AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **52** (2012), Pages 243–268

Identifying flaws in the security of critical sets in latin squares via triangulations

Diane M. Donovan James G. Lefevre

Thomas A. McCourt

School of Mathematics and Physics
The University of Queensland
Brisbane, QLD 4072
Australia

Nicholas J. Cavenagh

Department of Mathematics
University of Waikato
Private Bag 3105, Hamilton
New Zealand

Abdollah Khodkar

Department of Mathematics
University of West Georgia
Carrollton, GA 30118
U.S.A.

Abstract

In this paper we answer a question in theoretical cryptography by reducing it to a seemingly unrelated geometrical problem. Drápal (1991) showed that a given partition of an equilateral triangle of side n into smaller, integer-sided equilateral triangles gives rise to, under certain conditions, a latin trade within the latin square based on the addition table for the integers (mod n). We apply this result in the study of flaws within certain theoretical cryptographic schemes based on critical sets in latin squares. We classify exactly where the flaws occur for an infinite family of critical sets. Using Drápal's result, this classification is achieved via a study of the existence of triangulations of convex regions that contain prescribed triangles.

1 Introduction

A *critical set* in a latin square is a minimal defining set of the latin square. Thus a critical set provides a way of determining a latin square with only partial information. Knowledge about critical sets thus gives us insight into the security of using latin squares as cryptographic keys. In this paper we analyse this security through the framework of secret sharing schemes. We emphasize that our results contribute to painting a broad picture of the security of latin squares and the structural properties of critical sets in latin squares, and that our approach is from a theoretical perspective.

A *secret sharing scheme* is a way of sharing a key or password between the members of the scheme. Each member of the scheme receives a "share" of information, so that:

- to recover the key a specified number, x, of members of the scheme must contribute their share; and
- no subset of strictly less than x members can recover the key.

Seberry and Street [13] and Gamble, Maenhaut, Seberry and Street [8] discussed the use of minimal defining sets in block designs as a form of secret sharing. Grannell, Griggs and Street [9] identified a potential flaw in this scheme and gave examples of some block designs displaying this flaw. It will be shown that a similar flaw occurs in a scheme based on latin squares. The overall aim (Theorem 3.1) is to show that most elements of an infinite family of critical sets, which occur in the addition table (mod n), display this flaw.

To prove this, we first show, in Section 4, that the problem in question may be redefined in terms of latin bitrades. In Section 5, we further reduce the problem to one of geometry by using a result from Drápal [6] which shows that latin bitrades in the addition table (mod n) arise from certain partitions of integer-sided equilateral triangles into smaller, integer-sided equilateral triangles. In Section 6, we list results on the existence of such triangulations from [4] and [12], making frequent use of these in Sections 7 and 8 to complete the proof of Theorem 3.1.

2 Definitions

Let $N = \{i \mid 0 \leq i \leq n-1\} \subset \mathbb{N} \cup \{0\}$. Let N^2 and N^3 denote, respectively, the Cartesian products $N \times N$ and $N \times N \times N$. Let $P \subseteq N^3$, and suppose that if $(n_1, n_2, n_3), (n_1', n_2', n_3') \in N$, either at most one of $n_1 = n_1'$, $n_2 = n_2'$, $n_3 = n_3'$ is true, or all three are true. Then we say that P is a *partial latin square*. The *size* of P is equal to $|P|$. For ease of understanding the ordered triple (n_1, n_2, n_3) may be regarded as referring to the occurrence of *symbol* n_3 in *cell* (n_1, n_2) of an $n \times n$ array; this cell occurs in *row* n_1 and *column* n_2. If a cell contains no symbol then it is called *empty*. Conversely, if a cell contains a symbol it is said to be *filled*. If, in a partial latin square, there are no empty cells, then P is called a *latin square* of order n.

We define $\theta : N^3 \mapsto N^2$ so that $\theta(n_1, n_2, n_3) = (n_1, n_2)$. For any $S \subseteq N^3$, use the notation θS to denote the image of S under the map θ. For a partial latin square P, its *shape* is given by θP, that is, the set of filled cells of the partial latin square.

A partial latin square P of order n is said to be *completable* if there exists a latin square L of order n such that $P \subseteq L$. If there is only one such possible L of order n then P is said to be *uniquely completable* and P is called a *defining set* of L. Furthermore, if C is a uniquely completable partial latin square such that no proper subset of C is uniquely completable, C is said to be a *critical set* or a *minimal defining set*.

The *back circulant* latin square, B_n, is defined to be the set

$$B_n = \{(i, j, k) \mid k = i + j \,(\mathrm{mod}\ n) \text{ for all } i, j \in N\}.$$

Note that B_n arises as the addition table for the integers modulo n. Donovan and Cooper [5] and Cavenagh, Donovan and Khodkar [3] found infinite families of critical sets contained in back circulant latin squares.

Theorem 2.1. (Donovan & Cooper, [5]) *Let* $0 \leq r \leq n-1$, *then*

$$C_{n,r} = \{(i, j, i + j) \mid i, j \geq 0 \text{ and } i + j < r\} \cup$$

$$\{(i, j, i + j \,(mod\ n)) \mid i, j \leq n - 1 \text{ and } i + j \geq n + r\}$$

is a critical set of B_n.

These are the critical sets under consideration in this paper. For example, the critical set $C_{7,4}$ is

0	1	2	3			
1	2	3				
2	3					
3						
						4
					4	5

.

3 The secret sharing scheme and its flaw

The secret sharing scheme under analysis, in which the key is a latin square, is as follows. In general, start with a critical set C of size m in a latin square S of order n. Next, divide the critical set between $x \leq m$ individuals; such that each individual receives a *share* of the key consisting of a triple (or collection of triples) from the critical set. This is performed in such a manner that the union of shares of any i individuals, where $i < x$, does not contain the entire critical set.

At first glance it seems obvious that any subset of $m - 1$ individuals in the above scheme should not be able to recreate the key. However, if the value m is public, this is not necessarily the case. In some cases there is a unique critical set of size m which

contains a specified subset of size $m-1$. For example, it can be shown that $C_{7,4}$ is the unique critical set of size 13 containing the partial latin square $C_{7,4} \setminus \{(1,2,3)\}$.

In the following, consider the above scheme and suppose that C (and thus S) is secret, while m and n are known.

Definition 3.1. *Let C be a critical set of a latin square S. For a particular $(u,v,w) \in C$, let $\mathcal{L}$ be the set of latin squares L such that $C \setminus \{(u,v,w)\} \subset L$. Suppose that for each (x,y,z) such that $(x,y,z) \in M \in \mathcal{L}$ for some $M \neq S$, there exists $M' \in \mathcal{L}$ such that $M' \neq M$ and $(x,y,z) \in M'$. Then define (u,v,w) to be a* bad triple *of C. If (u,v,w) is not a bad triple define it to be a* good triple *of C.*

If a critical set C contains a bad triple (u,v,w), it is possible to break a secret sharing scheme, given that m and n are known, using only the information from $C \setminus \{(u,v,w)\}$. Simply generate all latin squares that contain $C \setminus \{(u,v,w)\}$; since $\{u,v,w\}$ is bad, precisely one such square, L, has elements unique to it and $L = S$. Thus it would seem desirable to be aware of bad triples in critical sets; it is precisely this identification, of bad triples, which is the goal of this paper.

Our main aim is to prove the following:

Theorem 3.1. *Let $1 \leq r \leq n-2$. A triple in $C_{n,r}$ is bad if it is not an element of the following set:*

$$\{(0,0,0),(0,r-1,r-1),(r-1,0,r-1),(n-1,n-1,n-2),$$
$$(n-1,r+1,r),(r+1,n-1,r)\} \cup$$
$$\left\{ \alpha \;\middle|\; \begin{array}{ll} \alpha \in \{(1,1,2)\} & \text{if } r=4, \text{ or} \\ \alpha \in \{(0,1,1),(1,0,1),(1,1,2)\} & \text{if } r=3, \text{ or} \\ \alpha \in \{(n-2,n-2,n-4)\} & \text{if } r=n-5, \text{ or} \\ \alpha \in \left\{ \begin{array}{l} (n-1,n-2,n-3),(n-2,n-1,n-3), \\ (n-2,n-2,n-4) \end{array} \right\} & \text{if } r=n-4 \end{array} \right\}.$$

Proof that the remaining triples are good is implied by Theorem 1 from [12]. For simplicity, we do not consider the cases $r \in \{0, n-1\}$; computational evidence suggests most of the triples are bad in these cases also, however the pattern is more complicated. For these cases, results establishing a subset of bad triples can be found in [12]. For $2 \leq n \leq 9$ we have verified Theorem 3.1 by computer, hence, from now on we assume $9 < n$.

It is economical at this point to take advantage of some of the symmetries of $C_{n,r}$ and B_n. We henceforth always use the notation $(a,b,a+b \pmod n) \in C_{n,r}$ to denote a triple which we wish to show is bad. The combinatorial properties of B_n are preserved trivially under the transformations $(i,j,i+j \pmod n) \mapsto (j,i,i+j \pmod n)$ and $(i,j,i+j \pmod n) \mapsto (n-1-i,n-1-j,-i-j-2 \pmod n)$. For these reasons and from above, we henceforth assume, without loss of generality, that:

$$9 \leq n, \quad 0 \leq a \leq b, \quad 0 < a+b < r \leq n-2, \tag{1}$$
$$r=3 \implies (a,b) \notin \{(0,1),(1,1)\}, \quad r=4 \implies (a,b) \notin \{(1,1)\}, \tag{2}$$
$$(a,b) \notin \{(0,0),(0,r-1)\}. \tag{3}$$

Moreover, the maps $(i, j, i+j \pmod n) \mapsto (j, r-i-j-1 \pmod n, r-i-1 \pmod n)$ and $(i, j, i+j \pmod n) \mapsto (r-i-j-1 \pmod n, j, r-i-1 \pmod n)$ fix both $C_{n,r}$ and B_n. By applying the former when $a+2b+1 \leq r$ (consider the second inequality in (1)) and the latter when $2a+b+1 < r < a+2b+1$, we may henceforth also assume that:

$$r \leq 2a+b+1. \tag{4}$$

4 Latin bitrades

In this section we show that bad triples within a critical set may be defined in terms of latin bitrades. Consider two latin squares L and M both of order n such that $L \neq M$. Then the pair (T_1, T_2) where

$$T_1 = L \setminus M \text{ and } T_2 = M \setminus L$$

is called a *latin bitrade*. Sometimes T_1 is called a *latin trade* in L and T_2 is called its *disjoint mate*. An equivalent definition of a latin trade is a subset T_1 of a latin square L such that there exists a partial latin square T_2 of order n with the same shape as T_1 where $T_1 \cap T_2 = \emptyset$ and $(L \setminus T_1) \cup T_2$ is also a latin square. Furthermore, $|T_1| = |T_2|$ is denoted as the *size* of the trade. For a recent survey on latin bitrades, see [2]. The following well known result connects latin trades and critical sets (again, for more discussion on this result see [10] or [11]).

Lemma 4.1. *Let L be a latin square and $C \subseteq L$ a critical set. Then C intersects all latin trades $T \subseteq L$ and for each entry $(i, j, k) \in C$ there exists a latin trade $T \subseteq L$ such that $C \cap T = \{(i, j, k)\}$.*

We are now ready to define bad triples in terms of latin bitrades.

