On approximate inclusion-exclusion

Andreas Klein* Klaus Metsch

Abstract

The inclusion-exclusion formula expresses the size of the union of a family of sets in terms of the sizes of intersections of all subfamilies. In [2] N. Linial and N. Nisan use linear programming to approximate the size of the union when the intersection sizes are known only for certain subfamilies. In this article we use purely combinatorial methods to generalize some of their results. As an application we will construct a contrast optimal $(n-1)$-out-of-n visual cryptography scheme.

Keywords: inclusion-exclusion formula, visual cryptography

MSC 2000: 05A20, 68P25

1. Introduction

The inclusion-exclusion formula states that

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

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

*The research of the author takes place within the project "Linear codes and cryptography" of the Fund for Scientific Research Flanders (FWO-Vlaanderen) (Project nr. G.0317.06), and is supported by the Interuniversitary Attraction Poles Programme-Belgian State-Belgian Science Policy: project P6/26-Bcrypt.

ACADEMIA PRESS
UNIVERSITEIT GENT

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

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

In [2] 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 exact bound for $m = n - 2$ and improve the asymptotic bound for $m = n - d$, d fixed. The results we find have applications in visual cryptography. More results for small m can be found in [1].

2. The case $m = n - 1$

We start with the case $m = n - 1$. This case was solved in [2] using linear programming methods. Here we present a more elementary purely combinatorial proof. Besides being interesting for itself, the proof is a good warm up for the more difficult case $m = n - 2$.

Theorem 2.1 (see [2, Theorem 3]). *Let $A_1, \ldots, A_n$ and $B_1, \ldots, B_n$ be two collections of sets satisfying*

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

for all proper subsets S of $\{1, \ldots, n\}$. Then

$$\frac{\left|\bigcup_{i=1}^n B_i\right| - \left|\bigcup_{i=1}^n A_i\right|}{\left|\bigcup_{i=1}^n B_i\right|} \leq \frac{1}{2^{n-1}}\,.$$

Proof. We prove by induction on n that the conditions

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

ACADEMIA PRESS
UNIVERSITEIT GENT

for all $S \subsetneq \{1, \ldots, n\}$ and the condition

$$\left|\bigcup_{i=1}^{n} A_i\right| + k = \left|\bigcup_{i=1}^{n} B_i\right|$$

with $k > 0$ imply that

$$\left|\bigcup_{i=1}^{n} B_i\right| \geq k2^{n-1}\,.$$

For $n = 1$ this is trivial. Now suppose that the theorem holds for n and let the sets $A_1, \ldots, A_{n+1}$ and $B_1, \ldots, B_{n+1}$ satisfy

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

for all $S \subsetneq \{1, \ldots, n+1\}$ and

$$\left|\bigcup_{i=1}^{n+1} A_i\right| + k = \left|\bigcup_{i=1}^{n+1} B_i\right|.$$

The collections $A_i' = A_i \backslash A_{n+1}$ and $B_i' = B_i \backslash B_{n+1}$ satisfy $|\bigcup_{i=1}^{n} A_i'| + k = |\bigcup_{i=1}^{n} B_i'|$ and for every proper subset $S \subsetneq \{1, \ldots, n\}$ we have

$$\begin{aligned}\left|\bigcap_{i\in S} A_i'\right| &= \left|\bigcap_{i\in S} A_i\right| - \left|\bigcap_{i\in S} A_i \cap A_{n+1}\right| \\ &= \left|\bigcap_{i\in S} B_i\right| - \left|\bigcap_{i\in S} B_i \cap B_{n+1}\right| = \left|\bigcap_{i\in S} B_i'\right|.\end{aligned}$$

Thus the collections A_i', B_i' satisfy the induction hypothesis, i.e. we have $|\bigcup_{i=1}^{n} B_i'| \geq k2^{n-1}$.

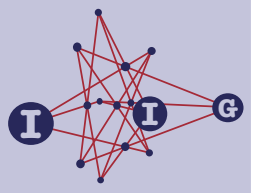
On the other hand, we have the collections $A_i'' = A_i \cap A_{n+1}$ and $B_i'' = B_i \cap B_{n+1}$. Since

$$\begin{aligned}&\left|\bigcup_{i=1}^{n} A_i\right| = \left|\bigcup_{i=1}^{n} B_i\right| \\ \Longleftrightarrow\ &\left|\bigcup_{i=1}^{n} A_i'\right| + \left|\bigcup_{i=1}^{n} A_i''\right| = \left|\bigcup_{i=1}^{n} B_i'\right| + \left|\bigcup_{i=1}^{n} B_i''\right|\end{aligned}$$

and $|\bigcup_{i=1}^{n} A_i'| + k = |\bigcup_{i=1}^{n} B_i'|$ we find that the collections A_i'' and B_i'' satisfy the induction hypothesis with $|\bigcup_{i=1}^{n} B_i''| + k = |\bigcup_{i=1}^{n} A_i''|$. Thus $|B_{n+1}| = |A_{n+1}| \geq |\bigcup_{i=1}^{n} A_i''| \geq k2^{n-1}$. This proves

$$\left|\bigcup_{i=1}^{n+1} B_i\right| = \left|\bigcup_{i=1}^{n} B_i'\right| + |B_{n+1}| \geq k2^{n-1} + k2^{n-1} = k2^n$$

ACADEMIA PRESS
UNIVERSITEIT GENT



as desired. □

This bound is sharp as the following example shows [3]: Let $\mathcal{P}(\{1,\dots,n\})$ be the power set of $\{1,\dots,n\}$. Choose $A_i \subseteq \mathcal{P}(\{1,\dots,n\})$ as the set of all subsets of $\{1,\dots,n\}$ that have even cardinality and contain i. Similarly $B_i \subseteq \mathcal{P}(\{1,\dots,n\})$ is set of all subsets of $\{1,\dots,n\}$ that have odd cardinality and contain i.

It is easy to check that $|\bigcap_{i\in S} A_i| = |\bigcap_{i\in S} B_i| = 2^{n-1-|S|}$ for each proper subset S of $\{1,\dots,n\}$. Furthermore $|\bigcup_{i=1}^n A_i| = 2^{n-1}-1$ and $|\bigcup_{i=1}^n B_i| = 2^{n-1}$, i.e. the bound in Theorem 2.1 is sharp.

3. The case $m = n - 2$

For $k, x \in \mathbb{Z}$ and $k \geq 0$ let $S_n(k,x)$ denote the minimal size of $|\bigcup_{i=1}^n B_n|$ given

(1a) $|\bigcap_{i\in S} A_i| = |\bigcap_{i\in S} B_i|$ for all S with $|S| \leq n-2$,

(2a) $|\bigcap_{i=1}^n A_i| = |\bigcap_{i=1}^n B_i| - (-1)^n x$,

(3a) $|\bigcup_{i=1}^n A_i| + k = |\bigcup_{i=1}^n B_i|$.

As in the previous section we want to determine the largest possible value of

$$\frac{|\bigcup_{i=1}^n B_i| - |\bigcup_{i=1}^n A_i|}{|\bigcup_{i=1}^n B_i|} = \frac{k}{|\bigcup_{i=1}^n B_i|}.$$

For this we have to minimize $\frac{S_n(k,x)}{k}$, provided $k \neq 0$.

