On the Complexity of Deciding Connectedness and Computing Betti Numbers of a Complex Algebraic Variety

Peter Scheiblechner [1]

Department of Mathematics, University of Paderborn, D-33095 Paderborn, Germany

Abstract

We extend the lower bounds on the complexity of computing Betti numbers proved in [6] to complex algebraic varieties. More precisely, we first prove that the problem of deciding connectedness of a complex affine or projective variety given as the zero set of integer polynomials is PSPACE-hard. Then we prove PSPACE-hardness for the more general problem of deciding whether the Betti number of fixed order of a complex affine or projective variety is at most some given integer.

Key words: connected components, Betti numbers, PSPACE, lower bounds

1 Introduction

It is shown in [8], that one can compute the number of connected components of a semialgebraic set given by integer polynomials in the complexity class FPSPACE, the class of Boolean functions computable by a Turing machine in polynomial space. The corresponding lower bound follows from work of Reif [13,14], thus the problem is indeed FPSPACE-complete. In [6] the stronger result for the problem restricted to compact real algebraic sets is proved (a gap in that proof will be filled in an appendix of this paper). In [7] also the PSPACE-completeness of the problem of deciding connectedness of the semilinear set described by an additive decision circuit is shown.

Email address: pscheib@math.uni-paderborn.de (Peter Scheiblechner).

[1] Partially supported by DFG grant BU 1371.

Since any complex algebraic variety can also be seen as a real algebraic set, it follows that the problem of counting the connected components of an algebraic variety over the complex numbers is also in FPSPACE. But clearly the corresponding lower bound does not follow from the results in [4,6,7]. Our goals in this paper are to prove that it is PSPACE-hard to decide if a complex variety is connected, and to generalise this hardness result to higher Betti numbers of fixed order. The inherent complexity of the latter problem is not as well understood as for the zeroth Betti number. The development of even single exponential time algorithms for computing all Betti numbers of a semialgebraic set is a major open problem. However, recent results of Basu [1] show that for fixed ℓ one can compute the first ℓ Betti numbers of a semialgebraic set in single exponential time. It is an interesting open question whether Basu's algorithm can be implemented in polynomial space.

1.1 Connectedness

We consider complex affine varieties $\mathcal{Z}(f_1, \ldots, f_r) \subseteq \mathbb{C}^n$ given as the zero set of finitely many polynomials $f_1, \ldots, f_r \in \mathbb{C}[X_1, \ldots, X_n]$, as well as complex projective varieties $\mathcal{Z}(f_1, \ldots, f_r) \subseteq \mathbb{P}^n$ given by homogeneous polynomials $f_1, \ldots, f_r \in \mathbb{C}[X_0, \ldots, X_n]$. Since we want to study our problems in the Turing model, we restrict to varieties given by polynomials with integer coefficients. A standard argument [5, Remark 6.3] shows that the complexity of the problems considered is not affected by changing the encoding of the input polynomials from dense to sparse or even straight-line program representation. To fix ideas we consider the *dense* representation, where a polynomial is represented by the vector of *all* of its coefficients. In [6] the *sparse* encoding was used, where only non-vanishing coefficients are listed together with the exponent vector of the corresponding monomial in binary. In [4,7] the semilinear sets where represented by *additive circuits*, which are algebraic circuits with arithmetic restriced to additions and subtractions.

Let us specify the exact formulation of our first problem.

CONN$_{\mathbb{C}}$ (*Connectedness of affine varieties*) Given polynomials $f_1, \ldots, f_r \in \mathbb{Z}[X_1, \ldots, X_n]$ in dense encoding, decide whether $\mathcal{Z}(f_1, \ldots, f_r) \subseteq \mathbb{C}^n$ is connected.

Our first main result is

Theorem 1.1 *The problem* CONN$_{\mathbb{C}}$ *is* PSPACE*-hard with respect to many-one reductions. More specifically, the problem remains* PSPACE*-hard when restricted to subspace arrangements, i.e., unions of affine subspaces.*

We will also prove a projective version of this theorem and conclude that the corresponding counting problems are FPSPACE-hard.

Our proof of Theorem 1.1 uses the strategy of [4], [6], and [7] together with some new ideas. Bürgisser and Cucker used the fact that each language in PSPACE can be decided by a symmetric Turing machine. Such a machine has a symmetric transition function and thus an undirected configuration graph. Hence deciding membership to the language is reduced to testing whether two given vertices in an undirected graph are connected, i.e., to the reachability problem. Note that this graph has an exponential number of vertices, but it can be described succinctly, i.e., by a Boolean circuit which decides adjacency of two given vertices. This configuration graph was represented in [4] as a semilinear set by mapping the vertices to points in real affine space and edges to the line segments between them. One can show that membership to this set can be decided by an additive circuit of polynomial size. In this way the reachability problem translates to the reachability problem in a succinctly given semilinear set, which in turn can be reduced to the problem of counting connected components as follows. One connects the two given points by new line segments obtaining a new semilinear set. Then the two points are connected in the original set if and only if the number of connected components does not change by this modification.

We modify this strategy in several respects. We avoid the use of symmetric Turing machines by observing that one can simply pass to the underlying undirected graph, since we are dealing with deterministic Turing machines (cf. Lemma 2.1). To be able to reduce to the problem of connectedness we construct from the given Turing machine a two-tape machine in order to obtain an acyclic configuration graph (cf. Lemma 3.1). Here special attention has to be paid to those configurations, which occur in no computation from any input. In this way, at the cost of a second tape, we gain the ability to transform the configuration graph into a forest of two trees. In this situation the reachability problem can easily be reduced to deciding connectedness. Since we are dealing with complex varieties, we embed these graphs into the complex affine or projective space by mapping edges to complex lines.

1.2 Betti Numbers

To formulate the generalisation to higher Betti numbers we introduce the following problems. For a topological space X we denote by $b_k(X)$ its kth Betti number with respect to singular homology.

BETTI$(k)_{\mathbb{C}}$ (*kth Betti number of affine varieties*) Given the polynomials $f_1, \ldots, f_r$ in $\mathbb{Z}[X_0, \ldots, X_n]$ in dense encoding and $b \in \mathbb{N}$, decide whether

$b_k(X) \leq b$, where $X = \mathcal{Z}(f_1, \ldots, f_r) \subseteq \mathbb{C}^n$.

PROJBETTI$(k)_{\mathbb{C}}$ (*kth Betti number of projective varieties*) Given homogeneous polynomials $f_1, \ldots, f_r \in \mathbb{Z}[X_0, \ldots, X_n]$ in dense encoding and $b \in \mathbb{N}$, decide whether $b_k(X) \leq b$, where $X = \mathcal{Z}(f_1, \ldots, f_r) \subseteq \mathbb{P}^n$.

Now we can state our second main result.

Theorem 1.2 *For each $k \in \mathbb{N}$ the problems* BETTI$(k)_{\mathbb{C}}$ *and* PROJBETTI$(k)_{\mathbb{C}}$ *are* PSPACE*-hard with respect to many-one reductions.*

We prove this theorem by induction on k. Clearly, the case $k = 0$ follows from Theorem 1.1 and its projective version. The induction step in the affine case is quite elementary and uses the idea of a similar result for semilinear sets given by additive circuits in [4].

For the projective result we treat the case $k = 1$ separately with the same reduction as for the case $k = 0$ by observing, that an additional edge from the leaf of a tree to its root introduces a cycle, whereas it does not, when the leaf is connected to the root of another tree. For the induction step we reduce PROJBETTI$(k)_{\mathbb{C}}$ to PROJBETTI$(k+2)_{\mathbb{C}}$. This reduction consists of the construction of the (algebraic) *suspension* $\Sigma(X)$ of a projective variety $X \subseteq \mathbb{P}^n$, which is defined as the join of X with an additional point p outside of $\mathbb{P}^n$. As an illustration consider the following toy example. Take X as being two distinct points in $\mathbb{P}^n$. Then the join of X with p is nothing else as the union of two lines meeting in p, thus topologically $S^2 \vee S^2$. One sees in this simple example that the zeroth Betti number of X agrees with the second Betti number of $\Sigma(X)$. This shift of the Betti numbers by 2 is generally true. This fact is shown in Appendix A.6, p. 78 of [9] for the more general construction of an m-fold cone (where the Betti numbers are shifted by $2m$), but only for the special case of a smooth variety. Here we will prove this result for possibly singular varieties for $m = 1$. In order to do so, we will construct the blow-up of $\Sigma(X)$ at p and show that this is a sphere bundle over X, whose homology can be computed with standard tools.

2 Preliminaries

In this section we fix some conventions and notations about Turing machines. Fix the input alphabet $\{0, 1\}$. Because of the construction mentioned above we use machines with several tapes. Let M be a deterministic k-tape Turing machine with set of states Q, starting state $q_0 \in Q$, tape alphabet Γ, and

transition function

$$\delta\colon (Q \setminus \{q_{\mathrm{acc}}, q_{\mathrm{rej}}\}) \times \Gamma^k \longrightarrow Q \times (\Gamma \times \mathcal{D})^k.$$

Here $q_{\mathrm{acc}}, q_{\mathrm{rej}} \in Q$ denote the accepting and rejecting state, respectively, and $\mathcal{D} := \{\leftarrow, -, \rightarrow\}$ denotes the set of possible movements of the read-write heads of M. Since we will not consider sub-linear space bounds, we do not require distinguished input- and output-tapes. We think of each tape as being infinite in both directions and filled up with blank symbols $\sqcup$, thus we assume $\{\sqcup, 0, 1\} \subseteq \Gamma$. At the beginning of the computation, all heads are placed at position 1, and an input word of length n is written on the first tape from position 1 to n. We can and will assume that the Turing machine operates only in the region of the tapes to the right of position 0 (the machine has to visit the cell at position 0 in order to detect the beginning of the word written on the tape). By the space demand of a computation we will mean the maximal number of cells the computation needs on each tape.

Let $p = p(n)$ be a space bound of M for a fixed input size $n \in \mathbb{N}$. A *configuration* of M is a $k \times (p+1)$-matrix c over the extended tape alphabet $\widetilde{\Gamma} := \Gamma \cup (\Gamma \times Q)$, whose rows correspond to the contents of the tapes, where the symbol at the head-position is replaced by the pair of that symbol and the current state, i.e., $c = (c^1, \ldots, c^k)^t$ with $c^\nu = (\sigma_0, \ldots, \sigma_{h-1}, (\sigma_h, q), \sigma_{h+1}, \ldots, \sigma_p)$, where $(\sigma_0, \ldots, \sigma_p)$ is the content and h is the head-position of the νth tape. Occasionally, we will call the tape positions 0 to p the *legal region* of the tape. We denote by $C_n \subseteq \widetilde{\Gamma}^{k \times (p+1)}$ the set of configurations of M. For $c, c' \in C_n$ we say that c *yields* c' and write $c \vdash c'$ iff c' is the resulting configuration after one computation step of M performed on c. The *configuration digraph* of M is defined to be the directed graph with vertex set C_n and an edge $(c, c') \in C_n^2$ iff $c \vdash c'$. We define the *configuration graph* G_n to be the undirected graph obtained from the configuration digraph by forgetting the orientation of the edges.

