Discrete Mathematics 47 (1983) 137–152
North-Holland

NOTE ON AN EXTREMAL PROBLEM ARISING FOR UNRELIABLE NETWORKS IN PARALLEL COMPUTING

R. AHLSWEDE and K.U. KOSCHNICK

Fakultät für Mathematik, Universität Bielefeld, Universitätsstraße, Postfach 8640, 4800 Bielefeld, Fed. Rep. Germany

Received 12 October 1982

Motivated by a certain model of parallel computing in unreliable networks we study combinatorial problems of the following type: For any graph and any integer c, what is the least number d such that removal of *any* d edges (or vertices) leaves a graph with a largest connected component of more than c vertices. We give rather precise estimates for the n-cube.

1. Introduction

Consider L processes operating asynchronously in parallel. The program of each process contains a specified area of code called critical section, which requires for its correct execution that no other processes are simultaneously in their critical section. Such a code might manipulate a common resource (e.g. line printer, tape drive), in which case access to the critical section corresponds to allocation of the resource. So the problem is to control access to the critical section in such a way, that the following basic requirement is satisfied:

(C1) *Mutual exclusion.* No two processes may be in their critical section at the same time.

In order to provide mutual exclusion at all, there must be the possibility of interprocess communication. In 1965 Dijkstra [1] proposed and solved the critical section problem for the case that the communication mechanism is a shared memory with elementary read and write operations. This solution satisfies (C1) and has the obviously desirable property:

(C2) *No deadlock.* It is not possible for all processes to become simultaneously blocked in such a fashion that none of them will be able to enter its critical sections.

Knuth [2] pointed out that Dijkstra's solution does not meet the following requirement:

(C3) *No lockout.* It is not possible for an individual process to be kept forever

from entering its critical section by some (perhaps highly improbable) sequence of actions by the other processes.

Knuth presented a solution which satisfies all of (C1)–(C3). Further improvements and new solutions were given by de Bruijn [3], Eisenberg and McGuire [4], Rabin [5] and in [6], [7].

All these solutions have the property that they employ a global variable. This has a serious drawback in a real multicomputer system: the failure of the memory unit containing the global variable will halt the entire system. Therefore Lamport [8] proposed a system in which each process contains a local communication variable. Each process may set only its own variable, but may read the communication variable of any other process. Lamport's solution was improved by Rivest and Pratt [9] and Peterson and Fischer [10].

In real multicomputer systems physical limitations are likely to imply that each computer can only be connected to a limited number of others. Then a failure of a few processes and connections may disconnect some computers from the rest of the system. In that case it is natural to replace condition (C3) by

(C3′) *Minimal lockout.* At any time the number of processes which are locked out from entering their critical section is minimal.

In other words, if certain processes and connections fail with the result that the rest of the system is disconnected, then it has to be guaranteed that the processes, which belong to the largest connected component, continue to compete for entering their critical section, while all other processes are locked out during this state. If every connected component of the system contains fewer than $\lfloor \frac{1}{2}L \rfloor + 1$ processes, then no process has the possibility to check whether the component it belongs to is maximal. In this case there exists no solution to the critical section problem, which satisfies the basic requirements (C1), (C2) and (C3′) simultaneously.

We ask how easy this case can occur for a multiprocessor system. Representing the network topology by a graph $G = (V, E)$, $|V| = L$, the question can be stated as follows:

How many arbitrary vertices and (or) edges can be removed from G such that the resulting graph has at least one connected component of size greater than $\lfloor \frac{1}{2}L \rfloor + 1$?

From a combinatorial point of view there is no reason to stick to the number $\lfloor \frac{1}{2}L \rfloor + 1$, and we therefore replace it by any number c. For graphs $G = (V, E)$ with a maximal connected component of size greater than c we are lead to the following extremal problems.

Problem 1. Denote by $\mu(G, c)$ the maximal number with the property that removal of any $m \leqslant \mu(G, c)$ *edges* results in a graph with a maximal component containing at least ($\geqslant$) c vertices. Derive estimates on $\mu(G, c)$.

Problem 2. Removing vertices instead of edges one can define analogously the function $\lambda(G, c)$ and try to obtain bounds for it.

Problem 3. More generally, denote by $P(G, c)$ the set of pairs (l, m) such that removal of any l vertices and any m edges leaves a connected component of size at least c. Characterize $P(G, c)$.

It is often more convenient to use the functions (defined for all G and all $c \in \{1, \ldots, |V|\}$ $\mu^*(G, c)$ (resp. $\lambda^*(G, c)$) = minimal number m (resp. l) with the property that there exist m edges (resp. l vertices) whose removal results in a graph with a maximal connected component of size smaller ($\leqslant$) than c.

Whenever μ or λ are defined, then

$$\mu^*(G, c) = \mu(G, c+1)+1, \qquad \lambda^*(G, c) = \lambda(G, c+1)+1. \tag{1.1}$$

Clearly, by (1.1) our estimates for μ (resp. λ) can be converted into estimates for μ^* (resp. λ^*), and vice versa. Thus we use whichever terminology seems more appropriate in a particular case.

