Constructing neighborly polytopes and oriented matroids

Arnau Padrol[†]

Universitat Politècnica de Catalunya, Barcelona, Spain.

Abstract. A *d*-polytope *P* is neighborly if every subset of $\lfloor \frac{d}{2} \rfloor$ vertices is a face of *P*. In 1982, Shemer introduced a sewing construction that allows to add a vertex to a neighborly polytope in such a way as to obtain a new neighborly polytope. With this, he constructed superexponentially many different neighborly polytopes. The concept of neighborliness extends naturally to oriented matroids. Duals of neighborly oriented matroids also have a nice characterization: balanced oriented matroids. In this paper, we generalize Shemer's sewing construction to oriented matroids, providing a simpler proof. Moreover we provide a new technique that allows to construct balanced oriented matroids. In the dual setting, it constructs a neighborly oriented matroid whose contraction at a particular vertex is a prescribed neighborly oriented matroid. We compare the families of polytopes that can be constructed with both methods, and show that the new construction allows to construct many new polytopes.

Résumé. Un *d*-polytope *P* est *neighborly* si tout sous-ensemble de $\lfloor \frac{d}{2} \rfloor$ sommets forme une face de *P*. En 1982, Shemer a introduit une construction de couture qui permet de rajouter un sommet à un polytope *neighborly* et d'obtenir un nouveau polytope *neighborly*. Cette construction lui permet de construire un nombre super-exponentiel de polytopes *neighborly* distincts. Le concept de *neighborliness* s'étend naturellement aux matroïdes orientés. Les duaux de matroïdes orientés *neighborly* ont de plus une belle caractérisation: ce sont les matroïdes orientés *équilibrés*. Dans cet article, nous généralizons la construction de couture de Shemer aux matroïdes orientés, ce qui en fournit une démonstration plus simple. Par ailleurs, nous proposons une nouvelle technique qui permet de construire matroïdes orientés équilibrés. Dans le cadre dual, on obtient un matroïde *neighborly* dont la contraction à un sommet distingué est un matroïde *neighborly* prescrit. Nous comparons les familles de polytopes qui peuvent être construites avec ces deux méthodes, et montrons que la nouvelle construction permet de construire plusieurs nouveaux polytopes.

Keywords: polytope, oriented matroid, neighborly, Gale dual, sewing construction.

1 Introduction

We say that a polytope is *k*-neighborly if every subset of vertices of size at most k is the set of vertices of one of its faces. It is easy to see that if a *d*-polytope is *k*-neighborly for any $k > \lfloor \frac{d}{2} \rfloor$, then it must be the *d*-dimensional simplex Δ_d . This is why we call a *d*-polytope neighborly if it is $\lfloor \frac{d}{2} \rfloor$ -neighborly.

Neighborly polytopes are one of the most interesting families of polytopes. One of the main reasons for this is the Upper Bound Theorem by McMullen (1970): The number of *i*-dimensional faces of a d-polytope P with n vertices is maximal for neighborly polytopes, for all i.

[†]Supported by AGAUR grant 2009 SGR 1040 and Catalunya's government and the ESF FI grant.

^{1365-8050 © 2012} Discrete Mathematics and Theoretical Computer Science (DMTCS), Nancy, France

The convex hull of any n points on the moment curve in \mathbb{R}^d , $\{(t, t^2, \ldots, t^d) : t \in \mathbb{R}\}$, determines a neighborly polytope: the cyclic polytope c(n, d). The first non-cyclic neighborly polytope was found by Grünbaum (2003). And the first infinite family of neighborly polytopes was found by Barnette (1981), using the *facet splitting* technique.

Strongly related to this technique, there is the *sewing construction* introduced by Shemer (1982). Given a neighborly *d*-polytope with *n* vertices and a suitable flag of faces, one can "sew" a new vertex onto it to get a new neighborly *d*-polytope with n + 1 vertices. With this construction, Shemer proved that the number of (combinatorial types of) neighborly *d*-polytopes with *n* vertices is greater than $\sim 2^{c_d n \log n}$, where $c_d \rightarrow \frac{1}{2}$ when $d \rightarrow \infty$.

This is a quite surprising result when it is combined with the upper bound of $(n/d)^{d^2n(1+o(1))}$ for the number of (combinatorial types of) vertex-labeled *d*-polytopes with *n* vertices, when $\frac{n}{d} \to \infty$. This bound was found by Alon (1986) slightly improving a previous one by Goodman and Pollack (1986).

Recently, Bisztriczky (2000/01) extended Shemer's technique to odd dimension, while Lee and Menzel (2010) provided a generalization of the sewing construction to non-simplicial polytopes. Trelford and Vigh (2011) studied how to compute the face lattice of a sewn polytope.

Oriented matroids are an abstract model for combinatorial geometry. In this sense, oriented matroids can be considered as a generalization of point configurations such as the vertex set of a convex polytope. The concept of neighborly polytope extends naturally to neighborly oriented matroids, see Cordovil and Duchet (2000) or Sturmfels (1988).

The structure of this paper is the following. The first part is devoted to some basic definitions and results on oriented matroids. It is just a reformulation of known results, most of them from Björner et al. (1993), in terms that make subsequent proofs easier to follow. In Section 3 we generalize Shemer's construction to oriented matroids. This allows for a simpler proof for the Sewing Theorem

Moreover, we propose an alternative construction for neighborly matroids in Section 4. Given a neighborly matroid of rank d with n elements, we obtain a new neighborly matroid of rank d + 1 with n + 1 vertices. In a sense that we precise in Section 5, this construction is a generalization of Shemer's.

In a full version of this paper, Padrol (2012), this new construction is used to prove that, $nb_l(n, d)$, the number of vertex-labeled neighborly polytopes with n = r + d + 1 vertices in even dimension d is greater than

$$\operatorname{nb}_{l}(r+d+1,d) \ge \frac{(r+d)^{\left(\frac{r}{2}+\frac{d}{2}\right)^{2}}}{r^{\left(\frac{r}{2}\right)^{2}}d^{\left(\frac{d}{2}\right)^{2}}\mathrm{e}^{3\frac{r}{2}\frac{d}{2}}}.$$

When n > 2d, this bound is greater than $((n-1)/e^{3/2})^{d(n-1)/2}$. This means the bound does not only improve Shemer's bound on the number of neighborly polytopes, but it is even greater than $((n-d)/d)^{nd/4}$, the current best lower bound on the number of all polytopes (valid only if $n \ge 2d$), found by Alon (1986).

