Three Constructions of Covers[1]

G.H.J. van Rees[2]

Dept. of Computer Science
University of Manitoba
Winnipeg, Manitoba
Canada R3T 2N2
e-mail: vanrees@ccm.umanitoba.ca

Abstract. Three general constructions for covers are given. A cover is a set of k-subsets of a v-set, V, such that every t-subset of V is contained in at least one of the k-sets. These constructions use the idea of dividing the v-set into either two or three equal sized subsets. The last two constructions also use the idea of establishing a correspondence between the two equal subsets in order to facilitate the construction.

1. Introduction

A (v,k,t)-cover is a set of k-subsets of a v-set, V, such that every t-subset of V is contained in at least one of the k-sets. We let $v \geq k \geq t$. The k-sets are often called blocks and the covers are often called covering designs. We define $C(v,k,t)$ to be the minimum number of blocks in any (v,k,t)-cover. It is convenient to set $C(v,k,t) = 1$ if $k > v \geq t$ and $C(v,k,t) = 0$ if $v < t$.

There are two main reasons why we study $C(v,k,t)$. The first reason is that the covers that have the extreme number of blocks often are special combinatorial objects like Balanced Incomplete Block Designs or Geometries. In the cases where the minimum covers are not special configurations (usually because the special configuration does not exist for the required parameters), the minimal covers are good approximations to the combinatorial configurations.

The second reason we study them is that they are used in betting schemes for lotteries. The idea is as follows. The gambler must pick r numbers from n numbers and pays a small fee for the privilege. The lottery company on the appointed day also chooses, at random, r numbers from n numbers. These r numbers are the winning numbers. The r is usually small like 6 and the n is somewhere around 50. If a gambler's ticket intersects the winning numbers in r numbers, he wins millions. If the intersection is smaller, he wins a lesser amount—the smaller the intersection, the smaller the winnings. Gamblers believe in lucky numbers. They have 10 to 20 of them. They would bet all combinations of them but that is too expensive. So entrepreneurs sell gamblers schemes to bet on certain combinations of these "lucky" numbers guaranteeing a minimum payoff if a subset of the lucky

[1] Some of the material in this paper was first presented at the Sixth Midwestern Conference on Combinatorics, Crytography and Computing that was held at the University of Nebraska in Lincoln, Nebraska on October 31 to November 2 of 1991.

[2] Supported by NSERC grant OGP0003558

numbers are picked as winning numbers. These schemes are exactly (v,k,t)-covers. However, the entrepreneurs seldom discover or get close to finding the value of $C(v,k,t)$. Of course, a lottery ticket is a fool's bet.

Nevertheless, there is or should be an interest in covers. In the rest of the paper, I will present three constructions for covers. I hope that this will stimulate interest in this problem and that more people will study this problem.

2. Known Results

There are not many results known about $C(v,k,t)$. We will state the two main results about lower bounds. Because the proofs are simple counting arguments we leave them out. The proofs may be found in a splendid survey paper by Mills and Mullin [2].

Theorem 2.1.

$$C(v,k,t) \geq \left\lceil \frac{vC(v-1,k-1,t-1)}{k} \right\rceil$$

Theorem 2.2.

$$C(v,k,t) \geq \left\lceil \frac{v}{k} \left\lceil \frac{v-1}{k-1} \left\lceil \cdots \left\lceil \frac{v-t+1}{k-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil$$

For upper bounds, constructions are used. The upper and lower bounds meet only when v, k, t, $v-k$, or $C(v,k,t)$ are quite small. There are open problems everywhere. Mills and Mullin review these results [2].

3. Constructions

The first construction is an old one by Turan [5]. In fact, he stated this problem as a graph theoretic problem before covers were discovered. We will not use graph theory terminology but we will use what are now called Turan Designs. We define a Turan Design (v,p,k) to be a set of k-subsets (blocks) of a v-set, V, such that every p-subset of V contains (or is represented by) at least one of the k-sets. Define $T(v,p,k)$ to be the minimum number of blocks in any Turan Design (v,p,k).

It is easy to check that if one has a (v,k,t)-cover and if one replaces each block of the cover with its complement in V, then one obtains a Turan Design $(v,v-t,v-k)$. Of course, if one complements the blocks of a Turan Design, one gets a cover. Lemma 3.3 follows.

Lemma 3.3.

$$C(v,k,t) = T(v,v-t,v-k).$$

We will now show how to construct Turan Designs $(v,4,3)$. Let the set of elements be V and split them into three sets as equally as possible. Call the sets V_0, V_1, and V_2. Define two groups of blocks. Group 1 consists of all 3-sets that

are purely from V_0, V_1, or V_2. The second group of blocks consists of all possible blocks that contain 2 elements from V_i and 1 element from V_{i+1} where the subscripts are taken modulo three.