The problems stated above are trivial in the following

Example 1. $G = K_L$, the complete graph with L vertices. Obviously, $\lambda(K_L, c) = L - c$. In order to determine $\mu^*(K_L, c)$ observe that one has to remove $\frac{1}{2}\sum_{i=1}^{I}(L - L_i)L_i$ edges, if the resulting connected components Z_i $(1 \leqslant i \leqslant I)$ shall have $L_1 \geqslant L_2 \geqslant \cdots \geqslant L_I$ vertices. Under the condition $L_i \leqslant c$ $(1 \leqslant i \leqslant I)$

$$\frac{1}{2}\sum_{i=1}^{I}(L - L_i)L_i = \frac{1}{2}\left(L^2 - \sum_{i=1}^{I} L_i^2\right).$$

is minimal exactly if

$$L_i = c \quad \text{for } 1 \leqslant i \leqslant t, \qquad L_{t+1} = c'$$

where $L = c \cdot t + c'$, $c' < c$. Therefore

$$\mu^*(K_L, c) = \tfrac{1}{2}(L^2 - c^2 \cdot t - c'^2).$$

Now also $P(K_L, c)$ can be determined, because the worst case arises, if we remove first vertices and then edges.

It seems hopeless to solve the problems above (even in an approximative sense) for arbitrary graphs, but the example shows that there is hope in special cases. The actual design of networks has to take into consideration constraints such as limitations of technical equipment, availability of tools, space etc. The study of special graphs is therefore also of interest. In subsequent sections we are concerned with the *n-dimensional cube*, which has been frequently suggested as network topology for computing problems. For a survey and bibliography see Siegel [11]. Two combinatorial results of Harper [12, 13], presented in Section 2, serve as basic tools in our analysis. Here we raise some questions and make some comments concerning general graphs.

1.) For which graphs can μ^* and/or λ^* be determined or can at least 'good' lower and upper bounds be derived?

2.) Denote by $G(L, M)$ the set of all graphs with L vertices and M edges. Which graphs in $G(L, M)$ are extremal in the sense that they have (a) maximal or (b) minimal μ^*(resp. λ^*) values?

For the model of parallel computing described above question (a) seems to be the most important one.

Given the number of vertices and edges, which graphs are least sensitive towards 'destruction'?

The answer will depend on the number of objects (edges or vertices) removed, as can be seen from the following simple

Example 2. $L=6$, $M=9$. See Fig. 1.

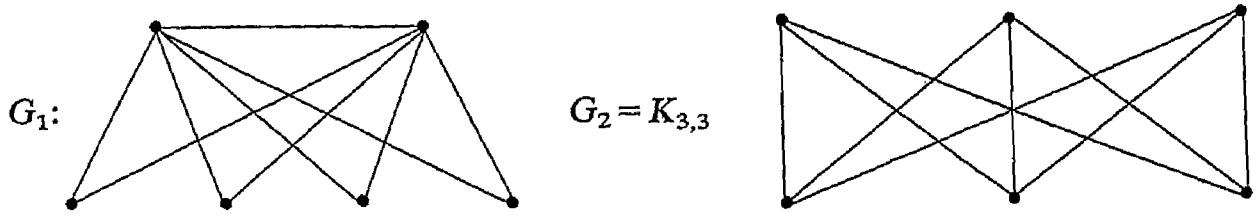

Fig. 1.

One readily verifies that $\mu^*(G, c)$ takes the values

c	1	2	3	4	5	6
G_1	9	7	5	4	2	0
G_2	9	6	5	4	3	0

Thus $\mu^*(G_1, 2) > \mu^*(G_2, 2)$, $\mu^*(G_1, 5) < \mu^*(G_2, 5)$.

It would be interesting to know whether one can exhibit a finite number of types of graphs (as for instance quasi-complete graphs, quasi-star graphs in the sense of [14], etc.) in which for all values of L, M and l (resp. m) extremal configurations can be found. Whereas this problem seems hard, the dual problem (b) is merely an exercise. We state the result therefore without proof as

Proposition 1. *Define*

$$\gamma(L, M) = \min_{G \in G(L, M)} \min\{c : \mu^*(G, c) = 0\},$$

that is the least size of the largest connected component for the graphs in $G(L, M)$. *Then*

$$(1)\quad \gamma(L, M) = \min\left\{k : 1 \leq k \leq L, \left\lfloor \frac{L}{k} \right\rfloor \binom{k}{2} + \binom{L \bmod k}{2} \geq M\right\}.$$

(2) $\mu(G, m) \geqslant \gamma(L, M-m)$ *for all* $G \in G(L, M)$.

(3) $\lambda(G, l) \geqslant \gamma\left(L-l, \max\left(M-\binom{l}{2}-l(M-l), 0\right)\right)$ *for all* $G \in G(L, M)$

(4) *For any* $G \in G(L, M)$ *removal of* l *points and* m *edges leads in the worst case to a largest connected component of size*

$$\max\left(L-l, \max\left(M-\binom{l}{2}-l(M-l)-m, 0\right)\right).$$

(*By convention* $\binom{t}{2}=0$ *for* $t<2$.)

3.) We can replace the $G(L, M)$ in 2.) by suitable subclasses such as the regular graphs $R(L, M)$ (if parameters permit). What are in this case the extremal configurations?

It is worth knowing that among the regular graphs the n-cubes do not always yield maximal μ^* values.

Example 3. The 4-cube C^4 has $L=16$ vertices and $M=32$ edges. Our Theorem 1, Section 3, implies that

$$\mu^*(C^4, 8)=8.$$

However, it has been checked by computer that for the graph G in Fig. 2 ($L=16$, $M=32$) $\mu^*(G, 8)=10$ holds.