It is a standard method to decide membership of an input to the language decided by M by solving the reachability problem for the directed configuration graph. Now we observe that, in the case of deterministic Turing machines, we can consider the undirected configuration graph, since each path from an input to a final configuration automatically has to be directed.

Lemma 2.1 *Let the language $L \subseteq \{0,1\}^*$ be decided by the deterministic Turing machine M. For any input $w \in \{0,1\}^n$ let $i(w)$ be its unique start configuration. Then for all $w \in \{0,1\}^n$ there exists a path from $i(w)$ to an accepting configuration c_{acc} in the configuration graph of M iff $w \in L$.*

Proof. We have to prove the "only if" direction. Let $G_n = (C_n, E_n)$ denote the configuration graph of M. Let $c_0 = i(w), c_1, \ldots, c_m = c_{\mathrm{acc}}$ be a path

from the start to an accepting configuration, i.e., for each $1 \leq i \leq m$ we have $\{c_{i-1}, c_i\} \in E_n$. If (c_{i-1}, c_i) is an edge in the configuration digraph for all i, we have a directed path and are done. So let us assume that there exists an i such that (c_{i-1}, c_i) is not a directed edge. Let i_0 be the maximal index with this property. But then (c_{i_0}, c_{i_0-1}) is a directed edge. Since c_{acc} has no next configuration, we have $i_0 < m$. Hence (c_{i_0}, c_{i_0+1}) is a directed edge, and c_{i_0} has the two following configurations c_{i_0+1} and c_{i_0-1}, in contradiction to determinism, so no such i_0 exists. □

3 Obtaining an Acyclic Configuration Graph

Since we want to consider the problem of deciding connectedness, our aim is to construct from the configuration graph a variety with exactly two connected components. The problem is that there are configurations occurring in no computation from any input and thus behaving unpredictably. We modify the Turing machine appropriately to control this behaviour, in particular we achieve that the configuration digraph has no cycles. Unfortunately, this costs the use of a second tape. This modification is constructed in the following technical lemma.

Lemma 3.1 *Let M be a single-tape Turing machine with space bound $s(n)$ deciding the language $L \subseteq \{0,1\}$. Then there exists a 2-tape Turing machine N with space bound $p(n) = \mathcal{O}(s(n))$ deciding L with the following properties:*

(1) the configuration digraph of N has no cycles,
(2) the machine N operates in each step on one tape only,

Remark 3.2 *Note that after the modification of the above lemma there are also no undirected cycles in the configuration graph, since otherwise there would exist a configuration with two successors (similar as in the proof of Lemma 2.1).*

Proof. The idea is to count the computation steps of M in binary representation on the second tape ensuring that a computation starting on an arbitrary configuration never returns to that configuration. For this purpose we write the digits of the counter in reversed order on the tape and interpret all symbols except 1 as 0.

Now let $M = (Q, \Gamma, \delta, q_0, q_{\text{acc}}, q_{\text{rej}})$ be a Turing machine as in the lemma. We construct a new machine N by replacing each computation step of M with the following procedure, which increments the counter on tape 2. During this procedure we store the state of M as the first component of a pair, whose

second component controls the incremention as follows. The head of tape 2 moves to the right, replaces each 1 by 0 until the first symbol other than 1 is reached and replaces it by 1. Then it moves to the left until the first blank symbol $\sqcup$ is reached, and moves again one position to the right. During all this, nothing on tape 1 is changed. Finally, the postponed transition of M can be performed on the first tape.

Formally, the machine $N = (R, \Gamma, \varepsilon, q_0, q_{\text{acc}}, q_{\text{rej}})$ is defined as follows. Let

$$R := Q \,\dot\cup\, (Q^\times \times \{q_0', q_1', q_2'\}),$$

where $Q^\times := Q \setminus \{q_{\text{acc}}, q_{\text{rej}}\}$, and define

$$\varepsilon\colon (R \setminus \{q_{\text{acc}}, q_{\text{rej}}\}) \times \Gamma^2 \longrightarrow R \times (\Gamma \times \mathcal{D})^2$$

by

$$\begin{aligned}
\varepsilon(q, \sigma_1, \sigma_2) &:= \Big((q, q_0'), \sigma_1, -, \sigma_2, -\Big) && \forall\, q \in Q^\times, \sigma_1, \sigma_2 \in \Gamma,\\
\varepsilon\Big((q, q_0'), \sigma, 1\Big) &:= \Big((q, q_0'), \sigma, -, 0, \rightarrow\Big) && \forall\, q \in Q^\times, \sigma \in \Gamma,\\
\varepsilon\Big((q, q_0'), \sigma_1, \sigma_2\Big) &:= \Big((q, q_1'), \sigma_1, -, 1, -\Big) && \forall\, q \in Q^\times, \sigma_1, \sigma_2 \in \Gamma, \sigma_2 \neq 1,\\
\varepsilon\Big((q, q_1'), \sigma_1, \sigma_2\Big) &:= \Big((q, q_1'), \sigma_1, -, \sigma_2, \leftarrow\Big) && \forall\, q \in Q^\times, \sigma_1, \sigma_2 \in \Gamma, \sigma_2 \neq \sqcup,\\
\varepsilon\Big((q, q_1'), \sigma, \sqcup\Big) &:= \Big((q, q_2'), \sigma, -, \sqcup, \rightarrow\Big) && \forall\, q \in Q^\times, \sigma \in \Gamma,\\
\varepsilon\Big((q, q_2'), \sigma_1, \sigma_2\Big) &:= \Big(\delta(q, \sigma_1), \sigma_2, -\Big) && \forall\, q \in Q^\times, \sigma_1, \sigma_2 \in \Gamma.
\end{aligned}$$

It is clear that N decides the same language as M and uses space $p(n) = \mathcal{O}(s(n))$.

We now prove claim 1. First note that the subroutine described above cannot lead to any cycle, whatever the starting configuration is. Indeed, during this procedure the state of N can only change in the order $q \to (q, q_0') \to (q, q_1') \to (q, q_2') \to q'$ with some $q, q' \in Q$. Further, in the state (q, q_0') the head either moves to the right or the state changes, in the state (q, q_1') it moves either to the left or the state changes, in the state (q, q_2') the state changes anyway. In all cases the configuration changes, and at the end of the procedure it is different from the one at the beginning unless $\delta(q, \sigma_1) = (q, \sigma_1, -)$.

So consider a cycle $c_0, \ldots, c_m$ in the configuration digraph of M, i.e., $c_{i-1} \vdash c_i$ for all $1 \leq i \leq m$ and $c_0 = c_m$. Let h denote the head position and $u = (\sigma_0, \ldots, \sigma_p)$ the content of tape 2, where $p = p(n)$. We start with configuration $(c_0, c_0^1)^t$, where $c_0^1 := (\sigma_0, \ldots, \sigma_{h-1}, (\sigma_h, q), \sigma_{h+1}, \ldots, \sigma_p)$, and consider the following cases:

(1) $\sigma_h = \cdots = \sigma_p = 1$. Then the head on tape 2 goes on moving to the right until it leaves the legal region of the tape. Thus, we reach a vertex with outdegree 0.
(2) $\sigma_j \neq 1$ for some $h \leq j \leq p$ and $\sigma_i = \sqcup$ for some $0 \leq i < h$. Let i_0 be the maximal such i and j_0 the minimal such j. Then the head moves to the right switching 1's to 0 as in case 1. Reaching position j_0, the head writes 1, enters state (q, q'_1), moves to the left until it reaches position i_0, enters state (q, q'_2), moves to the right, and enters the state of c_1. Thus, after this procedure the configuration $(c_0, c_0^1)^t$ has changed to $(c_1, c_1^1)^t$ with $c_1^1 := (\sigma_0, \ldots, \sigma_{i_0}, (\sigma'_{i_0+1}, q'), \sigma'_{i_0+2}, \ldots, \sigma'_p)$, where $(\sigma'_h, \ldots, \sigma'_{j_0})$ represents the binary number one bigger than $(\sigma_h, \ldots, \sigma_{j_0})$. Note that at the end the head can be placed to the left of the original position, so that the whole tape content can represent a number different than the original number plus one. But nevertheless, the number on the tape has become greater.
(3) $\sigma_j \neq 1$ for some $h \leq j \leq p$ and $\sigma_i \neq \sqcup$ for all $0 \leq i < h$. Then the machine begins as in case 2, but as the head moves to the left, it does not find any blank symbol, so that it leaves the legal region of the tape to the left.

In this way N runs through a sequence of configurations $(c_0, c_0^1)^t, (c_1, c_1^1)^t, \ldots$, each of which is different from the preceeding ones, since the numbers on tape 2 strictly increase. This process ends at some point with case 1 or case 3 above, where a final configuration is reached. Thus, claim 1 follows. Claim 2 is obvious by construction. □

4 Embedding the Configuration Graph

In order to transfer combinatorial to topological properties, we have to represent the configuration graph as a variety. In this section we study a technique to do so. In [4] an undirected graph has been embedded in real affine space by mapping vertices to points and edges to line segments joining them. Here we map vertices to points in affine or projective space and edges to lines through the two points corresponding to the vertices of that edge. Let K be either $\mathbb{R}$ or $\mathbb{C}$. Let $\mathbb{A}^n = \mathbb{A}^n(K)$ and $\mathbb{P}^n = \mathbb{P}^n(K)$ denote the affine or projective n-dimensional space over K, respectively. Two distinct points $x, y \in \mathbb{A}^n(\mathbb{P}^n)$ define a unique line $\ell(x, y)$ containing x and y. In the affine case we have $\ell(x, y) = \{tx + (1-t)y \,|\, t \in K\}$, and in the projective case $\ell(x, y) = \{sx + ty \,|\, s, t \in K\}$.

Let $G = (V, E)$ be a graph and $\varphi\colon V \longrightarrow \mathbb{A}^n(\mathbb{P}^n)$ an injective map. We assign to each edge $e = \{u, v\} \in E$ the line $\varphi(e) := \ell(\varphi(u), \varphi(v))$.

Definition 4.1 *The injective map* $\varphi\colon V \longrightarrow \mathbb{A}^n(\mathbb{P}^n)$ induces an embedding *of the graph* $G = (V, E)$ *into* $\mathbb{A}^n(\mathbb{P}^n)$ *iff*

(i) $\forall v \in V, e \in E\ (\varphi(v) \in \varphi(e) \Rightarrow v \in e)$,
(ii) $\forall e, e' \in E\ (e \cap e' = \emptyset \Rightarrow \varphi(e) \cap \varphi(e') = \emptyset)$.