3.1. A recursion formula for the upper bound

The first step is to prove a recursion formula for $S_n(k,x)$. For simplicity we extend the definition of $S_n(k,x)$ to negative integers k by putting

$$S_n(k,x) := S_n(-k,-x)$$

for $k < 0$. Thus, for $k < 0$, the number $S_n(k,x)$ can be interpreted as the size of $|\bigcup_{i=1}^n A_n|$.

Lemma 3.1. *Let $n \geq 2$, then*

$$S_{n+1}(k,x) \geq \min\{S_n(k,x+y) + S_n(k+y,x) \mid y \in \mathbb{Z}\}. \tag{1}$$

ACADEMIA PRESS
UNIVERSITEIT GENT

Proof. The proof is very similar to the proof of Theorem 2.1. It is sufficient to consider the case when $k \geq 0$. Suppose $A_1, \ldots, A_{n+1}$ and $B_1, \ldots, B_{n+1}$ are sets realizing $S_{n+1}(k, x)$, that is (1a), (2a) and (3a) are satisfied and $S_{n+1}(k, x) = |\bigcup_{i=1}^{n+1} B_i|$. Let y be the integer satisfying $|\bigcap_{i=1}^{n} A_i| = |\bigcap_{i=1}^{n} B_i| - (-1)^n y$.

The sets $A'_i = A_i \backslash A_{n+1}$ and $B'_i = B_i \backslash B_{n+1}$ satisfy the following conditions:

(1) $|\bigcap_{i\in S} A'_i| = |\bigcap_{i\in S} B'_i|$ for all S with $|S| \leq n-2$, since

$$\left|\bigcap_{i\in S} A'_i\right| = \left|\bigcap_{i\in S} A_i\right| - \left|\bigcap_{i\in S} A_i \cap A_{n+1}\right| = \left|\bigcap_{i\in S} B_i\right| - \left|\bigcap_{i\in S} B_i \cap B_{n+1}\right| = \left|\bigcap_{i\in S} B'_i\right|.$$

(2) $|\bigcap_{i=1}^{n} A'_i| = |\bigcap_{i=1}^{n} B'_i| - (-1)^n (y + x)$, since

$$\left|\bigcap_{i=1}^{n} A'_i\right| = \left|\bigcap_{i=1}^{n} A_i\right| - \left|\bigcap_{i=1}^{n+1} A_i\right| = \left|\bigcap_{i=1}^{n} B_i\right| - (-1)^n y - \left[\left|\bigcap_{i=1}^{n+1} B_i\right| - (-1)^{n+1} x\right].$$

(3) $|\bigcup_{i=1}^{n} A'_i| + k = |\bigcup_{i=1}^{n} B'_i|$, since

$$\left|\bigcup_{i=1}^{n} A'_i\right| + |A_{n+1}| + k = \left|\bigcup_{i=1}^{n+1} A_i\right| + k = \left|\bigcup_{i=1}^{n+1} B_i\right| = \left|\bigcup_{i=1}^{n} B'_i\right| + |B_{n+1}|$$

and $|A_{n+1}| = |B_{n+1}|$.

This proves $|\bigcup_{i=1}^{n} B'_i| = |(\bigcup_{i=1}^{n} B_i) \backslash B_{n+1}| \geq S_n(k, x + y)$.

Now we prove a lower bound for $|A_{n+1}| = |B_{n+1}|$. The sets $A''_i = A_i \cap A_{n+1}$, $B''_i = B_i \cap B_{n+1}$ satisfy

(1) $|\bigcap_{i\in S} A''_i| = |\bigcap_{i\in S} B''_i|$ for all S with $|S| \leq n-2$, since $|S|+1 \leq (n+1)-2$ and thus $|\bigcap_{i\in S} A''_i| = |\bigcap_{i\in S} A_i \cap A_{n+1}| = |\bigcap_{i\in S} B_i \cap B_{n+1}| = |\bigcap_{i\in S} B''_i|$,

(2) $|\bigcap_{i=1}^{n} A''_i| - (-1)^n x = |\bigcap_{i=1}^{n} B''_i|$, since $\bigcap_{i=1}^{n} A''_i = \bigcap_{i=1}^{n+1} A_i$,

(3) $|\bigcup_{i=1}^{n} A''_i| = |\bigcup_{i=1}^{n} B''_i| + k + y$, since

$$\left|\bigcup_{i=1}^{n} A''_i\right| + \left|\bigcup_{i=1}^{n} A'_i\right| = \sum_{S, n+1\notin S} (-1)^{|S|+1} \left|\bigcap_{i\in S} A_i\right| = \sum_{S, n+1\notin S} (-1)^{|S|+1} \left|\bigcap_{i\in S} B_i\right| + y = \left|\bigcup_{i=1}^{n} B''_i\right| + \left|\bigcup_{i=1}^{n} B'_i\right| + y.$$

ACADEMIA PRESS
UNIVERSITEIT GENT

We distinguish two cases. If $k+y \geq 0$ then $|B_{n+1}| = |A_{n+1}| \geq |\bigcup_{i=1}^{n} A_i''| \geq S_n(k+y,x)$. If $k+y \leq 0$ then $|A_{n+1}| = |B_{n+1}| \geq |\bigcup_{i=1}^{n} B_i''| \geq S_n(-k-y,-x)$, which is by definition equal to $S_n(k+y,x)$.

This proves $|\bigcup_{i=1}^{n+1} B_i| \geq S_n(k,x+y) + S_n(k+y,x)$. □

3.2. From discrete to continuous

In many aspects the discrete nature of the problem adds extra difficulties. Therefore we look at a continuous version of the inclusion-exclusion problem.

Let $(\Omega, \mathcal{A}, \mu)$ be an arbitrary measurable space and let $A_1, \ldots, A_n \in \mathcal{A}$ and $B_1, \ldots, B_n \in \mathcal{A}$ be collections of sets satisfying

(1b) $\mu(\bigcap_{i\in S} A_i) = \mu(\bigcap_{i\in S} B_i)$ for all S with $|S| \leq n-2$,

(2b) $\mu(\bigcap_{i=1}^{n} A_i) = \mu(\bigcap_{i=1}^{n} B_i) - (-1)^n x$,

(3b) $\mu(\bigcup_{i=1}^{n} A_i) + k = \mu(\bigcup_{i=1}^{n} B_i)$.

For $k, x \in \mathbb{R}$ and $k \geq 0$ we ask for the smallest possible value $\tilde{S}_n(k,x)$ for $\mu(\bigcup_{i=1}^{n} B_i)$ where the minimum is taken over all collections of sets in all finite measurable spaces. Again we extend the definition of $\tilde{S}_n(k,x)$ to negative k by putting $\tilde{S}_n(k,x) = \tilde{S}_n(-k,-x)$ for $k < 0$.

Lemma 3.1 also holds for the continuous problem and we get the recursion formula

$$\tilde{S}_{n+1}(k,x) \geq \min\{\tilde{S}_n(k,x+y) + \tilde{S}_n(k+y,x) \mid y \in \mathbb{R}\}. \tag{2}$$

The only difference to (1) is that k, x, y can take real values. The reason why the continuous case is easier than the discrete case is that we can restrict ourselves to symmetric collections.

Definition 3.2. A collection $A_1, \ldots, A_n$ is called symmetric if

$$\mu\Big(\bigcap_{i\in S} A_i\Big) = \mu\Big(\bigcap_{i\in S'} A_i\Big)$$

whenever $S, S' \subseteq \{1, \ldots, n\}$ and $|S| = |S'|$.

