Steiner triple systems and spreading sets in projective spaces

Zoltán Lóránt Nagy | Levente Szemerédi

1Faculty of Science, Institute of Mathematics, ELKH–ELTE Geometric and Algebraic Combinatorics Research Group, Eötvös Loránd University, Budapest, Hungary
2Faculty of Science, Institute of Mathematics, Eötvös Loránd University, Budapest, Hungary

Correspondence
Zoltán Lóránt Nagy, ELKH–ELTE Geometric and Algebraic Combinatorics Research Group, Pázmány Péter Sétány 1/C, Budapest H-1117, Hungary. Email: nagyzoli@caesar.elte.hu

Funding information
Nemzeti Kutatási Fejlesztési és Innovációs Hivatal, Grant/Award Numbers: K 120154, 124950, 134953; European Social Fund, Grant/Award Number: EFOP-3.6.3-VEKOP-16-2017-00002; Magyar Tudományos Akadémia János Bolyai Scholarship

Abstract
We address several extremal problems concerning the spreading property of point sets of Steiner triple systems. This property is closely related to the structure of subsystems, as a set is spreading if and only if there is no proper subsystem which contains it. We give sharp upper bounds on the size of a minimal spreading set in a Steiner triple system and show that if all the minimal spreading sets are large then the examined triple system must be a projective space. We also show that the size of a minimal spreading set is not an invariant of a Steiner triple system.

KEYWORDS
projective space, saturating set, Steiner triple system

1 | INTRODUCTION

Let $\mathbb{F}_q$ denote the Galois field with $q = p^h$ elements where $p$ is a prime, $h \geq 1$. $\mathbb{F}_q^d$ is the $d$-dimensional vector space over $\mathbb{F}_q$. Together with its subspaces and their translates, this structure corresponds naturally to the affine geometry $AG(d, q)$. The projective space $PG(d, q)$ of dimension $d$ over $\mathbb{F}_q$ is defined as the quotient $(\mathbb{F}_q^{d+1} \setminus \{0\})/\sim$, where $\mathbf{a} = (a_1, \ldots, a_{d+1}) \sim \mathbf{b} = (b_1, \ldots, b_{d+1})$ if there exists $\lambda \in \mathbb{F}_q \setminus \{0\}$ such that $\mathbf{a} = \lambda \mathbf{b}$; see [18] for an introduction to projective spaces over finite fields.
A block design of parameters $2 - (v, k, \lambda)$ is an underlying set $V$ of cardinality $v$ together with a family of $k$-element subsets whose members are satisfying the property that every pair of points in $V$ are contained in exactly $\lambda$ subsets. In this paper we deal with the case $\lambda = 1$ which means the block design forms a linear space as well. If $k = 3$, we get back the concept of the well-known Steiner triple systems or STSs in brief. Clearly, PG$(d, 2)$ and AG$(d, 3)$ provide infinite families of Steiner triple systems. A partial Steiner triple system on a set $V$ is a triple system in which every pair of points in $V$ are contained in exactly one (i.e., $\lambda = 1$) subset. If $k = 3$, we get back the concept of the well-known Steiner triple systems or STSs in brief. Clearly, PG$(d, 2)$ and AG$(d, 3)$ provide infinite families of Steiner triple systems.

In this paper we deal with the case $\lambda = 1$ which means the block design forms a linear space as well. A triple system induced by a proper subset $V' \subset V$ consists of those triples whose elements do not contain any element of $V \setminus V'$. A nontrivial Steiner subsystem of $S$ is an STS$(n')$ induced by a proper subset $V' \subset V$, with $|V'| = n' > 3$. Speaking about a triple system’s subsystem, we always suppose that it is of order greater than 3. Similarly but not analogously, we call a subset $V' \subset V$ of the underlying set of a triple system $\mathcal{F}$ nontrivial if it has size at least 3 and it is not an element of the triple system.

In contrast with the above-mentioned geometries where Steiner subsystems are abundant, most STSs do not have any nontrivial subsystem. A leading example for a subsystem-free ST can be the construction of Bose and Skolem (see [4]), where the order of the STS is $6k + 3$ for some prime number $2k + 1$. In [2] the first author describes and explains the subsystem-free property of the mentioned type of Steiner triple system STS$(6k + 3)$, examines the so-called spreading property of triple systems and defines a certain neighbourhood concept which describes how far a triple system can be from containing subsystems.

This paper is devoted to analyse the other side of the spectrum using these concepts to explore STSs which are relatively close to geometric settings, such as affine and projective spaces. Besides, it turns out that related extremal problems are in connection with geometric objects of independent interest, such as saturating sets or covering codes.

We recall here the main definitions and results of [2,21], and refer to the papers for further details.

