New Constructions of Lotto Designs

Pak Ching Li
Department of Computer Science
University of Manitoba
email : lipakc@cs.umanitoba.ca

G. H. John Van Rees
Department of Computer Science
University of Manitoba
email : vanrees@cs.umanitoba. ca

April 28, 2004

Abstract

An $LD(n, k, p, t; b)$ Lotto Design is a set of b k-sets (blocks) of an n-set such that any p-set intersects at least one k-set in t or more elements. Let $L(n, k, p, t)$ denote the minimum number of blocks in any $LD(n, k, p, t; b)$ Lotto Design. We shall discuss several techniques for constructing Lotto designs and determining upper bounds for $L(n, k, p, t)$.

1 Introduction

There are many lotteries in the world. They tend to be very similar in operation. The way most lotteries work is as follows. For a small fee, a person chooses k numbers from n numbers or has the numbers chosen randomly for him. This is the ticket. At a certain point no more tickets are sold and the government or casino picks p numbers from the n numbers, usually in a random fashion. These are called the winning numbers. If any of the tickets sold match t or more of the winning numbers, then a prize is given to the holder of the matching ticket. The larger the value of t, the larger the prize. Usually t must be three or more to receive a prize. Many people and researchers are interested to know what is the minimum number of tickets necessary to ensure that at least one ticket will intersect the winning numbers in t or more numbers, for varying values of t. For an enlightening overview on this subject see Colbourn and Dinitz[2].

More formally we may define an (n, k, p, t) Lotto Design to be a set of k-sets (blocks or tickets) of an n-set such that any p-set intersects at least one k-set in t or more elements. An LD$(n, k, p, t; b)$ is a (n, k, p, t) Lotto Design with exactly b blocks. Let $L(n, k, p, t)$ denote the minimum number of blocks in any $LD(n, k, p, t; b)$. We define $X(n)$ to be the set $\{1, 2, ..., n\}$. Clearly these definitions mirror the lottery situation and the fundamental problem is to determine $L(n, k, p, t)$. The following is a typical example of a Lottery Design.

Example 1.1 *:* $LD(13, 6, 5, 3; 5) = \{\{1, 2, 3, 4, 5, 6\}, \{1, 2, 3, 4, 5, 7\}, \{1, 2, 3, 4, 6, 7\}, \{1, 2, 3, 5, 6, 7\}, \{8, 9, 10, 11, 12, 13\}\}$

Two special subclasses of Lotto designs are covering designs and Turán designs. A (n, k, t) covering design is an (n, k, t, t) Lotto design and a (n, p, t) Turán design is an (n, t, p, t) Lotto design. The minimum number of blocks in any (n, k, t) is denoted by $C(n, k, t)$ and the minimum number of blocks of any (n, p, t) Turán design is denoted by $T(n, p, t)$. Both covering and Turán designs have been thoroughly studied. A good introduction to covering designs and Turán designs may be found in [2].

Upper bounds for Lotto designs are often determined using computer search algorithms. Bate [1] described an exhaustive search algorithm to determine the value $L(n, k, p, t)$. Nurmela and Ostergard [7] used simulated annealing to generate upper bounds for Lotto designs. Li [6] discusses several other algorithms for constructing Lotto designs. The unfortunate feature of computer search algorithms is that the search space tends to grow exponentially with respect to the values of n, k, p and t. Thus, most search algorithms are infeasible to run except for small values of n, k, p and t. Thus, it is important to have techniques for constructing Lotto designs which can be stated as a formula which involves no searching. The goal of this paper is to demonstrate several techniques for constructing Lotto designs. Some constructions make use of balanced incomplete block designs (BIBD) and others make use of existing Lotto designs.

2 History

Since Lotto designs are often obtained using some search algorithm, there are not many well known upper bound formulas. We shall state several well know upper bound formulas in this section.

In order to get an upper bound using covering designs, we partition the n-set into $p-1$ sets of sizes $a_1, a_2, ..., a_{p-1}$. On each part, contruct an (a_i, k, t) covering design. Now any p-subset intercepts one of these $p-1$ parts in at least two elements and since there is a cover on each part, any p-subset must intersect one of the blocks in at least two elements. Thus we can state the following result.

Theorem 2.1 *:*

$$L(n,k,p,2) \leq \min_{\sum_{i=1}^{p-1} a_i = n} \left(L(a_1,k,2,2) + ... + L(a_{p-1},k,2,2) \right).$$

The following result which appears in [2] is another useful upper bound formula.

Theorem 2.2 *: If $n = n_1 + n_2$ and $p = p_1 + p_2 - 1$, then $L(n,k,p,t)$ $\leq L(n_1,k,p_1,t)$ $+L(n_2,k,p_2,t)$.*

This result was applied to $L(49,6,6,3)$ giving

$$L(49,6,6,3) \leq L(22,6,3,3) + L(27,6,4,3).$$

It is well known that there exists a $(22,6,3)$ Steiner triple system with 77 blocks and $L(27,6,4,3)$ was determined to be at most 91, by simulated annealing. Hence $L(49,6,6,3) \leq 168$. Thus, for Canada's Lotto 6/49 lottery, if you buy a specific set of 168 tickets, you are guaranteed to match 3 numbers paying you \$10. Note that each ticket costs \$1.

3 BIBDs and Lotto Designs

The study of balanced incomplete block designs (BIBDs) was started by Euler and has been continuously studied since the Fisher and Yates paper [3] in 1935. Our focus is on determining which BIBDs are Lotto designs. We begin by stating conditions that a BIBD must satisfy in order for it to be a Lotto design. Then we consider resolvable BIBDs and symmetric BIBDs. We state conditions that must be satisfied in order for them to be Lotto designs. We begin by giving a definition for a BIBD. A good reference on BIBDs, resolvable BIBDS and symmetric BIBDS can be found in [5].