Lemma 3.3. *Let $(\Omega, \mathcal{A}, \mu)$ be a finite measurable space and let n be a natural number.*

(a) *Then there exists a finite measurable space $(\Omega', \mathcal{A}', \mu')$ with the following property:*

ACADEMIA PRESS
UNIVERSITEIT GENT

If $A_1, \ldots, A_n$ are elements of $\mathcal{A}$, then there exists elements $A'_1, \ldots, A'_n \in \mathcal{A}'$ such that for every k with $1 \leq k \leq n$ we have: If S is a k-subset of $\{1, \ldots, n\}$, then

$$\mu'\Big(\bigcap_{i \in S} A'_i\Big)$$

is equal to the average of the numbers $\mu(\bigcap_{i \in T} A_i)$ taken over all k-subsets T of $\{1, \ldots, n\}$.

(b) *If $A_1, \ldots, A_n$ and $B_1, \ldots, B_n$ are two collections that satisfy* (1b)–(3b)*, then the collections $A'_1, \ldots, A'_n$ and $B'_1, \ldots, B'_n$ constructed in (a), also satisfy* (1b)–(3b).

Proof. (a) Consider $n!$ mutually disjoint copies $(\Omega_\pi, \mathcal{A}_\pi, \mu_\pi)$ of $(\Omega, \mathcal{A}, \mu)$, one for each permutation π of $[n]$. There is a unique measure $\bar{\mu}$ on the union of these that extends each measure μ_π. Put $\mu' := \bar{\mu}/n!$. Let f_π be the canonical map from $\mathcal{A}$ to $\mathcal{A}_\pi$.

Consider any collection $A_1, \ldots, A_n$ of $(\Omega, \mathcal{A}, \mu)$. Let A'_i be the union of the sets $f_\pi(A_{\pi(i)})$ taken over all permutations π of $[n]$. This gives a collection $A'_1, \ldots, A'_n$ with the required property.

(b) Since $\mu(\bigcap_{i \in S} A_i) = \mu(\bigcap_{i \in S} B_i)$ for all S with $|S| \leq n-2$ also the averages must be equal, i.e. the collections $A'_1, \ldots, A'_n$ and $B'_1, \ldots, B'_n$ satisfy (1b). Since $\{1, \ldots, n\}$ is the only subset of size n of $\{1, \ldots, n\}$ we find

$$\mu\Big(\bigcap_{i=1}^{n} A_i\Big) = \mu'\Big(\bigcap_{i=1}^{n} A'_i\Big) \quad \text{and} \quad \mu\Big(\bigcap_{i=1}^{n} B_i\Big) = \mu'\Big(\bigcap_{i=1}^{n} B'_i\Big)\,;$$

hence the collections $A'_1, \ldots, A'_n$ and $B'_1, \ldots, B'_n$ satisfy (2b).

Use the inclusion-exclusion formula to compute $\mu(\bigcup_{i=1}^{n} A_i)$. It is invariant under a permutation π of the indices. Thus $\mu'(\bigcup_{i=1}^{n} A'_i) = \mu(\bigcup_{i=1}^{n} A_i)$ and thus the collections $A'_1, \ldots, A'_n$ and $B'_1, \ldots, B'_n$ satisfy (3b). □

If we have collections A_i and B_i satisfying (1b), (2b) and (3b), then we can use the preceding lemma to switch to symmetric collections A'_i and B'_i that satisfy (1b), (2b) and (3b) with the same numbers x and k and even with the same values of μ. This is the justification that $\tilde{S}_n(k, x)$ can be realized by symmetric collections.

Theorem 3.4. *For $n \geq 2$, we have*

$$\tilde{S}_{n+1}(k, x) = \tilde{S}_n(k, x + y) + \tilde{S}_n(k + y, x) \quad \textit{where} \quad y = -\frac{k + x}{n + 1}\,. \tag{3}$$

ACADEMIA PRESS
UNIVERSITEIT GENT

Proof. Without loss of generality we may assume $k \geq 0$.

Part 1: We show $\geq$ in (3).

Consider symmetric configurations $A_1, \ldots, A_{n+1}$ and $B_1, \ldots, B_{n+1}$ of sets minimizing $\tilde{S}_{n+1}(k, x)$. Using the symmetry and properties (1b), (2b), and (3b) we find

$$\mu\Big(\bigcap_{i=1}^{n} A_i\Big) = \mu\Big(\bigcap_{i=1}^{n} B_i\Big) + (-1)^n \frac{k+x}{n+1}\,.$$

Hence the value of y defined in the assertion is the one that was used in the proof of Lemma 3.1. The proof of Lemma 3.1 therefore shows the $\geq$-part of (3).

Part 2: We show $\leq$ in (3).

By induction there exist symmetric collections $A'_1, \ldots, A'_n$ and $B'_1, \ldots, B'_n$ realizing $\tilde{S}_n(k, x+y)$, that is satisfying (1b), (2b) and (3b) and such that $\mu'(\bigcup_{i=1}^n B'_i) = \tilde{S}_n(k, x+y)$. There also exist symmetric collections $B''_1, \ldots, B''_n$ and $A''_1, \ldots, A''_n$ realizing $\tilde{S}_n(k+y, x)$. Notice the order of the B''_i and the A''_i, which is meant as follows:

$$\begin{aligned}
&\mu''(\textstyle\bigcap_{i=1}^n B''_i) = \mu''(\bigcap_{i=1}^n A''_i) - (-1)^n x\,,\\
&\mu''(\textstyle\bigcup_{i=1}^n B''_i) + k + y = \mu''(\bigcup_{i=1}^n A''_i)\,,\\
&\mu''(\textstyle\bigcup_{i=1}^n B''_i) = \tilde{S}_n(k+y, x) \text{ if } k+y \leq 0\,, \text{ and}\\
&\mu''(\textstyle\bigcup_{i=1}^n A''_i) = \tilde{S}_n(k+y, x) \text{ if } k+y \geq 0\,.
\end{aligned}$$

Without loss of generality we may assume that $\Omega' = \bigcup_{i=1}^n A'_i \cup \bigcup_{i=1}^n B'_i$ and $\Omega'' = \bigcup_{i=1}^n A''_i \cup \bigcup_{i=1}^n B''_i$ are disjoint. The measures μ' on Ω' and μ'' on Ω'' induce a measure μ on $\Omega' \cup \Omega''$.