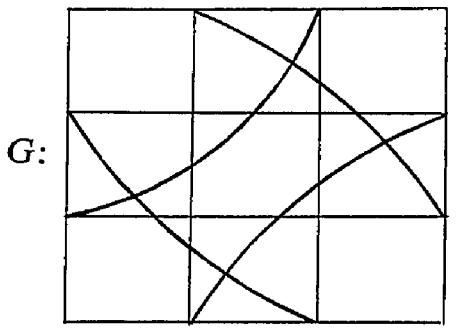

Fig. 2.

4.) Finally, we draw attention to the extensive literature [15–21] on network reliability problems in probabilistic settings. However, the present problem concerning the size of the largest connected component has to our knowledge not been considered. The combinatorics changes with changes of the probabilistic model and several problems arise.

Suppose for instance that edges are removed independently with the same probability. In our context it is of interest that the n-cube has asymptotically maximal probability for reliability (1 connected component) among all graphs with the same number of vertices and edges [30].

2. Harper's "isoperimetry" theorems

Let $H^n = \prod_1^n \{0, 1\}$ be the set of (0–1)-sequences of length n and let d denote the Hamming metric in H^n, that is, for any two elements $x^n = (x_1, \ldots, x_n)$, $y^n = (y_1, \ldots, y_n) \in H^n$

$$d(x^n, y^n) = |\{t : x_t \neq y_t, 1 \leq t \leq n\}|. \tag{2.1}$$

This is a very canonical metric for (0–1)-sequences and was used by Hamming for his investigation in the theory of error correcting codes. We therefore refer to (H^n, d) shortly as Hamming space. In this terminology the n-cube $C^n = (V_n, E_n)$ is a graph with vertex set $V_n \triangleq H_n$ and edge set $E_n \triangleq \{\{x^n, y^n\} : x^n, y^n \in H^n, d(x^n, y^n) = 1\}$. The following two configurations play a key role in several combinatorial extremal problems.

The quasi-sphere $S_{n,N}$

For any $n \in \mathbb{N}$ (the set of natural numbers) and any N, $1 \leq N < 2^n$, there is a unique representation

$$N = \binom{n}{n} + \cdots + \binom{n}{k+1} + \binom{a_k}{k} + \cdots + \binom{a_s}{s}$$

$$\text{for some } k,\ s-1 \leq k \leq n \quad \text{and} \quad n > a_k > a_{k-1} > \cdots > a_s \geq s \geq 1. \tag{2.2}$$

We denote by $S_{n,N}$ the set of all n-sequences with l zeros, $k+1 \leq l \leq n$ and $\binom{a_k}{k} + \cdots + \binom{a_s}{s}$ n-sequences with k zeroes chosen in lexicographical order.

The quasi-subcube $C_{n,N}$

Every N, $1 \leq N \leq 2^n$, can be (uniquely) written in the form

$$N = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_s} \tag{2.3}$$

where the exponents are nonnegative integers with $i_1 > i_2 > \cdots > i_s$.

Any set of 2^k vertices of the n-cube which agree in a specified set of $n-k$ coordinates will be called a k-subcube. A shadow of a k-subcube is a k-subcube obtained by complementing one of the $n-k$ fixed coordinates.

A quasi-subcube of C^n with N vertices is a subgraph, whose vertex set in the union of the vertex sets of subcubes of dimension i_j, $1 \leq j \leq s$, such that each subcube is contained in the shadow of every larger subcube.

In particular, if the components specified $z^{n-i_j} = (z_1, \ldots, z_{n-i_j})$, $j = 1, \ldots, s$, are always the first possible in lexicographical order, then we obtain the quasi-subcube $C_{n,N}$. We denote the i_j-subcube corresponding to z^{n-i_j} by $C(z^{n-i_j})$.

Motivated by certain coding problems Harper found the answer to two basic extremal problems, which for tutorial reasons we state in reversed historical order.

Minimal surface problem

For any set $A \subset H^n$ define

$$\Gamma^t A = \{x^n : x^n \in H^n, d(x^n, y^n) \leqslant t \text{ for some } y^n \in A\}. \tag{2.4}$$

$\Gamma^t A - A$ is called the t-surface of A.

Theorem I ([13]). *For all* $t = 1, 2, \ldots; 1 \leqslant N \leqslant 2^n$

$$\min_{A \subset H^n, |A| = N} |\Gamma^t A - A| = |\Gamma^t S_{n,N} - S_{n,N}|.$$

Furthermore, with the parameters of (2.2)

$$|\Gamma^t S_{n,N}| = \binom{n}{n} + \cdots + \binom{n}{k+1} + \cdots + \binom{n}{k-t+1} + \binom{a_k}{k-t} + \cdots + \binom{a_s}{s-t}.$$

Remark 1. In case $\binom{a_k}{k} + \cdots + \binom{a_s}{s-t} = 0$ the quasi-sphere $S_{n,N}$ is actually a sphere of Hamming radius $k+1$ and center $\mathbf{0} = (0, 0, \ldots, 0)$. H^n can be viewed as vector space over GF(2) and the metric d is invariant under translation by a vector. Therefore the above statement applies to spheres or quasi-spheres with any center. The special case $t = 1$ has a striking interpretation and simply means that given the cardinality ('volume') the sphere has minimal (cardinality of the) surface. This phenomenon is known as isoperimetric property for euclidean [22] and also non-euclidean geometries [23]. Since (H^n, d) is isomorphic to the family of subsets of an n-set endowed with the symmetric difference as distance function every result about (H^n, d) has directly a set theoretic interpretation.