Definition 3.1 : *An (v, b, r, k, λ) BIBD is a collection of b k-sets with elements chosen from a v-set such that each element appears r times and each pair appears λ times in the collection of k-sets.*

Theorem 3.1 : *If $\mathcal{B}$ is the set of blocks of a (v, b, r, k, λ) BIBD and p, t are positive integers where $\left\lfloor \frac{pr}{t-1} \right\rfloor \binom{t-1}{2} + \binom{pr - \lfloor \frac{pr}{t-1} \rfloor (t-1)}{2} < \binom{p}{2}\lambda$, then $\mathcal{B}$ is the set of blocks of an (v, k, p, t) Lotto design. Hence $L(v, k, p, t) \le b$.*

Proof : Let $\mathcal{B}$ denote the blocks of an (v, b, r, k, λ) BIBD. Suppose P is a p-set not represented by any block in $\mathcal{B}$. By the definition of a BIBD, each pair appears λ times in $\mathcal{B}$. Thus, the pairs of P appear $\binom{p}{2}\lambda$ times in $\mathcal{B}$. On the other hand, since P is not represented in $\mathcal{B}$, at most $t-1$ elements from P can appear together in any block of $\mathcal{B}$. The maximum number of pairs of P that can be forced in $\mathcal{B}$ is

$$\left\lfloor \frac{pr}{t-1} \right\rfloor \binom{t-1}{2} + \binom{pr - \lfloor \frac{pr}{t-1} \rfloor (t-1)}{2}. \tag{1}$$

But $\left\lfloor \frac{pr}{t-1} \right\rfloor \binom{t-1}{2} + \binom{pr - \lfloor \frac{pr}{t-1} \rfloor (t-1)}{2} < \binom{p}{2}\lambda$, by assumption, which is a contradiction. Hence all p-sets are represented in $\mathcal{B}$ and therefore $\mathcal{B}$ is an (v, k, p, t) Lotto design. □

We now give an example of the application of theorem 3.1 using the existence of a $(17, 34, 16, 8, 7)$ BIBD, whose existence can be confirmed in [2].

Example 3.1 *: Since there exists an* $(17, 34, 16, 8, 7)$ *BIBD that satisfies the conditions of the Theorem 3.1,* $L(17, 8, 6, 4) \leq 34$.

The following three results are consequences of Theorem 3.1.

Corollary 3.1 *: Suppose there exists a* (v, b, r, k, λ) *BIBD. If* $r < 2\lambda$ *, then* $L(v, k, 5, 4) \leq b$.

Proof : With the current parameters, Equation (1) becomes

$$\left\lfloor \frac{5r}{3} \right\rfloor \begin{pmatrix} 3 \\ 2 \end{pmatrix} + \begin{pmatrix} 5r - \left\lfloor \frac{5r}{3} \right\rfloor 3 \\ 2 \end{pmatrix}.$$

This simplifies to $5r$ if $3|r$ and to $5r - 1$ if $3 \not| r$. In any case, $p \leq 5r \leq 10\lambda$. So we can apply Theorem 3.1 and obtain $L(v, k, 5, 4) \leq b$. □

Corollary 3.2 *: Suppose there exists a* (v, b, r, k, λ) *BIBD. If* $r < \frac{5}{2}\lambda$*, then* $L(v, k, 6, 4) \leq b$

Proof : With the current parameters, Equation (1) reduces to

$$\left\lfloor \frac{6r}{3} \right\rfloor \begin{pmatrix} 3 \\ 2 \end{pmatrix} + \begin{pmatrix} 6r - \left\lfloor \frac{5r}{3} \right\rfloor 3 \\ 2 \end{pmatrix} = 6r.$$

Since $r < \frac{5}{2}\lambda$, then $6r < 15\lambda$. Thus, the conditions of Theorem 3.1 are satisfied and $L(v, k, 6, 4) \leq b$. □

Corollary 3.3 *: Suppose there exists a* (v, b, r, k, λ) *BIBD. If* $r < 3\lambda$*, then* $L(v, k, 7, 4) \leq b$.

Proof : With the current parameters, Equation (1) reduces to

$$\left\lfloor \frac{7r}{3} \right\rfloor \begin{pmatrix} 3 \\ 2 \end{pmatrix} + \begin{pmatrix} 7r - \left\lfloor \frac{5r}{3} \right\rfloor 3 \\ 2 \end{pmatrix}. \qquad (2)$$

Regardless of whether 3 divides r or not, Equation (2) is less than or equal to $7r$. Since $r < 3\lambda$, we have $7r < 21\lambda$. Thus, the conditions of Theorem 3.1 are satisfied and $L(n, k, 7, 4) < b$. □

Theorem 3.1 is a general result that covers all types of BIBDs. It is possible to determine weaker conditions than those given by Theorem 3.1 if the design is resolvable. We begin by stating the definition of a *resolvable BIBD.*

Definition 3.2 : *An (v, b, r, k, λ) BIBD is resolvable if the blocks of the BIBD can be partitioned into sets in such a way that every partition contains each point exactly once. A BIBD that is resolvable is called a resolvable BIBD (RBIBD). The partitions are called resolution classes.*

The parameters for a resolvable BIBD must be of the form (ks, rs, r, k, λ) where $r = \frac{\lambda(ks-1)}{k-1}$. For RBIBDs, a slightly weaker sufficient condition may be stated for it to be a Lotto design.

Theorem 3.2 : *If there exists a resolvable BIBD with parameters $(xk, \frac{\lambda x(xk-1)}{k-1}, \frac{\lambda(xk-1)}{k-1}, k, \lambda)$ and if p, t are positive integers where*

$$\left(\left\lfloor \frac{p}{t-1} \right\rfloor \binom{t-1}{2} + \binom{p - \lfloor \frac{p}{t-1} \rfloor (t-1), 2)}{2} \right) \frac{\lambda(xk-1)}{k-1} < \binom{p}{2} \lambda,$$

then $L(xk, k, p, t) \leq b$.

Proof : Let $\mathcal{B}$ denote the blocks of a $(xk, \frac{\lambda x(xk-1)}{k-1}, \frac{\lambda(xk-1)}{k-1}, \frac{\lambda(xk-1)}{k-1}, k, \lambda)$ BIBD. Suppose P is a p-set not represented by any block in $\mathcal{B}$. By the definition of a BIBD, each pair appears λ times in $\mathcal{B}$. Thus, the pairs of P appear $\binom{p}{2} \lambda$ times in $\mathcal{B}$. On the other hand, since P is not represented in $\mathcal{B}$, at most $t-1$ elements from P can appear together in any block of $\mathcal{B}$. In each resolution class, the elements of the set P must appear exactly once. Thus the maximum number of pairs of P in any given resolution class of the design is :

$$\left\lfloor \frac{p}{t-1} \right\rfloor \binom{t-1}{2} + \binom{p - \lfloor \frac{p}{t-1} \rfloor (t-1), 2)}{2}.$$

