

Description of polygonal regions by polynomials of bounded degree

Gennadiy Averkov · Christian Bey

Received: 27 May 2009 / Accepted: 15 April 2010
© Springer-Verlag 2010

Abstract We show that every (possibly unbounded) convex polygon P in \mathbb{R}^2 with m edges can be represented by inequalities $p_1 \geq 0, \dots, p_n \geq 0$, where the p_i 's are products of at most k affine functions each vanishing on an edge of P and $n = n(m, k)$ satisfies $s(m, k) \leq n(m, k) \leq (1 + \varepsilon_m)s(m, k)$ with $s(m, k) := \max\{m/k, \log_2 m\}$ and $\varepsilon_m \rightarrow 0$ as $m \rightarrow \infty$. This choice of n is asymptotically best possible. An analogous result on representing the interior of P in the form $p_1 > 0, \dots, p_n > 0$ is also given. For $k \leq m/\log_2 m$ these statements remain valid for representations with arbitrary polynomials of degree not exceeding k .

Keywords Gray code · Polygon · Polynomial · Semi-algebraic set · Theorem of Bröcker and Scheiderer

Mathematics Subject Classification (2000) Primary 14P10 · 52B11; Secondary 52A10

G. Averkov's work was supported by the German Research Foundation within the Research Unit 468 "Methods from Discrete Mathematics for the Synthesis and Control of Chemical Processes".

G. Averkov (✉) · C. Bey
Fakultät für Mathematik, Otto-von-Guericke-Universität Magdeburg,
Universitätsplatz 2, 39106 Magdeburg, Germany
e-mail: averkov@ovgu.de; gennadiy.averkov@gmail.com
URL: <http://fma2.math.uni-magdeburg.de/~averkov>

C. Bey
e-mail: bey@ovgu.de
URL: <http://fma2.math.uni-magdeburg.de/~bey>

1 Introduction

A set P in \mathbb{R}^d is said to be a d -dimensional polyhedron if P is intersection of finitely many closed half-spaces and has non-empty interior. Thus, a natural description of P is given in terms of its \mathcal{H} -representation, i.e. a collection of non-strict affine inequalities. As was suggested in [9, 11, 12], one could try to use more general polynomial representations of P , called \mathcal{P} -representations, for possibly developing new effective methods for solving combinatorial optimization problems. That is, one may look for representations of the form

$$P = \{p_1 \geq 0, \dots, p_n \geq 0\} := \left\{x \in \mathbb{R}^d : p_1(x) \geq 0, \dots, p_n(x) \geq 0\right\},$$

where p_1, \dots, p_n are real polynomials in d variables. Naturally, one tries to find \mathcal{P} -representations of P with a small number n of polynomials. Possible choices of n , also for the more general case when P is a semi-algebraic set, can be derived using results from real algebraic geometry, see [1, 7]. It has been recently established that every d -dimensional polyhedron has a \mathcal{P} -representation with d polynomials, see the end of this section for references and further details.

In this note we are interested in small \mathcal{P} -representations of polyhedra consisting of polynomials of bounded degree. We present a result in the 2-dimensional case, namely, we determine asymptotically the minimal number of polynomials of degree at most k which are needed to describe a 2-dimensional polyhedron with m edges, for all degrees $k \leq m/\log_2 m$. This improves earlier work in [13], see below.

Let us call a 2-dimensional polyhedron P a *polygon* (thus, we also allow unbounded polygons). Besides polynomial representations of P we shall also investigate polynomial representations of the interior $\text{int } P$ of P in terms of strict polynomial inequalities. Our main result is the following:

Theorem 1.1 *Let $m, k \in \mathbb{N}$. Let $N(m, k)$ (resp. $\overline{N}(m, k)$) denote the minimal $n \in \mathbb{N}$ such that for every polygon P with m edges there exist real polynomials p_1, \dots, p_n satisfying the conditions (A) and (B) (resp. (\overline{A}) and (\overline{B})), where*

$$(A) \quad \text{int } P = \{p_1 > 0, \dots, p_n > 0\};$$

$$(\overline{A}) \quad P = \{p_1 \geq 0, \dots, p_n \geq 0\};$$

$$(B) \quad \text{every } p_i \text{ has degree at most } k.$$

Then for all k satisfying

$$k \leq m/\log_2 m$$

one has

$$m/k \leq N(m, k) \leq (1 + \varepsilon_m)m/k,$$

where $\varepsilon_m \rightarrow 0$ as $m \rightarrow +\infty$.