2 Balanced and Neighborly Oriented Matroids

2.1 Preliminaries

We assume that the reader has some familiarity with the basics of oriented matroid theory; we refer to Finschi (2001) for a nice introduction and to Björner et al. (1993) for a comprehensive reference. We only present some results that we will directly use in our proofs.

Constructing neighborly polytopes and oriented matroids

As for notation, \mathcal{M} will be an oriented matroid of rank d on a ground set E, with circuits $\mathcal{C}(\mathcal{M})$, cocircuits $\mathcal{C}^*(\mathcal{M})$, vectors $\mathcal{V}(\mathcal{M})$ and covectors $\mathcal{V}^*(\mathcal{M})$. Its dual \mathcal{M}^* has rank r = n - d. \mathcal{M} is uniform if the underlying matroid \mathcal{M} is uniform, that is, every subset of size d is a basis.

We view every vector (resp. covector) X indistinctly as a signed subset of E, $X = (X^+, X^-, X^0)$, or as a function from E to $\{+, -, 0\}^n$. Hence, we will say X(e) = + (or even X(e) > 0) meaning $e \in X^+$. <u>X</u> denotes the support $X^+ \cup X^-$ of X.

We say that two oriented matroids \mathcal{M}_1 and \mathcal{M}_2 on respective ground sets E_1 and E_2 are isomorphic, $\mathcal{M}_1 \simeq \mathcal{M}_2$, when there is a bijection between E_1 and E_2 that sends circuits of \mathcal{M}_1 to circuits of \mathcal{M}_2 (equivalently vectors, cocircuits or covectors).

A matroid \mathcal{M} is *acyclic* if it contains $(+, +, \dots, +)$ as a covector. Its *facets* are the complements of the supports of its positive cocircuits, and its *faces* the complements of its positive covectors. Faces of rank 1 are called *vertices* of \mathcal{M} . In particular, every *d*-polytope is an acyclic matroid of rank (d + 1).

Similarly, a matroid is *totally cyclic* if it contains (+, +, ..., +) as a vector. We use the notation \mathcal{D}_r for the only totally cyclic oriented matroid of rank r with r + 1 elements.

Two elements $p, q \in E$ are *covariant* in \mathcal{M} if they have the same sign in all circuits containing them; equivalently, if they have opposite signs in the cocircuits containing them. They are *contravariant* if they are covariant in the dual. We will say that p and q are (+1)-*inseparable* when they are covariant and that they are (-1)-*inseparable* when they are contravariant.

We will need some constructions to deal with an oriented matroid \mathcal{M} , in particular the *deletion* $\mathcal{M} \setminus e$ and the *contraction* \mathcal{M}/e of an element e. They are defined by their covectors: if e is the last entry of Ethen

$$\mathcal{V}^*(\mathcal{M} \setminus e) = \left\{ V \in \{+, -, 0\}^{n-1} \mid (V, \sigma) \in \mathcal{V}^*(\mathcal{M}) \text{ for some } \sigma \in \{+, -, 0\} \right\},$$
$$\mathcal{V}^*(\mathcal{M}/e) = \left\{ V \in \{+, -, 0\}^{n-1} \mid (V, 0) \in \mathcal{V}^*(\mathcal{M}) \right\}.$$

Deletion and contraction are dual operations — $(\mathcal{M} \setminus e)^* = (\mathcal{M}^*/e)$ — that commute — $(\mathcal{M} \setminus p)/q = (\mathcal{M}/q) \setminus p$ — and naturally extend to subsets $S \subseteq E$ by iteratively deleting (resp. contracting) every element in S. An important observation is that $\mathcal{M} \setminus e$ and \mathcal{M}/e determine \mathcal{M} up to the reorientation of e:

Theorem 2.1 (Richter-Gebert and Ziegler (1994, Theorem 4.1)) Let \mathcal{M}' and \mathcal{M}'' be two oriented matroids with n-1 elements, of respective ranks d and d-1, such that $\mathcal{V}^*(\mathcal{M}') \subseteq \mathcal{V}^*(\mathcal{M}')$. Then there is an oriented matroid \mathcal{M} with n elements with an special element p that fulfills $\mathcal{M} \setminus p = \mathcal{M}'$ and $\mathcal{M}/p = \mathcal{M}''$. The oriented matroid \mathcal{M} has rank d and is unique up to reorientation of p.

2.2 Single Element Extensions

Let \mathcal{M} be an oriented matroid on a set E. A single element extension of \mathcal{M} is an oriented matroid $\tilde{\mathcal{M}}$ on a ground set $\tilde{E} = E \cup p$ for some $p \notin E$, such that every circuit of \mathcal{M} is a circuit in $\tilde{\mathcal{M}}$. Equivalently, $\tilde{\mathcal{M}}$ is a single element extension of \mathcal{M} if \mathcal{M} is a restriction of $\tilde{\mathcal{M}}$ by deleting one element. We will only consider extensions that do not increase the rank, *i.e.*, rank $(\tilde{\mathcal{M}}) = \operatorname{rank}(\mathcal{M})$.

Let \mathcal{M} be a single element extension of \mathcal{M} , on respective ground sets $E = E \cup p$ and E. Then, for every cocircuit $C = (C^+, C^-)$ of \mathcal{M} , there is a unique way to extend C to a cocircuit of $\tilde{\mathcal{M}}$: exactly one of $(C^+ \cup p, C^-)$, $(C^+, C^- \cup p)$ or (C^+, C^-) is a cocircuit of $\tilde{\mathcal{M}}$. Hence, there is a unique function σ that assigns to each cocircuit C of \mathcal{M} the value of $C(p) \in \{0, +, -\}$ in $\tilde{\mathcal{M}}$. We call such a function the signature of the extension. Not every map from $C^*(\mathcal{M})$ to $\{0, +, -\}$ corresponds to the signature of an extension. However, every valid signature uniquely determines the oriented matroid $\mathcal{M} \cup p$. In (Björner et al., 1993, Chapter 7) (originally from Las Vergnas (1978)) one can consult how to decide which signatures are valid, and how to determine all the cocircuits of $\tilde{\mathcal{M}}$ given the signature of the extension.

We will focus on one particular family of single element extensions called lexicographic extensions.