Lemma 4.2. *Let C be a critical set of a latin square S of order n, $(u, v, w) \in C$ and $I = C \setminus \{(u, v, w)\}$. Suppose that for each $(c, d, e) \in N^3 \setminus S$, either $I \cup \{(c, d, e)\}$ has no completion to a latin square of order n, or there exist two latin bitrades (T_1, T_2) and (T_1', T_2') such that $T_1, T_1' \subseteq S \setminus I$, $(c, d, e) \in T_2 \cap T_2'$ and $T_2' \neq T_2$. Then (u, v, w) is a bad triple in C.*

Our next aim is to determine when $(C_{n,r} \setminus \{(a, b, a+b \pmod n)\}) \cup \{(c, d, e)\}$ has a completion to a latin square. Let $\mathcal{L}$ be the set of all latin squares of order n which contain $C_{n,r} \setminus \{(a, b, a+b \pmod n)\}$. Define the set $K = \cap_{L \in \mathcal{L}} L$. The precise form of K was categorized by Fitina, Seberry and Chaudry [7]:

Theorem 4.3. (Fitina, Seberry & Chaudry, [7]) *In the following we assume that $0 \leq i, j \leq n-1$. If $0 \leq a \leq b$ and $a+b < r$ then*

$$K = \{(i, j, i+j \,(mod\, n)) \mid i \leq a-1 \text{ or } j \leq b-1 \text{ or } a+b < i+j < r$$

$$\text{or } a+b+n+1 \leq i+j\}.$$

Combining Lemma 4.2 and the above theorem, we have the following:

Lemma 4.4. *Let n, r, a, b satisfy* (1), (2), (3) *and* (4). *Let c, d and e be any positive integers satisfying*

$$a \leq c \leq n-1, \tag{5}$$
$$b \leq d \leq n-1, \tag{6}$$
$$r \leq c+d \leq a+b+n \text{ or } (a,b)=(c,d), \tag{7}$$
$$\begin{gathered}\text{either } \max\{r, b+c, a+d\} \leq e \leq n-1 \text{ or} \\ \max\{0, b+c-n, a+d-n\} \leq e < \min\{a+b+1, c, d\},\end{gathered} \tag{8}$$
$$c+d \not\equiv e \pmod{n}. \tag{9}$$

Suppose that there exists two latin bitrades (T_1, T_2) and (T_1', T_2') satisfying

- $T_2 \neq T_2'$,
- $T_1, T_1' \subset B_n \setminus K$ *and*
- $(c, d, e) \in T_2 \cap T_2'$.

Then $(a, b, a+b)$ is a bad triple in $C_{n,r}$.

So Theorem 3.1 can potentially be proven by showing the existence of certain latin bitrades. In the next section, we show how these latin bitrades may be defined geometrically, in the process making the proof of Theorem 3.1 manageable.

5 Drápal Triangulations

It was shown by Drápal [6] that if the cells of B_n are represented as points in the plane, then certain latin bitrades can be identified with a partition of an equilateral triangle with sides of length n into smaller, integer-sided equilateral triangles, with the property that each point is a vertex of at most three of these triangles. To explain this concept in more detail the following definitions are introduced.

A *region* in the plane is defined as follows. Let $k, i, x_i, y_i \in \mathbb{Z}$ and $0 \leq i \leq k-1$. Let $R = (x_0, y_0), (x_1, y_1), \ldots, (x_i, y_i), \ldots, (x_{k-1}, y_{k-1})$ be a sequence of points which satisfies the following condition: for all $0 \leq i \leq k-1$,

$$x_i = x_{i+1 \,(\mathrm{mod}\ k)} \text{ or } y_i = y_{i+1 \,(\mathrm{mod}\ k)} \text{ or } x_i + y_i = x_{i+1 \,(\mathrm{mod}\ k)} + y_{i+1 \,(\mathrm{mod}\ k)}.$$

The *reduced form* R' of R is formed by successively deleting any points (x_i, y_i) from R whenever $(x_{i-1}, y_{i-1}), (x_i, y_i)$ and (x_{i+1}, y_{i+1}) are collinear.

If the straight line segments between $(u_i, v_i) \in R'$ and $(u_{i+1 \,(\mathrm{mod}\ l)}, v_{i+1 \,(\mathrm{mod}\ l)}) \in R'$, $0 \leq i \leq l-1 = |R'|-1$, form the boundary of a polygon or two polygons intersecting at a point, then R is called a *region*. Furthermore, the region R is denoted by $R = (x_0, y_0) \to (x_1, y_1) \to \ldots \to (x_i, y_i) \to \ldots \to (x_{k-1}, y_{k-1})$, and if $1 < |R|$, we refer to the elements of the reduced form of R as the *corners* of R.

If the reduced form of R has precisely three corners, then R is said to be a *triangle*. For $0 \leq x$, denote the region

$$FT_x^{(z_1,z_2)} = (z_1, z_2) \to (z_1 + x, z_2) \to (z_1, z_2 + x) \text{ as a } \textit{forward triangle} \text{ and}$$
$$BT_x^{(z_1,z_2)} = (z_1, z_2) \to (z_1 - x, z_2) \to (z_1, z_2 - x) \text{ as a } \textit{backward triangle}.$$

Let R be the union of regions $R_1, R_2, \ldots, R_t$; that is, $R = \cup_{1 \leq i \leq t} R_i$. If for each $1 \leq i < j \leq t$, the regions R_i and R_j intersect in at most their respective boundaries, then $\{R_i \mid 1 \leq i \leq t\}$ is called a *tessellation* of R and each R_i is a *subregion* of R.

If each of the subregions R_i is a triangle, R is said to have a *triangulation*, namely $\{R_i \mid 1 \leq i \leq t\}$, furthermore each subregion, R_i, is referred to as a *subtriangle* of R. If, in addition, each element $(a, b) \in R$ is the corner of at most three distinct subtriangles, $\{R_i \mid 1 \leq i \leq t\}$ is called a *Drápal Triangulation* of the region R. It is this property which makes the problem of finding a Drápal triangulations of a specified region non-trivial.

Consider the following group of matrices, isomorphic to the Dihedral group D_6:

$$G = \left\langle \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \right\rangle.$$

Let $\lambda \in G$, $(p, q) \in \mathbb{R}^2$ and $S \subset \mathbb{R}^2$. In this paper the set $\{(m, n)\lambda + (p, q) \mid (m, n) \in S\}$ is denoted by $S\lambda + (p, q)$.

If there exists some $(i, j) \in \mathbb{Z}^2$ and some $\lambda \in G$ such that $R_2 = R_1\lambda + (i, j)$, then R_1 and R_2 are said to be *equivalent*. Observe that the property of possessing a Drápal Triangulation is invariant under this equivalence, even though the gradients of lines may change. We frequently make use of this observation.

We will next show how to construct a latin trade in B_n of size t from a Drápal Triangulation based on t triangles. Let $Q = \{R_i \mid 1 \leq i \leq t\}$ be a Drápal Triangulation of $FT_n^{(a,b)}$. Let $P = P(Q) \subset B_n$ be the partial latin square defined so that $(\alpha, \beta, \alpha + \beta) \in P$ if and only if (α, β) is a corner of R_i, some subtriangle in Q. Next, define the following map, σ, from P to N^3. If $R_i = FT_m^{(\alpha,\beta)}$, then

$$\sigma : (\alpha, \beta, \alpha + \beta) \mapsto (\alpha, \beta, \alpha + \beta + m).$$

Similarly, if $R_i = BT_m^{(\alpha,\beta)}$, then

$$\sigma : (\alpha, \beta, \alpha + \beta) \mapsto (\alpha, \beta, \alpha + \beta - m).$$

As usual, in the above maps all integers are evaluated mod n.

Theorem 5.1. (Drápal, [6]) *The set of triples given by σP is a partial latin square of order n. Moreover, $(P, \sigma P)$ is a latin bitrade.*

Proof. See [6] for details. □

For example, consider the following Drápal Triangulation of $FT_7^{(1,2)}$

$$Q = \{FT_4^{(1,2)}, FT_3^{(1,6)}, FT_2^{(3,4)}, FT_1^{(4,5)}, FT_3^{(5,2)}, BT_2^{(3,6)},$$

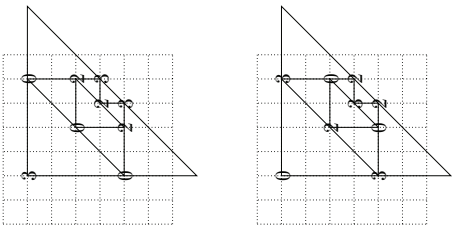


Figure 1: $(P(Q), \sigma P(Q))$

$$BT_1^{(4,6)}, BT_2^{(5,4)}, BT_1^{(5,5)}\}.$$

From above, this triangulation gives rise to the latin bitrade $(P(Q), \sigma P(Q))$, where

$$P(Q) = \{(1,2,3),(1,6,0),(3,4,0),(4,5,2),(5,2,0),(3,6,2),$$
$$(4,6,3),(5,4,2),(5,5,3)\},$$
$$\sigma P(Q) = \{(1,2,0),(1,6,3),(3,4,2),(4,5,3),(5,2,3),(3,6,0),$$
$$(4,6,2),(5,4,0),(5,5,2)\}.$$

Observe that $P(Q) \subset B_7$.

This trade is illustrated in Figure 1. Note the difference in orientation between the representation of a triangulation to that of a latin square. Thus to prove Theorem 3.1 via Lemma 4.4, for each n, r, a, b, c, d, e satisfying (1) through to (9), we need to show that there exist two distinct Drápal triangulations Q and Q' of $FT_n^{(a,b)}$ which contain the triangle $FT_x^{(c,d)}$, where either $r, c+d < e$ and $x = e-c-d$ or $c+d-n < e \leq a+b$ and $x = e+n-c-d$, or the triangle $BT_x^{(c,d)}$, where either $r \leq e < c+d$ and $x = c+d-e$ or $e < c+d-n$ and $x = c+d-e-n$.

The diagram in Figure 2 offers an intuitive approach to understanding the approach in this paper. With the above restrictions on a, b, c, d, r, n and x, the triangles $FT_x^{(c,d)}$ and $BT_x^{(c,d)}$ lie in the shaded region (except for the special case when $(a,b) = (c,d)$). The square in Figure 2 can be thought of as the latin square B_n (again, note the difference in orientation between the representation of a triangulation to that of a latin square).

From above, the following two theorems together prove Theorem 3.1. The first theorem considers forward triangles.

Theorem 5.2. *Let n, r, a and b be integers satisfying* (1), (2), (3) *and* (4) *and let c, d and $x > 0$ be any integers satisfying:*

$$a \leq c, \quad b \leq d, \tag{10}$$
$$(a,b) \neq (c,d) \implies r \leq c+d \tag{11}$$
$$(a,b) = (c,d) \implies r \leq x+a+b \tag{12}$$
$$d+x, c+x \leq n-1, \quad c+d+x \leq n+a+b. \tag{13}$$

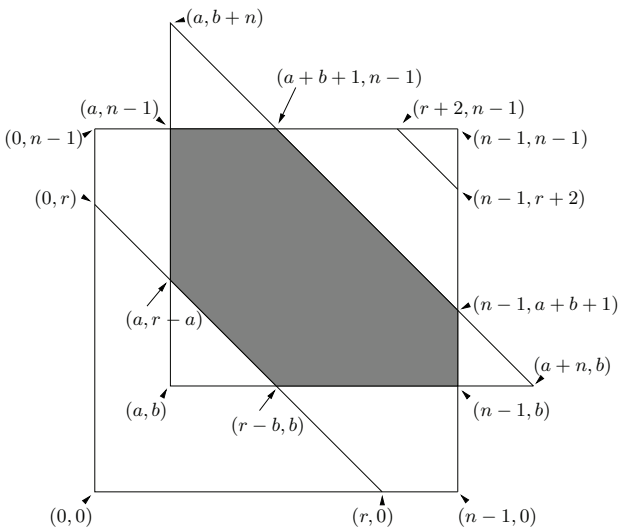


Figure 2: The triangle $FT_n^{(a,b)}$

Then there exist two distinct Drápal Triangulations Q and Q' of $FT_n^{(a,b)}$ both containing $FT_x^{(c,d)}$ such that

$$Q_0 = \{FT_f^{(a,b)}, FT_{b+n-g}^{(a,g)}, FT_{a+n-h}^{(h,b)}\} \subset Q \text{ and}$$

$$Q'_0 = \{FT_{f'}^{(a,b)}, FT_{b+n-g'}^{(a,g')}, FT_{a+n-h'}^{(h',b)}\} \subset Q,$$

for some integers f, f', g, g', h and h' satisfying

$$r - a - b \leq f, f', \tag{14}$$

$$b + f \leq g \leq n - 1 \text{ and } b + f' \leq g' \leq n - 1, \tag{15}$$

$$a + b + n - g, a + f \leq h \leq n - 1 \text{ and } a + b + n - g', a + f' \leq h' \leq n - 1. \tag{16}$$

The proof of Theorem 5.2 is given in Section 7. The next theorem considers backward triangles.

