The Stein-Lovász Theorem and Its Applications to Some Combinatorial arrays

Dameng Deng[*] and Yuan Zhang
Department of Mathematics
Shanghai Jiao Tong University
Shanghai, 200240, China

P. C. Li[†] and G. H. J. van Rees[‡]
Department of Computer Science
University of Manitoba
Winnipeg, Manitoba
Canada R3T 2N2

Abstract

The Stein-Lovász Theorem can be used to get existence results for some combinatorial problems using constructive methods rather than probabilistic methods. In this paper, we discuss applications of the Stein-Lovász Theorem to some combinatorial set systems and arrays, including perfect hash families, separating hash families, splitting systems, covering designs, lotto designs and Δ-free systems. We also compare some of the bounds obtained from the Stein-Lovász Theorem to those using the basic probabilistic method.

1 Introduction

The Stein-Lovász Theorem was first used by Stein [11] and Lovász [9] in studying some combinatorial covering problems. In [6], the authors applied this theorem to some problems in coding theory. The Stein-Lovász Theorem can be used to get existence results for some combinatorial problems using constructive methods rather than probabilistic methods. The Stein-Lovász Theorem is now stated and the proof is included for completeness. The proof follows [11] and [6].

Theorem 1.1 *[6] Let A be a $(0,1)$ matrix with N rows and M columns. Assume that each row contains at least v ones, and each column at most a ones. Then there exists an $N \times K$ sub matrix C with*

$$K \leq N/a + (M/v)\ln a \leq (M/v)(1 + \ln a),$$

[*] research supported by NSFC grant 10601032

[†] research supported by NSERC grant 250389-06

[‡] research supported by NSERC grant 3558-02

such that C does not contain an all-zero row.

Proof: A constructive approach for producing C is presented. Let $A_a = A$ and define A'_a to be any maximal set of columns from A_a whose supports are pairwise disjoint and whose columns each have a ones. Let $K_a = |A'_a|$. Discard from A_a the columns of A'_a and any row with a one in A'_a. We are left with a $k_a \times (M - K_a)$ matrix A_{a-1}, where $k_a = N - aK_a$. Clearly, the columns of A_{a-1} have at most $a-1$ ones (indeed, otherwise such a column could be added to the previously discarded set, contradicting its maximality). We continue by doing to A_{a-1} what we did to A_a. That is we define A'_{a-1} to be any maximal set of columns from A_{a-1} whose supports are pairwise disjoint and whose columns each have $a-1$ ones. Let $K_{a-1} = |A'_{a-1}|$. Then discard from A_{a-1} the columns of A'_{a-1} and any row with a one in A'_{a-1} getting a $k_{a-1} \times (M - K_a - K_{a-1})$ matrix A_{a-2}, where $k_{a-1} = N - aK_a - (a-1)K_{a-1}$.

The process will terminate after at most a steps. The union of the columns of the discarded sets form the desired sub matrix C with

$$K = \sum_{i=1}^{a} K_i.$$

The first step of the algorithm gives

$$k_a = N - aK_a,$$

which we rewrite, setting $k_{a+1} = N$, as

$$K_a = \frac{k_{a+1} - k_a}{a}.$$

Analogously,

$$K_i = \frac{k_{i+1} - k_i}{i},\ \ i = 1, \cdots, a.$$

Now we derive an upper bound for k_i by counting the number of ones in A_{i-1} in two ways: every row of A_{i-1} contains at least v ones, and every column at most $i-1$ ones, thus

$$vk_i \leq (i-1)(M - K_a - \cdots - K_{i+1}) \leq (i-1)M.$$

Furthermore,

$$K = \textstyle\sum_{i=1}^{a} K_i = \sum_{i=1}^{a} \displaystyle\frac{k_{i+1} - k_i}{i} = \frac{k_{a+1}}{a} + \frac{k_a}{a(a-1)} + \frac{k_{a-1}}{(a-1)(a-2)} + \cdots + \frac{k_2}{1 \cdot 2} - k_1$$
$$\leq N/a + M/v(1/a + 1/(a-1) + ... + 1/2),$$

thus giving the result. □

We now transform the above into a simple greedy algorithm which we present following.

