Search with small sets in presence of a liar

Iyaka O.H. Kamer

Abstract

The smallest element of an unknown set is sought by asking if it is contained in given subsets. It is assumed that the subsets are one of two: In a given subset, all of the elements are known; or the subset is empty. The decision of the subset can be made with a minimum of one test. The smallest element of the subset can be determined when the subset is of the second type. The problem can be formulated as determining whether the smallest element is in a given set. The problem can be solved in polynomial time. The question is: Can you find a minimum of one test of the subsets? © 2002 Elsevier Science B.V. All rights reserved.

MSc.: January 1999, secondary: 1999, ISSN: 0308-0101

Keywords: Search, liar, decision tree, non-growing search, entropy

1. Introduction

Let $S$ be a finite set of elements, say $S = \{x_1, \ldots, x_n\}$, and $1 \leq i \leq n$ an
unknown element. We want to find $i$ by asking questions of type "Is $i \in S"$, where
$x$ is a subset of $S$ with at least $i$ elements. However, some of the answers can be
false. It is assumed that the number of incorrect answers is at most $f$. The unknown
$x$ should be based simply on these informations. There are two different models,
the optimistic and the pessimistic, when the effect of the test question may depend on
the previous answers. In the first model, the optimistic, the answers are correct
when all the questions are asked in advance, and the minimum number of questions
$f(x_{\text{opt}})$ is the best. In the second model, the pessimistic, the answers are
correct only if none of the answers are incorrect, and the minimum number of questions
$f(x_{\text{pess}})$ is the worst. (An excellent survey of such problems can be found in [1].)

In other words, our task is to find the minimum number $f(x_{\text{opt}})$ of questions $x \in S \subseteq \{0, 1\}^n$ of the evidence $S$ with the knows the smallest element is $i$ if the evidence $S$ is located.
Let the characteristic vector of A be a 0-1 vector whose jth component is 1 if
\[ j \in A \]. Let our question sets be \( E_1, E_2, \ldots, E_m \), then define for \( m \) sets \( E \) of the
form \( E \equiv E_1 \cap E_2 \cap \cdots \cap E_m \). Observe that if the admissible elements \( I \) of \( E \) then the current answer
set of \( I \) can be identified with the \( I \)th column of \( X \). However, as most of the columns
are chosen to obtain the actual answer, it is easy to see that the answer \( I \) that is any column can be uniquely identified from the actual answer if these columns differ in at least \( 2 \) columns, or in other words that the minimum distance is at least \( 2 \) or 1.

Therefore, \( (a, b) \) is the minimum of such that there is an \( a \)-set \( I \) with at most \( b \) in each row and each column distance at least \( 2 \). In other words:

Voting the correctness of a set \( I \), or intransitive the role of \( a \) and \( b \) in any case of \( P \) queries the required property, therefore it can and will be supposed that

\[ P = 0 \].

The dual problem can be formulated in terms of non-increasing codes, too. The columns of the words are the row values. Thus set is an \( m \)-non-increasing code. The target problem of coding theory is to find the long (and in code of length \( m \) and

conditions is that at most \( a \) of its columns

Please refer to the reference text for more details.

In Section 2 we give, however, some improvements.

In Section 3 we give a linear estimator, while in Section 4 contains some constructions.

Finally, we give some final results on the use of these techniques.

Let \( \{x_i\} \) be a random sample taking on infinitely many distinct values with probabilities \( p_1, \ldots, p_n \) and \( \sum p_i = 1 \). In summary is defined by

\[ (2) \quad \frac{1}{n} \sum p_i \]

where \( \mu \) is the mean of the sample and \( \text{Var}(\mu) \) is the variance. If \( \mu \) is a random variable taking on infinitely many distinct values with probabilities \( p_1, \ldots, p_n \) and \( \sum p_i = 1 \), the entropy of \( \mu \) is defined as

\[H(\mu) = -\sum p_i \log p_i \]

This function is monotonically increasing in the interval \([0, 1]\) symmetric about the median in \([0, 1] \) and \(H(1/2) = 1\) (see e.g., Cover and Thomas, 1991 or Feller, 1968).
2. Improvements for the case of non-frac

Let $\mathcal{C}$ denote the polynomial $(x - 1)^{a - 1} \cdots (x - 1)^{b - 1}$. The following theorems give an asymptotic solution for $(x, a, b)$.