The edge skeleton $\varphi(G)$ *of the embedding is defined as the union of the lines corresponding to all edges of* G.

In other words, condition (i) says that each line $\varphi(e)$ meets only the images of vertices adjacent to e, whereas the condition (ii) states that images of disjoint edges don't intersect. It is clear that a map fulfilling these conditions preserves all combinatorial properties of the graph, in particular two vertices are connected in the graph iff their images are connected in the edge skeleton.

As in Section 2 let M be a k-tape Turing machine with space bound $p = p(n)$, and C_n its set of configurations. We adopt the notations from there, in particular recall that the extended tape alphabet $\widetilde{\Gamma} = \Gamma \cup (\Gamma \times Q)$ was defined on page 5. Now let S denote the vector space with basis $\widetilde{\Gamma}$ over K, i.e., $S = \bigoplus_{\gamma \in \widetilde{\Gamma}} K\gamma$. Define furthermore $V_n := \bigoplus_{\nu=1}^{k} \bigoplus_{i=0}^{p} S$. This means that for each tape, each head position, and each symbol we have a basis vector, so that if we write $\gamma \in V_n$ for some $\gamma \in \widetilde{\Gamma}$, γ "remembers" its tape number and position on the tape. We have $\dim V_n = k|\widetilde{\Gamma}|(p(n)+1) = \mathcal{O}(p(n))$. Now define the map

$$\varphi\colon C_n \longrightarrow V_n,\ (c_i^\nu) \mapsto \sum_{\nu=1}^{k} \sum_{i=0}^{p} c_i^\nu.$$

It is clear that φ is injective. Recall that G_n denotes the configuration graph of M.

Lemma 4.2 *Let* M *be a Turing machine which operates in each step on only one tape. Then the map* φ *induces an embedding of* G_n *into* V_n.

Proof. (i) Let $c \in C_n$ be a configuration and $e = \{d, \widetilde{d}\}$ be an edge in the configuration graph with $\varphi(c) \in \varphi(e)$. Then there exists $t \in K$ with

$$\sum_{\nu,i} c_i^\nu = \varphi(c) = t\varphi(d) + (1-t)\varphi(\widetilde{d}) = \sum_{\nu,i} (td_i^\nu + (1-t)\widetilde{d}_i^\nu),$$

hence $c_i^\nu = td_i^\nu + (1-t)\widetilde{d}_i^\nu$ for all ν, i. Thus $c_i^\nu, d_i^\nu, \widetilde{d}_i^\nu$ are linearly dependent basis vectors, so that at least two of them must coincide. Since $d \neq \widetilde{d}$, there exist ν, i with $d_i^\nu \neq \widetilde{d}_i^\nu$. Then $c_i^\nu \in \{d_i^\nu, \widetilde{d}_i^\nu\}$, and $t \in \{0, 1\}$. From this it follows, say $\varphi(c) = \varphi(d)$, and from injectivity $c = d$.

(ii) Let $e = \{c, d\}$ and $\widetilde{e} = \{\widetilde{c}, \widetilde{d}\}$ be edges with $\varphi(e) \cap \varphi(\widetilde{e}) \neq \emptyset$. We have to

show that $e \cap \widetilde{e} \neq \emptyset$. By assumption there exist $s, t \in K$ with

$$\sum_{\nu,i}(sc_i^\nu+(1-s)d_i^\nu) = s\varphi(c)+(1-s)\varphi(d) = t\varphi(\widetilde{c})+(1-t)\varphi(\widetilde{d}) = \sum_{\nu,i}(t\widetilde{c}_i^\nu+(1-t)\widetilde{d}_i^\nu),$$

hence $sc_i^\nu+(1-s)d_i^\nu = t\widetilde{c}_i^\nu+(1-t)\widetilde{d}_i^\nu$ for all ν, i. Now, if $s \in \{0,1\}$ or $t \in \{0,1\}$, then the claim follows from (i), so let's assume $s, t \notin \{0,1\}$. If $c_i^\nu = d_i^\nu$, then $c_i^\nu = t\widetilde{c}_i^\nu + (1-t)\widetilde{d}_i^\nu$, and since $t \notin \{0,1\}$ it follows $c_i^\nu = \widetilde{c}_i^\nu = \widetilde{d}_i^\nu$. By symmetry, we have for all ν, i

$$c_i^\nu = d_i^\nu \quad \Leftrightarrow \quad \widetilde{c}_i^\nu = \widetilde{d}_i^\nu \quad \Rightarrow \quad c_i^\nu = d_i^\nu = \widetilde{c}_i^\nu = \widetilde{d}_i^\nu. \tag{1}$$

In the case $c_i^\nu \neq d_i^\nu$ we have $c_i^\nu \in \{\widetilde{c}_i^\nu, \widetilde{d}_i^\nu\}$, since $s \neq 0$, and analogously $d_i^\nu \in \{\widetilde{c}_i^\nu, \widetilde{d}_i^\nu\}$. So we have for all ν, i

$$c_i^\nu \neq d_i^\nu \quad \Rightarrow \quad \{c_i^\nu, d_i^\nu\} = \{\widetilde{c}_i^\nu, \widetilde{d}_i^\nu\}. \tag{2}$$

By assumption, the Turing machine operates only on one tape, say on tape ν, so that on all other tapes the content and head position do not change. It follows that at most two entries of the configurations c and d differ (similarly for $\widetilde{c}$ and $\widetilde{d}$). We distinguish two cases.

(1) In the transition $c \vdash d$ the head on tape ν does not move, say it stays at position h. Say, the state changes (possibly) from q to q', and the symbol σ_1 is replaced by σ_1'. Thus, if we write all entries of a configurations in one line, we have the picture

$$\begin{array}{l} c: c_0^1 \cdots c_{h-1}^\nu \ (\sigma_1, q) \ c_{h+1}^\nu \cdots c_p^k \\ \top \\ d: c_0^1 \cdots c_{h-1}^\nu \ (\sigma_1', q') \ c_{h+1}^\nu \cdots c_p^k. \end{array}$$

From condition (1) it follows that the two configurations of the transition $\widetilde{c} \vdash \widetilde{d}$ have the same entries as c in all positions except (ν, h). Condition (2) implies that in position (ν, h) the same entries occur, possibly in different order. Hence, if they occur in the same order, we have that $c = \widetilde{c}$, if they occur in reversed order, $c = \widetilde{d}$.

(2) In the transition $c \vdash d$ the head on tape ν moves from position h, say to the right (the other case is treated similarly). Let the state change from q to q', the symbol σ_1 be replaced by σ_1', and σ_2 be the symbol at position $h+1$. Thus, we have

$$\begin{array}{l} c: c_0^1 \cdots c_{h-1}^\nu \ (\sigma_1, q) \quad \sigma_2 \quad c_{h+2}^\nu \cdots c_p^k \\ \top \\ d: c_0^1 \cdots c_{h-1}^\nu \quad \sigma_1' \quad (\sigma_2, q') \ c_{h+2}^\nu \cdots c_p^k. \end{array}$$

As above, from conditions (1) and (2) it follows that except for the trivial cases $c = \widetilde{c}$ and $c = \widetilde{d}$ we have, say

$$\begin{array}{l} \widetilde{c}: c_0^1 \cdots c_{h-1}^\nu \ (\sigma_1, q) \ (\sigma_2, q') \ c_{h+2}^\nu \cdots c_p^k \\ \top \\ \widetilde{d}: c_0^1 \cdots c_{h-1}^\nu \quad \sigma_1' \qquad \sigma_2 \quad c_{h+2}^\nu \cdots c_p^k. \end{array}$$

These are obviously no legal configurations. □

Now we derive an embedding into projective space. Let $P_n := \mathbb{P}(V_n)$ denote the projectivisation of V_n, i.e., the set of all one-dimensional linear subspaces. Then we have the canonical projection $\pi\colon V_n \setminus \{0\} \longrightarrow P_n$, mapping $x \neq 0$ to the linear span of x. Now define

$$\widetilde{\varphi}\colon C_n \longrightarrow P_n, \quad \widetilde{\varphi} := \pi \circ \varphi, \tag{3}$$

where φ is defined as above. Since the image vectors of φ are pairwise linearly independent, $\widetilde{\varphi}$ is injective. Furthermore, the following projective version of Lemma 4.2 follows with an almost identical proof, one only has to replace the coefficients $1 - t$ and $1 - s$ by new parameters t' and s', respectively.

Lemma 4.3 *Let M be a Turing machine which operates in each step on only one tape. Then the map $\widetilde{\varphi}$ induces an embedding of G_n into P_n.*

5 Computing Equations for the Embedded Graph

In this section we give explicit equations describing the edge skeletons of the embeddings constructed in the last section. Moreover, we will see that in case of a polynomial space Turing machine one can construct these equations in polynomial time (or even logarithmic space). Note that this is non-trivial, because the configuration graph of such a machine has exponentially many vertices and therefore edges, thus the straight-forward method would lead to an exponential number of equations. The following technique has some resemblance with the proof of the Theorem of Cook and Levin. We begin with the affine embedding.

Let M be a deterministic k-tape Turing machine. We use the notations of Sections 2 and 4. Recall that $V_n = \bigoplus_{\nu,i} S$, where $S = \bigoplus_{\gamma \in \widetilde{\Gamma}} K\gamma$. Thus, the vector space V_n is given by a natural basis consisting of $k(p+1)$ copies of the elements of $\widetilde{\Gamma}$, thus each element $x \in V_n$ can be written uniquely as a sum $x = \sum_{\nu=1}^{k} \sum_{i=0}^{p} \sum_{\gamma \in \widetilde{\Gamma}} x_{i\gamma}^\nu \gamma$, so we will use the $x_{i\gamma}^\nu$ as coordinates. We will identify a point $\sum_\gamma x_{i\gamma}^\nu \gamma \in S$ with the vector $(x_{i\gamma}^\nu)_\gamma$ and denote both by x_i^ν.

Let $X_{i\gamma}^{\nu}$ for $1 \leq \nu \leq k,\ 0 \leq i \leq p,\ \gamma \in \widetilde{\Gamma}$ be indeterminates, and denote by $X_i^{\nu} := (X_{i\gamma}^{\nu})_{\gamma \in \widetilde{\Gamma}}$ a family of indeterminates.

In the following a statement as $X_i^{\nu} \in A$ for an algebraic subset $A \subseteq S$ is a concise way to express that the point of S described by the coordinate vector x_i^{ν} belongs to A. For instance, $X_i^{\nu} \in \Gamma$ will mean that there exists $\sigma \in \Gamma$ such that $X_{i\sigma}^{\nu} = 1$ and $X_{i\gamma}^{\nu} = 0$ for all $\gamma \in \widetilde{\Gamma} \setminus \{\sigma\}$. Thus it says that at position i of tape ν there is a symbol of Γ.

