Explicit SoS lower bounds from high-dimensional expanders

Irit Dinur*  Yuval Filmus†  Prahladh Harsha‡  Madhur Tulsiani§

Abstract

We construct an explicit family of 3XOR instances which is hard for $O(\sqrt{\log n})$ levels of the Sum-of-Squares hierarchy. In contrast to earlier constructions, which involve a random component, our systems can be constructed explicitly in deterministic polynomial time.

Our construction is based on the high-dimensional expanders devised by Lubotzky, Samuels and Vishne, known as LSV complexes or Ramanujan complexes, and our analysis is based on two notions of expansion for these complexes: cosystolic expansion, and a local isoperimetric inequality due to Gromov.

Our construction offers an interesting contrast to the recent work of Alev, Jeronimo and the last author (FOCS 2019). They showed that 3XOR instances in which the variables correspond to vertices in a high-dimensional expander are easy to solve. In contrast, in our instances the variables correspond to the edges of the complex.

1 Introduction

We describe a new family of instances of 3XOR, based on high-dimensional expanders, that are hard for the Sum-of-Squares (SoS) hierarchy of semidefinite programming relaxations, which is the most powerful algorithmic framework known for optimizing over constraint satisfaction problems. Unlike previous constructions of 3XOR hard instances for SoS, our construction is explicit, as it is based on the explicit construction of high-dimensional expanders due to Lubotzky, Samuels and Vishne [LSV05a, LSV05b], which we refer to henceforth as LSV complexes.

Theorem 1.1. There exists a constant $\mu \in (0, 1)$ and an infinite family of 3XOR instances on $n$ variables, constructible in deterministic polynomial time, satisfying the following:

- No assignment satisfies more than $1 - \mu$ fraction of the constraints.

- Relaxations obtained by $O(\sqrt{\log n})$ levels of the SoS hierarchy fail to refute the instances.
We also remark that our construction can be used to obtain explicit integrality gap instances for various other optimization problems, using reductions in the SoS hierarchy [Tul09]. In particular, while our instances on the LSV complexes exhibit an integrality gap of $1 - \mu$ vs. $1$ for the SoS hierarchy, reductions can be used to obtain explicit 3XOR instances with a gap of $1/2 + \varepsilon$ vs. $1 - \varepsilon$ for any $\varepsilon > 0$. Indeed, this yields explicit hard instances with optimal gaps for all approximation resistant predicates based on pairwise independent subgroups [Cha16].

**Structured instances from High-dimensional expanders.** High-dimensional expanders (HDXs) are a high-dimensional analog of expander graphs. In recent years they have found a variety of applications in theoretical computer science, such as efficient CSP optimization [AJT19], improved sampling algorithms [ALGV19, ALG20, AL20], quantum LDPC codes [EKZ20, KT20], novel lattice constructions [KM18], direct sum testing [GK19], and others. Explicit constructions of HDXs have also led to improved list-decoding algorithms [DHKNT19, AJQST20] and to sparser agreement tests [DKi17, DD19]. In this work, we show how these explicit constructions can be used to construct explicit hard instances for SoS.

High-dimensional expanders are bounded-degree (hyper)graphs (or rather, simplicial complexes) with certain expansion properties. A simplicial complex is a non-empty collection of down-closed sets. Given a simplicial complex $X$, we will refer by $X(i)$ the family of all $i$-dimensional sets in $X$ (i.e., sets of size $i + 1$). The dimension of the simplicial complex $X$ is the maximal dimension of any set in it. It will be convenient to refer to the sets of dimension 0, 1, 2, 3 as vertices, edges, triangles, tetrahedra, respectively. Thus, a graph $G = (V, E)$ is a 1-dimensional complex, while in this work we will be using complexes of dimension at least 2. Given a 2-dimensional complex $X = (X(0), X(1), X(2))$, there are two natural ways to construct a 3XOR instance based on $X$ — a vertex-variable construction and an edge-variable construction. Let $\beta : X(2) \to \mathbb{F}_2$ be any $\mathbb{F}_2$-valued function on the set $X(2)$ of triangles.

**Vertex-variable construction:** The 3XOR instance corresponding to $(X, \beta)$ consists of the following constraints: $x_u + x_v + x_w = \beta_{\{u,v,w\}}$ for each $\{u, v, w\} \in X(2)$.

**Edge-variable construction:** The 3XOR instance corresponding to $(X, \beta)$ consists of the following constraints: $x_{\{u,v\}} + x_{\{v,w\}} + x_{\{w,u\}} = \beta_{\{u,v,w\}}$ for each $\{u, v, w\} \in X(2)$.

The vertex-variable construction whose underlying structure is a high-dimensional expander has been studied by Alev, Jeronimo and the last author [AJT19]. They gave an efficient algorithm for approximating vertex-variable constraint satisfaction problems (not necessarily 3XOR) on an underlying high-dimensional expander. Their result is a generalization to higher dimensions of the corresponding result for graphs that “CSPs are easy on expanders” [BRS11, GS11]. They prove this by showing that certain types of random walks on vertices converge very fast on high-dimensional expanders. However, the same analysis fails to show a similar result for the edge-variable construction, as the corresponding random walk on edges of a high-dimensional expander does not mix. Our work shows that this difference isn’t just a technical limitation of their analysis; it is inherent. The edge-variable variant is truly hard, at least for SoS. This demonstrates an interesting subtlety in the structure of high-dimensional expanders, and how it relates to optimization.