The same statement holds with $\overline{N}(m, k)$ instead of $N(m, k)$.

The upper bound in Theorem 1.1 will be established by using polynomials p_i each of which being a product of affine functions. In fact, for such polynomials we are able to determine their minimal number n asymptotically without any restriction on k :

Theorem 1.2 *Let $m, k \in \mathbb{N}$. Let $N(m, k)$ (resp. $\bar{N}(m, k)$) denote the minimal $n \in \mathbb{N}$ such that for every polygon P with m edges there exist real polynomials p_1, \dots, p_n satisfying the conditions conditions (A) and (C) (resp. (\bar{A}) and (C), where*

- (A) $\text{int } P = \{p_1 > 0, \dots, p_n > 0\}$;
- (\bar{A}) $P = \{p_1 \geq 0, \dots, p_n \geq 0\}$;
- (C) every p_i is a product of at most k affine functions each non-negative on P and vanishing on some edge of P .

Then, with $s(m, k) := \max\{m/k, \log_2 m\}$,

$$s(m, k) \leq N(m, k) \leq \bar{N}(m, k) \leq (1 + \varepsilon_m)s(m, k),$$

where $\varepsilon_m \rightarrow 0$ as $m \rightarrow +\infty$.

Prior to Theorem 1.2, an upper bound $\bar{N}(m, k) \leq m/k + \log_2 k$ was observed in [13] (see also [12, Satz 2.4]), which, together with the lower bound in Theorem 1.2, determines $\bar{N}(m, k)$ already up to a factor of 2.

Theorem 1.1 will follow from Theorem 1.2. The proof of Theorem 1.2 consists of a geometric and a combinatorial part. In the geometric part, given in Sect. 2, we show that essentially it suffices to consider unbounded polygons whose two unbounded edges are not parallel and express the minimal n from Theorem 1.2 for such polygons in purely combinatorial terms. In the combinatorial part, given in Sect. 3, we estimate this minimal n by employing results on Gray codes (cf. [14, 16]).

By Theorem 1.1, $N(m, k) \sim \bar{N}(m, k) \sim m/k$ for $k \leq m/\log_2 m$ as $m \rightarrow \infty$. Let us give a few remarks for other choices of k . We only discuss $N(m, k)$ here, since the comments on $\bar{N}(m, k)$ are analogous. Using results from real algebraic geometry, one can show that there exists a function $k_0(m)$ such that $N(m, k) = 2$ for every $k \geq k_0(m)$. This follows directly from the Theorem of Bröcker and Scheiderer [7, Sect. 6.5, Sect. 10.4] and [15, Theorem 5.1], which are formulated in the framework of real closed fields. One should point out that the existence of $k_0(m)$ is a non-constructive result. In fact, on the one hand it is known that every m -gon P can be described by two polynomials p_1, p_2 , see [8]. On the other hand, known formulas for p_1, p_2 depend on the metric structure of the m -gon P so that the degrees of p_1, p_2 are not bounded from above for any fixed m . Already for the case $m = 5$ it is not clear how to (efficiently) construct polynomials p_1, p_2 representing an arbitrary given pentagon P and having degrees bounded from above by an absolute constant, for further details see [5]. Finally, it would be interesting to estimate $N(m, k)$ for $m/\log_2 m \leq k \leq k_0(m)$, where $N(m, k)$ changes from about $\log_2 m$ to 2.

As for \mathcal{P} -representations of polyhedra of arbitrary dimensions, we point out that recently it was shown [4] that every d -dimensional polyhedron can be represented by d non-strict polynomial inequalities. This provides a positive answer to a conjecture posed in [9]. We also refer to [5, 6, 8, 9, 17] for preliminary results, [2, 3] for related results, and [12] for a survey on that topic. For the case $d \geq 3$ currently no results on

the interplay between the degrees and the number of polynomials in \mathcal{P} -representations of d -dimensional polyhedra seem available.

2 Geometric arguments

Let P be a polygon in \mathbb{R}^2 . By E we denote the set of all edges of P . For every edge $I \in E$, we fix a real polynomial $p_I(x)$ of degree one, vanishing on I and non-negative on P .

The following proposition is easily derived by standard arguments from real algebraic geometry. For completeness we give a proof (see also [3] and [11, Prop. 2.1]).

