Common Intersection Designs

Jooyoung Lee
Department of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada

Douglas R. Stinson
School of Computer Science
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada

January 7, 2005

Abstract

Certain combinatorial set systems have been proposed for use in the design of deterministic key predistribution schemes for distributed sensor networks. In this paper, we analyze combinatorial properties of the set systems, that relate to the connectivity and resilience of the resulting distributed sensor networks. Motivated by these considerations, we introduce a new class of set systems, called "common intersection designs" which seem to be of intrinsic interest. We discuss existence and properties of common intersection designs in this paper.

1 Introduction and motivation

In this paper, we introduce a new class of set systems, called *common intersection designs* or CIDs. These designs are motivated by an application to the construction of *key predistribution schemes* (KPSs) in *distributed sensor networks* (DSNs). DSNs are ad-hoc mobile networks that are comprised of sensor nodes having limited computation and communication capabilities. KPSs for DSNs are different from conventional KPSs in that pairs of nodes are not required to share a common secret key. This relaxation is permitted due to memory constraints of sensor nodes. For a discussion of this model and approaches to key establishment in DSNs, we refer to [2].

Eschenauer and Gligor [4] recently proposed a randomized key predistribution scheme for DSNs. In this scheme, each sensor node is loaded with a fixed number of keys, which are chosen randomly from a large key pool. Two nodes in wireless communication range can establish a secure channel provided that they share a common key. If they share no common key, then they look for a series of two or more secure "hops" to reach each other. Then one of them can choose an arbitrary session key and then relay it through the secure links in encrypted form to create a secure channel with the destination node.

We modify this approach by considering deterministic assignment of keys to sensor nodes. Such KPSs can be described by set systems, where the points of the set system correspond to the keys in the key pool and the blocks correspond to the subsets of keys held by the various nodes in the network.

Papers studying deterministic KPSs for DSNs include Çamtepe and Yener [1], Lee and Stinson [5, 6], and Wei and Wu [9]. The use of combinatorial designs for KPSs was first proposed in [1]. The notion of common intersection designs was defined by Lee and Stinson [5], where the application to KPSs was developed. Here, we study combinatorial properties of CIDs.

In Section 2, we define some basic types of combinatorial set systems and demonstrate how they can be used to set up deterministic KPSs for DSNs. In particular, we define *common intersection designs* (CIDs) having a parameter μ which enables us to evaluate the local connectivity of the network. (A μ-CID is a set system that satisfies the property that, given any two disjoint blocks A and B, there exist at least μ blocks intersecting both A and B.)

In Section 3, we present upper bounds on μ, in terms of other parameters of common intersection designs. These bounds arise from counting subsets of three blocks. In Section 4, we consider the conditions under which there exist common intersection designs having the maximum possible value of μ (these are termed "optimal configurations"). In Section 5, we focus on counting sets of three pairwise intersecting blocks (i.e., "triangles") in common intersection designs. This analysis leads to improved bounds when the designs contain triangles.

2 Configurations and common intersection designs

We begin with the definition of a set system.

Definition 2.1. *A* set system *is a pair $(X, \mathcal{A})$, where $\mathcal{A}$ is a finite set of subsets of X called* blocks. *The* degree *of a point $x \in X$ is the number of* *blocks containing x. $(X, \mathcal{A})$ is* regular *(of degree r) if all points have the same degree, r. The* rank *of $(X, \mathcal{A})$ is the size of the largest block. If all blocks have the same size, say k, then $(X, \mathcal{A})$ is said to be* uniform *(of rank k).*

A set system is used for key predistribution of distributed sensor networks as follows. Suppose that $X = \{x_i : 1 \leq i \leq v\}$ and $\mathcal{A} = \{A_j : 1 \leq j \leq b\}$. We identify the blocks in $\mathcal{A}$ and the points in X with sensor nodes and keys, respectively. A sensor node associated with $A_i \in \mathcal{A}$ receives the keys indexed by the block A_i of the set system. Then two nodes, say A_i and A_j, share a common key if and only if $A_i \cap A_j \neq \emptyset$. In this case, they can choose one of the common keys to use as their secret key for secure communication.

It is desirable for every node to receive a constant number of keys and for the compromise of a single key to affect a constant number of sensor nodes. Therefore, we will only consider regular and uniform set systems from now on. Such a set system is referred to as a (v, b, r, k)-1-*design*, where $|X| = v$, $|\mathcal{A}| = b$, r is the degree and k is the rank. A necessary condition for existence of a (v, b, r, k)-1-design is that $bk = vr$. It is well-known that this necessary condition is also sufficient for existence of a (v, b, r, k)-1-design (see, for example [8]).

We can evaluate the connectivity of the network layer of the DSN by analyzing the *block graph* of the set system $(X, \mathcal{A})$. The *block graph* of $(X, \mathcal{A})$ is the graph defined on vertex set $\mathcal{A}$ such that two blocks are adjacent if and only if they have nonempty intersection.

Definition 2.2. *A (v, b, r, k)-1-design is called a (v, b, r, k)-*configuration *if any two points occur in at most one block.*

Among all the (v, b, r, k)-1-designs, the (v, b, r, k)-configurations are the ones that have the largest number of blocks intersecting each block in the design (i.e., the block graph has maximum possible degree). This provides for the maximum possible connectivity of the network layer. For some results on the existence of configurations, we refer to [3, §IV.6].

The following lemma is obvious from an elementary counting argument:

Lemma 2.1. *The block graph of a (v, b, r, k)-configuration is a regular graph of degree $(r - 1)k$.*

Now suppose that we use a configuration $(X, \mathcal{A})$ for key predistribution. If the block graph of the set system is not a complete graph, then two nodes A_i and A_j might share no common key. In this case, they can communicate via "two hops" provided that there is a node A_h (in a wireless communication range) such that $A_i \cap A_h \neq \emptyset$ and $A_j \cap A_h \neq \emptyset$. Ideally, we would like there to be many choices for an intermediate node that satisfies this condition.

