ISSN 2590-9770
The Art of Discrete and Applied Mathematics 4 (2021) #P3.05
https://doi.org/10.26493/2590-9770.1345.300
(Also available at http://adam-journal.eu)

Small stopping sets in finite projective planes of order q

Vito Napolitano*

Dipartimento di Matematica e Fisica, Università degli Studi della Campania
Viale Lincoln 5, 81100 Caserta

Received 27 December 2019, accepted 08 June 2020, published online 23 August 2021

Abstract

A *configuration* $\mathcal{C}$ in a (finite) incidence structure is a subset $\mathcal{C}$ of blocks. If every point on a block of $\mathcal{C}$ belongs to at least one other block of $\mathcal{C}$, then $\mathcal{C}$ is called *stopping set* (or equivalently *full configuration*). If $s_{min}(q)$ is the minimal size of a stopping set in a finite projective plane of odd order q, then either $s_{min}(q) \geq q+5$ if $3 \not| q$ or $s_{min}(q) \geq q+3$ if $3|q$. In this note, we prove that $s_{min}(q) \geq q+5$ for any odd $q \neq 3$. If $q = 3$, then $s_{min}(3) = 6$ and a stopping set of minimal size 6 in $\mathrm{PG}(2,3)$ is the dual set of the symmetric difference of two lines. Also, we study stopping sets of size $q+4$ in a finite projective plane of order q.

Keywords: Low density parity check codes, projective planes, KM*–arcs, stopping sets, linear spaces.*

Math. Subj. Class.: 51E20, 51E21, 05B25

1 Introduction

Low density parity check (LDPC) codes based on finite geometries and combinatorial designs are codes with good minimum distance properties. Since the performance of a LDPC code over the binary erasure channel is determined by certain combinatorial objects called *stopping sets*, in [6] the authors define and analyze the notion of stopping set in the underlying design.

Let $\mathbb{G}$ be a finite incidence structure, with set of points $\mathcal{P}$ and with set of blocks $\mathcal{B} \subseteq 2^{\mathcal{P}}$. Let $1 \leq s \leq |\mathcal{B}|$ be an integer, a set $\Sigma = \{B_1, \ldots, B_s\}$ of blocks of $\mathbb{G}$ is a *stopping set* (or, equivalently, a *full configuration* [3]) if every point on a block of Σ belongs to at least one other block of Σ.

*This research was partially supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM).

E-mail address: vito.napolitano@unicampania.it (Vito Napolitano)

This work is licensed under https://creativecommons.org/licenses/by/4.0/

In [6], the authors give a lower bound and an upper bound for the size of a stopping set and for the smallest size s_{min} of a stopping set in a $2-(v,k,\lambda)$–design, respectively. They provide examples of designs having stopping set whose sizes achieve the lower bound. Also, they give some necessary conditions for the existence of a stopping set in finite projective planes, and one of their results reads as follows.

Result 1.1. *Let $s_{min}(q)$ denote the minimal size for a stopping set in a finite projective plane π_q of order q. If q is odd, then*

$$s_{min}(q) \geq \begin{cases} q+3 \text{ if } 3|q \\ q+5 \text{ if } 3\not|q \end{cases}.$$

In projective planes of even order q, we have $s_{min}(q) = q+2$, and the dual of a hyperoval (in planes containing such sets) is an example of stopping set of size $q+2$.

Since the integer s_{min} is related to the size of the smallest stopping set in a low-density parity check (LDPC) code, which determines, to some extent, the performance of iterative decoding methods over the binary erasure channel, it seems natural to study stopping sets of minimal size in designs.

In [3] Colbourn and Fujiwara studied the existence of small stopping sets in Steiner and partial Steiner triple systems. Recently, in [5] stopping sets in finite projective spaces and affine spaces of any finite dimension $m \geq 2$ have been considered.

In this paper, first we describe stopping sets having the minimum number of points in a finite incidence structure with no assumption on the size of its blocks. Then we prove the following two results.