Proposition 2.1 *Let P be a polygon and let p_1, \dots, p_n be real polynomials such that $P = \{p_1 \geq 0, \dots, p_n \geq 0\}$ or $\text{int } P = \{p_1 > 0, \dots, p_n > 0\}$. Then for every $I \in E$ the polynomial p_I is a factor of odd multiplicity of some p_i , $1 \leq i \leq n$.*

Proof Fix an edge $I \in E$ and let $\prod_{i=1}^n p_i = p_I^e \prod_{j=1}^m q_j$ with $e \in \mathbb{N} \cup \{0\}$ and irreducible polynomials q_j not divisible by p_I , $1 \leq j \leq m$. Since every q_j has only finitely many zeros in $\{p_I = 0\}$ there exists an $x \in I$ with $q_j(x) \neq 0$ for all $j = 1, \dots, m$, and hence, by continuity, there is a neighborhood \mathcal{N} of x on which for all $j = 1, \dots, m$ the sign of q_j is constant. If p_I would have even multiplicity in every p_i then the sign of every p_i would be constant on $\mathcal{N} \setminus \{p_I = 0\}$ so that, in both cases $P = \{p_1 \geq 0, \dots, p_n \geq 0\}$ and $\text{int } P = \{p_1 > 0, \dots, p_n > 0\}$, either $\mathcal{N} \setminus \{p_I = 0\} \subseteq P$ or $(\mathcal{N} \setminus \{p_I = 0\}) \cap \text{int } P = \emptyset$. But this is impossible since x is a boundary point of P and hence $\mathcal{N} \cap \{p_I < 0\} \not\subseteq P$ and $\mathcal{N} \cap \{p_I > 0\} \cap \text{int } P \neq \emptyset$. \square

Recall that a real polynomial is called *squarefree* if every irreducible factor of it occurs with multiplicity one.

Lemma 2.2 *Let $m, k \in \mathbb{N}$. The quantity $N(m, k)$ (resp. $\bar{N}(m, k)$) from Theorem 1.2 is attained at squarefree polynomials p_1, \dots, p_n satisfying (A) and (C) (resp. \bar{A} and \bar{C}).*

Proof Given a polygon P with m edges and polynomials p_1, \dots, p_n satisfying the conditions (A) and (C), we can clearly replace factors of p_1, \dots, p_n with odd multiplicities by the same factors with multiplicity one while maintaining the conditions (A) and (C). Furthermore, factors with even multiplicities can just be dropped out. In fact, if for some edge I , p_I is a factor of p_1 with even multiplicity, say with multiplicity two, then, in view of Proposition 2.1, p_I is a factor of odd multiplicity of some p_i , $1 < i \leq n$, say p_2 , so that $\{p_1 > 0, p_2 > 0\} = \{p_1/p_I^2 > 0, p_2 > 0\}$.

Similarly, given polynomials p_1, \dots, p_n satisfying the conditions (\bar{A}) and (C), odd multiplicities can be replaced by multiplicity one, and factors with even multiplicities can be dropped out, since, with the notation above, $P \subseteq \{p_1/p_I^2 \geq 0, p_2 \geq 0\} \subseteq \{p_1 \geq 0, p_2 \geq 0\}$.

Performing the above reductions we obtain polynomials p_1, \dots, p_n each of which being a product of at most k different p_I , $I \in E$. \square

For every set $F \subseteq E$ of edges of the polygon P we put

$$p_F(x) := \prod_{I \in F} p_I(x).$$

For $x \in \mathbb{R}^2 \setminus P$ we define the set $E_{<}(x) := \{I \in E : p_I(x) < 0\}$. Geometrically, $E_{<}(x)$ is the set of edges of P illuminated from x . The sets $E_{\leq}(x)$ and $E_{=}(x)$ are defined analogously.

Lemma 2.3 *Let P be a polygon and let $F_1, \dots, F_n \subseteq E$. Then the following statements hold.*

- I. *If $P = \{p_{F_1} \geq 0, \dots, p_{F_n} \geq 0\}$ then $\text{int } P = \{p_{F_1} > 0, \dots, p_{F_n} > 0\}$.*
- II. *If $\text{int } P = \{p_{F_1} > 0, \dots, p_{F_n} > 0\}$ then $E = F_1 \cup \dots \cup F_n$.*
- III. *$P = \{p_{F_1} \geq 0, \dots, p_{F_n} \geq 0\}$ if and only if for every $x \in \mathbb{R}^2 \setminus P$ there exists $i \in \{1, \dots, n\}$ such that $\#(F_i \cap E_{<}(x))$ is odd and $F_i \cap E_{=}(x) = \emptyset$.*
- IV. *$\text{int } P = \{p_{F_1} > 0, \dots, p_{F_n} > 0\}$ if and only if for every $x \in \mathbb{R}^2 \setminus P$ there exists $i \in \{1, \dots, n\}$ such that $\#(F_i \cap E_{<}(x))$ is odd.*