Definition 2.2 Let \mathcal{M} be a rank r oriented matroid on a ground set E. Let $k \leq r$, let (a_1, a_2, \ldots, a_k) be an ordered subset of E and let $(s_1, s_2, \ldots, s_k) \in \{+, -\}^k$ be a sign vector. The lexicographic extension $\mathcal{M}[p]$ of \mathcal{M} by $p = [a_1^{s_1}, a_2^{s_2}, \ldots, a_k^{s_k}]$ is the oriented matroid on the ground set $E \cup \{p\}$ which is the single element extension with cocircuit signature

$$\sigma(C) = \begin{cases} s_i C(a_i) & \text{if } i \text{ is minimal with } C(a_i) \neq 0, \\ 0 & \text{if } C(a_i) = 0 \text{ for } i = 1, \dots, k. \end{cases}$$

We will also use $\mathcal{M}[a_1^{s_1}, \ldots, a_k^{s_k}]$ to denote the lexicographic extension $\mathcal{M}[p]$ of \mathcal{M} by $p = [a_1^{s_1}, \ldots, a_k^{s_k}]$. **Proposition 2.3** If \mathcal{M} is realizable, and $\mathcal{M}[p]$ is a lexicographic extension of \mathcal{M} , then $\mathcal{M}[p]$ is realizable.

Proof: Let the vector configuration $V \subset \mathbb{R}^r$ be a realization of \mathcal{M} . If the signature of the lexicographic extension is $p = [v_1^{s_1}, v_2^{s_2}, \dots, v_k^{s_k}]$, let $v = s_1v_1 + \varepsilon s_2v_2 + \varepsilon^2 s_3v_3 + \dots + \varepsilon^{k-1}s_kv_k$, for $\varepsilon > 0$ small enough. Then $V \cup v$ realizes $\mathcal{M}[p]$. \Box

If $\mathcal{M}[p]$ is a lexicographic extension by $p = [a_1^{s_1}, \dots]$, then p and a_1 are $(-s_1)$ -inseparable.

Lexicographic extensions on uniform matroids behave well with respect to contractions. Proposition 2.4 can be seen as the restriction of (Björner et al., 1993, Proposition 7.1.2) to lexicographic extensions, and will be a very useful tool. We omit the proof, which proceeds via an easy reduction to matroids of rank 2

Proposition 2.4 Let \mathcal{M} be a uniform oriented matroid of rank d on a ground set E, and $\tilde{\mathcal{M}} = \mathcal{M}[p]$ a lexicographic extension by $p = [a_1^{s_1}, a_2^{s_2}, \dots, a_d^{s_d}]$. Then

$$\tilde{\mathcal{M}}/p \simeq (\mathcal{M}/a_1)[a_2^{-s_1s_2}, \dots, a_d^{-s_1s_d}],\tag{1}$$

$$\tilde{\mathcal{M}}/a_i = (\mathcal{M}/a_i)[a_1^{s_1}, \dots, a_{i-1}^{s_{i-1}}, a_{i+1}^{s_{i+1}}, \dots, a_d^{s_d}],$$
(2)

$$\tilde{\mathcal{M}}/e = (\mathcal{M}/e)[a_1^{s_1}, a_2^{s_2}, \dots, a_{d-1}^{s_{d-1}}],\tag{3}$$

where $e \in E$ is any element different from p and any a_i , and the isomorphism φ in eq. (1) is $\varphi(a) = a$ for all $a \in E \setminus \{p, a_1\}$ and $\varphi(a_1) = [a_2^{-s_1s_2}, \ldots, a_d^{-s_1s_d}]$ is the extending element.

Corollary 2.5 If \mathcal{M} is uniform and $p = [a_1^{s_1}, \ldots]$, then

$$\mathcal{M}/a_1 = (\mathcal{M}[p] \setminus p)/a_1 = (\mathcal{M}[p] \setminus a_1)/p.$$

2.3 Balanced and neighborly oriented matroids

The definition of neighborliness can be generalized to oriented matroids, so that neighborly polytopes correspond to realizable neighborly oriented matroids. In particular, every neighborly matroid is acyclic and all of its elements are vertices.

Constructing neighborly polytopes and oriented matroids

Definition 2.6 Let \mathcal{M} be an oriented matroid of rank d on a ground set E. We say that \mathcal{M} is neighborly if every subset $R \subset E$ of size at most $\lfloor \frac{d-1}{2} \rfloor$ is a face of \mathcal{M} . That is, there must exist a covector C of \mathcal{M} with $C^+ = E \setminus R$ and $C^- = \emptyset$.

Another important concept for this paper is that of balanced matroid.

Definition 2.7 An oriented matroid of rank $d \mathcal{M}$ is balanced if every cocircuit C of \mathcal{M} is halving, i.e.,

$$\left\lfloor \frac{n-d+1}{2} \right\rfloor \le |C^+| \le \left\lceil \frac{n-d+1}{2} \right\rceil$$

A key result is that neighborliness and balancedness are dual concepts:

Proposition 2.8 (Sturmfels (1988, Proposition 3.2)) An oriented matroid \mathcal{M} is neighborly if and only if its dual matroid \mathcal{M}^* is balanced.

3 The sewing construction

We next explain the sewing construction, introduced by Shemer (1982), that allows to construct an infinite class of neighborly polytopes. Even if Shemer described the sewing construction in terms of Grünbaum's *beneath-beyond* technique, it is indeed a lexicographic extension, and we will explain it in these terms. Matroids in this section will be denoted by \mathcal{P} , to recall that all the following results translate directly to polytopes.

The sewing construction starts with a neighborly matroid \mathcal{P} of rank d and n elements and gives a neighborly matroid $\tilde{\mathcal{P}}$ of rank d and n + 1 elements, provided that \mathcal{P} has a *universal flag*.

Definition 3.1 Let \mathcal{P} be a uniform acyclic oriented matroid on E of rank d, and let $m = \lfloor \frac{d-1}{2} \rfloor$.

- (i) $F \subseteq E$ is a face of \mathcal{P} if there is a covector C of \mathcal{P} with $C^+ = E \setminus F$ and $C^- = \emptyset$.
- (ii) A face F of \mathcal{P} is a universal face if the contraction \mathcal{P}/F is a neighborly oriented matroid.
- (iii) A flag of \mathcal{P} is a strictly increasing sequence of faces $T_1 \subset T_2 \subset \cdots \subset T_k$.
- (iv) A flag \mathcal{T} of \mathcal{P} is a universal flag if $\mathcal{T} = \{T_i\}_{i=1}^m$ where each T_j is a universal face with 2j vertices.

