Proceedings of the 12th European Conference on Combinatorics, Graph Theory and Applications
EUROCOMB'23
Prague, August 28 - September 1, 2023

Expander graphs, strong blocking sets and minimal codes

(Extended abstract)

Noga Alon* Anurag Bishnoi† Shagnik Das‡ Alessandro Neri§

Abstract

We give a new explicit construction of strong blocking sets in finite projective spaces using expander graphs and asymptotically good linear codes. Using the recently found equivalence between strong blocking sets and linear minimal codes, we give the first explicit construction of $\mathbb{F}_q$-linear minimal codes of length n and dimension k such that n is at most a constant times qk. This solves one of the main open problems on minimal codes.

DOI: https://doi.org/10.5817/CZ.MUNI.EUROCOMB23-003

1 Introduction

Blocking sets are sets of points in a finite projective or affine space that meet every hyperplane non-trivially. Studying these objects is a classical topic in finite geometry [15,17]. A stronger notion of blocking sets is that of a set of points that meets every hyperplane in a spanning set. For example, in a projective plane, the set of all points on a single line is a blocking set while the set of all points on three non-concurrent lines is a strong blocking set. These special kind of blocking sets have been studied under the names of generating

*Department of Mathematics, Princeton University, United States of America. E-mail: nalon@math.princeton.edu . Supported by NSF grant DMS-2154082 and BSF grant 2018267.

†Delft Institute of Applied Mathematics, Delft University of Technology, Netherlands. E-mail: A.Bishnoi@tudelft.nl.

‡Department of Mathematics, National Taiwan University, Taiwan. E-mail: shagnik@ntu.edu.tw.

§Department of Mathematics: Analysis, Logic and Discrete Mathematics, Ghent University, Belgium. E-mail: Alessandro.Neri@ugent.be.

sets [23, 25], cutting blocking sets [1, 12, 16] and strong blocking sets [21, 24]. It is the last terminology that we use in this paper.

Strong blocking sets have recently been shown to be in one-to-one correspondence with the notion of *minimal codes* [1, 32]. Minimal codes are linear subspaces of $\mathbb{F}_q^n$ such that the support of any non-zero vector in the subspace does not contain the support of any other non-zero vector of the subspace as a proper subset. These codes have been studied for their application in decoding algorithms [27] and cryptography [18, 29]. Recently, minimal codes have also been linked to perfect hash families [14], which have important applications in computer science. The main problem is to find minimal codes of dimension k and the shortest possible length n as a function of k and the size of the underlying finite field $\mathbb{F}_q$ [18]. It is known that any strong blocking set in the $(k-1)$-dimensional projective space obtained from $\mathbb{F}_q^k$, denoted by $\mathrm{PG}(k-1,q)$, must have size at least $(q+1)(k-1)$ [3], which implies that any minimal code of length n and dimension k over $\mathbb{F}_q$ must satisfy $n \geq (q+1)(k-1)$. Therefore, we would like to construct minimal codes whose length is at most a constant times qk. It follows from [3, Theorem 2.8] that such a minimal code will also be an asymptotically good error-correcting code, which provides another motivation for the problem. While it is easy to show the existence of such short minimal codes using the probabilistic method (for the best results, see [30] for $q = 2$ and [2, 14] for $q > 2$), it is a challenging and central open problem to give explicit constructions [20]. Many constructions of minimal codes have appeared in the last few years [1, 10, 20, 22, 23], and the current best explicit construction has length $n \sim q^4k/4$ [11, 19].

In this paper, we give a new graph-theoretical construction of strong blocking sets, and thus minimal codes. By using asymptotically good linear codes and constant-degree expander graphs, we obtain an explicit construction of strong blocking sets of size cqk, in the projective space $\mathrm{PG}(k-1,q)$, for an absolute constant c.

A graph parameter known as the (vertex) integrity of a graph plays a crucial role in our construction. We prove a new lower bound on the vertex integrity of d-regular graphs in terms of their eigenvalues. Our lower bound implies that any expander graph of bounded degree on n vertices has vertex integrity at least a constant times n. We combine explicit constructions of such graphs with explicit constructions of asymptotically good linear codes, to get explicit minimal codes.