To formulate the equations we construct an embedded graph describing all possible local transitions of M from one configuration to another. For this purpose we will introduce some notations. We set $\Delta := \widetilde{\Gamma} \setminus \Gamma = \Gamma \times Q$. We call a $k \times 2$-matrix $\Sigma = (\Sigma_i^{\nu}) \in \widetilde{\Gamma}^{k \times 2}$ a *window*. A pair of windows $(\Sigma, \widetilde{\Sigma})$ is called a *legal transition* iff there exist $q, q' \in Q$, $\sigma_1^1, \ldots, \sigma_1^k, \widetilde{\sigma}_1^1, \ldots, \widetilde{\sigma}_1^k, \sigma_2^1, \ldots, \sigma_2^k \in \Gamma$, and $D_1, \ldots, D_k \in \mathcal{D} = \{\leftarrow, -, \rightarrow\}$ such that

(i) $\delta(q, \sigma_1^1, \ldots, \sigma_1^k) = (q', \widetilde{\sigma}_1^1, \ldots, \widetilde{\sigma}_1^k, D_1, \ldots, D_k)$,
(ii) for all $1 \leq \nu \leq k$ we have

$$\begin{aligned}
D_\nu = \rightarrow \quad &\Rightarrow \quad (\Sigma_1^\nu, \Sigma_2^\nu) = ((\sigma_1^\nu, q), \sigma_2^\nu) \wedge (\widetilde{\Sigma}_1^\nu, \widetilde{\Sigma}_2^\nu) = (\widetilde{\sigma}_1^\nu, (\sigma_2^\nu, q')), \\
D_\nu = - \quad &\Rightarrow \quad (\Sigma_1^\nu, \Sigma_2^\nu) = ((\sigma_1^\nu, q), \sigma_2^\nu) \wedge (\widetilde{\Sigma}_1^\nu, \widetilde{\Sigma}_2^\nu) = ((\widetilde{\sigma}_1^\nu, q'), \sigma_2^\nu), \\
D_\nu = \leftarrow \quad &\Rightarrow \quad (\Sigma_1^\nu, \Sigma_2^\nu) = (\sigma_2^\nu, (\sigma_1^\nu, q)) \wedge (\widetilde{\Sigma}_1^\nu, \widetilde{\Sigma}_2^\nu) = ((\sigma_2^\nu, q'), \widetilde{\sigma}_1^\nu).
\end{aligned}$$

We call a window Σ *legal*, iff there exists a window $\widetilde{\Sigma}$ such that $(\Sigma, \widetilde{\Sigma})$ or $(\widetilde{\Sigma}, \Sigma)$ is a legal transition. Let $W \subseteq \widetilde{\Gamma}^{k \times 2}$ denote the set of legal windows.

We define the graph T with vertex set W and an edge $\{\Sigma, \widetilde{\Sigma}\}$ for each legal transition $(\Sigma, \widetilde{\Sigma})$. We embed T into $S^k \oplus S^k$ via the map

$$\vartheta \colon W \longrightarrow \bigoplus_{\nu=1}^{k} \bigoplus_{i=1}^{2} S,\ \Sigma \mapsto \sum_{\nu,i} \Sigma_i^\nu.$$

Now let $\Theta := \vartheta(T)$ denote the edge skeleton of this embedding. Note that this graph does not depend on the input length, and it is in particular describable by a fixed set of equations.

Lemma 5.1 *The edge skeleton $\varphi(G_n)$ can be described by the following formula:*

$$\bigwedge_{\nu} \bigwedge_{i<j<\ell} (X_i^\nu \in \Gamma \vee X_j^\nu \in \Gamma \vee X_\ell^\nu \in \Gamma) \wedge \tag{4}$$

$$\bigwedge_{\nu} \bigwedge_{i+1<j} (X_i^\nu \in \Gamma \vee X_j^\nu \in \Gamma) \wedge \tag{5}$$

$$\bigwedge_{\nu} \left(\sum_i \sum_{\gamma \in \Delta} X_{i\gamma}^\nu = 1 \right) \wedge \tag{6}$$

$$\bigwedge_{1<i_1,\ldots,i_k<p} (F_{i_1,\ldots,i_k} \vee G_{i_1,\ldots,i_k}), \tag{7}$$

where

$$F_{i_1,\ldots,i_k} := \bigvee_{d\in\{-1,0\}^k} \Big((X^1_{i_1+d_1},\ldots,X^k_{i_k+d_k},X^1_{i_1+d_1+1},\ldots,X^k_{i_k+d_k+1}) \in \Theta \wedge \bigwedge_\nu X^\nu_{i_\nu+(-1)^{d_\nu+1}} \in \Gamma \Big)$$

and

$$G_{i_1,\ldots,i_k} := \bigvee_\nu \Big((X^\nu_{i_\nu-1}, X^\nu_{i_\nu}) \in \Gamma^2 \vee (X^\nu_{i_\nu}, X^\nu_{i_\nu+1}) \in \Gamma^2 \Big).$$

Furthermore, the above formula can be expressed as a conjunction of $p^{\mathcal{O}(1)}$ equations of degree bounded by a constant.

Proof. First let $x = \sum_{\nu,i} x^\nu_i$ with $x^\nu_i \in S$ be an element of the edge skeleton $\varphi(G_n)$. We have to show that it satisfies the formula above. There exist configurations $c, \widetilde{c} \in C_n$ and $t \in K$ with $c \vdash \widetilde{c}$ and

$$x = t\varphi(c) + (1-t)\varphi(\widetilde{c}) = \sum_{\nu,i} (tc^\nu_i + (1-t)\widetilde{c}^\nu_i),$$

where $c = (c^\nu_i)_{\nu,i}$ and $\widetilde{c} = (\widetilde{c}^\nu_i)_{\nu,i}$. It follows $x^\nu_i = tc^\nu_i + (1-t)\widetilde{c}^\nu_i$ for all ν, i. Let h_ν denote the head position on tape ν in configuration c, and $D_\nu \in \{-1,0,1\}$ correspond to the movement of the head. Then for all $i \notin \{h_\nu, h_\nu + D_\nu\}$ we have $c^\nu_i = \widetilde{c}^\nu_i \in \Gamma$, thus

$$x^\nu_i = tc^\nu_i + (1-t)c^\nu_i = c^\nu_i \in \Gamma$$

for those i, hence (4) and (5). By the same reason we have $\sum_{\gamma\in\Delta} x^\nu_{i\gamma} = 0$ for all $i \notin \{h_\nu, h_\nu + D_\nu\}$. To compute the sum for these special indices, assume first that the head on tape ν moves (say, to the right). To simplify notation, let $\gamma_1 := c^\nu_{h_\nu}$, $\gamma_2 := c^\nu_{h_\nu+1}$, $\widetilde{\gamma}_1 := \widetilde{c}^\nu_{h_\nu}$, and $\widetilde{\gamma}_2 := \widetilde{c}^\nu_{h_\nu+1}$. Then it follows $\gamma_1 \in \Delta$, $\gamma_2 \in \Gamma$, $\widetilde{\gamma}_1 \in \Gamma$, and $\widetilde{\gamma}_2 \in \Delta$, hence

$$\sum_{\gamma\in\Delta} x^\nu_{h_\nu\gamma} = x^\nu_{h_\nu\gamma_1} = t, \quad \sum_{\gamma\in\Delta} x^\nu_{h_\nu+1,\gamma} = x^\nu_{h_\nu+1,\widetilde{\gamma}_2} = 1-t,$$

and (6) follows in this case. If the head on tape ν stays at position h_ν, then $\gamma_2 = \widetilde{\gamma}_2 \in \Gamma$ and $\gamma_1, \widetilde{\gamma}_1 \in \Delta$. Hence,

$$\sum_{\gamma\in\Delta} x^\nu_{i_\nu\gamma} = x^\nu_{h_\nu\gamma_1} + x^\nu_{h_\nu\widetilde{\gamma}_1} = 1,$$

and (6) follows also in this case. It remains to show formula (7). Let $1 < i_1, \ldots, i_k < p$, and assume that $G_{i_1,\ldots,i_k}$ is not satisfied. This implies $\forall\nu\ x^\nu_{i_\nu} \notin$

Γ, i.e., the head stays at position i_ν or moves from/to this position. Define $d_\nu := \min\{h_\nu, h_\nu + D_\nu\} - i_\nu$. Then $d_\nu \in \{-1, 0\}$, and $i_\nu + d_\nu$ is the leftmost position which is affected by the transition. It follows, that the windows

$$\Sigma := \begin{pmatrix} c^1_{i_1+d_1} & c^1_{i_1+d_1+1} \\ \vdots & \vdots \\ c^k_{i_k+d_k} & c^k_{i_k+d_k+1} \end{pmatrix}, \quad \widetilde{\Sigma} := \begin{pmatrix} \widetilde{c}^1_{i_1+d_1} & \widetilde{c}^1_{i_1+d_1+1} \\ \vdots & \vdots \\ \widetilde{c}^k_{i_k+d_k} & \widetilde{c}^k_{i_k+d_k+1} \end{pmatrix}$$

are legal and $(\Sigma, \widetilde{\Sigma})$is a legal transition. Thus, (7) follows.

To show the other direction, let $x = \sum_{\nu,i} x^\nu_i$ with $x^\nu_i \in S$ be an element of V_n satisfying equations (4) to (7). From (4) it follows that for all ν at most two of the components $x^\nu_i \notin \Gamma$, and from (5) that these must be located at neighbouring positions. Hence, there exist i_ν such that $x^\nu_i \in \Gamma$ for all $i \notin \{i_\nu, i_\nu + 1\}$ holds. Chose i_ν to be the maximal indices with this property. From (6) we have

$$\sum_i \sum_{\gamma\in\Delta} x^\nu_{i\gamma} = \sum_{\gamma\in\Delta} (x^\nu_{i_\nu,\gamma} + x^\nu_{i_\nu+1,\gamma}) = 1,$$

hence $x^\nu_{i_\nu} \notin \Gamma$ or $x^\nu_{i_\nu+1} \notin \Gamma$ for all ν. By maximality it follows $x^\nu_{i_\nu} \notin \Gamma$. Then $G_{i_1,\dots,i_k}$ is not fulfilled, so that $F_{i_1,\dots,i_k}$ has to be. Hence, there exist $d_1, \dots, d_k \in \{-1, 0\}$, a legal transition of windows $(\Sigma, \widetilde{\Sigma})$, and $t \in K$ with

$$\sum_\nu x^\nu_{i_\nu+d_\nu} + \sum_\nu x^\nu_{i_\nu+d_\nu+1} = t \sum_{\nu,i=1,2} \Sigma^\nu_i + (1-t) \sum_{\nu,i=1,2} \widetilde{\Sigma}^\nu_i = \sum_{\nu,i=1,2} (t\Sigma^\nu_i + (1-t)\widetilde{\Sigma}^\nu_i),$$

hence $x^\nu_{i_\nu+d_\nu} = t\Sigma^\nu_1 + (1-t)\widetilde{\Sigma}^\nu_1$ and $x^\nu_{i_\nu+d_\nu+1} = t\Sigma^\nu_2 + (1-t)\widetilde{\Sigma}^\nu_2$ for all ν. Furthermore $x^\nu_{i_\nu+(-1)^{d_\nu+1}} \in \Gamma$, which just means, that the one of the three components $x^\nu_{i_\nu-1}, x^\nu_{i_\nu}, x^\nu_{i_\nu+1}$, which is not yet determined, must be an element of Γ. Now we can define the two configurations $c := (c^\nu_i)_{\nu,i}$ and $\widetilde{c} := (\widetilde{c}^\nu_i)_{\nu,i}$ as follows. Set $j_\nu := i_\nu + d_\nu$,

$$c^\nu_i := \begin{cases} x^\nu_i, \text{ if } i \notin \{j_\nu, j_\nu + 1\} \\ \Sigma^\nu_1, \text{ if } i = j_\nu \\ \Sigma^\nu_2, \text{ if } i = j_\nu + 1 \end{cases}, \quad \widetilde{c}^\nu_i := \begin{cases} x^\nu_i, \text{ if } i \notin \{j_\nu, j_\nu + 1\} \\ \widetilde{\Sigma}^\nu_1, \text{ if } i = j_\nu \\ \widetilde{\Sigma}^\nu_2, \text{ if } i = j_\nu + 1 \end{cases}.$$

