Skewincidence

Gérard Cohen, *Senior Member, IEEE*, Emanuela Fachini, and János Körner

***Abstract*—We introduce a new class of problems lying halfway between questions about graph capacity and intersection. We say that two binary sequences $\mathbf{x}$ and $\mathbf{y}$ of the same length have a skewincidence if there is a coordinate i for which $x_i = y_{i+1} = 1$ or vice versa. We give relatively close bounds on the maximum number of binary sequences of length n any pair of which has a skewincidence. A systematic study of these problems helps to understand the mathematical difficulties to solve zero-error problems in information theory.**

***Index Terms*—Asymptotic combinatorics, zero-error capacity.**

I. Information-Theoretic Combinatorics

The reader might wonder whether the topic of our paper belongs to information theory. One might argue that information theory is the collection of problems and results concerning information transmission. We believe, however, that the scope of information theory should be larger, at least from a mathematical point of view.

Undoubtedly, the problem of graph capacity, Shannon's mathematical formulation of the zero-error capacity of a discrete, memoryless, and stationary channel, belongs to information theory. Yet, the traditional methods of the theory don't seem to work here, and it is very likely that no capacity formula in terms of the usual information measures exists. Thus, it becomes important to look at this problem as mathematicians are used to do, varying some aspects of it and exploring how these variations affect the solution. We believe that the systematic study of all these variations not only leads to an exciting new field in asymptotic combinatorics with plenty of applications in information theory, but we do hope that this kind of asymptotic combinatorics will contribute to the solution of Shannon's beautiful and important problem.

II. Introduction

We consider binary relations of strings of some fixed finite length n from a finite alphabet (or strings representing the linear orders of $[n]$). We are interested in the maximum number of strings any two of which are in the given relation. Most problems of this kind belong to one of two well-investigated classes of opposite nature.

Intersection problems have been studied in extremal combinatorics. The first of these goes back to the seminal paper of Erdös, Ko, and Rado [6]. These authors say that the binary strings $\mathbf{x} = x_1x_2\ldots x_n$ and $\mathbf{y} = y_1y_2\ldots y_n$ intersect if for some coordinate i they have $x_i = y_i = 1$. They then determine the maximum number of pairwise intersecting binary strings of length n and weight k; here the weight of a string is its number of 1's. (In other words, they determine the largest stable sets in the Kneser graph whose vertices are the elements of $\binom{[n]}{k}$ and whose edges are the vertex pairs corresponding to disjoint pairs of sets.) They show that any optimal configuration has the same structure; it consists of all those strings that have a 1 in the same fixed position. In other words, these sequences have a fixed projection on some coordinate. Such a structure is often called a *kernel structure* and it is the natural candidate solution for all the intersection problems. The reason for this seems to be the fact that the relation underlying the problem is a *similarity relation*. We will say that a binary relation for strings of the same length is a similarity relation if it is reflexive and locally verifiable, meaning that if some projections of two strings are in this relation then this implies that so are the strings themselves. For more on this, we refer to [4] and [5].

Capacity problems originate in the fundamental paper of Claude Shannon on zero-error capacity of the discrete memoryless stationary channel [12] and come from information theory. We will say that a binary relation for strings of the same length is a difference relation if the relation is irreflexive and locally verifiable [7]. For easy reference, we will say that two sequences are very different if they are in the given difference relation. For a fixed length, one is interested, as before, in the maximum number of pairwise very different sequences. The classical example is Shannon's graph capacity [12] and has been generalized in a series of papers; for more on this we refer to [3] and the survey [9]. Unlike for intersection problems, here there is no natural conjecture for the optimal constructions and most problems of this kind remain wide open.

Both of these groups of problems have been generalized in recent work to permutations of $[n]$. For intersection problems on permutations we refer to [5]. Capacity problems for permutations have been introduced in [8]; for further developments we cite [2]. In order to introduce our new problems it will be interesting to recall the first capacity problem on permutations from [8]. We call two permutations of $[n]$ *colliding* if they map some $i \in [n]$ into two consecutive integers. Let us denote by $T(n)$ the maximum cardinality of a set of pairwise colliding permutations of $[n]$. Körner and Malvenuto [8] conjecture that $T(n)$ equals the middle binomial coefficent $\binom{n}{\lfloor \frac{n}{2} \rfloor}$. This conjecture is still open; for the best bounds we refer to [2].