For example, if $V_0 = \{1,2,3\}$ and $V_1 = \{4,5,6\}$ and $V_2 = \{7,8\}$ then the blocks are: 123 and 456 in group 1 and 124, 125, 126, 134, 135, 136, 234, 235, 236, 457, 458, 467, 468, 567, 568, 781, 782, 783 in group 2.

Proving that this is a Turan Design is fairly straightforward. Consider any 4-set. Consider the triple (i_0, i_1, i_2) where $i_0 + i_1 + i_2 = 4$ and i_j is the number of elements in the 4-set that comes from V_j. If any $i_j = 3$ or 4 then that 4-set is represented by a block in group 1 that consists of three elements from V_j. Otherwise, for some j, we have $i_j = 2$ and $i_{j+1} \geq 1$ where $j+1$ is taken modulo three. This 4-set is represented by a block in group 2 that has the two elements from V_j and one element from V_{j+1}. Hence we have the following theorem.

Theorem 3.4.

$$T(3m+s,4,3) \leq m(m-1+\lceil s/2 \rceil)(2m-1+2\lfloor s/2 \rfloor) \text{ for } 3m+s>3,$$

where $s = 0,1,2$.

Turan went on to conjecture that these designs are minimum design but not necessarily unique. Translating this conjecture to covers, we get the following.

Conjecture 3.5.

$$C(3m+s,3m+s-3,3m+s-4) = m(m-1+\lceil s/2 \rceil)$$
$$(2m-2+2\lfloor s/2 \rfloor) \text{ for } 3m+s>3,$$

where $s = 0,1,2$.

This conjecture has been proved for $v = 4,5,\ldots,12$. In the cases where the upper bound of Theorem 3.4 does not meet the lower bound of Theorem 2.1, there is a great deal of work to be done. For $v \geq 13$, the conjecture is open. For $v = 13$, there is a gap of 6 between the bounds. Better constructions are needed.

The next construction first appeared in Morley and van Rees [4]. This constructs $(4s-4, 2s-2, s)$ covers. Let the v-set, V, be on the elements $1,2,\ldots,4s-4$. Divide V into two sets V_0 and V_1. Let V_0 contain the elements $1,2,\ldots,2s-2$ and let V_1 contain the elements $2s-1, 2s, \ldots, 4s-4$. Also, let the element i in V_0 correspond to the element $i+2s-2$ in V_1. The first set of blocks are all possible blocks consisting of $s-1$ elements from V_0 with the corresponding $s-1$ elements from V_1. The second set of blocks are all possible blocks consisting of $s-1$ elements from V_0 and the $s-1$ non-corresponding elements from V_1. Also included are two blocks: one consisting of the elements from V_0 and the other consisting of the elements of V_1. We obtain the following theorem.

Theorem 3.6.

$$C(4s-4,2s-2,s) \leq 2\binom{2s-2}{s-1} + 2 \text{ for } s \geq 2.$$

Proof: Clearly, the construction has the correct number of blocks. But does it produce a cover? If we consider any s set as an ordered pair (i,j) where $i+j=s$ and where i is the number of elements from V_0 and j is the number of elements from V_1. If $i=s$ or $i=0$, then the set is covered by the one of the two last blocks.

If the s-set, S, has $0 < i < s$, then let the i elements from V_0 be the set A and let the j elements from V_1 be B. Let B consist of B_1, m elements that correspond to m elements in A, and $B_2, j-m$ elements that do not correspond to any element in A. If $m \geq 1$, consider the following $(s-1)$-subset from V_0. It consists of the i elements in A united with the $j-m$ elements in V_0 that correspond to the elements of B_2 united with $s-1-i-j+m = m-1$ other elements from V_0. This set, W, along with its corresponding elements from V_1 form a block containing S. If $m=0$, then consider the following $(s-1)$-subset from V_0. It consists of i elements from A united with any $s-1-i$ elements from V_0 that do not correspond with any element from B_2 and that are not in A. This set, W, along with the elements in V_1 that do not correspond to any element in W form a block that contains S. In either case, the s-set is contained in a block and the construction produces the required cover. ∎

This cover has an automorphism group that is isomorphic to the direct product $S_{t-1} \times S_2$. By looking at the blocks that contain a specific element we get the next theorem which was incorrectly stated in [4].