Result 1.2. *If a projective plane of order q has a stopping set Σ of size $q+3$, then $q=3$ and Σ is the stopping set described in Example 1.2.*

Thus, $s_{min}(q) \geq q+5$ in any finite projective plane of odd order q, $q \neq 3$.

Result 1.3. *If a finite projective plane π_q of order q contains a stopping set Σ of size $q+4$, then either Σ consists of six of the seven lines of* $\mathrm{PG}(2,2)$*, or $4|q$ and either $q=4$ and Σ is the stopping set described in Example 1.2 or $q>4$ and every point covered by the lines of Σ belongs to exactly 2 or 4 lines of Σ.*

If $\pi_q = \mathrm{PG}(2,q)$, there are examples of stopping sets of size $q+4$, $q>4$ (cf. e.g. [7, 8, 9]). Moreover, all the $q/4+1$ points through which there pass exactly four lines of Σ are collinear on a line not in Σ (cf. Section 3).

Below, there are three examples of stopping sets of small size[1] in finite projective and affine geometries which give upper bounds for the minimal size of a stopping set in these geometries.

Example 1.1. The set of all the lines of a regulus $\mathcal{R}$ union those of the opposite regulus to $\mathcal{R}$ is a stopping set in $\mathrm{PG}(3,q)$ of size $2q+2$.

Example 1.2. Let π_q be a finite projective plane of order q, consider two distinct points p and p' in π_q. The set Σ consisting of all the lines of π_q through p and p', respectively, and different from the line pp' is a stopping set of size $2q$. Thus the minimum size of a stopping set in a projective plane of order q is at most $2q$.

[1] Examples 1.2 and 1.3 are given by a construction in [6].

Example 1.3. Let α_q be an affine plane of order q, consider a line ℓ, and all the lines of α_q parallel to ℓ. Let L be one of the lines of the parallel class of ℓ, and let p be a point of L. The set of lines Σ consisting of ℓ, all the lines parallel to ℓ and different from L and all the lines containing p and different from L has size $q-1+q$ and is a stopping set, so in affine plane of order q the minimum size of a stopping set is at most $2q-1$. Note that in an affine plane the set of all the lines of at least two parallel classes give rise to a stopping set of size $2q$.

2 Stopping sets with the smallest size

The next result describes the structure of a stopping set with the smallest possible size.

Proposition 2.1. *Let Σ be stopping set in an incidence structure $\mathbb{G}$ and let m be the minimum size of the blocks of Σ. Then $|\Sigma| \geq m+1$. If $|\Sigma| = m+1$ then the blocks of Σ have constant size m, are pairwise intersecting each other, no three of them are confluent at a same point and they cover $\binom{m+1}{2}$ points of $\mathbb{G}$.*

Proof. If B is a block of a stopping set Σ, since on each point of B there is at least one block of Σ different from B, it follows that $|\Sigma| \geq |B|+1$. Thus, if B is a block of minimum size m, we have that $|\Sigma| \geq m+1$.

Let Σ be a stopping set of size $m+1$ and with minimum block size m. Then, on every point on a block of Σ there are exactly two blocks of Σ and any block of Σ has size m. If there are two disjoint blocks, say B_1 and B_2, since B_1 is intersected by at least m blocks of Σ, then $|\Sigma| \geq m+2$, a contradiction. So any two blocks of Σ intersect each other.

Thus the blocks of Σ and the points they cover form a finite linear space on $|\Sigma| = m+1$ points with constant point degree m and constant line size 2, that is the complete graph on $m+1$ vertices and so with $\binom{m+1}{2}$ edges. It follows that the lines of Σ cover $\binom{m+1}{2}$ points of $\mathbb{G}$. □

If one assumes that any two distinct points of $\mathbb{G}$ are incident with at most one block (*semilinearity condition*), then the converse of the last part of the statement of Proposition 2.1 holds, (cf. [6]).