Since there are $\frac{\lambda(xk-1)}{k-1}$ resolution classes in the design, the maximum number of pairs from P in the design is

$$\left[\left\lfloor \frac{p}{t-1} \right\rfloor \binom{t-1}{2} + \binom{p - \lfloor \frac{p}{t-1} \rfloor (t-1), 2)}{2} \right] \frac{\lambda(xk-1)}{k-1}. \tag{3}$$

But by assumption,

$$\left[\left\lfloor \frac{p}{t-1} \right\rfloor \binom{t-1}{2} + \binom{p - \lfloor \frac{p}{t-1} \rfloor (t-1), 2)}{2} \right] \frac{\lambda(xk-1)}{k-1} < \binom{p}{2} \lambda.$$

This is a contradiction since the number of pairs of P occurring in $\mathcal{B}$ must be at least $\binom{p}{2} \lambda$. Therefore every p-set is represented by the design. $\square$

Corollary 3.4 : *If an* $(2a+2, 4a+2, 2a+1, a+1, a)$ *RBIBD exists, and* $4 < t < 2a+4$*, then* $L(2a+2, a+1, 2t-3, t) \leq 4a+2$.

Proof : Consider a $(2a+2, 4a+2, 2a+1, a+1, a)$ RBIBD $\mathcal{B}$. Using the notation of theorem 3.2, $p = 2t-3$, $\lambda = a$, $k = a+1$ and $x = 2$. Equation 3 becomes

$$\left[\left\lfloor \frac{2t-3}{t-1} \right\rfloor \binom{t-1}{2} + \binom{2t-3-\left\lfloor \frac{2t-3}{t-1} \right\rfloor (t-1)}{2}\right](2a+1).$$

If this is less than $a\binom{2t-3}{2}$, then the conditions of theorem 3.2 are satisfied and hence our result holds. Now,

$$\left[\left\lfloor \frac{2t-3}{t-1} \right\rfloor \binom{t-1}{2} + \binom{2t-3-\left\lfloor \frac{2t-3}{t-1} \right\rfloor (t-1)}{2}\right](2a+1) < a\binom{2t-3}{2}$$

if and only if $2t^2 - (8+2a)t + 4a + 8 < 0$. This is the case if and only if $4 < t < 2a+4$. But we assumed that this was the case. Hence, $\mathcal{B}$ is a $(2a+2, a+1, 2t-3, t)$ Lotto design with $4a+2$ blocks. □

We now state some examples of Resolvable BIBDs that are Lotto designs. Notice that one RBIBD may give several Lotto designs.

Example 3.2 : *Consider a* $(12, 22, 11, 6, 5)$ *resolvable BIBD. Its existence is confirmed by [2]. Since*

$$\left[\left\lfloor \frac{5}{3} \right\rfloor \binom{3}{2} + \binom{5-\left\lfloor \frac{5}{3} \right\rfloor (3), 2}{2}\right] 11 < \binom{5}{2} 5,$$

then $L(12, 6, 5, 4) \leq 22$ *by Corollary 3.4.*

Example 3.3 : *Consider an* $(8, 14, 7, 4, 3)$ *RBIBD. Its existence is confirmed by [2]. By corollary 3.4, we have* $L(8, 4, 3, 3) \leq 14$ *and* $L(8, 4, 5, 4) \leq 14$.

Example 3.4 : *Consider a* $(12, 22, 11, 6, 5)$ *RBIBD. Its existence is confirmed by [2]. By corollary 3.4, we have* $L(12, 6, 3, 3) \leq 22$ *and* $L(12, 6, 5, 4) \leq 22$.

Example 3.5 : *Consider a* $(16, 30, 15, 8, 7)$ *RBIBD. Its existence is confirmed by [2]. By corollary 3.4, we have* $L(16, 8, 3, 3) \leq 30$*,* $L(16, 8, 5, 5) \leq 30$ *and* $L(16, 8, 7, 5) \leq 30$.

Symmetric BIBDs are another special type of BIBDs. For a specific collection of symmetric BIBDs, a sufficient condition may be stated for it to be a Lotto design.

Definition 3.3 : *A BIBD is a symmetric BIBD (SBIBD) if* $v = b$.

The following result applies specifically to symmetric designs.

Theorem 3.3 : *If there exists a* $(4a + 3, 4a + 3, 2a + 1, 2a + 1, a)$ *symmetric BIBD and* $a > t-2$, *then* $L(4a+3, 2a+1, 2t-2, t) \leq 4a+3$.

Proof: Let $\mathcal{B}$ denote the blocks of a $(4a + 3, 4a + 3, 2a + 1, 2a + 1, a)$ symmetric BIBD. Suppose P is a $(2t-2)$-set not represented by any block in $\mathcal{B}$. There are $\binom{2t-2}{2}a$ pairs of P in $\mathcal{B}$. On the other hand, each variety appears $2a + 1$ times in $\mathcal{B}$. Since P can intersect a block in $\mathcal{B}$ in at most $t-1$ elements, the maximum number of these pairs of elements of P can be obtained if P intersects blocks in $\mathcal{B}$ in $t-1$ elements. The number of blocks that P can intersect in $t-1$ elements is $\lfloor \frac{(2a+1)(2t-2)}{t-1} \rfloor = 2(2a+1)$ giving $2(2a+1)\binom{t-1}{2}$ pairs. Now $2(2a+1)\binom{t-1}{2} \leq \binom{2t-2}{2}a$ which simplifies to $a \leq t-2$ which is a contradiction. Hence, every $(2t-2)$-set must be represented by $\mathcal{B}$ and hence $\mathcal{B}$ is a $(4a + 3, 2a + 1, 2t - 2, t)$ Lotto design. □
The following is an example of an SBIBD that is a Lotto design.

Example 3.6 : *Consider a* $(15, 15, 7, 7, 3)$ *symmetric design. Its existence is confirmed by [2]. Since* $a = 3, t = 4$ *and* $a > t - 2$, *then the* 15 *blocks of the BIBD form an* $(15, 7, 6, 4)$ *Lotto design.*

As we have seen, under certain conditions, balanced incomplete block designs may be Lotto designs so that BIBDs may be able to give an upper bound for Lotto Designs. However, these upper bounds may not always be very good due to the strict conditions that BIBDs adhere to. The results in this section have been used to generate upper bounds for Lotto designs which we keep in tables. We have established a link between BIBDs and Lotto designs which generates upper bounds for Lotto Designs based on BIBDs. In most cases, the upper bounds for $L(n, k, p, t)$ derived from BIBDs were super-ceded by upper bounds generated by other methods. However, a BIBD was used in determining that $L(13, 4, 5, 3) = 13$, which has not been superceded.