Theorem 5.3. *Let n, r, a and b be integers satisfying* (1), (2), (3) *and* (4), *and let c, d and $x > 0$ be integers satisfying:*

$$c, d \leq n - 1, \quad c + d \leq a + b + n, \tag{17}$$

$$a \leq c - x, \quad b \leq d - x, \quad r \leq c + d - x. \tag{18}$$

Then there exist two distinct Drápal triangulations Q and Q' of $FT_n^{(a,b)}$ both containing $BT_x^{(c,d)}$ such that $Q_0 \subset Q$, $Q'_0 \subset Q'$, for some integers f, f', g, g', h and h' satisfying (14), (15) *and* (16).

The proof of Theorem 5.3 is given in Section 8. The proofs of these theorems rely extensively on results from [4], in which the geometric theory for constructing Drápal Triangulations of various non-triangular regions is developed.

6 Drápal triangulations of specified regions

In the process of embedding a triangle within a Drápal Triangulation, it is often useful to know the existence of Drápal Triangulations of various non-triangular regions. The proofs of the first four results in this section are given in [4] and the proofs of the last two results are given in [12].

An L-region will be defined to be a region equivalent to

$$(\delta, 0) \to (\delta, \beta) \to (0, \beta) \to (0, \alpha) \to (\gamma, \alpha) \to (\gamma, 0),$$

where $0 < \alpha < \beta$ and $0 < \gamma < \delta$.

Theorem 6.1. ([4]) *Any region which is a convex polygon or an L-region possesses two distinct Drápal triangulations, unless it is equivalent to one of the following, where $\alpha, \beta \in \mathbb{Z}$ (see the Appendix for illustrations):*

$Z_0 = (0, 0)$,

$Z_1 = (0, 0) \to (1, 0) \to (1, \alpha) \to (0, \alpha)$ *where* $0 < \alpha$,

$Z_2 = (1, 0) \to (\alpha, 0) \to (\alpha, 1) \to (0, 1)$ *where* $0 < \alpha$,

$Z_3 = (\alpha, 0) \to (\alpha, \beta) \to (0, \beta) \to (0, \beta - 1) \to (\alpha - 1, \beta - 1) \to (\alpha - 1, 0)$ *where* $1 < \alpha, \beta$,

$Z_4 = (2, 0) \to (2, 2) \to (0, 2) \to (0, 1) \to (1, 0)$,

$Z_5 = (3, 0) \to (3, 1) \to (1, 3) \to (0, 3) \to (0, 1) \to (1, 0)$ *and*

$Z_6 = (2, 0) \to (2, 1) \to (1, 2) \to (0, 2) \to (0, 1) \to (1, 0)$.

Moreover, the regions equivalent to Z_i where $0 \leq i \leq 5$ have a unique Drápal Triangulation, while Z_6 has no Drápal triangulation.

Let $\mathcal{Z}$ be the set of all regions equivalent to any Z_i, where $1 \leq i \leq 6$ and the regions are defined as in Theorem 6.1 (see the Appendix for illustrations).

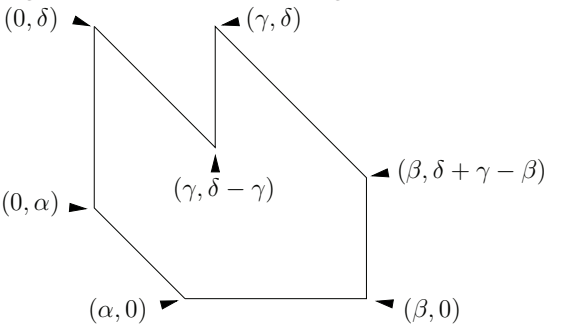
Let R be a region equivalent to

$$(\beta, 0) \to (\beta, \delta + \gamma - \beta) \to (\gamma, \delta) \to (\gamma, \delta - \gamma) \to (0, \delta) \to (0, \alpha) \to (\alpha, 0)$$

with $0 \leq \alpha < \beta, \delta$, $0 < \gamma < \beta, \delta + 1$ and $0 \leq \delta + \gamma - \beta$ (this region is illustrated in Figure 3).

$X_1 = (\beta, 0) \to (\beta, \beta - 1) \to (\beta - 1, \beta) \to (\beta - 1, 1) \to (0, \beta) \to (0, \beta - 1) \to (\beta - 1, 0)$,

Figure 3: Illustration of the region R.



$X_2 = (3,0) \to (1,2) \to (1,1) \to (0,2) \to (0,1) \to (1,0)$,

$X_3 = (3,0) \to (3,1) \to (1,3) \to (1,2) \to (0,3) \to (0,1) \to (1,0)$,

$X_4 = (3,0) \to (3,2) \to (2,3) \to (2,1) \to (0,3) \to (0,1) \to (1,0)$ and

$X_5 = (\beta,0) \to (\beta,\beta-2) \to (\beta-1,\beta-1) \to (\beta-1,0) \to (0,\beta-1) \to (0,\beta-2) \to (\beta-2,0)$.

Let $\mathcal{X}$ be the set of all regions equivalent to any X_i, where $1 \leq i \leq 5$ (see the Appendix for illustrations).

Theorem 6.2. ([4]) *Let $0 \leq \alpha < \beta, \delta$; $0 < \gamma < \beta, \delta + 1$; and $0 \leq \delta + \gamma - \beta$. The region $R = (\beta,0) \to (\beta,\delta+\gamma-\beta) \to (\gamma,\delta) \to (\gamma,\delta-\gamma) \to (0,\delta) \to (0,\alpha) \to (\alpha,0)$ has a Drápal Triangulation if and only if $R \neq X_1$ and a second distinct Drápal Triangulation if and only if R is not equivalent to any X_i, where $1 \leq i \leq 5$.*

The next four lemmas are the first results discussed in which two distinct Drápal Triangulations of a specific region both contain some fixed triangle.

Lemma 6.3. ([4]) *Let $1 < \alpha \leq \beta$; $0 < \chi \leq \alpha$; $0 < \gamma \leq \beta - \chi$; $0 \leq \delta \leq \alpha - \chi$; and $\alpha \leq \gamma + \delta$. If $6 < \alpha + \beta$, then there exist two distinct Drápal Triangulations of the region $R = (\beta,0) \to (\beta,\alpha) \to (0,\alpha) \to (\alpha,0)$ both of which contain $FT_\chi^{(\gamma,\delta)}$.*

Lemma 6.4. ([4]) *Let $0 < \chi \leq \delta \leq \alpha \leq \beta$; $\gamma \leq \beta$; $\alpha \leq \gamma + \delta - \chi$, and suppose the condition $1 = \beta - \gamma = \beta - \alpha = \delta - \chi$ does not hold. There exists a Drápal Triangulation of the region $R = (\beta,0) \to (\beta,\alpha) \to (0,\alpha) \to (\alpha,0)$ containing $BT_\chi^{(\gamma,\delta)}$. If $6 < \alpha + \beta$ and $1 < \alpha$, then there exists a second distinct Drápal Triangulation of R which contains $BT_\chi^{(\gamma,\delta)}$ whenever $1 < \alpha - \delta$ or $1 < \beta - \gamma$ or $1 < \gamma + \delta - \alpha - \chi$.*

The next two lemmas are proved in [12] using similar techniques to the proofs from [4] of the previous four results.

Lemma 6.5. ([12]) *Let* $3 \leq \chi \leq \delta \leq \alpha \leq \beta$*;* $\gamma \leq \beta$*;* $\alpha \leq \gamma + \delta - \chi$*;* $6 < \alpha + \beta$*;* $\beta - \gamma, \alpha - \delta, \gamma + \delta - \chi - \alpha \leq 1$*; and suppose the condition* $1 = \beta - \gamma = \beta - \alpha = \delta - \chi$ *does not hold. There exists a Drápal Triangulation of the region* $R = (\beta, 0) \to (\beta, \alpha) \to (\beta - 2, \alpha + 2) \to (0, \alpha + 2) \to (0, \alpha) \to (\alpha, 0)$ *containing* $BT_{\chi}^{(\gamma,\delta)}$.

Lemma 6.6. ([12]) *Let* $3 \leq \chi \leq \delta \leq \alpha \leq \beta$*;* $\gamma \leq \beta$*;* $\alpha \leq \gamma + \delta - \chi$*;* $6 < \alpha + \beta$*; and* $\beta - \gamma, \alpha - \delta, \gamma + \delta - \alpha - \chi \leq 1$*. There exists a Drápal Triangulation of the region* $R = (\beta + 2, 0) \to (\beta + 2, \alpha - 2) \to (\beta, \alpha) \to (0, \alpha) \to (\alpha, 0)$ *containing* $BT_{\chi}^{(\gamma,\delta)}$.

7 Forward Triangles

The aim of this section is to prove Theorem 5.2. Recall that n, r, a, b, c, d, x are any integers satisfying $(1), (2), (3), (4), (10), (11), (12), (13)$ and $x > 0$. Five cases are considered. These are listed in Table 1. Frequent use is made of the constructive lemmas from Section 6. We remind the reader that for a Drápal Triangulation, the condition that each vertex of a triangle is the vertex of at most three triangles must be satisfied.

Table 1: Cases for placing $FT_x^{(c,d)}$

$F1$	$(c, d) = (a, b)$.
$F2.1$	$d + x \leq a + b + 1$ and $c + d - a \leq a + b + 1$.
$F2.2$	$d + x \leq a + b + 1$ and $a + b + 1 < c + d - a$.
$F3.1$	$a + b + 1 \leq d + x$ and $c + d - a \leq d + x$.
$F3.2$	$a + b + 1 \leq d + x$ and $d + x < c + d - a$.

7.1 Case $F1$: $(c, d) = (a, b)$.

From (10) and (13), $b + x \leq d + x \leq n - 1$. There are two subcases to consider.

$F1.1$: $a + n - x \leq n - 1$.

$F1.2$: $a + n - x > n - 1$.

Subcase $F1.1$: $a + n - x \leq n - 1$.

Let $(f, g, h) = (x, b + x, n - 1)$. From (12), $r - a - b \leq f$ and $g \leq n - 1$. From (10) and (13), $a + f \leq h$. By the conditions for this subcase, $a + b + n - (b + x) \leq n - 1$. Thus f, g and h satisfy (14), (15) and (16). Consider the tessellation $Q_1 = Q_0 \cup \{R_1 = (h, b) \to (h, a + b + n - h) \to (a + b + n - g, g) \to (a, g) \to (a + x, b)\}$ of $FT_n^{(a,b)}$. This tessellation is illustrated in the Appendix. By Theorem 6.1, there exists a Drápal Triangulation of $FT_n^{(a,b)}$ containing $FT_x^{(a,b)}$ and if $R_1 \notin \mathcal{Z}$ then, there exists a second such triangulation with $(f', g', h') = (f, g, h)$.

Let $R_1 \in \mathcal{Z}$. If $a + x, a + n - x < n - 1$, let $(f', g', h') = (x, b + x, n - 2) = (f, g, h - 1)$. Consider the tessellation $Q_2 = Q_0' \cup \{R_2 = (h', b) \to (h', a + b + n - h') \to (a + b + n - g', g') \to (a, g') \to (a + x, b)\}$ of $FT_n^{(a,b)}$. By Theorem 6.1, there exists a second distinct Drápal Triangulation of $FT_n^{(a,b)}$ containing $FT_x^{(a,b)}$.