Remark 2. Surface problems have been treated in a more general probabilistic setting by Margulis [21] and his asymptotic solution has been further extended by Ahlswede/Gács/Körner [24] to the so called 'blowing up technique' with far reaching consequences in Multi-user Information Theory. Theorem I was also used in [25] for the construction of good ciphers.

Minimal surfaces with multiplicities

The second problem is for 1-surfaces (and unsolved for $t > 1$). Define for $A, A' \subset H^n$

$$\Theta(A, A') = \{(x^n, y^n) : x^n \in A, y^n \in A', d(x^n, y^n) = 1\} \tag{2.5}$$

and in case $A' = A^c$

$$\Theta A = \Theta(A, A^c). \tag{2.6}$$

Theorem II ([12]). *For all* $n \in \mathbb{N}$ *and* $1 \leqslant N \leqslant 2^n$

$$\min_{A \subset H^n, |A| = N} |\Theta A| = |\Theta C_{n,N}|.$$

Remark 3. Harper's proof had a gap. Theorem II was first proved with a different approach by Lindsey [26], who solved right away the more general case $V_n \triangleq \{1, \ldots, a\}^n$. Bernstein [27] completed Harper's original argument. Theorem II has been rediscovered in [28] and by now several proofs exist. It is also a consequence of Theorem 4.2 of [29], where order ideals are maximized subject to certain weight assignments to the ranks.

3. Removing edges from the n-cube

We formulate and prove now our main result.

Theorem 1. *For all* $n \in \mathbb{N}$ *and* k, $0 \leqslant k \leqslant n-1$,

$$\mu^*(C^n, 2^k) = (n-k)2^{n-1}.$$

The key idea is to look at densities $|\Theta A|\,|A|^{-1}$, which we estimate from below.

Lemma 1. *For any* $A \subset H^n$ *with* $|A| \leqslant 2^k$, $0 \leqslant k \leqslant n-1$,

$$|\Theta A|\,|A|^{-1} \geqslant n-k.$$

Proof. By Theorem II and since $C_{n,|A|} \subset C(z^{n-k})$, $z^{n-k} = (1, 1, 1, \ldots, 1)$

$$|\Theta A| \geqslant |\Theta C_{n,|A|}| \geqslant (n-k)\,|A|. \qquad \square \tag{3.1}$$

Proof of Theorem 1. Obviously C^n can be decomposed into the 2^{n-k} k-subcubes $C(z^{n-k})$, $z^{n-k} \in \{0, 1\}^{n-k}$ by removing $\frac{1}{2}(n-k)2^k 2^{n-k} = (n-k)2^{n-1}$ edges. Since a k-subcube has 2^k vertices, this shows that $\mu^*(C^n, 2^k) \leqslant (n-k)2^{n-1}$.

The reverse inequality is now also readily established. Suppose that removal of m edges from C^n leaves us with connected components $Z_1, \ldots, Z_I$, all with not more than 2^k vertices. Then

$$\begin{aligned} m &\geqslant \frac{1}{2}\sum_{i=1}^{I} |\Theta Z_i| = \frac{1}{2}\sum_{i=1}^{I} \frac{|\Theta Z_i|}{|Z_i|}\,|Z_i| \\ &\geqslant \frac{1}{2}(n-k)\sum_{i=1}^{I} |Z_i| = (n-k)2^{n-1}, \end{aligned} \tag{3.2}$$

where the second inequality follows from Lemma 1.

Remark 4. The guiding idea of the proof is the notion of 'density' $|\Theta A|\,|A|^{-1}$ = average number of edges connecting a vertex from A with A^C. Notice that

$|\Theta C_{n,N}|\, N^{-1}$ is *not* monotonically decreasing in N. However, since $|\Theta C_{n,2^k}|\, 2^{-k} = n-k$, Lemma 1 implies that

$$|\Theta C_{n,N}|\, N^{-1} \geqslant |\Theta C_{n,2^k}|\, 2^{-k} \quad \text{for all } k = 1, 2, \ldots, n \text{ and all } N \leqslant 2^k. \tag{3.3}$$

This fact and Theorem II are the reasons for Theorem 1 to hold.

Remark 5. Theorem 1 determines $\mu^*(C^n, c)$ for all c of the form $c = 2^k$, which should be sufficient for all practical purposes, because for any c, $2^k \leqslant c \leqslant 2^{k+1}$,

$$(n-k)2^{n-1} = \mu^*(C^n, 2^k) \geqslant \mu^*(C^n, c) \geqslant \mu^*(C^n, 2^{k+1}) = (n-k-1)2^{n-1}$$

and then $\mu^*(C^n, c)$ is known within 2^{n-1} deviation.

A theoretically challenging problem is to find a reasonably simple formula for all values of c, but this appears to be quite tedious. However, by a more precise evaluation we can improve Lemma 1 and thus obtain an extension of Theorem 1 to all c with $2^k \leqslant c < \frac{4}{3}2^k$ for some k, $0 \leqslant k \leqslant n-1$.

A more general result

Lemma 2. *For any* $A \subset H^n$ *with* $|A| \leqslant \frac{4}{3}2^k$, $0 \leqslant k \leqslant n$,

$$|\Theta A|\, |A|^{-1} \geqslant n-k.$$

Proof. We can assume

$$2 \leqslant k \leqslant n-1, \qquad 2^k < |A| < \tfrac{4}{3}2^k,$$

because the result obviously holds for $k = 0$, n, for $|A| \leqslant 2^k$ by Lemma 1, and $k = 1$, $2^k < |A| < \frac{4}{3}2^k$ are incompatible.

