Europ. J. Combinatorics (1995) **16**, 263–266

Cancellative Pairs of Families of Sets

Ron Holzman and János Körner

A pair $(\mathscr{A}, \mathscr{B})$ of families of subsets of an n-element set X is cancellative if, for all $A, A' \in \mathscr{A}$ and $B, B' \in \mathscr{B}$, the following conditions hold: $A \backslash B = A' \backslash B \Rightarrow A = A'$ and $B \backslash A = B' \backslash A \Rightarrow B = B'$. We prove that every such pair satisfies $|\mathscr{A}|\,|\mathscr{B}| < \theta^n$, where $\theta \approx 2.3264$. This is related to a conjecture of Erdős and Katona on cancellative families and to a conjecture of Simonyi on recovering pairs. For the latter, our result gives the best known upper bound.

1. Introduction

Our research was prompted by the following beautiful conjecture of G. Simonyi. Let $\mathscr{A}$ and $\mathscr{B}$ be two families of subsets of an n-element set X. The pair $(\mathscr{A}, \mathscr{B})$ is a *recovering pair* if for all $A, A' \in \mathscr{A}$ and $B, B' \in \mathscr{B}$ the following conditions hold:

$$A \backslash B = A' \backslash B' \Rightarrow A = A', \qquad B \backslash A = B' \backslash A' \Rightarrow B = B'. \tag{1a,b}$$

Conjecture (Simonyi). *If $(\mathscr{A}, \mathscr{B})$ is a recovering pair, then $|\mathscr{A}|\,|\mathscr{B}| \leq 2^n$.*

If true, this upper bound is best possible. Take any subset S of X: let $\mathscr{A}$ consist of the subsets of S and let $\mathscr{B}$ consist of the subsets of $X \backslash S$. The study of recovering pairs originally arose in an information-theoretic context (see [5]). The conjecture was discussed further by Ahlswede and Simonyi [1]; its formulation there is different but equivalent to the above, using unions and intersections in (1a) and (1b) respectively instead of differences. They also offered a more general version of the conjecture for pairs of subsets of a finite lattice, called the 'Sandglass Conjecture', and proved it in the special case when the lattice is the product of two chains. For the original conjecture, where the lattice is the boolean lattice, they gave an argument proposed by G. Cohen which yields an upper bound of 3^n.

In our attempts to improve this upper bound, we noticed that our arguments did not take advantage of the full force of the conditions (1), but only of a weaker version of the conditions. The pair $(\mathscr{A}, \mathscr{B})$ is a *cancellative pair* if for all $A, A' \in \mathscr{A}$ and $B, B' \in \mathscr{B}$ the following conditions hold:

$$A \backslash B = A' \backslash B \Rightarrow A = A', \qquad B \backslash A = B' \backslash A \Rightarrow B = B'. \tag{2a,b}$$

Thus, we require only that distinct sets in $\mathscr{A}$ yield distinct differences when the *same* set in $\mathscr{B}$ is subtracted from both, and vice versa.

In order to state our result, we recall that the *entropy function* $h(p)$ is defined for $0 \leq p \leq 1$ by

$$h(p) = -p \log p - (1-p)\log(1-p),$$

where 'log' denotes logarithm to the base 2, and we use the convention $0 \log 0 = 0$. Let θ be the largest solution of the equation $\sqrt{1/t}\, h(\sqrt{1/t}) = \log \sqrt{t}$. Then $\theta \approx 2.3264$.

Theorem. *If $(\mathscr{A}, \mathscr{B})$ is a cancellative pair, then $|\mathscr{A}|\,|\mathscr{B}| < \theta^n$.*

We chose the term 'cancellative pair' in order to suggest a connection with

0195-6698/95/030263 + 04 $08.00/0

cancellative families. We recall that a family $\mathscr{A}$ is *cancellative* if no three distinct sets $A, B, C \in \mathscr{A}$ satisfy $A \cup B = A \cup C$ (or, equivalently, $B \setminus A = C \setminus A$). When the above definition of a cancellative pair is applied to a pair $(\mathscr{A}, \mathscr{A})$, where $\mathscr{A}$ is an antichain with respect to inclusion, one obtains the concept of a cancellative family. Given an n-element set X with n divisible by 3, one can construct a cancellative family $\mathscr{A}$ of subsets of X having $|\mathscr{A}| = 3^{n/3}$ as follows: let $X_1, \ldots, X_{n/3}$ be a partition of X into triples, and let $\mathscr{A}$ consist of those subsets of X which intersect each X_i in exactly one element (a slight modification is required if $3 \nmid n$). Erdős and Katona (see [4]) found this construction and conjectured that it is optimal. Frankl and Füredi [3] proved an upper bound of $c\sqrt{n}\,1.5^n$ for the size of a cancellative family of subsets of an n-element set.