**Definition 1.1 (Closure and spreading property; Blázsik and Nagy [2]).** Consider a graph $G = G(V, E)$ that admits a triangle decomposition. This decomposition corresponds to a linear triple system $\mathcal{F}$. For an arbitrary set $V' \subset V$, $N(V')$ denotes the set of its neighbours:

$$z \in N(V') \iff z \in V \setminus V' \quad \text{and} \quad \exists xy \in E(G[V']) : \{x, y, z\} \in \mathcal{F}.$$  

The closure $\text{cl}_{\mathcal{F}}(V')$ of a subset $V'$ w.r.t. a (linear) triple system $\mathcal{F}$ is the smallest set $W \supseteq V'$ for which $N(W) = 0$ holds. If it does not make any confusion, we omit the index and briefly note it by $\text{cl}(V')$. Note that the closure uniquely exists for each set $V'$.

We call a vertex subset $V'$ spreading if $\text{cl}(V') = V$, and we also call a (linear) triple system $\mathcal{F}$ spreading if $\text{cl}(V') = V$ for every nontrivial subset $V' \subset V$.

Consequently, an STS$(n)$ is subsystem-free if and only if $|N(V')| > 0$ holds for all nontrivial subsets $V'$ of the underlying set $V$ of the system. Note that Doyen used the term nondegenerate plane for STSs which has no nontrivial subsystems [12,13]. As it was pointed out in [2], this property is equivalent to have the spreading property.

A Steiner triple system which is subsystem-free or which contains only few subsystems, contains sets $V'$ of only 3 vertices which spread, that is, for which $\text{cl}(V') = V$. This observation gives rise to the following question.
**Problem 1.2.** What is the minimum number $k$ such that there exists a spreading set of size $k$ in every $STS(n)$ of order $n$? In connection with this problem, we proved the result below which describes the Steiner triple systems attaining the maximum of the minimum size.

**Proposition 1.3.** In any Steiner triple system $STS(n)$ of order $n > 1$, there exists a spreading set $U$ of size $|U| \leq \log_2(n + 1)$ and this bound is best possible for infinitely many values of $n$.

Next we characterise the extremal Steiner triple systems where $|U| \geq \log_2(n + 1)$ holds for each spreading set in our first main result.

**Theorem 1.4.** Suppose that the smallest size of a spreading set in $STS(n)$ is $\log_2(n + 1)$. Then $STS(n)$ is a projective space over $\mathbb{F}_2$.

One would be tempted to conjecture that a much stronger stability result also holds, that is, that in any Steiner triple system $STS(n)$ of order $n > 1$ which is not isomorphic to some projective space $PG(d, 2)$, there exists a spreading set $U$ of size $|U| \leq \log_2(n) + 1$ with equality attained for affine spaces $AG(d, 3)$ for $n = 3^d$.

However, this is far from the truth. We call a spreading set minimal if none of its proper subsets is a spreading set.

**Proposition 1.5.** There exists a family of Steiner triple systems $STS(n)$ with minimal spreading set of size $\log_2(n + 1) - 1$.

We also investigate whether the minimal spreading sets of an arbitrarily chosen STS are of the same size or how much their cardinality may alter. Although the minimal spreading sets of STSs mentioned above, that is, of geometric STSs or of STSs without subsystems have a uniform cardinality, this does not hold for every STS.

**Theorem 1.6.** For every integer $t > 3$ there exists a Steiner triple system which has both a minimal spreading set of size 3 and of size $t$.

Next we make connections to previously studied concepts. Let us define recursively the quasiclosure of a set $S$ after $i$ spreading steps.

$S_0 := S$, and $S_i = S_{i-1} \cup N(S_{i-1})$. Obviously, if $S_i = S_{i+1}$ for some $i$, then $cl(S) = S_i$.

**Definition 1.7.** Suppose we are given a subset $S \subset V$ of the underlying set of a Steiner triple system. If the quasiclosure $S_i$ of $S$ after 1 step coincides with the complete set $V$, then $S$ is called a saturating set.

Saturating sets are already defined in projective geometries and have a large literature, see, for example, [7,11,17]. In the terminology of projective geometries, these are point sets $U$ such that the lines determined by the pairs of points from $U$ cover every point of the projective geometry. Consequently, Definition 1.7 extends this geometric concept in triple systems. These objects have a significant application in coding theory as well. In fact, saturating sets in projective geometry are corresponding to covering codes, more precisely, linear codes with
covering radius 2 see [5, 6, 9, 10, 19, 20]. The above Definition 1.7 basically generalises the concept of saturation to partial linear spaces. We get back to this relation in the last section of the paper.