Algorithm 1.1: STEIN-LOVÁSZ(A)

```
comment: $A$ is an $N \times K$ matrix, each column has at most $a$ ones
                                        each row has at least $v$ ones
comment: Returns a submatrix of $A$ with no all-zero row
$C \leftarrow \emptyset$
while $A$ has at least one row
  do {
    find a column $c$ in $A$ having maximum weight
    delete all rows of $A$ that contain a "1" in column $c$
    delete column $c$ from $A$
    $C \leftarrow C \cup c$
  }
```

Finding the maximum weight column can be done in $O(NK)$. The loop gets executed at most a times so the algorithm runs in time $O(aKN) \in O(kN2)$. A tighter analysis may be performed by taking into account that the number of rows decrease in each iteration.

The remainder of the paper is organized as follows. In Section 2, we discuss applications of the Stein-Lovász Theorem to some combinatorial set systems and arrays such as perfect hash families, separating hash families, splitting systems, covering designs, lotto designs and Δ-free systems. For most of these combinatorial structures, we get roughly the same existence results compared to the classic probabilistic method. In Section 3, we conclude the paper with a few final remarks.

2 Applications of the Stein-Lovász Theorem

Nonconstructive existence results can often be obtained by probabilistic methods. The interested readers may refer to [1]. For all of the combinatorial structures under discussion in this paper, bounds of this type have been derived by the probabilistic method. In this section, we present a unified treatment of several of these bounds by the Stein-Lovász Theorem. Furthermore, we show that most of these bounds are roughly the same as those obtained by the basic probabilistic method. As a result, the Stein-Lovász Theorem can replace the basic probabilistic method for some problems.

Most of the combinatorial structures discussed in this paper can be viewed as set systems or arrays. We present some relevant definitions. A set system is a pair $(X, \mathcal{B})$, where X is a set of points and $\mathcal{B}$ is a set of subsets of X (called blocks). A set system $(X, \mathcal{B})$ is called k-uniform if $|B| = k$ for each $B \in \mathcal{B}$. A set system can be described by an incidence matrix. Let $(X, \mathcal{B})$ be a set system where $X = \{x_1, x_2, \cdots, x_N\}$ and $B = \{B_1, B_2, \cdots, B_T\}$. The *incidence matrix* of $(X, \mathcal{B})$ is the $N \times T$ matrix $A = (a_{ij})$, where

$$a_{ij} = \begin{cases} 1 & \text{if } x_i \in B_j \\ 0 & \text{if } x_i \notin B_j. \end{cases}$$

2.1 Perfect Hash Families

An (n, m, w)-perfect hash family is a set of functions $\mathcal{F}$, such that $|Y| = n$, $|X| = m$, $f : Y \to X$ for each $f \in \mathcal{F}$, and for any $C \subseteq \{1, 2, \ldots, n\}$ such that $|C| = w$, there exists at least one $f \in \mathcal{F}$ such that $f|_C$ is one-to-one. When $|\mathcal{F}| = \mathrm{N}$, an (n, m, w)-perfect hash family will be denoted by PHF$(N; n, m, w)$.

A PHF$(N; n, m, w)$ can be described as an (N, n, q)-array, A, satisfying certain properties. The rows of A are indexed by the functions in F, the columns are indexed by the elements of Y, and $A(f, y)$ is defined to be $f(y)$, for all $f \in F$ and all $y \in Y$. This array satisfies the property that, for all choices of w columns of A, there exists a row of A in which the entries in the w given columns are distinct.

The following result is essentially the bound proved by Mehlhorn (see [10]) by the classic probabilistic method.

Theorem 2.1 *There exists a PHF$(N; n, m, w)$ if*

$$N > \frac{\log \binom{n}{w}}{-\log q}$$

where

$$q = 1 - \frac{w!\binom{m}{w}}{m^w}$$

We can get the following result by the Stein-Lovász Theorem.

Theorem 2.2 *There exists a PHF$(N; n, m, w)$ with*

$$N \leq \frac{m^w}{w!\binom{m}{w}} \left(1 + \log \binom{n}{w}\right)$$

Proof: We construct the following incidence matrix $A = (a_{ij})$, with m^n columns labeled by all the vectors of length n over an alphabet of cardinality m. The number of rows is $\binom{n}{w}$. There is natural correspondence between the w-subsets and the numbers from 1 to $\binom{n}{w}$. If, in the vector labeling column j, the entries confined to the w-subset with number i are distinct, then $a_{ij} = 1$. Otherwise, $a_{ij} = 0$.

Therefore, if there is a sub matrix having N columns, with each row having at least one "1", then there exists a PHF$(N; n, m, w)$. We can now bound N by the Stein-Lovász Theorem.