The first example of neighborly polytopes with universal flags are cyclic polytopes (see (Shemer, 1982, Theorem 3.4)).

Example 3.2 Let c(n, 2m) be a cyclic polytope of even dimension 2m, with vertices s_1, \ldots, s_n labeled in cyclic order. Then $\{s_i, s_{i+1}\}$, $1 \le i < n$ and $\{s_1, s_n\}$ are universal edges of c(n, 2m). Moreover, $c(n, 2m)/\{s_i, s_{i+1}\} \simeq c(n-2, 2m-2)$ with the same cyclic order. In particular this gives a large family of universal flags of c(n, 2m) formed by faces that are the union of a universal edge of c(n, 2m)with a (possibly empty) universal face of c(n-2, 2m-2).

Definition 3.3 (Sewing onto a flag) Let $\mathcal{T} = \{T_j\}_{j=1}^k$ be a flag of an acyclic matroid \mathcal{P} . We extend it with $T_{k+1} = \mathcal{P}$ and define $U_i = T_i \setminus T_{i-1}$. We say that p is sewn onto \mathcal{P} through \mathcal{T} , if $\mathcal{P}[p]$ is the lexicographic extension

$$\mathcal{P}[\mathcal{T}] = \mathcal{P}[T_1^+, U_2^-, U_3^+, \dots, U_{k+1}^{(-1)^{\kappa}}],$$

where these sets represent their elements in any order.

That is, $\mathcal{P}[p]$ is the lexicographic extension of \mathcal{P} by $p = [a_1^{s_1}, a_2^{s_2}, \dots, a_n^{s_n}]$ where a_1, \dots, a_n are the points in T_{k+1} , sorted such that if a_i belongs to a T_s and a_j does not then i < j, and where $s_j = +$ if the smallest i such that $x_j \in T_i$ is odd, and $s_j = -$ otherwise.

We use the notation $\mathcal{P}[\mathcal{T}]$ to designate the extension $\mathcal{P}[p]$ when p is sewn onto \mathcal{P} through \mathcal{T} .

Lemma 3.4 Let \mathcal{P} be a uniform neighborly matroid of rank d with a universal flag $\mathcal{T} = \{T_j\}_{j=1}^m$, where $m = \lfloor \frac{d-1}{2} \rfloor$ and $T_j = \{x_i, y_i\}_{i=1}^j$. Let p be sewn onto \mathcal{P} through \mathcal{T} . Then

$$\mathcal{P}[\mathcal{T}]/\{T_{i-1}, x_i, p\} \simeq \mathcal{P}[\mathcal{T}]/\{T_{i-1}, y_i, p\} \simeq (\mathcal{P}/T_i)[\mathcal{T}/T_i].$$

The first isomorphism sends y_i to x_i , the second sends x_i to the sewn vertex and the remaining are the natural mappings.

Proof: The proof relies on using Proposition 2.4 twice on the lexicographic extension $\mathcal{P}[\mathcal{T}]$, and follows inductively from $\mathcal{P}[\mathcal{T}]/\{p, x_1\} \simeq \mathcal{P}[\mathcal{T}]/\{p, y_1\} \simeq \mathcal{P}/T_1[\mathcal{T}/T_1]$. \Box

The following technical lemma about inseparable elements will be needed.

Lemma 3.5 Let \mathcal{M} be a uniform oriented matroid with two α -inseparable elements x and y. Then for every circuit $X \in \mathcal{C}(\mathcal{M})$ with X(x) = 0 and $X(y) \neq 0$, there is a circuit $X' \in \mathcal{C}(\mathcal{M})$ with $X'(x) = -\alpha X(y)$, X'(y) = 0 and X'(e) = X(e) for all $e \notin \{x, y\}$.

With these tools, we can prove our version of the sewing theorem (Shemer, 1982, Theorem 4.6), extended to neighborly matroids of any rank.

Theorem 3.6 (The Sewing Theorem) Let \mathcal{P} be a uniform neighborly oriented matroid of rank d with a universal flag $\mathcal{T} = \{T_j\}_{j=1}^m$, where $T_j = \{x_i, y_i\}_{i=1}^j$ and $m = \lfloor \frac{d-1}{2} \rfloor$. Let $\tilde{\mathcal{P}} = \mathcal{P}[\mathcal{T}]$, with p sewn onto \mathcal{P} through \mathcal{T} . Then,

- 1. $\tilde{\mathcal{P}}$ is a uniform neighborly matroid of rank d.
- 2. Let $\tilde{T}_i = [T_{i-1}, z_i, p]$, where $z_i \in \{x_i, y_i\}$ and $1 \le j \le m$. Then \tilde{T}_i is a universal face of $\tilde{\mathcal{P}}$.

Proof: The extension $\tilde{\mathcal{P}} = \mathcal{P} \cup p$ is the lexicographic extension $\tilde{\mathcal{P}} = \mathcal{P} \left[x_1^+, y_1^+, x_2^-, y_2^-, \ldots \right]$. We check that $\tilde{\mathcal{P}}$ is neighborly by checking that $\tilde{\mathcal{P}}^*$ is balanced, *i.e.*, we check that every circuit X of $\tilde{\mathcal{P}}$ is halving:

- 1. If X(p) = 0, then X is halving, since it is a circuit of \mathcal{P} , and \mathcal{P} is neighborly.
- 2. If $X(p) \neq 0$ and $X(x_1) = 0$, we use that p and x_1 are contravariant. By Lemma 3.5, if $X' \in C(\tilde{\mathcal{P}})$ is the circuit with $X'(x_1) = X(p)$ and support $\underline{X}' = \underline{X} \setminus p \cup x_1$, then $|X^+| = |X'^+|$ and $|X^-| = |X'^-|$. Since X'(p) = 0, X' is halving by the previous point. Hence so is X.
- 3. If X(p) ≠ 0 and X(x₁) ≠ 0, since p and x₁ are contravariant, X(p) = -X(x₁). Observe that the rest of the values of X correspond to a circuit of P̃/{p, x₁}. If P̃/{p, x₁} is balanced, we are done. By Lemma 3.4, P̃/{p, x₁} ≃ P/T₁[T'/T₁]. Since {x₁, y₁} was a universal edge, P/T₁ is a neighborly matroid and T'/T₁ is a flag that contains the universal flag T/T₁. Then the result follows by induction on d. Observe for the base case that all acyclic universal matroids of rank 1 or 2 are neighborly.