The paper is organised as follows. In Section 2 we collect some basic results that we intend to apply later on. We discuss the results on the size of minimal spreading sets in Section 3, and prove Proposition 1.3, Theorems 1.4 and 1.5. Section 4 is dedicated to the description of Steiner triple system constructions which contain minimal spreading sets of different sizes. Finally we propose an approach which may be used to improve the lower bound on saturating sets of projective spaces, and pose some open problems in Section 5.

2 | PRELIMINARIES

In this preliminary section we point out the correspondence between the set of closures and the set of subspaces in projective and affine geometries and address some partial results concerning the deviation of the size of intersections from the average intersection size of a point set \( U \) and a hyperplane \( \mathcal{H} \) in projective spaces.

**Lemma 2.1** (Folklore). If \( U \) is a point set of PG\((n, q)\) such that every line intersects \( U \) in 0, 1 or \( q + 1 \) points then \( U \) is a subspace of PG\((n, q)\). If \( U \) is a point set of AG\((n, q)\) such that every line intersects \( U \) in 0, 1 or \( q \) points then \( U \) is a subspace of AG\((n, q)\) provided that \( q > 2 \).

**Proposition 2.2.** The closure \( \text{cl}(U) \) of an arbitrary set \( U \in \text{PG}(n, 2) \) coincides with the smallest subspace in which \( U \) can be embedded.

**Proof:** First observe that \( \text{cl}(U) \) is a subset of the smallest subspace in which \( U \) can be embedded. Any point \( P \) of \( \text{cl}(U) \) is obtained after some number of spreading steps, that is, there is a number \( i \) s.t. \( P \) is contained in the quasiclosure \( U_i \) of a set \( U \) after \( i \) spreading steps, but \( P \notin U_{i-1} \). This also means that there is a line \( \ell \) which contains \( P \) and intersects \( U_{i-1} \) in exactly 2 points. Therefore by induction each quasiclosure \( U_i \) is contained in the smallest subspace in which \( U \) can be embedded, since each point of \( U_i \setminus U_{i-1} \) is a point of a line fully contained in the subspace in view.

On the other hand, the closure intersects each line of the space in 0, 1 or 3 points, hence it must be a subspace according to Lemma 2.1.

Next we examine the distribution of the size of intersections of a fixed set having \( m \) elements and the hyperplanes of the projective space. We present the result for the case when the order is \( q = 2 \), but it is easy to generalise the method.

**Proposition 2.3.** Let \( U \) be a set of \( m \) points in PG\((n, 2)\) and let \( u(\mathcal{H}) \) denote the size of the intersection of \( U \) and a hyperplane \( \mathcal{H} \) of the projective space. Then there exists a hyperplane \( H \) for which

\[
|u(H) - m/2| > \sqrt{\frac{m}{4} - \frac{m^2}{2^{n+3}}}. 
\]
Here note that the expected value of the intersection size is \( \frac{x^n - 1}{2^{n+1} - 1} \) which is almost \( m/2 \), thus the above estimate is closely related to the variance.

**Proof.** Let us consider the sum \( \sum_{\mathcal{H}} |u(\mathcal{H}) - m/2|^2 \) for all hyperplanes \( \mathcal{H} \) of \( \text{PG}(n, 2) \). Taking into consideration that the number of hyperplanes is \( 2^n - 1 \), the number of hyperplanes through a point is \( 2^{n-1} - 1 \) and the number of hyperplanes through a line is \( 2^{n-1} - 1 \), we obtain the following by standard double counting.

\[
\sum_{\mathcal{H}} |u(\mathcal{H}) - m/2|^2 = \sum_{\mathcal{H}} u(\mathcal{H})(u(\mathcal{H}) - 1) + \sum_{\mathcal{H}} u(\mathcal{H}) - m\sum_{\mathcal{H}} u(\mathcal{H}) + \frac{m^2}{4}
\]

\[
= 2\left(\frac{m}{2}\right)(2^{n-1} - 1) - (m - 1)m \cdot (2^n - 1) + \frac{m^2}{4}(2^{n+1} - 1)
\]

\[
= - \frac{m^2}{4} + m \cdot 2^{n-1}.
\]

The claim thus in turn follows. \( \square \)

### 3 | SIZE OF SPREADING SETS

Throughout the rest of the paper, we use capital letters for ordinary vertex sets and calligraphic capital letters for sets together with the (induced) partial Steiner system defined on the set.

Building on the observations we made in the Preliminaries, we give sharp upper bounds on the maximum size of minimal spreading sets of Steiner triple systems \( STS(n) \). First we prove Proposition 1.3 by confirming the bound \( |U| \leq \log_2(n + 1) \).