Obviously, every row of A has weight $w!\binom{m}{w} m^{n-w}$. The weight of every column is at most $\binom{n}{w}$. So by the Stein-Lovász Theorem,

$$N \leq \frac{m^w}{w!\binom{m}{w}} \left(1 + \log \binom{n}{w}\right),$$

which is the desired result. □

Remark 2.3 *It is easy to see that $-\log(1 - x) \approx x$. Let $x = \frac{w!\binom{m}{w}}{m^w}$, then we conclude that the two bounds from Theorem 2.1 and Theorem 2.2 are roughly the same. The algorithm as presented constructs a Perfect Hash Family one function at a time. At each stage, a new function is added to the family that maximizes the number of "new" w-subsets that are separated. When all w-subsets are separated, the algorithm stops. It seems quite interesting that such a simple greedy stategy yields such good bounds.*

2.2 Separating Hash Families

We can use similar approach to prove bounds for separating hash families.

An $(n, m, \{w_1, w_2\})$-*separating hash family* is a set of functions $\mathcal{F}$, such that $|Y| = n$, $|X| = m$, $f : Y \to X$ for each $f \in \mathcal{F}$, and for any $C_1, C_2 \subseteq \{1, 2, \ldots, n\}$ such that $|C_1| = w_1$, $|C_2| = w_2$ and $C_1 \cap C_2 = \emptyset$, there exists at least one $f \in \mathcal{F}$ such that

$$\{f(y) : y \in C_1\} \cap \{f(y) : y \in C_2\} = \emptyset.$$

The notation SHF$(N; n, m, \{w_1, w_2\})$ will be used to denote an $(n, m, \{w_1, w_2\})$-separating hash family with $|\mathcal{F}| =$ N.

An SHF$(N; n, m, \{w_1, w_2\})$ yields an (N, n, q)-array, say A, which satisfies the property that, for any choice of w_1 columns of A, say C_1, and for any choice of w_2 columns of A, say C_2, where $C_1 \bigcap C_2 = \emptyset$, there exists a row of A in which the entries in the columns in C_1 are different from the entries in the columns in C_2. We only discuss results where $w_1 \neq w_2$. The cases when $w_1 = w_2$ can be handled in a similar way.

The bounds for separating hash families depend on values of certain chromatic polynomials which we now define. Given a graph $G = (V, E)$, let $\Pi(G, m)$ be the chromatic polynomial of G, which is defined as follows: For a positive integer m, let $\Pi(G, m)$ denote the number of m-colorings of G (i.e., the number of ways to color the vertices of G using a specified set of m colors, such that no two vertices having the same color are joined by an edge $e \in E$). It is well-known that $\Pi(G, m)$ is a polynomial in m of degree $|V|$. If the vertices of G are colored independently, at random, using m colors, then the probability that the result is an m-coloring is $\Pi(G, m)/m^{|V|}$. The complete bipartite graph with parts $w_1$and w_2 is denoted K_{w_1,w_2}.

The following result is given in [14] using the basic probabilistic method.

Theorem 2.4 *Suppose $w_1 \neq w_2$. Then there exists a SHF$(N; n, m, \{w_1, w_2\})$ if*

$$N > \frac{\log \binom{n}{w_1} + \log \binom{n-w_1}{w_2}}{-\log p}$$

where

$$p = 1 - \frac{\Pi(K_{w_1,w_2}, m)}{m^{w_1+w_2}}.$$

Now we use the Stein-Lovász Theorem to get a similar result.

Theorem 2.5 *There exists a SHF$(N; n, m, \{w_1, w_2\})$ with*

$$N \leq \frac{m^{w_1+w_2}}{\Pi(K_{w_1,w_2}, m)} \left(1 + \log \binom{n}{w_1} \binom{n - w_1}{w_2}\right)$$

Proof: We construct the following incidence matrix $A = (a_{ij})$, with m^n columns labeled by all the vectors of length n over an alphabet of cardinality m. The number of rows is $\binom{n}{w_1}\binom{n-w_1}{w_2}$. Let us associate to each row a double number, the first part being a number from 1 to $\binom{n}{w_1}$, and the second being a number from 1 to $\binom{n-w_1}{w_2}$. For a w_1-subset and a disjoint w_2-subset, We can assign a double number $(i_1, i_2$ to it, where $i_1 \in \{1, 2, \cdots \binom{n}{w_1}\}$ and $i_2 \in \{1, 2, \cdots \binom{n-w_1}{w-2}\}$. Then we have $a_{ij} = 1$ if, in the vector labeling the column j, the entries confined to the w_1-subset with number i_1 are distinct from the entries confined to the disjoint w_2-subset with number i_2. Otherwise, $a_{ij} = 0$.