The Desarguesian projective plane $\mathrm{PG}(2,q)$, q even, is an example of a 2-$(v,k,1)$-design with stopping sets of minimum size $k+1$. Also, Example 1.3 for $q=2$ yields a set of size $q+1$ in an affine plane of order q, whose lines are pairwise intersecting.

Let us end this section with a remark on stopping sets whose lines are pairwise intersecting, and so in particular for those contained in projective planes. The lines of such a stopping set are the points of a linear space[2] $\mathbb{S} = (\Sigma, \mathcal{P}_\Sigma)$ with constant point degree $q+1$. Since the list of all possible finite linear spaces with at most 18 points is known (cf. [1] and its bibliography), in the enumeration question (cf. [6]), for stopping sets with at most 18 lines this classification may be of help.

3 Small stopping sets in finite projective planes

By the results in the previous section, for every stopping set Σ in a projective plane we may assume that its size is at least $q+3$. So, let $q+t$, $t \geq 3$ denote the size of a stopping set.

[2]Throughout the paper, $\mathcal{P}_\Sigma$ denotes the set of points covered by the lines of a stopping set Σ.

Since we are interested in minimal stopping sets, in view of Example 1.2, we may assume $t \leq q$. Thus, from now on, Σ denotes a stopping set of size $|\Sigma| = q + t$, $3 \leq t \leq q$, in a projective plane of order q.

Proposition 3.1. *Every line of Σ contains at least three points on exactly two lines of Σ.*

Proof. Let $\mathbb{S} = (\Sigma, \mathcal{P}_\Sigma)$ be the linear space dual of Σ, it has $q + t$ points and all its points have degree $q + 1$.

Let p be a point of $\mathbb{S}$, the lines through p contain at least $q + 2$ points of $\mathbb{S}$. If there are at least $q - 1$ lines of size at least 3 on p then:

$$2q \geq q + t \geq 2(q - 1) + 2 + 1,$$

a contradiction. □

Now, we recall some definitions which will be useful in the following.

If X is a subset of points of a finite projective plane π_q of order q, and $0 \leq i \leq q + 1$ is an integer, a line ℓ of π_q is an i*–line* if it intersects X in exactly i points. The line ℓ is an *external* line if $i = 0$, and a *tangent* line if $i = 1$.

Definition 3.2. A $\mathrm{KM}_{q,t}$–arc in $\mathrm{PG}(2, q)$ (or a $(q + t)$–arc of type $(0, 2, t)$) is a set S of $q + t$ points in $\mathrm{PG}(2, q)$ intersected by every line in either 0, 2 or t points.

If $t = 1$, the set is an arc (degenerate case), if $t = q$, there is only one example: the symmetric difference of two lines. So $\mathrm{KM}_{q,t}$–arcs, are studied for $1 < t < q$.

Examples of these sets first appeared in [8] and [7]. Moreover, in [7] these sets were studied and the following result[3] was proved

- $\mathrm{KM}_{q,t}$*–arcs in* $\mathrm{PG}(2, q)$ *of type* $(0, 2, t)$, $1 < t < q$ *can only exist if* q *is even. Moreover,* t *needs to be a divisor of* q.

Also, the following structural result [4] is known.

- *All* t*–secant lines of a* $\mathrm{KM}_{q,t}$*–arc in* $\mathrm{PG}(2, q)$ *with* $t > 2$ *are concurrent in a point outside the set, which is called the* **nucleus**.

If Σ is a stopping set in a projective plane π_q and $\mathbb{S}$ is the linear space it forms in the dual plane π^*, let b_i denote the number of lines of size i in $\mathbb{S}$. Since $\mathbb{S}$ is embedded in the projective plane π^* of order q, Σ is a subset of points of π^*, and the lines of $\mathbb{S}$ are the set of points of π^* obtained by intersecting the lines of π^* with Σ and having at least two points in Σ. So, b_i also indicates the number of i–lines of Σ in π^*. Finally, since every point of $\mathbb{S}$ has degree $q + 1$, the set Σ of points of π^* has no tangent lines.