Then it is clear that $c \vdash \widetilde{c}$ and

$$\begin{aligned} x &= \sum_{\nu,i} x^\nu_i \\ &= \sum_{\nu,i\neq j_\nu,j_\nu+1} c^\nu_i + \sum_\nu (tc^\nu_{j_\nu} + (1-t)\widetilde{c}^\nu_{j_\nu}) + \sum_\nu (tc^\nu_{j_\nu+1} + (1-t)\widetilde{c}^\nu_{j_\nu+1}) \\ &= t\varphi(c) + (1-t)\varphi(\widetilde{c}). \end{aligned}$$

It remains to transform the formula into a conjunction of equations. First note that both Γ and Θ can be described by fixed sets of equations. Using the general equivalence

$$\bigvee_{i=1}^{s} (f_{i1} = 0 \wedge \cdots \wedge f_{it} = 0) \quad \Leftrightarrow \quad \bigwedge_{1 \le j_1, \ldots, j_s \le t} f_{1j_1} \cdots f_{sj_s} = 0 \tag{8}$$

one can write the formulas (4) and (5) as a conjunction of $\mathcal{O}(p^3)$ equations of bounded degree. Formula (6) is already a conjunction of $\mathcal{O}(p)$ linear equations. Since the total number of equations involved in formula $F_{i_1,\ldots,i_k}$ is constant, the rule (8) yields a conjunction of a constant number of equations of bounded degree. The same holds for $G_{i_1,\ldots,i_k}$. It follows that formula (7) is a conjunction of $\mathcal{O}(p^k)$ equations of bounded degree. □

Remark 5.2 *It should be clear that (under the condition that $p(n)$ can be computed in space logarithmic in n) on input n, the equations of the above lemma in dense encoding can be computed in space logarithmic in $p(n)$.*

Now we give the corresponding equations for the projective embedding. Similarly as above we will write $X_i^\nu \in A$ with an algebraic subset $A \subseteq P_n$ for the statement, that the point given by the homogeneous coordinates x_i^ν lies in A. For instance, $X_i^\nu \in \pi(\Gamma)$, where $\pi\colon V_n \setminus \{0\} \longrightarrow P_n$ denotes the canonical projection, means that there exists $\sigma \in \Gamma$ such that $X_{i\sigma}^\nu \neq 0$ and $X_{i\gamma}^\nu = 0$ for all $\gamma \in \widetilde{\Gamma} \setminus \{\sigma\}$.

Lemma 5.3 *The edge skeleton $\widetilde{\varphi}(G_n)$ can be described by the following formula:*

$$\bigwedge_\nu \bigwedge_{i<j<\ell} (X_i^\nu \in \pi(\Gamma) \vee X_j^\nu \in \pi(\Gamma) \vee X_\ell^\nu \in \pi(\Gamma)) \wedge \tag{9}$$

$$\bigwedge_\nu \bigwedge_{i+1<j} (X_i^\nu \in \pi(\Gamma) \vee X_j^\nu \in \pi(\Gamma)) \wedge \tag{10}$$

$$\bigwedge_\nu \bigwedge_i \left(\sum_{\gamma \in \widetilde{\Gamma}} X_{i\gamma}^\nu = \sum_j \sum_{\gamma \in \Delta} X_{j\gamma}^\nu \right) \wedge \tag{11}$$

$$\bigwedge_{1<i_1,\ldots,i_k<p} (F_{i_1,\ldots,i_k} \vee G_{i_1,\ldots,i_k}), \tag{12}$$

where

$$F_{i_1,\ldots,i_k} := \bigvee_{d \in \{-1,0\}^k} \Big((X_{i_1+d_1}^1, \ldots, X_{i_k+d_k}^k, X_{i_1+d_1+1}^1, \ldots, X_{i_k+d_k+1}^k) \in \pi(\Theta) \wedge \bigwedge_\nu X_{i_\nu+(-1)^{d_\nu+1}}^\nu \in \pi(\Gamma) \Big)$$

and

$$G_{i_1,\ldots,i_k} := \bigvee_{\nu} \Big((X^{\nu}_{i_\nu - 1}, X^{\nu}_{i_\nu}) \in \pi(\Gamma)^2 \vee (X^{\nu}_{i_\nu}, X^{\nu}_{i_\nu + 1}) \in \pi(\Gamma)^2 \Big) \Big).$$

Furthermore, the above formula can be expressed as a conjunction of $p^{\mathcal{O}(1)}$ homogeneous equations of degree bounded by a constant.

Proof. Note that formulas (9), (10), and (12) are analogous to the affine versions (4), (5), and (7), only formula (11) is substantially different from (6). Formula (6) ensures that on each tape there exists a position containing a non-symbol. In the projective case formula (11) has an additional task. It has to ensure that all the coordinates which are non-zero by the other homogeneous equations, have the correct value.

The proof is similar to the proof of Lemma 5.1, we therefore only point out the differences. Let $x = \sum_{\nu,i} x^{\nu}_i$ with $x^{\nu}_i \in S$ be a representative of the point $\pi(x) \in \widetilde{\varphi}(G_n)$, i.e., there exist configurations $c = (c^{\nu}_i)_{\nu,i}$ and $\widetilde{c} = (\widetilde{c}^{\nu}_i)_{\nu,i}$ and $s, t \in K$ with $c \vdash \widetilde{c}$ and

$$x = s\varphi(c) + t\varphi(\widetilde{c}) = \sum_{\nu,i} (sc^{\nu}_i + t\widetilde{c}^{\nu}_i).$$

Formulas (9), (10), and (12) are derived analogously as in the proof of Lemma 5.1. To prove (11), note that $\sum_{\gamma} x^{\nu}_{i\gamma} = s + t$ for all ν, i. Similarly as in the affine case we get $\sum_j \sum_{\gamma \in \Delta} x^{\nu}_{j\gamma} = s + t$, hence (11).

On the other hand, let $x = \sum_{\nu,i} x^{\nu}_i$ with $x^{\nu}_i \in S$ be an element of V_n satisfying equations (9) to (12). As in the proof of Lemma 5.1 it follows that for all ν there exist i_ν with $x^{\nu}_{i_\nu} \notin \pi(\Gamma)$ and $t^{\nu}_i \neq 0$, $\sigma^{\nu}_i \in \Gamma$ such that $x^{\nu}_i = t^{\nu}_i \sigma^{\nu}_i$ for all $i \notin \{i_\nu, i_\nu + 1\}$. From (11) we have that for each ν all the t^{ν}_i have the same value, say $u^{\nu} \in K^{\times}$. As in the affine case we obtain $d_1, \ldots, d_k \in \{-1, 0\}$, a legal transition of windows $(\Sigma, \widetilde{\Sigma})$, and $s, t \in K$ such that $x^{\nu}_{i_\nu + d_\nu} = s\Sigma^{\nu}_1 + t\widetilde{\Sigma}^{\nu}_1$ and $x^{\nu}_{i_\nu + d_\nu + 1} = s\Sigma^{\nu}_2 + t\widetilde{\Sigma}^{\nu}_2$ for all ν. Furthermore, from (11) it follows $u^{\nu} = s + t$ for all ν. Now we can define the two configurations $c := (c^{\nu}_i)_{\nu,i}$ and $\widetilde{c} := (\widetilde{c}^{\nu}_i)_{\nu,i}$ as in the proof of Lemma 5.1 and conclude $c \vdash \widetilde{c}$, as well as $x = s\varphi(c) + t\varphi(\widetilde{c})$.

The proof of the statement about the formula size is similar to the affine case. □

Remark 5.4 *Under the condition that $p(n)$ can be computed in logarithmic space, the equations of the above lemma in dense representation can be computed in space logarithmic in $p(n)$.*

6 Proof of Theorem 1.1

Now we use the constructions of Sections 4 and 5 for $K = \mathbb{C}$ to prove Theorem 1.1.

Proof. Let $L \in \mathsf{PSPACE}$. Then L can be decided by a deterministic 2-tape Turing machine M with the polynomial space bound $p(n)$ and the properties of Lemma 3.1. Let $G_n = (C_n, E_n)$ be the configuration graph of M for a fixed $n \in \mathbb{N}$, and $\varphi : C_n \longrightarrow V_n \simeq \mathbb{C}^m$ its embedding as defined in Section 4, where $m = 2|\widetilde{\Gamma}|(p(n)+1)$. The aim now is to construct a variety with exactly two connected components. For this purpose we modify the configuration graph by adding two new vertices a, r and connecting all accepting configurations with a and all other configurations with no successor with r. Formally, we proceed as follows. Let A and R denote the sets of accepting and rejecting configurations, respectively. Let further F be the set of configurations, where the next step would lead the head of some tape out of the legal region. Note that the sets A, R, and F can easily be described combinatorially. Now define the graph H_n with vertex set $D_n := \{a, r\} \dot\cup C_n$ and edge set $E_n \cup \{\{c, a\} \mid c \in A\} \cup \{\{c, r\} \mid c \in R \cup F\}$. We embed this graph into the vector space $W_n := \mathbb{C}a \oplus \mathbb{C}r \oplus V_n$ via the map

$$\psi\colon D_n \longrightarrow W_n, \quad c \mapsto \begin{cases} \varphi(c) & \text{if } c \in C_n, \\ c & \text{if } c \in \{a, r\}. \end{cases}$$

Now we construct our reduction as follows. Let $w \in \{0,1\}^n$ be an arbitrary input. Define the variety $Z_w := \psi(H_n) \cup \ell(\psi(i(w)), \psi(r)) \subseteq W_n$, where $i(w) \in C_n$ denotes the start configuration on input w. In other words, we connect the image point of the start configuration with the point where all rejecting paths end. Then we have by Lemma 2.1, that $w \in L$ iff $i(w)$ and an accepting configuration of M (i.e., an element of A) are connected in G_n, which in turn is equivalent to the property that $i(w)$ and a are connected in H_n. Since by Lemma 3.1 G_n has no cycles, and in H_n all vertices are connected to either a or r, H_n has exactly two connected components. As a result we have

$$w \in L \quad \Leftrightarrow \quad Z_w \text{ is connected.}$$

By Lemma 5.1 we can compute equations for $\varphi(G_n)$, and hence for Z_w in logarithmic space. Thus, the desired reduction is established. □

Now we consider the following problems.