The above discussion motivates the following definition:

Definition 2.3. *Suppose that $(X, \mathcal{A})$ is a (v, b, r, k)-configuration. We say that $(X, \mathcal{A})$ is a μ-*common intersection design *(or* $(v, b, r, k; \mu)$-CID*) provided that*

$$|\{A_h \in \mathcal{A} : A_i \cap A_h \neq \emptyset \text{ and } A_j \cap A_h \neq \emptyset\}| \geq \mu$$

whenever $A_i \cap A_j = \emptyset$.

In general, given parameters (v, b, r, k) such that $bk = vr$, we would like to construct a (v, b, r, k)-configuration with μ as large as possible. This maximum value of μ will be denoted $\mu^*(v, b, r, k)$.

For parameter sets (v, b, r, k) for which there is no configuration, we define $\mu^*(v, b, r, k) = -\infty$. If there exists a (v, b, r, k)-configuration in which any two blocks intersect, then we define $\mu^*(v, b, r, k) = \infty$.

2.1 Definitions of set systems

While we will concentrate on the study of configurations in the rest of the paper, we also define some other combinatorial structures here for later use. These are all widely studied set systems.

Definition 2.4. *A* (v, k, λ)-BIBD (balanced incomplete block design) *is a uniform set system $(X, \mathcal{A})$ of rank k such that $|X| = v$ and every pair of points in X occurs in exactly λ blocks.*

Since BIBDs are always regular, say, of degree r, we will sometimes use the notation (v, b, r, k, λ)-*BIBD* to record the degree and the number of blocks in a BIBD.

Definition 2.5. *Let g, u and k be positive integers such that $2 \leq k \leq u$. A* group-divisible design *of* type g^u *and* block-size k *is a triple $(X, \mathcal{H}, \mathcal{A})$, where X is a finite set of cardinality gu, $\mathcal{H}$ is a partition of X into u parts (called* groups*) of size g, and $\mathcal{A}$ is a set of subsets of X (called* blocks*), which satisfy the following properties:*

1. *$|A| = k$ for every $A \in \mathcal{A}$.*
2. *$|H \cap A| \leq 1$ for every $H \in \mathcal{H}$ and every $A \in \mathcal{A}$.*

3. *Every pair of points from different groups occurs in exactly one block in $\mathcal{A}$.*

A group-divisible design of type n^k and block-size k is called a *transversal design* and it is denoted $\mathrm{TD}(k,n)$. It follows that $|H \cap A| = 1$ for any block A and any group H in a transversal design.

Definition 2.6. *A* partial geometry *with* parameters $s \geq 1$, $t \geq 1$ *and* α *is a* $(v, b, t+1, s+1)$*-configuration such that for any block* A *and a point* $x \notin A$*, there exist exactly* α *blocks which contain* x *and intersect* A*.*

In fact, the parameters s, t and α of a partial geometry determine the values of v and b, as follows:

$$v = (s+1)\left(\frac{st}{\alpha} + 1\right) \quad \text{and} \quad b = (t+1)\left(\frac{st}{\alpha} + 1\right).$$

Definition 2.7. *A* generalized quadrangle *is a partial geometry with* $\alpha = 1$*.*

Definition 2.8. *Let* $(X, \mathcal{A})$ *be a set system. The* dual set system *of* $(X, \mathcal{A})$ *is any set system isomorphic to* $(Y, \mathcal{B})$*, where* $Y = \mathcal{A}$ *and*

$$\mathcal{B} = \{\{a \in \mathcal{A} : x \in a\} : x \in X\}.$$

2.2 Preliminary Results

We present some simple preliminary results in this section.

Lemma 2.2. *There exists a* $(v, b, r, k, 1)$*-BIBD if and only if* $\mu^*(b, v, k, r) = \infty$*.*

Proof. Suppose $(X, \mathcal{A})$ is a $(v, b, r, k, 1)$-BIBD. Then the dual set system is a (b, v, k, r)-configuration in which any two blocks intersect, and hence $\mu^*(b, v, k, r) = \infty$.

Conversely, if we have a configuration with $\mu = \infty$, then the dual set system is a BIBD with $\lambda = 1$. □

Lemma 2.3. *If there is a TD*(k, n)*, then* $\mu^*(nk, n^2, n, k) \geq k(k-1)$*.*

Proof. Let X and $\mathcal{A}$ be the points and blocks (respectively) of a $\mathrm{TD}(k, n)$. It is clear that $(X, \mathcal{A})$ is an (nk, n^2, n, k)-configuration.

The existence of a $\mathrm{TD}(k, n)$ implies that $k \leq n + 1$. If $k = n + 1$, then any two blocks of the transversal design intersect; in this case, $\mu^* = \infty$. If $k \leq n$, then the transversal design contains pairs of disjoint blocks. For any two disjoint blocks A and A' and for any $x \in A$, $x' \in A'$, there is a unique block containing x and x' provided that x and x' are not from the same group. Therefore $(X, \mathcal{A})$ is an $(nk, n^2, n, k; k(k-1))$-CID. □

Remark 2.1. *More generally, a group-divisible design of type g^u and block-size k yields a $\left(gu, \frac{g^2u(u-1)}{k(k-1)}, \frac{g(u-1)}{k-1}, k; k(k-1)\right)$-CID.*

Lemma 2.4. *If there exists a partial geometry with parameters s, t and α, then*

$$\mu^* \left((s+1) \left(\frac{st}{\alpha} + 1 \right), (t+1) \left(\frac{st}{\alpha} + 1 \right), t+1, s+1 \right) \geq \alpha(s+1).$$