Define $A_i = A'_i \cup A''_i$ and $B_i = B'_i \cup B''_i$, $i = 1, \ldots, n$, $A_{n+1} = \bigcup_{i=1}^n A''_i \cup A$, and $B_{n+1} = \bigcup_{i=1}^n B''_i \cup B$ where A and B are chosen outside $\Omega' \cup \Omega''$ and the measure μ is extended in such a way that $\mu(A_{n+1}) = \mu(B_{n+1}) = \tilde{S}_n(k+y, x)$. Depending on the sign of $k+y$ we have either $\mu(A) = 0$ or $\mu(B) = 0$, i.e. we may choose $A = \emptyset$ or $B = \emptyset$. We will show that the so defined collections A_i and B_i satisfy (1b), (2b) and (3b) for $n+1$. Having done this, we can conclude that $\mu(\bigcup_{i=1}^{n+1} B_i) \geq S_{n+1}(k, x)$ and then the proof can be finished as follows:

$$\begin{aligned}
\tilde{S}_{n+1}(k, x) \leq \mu\Big(\bigcup_{i=1}^{n+1} B_i\Big) &= \mu\Big(\bigcup_{i=1}^{n} B'_i\Big) + \mu(B_{n+1})\\
&= \tilde{S}_n(k, x+y) + \tilde{S}_n(k+y, x)\,.
\end{aligned}$$

ACADEMIA PRESS
UNIVERSITEIT GENT

The properties (2b) and (3b) are easy to see. In fact we have

$$\mu\Big(\bigcup_{i=1}^{n+1} A_i\Big) + k = \mu\Big(\bigcup_{i=1}^{n} A'_i\Big) + \mu(A_{n+1}) + k$$
$$= \mu\Big(\bigcup_{i=1}^{n} B'_i\Big) + \mu(B_{n+1}) = \mu\Big(\bigcup_{i=1}^{n+1} B_i\Big)$$

and

$$\mu\Big(\bigcap_{i=1}^{n+1} A_i\Big) = \mu\Big(\bigcap_{i=1}^{n} A''_i\Big) = \mu\Big(\bigcap_{i=1}^{n} B''_i\Big) + (-1)^n x = \mu\Big(\bigcap_{i=1}^{n+1} B_i\Big) - (-1)^{n+1} x\,.$$

To see (1b) first notice that by construction we have

$$\mu\Big(\bigcap_{i\in S} A_i\Big) = \mu\Big(\bigcap_{i\in S} B_i\Big)$$

whenever $|S| \leq n-2$ or $|S| = n-1$ and $n+1 \in S$. The only difficult part is to prove the equality when $|S| = n-1$ and $n+1 \notin S$. In that case we have

$$\begin{aligned}\mu\Big(\bigcap_{i\in S} A_i\Big) &= \mu\Big(\bigcap_{i\in S} A'_i\Big) + \mu\Big(\bigcap_{i\in S} A''_i\Big)\\ &= \left[\mu\Big(\bigcap_{i\in S} B'_i\Big) + \frac{k+(x+y)}{n}\right] + \left[\mu\Big(\bigcap_{i\in S} B''_i\Big) - \frac{(k+y)+x}{n}\right]\\ &= \mu\Big(\bigcap_{i\in S} B_i\Big).\end{aligned}$$

This finishes the proof of (1b). □

3.3. Solving the recursion formula

In this section we derive an explicit formula for the recursion formula in Theorem 3.4. To that end we define the numbers

$$c_{n,i} := 2^{n-2} - \sum_{j=0}^{i-1} \binom{n-1}{j}, \quad -1 \leq i \leq n \tag{4}$$

(so $c_{-1} = c_0 = 2^{n-2}$), and the intervals

$$\begin{aligned} I_{n,-1} &:= (-\infty, 0]\\ I_{n,j} &:= \left[\frac{j}{n-j}, \frac{j+1}{n-j-1}\right] \qquad (0 \leq j \leq n-2)\\ I_{n,n-1} &:= [n-1, \infty)\,.\end{aligned} \tag{5}$$

ACADEMIA PRESS
UNIVERSITEIT GENT

Theorem 3.5. *The function $\tilde{S}_n(k,x)$ defined in the previous section satisfies*

$$\tilde{S}_n(k,x) = \begin{cases} c_{n,i}k - c_{n,i+1}x & \text{for } k>0 \text{ and } \frac{x}{k} \in I_{n,i}\,, \\ 2^{n-2}|x| & \text{for } k=0\,, \\ -c_{n,i}k + c_{n,i+1}x & \text{for } k<0 \text{ and } \frac{x}{k} \in I_{n,i}\,. \end{cases} \tag{6}$$

Proof. We may restrict ourselves to $k \geq 0$ since $\tilde{S}_n(-k,x) = \tilde{S}_n(k,-x)$ by definition. First note that

$$c_{n,i} - c_{n,i+1}\frac{i+1}{n-i-1} = c_{n,i+1} - c_{n,i+2}\frac{i+1}{n-i-1}$$

and thus the function on the right hande side of (6) is well-defined. We prove (6) using induction on $n \geq 2$.

To determine $\tilde{S}_2(k,x)$, we search sets A_1, A_2, B_1, B_2 with $\mu(A_1 \cap A_2) + x = \mu(B_1 \cap B_2)$ and $\mu(A_1 \cup A_2) + k = \mu(B_1 \cup B_2)$. It is easy to see that this implies

$$\mu(B_1 \cup B_2) \geq \max\{x,k\}\,.$$

Also, if $x<0$, then $\mu(A_1 \cup A_2) \geq \mu(A_1 \cap A_2) \geq -x$ and thus $\mu(B_1 \cup B_2) \geq k-x$. Moreover, equality can be obtained easily. For example, if $x > k \geq 0$, choose sets satisfying $B_1 = B_2$ and $A_2 = \emptyset$ and such that $\mu(B_i) = x$, $\mu(A_1) = x-k$ and $\mu(A_2) = 0$. Thus for $k \geq 0$ we have

$$\tilde{S}_2(k,x) = \begin{cases} k-x & \text{for } x \leq 0\,, \\ k & \text{for } 0 \leq x \leq k\,, \\ x & \text{for } k \leq x\,, \end{cases}$$

which proves (6) for $n=2$.

For the induction step assume now that $n \geq 3$. If $k=0$ we may assume without loss of generality $x \geq 0$. In this case the recursion formula (3) gives

$$\begin{aligned} \tilde{S}_{n+1}(0,x) &= \tilde{S}_n\Big(0, \frac{n}{n+1}x\Big) + \tilde{S}_n\Big(-\frac{x}{n+1}, x\Big) \\ &= 2^{n-2}\frac{n}{n+1}x + \Big(c_{n,-1}\frac{x}{n+1} + c_{n,0}x\Big) \\ &= 2^{n-1}x \end{aligned}$$

as desired. Finally consider the case when $n \geq 3$ and $k>0$. Put $y = -\frac{k+x}{n+1}$. Using

$$\frac{x+y}{k} = \frac{n}{n+1}\cdot\frac{x}{k} - \frac{1}{n+1} \quad \text{and, for } x \neq nk, \quad \frac{x}{k+y} = \frac{n+1}{n\frac{k}{x}-1}\,,$$

ACADEMIA PRESS
UNIVERSITEIT GENT

it is straightforward to check the following implications.

$$\begin{aligned}
\frac{x}{k} \in I_{n+1,j} \quad &\Rightarrow \quad \frac{x+y}{k} \in I_{n,j-1} \quad \text{for } 0 \le j \le n\,;\\
\frac{x}{k} \in I_{n+1,-1} \quad &\Rightarrow \quad \frac{x+y}{k} \in I_{n,-1}\,;\\
n \neq \frac{x}{k} \in I_{n+1,j} \quad &\Rightarrow \quad \frac{x}{k+y} \in I_{n,j} \qquad \text{for } -1 \le j \le n-1\,;\\
\frac{x}{k} = n \quad &\Rightarrow \quad k+y=0\,;\\
\frac{x}{k} > n \quad &\Rightarrow \quad k+y<0 \quad \text{and} \quad \frac{x}{k+y} \in I_{n,-1}\,.
\end{aligned}$$