**Theorem 2.1** (Kane, 1962). Let $1 < a < b$ be integers. The inequality system:

\[
\begin{align*}
\sum_{i=1}^{b} \binom{b}{i} x^i &> 0, \\
\sum_{i=1}^{b} \binom{b}{i} x^i &\leq \frac{1}{b}
\end{align*}
\]

for a unique solution of $(x, a, b)$ satisfying that $x > 1$ is a positive integer, $a$ is real and $b - 1 < x < b$ holds. Then

\[\text{[See 4.1.1].}\]

The following lower and upper estimates are known.

**Theorem 2.2** (Kane, 1961; Lépine, 1990; Wegner, 1979)

\[
\begin{align*}
\log \frac{b}{a} &< \log \left( \frac{e}{a} \right) + \frac{1}{2} \log \left( \frac{e}{a} \right) (\log 2 - 1) \\
\end{align*}
\]

The lower estimate was proved in Kane (1961). A somewhat weaker than the present one upper estimate was derived in Kane (1964) from Theorem 2.2. However, it was not proved that the upper estimate was only a logarithmic lower rather than logarithmic lower. Hence, Kane (1961) and Wegner (1979) published the above conclusions proving the present, somewhat improved bound. The aim of the present section is to demonstrate that Theorem 2.1 provides good asymptotic solutions, too.

**Theorem 2.3.** Let the integer $2 \leq a$ and the real number

\[
\log x > x \frac{e}{2}
\]

be fixed. Then

\[
\log x \geq -e^2 - \Theta(1),
\]

where $\Theta$ is the only real solution of the equation

\[
\frac{e}{2} - e + 1
\]

and $(x)$ does not depend on $a$, but may depend on $b$ and $x$. On the other hand,

\[
\log x \leq \frac{e}{2}
\]
holds then
\[ f(n, x) = x^{n-1} + O(1) \]  
(27.7)
in the appropriate context.

Proof. Since it satisfies (2.5) holds with some complexity.
We will use that the pair \((b+1, a+b)\) is an asymptotic scheme of system (2.5).
(2.5), in the situation described above.
Let
\[ g(a+b) \leq a+b \sum_{i=1}^{a+b} \binom{a+b}{i} \]
that is, the polynomial on the left hand side of (2.5) with one actual value of \( b \).
It is easy to see that
\[ g(a+b) = \sum_{i=1}^{a+b} \binom{a+b}{i} b^{a+b-i} \cdot x^i = (b+1) x^{a+b} - (a+b) x^a + x \]
By (2.7) it implies
\[ g(a+b) \leq (a+b) x^{a+b} \]
(2.8)

Lemma 2.4. Let \( g(x) \) be a polynomial of order \( r+1 \) whose coefficients may depend
on \( n \) and suppose that it satisfies the following conditions:
\[ g(r)(x) = x^{r-2} \quad \text{for } r \geq 2 \quad \text{a.s.} \]
(2.9)
\[ g(r)(x) = 0 \quad \text{for some } r - 2 \leq x \leq a \]
(2.10)
\[ g(r)(x) = O(x^{r-2}) \quad \text{for some } r - 2 \leq x \leq a \]
(2.11)
Then
\[ |g(r)(x)| \leq \delta \]
(2.12)
holds where \( \delta \) does not depend on \( n \).
Proof. By Rolle's theorem,
\[ g(r)(x) = f(x) \]
in some interval \( \delta \) for some value \( \gamma \) in the interval determined by \( x_{\gamma} \) and \( x_{\gamma+1} \).
Therefore, by (2.6) it is at least \( e^{-\delta} \). Hence, we have
\[ g(r)(x) = O(e^{-\delta}) \]
by (2.12) and (2.11). The last step can be bounded by a constant \( \delta \). \( \square \)
Let us check that our $\phi(x)$ satisfies the conditions of the lemma.

\[
\phi(x) = \sum_{j=1}^{k} \sum_{i=1}^{n} \left( \frac{(-1)^{j-1}(-1)^{i-1}(x_{j} - 1)}{x_{j}} \right)
\]

is monotonically increasing for $x > 0$, and therefore it is enough to prove (3.1) at
$x = -1$, which is achieved since all the terms are non-negative at $x = -1$.

It is easy to see that $\phi(-1) = 0$ if $\phi$ is large enough. On the other hand, the
function is monotonous for $x > 0$, therefore $\phi(x) > 0$ for any real solution of
(3.1). Hence, the claim is proven, and the proof of condition (3.1) holds for
$\phi(x) > 0$, which means $\phi(x) > 0$ bound by $\phi(x) > 0$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.