Our starting point in the present work is the problem about colliding permutations. We note that if two permutations, ρ and σ are colliding, then their inverses are skewincident. In fact, the collision relation means that for some $j \in [n]$ we have

$$|\rho(j) - \sigma(j)| = 1.$$

Manuscript received March 23, 2011; revised June 28, 2011; accepted July 05, 2011. Date of current version November 11, 2011.

G. Cohen is with the ENST, France (e-mail: cohen@telecom-paristech.fr).

E. Fachini and J. Körner are with the "La Sapienza" University of Rome, Rome, Italy (e-mail: fachini@di.uniroma1.it; korner@di.uniroma1.it).

Communicated by I. F. Blake, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2011.2161753

Suppose without loss of generality that $\sigma(j)=\rho(j)+1$. Denoting $i:=\rho(j)$ we have $\rho^{-1}(i)=\sigma^{-1}(i+1)=j$ meaning that there is a skewincidence between the strings describing the two permutations (in form of linear orders of $[n]$); we find in them the same symbol j in adjacent positions. The resulting relation of coincidence is irreflexive for permutations. For sequences with repetitions such as long strings from a finite alphabet the analogous relation is not irreflexive any more. In fact, it is neither reflexive nor irreflexive and as our initial findings show the optimal solution has a somewhat unusual behaviour. Our results are asymptotic. Logarithms and exponentials are to the base 2.

III. Results

Let us fix a natural number n and consider the set $\{0,1\}^n$ of the binary strings of length n. We say that the sequences $\mathbf{x}\in\{0,1\}^n$ and $\mathbf{y}\in\{0,1\}^n$ have a *skew coincidence* (abbreviated as skewincidence) if for some coordinate $i\in[n-1]$ we have either $x_i=y_{i+1}=1$ or $x_{i+1}=y_i=1$. Let us denote by $M(n)$ the maximum number of binary strings of length n any two of which have a skewincidence. We have the following result.

Theorem 1:

$$2^n-2^{0.98n}\le M(n)\le 2^n-2^{0.69n}.$$

for n sufficiently large.

This implies the following.

Corollary 1:

$$\lim_{n\to\infty}\frac{M(n)}{2^n}=1.$$

Proof: To prove the upper bound, let us consider the set $\mathsf{F_n}\subseteq\{0,1\}^\mathsf{n}$ of those binary sequences that do not contain a 1 in consecutive positions. It is well known that

$$|\mathsf{F}_n|=f_n$$

where $f_1=2$, $f_2=3$, $f_n=f_{n-1}+f_{n-2}$ meaning that $\{f_n\}_{n=1}^{\infty}$ is the standard Fibonacci sequence. Given two binary sequences $\mathbf{x}$ and $\mathbf{y}$ we say that $\mathbf{x}\le\mathbf{y}$ if $\mathbf{x}=x_1x_2\dots x_n$, $\mathbf{y}=y_1y_2\dots y_n$, and $x_i\le y_i$ for every $i\in[n]$. We say that $\mathbf{x}$ and $\mathbf{y}$ are comparable if $\mathbf{x}\le\mathbf{y}$ or vice versa. Consider now a set B of pairwise skewincident binary strings from $\{0,1\}^n$. It is obvious that if two strings belong to the intersection of B and $\mathsf{F_n}$ then they cannot be comparable. Hence we see that the elements of $\mathsf{B}\cap\mathsf{F_n}$ are the characteristic vectors of a Sperner family in $[n]$. Let m_n be the largest cardinality of a Sperner family of subsets of $[n]$ whose characteristic vectors are in $\mathsf{F_n}$. If we drop the last coordinate of the characteristic vectors, these remain distinct because if two vectors are incomparable, then they differ in at least two coordinates. Further, the shortened strings of length $n-1$ clearly belong to $\mathsf{F_{n-1}}$. This yields