Hence, for $0 \le j \le n-1$ and $\frac{x}{k} \in I_{n+1,j}$ we have

$$\begin{aligned}
\tilde{S}_{n+1}(k,x) &= \tilde{S}_n(k,x+y) + \tilde{S}_n(k+y,x)\\
&= [c_{n,j-1}k - c_{n,j}(x+y)] + [c_{n,j}(k+y) - c_{n,j+1}x]\\
&= c_{n+1,j}k - c_{n,j+1}x\,,
\end{aligned}$$

since $c_{n,j-1}+c_{n,j} = c_{n+1,j}$ by the recursion formula of the binomial coefficients. If $\frac{x}{k} \in I_{n+1,-1}$ we have

$$\begin{aligned}
\tilde{S}_{n+1}(k,x) &= \tilde{S}_n(k,x+y) + \tilde{S}_n(k+y,x)\\
&= [2^{n-2}k - 2^{n-2}(x+y)] + [2^{n-2}(k+y) - 2^{n-2}x]\\
&= 2^{n-1}k - 2^{n-1}x\,.
\end{aligned}$$

And finally for $\frac{x}{k} \in I_{n+1,n}$ we have $k+y \le 0$ and thus

$$\begin{aligned}
\tilde{S}_{n+1}(k,x) &= \tilde{S}_n(k,x+y) + \tilde{S}_n(k+y,x)\\
&= [(1-2^{n-2})k + 2^{n-2}(x+y)] + [-2^{n-2}(k+y) + 2^{n-2}x]\\
&= (-2^{n-1}+1)k + 2^{n-1}x\,.
\end{aligned}$$

This proves the formula for $\tilde{S}_{n+1}$ and completes the induction. □

With the explicit formula we are able to determine $\min_x \tilde{S}_n(k,x)$.

Theorem 3.6.

$$\min\left\{ \frac{\tilde{S}_n(k,x)}{k} \;\middle|\; k,x \in \mathbb{R},\ k>0 \right\} = \binom{n-1}{\lfloor \frac{n-1}{2} \rfloor}. \tag{7}$$

ACADEMIA PRESS
UNIVERSITEIT GENT

Proof. We have $c_{n,i} > 0$ for $i < \frac{n}{2}$, $c_{n,i} < 0$ for $i > \frac{n}{2}$ and $c_{n,\frac{n}{2}} = 0$ for n even. Thus for n even, the function $x \mapsto S_n(k,x)$ is decreasing for $x \leq \frac{n/2-1}{n/2+1}k$, constant in the interval $\frac{n/2-1}{n/2+1}k \leq x \leq k$ and increasing for $x \geq k$. To obtain the minimum we set $x = k$ and get

$$\tilde{S}_n(k,k) = c_{n,n/2-1}k - c_{n,n/2}k = k\binom{n-1}{n/2-1}.$$

For n odd we find that the unique minimum is reached at $x = k$ and is equal to

$$\tilde{S}_n(k,k) = c_{n,n/2-1}k - c_{n,n/2}k = k\binom{n-1}{(n-1)/2}.$$

For n even and odd, this is expressed in the formula (7). □

This proves that two collections $A_1, \ldots, A_n$ and $B_1, \ldots, B_n$ with $\mu(\bigcap_{i\in S} A_i) = \mu(\bigcap_{i\in S} B_i)$ for $|S| \leq n-2$ satisfy

$$\frac{\mu(\bigcup_{i\in S} A_i)}{\mu(\bigcup_{i\in S} B_i)} \geq 1 - \binom{n-1}{\lfloor \frac{n-1}{2} \rfloor}^{-1}.$$

With Stirlings formula this can be expressed as

$$\frac{\mu(\bigcup_{i\in S} A_i)}{\mu(\bigcup_{i\in S} B_i)} = 1 + O(\sqrt{n}2^{-n})$$

which is far better that the general bound

$$\frac{\mu(\bigcup_{i\in S} A_i)}{\mu(\bigcup_{i\in S} B_i)} = 1 + O(\exp(-\sqrt{n}))$$

from Theorem 1 (part 1) in [2].

3.4. From continuous to discrete

We have now solved the continuous version of the approximation problem. Now we want to have a closer look on the discrete problem. First note that if we start with rational numbers k, x every number occurring in Theorem 3.4 is rational. Thus the measure of the sets in solution will be rational. We can make them integral by multiplication with a suitable integer. This proves for each $k, x \in \mathbb{Q}$ that there exist an integer $t \in \mathbb{Z}$ with $tk, tx \in \mathbb{Z}$ and

$$t\tilde{S}_n(k,x) = S_n(tk,tx).$$

ACADEMIA PRESS
UNIVERSITEIT GENT

So the results translate from continuous to discrete. Especially Theorem 3.6 is also valid for the discrete case.

But we are left with the question of finding small discrete examples. For a reason that will become clear in the next section we are especially interested in symmetric collections $A_1, \ldots, A_n$ and $B_1, \ldots, B_n$ that maximize

$$\frac{|B_1 \cap \cdots \cap B_{n-1}| - |A_1 \cap \cdots \cap A_{n-1}|}{|B_1 \cup \cdots \cup B_n|}.$$

Similar to Theorem 3.6 we obtain the following result.

Theorem 3.7. *For symmetric collections $A_1, \ldots, A_n$ and $B_1, \ldots, B_n$ we have*

$$\begin{aligned}\frac{|B_1 \cap \cdots \cap B_{n-1}| - |A_1 \cap \cdots \cap A_{n-1}|}{|B_1 \cup \cdots \cup B_n|} &\leq \max\left\{ \frac{x+k}{nS_n(k,x)} \;\middle|\; k, x \in \mathbb{R} \right\} \\ &= \frac{2}{n\binom{n-1}{\lfloor \frac{n-1}{2} \rfloor}}.\end{aligned} \tag{8}$$

Since the numbers on the left-hand side are integers we know that the smallest collection of that kind must satisfy

$$|B_1 \cup \cdots \cup B_n| \geq \frac{n\binom{n-1}{\lfloor \frac{n-1}{2} \rfloor}}{2}. \tag{9}$$

To prove that equality is possible in (9) we give an example. We give for every subset $S \subseteq \{1, \ldots, n\}$ the sizes

$$\left| \bigcap_{i \in S} A_i \setminus \bigcup_{i \notin S} A_i \right| \quad \text{and} \quad \left| \bigcap_{i \in S} B_i \setminus \bigcup_{i \notin S} B_i \right|.$$

The construction is best understood if we look at the example $n = 9$ first.