The lemma can be used as follows: the lower for $\phi(x)$ is $\phi_{0}(x) = a_{n-1} + \phi_{0}(x)$.
A more precise solution is needed here: let \( \mathcal{A}(x) \) and \( \mathcal{B}(x) \) denote the real solutions to the quadratures:

\[
\begin{align*}
\mathcal{A}''(x) &= 0, \\
\mathcal{B}''(x) &= 0
\end{align*}
\]

respectively. By the theorem we have

\[
\mathcal{A}(0) = 0, \quad \mathcal{B}(0) = 0
\]

We want to show that when \( \mathcal{A}(x) \) or \( \mathcal{B}(x) \) is the solution of (2.11) and

(2.2) the inequalities

\[
\frac{\mathcal{A}'}{\mathcal{A}}(x) > \frac{\mathcal{B}'}{\mathcal{B}}(x) = c
\]

can be proved as earlier, we conclude

\[
\mathcal{A}' = \frac{\mathcal{A}}{c} \mathcal{A}(x)
\]

holds true (2.16) implies that \( \mathcal{A}(x) \) is the solution, while

\[
\mathcal{A}' = \frac{\mathcal{A}}{c} \mathcal{A}(x)
\]

implies the same for \( \mathcal{B}(x) \). An indirect way may be used to prove that either (2.16) or (2.17) must hold. Suppose

\[
\frac{\mathcal{A}'}{\mathcal{A}}(x) > \frac{\mathcal{B}'}{\mathcal{B}}(x)
\]

(2.17) is monotonically increasing for \( r > 1 \) on the other hand if \( r < 1 \) then \( \mathcal{A}(x) \) holds for large \( r \) and therefore (2.17) yields

\[
\mathcal{A}' = \mathcal{A}'(x)
\]

Consider

\[
\mathcal{A}''(x) = \mathcal{A}'(x) \frac{\mathcal{A}'(x) - c}{\mathcal{A}(x)} - \mathcal{A}'(x)
\]

Replacing \( c \) by \( \mathcal{A}'(x) \) in the above equality

\[
\mathcal{A}'(x) = \mathcal{A}'(x)
\]

is obtained. By (2.17) implies \( \mathcal{A}'(x) > 0 \) and this contradicts (2.11). \( \square \)

Remark: Theorem 2.5 states that the order of magnitude of \( A(x) e^{-x} \) is \( x^{-1} \).

However, it gives only that the constant is between \( \lambda \) and \( k \). Evidently one can easily see that the \( \lambda \) in Theorem 2.5 is between these numbers.
5. A lower estimate

Theorem 3.4. \( m = (k, l, t) \) always satisfies the inequality:
\[
\log \frac{\log \left( \frac{1}{1 - \alpha} \right)}{\log \left( \frac{1}{1 - \beta} \right)} \leq m.
\]

Hence,
\[
\log \left( \frac{1}{1 - \alpha} \right) \leq \log \left( \frac{1}{1 - \beta} \right).
\]

Proof. Let \( \mathcal{S} \) be a correctly chosen subset of \( M \) with probability \( \alpha \). On the other hand, \( \mathcal{S} \) is a random subset of size \( M \) whose probability of choosing a set in \( \mathcal{S} \) is \( \frac{1}{1 - \alpha} \). If the size of the set is at most \( l \), then \( \mathcal{S} \) is an independent event. If the size of the set is \( l \), then the event \( \mathcal{S} \) is not independent. The same holds for the event \( \mathcal{S} \) in \( \mathcal{S} \). Thus, \( \mathcal{S} \) is independent from \( \mathcal{S} \).

On the other hand, the size of the set is given by \( \mathcal{S} \) and \( \mathcal{S} \). The size of the set is exactly \( \alpha \). The conclusion is that \( \mathcal{S} \). (3.5)

Let \( \mathcal{S} \) be the set of positions where \( \mathcal{S} \) and \( \mathcal{S} \) differ in exactly \( \alpha \). This implies
\[
\log \left( \frac{1}{1 - \alpha} \right) \leq \log \left( \frac{1}{1 - \beta} \right).
\]

Both, \( \log \frac{1}{1 - \alpha} \) and \( \log \frac{1}{1 - \beta} \) take on only two distinct values, 0 and 1, and we have \( \log \frac{1}{1 - \alpha} = \log \frac{1}{1 - \beta} = 1 \) if this set, (3.4) and (3.5) prove inequality (3.3) in the theorem.
To obtain a stronger estimate we need an upper estimate on \( \phi_1(x) \). Find the probability \( P(x; \Theta) \) to be estimated.