$$m_n\le f_{n-1}\le\beta f_n$$

for some constant $\beta<1$ and every natural n, where the last inequality follows from the monotonicity and the well-known asymptotics of the standard Fibonacci sequence, according to which $\frac{f_{n-1}}{f_n}$ converges to $\frac{2}{1+\sqrt{5}}<1$. Observing that $f_n\ge 2^{0.694n}$ for suffficiently large n, we conclude that

$$|\bar{\mathsf{B}}|\ge f_n-m_n\ge(1-\beta)f_n\ge(1-\beta)2^{0.694n}>2^{0.69n}$$

for n large enough. Hence

$$|\mathsf{B}|\le 2^n-2^{0.69n}$$

for sufficiently large n, as claimed.

To prove the lower bound we shall exhibit a set of pairwise skewincident sequences. The weight $w(\mathbf{x})$ of a binary string $\mathbf{x}\in\{0,1\}^n$ is its number of 1's. In case of $\mathbf{x}=x_1x_2\dots x_n$ we have

$$w(\mathbf{x}):=\sum_{i=1}^{n}x_i.$$

The support set of a string $\mathbf{x}\in\{0,1\}^n$ is the set $\mathsf{S}(\mathbf{x})\subseteq[n]$ of positions i in which $x_i=1$. In other words, $w(\mathbf{x})=|\mathsf{S}(\mathbf{x})|$. The influence $\mathbf{i}(\mathbf{x})$ of string $\mathbf{x}$ is a binary string of the same length that has a 1 in position $j\in[n]$ if and only if either $x_{j-1}=1$ and/or $x_{j+1}=1$. We write

$$\gamma(\mathbf{x}):=w(\mathbf{x})+w(\mathbf{i}(\mathbf{x}))$$

and define the set $\mathsf{C}_n\subseteq\{0,1\}^n$ as

$$\mathsf{C}_n:=\{\mathbf{x}\,|\,\gamma(\mathbf{x})>n\}.$$

We claim that any two distinct elements of C_n are skew coincident. In fact, consider $\mathbf{x}\in\mathsf{C}_n$ and $\mathbf{y}\in\mathsf{C}_n$. Then we have

$$w(\mathbf{x})+w(\mathbf{i}(\mathbf{x}))>n \text{ and } w(\mathbf{y})+w(\mathbf{i}(\mathbf{y}))>n$$

hence

$$w(\mathbf{x})+w(\mathbf{i}(\mathbf{x}))+w(\mathbf{y})+w(\mathbf{i}(\mathbf{y}))>2n. \tag{1}$$

If $\mathbf{x}$ and $\mathbf{y}$ were not skew coincident, the sets $\mathsf{S}(\mathbf{x})$ and $\mathsf{S}(\mathbf{i}(\mathbf{y}))$ would be disjoint, implying that

$$w(\mathbf{x})+w(\mathbf{i}(\mathbf{y}))\le n$$

and likewise

$$w(\mathbf{y})+w(\mathbf{i}(\mathbf{x}))\le n$$

yielding

$$w(\mathbf{x})+w(\mathbf{i}(\mathbf{y}))+w(\mathbf{y})+w(\mathbf{i}(\mathbf{x}))\le 2n$$

in contradiction with (1).

To lower bound the cardinality of C_n we shall use a well-known concentration inequality of McDiarmid [11]. Let the random variable $X^n=X_1X_2\dots X_n$ be uniformly distributed on $\{0,1\}^n$. Then the variables X_i, $i\in[n]$ are totally independent and uniformly distributed over $\{0,1\}$. To prove our lower bound, it suffices to show that

$$\Pr\{\gamma(X^n)\le n\}\le 2^{-0.02n} \tag{2}$$

Let $\alpha_i(\mathbf{x})$ denote the i'th coordinate of the vector $\mathbf{i}(\mathbf{x})$. We write