Therefore, if there is a sub matrix having N columns, with each row having at least one "1", then there exists a SHF$(N; n, m, \{w_1, w_2\})$. Now we can evaluate the block number N by the Stein-Lovász Theorem.

Obviously, every row of A has weight $\Pi(K_{w_1,w_2}, m)m^{n-w_1-w_2}$. The weight of every column is at most $\binom{n}{w_1}\binom{n-w_1}{w_2}$. So by the Stein-Lovász Theorem,

$$N \leq \frac{m^{w_1+w_2}}{\Pi(K_{w_1,w_2}, m)}\left(1 + \log\binom{n}{w_1}\binom{n-w_1}{w_2}\right),$$

which is the desired result. □

Note that the analysis in Remark 2.3 also applies here, so the two bounds from Theorem 2.4 and Theorem 2.5 are also roughly the same.

2.3 Splitting systems

Suppose n and t are even integers, $0 < t < n$. An (n, t)-*splitting system* is a pair $(X, \mathcal{B})$ that satisfies the following properties:

1. $|X| = n$, and $\mathcal{B}$ is a set of $\frac{n}{2}$-subsets of X, called *blocks*
2. for every $Y \subseteq X$ such that $|Y| = t$, there exists a block $B \in \mathcal{B}$ such that $|B \cap Y| = t/2$.

We will use the notation $(N; n, t)$-SS to denote an (m, t)-splitting system having N blocks.

In [13], splitting systems were used in baby-step giant-step algorithms for discrete logarithm problem with low hamming weight. In these baby-step giant-step algorithms, better time complexity can be achieved if the splitting system used fewer blocks..

The following result was proved by classic probabilistic method in [13].

Theorem 2.6 *A $(N; n, t)$-SS, where n and t are even, exists whenever*

$$N > \frac{\log\binom{n}{t}}{-\log q}$$

where

$$q = 1 - \frac{\binom{t}{t/2}\binom{n-t}{(n-t)/2}}{\binom{n}{n/2}}$$

We can use the Stein-Lovász Theorem to get a similar result.

Theorem 2.7 *A $(N; m, t)$-SS exists with*

$$N \leq \frac{\binom{n}{\frac{n}{2}}}{\binom{t}{\frac{t}{2}}\binom{n-t}{\frac{n-t}{2}}}\left(1 + 2\ln\binom{\frac{n}{2}}{\frac{t}{2}}\right)$$

Proof: We construct the following incidence matrix $A = (a_{ij})$, with $\binom{n}{\frac{n}{2}}$ columns labeled by all the vectors of length n and weight $\frac{n}{2}$, which ensures the set is uniform. We label the columns with $j = 1, 2, \cdots, \binom{n}{\frac{n}{2}}$. The number of rows is $\binom{n}{t}$. Since there is natural correspondence between the t-subsets and the numbers from 1 to $\binom{n}{t}$, denote the rows by i. If, in the vector labeling the column j, the t-subset with number i has exactly $t/2$ ones, then $a_{ij} = 0$. Otherwise, $a_{ij} = 0$.

Therefore, if there is a sub matrix having N columns, with each row having at least one "1", then there exists a (n, t)-splitting system on N blocks. Now we will bound the number of blocks, N. Obviously, every row of A has weight $v = \binom{t}{\frac{t}{2}}\binom{n-t}{\frac{n-t}{2}}$ and the weight of every column is $a = \binom{\frac{n}{2}}{\frac{t}{2}}^2$. Then, by the Stein-Lovász Theorem,

$$N \leq \frac{\binom{n}{\frac{n}{2}}}{\binom{t}{\frac{t}{2}}\binom{n-t}{\frac{n-t}{2}}}\left(1 + 2\ln\binom{\frac{n}{2}}{\frac{t}{2}}\right),$$

which is the desired result. □

2.4 Covering Designs

Suppose v, k, t are integers and $0 < t \leq k \leq v$. An (v, k, t) covering design is a pair $(X, \mathcal{B})$ such that

1. $|X| = v$ and $\mathcal{B}$ is a set of k-subsets of X, called *blocks* and
2. every t-subset of X is a subset of at least one member of $\mathcal{B}$.