\[
\begin{align*}
\mathcal{P}(x; \Theta) & = \mathcal{P}(x; \Theta) \approx \frac{1}{2} \left( \mathcal{P}(x; \Theta) + \frac{1}{2} \mathcal{P}(x; \Theta) \right) + \mathcal{P}(x; \Theta) \\
& = \frac{1}{2} \left( \mathcal{P}(x; \Theta) + \left( \frac{1 - \Delta}{\Delta} \right) \mathcal{P}(x; \Theta) \right) \\
& < \frac{1}{2} \left( \mathcal{P}(x; \Theta) + 1 \right) 
\end{align*}
\]

The number of possible choices of a 1-element \( \mathcal{C}_1 \) is

\[
\mathcal{C}_1 = \binom{n-1}{1} = \frac{n-1}{1} = n-1
\]

Therefore

\[
\mathcal{P}(x; \Theta) \leq \frac{1}{2}n
\]

This cannot exceed \( \frac{1}{2} n \) when

\[
\binom{n-1}{1} = \frac{n-1}{1} = n-1
\]

holds for all \( 0 < x \leq 1 \). Since we have \( \mathcal{P}(x; \Theta) \leq 0 \), (3.4) implies

\[
\mathcal{P}(x; \Theta) \leq 0
\]

If the right hand side is at most \( \frac{1}{2}n \), then we can use the monotonicity of \( \mathcal{K}(x) \) on the interval \([0, 1] \). If the inequality \( \mathcal{K}(x) \leq 0 \) on \([0, 1] \) is equivalent to (3.3). Under this condition (3.7) implies

\[
\mathcal{K}(x) \leq \frac{1}{2} n
\]

consequently (3.6) and (3.7) lead to (3.5). \( \square \)

Remark 3.2. Eq. (3.3) is nothing else but the so-called sphere packing bound if expressed for \( m = 1 \) well known in coding theory (see e.g. van Lint, 1971). If \( x = \frac{1}{2} \), i.e., on one hand, (3.3) cannot be satisfied, on the other hand, the condition on the size of the question and \( \Delta \), is satisfied. Therefore, cannot expect anything else but the inequality expressing that the solutions of \( \Delta \) form an outer-rounding code.
Remark 3.5. Suppose that \( n \) and \( d \) tend to infinity and \( lx \to n \). Eq. (3.1) implies that \( \alpha = \beta = \text{const} \). Assume that \( \alpha_n \to \alpha \) (that is, the probability of \( \Gamma \) being composed of \( \lambda = \text{const} \) elements). If \( \alpha_n \to \infty \), then \( \Gamma \) holds the large \( \alpha_n \), so (4) the following holds:

\[
\lim_{\alpha_n \to \infty} \frac{\log N(\alpha_n)}{\alpha_n} = \log N(\Gamma)
\]

in this case, so (4) holds to

\[
\frac{\log N(\alpha_n)}{\alpha_n} \to \log N(\Gamma)
\]

4. Construction

Let \( F \) be a set of \( n \) elements. A Steiner system \( \text{Steiner}(n,t) \) is a family of \( v \)-element subsets \( F \) such that for every \( t \)-element subset \( \gamma \) of \( F \) is included in exactly one member of the family. The Steiner system is such that the number of members is

\[
N = \binom{v}{t}
\]

Let \( \mathcal{F} \) be a family of subsets of \( V \). The degree of the family \( \mathcal{F} \) as \( \gamma \in \mathcal{F} \) is the number of members \( F \) of \( \mathcal{F} \) such that \( \gamma \subseteq F \). A family is almost regular if the difference of the degree of the family for different elements \( \gamma \) is at most one:

\[
|d(F) - d(F')| \leq 1 \quad \forall F, F' \in \mathcal{F}
\]

The family \( \mathcal{F} \) is then regular if it is almost regular for all \( \gamma \). It is then called Steiner regular. If \( \mathcal{F} \) is almost regular, then it can be partitioned into \( \lambda \) non-intersecting subsets, each of which is a Steiner system. If \( \mathcal{F} \) is regular, then it can be partitioned into \( \lambda \) non-intersecting subsets, each of which is a Steiner system. If \( \mathcal{F} \) is almost regular, then it can be partitioned into \( \lambda \) non-intersecting subsets, each of which is a Steiner system.