Proof. If $t+1 = \alpha$, then all pairs of blocks intersect and $\mu^* = \infty$. Otherwise, if $t+1 > \alpha$, let A and A' be any two disjoint blocks. For every point $x \in A'$, there are α blocks containing x and intersecting A. Hence, $\mu^* \geq \alpha(s+1)$. □

Lemma 2.5. *If $\mu^*(v, b, r, k) \neq \infty$, then*

$$\mu^*(v, b, r, k) \leq k^2.$$

Proof. Let A and A' be any two disjoint blocks. For any point $x \in A$ and any point $x' \in A'$, there is at most one block containing x and x'. Therefore there are at most k^2 blocks intersecting both A and A'. □

Corollary 2.6. *If $v < b$ and there exists a $(v, b, r, k, 1)$-BIBD, then*

$$\mu^*(v, b, r, k) = k^2.$$

Proof. Let $(X, \mathcal{A})$ be a $(v, b, r, k, 1)$-BIBD where $v < b$. It is easy to see that $(X, \mathcal{A})$ is a $(v, b, r, k; k^2)$-CID, and hence $\mu^*(v, b, r, k) \geq k^2$.

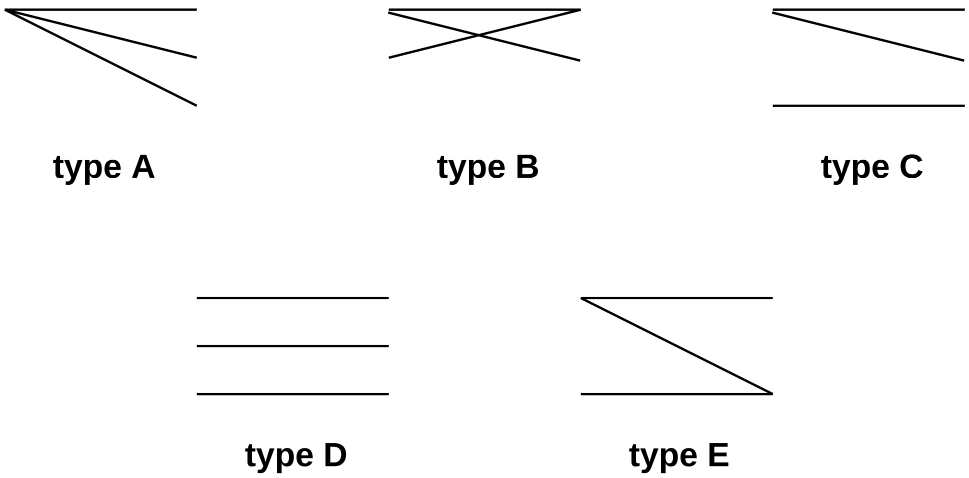
To finish the proof, we need to show that $\mu^*(v, b, r, k) \neq \infty$ (then the desired result will follow from Lemma 2.5). However, applying Lemma 2.2, we have that $\mu^*(v, b, r, k) = \infty$ if and only if there is a $(b, v, k, r, 1)$-BIBD. Because $v < b$, this is impossible. □

3 Counting subsets of three blocks

In this section, we obtain some bounds by counting subsets of three blocks in a (v, b, r, k)-configuration, $(X, \mathcal{A})$. Assuming that $\mu^*(v, b, r, k) \neq \pm\infty$, we compute an upper bound on $\mu^*(v, b, r, k)$ as a result.

We first define the following variables:

Figure 1: Possible three-subsets of blocks



- Let x_0 denote the number of subsets of three blocks that intersect in a point $x \in X$ (subsets of this form are called *type A*).
- Let x_1 denote the number of subsets of three blocks that pairwise intersect in three distinct points (subsets of this form are called *type B*).
- Let x_2 denote the number of subsets of three blocks such that two of them intersect and the third block is disjoint from the first two (subsets of this form are called *type C*).
- Let x_3 denote the number of subsets of three blocks that are mutually disjoint (subsets of this form are called *type D*).
- Let x_4 denote the number of subsets of three blocks such that two of them are disjoint and the third block intersects both of the others (subsets of this form are called *type E*).

The five types of three-subsets of blocks are illustrated in Figure 1.

We can obtain all the three-subsets of blocks of type A by first choosing a point and then choosing three blocks containing the point. From this observation, we have that

$$x_0 = v\binom{r}{3}. \tag{1}$$

If we count all possible subsets of three blocks, then every block of type A to E is counted exactly once. Hence, we obtain the equation

$$x_0 + x_1 + x_2 + x_3 + x_4 = \binom{b}{3}. \tag{2}$$

Now we consider pairs of blocks. The number of pairs of intersecting blocks is $v\binom{r}{2}$ (by choosing a point and then choosing any two blocks containing the point). If we denote the total number of pairs of disjoint blocks by δ, then we have the following equation:

$$\delta = \binom{b}{2} - v\binom{r}{2}. \tag{3}$$

For each pair of disjoint blocks, we choose any additional block. In this way, we count the subsets of type C twice, the subsets of type D three times, and the subsets of type E exactly once. Hence, we have the equation

$$2x_2 + 3x_3 + x_4 = (b-2)\delta. \tag{4}$$

Finally, we choose any pair of disjoint blocks and any point x contained in one of them. Choosing an additional block containing the point x, we count each of the subsets of type C and E twice. Therefore we have the equation

$$2x_2 + 2x_4 = 2k(r-1)\delta. \tag{5}$$

Substituting (1) into (2), we obtain the following system of equations:

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= c_1 && (6)\\ 2x_2 + 3x_3 + x_4 &= c_2 && (7)\\ x_2 + x_4 &= c_3, && (8) \end{aligned}$$

where

$$\begin{aligned} c_1 &= \binom{b}{3} - v\binom{r}{3} && (9)\\ c_2 &= \delta(b-2) && (10)\\ c_3 &= \delta k(r-1). && (11) \end{aligned}$$

Assuming that there exists at least one (v, b, r, k)-configuration, the system of equations (6), (7) and (8) has a solution in non-negative integers.