**Proof of Proposition 1.3.** We can construct a spreading set in the following way. If \( n = 3 \) then the statement clearly holds. Otherwise, we do the following procedure: \( U_i = \{v_0, v_i\} \) for an arbitrary point pair, and \( U_{i+1} = U_i \cup \{v_{i+1}\} \) where \( v_{i+1} \in V \setminus \text{cl}(U_i) \) is arbitrarily chosen if \( V \setminus \text{cl}(U_i) \) is nonempty, otherwise \( U = U_i \). The key observation is the following: \( |\text{cl}(U_{i+1})| \geq 2|\text{cl}(U_i)| + 1 \) which is the easy part of the Theorem of Doyen and Wilson [14], claiming that there exists an STS(\( v \)) which contains an STS(w) as a proper subdesign if and only if \( v \geq 2w + 1 \), and \( v, w \equiv 1 \) or 3 (mod 6). This in turn implies by induction the upper bound of \( |U| \).

As it was pointed out in Theorem 1.4, we have equality if \( n = 2^{d+1} - 1 \) and the triple system is isomorphic to \( \text{PG}(d, 2) \). \( \square \)

In fact, the above proof pointed out that the size of each minimal spreading set is bounded by the logarithmic formula. Indeed, for a minimal spreading set \( \{v_0, v_1, ..., v_i\} \),

\[
\left| \text{cl}\left( \bigcup_{i=0}^{s} [v_i] \right) \right| \geq 2 \left| \text{cl}\left( \bigcup_{i=0}^{s-1} [v_i] \right) \right| + 1
\]
for every $1 < s \leq t$, otherwise we are in contradiction with the property of minimality. This implies

**Proposition 3.1.** If there is a minimal spreading set $U$ in a Steiner triple system $STS(n)$ then $|U| \leq \log_2(n + 1)$.

**Remark 3.2.** This is sharp for $AG(2, 3)$ as all of the minimal spreading sets are of cardinality $3 = \lfloor \log_2(9 + 1) \rfloor$. But if we restrict ourselves to equality in Proposition 1.3, then we one can obtain a characterisation of Steiner triple systems for which the bound is attained. These are exactly the projective spaces.

**Proof of Theorem 1.4.** In this proof we will denote the underlying set of $STS(n)$ by $X$. Furthermore, we will call a subset $U \subseteq X$ a quasi-subspace if $cl(U) = U$ and use the notation $U \leq X$. (Note that such a subset corresponds to a subsystem of the triple system.) Our goal is to confirm that the structure and “dimension” of quasi-subspaces is in one-to-one correspondence with the respective structure of subspaces of a projective space of order $\log_2(n + 1) - 1$. Here we follow the description of projective spaces from [18, Chap. 4].

Each subset $S \subseteq X$ constructed in the proof of Proposition 1.3 is a minimal spreading set. Indeed, otherwise there would be a $W \subseteq S$ minimal spreading set of size $|W| < \log_2(n + 1)$.

Observe that if $Y, Z \leq X$ are two quasi-subspaces, then $Y \cap Z$ is also a quasi-subspace as its closure should be both in $Y$ and $Z$.

Consider a quasi-subspace $Y \leq X$ and two minimal spreading sets $A, B \subseteq Y$ of $Y$. Then, applying Proposition 3.1, we obtain $|A| = |B| = \log_2(|Y| + 1)$ by induction, that is, if the bound from Proposition 3.1 is sharp for an STS, then it is also sharp for each of its quasi-subspaces.

Let us denote by $\dim Y := |A| - 1$ the concept analogue to dimension. To complete the proof we have to prove the dimension theorem.

Let $Y, Z \leq X$ be two quasi-subspaces. Then it is easy to see by taking a suitable minimal spreading set in each quasi-subspace that $Y$ and $Z$ are disjoint if and only if $\dim(cl(Y \cup Z)) = \dim Y + \dim Z + 1$.

If $Y, Z \leq X$ are two arbitrary quasi-subspaces then $\dim(cl(Y \cup Z)) + \dim(Y \cap Z) = \dim Y + \dim Z$: take a minimal spreading set $A$ of $Y \cap Z$ and a set $B$ from $Z$ such that $A \cup B$ is a minimal spreading set in $Z$. Then $Y$ and $cl(B)$ are disjoint so we can apply the statement above.

We continue by studying whether some stability holds for this bound. The next statement asserts that there is no stability in the sense that if we decrease the size by 1, we will have infinitely many Steiner triple systems $STS(n)$ having minimal spreading sets with this respective size.

**Proposition 3.3.** There exists a family of Steiner triple systems $STS(n)$ with minimal spreading set of size $|U| = \log_2(n + 1) - 1$. 
Proof. Our goal is to present a construction gained from a projective space by slightly modifying the system triples (i.e., lines) of $\text{PG}(d, 2)$ with $n = 2^{d+1} - 1$ so that the structure of subspaces does not change significantly.

Consider $\text{PG}(d, 2)$ with a minimal spreading set $\{v_0, ..., v_d\}$. Take a basis in $\mathbb{F}_2^{d+1}$ such that the $i$th basis vector is the representative vector of $v_i$ ($i \in \{0, ..., d\}$).

