On the Strategyproofness of the Geometric Median

El-Mahdi El-Mhamdi
Calicarpa, École Polytechnique

Sadegh Farhadkhani*
EPFL

Rachid Guerraoui
EPFL

Lê-Nguyên Hoang*
Calicarpa, Tournesol

Abstract

The *geometric median*, an instrumental component of the secure machine learning toolbox, is known to be effective when robustly aggregating models (or gradients), gathered from potentially malicious (or strategic) users. What is less known is the extent to which the geometric median incentivizes dishonest behaviors. This paper addresses this fundamental question by quantifying its *strategyproofness*. While we observe that the geometric median is not even approximately strategyproof, we prove that it is *asymptotically α-strategyproof*: when the number of users is large enough, a user that misbehaves can gain at most a multiplicative factor α, which we compute as a function of the distribution followed by the users. We then generalize our results to the case where users actually care more about specific dimensions, determining how this impacts α. We also show how the *skewed geometric medians* can be used to improve strategyproofness.

1 INTRODUCTION

There has recently been a growing interest in collaborative machine learning to efficiently utilize the ever-increasing amount of data and computational resources (McMahan et al., 2017; Kairouz et al., 2021; Abadi et al., 2015). Collaborative learning gathers information from multiple users (e.g., gradient vectors (Zinkevich et al., 2010), local model parameters (Dinh et al., 2020; Farhadkhani et al., 2022b) or users' preferences (Noothigattu et al., 2018; Allouah et al., 2022)) and typically summarizes it in a single vector. While averaging is the most widely used method for aggregating multiple vectors into a single vector (Polyak and Juditsky, 1992), it suffers from severe security flaws: averaging can be arbitrarily manipulated by a single strategic user (Blanchard et al., 2017).

The geometric median is a promising "robust" alternative to averaging. It has been widely used in collaborative learning as it is a provably good approximation of the average (Minsker, 2015) and it is robust to a minority of malicious users (Lopuhaa and Rousseeuw, 1989). A large body of research known as "Byzantine learning" (Blanchard et al., 2017; Chen et al., 2017; El-Mhamdi et al., 2018; Rajput et al., 2019; Alistarh et al., 2018) uses the geometric median to ensure safe learning despite the presence of participants with arbitrarily malicious behavior (Farhadkhani et al., 2022a; Karimireddy et al., 2022; Acharya et al., 2022; Wu et al., 2020; So et al., 2021; Gu and Yang, 2021; Pillutla et al., 2022; Farhadkhani et al., 2022b). Interestingly, the geometric median also satisfies the fairness principle *"one voter, one vote with a unit force"* (see Section 2.2), making it ethically appealing.

In this paper, we study the extent to which the geometric median *incentivizes* strategic manipulations[1]. Ideally, we would like the geometric median to be *strategyproof* (Gibbard, 1973; Satterthwaite, 1975; Brandt et al., 2016), i.e., we want it to be in each voter's best interest to report their true preferred vector. Put differently, honesty would ideally be a *dominant strategy* (Chung and Ely, 2007). This is very different from *Byzantine learning*, which only focuses on the resilience of the training, usually assuming a *majority* of honest users. Conversely, we consider the more realistic case where *every* user wants to bias the algorithm towards their specific target states. Such considerations are critical for high-stake life-endangering applications such as content moderation and recommendation (Yue, 2019;

Authors are listed in alphabetical order.
*Correspondence to: sadegh.farhadkhani@epfl.ch, and len@tournesol.app.

Proceedings of the 26th International Conference on Artificial Intelligence and Statistics (AISTATS) 2023, Valencia, Spain. PMLR: Volume 206. Copyright 2023 by the author(s).

[1] Hence, we often use the term "voter" instead of "user".

