Hard Metrics From Cayley Graphs Of Abelian Groups

Ilan Newman and Yuri Rabinovich

Computer Science Department, University of Haifa, Haifa 31905, Israel.
ilan@cs.haifa.ac.il, yuri@cs.haifa.ac.il *

Abstract. Hard metrics are the class of extremal metrics with respect to embedding into Euclidean Spaces: their distortion is as bad as it possibly gets, which is $\Omega(\log n)$. Besides being very interesting objects akin to expanders and good codes, with rich structure of independent interest, such metrics are important for obtaining lower bounds in Combinatorial Optimization, e.g., on the value of MinCut/MaxFlow ratio for multicommodity flows.
For more than a decade, a single family of hard metrics was known (see [10, 3]). Recently, a different such family was found (see [8]), causing a certain excitement among the researchers in the area.
In this paper we present another construction of hard metrics, different from [10, 3], and more general yet clearer and simpler than [8]. Our results naturally extend to NEG and to ℓ_1.

1 Introduction

A famous theorem of Bourgain [4] states that every metric space (X, d) of size n can be embedded into an Euclidean space with multiplicative distortion at most $\mathrm{dist}(d \hookrightarrow \ell_2) = O(\log n)$. We call a metric space *hard* if $\mathrm{dist}(d \hookrightarrow \ell_2) = \Omega(\log n)$.

When studying a special class of metric spaces, perhaps the most natural first question is whether this class contains hard metrics. Many fundamental results in the modern Theory of Finite Metric Spaces may be viewed as a negative answer to this question for some special important class of metrics. E.g., Arora et al. [1] (improving on Chawla et al. [5]) show this for Negative Type metrics, Klein et al. [9] for planar metrics, and Gupta et al. [6] for doubling metrics. For a long time (since Linial, London and Rabinovich [10] and Rabani and Aumann [3]), the only known family of hard metrics was, essentially, the shortest-path metrics of constant-degree expander graphs. It was even conjectured that in some vague sense this is always the case. Recently, however, Khot and Naor [8] constructed a different family of hard metrics by considering certain quotient spaces of $\mathbb{Z}_2^n$ equipped with the Hamming distance.

The starting point of the current research was a plausible conjecture that a *circular* metric cannot be hard, where by circular we mean a metric on the

* Supported in part by a grant ISF-247-020-10.5

underlying space $\mathbb{Z}_n$, such that $d(a,b)$ depends solely on $((a-b) \mod n)$. Rather surprisingly, the conjecture turns out to be false, and, moreover, it fails not only for $\mathbb{Z}_n$, but for *any* Abelian group H. More precisely, it is always possible to choose a set A of generators for H, so that the shortest-path metric of the corresponding Cayley graph $G(H,A)$ is hard. In the special case of $\mathbb{Z}_2^n$, good sets of generators are closely related to error-correcting codes of constant rate and linear distance.

Our construction is both simple to describe and easy to analyze. It differs from that of [10, 3], as the degree of such Cayley graphs is necessarily non-constant. It is more general than the construction of [8], since the latter, despite very different description and analysis, can be shown to produce the same mertic space as does our construction in the special case of $\mathbb{Z}_2^n$.

Note: Although in what follows we restrict the discussion to Euclidean Spaces, the same method shows the hardness of the metrics that we construct also with respect to much richer spaces of NEG, and consequently ℓ_1.

2 General Abelian Groups

Let G be a d-regular connected graph on n vertices, and let μ_G be its shortest-path metric. Our first step is to get a general lower bound on distortion of embedding μ_G into an Euclidean space. We use a standard (dual) method of comparing the so-called Poincare forms (see, e.g., [10, 11], with further details therein). Consider the following projective quadratic form:

$$F(\Delta) \;=\; \frac{\sum_{(i,j)\in E(G)} \Delta^2(i,j)}{\sum_{i<j\in V(G)} \Delta^2(i,j)}$$

Then,

$$F(\mu_G) \;=\; \frac{|E|}{\binom{n}{2}\mathrm{Ave}(\mu_G^2)}\,,$$

where $\mathrm{Ave}(\mu_G^2)$ is the average value of $\mu_G^2(i,j)$ over all pairs of vertices of G. On the other hand let δ be *any* Euclidean metric on $V(G)$, i.e., a metric of the form

$$\delta(i,j) \;=\; \|x^i - x^j\|_2\,, \quad \text{where} \quad \{x^i\}_{i\in V(G)} \subset \mathbb{R}^m\,.$$