Theorem 3.7.

$$C(4s-5,2s-3,s-1) \leq \binom{2s-2}{s-1} + 1 \text{ for } s \geq 2.$$

How good are these constructions? For $s=2$ and $s=3$, they are minimal. For $s=4$, they are off by 2 and 1 respectively. Morley and van Rees [4] claimed that $C(11,5,3) = 21$ and hence $C(12,6,4) = 42$. As pointed out by Mills [1], this is incorrect. Mills discovered these three base blocks: $\{\infty,1,6,2,7\}$, $\{\infty,1,6,3,7\}$ and $\{0,2,3,4,6\}$ which when developed modulo 10, show that $C(11,5,3) = 20$ and it is also unique. Hence, $40 \leq C(12,6,4) \leq 42$. For larger s, the construction probably does not produce minimal covers but they are the best ones known.

The third construction is new and is for $C(4s,4s-4,2s+1)$. Since $v-k=4$, it is easier to describe the construction if we do it as a Turan Design $(4s,2s-1,4)$. Divide the $4s$ elements of the v-set, V, into two sets, V_0 containing $1,2,\ldots,2s$ and V_1 containing $2s+1,2s+2,\ldots,4s$. Also let element i in V_0 and the element $i+2s$ in V_1 correspond to each other. The blocks fall into two types.

To construct the first type of block think of the elements of V_0 as the points of a complete graph and consider the $2s-1$ disjoint one factors in some complete one-factorization of the complete graph of K_{2s}. For each pair of elements, i and j, that represent one edge in a one factor, form s blocks containing i, j and all possible pairs of elements from V_1 which correspond to the pairs in that one factor. e.g. if $s = 4$ and the one factor was 12 34 56 78 then the 4-sets containing 1 and 2 are $\{1,2,9,10\}$, $\{1,2,11,12\}$, $\{1,2,13,14\}$ and $\{1,2,15,16\}$. Since it is well known that a complete one-factorization exists for K_n when n is even, this constructs $s2(2s-1)$ blocks. Note the construction could have been done using V_1 and V_0 interchanged and we would have an identical result. So we will talk about the one factors of V_1 also.

The second type of block is constructed from other Turan Designs as follows. Add on the blocks of a Turan Design $(2s, 2s-2, 4)$ twice, once on the elements of V_0 and once on the elements of V_1. We now state the theorem.

Theorem 3.8.

$$T(4s, 2s-1, 4) \leq s^2(s-1) + 2T(2s, 2s-2, 4) \text{ for } s > 3.$$

Proof: It is clear that the construction produces the correct number of blocks but do they form a Turan Design? Any $2s-1$ set can be considered as an ordered pair (i,j) where $i + j = 2s - 1$. The i represents the number of elements from V_0 and the j represents the number of elements from V_1. The blocks of the first type represent all $2s-1$ sets with i and j greater than or equal to 2. Let T be such a $(2s-1)$-set and let A be the set of elements from V_0 in T. Let B_1 be the set of elements from V_1 in T that correspond to some element in A. Let B_2 be the set of elements from V_1 in T that do not correspond to some element in A. Let $|B_1| = m$ and $|B_2| = j - m$. Let $2 \leq j < s$.

If $m \geq 2$, then let x and y be elements in B_1. Clearly, every pair of elements in V_1 occurs as an edge in some one factor of the complete one-factorization of the complete graph on the vertices labelled with elements of V_1. The corresponding points to x and y, call them xx and yy, are in A and are an edge in the corresponding one factor. So $\{xx, yy, x, y\}$ represents T. If $m \leq 1$ and $j - m \geq 2$, then let x and y be elements in B_2 and let xx and yy be their corresponding elements which are not in A. Consider the one factor containing xy and the corresponding one factor containing $xxyy$. The corresponding one factor has an additional $s-1$ edges. Since $i \geq s$, one edge of the corresponding one factor has ends in A, call the ends a and b. Then, $\{a, b, x, y\}$ represent T. The one case that is left out is if $j - m = 1$, $m = 1$ and $i = 2s-3$. Let x be in B_1 and y in B_2. Let xx correspond to x and xx is in A. Let yy correspond to y and it is not in A. Consider the one factor containing xy and the corresponding one factor containing $xxyy$. The number of other edges in the corresponding one factor is $s-1$ while the number of elements, other than xx in A, is $2s-4$ which is bigger than $s-1$ for $s > 3$. So

one edge of the corresponding one factor has ends in A and $\{a, b, x, y\}$ represents T, where a and b are the ends of that edge.