We are especially interested in upper bounds on the quantity x_4, because of the following obvious result.

Lemma 3.1. *If* $\mu^*(v,b,r,k) < \infty$*, then*

$$\mu^*(v,b,r,k) \leq \frac{x_4}{\delta}. \tag{12}$$

We can derive inequalities on x_4 by solving (6), (7) and (8) for x_1, x_2 and x_3 in terms of x_4. We obtain the following solution to the system:

$$x_1 = c_1 - \frac{c_2}{3} - \frac{c_3}{3} - \frac{x_4}{3} \tag{13}$$

$$x_2 = c_3 - x_4 \tag{14}$$

$$x_3 = \frac{c_2}{3} - \frac{2c_3}{3} + \frac{x_4}{3} \tag{15}$$

We know that $x_1, x_2, x_3, x_4 \geq 0$. We can obtain upper bounds on x_4 from (13) and (14) by setting $x_1 \geq 0$ and $x_2 \geq 0$, respectively. The following two bounds are obtained.

Theorem 3.2. *[5] If* $\mu^*(v,b,r,k) < \infty$*, then* $\mu^*(v,b,r,k) \leq (r-1)k$*.*

Proof. We have $0 \leq x_2 = c_3 - x_4$, so $x_4 \leq c_3$. Applying Lemma 3.1, we obtain

$$\mu^*(v,b,r,k) \leq \frac{c_3}{\delta} = k(r-1).$$

□

Remark 3.1. Theorem 3.2 is proven in [5] by a simple and direct combinatorial argument. Here we have shown that it is also a consequence of the general results obtained by counting subsets of three blocks.

Theorem 3.3. *If* $\mu^*(v,b,r,k) < \infty$*, then*

$$\mu^*(v,b,r,k) \leq \frac{(r-1)^2 k(k-1)}{b - k(r-1) - 1}.$$

Proof. We have

$$0 \leq x_1 = c_1 - \frac{c_2}{3} - \frac{c_3}{3} - \frac{x_4}{3},$$

so

$$x_4 \leq 3c_1 - c_2 - c_3.$$

Applying Lemma 3.1, we obtain

$$\mu^*(v,b,r,k) \leq \frac{3c_1 - c_2 - c_3}{\delta}.$$

Some tedious algebraic simplification shows that

$$\frac{3c_1 - c_2 - c_3}{\delta} = \frac{(r-1)^2 k(k-1)}{b - k(r-1) - 1} \tag{16}$$

(see the Appendix for details). The result follows. □

The relatively simple form of the bound in Theorem 3.3 suggests that a direct combinatorial proof might be possible. Indeed, we will present an alternate proof in Section 4.2.

4 Optimal configurations

In this section, we consider configurations which satisfy the upper bounds of Theorem 3.2 or Theorem 3.3. We will call a configuration that meets the bound of Theorem 3.2 *optimal of type I*, and one that meets the bound of Theorem 3.3 *optimal of type II* .

Optimal configurations of type I were considered in [5], where the following result was proven.

Theorem 4.1. *[5] A (v, b, r, k)-configuration is optimal of type I if and only if the dual set system is a group-divisible design of type s^m and block-size r, where*

$$s = b - (r-1)k \quad \text{and} \quad m = \frac{b}{b - (r-1)k}.$$

Example 4.1. *There exists a group-divisible design of type 3^9 and block size 4 (see, for example, [3, §III.1]). The dual set system is a type I optimal $(54, 27, 4, 8)$-configuration.*

The next theorem establishes some properties of optimal configurations of type II. We require some definitions first.

Definition 4.1. *A 3-subset of blocks of type B is called a* triangle. *A configuration is* triangle-free *if it contains no triangle (i.e., if $x_1 = 0$).*

Definition 4.2. *A (n, r, λ, μ)*-strongly regular graph *(or (n, r, λ, μ)*-SRG*) is a graph on n vertices which is regular of degree r (with $0 < r < n - 1$), and such that any two distinct vertices have λ common neighbours if they are adjacent, and μ common neighbours if they are nonadjacent.*

Lemma 4.2. *An optimal configuration of type II is triangle-free.*

Proof. ¿From the proof of Theorem 3.3, it is easy to see that, in order for a configuration to be optimal of type II, it must be the case that $x_1 = 0$. Therefore the configuration is triangle-free. □

Theorem 4.3. *A (v, b, r, k)-configuration is optimal of type II if and only if its block graph is a $\left(b, (r-1)k, r-2, \frac{(r-1)^2k(k-1)}{b-k(r-1)-1}\right)$-SRG.*

Proof. Suppose that a (v, b, r, k)-configuration $(X, \mathcal{A})$ is optimal of type II. First, we observe that the block graph of any (v, b, r, k)-configuration is regular of degree $(r-1)k$. The parameter $\lambda = r-2$ because the configuration is triangle-free.

For any two disjoint blocks A_i and A_j, define

$$\mu(A_i, A_j) = |\{A_h \in \mathcal{A} : A_i \cap A_h \neq \emptyset \text{ and } A_j \cap A_h \neq \emptyset\}|.$$

We need to show that

$$\mu(A_i, A_j) = \frac{(r-1)^2k(k-1)}{b-k(r-1)-1} \tag{17}$$

for all pairs of disjoint blocks A_i, A_j.