$\lvert S \rvert$	1	2	3	4	5	6	7	8	9
$\lvert \bigcap_{i \in S} A_i \setminus \bigcup_{i \notin S} A_i \rvert$	0	3	0	1	0	0	2	0	4
$\lvert \bigcap_{i \in S} B_i \setminus \bigcup_{i \notin S} B_i \rvert$	4	0	2	0	0	1	0	3	0

In general we will have a zigzag-line of numbers starting on the left side in the B-row with the value $\lfloor \frac{n-1}{2} \rfloor$, going down to 1, then has one gap and restart with 1. The general rule is as follows:

$$\left| \bigcap_{i \in S} A_i \setminus \bigcup_{i \notin S} A_i \right| = \begin{cases} |S| - \lceil \frac{n}{2} \rceil & \text{if } |S| > n/2, \text{ and } |S| \text{ is odd}, \\ \lceil \frac{n}{2} \rceil - |S| & \text{if } |S| < n/2, \text{ and } |S| \text{ is even}, \\ 0 & \text{in all other cases}; \end{cases} \tag{10}$$

ACADEMIA PRESS
UNIVERSITEIT GENT

$$\left|\bigcap_{i\in S} B_i \setminus \bigcup_{i\notin S} B_i\right| = \begin{cases} |S| - \lceil \frac{n}{2} \rceil & \text{if } |S| > n/2, \text{ and } |S| \text{ is even}, \\ \lceil \frac{n}{2} \rceil - |S| & \text{if } |S| < n/2, \text{ and } |S| \text{ is odd}, \\ 0 & \text{in all other cases}. \end{cases} \tag{11}$$

Theorem 3.8. *For each positive integer n, the collections $A_1, \ldots, A_n$ and $B_1, \ldots, B_n$ described above satisfy*

$$|B_1 \cup \cdots \cup B_n| = \frac{n}{2}\binom{n-1}{\lfloor \frac{n-1}{2} \rfloor} \tag{12}$$

$$|B_1 \cup \cdots \cup B_{n-1}| = |A_1 \cup \cdots \cup A_{n-1}| + 1 \tag{13}$$

and

$$|B_1 \cup \cdots \cup B_{n-k}| = |A_1 \cup \cdots \cup A_{n-k}| \quad \textit{for each } k \geq 2\,. \tag{14}$$

Proof. To simplify notation, we shall prove this only for $n = 4m$. The other cases can be handled by similar arguments. In the proof we will make use of the following well known identities:

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} = 0 \qquad \text{for } n \geq 1\,, \tag{15}$$

$$\sum_{i=0}^{n} (-1)^i i \binom{n}{i} = 0 \qquad \text{for } n \geq 2\,. \tag{16}$$

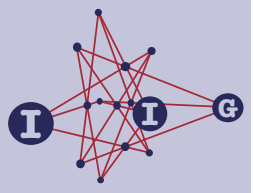
(The second identity follows from the first using $i\binom{n}{i} = n\binom{n-1}{i-1}$.) We have

$$\left|\bigcap_{i\in S} A_i\right| = \sum_{S \subseteq S' \subseteq \{1,\ldots,n\}} \left|\bigcap_{i\in S'} A_i \setminus \bigcup_{i\notin S'} A_i\right|$$

and thus

$$\left|\bigcap_{i=1}^{n-k} B_i\right| - \left|\bigcap_{i=1}^{n-k} A_i\right| = \sum_{i=0}^{k} (-1)^i (2m - i) \binom{k}{i}\,;$$

by (15) and (16) this sum vanishes for $k \geq 2$. With the inclusion-exclusion



formula this proves (13) and (14). Furthermore

$$\begin{aligned}\left|\bigcup_{i=1}^{n} B_i\right| &= \sum_{S\subseteq\{1,\ldots,n\}} \left|\bigcap_{i\in S} B_i \setminus \bigcup_{i\notin S} B_i\right| \\ &= \sum_{i=0}^{2m-1} (2m-i)\binom{n}{i} \\ &= \sum_{i=0}^{2m-1} \left[2m\binom{n}{i} - 4m\binom{n-1}{i-1}\right] \\ &= \sum_{i=0}^{2m-1} \left[2m\binom{n-1}{i} - 2m\binom{n-1}{i-1}\right] \\ &= 2m\binom{n-1}{2m-1} = \frac{n}{2}\binom{n-1}{\lfloor\frac{n-1}{2}\rfloor}\end{aligned}$$

which proves (12). □

3.5. Application to visual cryptography

In this section we want to study a particular nice application of the approximate inclusion-exclusion formula.

In 1995 M. Naor and A. Shamir [3] invented a new type of cryptography. The ciphertext and key consist of two transparencies showing a pattern of white and black dots indistinguishable from random noise. The stack of the two transparencies reveals an encrypted image. Due to its simplicity visual cryptography can be used by anyone without any knowledge of cryptography and without the help of a computer.

We look at a generalization of visual cryptography that uses n transparencies so that the secret image is reconstructed whenever at least k of these transparencies are stacked together whereas less than k transparencies reveal no information about the secret image.

Formally the distribution of white and black pixels is described by boolean $n \times m$ matrices, which leads to the following definition.

Definition 3.9 (see [3, Definition 1]). A k out of n visual secret sharing scheme consists of two multisets C_0 and C_1 of $(n \times m)$-matrices satisfying

1. For any subset $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ of size k and any M in C_0 let M' be the $(k \times m)$-matrix obtained by restricting M to the rows $i_1, \ldots, i_k$. Then at most $d - \alpha m$ columns of M' contain a non-zero entry.

ACADEMIA PRESS

UNIVERSITEIT GENT

2. For any subset $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ of size k and any M in C_1 let M' be the $k \times m$ matrix obtained by restricting M to the rows $i_1, \ldots, i_k$. Then at least d columns of M' contain a non-zero entry.

3. For any subset $\{i_1, \ldots, i_q\}$ of size $q < k$, the two multisets of $q \times m$ matrices D_0 and D_1 obtained by restricting each $n \times m$ matrix in C_0 and C_1 to the rows $i_1, \ldots, i_q$ are indistinguishable in the sense that they contain the same matrices in the same frequencies.

A visual secret sharing scheme has three important parameters:

- The contrast α, that is a measure for the relative difference between 'white' and 'black' in the reconstructed image.
- The number of subpixels m used to encode the images. A white pixel is encoded as follows. One chooses randomly a matrix M from C_0. The j-subpixel on transparency i, $i = 1, \ldots, n$, is colored black if and only if the (i, j)-entry of M is 1; otherwise it is left *white*. Similarly, a matrix of C_1 is used to encode a black pixel.
- The randomness $r = \max\{|C_0|, |C_1|\}$, which is a measure for the number of random bits needed to generate the visual secret sharing scheme. The randomness r does not effect the quality of the picture.

The contrast α is commonly considered as the most important parameter, while the randomness r is the least important parameter.

Theorem 3.8 allows us the construction of an optimal $(n-1)$ out of n visual secret sharing scheme.

Theorem 3.10. *The contrast of an $(n-1)$ out of n visual secret sharing scheme satisfies*

$$\alpha \leq \frac{2}{n\binom{n-1}{\lfloor \frac{n-1}{2} \rfloor}} \tag{17}$$

and there exists an $(n-1)$ out of n visual secret sharing scheme with

$$\alpha = \frac{2}{n\binom{n-1}{\lfloor \frac{n-1}{2} \rfloor}} \quad \text{and} \quad m = \frac{n\binom{n-1}{\lfloor \frac{n-1}{2} \rfloor}}{2}. \tag{18}$$

Proof. Without loss of generality we may assume that $|C_0| = |C_1| = r$. Define

ACADEMIA PRESS
UNIVERSITEIT GENT

the collections A_i, B_i with $1 \leq i \leq n$ by

$$A_i = \{(j,l) \mid 1 \leq j \leq m, 1 \leq l \leq r, \text{ the } l\text{-th matrix in the collection } C_0 \text{ has a } 1 \text{ at position } (i,j)\};$$
$$B_i = \{(j,l) \mid 1 \leq j \leq m, 1 \leq l \leq r, \text{ the } l\text{-th matrix in the collection } C_1 \text{ has a } 1 \text{ at position } (i,j)\}.$$

Condition 3 of Definition 3.9 guarantees that $|\bigcap_{i\in S} A_i| = |\bigcap_{i\in S} B_i|$ for each $S \subseteq \{1,\ldots,n\}$ with $|S| \leq n-2$.