Proof The proof is straightforward. Part II follows directly from Proposition 2.1. Let us show only IV. We start with the “only if” part. Let $x \in \mathbb{R}^2 \setminus P$. If $p_I(x) \neq 0$ for every $I \in E$ then, by assumption, there exists $i \in \{1, \dots, n\}$ such that $p_{F_i}(x) < 0$ and consequently $\#(F_i \cap E_{<}(x))$ is odd. If $p_I(x) = 0$ for some $I \in E$ then we can choose an $y \in \mathbb{R}^d \setminus P$ with $E_{<}(y) = E_{<}(x)$ and $p_J(y) \neq 0$ for every $J \in E$. Thus, by the previous case, there exists $i \in \{1, \dots, n\}$ such that $\#(F_i \cap E_{<}(x))$ is odd. Next we show the “if” part. Since obviously $\text{int } P \subseteq \{p_{F_1} > 0, \dots, p_{F_n} > 0\}$, we have to show that for every $x \in \mathbb{R}^2 \setminus \text{int } P$ there exists $i \in \{1, \dots, n\}$ with $p_{F_i}(x) \leq 0$. If $x \notin P$ this is clear by assumption. If $x \in P \setminus \text{int } P$ we have $x \in I$ for some $I \in E$, and we can choose an $y \in \mathbb{R}^2 \setminus P$ with $E_{<}(y) = \{I\}$. Then, by assumption, there exists $i \in \{1, \dots, n\}$ with $I \in F_i$, so $p_{F_i}(x) = 0$. □

We remark that the converse of Lemma 2.3.I is not true in general. For example, the interior of the quadrant $P := \{x \in \mathbb{R}^2 : x_1 \geq 0, x_2 \geq 0\}$ is equal to

$$\{x \in \mathbb{R}^2 : x_1 > 0, x_2 > 0\} = \{x \in \mathbb{R}^2 : x_1 > 0, x_1 x_2 > 0\},$$

and relaxing the inequalities on the right hand side gives $\{x \in \mathbb{R}^2 : x_1 \geq 0, x_1 x_2 \geq 0\}$, the union of P with the x_1 -axis.

By $n(P, k)$ (resp. $\bar{n}(P, k)$) we denote the minimal $n \in \mathbb{N}$ such that there exist $F_1, \dots, F_n \subseteq E$, each F_i of cardinality at most k , such that $\text{int } P = \{p_{F_1} > 0, \dots, p_{F_n} > 0\}$ (resp. $P = \{p_{F_1} \geq 0, \dots, p_{F_n} \geq 0\}$). Clearly, in view of Lemma 2.2, the quantity $N(m, k)$ (resp. $\bar{N}(m, k)$) in Theorem 1.2 is the maximum of $n(P, k)$ (resp. $\bar{n}(P, k)$) over all polygons P with m edges.

We can now state our two main propositions in this section.

Proposition 2.4 *Let P be an unbounded polygon with m edges such that the unbounded edges of P are not parallel. Then the quantities $n(P, k)$ and $\bar{n}(P, k)$ depend*

only on m and k . Furthermore, $n(m, k) := n(P, k)$ and $\bar{n}(m, k) := \bar{n}(P, k)$ are determined as follows:

- I. $n(m, k)$ is the minimal $n \in \mathbb{N}$ such that there exist sets $S_1, \dots, S_n \subseteq \{1, \dots, m\}$ satisfying the following conditions:
 - (I) for every $a, b \in \mathbb{N}$ with $1 \leq a \leq b \leq m$ there exists $i \in \{1, \dots, n\}$ such that $\#(S_i \cap \{a, \dots, b\})$ is odd;
 - (K) $\#S_i \leq k$ for all $i \in \{1, \dots, n\}$.
- II. $\bar{n}(m, k)$ is the minimal $n \in \mathbb{N}$ such that there exist sets $S_1, \dots, S_n \subseteq \{1, \dots, m\}$ satisfying the following conditions:
 - (J) for every $a, b \in \mathbb{N}$ with $1 \leq a \leq b \leq m$ there exists $i \in \{1, \dots, n\}$ such that $\#(S_i \cap \{a, \dots, b\})$ is odd and $\{a - 1, b + 1\} \cap S_i = \emptyset$;
 - (K) $\#S_i \leq k$ for all $i \in \{1, \dots, n\}$.