To understand our edge-variable construction better, it will be convenient to set up some notation. Let $C^i$ denote the set of all $\mathbb{F}_2$-valued functions on $X(i)$. For each $0 \leq i < d$, we...
consider the operator \( \delta_i : C^i \to C^{i+1} \) defined as follows:

\[
\delta_i f(s) := \sum_{u \in s} f(s - \{u\}).
\]

This is usually referred to as the coboundary operator. Let \( B^i \) be the image of \( \delta_{i-1} \), and let \( Z^i \) be the kernel of \( \delta_i \). Clearly, \( B^i, Z^i \subseteq C^i \). Furthermore, it is not hard to see that \( B^i \subseteq Z^i \).

It easily follows from the definitions that the edge-variable construction corresponding to \((X, \beta)\) is a satisfiable instance iff \( \beta \in B^2 \).

Typically, soundness of SoS-hard instances is proved by choosing \( \beta \) at random from \( C^2 \). In contrast, we construct our explicit instances by choosing \( \beta \) more carefully, and relying on a certain type of expansion property of the complex. Recall that \( B^2 \subseteq Z^2 \), and the instance is satisfiable iff \( \beta \in B^2 \). Complexes for which \( B^2 = Z^2 \) are said to have trivial second cohomology. We will be working with complexes with non-trivial second cohomology, i.e., \( B^2 \neq Z^2 \). This lets us choose a \( \beta \in Z^2 \setminus B^2 \) to prove soundness. It is known that the explicit constructions of HDXs due to Lubotzky, Samuels and Vishne \([LSV05a, LSV05b]\) have non-trivial second cohomology.\(^1\) In fact, these complexes have the stronger property (due to a theorem of Evra and Kaufman \([EK16]\)) that all \( \beta \in Z^2 \setminus B^2 \) are not only not in \( B^2 \), but in fact far from any function in \( B^2 \). This latter property follows from the cosystolic expansion of the complex, and forms the basis for the soundness of our instances.

How do we prove the completeness of our instance, namely, that SoS fails to detect that it is a negative instance? The LSV construction is a quotient of the so-called affine building which is, from a topological point of view, a simple “Euclidean-like” object with trivial cohomologies. The hardness of our instance comes from the inherent difference between the LSV complex and the building, which cannot be seen through local balls whose radius is at most the injectivity radius of the complex, in our case \( \Theta(\log n) \). Locally, the LSV quotient is isomorphic to the building. However, unlike the building, the LSV complex is a quotient with non-trivial cohomologies. The hardness comes from the fact that local views cannot capture the cohomology, which is a global property. Given this observation, the proof of completeness can be carried out following the argument of Ben-Sasson and Wigderson \([BW01]\) that any short resolution proof is narrow, and Grigoriev \([Gri01]\) and Schoenebeck \([Sch08]\)’s transformation from resolution lower bounds to SoS lower bounds.

Technically, we rely on two very different types of expansion or isoperimetry. In our proof of completeness, we rely on an isoperimetric inequality called Gromov’s filling inequality, that says that balls are essentially the objects with smallest boundary in any CAT(0) space (a class of spaces that includes both Euclidean spaces and the affine building). In our proof of soundness, we rely on the cosystolic expansion of the LSV complex, as proven by Evra and Kaufman \([EK16]\), which implies that any non-trivial element in the cohomology has constant weight. Both of these statements are related to expansion, yet they are distinct from other notions of expansion used in previous SoS lower bounds.

**Relation to previous SoS gap constructions.** All previous constructions of hard instances for SoS can be viewed in the vertex/edge-variable framework (typically vertex-variable). To the best of our knowledge, all known hard instances, proving inapproximability in the SoS hierarchy, are random instances; either both the complex \( X \) and the function \( \beta \) are random, or just the function \( \beta \) is random. Explicit hard instances for SoS are known in proof

\(^1\)More accurately, their construction depends on the group defining the quotient. They show that a certain choice of groups yields non-trivial second cohomology.
complexity (e.g., Tseitin tautologies on expanders), however, we do not know how to transform these hard instances into ones for inapproximability. The proof of SoS hardness of these random instances relies on very strong expansion of the underlying complex [Sch08] or on certain pseudorandom properties [KMOW17], both of which are not yet known to be explicitly constructible.

In contrast, our instances are “anti-random”. They are very structured and easily distinguishable from random instances. For example, all balls around a vertex up to some radius are identical and have very specific structure. Naturally, the typical analysis that works for random instances cannot work here. For example, soundness for random instances is based on choosing a random $\beta$ and using a union-bound argument to show that with high probability, every solution violates nearly half of the constraints. In contrast, for us, a random $\beta$ is not a good choice because the local structure will quickly detect local contradictions, ruining the completeness altogether.

**Open directions.** Our construction of explicit hard SoS instances based on HDXs begs several questions, some of which we discuss below.

**Improved soundness** Our construction yields 3XOR hard instances which are at most $(1 - \mu)$-satisfiable, owing to the cosystolic expansion of the underlying HDX (more precisely, $\text{CoSys}^2(X) \geq \mu$, see Section 2.2 for the definition of $\text{CoSys}^2$). Coupled with reductions in the SoS hierarchy [Tul09], this yields 3XOR hard instances which are at most $(1/2 + \epsilon)$-satisfiable for every $\epsilon \in (0, 1)$. Can we obtain such a result directly from the HDX construction (bypassing reductions), say by constructing HDXs which satisfy $\text{CoSys}^2(X) \geq 1/2 - \epsilon$? In addition to maintaining the HDX structure, bypassing reductions would also allow for perfect completeness, which is lost while using NP-hardness reductions.

**Fooling more levels of the SoS hierarchy** Our hard instances fool only $O(\sqrt{\log n})$ levels of the SoS hierarchy, as our argument is based on the injectivity radius of the complexes, which is $O(\log n)$, and we suffer a further square-root loss due to the use of Gromov’s isoperimetry inequality. It is possible that a much stronger lower bound holds for these instances. Can one construct explicit hard instances that fool linearly many levels of the SoS hierarchy?