Whitten-Woodring et al., 2020), in which different people have diverging preferences over what should be removed (Ribeiro et al., 2020; Bhat and Klein, 2020), accompanied with a warning message Mena (2020), and be promoted at scale (Michelman, 2020). Clearly, activists, companies and politicians all want to bias algorithms to promote certain views, products or ideologies (Hoang, 2020). These entities should thus be expected to behave untruthfully, if they can easily game the algorithms with fabricated behaviors.

Now, assuming that each user wants to minimize the distance between the computed geometric median and their target vector, it is actually known that the geometric median fails to be strategyproof (Kim and Roush, 1984) (see Figure 1). However, raw strategyproofness is a binary worst-case analysis. In practice, optimizing strategic reporting may be costly (e.g., information gathering and computational costs, and the risk of being exposed), and hence may not be profitable if the potential gain is small. This prompts us to *quantify* the strategyproofness of the geometric median: how much can a strategic voter gain by misreporting their preferred vector (Lubin and Parkes, 2012; Wang et al., 2015; Han et al., 2015)?

Contributions. Our first contribution is to show that the geometric median fails to guarantee approximate strategyproofness. More precisely, for any α, we show that there exists a configuration where a strategic voter can gain a factor α by behaving strategically rather than truthfully.

Our main contribution is to then study the more specific case where voters' reported vectors come independently from an underlying distribution. We prove that, in the limit where the number of voters is large enough, and with high probability, the geometric median is indeed α-strategyproof. This goes through introducing and formalizing the notion of *asymptotic strategyproofness* with respect to the distribution of reported vectors. We show how to compute the bound α as a function of this distribution.

Our two first contributions apply to the case where a voter wants to minimize the *Euclidean* distance between the geometric median and their target vector. Essentially, this amounts to saying that the voters' preferences are isotropic, i.e., all dimensions have the same importance for the voters. However, in practical applications, a voter may care a lot more about certain dimensions than others, Our third contribution is a generalization to this setting, proving that, in a rigorous sense, the geometric median becomes *less* strategyproof if some dimensions are both more polarized and more important than others.

As a fourth important contribution, we show how strategyproofness can be improved by introducing and analyzing the *skewed geometric median*. Intuitively, this corresponds to skewing the feature space using a linear transformation , computing the geometric median in the skewed space, and de-skewing the computed geometric median by applying $^{-1}$. In essence, the skewed geometric median can be used to weaken pulls along polarized dimensions, and strengthen pulls along others. This helps limit the incentives to exaggerate preferences along more polarized dimensions, by intuitively giving voters more voting power along orthogonal dimensions "at the same cost".

Background. Classically called the Fermat-Weber solution (Brimberg, 2017), the geometric median solves a version of the widely studied (optimal) facility location problem (Hansen et al., 1985; Walsh, 2020; Lu et al., 2009; Feigenbaum and Sethuraman, 2015; Tang et al., 2020; Escoffier et al., 2011; Sui and Boutilier, 2015; Kyropoulou et al., 2019; Fotakis and Tzamos, 2013), as it minimizes the sum of distances of the agents to the chosen location. In one dimension, the geometric median coincides with the median, which was shown (Moulin, 1980) to be (group) strategyproof. But in higher dimensions, the geometric median is known to be *not* strategyproof (Kim and Roush, 1984). To the best of our knowledge, however, our paper is the first to analyze the geometric median in high dimension, with weakened forms of strategyproofness like (asymptotic) α-strategyproofness. As far as we know, we are also the first to investigate skewed geometric medians and skewed preferences.

Roadmap. The rest of the paper is organized as follows. Section 2 formally defines different notions of strategyproofness and the geometric median aggregation rule. Section 3 proves that this rule is not α-strategyproof, whilst Section 4 proves that it is asymptotically α-strategyproof. In Section 5, we generalize our result to non-isotropic voters' preferences and to the skewed geometric median. Section 7 discusses related work, and Section 8 concludes. Due to space limitations, most of the proofs and some auxiliary results are provided in the appendices.