If $a+x=n-1$, then $x=n-1-a$. From above, $b+x\leq n-1$. From (1), $a\leq b$. Thus, $a+x\leq b+x\leq n-1=a+x$, so, $a=b$. If $2<x$, as $R_1\in\mathcal{Z}$, then $a+1\leq 1$. So, $a=b=0$, contradicting (3). If $x\leq 2$, then $n-3\leq a$, thus, by (1), $n-3\leq a\leq b$. So, again by (1), $2n-6\leq a+b\leq n-3$, hence, $n\leq 3$, a contradiction.

If $a+n-x=n-1$, then $a=x-1$. As $R_1\in\mathcal{Z}$, $a+1\leq 1$, so, $a=0$ and $x=1$. Thus, as $r-a-b\leq x$ (12), it follows that $r\leq b+1$. By (1), $b<r$, so, $b+1=r$, contradicting (3).

Subcase $F1.2$**:** $a+n-x>n-1$**.**

Let $(f,g,h)=(x,a+b+1,n-1)$. From the conditions for this subcase, $x<a+1$, hence, $b+f\leq g$. Now, by (1), $a+b<r\leq n-2$. Thus, as in the previous subcase, f, g and h satisfy (14), (15) and (16). Consider the tessellation $Q_3=Q_0\cup\{R_3=(h,b)\rightarrow(h,g)\rightarrow(a,g)\rightarrow(a,b+x)\rightarrow(a+x,b)\}$ of $FT_n^{(a,b)}$. By Theorem 6.1, there exists a Drápal Triangulation of $FT_n^{(a,b)}$ containing $FT_x^{(a,b)}$. This tessellation is illustrated in the Appendix.

From (1), $a+b+1<n-1$. From the conditions of this subcase, $x<a+1$, so, $b+x<a+b+1$. Hence, by (1), $a+x\leq b+x<a+b+1<n-1$. Let $(f',g',h')=(x,n-1,a+b+1)$. Consider the tessellation $Q_4=Q_0'\cup\{R_4=(h',b)\rightarrow(h',g')\rightarrow(a,g')\rightarrow(a,b+x)\rightarrow(a+x,b)\}$ of $FT_n^{(a,b)}$. By Theorem 6.1, we are done.

For the remaining cases in this section, we assume that $(c,d)\neq(a,b)$.

7.2 Case $F2.1$: $d+x\leq a+b+1$ and $c+d-a\leq a+b+1$.

Let $(f,g,h)=(f',g',h')=(c+d-a-b,a+b+1,n-1)$. From the conditions for this case, (1) and (11), f, g and h satisfy (14), (15) and (16). Let $m_1=\min\{c+d+x-a,g\}$ and $m_2=\min\{c+d+x-b,h\}$. Let $Q_1=Q_0\cup\{BT^{(m_2,m_1)}_{m_1+m_2-c-d-x},FT_x^{(c,d)},R_1=(h,b)\rightarrow(h,g)\rightarrow(a,g)\rightarrow(a,m_1)\rightarrow(m_2,m_1)\rightarrow(m_2,b),R_2=(m_2,b)\rightarrow(m_2,c+d+x-m_2)\rightarrow(c+x,d)\rightarrow(c,d)\rightarrow(c+d-b,b),R_3=(c,d)\rightarrow(c,d+x)\rightarrow(c+d+x-m_1,m_1)\rightarrow(a,m_1)\rightarrow(a,c+d-a)\}$. (See the Appendix.) By Theorem 6.1, we are done unless for all $1\leq i\leq 3$, $R_i\in\mathcal{Z}$.

Suppose this is so. If $a+b+1=n-1$, then $a+b=n-2$, which contradicts (1). Thus $a+b+1\leq n-2$. From the conditions for this case and (1), $c+d-b\leq c+d-a\leq a+b+1\leq n-2$. From (13), $c+x\leq n-1$.

If $c+x<n-1$ and $c+d-b<n-1$, then let $(f',g',h')=(f,g+1,h-1)$. Let $m_3=\min\{c+d+x-a,g+1\}$ and $m_4=\min\{c+d+x-b,h-1\}$. Consider the tessellation $Q_2=Q_0'\cup\{BT^{(m_4,m_3)}_{m_3+m_4-c-d-x},FT_x^{(c,d)},R_4=(h-1,b)\rightarrow(h-1,g+1)\rightarrow(a,g+1)\rightarrow(a,m_3)\rightarrow(m_4,m_3)\rightarrow(m_4,b),R_5=(m_4,b)\rightarrow(m_4,c+d+x-m_4)\rightarrow(c+x,d)\rightarrow(c,d)\rightarrow(c+d-b,b),R_6=(c,d)\rightarrow(c,d+x)\rightarrow(c+d+x-m_3,m_3)\rightarrow(a,m_3)\rightarrow(a,c+d-a)\}$. The second distinct Drápal Triangulation of $FT_n^{(a,b)}$ follows by Theorem 6.1.

Suppose that $c+x<n-1$ and $c+d-b=n-1$ (so, $m_2=n-1$). As $R_2\in\mathcal{Z}$, $x=1$. Let $(f',g',h')=(f,g,h)$, $Q_3=Q_0'\cup\{BT^{(h',d)}_{d-b},BT^{(c+x,m_1)}_{m_1-d},FT_x^{(c,d)},R_3,R_7=(h',d)\rightarrow(h',g')\rightarrow(a,g')\rightarrow(a,m_1)\rightarrow(c+x,m_1)\rightarrow(c+x,d)\}$. Apply Theorem 6.1 as above.

Otherwise $c+x=n-1$. Suppose that $1<x$. Let $(f',g',h')=(f,g,h)$. Let

$Q_4 = Q'_0 \cup \{BT^{(h'-1,m_1)}_{m_1-d-1}, BT^{(h',d+1)}_1, FT^{(c,d)}_x, R_2, R_3, R_8 = (h', d+1) \to (h', g') \to (a, g') \to (a, m_1) \to (h'-1, m_1) \to (h'-1, d+1)\}$. Apply Theorem 6.1.

Otherwise $c+x = n-1$ and $x = 1$. Suppose $1 < c-a$ and let $(f', g', h') = (f, g, h)$. Let $Q_5 = Q'_0 \cup \{BT^{(c,c+d-a)}_{c-a}, BT^{(h',d+1)}_1, FT^{(c,d)}_x, R_2, R_9 = (h', d+1) \to (h', g') \to (a, g') \to (a, c+d-a) \to (c, c+d-a) \to (c, d+1)\}$. Apply Theorem 6.1. Otherwise, $c + x = n - 1$, $x = 1$ and $c - a \leq 1$. Then $n - 3 \leq a$, contradicting (1).

7.3 Case $F2.2$: $d + x \leq a + b + 1$ and $a + b + 1 < c + d - a$.

Let $(f, g, h) = (f'g', h') = (a+1, a+b+1, n-1)$. From (1), $a \leq b$ and $a+b < r \leq n-2$. Thus $2a + 1 < h = n - 1$. Thus g and h satisfy (15) and (16). From (10), (12) and the conditions of this case, $r - a \leq b + x \leq d + x \leq a + b + 1$, so f also satisfies (14). Consider the tessellation $Q_1 = Q_0 \cup \{H_1 = (h, b) \to (h, g) \to (a, g) \to (a + f, b)\}$ of $FT^{(a,b)}_n$. See the Appendix for an illustration of this tessellation. Let $\alpha = a + 1$ and $\beta = n - a - 1$. Consider the linear transformation $H_1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + (-a, -b)$. If $a+1 = 1$, then, by (4), $r \leq b+1$, which contradicts (3). Hence, $2 \leq a+1$, so, $1 < \alpha$. From (1), $9 < n$, so, $9 < (a + 1) + (n - a - 1) = \alpha + \beta$. From above $2a + 1 \leq n - 1$, so, $\alpha \leq \beta$. Now apply Lemma 6.3.

7.4 Case $F3.1$: $a + b + 1 \leq d + x$ and $c + d - a \leq d + x$.

Let $(f, g) = (f', g') = (c + d - a - b, d + x)$. By (11), (13) and the conditions of this case, f and g satisfy (14) and (15). Consider the tessellation $\{FT^{(a,b)}_f, FT^{(a,g)}_{b+n-g}, H_1 = (a + n, b) \to (a + b + n - g, g) \to (a, g) \to (a, b + f) \to (a + f, b)\}$ of $FT^{(a,b)}_n$. See the Appendix for an illustration of this tessellation. In order to complete this case two distinct Drápal Triangulations of the region H_1 are required. Recall that in each of these Drápal Triangulations the triangles $FT^{(c,d)}_x$ and $FT^{(h,b)}_{a+n-h}$ for some h satisfying (16) must occur. From (13), $c + x \leq n - 1$. There are three subcases to consider.

$F3.1.1$: $c + x < n - 1$ and either $a \neq 0$, $d \neq b + 1$ or $c + x \neq n - 2$.

$F3.1.2$: $a = 0$, $d = b + 1$ and $c + x = n - 2$.

$F3.1.3$: $c + x = n - 1$.

Subcase $F3.1.1$: $c + x < n - 1$ **and either** $a \neq 0$, $d \neq b + 1$ **or** $c + x \neq n - 2$.

Let $h = n - 1$. By the conditions of this case, $c + d - a \leq g$. From (1), $a \leq b$. Thus, $a + f = c + d - b \leq c + d - a \leq d + x \leq n - 1$. Also, from the conditions of this case, $a + b + n - d - x \leq n - 1$. Thus, h satisfies (16). Consider the tessellation $Q_1 = \{FT^{(h,b)}_{a+n-h}, FT^{(c,d)}_x, R_1 = (c, d) \to (c, g) \to (a, g) \to (a, b + f), R_2 = (h, b) \to (h, a + b + n - h) \to (a + b + n - g, g) \to (c, g) \to (c + x, d) \to (c, d) \to (a + f, b)\}$ of H_1. The conditions for this subcase imply that R_2 is not equivalent to X_1. By Theorems 6.1 and 6.2, there exists a Drápal Triangulation of $FT^{(a,b)}_n$ containing $FT^{(c,d)}_x$. Furthermore, if $\{R_1, R_2\} \not\subset \mathcal{Z} \cup \mathcal{X}$, then there exists a second distinct Drápal Triangulation of $FT^{(a,b)}_n$ containing $FT^{(c,d)}_x$ with $h' = h$. Hence we may assume that $R_1, R_2 \in \mathcal{Z} \cup \mathcal{X}$. From the conditions for this case, $a + b + n - d - x \leq n - 1$ and $c + d - a \leq d + x$. Thus, as $a \leq b$ (1), $c + d - b \leq d + x$. Hence, as $d + x \leq n - 1$ (13), it follows that $c + d - b \leq n - 1$.

Suppose that $c+d-b, a+b+n-d-x \leq n-2$. Let $h'=n-2$ and observe that h' satisfies (16). Consider the tessellation $Q_2 = \{FT_{a+2}^{(n-2,b)}, FT_x^{(c,d)}, R_1, R_3 = (n-2,b) \to (n-2, a+b+2) \to (a+b+n-g, g) \to (c,g) \to (c+x,d) \to (c,d) \to (a+f,b)\}$ of H_1. Since $2 \leq (a+b+2)-b$, R_3 is not equivalent to X_1. By Theorems 6.1 and 6.2, there exists a second distinct Drápal Triangulation of $FT_n^{(a,b)}$ containing $FT_x^{(c,d)}$.

Next, suppose that $c+d-b = n-1$ or $a+b+n-d-x = n-1$. By observation, R_2 is equivalent to neither Z_1, Z_4, Z_5, Z_6, X_3 nor X_4. From the conditions for this subcase, $c+x < n-1$, so R_2 is not equivalent to X_5. Since $1 \leq a+1$, R_2 is not equivalent to Z_0 or Z_3.