$$\gamma_i(\mathbf{x}) := x_i + \alpha_i(\mathbf{x}).$$

Hence

$$\gamma(X^n) = \sum_{i=1}^{n} \gamma_i(X^n).$$

The function $\gamma(\mathbf{x})$ defined on $\{0,1\}^n$ satisfies the Lipschitz condition that given any two arguments $\mathbf{x}$ and $\mathbf{y}$ differing only in the ith coordinate we have, for every $i \in [n]$

$$|\gamma(\mathbf{x}) - \gamma(\mathbf{y})| \leq 3.$$

This is true because for such an $\mathbf{x}$ and $\mathbf{y}$ the values of $w(\mathbf{x})$ and $w(\mathbf{y})$ differ by 1 while the values of $w(\mathbf{i}(\mathbf{x}))$ and $w(\mathbf{i}(\mathbf{y}))$ cannot differ by more than 2. Let us now calculate the expected value of the random variable $\gamma(X^n)$. By the linearity of the expected value and the definition of γ_i we have

$$\mathbb{E}\gamma(X^n) = \sum_{i=1}^{n} \mathbb{E}\gamma_i(X^n) = \sum_{i=1}^{n} \left[\mathbb{E}X_i + \mathbb{E}\alpha_i(X^n)\right]. \qquad (3)$$

Since, for every i, both X_i and $\alpha_i(X^n)$ take only the values 0 and 1, we have that

$$\mathbb{E}X_i + \mathbb{E}\alpha_i(X^n) = \Pr\{X_i = 1\} + \Pr\{\alpha_i(X^n) = 1\}.$$

Since X_i is uniformly distributed, for every $i \in [n]$

$$\Pr\{X_i = 1\} = \frac{1}{2}$$

Also, since the X_i are totally independent, and because $\alpha_i(X^n) = 0$ if and only if $X_{i-1} = X_{i+1} = 0$, for $1 < i < n$ we see that

$$\Pr\{\alpha_i(X^n) = 1\} = \frac{3}{4}$$

while $\Pr\{\alpha_i(X^n) = 1\} = \frac{1}{2}$ else. Thus we obtain

$$\mathbb{E}\gamma(X^n) = \frac{5n}{4} - \frac{1}{2}$$

and

$$\Pr\left\{X^n \in \overline{\mathsf{C}_n}\right\} = \Pr\{\gamma(X^n) \leq n\} \leq \Pr\left\{|\gamma(X^n) - \mathbb{E}(\gamma(X^n))| > \frac{n}{4} - \frac{1}{2}\right\}.$$

Upper bounding the right-most probability by [11, eq. (13) in Theorem 3.1], we see that for large enough n

$$\Pr\left\{X^n \in \overline{\mathsf{C}_n}\right\} \leq \exp\left(-\frac{2n^2}{(\ln 2)\cdot 144n}\right) \leq \exp(-0.02n).$$

(We recall that exponentials are to the base 2.) □

Remark: It is easy to see that the set of strings used to establish the lower bound does not have maximum cardinality. In fact, it is not even maximal. To see this, observe that, for every n, the two sequences in which the two binary digits alternate can both be added to the construction we have specified for our lower bound. However, even this augmented set is not maximal for large enough string lengths.

IV. Generalizations

The question about skewincidence can be generalized to a problem about subgraphs of an arbitrary finite graph. We will say that two subsets of the vertex set of a graph are *neighbors* if they contain two respective vertices that are adjacent in the graph. Note that a subset may or may not be its own neighbor. Let us denote by $M(G)$ the maximum number of distinct subsets of the vertex set of the graph such that any two of them are neighbors. For many graphs we will be able to completely determine this number. In particular, this is the case for complete bipartite graphs. Complete multipartite graphs are equally easy to treat so that we omit the details. In case of other graphs things can be much more complicated. In particular, it is easy to see that $M(n) = M(P_n)$ where P_n is the path of n vertices. In what follows, a stable set in a graph is a set of pairwise nonadjacent vertices.