By a standard argument (see e.g., [11], Sect. 15.5), the minimum of $F(\delta)$ over all such δ's is precisely γ_G/n, where γ_G is the *spectral gap* of G, i.e., $(d-\lambda_G)$ where λ_G is the second largest eigenvalue of the adjacency matrix of G. If the minimum of $F(\delta)$ over all Euclidean metrics is larger than $F(\mu_G)$, we conclude that the square of distortion of any embedding of μ_G into an Euclidean space is at least the ratio between these two values:

Proposition 1.

$$\mathrm{dist}^2(\mu_G \hookrightarrow \ell_2) \;\geq\; \frac{n-1}{n}\cdot\frac{\gamma_G}{d}\cdot\mathrm{Ave}(\mu_G^2)\,.$$

In particular,

Corollary 1. *If a graph G has a constant normalized spectral gap γ_G/d, and* $\mathrm{Ave}(\mu_G^2) = \Omega(\log^2 n)$*, then the above method yields an $\Omega(\log n)$ lower bound on the distortion of embedding μ_G into an Euclidean space.*

In the following we shall deal solely with vertex-transitive graphs; let us remark that for such graphs $\mathrm{Ave}(\mu_G^2) \approx \mathrm{Diam}(G)^2$. Indeed, let r be the smallest radius such that the corresponding r-ball in μ_G contains at least $n/2$ vertices. Clearly, $\mathrm{Ave}(\mu_G^2) \geq r^2/2$, while $\mathrm{Diam}(G) \leq 2r+1$. Thus, it suffices to ensure that the diameter of G is at least $\Omega(\log n)$.

Turning to Cayley graphs, it is well known that for (some) non-Abelian groups, there exist Cayley graphs with *constantly many* generators, and a constant spectral gap (see, e.g., [12], the section on Cayley expander graphs). Since the constant number of generators guarantees that the diameter is $\Omega(\log n)$, this yields a graph as required in Corollary 1. (This is precisely the construction used in [10, 3]). For Abelian groups such construction is impossible, since in order to ensure a constant normalized gap γ_G/d, the number of generators must be at least $\Omega(\log n)$ (see, e.g., [12]). This might seem to be a problem, since, at least for general groups, that many generators may well cause the diameter be $O(\log n/\log\log n) = o(\log n)$. For Abelian groups, however, this does not happen! While the following simple fact is well known (see, e.g., [12], proof of Prop. 11.5), it has been apparently overlooked in the context of hard metrics. Let $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$ be the entropy function.

Proposition 2. *Let H be an Abelian group of size n, and let $A \subset H$, $A = -A$, be a set of generators of size $d = c_0\log_2 n$. Then, for any constant c_1 such that $(c_0+c_1)\cdot h(c_1/(c_0+c_1)) < 1$, the diameter of the corresponding Cayley graph $G(H, A)$ is $\geq c_1\log_2 n$ for a large enough n.*

The proposition follows from the observation that the number of distinct endpoints of paths of of length l in G is at most $\binom{d+l}{l}$, since due to commutativity of G it is at most the number of partitions of a set of l (identical) elements to d (distinct) parts. Therefore, the number of points reachable by a path of length $\leq c_1\log_2 n$ is at most

$$\sum_{l=0}^{c_1\log_2 n}\binom{c_0\log_2 n + l}{l} = 2^{h\left(\frac{c_1}{c_0+c_1}\right)\cdot(c_0+c_1)\cdot\log_2 n + o(\log n)} =$$

$$n^{(c_0+c_1)\cdot h\left(\frac{c_1}{c_0+c_1}\right)+o(1)} < n.$$

Thus, as long as the number of generators is $O(\log n)$, our only concern is getting a constant normalized spectral gap γ_G/d. This is summed up in the following theorem.

Theorem 1. *Let H be an Abelian group of size n, let $A \subset H$ be a symmetric set of generators of size $d = c_0\log_2 n$ for a suitable universal constant c_0 (a 100 would certainly suffice) and let $G(H, A)$ be the corresponding Cayley graph. If the normalized spectral gap $\gamma_G/|A| = \Omega(1)$, then μ_G is a hard metric.*

It is well known that a random construction achieves this goal (see, e.g., [2], in particular the section on Abelian groups):

Proposition 3. *Let H be a an Abelian group of size n, and let $A \subset H$ be a random symmetric set of generators of size $d = c_0 \log_2 n$ for a suitable universal constant c_0 (a 100 would certainly suffice). Then, the corresponding Cayley graph $G(H, A)$ is almost surely connected, and has a normalized spectral gap ≥ 0.5.*

To prove the proposition, one needs first to realize that the eigenvectors of G are the *characters* of H, i.e., functions χ from H to the unit circle in $\mathbb{C}$, such that $\chi(a+b) = \chi(a) \cdot \chi(b)$. In particular, all such functions with the exception of the constant one (that corresponds to the eigenvalue d), sum up to 0. From here it is little more than an application of the Chernoff Bound. For an efficient deterministic construction of such A's see [13].