There is a rich history of using expander graphs to construct asymptotically good linear codes [6, 31, 33]. Our work contributes to this line of research by using these graphs in a novel way to construct (asymptotically good) minimal codes. Our construction is the first of its kind in finite geometry as it uses graphs to pick a subset of lines in a finite projective space whose union has certain intersection properties with hyperplanes. This construction has already led to explicit constructions of small affine blocking sets [14], and we expect that it will lead to many new results in finite geometry.

2 Preliminaries

Definition 2.1. The (Hamming) support of a vector $v \in \mathbb{F}_q^n$ is the set $\sigma(v) := \{i : v_i \neq 0\} \subseteq [n]$. The (Hamming) weight of v is $\mathrm{wt}(v) := |\sigma(v)|$.

Definition 2.2. An $[n, k, d]_q$ code $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_q^n$, with $d := \min\{\mathrm{wt}(v) : v \in \mathcal{C} \setminus \{\vec{0}\}\}$ is called the minimum distance of $\mathcal{C}$. The elements of $\mathcal{C}$ are called codewords. Moreover, a generator matrix for $\mathcal{C}$ is a matrix $G \in \mathbb{F}_q^{k\times n}$ such that $\mathcal{C} = \{uG : u \in \mathbb{F}_q^k\}$.

Definition 2.3. Let $\{n_i\}_{i\geq 1}$ be an increasing sequence of positive numbers and suppose that there exist sequences $\{k_i\}_{i\geq 1}$ and $\{d_i\}_{i\geq 1}$ such that for all $i \geq 1$ there exists an $[n_i, k_i, d_i]_q$ code $\mathcal{C}_i$. Then the sequence $\{\mathcal{C}_i\}_{i\geq 1}$ is called an $(R, \delta)_q$-family of codes, where the rate R of this family is defined as $R = \liminf_{i\to\infty} \frac{k_i}{n_i}$, and the relative distance δ is defined as $\delta = \liminf_{i\to\infty} \frac{d_i}{n_i}$.

One of the central problems on error-correcting codes is to understand the trade-off between the rate and the relative distance of codes. A family of codes for which $R > 0$ and $\delta > 0$, is known as an *asymptotically good code*. An easy probablistic argument known as the Gilbert-Varshamov bound shows the existence of such codes for every $\delta \in [0, 1 - 1/q)$ and $R = 1 - H_q(\delta)$, where $H_q(x) := x\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x)$, is the q-ary entropy function, defined on the domain $0 \leq x \leq 1 - 1/q$. The first explicit construction of asymptotically good codes was given by Justesen [28], who showed that for every $0 < R < 1/2$, there is an explicit family of codes with rate R and relative distance $\delta \geq (1 - 2R)H_q^{-1}\left(\frac{1}{2}\right)$. Note that for any prime power q, $H_q^{-1}\left(\frac{1}{2}\right) \geq H_2^{-1}\left(\frac{1}{2}\right) > 0.11$, and thus there are absolute constants $R, \delta > 0$, not depending on q, for which we have an explicit construction of a family of $\mathbb{F}_q$-linear codes with rate R and relative distance δ.

Definition 2.4. Let $\mathcal{C}$ be an $[n, k, d]_q$ code. A nonzero codeword $v \in \mathcal{C}$ is said to be minimal (in $\mathcal{C}$) if $\sigma(v)$ is minimal with respect to the inclusion in the set $\sigma(\mathcal{C}) := \{\sigma(u) : u \in \mathcal{C}\setminus\{\vec{0}\}\}$. The code $\mathcal{C}$ is a minimal linear code if all its nonzero codewords are minimal.

For $k > 1$, the finite projective space of dimension $k - 1$ over the finite field $\mathbb{F}_q$ is defined as $\mathrm{PG}(k-1, q) := \left(\mathbb{F}_q^k \setminus \{\vec{0}\}\right) / \sim$, where $u \sim v$ if $u = \lambda v$ for some non-zero $\lambda \in \mathbb{F}_q$ (in some circles the same object will be denoted by $\mathbb{P}^{k-1}(\mathbb{F}_q)$). The equivalence class that a non-zero vector v belongs to is denoted by $[v]$. The 1-dimensional, 2-dimensional, ..., $(k-1)$-dimensional vector subspaces of $\mathbb{F}_q^k$ correspond to the points, lines, ..., hyperplanes of $\mathrm{PG}(k-1, q)$. We denote the span of a subset S of points in a projective space by $\langle S\rangle$ and the dimension $\dim(\langle S\rangle)$ is one less than the vector space dimension of the corresponding vector subspace. For example, the span of two distinct points P, Q in a projective space, which we will also denote by $\langle P, Q\rangle$, is a 1-dimensional projective subspace corresponding to a 2-dimensional vector subspace, and we refer to it as the line joining P and Q in $\mathrm{PG}(k-1, q)$.