4 Semi-Direct Product Construction

Constructing Lotto designs based on other Lotto designs is one way to obtain upper bounds. The methods described in this section uses this technique. We termed the construction in this section "Semi-Direct Product" construction. The construction technique described may be used to obtain an (n, k, p, t) Lotto design for arbitrary values of n,k,p and t. In general, the larger the value of k, the better the construction will be.
We begin with a useful lemma.

Lemma 4.1 *: Suppose $\mathcal{B}$ is an (n, k, p, t) Lotto design. If $m \leq p$ is an integer, then any m-set intersects some block of $\mathcal{B}$ in at least $t - p + m$ elements.*

Proof : Let M be an m-set. Add $p - m$ elements to M to form a p-set P. Since P now has p elements, it is represented by some block B in $\mathcal{B}$. Since at most $p - m$ of the elements added to M to form P can appear in B, then at least $t - p + m$ elements from M appear in B. $\Box$

We now state the main result of this section. This result will give us a way to compute upper bounds for Lotto designs.

Theorem 4.1 *: Suppose n, k, p, t, n_1, k_1 and r are integers such that $n_1 < n$, $p - r \geq t$, $k_1 \geq t - r - 1$ and $k_1 = k - n + n_1$. Then $L(n, k, p, t) \leq L(n_1, k, p - r, t) + L(n_1, k_1, p - r - 1, t - r - 1)$.*

Proof : We shall proceed to construct an (n, k, p, t) Lotto design using $(n_1, k, p - r, t)$ and $(n_1, k_1, p - r - 1, t - r - 1)$ Lotto designs.

Let $\mathcal{A}$ be an $(n_1, k, p - r, t)$ Lotto design, $\mathcal{B}'$ be an $(n_1, k_1, p - r - 1, t - r - 1)$ Lotto design and let C be the set $\{n_1 + 1, n_1 + 2, ..., n\}$. For each block in $\mathcal{B}'$, adjoin the set C to it. Denote this new collection of k-sets as $\mathcal{B}$. We claim that $\mathcal{A} \cup \mathcal{B}$ is an (n, k, p, t) Lotto design.

Consider a p-set P from $X(n)$. Suppose $p - x$ elements in P come from $\{1, 2, 3, ..., n_1\}$ and the remaining x elements of P come from $\{n_1+1, n_1+2, ..., n\}$. Since $n-n_1 = k-k_1$, the set $\{n_1+1, n_1+2, ..., n\}$ has exactly $k - k_1$ elements and hence x can be at most $k - k_1$. We need to show that the p-set is represented by $\mathcal{A} \cup \mathcal{B}$. If $x \leq r$ then the p-set would be represented by a block in $\mathcal{A}$ since it is an $(n_1, k, p-r, t)$

Lotto design. If $r+1 \leq x \leq p$, then by Lemma 4.1, with $m = p - x$, there is a block from $\mathcal{B}'$ that intersects P in at least $t - x$ and P intersects C in x elements. Hence P is represented by a block in $\mathcal{B}$.

Since P is always represented by some block in $\mathcal{A} \cup \mathcal{B}$, we conclude that $\mathcal{A} \cup \mathcal{B}$ is an (n, k, p, t) Lotto design. □

If $r \geq n - n_1$ in the previous theorem, then $\mathcal{B}$ is not used and Theorem 4.1 simplifies to $L(n, k, p, t) \leq L(n_1, k, p - r, t)$.

A construction of a $(20, 10, 6, 4)$ Lotto design using Theorem 4.1 will now be given.

Example 4.1 : Let $n = 20$, $k = 10$, $p = 6$, $t = 4$, $n_1 = 15, r = 1$. Then $k_1 = 5$. Let $\mathcal{A} = \{\{1, 3, 5, 6, 7, 10, 11, 12, 13, 14\}, \{2, 4, 5, 6, 7, 8, 9, 10, 12, 15\}, \{1, 2, 3, 4, 8, 9, 11, 13, 14, 15\}\}$. Let $\mathcal{B} = \{\{3, 5, 6, 10, 12\}, \{1, 7, 9, 11, 14\}, \{2, 4, 8, 13, 15\}\}$ and let $C = \{16, 17, 18, 19, 20\}$. It can be shown that $\mathcal{A}$ is a $(15, 10, 5, 4)$ Lotto design and $\mathcal{B}$ is an $(15, 5, 4, 2)$ Lotto design. We construct $\mathcal{B}'$ from $\mathcal{B}$ and C by adjoining C to each block of $\mathcal{B}$. Thus $\mathcal{B}' = \{\{3, 5, 6, 10, 12, 16, 17, 18, 19, 20\}, \{1, 7, 9, 11, 14, 16, 17, 18, 19, 20\}, \{2, 4, 8, 13, 15, 16, 17, 18, 19, 20\}\}$. By Theorem 4.1, $\mathcal{A} \cup \mathcal{B}$ is a $(20, 10, 6, 4)$ Lotto design. The blocks of this $(20, 10, 6, 4)$ Lotto design are $\{\{1, 3, 5, 6, 7, 10, 11, 12, 13, 14\}, \{2, 4, 5, 6, 7, 8, 9, 10, 12, 15\}, \{1, 2, 3, 4, 8, 9, 11, 13, 14, 15\}, \{3, 5, 6, 10, 12, 16, 17, 18, 19, 20\}, \{1, 7, 9, 11, 14, 16, 17, 18, 19, 20\}, \{2, 4, 8, 13, 15, 16, 17, 18, 19, 20\}\}$.

By applying Theorem 4.1, we can compute uppers bounds for $L(n, k, p, t)$ by varying the value of n_1 (which in turn varies k_1) in the construction of an (n, k, p, t) Lotto design and taking the minimum size of all the designs constructed. This approach can be easily programmed and used to update our tables. Table 1 displays upper bounds for $L(19, 10, 6, 4)$ using the semi-direct product construction. We fixed the value of r from Theorem 4.1 at 1.