Taking the Erdős–Katona construction to play the role of both $\mathscr{A}$ and $\mathscr{B}$, we obtain a cancellative pair with $|\mathscr{A}|\,|\mathscr{B}| = 9^{n/3} \approx 2.08^n$. This is the best construction that we have for a cancellative pair. In terms of bringing the upper bound closer to the value suggested by this construction, one may attempt to adapt the argument of Frankl and Füredi to the two-family version of the problem. This would improve our upper bound to about 2.25^n, but we do not see how to do this.

Returning to recovering pairs, we remark that the upper bound stated in our theorem is also the best we know for recovering pairs. However, the conjectured upper bound of 2^n for recovering pairs does not hold under the weaker assumption of a cancellative pair, as indicated by the above-mentioned construction.

2. Proof of the Theorem

In preparation for the proof, we recall the information-theoretic concept of the entropy of a discrete random variable. Let ξ be a random variable which assumes k distinct values with respective probabilities $p_1, \ldots, p_k$ ($p_j > 0$, $\sum_{j=1}^k p_j = 1$). The *entropy* of ξ is defined as:

$$H(\xi) = -\sum_{j=1}^{k} p_j \log p_j.$$

In the special case in which $k = 2$ and the probabilities are p and $1 - p$, one obtains the entropy function $h(p)$. We shall use the following well-known fact (see [2]): if $\xi = (\xi_1, \ldots, \xi_n)$ is an n-dimensional random variable, then

$$H(\xi) \leqslant \sum_{i=1}^{n} H(\xi_i). \tag{3}$$

We prove the theorem by induction on n. The induction base being trivial to verify, we proceed directly to the inductive step. Let $(\mathscr{A}, \mathscr{B})$ be a cancellative pair of families of subsets of an n-element set, which we assume, w.l.o.g., to be $X = \{1, \ldots, n\}$. For $i = 1, \ldots, n$, we introduce the notations:

$$\mathscr{A}_i = \{A \in \mathscr{A}: i \notin A\}, \qquad p_i = |\mathscr{A}_i|/|\mathscr{A}|;$$

$$\mathscr{B}_i = \{B \in \mathscr{B}: i \notin B\}, \qquad q_i = |\mathscr{B}_i|/|\mathscr{B}|.$$

We observe that $(\mathscr{A}_i, \mathscr{B}_i)$ is a cancellative pair of families of subsets of $X \setminus \{i\}$, and so the induction hypothesis implies that $|\mathscr{A}_i|\,|\mathscr{B}_i| < \theta^{n-1}$. If $p_i q_i \geqslant 1/\theta$, then we obtain $|\mathscr{A}|\,|\mathscr{B}| < \theta^n$ as desired. So we may assume that $p_i q_i < 1/\theta$ for every $i = 1, \ldots, n$.

Now, fix a set $B \in \mathscr{B}$ and consider the random variable $\xi^B = A \setminus B$, where $A \in \mathscr{A}$ is chosen according to the uniform distribution on $\mathscr{A}$. By (2a), ξ^B assumes distinct values for distinct realizations of A, and therefore its entropy is $H(\xi^B) = \log|\mathscr{A}|$. On the other hand, ξ^B can be viewed as an n-dimensional random variable with components $\xi_1^B, \ldots, \xi_n^B$, where $\xi_i^B = 1$ if $i \in A \setminus B$ and $\xi_i^B = 0$ otherwise. For $i \in B$ we have $H(\xi_i^B) = 0$ and for $i \notin B$ we have $H(\xi_i^B) = h(p_i)$. Applying (3) we obtain:

$$\log |\mathscr{A}| \leq \sum_{i \in X \setminus B} h(p_i).$$

We have such an inequality for every $B \in \mathscr{B}$. Averaging these inequalities we obtain

$$\log |\mathscr{A}| \leq \frac{1}{|\mathscr{B}|} \sum_{B \in \mathscr{B}} \sum_{i \in X \setminus B} h(p_i) = \frac{1}{|\mathscr{B}|} \sum_{i=1}^{n} |\mathscr{B}_i| h(p_i) = \sum_{i=1}^{n} q_i h(p_i).$$

Arguing similarly with the roles of $\mathscr{A}$ and $\mathscr{B}$ interchanged, we obtain

$$\log |\mathscr{B}| \leq \sum_{i=1}^{n} p_i h(q_i).$$

Adding up the two inequalities results in

$$\log |\mathscr{A}|\,|\mathscr{B}| \leq \sum_{i=1}^{n} [q_i h(p_i) + p_i h(q_i)]. \tag{4}$$

What remains to be done is some investigation of the function

$$f(p, q) = qh(p) + ph(q) \qquad (0 \leq p, q \leq 1).$$

The following facts and our assumption that $p_i q_i < 1/\theta$, $i = 1, \ldots, n$, permit us to conclude from (4) that $|\mathscr{A}|\,|\mathscr{B}| < \theta^n$ as desired.