In particular this implies the result for $n = 1, 2$. We proceed by induction in n. $C_{n,|A|}$ can be written as disjoint union of $C(z^{n-k})$, $z^{n-k} = (1, 1, 1, \ldots, 1)$, and $B(z_0^{n-k}) \triangleq C_{n,|A|} \cap C(z_0^{n-k})$, $z_0^{n-k} = (1, 1, 1, \ldots, 1, 0)$. Now

$$\begin{aligned}\Theta(C_{n,|A|}) &= \Theta(C_{n,|A|}, C^c_{n,|A|}) \\ &= \Theta(C(z^{n-k})) - \Theta(C(z^{n-k}), B(z_0^{n-k})) \\ &\quad + \Theta(B(z_0^{n-k}), [C(z^{n-k}) \cup C(z_0^{n-k})]^c) \\ &\quad + \Theta(B(z_0^{n-k}), C(z_0^{n-k}) - B(z_0^{n-k})).\end{aligned}$$

Furthermore, since $|B(z_0^{n-k})| < \frac{1}{3}2^k = \frac{4}{3}2^{k-2}$, by induction hypothesis ($k-2 \leqslant n-1$):

$$\Theta(B(z_0^{n-k}), C(z_0^{n-k}) - B(z_0^{n-k})) \geqslant (k-(k-2))\, |B(z_0^{n-k})| = 2\, |B(z_0^{n-k})|.$$

Thus

$$\begin{aligned}\Theta(C_{n,|A|}) &\geqslant (n-k)2^k - |B(z_0^{n-k})| + (n-k-1)\, |B(z_0^{n-k})| + 2\, |B(z_0^{n-k})| \\ &= (n-k)(2^k + |B(z_0^{n-k})|) = (n-k)\, |A|.\end{aligned}$$

Since by Theorem II $|\Theta(A)| \geqslant |\Theta(C_{n,|A|})|$, this proves the inequality.

Theorem 2. *For all* $n \in \mathbb{N}$ *and* k, $0 \leq k \leq n-1$,

$$\mu^*(C^n, c) = (n-k)2^{n-1} \quad \text{if } 2^k \leq c < \tfrac{4}{3}2^k.$$

Proof. Since $\mu^*(C^n, c)$ is monotonically decreasing in c, we have for $c \geq 2^k$

$$\mu^*(C^n, c) \leq \mu^*(C^n, 2^k) = (n-k)2^{n-1},$$

by Theorem 1. Suppose that removal of m edges from C^n leaves us with connected components $Z_1, \ldots, Z_I$, $|Z_i| \leq c$ for $1 \leq i \leq I$, then

$$m \geq \frac{1}{2}\sum_{i=1}^{I} |\Theta Z_i| = \frac{1}{2}\sum_{i=1}^{I} \frac{|\Theta Z_i|}{|Z_i|}|Z_i|$$

$$\geq \frac{1}{2}(n-k)\sum_{i=1}^{I} |Z_i| = (n-k)2^{n-1},$$

where the second inequality follows from Lemma 2. □

Remark 6. It is easy to show for instance inductively that in terms of the representation (2.3)

$$\Theta(C_{n,N}) = \sum_{j=1}^{s} (n - i_j - 2(j-1))2^{i_j},$$

which can be used to derive other bounds on $\mu^*(C^n, c)$.

4. Removing vertices from the *n*-cube

We consider now the problem of getting bounds on $\lambda^*(C^n, c)$, which was defined in Section 1. Unfortunately the close connection between Theorem II, Section 2, and the μ^*-function is not paralleled by an equally close connection between Theorem I (the analogue to Theorem II) and the λ^*-function, even-though Lemma 2 has a canonical analogue, namely Lemma 3 below. However, in case $c > 2^{n-1}$, which is the case of interest for our problem in parallel computing, we get very good and in case $c > \frac{2}{3}2^n$ almost exact bounds.

Analogue to Lemma 2 and its consequence

Let us use the abbreviation

$$R(B) \triangleq |\Gamma(B) - B| \quad \text{for every } B \subset H^n.$$

Lemma 3. *For every* N, $1 \leq N \leq N_{k-1} \triangleq \binom{n}{n} + \cdots + \binom{n}{k}$ $(1 \leq k \leq n)$

$$R(S_{n,N})\,|S_{n,N}|^{-1} \geq R(S_{n,N_{k-1}})\,|S_{n,N_{k-1}}|^{-1}.$$

Proof. It suffices to prove the inequality for

$$N=\binom{n}{n}+\cdots+\binom{n}{k+1}+l, \quad 0\leqslant l<\binom{n}{k}, \tag{4.1}$$

because we can then iteratively apply the estimate.

We actually prove a somewhat stronger result:

$$\begin{aligned} &R(S_{n,N_k}\cup A)\,|S_{n,N_k}\cup A|^{-1}\geqslant R(S_{n,N_{k-1}})\,|S_{n,N_{k-1}}|^{-1} \\ &\text{for all } A\subset S_{n,N_{k-1}}-S_{n,N_k}, \qquad |A|=l. \end{aligned} \tag{4.2}$$

For this notice that

$$|S_{n,N_{k-1}}|=N_{k-1}=N_k+\binom{n}{k},$$

$$|S_{n,N_k}\cup A|=N_k+l, \qquad R(S_{n,N_{k-1}})=\binom{n}{k-1},$$

$$R(S_{n,N_k}\cup A)=\binom{n}{k}-l+|B|,$$

where

$$B\triangleq\{b\in S_{n,N_{k-2}}-S_{n,N_{k-1}}:\exists a\in A,\ d(a,b)=1\}$$

and obviously $|B|\geqslant k\,|A|/(n-k+1)$.