**HDX dimension and CSP definition** We find the contrast between the vertex-variable and edge-variable constructions baffling: while the vertex-variable construction is easy, our result demonstrates the hardness of the edge-variable construction. As we go to higher dimensions of HDX, there are more ways to define CSPs. Which of these are easy and which are hard?

2 Preliminaries

2.1 The Sum-of-Squares hierarchy

The sum-of-squares hierarchy\(^2\) provides a hierarchy of semidefinite programming (SDP) relaxations, for various combinatorial optimization problems. Figure 1 describes the relaxation given by $t$ levels of the hierarchy for an instance $I$ of 3XOR in $n$ variables, with

\(^2\)For more on Sum-of-Squares, see the recent monograph by Fleming, Kothari and Pitassi [FKP19].
Let \( X \) be a simplicial complex. A ball of radius \( r \) around a vertex \( v \) is the subcomplex induced by all vertices at distance at most \( r \) from \( v \), as measured on the skeleton of \( X \). That is, the subcomplex contains a face of \( X \) if it contains all the vertices of the face.

**Links**

Let \( X \) be a simplicial complex. A link \( X_s \) of a face \( s \in X(i) \) is a simplicial complex of dimension \( d - (i + 1) \) given by \( X_s(j) := \{ t : s \cup t \in X(j + i + 1) \} \). In other words, \( X_s \) contains all faces in \( X \) which contain \( s \), with \( s \) itself removed.

**Balls**

Let \( X \) be a simplicial complex. A ball of radius \( r \) around a vertex \( v \) is the subcomplex induced by all vertices at distance at most \( r \) from \( v \), as measured on the skeleton of \( X \). That is, the subcomplex contains a face of \( X \) if it contains all the vertices of the face.

**Simplicial map**

If \( X \) and \( Y \) are two simplicial complexes, then a simplicial map \( \psi : Y \to X \) is a map from \( Y(0) \) to \( X(0) \) that maps faces to faces.
Chains  Fix a $d$-dimensional simplicial complex $X$. Let $C^i = C^i(X, \mathbb{F}_2)$ be the set of all functions from $X(i)$ to $\mathbb{F}_2$. Elements of $C^i$ are also known as $i$-chains.

For an $i$-chain $f$, we define $|f|$ to be the number of non-zero elements in $f$. For two $i$-chains $f, g$, we define the distance between $f$ and $g$ to be $\text{dist}(f, g) = |f + g|$.

Inner product  For $f, f' \in C^i$, let us denote by $\langle f, f' \rangle_i$ the following sum modulo 2:

$$\langle f, f' \rangle_i := \sum_{s \in X(i)} f(s) f'(s).$$

This is not an inner product in the usual sense as we are working over a field of non-zero characteristic, but it is convenient notation. We will usually drop the subscript $i$.

Dual space  Given any subspace $V \subset C^i$, the dual of $V$ (under $\langle \cdot, \cdot \rangle_i$) is defined as:

$$V^\perp := \{ f \in C^i \mid \text{for all } g \in V, \langle f, g \rangle_i = 0 \}.$$

Boundaries, Cycles, Homology  The boundary operator $\partial_i : C^i \to C^{i-1}$ is given by

$$\partial_i f(s) := \sum_{t \in X(i) : t \supset s} f(t).$$

It gives rise to boundaries $B_i$ and cycles $Z_i$:

$$B_i := \text{im} \partial_{i+1}, \quad Z_i := \ker \partial_i.$$

In the case of graphs, $Z_1$ consists of all sums of cycles (in the usual sense).

The coboundary operator $\delta_i : C^i \to C^{i+1}$, which is the adjoint of the boundary operator, is given by

$$\delta_i f(t) := \sum_{s \in X(i) : s \subset t} f(s) = \sum_{u \in t} f(t - \{u\}).$$

It gives rise to coboundaries and cocycles:

$$B^i := \text{im} \delta_{i-1}, \quad Z^i := \ker \delta_i.$$

We will usually drop the subscript $i$ when invoking $\partial, \delta$.

It is easy to see that $B_i \subset Z_i$ (every boundary is a cycle) and $B^i \subset Z^i$ (every coboundary is a cocycle). For example, in a 2-dimensional complex, the boundary of every triangle is a cycle. We call such cycles trivial cycles. Modding out by trivial cycles and cocycles, we obtain the homology and cohomology spaces

$$H_i := Z_i / B_i, \quad H^i := Z^i / B^i.$$

The dimensions of these spaces (which are identical) measure the number of “holes” in a particular dimension. Nice complexes (such as the buildings considered below) have no holes.

The following claim shows that that the coboundary operator is the adjoint of the boundary operator.

**Claim 2.2.** Let $f \in C^i, g \in C^{i-1}$. Then $\langle f, \delta g \rangle_i = \langle \partial f, g \rangle_{i-1}$. 


Proof.

\[
\langle f, \delta_{i-1}g \rangle_i = \sum_{t \in X(i)} f(t) \cdot \delta_{i-1}g(t) = \sum_{t \in X(i)} f(t) \cdot \left( \sum_{s \in X(i-1): s \subseteq t} g(s) \right)
= \sum_{s \in X(i-1)} \left( \sum_{t \in X(i): t \supset s} f(t) \right) \cdot g(s) = \langle \partial_i f, g \rangle_{i-1}. \]

The following claims shows the dimensions of homology and cohomology spaces are identical.