Let $C(v, k, t)$ denote the size of an (v, k, t) covering design with the smallest number of blocks possible. It is clear that $C(v, k, t) \geq \frac{\binom{v}{t}}{\binom{k}{t}}$.

In [12], Rödl showed that $C(v, k, t) \leq (1 + o(1))\binom{v}{t}/\binom{k}{t}$, using a non-constructive probabilistic argument. We now show that we can construct a (v, k, t) covering design with at most $\binom{v}{k}/\binom{k}{t}\left(1 + \ln\binom{k}{t}\right)$ blocks. This is not as sharp as Rödl's result, but it is constructive.

Theorem 2.8 $C(v, k, t) \leq \binom{v}{k}/\binom{k}{t}\left(1 + \ln\binom{k}{t}\right)$

Proof: Let X be a set of size v. We construct the following incidence matrix $A = (a_{ij})$, with $\binom{v}{k}$ columns labeled by the k-subsets of X. Label the rows of A with the t-subsets of X. Now, set $a_{ij} = 1$ if the k-subset corresponding to the i^{th} column of A contains the t-subset corresponding to the j^{th} row of A. Otherwise, set $a_{ij} = 0$. Notice that each row contains exactly $\binom{v-t}{k-t}$ entries that are 1 and each column has exactly $\binom{k}{t}$ entries that are 1.

By the Stein-Lovász Theorem, there is a $\binom{v}{k} \times K$ sub matrix C such that C does not contain an all-zero row and $K \leq \binom{v}{k}/\binom{v-t}{k-t}(1 + \ln\binom{k}{t}$. We see that $\binom{v}{k}/\binom{v-t}{k-t}\left(1 + \ln\binom{k}{t}\right) = \binom{v}{t}/\binom{k}{t}\left(1 + \ln\binom{k}{t}\right)$, as $\binom{v}{k}\binom{k}{l} = \binom{v}{t}\binom{v-t}{k-t}$. Therefore, there are at most $\binom{v}{t}/\binom{k}{t}\left(1 + \ln\binom{k}{t}\right)$ columns in C. Finally, by definition of A and C, the k-subsets that correspond to the columns of C form a (v, k, t) covering design. □

2.5 Lotto Designs

An (n, k, p, t)-lotto design or generalized covering is an n-set, V, of elements and a set $\mathcal{B}$ of k-element subsets of V, so that for any p-set, P of V, there is a k-set, $B \in \mathcal{B}$ for which $|P \cup B| \geq t$. $L(n, k, p, t)$ denotes the smallest number of k-sets in any (n, k, p, t)-lotto design.

In [8], there is a survey of results on lotto designs. The volume bound is $L(n, k, p, t) \geq \binom{n}{p}/\sum_{i=t}^{min(p,k)} \binom{p}{i}\binom{n-p}{k-i}$ and a general upper bound is $L(n, k, p, t) \leq \lceil \frac{min(\binom{n}{p},\binom{n}{t})}{\lfloor \frac{k}{t} \rfloor} \rceil$ There is no probabilistic upper bound for lotto designs in the literature. However, one can get a constructive upper bound with the following theorem.

Theorem 2.9 $L(n, k, p, t) \leq \binom{n}{k}\frac{1+\ln\sum_{i=t}^{min(p,k)}\binom{k}{i}\binom{n-k}{p-i}}{\sum_{i=t}^{min(p,k)}\binom{p}{i}\binom{n-p}{k-i}}$.

Proof: A lotto design has the following incidence matrix $A = (a_{ij})$, with $\binom{n}{k}$ columns labeled by the k-subsets of V and with $\binom{n}{p}$ rows of A labeled by the p-subsets of V. Now, set $a_{ij} = 1$ if the p-subset corresponding to the i^{th} row of A intersects the k-subset corresponding to the j^{th} column of A in t or more elements. Otherwise, set $a_{ij} = 0$. Notice that each row contains exactly $\sum_{i=t}^{min(p,k)} \binom{p}{i}\binom{n-p}{k-i}$ entries that are 1 and each column has exactly $\sum_{i=t}^{min(p,k)} \binom{k}{i}\binom{n-k}{p-i}$. entries that are 1.