When $j \geq s$, then $i < s$ and the argument can be done with V_0 and V_1 switched. When one of i or j is less than two, then the blocks of the second type represent the t-sets. ∎

It happens that $T(2s, 2s-2, 4)$ is a small number. In [2], it can be checked that $T(8,6,4) = 6$, and $T(10,8,4) = 4$. For $s \geq 6$, $T(2s, 2s-2, 4) = 3$, as is shown by this Turan Design: $\{\{1,2,3,4\}, \{5,6,7,8\}, \{9,10,11,12\}\}$. It is true that Theorem 3.8 requires that $s \geq 4$ but a similar construction still works for $s = 2, 3$. The blocks of type 1 are the same but the blocks of type two require a different Turan Design. For $s = 2$, use a Turan Design $(4,4,4)$ on 1 block. For $s = 3$, use a Turan Design $(6,5,4)$ on 3 blocks. These two small Turan Designs are trivial to construct. The proof of Theorem 3.8 does not apply for $s = 2$ or 3 unless p is increased. Therefore using Lemma 3.3, we can write Theorem 3.8 in terms of covers as follows. A $(12,8,6)$ covering design on 51 blocks was first found by Morley [3].

Theorem 3.9.

$$C(8,4,3) = 14$$
$$C(12,8,6) \leq 51$$
$$C(16,12,9) \leq 124$$
$$C(20,16,11) \leq 233$$
$$C(4s, 4s-4, 2s+1) \leq s^2(2s-1) + 6, \text{ for } s \geq 6.$$

By checking the tables in [2], the $(8,4,3)$-cover is best possible and the $(12,8,6)$-cover is off by at most 3. For larger covers in this family it is hard to say how good the construction is. Of course, Theorem 2.1 can be used to get bounds in the non-zero modulo 4 cases.

At this point, we will now give a generalization to Theorem 3.6 which was not in Morley and van Rees. It is more convenient to prove this theorem using Turan Designs. The construction for a Turan Design $(4r+2e, 3r-1, 2r)$ proceeds as follows. Divide the $v = 4r + 2e$ set, V, into two sets of elements. The first set, V_0, consists of the elements $1, 2, 3, \ldots, 2r+e$ while the second set, V_1, consists of the elements $2r+e+1, 2r+e+2, \ldots, 4r+2e$. Also the element i from V_0 corresponds to the element $i + 2r + e$ in V_1 and vice versa.

There are two groups of blocks. The first group consists of all possible $2r$-sets exclusively from V_0 or exclusively from V_1. The second group of blocks consists of every possible r-subset from V_0 united with the corresponding r-set from V_1 along with every possible r-subset from V_0 united with each possible r-set consisting of elements from V_1 that do not correspond to any element in the r-subset. This construction allows us to state the following theorem.

Theorem 3.10.

$$T(4r+2e,3r-1,2r) \leq 2\binom{2r+e}{2r} + \binom{2r+e}{r}\left[1+\binom{r+e}{r}\right],$$

for $r \geq 1, e \geq 0$.

Proof: Clearly the construction above produces the correct number of blocks so we need only prove that a Turan Design is constructed. Let the $(3r-1)$-set, T, consist of the set A which consists of i elements from V_0 and the set B which consists of j elements from V_1. Let B consist of the set B_1 which consists of m elements that correspond to some element in A and the set B_2 that consists of $j-m$ elements that do not correspond to any element in A.

If i or j is less than r, the $(3r-1)$-set, T, is represented by one of the blocks in the first group. If $2r-1 \geq i \geq r$, then either $m \geq r$ in which case T is represented by a group 2 block consisting of any r elements from B_1 and the corresponding r elements from A; or $m < r$ and the situation is a bit more complicated. If $j-m \geq r$, then T is represented by any r elements from B_2 along with any r elements from A. If $j-m < r$, then T is represented by the elements of B_2 along with any $r-j+m$ elements from B_1 along with r elements from A that do not correspond to any elements from B_1. Since $i-(r-(j-m)) = 3r-1-r-m = 2r-1-m \geq 2r-1-(r-1) = r$, we know that there are r elements in A with the required property. ∎

Translating this theorem to cover terminology, the following theorem is obtained.

Theorem 3.11.

$$C(4r+2e,2r+2e,r+2e+1) \leq 2\binom{2r+e}{2r} + \binom{2r+e}{r}\left[1+\binom{r+e}{r}\right]$$

for $r \geq 1, e \geq 0$.

This construction gives the its best result when e equals 0 or 1.

There must be many more constructions of this type that give good results. Hopefully, this paper will stimulate more research in this area.

References

1. W.H. Mills. Private communication.
2. W.H. Mills and R.C. Mullin, *Coverings and Packings*, in "Contemporary Design Theory—A Collection of Surveys", ed. J.H. Dinitz and D.R. Stinson, John Wiley Sons Inc., 1992.
3. M. Morley. Private communication.
4. M. Morley and G.H.J. van Rees, *Lottery Schemes and Covers*, Utilitas Math. 37 (1990), 159–166.
5. P. Turan, *Eine Extremalaufgabe aus der Graphtheotie*, Mat. Fiz. Lapok 48 (1941), 436–452.