Doyen [12] showed that there are Steiner triple systems of any admissible order larger than 9 which contain no nontrivial subsystems, that is, every minimal spreading system is of size 3. Let us modify the 3-dimensional subspace generated by $v_0, v_1, v_2, v_3$ in $\text{PG}(d, 2)$ to a Steiner system described above of size 15, the well-known Bose–Skolem construction on 15 points serves as an example [4]. This modified “subspace” is now generated by any three “noncollinear” elements. We can choose the position of the triples such that the triplet on each pair $\{v_1, v_2\}, \{v_2, v_3\}, \{v_1, v_3\}$ in this STS remain intact.

We will show that this modified triple system on $n = 2^{d+1} - 1$ points, which we denote by $\mathcal{X}$, has a minimal spreading set of size $\log_2(n + 1) - 1 = d$. Note that the points of $\text{PG}(d, 2)$ and $\mathcal{X}$ are the same so we will denote them with their homogeneous coordinates.

Consider $U = \{v_1, ..., v_d\}$. This is a spreading system in $\mathcal{X}$ because $\{v_0, ..., v_d\}$ was a spreading system in $\text{PG}(d, 2)$ and $\text{cl}_{\mathcal{X}}(v_1, v_2, v_3) = \text{cl}_{\text{PG}(d, 2)}(v_0, v_1, v_2, v_3)$. To show that $U$ is a minimal spreading set it is enough to prove that any subset of $U$ of size $d - 1$ is not a spreading set.

$U \setminus \{v_d\}$ is not a spreading system because $\text{cl}_{\mathcal{X}}(U \setminus \{v_d\}) = \text{cl}_{\text{PG}(d, 2)}(v_0, ..., v_{d-1})$ which is not the whole system since $\{v_0, ..., v_d\}$ is a minimal spreading set in $\text{PG}(d, 2)$. Similarly for any $k \in \{4, ..., d\}$ the set $U \setminus \{v_k\}$ is not a spreading system of $\mathcal{X}$.

$U \setminus \{v_l\}$ (for $l \in \{1, 2, 3\}$) is also not a spreading system because $\text{cl}_{\text{PG}(d, 2)}(U \setminus \{v_l\})$ is a subspace where all the triplets are remained intact during the modification, thus $\text{cl}_{\text{PG}(d, 2)}(U \setminus \{v_l\})$ coincides with the same point set. $\square$

4 | MINIMAL SPREADING SETS OF DIFFERENT SIZES

In this section we will show that for an arbitrary integer $n > 3$ there exists a Steiner triple system $\mathcal{S}_n$ which has a minimal spreading set of size 3 and one of size $n$.

Let $a_1, a_2, ..., a_n$ be an affine base in $\text{AG}(n - 1, 3)$, which is a minimal spreading set in $\text{AG}(n - 1, 3)$. Let us denote by $\mathcal{H}_i$ the affine hyperplanes $\text{cl}(a_1, ..., a_{i-1}, a_{i+1}, ..., a_n)$ for $1 \leq i \leq n$. Finally, let $\mathcal{X} := \bigcup_{i=1}^n \mathcal{H}_i$ and let $X_i$ be the underlying set of $\mathcal{H}_i$.

**Proposition 4.1.** The system $\mathcal{X}$ is a partial Steiner triple system and has a minimal spreading set of size $n$.

*Proof.* The affine space $\text{AG}(n - 1, 3)$ is a Steiner triple system and $\mathcal{X} \subset \text{AG}(n - 1, 3)$ thus $\mathcal{X}$ is a partial Steiner triple system.

The set $\{a_1, ..., a_n\}$ is a minimal spreading set of $\mathcal{X}$ as $\text{cl}_{\mathcal{X}}(\{a_1, ..., a_n\}) = \mathcal{X}$ and $a_i \notin \mathcal{H}_i = \text{cl}(a_1, ..., a_{i-1}, a_{i+1}, ..., a_n)$. $\square$
Let us choose points $b_1, b_2$ and $b_3$ from $X \setminus (X_2 \cup \ldots \cup X_n)$, $X \setminus (X_1 \cup X_3 \cup \ldots \cup X_n)$ and $X \setminus (X_1 \cup X_2 \cup X_4 \cup \ldots \cup X_n)$, respectively. Note that these sets are nonempty. Add $n + 4$ further points $b_4, \ldots, b_{n+7}$ to $X$. For $k = 1, \ldots, n + 4$ add the triplet $(b_k, b_{k+1}, b_{k+3})$ and for $l = 4, \ldots, n + 3$ add the triplet $(b_l, b_{l+4}, a_{l-3})$ to the existing partial triple system $\mathcal{X}$. Let us denote this extended triple system by $\mathcal{X}^\ast$.