Combining Theorem 1 and Proposition 3, we arrive at the main result of this section:

Theorem 2. *Let $G = G(H, A)$ be a Cayley graph obtained by taking a random symmetric set of generators $A \subset H$ of size $d = c_0 \log_2 |H|$ for a suitable universal constant c_0. Then, the shortest-path metric of G is almost surely a hard metric.*

Remark: *It is natural to ask whether the Cayley graph whose shortest-path metric is hard, may have super-logarithmic degree. The answer is positive, and in fact for any Abelian H it is possible to get degree $O(n^{1-\epsilon})$ for any constant ϵ. We postpone the detailed discussion of this matter to the journal version of this paper.*

3 When the Group is $\mathbb{Z}_2^n$

In this case the group is just an n-dimensional vector space over $\mathbb{Z}_2$. Any set of generators (vectors) A is automatically symmetric. Following the requirements of Corollary 1, we have to ensure three conditions: a constant normalized spectral gap, conectivity of $G(\mathbb{Z}_2^n, A)$, and $\Omega(n)$ diameter.

The construction is based on linear good codes. Let $\mathcal{C} \subset \mathbb{Z}_2^m$ be a linear code of *dimension* n, that is, $\mathcal{C}$ is generated by a set of n linearly independent m-dimensional vectors. The *distance* $D(\mathcal{C})$ of $\mathcal{C}$ is the minimum number of 1's in any $c \in \mathcal{C}$. $\mathcal{C}$ is said to be of linear distance if $D(\mathcal{C}) = \Omega(m)$. In addition, if $m = O(n)$ the code is said to have a *constant rate.*

Let M be an $n \times m$ matrix whose rows are a basis for $\mathcal{C}$ (such an M is called the generator matrix of $\mathcal{C}$) and let $A \subset \mathbb{Z}_2^n$, $|A| = m$, be the set of columns M. It is easy to see that for any such linear code, the graph $G(\mathbb{Z}_2^n, A)$ is connected due to the fact that the rank of M is n.

Proposition 4. *Let $\mathcal{C}$ be a linear code of linear distance and let M and A be the corresponding matrix and set of vectors as above. Then normalized spectral gap γ_G/n of $G(\mathbb{Z}_2^n, A)$ is constant. Conversely, any A with this property is necessarily the set of columns of a generator matrix of a linear code with linear distance.*

The proposition is a folklore (see e.g. [2], proof of Proposition 2). Here is a sketch of the proof.

Proof. The characters of $\mathbb{Z}_2^n$, indexed by the group elements, $\{\chi_u\}$, $u \in \mathbb{Z}_2^n$, are of the form

$$\chi_u(x) \;=\; (-1)^{\langle u,x\rangle}\,,$$

where the inner product (with a slight abuse of notation) is (mod 2). Let $A \subset \mathbb{Z}_2^n$, $|A| = m$, be a set of generators (vectors), and let M_A be an $n \times m$ matrix over $\mathbb{Z}_2$ whose columns are the vectors of A. For a vector in $v \in \mathbb{Z}_2^m$ let $w(v)$ be the number of 1's in v. The second largest eigenvalue λ_G of $G(\mathbb{Z}_2^n, A)$ is

$$\lambda_G \;=\; \max_{u\neq 0} \sum_{a\in A} (-1)^{\langle u,a\rangle} \;=\; \max_{u\neq \mathbf{0}} \left\{m - 2w(u^T M_A)\right\}\,.$$

Let $\mathcal{C} \subseteq \mathbb{Z}_2^n$ be a linear code generated by M_A, that is, all linear combinations of rows of M_A. Then $\mathcal{C} = \{u^T M_A\}_{u\in\mathbb{Z}_2^n} \subset \mathbb{Z}_2^m$ and hence $\lambda_G = m - 2D(\mathcal{C})$. Keeping in mind that $\gamma_G = m - \lambda_G$ we conclude that $\gamma_G \;=\; 2D(\mathcal{C})$. Therefore, $\gamma_G = \Omega(m)$ if and only $\mathcal{C}$ is a linear code of linear distace. □

It remains to ensure that the diameter of $G(\mathbb{Z}_2^n, A)$ is $\Omega(n)$. By Proposition 2, this condition will necessarily hold provided $m = O(n)$, that is, if $\mathcal{C}$ is of constant rate. Thus,

Theorem 3. *Let $\mathcal{C}$ be a linear code of constant rate and linear distance, and* $\dim(\mathcal{C}) = n$. *Let M be an $n \times m$ matrix whose rows form a basis for $\mathcal{C}$, and let $A \subset \mathbb{Z}_2^n$, be the set of M's columns. Then the metric of $G(\mathbb{Z}_2^n, A)$ is hard.*

Such codes are at the core of the Coding Theory and they have received a considerable attention. Their existence has been established by numerous randomized and deterministic efficient constructions, with the first explicit construction due to Justesen [7].