**Claim 2.3.** \( Z_i = (B^i)^\perp, \quad Z^i = (B_i)^\perp. \)

*Proof.* \( Z_i = \ker \partial_i = \ker \delta_{i-1}^* = (\im \delta_{i-1})^\perp = (B^i)^\perp. \)

**Claim 2.4.** \( \dim H_i = \dim H^i \)

*Proof.*

\[
\dim H_i = \dim Z_i - \dim B_i = \dim C^i - \dim B^i - \dim B_i \quad [\text{By Claim 2.3}]
= \dim Z^i - \dim B^i \quad [\text{By Claim 2.3}]
= \dim H^i. \]

**Cosystoles** We define, following Evra and Kaufman [EK16, Definition 2.14], the \( i \)-cosystole of a complex \( X \) to be the minimal (fractional) size of \( f \in Z^i \setminus B^i \),

\[
\text{CoSys}^i(X) := \min_{f \in Z^i \setminus B^i} |f|/|X(i)|.
\]

### 2.3 The building \( B^{(d+1)} \)

The infinite \( k \)-regular tree is the unique connected \( k \)-regular graph without cycles. Affine buildings are higher-dimensional analogs of the infinite \( k \)-regular tree. For \( d = 1 \), the one-dimensional affine building \( B^{(1)} \) is the \( k \)-regular tree. For higher dimensions they are regular in the sense that all vertex links are bounded and identical in structure, they are connected and contractible,\(^3\) and so have vanishing cohomologies, that is, the cohomology spaces \( H^1, \ldots, H^{d-1} \) are trivial, where \( d \) is the dimension.

We won’t describe \( B^{(d+1)} \) any further; the interested reader can check [Ji12, AB08]. A crucial property of \( B^{(d+1)} \) which we will need in the sequel is its being a CAT(0) space,\(^4\) which is a geometric definition capturing non-positive curvature; see [BH99] for more information. The property of being CAT(0) has the following implication, due to Gromov [Gro83, Gut06, Wen08]:

---

\(^3\)A complex is contractible, roughly speaking, if it can be continuously deformed to a point (technically, it is homotopy-equivalent to a point). Since (co)homologies are preserved by such deformations, all (co)homologies of a contractible complex vanish.

\(^4\)A space is CAT(0) if for every triangle \( x, y, z \), the distance between \( x \) and the midpoint of \( y, z \) is at most the corresponding distance in a congruent triangle in Euclidean space.
Theorem 2.5 (Gromov’s filling inequality for CAT(0) spaces). For every cycle \( f \in Z_1 \) there is a filling \( g \in C_2 \) such that \( f = \partial g \) and \(|g| = O(|f|^2)\).

Gromov’s filling inequality is an isoperimetric inequality. It generalizes the classic isoperimetric inequality in the plane, which states that any simple closed curve of length \( L \) encloses a region whose area is at most \( \frac{L^2}{4\pi} \).

The isoperimetric inequality in the plane can be stated in an equivalent way: the boundary of any bounded region of area \( A \) is a curve whose length is at least \( \sqrt{4\pi A} \). This inequality fails for unbounded regions, which could have infinite area but finite boundary (for example, consider the complement of a circle). In the same way, Gromov’s inequality doesn’t imply that each \( g \in C_2 \) satisfies \( |\partial g| = \Omega(\sqrt{|g|}) \). Rather, we have to replace \(|g|\) with \( \min_{h \in Z_2} |g + h| \).

Gromov’s filling inequality also applies to \( i \)-chains, with an exponent of \( i + 1 \), but we will only need the case \( i = 1 \).

In the sequel, we will apply Gromov’s filling inequality not to the building itself, but rather to balls in the building. The CAT(0) property almost immediately implies that a ball in a CAT(0) space is itself CAT(0) [BH99, Exercise II.1.6]. Furthermore, it is well-known that CAT(0) spaces are contractible, and so have vanishing homologies.

Lemma 2.6. Balls in \( B^{(d+1)} \) have vanishing homologies and satisfy Gromov’s filling inequality.

2.4 The LSV quotient

Whereas the affine building is an infinite simplicial complex, Lubotzky, Samuels and Vishne constructed a growing family of finite complexes that are obtained from quotients of the affine building. These quotients have a growing number of vertices, and locally, in a ball around each vertex, the complex is isomorphic to the affine building. Moreover, they gave a very explicit algorithm for constructing these complexes by first constructing a Cayley graph with an explicit set of generators, and then the higher dimensional faces are simply the cliques in the Cayley graph.

Theorem 2.7 (Lubotzky, Samuels, Vishne [LSV05a, Theorem 1.1]). Let \( q \) be a prime power, \( d \geq 2 \). For every \( e > 1 \) the group \( G = \text{PGL}_d(\mathbb{F}_q) \) has an (explicit) set of \([\frac{d}{1}]_q + [\frac{d}{2}]_q + \ldots + [\frac{d}{d-1}]_q \) generators, such that the Cayley complex of \( G \) with respect to these generators is a Ramanujan complex \( X \) covered by \( B^{(d)}(F) \) for \( F = \mathbb{F}_q((y)) \).

The precise definition of “Ramanujan complex” is not important for this context. For us, there are three important aspects of this theorem: efficient construction, local structure, and global structure.

- **Efficient construction:** Firstly, the fact that the complex is constructible in polynomial time.

- **Local structure:** Next, we highlight the fact that locally the complex looks like the building. The theorem states that the complex \( X \) is covered by \( B^{(d)} \). A covering map maps a simplicial complex \( Y \) surjectively to a simplicial complex \( X \) by mapping the vertices \( \psi : Y(0) \to X(0) \) such that for every \( k \leq d \) the image of every \( k \)-face \( \{v_0, \ldots, v_k\} \in Y(k) \) is a \( k \)-face \( \{\psi(v_0), \ldots, \psi(v_k)\} \in X(k) \).