Define $\mu_{\min}$ to be the minimum value of $\mu(A_i, A_j)$ and define $\overline{\mu}$ to be the average value of $\mu(A_i, A_j)$, over all pairs of disjoint blocks A_i, A_j. Clearly $(X, \mathcal{A})$ is a $(v, b, r, k; \mu_{\min})$-CD, and we have that

$$\mu_{\min} = \frac{(r-1)^2k(k-1)}{b-k(r-1)-1}$$

because $(X, \mathcal{A})$ is optimal of type II.

On the other hand, from the proofs of Lemma 3.1 and Theorem 3.3, we have that

$$\overline{\mu} \leq \frac{(r-1)^2k(k-1)}{b-k(r-1)-1}.$$

Since $\mu_{\min} \leq \overline{\mu}$, it follows that (17) holds for all pairs of disjoint blocks A_i, A_j, as desired.

Conversely, suppose that $(X, \mathcal{A})$ is a configuration whose block graph is an SRG having the stated parameters. Then it is immediate that $(X, \mathcal{A})$ is optimal of type II. □

A type II optimal configuration is triangle-free, which implies that $\mu \leq k$. The extremal case, when $\mu = k$, provides a subclass of type II optimal configurations that are easy to characterize.

Theorem 4.4. *A type II optimal (v, b, r, k)-configuration with $\mu = k$ is equivalent to a generalized quadrangle with $s = k - 1$ and $t = r - 1$.*

Proof. Suppose that $(X, \mathcal{A})$ is a type II optimal (v, b, r, k)-configuration. Let $A \in \mathcal{A}$ and let $x \notin A$. Let $A' \in \mathcal{A}$ be a block such that $x \in A'$ and $A \cap A' = \emptyset$. For each $x' \in A'$, let $\alpha(x')$ denote the number of blocks containing x' that intersect A. Then $\alpha(x') \leq 1$ for all $x' \in A'$ and

$$\sum_{x' \in A'} \alpha(x') = k.$$

It follows that $\alpha(x') = 1$ for all $x' \in A'$. Hence, $(X, \mathcal{A})$ is a generalized quadrangle.

Conversely, suppose that $(X, \mathcal{A})$ is a generalized quadrangle with $s = k - 1$ and $t = r - 1$. Now, in a generalized quadrangle, we have that $b = (t + 1)(st + 1)$. Substituting $k = s + 1$ and $r = t + 1$, we have that

$$\begin{aligned} k(r-1) + 1 + (r-1)^2(k-1) &= st + t + 1 + st^2 \\ &= (t+1)(st+1) \\ &= b. \end{aligned}$$

Because $k, r > 1$, it follows that $b > k(r - 1) + 1$, and $\mu^*(v, b, r, k) \neq \infty$ from Lemma 2.2.

It is easy to see that $(X, \mathcal{A})$ is a k-CID. Also, we have that

$$k = \frac{(r-1)^2 k(k-1)}{b - k(r-1) - 1}.$$

Hence, $(X, \mathcal{A})$ is optimal of type II. ☐

We can give a more general characterization of type II optimal (v, b, r, k)-configurations in terms of structural properties of the block graph. In fact, this characterization will apply to any $(v, b, r, k; \mu)$-CID with no triangle having the property that any pair of disjoint blocks have exactly μ common intersecting blocks.

Suppose a configuration is triangle-free. Then, for any pair of intersecting blocks in such a configuration, there are exactly $r-2$ additional blocks which intersect both of them (and these r blocks all contain one common point). It follows that the block graph G can be edge-decomposed into complete graphs K_r. (Any pair of adjacent vertices in G have exactly $r - 2$ common neighbors, and these r vertices will form a complete graph K_r.)

From this observation, we have the following theorem:

Theorem 4.5. *The existence of a $(v, b, r, k; \mu)$-CID with no triangle having the property that any pair of disjoint blocks have exactly μ common intersecting blocks is equivalent to the existence of a $(b, (r-1)k, r-2, \mu)$-SRG that can be edge-decomposed into complete graphs K_r.*

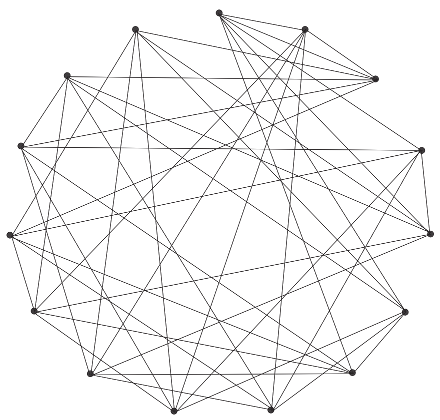
Corollary 4.6. *The existence of a type II optimal (v, b, r, k)-configuration with $r = 2$ or 3 is equivalent to the existence of a*

$$\left(b, (r-1)k, r-2, \tfrac{(r-1)^2 k(k-1)}{b-k(r-1)-1}\right)\text{-}SRG.$$

Proof. We can assume that $b - 1 \neq (r-1)k$, so $\mu^*(v, b, r, k) \neq \infty$ by Lemma 2.2. When $r = 2$, the complete graphs K_2 are just the edges in the block graph. When $r = 3$, each complete graph K_3 is formed by taking an edge xy in the block graph together with the unique common neighbour z of x and y. $\square$

Example 4.2. *Suppose we take $v = b = 15$ and $r = k = 3$. The web page* `http://www.maths.gla.ac.uk/~es/15-6-1-3` *presents a $(15, 6, 1, 3)$-strongly regular graph, which we depict in Figure 2. It can be decomposed into triangles, from which we know that there exists a $(15, 15, 3, 3)$-configuration with $\mu = 3$ that is optimal of type II.*

Figure 2: A $(15, 6, 1, 3)$-strongly regular graph



Example 4.3. *A $(243, 22, 1, 2)$-SRG regular graph is known to exist. Therefore, there exists an $(891, 243, 3, 11)$-configuration with $\mu = 2$ that is optimal of type II.*

Referring to the listing in [3, §VI 5], we examined all the feasible parameter sets for a $(b,(r-1)k,r-2,\mu)$-SRG such that

$$k \geq \mu = \frac{(r-1)^2 k(k-1)}{b-k(r-1)-1}$$

and bk/r is an integer, up to $b = 280$. The feasible parameter sets are summarized as follows.