$\#\mathrm{CC}_{\mathbb{C}}$ (*Counting connected components of affine varieties*) Given poly-

nomials $f_1, \ldots, f_r \in \mathbb{Z}[X_1, \ldots, X_n]$ in dense encoding, compute the number of connected components of $\mathcal{Z}(f_1, \ldots, f_r) \subseteq \mathbb{C}^n$.

PROJCONN$_{\mathbb{C}}$ (*Connectedness of projective varieties*) Given homogeneous polynomials $f_1, \ldots, f_r \in \mathbb{Z}[X_0, \ldots, X_n]$ in dense encoding, decide whether $\mathcal{Z}(f_1, \ldots, f_r) \subseteq \mathbb{P}^n$ is connected.

#PROJCC$_{\mathbb{C}}$ (*Counting connected components of projective varieties*) Given homogeneous polynomials $f_1, \ldots, f_r \in \mathbb{Z}[X_0, \ldots, X_n]$ in dense encoding, compute the number of connected components of $\mathcal{Z}(f_1, \ldots, f_r) \subseteq \mathbb{P}^n$.

An immediate consequence of Theorem 1.1 is

Corollary 6.1 *The problem* #CC$_{\mathbb{C}}$ *is* FPSPACE*-hard with respect to Turing reductions.*

Note that we understand FPSPACE to be the class of functions computable in polynomial space, whose output size is required to be polynomially bounded. This class was called FPSPACE(poly) in [12].

The following projective version of Theorem 1.1 is proved analogously.

Theorem 6.2 *The problem* PROJCONN$_{\mathbb{C}}$ *is* PSPACE*-hard with respect to many-one reductions.*

Corollary 6.3 *The problem* #PROJCC$_{\mathbb{C}}$ *is* FPSPACE*-hard with respect to Turing reductions.*

7 Proof of Theorem 1.2

Here we are going to prove Theorem 1.2. For the definition of Betti numbers we will use singular homology, i.e., the kth Betti number $b_k(X)$ of a topological space X is the rank of its kth singular homology group $H_k(X)$ with integer coefficients [11,15]. For topological spaces X and Y we write $X \approx Y$ if X is homeomorphic to Y, and $X \simeq Y$ if X is homotopy equivalent to Y.

7.1 The affine Case

To prove Theorem 1.2 for BETTI$(0)_{\mathbb{C}}$ we note that CONN$_{\mathbb{C}}$ is a special case of BETTI$(0)_{\mathbb{C}}$, hence this case follows from Theorem 1.1. For the induction step

we use the following construction inspired by a proof in [4]. Let $X \subseteq \mathbb{C}^n$ be an affine variety. Define

$$Z(X) := (X \times \mathbb{C}) \cup (\mathbb{C}^n \times \{\pm 1\})$$

as the union of the (complex) cylinder over X with the two hyperplanes $L^{\pm} := \mathbb{C}^n \times \{\pm 1\}$. Equations for $Z(X)$ are given by the equations for X multiplied by the polynomial $X_{n+1}^2 - 1$, so they are easy to compute. We denote by $\widetilde{b}_k(X)$ the rank of the kth reduced homology group $\widetilde{H}_k(X)$. Note that the reduced homology is defined only in the case $X \neq \emptyset$.

Proposition 7.1 *For each $k \in \mathbb{N}$ and $X \neq \emptyset$ we have*

$$\widetilde{b}_k(X) = \widetilde{b}_{k+1}(Z(X)) \quad \textit{and} \quad b_k(\emptyset) = b_{k+1}(Z(\emptyset)) = 0.$$

Recall that if $X \neq \emptyset$, then $\widetilde{b}_0(X) = b_0(X) - 1$ and $\widetilde{b}_k(X) = b_k(X)$ for all $k > 0$. Hence it follows from the proposition that the map $X \mapsto (Z(X), 0)$ is a many-one reduction from $\textsc{Conn}_{\mathbb{C}}$ to $\textsc{Betti}(1)_{\mathbb{C}}$. Similarly the map $(X, b) \mapsto (Z(X), b)$ reduces $\textsc{Betti}(k)_{\mathbb{C}}$ to $\textsc{Betti}(k+1)_{\mathbb{C}}$ for $k > 0$.

Proof of Proposition 7.1. We first treat the case $X = \emptyset$. Then $Z(X)$ is just the union $L^+ \cup L^-$, hence $0 = b_k(\emptyset) = b_{k+1}(Z(\emptyset))$ for all $k \in \mathbb{N}$.

We prove the case $X \neq \emptyset$ by a Mayer-Vietoris argument guided by the intuition for the corresponding construction over the reals. Let $U^+ \subseteq \mathbb{C}$ be the open halfplane defined by $\operatorname{Im} z > -\varepsilon$, and analogously $U^- \subseteq \mathbb{C}$ defined by $\operatorname{Im} z < \varepsilon$, where $0 < \varepsilon < 1$. Then define the two open subsets

$$U := (X \times U^+) \cup L^+ \quad \text{and} \quad V := (X \times U^-) \cup L^-$$

of $Z(X)$. Then it is clear that $U \cup V = Z(X)$ and $U \cap V \simeq X$. It is also easy to see that U and V are contractible (contract $X \times U^+$, say, to $X \times \{1\} \subseteq L^+$). The Mayer-Vietoris sequence for reduced homology [15, §4.6] yields

$$\cdots \to \widetilde{H}_{k+1}(U) \oplus \widetilde{H}_{k+1}(V) \to \widetilde{H}_{k+1}(U \cup V) \to \widetilde{H}_k(U \cap V) \to \widetilde{H}_k(U) \oplus \widetilde{H}_k(V),$$

hence

$$0 \longrightarrow \widetilde{H}_{k+1}(Z(X)) \longrightarrow \widetilde{H}_k(X) \longrightarrow 0,$$

from which the claim follows. □

7.2 The projective Case

The proof of Theorem 1.2 for $\textsc{ProjBetti}(k)_{\mathbb{C}}$ is more involved. As a first step we consider $\textsc{ProjBetti}(1)_{\mathbb{C}}$. For this purpose we need the following

Lemma 7.2 *Let $T = (V, E)$ be a tree and $\varphi\colon V \longrightarrow \mathbb{P}^m$ induce an embedding of T. Then $H_1(\varphi(T)) = 0$.*

Proof. We show this by induction on the number N of vertices. The cases $N = 0, 1$ are trivial, so let $T = (V, E)$ be a tree on $N+1$ vertices, and $\varphi\colon V \longrightarrow \mathbb{P}^m$ induce an embedding of T. Let v be a leaf of T, e the unique edge adjacent to v and consider the subgraph $S := (V \setminus \{v\}, E \setminus \{e\})$. Further, denote $X := \varphi(T)$, let U_v be a contractible open neighbourhood of $\varphi(v)$ in $\varphi(e) \approx S^2$, and $U_S := X \setminus \{\varphi(v)\}$. Then U_S is homotopy equivalent to $\varphi(S)$, and $X = U_v \cup U_S$. A portion of the Mayer-Vietoris sequence for the excisive couple (U_v, U_S) is

$$H_1(U_v) \oplus H_1(U_S) \longrightarrow H_1(X) \longrightarrow H_0(U_v \cap U_S) \xrightarrow{f} H_0(U_v) \oplus H_0(U_S),$$

where $f = (i_*, -j_*)$ with the inclusions $i\colon U_v \cap U_S \longrightarrow U_v$ and $j\colon U_v \cap U_S \longrightarrow U_S$. Now, $H_1(U_v) \simeq H_1(U_S) \simeq 0$ by contractibility and induction hypothesis. Further, $U_v \cap U_S$, U_v, and U_S are connected, hence we have the exact sequence

$$0 \longrightarrow H_1(X) \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z} \oplus \mathbb{Z}.$$

Since the kernel of f is trivial, $H_1(X) \simeq 0$ follows. □

Proposition 7.3 *The problem* ProjBetti$(1)_{\mathbb{C}}$ *is* PSPACE*-hard.*

Proof. We will use basically the same reduction as in the proof of Theorem 1.1. Let H_n, W_n, and ψ as defined there. Consider the projective space $\mathbb{P}(W_n)$ and define $\widetilde{\psi} := \pi \circ \psi$, where $\pi\colon W_n \setminus \{0\} \longrightarrow \mathbb{P}(W_n)$ denotes the canonical projection. Let $Z_w := \widetilde{\psi}(H_n) \cup \ell(\widetilde{\psi}(i(w)), \widetilde{\psi}(r))$ and recall that H_n is a forest with two trees rooted at a and r, respectively. Let T_a and T_r denote these trees. All we have to prove is the following:

$$w \in L \quad \Leftrightarrow \quad b_1(Z_w) = 0. \tag{13}$$

To do so, view Z_w as the edge skeleton under the embedding $\widetilde{\psi}$ of the graph H_n with an additional edge between r and $i(w)$. Let this modified graph be M_w.

For the first implication of (13) let $w \in L$. Then $i(w)$ is a leaf in T_a. In M_w this leaf is connected to the root of T_r, thus M_w is a tree and the claim follows from Lemma 7.2.