Let \( \text{Steiner}(n,t) \) be a Steiner system, and suppose that

\[
\mathcal{F} = \{ \gamma_1, \gamma_2, \ldots, \gamma_\lambda \}
\]
Define the matrix $A$ with the help of $\{x, y, z\}$ the columns of the matrix are the characteristic (zero-one) version of the first $x$ members of $\{x, y, z\}$ in the order of the definition of a winning family. It is easy to see that the Hamming distance between any two columns of $A$ is at most $x$. Moreover, if a column $A_i$ has the value $0$ at most once, then it is in the row $(w, v)$, where the number of ones in any given row is at most $1$. That is, if it satisfies (4.2), $A_i$ satisfies

$$\begin{bmatrix} 1 & 0 & \vdots & 0 \\ a_{i1} & a_{i2} & \cdots & a_{in} \end{bmatrix}$$

Then

$$(a_{i1}, a_{i2}, \ldots, a_{in}) \in H$$

holds.

\textbf{Lemma 6.1.} Suppose that $a, b$ are given and

$$k = \rho(a, b)$$

and

$$\frac{p}{q} = \frac{a}{b}$$

hold with some integer $k$. Then (4.2) and (4.3) also hold.

\textbf{Proof.} Suppose that (4.3) holds. Then we have

$$a = \left\lfloor \frac{k}{b} \right\rfloor b + r$$

On the other hand, (4.3) implies the following inequality:

$$1 \leq a \leq \frac{k}{b} + 1$$

Thus, by using (4.6), we obtain

$$a \in \left\{ \frac{k}{b} - 1, \frac{k}{b} - \frac{1}{b}, \ldots, 0 \right\}$$

This lemma and (4.1) yield

\textbf{Theorem 6.2.} If $a, b, c$ and $d$ satisfy (4.2) with some positive integer of $(c,b)$ and there is a winning family $\{x, y, z\}$, then in satisfies (4.4) that

$$A_{i1}, A_{i2}, \ldots, A_{in} \in H$$
Theorem 45. Suppose that \( v_0 \) is fixed and \( u \) tends to infinity, i.e.,
\[
\lim_{u \to \infty} u^{1/2} = u.
\]
\[
(57)
\]
Then
\[
\frac{R - 2}{u} > \sin \left( \frac{\pi \theta}{2} \right)
\]
(58)
holds. On the other hand, if
\[
\omega = R
\]
(59)
and there is an infinite series of such pairs \((u, \theta)\) which satisfy (47) with some \( \beta > 0 \) and there is a covering theorem family \( \{ \omega, \beta, \theta \} \) where
\[
\left| \frac{D_{\omega, \beta, \theta}}{u} \right| < \frac{R}{u}
\]
(60)
then
\[
\lim_{u \to \infty} \left( \frac{\left| D_{\omega, \beta, \theta} \right|}{u} \right) = 0
\]
(61)
completes (48).

Proof. A weakened form of (5.1) will be used in place (6.4). \((\theta)\)
\[
\omega \leq u \left( \left| \frac{\omega}{R} \right| \right)
\]
(62)
It will be shown that if
\[
\omega \left( \frac{R - 2}{u} \right)^{1/2} < \sin \left( \frac{\pi \theta}{2} \right)
\]
(63)
then some \((\theta)\) and \((\theta)\) satisfy (47) if (6.1) cannot hold. The trivial inequality
\[
-2 \leq \sin (1) \quad (0 < u < 1)
\]
implies
\[
A(1) = -2 \sin (1) - \frac{1}{2} \sin (1) - \frac{1}{2} \sin (1) = -2 \sin (1) - \frac{1}{2} \sin (1)\]
(64)