Thus it suffices to show that

$$\left[\binom{n}{k}-l+\frac{k}{n-k+1}\,l\right]\left[N_k+\binom{n}{k}\right]\geqslant\binom{n}{k-1}(N_k+l)$$

or equivalently that the inequality holds if

$$\begin{aligned} \left[\binom{n}{k}-l\right]\left[N_k+\binom{n}{k}\right] &\geqslant\binom{n}{k-1}[N_k+l]-\frac{k}{n-k+1}\,l\left[N_k+\binom{n}{k}\right] \\ &=\binom{n}{k}\frac{k}{n-k+1}[N_k+l]-\frac{k}{n-k+1}\,l\left[N_k+\binom{n}{k}\right] \\ &=\left[\binom{n}{k}-l\right]\frac{k}{n-k+1}N_k. \end{aligned}$$

This simplifies to

$$N_k+\binom{n}{k}\geqslant\frac{k}{n-k+1}N_k. \tag{4.3}$$

Now observe that for $t\geqslant k$

$$\frac{k}{n-k+1}\frac{n-t}{t+1}\leqslant 1,$$

and thus

$$\binom{n}{t} \geqslant \frac{k}{n-k+1}\frac{n-t}{t+1}\binom{n}{t} = \frac{k}{n-k+1}\binom{n}{t+1}.$$

Therefore

$$N_k + \binom{n}{k} = 1 + \sum_{k \leqslant t \leqslant n-1} \binom{n}{t} \geqslant \sum_{k \leqslant t \leqslant n-1} \frac{k}{n-k+1}\binom{n}{t+1} = \frac{k}{n-k+1} N_k$$

and we have proved (4.3) □

Notice that $R(S_{n,N})\,|S_{n,N}|^{-1}$ is *not* monotonically decreasing in N.

Example 4. $n=5$, $N_1=16$, $N_2=17$.

$$16 = \binom{5}{5} + \binom{5}{4} + \binom{5}{3},$$

$$17 = \binom{5}{5} + \binom{5}{4} + \binom{5}{3} + \binom{2}{2},$$

$$\Gamma S_{5,16} = \binom{5}{5} + \binom{5}{4} + \binom{5}{3} + \binom{5}{2} = 26,$$

$$\Gamma S_{5,17} = \binom{5}{5} + \binom{5}{4} + \binom{5}{3} + \binom{5}{2} + \binom{2}{1} = 28$$

and

$$\frac{26-16}{16} \not\geqslant \frac{28-17}{17}.$$

The reasoning which led to Theorem 1 yields now

Proposition 2. *For* $k > \frac{1}{2}n$

$$\lambda^*(C^n, N_{k-1}) \geqslant \frac{2k-n}{n^2-nk+2k}\,2^n. \tag{4.4}$$

Proof. Suppose that removal of l vertices results in the connected components $Z_1, \ldots, Z_I$ with $\max_{1 \leqslant i \leqslant I} |Z_i| \leqslant N_{k-1}$. Then

$$l = \left| \bigcup_{i=1}^{I} (\Gamma Z_i - Z_i) \right| \geqslant \frac{1}{n} \sum_{i=1}^{I} \frac{|\Gamma Z_i - Z_i|}{|Z_i|} |Z_i|. \tag{4.5}$$

By Theorem I for any $A \subset H^n$, $|A| = N$

$$R(A)\,|A|^{-1} \geqslant R(S_{n,N})\,|S_{n,N}|^{-1} \tag{4.6}$$

and by Lemma 3 for $N \leqslant N_{k-1}$

$$\begin{aligned} R(S_{n,N})\,|S_{n,N}|^{-1} &\geqslant R(S_{n,N_{k-1}})\,|S_{n,N_{k-1}}|^{-1} \\ &= \binom{n}{k-1}\left[\binom{n}{n} + \cdots + \binom{n}{k}\right]^{-1} \end{aligned} \tag{4.7}$$

Therefore

$$l \geqslant \frac{1}{n}\binom{n}{k-1}\left[\binom{n}{n}+\cdots+\binom{n}{k}\right]^{-1}(2^n-l). \tag{4.8}$$

It is well-known (see for instance Peterson "Error correcting codes") that

$$\sum_{i=\lambda n}^{n}\binom{n}{i} \leqslant \frac{\lambda}{2\lambda-1}\binom{n}{\lambda n} \quad \text{for } \frac{1}{2}<\lambda \leqslant 1.$$