The fact that \( X \) is covered by \( B^{(d)} \) means that the neighborhood of a vertex in \( X \) and in \( B^{(d)} \) look exactly the same. It turns out that for the LSV complexes this continues to
be true also for balls of larger radius around any vertex. This is a higher-dimensional
analog of the graph property of containing no short cycles (locally looking like a
tree). Define the injectivity radius of $X$ to be the largest $r$ such that the covering map
$B^{(d)} \to X$ is injective from balls of radius $\leq r$ in $B^{(d)}$ and the ball of radius $\leq r$ in $X$.
We do not mention the center of the ball they are all isomorphic.

**Theorem 2.8** (Lubotzky and Meshulam [LM07], see also\(^5\) [EGL15, Corollary 5.2]). *Let
$X$ be the LSV complex above. Then the injectivity radius $r(X)$ of $X$ satisfies

$$r(X) \geq \frac{\log_q |X|}{2(d-1)(d^2-1)} - \frac{1}{2}$$

where $|X|$ is the number of vertices in $X$.*

- **Global structure:** Finally, we look at the second cohomology group of the LSV com-
plexes. Kaufman, Kazhdan and Lubotzky [KKL16] showed that the groups defining the LSV quotient complexes can be chosen so that the second homology is non-
empty.

**Proposition 2.9** (Kaufman, Kazhdan, Lubotzky [KKL16, Proposition 3.6]). *There is an
infinite and explicit sequence of LSV complexes with a non-vanishing second cohomology.*

We remark that Kaufman, Kazhdan and Lubotzky [KKL16] proved that these complexes exist. To show that they are also efficiently constructible, we look into their proof to recall the construction: start with any LSV complex $X$ viewed as a Cayley
graph of a group $G$. Find some element of order 2 in $G$ (such an element always
exists), and then quotient $X$ by this element, thus obtaining a complex $Y$ that is itself
is a Ramanujan complex because it is a quotient of one. $Y$ is clearly efficiently con-
structible from $X$, and has half as any vertices. This construction shows (see [KKL16,
Proposition 3.5]) that $H^1(Y) \neq 0$. Furthermore, the proof of [KKL16, Proposition 3.6]
shows that because $G$ has property $T$ one can deduce also that $H^2(Y) \neq 0$.

Evra and Kaufman proved [EK16, Theorem 1.9] that quotients of $B^{(d)}$ (and even a more
general class of complexes) are so-called “cosystolic expanders” which in particular implies the following.

**Theorem 2.10** (Evra and Kaufman [EK16, Part of Theorem 1.9]). *Let $\{X_n\}$ be a family
of LSV complexes. There exists some constant $\mu > 0$ that depends only on $q$ and $d$ but not
on the size $n$ of the complex, such that every $f \in Z^2(X) \setminus B^2(X)$ must have weight at least
$\mu \cdot |X(2)|$.\(^5\)

3 **Main result**

3.1 **Local geometry of LSV complexes**

The infinite sequence of complexes we will be working with are the LSV complexes de-
scribed in Section 2.4 above. The properties we care about are (1) that they are efficiently

\(^5\)The theorem was proven by [LM07]. They stated their theorem using a slightly different definition for
injectivity radius but one can prove that the two definitions coincide in this case. This was reproven in [EGL15]
who use the definition of injectivity radius that is convenient for us.
constructible, (2) that small balls in these complexes are isomorphic to the affine building, which satisfies certain isoperimetric inequalities because it is a CAT(0) space, and (3) that each complex has a two-dimensional cocycle with linear distance from the set of coboundaries. The second and third properties provide the tension between the local and the global structure of these complexes that we now harness for our hardness.

To construct an SDP solution, we will need to show that our instance based on the LSV complex “locally looks satisfiable”. To this end, we will first develop some local properties of the LSV complex.

Note that each \( h \in C^2 \) corresponds to a set of triangles. For the following statements, we consider two triangles to be connected if they share an edge. This can be used to define connected components. Note that if \( h \) can be split into connected components \( h_1, \ldots, h_s \), then the components correspond to disjoint sets of triangles. Moreover, no triangle in \( h_i \) shares an edge with a triangle in \( h_j \) when \( i \neq j \), which also implies that the boundaries \( \partial h_i \) and \( \partial h_j \) correspond to disjoint sets of edges.

We prove the following claims by mapping small connected sets in \( X(2) \) to corresponding sets in the infinite building \( B \). The first proposition shows that there can be no small non-trivial cancellations (i.e., not coming from tetrahedra).

**Proposition 3.1.** Let \( h_0 \in C^2 \) be a connected set of triangles such that \( |h_0| < r \) and \( \partial h_0 = 0 \). Then \( h_0 \in B_2 \).

**Proof.** Since \( |h_0| < r \), there is a ball \( N \) of radius \( r \) that contains the support of \( h_0 \). By assumption, the covering map \( \psi : B \to X \) has injectivity radius of at least \( r \). This means that there is a radius-\( r \) ball \( \hat{N} = \psi^{-1}(N) \) in \( B \) that is isomorphically mapped by \( \psi \) to \( N \). Look at \( \hat{h}_0 = \psi^{-1}(h_0) \in C^2(\hat{N}) \), the chain isomorphic to \( h_0 \) in the building. Clearly \( \partial \hat{h}_0 = \psi^{-1}(\partial h_0) = 0 \), and since balls in the building have zero homologies by Lemma 2.6, we deduce that \( \hat{h}_0 \) itself must be a boundary, i.e. there must be some \( \hat{g}_0 \in C^3(\hat{N}) \) such that \( \partial \hat{g}_0 = \hat{h}_0 \). Moving back to \( X \), we see that \( g_0 := \psi(\hat{g}_0) \in C^3(X) \) necessarily satisfies \( \partial g_0 = h_0 \), and so \( h_0 \in B_2 \). \( \square \)

This proposition states that locally (i.e., within the injective radius \( r \)), \( Z_2 \) looks like \( B_2 \). We thus have a complex whose cohomology group is non-trivial, yet locally, the homology group “looks” trivial. Note that this is a twist on what we had claimed in the introduction, a complex whose cohomology group is non-trivial, yet locally, the cohomology group “looks” trivial. However, these are identical statements owing to Claim 2.4.