Finally, observe that the second claim of the theorem is also a direct consequence of Lemma 3.4. \Box

Combining Example 3.2 and Theorem 3.6, we can obtain a large family of neighborly polytopes: We start with an even-dimensional cyclic polytope and one of its universal flags, sew a new vertex onto it and obtain a new neighborly polytope (point 1 of Theorem 3.6) with new universal flags (from point 2 of Theorem 3.6). Now we can keep sewing again. This method generates a family of neighborly polytopes S, that we call *totally sewn* polytopes⁽ⁱ⁾.

Moreover, since every subpolytope of a neighborly polytope is a neighborly polytope, any polytope obtained from a polytope in S and then omitting some vertices is also a neighborly polytope. The polytopes that can be obtained this way via sewing and omitting form a family that we denote O.

4 The Gale sewing construction

We present here a different construction, also based on lexicographic extensions, that allows us to construct neighborly matroids. This construction works in the dual, that is, it extends balanced matroids to new balanced matroids.

Theorem 4.1 Let \mathcal{M} be a balanced oriented matroid of rank r, let $\mathcal{M}[p]$ be the lexicographic extension of \mathcal{M} by $p = [a_1^{s_1}, a_2^{s_2}, \dots, a_r^{s_r}]$, and let $\mathcal{M}[p][q]$ be the lexicographic extension of $\mathcal{M}[p]$ by $q = [p^-, a_1^-, \dots, a_{r-1}^-]$. Then $\tilde{\mathcal{M}} = \mathcal{M}[p][q]$ is balanced.

Proof: We prove that $\tilde{\mathcal{M}}$ is balanced by checking that all its cocircuits \tilde{C} are halving.

If $\tilde{C}(p) \neq 0$ and $\tilde{C}(q) \neq 0$ then, by the definition of lexicographic extension, there is a halving cocircuit C of \mathcal{M} such that $\tilde{C}|_{\mathcal{M}} = C$ and $\tilde{C}(p) = -\tilde{C}(q)$. Hence $|\tilde{C}^+| = |C^+| + 1$ and $|\tilde{C}^-| = |C^-| + 1$.

The cocircuits \hat{C} with $\hat{C}(p) = 0$ correspond to cocircuits of $\hat{\mathcal{M}}/p$, and those with $\hat{C}(q) = 0$ correspond to cocircuits of $\hat{\mathcal{M}}/q$. Proposition 2.4 tells us that

$$\mathcal{M}/p \simeq \mathcal{M}/q \simeq \mathcal{M}/a_1[a_2^{-s_1s_2}, \dots, a_r^{-s_1s_2}][p^-, a_2^-, \dots, a_{r-1}^-],$$

and the result follows by induction on r (it is trivial for r = 1).

This provides the following construction to construct balanced matroids (and hence, by duality, to construct neighborly matroids). Let $\mathcal{M}_0 = \mathcal{D}_r$ be the oriented matroid associated to the totally cyclic vector configuration of rank r of minimal cardinality, which is balanced. And let

$$x_k = [e_{k1}^{s_{k1}}, \dots, e_{kr}^{s_{kr}}], \qquad y_k = [x_k^-, e_{k1}^-, \dots, e_{k(r-1)}^-], \qquad \mathcal{M}_k = \mathcal{M}_{k-1}[x_k][y_k],$$

where each e_{ij} is a different element of \mathcal{M}_{i-1} . Then \mathcal{M}_k is balanced, and \mathcal{M}_k^* neighborly. Since \mathcal{M}_0 is realizable, \mathcal{M}_k^* is too, and hence \mathcal{M}_k^* represents a neighborly polytope.

We call the double extension of Theorem 4.1 *Gale sewing*, and we denote by \mathcal{G} the family of polytopes whose dual is constructed by repeatedly Gale sewing from some \mathcal{D}_r . We will call these polytopes *Gale sewn*.

Remark 4.2 Gale sewing can be applied onto any balanced matroid. In particular, it can be used to construct infinitely many non-realizable neighborly oriented matroids, just by starting from the dual of a non-realizable neighborly oriented matroid. For example the sphere " M_{425}^{10} " from Altshuler (1977) is a non-realizable neighborly oriented matroid (see Bokowski and Garms (1987)).

⁽i) Shemer's concept of totally sewn polytopes is slightly different, because we only admit those flags that come from Theorem 3.6.

Cyclic polytopes are a first example of polytopes in \mathcal{G} .

Proposition 4.3 Let \mathcal{M} be an oriented matroid dual to a cyclic polytope c(d, n), with elements s_1, s_2, \ldots, s_n labeled according to the cyclic order. Then $\mathcal{M}[x] = \mathcal{M}[s_n^-, s_{n-1}^-, \ldots, s_d^-]$ is an oriented matroid dual to c(d+1, n+1), with $x = s_{n+1}$.

When Gale sewing, one can interchange the role of a_1 , p and q as follows.

Lemma 4.4 Let \mathcal{M} be a uniform oriented matroid on a ground set E, and consider the lexicographic extensions $\mathcal{M}[p][q]$, $\mathcal{M}[p'][q']$ and $\mathcal{M}[p''][q'']$ defined by

$$p = [a_1^{s_1}, \dots, a_r^{s_r}], \qquad q = [p^-, a_1^-, \dots, a_{r-1}^-];$$

$$p' = [a_1^{-s_1}, \dots, a_r^{-s_r}], \qquad q' = [p'^-, a_1^-, \dots, a_{r-1}^-];$$

$$p'' = [a_1^+, a_2^{-s_1s_2}, \dots, a_r^{-s_1s_r}], \qquad q'' = [p''^-, a_1^-, \dots, a_{r-1}^-].$$

Then,

$$\mathcal{M}[p][q] \stackrel{\varphi}{\simeq} \mathcal{M}[p'][q'], \qquad \qquad and \qquad \qquad \mathcal{M}[p][q] \stackrel{\psi}{\simeq} \mathcal{M}[p''][q''],$$

where $\varphi(p) = q'$, $\varphi(q) = p'$ and $\varphi(e) = e$ for $e \in E$. If $s_1 = +$, then $\psi(p) = a_1$, $\psi(q) = q''$, $\psi(a_1) = p''$ and $\psi(e) = e$ for $e \in E \setminus \{a_1\}$, and if $s_1 = -$, then $\psi(p) = q''$, $\psi(q) = a_1$, $\psi(a_1) = p''$ and $\psi(e) = e$ for $e \in E \setminus \{a_1\}$.