This inequality will be applied to \(v = \omega + \frac{1}{u} \) where \( \omega \) and \( \omega \) are determined by (47) and (6.1), respectively, for each
It is easy to see that
\[ \frac{2x}{\sqrt{1-x^2}} = \frac{2x}{\sqrt{1-\frac{1}{4}}} \]
This is trivially true when \( n \equiv m \pmod{1} \) and \( m \equiv 1 \pmod{1} \). Therefore, \( n \equiv m \pmod{1} \) can be assumed. Now, let us consider the case where \( n \neq m \pmod{1} \). The kernel of \( (\mathbb{Z}^2) \to \mathbb{Z}/m \mathbb{Z} \) is trivial, and the surjection is surjective. The stabilizing property implies that
\[
\begin{vmatrix}
-2 & -3 + i \equiv 1 \\
1 & 1 + i
\end{vmatrix}
\]
(4.15)
By (4.14), we have
\[
\frac{\sqrt{2}}{\sqrt{\lambda}} + \frac{1}{\sqrt{\lambda}}
\]
and hence (4.13) is at most 5, proving the other important property of \( \mathcal{H} \). Of course, this computation holds only when \( \lambda \) does not exceed the number of vertices of \( \mathcal{H} \) in the interval of \( \sqrt{\lambda} \). It can be determined from the equality
\[
\begin{pmatrix}
1 \\
1 + i
\end{pmatrix} + \begin{pmatrix}
1 \\
1 + i
\end{pmatrix} = \begin{pmatrix}
1 \\
1 + i
\end{pmatrix} + \begin{pmatrix}
1 \\
1 + i
\end{pmatrix}
\]
Therefore, we have the following inequality:
\[
\frac{m}{\sqrt{\lambda}} = \frac{1}{\sqrt{\lambda}} \leq \frac{\sqrt{2}}{\sqrt{\lambda}} + \frac{1}{\sqrt{\lambda}}
\]
(4.13)
We claim that this holds when
\[
\delta = \frac{\sqrt{2}}{\sqrt{\lambda}} + \frac{1}{\sqrt{\lambda}}
\]
Indeed, the latter inequality implies
\[
\frac{1}{\sqrt{\lambda}} \leq \frac{\sqrt{2}}{\sqrt{\lambda}} + \frac{1}{\sqrt{\lambda}}
\]
Note that (4.15) holds if \( \lambda \geq 1 \) is obtained, proving (4.14).

A somewhat surprising result is that this construction is the best possible for the given

**Theorem 4A.** If \( \mathcal{H} \) is a directed graph of \( \lambda \) vertices, then
\[
\begin{vmatrix}
-2 & -3 + i \equiv 1 \\
1 & 1 + i
\end{vmatrix}
\]
is divisible by \( i + 1 \) and there is a nearly linear system \( X(\mathcal{H}, 1, 2) \) such
\[
\begin{pmatrix}
\mathcal{H} \\
\mathcal{H} \cup \mathcal{H}
\end{pmatrix}
\]

**Proof.** Let \( \mathcal{H} \) be an \( m \times n \) matrix, in which the non-zero entries of columns are at least \( 2 \) and the stability of \( \mathcal{H} \) is at most \( 1 \). Define the number
of columns containing 1's is by $q_i (i = 0, n)$. We give now a lower estimate on the total number of 1's in 
\[ \sum_{i=1}^{n} \frac{2}{\sqrt{i}} + \frac{1}{i} \leq \sqrt{2} + 2 \sum_{i=1}^{n} \left( \frac{1}{\sqrt{i}} - \frac{1}{\sqrt{i+1}} \right) \]

Comparing it with the trivial upper estimate, the following inequality is obtained:
\[ m^2 \geq 2 \sum_{i=1}^{n} \frac{1}{\sqrt{i}} \implies \text{for } i > 4m. \] (4.17)

It is easy to see that
\[ \sum_{i=1}^{m} \frac{1}{\sqrt{i}} \leq 1 \] (4.19)

holds by the distance condition for the columns.

Some cases will be distinguished.

Case 1: $\sum_{i=1}^{n} \frac{1}{\sqrt{i}} < 1$. Two columns containing exactly $1-1$'s cannot have a common zero element.

\[ mL \geq 2 \sum_{i=1}^{n} \frac{1}{\sqrt{i}} \implies mL \geq 2 \sum_{i=1}^{m} \frac{1}{\sqrt{i}} \] (4.18)

proving the statement for this case.

Case 2: $\sum_{i=1}^{n} \frac{1}{\sqrt{i}} > 1$. A sharpening of (4.18) will be used in this case. It can be supposed, without loss of generality, that the first column contains 1's and they tend to the first $j$ rows. Let $m_j$ denote the number of columns containing a column with exactly $j$ 1's. We give an upper bound on the number of 1's in the matrix formed by the last $n-j$ columns of $M$.

\[ \sum_{i=1}^{n} \frac{1}{\sqrt{i}} < 1 \implies mL \geq 2 \sum_{i=1}^{m} \frac{1}{\sqrt{i}} \] (4.20)

(To be precise, one should deal with $Q_j$ for the submatrix but one gives a lower estimate on the left hand side, analogue to (4.17)

\[ mL \geq 2 \sum_{i=1}^{n} \frac{1}{\sqrt{i}} \] (4.21)