The next proposition shows that Gromov’s filling inequality in the infinite building \( B \) can be used to yield a similar consequence for small sets in the finite complex \( X \).

**Proposition 3.2.** Let \( h_0 \in C_2 \) be a connected set of triangles such that \( |h_0| < r \) and \( |h_0| \leq |h_0 + h| \) for all \( h \in B \). Then, \( |\partial h_0| \geq c \cdot |h_0|^{1/2} \), where \( c > 0 \) is an absolute constant.

**Proof.** As before, the support of \( h_0 \) is contained in a ball \( N \) of \( X \) which is isomorphic under \( \psi \) to a ball \( \hat{N} \) in \( B \). Let \( \hat{h}_0 = \psi^{-1}(h_0) \in C^2(\hat{B}) \), and let \( \hat{f}_0 = \partial \hat{h}_0 \). We now apply the filling theorem of Gromov, which holds in \( \hat{N} \) due to Lemma 2.6, to deduce that there is some \( \hat{h}_1 \) that fills \( \hat{f}_0 \), namely \( \partial \hat{h}_1 = \hat{f}_0 \) and whose size is at most \( |\hat{h}_1| = O(|\hat{f}_0|^2) \).

Now \( \partial (\hat{h}_0 - \hat{h}_1) = \hat{f}_0 - \hat{f}_0 = 0 \). Since the ball \( \hat{N} \) has zero homologies by Lemma 2.6, \( \hat{h}_0 - \hat{h}_1 \) itself must be a boundary: there must be some \( \hat{g} \in C^3(\hat{N}) \) such that \( \partial \hat{g} = \hat{h}_0 - \hat{h}_1 \). Pushing \( \hat{g} \) and \( \hat{h}_1 \) back to \( X \), we get \( g = \psi(\hat{g}) \) and \( h_1 = \psi(\hat{h}_1) \), which satisfy \( \partial g = h_0 - h_1 \).
At this point we have a small \( h_1 \) that is close via a boundary to \( h_0 \). Finally, observe that \( f_0 = \partial h_0 \) satisfies \( f_0 = \psi^{-1}(f_0) \). So
\[
|f_0| = |\hat{f}_0| \geq c \cdot |\hat{h}_1|^{1/2} = c \cdot |h_1|^{1/2} \geq c \cdot |h_0|^{1/2},
\]
where the last inequality used that \( |h_0| \leq |h_0 + (h_1 - h_0)| \), since \( h_1 - h_0 = \partial g \in B_2 \).

\[ \square \]

### 3.2 Fooling \( \Omega(\sqrt{\log n}) \) levels of SoS hierarchy

Let \( X \) be a \( d \)-dimensional LSV complex, with \( |X(1)| = n \) and non-trivial second cohomology group, as per Proposition 2.9. Below, we construct an instance of 3XOR in \( n \) variables using this complex, and prove a lower bound on the integrality gap of the relaxation obtained by \( \Omega(\sqrt{\log n}) \) levels of the SoS hierarchy.

**Construction.** We construct a system of equations on \( X \) by putting a variable \( x_{\{a,b\}} \) for each edge \( \{a,b\} \in X(1) \) of the complex, and an equation
\[
x_{\{a,b\}} + x_{\{b,c\}} + x_{\{c,a\}} = \beta_{\{a,b,c\}}
\]
for each triangle \( \{a,b,c\} \in X(2) \), where \( \beta \) is an arbitrary element of \( \mathbb{Z}^2 \setminus B^2 \).

Recall that \( X \) can be constructed efficiently. Given \( X \), we can find a vector \( \beta \in \mathbb{Z}^2 \setminus B^2 \) using elementary linear algebra. Therefore the entire system can be constructed efficiently.

**Soundness.** Soundness of this system follows easily from the fact that the cosystole is large.

**Claim 3.3 (Soundness).** Every assignment to the system defined above falsifies at least \( \mu \) fraction of the equations.

**Proof.** An assignment to the variables is equivalent to an \( f \in C^1 \). Every equation satisfied by \( f \) is a triangle in which \( \delta f(\{a,b,c\}) = \beta_{\{a,b,c\}} \), and so the number of unsatisfied equations is \( \text{dist}(\delta f, \beta) = |\delta f + \beta| \). Since \( \delta f \in B^2 \) and \( \beta \in \mathbb{Z}^2 \setminus B^2 \), also \( \delta f + \beta \in \mathbb{Z}^2 \setminus B^2 \), and so \( |\delta f + \beta|/|X(2)| \geq \text{CoSys}^2(X) \geq \mu \). In other words, the assignment falsifies at least \( \mu \) fraction of the equations.

The main work is to prove completeness, namely to show that the system looks locally satisfiable.

**Completeness.** Our main result is that this system appears satisfiable to the Sum-of-Squares hierarchy with \( O(\sqrt{\log n}) \) levels. Grigoriev [Gri01] and Schoenebeck [Sch08] showed that to prove such a statement it suffices to analyze the refutation width of the system of equations (see Lemma 2.1). If the refutation width is at least \( w \), then \( w/2 \) levels of the Sum-of-Squares hierarchy cannot refute the system.