It is easy to see that $\mathcal{X}^\ast$ is a partial Steiner triple system, that is, there does not exist a point pair $x, y \in X'$ such that there is more than one triplet in $\mathcal{X}^\ast$ which contains both $x$ and $y$.

**Proposition 4.2.** The set $\{b_1, b_2, b_3\}$ is a minimal spreading set of $\mathcal{X}^\ast$.

**Proof.** From the construction we get that $a_l, b_k \in \text{cl}_{\mathcal{X}^\ast}(\{b_1, b_2, b_3\})$ for all $l = 1, \ldots, n$ and $k = 1, \ldots, n + 7$. Thus $\text{cl}_{\mathcal{X}^\ast}(\{a_1, ..., a_n\}) \subseteq \text{cl}_{\mathcal{X}^\ast}(\{b_1, b_2, b_3\})$. But $\mathcal{X} \subset \mathcal{X}^\ast$ thus $X = \text{cl}_{\mathcal{X}^\ast}(\{a_1, ..., a_n\}) \subseteq \text{cl}_{\mathcal{X}^\ast}(\{a_1, ..., a_n\})$. So $\text{cl}_{\mathcal{X}^\ast}(\{b_1, b_2, b_3\}) = X'$ which means that the set $\{b_1, b_2, b_3\}$ is a spreading set. It must be also a minimal spreading set because the closure of a set of size 2 in a partial Steiner triple system is either of size 2 or of size 3. □

**Proposition 4.3.** The set $\{a_1, ..., a_n\}$ is a minimal spreading set of $\mathcal{X}^\ast$.

**Proof.** $\{a_1, ..., a_n\}$ is a spreading set because its closure contains the set $\{b_1, b_2, b_3\}$ which is a spreading set. It is also a minimal spreading set. Indeed, $\text{cl}_{\mathcal{X}^\ast}(\{a_1, ..., a_{i-1}, a_{i+1}, ..., a_n\}) = \text{cl}_{\mathcal{X}^\ast}(X_i) = \text{cl}_{\mathcal{X}^\ast}(X_i) = X_i \neq X'$ for all $i$, since none of the triplets added to $\mathcal{X}^\ast$ has more than 1 point from $X_i$. □

We will use a theorem of Bryant and Horsley to show that not only a partial Steiner triple system exists with the required property but also a Steiner triple system.

**Theorem 4.4** (Bryant and Horsley [3]). *Any partial Steiner triple system of order $u$ can be embedded in a Steiner triple system of order $v$ if $v \equiv 1, 3 \pmod{6}$ and $v \geq 2u + 1$.*

The theorem above guarantees that there exists a Steiner triple system which contains $\mathcal{X}^\ast$. Let $\mathcal{S}$ be an STS which contains $\mathcal{X}^\ast$ and is of the least possible size.

**Theorem 4.5.** There exists a Steiner triple system which has both a minimal spreading set of size 3 and $n$.

**Proof.** We will show that $\mathcal{S}$ is appropriate.

Both the sets $\{a_1, ..., a_n\}$ and $\{b_1, b_2, b_3\}$ are spreading sets in $\mathcal{S}$ because their closure is $X'$ in $\mathcal{X}^\ast$ so in $\mathcal{S}$ their closure is the same as of $\mathcal{X}^\ast$ but $\text{cl}_{\mathcal{S}(\mathcal{X}^\ast)} = S$ because $\mathcal{S}$ is an STS contains $\mathcal{X}^\ast$ of minimal size.

The set $\{b_1, b_2, b_3\}$ is a minimal spreading set because its each subset has a closure of size at most 3.

The set $\{a_1, a_2, ..., a_n\}$ is also a minimal spreading set. Let $A \subset \{a_1, a_2, ..., a_n\}$. The closure $\text{cl}_{\mathcal{S}}(A)$ of $A$ is the same as the closure $\text{cl}_{\mathcal{S}^\ast}(A)$ because it is a sub-STS since it was an affine subspace in the original affine space thus during the extension of $\mathcal{X}$ we could not add any triplet which has at least two points in $\text{cl}_{\mathcal{X}}(A)$. □
For any $n > 3$, we presented a family of STS($u$) in which both a minimal spreading set of size 3 and one of size $n$ exist, where $\frac{\log_u n}{n} \to 1$ as $n \to \infty$. In view of Proposition 3.1, $\lim \inf \frac{\log_u n}{n} \geq \log 2$ holds for such triple systems of order $u$. This motivates the following problem.

**Problem 4.6.** Determine $\lim \inf \frac{\log_u (n)}{n}$, where $u(n)$ denotes the minimum order of a Steiner triple system where both a minimal spreading set of size 3 and one of size $n$ exist.

