_1(n, a), \ldots, A_n(n, a)$ be the weight distribution of $C(n, a)$, that is $A_i(n, a) := \#$ {codewords of Hamming weight i}.
Then it can be easily seen that $|\mathcal{C}(n, a, \alpha)| = \sum_{i=0}^{n-1} A_i(n, a) \cdot (q-1)^{n-i-1} + A_n(n, a)$. Since $|\mathcal{C}(n, a, \alpha)| = |\mathcal{C}(n, a, 0)|$ we simplify the notation denoting $\mathcal{C}(n, a) = \mathcal{C}(n, a, 0)$. Thus we have proved the following

Theorem 18 *For integers $0 \le a \le n$ and $q \ge 3$ the code $\mathcal{C}(n, a)$ is a q–ary single–error correcting Z_q-code with*

$$|\mathcal{C}(n, a)| = \sum_{i=0}^{n-1} A_i(n, a) \cdot (q-1)^{n-i-1} + A_n(n, a). \tag{4.9}$$

Example. $n = 8,\ q = 4\ (r = 2), a = 0$.
Let A_i denote the number of codewords of weight i in the VT code $C(8, 0)$. We have $A_0 = A_8 = 1$, $A_1 = A_7 = 0$, $A_2 = A_6 = 4$, $A_3 = A_5 = 6$, $A_4 = 8$.
Our construction gives us a single–error correcting $(2 \times 8, 1)$ Z_q-code $\mathcal{C}(8, 0)$ with
$|\mathcal{C}(8, 0)| = A_0 \cdot 3^7 + A_2 \cdot 3^5 + A_3 \cdot 3^4 + A_4 \cdot 3^3 + A_5 \cdot 3^2 + A_6 \cdot 3 + A_8 = 3^7 + 4 \cdot 3^5 + 6 \cdot 3^4 + 8 \cdot 3^3 + 6 \cdot 3^2 + 4 \cdot 3 + 1 = 3928$.
Note that the size of a single symmetric error correcting code of length 8 (over an alphabet of size 4) is upper bounded (Hamming bound) by $\lfloor 2^{16}/(3 \cdot 8 + 1) \rfloor = 2621$.
Next we give an upper bound for a single–error correcting Z_q–code

Theorem 19 *Let $\mathcal{C}(n)_q$ be a single–error correcting Z_q-code of length n. Then*

$$|\mathcal{C}(n)_q| < \sum_{k=0}^{n-1} \frac{\binom{n}{k}(q-1)^{n-k-1}}{k+1}. \tag{4.10}$$

Codes for PZ-channels

Let $\mathcal{M}(r \times n)$ be the set of all $r \times n$ $(0,1)$–matrices. Recall that $\mathcal{C} \subset \mathcal{M}(r \times n)$ is a t-error correcting/detecting PZ-code if $\mathcal{C}$ is capable of correcting/detecting all asymmetric errors in t or less columns. We call such codes for short $(r \times n, t)$–codes.
Note that any t-error correcting/detecting PZ-code $\mathcal{C} \subset \mathcal{M}(r \times n)$ is also a t–error correcting/detecting PEZ code.
We discuss first the error detection problem.
For $A \in \mathcal{M}(r \times n)$ the Hamming weight $w_H(A)$ is the number of nonzero entries in A.

Theorem 20 *Given integers* $1 \leq t \leq n$, $1 \leq r$

$$\mathcal{A} := \left\{A \in \mathcal{M}(r \times n) : wt_H(A) \equiv \lfloor \frac{rn}{2} \rfloor \bmod (tr+1)\right\} \tag{4.11}$$

is a t*-error detecting* PZ*-code.*

Code $\mathcal{A}$ defined in (3.13) is optimal for $r = 1$, however, this is not the case in general.