We stop computing Table 1 at $n_1 = 11$ because for $n_1 < 11$, the construction makes no sense. In general, for fixed r, we would stop when $k_1 < t - r - 1$ for an (n, k, p, t) design. From Table 1, we see that the best upper bound for $L(19, 10, 6, 4)$ determined using the semi-direct product construction is 6.

The semi-direct product construction allowed us to construct an arbitrary (n, k, p, t) Lotto design from smaller Lotto designs. This

n_1	Sub-designs used	upper bound obtained
18	$(18, 10, 5, 4)$	14
17	$(17, 10, 5, 4)$ and $(17, 8, 4, 2)$	11
16	$(16, 10, 5, 4)$ and $(16, 7, 4, 2)$	8
15	$(15, 10, 5, 4)$ and $(15, 6, 4, 2)$	6
14	$(14, 10, 5, 4)$ and $(14, 5, 4, 2)$	6
13	$(13, 10, 5, 4)$ and $(13, 4, 4, 2)$	8
12	$(12, 10, 5, 4)$ and $(12, 3, 4, 2)$	11
11	$(11, 10, 5, 4)$ and $(11, 2, 4, 2)$	16

Table 1: Some upper bounds generated by semi-product construction

construction empowered us with another way of obtaining an upper bound for $L(n, k, p, t)$. This construction works best when k is large. This is because a large value of k gives more ways of constructing a Lotto design from smaller ones. This construction does not work well for cases where k is close to p or t. Finally, since this construction depends on other Lotto designs, better upper bounds for these designs would generate a better design.

5 Other Upper Bound Constructions

In this section, we will state other upper bound constructions that we have developed.

One way of constructing an $(n+1, k+1, p+1, t+1)$ Lotto design from an (n, k, p, t) Lotto design and an $(n, k+1, p+1, t+1)$ Lotto design is to attach to each block of the (n, k, p, t) design the element $n+1$. The blocks of this new design along with the blocks of the $(n, k+1, p+1, t+1)$ design form an $(n+1, k+1, p+1, t+1)$ Lotto design. This result is a direct generalization of a result on Covering designs that can be found in the CRC handbook [2].

Theorem 5.1 *:* $L(n+1, k+1, p+1, t+1) \leq L(n, k, p, t) + L(n, k+1, p+1, t+1)$.

Proof: Let $\mathcal{A}$ be an (n, k, p, t) Lotto design and $\mathcal{B}$ be and $(n, k+1, p+1, t+1)$ Lotto design. To each block of $\mathcal{A}$, attach the element $n+1$ and denote this new collection by $\mathcal{A}^*$. We claim that $\mathcal{A}^* \cup \mathcal{B}$ is an $(n+1, k+1, p+1, t+1)$ Lotto design. To show this, let P be a $(p+1)$-set. If $n+1 \notin P$ then there is a block in $\mathcal{B}$ that represents P. Otherwise, $n+1 \in P$. Then, $P \setminus \{n+1\}$ is a p-set and hence intersects some block A from $\mathcal{A}$ in t elements. The block $\{n+1\} \cup A$ belongs in $\mathcal{A}^*$ by construction, and intersects P in $t+1$ elements. Hence $\mathcal{A}^* \cup \mathcal{B}$ is an $(n+1, k+1, p+1, t+1)$ Lotto design and $L(n+1, k+1, p+1, t+1) \leq L(n, k, p, t) + L(n, k+1, p+1, t+1)$. □

In the study of Covering designs, it is well known that $C(mn, mk, t) \leq C(n, k, t)$ for any integer $m \geq 1$. For Lotto designs, the obvious generalization is not always true. An extra condition must be added to the theorem.

Theorem 5.2 *: Suppose there exists an (n, k, p, t) Lotto design D_1 where every $(t-1)$-set is contained in some block of the design. Then $L(mn, mk, p, t) \leq L(n, k, p, t)$ where $m > 1$ is an integer.*

Proof: Let D_1 be an (n, k, p, t) Lotto design such that every $(t-1)$-set appears in the design and the elements of D_1 are $\{1^1, 2^1, 3^1, ..., n^1\}$. Suppose the blocks of D_1 are ordered using some ordering. Since every $(t-1)$-set appears in the design, so does every u-set, for any integer $u < t$. Create $m-1$ copies $D_2, D_3, ..., D_m$ of D_1 keeping D_1's ordering of the blocks, relabeling the elements $\{1^1, 2^1, ..., n^1\}$ in D_i with $\{1^i, 2^i, ..., n^i\}$, for $i = 2$ to m in the obvious way. For each j from 1 to $|D_1|$, unite the j^{th} blocks of $D_1, D_2, ..., D_m$ to form a mk-set. Let D denote the set of all mk-sets formed. We claim that D is an (nm, km, p, t) Lotto design.

Suppose P is a p-set in D. In order to show that D is a Lotto design, we need to show that P is represented by some block of D. Let P be denoted $\{(x_1)^{i_1}, (x_2)^{i_2}, ..., (x_p)^{i_p}\}$ where $x_j \in \{1, 2, ..., n\}$ and $i_j \in \{1, 2, ..., m\}$ for $j = 1$ to p. There are three possible cases that we need to consider.

Case 1 : Suppose all the x_j's are distinct, then the p-set $\{(x_1)^1, (x_2)^1, ..(x_p)^1\}$ is represented by some block in D_1. Without loss of generality suppose $\{(x_1)^1, (x_2)^1, ..., (x_t)^1\}$ appears in this block of D_1. Then the corresponding block in D will contain the subset $\{(x_1)^{i_1}, (x_2)^{i_2}, ..., (x_t)^{i_t}\}$ of P. Thus P is represented in this case.

Case 2 : Suppose not all the x_j's are distinct and some x_j appears at least t times in the collection $\{x_1, x_2, ...x_p\}$. Without loss of generality, suppose $x_1 = x_2 = ... = x_t$. Since $(x_1)^1$ has to appear in some block of D_1, the corresponding block in D must contain the subset

$\{(x_1)^{i_1}, (x_2)^{i_2}, ..., (x_t)^{i_t}\}$ of P. Thus P is represented in this case.
Case 3 : Suppose not all the x_j's are distinct and at most $t-1$ of any of the x_j's are the same, then select t elements from the collection $\{x_1, x_2, ..., x_p\}$ such that at least two of the chosen elements are the same. Without loss of generality, suppose we chose $x_1, x_2, ..x_t$ where $x_1 = x_t$. Now there are at most $t-1$ distinct elements in the collection $\{(x_1)^1, (x_2)^1, ..., (x_t)^1\}$, since $x_1 = x_t$. By hypothesis, the set $\{(x_1)^1, (x_2)^1, ..., (x_t)^1\}$ is contained in some block of D_1. Then the corresponding block in D will contain the subset $\{(x_1)^{i_1}, (x_2)^{i_2}, ..., (x_t)^{i_t}\}$ of P. Thus P is represented in this case.