Proof Let I_1, I_2, \dots, I_m denote the edges of P in consecutive order. Thus, I_1 and I_m are the non-parallel unbounded edges. By identifying edge sets $F_1, \dots, F_n \subseteq E = \{I_1, \dots, I_m\}$ with subsets $S_1, \dots, S_n \subseteq \{1, \dots, m\}$ in the obvious way, part I follows from Lemma 2.3.IV and the equality

$$\{E_{<}(x) : x \in \mathbb{R}^2 \setminus P\} = \{\{I_a, \dots, I_b\} : 1 \leq a \leq b \leq m\},$$

and part II follows from Lemma 2.3.III and the equality

$$\begin{aligned} & \{(E_{<}(x), E_{=}(x)) : x \in \mathbb{R}^2 \setminus P\} \\ &= \{(\{I_a, \dots, I_b\}, F) : 1 \leq a \leq b \leq m, F \subseteq \{I_{a-1}, I_{b+1}\} \cap E\}. \end{aligned}$$

□

Proposition 2.5 For $m, k \in \mathbb{N}$ let $N(m, k)$ and $\bar{N}(m, k)$ be defined as in Theorem 1.2, and $n(m, k)$ and $\bar{n}(m, k)$ as in Proposition 2.4. Then one has

$$\begin{aligned} n(m, k) &\leq N(m, k) \leq 1 + n(m - 1, k), \\ \bar{n}(m, k) &\leq \bar{N}(m, k) \leq 1 + \bar{n}(m - 1, k). \end{aligned}$$

Proof The lower bounds for $N(m, k)$ and $\bar{N}(m, k)$ are clear by Proposition 2.4 and the remark preceding it. As for the upper bounds consider an arbitrary polygon P with $m + 1$ consecutive edges I_0, \dots, I_m . Notice that

$$\{E_{<}(x) : x \in \mathbb{R}^2 \setminus P, I_0 \notin E_{<}(x)\} = \{\{I_a, \dots, I_b\} : 1 \leq a \leq b \leq m\}.$$

Consider sets $S_1, \dots, S_n \subseteq \{1, \dots, m\}$ satisfying (I) and (K). As in the proof of Proposition 2.4 we identify each set S_i with the corresponding edge set $F_i \subseteq \{I_1, \dots, I_m\}$. In view of Lemma 2.3.IV we have $\text{int } P = \{p_{I_0} > 0, p_{F_1} > 0, \dots, p_{F_n} > 0\}$. Hence $N(m + 1, k) \leq 1 + n(m, k)$. The upper bound for $\bar{N}(m, k)$ is proved analogously and employs Lemma 2.3.III. □

3 Combinatorial arguments and conclusion

In view of the results from Sect. 2, the proofs of Theorem 1.1 and 1.2 require the determination of the asymptotic behavior of the functions $n(m, k)$ and $\bar{n}(m, k)$ (defined in Proposition 2.4). We will show the following.

Theorem 3.1 *Let $m, k \in \mathbb{N}, k \leq m$. Then*

$$\begin{aligned} \max\{m/k, \log_2(m+1)\} &\leq n(m, k) \leq \bar{n}(m, k) \\ &\leq \max\left\{\frac{m}{k} + 3 \log_2 \frac{m}{k} + C, \lceil \log_2(m+1) \rceil\right\}, \end{aligned}$$

where $C > 0$ is an absolute constant.

In particular, for every $\varepsilon > 0$ and all $(1 + \varepsilon)m / \log_2 m \leq k \leq m$ with m sufficiently large, we have the exact values $\bar{n}(m, k) = n(m, k) = \lceil \log_2(m + 1) \rceil$.

The proof of Theorem 3.1 employs results on Gray codes and is based on the following reformulations for $n(m, k)$ and $\bar{n}(m, k)$.