For each $S \subseteq \{1,\ldots,n\}$ with $|S| = n-1$ condition 1 says that

$$\left|\bigcap_{i\in S} A_i\right| \leq r(d-\alpha m)$$

and condition 2 says that

$$\left|\bigcap_{i\in S} B_i\right| \geq rd\,.$$

Application of Theorem 3.7 to the collections $A_1,\ldots,A_n$ and $B_1,\ldots,B_n$ yields

$$\alpha \leq \frac{2}{n\binom{n-1}{\lfloor\frac{n-1}{2}\rfloor}}\,.$$

Now we give a construction of an good $(n-1)$ out of n visual secret sharing scheme. Choose collections $A_1,\ldots,A_n$ and $B_1,\ldots,B_n$ as described in Theorem 3.8. Without loss of generality these sets are subsets of $\{1,\ldots,m\}$ where $m = \frac{n}{2}\binom{n-1}{\lfloor\frac{n-1}{2}\rfloor}$. Let S_0 be the boolean $n \times m$ matrix with 1 at position (i,j) if and only if $j \in A_i$. Similar let S_1 be the $n \times m$ matrix corresponding to the collection $B_1,\ldots,B_n$. By construction S_0 and S_1 satisfy the conditions 1 and 2 of Definition 3.9. Let C_i $(i = 0,1)$ be the multiset of size $m!$ that contains S_i and all column permutations of S_i. Then the collections C_0 and C_1 satisfy Definition 3.9. □

4. The case $m = n - d$, d fixed

Now we consider the case of two collections $A_1,\ldots,A_n$ and $B_1,\ldots,B_n$ with $|\bigcap_{i\in S} A_i| = |\bigcap_{i\in S} B_i|$ for each subset S with $|S| \leq m = n-d$ for some fixed d. For this case we are still able to prove a recursion formula, but we have no closed form.

Let μ be an arbitrary measure and let $A_1,\ldots,A_n$ and $B_1,\ldots,B_n$ be symmetric collections of sets satisfying

ACADEMIA PRESS
UNIVERSITEIT GENT

(1c) $\mu(\bigcap_{i=1}^{j} A_i) = \mu(\bigcap_{i=1}^{j} B_i)$ for all $j \le n-d$,

(2c) $\mu(\bigcap_{i=1}^{n-j} A_i) = \mu(\bigcap_{i=1}^{n-j} B_i) - (-1)^{n-j}x_j$, for $0 \le j < d$.

As in the previous sections we ask for the smallest possible value $S_n(x_0,\dots,x_{d-1})$ for $\max\{\mu(\bigcup_{i=1}^{n} A_i), \mu(\bigcup_{i=1}^{n} B_i)\}$ where again the minimum is taken over all collections of sets in all finite measurable spaces. With arguments similar to Theorem 3.4 we obtain the following result.

Theorem 4.1. *The function $S_n(x_0,\dots,x_{d-1})$ defined above satisfies the recursion formula*

$$S_{n+1}(x_0,\dots,x_{d-1}) \ge S_n(x_0+x_1, x_1+x_2, \dots, x_{d-2}+x_{d-1}, x_{d-1}+0) + S_n(x_0,\dots,x_{d-1}) \quad (19)$$

for $n \ge d$.

Proof. As in the proof of Lemma 3.1 we define $A_i' = A_i \backslash A_{n+1}$, $B_i' = B_i \backslash B_{n+1}$, $A_i'' = A_i \cap A_{i+1}$ and $B_i'' = B_i \cap B_{n+1}$.

It is easy to check intersections of collections A_i'', B_i'' to see that

$$\max\Big\{\mu\Big(\bigcup_{i=1}^{n} A_i''\Big), \mu\Big(\bigcup_{i=1}^{n} B_i''\Big)\Big\} \ge S_n(x_0,\dots,x_{d-1}).$$

And it is only slightly more complex the see that

$$\begin{aligned}
\mu\Big(\bigcap_{i=1}^{n-j} A_i'\Big) &= \mu\Big(\bigcap_{i=1}^{n-1} A_i\Big) - \mu\Big(\bigcap_{i=1}^{n-1} A_i \cap A_{n+1}\Big) \\
&= \Big[\mu\Big(\bigcap_{i=1}^{n-1} B_i\Big) - (-1)^{n+1-j}x_j\Big] \\
&\qquad - \Big[\mu\Big(\bigcap_{i=1}^{n-1} B_i \cap B_{n+1}\Big) - (-1)^{n+1-j-1}x_{j+1}\Big] \\
&= \mu\Big(\bigcap_{i=1}^{n-j} B_i'\Big) - (-1)^{n-j}(-x_j - x_{j+1})
\end{aligned}$$

where $x_j = 0$ for $j \ge d$. Thus

$$\max\Big\{\mu\Big(\bigcup_{i=1}^{n} A_i'\Big), \mu\Big(\bigcup_{i=1}^{n} B_i'\Big)\Big\} \ge S_n(x_0+x_1, x_1+x_2, \dots, x_{d-2}+x_{d-1}, x_{d-1}+0).$$

ACADEMIA PRESS
UNIVERSITEIT GENT

All together we have

$$\begin{aligned}
&S_{n+1}(x_0,\dots,x_{d-1})\\
&\quad= \max\Big\{\mu\Big(\bigcup_{i=1}^{n} A_i\Big),\mu\Big(\bigcup_{i=1}^{n} B_i\Big)\Big\}\\
&\quad= \max\Big\{\mu\Big(\bigcup_{i=1}^{n} A'_i\Big),\mu\Big(\bigcup_{i=1}^{n} B'_i\Big)\Big\}+\mu(A_{n+1})\\
&\quad\geq \max\Big\{\mu\Big(\bigcup_{i=1}^{n} A'_i\Big),\mu\Big(\bigcup_{i=1}^{n} B'_i\Big)\Big\}+\max\Big\{\mu\Big(\bigcup_{i=1}^{n} A''_i\Big),\mu\Big(\bigcup_{i=1}^{n} B''_i\Big)\Big\}\\
&\quad= S_n(x_0+x_1,x_1+x_2,\dots,x_{d-2}+x_{d-1},x_{d-1}+0)+S_n(x_0,\dots,x_{d-1})\,,
\end{aligned}$$

which completes the proof. □

With the trivial bound $S_{d-1}(x_0,\dots,x_{d-1}) \geq |x_{d-1}|$ we can use Theorem 4.1 to obtain

$$S_n(x_0,\dots,x_{d-1}) \geq 2^{n-d+1}|x_{d-1}|\,.$$

This is almost all we need for the following asymptotic theorem.

Theorem 4.2. *Let $A_1,\dots,A_n$ and $B_1,\dots,B_n$ be two collections of sets satisfying $|\bigcap_{i\in S} A_i| = |\bigcap_{i\in S} B_i|$ for all subsets $S\subseteq\{1,\dots,n\}$ with $|S|\leq n-d$. Then*

$$\frac{|\bigcup_{i=1}^n B_i| - |\bigcup_{i=1}^n A_i|}{|\bigcup_{i=1}^n B_i|} \leq O(n^{d-1}2^{-n})$$

or equivalently

$$\frac{|\bigcup_{i=1}^n A_i|}{|\bigcup_{i=1}^n B_i|} \leq 1+O(n^{d-1}2^{-n})\,.$$

Remarks. (1) Remember that we assume d constant in this section. The O-constant in the theorem will thus depend on d.