The following result follows from Proposition 2.4 and explains the contractions of Gale sewing extensions. From it, it is easy to derive that subpolytopes of Gale sewn polytopes are also Gale sewn:

Lemma 4.5 Let \mathcal{M} be a uniform oriented matroid of rank r, and consider the lexicographic extensions

$$p = [a_1^{s_1}, a_2^{s_2}, \dots, a_r^{s_r}], \qquad q = [p^-, a_1^-, \dots, a_{r-1}^-];$$

$$p' = [a_2^{-s_1s_2}, \dots, a_r^{-s_1s_r}], \qquad q' = [p'^-, \dots, a_{r-1}^-].$$

Then $(\mathcal{M}[p][q])/q \simeq (\mathcal{M}/a_1)[p'][q'].$

Proposition 4.6 If \mathcal{P} is a neighborly polytope in \mathcal{G} , and e an element of \mathcal{P} , then $\mathcal{P} \setminus e$ is also in \mathcal{G} .

5 Comparing the constructions

In this section we compare the two constructions, which are strongly related. Our goal is to prove that all neighborly polytopes in \mathcal{O} belong to \mathcal{G} . From Proposition 4.6 one deduces that to prove that $\mathcal{O} \subseteq \mathcal{G}$ it is enough to see that $\mathcal{S} \subseteq \mathcal{G}$. As a first step we will prove that if we sew on a neighborly polytope in \mathcal{G} (through a specific universal flag), we obtain a new polytope in \mathcal{G} .

Let \mathcal{P} be a neighborly matroid in \mathcal{G} . That means that its dual matroid $\mathcal{M} = \mathcal{P}^*$ is constructed using Gale sewing as in Section 4. Specifically, $\mathcal{M} = \mathcal{M}_m$ where $\mathcal{M}_0 = \mathcal{D}_r$ is a minimal totally cyclic configuration $\{a_0, \ldots, a_r\}$ of rank r and

$$\mathcal{M}_k = \mathcal{M}_{k-1}[x_k][y_k],$$

with x_k and y_k being the lexicographic extensions

$$x_k = [e_{k1}^{s_{k1}}, \dots, e_{kr}^{s_{kr}}], \qquad y_k = [x_k^-, e_{k1}^-, \dots, e_{k(r-1)}^-]$$

Let $T_j = \bigcup_{i=0}^{j-1} \{x_{m-i}, y_{m-i}\}$, that is $T_{m-k} = \{x_m, y_m, \dots, x_{k+1}, y_{k+1}\}$. And let $\mathcal{T} = \{T_i\}_{i=1}^m$. Define $\mathcal{P}_k = \mathcal{M}_k^*$, and observe that $\mathcal{P}_k = \mathcal{P}/T_{m-k}$ for $k = 0, \dots, m$. By construction, \mathcal{T} is a universal flag of \mathcal{P} .

We can apply the Sewing Theorem 3.6 to \mathcal{P} and \mathcal{T} . Let $\tilde{\mathcal{P}}$ be $\mathcal{P} \cup p$, with p sewn onto \mathcal{P} through \mathcal{T} . We define $\tilde{T}_{j+1} = T_j \cup y_{m-j} \cup p$, that is $\tilde{T}_{m-k} = \{x_m, y_m, \dots, x_{k+2}, y_{k+2}\} \cup \{y_{k+1}\} \cup \{p\}$. Then $\tilde{\mathcal{T}} = \{\tilde{T}_i\}_{i=1}^m$ is a universal flag of $\tilde{\mathcal{P}}$. We denote $\tilde{\mathcal{P}}_k = \tilde{\mathcal{P}}/\tilde{T}_{m-k}$ and observe that $\tilde{\mathcal{P}}_k \simeq \mathcal{P}_k[\mathcal{T}/T_{m-k}]$ where the sewn vertex is x_{k+1} , and thus $\tilde{\mathcal{P}}_k \setminus x_{k+1} \simeq \mathcal{P}_k$. To provide shorter proofs, we will sometimes refer to p as x_{m+1} .

Finally, let $\tilde{\mathcal{M}} = \tilde{\mathcal{M}}_m$ be the oriented matroid constructed as follows:

$$\tilde{\mathcal{M}}_{0} = \mathcal{D}_{r+1} \text{ on a ground set } \{\tilde{a}_{1}, \dots, \tilde{a}_{r+1}, \tilde{x}_{1}\}, \\
\tilde{y}_{k} = [\tilde{x}_{k}^{+}, (\tilde{e}_{k1})^{-s_{k1}}, \dots, (\tilde{e}_{kr})^{-s_{kr}}] \\
\tilde{x}_{k+1} = [\tilde{y}_{k}^{-}, (\tilde{e}_{k1})^{-}, \dots, (\tilde{e}_{k(r-1)})^{-}], \\
\tilde{\mathcal{M}}_{k} = \tilde{\mathcal{M}}_{k-1}[\tilde{y}_{k}][\tilde{x}_{k+1}],$$

where if $e_{ij} = x$ then \tilde{e}_{ij} means the element labeled as \tilde{x} .

Then we claim that $\tilde{\mathcal{M}}$ is the dual configuration of $\tilde{\mathcal{P}}$, and hence $\tilde{\mathcal{P}}$ is in \mathcal{G} .

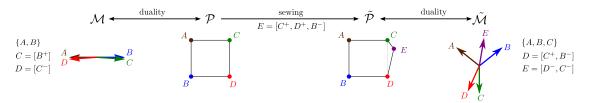


Fig. 1: Example: \mathcal{M} is constructed from $\{A, B\}$ after Gale sewing $C = [B^+]$ and $D = [C^-]$. In its dual $\mathcal{P} = \mathcal{M}^*$, $\{C, D\}$ is a universal edge. $\tilde{\mathcal{P}} = \mathcal{P}[E]$ is obtained by sewing E on \mathcal{P} through $\{C, D\}$. Its dual matroid, $\tilde{\mathcal{M}} = \tilde{\mathcal{P}}^*$ can be constructed from $\{A, B, C\}$ and Gale sewing $D = [C^+, B^-]$ and $E = [D^-, C^-]$.

Proposition 5.1 With the notations as above, $\tilde{\mathcal{M}} \simeq \tilde{\mathcal{P}}^*$ via the isomorphism $x \mapsto \tilde{x}$.