Definition 2.5. A projective $[n, k, d]_q$ system is a (multi)set of n points, $\mathcal{M} \subseteq \mathrm{PG}(k-1, q)$, such that $\langle\mathcal{M}\rangle = \mathrm{PG}(k-1, q)$ and $d = n - \max\{|H \cap \mathcal{M}| : H \text{ is a hyperplane}\}$.

A projective $[n,k,d]_q$ system is simply a dual interpretation of a nondegenerate $[n,k,d]_q$ code, that is, codes with no identically zero entry in all the codewords. If G is the $k \times n$ generator matrix of the code, then the columns of G correspond to a multiset of n points in $\mathrm{PG}(k-1,q)$ with the property that the maximum intersection with a hyperplane of this multiset is equal to $n-d$. This process can clearly be reversed.

Definition 2.6. A set $\mathcal{M} \subseteq \mathrm{PG}(k-1,q)$ is said to be a strong blocking set if $\langle H \cap \mathcal{M} \rangle = H$, for every hyperplane H of $\mathrm{PG}(k-1,q)$.

Theorem 2.7 (see [1], [32])**.** Let $\mathcal{C}$ be a nondegenerate $[n,k,d]_q$ code and let $G = (g_1 \mid \ldots \mid g_n) \in \mathbb{F}_q^{k \times n}$ be any of its generator matrices. The following are equivalent:

1. $\mathcal{C}$ is a minimal code;
2. $\mathcal{M} = \{[g_1], \ldots, [g_n]\}$ is a strong blocking set in $\mathrm{PG}(k-1,q)$.

All known explicit constructions of strong blocking sets are obtained as union of lines in the projective space. This is mainly due to the fact that with such a structure it is easy to control their intersections with subspaces. In particular, the main feature that these constructions possess is the following stronger property than being a strong blocking set.

Definition 2.8. A set $\mathcal{L}$ of lines in a projective space satisfies the avoidance property if there is no codimension-2 space meeting every line $\ell \in \mathcal{L}$.

The relation between these sets of lines and strong blocking sets is the observation of Fancsali and Sziklai [23, Theorem 11] that if a set $\mathcal{L}$ of lines satisfying the avoidance property, then the point-set $\mathcal{B} \coloneqq \cup_{\ell \in \mathcal{L}} \ell$ is a strong blocking set.

For our explicit construction of strong blocking sets we will need explicit constructions of constant-degree expander graphs. Informally, expander graphs have the property that for any vertex subset which is not too large, its boundary is at least a constant times its size. Expansion in graphs can be measured by their spectral properties (see [26]). For a graph G we denote the eigenvalues of its adjacency matrix by $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. If G is d-regular, then $\lambda_1 = d$. Moreover, if it is also connected then $\lambda_2 < d$. A graph G is called an (n,d,λ)-graph if it is a d-regular graph on n vertices with $|\lambda_i| \leq \lambda$ for all $i > 1$. The smaller the value of λ, the larger is the expansion of an (n,d,λ)-graph. Asymptotically, the smallest possible value is close to $2\sqrt{d-1}$, and the graphs achieving that bound are known as Ramanujan graphs. We will use the following result of Alon on explicit constructions of almost Ramanujan graphs.

Theorem 2.9 (see [5, Theorem 1.3])**.** For every positive integer d, and every $\varepsilon > 0$, there is an $n_0(d,\varepsilon)$, such that for all $n \geq n_0(d,\varepsilon)$, with nd even, there is an explicit construction of an (n,d,λ)-graph $G_{n,d}^{\varepsilon}$ with $\lambda \leq 2\sqrt{d-1} + \varepsilon$

3 Integrity of a graph

We will need the following graph parameter, known as the (vertex) *integrity* of a graph, which was introduced in the late 1980s as a measure of the robustness of the connectivity of a network under vertex deletion [7, 9].