A system of linear equations over \( \mathbb{F}_2 \) can be refuted using a proof system known as \( \oplus \)-resolution, in which the only inference rule is: given \( \ell_1 = b_1 \) and \( \ell_2 = b_2 \), deduce \( \ell_1 \oplus \ell_2 = b_1 \oplus b_2 \); here \( \ell_1, \ell_2 \) are XORs of variables, and \( b_1, b_2 \) are constants. A refutation has the structure of a directed acyclic graph (DAG) where each non-leaf node has two incoming edges. A refutation is a derivation which starts with the given linear equations, placed at the leaves of a DAG, and reaches the equation \( 0 = 1 \) at the root of the DAG. The width of a
linear equation $\ell = b$ is the number of variables appearing in $\ell$. The width of a refutation is the maximum width of an equation in any of the nodes of the DAG.

In the remainder of this section, we prove the following theorem, which together with Lemma 2.1 implies Theorem 1.1.

**Theorem 3.4.** The construction above requires width at least $\Omega(\sqrt{r})$ to refute in $\oplus$-resolution, where $r = \Theta(\log n)$ is the injectivity radius of the complex.

The proof follows classical arguments of Ben-Sasson and Wigderson [BW01] regarding lower bounds on resolution width, which were also used in the proof of Schoenebeck [Sch08]. Whereas Ben-Sasson and Wigderson relied on boundary expansion, we rely on Gromov’s filling inequality (and so lose a square root).

Suppose we are given a refutation for this system, and consider the corresponding DAG. Each leaf $\nu$ in the DAG is labeled by a triangle $T_\nu \in X(2)$. Define

\[ h_\nu := 1_{T_\nu} \in C^2, \quad b_\nu := \beta_{T_\nu} \in F_2. \]

For each inner node $\nu$ in the DAG, let $\nu_1, \nu_2$ be its two incoming nodes. Define inductively,

\[ h_\nu := h_{\nu_1} + h_{\nu_2} \in C^2, \quad b_\nu := b_{\nu_1} + b_{\nu_2} \in F_2. \]

**Proposition 3.5.** For every node $\nu$, $b_\nu = \langle \beta, h_\nu \rangle$.

**Proof.** This is immediate by following inductively the structure of the DAG. \(\square\)

As in [BW01], we next define a complexity measure for each node of the DAG. While in [BW01] the complexity measure is based on the number of “leaf equations” used to derive the one at a given node, we will need to discount sets of triangles corresponding to tetrahedra, as these cannot lead to contradictions. Recall that $B_2 = \text{im} \partial_3$ is the set of triangle chains that “come from” tetrahedra chains, which we consider as the “trivial” cycles. We define a complexity measure at each node,

\[ \kappa(\nu) := \text{dist}(h_\nu, B_2) = \min_{h \in B_2} |h_\nu + h| \]

that measures the distance of $h_\nu$ from these trivial cycles. The complexity measure $\kappa$ satisfies the following sub-additivity property.

**Proposition 3.6.** If $\nu$ is an inner node in the DAG with $\nu_1, \nu_2$ its two incoming nodes, then

\[ \kappa(\nu) \leq \kappa(\nu_1) + \kappa(\nu_2). \]

**Proof.** Let $h_1, h_2 \in B_2$ be such that $\kappa(\nu_1) = |h_{\nu_1} + h_1|$ and $\kappa(\nu_2) = |h_{\nu_2} + h_2|$. Recall that $h_\nu = h_{\nu_1} + h_{\nu_2}$. Then, we have

\[ \kappa(\nu_1) + \kappa(\nu_2) = |h_{\nu_1} + h_1| + |h_{\nu_2} + h_2| \geq |h_{\nu_1} + h_{\nu_2} + h_1 + h_2| = |h_\nu + h_1 + h_2| \geq \kappa(\nu). \] \(\square\)

We also need the fact that the complexity of a node with a contradiction must be non-zero.

**Proposition 3.7.** If $\kappa(\nu) = 0$ then $b_\nu = 0$. 

12
Proof. If $\kappa(v) = 0$ then $h_v \in B_2$. Hence $b_v = \langle \beta, h_v \rangle = 0$ since $\beta \in Z^2 = (B_2)\perp$ (Claim 2.3).

Next, we consider the width of each node in the DAG. For a node $v$, let

$$f_v := \partial h_v \in C^1.$$  

Thus $f_v$ indicates the set of variables appearing in the left-hand side of the equation on node $v$. So the width of the system is the maximum, over all nodes $v$ in the DAG, of $|f_v|$.

We can now prove Theorem 3.4 using the above complexity measure, and results from Section 3.1.

Proof of Theorem 3.4. Let $v^*$ denote the root of the DAG. By virtue of being a refutation, $b_{v^*} = 1$ while $f_{v^*} = 0$. In other words, $\partial h_{v^*} = f_{v^*} = 0$, which means that $h_{v^*} \in Z_2$. Since $b_{v^*} = 1$, we also have by Proposition 3.7 that $\kappa(v^*) > 0$.

Let $h \in B_2$ be such that $\kappa(v^*) = |h_{v^*} + h|$, and let $h_1, \ldots, h_s$ be the disjoint connected components of $h_{v^*} + h$. We will first show that $\kappa(v^*) = |h_{v^*} + h| \geq r$. Assuming $\kappa(v^*) < r$, we have that

$$|h_1| + \cdots + |h_s| = |h_{v^*} + h| < r.$$  

Also, since

$$\partial h_1 + \cdots + \partial h_s = \partial (h_{v^*} + h) = \partial h_{v^*} = 0,$$

we must have that $\partial h_i = 0$ for each $i \in [s]$, since connected components have disjoint boundaries. Applying Proposition 3.1 to each $h_i$, we get that $h_i \in B_2$ for each $i \in [s]$. However, this implies $h_{v^*} + h \in B_2$ and hence $\kappa(v^*) = 0$, which is a contradiction.

