On Approximate Inclusion-Exclusion

Andreas Klein[*] and Klaus Metsch[†]

The inclusion-exclusion formula states

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \ldots - (-1^n)|A_1 \cap \ldots \cap A_n| \ .$$

Obviously every term on the right-hand side is needed to determine the size of the union. At this point we can ask if it is possible to give an approximate inclusion-exclusion formula. More formally we ask:

Given integers m, n with $m < n$ and sets $A_1, \ldots, A_n$ and $B_1, \ldots, B_n$ where not all B_i are empty and where

$$\left|\bigcap_{i \in S} A_i\right| = \left|\bigcap_{i \in S} B_i\right|$$

for every subset $S \subseteq \{1, \ldots, n\}$ such that $|S| < m$, what is the smallest (or largest) possible value for the fraction

$$\frac{|A_1 \cup \ldots \cup A_n|}{|B_1 \cup \ldots \cup B_n|}?$$

In [1] N. Linial and N. Nisan use linear programming to reduce this question to questions in approximation theory and in particular to the theory of Chebyshev polynomials. Their bound is nearly optimal for $m \leq \sqrt{n}$, but for larger m the bound gets worse. In this paper we give an explicit bound for $m = n - 2$ and improve the asymptotic bound for $n = n - d$, d fixed.

As an application we will construct a contrast optimal $(n-1)$-out-of-n visual cryptography scheme.

References

[1] N. Linial and N. Nisan. Approximate Inclusion-Exclusion. *Combinatorica*, 10(4):349–365, 1990.

[2] Moni Naor and Adi Shamir. Visual cryptography. In Alfredo De Santis, editor, *Advances in cryptology - EUROCRYPT '94*, volume 950 of *Lect. Notes Comput. Sci.*, pages 1–12. Springer-Verlag, 1995.

[*] Fachbereich für Mathematik und Informatik, Heinrich Plett Str. 40, D-34132 Kassel, Germany

[†] Mathematisches Institut, Arndtstrasse 2, D-35392 Giessen, Germany