Theorem 21 *Given integers* $1 < r$ *and* $1 \leq t < n$, *let* $\mathcal{A}(r \times n, t)$ *be an optimal* t*-error detecting* PZ *code. Then*

$$\frac{2^{rn}}{tr+1} \leq |\mathcal{A}(r \times n, t)| \leq \frac{2^{rn}}{\sqrt{tr}}. \tag{4.12}$$

The lower bound in (3.14) follows from the code construction in Theorem 13.
We consider now the error correction problem for the simplest case $t = 1$.
Every matrix $M \subset \mathcal{M}(r \times n)$, with columns $\bar{b}_1, \ldots, \bar{b}_n$, is associated with the sequence $(b_1, \ldots, b_n)$ where $\bar{b}_i$ $(i = 1, \ldots, n)$ is the binary representation of b_i. For a subset $\mathcal{S} \subset Q^n$, $Q := [0, 2^r - 1]$ we denote by $\mathcal{S}(r \times n) \subset \mathcal{M}$ the set of matrices corresponding to the elements of $\mathcal{S}$.
We say that there exists a k–factorization of $\mathbb{Z}_m^*$ ($\mathbb{Z}_m^* := \mathbb{Z}_m \setminus \{0\}$) if there exists a subset $A \subset \mathbb{Z}_m^*$ such that each element of $\mathbb{Z}_m^*$ can be uniquely represented as a product $i \cdot a$ where $i \in \{1, \ldots, k\}$ and $a \in A$.

Theorem 22 *Given integers* $n, r \geq 2$ *let* $m := n(2^r - 1) + 1$ *and let there exist a* $(2^r - 1)$*–factorization of* $\mathbb{Z}_m^*$ *by a subset* $A = \{a_1, \ldots, a_n\}$. *For* $a \in \mathbb{Z}_m$ *let* $\mathcal{B} \subset Q^n$ *be defined by*

$$\mathcal{B} = \{(x_1, \ldots, x_n) \in Q^n : \sum_{i=1}^{n} a_i x_i \equiv a \mod m\}. \tag{4.13}$$

Then $\mathcal{B}(r \times n)$ *is a single-error correcting* PZ*-code with*

$$|\mathcal{B}(r \times n)| \geq \frac{2^{rn}}{n(2^r - 1) + 1}. \tag{4.14}$$

Example Let $n = 12$, $r = 2$, and hence $n(2^r - 1) + 1 = 37$. One can check that there exists a 3–factorization of $\mathbb{Z}_{37}^*$ by the set $A = \{2, 9, 12, 15, 16, 17, 20, 21, 22, 25, 28, 35\}$. That is $\mathbb{Z}_{37}^* = A \cup 2A \cup 3A$ where $iA := \{ia \mod 37 : a \in A\}$, $i = 2, 3$. Therefore, the code $\mathcal{B}(2 \times 12)$ defined by (4.14) is a single-error correcting PZ-code with cardinality $|\mathcal{B}(2 \times 12)| \geq 4^{12}/37$ exceeding the Hamming bound for a quaternary single symmetric error correcting code of length 12.
We give now a construction of single-error correcting PZ-codes with a very simple decoding algorithm.
Code construction: For integers $1 < r \leq n$, let $\mathcal{E}(r \times n)$ denote the set of all $r \times n$ $(0,1)$-matrices with even row weights. Thus $|\mathcal{E}(r \times n)| = 2^{(n-1)r}$. For an $r \times n$ $(0,1)$-matrix M let $h_i(M)$ denote the Hamming weight of its i-th column. Let also p be the smallest prime such that $p \geq n + 1$. We define now the code $\mathcal{C}(r \times n)$ as follows.

$$\mathcal{C}(r \times n) = \{M \subset \mathcal{E}(r \times n) : \sum_{i=1}^{n} i \cdot h_i(M) \equiv a \mod p\}. \tag{4.15}$$

Theorem 23 *(i)* $\mathcal{C}(r \times n)$ *is capable of correcting all asymmetric errors in a single column.*
(ii) There exists $0 \leq a \leq p - 1$ *such that*

$$|\mathcal{C}(r \times n)| \geq \frac{2^{(n-1)r}}{p}. \tag{4.16}$$

Decoding algorithm

For a received word $M' \in \mathcal{M}(r \times n)$
1. Determine the column vector

$(\varepsilon_1, \ldots, \varepsilon_r)^T := M' \cdot (1, \ldots, 1)^T \mod 2$.
2. Compute $t := w_H(\varepsilon_1, \ldots, \varepsilon_r)$.
If $t = 0$ then M' is a code matrix, otherwise
3. Compute $b := \sum_{i=1}^{n} i \cdot h_i(M') \mod p$.
4. Compute $k := \frac{b-a}{t} \mod p$.
5. Evaluate the error matrix $E \in \mathcal{M}(r \times n)$ with the k-th column $(\varepsilon_1, \ldots, \varepsilon_r)^T$ and with zero
entries elsewhere.
6. Determine the transmitted code matrix $M = M' - E$.