In each case, the p-set P is represented in D. Hence D is an (nm, km, p, t) Lotto design and $L(mn, km, p, t) \leq L(n, k, p, t)$. □

The construction process above is called "m-ing a design". The following is a special case of a result from Bate [1] which we will need, to prove a later theorem.

Theorem 5.3 *: If $L(n, k, p, 2) \geq \frac{n}{k}$ then there exists a $(n, k, p, 2)$ Lotto design with $\frac{n}{k}$ blocks such that every element appears in the design.*

The following theorem states that m-ing an $(n, k, p, 2)$ Lotto design is always possible if every element appears in the original design.

Theorem 5.4 *: If $L(n, k, p, 2) = b \geq \frac{n}{k}$ then $L(mn, mk, p, t) \leq b$.*

Proof: By Theorem 5.3 there is an $(n, k, p, 2)$ Lotto design with b blocks such that every element appears in the design. By Theorem 5.2, $L(mn, mk, p, t) \leq L(n, k, p, 2) = b$ □

Theorem 5.5 *: $L(mn, 2m, zn+2, 2z+2) \leq \binom{n}{2}$ for $z \leq m$, where m is an integer.*

Proof : Let D_1 be the $(n, 2, 2, 2)$ Lotto design which consists of blocks that are all pairs from the n-set. Order the blocks using some ordering. Create $m-1$ copies $D_2, D_3, ..., D_m$ of D_1, each keeping D_1's ordering of the blocks, relabeling the elements $\{1^1, 2^1, ..., n^1\}$ in D_i with $\{1^i, 2^i, ..., n^i\}$, for $i = 2$ to m in the obvious way. For each j from 1 to

$|D_1|$, unite the j^{th} blocks of $D_1, D_2, ..., D_m$ to form a mn-set. Let D denote the set of all $2m$-sets formed. We claim that D is an $(mn, 2m, zn+2, 2z+2)$ Lotto design. To show that D is an $(mn, 2m, zn+2, 2z+2)$ Lotto design, let $P = \{(x_1)^{i_1}, (x_2)^{i_2}, ..., (x_{zn+2})^{i_{zn+2}}\}$ be an arbitrary $(zn+2)$-set chosen from the elements of D, where $x_j \in \{1, 2, ..., n\}$ and $i_j \in \{1, 2, ..., m\}$ for $j = 1$ to $zn+2$. We need to show it intersects some block of D in at least $2z+2$ elements. We note that there is at least one element in the collection $\{x_1, x_2, ..., x_{zn+2}\}$ that occurs $z+1$ or more times in the collection, as $\frac{zn+2}{n} > z$. We need to consider the possible cases :

Case 1 : Suppose the collection $\{x_1, x_2, x_3, ..., x_{zn+2}\}$ contains two elements, say x_1 and x_{z+2} such that $x_1 \neq x_{z+2}$ and x_1 is appears at least $z+1$ times in the collection and x_{z+2} appears at least $z+1$ times in the collection also. Then, without loss of generality, assume $x_1 = x_2 = ... = x_{z+1}$ and $x_{z+2} = x_{z+3} = ... = x_{2z+2}$. Since D_1 is an $(n, 2, 2, 2)$ Lotto design the the set $\{(x_1)^1, (x_{z+2})^1\}$ must appear in some block of D_1. Thus the subset $\{(x_1)^{i_1}, (x_2)^{i_2}, ..., (x_{z+1})^{i_{z+1}}, (x_{z+2})^{i_{z+2}}, ..., (x_{2z+2})^{i_{2z+2}}\}$ (which contains $2z+2$ elements of P) must be contained in some block of D. Since P was arbitrarily chosen, D is an $(mn, 2m, zn+2, 2z+2)$ Lotto design.

Case 2 : Suppose the collection $\{x_1, x_2, x_3, ..., x_{zn+2}\}$ contains only one element, say x_1 that appears at least $z+1$ times in the collection. It is easy to see that there exists an element x_2 distinct from x_1 that appears in the collection, and x_1 along with x_2 together appear at least $2z+2$ times in the collection. To see this, suppose that x_1 appears $z+l$ times in the collection where $l \geq 1$ and suppose every element in the collection distinct from x_1 appears fewer than $z-l+2$ times in the collection. Counting the total number of elements in the collection, there are at most $(n-1)(z-l+1)+(z+l) = zn+(n-nl+2l-1)$ elements. We can easily show that $n-nl+2l-1 < 2$ since $\frac{2l-3}{l-1} < 2$. Hence our method of counting showed that there are less than $zn+2$ elements in the collection which is a contradiction. Considering the elements x_1 and x_2 and using almost the same argument as in the previous case, we conclude that P must be contained in some block of D. Since P was arbitrarily chosen, D is an $(mn, 2m, zn+2, 2z+2)$ Lotto design. □

Table 2 shows some upper bounds resulting from Theorem 5.5.

Gordon et. al [4] stated the following theorem for Covering designs.

Theorem 5.6 *:* $C(v+1, k+1, t+1) \leq \left\lfloor (2 - \frac{k}{v}C(v,k,t) \right\rfloor + C(v -$

mn	k	l	t	# of blocks	n
12	6	6	4	6	4
16	8	6	4	6	4
16	8	10	6	6	4
20	8	12	6	10	5
20	10	6	4	6	4
20	10	14	8	6	4

Table 2: Some Upper Bounds generated by m-ing a base design

$1, k+1, t+1)$.

We shall generalize Theorem 5.6 for Lotto designs with the following construction.

Consider an (n, k, p, t) Lotto design D. Let $x \in X(n)$ and choose 2 new points x' and x'' not in $X(n)$. On the blocks of D, perform the following operations :

1. If a block B of D does not contain x, replace B with the two blocks : $B \cup \{x'\}$ and $B \cup \{x''\}$.
2. If a block B of D contains x, replace B with the block $(B \setminus \{x\}) \cup \{x', x''\}$.

Let us denote this new design by D'. Finally, add an $(n-1, k+1, p+1, t)$ Lotto design E on $X(n) \setminus \{x\}$ to the end of D'.