Using sub-additivity (Proposition 3.6), $\kappa(v^*) \geq r$, and the fact that the leaves of the DAG satisfy $\kappa(v) = 1$, we get that there must be some internal node $v$ for which $r/2 \leq \kappa(v) < r$. We can find such a node by starting at the root and always going to the child with higher complexity, until reaching a node $v$ such that $\kappa(v) < r$. We will prove that for such a node, we must have $|f_v| = \Omega(\sqrt{r})$.

As before, let $h \in B_2$ now be such that $\kappa(v) = |h_v + h|$, and let $h_1, \ldots, h_s$ be the disjoint connected components of $h_v + h$. We have that $|h_i| \leq |h_v + h| < r$ for each $i \in [s]$. By the minimality of $|h_v + h|$, we also have that for any $h' \in B_2$ and any $i \in [s]$,

$$|h_i| + |h_v + h - h_i| = |h_v + h| \leq |h_v + h + h'| \leq |h_i + h'| + |h_v + h - h_i|.$$  

Thus, $|h_i|$ is also minimal for each $i$, and we can apply Proposition 3.2 to each connected component $h_i$, to obtain

$$|f_v| = |\partial (h_v + h)| = |\partial h_1| + \cdots + |\partial h_s| \geq c \cdot |h_1|^{1/2} + \cdots + c \cdot |h_s|^{1/2} \geq c \cdot (|h_1| + \cdots + |h_s|)^{1/2} = c \cdot |h_v + h|^{1/2} \geq (c/\sqrt{2}) \cdot \sqrt{r}. \quad \Box$$

Acknowledgements

Part of this work was done when the authors were visiting the Simons Institute of Theory of Computing, Berkeley for the 2020 summer cluster on “Error-Correcting Codes and High-Dimensional Expansion”. We thank the Simons Institute for their kind hospitality.


References


A Proof of Lemma 2.1

Lemma 2.1 (Restated) ([Sch08, Lemma 13], [Tul09, Theorem 4.2]) Let $\Lambda$ be a system of equations in $n$ variables over $\mathbb{F}_2$, which does not admit any refutations of width at most $2t$. Then there exist vectors $\{u_S\}_{S \subseteq [n], |S| \leq t}$ satisfying the constraints in Figure 1, such that for all equations $\sum_{i \in T} x_i = b_T$ in $\Lambda$ with $|T| \leq t$, we have $\langle u_T, u_S \rangle = (-1)^{|S|}$. 

Proof. We assume that $\Lambda$ is closed under width-2t $\oplus$-resolution, replacing $\Lambda$ by its closure if necessary, and also that it contains the trivial equation $0 = 0$. We will now construct the unit vector $u_S$.

Define a relation $\sim$ on subsets of $[n]$ of size at most $t$ as follows: $S \sim T$ iff there exists an equation $\sum_{i \in S \Delta T} x_i = b$ in $\Lambda$ for some $b \in \mathbb{F}_2$. It is easy to check that the relation is reflexive and symmetric. It is also transitive since for $S_1 \sim S_2$, $S_2 \sim S_3$, we can add the corresponding equations to obtain one of the form $\sum_{i \in S_1 \Delta S_3} x_i = b$ for some $b \in \mathbb{F}_2$. Since $|S_1|, |S_3| \leq t$, this equation has at most 2t variables and must be in $\Lambda$ by the closure property. Thus, we have an equivalence relation which partitions all sets of size at most $t$ into equivalence classes, say $C_1, \ldots, C_s$. Choose an arbitrary representative $R_i$ for each class $C_i$, and let $R(S)$ denote the representative for the class containing $S$. For convenience, we choose $R(\emptyset) = \emptyset$.

We now construct the SDP vectors. Let $e_1, \ldots, e_s$ be an arbitrary orthonormal set of vectors, and assign $u_{C_i} = e_i$ for all $i \in [s]$. Note that for any $S$ with $|S| \leq t$, there must be a unique equation of the form $\sum_{i \in S \Delta R(S)} x_i = b_S$ in $\Lambda$, since different equations can be used to obtain a width-2t refutation. We assign the vector for $S$ as

$$u_S := (-1)^{|S|} \cdot u_{R(S)}.$$ 

The vectors are unit-length by construction. Note that if $S_1 \Delta S_2 = S_3 \Delta S_4$, we must have $S_1 \sim S_2 \Leftrightarrow S_3 \sim S_4$. If $S_1 \not\sim S_2$, then we have that $\langle u_{S_1}, u_{S_2} \rangle = \langle u_{S_3}, u_{S_4} \rangle = 0$. Otherwise, we have $R(S_1) = R(S_2)$, $R(S_3) = R(S_4)$, and equations of the form

$$\sum_{i \in S_1 \Delta R(S_1)} x_i = b_{S_1}, \quad j \in \{1, 2, 3, 4\}.$$ 

We must also have $b_{S_1} + b_{S_2} = b_{S_3} + b_{S_4}$, since otherwise we obtain two different equations with variables in $S_1 \Delta S_2 = S_3 \Delta S_4$, yielding a refutation. This suffices to satisfy the SDP constraints, since

$$\langle u_{S_1}, u_{S_2} \rangle = (-1)^{b_{S_1} + b_{S_2}} \cdot \langle u_{R(S_1)}, u_{R(S_2)} \rangle = (-1)^{b_{S_1} + b_{S_2}} = (-1)^{b_{S_3} + b_{S_4}} = \langle u_{S_3}, u_{S_4} \rangle.$$ 

Finally, for any equation $\sum_{i \in T} x_i = b_T$ in $\Lambda$ with $|T| \leq t$, we get $\langle u_T, u_{\emptyset} \rangle = (-1)^{|T|}$, since we must have $T \sim \emptyset$ and $R(T) = \emptyset$. \qed