Definition 3.1. Let $G = (V, E)$ be a simple connected graph. For any subgraph H, let $\kappa(G)$ denote the largest size of a connected component in H. The integrity of G is the integer

$$\iota(G) := \min_{S \subseteq V} \left(|S| + \kappa(G - S) \right).$$

It is a challenging problem to determine the integrity of graphs precisely, or even asymptotically (see [7] for an old survey and [8, 13] for some recent bounds on different families of graphs). We prove new lower bounds on the vertex integrity of (n, d, λ)-graphs. First, we relate the integrity of a graph to another graph parameter.

Definition 3.2. For a graph G, let $z(G)$ denote the largest integer z so that there are two disjoint sets of vertices in G, each of size z, with no edge connecting them.

Proposition 3.3. For every graph $G = (V, E)$ on n vertices,

$$n - 2z(G) \leq \iota(G) \leq n - z(G).$$

Theorem 3.4. For any (n, d, λ)-graph G, we have $\iota(G) \geq \left(\frac{d-\lambda}{d+\lambda}\right) n$.

Proof. Let $z(G)$ be the maximum integer z such that the vertices of a graph G contains two disjoint parts of size z each with no edge between them. A direct application of the expander mixing lemma implies that

$$z(G) \leq \frac{\lambda n}{d + \lambda}.$$

Applying the lower bound $\iota(G) \geq n - 2z(G)$ from Proposition 3.3, implies $\iota(G) \geq n - 2\frac{\lambda}{d+\lambda} n = \frac{d-\lambda}{d+\lambda} n$. □

4 Constructing Strong Blocking Sets from Graphs

Definition 4.1. Let $\mathcal{M} = \{P_1, \ldots, P_n\}$ be a set of n points in $\mathrm{PG}(k-1, q)$ and let $G = (\mathcal{M}, E)$ be a graph with vertex set equal to $\mathcal{M}$. We define the following sets of lines

$$\mathcal{L}(\mathcal{M}, G) := \{\langle P_i, P_j \rangle : P_i P_j \in E\}$$

and the following set of points

$$\mathcal{B}(\mathcal{M}, G) := \bigcup_{\ell \in \mathcal{L}(\mathcal{M}, G)} \ell,$$

obtained from $\mathcal{M}$ and G.

We make the following crucial observation relating the properties of the graph G and the projective sets defined above.

Proposition 4.2. Let $\mathcal{M} = \{P_1, \ldots, P_n\}$ be a set of points in $\mathrm{PG}(k-1,q)$ and let $G = (\mathcal{M}, E)$ be a graph whose set of vertices is $\mathcal{M}$. If for every $S \subseteq \mathcal{M}$ there exists a connected component C in $G - S$ such that $\langle S \cup C\rangle = \mathrm{PG}(k-1,q)$, then the set $\mathcal{L}(\mathcal{M}, G) = \{\langle P_i, P_j\rangle : P_iP_j \in E\}$ satisfies the avoidance property, that is, no codimension-2 subspace of $\mathrm{PG}(k-1,q)$ meets every line of $\mathcal{L}(\mathcal{M}, G)$.

Lemma 4.3. Let $\mathcal{M}$ be a projective $[n,k,d]_q$ system and let $G = (\mathcal{M}, E)$ be a graph such that $\iota(G) \geq n - d + 1$. Then $\mathcal{L}(\mathcal{M}, G)$ satisfies the avoidance property, and thus $\mathcal{B}(\mathcal{M}, G)$ is a strong blocking set in $\mathrm{PG}(k-1,q)$ of size at most $n + (q-1)|E|$.