Suppose that $c+d-b = n-1$. If R_2 is equivalent to X_2, then $c = n-3$, $x=1$ and $a=1$. From the conditions of this case, $c \leq a+x$. Thus $n \leq 5$, contradicting (1). We may deduce that R_2 is equivalent to Z_2. Hence, $x=1$ and $a+1=1$. As $R_1 \in \mathcal{Z}$, $c-a \leq 1$. Thus, $c \leq 1$. Now, from (13), $d \leq n-2$. Since $c+d-b = n-1$, we have that $b \leq c-1$, so, $b=0$, which contradicts (3).

Otherwise, $c+d-b \leq n-2$ and $a+b+n-d-x = n-1$. As above, $c-a \leq 1$. Thus, either $x=1$, $c=n-3$, $d=b+1$ and $a+1=2$ (this case occurs when R_2 is equivalent to X_2), hence, $c \leq a+1=2$ and $n \leq 5$ contradicting (1), or, $x=1$, $a=0$ and $d=b$ (this case occurs when R_2 is equivalent to Z_2).

Finally, we have that $c+d-b \leq n-2$, $a+b+n-d-x = n-1$, $c-a \leq 1$, $x=1$, $a=0$ and $d=b$. If $d+x = n-1$, then $b=n-2$, contradicting (1). Thus, $d+x < n-1$. If $n-3 \leq c$, then $n \leq 4$ which contradicts (1). Thus $c < n-3$. Let $(f',g',h') = (c+d-a-b, d+x+1, n-1) = (f, g+1, h)$. Let $Q_3 = Q_0' \cup \{BT_2^{(a+2,b+2)}, FT_x^{(c,d)}, R_4 = (h,b) \to (h,g) \to (h-1,g+1) \to (2,g+1) \to (2,b), R_5 = (c,b) \to (c,b+1) \to (c+1,b) \to (2,b) \to (0,g+1) \to (0,g)\}$. By Theorem 6.1, we are done.

Subcase $F3.1.2$**:** $a=0$**,** $d=b+1$ **and** $c+x=n-2$**.**

Let $h=h'=n-2$. Note that $a+f = c+d-b = c+1 \leq c+x = n-2$. From the conditions for this subcase and $x>0$, we have that $a+b+n-d-x = n-1-x < n-1$. Hence, (16) is satisfied. Consider the tessellation $Q_4 = \{FT_{a+n-h}^{(h,b)}, FT_x^{(c,d)} = FT_{n-c-2}^{(c,b+1)}, R_1, R_6 = (h,b) \to (h,d) \to (c,d) \to (c+1,b), R_7 = (h,b+1) \to (h,b+2) \to (a+b+n-g,g) \to (c,g)\}$ of H_1. By Theorem 6.1, there exists a Drápal Triangulation of $FT_n^{(a,b)}$ containing $FT_x^{(c,d)}$ and if $R_1 \notin \mathcal{Z}$, then there exists a second distinct Drápal Triangulation of $FT_n^{(a,b)}$ containing $FT_x^{(c,d)}$.

If $R_1 \in \mathcal{Z}$, then $c-a=c \leq 1$ and, by (10), $0=a \leq c$. Hence, $n-3 \leq x \leq n-2$ and $n-x-1 \leq 2$. So, from the conditions for this subcase, $b+n-d-x \leq 2$. Thus, from (13), it follows that $b \leq 1$. From the conditions for this subcase, $d \leq 2$ and from (1) and (11), $1 \leq a+b < r \leq c+d \leq 3$, hence, $r=2$ or $r=3$, contradicting (2) or (3).

Subcase $F3.1.3$**:** $c+x=n-1$**.**

Let $h=h'=n-1$. As in Subcase $F1.1.1$, $h=h'$ satisfies (16). Consider the tessellation $Q_5 = \{FT_{a+n-h}^{(h,b)}, FT_x^{(c,d)}, R_1, R_8 = (h,b) \to (h,d) \to (c,d) \to (c+d-b,b), R_9 = (h,d) \to (h,a+b+1) \to (a+b+n-d-x, d+x) \to (c,d+x)\}$ of H_1. By Theorem 6.1, there exists a Drápal Triangulation of $FT_n^{(a,b)}$ containing $FT_x^{(c,d)}$

and if $\{R_1, R_8, R_9\} \not\subset \mathcal{Z}$, then there exists a second distinct Drápal Triangulation of $FT_n^{(a,b)}$ containing $FT_x^{(c,d)}$.

Hence, let $\{R_1, R_8, R_9\} \subset \mathcal{Z}$. Now, (1), implies that $1 \leq b$. As $R_1 \in \mathcal{Z}$, $c - a \leq 1$. As $R_9 \in \mathcal{Z}$, $a + b + n - c - d - x \leq 1$. So, $b + n - d - x \leq 2$. Hence, as $1 \leq b$, it follows that $1 + n - d - x \leq b + n - d - x \leq 2$, thus, $n - 1 \leq d + x$. Thus from (13), $d + x = n - 1$. Thus $a + b - c + 1 = a + b + n - c - d - x$, so $(a + b - c + 1) + (c - a) \leq 2$. It follows from (1), that $b = 1$. So, by (1), $a \leq 1$. If $a = 0$, then by (4), $r \leq 2$, contradicting (2). If $a = 1$, by (4), $r \leq 4$, contradicting (3).

7.5 Case $F3.2$: $r - a, a + b + 1 \leq d + x$ and $d + x < c + d - a$.

Three subcases are considered.

$F3.2.1$: $a + d + x - b, c + x \leq a + b + n - d - x$.

$F3.2.2$: $a + b + n - d - x, a + d + x - b \leq c + x$.

$F3.2.3$: $c + x, a + b + n - d - x < a + d + x - b$.

Subcase $F3.2.1$: $a + d + x - b, c + x \leq a + b + n - d - x$.

Let $(f, g, h) = (f', g', h') = (d + x - b, d + x, a + b + n - d - x)$. From the conditions for this case, subcase, (12) and (13), f, g and h satisfy (14), (15) and (16). Let $Q_1 = Q_0 \cup \{H_1 = (h, b) \to (h, g) \to (a, g) \to (a + f, b)\}$. This tessellation is illustrated in the Appendix. Let $\alpha = g - b$ and $\beta = b + n - d - x$. Consider the linear transformation $H_1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + (-a, -b)$. If $g - b = 1$, then from the conditions of this case and (1), $1 \leq a + 1 \leq d + x - b$, so, $a = 0$. Also, from the conditions for this case, $r \leq a + d + x = a + b + 1 = b + 1$. From (1), $a + b < r$, hence, $b = r - 1$, contradicting (3). Thus, $1 < g - b = \alpha$. From (1), $9 < n$ so $9 < (g - b) + (h - a) = (d + x - b) + (b + n - d - x) = \alpha + \beta$. From the conditions for this subcase, $\alpha \leq \beta$. Now apply Lemma 6.3.

Subcase $F3.2.2$: $a + b + n - d - x, a + d + x - b \leq c + x$.

Let $(f, g, h) = (d + x - b, d + x, c + x)$ and $m_1 = \max\{a + d + x - c, b\}$. From the conditions for this subcase, (10), (12) and (13), f, g and h satisfy (14), (15) and (16). Let $Q_2 = Q_0 \cup \{BT_{g-m_1}^{(c,g)}, FT_x^{(c,d)}, R_1 = (h, b) \to (h, d) \to (c, d) \to (c, m_1) \to (a + f, b), R_2 = (h, d) \to (h, a + b + n - h) \to (a + b + n - g, g) \to (c, g), R_3 = (c, m_1) \to (c + m_1 - g, g) \to (a, g) \to (a + f, b)\}$. Part of the tessellation Q_2 is illustrated in the Appendix. By Theorem 6.1, there exists a Drápal Triangulation of $FT_n^{(a,b)}$ which contains $FT_x^{(c,d)}$ and if $\{R_1, R_2, R_3\} \not\subset \mathcal{Z}$, then there exists a second distinct Drápal Triangulation of $FT_n^{(a,b)}$ containing $FT_x^{(c,d)}$, with $(f', g', h') = (f, g, h)$. Hence, assume that $\{R_1, R_2, R_3\} \subset \mathcal{Z}$.

If $x \neq 1$, let $(f', g', h') = (f, g, h)$. Consider the tessellation $Q_3 = (Q_2 \setminus \{BT_{g-m_1}^{(c,g)}, R_3\}) \cup \{BT_{g'-m_1-1}^{(c,g'-1)}, BT_1^{(c,g')}, R_4 = (c, m_1) \to (c + m_1 - g' + 1, g' - 1) \to (c, g' - 1) \to (c - 1, g') \to (a, g') \to (a + f', b)\}$ of $FT_n^{(a,b)}$. By Theorem 6.1, there exists a second distinct Drápal Triangulation of $FT_n^{(a,b)}$ which contains $FT_x^{(c,d)}$.

Otherwise, $x = 1$. From (10), $b \leq d$. Suppose $d = b$; then, from the conditions of this case, $a = 0$ and $r - a \leq b + 1$. From (1), $a + b < r$, thus, $r = b + 1$, which contradicts (3).

Suppose $d - b = 1$; then from the conditions for this case, $a \leq 1$. From the conditions for this subcase, $c \geq a + b + n - d - 2 = a + n - 3 \geq n - 3$. As $R_3 \in \mathcal{Z}$, $c - (a + d + x - b) \leq 1$, thus, $n - 3 \leq c \leq a + d - b + 2 = a + 3 \leq 4$. Hence, $n \leq 7$ contradicting (1).

Otherwise, $1 < d - b$. Let $(f', g', h') = (f, g, h)$ and $Q_4 = (Q_2 \setminus \{BT_{g-m_1}^{(c,g)}, R_1, R_3\}) \cup \{BT_{d-b}^{(h',d)}, BT_1^{(c,g')}, R_5 = (h', b) \to (h' + b - d, d) \to (c, d) \to (c - 1, g') \to (a, g') \to (a + f', b)\}$. By Theorem 6.1, there exists a second distinct Drápal Triangulation of $FT_n^{(a,b)}$ which contains $FT_x^{(c,d)}$.

Subcase $F3.2.3$**:** $c + x, a + b + n - d - x < a + d + x - b$**.**

Let $(f, g, h) = (f', g', h') = (d + x - b, d + x, a + d + x - b)$. From the conditions for this case, (1), (10), (12) and (13), f, g and h satisfy (14), (15) and (16). Consider the tessellation $Q_5 = Q_0 \cup \{H_2 = (h, b) \to (h, a+b+n-h) \to (a+b+n-g, g) \to (a, g)\}$ of $FT_n^{(a,b)}$. See the Appendix for an illustration of this tessellation. Let $\alpha = b+n-d-x$ and $\beta = d + x - b$. Consider the linear transformation $H_2\lambda + (-a, a + b + n)$, where $\lambda = \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix} \in G$. If $b + n - d - x \leq 1$, then, by (13), $b = 0$, contradicting (1). So, $1 < b+n-d-x$, hence, $1 < \alpha$. From (1), $9 < n$ so $9 < (b+n-d-x)+(d+x-b) = \alpha+\beta$. From the conditions for this subcase, $b + n - d - x < d + x - b$, so, $\alpha \leq \beta$. Now apply Lemma 6.3.

8 Backward Triangles

The aim of this section is to prove Theorem 5.3. Recall that n, r, a, b, c, d, x are any integers satisfying $(1), (2), (3), (4), (17), (18)$ and $x > 0$. Four cases are considered. These are listed in Table 2. Again the constructive lemmas from Section 6 will be frequently used.

Table 2: Cases for placing $BT_x^{(c,d)}$

$B1.1$	$r - a, a + b + 1 \leq d$ and $a + b + n - d \leq a + d - b$.
$B1.2$	$r - a, a + b + 1 \leq d$ and $a + d - b < a + b + n - d$.
$B2.1$	$r - a, d, d + c - x - a \leq a + b + 1$.
$B2.2$	$r - a, d \leq a + b + 1 < d + c - x - a$.