Proof: We will prove that $\tilde{\mathcal{M}}_k \simeq \tilde{\mathcal{P}}_k^*$, for all k. The proof will use induction on k and assume that $\tilde{\mathcal{M}}_{k-1} \simeq \tilde{\mathcal{P}}_{k-1}^*$. It is straightforward that $\tilde{\mathcal{M}}_0 \simeq \tilde{\mathcal{P}}_0^*$ since \mathcal{P}_0 is 0-dimensional.

We will use Theorem 2.1 twice. Specifically, we will use that if $\mathcal{M} \setminus p \simeq \mathcal{N} \setminus p$ and $\mathcal{M}/p \simeq \mathcal{N}/p$, then \mathcal{M} and \mathcal{N} are the same oriented matroid up to the reorientation of p. If additionally there is an element q such that p and q are covariant (or contravariant) in \mathcal{N} and \mathcal{M} , then $\mathcal{M} \simeq \mathcal{N}$.

In particular, we will prove that $\tilde{\mathcal{M}}_k/\tilde{x}_{k+1} \simeq \tilde{\mathcal{P}}_k^*/x_{k+1}$ and that $\tilde{\mathcal{M}}_k \setminus \tilde{x}_{k+1} \simeq \tilde{\mathcal{P}}_k^* \setminus x_{k+1}$. Then the claim $\tilde{\mathcal{M}} \simeq \tilde{\mathcal{P}}^*$ will follow directly from the fact that \tilde{x}_{k+1} and \tilde{y}_k are covariant in $\tilde{\mathcal{M}}_k$ and that x_{k+1} and y_k are covariant in $\tilde{\mathcal{P}}_k^*$.

Arnau Padrol

 $\frac{\tilde{\mathcal{M}}_k/\tilde{x}_{k+1} \simeq \tilde{\mathcal{P}}_k^*/x_{k+1}}{\text{Since }\tilde{\mathcal{P}}_k^*/x_{k+1} \simeq \mathcal{P}_k^*} = \mathcal{M}_k \text{ because } \tilde{\mathcal{P}}_k \setminus x_{k+1} \simeq \mathcal{P}_k, \text{ we just need to prove that}$

$$\tilde{\mathcal{M}}_k/\tilde{x}_{k+1} \simeq \mathcal{M}_k. \tag{4}$$

By Lemma 4.5, $(\tilde{\mathcal{M}}_k/\tilde{x}_{k+1}) \simeq (\tilde{\mathcal{M}}_{k-1}/\tilde{x}_k)[x'_k][y'_k]$, where $x'_k = [\tilde{e}^{s_{k1}}_{k1}, \ldots, \tilde{e}^{s_{kr}}_{kr}]$ and $y'_k = [x'_k, \tilde{e}_{k1}, \ldots, \tilde{e}_{k(r-1)}]$. Using that $\tilde{\mathcal{M}}_0/\tilde{x}_1 \simeq \mathcal{M}_0$ we get the desired result by induction on k.

$$\underline{\mathcal{M}_k \setminus \tilde{x}_{k+1} \simeq \mathcal{P}_k^* \setminus x_{k+1}}$$

The first step is to prove that $(\tilde{\mathcal{M}}_k \setminus \tilde{x}_{k+1}) \setminus \tilde{y}_k \simeq (\tilde{\mathcal{P}}_k^* \setminus x_{k+1}) \setminus y_k$. Indeed, using the induction hypothesis,

$$(\tilde{\mathcal{M}}_k \setminus \tilde{x}_{k+1}) \setminus \tilde{y}_k = \tilde{\mathcal{M}}_{k-1} \simeq \tilde{\mathcal{P}}_{k-1}^* = (\tilde{\mathcal{P}}_k / \{y_k, x_{k+1}\})^* = (\tilde{\mathcal{P}}_k^* \setminus x_{k+1}) \setminus y_k$$

Now we prove that $(\tilde{\mathcal{M}}_k \setminus \tilde{x}_{k+1})/\tilde{y}_k \simeq (\tilde{\mathcal{P}}_k^* \setminus x_{k+1})/y_k$. First, using Corollary 2.5 and (4), we see that

$$(\mathcal{M}_k \setminus \tilde{x}_{k+1})/\tilde{y}_k \simeq (\mathcal{M}_k/\tilde{x}_{k+1}) \setminus \tilde{y}_k \simeq \mathcal{M}_k \setminus y_k.$$

Now, using again Corollary 2.5 and that $\tilde{\mathcal{P}}_k \setminus x_{k+1} \simeq \mathcal{P}_k$, we see that

$$(\tilde{\mathcal{P}}_k^* \setminus x_{k+1})/y_k = (\tilde{\mathcal{P}}_k/x_{k+1} \setminus y_k)^* \simeq (\tilde{\mathcal{P}}_k \setminus x_{k+1}/y_k)^* = (\mathcal{P}_k/y_k)^* = \mathcal{P}_k^* \setminus y_k.$$

Our claim follows since $\mathcal{M}_k = \mathcal{P}_k^*$ by definition.

Because of Theorem 2.1, so far we have seen that $\tilde{\mathcal{M}}_k \setminus \tilde{x}_{k+1} \simeq \tilde{\mathcal{P}}_k^* \setminus x_{k+1}$ up to reorientation of y_k . We will conclude the proof by seeing that y_k and \tilde{y}_k have the same orientation in \mathcal{M}_k and in $\tilde{\mathcal{M}}_k$ respectively.

Observe that \tilde{y}_k is contravariant with \tilde{x}_k in \mathcal{M}_k by construction. Moreover, y_k is contravariant with x_k in $(\mathcal{\tilde{P}}_k/x_{k+1})^*$ since they are covariant in the primal: by Proposition 2.4

$$\tilde{\mathcal{P}}_k/x_{k+1} \simeq \left(\mathcal{P}_k[\underline{\mathcal{T}'/T_{m-k}}]\right)/x_{k+1} \simeq \left(\mathcal{P}_k/x_k\right)[\underline{y_k^-,\dots}]_{x_k}$$

where the last isomorphism sends x_k to the sewn vertex, which is (+1)-inseparable from y_k .