2 MODEL

We consider $1 + V$ voters. Each voter $v \in [V]$, $f1, \ldots, Vg$ reports a (potentially fabricated) vector $\theta_v \in \mathsf{R}^d$. We denote by $\vec{\theta}$, $(\theta_1, \ldots, \theta_V)$ the family of other voters' reported vectors. We then, without loss of generality[2], analyze the incentives of voter 0. We assume that voter 0 has a preferred *target* vector $t \in \mathsf{R}^d$, but they report a potentially different, *strategically* crafted, vector $s \in \mathsf{R}^d$. A voting algorithm VOTE then aggregates all voters' vectors into a common decision vector $\text{VOTE}(s, \vec{\theta}) \in \mathsf{R}^d$, which voter 0 would prefer to be close to their target vector t.

[2]Because all the votes that we consider are permutation invariant (Proposition 5 in Appendix A).

2.1 The Many Faces of Strategyproofness

We define the strategic gain as the best multiplicative gain that voter 0 can obtain by misreporting their preference, i.e. by reporting s instead of t. Strategyproofness bounds the maximal strategic gain.

Definition 1 (α-strategyproofness)**.** VOTE *is α-strategyproof if, for any others' vectors $\vec{\theta} \in \mathbb{R}^{d\times V}$, any target vector $t \in \mathbb{R}^d$ and any strategic vote $s \in \mathbb{R}^d$, the strategic gain is at most $1+\alpha$, i.e.*

$$\forall \vec{\theta}, t, s, \quad \left\| \text{VOTE}(t, \vec{\theta}) \quad t \right\|_2 \quad (1+\alpha) \left\| \text{VOTE}(s, \vec{\theta}) \quad t \right\|_2 .$$

Smaller values of α yield stronger guarantees. If $\alpha = 0$, then we simply say that VOTE *is strategyproof.*

The opposite of strategyproofness is an arbitrarily manipulable vote, which we define as follows.

Definition 2 (Arbitrarily manipulable)**.** VOTE *is arbitrarily manipulable by a single voter if, for any others' vectors $\vec{\theta} \in \mathbb{R}^{d\times V}$ and any target vector $t \in \mathbb{R}^d$, there exists $s \in \mathbb{R}^d$ such that* $\text{VOTE}(s, \vec{\theta}) = t$.

It is possible for a vector aggregation rule to be neither α-strategyproof nor arbitrarily manipulable. In fact, we show that this is the case for the geometric median. This remark calls for more subtle definitions of strategyproofness. In particular, it may be unreasonable to demand α-strategyproofness for *all* other voters' inputs $\vec{\theta} \in \mathbb{R}^{d\times V}$ (this is known as *dominant strategy incentive compatibility*). In practice, other voters are usually expected to report some vectors more often than others. This motivates us to consider an alternative high-probability definition of α-strategyproofness[3] taking into account the distribution of vectors. We thus introduce and study *asymptotic α-strategyproofness*. To define this notion, we first assume that other voters' vectors are drawn[4] independently from some distribution θ over $\mathbb{R}^d$. Asymptotic strategyproofness then corresponds to strategyproofness in the limit where V is large enough.

Definition 3 (Asymptotic α-strategyproofness)**.** VOTE *is asymptotically α-strategyproof if, for any $\varepsilon, \delta > 0$, there exists $V_0 \quad 1$ such that, as long as there are $V \quad V_0$ other voters whose reported vectors are drawn independently from distribution θ, then with probability at least $1 \quad \delta$, for any target vector $t \in \mathbb{R}^d$, and any strategic vote $s \in \mathbb{R}^d$, the strategic gain is bounded by $1 + \alpha + \varepsilon$, i.e.,*

$$\mathbb{P}_{\vec{\theta}\sim(\theta)^V} [\forall t, s : E(\alpha + \varepsilon, t, s)] \quad 1 \quad \delta,$$

where $E(\alpha + \varepsilon, t, s)$ is the event

$$\left\{ \left\| \text{VOTE}(t, \vec{\theta}) \quad t \right\| \quad (1 + \alpha + \varepsilon) \left\| \text{VOTE}(s, \vec{\theta}) \quad t \right\| \right\}.$$

If $\alpha = 0$, we say that VOTE *is asymptotically strategyproof.*

Note that this definition implicitly depends on the distribution θ of voters' inputs. In fact, we prove that the geometric median is asymptotically α-strategyproof, for a value of α that we derive from the distribution θ.