For the other implication of (13) assume $w \notin L$, hence $i(w)$ is a leaf in T_r. Since the Betti numbers are additive on connected components and a tree has vanishing first Betti number by Lemma 7.2, we can consider the graph $\widetilde{M}_w := M_w \setminus T_a$. Let e denote the unique edge in T_r adjacent to $i(w)$ and $e' := \{i(w), r\}$ the special edge connecting the leaf to the root. Denote $X :=$

$\widetilde{\psi}(\widetilde{M}_w)$ and $p := \widetilde{\psi}(i(w))$. Let U_p be a contractible open neighbourhood of p in $\widetilde{\psi}(e) \cup \widetilde{\psi}(e') \approx S^2 \vee S^2$, and $U_r := X \setminus \{p\}$. Then U_r is homotopy equivalent to the edge skeleton of a tree, hence has trivial first homology. Furthermore, we have $U_p \cup U_r = X$ and $U_p \cap U_r \simeq S^1 \dot{\cup} S^1$. The Mayer-Vietoris sequence yields

$$H_1(U_p) \oplus H_1(U_r) \longrightarrow H_1(X) \longrightarrow H_0(U_p \cap U_r) \xrightarrow{f} H_0(U_p) \oplus H_0(U_r),$$

where f is defined as in the proof of Lemma 7.2. We have $H_1(U_p) \simeq H_1(U_r) \simeq 0$, $H_0(U_p \cap U_r) \simeq \mathbb{Z} \oplus \mathbb{Z}$, thus

$$0 \longrightarrow H_1(X) \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \xrightarrow{f} \mathbb{Z} \oplus \mathbb{Z}$$

is exact. The map f is given by $f(x, y) = (x + y, -x - y) = (x + y)(1, -1)$, thus its kernel is isomorphic to $\mathbb{Z}$, hence $H_1(X) \simeq \mathbb{Z}$. □

To prove the corresponding result for higher Betti numbers we utilise the following construction. Let $X \subseteq \mathbb{P}^n$ be a projective variety, and embed $\mathbb{P}^n \subseteq \mathbb{P}^{n+1}$ via $(x_0 : \cdots : x_n) \mapsto (x_0 : \cdots : x_n : 0)$. The (algebraic) *suspension* $\Sigma(X) \subseteq \mathbb{P}^{n+1}$ is by definition the join of X with one point in $\mathbb{P}^{n+1} \setminus \mathbb{P}^n$, say $p := (0 : \cdots : 0 : 1)$, i.e., $\Sigma(X)$ is the union of all lines in $\mathbb{P}^{n+1}$ joining some point $x \in X$ with p. The suspension is described by the same equations as X, now considered as polynomials in $\mathbb{C}[X_0, \ldots, X_{n+1}]$. Thus, the computation of the suspension is trivial.

For us, the crucial property of the suspension is the following shift of Betti numbers.

Proposition 7.4

$$b_k(X) = b_{k+2}(\Sigma(X)) \quad \textit{for all } k \in \mathbb{N}. \tag{14}$$

With Proposition 7.4 it is clear that the mapping $(X, b) \mapsto (\Sigma(X), b)$ is a reduction from $\textsc{ProjBetti}(k)_{\mathbb{C}}$ to $\textsc{ProjBetti}(k+2)_{\mathbb{C}}$. Together with Theorem 6.2 and Proposition 7.3 this proves Theorem 1.2.

Remark 7.5 *One can carry out an analogous construction over* $\mathbb{R}$*. In this way one gets an alternative proof for the* FPSPACE*-hardness of the problem to compute the* k*th Betti number of a real projective or affine algebraic set.*

To prepare for the proof of Proposition 7.4 we will construct the blow-up of $\Sigma(X)$ and show that it is a sphere bundle over X. We proceed as follows.

Consider the projection centered at p as a rational map $\mathbb{P}^{n+1} \dashrightarrow \mathbb{P}^n$, and let $\varphi\colon \Sigma(X) \dashrightarrow X$ denote its restriction to $\Sigma(X)$. Now we define $\widetilde{\Sigma}(X) \subseteq$

$\mathbb{P}^{n+1} \times \mathbb{P}^n$ to be the graph of φ, i.e., the closure of the graph of $\varphi|\Sigma(X) \setminus \{p\}$ in $\mathbb{P}^{n+1} \times \mathbb{P}^n$. Let $q\colon \widetilde{\Sigma}(X) \longrightarrow \mathbb{P}^{n+1}$ be the restriction of the projection onto the first factor, which is a closed map by compactness. This map (or simply the space $\widetilde{\Sigma}(X)$) is called the *blow-up* of $\Sigma(X)$ at p (cf. [10]). The set $U := q^{-1}(\Sigma(X) \setminus \{p\})$ is dense in $\widetilde{\Sigma}(X)$, and

$$q\colon \widetilde{\Sigma}(X) \longrightarrow \Sigma(X) \tag{15}$$

is a surjection mapping U homeomorphically onto $\Sigma(X) \setminus \{p\}$. Now consider the special fibre $E := q^{-1}(p)$. Then q induces a homeomorphism

$$\widetilde{\Sigma}(X)/E \xrightarrow{\approx} \Sigma(X).$$

We also note that $E = \{(p, x) \,|\, x \in X\}$. Indeed, for $x \in X$ we have

$$(p, x) = \lim_{s \to 0} \underbrace{((sx : 1), x)}_{\in U}, \tag{16}$$

and this point lies in the closure of U, hence in E. On the other hand, each point in U is of the form $((sx : t), x)$ with $s, t \in \mathbb{C}$, $s \neq 0$ and $x \in X$. Since each point $(p, x) \in E$ can be written as a limit of points in U, it follows $x \in X$.

Our aim is to apply the Thom-Gysin sequence to $\widetilde{\Sigma}(X)$. In order to do this we have to prove that it is an orientable sphere bundle in the sense of orientation according to [15, p. 259], which applies to general q-sphere bundles $\xi = (\pi\colon \dot{E} \longrightarrow X)$. To define this notion, construct the corresponding $(q+1)$-disc bundle $E \longrightarrow X$ with $\partial E = \dot{E}$. By definition E is the mapping cylinder of the bundle projection π together with the retraction of E to X as the new bundle projection. By an *orientation class* of the q-sphere bundle ξ we mean a class $U \in H^{q+1}(E, \dot{E})$ with the property that its restriction U_x to each fibre pair $(E_x, \dot{E}_x) \approx (D^{q+1}, S^q)$ over x generates $H^{q+1}(E_x, \dot{E}_x) \simeq \mathbb{Z}$. If such a class U_ξ exists, ξ is called *orientable*, and in this case (ξ, U_ξ) is called an *oriented* q-sphere bundle.

Lemma 7.6 *Let $\xi = (\pi\colon \dot{E} \longrightarrow X)$ be an oriented q-sphere bundle, and $Y \subseteq X$ a subspace. Then $\pi^{-1}(Y) \longrightarrow Y$ is also an orientable q-sphere bundle.*

Proof. Let $\dot{F} := \pi^{-1}(Y)$, and $F \longrightarrow Y$ be the corresponding $q+1$-disc bundle. Then the claim follows immediately from the fact, that the diagram

$$\begin{array}{ccc} (E_x, \dot{E}_x) & \hookrightarrow & (E, \dot{E}) \\ \| & & \uparrow \\ (F_x, \dot{F}_x) & \hookrightarrow & (F, \dot{F}) \end{array}$$

commutes for each $x \in Y$. □

Lemma 7.7 *The space $\widetilde{\Sigma}(X)$ is an orientable 2-sphere bundle over X.*

Proof. Define $\pi\colon \widetilde{\Sigma}(X) \longrightarrow X$ to be the restriction of the projection $\mathrm{pr}_2\colon \mathbb{P}^{n+1}\times \mathbb{P}^n \longrightarrow \mathbb{P}^n$ onto the second factor.

To show that $\widetilde{\Sigma}(X)$ is locally trivial we use coordinates $X_0,\dots,X_n$ for $\mathbb{P}^n$ and $Z_0,\dots,Z_{n+1}$ for $\mathbb{P}^{n+1}$. Set $U_i := X \cap \{X_i \neq 0\} \subseteq X \subseteq \mathbb{P}^n$ and $V_i := \pi^{-1}(U_i)$ for $0 \leq i \leq n$. Then $V_i = \widetilde{\Sigma}(X) \cap (\mathbb{P}^{n+1} \times \{X_i \neq 0\})$. Now define the maps

$$\varphi_i\colon V_i \longrightarrow U_i \times \mathbb{P}^1, \quad (z,x) \mapsto (x,(z_i : z_{n+1})), \tag{17}$$

as well as

$$\psi_i\colon U_i \times \mathbb{P}^1 \longrightarrow V_i, \quad (x,(s:t)) \mapsto ((sx : tx_i),x).$$

One easily checks that these maps are inverse to each other, hence φ_i is a homeomorphism.

It remains to show that $\widetilde{\Sigma}(X)$ is orientable. Denote by $D(X) \longrightarrow X$ the 3-disc bundle corresponding to $\widetilde{\Sigma}(X)$. To prove the existence of an orientation class, we use the embedding of X in the smooth complex manifold $\mathbb{P}^n$, i.e., we consider the diagram

$$\begin{array}{ccc} (D(X),\widetilde{\Sigma}(X)) & \subseteq & (D(\mathbb{P}^n),\widetilde{\Sigma}(\mathbb{P}^n)) \\ \downarrow & & \downarrow \\ X & \subseteq & \mathbb{P}^n, \end{array}$$

where the spaces on the right are smooth, hence orientable (as manifolds). Then it is well-known that there exists the *Thom class* $\tau \in H^3(D(\mathbb{P}^n),\widetilde{\Sigma}(\mathbb{P}^n))$ [3, p. 368]. Since $\mathbb{P}^n$ is also connected, it follows from Corollary 11.6 of [3, p. 370] that the restriction of τ to the fibre $(D(\mathbb{P}^n)_x,\widetilde{\Sigma}(\mathbb{P}^n)_x)$ of each point $x \in X$ is a generator. Hence the Thom class serves as an orientation class for $\widetilde{\Sigma}(\mathbb{P}^n)$ in the above sense. It follows from Lemma 7.6 that $\widetilde{\Sigma}(X) \longrightarrow X$ is also orientable. □

Proof of Proposition 7.4. Because of Lemma 7.7 we can apply the Thom-Gysin sequence (Theorem 11 from Section 5.7 of [15, p. 260]) to the orientable 2-sphere bundle $\widetilde{\Sigma}(X) \longrightarrow X$ and get the exact sequence

$$\cdots \longrightarrow H_k(X) \xrightarrow{\rho} H_{k+2}(\widetilde{\Sigma}(X)) \xrightarrow{\pi_*} H_{k+2}(X) \xrightarrow{\Psi} H_{k-1}(X) \longrightarrow \cdots$$

The embedding $i\colon X \longrightarrow \widetilde{\Sigma}(X),\ x \mapsto (p,x)$ satisfies $\pi \circ i = \mathrm{id}_X$, hence $\pi_* \circ i_* = \mathrm{id}_{H_*(X)}$, thus π_* is surjective. Then Ψ is the zero map, hence ρ is injective, and we get the short exact sequence

$$0 \longrightarrow H_k(X) \longrightarrow H_{k+2}(\widetilde{\Sigma}(X)) \longrightarrow H_{k+2}(X) \longrightarrow 0, \tag{18}$$

which splits by i_*. It follows

$$H_{k+2}(\widetilde{\Sigma}(X)) = H_{k+2}(X) \oplus H_k(X) \quad \text{for } k \in \mathbb{Z}. \tag{19}$$

To compute the homology of $\Sigma(X)$ recall that it is homeomorphic to the quotient space $\widetilde{\Sigma}(X)/E$. We want to apply Theorem 2.13 from [11, p. 114], where we need the following technical condition.