For subsets S_1, \dots, S_n of $\{1, \dots, m\}$ let M denote their incidence matrix, i.e., the $n \times m$ -matrix whose (i, j) -entry is 1 if $j \in S_i$ and 0 otherwise. Let c_j be the j th column of M , and let M' denote the binary $n \times (m + 1)$ matrix whose j th column is c'_j is $c_1 + \dots + c_j \pmod{2}$, $j = 0, \dots, m$. In particular, c'_0 is the zero column. Clearly, $c_j = c'_{j-1} + c'_j \pmod{2}$ for all $j = 1, \dots, m$. Now it is easy to see that the conditions (I), (J) and (K) (in Proposition 2.4) on the sets S_1, \dots, S_n are equivalent to the following conditions (I'), (J') and (K'), respectively, on the matrix M' :

- (I') the $m + 1$ columns of M' are pairwise distinct;
- (J') for every $a, b \in \mathbb{N}$ with $0 \leq a < b \leq m$ there exists $i \in \{1, \dots, n\}$ such that $M'_{i,a-1} = M'_{i,a} \neq M'_{i,b} = M'_{i,b+1}$ (with $M'_{i,-1} := M'_{i,0}$ and $M'_{i,m+1} := M'_{i,m}$);
- (K') every row of M' has at most k bit changes.

Here a *bit change* in row i of M' is a column index $j \in \{1, \dots, m\}$ for which $M'_{i,j-1} \neq M'_{i,j}$.

Thus, $n(m, k)$ (resp. $\bar{n}(m, k)$) is the minimal $n \in \mathbb{N}$ such that there exists a binary $n \times (m + 1)$ -matrix M' starting with the zero column and satisfying (I') and (K') (resp. (J') and (K')).

Next we cite some facts about Gray codes (cf. [14, 16]). Recall that an n -bit Gray code is a binary $n \times 2^n$ -matrix G with distinct columns $g_j, j = 0, \dots, 2^n - 1$, such that g_j and g_{j+1} differ in exactly one coordinate, $j = 0, \dots, 2^n - 1$, where $g_{2^n} := g_0$. Without loss of generality we shall always assume that g_0 is the zero column.

A *bit run* of length ℓ of G is a $1 \times \ell$ -submatrix $(G_{i,j+1}, \dots, G_{i,j+\ell})$ of G with $G_{i,j} \neq G_{i,j+1} = G_{i,j+2} = \dots = G_{i,j+\ell} \neq G_{i,j+\ell+1}$, where the columns are indexed modulo 2^n .

The upper bound in Theorem 3.1 essentially follows from the following result due to Goddyn and Gvozdzjak [10], see also [14, Section 7.2.1.1].

Theorem 3.2 *For every $n \in \mathbb{N}$ there exists an n -bit Gray code for which every bit run has length at least $n - 3 \log_2 n$. □*

In fact, as shown in [10], Theorem 3.2 holds with the slightly stronger bound $\lfloor n - 2.001 \log_2 n \rfloor$.

We will also need the following simple observation.

Lemma 3.3 *Every n -bit Gray code G satisfies condition (J') (with $M' = G$).*

Proof Fix $a, b \in \mathbb{N}$ with $0 < a < b < m$. Consider the row indices $j, k \in \{1, \dots, n\}$ for which $M'_{j,a-1} \neq M'_{j,a}$ and $M'_{k,b} \neq M'_{k,b+1}$. Then, since M' is a Gray code, $M'_{i,a-1} = M'_{i,a}$ for all $i \neq j$, and $M'_{i,b} = M'_{i,b+1}$ for all $i \neq k$. In particular, the submatrix of M' corresponding to the row indices j, k and column indices $a-1, a, b, b+1$ contains two equal columns (in both cases $j \neq k$ and $j = k$). Since the four columns of M' corresponding to the column indices $a-1, a, b, b+1$ are pairwise different, there exists an $i \neq j, k$ for which $M'_{i,a-1} = M'_{i,a} \neq M'_{i,b} = M'_{i,b+1}$.

A similar argument works if $a = 0$ or $b = m$. \square

Proof of Theorem 3.1 We shall use the matrices M and M' introduced above.

The lower bound on $n(m, k)$ is clear in view of the conditions on M and M' . Indeed, with $a = b$ in condition (I) we see that every element from $\{1, \dots, m\}$ is covered by at least one of the sets S_1, \dots, S_n , which in view of (K) yields $n \geq m/k$. (Alternatively, we can count the total number of bit changes in M' .) Further, we have $n \geq \log_2(m+1)$ since the $m+1$ columns of M' are distinct.

The bound $n(m, k) \leq \bar{n}(m, k)$ is trivial.