The parameters sets with $r = 2$ or 3 for which the strongly regular graphs are known to exist are listed in Table 1. For these parameter sets, the strongly regular graphs are equivalent to the corresponding type II optimal configurations. There are twelve type II optimal configurations obtained in this way.

Table 1: Strongly regular graphs yielding type II optimal configurations

b	$(r-1)k$	$r-2$	μ	v	r	k
5	2	0	1	5	2	2
9	4	1	2	6	3	2
10	3	0	1	15	2	3
15	6	1	3	15	3	3
16	5	0	2	40	2	5
27	10	1	5	45	3	5
50	7	0	1	175	2	7
56	10	0	2	280	2	10
77	16	0	4	616	2	16
81	20	1	6	270	3	10
100	22	0	6	1100	2	22
243	22	1	2	891	3	11

There are three parameter sets of this type with $r > 3$. These are $(196,39,2,9)$, $(232,33,2,5)$ and $(256,51,2,12)$. Existence of $(196,39,2,9)$- and $(232,33,2,5)$-SRGs is not known. However, it is known that there exists a $(256,51,2,12)$-SRG. It turns out that this SRG can be partitioned into K_4's, so we obtain the following theorem.

Theorem 4.7. *There exists a type II optimal* $(1088,256,4,17)$*-configuration with* $\mu = 12$*.*

Proof. A $(256,51,2,12)$-strongly regular graph is constructed in [7]. We briefly describe the construction in a simplified form. Let p and e be primes, where $e > 2$ and p is a primitive element modulo e. Let $t \geq 1$ and define $q = p^{(e-1)t}$. Consider the field $K = \mathbb{F}_q$ and let α be a primitive element of K. We denote the set

$$\{\alpha^{me} : 0 \leq m < (q-1)/e\}$$

by $K^{(e)}$.

Now we can define a strongly regular graph G by taking the elements of K as vertices and joining x and y by an edge if and only if $x-y \in K^{(e)}$. Refer to [7] for the parameters of the strongly regular graphs and other details.

When $p = 2$, $e = 5$ and $t = 2$, we obtain a $(256, 51, 2, 12)$-strongly regular graph defined on the finite field $K = \mathbb{F}_{2^8}$. Suppose that x and y are adjacent and w_1 and w_2 are the vertices adjacent to both of x and y. This means that $x + y$, $x + w_1$, $x + w_2$, $w_1 + y$ and $w_2 + y$ are all elements in the subset $K^{(e)}$. Now consider the element $z = x + y + w_1$. We have that $x + z = y + w_1 \in K^{(e)}$ and $y + z = x + w_1 \in K^{(e)}$. Hence z is adjacent to both x and y, and therefore $z = w_1$ or $z = w_2$. If $z = x+y+w_1 = w_1$, then $x = y$, which is a contradiction. Therefore we have $z = x + y + w_1 = w_2$, or $w_1 + w_2 = x + y$. Since $x + y \in K^{(e)}$, w_1 and w_2 are adjacent. Hence, the four vertices x, y, w_1 and w_2 form a complete graph K_4.

Therefore, by Theorem 4.5, we obtain a type II optimal $(1088, 256, 4, 17)$-configuration with $\mu = 12$. $\square$

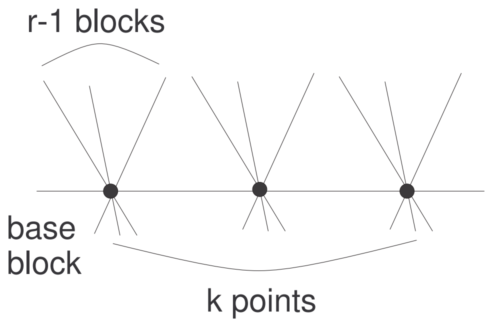
4.1 Subconfigurations

An interesting feature of optimal type II configurations is that they contain certain "subconfigurations". Suppose that $(X, \mathcal{A})$ is a $(v, b, r, k; \mu)$-CID with no triangle and such that any pair of disjoint blocks have exactly μ common intersecting blocks. Choose any block B and call it a *base block* B (see Figure 3).

Then we can classify the blocks and points in $(X, \mathcal{A})$ as follows:

- The base block B is called a type (0) block.
- A block intersecting B is called a type (1) block.
- A block disjoint from B is called a type (2) block.
- A point in B is called a type (0) point.
- A point in a type (1) block but not in B is called a type (1) point.
- The remaining points are called type (2) points.

Figure 3: A base block and the blocks intersecting it



Then we observe a regular incidence structure between the subclasses of the points and blocks as follows:

- A block of type (0) contains k points of type (0). The number of type (0) blocks is 1.
- A block of type (1) contains 1 point of type (0) and $k-1$ points of type (1). The number of type (1) blocks is $(r-1)k$.
- A block of type (2) contains μ points of type (1) and $k-\mu$ points of type (2). The number of type (2) blocks is $b-(r-1)k-1$.
- A point of type (0) is contained in 1 block of type (0) and $r-1$ blocks of type (1). The number of type (0) points is k.
- A point of type (1) is contained in 1 block of type (1) and $r-1$ blocks of type (2). The number of type (1) points is $k(k-1)(r-1)$.
- A point of type (2) is contained in r blocks of type (2). The number of type (2) points is $v-k(k-1)(r-1)-k$.