Proof. Let S be an arbitrary subset of $\mathcal{M}$. Since $\iota(G) \geq n-d+1$, there exists a connected component C in $G - S$ such that $|S| + |C| \geq n - d + 1$. From the definition of projective systems, it follows that every hyperplane meets $\mathcal{M}$ in at most $n - d$ points. Therefore, $S \cup C \subseteq \mathcal{M}$ is not contained in any hyperplane of $\mathrm{PG}(k-1,q)$, thus implying $\langle S \cup C\rangle = \mathrm{PG}(k-1,q)$. From Proposition 4.2, we conclude that $\mathcal{L}(\mathcal{M}, G)$ satisfies the avoidance property, and thus $\mathcal{B}(\mathcal{M}, G)$ is a strong blocking set. Each line in $\mathcal{L}(\mathcal{M}, G)$ contains exactly $q+1$ points, of which at most $q-1$ are non-vertices. As there are $|E|$-many lines in this set, we get $|\mathcal{B}(\mathcal{M}, G)| \leq n + (q-1)|E|$. □

Finally, we prove the main result of our paper.

Theorem 4.4. There is an absolute constant c such that for every prime power q, there is an explicit construction of strong blocking sets of size at most cqk_i in $\mathrm{PG}(k_i - 1, q)$, for some increasing infinite sequence $\{k_i\}_{i\in\mathbb{N}}$.

Proof. Let R be any constant satisfying $0 < R < 1/2$ and let $\delta = (1-2R)0.11$. Let $\mathcal{M}_i$ be projective $[n_i, k_i, d_i]_q$ systems given by the Justesen construction [28]. Then $\lim_{i\to\infty} k_i/n_i = R$ and $\lim_{i\to\infty} d_i/n_i \geq (1-2R)H_q^{-1}(1/2) > \delta$. Therefore, there exists an i_0 such that for all $i \geq i_0$, we have $d_i/n_i \geq \delta$ and $k_i/n_i \geq R/2$. For the rest of this proof let i_0 be large enough. Let $\{G_i\}_{i\geq i_0}$ be an explicit family of (n_i, d, λ)-graphs, where d and λ are positive constants for which $(d-\lambda)/(d+\lambda) \geq 1 - \delta + 1/n_i$. From Theorem 2.9, it follows that such an explicit construction of graphs is always possible. By Theorem 3.4, we have $\iota(G_i) \geq (1-\delta)n_i + 1 \geq n_i - d_i + 1$. Therefore, by Lemma 4.3, $\mathcal{B}(\mathcal{M}_i, G_i)$ is a strong blocking set in $\mathrm{PG}(k_i - 1, q)$ of size at most

$$n_i + (q-1)\frac{dn_i}{2} < \frac{d}{2}qn_i \leq \frac{d}{R}qk_i.$$

This concludes the proof with $c = \frac{d}{R}$. □

In the expanded version of this short abstract [4], we obtain the optimal value of the constant c by using algebraic-geometric codes, and in particular, we show that we can take $c = 20$ for large enough q. Moreover, for any fixed $q \geq 7$, and $k \to \infty$, we show that our explicit construction is better than [11].

References

[1] G. N. Alfarano, M. Borello, and A. Neri. A geometric characterization of minimal codes and their asymptotic performance. *Advances in Mathematics of Communications*, 16(1):115–133, 2022.

[2] G. N. Alfarano, M. Borello, and A. Neri. Outer strong blocking sets. *preprint arXiv:2301.09590*, 2023.

[3] G. N. Alfarano, M. Borello, A. Neri, and A. Ravagnani. Three combinatorial perspectives on minimal codes. *SIAM Journal on Discrete Mathematics*, 36(1):461–489, 2022.

[4] N. Alon, A. Bishnoi, S. Das, and A. Neri. Strong blocking sets and minimal codes from expander graphs. *arXiv:2305.15297*, 2023.

[5] Noga Alon. Explicit expanders of every degree and size. *Combinatorica*, pages 1–17, 2021.

[6] Noga Alon, Jehoshua Bruck, Joseph Naor, Moni Naor, and Ron M Roth. Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs. *IEEE Transactions on Information Theory*, 38(2):509–516, 1992.

[7] K. S. Bagga, L. W. Beineke, W. D. Goddard, M. J. Lipman, and R. E. Pippert. A survey of integrity. *Discrete Applied Mathematics*, 37:13–28, 1992.

[8] József Balogh, Tamás Mészáros, and Adam Zsolt Wagner. Two results about the hypercube. *Discrete Applied Mathematics*, 247:322–326, 2018.

[9] Curtis A Barefoot, Roger Entringer, and Henda Swart. Vulnerability in graphs-a comparative survey. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 1(38):13–22, 1987.