Theorem 5.7 *: The above construction gives an $(n+1, k+1, p+1, t)$ Lotto design on the elements $X(n) \setminus \{x\} \cup \{x', x''\}$.*

Proof : Consider a $(p+1)$-set $P = \{a_1, a_2, ..., a_{p+1}\}$. We must show it is represented by some block in $D' \cup E$. Consider the three possible cases :
Case 1 : Suppose $x' \notin P$ and $x'' \notin P$. Then P is represented by E.
Case 2 : Suppose $x' \in P$ but $x'' \notin P$. Then $P \setminus \{x'\} \cup \{x\}$ is represented by some block of B in D. If $x \in B$, then P is represented by the block B' constructed from B. Otherwise, if $x \notin B$, then the block $B \cup \{x'\}$ from D' represents P. Symmetrically, the same is true if $x'' \in P$ but $x' \notin P$.
Case 3 : Suppose x' and x'' is in P. Let $P = \{x', x'', a_1, a_2, ..., a_{p-2}\}$.

Consider the set $\{x, a_1, a_2, ..., a_{p-2}, b\}$ where b is any other element. This set is represented by some block, B, in the original design. If B contains x, then $B \setminus \{x\}$ intersects P in at least $t-2$ elements. But then, P intersects $B \setminus \{x\} \cup \{x', x''\}$ in t elements. If B does not contain x then it intersects P in at least $t-1$ elements and either $B \cup \{x'\}$ or $B \cup \{x''\}$ can represent P in t elements.

Since in each case, P was represented by the constructed design, the design must be an $(n+1, k+1, p+1, t)$ Lotto design. □

Corollary 5.1 *: If $x \in X(n)$ and b_x denotes the number of blocks in a minimal (n, k, p, t) Lotto design that contain x, then $L(n+1, k+1, p+1, t) \leq 2L(n, k, p, t) - b_x + L(n-1, k+1, p+1, t)$.*

Proof : The construction creates $b_x + 2(L(n, k, p, t) - b_x) + L(n-1, k+1, p+1, t)$ blocks. Hence $L(n+1, k+1, p+1, t) \leq 2L(n, k, p, t)$ $-b_x + L(n-1, k+1, p+1, t)$. □

The next result follows immediately from Corollary 5.1.

Corollary 5.2 *: $L(n+1, k+1, p+1, t) \leq \left\lfloor (2 - \frac{k}{v} L(n, k, p, t) \right\rfloor + L(n-1, k+1, p+1, t)$.*

Proof : For a minimal (n, k, p, t) Lotto design, there exists some $x \in X(n)$ such that x appears in at least $\left\lceil \frac{k}{v} L(n, k, p, t) \right\rceil$ blocks of the design. Then by Corollary 5.1, we have

$$L(v+1, k+1, p+1, t) \leq 2L(v, k, p, t) - \left\lceil \frac{k}{v} L(n, k, p, t) \right\rceil + L(v-1, k+1, p+1, t).$$

Hence we are done. □

The following results determine upper bound formulas for fixed values of p and t.

Theorem 5.8 *: $L(k+2, k, 4, 3) \leq 3$, for $k \geq 3$.*

Proof: The blocks $B_1 = \{1, 2, 3, ..., k\}$, $B_2 = \{1, 2, 3, ..., k-1, k+1\}$ and $B_3 = \{1, 2, 3, ..., k-3, k, k+1, k+2\}$ form a $(k+2, k, 4, 3)$ Lotto design. To show this, consider a 4-set P. If P is not represented by B_1 or B_2, then $|P \cap B_1| \leq 2$ which implies $\{k+1, k+2\} \subset P$. Similarly, $|P \cap B_2| \leq 2$ implying that $\{k, k+2\} \subset P$. Thus, $\{k, k+1, k+2\} \subset P$ which is contained in B_3. Hence, the three blocks B_1, B_2, B_3 form an $(k+2, k, 4, 3)$ Lotto design. □

Theorem 5.9 *: $L(2k+1, k, 5, 3) \leq 5$, for $k \geq 4$.*

Proof: Consider the five blocks : $B_1 = \{1, 2, 3, ..., k-2, k-1, k\}$, $B_2 = \{1, 2, 3, ..., k-2, k+1, 2k+1\}$, $B_3 = \{3, ..., k-2, k-1, k, k+1, 2k+1\}$, $B_4 = \{k+2, ..., 2k-1, 2k, 2k+1\}$ and $B_5 = \{k+1, k+2, ..., 2k-1, 2k\}$. We claim these five blocks make up a $(2k+1, k, 5, 3)$ Lotto design. To show this, divide $X(2k+1)$ into two sets $A = \{1, 2, 3, ..., k\}$ and $B = \{k+1, k+2, ..., 2k+1\}$. Consider an arbitrary 5-set P. Clearly, if three or more of P's elements come from A, then it will be represented by the block B_1. Similarly, if four or more of P's elements come from B, then it will be represented by the block B_5.

We consider the remaining case where two elements of P are from A and three elements of P are from B. If $2k+1 \notin P$, then $|\{k+1, k+2, ..., 2k\} \cap P| = 3$, which implies that P is represented by B_5. So assume that $2k+1 \in P$. Similarly, if $k+1 \notin P$, then $|\{k+2, ..., 2k, 2k+1\} \cap P| \geq 3$, which implies that P is represented by B_4. Thus we assume $k+1 \in P$. So both $k+1$ and $2k+1 \in P$. Now, consider an element from $P \cap A$ (there are two of these); it must be in B_2 or B_3 or both. In any case, since $k+1$ and $2k+1$ appear in both B_2 and B_3, P is represented in this case.

We have shown that an arbitrary 5-set is represented by these five blocks, and hence, it forms a $(2k+1, k, 5, 3)$ Lotto design. □

Theorem 5.10 *: $L(2k+2, k, 8, 4) \leq 4$, for $k \geq 4$.*

Proof : We claim that the blocks $B_1 = \{1, 2, 3, ..., k\}$, $B_2 = \{k+3, k+4, ..., 2k+2\}$, $B_3 = \{k+1, k+2, ..., 2k-2, 2k-1, 2k\}$ and $B_4 = \{k+1, k+2, ..., 2k-2, 2k+1, 2k+2\}$ form a $(2k+2, k, 8, 4)$ Lotto design. To show this, divide $X(2k+2)$ into two sets $A = \{1, 2, 3, ..., k\}$ and $B = \{k+1, k+2, ..., 2k+1, 2k+2\}$. Consider an arbitrary 8-set P. Clearly if four or more of P's elements come from A, then it will be represented by the block B_1. Similarly, if six or more of P's elements come from B, then it will be represented by the blocks B_2 or B_4.