Open problems

A challenging combinatorial optimization problem is construction of optimal or near optimal t–error detecting codes for PZ–channels (even for $t = 1$).
Constructions of "good" t–error correcting codes (for both channels) with efficient decoding algorithms is another problem for further research
We considered only errors occurring in a restricted set of columns. Consider codes for correction/detection clusters of errors.

5 Interaction with other projects

There have been **intense connections to other projects** in the DFG Schwerpunktprogramm 1126 Algorithmik großer und komplexer Netzwerke, which were supported by several workshops.
We have explained this above in great detail for **Connectors in Communication Networks** (see related work [15]) for the Kiel research group, project: "Entwurf effizienter Architekturen und Algorithmen für Multicast-ATM-Netzwerke" Prof. Dr. Anand Srivastav, Prof. Dr. Klaus Jansen (Institut für Informatik, Christian-Albrechts-Universität zu Kiel).
In the poster you find connections for **Network Coding** to work of the project: "Algorithm Engineering für große Graphen und Speicherhierarchien" by P. Sanders and U. Meyer and for **Buffer Management** to work of the project: "Effiziente Algorithmen für die Ressourcenverwaltung in großen Netwerken", by S. Albers.

6 Further reports and research

The work not reported here concerns the subjects:

- Network coding,
- Identification entropy,
- Weighted constrained error-correction, and
- Buffer management strategies.

However, contributions to these subjects can be found in the books "General Theory of Information Transfer and Combinatorics" (Eds. R. Ahlswede et al.), Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 2006 and "Lectures on Advances in Combinatorics" (R. Ahlswede and V. Blinovsky), Universitext, Springer Verlag, 2008, the Special Issue "General Theory of Information Transfer and Combinatorics" (Eds. R. Ahlswede et al.) of Discrete Applied Mathematics, Vol. 156, No. 9, 2008, and in the 2006 Shannon Lecture " Towards a General Theory of Information Transfer" (R. Ahlswede), Shannon Lecture at ISIT in Seattle 13th July 2006, IEEE Inform. Theory Society Newsletter, Vol. 57, No. 3, 6-28, 2007.
Their investigation will be continued in the three DFG projects:

- Information Flows in Networks,
- General Theory of Information Transfer, and
- Advances in Search and Sorting.

More extensive reports are planed at the end of these projects.
Finally, Network Coding received attention in the article of Scientific American "Breaking Network Logjams", 78-85, June 2007 and its translation "Staufrei fahren auf der Datenautobahn" in the article of Spektrum der Wissenschaft, 88-95, March 2008.