[3] Since we use the recent terminology of KM–arc, we state this result in a Desarguesian plane, but it holds for any projective plane.

3.1 The case $|\Sigma| = q + 3$

We are going to prove the following result:

Proposition 3.3. *If π_q contains a stopping set Σ of size $q+3$ then $q = 3$ (and so π_q is Desarguesian) and Σ is the stopping set described in Example 1.2.*

Proof. If $t = 3$, arguing as in Proposition 3.1 one has that for every point of $\mathbb{S} = (\Sigma, \mathcal{L}_\Sigma)$ the numbers of incident 3-lines and 2-lines are 1 and q, respectively. Double counting gives

$$q + 3 = 3b_3 \qquad \text{and} \qquad q(q+3) = 2b_2.$$

So, $3|q$.

Now, assume $q > 3$. Recall that $\mathbb{S}$ is embedded in a projective plane of order q, namely, the dual of π_q. So Σ is a subset of points of π^*, with b_3 3–lines and b_2 2–lines. For any point p of π^* not in Σ, let $x_i(p)$ denote the number of i–lines through p.

Thus, for any point $p \in \pi^* \setminus \Sigma$ we have

$$2x_2(p) + 3x_3(p) = q + 3. \tag{3.1}$$

Let ℓ be a 3–line. At least one of the points of ℓ outside Σ is on exactly one 3–line, otherwise $q/3 \geq q - 2$, and so $q = 3$ contradicting our assumption.

Let p be such a point of ℓ on exactly one 3–line, then

$$q + 3 = 3 + 2x_2(p),$$

and so q is even.

Then, by (3.1), $x_3(p) > 0$ for every point p outside Σ. So,

$$q^2 + q + 1 - q - 3 \leq \sum_{p \notin \mathbb{S}} x_3(p) = b_3(q-2) = (\frac{q}{3} + 1)(q-2),$$

$$3(q-2)(q+2) + 6 = 3(q^2 - 2) \leq (q+3)(q-2),$$

$$3q + 6 + \frac{6}{q-2} \leq q + 3,$$

a contradiction.

Thus, $q = 3$, π_q is Desarguesian and $\mathbb{S}$ is the linear space all whose points lie on two disjoint lines of size 3 and so Σ is the stopping set described in Example 1.2. □

3.2 The case $|\Sigma| = q + 4$

In this case, $\mathbb{S}$ has $q+4$ points and for each point the numbers of incident 3-lines and 2-lines are either 1 and q, respectively, or 2 and $q-1$. Let u denote the number of points contained in a 3–line. Hence $3b_3 = 2u \leq 2(q+4)$.

Proposition 3.4. *q is even, and if $q \neq 2$ then $\mathbb{S}$ contains no 3–lines.*

Proof. For any point p outside Σ let $x_i(p)$ denote the number of i–lines on p. So,

$$2x_2(p) + 3x_3(p) + 4x_4(p) = q + 4. \tag{3.2}$$

If q is odd, then $x_3(p) > 0$. It follows that:

$$q^2 - 3 = q^2 + q + 1 - q - 4 \leq \sum_{p \notin \mathbb{S}} x_3(p) = b_3(q-2) \leq \frac{2(q+4)}{3}(q-2),$$

$$3q^2 - 9 \leq 2q^2 + 4q - 16,$$

$$q^2 - 4q + 7 \leq 0,$$

which cannot occur.

Thus, q is even.

Assume that $\mathbb{S}$ contains a 3–line. Then, in π^* there is a line ℓ intersecting Σ in three points. By Equation (3.2) and since q is even it follows that on any point of ℓ outside Σ there are at least two 3–lines. Thus,

$$3 + 1 + q - 2 \leq b_3 \leq \frac{2}{3}(q+4)$$

and so $q \leq 2$. Thus, either $q = 2$ or $\mathbb{S}$ contains no 3–line. □

If $q = 2$, then $|\Sigma| = 6$ and so Σ is given by six of the seven lines of $\mathrm{PG}(2, 2)$ (i.e. the $STS(7)$–*Line* full configuration in [3]).