Finally, we also study the more general case of non-isotropic preferences. To model this, we replace the Euclidean norm by the S-Mahalanobis norm, for some positive definite matrix $S \quad 0$, which is given by $\|x\|_S \triangleq \|Sx\|_2$. Intuitively, the eigenvectors with larger eigenvalues of S represent the directions that matter more to the voter. Now, if voter 0 has an S-skewed preference, then they aim to minimize the S-Mahalanobis norm between the result of $\text{VOTE}(s, \vec{\theta})$ and the target vector t. This leads us to define strategyproofness for skewed preferences as follows.

Definition 4. VOTE *is α-strategyproof for an S-skewed preference if, for any others' vectors $\vec{\theta} \in \mathbb{R}^{d\times V}$, any target vector $t \in \mathbb{R}^d$ and any strategic vote $s \in \mathbb{R}^d$, The maximal strategic S-skewed gain is at most $1 + \alpha$, i.e.*

$$\forall t, s, \quad \left\| \text{VOTE}(t, \vec{\theta}) \quad t \right\|_S \quad (1 + \alpha) \left\| \text{VOTE}(s, \vec{\theta}) \quad t \right\|_S .$$

This notion can then be straightforwardly adapted to define asymptotic α-strategyproofness.

2.2 The Geometric Median

In this paper, we study the strategyproofness property of a particular VOTE, i.e., the geometric median. It can be defined for $1 + V$ voters using the average of distances between a vector z and the reported vectors:

$$L(s, \vec{\theta}, z) \triangleq \frac{1}{1 + V} \left(\|z \quad s\|_2 + \sum_{v\in[V]} \|z \quad \theta_v\|_2 \right).$$

We can now precisely define the geometric median.

Definition 5. *A geometric median* GM *operator is a function $\mathbb{R}^{d\times(1+V)} \to \mathbb{R}^d$ that outputs a minimizer of this average of distances, i.e., for any inputs $s \in \mathbb{R}^d$ and $\vec{\theta} \in \mathbb{R}^{d\times V}$, we must have $\text{GM}(s, \vec{\theta}) \in \arg\min_{z\in\mathbb{R}^d} L(s, \vec{\theta}, z)$.*

In dimension $d \quad 2$, the uniqueness of $\text{GM}(s, \vec{\theta})$ can be guaranteed when all vectors do not lie on a 1-dimensional line (Proposition 4 in Appendix A.2). Interestingly, the geometric median can be regarded as the result of a dynamic process, where, each voter pulls a point z towards their preferred vector with a unitary force. The geometric median is the equilibrium point, when all forces acting on z cancel out. It thus verifies the fairness principle *"one voter, one vote with a unit force"*. Formal discussion is provided in Appendix A.1.

[3] Our definition does not coincide with *Bayesian incentive compatibility*, which aims to bound one's *expected* strategic gain.

[4] This setting is similar to "Worst-case IID susceptibility" proposed by Lubin and Parkes (2012). But, we consider high probability bounds on the gain which is different from the expected regret defined by Lubin and Parkes (2012).