Proposition 1: Let $K_{m,n}$ be the complete bipartite graph whose maximal stable(edge-free) sets have m and n vertices, respectively. Then

$$M(K_{m,n}) = (2^m - 1)(2^n - 1) + 2.$$

More generally, if $K_{n_1,n_2,\ldots n_r}$ is a complete multipartite graph with disjoint stable sets of cardinality $n_1, n_2, \ldots n_r$, respectively, we have

$$M\left(K_{n_1,n_2,\ldots n_r}\right) = 2^{\sum_{i=1}^{r} n_i} - \sum_{i=1}^{r} 2^{n_i} + 2r - 1.$$

Proof: It is obvious in the bipartite case that a family of subsets with the desired property cannot contain more than one subset of any of the two maximal stable sets. In the r-partite case for $r > 2$, exactly in the same way, a family as required cannot contain more than one subset of any of the maximal stable sets. On the other hand, any subset having nonempty intersection with at least two partite classes will be the neighbor of any other nonempty subset. □

All the above can be considered as special cases of a single more general problem other special cases of which contain the original Shannon setup of graph capacity.

Let F be a graph with vertex set $\mathbb{N}$ and let be G an arbitrary, not necessarily finite graph. Consider, for every $n \in \mathbb{N}$ the family of all the mappings $f : [n] \to V(G)$. We will say that two of these mappings, a and b, form an *attractive couple* if there exist two, not necessarily distinct numbers $i \in [n]$ and $j \in [n]$ such that i and j are adjacent in F while $a(i)$ and $b(j)$ are adjacent in G. We are interested in determining the largest cardinality $M(F, G, n)$ of a subset of pairwise attractive mappings from $[n]$ to $V(G)$.

If F is the all-loops graph and G an arbitrary simple graph, then $M(F, G, n)$ is exponential in n and the (always existing) limit of $\sqrt[n]{M(F, G, n)}$ is the Shannon capacity of the graph G. (Notice, however, that our formulation of Shannon's problem is equivalent to, but different from that in [12].) If F is the semi-infinite path and G is a graph with two vertices and a loop as its only edge, we get back the problem of skewincidence. Its immediate generalizations are obtained if F is arbitrary while G remains the same one-edge graph as for the skewincidence problem.

If G also has $\mathbb{N}$ as its vertex set then one can restrict attention to the subset of bijective mappings from $[n]$ onto itself. This leads, in case of the all-loop graph in the role of F to the concept of permutation capacity.

V. A Sperner-Type Problem

As a byproduct from the proof of the Theorem, we get the following extremely simple sounding problem in classical extremal set theory. Let F_n be the set of all the binary sequences of length n without 1's in consecutive positions. (This is the already mentioned classical example for the standard Fibonacci sequence.) We consider these binary sequences as the characteristic vectors of subsets of the set $[n]$ in the usual manner and ask for the maximum cardinality of a Sperner family they contain.

In our proof a very weak upper bound on this cardinality was sufficient. The present problem is interesting inasmuch no classical proof for Sperner's theorem [13] seems to be suitable to solve it.

VI. Conclusion

The zero-error capacity of the discrete memoryless channel stays out as the most well-known unsolved mathematical problem in information theory, and this despite the concerted effort of such brilliant mathematicians as Shannon [12], Lovász [10] or Alon [1]. We believe that it helps to understand the true reason of the difficulty of this problem if we explore all its reasonable and mathematically appealing variations.

References

[1] N. Alon, "Combinatorial reasoning in information theory," in *Proc. IEEE Inf. Theory Soc. Newsl.*, 2009, vol. 59, pp. 10–13.

[2] G. Brightwell, G. Cohen, E. Fachini, M. Fairthorne, J. Körner, G. Simonyi, and Á. Tóth, "Permutation capacities of families of oriented infinite paths," *SIAM J. Discr. Math.*, vol. 2, no. 24, pp. 441–456, 2010.

[3] G. Cohen, J. Körner, and G. Simonyi, R. M. Capocelli, Ed., "Zero-error capacities and very different sequences," in *Proc. Sequences. Combinator., Secur. Transmiss., Adv. Int. Workshop on Sequences*, Positano, Italy, Jun. 1988, pp. 144–155.