There are two missing details to conclude that $S \subseteq G$ from Proposition 5.1:

- i) We have to check that cyclic polytopes are in \mathcal{G} and that the universal flags of Example 3.2 are of the form $T_j = \bigcup_{i=0}^{j-1} (x_{m-i}, y_{m-i})$ for some Gale sewn configuration. Indeed, Proposition 4.3 shows that cyclic polytopes are in \mathcal{G} . And using that the automorphism group of c(2m, n) contains the dihedral group (see Altshuler and Perles (1980)) together with Lemma 4.4 we can build the flags of Example 3.2.
- ii) We have to check that after sewing, the universal flags arising from Point (2) in Theorem 3.6 are also of the form $T_j = \bigcup_{i=0}^{j-1} (x_{m-i}, y_{m-i})$ for some Gale sewn configuration. This follows directly from Lemma 4.4.

Remark 5.2 The fact that $S \subsetneq G$ implies that in some sense Gale sewing generalizes ordinary sewing. However, it is not true that Theorem 3.6 is a consequence of Theorem 4.1, because there are neighborly matroids that have universal flags but are not in G. Hence one can sew on them but they cannot be treated with Proposition 5.1.

6 Concluding remarks

Fix n and d = 2m. We have worked with four families of neighborly d-polytopes with n vertices:

- \mathcal{N} : All neighborly *d*-polytopes with *n* vertices.
- \mathcal{G} : All Gale sewn *d*-polytopes with *n* vertices.
- \mathcal{O} : All *d*-polytopes with *n* vertices obtained by sewing and omitting.
- S: All totally sewn d-polytopes with n vertices.

Table 1 contains the exact number of combinatorial types in each of these families for some particular cases. Exact numbers for \mathcal{N} come from Altshuler and Steinberg (1973) and Bokowski and Shemer (1987), exact numbers for \mathcal{S} and \mathcal{O} come from Shemer (1982). Numbers for \mathcal{G} have been computed with the help of polymake Gawrilow and Joswig (2000).

d	n	S	\mathcal{O}	\mathcal{G}	\mathcal{N}
2	n	1	1	1	1
2d	$\leq 2d+3$	1	1	1	1
4	8	3	3	3	3
4	9	18	18	18	23
6	10	15	28	28	37

Tab. 1: Exact number of combinatorial types

In view of Table 1, the relationships that we know between these families are the following:

$$\mathcal{S} \subsetneq \mathcal{O} \subseteq \mathcal{G} \subsetneq \mathcal{N}$$

Whether $\mathcal{O} = \mathcal{G}$ or not is an open question.

Acknowledgements

I would like to thank Uli Wagner for stimulating discussions. In particular, he suggested me a problem stated by Wagner (2006) that was the original motivation for studying constructions of neighborly oriented matroids: do they exist matroids \mathcal{M} of rank d with n elements that have an element o such that \mathcal{M}/o is balanced and $\mathcal{M} \setminus o$ is neighborly? This question remains open.

Moreover, I am greatly indebted to Julian Pfeifle for his comments and corrections that greatly helped to improve the presentation.

References

N. Alon. The number of polytopes, configurations and real matroids. Mathematika, 33(1):62-71, 1986.

A. Altshuler. Neighborly 4-polytopes and neighborly combinatorial 3-manifolds with ten vertices. *Can. J. Math.*, 29:225–420, 1977.

- A. Altshuler and M. A. Perles. Quotient polytopes of cyclic polytopes. I: Structure and characterization. *Isr. J. Math.*, 36:97–125, 1980.
- A. Altshuler and L. Steinberg. Neighborly 4-polytopes with 9 vertices. J. Comb. Theory, Ser. A, 15: 270–287, 1973.
- D. Barnette. A family of neighborly polytopes. Isr. J. Math., 39:127-140, 1981.
- T. Bisztriczky. On sewing neighbourly polytopes. Note Mat., 20(1):73-80, 2000/01. ISSN 1123-2536.
- A. Björner, M. Las Vergnas, B. Sturmfels, N. White, and G. M. Ziegler. *Oriented matroids*. Encyclopedia of Mathematics and Its Applications. 46. Cambridge: Cambridge University Press. 516 p., 1993.
- J. Bokowski and K. Garms. Altshuler's sphere M_{425}^{10} is not polytopal. *Eur. J. Comb.*, 8:227–229, 1987.
- J. Bokowski and I. Shemer. Neighborly 6-polytopes with 10 vertices. Isr. J. Math., 58:103–124, 1987.
- R. Cordovil and P. Duchet. Cyclic polytopes and oriented matroids. Eur. J. Comb., 21(1):49-64, 2000.
- L. Finschi. A Graph Theoretical Approach for Reconstruction and Generation of Oriented Matroids. PhD thesis, ETH Zürich, 2001.
- E. Gawrilow and M. Joswig. polymake: a framework for analyzing convex polytopes. In G. Kalai and G. M. Ziegler, editors, *Polytopes — Combinatorics and Computation*, pages 43–74. Birkhäuser, 2000.
- J. E. Goodman and R. Pollack. Upper bounds for configurations and polytopes in \mathbb{R}^d . *Discrete Comput. Geom.*, 1:219–227, 1986.
- B. Grünbaum. Convex polytopes, volume 221 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 2003. Prepared by Volker Kaibel, Victor Klee and Günter M. Ziegler.
- M. Las Vergnas. Extensions ponctuelles d'une géométrie combinatoire orientee. Problèmes combinatoires et théorie des graphes, Orsay 1976, Colloq. int. CNRS No.260, 265-270 (1978)., 1978.
- C. W. Lee and M. M. Menzel. A generalized sewing construction for polytopes. *Isr. J. Math.*, 176: 241–267, 2010.
- P. McMullen. The maximum numbers of faces of a convex polytope. *Mathematika*, *Lond.*, 17:179–184, 1970.
- A. Padrol. Many neighborly polytopes and oriented matroids. Preprint, arXiv:1202.2810, 2012.
- J. Richter-Gebert and G. M. Ziegler. Zonotopal tilings and the Bohne-Dress theorem. In *Jerusalem combinatorics '93*, volume 178 of *Contemp. Math.*, pages 211–232. Amer. Math. Soc., 1994.
- I. Shemer. Neighborly polytopes. Isr. J. Math., 43:291–314, 1982.
- B. Sturmfels. Neighborly polytopes and oriented matroids. Eur. J. Comb., 9(6):537–546, 1988.
- R. Trelford and V. Vigh. How to sew in practice? Preprint, arXiv:1102.4862v1, 2011.
- U. Wagner. On a geometric generalization of the upper bound theorem. In *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science*, pages 635–645, 2006.