FACT 1. *On each hyperbola of the form $pq = C$, the maximum of $f(p, q)$ is attained when $p = q$.*

FACT 2. *$f(p, p)$ is increasing for $0 \leq p \leq \sqrt{1/\theta}$ and assumes the value $\log \theta$ at $p = \sqrt{1/\theta}$.*

To prove Fact 1, we compute the derivative of $f(p, q)$ with respect to p when q varies with p, so as to keep their product constant:

$$\begin{aligned}
\left.\frac{\mathrm{d}f(p,q)}{\mathrm{d}p}\right|_{pq=C} &= \left.\frac{\partial f(p,q)}{\partial p} + \frac{\partial f(p,q)}{\partial q}\frac{\mathrm{d}q}{\mathrm{d}p}\right|_{pq=C} \\
&= q \log \frac{1-p}{p} + h(q) + \left[p \log \frac{1-q}{q} + h(p)\right]\left(-\frac{q}{p}\right) \\
&= q\left[\log \frac{1-p}{p} + \frac{h(q)}{q} - \log \frac{1-q}{q} - \frac{h(p)}{p}\right] \\
&= q\left[\log \frac{1-p}{p} - \log q - \frac{1-q}{q} \log(1-q)\right. \\
&\qquad \left. - \log \frac{1-q}{q} + \log p + \frac{1-p}{p} \log(1-p)\right] \\
&= q\left[\frac{1}{p} \log(1-p) - \frac{1}{q} \log(1-q)\right].
\end{aligned}$$

The assertion of Fact 1 will follow if we show that the derivative computed above is positive for $p<q$ and negative for $p>q$. Thus, it suffices to show that

$$g(p)=\frac{\ln(1-p)}{p}$$

is a decreasing function (we have switched to natural logarithms for convenience). Indeed,

$$\frac{dg(p)}{dp}=\left[-\frac{p}{1-p}-\ln(1-p)\right]\Big/p^2=\left[\ln\left(1+\frac{p}{1-p}\right)-\frac{p}{1-p}\right]\Big/p^2<0$$

since $\ln(1+x)<x$ for all $x>-1$, $x\neq 0$.

For Fact 2, we observe that

$$\frac{df(p,p)}{dp}=2\left[p\log\frac{1-p}{p}+h(p)\right]$$

is positive for $p<p_0$ and negative for $p>p_0$, where $p_0\approx 0.7$. It can be verified that $\sqrt{1/\theta}<p_0$ and $f(\sqrt{1/\theta},\sqrt{1/\theta})=\log\theta$.

Acknowledgements

This research was conducted while the authors visited SFB 343 'Diskrete Strukturen in der Mathematik' at the University of Bielefeld. The hospitality of the SFB and discussions held there with Rudolf Ahlswede and Ron Aharoni are gratefully acknowledged.

References

1. R. Ahlswede and G. Simonyi, On the optimal structure of recovering set pairs in lattices: the sandglass conjecture, *Discr. Math.*, **128** (1994), 389–394.
2. I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Academic Press, New York, 1982.
3. P. Frankl and Z. Füredi, Union-free hypergraphs and probability theory, *Europ. J. Combin.*, **5** (1984), 127–131.
4. G. O. H. Katona, Extremal problems for hypergraphs, *Math. Ctr. Tracts*, **56** (1974), 13–42.
5. G. Simonyi, On write-unidirectional memory codes, *IEEE Trans. Inform. Theory* **IT-35** (1989), 663–669.

Received 28 March 1993 and accepted 13 June 1994

Ron Holzman†
Department of Applied Mathematics and Computer Science,
The Weizmann Institute of Science, Rehovot 76100, Israel

E-mail: holzman@tx.technion.ac.il

János Körner
Department of Mathematics, Bologna University,
Piazza di Porta S. Donato 5, 40127 Bologna, Italy

E-mail: korner@dsi.uniroma1.it

† Incumbent of the Robert Edward and Roselyn Rich Manson Career Development Chair. Current address: Department of Mathematics, Technion—Israel Institute of Technology, Haifa 32000, Israel.