8.1 Case $B1.1$: $r - a, a + b + 1 \leq d$ and $a + b + n - d \leq a + d - b$.

Let $(f, g, h) = (f', g', h') = (d - b, d, a + d - b)$. From the conditions for this case, f satisfies (14). From (17), $d \leq n - 1$, so, g satisfies (15). By (1), $a \leq b$, so, $a + d - b \leq d \leq n-1$ and from the conditions for this case, $a+b+n-d \leq a+d-b$, thus, h satisfies (16). Let $Q_1 = Q_0 \cup \{H_1 = (h, b) \to (h, a + b + n - h) \to (a + b + n - g, g) \to (a, g)\}$ (see the Appendix).

Let $(\alpha, \beta, \gamma, \delta, \chi) = (b + n - d, d - b, c - a, a + b + n + x - c - d, x)$. Consider the linear transformation $H_1\lambda + (-a, a + b + n)$ where $\lambda = \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix} \in G$. Recall, from

(1), that $9 < (b+n-d)+(d-b)$, so, $9 < \alpha+\beta$. Note that, $\alpha-\gamma = \delta-\chi$. If $1 = \beta-\gamma = \beta-\alpha = \delta-\chi$, then $\beta-\gamma = \alpha-\gamma$, so, $\alpha = \beta$ and $\beta-\alpha = 0$, which is a contradiction. Thus, the condition $1 = \beta-\gamma = \beta-\alpha = \delta-\chi$ does not hold. From the conditions for this case, $b+n-d \leq d-b$, thus, $\alpha \leq \beta$. By Lemma 6.4, there exists a Drápal Triangulation of $FT_n^{(a,b)}$ containing $BT_x^{(c,d)}$. Note that $\gamma+\delta-\alpha-\chi = 0$. Thus, if in addition $1 < \alpha(= b+n-d)$ and either $1 < \beta-\gamma(= a+d-b-c)$, or $1 < \alpha-\delta(= c-a-x)$, then there exists a second distinct Drápal Triangulation of $FT_n^{(a,b)}$ containing $BT_x^{(c,d)}$.

Recall, from (1), that $1 \leq b$ and from (17), $d \leq n-1$. Hence, if $b+n-d \leq 1$, then $n-1 = d-b$, so, $d = n-1$ and $b = 0$, a contradiction. Thus, $1 < b+n-d$. Let $a+d-b-c, c-a-x \leq 1$ and recall that $\gamma+\delta-\alpha-\chi = 0$. Now, from the conditions of this case, $b+n-d \leq d-b$ and, from (1), $9 < n$, so, $9 < (b+n-d)+(d-b) \leq 2(d-b)$, hence, $9 < 2(x+(a+d-b-c)+(c-a-x)) \leq 2(x+2)$. So, $3 \leq x$.

Suppose that $n-2 \leq a+d-b \leq r-b+1$. Hence, as $a+d-b-c \leq 1$, it follows that $n-2 \leq a+d-b \leq c+1$. By (17), $c \leq a+b+n-d$, so, $n-2 \leq a+b+n-d+1$. Now, $n-2 \leq r-b+1$, so, from (1), $r = n-2$ and $b = 1$. By (1), $a \leq b$, so, as $n-2 \leq a+b+n-d+1$, it follows that $d-3 \leq a+b \leq 2$, hence, $d \leq 5$. As $a \leq b$ and $n-2 \leq a+d-b$ it follows that $n-2 \leq a+d-b \leq d \leq 5$, hence, $n \leq 7$, contradicting (1).

Otherwise, either $a+d-b < n-2$ or $r-b+1 < a+d-b$. Suppose that $a+d-b < n-2$. Let $(f',g',h') = (d-b, d, a+d-b+2) = (f,g,h+2)$. Consider the tessellation $Q_2 = Q_0' \cup \{H_2 = (h+2,b) \to (h+2, a+b+n-h-2) \to (a+b+n-g, g) \to (a,g) \to (h,b)\}$ of $FT_n^{(a,b)}$. Again, let $(\alpha,\beta,\gamma,\delta,\chi) = (b+n-d, d-b, c-a, a+b+n+x-c-d, x)$. Again, consider the linear transformation $H_2\begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix} + (-a, a+b+n)$. As $\gamma+\delta-\alpha-\chi = 0$ and the assumption $a+d-b-c, c-a-x \leq 1$ holds it follows that $\alpha-\delta, \beta-\gamma, \gamma+\delta-\alpha-\chi \leq 1$. By Lemma 6.6, we are done.

Otherwise, $r-b+1 < a+d-b$. Let $(f',g',h') = (d-b-2, d, a+d-b) = (f-2,g,h)$. Consider the tessellation $Q_3 = Q_0' \cup \{H_3 = (h,b) \to (h, a+b+n-h) \to (a+b+n-g, g) \to (a,g) \to (a, b+f-2) \to (a+f-2, b)\}$ of $FT_n^{(a,b)}$. Once more let $(\alpha,\beta,\gamma,\delta,\chi) = (b+n-d, d-b, c-a, a+b+n+x-c-d, x)$. Consider the linear transformation $H_3\begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix} + (-a, a+b+n)$. Again, as $\gamma+\delta-\alpha-\chi = 0$ and $a+d-b-c, c-a-x \leq 1$, it follows that $\alpha-\delta, \beta-\gamma, \gamma+\delta-\alpha-\chi \leq 1$. By Lemma 6.5, we are done.

8.2 Case $B1.2$: $r-a, a+b+1 \leq d$ and $a+d-b < a+b+n-d$.

From (1), $r-b \leq n-3$. Two subcases are considered.

$B1.2.1$: $1 = a+b+n-c-d = 2b+n-2d = d-b-x$.

$B1.2.2$: $1 \neq a+b+n-c-d$ or $1 \neq 2b+n-2d$ or $1 \neq d-b-x$.

Subcase $B1.2.1$: $1 = a+b+n-c-d = 2b+n-2d = d-b-x$.

Note $(2b+n-2d)+(d-b-x)-(a+b+n-c-d) = 1$, so, $c-a-x = 1$. From (1), $9 < (d-b)+(b+n-d)$, and, from the conditions for this case, $d-b < b+n-d$, so, $10 < 2(b+n-d)$. Hence, $10 < 2(x+(a+b+n-c-d)+(c-a-x))$. Thus, $10 < 2(x+2)$. So, $4 \leq x$. From the conditions for this case, $a+b+1 \leq d$, so,

$a+b+n-d \leq n-1$.

Suppose that $a+b+n-d < n-1$; let $(f,g,h) = (f',g',h') = (d-b,d,c+2)$. From the conditions for this case, f satisfies (14). From (17), g satisfies (15). From the conditions for this subcase, $c = a+d-b = a+b+n-d-1$, so, $a+d-b < a+d-b+1 = c+1 = a+b+n-d < n-1$, thus, h satisfies (16). Consider the tessellation $Q_1 = Q_0 \cup \{FT_2^{(c,b)}, BT_x^{(c,d)} = BT_{g-b-1}^{(h-2,g)}, R_3 = (h,b) \rightarrow (h,g-1) \rightarrow (h-1,g) \rightarrow (c,g) \rightarrow (c,b+2), R_4 = (c,b) \rightarrow (c,b+1) \rightarrow (a+1,g) \rightarrow (a,g)\}$ of $FT_n^{(a,b)}$. As $3 < x$, it follows that $R_3 \notin \mathcal{Z}$. By Theorem 6.1, we are done.

Otherwise, $a+b+n-d = n-1$; then, $d-a-b = 1$. From (1) and the conditions of this subcase, $r-b < n-2 = a+b+n-d-1 = a+d-b = c$. Let $(f,g,h) = (f',g',h') = (d-b-1,d,c+1)$. As $r-b < a+d-b$, f satisfies (14). From (17), g satisfies (15). From the conditions for this subcase, $a+b+n-d-1 = a+d-b = c$, thus, h satisfies (16). Consider the tessellation $Q_2 = Q_0' \cup \{FT_2^{(c-1,b)}, BT_x^{(c,d)} = BT_{g-b-1}^{(h-1,g)}, R_1 = (c-1,b) \rightarrow (c-1,b+2) \rightarrow (a+1,g) \rightarrow (a,g) \rightarrow (a,g-1), R_2 = (h,b) \rightarrow (h,g) \rightarrow (h-1,g) \rightarrow (h-1,b+1)\}$ of $FT_n^{(a,b)}$. As $4 \leq x$, it follows that $R_1 \notin \mathcal{Z}$. By Theorem 6.1, we are done.

Subcase $B1.2.2$**:** $1 \neq a+b+n-c-d$ **or** $1 \neq 2b+n-2d$ **or** $1 \neq d-b-x$**.**

Let $(f,g,h) = (d-b,d,a+b+n-d)$. From the conditions for this case, f satisfies (14). From (17), g satisfies (15). By the conditions of this case, $a+d-b < a+b+n-d$ and $a+b+1 \leq d$, so, $a+d-b < a+b+n-d \leq n-1$, thus, h satisfies (16). Consider the tessellation $Q_3 = Q_0 \cup \{H_1 = (h,b) \rightarrow (h,g) \rightarrow (a,g) \rightarrow (a+f,b)\}$ of $FT_n^{(a,b)}$ (see the Appendix). Let $(\alpha,\beta,\gamma,\delta,\chi) = (d-b,b+n-d,c-a,d-b,x)$. Consider the linear transformation $H_1\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + (-a,-b)$. From (1), $9 < (d-b)+(b+n-d)$, so, $9 < \alpha+\beta$. Note that from the conditions for this subcase, $1 \neq a+b+n-c-d = \beta-\gamma$, or $1 \neq 2b+n-2d = \beta-\alpha$, or $1 \neq d-b-x = \delta-\chi$. From the conditions for this case, $d-b < b+n-d$, so, $\alpha < \beta$. By Lemma 6.4, there exists a Drápal Triangulation of $FT_n^{(a,b)}$ containing $BT_x^{(c,d)}$. Note that $\alpha-\delta = 0$. Thus, if in addition $1 < \alpha(= d-b)$ and either $1 < \beta-\gamma(= a+b+n-c-d)$, or $1 < \gamma+\delta-\alpha-\chi(= c-a-x)$, then there exists a second distinct such triangulation, with $(f',g',h') = (f,g,h)$.

If $d-b \leq 1$, then from the conditions for this case, $a+1 \leq 1$, so $a = 0$. Also, from the conditions for this case, $r-a \leq d$, hence, $r \leq d \leq b+1$. From (1), $b < r$; it follows that $b = r-1$, contradicting (3). Hence, $1 < d-b$. So we may assume that $a+b+n-c-d, c-a-x \leq 1$.

Recall that $\alpha-\delta = 0$. From the conditions for this case, $d-b < b+n-d = x+(c-a-x)+(a+b+n-c-d)$, but, $a+b+n-c-d, c-a-x \leq 1$, so, $d-b < x+2$. From (18), $b \leq d-x$. So, $b \leq d-x \leq b+1$. If $d-x = b+1$, then $d-b = x+1 < x+(c-a-x)+(a+b+n-c-d)$, hence, $c-a-x = a+b+n-c-d = 1$. Thus, $(c-a-x)+(a+b+n-c-d)-(d-b-x) = 1$, so, $2b+n-2d = 1$, contradicting the conditions for this subcase. Hence, $b = d-x$.

Again noting that in this case, $d-b < b+n-d$ it follows that $0 < 2b+n-2d = (a+b+n-c-d)+c-(a+d-b)$. As $a+b+n-c-d \leq 1$, $2b+n-2d \leq 1+c-a-d+b$, so, as $b = d-x$, $2b+n-2d \leq 1+c-a-x$, but, $c-a-x \leq 1$, hence, $2b+n-2d \leq 2$. Thus, $0 < 2b+n-2d \leq 2$. Recall that from the conditions of this case, $a+b+1 \leq d$,

so, $a+b+n-d \leq n-1$. Also from the conditions for this case, $r-b \leq a+d-b$.