Combining this inequality with (4.20),

\[ mL \geq 2 \sum_{i=1}^{m} \frac{1}{\sqrt{i}} \sum_{i=1}^{m} \frac{1}{\sqrt{i}} \geq 2 \sum_{i=1}^{m} \frac{1}{\sqrt{i}} \] (4.22)

Case 3: $j < \sum_{i=1}^{n} \frac{1}{\sqrt{i}}$. It is sufficient to consider the terms with $j = n-1$. All other terms are 0. Therefore, $m_j$ is zero for all $j < n-1$ because of the distance condition between the columns. For the same reason $m_{n-1} = 0$ because of (4.17) and (4.21) leads to

\[ mL \geq 2 \sum_{i=1}^{n} \frac{1}{\sqrt{i}} \] (4.23)

This inequality is stronger than (4.19), proving the statement in this case.
The above constructions are good when the solution size is relatively small. The new construction is trivial and rather weak, but works for all values of the parameters. For $2^r \geq \frac{4}{3}c^2 - 1$, the code is of a binary expansion of length $n'$, with pairwise Hamming distance at least $2^{r+1}$. Consider the $n$ columns of a matrix. If "obtained" satisfies the conditions, the matrix can be transformed into a binary expansion of the form $\mathbf{Y}_1 \oplus \mathbf{Y}_2$, where $\mathbf{Y}_1$ has $r$ columns, and $\mathbf{Y}_2$ has $n-r$ columns, by the following procedure: (a) cut the matrix into parts of width $r$ and making from [12] parts "simple" by "pulling" the matrix entries in $r$ columns longer, the so obtained matrix will satisfy all the conditions if $n'(n') = n$. This trivial construction can be somewhat improved if we exploit the fact that the large Hamming distance between large number of $\mathbf{Y}_1$s.

**Theorem 5.4.** Let $n'(n')$ be the maximum number of codewords in a binary code of length $n'$, with pairwise Hamming distance at least $2^{r+1}$. Then

$$f(n, n') = \frac{1}{2^n} \frac{1}{2^{n'}} \left( \sum_{i=0}^{n'} \binom{n'}{i} (-1)^i \frac{1}{2^{n'-i}} \right)$$

where $n'$ is the smallest integer such that $n'(n')^2 \geq \frac{4}{3} c^2 - 1$.

**Proof.** By (4.23) there exists an $n = n'(n')$ matrix $M$ such that the pairwise Hamming distance of its columns are at least $2^{r+1}$. Denote the number of $1$s in the $A$ row by $a = \frac{1}{2^n} \sum_{i=0}^{n'} \binom{n'}{i} (-1)^i \frac{1}{2^{n'-i}}$. Replace the first row of $M$ by $\{a, 0, \ldots, 0\}$ on top row, obtained by stemming the first one into parts containing at most $1/2$ of the entries of these rows. Replace the top row from $[0, 0, \ldots, 0]$ by $[a, a, a, \ldots, a]$. Denote the so obtained matrix by $\mathbf{Y}_1$. It is obvious that the pairwise Hamming distance between the columns of $\mathbf{Y}_1$ is at least $2^{r+1}$ single.

Repeating the step with all the rows of $\mathbf{Y}_1$ we arrive at a matrix $\mathbf{Y}_2$ having at most

$$\sum_{i=0}^{n'} \binom{n'}{i} \frac{1}{2^{n'-i}}$$

rows, a column and the Hamming distance is not less than before.

Counting the number of (1,1) pairs in the same rows of $\mathbf{Y}_1$, the following inequality can be obtained:

$$\sum_{i=0}^{n'} \binom{n'}{i} \frac{1}{2^{n'-i}} \leq \frac{1}{2^n} - \frac{1}{2^n}$$
Apply the Cauchy–Schwarz inequality for the right hand side:
\[ \sum_{x} x^2 \leq \left( \sum_{x} 1 \right) \left( \sum_{x} x^2 \right)^{1/2}. \]

The last two inequalities lead to
\[ \left( \sum_{x} 1 \right)^2 \leq \sum_{x} x^2 \leq \left( \sum_{x} x \right)^2. \]

Solve the quadratic inequality for \( \sum_{x} x \)
\[ \sum_{x} x \leq \left( \sum_{x} 1 \right)^{1/2} \left( \sum_{x} x^2 \right)^{1/2}. \]

Substituting this in (13.13), the right hand side of (14.21) is obtained.