By these observations, it follows that the set of type (2) points and type (2) blocks yields a subconfiguration of $(X, \mathcal{A})$.

Theorem 4.8. *Suppose that $(X, \mathcal{A})$ is a $(v, b, r, k; \mu)$-CID with no triangle and such that any pair of disjoint blocks have exactly μ common intersecting* *blocks. Let B be any base block, let X_B be the set of type (2) points and let $\mathcal{A}_B$ be the set of type (2) blocks (restricted to the points in X_B). Then $(X_B, \mathcal{A}_B)$ is a $(v', b', r, k-\mu)$-configuration, where*

$$v' = v - k - k(k-1)(r-1),$$

and

$$b' = b - 1 - k(r-1).$$

Remark 4.1. Other subsystems can also be obtained from the above observations, but they amount to trivial designs.

Example 4.4. *In Theorem 4.7, we showed that there exists a triangle-free $(1088, 256, 4, 17; 12)$-CID such that any pair of disjoint blocks intersect exactly 12 common blocks. Applying Theorem 4.8, we see that this CID contains $(255, 204, 4, 5)$-configurations as subsystems.*

4.2 Alternate proof of Theorem 3.3

We now give a direct combinatorial proof of Theorem 3.3, as promised.

Proof. Assume that $\mu^*(v, b, r, k) < \infty$ and let $(X, \mathcal{A})$ be any $(v, b, r, k; \mu)$-CID. We pick an arbitrary base block B and designate blocks as type (0), (1) and (2), as in Section 4.1. Note that $(X, \mathcal{A})$ need not satisfy the conditions assumed in Section 4.1. However, it is easy to see that there are $k(r-1)$ blocks of type (1) and $b - k(r-1) - 1$ blocks of type (2) (as was the case in Section 4.1).

Define a set

$$\mathcal{I} = \{(A_1, A_2) \subseteq \mathcal{A} \times \mathcal{A} : A_1 \text{ is type (1)},\ A_2 \text{ is type (2)},\ A_1 \cap A_2 \neq \emptyset\}.$$

We will compute $|\mathcal{I}|$ in two different ways.

First, we choose a block of type (1). Since each block of type (1) intersects at most $(k-1)(r-1)$ blocks of type (2), we have

$$|\mathcal{I}| \leq (r-1)^2 k(k-1). \tag{18}$$

Second, we choose a block A of type (2). Since a block of type (2) is disjoint from B, there are at least μ blocks of type (1) that intersect both A and B. Thus, we have the inequality

$$|\mathcal{I}| \geq \mu(b - k(r-1) - 1). \tag{19}$$

¿From inequalities (18) and (19), we obtain

$$\mu \leq \frac{(r-1)^2 k(k-1)}{b-k(r-1)-1}.$$

□

5 Counting triangles

Recall that the variable x_1 denotes the number of triangles in a configuration. Theorem 3.3 was derived using the fact that $x_1 \geq 0$. If we are able to find a positive lower bound on x_1, say $x_1 \geq \tau$, then the bound can be strengthened. The following is proven in the same manner as Theorem 3.3 (in fact, both proofs of Theorem 3.3 can be adapted to yield Theorem 5.1).

Theorem 5.1. *Suppose $\mu^*(v,b,r,k) < \infty$, and suppose that any (v,b,r,k)-configuration has at least τ triangles. then*

$$\mu^*(v,b,r,k) \leq \frac{(r-1)^2 k(k-1)}{b-k(r-1)-1} - \frac{3\tau}{\delta},$$

where δ is defined in (3).

In view of this theorem, we investigate the existence of triangles in configurations. We begin with a simple observation that will then be generalized.

Fix a base block B in a (v,b,r,k)-configuration $(X,\mathcal{B})$ and consider all the blocks intersecting B. There are $k(r-1)$ such blocks, as depicted in Figure 3. If there is no triangle in the configuration, then the points in these blocks (excluding the points in B) must all be distinct. Hence, in triangle-free configuration, we have

$$v \geq k(k-1)(r-1)+k.$$

In other words, if $v < k(k-1)(r-1)+k$, there must be at least one triangle in the configuration.

We now generalize this argument. As above, fix a base block B. For any point $x \in X \backslash B$, define

$$\gamma_x = |\{y \in B : \exists A \in \mathcal{B} \text{ such that } \{x,y\} \subseteq A\}|.$$

Then we have $0 \leq \gamma_x \leq k$ for all $x \in X \backslash B$.

We also define

$$p_i = |\{x \in X \setminus B : \gamma_x = i\}|,$$

for $i = 0, \ldots, k$. Since any point in $X \setminus B$ has a unique value of γ_x, we obtain the equation

$$\sum_{i=0}^{k} p_i = v - k. \tag{20}$$

Now we count pairs of the form (x, A), where $x \in X \setminus B$, $A \in \mathcal{B}$, $x \in A$ and $A \cap B \neq \emptyset$. This yields another equation :

$$k(k-1)(r-1) = \sum_{x \in X \setminus B} \gamma_x = \sum_{i=0}^{k} i p_i. \tag{21}$$

Finally, the number of the triangles that include B, which we denote by τ_B, is counted as follows:

$$\tau_B = \sum_{x \in X \setminus B} \binom{\gamma_x}{2} = \sum_{i=0}^{k} \binom{i}{2} p_i. \tag{22}$$