## 5 | CONNECTIONS TO SATURATING SETS AND FINAL REMARKS

We begin this section with some connections to saturating sets of projective spaces.

**Notation 5.1.** The minimum size of a saturating set in $\text{PG}(n, q)$ is denoted by $s(n, q)$.

The trivial lower bound on $s(n, q)$ is due to Lunelli and Sce, and reads as follows [22].

**Proposition 5.2.**

\[
(q - 1) \left( \frac{s(n, q)}{2} \right) + s(n, q) \geq \frac{q^{n+1} - 1}{q - 1},
\]

thus $s(n, q) > \sqrt{2} q^{n+1}$.

For smaller values of $q$, the bound $s(n, q) > \sqrt{2} q^{n+1}$ can be refined. The bound in turn implies the next statement.

**Corollary 5.3.**

\[
s(n, 2) \geq \sqrt{2^{n+2} - 2} - 0.5, \quad s(n, 3) \geq \sqrt{3^{n+1} - 1}.\]

There are no known matching or asymptotically matching upper bounds in general. However in the case $q = 2$, relatively close upper bounds are obtained in the articles of Gabidulin, Davydov and Tombak [16] and of Davydov and Drozhzhina-Labvinskaya [8]. These bounds read as follows.

**Result 5.4** (Davydov and Drozhzhina-Labvinskaya [8] and Gabidulin et al. [16]).

\[
s(n, 2) < 1.1933 \sqrt{2^{n+2}} \quad \text{if } n \text{ is odd};
\]

\[
s(n, 2) < 1.25 \sqrt{2^{n+2}} \quad \text{if } n \text{ is even}.
\]
We refer the interested reader to the recent paper [11] concerning the construction of small saturating sets.

Let us mention an approach to improve the lower bound. The core of the idea relies on an extremal combinatorial problem which is interesting on its own.

**Problem 5.5.** Let $U$ denote a point set in a projective space $PG(n, q)$ of cardinality $m$. Determine

$$\max_{|U|=mH \subseteq PG(n, q)} \min |U \cap H|$$

and

$$\min_{|U|=mH \subseteq PG(n, q)} \max |U \cap H|.$$ 

Concerning Problem 5.5, Proposition 2.3 implies that there exists a hyperplane which intersects the set $U$ in either significantly less point than expected, or in significantly more points. Note that in general we cannot expect to obtain similar bounds for intersections with many points or intersections with few points separately. Indeed, if $U$ is the point set of a hyperplane or a point set of the complement of a hyperplane of $PG(n, 2)$, then the intersection sizes are $|U|$ or $\frac{|U|-1}{2}$ and 0 or $\frac{|U|+1}{2}$, respectively, hence the minimum, respectively, maximum size only differs from expected number by less than 1.

Note that these questions are strongly connected to determine the minimum size of a $t$-fold blocking set in projective space $PG(n, q)$. Once one have a lower bound on a $t$-fold blocking set which exceeds $|U| = m$, we get that there should be a hyperplane on which there are at most $t-1$ points of $U$. On results concerning $t$-fold blocking sets of projective spaces we refer to [1,15].

To present the link to saturating sets in projective spaces, consider the case $q = 2$. (If $q > 2$ one can follow the same lines but the calculation is slightly more involved.) Take a saturating set $S$ of $m$ points and hyperplane on which the number $m_1$ of points $v \in S$ is either small or large compared to $m/2$. Each point not on the hyperplane should be saturated, hence it is either a point of $S$ or on a line determined by two points from $S$: one from the hyperplane and one from its complement. Thus we obtain a necessary condition $m - m_1 + m_1(m - m_1) \geq 2^n - 1$.

Once we have a result stating that for each point set of size $m$ we can find a hyperplane containing $m_1$ points where $|m/2 - m_1|$ is large, we in turn get a lower bound on $m$. One immediately gets from Proposition 2.3 that $|m/2 - m_1|$ cannot be small, but the derived bound does not yield an improvement worth discussing in detail. Finally we mention an open problem in connection with Proposition 3.3: As we have seen before, large minimal spreading sets could also be constructed via the perturbation of the structure of a projective geometry over $\mathbb{F}_2$, however all these triple systems are defined on a point set of size one less than a power of 2.

**Problem 5.6.** Does there exist a Steiner triple system $S$ of order $n$ such that the minimal spreading set in $S$ is larger than $\log_3(n) + 1$ and the order of the system is not of form $n = 2^i - 1$?
ACKNOWLEDGEMENT

We are grateful to the anonymous referees whose suggestions helped us to improve the presentation of the paper. The author is supported by the Hungarian Research Grant (NKFI) Nos. K 120154, 124950, and 134953 and by the János Bolyai Scholarship of the Hungarian Academy of Sciences. The project was supported by the European Union, cofinanced by the European Social Fund (EFOP-3.6.3-VEKOP-16-2017-00002).