(2) This bound is much better than the one given in [2, Theorem 1, Part 2].

(3) This a remark that motivates the method used in the proof. Clearly

$$\frac{\mu(\bigcup_{i=1}^n B_i) - \mu(\bigcup_{i=1}^n A_i)}{\mu(\bigcup_{i=1}^n B_i)} = \frac{\sum_{i=0}^{d-1}\binom{n}{i}x_i}{S_n(x_0,\dots,x_{d-1})}\,.$$

If we could assure that $|x_i| \leq cn^{d-1-i}|x_{d-1}|$ for some constant c, then the

theorem would follow directly from

$$\frac{\sum_{i=0}^{d-1}\binom{n}{i}x_i}{S_n(x_0,\dots,x_{d-1})} \le \frac{\sum_{i=0}^{d-1}\binom{n}{i}n^{d-1-i}cx_{d-1}}{S_n(x_0,\dots,x_{d-1})} = \frac{O(n^{d-1}|x_{d-1}|)}{2^{n-d+1}|x_{d-1}|)} = O(n^{d-1}2^{-n})\,.$$

The difficulty of the proof is to remove the restriction $|x_i| \le cn^{d-1-i}|x_{d-1}|$.

Proof of Theorem 4.2. Choose constants $c_0,\dots,c_{d-1} > 0$ satisfying

$$1 - \sum_{j=i+1}^{d-1}\binom{n-d-1}{j-i}\frac{c_i}{c_j n^{j-i}} \ge \frac{1}{2} \tag{20}$$

for $i = 0,\dots,d-2$. Let $i_{\max}$ be the value of i for which $c_i n^i|x_i|$ is maximal. Using an inductive argument, the recursion formula (19) shows that

$$S_n(x_0,\dots,x_{d-1}) \ge \sum_{j=1}^{n+1-d}\binom{n+1-d}{j} S_{d-1}\big(x_0^{(j)},\dots,x_{d-1}^{(j)}\big) \tag{21}$$

where

$$x_k^{(j)} = \sum_{\ell=k}^{d-1}\binom{j}{\ell-k}x_\ell\,. \tag{22}$$

For $k = i_{\max}$ and all $j \in \{1,\dots,n-d+1\}$ this implies that (in the second step we use the definition of $i_{\max}$ and the last step uses (20))

$$\begin{aligned}
|x_{i_{\max}}^{(j)}| &\ge |x_{i_{\max}}| - \sum_{\ell=i_{\max}+1}^{d-1}\binom{n-d+1}{\ell-i_{\max}}|x_\ell| \\
&\ge |x_{i_{\max}}| - \sum_{\ell=i_{\max}+1}^{d-1}\binom{n-d-1}{\ell-i_{\max}}\frac{c_{i_{\max}}}{c_\ell n^{\ell-i_{\max}}}|x_{i_{\max}}| \\
&\ge \frac{1}{2}|x_{i_{\max}}|\,.
\end{aligned}$$

Together with the trivial bound

$$S_{d-1}\big(x_0^{(n-d+1,i)},\dots,x_{d-1}^{(j)}\big) \ge |x_{i_{\max}}^{(j)}|$$

and (21) we find

$$S_n(x_0,\dots,x_{d-1}) \ge \sum_{j=1}^{n+1-d}\binom{n+1-d}{j}\frac{1}{2}|x_{i_{\max}}| = 2^{n-d}|x_{i_{\max}}|\,.$$

ACADEMIA PRESS
UNIVERSITEIT GENT

Now we are finished, since by definition of $i_{\max}$,

$$\begin{aligned}\frac{\sum_{i=0}^{d-1}\binom{n}{i}x_i}{S_n(x_0,\ldots,x_{d-1})} &\leq \frac{\sum_{i=0}^{d-1} n^i|x_i|}{2^{n-d}|x_{i_{\max}}|}\\ &\leq \frac{\sum_{i=0}^{d-1}\frac{c_{i_{\max}}}{c_i}n^{i_{\max}}|x_{i_{\max}}|}{2^{n-d}|x_{i_{\max}}|}\\ &\leq \left(2^d\sum_{i=0}^{d-1}\frac{c_{i_{\max}}}{c_i}\right)n^{i_{\max}}2^{-n} = O(n^{i_{\max}}2^{-n})\end{aligned}$$

The worst bound is obtained for $i_{\max} = d-1$, i.e. in the simple case $|x_i| \leq cn^{d-1-i}|x_{d-1}|$ mentioned in Remark (3) above. □

5. Open problems

We want to close this article with some open problems.

1. What is the discrete analogue for Theorem 3.6, i.e. find the minimal k for which $\min_{x\in\mathbb{Z}} S(k,x) = \min_{x\in\mathbb{R}} \tilde{S}(k,x)$. This is more difficult than the discrete analogue for Theorem 3.7, since this time the discrete minimum has to be asymmetric.

2. The visual cryptography scheme in Theorem 3.10 has randomness $m!$. That is the trivial upper bound for the randomness. Improve that bound.

3. The explicit solution for $m = n-2$ (Theorem 3.6) proves

$$\frac{|\bigcup_{i=1}^n A_i|}{|\bigcup_{i=1}^n B_i|} \leq 1 + O(\sqrt{n}2^{-n})$$

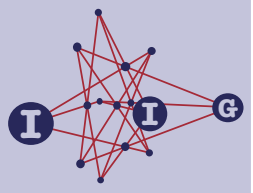
   which is better than the general bound

$$\frac{|\bigcup_{i=1}^n A_i|}{|\bigcup_{i=1}^n B_i|} \leq 1 + O(n2^{-n})$$

   proven in Theorem 4.2. Improve the bound of Theorem 4.2 for $m = n-d$, $d > 2$.

4. Is it possible to adapt the arguments of Theorem 4.2 to deal with non-constant d?

ACADEMIA PRESS
UNIVERSITEIT GENT



References

[1] **J. Kahn**, **N. Linial** and **A. Samorodnitsky**, Inclusion-exclusion: exact and approximate, *Combinatorica* **16**, no. 4 (1996), 465–477.

[2] **N. Linial** and **N. Nisan**, Approximate inclusion-exclusion, *Combinatorica* **10**, no. 4 (1990), 349–365.

[3] **M. Naor** and **A. Shamir**, Visual cryptography, in Alfredo De Santis, editor, *Advances in cryptology – EUROCRYPT '94*, *Lect. Notes Comput. Sci.* **950**, 1–12, Springer-Verlag, 1995.

Andreas Klein

GHENT UNIVERSITY, DEPT. OF PURE MATHEMATICS AND COMPUTER ALGEBRA, KRIJGSLAAN 281-S22, 9000 GHENT, BELGIUM

e-mail: klein@cage.ugent.be

Klaus Metsch

MATHEMATISCHES INSTITUT, ARNDTSTRASSE 2, D-35392 GIESSEN, GERMANY

e-mail: klaus.metsch@math.uni-giessen.de

ACADEMIA PRESS

UNIVERSITEIT GENT