It remains to show the upper bound on $\bar{n}(m, k)$. Fix the minimal $n \in \mathbb{N}$ satisfying $m \leq 2^n - 1$ and $m \leq k(n - 3 \log_2 n)$ and consider an n -bit Gray code G as in Theorem 3.2. Then the $n \times (m+1)$ -matrix M' consisting of the first $m+1$ columns of G starts with the zero column and clearly satisfies condition (K') . By Lemma 3.3, M' also satisfies condition (J') . Thus, $n(m, k) \leq n$, from which the desired upper bound follows by elementary calculations. Indeed, if $n > \lceil \log_2(m+1) \rceil$ then, by minimality of n , $m/k > ((n-1) - 3 \log_2(n-1)) \geq (n-1)/4$ (the last inequality for $n \geq 8$) and thus

$$n-1 < m/k + 3 \log_2(n-1) < m/k + 3 \log_2(4m/k) = m/k + 3 \log_2(m/k) + 6.$$

\square

Proof of Theorem 1.2 The inequality $N(m, k) \leq \bar{N}(m, k)$ is clear in view of Proposition 2.3.I. The remaining inequalities follow from Proposition 2.5 and Theorem 3.1.

Proof of Theorem 1.1 The lower bounds on $N(m, k)$ and $\bar{N}(m, k)$ follow from Proposition 2.1. The upper bounds follow directly from Theorem 1.2.

Acknowledgments We thank Ludwig Bröcker, Martin Henk, Bettina Matzke and Claus Scheiderer for helpful discussions.

References

1. Andradas, C., Bröcker, L., Ruiz, J.M.: Constructible Sets in Real Geometry, *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*, vol. 33. Springer, Berlin (1996)

2. Averkov, G.: Representing elementary semi-algebraic sets by a few polynomial inequalities: a constructive approach (2008, preprint), arXiv:0804.2134
3. Averkov, G.: Notes on the algebra and geometry of polynomial representations. *Beiträge Algebra Geom.* **50**(1), 271–282 (2009)
4. Averkov, G., Bröcker, L.: Minimal polynomial descriptions of polyhedra and special semialgebraic sets (2010, preprint), arXiv:1002.0921v1
5. Averkov, G., Henk, M.: Three-dimensional polyhedra can be described by three polynomial inequalities. *Discret. Comput. Geom.* **42**, 166–186 (2009)
6. Averkov, G., Henk, M.: Representing simple d -dimensional polytopes by d polynomial inequalities. *Math. Program. (A)* (to appear, 2009), arXiv:0709.2099
7. Bochnak, J., Coste, M., Roy, M.-F.: *Real Algebraic Geometry*, *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*, vol. 36. Springer, Berlin (1998)
8. Bernig, A.: *Constructions for the theorem of Bröcker and Scheiderer*, Diplomarbeit, Universität Dortmund (1998)
9. Bosse, H., Grötschel, M., Henk, M.: Polynomial inequalities representing polyhedra. *Math. Program.* **103**(1, Ser. A), 35–44 (2005)
10. Goddyn, L., Gvozdjak, P.: Binary Gray codes with long bit runs. *Electron. J. Comb.* **10**, Research Paper 27, 10 pp. (electronic) (2003)
11. Grötschel, M., Henk, M.: The representation of polyhedra by polynomial inequalities. *Discret. Comput. Geom.* **29**(4), 485–504 (2003)
12. Henk, M.: Polynomdarstellungen von Polyedern. *Jber. Deutsch. Math.-Verein.* **109**(2), 51–69 (2007)
13. Henk, M., Matzke, B.: Representing polygons with polynomials of fixed degree. unpublished manuscript (2006)
14. Knuth, D.E.: *The art of computer programming*. In: *Generating All Tuples and Permutations*. vol. 4, Fasc. 2. Addison-Wesley, Upper Saddle River, NJ (2005)
15. Prestel, A.: *Model theory for the real algebraic geometer*. Dottorato di ricerca in matematica, Istituti editoriali e poligrafici internazionali, Dipartimento di matematica dell'università di Pisa (1998)
16. Savage, C.: A survey of combinatorial Gray codes. *SIAM Rev.* **39**(4), 605–629 (1997)
17. vom Hofe, G.: *Beschreibung von ebenen konvexen n -Ecken durch höchstens drei algebraische Ungleichungen*. Dissertation, Universität Dortmund (1992)