**Remark 4.7.** Suppose that \( a \to \infty \) and \( \varepsilon \to 0 \), moreover \( \varepsilon \) tends to 0. The expression Vanderbosch–Gilbert bound (see e.g. MacWilliams and Sloane, 1977) gives
\[ \log_{2} \frac{16}{\pi^2} \approx 3.21 \]
when \( 2^{-k} - \varepsilon < 1 \). Use the inequality of \( \varepsilon \)
\[ \varepsilon \frac{2^{-k}}{2} \frac{1}{1+k} \]
these two inequalities imply
\[ 2^{-k} \approx \frac{-\log_{2} (\pi/4)}{\log_{2} (1+k)} \]

Use a rounded version of (14.22)
\[ a \approx \frac{-\log_{2} (\pi/4)}{\log_{2} (1+k)} + \log_{2} (\pi/4) \]

Then
\[ \frac{2^{-k}}{2} \frac{1}{1+k} \approx \frac{2^{-k}}{2} \frac{1}{1+k} \]

is obtained. Eq. (14.22) also implies
\[ a \leq \frac{2}{k} - 1 \times \frac{1}{1+k}. \]

Hence we have
\[ 2^{-k} \approx \frac{-\log_{2} (\pi/4)}{\log_{2} (1+k)} + \log_{2} (\pi/4) \]

Due to
\[ a = \frac{2}{k} - 1 \times \frac{1}{1+k}. \]
A. Further remarks and questions

1. Let us illustrate the difference among the resolvability, building, and storing properties on the family of all relevant subsets of an atomistic set. The family can be considered within our problem. The fundamental theorem of Heine (1941) states that these properties are equivalent.

2. It is easy to see that the family of all relevant subsets of a Boolean algebra forms a Boolean algebra, and as such, the complete lattice (the Boolean algebra) of the relevant subsets, each of which covers $\mathcal{F}$, is $\mathcal{F}$-directed. Thus, they can be obtained from each other by passing the elements of $\mathcal{F}$. This is an important formulation of the definition of building property for the special case. It was only conjectured by Heine and was further developed by the notion of a family of all relevant subsets of an atomistic set in Heine (1941).

3. However, as Tarski (1951) has shown, the relevant property of the same family is preserved at any terms in Kurepa (1954).

2. Suppose that a family is regular, that is, any element of the family is contained in the same number of subfamilies. It is easy to see that this does not imply even the existence of a relevant subset, and only for the case $r=2$, the relevant algebra of two and cyclic with $r=2$ gives a nontrivial example. A finite projective geometry is another obvious occurrence.

Problem 5.3. Find a sufficient condition for a regular family to be regular.

The resolvability property is not independent of the relevant property. It is the degree of the elements in the relevant subset of a subfamily which is required. This serves as a motivation for the following problem. Let $\mathcal{F}(t_1, t_2, \ldots, t_r)$ be a family of relevant subsets of an atomistic set. Let $d(\mathcal{F})$ denote the difference between the maximum and minimum degree of the family $\mathcal{F}$ at the elements of $\mathcal{F}(t_1, t_2, \ldots, t_r)$.

Problem 5.4. Prove that there is a finite system $\mathcal{T}(n, s, a)$, where $a$ is small, where $\mathcal{T}$ is a function of $t_1$ and $s$.

On the other hand, it would also be interesting to determine $d(\mathcal{F})$ for difference classes of families.
Our results are valid only in the case when it is small, namely, if its order of magnitude is $o(n^2)$ when $\frac{n}{12}$ is small, then the problem becomes hard, solving large. The essential condition is that the problem is solvable, improved by the three lemmas, and the error term is $o(1)$. The relation between the number of solutions and the order of magnitude of the error term must be similar to the orders known from the theory of error-correcting codes.

**Problem 5.3.** Find good lower and upper estimates on $f(n,k)$ when $k = o(n^2)$ and $\frac{n}{12} = o(1)$.

**Problem 5.4.** Find good lower and upper estimates on $f(n,k)$ when $k = o(n^2)$ and $\frac{n}{12} = o(1)$. (The last condition might make more sense in the form $\frac{n}{12} = o(n^2)$.)

Remarks 5.3 and 5.4 show that the order of magnitude in these cases is constant times a large number which both the lower and upper estimates can be improved. (A 47) is especially weak and is valid only for the case when $l$ is less than half of $n$.

**References**