It is not hard to find the minimum value of τ_B, subject to (20), (21), and the requirement that $p_i \geq 0$ for all i. Basically, we can assume that all but two of the values p_i equal zero when computing the minimum. More precisely, the minimum is attained when we have $p_i = 0$ if $i \notin \{s, s+1\}$, for a particular value of s. The value of s, and the values of p_s and p_{s+1}, are as follows:

$$\begin{aligned} s &= \left\lfloor \frac{k(k-1)(r-1)}{v-k} \right\rfloor \\ p_s &= (s+1)(v-k) - k(k-1)(r-1), \quad \text{and} \\ p_{s+1} &= k(k-1)(r-1) - s(v-k). \end{aligned}$$

Then

$$\tau_B \geq \tau_B^* = k(k-1)(r-1)s - \frac{(v-k)s(s+1)}{2}. \tag{23}$$

Remark 5.1. If

$$\frac{k(k-1)(r-1)}{v-k} \in \mathbb{Z},$$

then we have

$$\begin{aligned} s &= \frac{k(k-1)(r-1)}{v-k}, \\ p_s &= v-k, \quad \text{and} \\ p_{s+1} &= 0. \end{aligned}$$

In this case,

$$\tau_B^* = \frac{s(s-1)(v-k)}{2}.$$

Once we have computed the above-described lower bound τ_B^* for τ_B, we compute a lower bound on τ:

$$\tau \geq \frac{b\,\tau_B^*}{3}. \tag{24}$$

Then we can apply Theorem 5.1.

We provide an example to illustrate.

Example 5.1. *We will show that* $\mu^*(12,12,3,3) = 3$.

First, observe that $\mu^*(12,12,3,3) < \infty$ *by Lemma 2.2. If we apply Theorem 3.3, we get*

$$\mu^*(12,12,3,3) \leq \frac{24}{5} = 4.8.$$

Since μ *must be an integer, it follows that* $\mu^*(12,12,3,3) \leq 4$.

However, if we count triangles, then this upper bound can be improved. Using the formulas presented above, we have $s = 1$, $p_1 = 6$ *and* $p_1 = 3$. *Then, from (23) and (24), we compute* $\tau_B^* = 3$ *and*

$$\tau \geq \frac{12 \times 3}{3} = 12.$$

Finally, applying Theorem 5.1, we have

$$\mu^*(12,12,3,3) \leq \frac{24}{5} - \frac{3 \times 12}{30} = \frac{18}{5}.$$

Since μ *must be an integer, we have that* $\mu^*(12,12,3,3) \leq 3$.

It is in fact possible to construct a $(12,12,3,3;3)$*-CID. The blocks and points of this CID are as follows:*

$$\begin{aligned} X &= \{1,2,3,4,5,6,7,8,9,T,E,V\}, \quad \textit{and} \\ \mathcal{A} &= \{159, 17V, 18T, 25V, 26T, 28E, 36V, 37E, 389, 45T, 46E, 479\}. \end{aligned}$$

Summarizing, it follows that $\mu^*(12,12,3,3) = 3$.

6 Summary

We have presented several bounds on common intersection designs, and analyzed several interesting extremal cases. There remains much work to be done on common intersection designs, especially constructing designs that have the maximum possible value of μ, for various values of the parameters v, b, r and k.

Acknowledgements

D.R. Stinson's research is supported by the Natural Sciences and Engineering Research Council of Canada through the grant NSERC-RGPIN #203114-02.

References

[1] S.A. Çamtepe and B. Yener. Combinatorial design of key distribution mechanisms for wireless sensor networks. *Lecture Notes in Computer Science* **3193** (2004), 293–308 (ESORICS 2004 Proceedings).

[2] D.W. Carman, P.S. Kruus and B.J. Matt. Constraints and Approaches for Distributed Sensor Network Security. *NAI Labs Technical Report #00-010*, September 2000.

[3] C.J. Colbourn and J.H. Dinitz, editors. *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, 1996.

[4] L. Eschenauer and V.D. Gligor. A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 41–47.

[5] J. Lee and D.R. Stinson. A combinatorial approach to key predistribution for distributed sensor networks. To appear in *Proceedings of the IEEE Wireless Communications and Networking Conference* (WCNC 2005 Proceedings).

[6] J. Lee and D.R. Stinson. Deterministic key predistribution schemes for distributed sensor networks. To appear in *Lecture Notes in Computer Science* (SAC 2004 Proceedings).

[7] J.H. van Lint and A. Schrijver. Constructions of strongly regular graphs, two-weight codes and partial geometries by finite fields. *Combinatorica* **1** (1981), 63–73.

[8] D.R. Stinson. *Combinatorial Designs: Constructions and Analysis.* Springer-Verlag, New York, 2003.

[9] R. Wei and J. Wu. Product construction of key distribution schemes for sensor networks. To appear in *Lecture Notes in Computer Science* (SAC 2004 Proceedings).

Appendix: Derivation of equation (16)

Here, we present an algebraic derivation of equation (16). Note that we use the identity $bk = vr$ in several places.

$$
\begin{aligned}
&\frac{3c_1 - c_2 - c_3}{\delta} \\
= \quad & \frac{3\left(\frac{b(b-1)(b-2)-vr(r-1)(r-2)}{6}\right)}{\left(\frac{b(b-1)-vr(r-1)}{2}\right)} - (b-2) - k(r-1) \\
= \quad & \frac{(b-1)(b-2) - k(r-1)(r-2)}{b-1-k(r-1)} - (b-2) - k(r-1) \\
= \quad & \frac{(b-1)(b-2) - k(r-1)(r-2) - (b-1-k(r-1))(b-2+k(r-1))}{b-1-k(r-1)} \\
= \quad & \frac{-k(r-1)(r-2) - k(r-1) + k^2(r-1)^2}{b-1-k(r-1)} \\
= \quad & \frac{(r-1)^2 k(k-1)}{b-1-k(r-1)}.
\end{aligned}
$$