We consider the remaining case where three elements of P are from A and five elements of P are from B. Split the set B into two subsets $C = \{k+1, k+2, ..., 2k-2\}$ and $D = \{2k-1, 2k, 2k+1, 2k+2\}$, and consider the possible subcases. If two or more elements of P appear in C, then P is represented by either B_3 or B_4. If one element of P

appear in C, then P is represented by B_2. It is not possible for no elements of P to appear in C, since $|P| = 5$ and $|D| = 4$. Thus all subcases have been considered.

We have shown that an arbitrary 8-set is represented by these four blocks, and hence it is a $(2k+2, k, 8, 4)$ Lotto design. □

Theorem 5.11 *: $L(3k+2, k, 8, 3) \leq 5$, for $k \geq 4$.*

Proof: Let the elements 1,2,3,...,$k+4$ have frequency one and the rest of the elements have frequency two. Put the elements 1,2,..., k in the first block B_1. Let the second block B_2 be $\{k+1, k+2, k+3, k+4, k+5, ..., 2k\}$. Now put the elements $k+5, k+6, ..., 3k+2$ into the last three blocks B_3, B_4 and B_5 in any way that does not place the same element twice in any block. We claim this is a $(3k+2, k, 8, 3)$ Lotto design. To show this, consider an arbitrary 8-set P chosen from the two sets $A = \{1, 2, ..., k+4\}$ and $B = \{k+5, ..., 3k+2\}$. We must show that this 8-set is represented. We denote the number of elements chosen for P from each set by (a, b) where a is the number of elements from A and b is the number of elements from B. If $a \geq 5$, then clearly, B_1 or B_2 contains at least three elements of the 8-set and hence, P is represented in this case. If $a = 4$, then it is easy to see that we may assume that exactly two elements chosen from A appear in B_1 and the remaining two elements chosen from A appears in B_2. Otherwise, either B_1 or B_2 would contain at least three elements of the 8-set, and hence, the P is represented. As B_2 contains two elements from the 8-set, we may assume that no element in $\{k+5, k+6, ..., 2k\}$ may belong to the P, or else B_2 would represent P. So the 4 elements of the P chosen from B must actually be contained in $\{2k+1, 2k+2, ..., 3k+2\}$, all of which have frequency two. This implies that at least one of three blocks B_3, B_4 and B_5 contains 3 elements of the P. Finally, consider the remaining cases where $(a, b) = (4-x, 4+x)$ where $0 < x \leq 4$. If 0 or 1 element of P are from $\{k+5, k+6, ..., 2k\}$, then there are at least $3+x \geq 4$ elements of P from $\{2k+1, 2k+2, ..., 3k+2\}$ which can be handled by the case where $a = 4$. If 2 elements of P are from $\{k+5, k+6, ..., 2k\}$, then there are at least $2+x \geq 3$ elements of P from $\{2k+1, 2k+2, ..., 3k+2\}$, which implies that the elements of P appear at least 3(2)+2=8 times in the blocks B_3, B_4 and B_5. Clearly, some block must contain at least three of these elements of P and hence P is represented in this case. Finally, if 3 or more elements of P are from $\{k+5, k+6, ..., 2k\}$, then P is represented by the block B_2. So, no matter what 8-set we choose, it is always represented. Thus, the construction design is a $(3k+2, k, 8, 3)$ Lotto Design with five blocks. □

The next three results although specific are useful.

Theorem 5.12 : $L(16, 8, 4, 3) \leq 7$

Proof : The blocks $\{1,3,4,6\}, \{1,2,5,7\}, \{3,4,6,7\}, \{2,3,5,8\}, \{2,4,5,8\}, \{1,6,7,8\}$, and $\{2,5,6,8\}$ form an $(8,4,4,3)$ Lotto design on seven blocks where every 2-set appears in the design. Hence by Theorem 5.2, $L(16,8,4,3) \leq 7$. □

Theorem 5.13 : $L(18, 8, 4, 3) \leq 9$.

Proof : Since we can generate a $(9,4,4,3)$ Lotto design cyclically from the block $\{0,1,2,4\}$ modulo 9, every 2-set appears in the constructed design. Hence by Theorem 5.2, we can double this design to get an $(18,8,4,3)$ Lotto design with 9 blocks. Thus, $L(18,8,4,3) \leq 9$. □

Theorem 5.14 : $L(18, 9, 4, 3) \leq 6$.

Proof: The blocks $\{1,2,3\}, \{1,3,5\}, \{2,4,5\}, \{1,4,6\}, \{3,4,6\}, \{2,5,6\}$ form an $(6,3,4,3)$ Lotto design in which every 2-set appears. By tripling this design, we get an $(18,9,4,3)$ Lotto design. Hence $L(18,9,4,3) \leq 6$. □

6 Conclusion

We have presented several constructions of Lotto designs. These constructions give upper bounds for $L(n,k,p,t)$. Several of these results are generalized from the theory of Covering designs. The semi-direct product is one construction that may be generalized further.

7 Concluding Remarks

References

[1] J.A. Bate. *A Generalized Covering Problem*, Ph.D. thesis, University of Manitoba, 1978.

[2] C. J. Colbourn, J. H. Dinitz. *The CRC Handbook of Combinatorial Designs*, CRC Press (1996).

[3] R. A. Fisher, F. Yates, *Statistical Tables for Biological, Agricultural and Medical Research*, First Edition, Oliver and Boyd Ltd, 1938.

[4] D. M. Gordon, O. Patashnik, G. Kuperberg. *New Constructions for Covering Designs*, Journal of Combinatorial Designs, **3**(4) (1995), 269-284.

[5] M. Hall Jr. *Combinatorial Theory*, Blaisdell, Waltham, Mass., 1967.

[6] P. C. Li. *Some Results on Lotto Designs*, Ph.D. thesis, University of Manitoba, 1999.

[7] K.J. Nurmela, P.R.J. Ostergard. *Upper Bounds for Covering Designs by Simulated Annealing*, Congr. Numer. 96 (1993), 93-111.