References

1. R. Ahlswede and H. Aydinian, Sparse asymmetric connectors in communication networks, General Theory of Information Transfer and Combinatorics, Eds. R. Ahlswede et al., Lecture Notes in Comp. Sci., Vol. 4123, 1056-1062, Springer, 2006.
2. R. Ahlswede and H. Aydinian, Construction of asymmetric connectors of depth two, Special Issue in Honor of Jacobus H. van Lint of J. Combinatorial Theory, Series A, Vol. 113, No. 8, 1614-1620, 2006.
3. R. Ahlswede and H. Aydinian, Diagnosability of large multiprocessor systems, 2nd COMBSTRU workshop 2004, Venice, 20-22 Sept., 2004.
4. R. Ahlswede and H. Aydinian, On diagnosability of large multiprocessor networks. Electronic Notes in Discrete Mathematics 21, 101-104, 2005, to appear in Discrete Applied Math., 2008.
5. R. Ahlswede, H. Aydinian, and L.H. Khachatrian, Undirectional error control codes and related combinatorial problems, in Proceedings of Eight Intern. Workshop on Algebraic and Combinatorial Coding Theory,Tsarskoe Selo, Russia, 8–14 Sept., 6–9, 2002.
6. R. Ahlswede and H. Aydinian, On t/s- diagnosability of multiprocessor systems, Final conference: General Theory of Information Transfer and Combinatorics, Center of Interdisciplinary Research (ZIF), Bielefeld, 26-30 April, 2004.
7. R. Ahlswede and H. Aydinian, An extremal problem on graphs, in Proceedings of Workshop on graphs and combinatorial optimization, Lambrecht, Germany, 6-9 June, 2006.
8. R. Ahlswede, H. Aydinian, L.H. Khachatrian, and L.M.G.M. Tolhuizen, On q–ary codes correcting all unidirectional errors of a limited magnitude, in Proc. Ninth Intern. workshop on Algebraic and Combin. Coding Theory, 19–25 June, Kranevo, Bulgaria, 20–26, 2004, (full version: http://arxiv.org/pdf/cs.IT/0607132), to appear in a special issue dedicated to Varshamov.
9. R. Ahlswede and H. Aydinian, Error correcting codes for parallel asymmetric channels, in Proceedings of International Symposium on Information Theory ISIT2006, Seattle, 6-12 July, 2006.
10. R. Ahlswede and H. Aydinian, Error control codes for parallel asymmetric channels, IEEE Trans. Inform. Theory, Vol. 54, No. 2, 831-836, 2008.
11. R. Ahlswede, B. Balkenhol, and N. Cai, Parallel error correcting codes, IEEE Trans. Inform. Theory, Vol. 48, No. 4, 959-962, 2002.
12. R. Ahlswede, N. Cai, S.Y.R. Li, and R.W. Yeung, Network information flow, IEEE Trans. Inform. Theory, Vol. 46, No. 4, 1204-1216, 2000.
13. R. Ahlswede and K.U. Koschnick, Note on an extremal problem arising for unreliable networks in parallel computing, Discrete Math. Vol. 47, 137-152, 1983.
14. S. Albers and M. Schmidt, On the performance of greedy algorithms in packet buffering, in 36th ACM Symposium on Theory of Computing (STOC'04), 35-44, 2004.
15. A. Baltz, G. Jäger, and A. Srivastav, Constructions of sparse asymmetric connectors with number theoretic methods, Networks, Vol. 45, No. 3, 1-6, 2005.
16. M. Barborak, M. Malek, and A. Dahbura, The consensus problem in fault-tolerant computing, ACM Computing Surveys, Vol. 25, No. 2, 171-220, 1993.
17. V.E. Beneš, Optimal rearrangeable multistage connecting networks, Bell System Tech. J. Vol. 43, 1641–1656, 1964.
18. M. Blaum (ed.), Codes for Detecting and Correcting Unidirectional Errors, IEEE Computer Society Press Reprint Collections, IEEE Computer Society Press, Los Alamitos, CA, 1993.
19. B. Bollobas, Extremal Graph Theory, Academic Press, London, 1978.
20. A. Caruso, S. Chessa, P. Maestrini, and P. Santi, Diagnosability of regular systems, J. Algorithms 45, 126-143, 2002.
21. Y. Cassuto, M. Schwartz, V. Bohossian, and J. Bruck, Codes for multilevel flash memories: correcting asymmetric limited magnitude errors, International Symposium on Information theory ISIT2007, Nice, France, June 24- 29, 1176-1180, 2007.
22. C. Clos, A study of non–blocking switching networks, Bell System Tech. J. Vol. 32, 406–424, 1953.
23. P. Elias, The noisy channel coding theorem for erasure channels, Amer. Math. Monthly Vol. 81, 853-862, 1974.
24. K. Engel, Sperner Theory, Cambridge University Press, 1997.
25. P. Feldman, J. Friedman, and N. Pippenger, Wide-sense nonblocking networks, SIAM J. Discr. Math. Vol.1, 158 -173, 1988.
26. A.D. Friedman, A new measure of digital system diagnosis, In Proc. Fifth Intern. Symp. Fault Tolerant Computing, 167-170, 1975.
27. S. Jaggi, P. Sanders, P.A. Chou, M. Effros, S. Egner, K. Jain, and L. M. G. M. Tolhuizen, Polynomial time algorithms for multicast network code construction, IEEE Trans. Inform. Theory, Vol. 51, No. 6, 1973–1982, 2005.
28. L.H. Harper, Optimal numberings and isoperimetric problems on graphs, J. Combin. Theory 1, 385-395, 1966.