Claim $E = i(X)$ is a deformation retract of a neighbourhood in $\widetilde{\Sigma}(X)$.
Let $D \subseteq \mathbb{P}^1$ be an open disc around $(0 : 1)$. Define $\widetilde{D} := \bigcup_{i=0}^{n} \varphi_i^{-1}(U_i \times D)$, where the φ_i are the trivialisations defined in (17). Then $\widetilde{D}$ is an open neighbourhood of E, and for all $(z, x) \in \widetilde{D}$ we have $z_{n+1} \neq 0$. Now define

$$r \colon \widetilde{D} \longrightarrow E, \quad (z, x) \mapsto (p, x).$$

Then $r \circ i = \mathrm{id}_E$, thus r is a retraction. To show that r is homotopic to the identity on $\widetilde{D}$, define

$$H \colon [0, 1] \times \widetilde{D} \longrightarrow \widetilde{D}, \quad H_t(z, x) := ((tz_0 : \cdots : tz_n : z_{n+1}), x).$$

Then H is continuous, and we have $H_0(z, x) = ((0 : z_{n+1}), x) = (p, x) = r(z, x)$, as well as $H_1(z, x) = (z, x)$ for all $(z, x) \in \widetilde{D}$. Thus, the claim is proved.

Now we can apply Theorem 2.13 from [11, p. 114], and get the following exact sequence.

$$\cdots \longrightarrow H_{k+2}(X) \xrightarrow{i_*} H_{k+2}(\widetilde{\Sigma}(X)) \xrightarrow{q_*} H_{k+2}(\Sigma(X)) \xrightarrow{\partial} H_{k+1}(X) \longrightarrow \cdots$$

Here $q \colon \widetilde{\Sigma}(X) \longrightarrow \Sigma(X)$ is the projection (15). The above sequence is originally formulated for the reduced homology, but we restrict to the case $k \geq 0$.

Now we use (19) and deduce from (18), that $\ker q_* = \operatorname{im} i_* = H_{k+2}(X)$ via the isomorphism (19). Hence, q_* induces an injective map $H_k(X) \longrightarrow H_{k+2}(\Sigma(X))$. Since i_* is injective, we have $0 = \ker i_* = \operatorname{im} \partial$, hence $\ker \partial = H_{k+2}(\Sigma(X)) = \operatorname{im} q_*$, thus q_* is surjective. It follows

$$H_k(X) = H_{k+2}(\Sigma(X)) \quad \text{for } k \geq 0,$$

completing the proof of Proposition 7.4. □

A The Real Reachability Problem

In this appendix we prove that the reachability problem for compact real algebraic sets is PSPACE-hard. This fills a gap in the original FPSPACE-hardness

proof for the problem of counting the connected components of real algebraic sets in [6]. There the Lemmas 8.14 and 8.15 are false, which are used to prove Proposition 8.16. We prove this proposition here with different methods. Note that in this appendix we use the sparse encoding of polynomials to match the setting of [6]. However, since the sparse size is bounded by the dense size, this amounts in a relaxation of the result.

Let us first state the precise problem. We denote by $\mathcal{Z}_{\mathbb{R}}(f_1, \ldots, f_r)$ the real affine zero set of the polynomials $f_1, \ldots, f_r \in \mathbb{R}[X_1, \ldots, X_n]$.

REACH$_{\mathbb{R}}$ (*Reachability of real algebraic varieties*) Given sparse polynomials $f, g, h \in \mathbb{Z}[X_1, \ldots, X_n]$, decide whether there exist points $p \in \mathcal{Z}_{\mathbb{R}}(f, g)$ and $q \in \mathcal{Z}_{\mathbb{R}}(f, h)$ which lie in the same connected component of $\mathcal{Z}_{\mathbb{R}}(f)$.

We denote by CREACH$_{\mathbb{R}}$ the same problem restricted to the case where $\mathcal{Z}_{\mathbb{R}}(f)$ is compact. We prove the following

Proposition A.1 *The problem* CREACH$_{\mathbb{R}}$ *is* PSPACE*-hard with respect to many-one reductions.*

Proof. Since projective varieties are compact, we use the projective embedding of Section 4 and a standard realisation of the real projective space as an affine variety. So let M be a polynomial space Turing machine (with one tape) deciding the language L. We can assume that M has only one accepting configuration c_{acc}. Let the real projective space P_n and the map $\widetilde{\varphi}\colon C_n \longrightarrow P_n$ be defined as in (3) with $K = \mathbb{R}$. According to Lemmas 4.3 and 5.3 this map induces an embedding of the configuration graph of M, and its edge skeleton can be described by equations, whose dense representation can be computed in space logarithmic in n. Let m be the dimension of the projective space P_n, so that $P_n \simeq \mathbb{P}^m$. It is well known (see for instance [2]) that $\mathbb{P}^m$ is homeomorphic to the following subvariety of the set of real $(m+1) \times (m+1)$-matrices

$$W_m := \{A \in \mathbb{R}^{(m+1)\times(m+1)} \mid A = A^t,\ A = A^2,\ \mathrm{tr}A = 1\}.$$

The homeomorphism maps a line in $\mathbb{R}^{m+1}$ to the matrix describing the orthogonal projection onto the line with respect to the standard basis. It is explicitly given by

$$h\colon \mathbb{P}^m \longrightarrow W_m,\ (x_0 : \cdots : x_m) \mapsto \left(\frac{x_i x_j}{\langle x, x\rangle}\right)_{i,j},$$

where $\langle \cdot, \cdot \rangle$ denotes the standard scalar product on $\mathbb{R}^{m+1}$. Now let $Z \subseteq \mathbb{P}^m$ be an algebraic variety given by the homogeneous polynomials $f_1, \ldots, f_r \in$

$\mathbb{R}[X_0, \ldots, X_m]$. Then its image $h(Z) \subseteq W_m \subseteq \mathbb{R}^{(m+1)^2}$ is given as follows

$$h(Z) = \{A = (a_{ij}) \in W_m \mid \bigwedge_{i=1}^{r} \bigwedge_{j=0}^{m} f_i(a_{0j}, \ldots, a_{mj}) = 0\}. \tag{A.1}$$

Indeed, let $x \in \mathbb{P}^m$ be some zero of $f_1, \ldots, f_r$. Then

$$\begin{aligned} f_i(h(x)_{0j}, \ldots, h(x)_{mj}) &= f_i\left(\frac{x_j}{\langle x, x\rangle} x_0, \ldots, \frac{x_j}{\langle x, x\rangle} x_m\right) \\ &= \left(\frac{x_j}{\langle x, x\rangle}\right)^{\deg f_i} f_i(x) = 0 \end{aligned}$$

for all i, j. On the other hand, let $A \in W_m$ be some matrix satisfying equations (A.1). This means that all column vectors of A lie in Z, which are just the images of the canonical basis vectors under the linear map described by A. Hence the line $\ell \subseteq \mathbb{R}^{m+1}$ which is the image of the projection defined by A lies in Z, i.e., $h^{-1}(A) = \ell \in Z$.

Now we describe the desired reduction. On input $w \in \{0,1\}^n$ we can compute the homogeneous equations in sparse encoding for the edge skeleton $\widetilde{\varphi}(G_n) \subseteq \mathbb{P}^m$ of the configuration graph, use these equations to construct equations for $Z := h(\widetilde{\varphi}(G_n)) \subseteq \mathbb{R}^{(m+1)^2}$ according to (A.1), and use the usual sum-of-squares trick to obtain one integer polynomial f describing Z. Furthermore, we take the two configurations $i(w)$ and c_{acc}, compute their images $p_w := h(\widetilde{\varphi}(i(w)))$ and $q_{\mathrm{acc}} := h(\widetilde{\varphi}(c_{\mathrm{acc}}))$ explicitly, from which we can easily compute polynomials g and h describing the points implicitly, i.e., $\mathcal{Z}_{\mathbb{R}}(g) = \{p_w\}$ and $\mathcal{Z}_{\mathbb{R}}(h) = \{q_{\mathrm{acc}}\}$. Then it is clear that the map $w \mapsto (f, g, h)$ is computable in logarithmic space and $w \in L$ iff $(f, g, h) \in \mathrm{CREACH}_{\mathbb{R}}$. □

Acknowledgment. I would like to thank my advisor Prof. Peter Bürgisser for suggesting the study of these problems, providing basic ideas and many helpful discussions.

References

[1] S. Basu. Computing the first few Betti numbers of semi-algebraic sets in single exponential time. *J. Symbolic Comput.*, 41(10):1125–1154, 2006.

[2] J. Bochnak, M. Coste, and M. F. Roy. *Real Algebraic Geometry*, volume 36 of *Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge*. Springer Verlag, 1998.

[3] G. E. Bredon. *Topology and geometry*, volume 139 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1997.

[4] P. Bürgisser and F. Cucker. Counting complexity classes for numeric computations I: Semilinear sets. *SIAM J. Comp.*, 33:227–260, 2003.

[5] P. Bürgisser and F. Cucker. Variations by complexity theorists on three themes of Euler, Bézout, Betti, and Poincaré. In Jan Krajicek, editor, *Complexity of computations and proofs*, volume 13 of *Quaderni di Matematica*, pages 73–152. Department of Mathematics, Seconda Università di Napoli, Caserta, Napoli, Italy, 2005.

[6] P. Bürgisser and F. Cucker. Counting complexity classes for numeric computations II: Algebraic and semialgebraic sets. *J. Compl.*, 22:147–191, 2006.

[7] P. Bürgisser, F. Cucker, and P. de Naurois. The complexity of semilinear problems in succinct representation. *Comp. Compl.*, 15(3):197–235, 2006.

[8] J. Canny. Some algebraic and geometric computations in PSPACE. In *Proc. 20th Ann. ACM STOC*, pages 460–467, 1988.

[9] E. M. Friedlander and B. Mazur. Filtrations on the homology of algebraic varieties. *Mem. Amer. Math. Soc.*, 110(529):ix+110, 1994.

[10] J. Harris. *Algebraic geometry*, volume 133 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992.

[11] A. Hatcher. *Algebraic topology*. Cambridge University Press, Cambridge, 2002.

[12] R. E. Ladner. Polynomial space counting problems. *SIAM J. Comp.*, 18(6):1087–1097, 1989.

[13] J. H. Reif. Complexity of the mover's problem and generalizations. In *Proc. 20th FOCS*, pages 421–427, 1979.

[14] J. H. Reif. Complexity of the generalized mover's problem. In J.T. Schwartz, M. Sharir, and J. Hopcroft, editors, *Planning, Geometry and Complexity of Robot Motion*, pages 267–281. Ablex Publishing Corporation, 1987.

[15] E. H. Spanier. *Algebraic Topology*. McGraw-Hill Series in Higher Mathematics. McGraw-Hill Book Company, New York, 1966.