ORCID

Zoltán Lóránt Nagy https://orcid.org/0000-0003-2062-5668

REFERENCES

1. J. Barát and L. Storme, Multiple blocking sets in $\text{PG}(n, q)$, $n > 3$, Des. Codes Cryptogr. 33 (2004), no. 1, 5–21.
2. Z. L. Blázskik and Z. L. Nagy, Spreading linear triple systems and expander triple systems, European J. Combin. 39 (2020), 103155.
3. D. Bryant and D. Horsley, A proof of Lindner’s conjecture on embeddings of partial Steiner triple systems, J. Combin. Des. 17 (2009), no. 1, 63–89.
4. C. J. Colbourn and J. H. Dinitz, The CRC handbook of combinatorial designs, Vol. 5005, CRC Press, Boca Raton, FL, 2007.
5. G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, Covering codes, North-Holland Mathematical Library, Vol. 54, Elsevier, Amsterdam, The Netherlands, 1997.
6. A. A. Davydov, Constructions and families of covering codes and saturated sets of points in projective geometry, IEEE Trans. Inform. Theory. 41 (1995), 2071–2080.
7. A. A. Davydov, Constructions and families of nonbinary linear codes with covering radius 2, IEEE Trans. Inform. Theory. 45 (1999), no. 5, 1679–1686.
8. A. A. Davydov and A. Y. Drozhzhina-Labvinskaya, Constructions, families, and tables of binary linear covering codes, IEEE Trans. Inform. Theory. 40 (1994), no. 4, 1270–1279.
9. A. A. Davydov, M. Giulietti, F. Pambianco, and S Marcugini, Linear nonbinary covering codes and saturating sets in projective spaces, Adv. Math. Commun. 5 (2011), no. 1, 119–147.
10. A. A. Davydov, S. Marcugini, and F. Pambianco, New covering codes of radius $R$, codimension $\frac{r}{2}$ and saturating sets in projective spaces, Des. Codes Cryptogr. 87 (2019), no. 12, 2771–2792.
11. L. Denaux, Constructing saturating sets in projective spaces using subgeometries, Des. Codes Cryptogr. (2021). https://doi.org/10.1007/s10623-021-00951-y
12. J. Doyen, Sur la structure de certains systemes triples de Steiner. Math. Z. 111 (1969), no. 4, 289–300.
13. J. Doyen, Systèmes triples de Steiner non engendrés par tous leurs triangles, Math Z. 118 (1970), no. 3, 197–206.
14. J. Doyen and R. M. Wilson, Embeddings of Steiner triple systems, Discrete Math. 5 (1973), 229–239.
15. S. Ferret, L. Storme, P. Sziklai, and Z. Weiner, A $t$ (mod $p$) result on weighted multiple $(n - k)$ -blocking sets in $\text{PG}(n, q)$, Innov. Incidence Geom. 6 (2008), no. 1, 169–188.
16. E. M. Gabidulin, A. A. Davydov, and L. M. Tombak, Linear codes with covering radius 2 and other new covering codes, IEEE Trans. Inform. Theory. 37 (1991), no. 1, 219–224.
17. M. Giulietti, The geometry of covering codes: Small complete caps and saturating sets in Galois spaces, Surveys in Combinatorics, London Math. Soc., Lecture Note Series (S. R. Blackburn, R. Holloway, and M. Wildon, eds.), Cambridge University Press, Cambridge, 2013, pp. 51–90.
18. G. Kiss and T. Szőnyi, Finite geometries, CRC Press, New York, 2019.
19. A. Klein and L. Storme, Applications of finite geometry in coding theory and cryptography, NATO Science for Peace and Security, Ser. D: Information and Communication Security, Information Security, Coding Theory and Related Combinatorics (D. Crnković and V. Tonchev, eds.), Vol. 29, 2011, pp. 38–58.
20. I. Landjev and L. Storme, Galois geometry and coding theory, Current Research Topics in Galois Geometry (J. De. Beule and L. Storme, eds.), NOVA Academic Publisher, New York, 2012, pp. 187–214. Chapter 8.
21. Z. L. Nagy and Z. L. Blázsik, *Spreading linear triple systems and expander triple systems*, Acta Math. Univ. Comenian. 88 (2019), no. 3, 977–984.

22. E. Ughi, *Saturated configurations of points in projective Galois spaces*, European J. Combin. 8 (1987), no. 3, 325–334.

**How to cite this article:** Z. L. Nagy and L. Szemerédi, *Steiner triple systems and spreading sets in projective spaces*, J. Combin. Des. (2022), 30, 549–560.

https://doi.org/10.1002/jcd.21841