We conclude the paper with a discussion of the construction of hard metrics due to Khot and Naor [8]. Let $\mathcal{C} \subset \mathbb{Z}_2^m$ be a linear code of constant rate and linear distance, of dimension n. Let $\mathcal{C}^\perp$ be the dual code, i.e., $\mathcal{C}^\perp = \{u | Mu = 0\}$ where M is the generator matrix of $\mathcal{C}$. Define an equivalence relation on $\mathbb{Z}_2^m$ by $x \equiv y$ iff $(x - y) \in \mathcal{C}^\perp$. Now, let X be a quotient metric space of Z_2^m equipped with the Hamming metric, with respect to $\equiv$. That is, the distance between two points a and b in X is the Hamming distance between the two corresponding cosets $A, B \subset \mathbb{Z}_2^m$. Khot and Naor show that X with the induced metric is hard.

Proposition 5. *The above construction is isometric to the construction described in Theorem 3.*

Proof. Let M be a matrix as in Theorem 3. Then X can be viewed as the image of $\mathbb{Z}_2^m$ under the linear mapping $\phi : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$, $\phi(x) = Mx$. Define the *edges* of X as the images of Hamming edges of $\mathbb{Z}_2^m$ under ϕ. Clearly, the quotient metric of X is precisely the shortest-path metric of the resulting graph. The images of the Hamming edges are, however, precisely the column vectors of M, and the isometry follows. □

Without diminishing the achievement of [8], which in addition to the result discussed here contains a number of other wonderful results, it appears that our construction, besides being more general, is simpler both in terms of description and analysis.

References

1. S.Arora, J.Lee, A.Naor. Euclidean distortion and the sparsest cut. in *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, STOC'05*, pp.553–562, 2005.
2. N. Alon and Y. Roichman. Random Cayley graphs and expanders. *Random Structures Appl.*, 5:271–284, 1994.
3. Y. Aumann and Y. Rabani. An $O(\log k)$ Approximate min-cut max-flow theorem and approximation algorithm. *SIAM Journal on Computing*, 27(1):291–301, 1998.
4. Jean Bourgain. On Lipschitz embeddings of finite metric spaces in Hilbert space. *Israel Journal of Mathematics*, 52(1-2):46–52, 1985.
5. S.Chawla, A.Gupta, H.Rcke. Embeddings of negative-type metrics and an improved approximation to generalized sparsest cut. in Proceedings of the 16'th Annual ACM-SIAM Symposium on Discrete Algorithms, SODA'05., pp. 102-111, 2005.
6. A.Gupta, R.Krauthgamer, J.Lee. Bounded Geometries, Fractals, and Low-Distortion Embeddings. in *Proceedings of the 44th Annual Symposium on Foundations of CS, FOCS'03*, pp. 534-543, 2003.
7. J. Justesen, A class of constructive asymptotically good algebraic codes, *IEEE Transactions on Information*, 18:652-656, 1972.
8. S.Khot, A.Naor. Nonembeddability theorems via Fourier analysis. in *Proceedings of 46th Annual Symposium of FOCS 2005*:101-112, 2005.
9. P.Klein, S.Plotkin, and S.Rao. Excluded minors, network decomposition, and multicommodity flow. In *Proceedings of the 25th Annual ACM Symposium on Theory of Computing*, pages 682–690, 1993.
10. Nathan Linial, Eran London, and Yuri Rabinovich. The geometry of graphs and some of its algorithmic applications. *Combinatorica*, 15(2):215–245, 1995.
11. J.Matousek. Lectures on Discrete Geometry. Springer, 2002.
12. N.Linial, A.Wigderson Expander Graphs and their Applications. Bulletin of the American Math. Society, 43(4):439-561, 2006.
13. A.Wigderson, D.Xiao. Derandomizing the AW matrix-valued Chernoff bound using pessimistic estimators and applications. Electronic Colloquium on Computational Complexity, Report TR06-105, ISSN 1433-8092, 13th Year, 105th Report.