With the permittable choice $\lambda = k/n$ we obtain

$$\sum_{i=k}^{n}\binom{n}{i} \leqslant \frac{k/n}{2k/n-1}\binom{n}{k} = \frac{n-k+1}{2k-n}\binom{n}{k-1}$$

and thus from (4.8)

$$l \geqslant \frac{2k-n}{n(n-k+1)}(2^n-l)$$

or equivalently (by elementary calculation)

$$l \geqslant \frac{2k-n}{n^2-nk+2k}2^n. \qquad \square \tag{4.9}$$

Discussion of the bound

Often the elementary inequality

$$\lambda^*(C^n, c) \geqslant \frac{1}{n}\mu^*(C^n, c) \tag{4.10}$$

in conjunction with Theorem 2 gives better results than the lower bound of Proposition 1. Responsible for the poor performance of this bound is obviously the factor $1/n$ in (4.4) needed for the present approach. In order to compare the bounds choose for δ, $1>\delta>\frac{1}{2}$, $k=\delta n$ and use the approximation

$$\binom{n}{\delta n} = 2^{h(\delta)n+O(\log n)}, \quad \text{where } h(\delta) = -\delta\log_2\delta-(1-\delta)\log_2(1-\delta).$$

Obviously

$$\binom{n}{k} \leqslant \sum_{i=1}^{k}\binom{n}{i} \leqslant n\binom{n}{k}$$

and therefore

$$\sum_{i=1}^{k}\binom{n}{i} = 2^{h(\delta)n+O(\log n)}.$$

With $\delta'(n)=h(\delta)+O(\log n)/n$ the bounds take the forms

$$\frac{1}{n}\frac{2\delta-1}{1-\delta+2\delta/n}2^n \quad \text{and} \quad \frac{1-\delta'(n)}{2}2^n,$$

and the second is obviously better by a factor const. $\cdot n$.

Inequality (4.4) is better for very small values of c. For instance

$$\lambda^*(C^n,1)=2^{n-1} \qquad \text{(the bound of (4.4))}. \tag{4.11}$$

To see this remove from C^n all vertices with an odd number of 1's in their coordinates. Then C^n decomposes into isolated vertices. Since

$$\sum_{0\leq t\leq n,\,\text{odd}}\binom{n}{t}=\sum_{0\leq t\leq n,\,\text{even}}\binom{n}{t}=2^{n-1},$$

clearly $\lambda^*(C^n,1)\leq 2^{n-1}$.

The main result

Theorem 3.

(a) $\lambda^*(C^n,N_k)=\binom{n}{k}$ *for* $N_k>\frac{2}{3}2^n$.

(b) $\binom{n}{k-1}\leq\lambda^*(C^n,c)\leq\binom{n}{k}$ *if* $\max(\frac{2}{3}2^n,N_k)<c\leq N_{k-1}$.

(c) *Define* $k_0=\max\{k:\binom{n}{0}+\cdots+\binom{n}{k}<\frac{1}{3}2^n\}$ *and* $L_0=\binom{n}{0}+\cdots+\binom{n}{k_0}$. *Then for any* c, $2^n-2L_0\leq c\leq 2^n-L_0$

$$\binom{n}{k_0}\leq\lambda^*(C^n,c)\leq 2\binom{n}{k_0}.$$

Proof. (a) If we remove from C^n all vertices with k 0's in their coordinates, then C^n decomposes into two connected components Z_1, Z_2 with

$$|Z_1|=\binom{n}{n}+\cdots+\binom{n}{k+1}=N_k \quad \text{and} \quad |Z_2|=\binom{n}{k-1}+\cdots+\binom{n}{0}<N_k.$$

Therefore $\lambda^*(C^n,N_k)\leq\binom{n}{k}$.

In order to show the reverse inequality assume that removal of l vertices results in the connected components $Z_1,\ldots,Z_I$ with $\max_{1\leq i\leq I}|Z_i|\leq N_k$. By taking unions of suitable Z_i's we can obtain *disjoint* sets $U_1,\ldots,U_J$ with

$$\bigcup_{j=1}^{J}U_j=\bigcup_{i=1}^{I}Z_i, \qquad \max_{1\leq j\leq J}|U_j|\leq N_k \quad \text{and} \quad |U_j\cup U_{j'}|>N_k \quad \text{for } j\neq j'. \tag{4.12}$$

Since $|\bigcup_{j=1}^{J} U_j| \leqslant 2^n$, (4.12) implies $J=2$, and thus by Theorem I

$$l \geqslant \max_{j=1,2} R(U_j) \geqslant R(S_{n,N_k}) = \binom{n}{k}.$$

(b) The upper bound follows exactly as in (a) and the lower bound with the additional fact $R(S_{n,c}) \geqslant R(S_{n,N_{k-1}})$. (Note that $R(S_{n,N})$ is not monotonically decreasing in N for $N \geqslant 2^{n-1}$.)

(c) Removal of all vertices from C^n, which have k_0 0's or k_0 1's in their coordinates results in three connected components Z_1, Z_2, Z_3 with

$$|Z_1| = \binom{n}{0} + \cdots + \binom{n}{k_0-1} < \tfrac{1}{3}2^n < 2^n - 2L_0,$$

$$|Z_2| = \binom{n}{k_0+1} + \cdots + \binom{n}{n-(k_0+1)} = 2^n - 2L_0,$$

$$|Z_3| = \binom{n}{n-(k_0-1)} + \cdots + \binom{n}{n} < \tfrac{1}{3}2^n < 2^n - 2L_0.$$

Since λ^* is monotonically decreasing therefore

$$\lambda^*(C^n, c) \leqslant \lambda^*(C^n, 2^n - 2L_0) \leqslant 2\binom{n}{k_0}.$$

Furthermore

$$\lambda^*(C^n, c) \geqslant \lambda^*(C^n, 2^n - L_0)$$

and since $N_{k_0} = 2^n - L_0 > \frac{2}{3}2^n$ we know from (a) that $\lambda^*(C^n, 2^n - L_0) = \binom{n}{k_0}$. Thus $\lambda^*(C^n, c) \geqslant \binom{n}{k_0}$. □

In conclusion we state the following

Problem. Find good upper bounds on minimal coverings of H^n with spheres of identical radii. This is one way to get good upper bounds on $\lambda^*(C^n, c)$.