Suppose that $a+b+n-d = n-1$ and $r-b = a+d-b$; then, $2b+n-2d = (n-1)-(r-b)$. So, as $2b+n-2d \leq 2$, $n-3 \leq r-b$. But (1), implies that $r-b \leq n-3$, so $r-b = n-3$. Hence, $r = n-2$ and $b = 1$. From (1), it follows that $a+b \leq 2$. Thus, $d-2 \leq d-a-b$ and, as $a+b+n-d = n-1$, $d-2 \leq d-a-b = 1$, or $d \leq 3$. From the conditions for this case, $r \leq a+d$, hence, $r \leq 4$ and, as $n-2 = r$, $n \leq 6$, contradicting (1).

Thus, either $a+b+n-d < n-1$ or $r-b < a+d-b$. Recall that $b = d-x$. If $a+b+n-d < n-1$, let $(f', g', h') = (d-b, d, a+b+n-d+1) = (f, g, h+1)$. As $a+b+n-d < n-1$, h' satisfies (16). Consider the tessellation $Q_4 = Q'_0 \cup \{BT_x^{(c,d)} = BT_f^{(c,g)}, R_1 = (c,b) \to (c+b-g, g) \to (a,g) \to (a+f, b), R_2 = (h+1, b) \to (h+1, g-1) \to (h, g) \to (c, g) \to (c, b)\}$ of $FT_n^{(a,b)}$.

Otherwise $r-b < a+d-b$. Let $(f', g', h') = (d-b-1, d, a+b+n-d) = (f-1, g, h)$. As $r-b < a+d-b$, f' satisfies (14). Let $Q_5 = Q'_0 \cup \{BT_x^{(c,d)} = BT_f^{(c,g)}, R_3 = (c,b) \to (c+b-g, g) \to (a,g) \to (a, g-1) \to (a+f-1, b), R_4 = (h,b) \to (h,g) \to (c,g) \to (c,b)\}$. By Theorem 6.1, in both these instances there exists a second distinct Drápal Triangulation of $FT_n^{(a,b)}$ containing $BT_x^{(c,d)}$.

8.3 Case $B2.1$: $d, c+d-a-x \leq a+b+1$.

Let $(f, g, h) = (c+d-a-b-x, a+b+1, n-1)$. From (18), $r \leq c+d-x$, thus, $r-a-b \leq c+d-a-b-x$, hence, f satisfies (14). From the conditions for this case, $c+d-a-x \leq a+b+1$, so, $b+f \leq g$ and by (1), $a+b < r < n-1$, thus, g satisfies (15). From the conditions for this case and as, by (1), $a \leq b$ it follows that $c+d-b-x \leq c+d-a-x \leq a+b+1 \leq n-1$, hence, h satisfies (16). Let $m_1 = \min\{c+d-a, g\}$ and $m_2 = \min\{c+d-b, h\}$. Let $Q_1 = Q_0 \cup \{BT_{m_1+m_2-c-d}^{(m_2,m_1)}, BT_x^{(c,d)}, R_1 = (h,b) \to (h,g) \to (a,g) \to (a,m_1) \to (m_2,m_1) \to (m_2,b), R_2 = (m_2,b) \to (m_2, c+d-m_2) \to (c,d) \to (c,d-x) \to (a+f,b), R_3 = (c,d) \to (c+d-m_1, m_1) \to (a,m_1) \to (a,b+f) \to (c-x,d)\}$. (See the Appendix illustration.) By Theorem 6.1, we are done.

Let $(f', g', h') = (c+d-a-b-x, a+b+2, n-2) = (f, g+1, h-1)$. From (1), $a+b+1 < n-1$, thus, g' satisfies (15). From the conditions for this case and (1), $c+d-b-x \leq c+d-a-x \leq a+b+1 < n-1$. Hence, h' satisfies (16). Let $m_3 = \min\{c+d-a, g+1\}$ and $m_4 = \min\{c+d-b, h-1\}$. Let $Q_2 = Q'_0 \cup \{BT_{m_3+m_4-c-d}^{(m_4,m_3)}, BT_x^{(c,d)}, R_4 = (h-1,b) \to (h-1,g+1) \to (a,g+1) \to (a,m_3) \to (m_4,m_3) \to (m_4,b), R_5 = (m_4,b) \to (m_4, c+d-m_4) \to (c,d) \to (c,d-x) \to (a+f,b), R_6 = (c,d) \to (c+d-m_3, m_3) \to (a,m_3) \to (a,b+f) \to (c-x,d)\}$. By Theorem 6.1, we are done.

8.4 Case $B2.2$: $d \leq a+b+1 < c+d-a-x$.

There are two subcases to consider.

$B2.2.1$: $1 = n-c-1 = n-2a-2 = d-b-x$.

$B2.2.2$: $1 \neq n-c-1$ or $1 \neq n-2a-2$ or $1 \neq d-b-x$.

Subcase $B2.2.1$: $1 = n-c-1 = n-2a-2 = d-b-x$.

Suppose that $d < a+b+1$. Let $(f,g,h) = (f',g',h') = (a+1, a+b+2, n-2)$. From (1), $a+b+1 < n-1$ and $0 \le a \le b$, so, $2a+1 < n-1$. Thus g and h satisfy (15) and (16). From (4), $r - a \le a+b+1$, so, f satisfies (14). Consider the tessellation $Q_1 = Q_0 \cup \{H_1 = (h,b) \to (h,g) \to (a,g) \to (a,b+f)\}$ of $FT_n^{(a,b)}$. Let $(\alpha,\beta,\gamma,\delta,\chi) = (a+1, a+2, d-b, a+c+3-n, x)$. Consider the linear transformation $H_1\lambda + (-b, a+3-n)$ where $\lambda = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] \in G$. Note that, $\alpha < \beta$. Since $1 = n-2a-2$, $a+c+3-n = c-a$. Thus from (18), $\chi \le \delta$. By (1), $9 < n$, from the conditions for this subcase, $n = 2a+3$, thus, $9 < (a+1)+(a+2)$, so, $9 < \alpha+\beta$. From the assumption that $d < a+b+1$, it follows that $1 < a+b-d+2$, so, $1 < \beta - \gamma$. By Lemma 6.4, there exists a Drápal Triangulation of $FT_n^{(a,b)}$ containing $BT_x^{(c,d)}$. If $a = 0$, then, by the conditions for this subcase, $1 = n-2$, contradicting (1). Hence $1 < a+1 = \alpha$. As $1 < \beta - \gamma$, by Lemma 6.4, we are done.

Otherwise $d = a+b+1$. By (1), $9 < n$ and, by the conditions for this subcase, $n = 2a+3$, so, $9 < 2a+3$, hence, $3 < a$. Thus, by (1), $3 < a \le b$ and $r - b < n-5$. Also, by the conditions for this subcase, $1 = d-b-x$, thus, as it is assumed that $d = a+b+1$, $a = x$. Hence, $3 < x$. Let $(f,g,h) = (f',g',h') = (a, a+b+1, n-1)$. From the conditions for this subcase, $2a = n-3$, so, as $r - b < n-5$, it follows that $r - b - a < a-2$, hence, f satisfies (14). From (1), it follows that $2a \le a+b < r < n-1$, thus g and h satisfy (15) and (16). Consider the tessellation $Q_2 = Q_0 \cup \{FT_2^{(a+f,b)}, BT_x^{(c,d)} = BT_a^{(h-1,g)}, R_1 = (a+f,b) \to (a+f, b+2) \to (h-a-1, g) \to (a,g) \to (a, g-1), R_2 = (h,b) \to (h,g) \to (c,g) \to (c, b+1)\}$ of $FT_n^{(a,b)}$. As $3 < x$, it follows that, $R_1 \notin \mathcal{Z}$. By Theorem 6.1, we are done.

Subcase $B2.2.2$**:** $1 \ne n-c-1$ **or** $1 \ne n-2a-2$ **or** $1 \ne d-b-x$**.**

Let $(f,g,h) = (f',g',h') = (a+1, a+b+1, n-1)$. From (4), $r - a - b \le a+1$; hence f satisfies (14). From (1), $a+b < r \le n-2$, thus, g satisfies (15). From (1), $a \le b$, so, $2a+1 \le a+b+1 \le n-1$, hence, h satisfies (16). Let $Q_3 = Q_0 \cup \{H_2 = (h,b) \to (h,g) \to (a,g) \to (a+f,b)\}$ (see the Appendix). Let $(\alpha,\beta,\gamma,\delta,\chi) = (a+1, n-a-1, c-a, d-b, x)$. Consider the linear transformation $H_2\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] + (-a,-b)$.

From (1), $9 < (a+1)+(n-a-1)$, so, $9 < \alpha+\beta$. From (1), $a+b+1 < n-1$ and $a \le b$, so, $2a+1 < n-1$, thus $\alpha < \beta$. Note that from the conditions for this case, $1 \ne n-c-1 = \beta - \gamma$, or $1 \ne n-2a-2 = \beta - \alpha$, or $1 \ne d-b-x = \delta - \chi$. By Lemma 6.4, there exists a Drápal Triangulation of $FT_n^{(a,b)}$ containing $BT_x^{(c,d)}$. Furthermore, if in addition $1 < \alpha (= a+1)$ and either $1 < \alpha - \delta (= a+b-d+1)$, or $1 < \beta - \gamma (= n-c-1)$, or $1 < \gamma + \delta - \alpha - \chi (= c+d-2a-b-x-1)$, then there exists a second distinct Drápal Triangulation of $FT_n^{(a,b)}$ containing $BT_x^{(c,d)}$ and we are done.

If $a = 0$, then from (4), $r \le b+1$, so, by (1), $r = b+1$, contradicting (3). So, $1 < a+1$ and we may assume that $n-c-1, a+b-d+1, c+d-2a-b-x-1 \le 1$. From above, $a+1 < n-a-1$. Recall, from (1), $9 < (a+1)+(n-a-1)$, thus, $9 < 2(n-a-1)-1 = 2(x+(n-c-1)+(a+b-d+1)+(c+d-2a-b-x-1))-1$. As $n-c-1, a+b-d+1, c+d-2a-b-x-1 \le 1$, it follows that $9 < 2(x+3)-1$. Thus $2 < x$.

From (1), $a+b+1 < n-1$. Suppose that $a+b+1 < n-2$. Let $(f',g',h') = (a+1, a+b+3, n-1) = (f, g+2, h)$. As $a+b+1 < n-2$, g' satisfies (15). Consider the tessellation $Q_4 = Q_0' \cup \{H_3 = (h,b) \to (h,g) \to (h-2, g+2) \to (a, g+2) \to (a,g) \to (a+f, b)\}$ of $FT_n^{(a,b)}$. As above let $(\alpha, \beta, \gamma, \delta, \chi) = (a+1, n-a-1, c-a, d-b, x)$. Again, consider the linear transformation $H_3 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + (-a, -b)$. As $n-c-1, a+b-d+1, c+d-2a-b-x-1 \leq 1$, it follows that $\beta-\gamma, \alpha-\delta, \gamma+\delta-\alpha-\chi \leq 1$. By Lemma 6.5, we are done.

Otherwise, $a+b+1 = n-2$. From (1), $n-2 = r$. If $r-a \geq a+b$, then $n-2-a = r-a \geq a+b = n-3$, so $a \leq 1$. Now, $n-1-2a-1 = (n-c-1) + (c+d-2a-b-x-1) + (b-d+x)$. From the above assumption, that $n-c-1, c+d-2a-b-x-1 \leq 1$, it follows that $n-1-2a-1 \leq 2+(b-d+x)$. From (18), $b-d+x \leq 0$. Hence, $n \leq 2a+4$, thus $n \leq 6$, contradicting (1). Thus $r-a < a+b$.