29. S. Hoory, N. Linial, and A. Wigderson, Expander graphs and their applications, Bulletin AMS Vol. 43, No.4, 435-561, 2006.
30. F.K. Hwang and G.W. Richards, A two–stage rearrangeable broadcast switching network, IEEE Trans. on Communications, Vol. 33, 1025–1035, 1985.
31. A. Kavianpour and K.H. Kim, Diagnosabilities of hypercubes under the pessimistic one-step diagnosis strategy, IEEE Trans. Comput., Vol.40, No. 2, 233-237, 1991.
32. S. Khanna and W.K. Fuchs, A graph partitioning approach to sequantial diagnosis, IEEE Trans. Comput., Vol. 46, No. 1, 39-47, 1996.
33. T. Kløve, Error correcting codes for the asymmetric channel, Report, Dept. of Math. Univ. of Bergen, 1981 (with updated bibliography in 1995).
34. K. Leeb, Salami- Taktik beim Quader-Packen, Arbeitsberichte des Instituts für Mathematische Maschinen und Datenverarbeitung, Universität Erlangen 11(5), 1-15, 1978.
35. S.-Y. Li, R.W. Yeung, and N. Cai, Linear network coding, IEEE Trans. Inf. Theory, Vol. 49, No. 2, 371-381, 2003.
36. F.J. MacWilliams and N.J. Sloane, The Theory of Error-Correcting Codes, New York: North-Holland, 1988.
37. A.Y. Oruc, A study of permutation networks: some generalizations and tradeoffs, J. of Parallel and Distributed Computing, Vol. 22, 359–366, 1994.
38. N. Pippenger, Communication Networks, Handbook of Theoretical Computer Science, Elsevier, Amsterdam, 1990.
39. N. Pippenger and A.C. Yao, On rearangeable networks with limited depth, SIAM J. Algebraic Discrete Methods, Vol. 3, 411–417, 1982.
40. N. Pippenger, On rearangeable and nonblocking switching networks, J. Comput. System Sci., Vol. 17, 145–162, 1987.
41. N. Pippenger, Sorting and selecting in rounds, SIAM J. Comput. Vol. 16, 1032-1038, 1987.
42. F.P. Preparata, G. Metze, and R.T. Chien, On the connection assignment problem of diagnosable systems, IEEE Trans. Comput., Vol. 16 (12), 848-854, 1967.
43. P. Sanders, S. Egner, and L. Tolhuizen, Polynomial time algorithms for network information flow, in 15th ACM Symposium on Parallel Algorithms and Architectures, 286-294, 2003.
44. C.E. Shannon, Memory requirements in a telephone exchange, Bell System Tech. J. 29, 343–349, 1950.
45. D. Slepian, Two theorems on a particular crossbar switching network, unpublished manuscript, 1952.
46. V. Raghavan and A. Tripathi, Sequential diagnosability is co-NP complete, IEEE Trans. Comput., Vol. 40 (5), 584-595, 1991.
47. S. Riis and R. Ahlswede, Problems in Network coding and error correcting codes, NETCOD 2005 (The First Workshop on Network Coding Theory and Applications), Trento Italy, April 7, 2005, General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 861-897, 2006.
48. P. Santi and S. Chessa, Reducing the number of sequential diagnosis iterations in hypercubes, IEEE Trans. Comput., Vol. 53, 89-92, 2004.
49. R.R. Varshamov and G.M. Tennengolts, A code which corrects single asymmetric errors (in Russian) Avtomat. Telemeh. 26, 282–292, 1965. (transl: Automat. and Remote Contr. 26, 286–290, 1965).
50. R.R. Varshamov, On the theory of assymmetric codes (in Russian), Doklady Akademii Nauk USSR, Vol. 164, 757–760, 1965. (transl: Soviet Physics-Doklady 10, 185–187, 1965).
51. B. Wicker and V.K. Bhargava (Eds), Reed-Solomon Codes and their Applications, IEEE PRESS, NY, 1994.
52. S.B. Wickler and S. Kim, Fundamentals of Codes, Graphs, and Iterative Decoding, Kluwer Academic Publ., Norwell, MA, 2003.
53. A. Wigderson, D. Zuckerman, Expanders that beat the eigenvalue bound: explicit construction and applications, Combinatorica 19 (1), 125-138, 1999.
54. T. Yamada, T. Otsuka, A. Watanabe, and S. Ueno, On sequential diagnosis of multiprocessor systems, Discrete Appl. Math., Vol. 146, No. 3, 311-342, 2005.