The Stein-Lovász Theorem can now be used to get the result. □

2.6 Δ-free systems

A family of r sets is called a Δ- system of size r if any two of the r sets have the same intersection. That is, $B_1, \ldots, B_r$ is a Δ-system of size r if

$$B_j \cap B_{j'} = \bigcap_{i=1}^{r} B_i,$$

for all $j, j' \in \{1, \ldots, r\}, j \neq j'$. An $(N, n, r) - \Delta-$free system is a set system (X, B), with $|X| = N$ and $|B| = n$, such that no subset of r of the blocks in B forms a Δ- system of size r. Denote by $N(n, r)$ the minimum integer N such that there exists an $(N, n, r) - \Delta-$free system. The problem of determining bounds on $N(n, r)$ has a long history and has been studied by many authors (for a paper on this topic, see [4]). It has been observed as early as 1978 (see[5]) that upper bounds on (N, n, r) can be obtained by using the probabilistic method, though detailed results do not seem to have been published.

We can use the Stein-Lovász Theorem to get a bound. The proof is a modification of the proof given in [3] and is similar to other proofs we have presented in this paper, and therefore it is omitted.

Theorem 2.10 *A* $(N, n, r) - \Delta$*-free system exists with*

$$N \leq \frac{1}{1-q}(1 + \ln\binom{n}{r})$$

where

$$q = \rho^r + r\rho^{r-1}(1-\rho) + (1-\rho)^r, \rho = \frac{1}{(r-1)^{1/(r-2)} + 1}$$

3 Concluding remarks

In this paper, we use the Stein-Lovász Theorem to get bounds for some combinatorial structures, such as perfect hash families, separating hash families, splitting systems, covering designs, lotto designs and Δ-free systems, and most of these bounds are roughly the same as those obtained by the basic probabilistic method. Thus, the Stein-Lovász Theorem, due to its constructive nature, can be looked at as a de-randomized algorithm for the basic probabilistic methods for most of the discussed problems. Note that better bounds for these problems have been obtained by more sophisticated probabilistic methods, like the Lovász Local Lemma[3],or the second moment method (see [1] or [12]). It is an interesting open problem to find the corresponding de-randomized algorithms.

4 Acknowledgements

We wish to thank Doug Stinson for his helpful remarks on presentation of the material.

References

[1] N. Alon and J. H. Spencer. The Probabilistic method, Second edition, John Wiley and Sons, 2002.

[2] S. R. Blackburn. Perfect Hash Families: Probabilistic Methods and Explicit Constructions, Journal of Combinatorial Theory, Ser. A, **92**(2000),54-60.

[3] D. Deng, D. R. Stinson and R. Wei. The Lovász Local Lemma and its applications to some combinatorial array, Designs, Codes and Cryptography, **32** (2004), 121-134.

[4] W. A. Deuber, D .S. Gunderson, A. V. Kostochka and A. G. Meyer. Intersection statements for systems of sets, Journal of Combinatorial Theory, Ser. A, **79** (1997), 118-132.

[5] P. Erdös and E. Szemerédi. Combinatorial properties of systems of sets, Journal of Combinatorial Theory, Ser. A, **24** (1978), 308-313.

[6] G. Cohen, S. Litsyn and G. Zémor, On greedy algorithms in coding theory, IEEE Transactions on Information Theory, **Vol. 42** no.6 (1996), 2053-2057.

[7] A. C. H. Ling, P. C. Li, and G. H. J. van Rees. Splitting systems and separating systems. Discrete Mathematics, **279**, no. 1-3 (2004), 355-368.

[8] P. C. Li, and G. H. J. van Rees. Lotto Designs. in Handbook of Combinatorial Designs (Editors- C.C.Colbourn and J.H.Dinitz), (2007), 512-518.

[9] L. Lovász. On the ratio of optimal integral and fractional covers, Discrete Mathematics, **13** (1975), 383-390.

[10] K. Mehlhorn. On the program size of perfect and universal hash functions, in Proc. 23rd Annual IEEE Symposium on Foundations of Computer Science, pp. 170–175.

[11] S. K. Stein, Two combinatorial covering problems, J.Combinatorial Theory, Ser. A, **16** (1974), 391-397.

[12] V. Rödl, On a packing and covering problem, European Journal of Combinatorics **6** (1985), 69-78.

[13] D. R. Stinson. Some baby-step giant-step algorithms for the low hamming weight discrete logarithm problem. *Mathematics of Computation* **Vol. 71**, no 237 (2001), 379–391.

[14] D. R. Stinson, Tran van Trung and R. Wei. Secure frameproof codes, key distribution patterns,group testing algorithms and related structures, Journal of Statistical Planning and Inference, **86** (2000), 595-617.