If $q \neq 2$, then on each point of $\mathbb{S}$ there is exactly one 4–line and so $4b_4 = q + 4$, that is $4|q$ and a projective stopping set of size $q + 4$ gives rise to a set of points of π^* intersected by any line in 0, 2 or 4 points and each point of a line of Σ belongs to exactly one 4–line. If $q = 4$ then Σ is the set of lines decribed in Example 1.2. Hence, also Result 1.3 is proved.

Let $q > 4$ and assume that π_q is Desarguesian, hence the dual of Σ is a $KM_{q,4}$–arc [9] and examples of $KM_{q,4}$–arc exist (cf. e.g. [7, 8, 9]).

For the next cases, that is for stopping sets of size $q + t$, $t \geq 5$, we recall that the dual of a stopping set is a set of points of a projective plane with no tangent lines. So, in the Desarguesian case, when t is small with respect to q, the results on these sets of points (cf. [2, 10]) show that, if q is odd then it is upper bounded by a quadratic function of t. For q even, if the dual of the stopping set has an i–line with i odd, again q is upper bounded by a quadratic function of t. If q even, and i is even for any i–line, then not much is known about the size of such sets.

ORCID iDs

Vito Napolitano https://orcid.org/0000-0002-2504-6967

References

[1] A. Betten and D. Betten, Note on the proper linear spaces on 18 points, in: *Algebraic combinatorics and applications (Gößweinstein, 1999)*, Springer, Berlin, pp. 40–54, 2001, doi: 10.1007/978-3-642-59448-9_2.

[2] A. Blokhuis, A. Seress and H. A. Wilbrink, On sets of points in $\mathrm{PG}(2, q)$ without tangents, in: *Proceedings of the First International Conference on Blocking Sets (Giessen, 1989)*, 201, 1991 pp. 39–44.

[3] C. J. Colbourn and Y. Fujiwara, Small stopping sets in Steiner triple systems, *Cryptogr. Commun.* **1** (2009), 31–46, doi:10.1007/s12095-008-0002-y.

[4] A. Gács and Z. Weiner, On $(q+t,t)$–arcs of type $(0,2,t)$, *Designs, Codes and Cryptography* **29** (2003), 131–139, doi:10.1023/a:1024152424893.

[5] A. Gruner, *Structural Design and Analysis of Low-Density Parity-Check Codes and Systematic Repeat-Accumulate Codes*, Ph.D. thesis, der Eberhard Karls Universität Tübingen, 01 2015, doi:10.15496/publikation-5257.

[6] N. Kashyap and A. Vardy, Stopping sets in codes from designs, in: *IEEE International Symposium on Information Theory, 2003. Proceedings.*, IEEE, 2003 p. 122, doi:10.1109/isit.2003.1228136.

[7] G. Korchmáros and F. Mazzocca, On $(q+t)$-arcs of type $(0,2,t)$ in a Desarguesian plane of order q, *Math. Proc. Cambridge Philos. Soc.* **108** (1990), 445–459, doi:10.1017/s0305004100069346.

[8] P. M. Lo Re and D. Olanda, $\{0,2,4\}$-semiaffine planes, in: *Combinatorics '88, Vol. 2 (Ravello, 1988)*, Mediterranean, Rende, Res. Lecture Notes Math., pp. 195–210, 1991.

[9] P. Vandendriessche, On KM-arcs in small Desarguesian planes, *Electron. J. Combin.* **24** (2017), Paper No. 1.51, 11, doi:10.37236/6057.

[10] Z. Weiner and T. Szőnyi, On the stability of sets of even type, *Adv. Math.* **267** (2014), 381–394, doi:10.1016/j.aim.2014.09.007.