[4] F. R. K. Chung, R. L. Graham, P. Frankl, and J. B. Shearer, "Some intersection theorems for ordered sets and graphs," *J. Combin. Theory Ser. A*, vol. 43, pp. 23–37, 1986.

[5] D. Ellis, E. Friedgut, and H. Pilpel, "Intersecting families of permutations," *J. AMS*, vol. 24, pp. 649–682, 2011.

[6] P. Erdös, C. Ko, and R. Rado, "Intersection theorems for systems of finite sets," *Quart. J. Math. Oxford Ser. 2*, vol. 12, pp. 313–320, 1961.

[7] E. Fachini and J. Körner, "Forbiddance and capacity," *Graphs Combinator.*, vol. 4, no. 27, pp. 495–503, 2011.

[8] J. Körner and C. Malvenuto, "Pairwise colliding permutations and the capacity of infinite graphs," *SIAM J. Discr. Math.*, vol. 20, pp. 203–212, 2006.

[9] J. Körner and A. Orlitsky, "Zero-error information theory," *IEEE Trans. Inf. Theory*, vol. 44, pp. 2207–2229, 1998.

[10] L. Lovász, "On the Shannon capacity of a graph," *IEEE Trans. Inf. Theory*, vol. 25, pp. 1–7, 1979.

[11] C. McDiarmid, "Concentration Probabilistic methods for algorithmic discrete mathematics," in *Algorithms Combin.*. Berlin: Springer, 1998, vol. 16, pp. 195–248.

[12] C. E. Shannon, "The zero-error capacity of a noisy channel," *IRE Trans. Inf. Theory*, vol. 2, pp. 8–19, 1956.

[13] E. Sperner, "Ein Satz über untermengen einer endlichen menge," *Math. Z.*, vol. 27, pp. 544–548, 1928.

Gérard Cohen (SM'87) received the Engineer's degree from Ecole Nationale Superieure des Telecommunications (ENST) in 1973 and Doctorat d'Etat es Sciences in mathematics in 1980 from University Paris 6.

He is currently Professor at ENST and has taught at various Universities, including Ecole Normale Superieure de Paris (Ulm), Paris 6 and supervised many Ph.D. degree students. His main fields of interest are coding theory, combinatorics, information theory, and cryptography. He has written more than 130 papers in international Journals and coauthored three books.

Dr. Cohen is Chairman and founder of the IEEE French Chapter in Information Theory in 1993. He is an Associate Editor of the IEEE Transactions on Information Theory.

Emanuela Fachini received the degree in mathematics from the University of Naples in 1975.

She joined the Department of Computer Science, Sapienza University of Rome, Italy, in 1997. From 1976 to 1984, she was a research associate with the Dipartimento di Informatica e Applicazioni, University of Salerno, where she became an Associate Professor in 1985 and Full Professor in 1987. She also acted first as Director of the Dipartimento di Informatica and Applicazioni and then of the Degree Program in information science. In 1990, she became a Full Professor with the Dipartimento di Informatica Sistemi e Produzione, University of Rome "Tor Vergata." Her research interests are in automata theory and in combinatorics.

János Körner was born in Budapest, Hungary, on November 30, 1946. He received the Degree in mathematics from the Eötvös University, Budapest, in 1970.

After graduation, he joined the Mathematical Institute of the Hungarian Academy of Sciences, where he worked until he left Hungary, in 1989. From 1981 to 1983, he was on leave at AT&T Bell Laboratories, Murray Hill, NJ. At present, he is a Professor with the Department of Computer Science, Sapienza University of Rome, Italy. Jointly with I. Csiszár, he is the author of the book *Information Theory: Coding Theorems for Discrete Memoryless Systems*, now at its second revised edition with Cambridge University Press. His main research interests are in combinatorics, information theory and their interplay.

Dr. Körner served as Associate Editor for Shannon Theory of the IEEE Transactions on Information Theory from 1983 to 1986. He is an external member of the Hungarian Academy of Sciences.