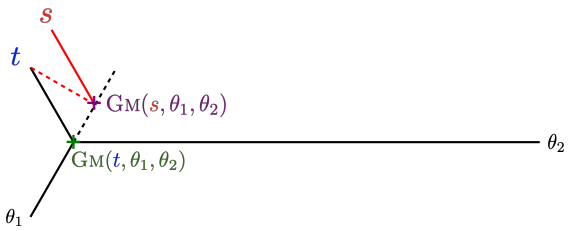

Figure 1: A simple example where the geometric median fails to be strategyproof. This example is easy to analyze in the limit where θ_2 is infinitely far on the right, in which case its pull is always towards the right. Since the unit pulls of all voters must cancel out, there must be a third of a turn between any two unit pull. This shows why, as the strategic voter reports s rather than their target vector t, the geometric median moves up the dotted line, closer to t.

3 MANIPULABILITY AND STRATEGYPROOFNESS

While the average is arbitrarily manipulable by a single voter (Blanchard et al., 2017), the geometric median is robust even to a collusion of a strict minority of voters. However, we prove that the geometric median is not (even approximately) strategyproof in the general case.

3.1 The Geometric Median is Not Arbitrarily Manipulable

As opposed to the average, a strategic voter cannot arbitrarily manipulate the geometric median. This property is sometimes known as *Byzantine resilience* in distributed computing, or as *statistical breakdown* in robust statistics. Here, we state it in the terminology of computational social choice, and we consider a slightly more general setting than *individual* manipulation. Namely, we consider *group* manipulation, by allowing a set of voters to collude. Even then, strategic voters can at most have a bounded impact. The proof of this result which is adapted from Lopuhaa and Rousseeuw (1989) is given in Appendix B.1.

Proposition 1 (Lopuhaa and Rousseeuw (1989))**.** *The geometric median is not arbitrarily manipulable by any minority of colluding voters.*

This result shows that a minority of strategic voters whose target vectors differ a lot from a large majority of other voters' reported vectors do not have full control over the output of the geometric median.

3.2 The Geometric Median is Not α-Strategyproof

The (geometric) median is slightly ill-behaved in dimension 1, when $1 + V$ is even. Typically, if $V = 1$, $s = t = 0$ and $\theta_1 = 1$, then any point between 0 and 1 is a geometric median (according to our definition). A common solution for this case is to take the middle point of the interval of the middle vectors. However, this solution now fails to be strategyproof. Indeed, voter 0 could now obtain $\text{GM}(s, \theta_1) = t$ by reporting $s = 1$. To retrieve strategyproofness in this setting, Moulin (1980) essentially proposed to add one (or any odd number of) fictitious voters. But, in higher dimensions, even when it is perfectly well-defined, the geometric median fails to guarantee strategyproofness. Figure 1 provides a simple proof of this, where voter 0 can gain by a factor of nearly $2\sqrt{3}/3 \approx 1.15$. Below, we prove a stronger result.

Theorem 1. *Even under* $\dim \vec{\theta} \geq 2$*, there is no value of* α *for which the geometric median is* α*-strategyproof.*

This more precise result has important implications: if a voter knows they gain a lot by strategic misreporting, then they will more likely invest in, e.g., business intelligence, to optimize their (mis)reporting. Their reported preferences will then more likely diverge from their honest preferences. We sketch the proof of Theorem 1 below. The full proof is highly non-trivial and is given in Appendix B.2.

Sketch of proof. We study the achievable set A_V, gathering all the possible values of the geometric median that a strategic voter can achieve by strategically choosing their reported vector. First we show that this set is the set

$$A_V \coloneqq \left\{ z \in \mathbb{R}^d \,\middle|\, \exists h \in \mathbb{R}_+ \; \nabla_z L(\vec{\theta}, z), \; \|h\|_2 \leq 1/V \right\}, \quad (1)$$

of points z where the loss restricted to other voters $v \in [V]$ has a subgradient of norm at most $1/V$ (Lemma 8). The proof of the theorem then corresponds to the example of Figure 2, where other voters' vectors are nearly one-dimensional. For a large number of voters, we prove, the achievable set is approximately a very flat ellipsoid defined by a matrix H that has very different eigenvalues. Then we show that the target vector t's pull is heavily skewed compared to the normal to the ellipsoid. This implies that voter 0 can obtain a significantly better geometric median by misreporting their target vector. □