Let $(f',g',h') = (a-1, a+b+1, n-1) = (f-2, g, h)$. As $r-a < a+b$, f' satisfies (14). Consider the tessellation $Q_5 = Q_0' \cup \{H_4 = (h',b) \to (h',g') \to (a,g') \to (a,g'-2) \to (a+f',b)\}$ of $FT_n^{(a,b)}$. Let $(\alpha, \beta, \gamma, \delta, \chi) = (a+1, n-a-1, a+b+n+x-c-d, d-b, x)$. Consider the linear transformation $H_4\lambda + (a+b+n, -b)$ where $\lambda = \begin{bmatrix} -1 & 0 \\ -1 & 1 \end{bmatrix} \in G$. As before $\alpha \leq \beta$ and $9 < \alpha+\beta$. Also, as $n-c-1, a+b-d+1, c+d-2a-b-x-1 \leq 1$, it follows that $\gamma+\delta-\alpha-\chi, \alpha-\delta, \beta-\gamma \leq 1$. By Lemma 6.6, we are done.

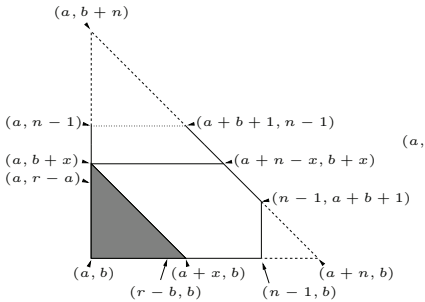
9 Conclusion

Theorem 3.1 tells us that most triples in the critical sets $C_{n,r}$ for $1 \leq r \leq n-2$ are bad, and thus a secret sharing scheme in which each individual receives one triple from $C_{n,r}$ is flawed. One alternative would be to give each individual a set of triples rather than just one triple. However, even in this scenario there are potential flaws - for example it is theoretically possible that a critical set C of a latin square S may have a subset I such that $|I|+1 < |C|$ and C is the only critical set which contains I. We also make the comment that the flaws of the type first indicated in [9] are important to be aware of in any cryptographic application which involves using a block design or latin square as a key, not just secret sharing schemes.

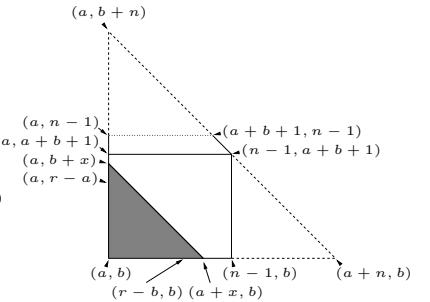
The results in this paper have implications for the study of critical sets in latin squares which we have not fully explored here. For example, with a little extra work, in [12] elements $(u,v,w) \in C_{n,r}$ are classified for which there exists no $(u',v',w') \neq (u,v,w)$ such that $(C_{n,r} \setminus \{(u,v,w)\}) \cup \{(u',v',w')\}$ is also a critical set. There is also preliminary evidence to suggest the results in this paper will be useful in constructing *premature partial latin squares* [1]: those which have no completion to a latin square, but if any symbol is deleted, a completion exists.

Appendix

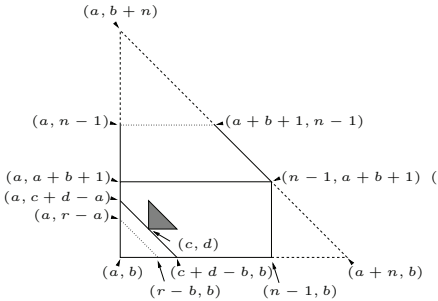
$F1.1$



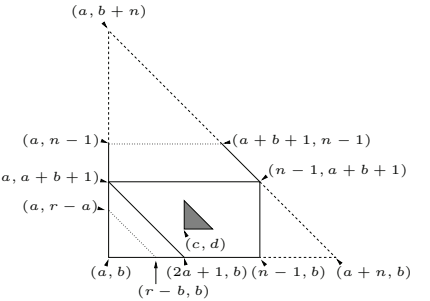
$F1.2$



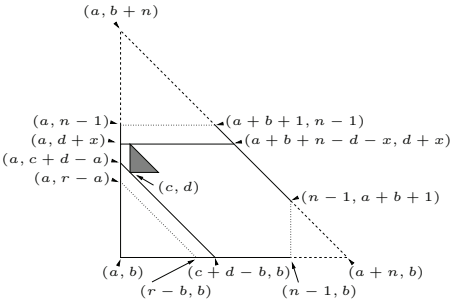
$F2.1$



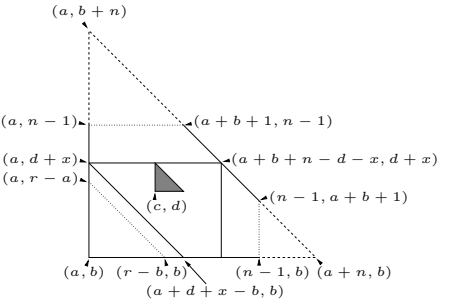
$F2.2$



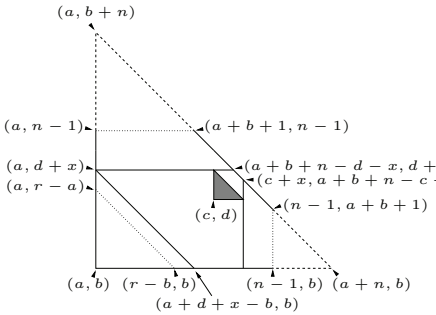
$F3.1$



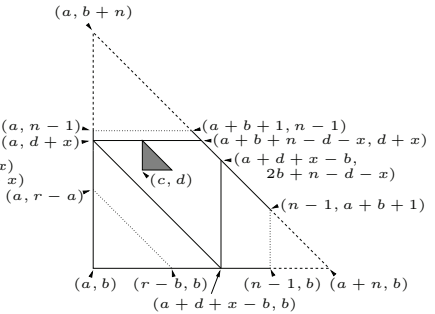
$F3.2.1$



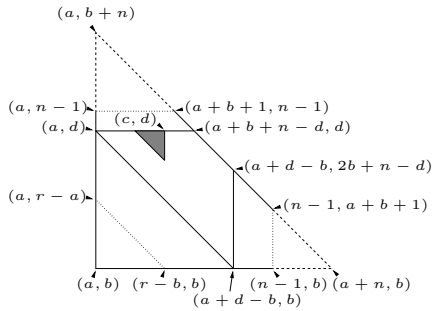
$F3.2.2$



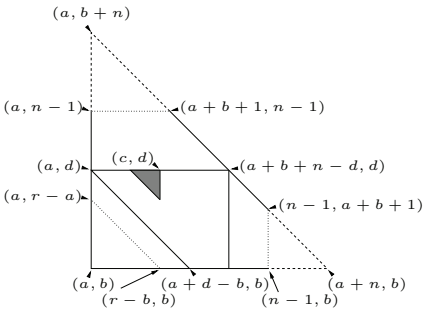
$F3.2.3$



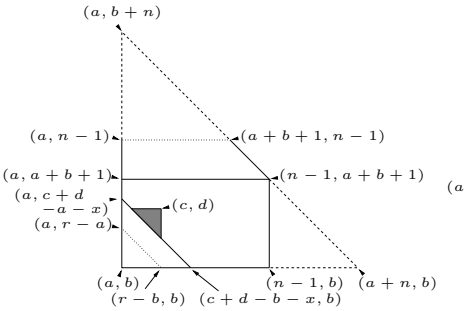
$B1.1$



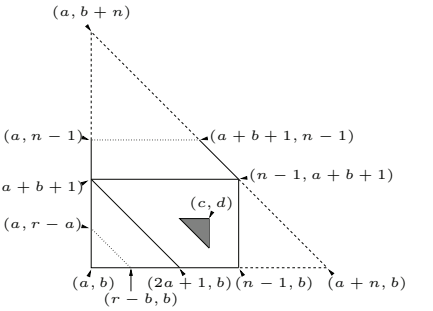
$B1.2.2$



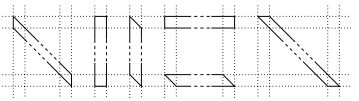
$B2.1$



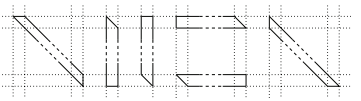
$B2.2.2$



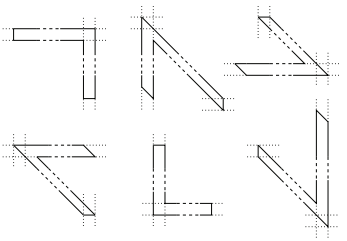
Regions equivalent to Z_1



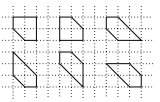
Regions equivalent to Z_2



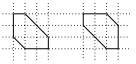
Regions equivalent to Z_3



Regions equivalent to Z_4

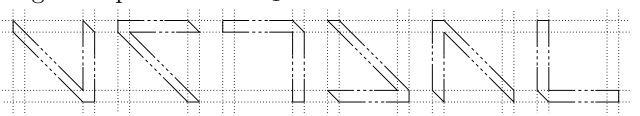


Regions equivalent to Z_5

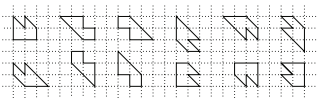


A Region equivalent to Z_6

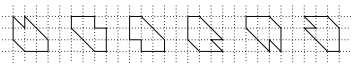
Regions equivalent to X_1



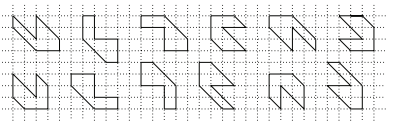
Regions equivalent to X_2



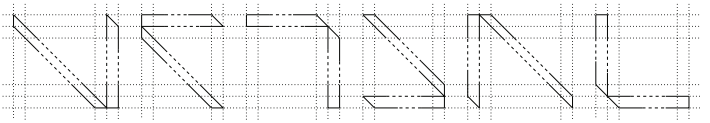
Regions equivalent to X_3



Regions equivalent to X_4



Regions equivalent to X_5



References

[1] Ljiljana Brankovic, Peter Horak, Mirka Miller and Alexander Rosa, Premature partial latin squares, *Ars Combin.* **63** (2002), 175–184.

[2] Nicholas Cavenagh, The theory and application of latin bitrades: a survey, *Math. Slovaca* **58** (2008), 691–718.

[3] Nicholas Cavenagh, Diane Donovan and Abdollah Khodkar, On the spectrum of critical sets in back circulant latin squares, *Ars Combin.* **82** (2007), 287–319.

[4] Nicholas Cavenagh, Diane Donovan, James Lefevre and Thomas McCourt, Distinct equilateral triangle dissections of convex regions, *Comment. Math. Univ. Carolin.* (to appear).

[5] Joan Cooper and Diane Donovan, Critical sets in back circulant latin squares, *Aequationes Math.* **52** (1996), 157–179.

[6] Aleš Drápal, On a planar construction of quasigroups, *Czechoslovak Math. J.* **41** (1991), 538–548.

[7] L. F. Fitina, Jennifer Seberry and Ghulam R. Chaudhry, Back circulant Latin squares and the influence of a set, *Australas. J. Combin.* **20** (1999), 163–180.

[8] Greg Gamble, Barbara M. Maenhaut, Jennifer Seberry and Anne Penfold Street, Further results on strongbox secured secret sharing schemes, *Util. Math.* **66** (2004), 165–193.

[9] Mike J. Grannell, Terry S. Griggs and Anne Penfold Street, A flaw in the use of minimal defining sets for secret sharing schemes, *Des. Codes Crypt.* **40** (2006), 225–236.

[10] A. D. Keedwell, Critical sets for latin squares, graphs and block designs: a survey, *Congr. Numer.* **113** (1996), 231–245.

[11] A. D. Keedwell, Critical sets in latin squares and related matters: an update, *Util. Math.* **65** (2004), 97–131.

[12] T. McCourt, "On Defining Sets in Latin Squares and two Intersection Problems, one for Latin Squares and one for Steiner Triple Systems," PhD Thesis, University of Queensland, Australia, 2010.

[13] Jennifer Seberry and Anne Penfold Street, Strongbox secured secret sharing schemes, *Util. Math.* **57** (2000), 147–163.

(Received 26 July 2011)