References

[1] E.W. Dijkstra, Solution of a problem in concurrent programming control, CACM 8 (9) (Sept. 1965) 569.

[2] D.E. Knuth, Additional comments on a problem in concurrent programming control, CACM 9 (5) (May 1966) 321–322.

[3] N.G. de Bruijn, Additional comments on a problem in concurrent programming control, CACM 10 (3) (Mar. 1967) 137–138.

[4] M.A. Eisenberg, and M.R. McGuire, Further comments on Dijkstra's concurrent programming control problem, CACM 15 (11) (Nov. 1972) 999.

[5] M.O. Rabin, N-Process synchronization by $4 \log_2 N$-valued shared variable, Proc. 21st. Annual Symp. Foundation of Computer Science (1980) 407–410.

[6] J.E. Burns, M.J. Fischer, P. Jackson, N.A. Lynch and G.L. Peterson, Shared data requirements for implementation of mutual exclusion using a test-and-set primitive, Proc. 1978 Int. Conf. Parallel Processing (Aug. 1978) 79–87.

[7] J.E. Burns, Symmetry in systems of asynchronous processes, Proc. 22nd. Annual Symp. Foundation of Computer Science (1981) 169–174.
[8] L. Lamport, A new solution of Dijkstra's concurrent programming problem, CACM 17 (8) (Aug. 1974) 453–455.
[9] R. Rivest and V. Pratt, The mutual exclusion problem for unreliable processes: preliminary report, Proc. 17th Annual Symp. Foundation of Computer Science (1976) 1–8.
[10] G.L. Peterson and M.J. Fischer, Economical solutions for the critical section problem in a distributed system, Proc. 9th ACM Symp. Theory of Computing (1977) 91–97.
[11] H.J. Siegel, Interconnection networks for SIMD machines, Computer 12 (6) (June 1979) 57–65.
[12] L.H. Harper, Optimal assignment of numbers to vertices. J. Soc. Industr. Appl. Math. 12 (1) (1964) 385–393.
[13] L.H. Harper, Optimal numberings and isoperimetric problems on graphs, J. Combin. Theory 1 (1966) 385–393.
[14] R. Ahlswede and G. Katona, Graphs with maximal number of adjacent pairs of edges, Acta Math. Sci. Hung. 32 (1978) 97–120.
[15] A. Renyi and P. Erdös, On the strength of connectedness of a random graph, Acta Math. Acad. Sci. Hungar. 12 (1961) 262–267.
[16] A.K. Kel'mans, Connectivity of probabilistic networks, Automatika i Telemekhanika 3 (1967) 98–116.
[17] V.E. Stepanov, Combinatorial algebra and random graphs, Theoriya Veroyatnostei i u Primeniya 14 (3) (1969) 393–420.
[18] V.E. Stepanov, On the probability of the connectedness of a random graph, Theoriya Veroyatnostei i u Primeniya 15 (1) (1970) 55–67.
[19] M.V. Lomonosov, and V.P. Polesskii, An upper bound of the reliability of information networks, Problemy Peredači Informacii 7 (4) (1971) 78–81.
[20] M.V. Lomonosov and V.P. Polesskii, Lower bound of network reliability, Problemy Peredači Informacii 8 2 (1972) 47–53.
[21] G.A. Margulis, Probabilistic characteristics of graphs with large connectivity, Problemy Peredači Informacii 10 (2) (1974) 101–108.
[22] H.A. Schwarz, Beweis des Satzes, daß die Kugel eine kleinere Oberfläche besitzt als jeder andere Körper gleichen Volumens. Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. (1884) 1–13.
[23] E. Schmidt, Die Brunn-Minkowskische Ungleichung und ihr Spiegelbild sowie die isoperimetrische Eigenschaft in der euklidischen und nicht-euklidischen Geometrie I, Math. Nachr. 1 (1948) 81–157; II, Math. Nachr. 2 (1949) 171–244.
[24] R. Ahlswede, P. Gács and J. Körner, Bounds on conditional probabilities with applications in multi-user communication. Z. Wahrscheinlichkeits theorie und verw. Geb. 34 (1976) 157–177.
[25] R. Ahlswede, Remarks on Shannon's secrecy systems, Problems of Control and Information Theory 11 (4) (1982) 301–318.
[26] H.H. Lindsey, Assignment of numbers to vertices Amer. Math. Monthly 71 (May 1964) 508–516.
[27] A.J. Bernstein, Maximally connected arrays on the n-cube, SIAM J. Appl. Math. 15 (6) (Nov. 1967) 1485–1489.
[28] D.J. Kleitmann, M.M. Krieger and R.L. Rothschild, Configurations maximizing the number of pairs of Hamming-adjacent lattice points 50 (2) (June 1971) 115–119.
[29] R. Ahlswede and G. Katona, Contributions to the geometry of Hamming spaces, Discrete Math. 17 (1977) 1–22.
[30] Y.D. Burtin, Connection probability of a random subgraph of an n-dimensional cube, Problemy Peredači Informacii 13, (2) (1977) 90–95.