[10] D. Bartoli and M. Bonini. Minimal linear codes in odd characteristic. *IEEE Transactions on Information Theory*, 65(7):4152–4155, 2019.

[11] Daniele Bartoli and Martino Borello. Small strong blocking sets by concatenation. *SIAM Journal on Discrete Mathematics*, 37(1):65–82, 2023.

[12] Daniele Bartoli, Antonio Cossidente, Giuseppe Marino, and Francesco Pavese. On cutting blocking sets and their codes. *Forum Mathematicum*, 34(2):347–368, 2022.

[13] D Benko, C Ernst, and Dominic Lanphier. Asymptotic bounds on the integrity of graphs and separator theorems for graphs. *SIAM Journal on Discrete Mathematics*, 23(1):265–277, 2009.

[14] A. Bishnoi, J. D'haeseleer, D. Gijswijt, and A. Potukuchi. Blocking sets, minimal codes and trifferent codes. *arXiv:2301.09457*, 2023.

[15] A. Blokhuis, P. Sziklai, and T. Szonyi. Blocking sets in projective spaces. *Current research topics in Galois geometry*, pages 61–84, 2011.

[16] Matteo Bonini and Martino Borello. Minimal linear codes arising from blocking sets. *Journal of Algebraic Combinatorics*, 53:327–341, 2021.

[17] A. E Brouwer and A. Schrijver. The blocking number of an affine space. *Journal of Combinatorial Theory, Series A*, 24(2):251–253, 1978.

[18] H. Chabanne, G. Cohen, and A. Patey. Towards secure two-party computation from the wire-tap channel. In *International Conference on Information Security and Cryptology*, pages 34–46. Springer, 2013.

[19] G. Cohen, S. Mesnager, and H. Randriam. Yet another variation on minimal linear codes. *Advances in Mathematics of Communications*, 10(1):53–61, 2016.

[20] G. D. Cohen, S. Mesnager, and A. Patey. On minimal and quasi-minimal linear codes. In *IMA International Conference on Cryptography and Coding*, pages 85–98. Springer, 2013.

[21] A. A. Davydov, M. Giulietti, S. Marcugini, and F. Pambianco. Linear nonbinary covering codes and saturating sets in projective spaces. *Advances in Mathematics of Communications*, 5(1):119–147, 2011.

[22] C. Ding. Linear codes from some 2-designs. *IEEE Transactions on Information Theory*, 61(6):3265–3275, 2015.

[23] S. Fancsali and P. Sziklai. Lines in higgledy-piggledy arrangement. *Electronic Journal of Combinatorics*, 21, 2014.

[24] T. Héger and Z. L. Nagy. Short minimal codes and covering codes via strong blocking sets in projective spaces. *IEEE Transactions on Information Theory*, 68(2):881–890, 2021.

[25] T. Héger, B. Patkós, and M. Takáts. Search problems in vector spaces. *Designs, Codes and Cryptography*, 76(2):207–216, 2015.

[26] S. Hoory, N. Linial, and A. Wigderson. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 43(4):439–561, 2006.

[27] Tai-Yang Hwang. Decoding linear block codes for minimizing word error rate (corresp.). *IEEE Transactions on Information Theory*, 25(6):733–737, 1979.

[28] Jørn Justesen. Class of constructive asymptotically good algebraic codes. *IEEE Transactions on Information Theory*, 18(5):652–656, 1972.

[29] J. L. Massey. Minimal codewords and secret sharing. In *Proceedings of the 6th joint Swedish-Russian international workshop on information theory*, pages 276–279, 1993.

[30] D Miklós. Linear binary codes with intersection properties. *Discrete Applied Mathematics*, 9(2):187–196, 1984.

[31] Michael Sipser and Daniel A Spielman. Expander codes. *IEEE Transactions on Information Theory*, 42(6):1710–1722, 1996.

[32] C. Tang, Y. Qiu, Q. Liao, and Z. Zhou. Full characterization of minimal linear codes as cutting blocking sets. *IEEE Transactions on Information Theory*, 67(6):3690–3700, 2021.

[33] R Tanner. A recursive approach to low complexity codes. *IEEE Transactions on Information Theory*, 27(5):533–547, 1981.