Interestingly, on the positive side, the proof of Theorem 1 requires the strategic voter's target vector to take very precise locations to gain a lot by lying. Thus, while the geometric median has failure modes where some voters have strong incentives to misreport their preferences, in practice, such incentives are unlikely to be strong. On the negative side, our proof suggests the possibility of a vicious cycle. Namely, it underlines the fact that a strategic voter's optimal strategy is to report a vector that is closer to the subspaces where other voters' vectors mostly lie. These subspaces may be interpreted as the more polarized dimensions. As a result, if all voters behave strategically, we should expect the reported vectors to be even more flattened on these subspaces than voters' true target vectors. But

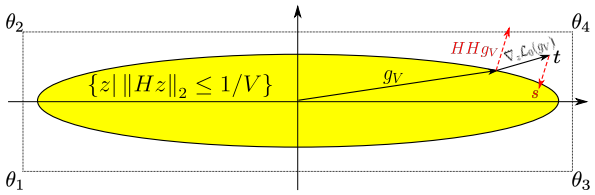

Figure 2: Illustration of the example where the geometric median fails to be α-strategyproof, for any value of α. Voters v 2 [4] report vectors that are nearly one dimensional. In the limit of a large number of voters, the achievable set for voter 0 is an ellipsoid. But the pull of voter 0's preferred vector turns out to be skewed compared to the normal to the ellipsoid. This means that voter 0 can obtain a significantly better geometric median by misreporting their preference.

then, if voters react strategically to the other voters' strategic votes, there are even more incentives to vote according to the one-dimensional line. In other words, the geometric median seems to initiate a vicious cycle where strategic voters are incentivized to escalate strategic behaviours, and this would lead them to essentially ignore all the dimensions of the vote except the most polarized one.

4 ASYMPTOTIC STRATEGYPROOFNESS

Our negative result of the previous section encourages us to weaken the notion of strategyproofness. We do so by replacing the bound on voters' strategic gains for *all* other voters' inputs with a bound for *most* of other inputs. We assume that each voter v reports a vector θ_v drawn independently from a probability distribution $\bar{\theta}$. We then study the maximal strategic gain of voter 0, when there are many other voters whose reported vectors are obtained this way. Any bound α that holds with high probability as the number V of voters is sufficiently large guarantees what we call *asymptotic α-strategyproofness* (see Definition 3).

Throughout this section, we consider a given fixed distribution $\bar{\theta}$ of voters' reported vectors. Our main result relies on the following mild smoothness assumption about the distribution $\bar{\theta}$ of other voters' vectors, which is clearly satisfied by numerous classical probability distributions over $\mathbb{R}^d$, like the normal distribution (with , $\mathbb{R}^d$).

Assumption 1. *There is a convex open set* $\mathbb{R}^d$, *with* d 5, *such that the distribution $\bar{\theta}$ yields a probability density function p continuously differentiable on , and such that* $\mathbb{P}[\theta$ 2] = 1 *and* $\mathbb{E}\|\theta\|_2 = \int_{\mathbb{R}^d} \|\theta\|_2 \, p(\theta) d\theta < 1$.

To simplify notations, we leave the dependence to the distribution implicit. For any number V 2 N of other voters, we denote by $\vec{\theta}_V$ 2 $\mathbb{R}^{d \times V}$ the random tuple of the V voters' reported vectors, and we define

$$L_{1:V}(z) \;,\; \frac{1}{V} \sum_{v \in [V]} \|z - \theta_v\|_2 \,, \tag{2}$$

and $g_{1:V}$, $\mathrm{GM}(\vec{\theta}_V)$ the random average of distances and the geometric median for the voters v 2 $[V]$. We denote by $L_{0:V}(s, z)$ and $g_{0:V}$, $\mathrm{GM}(s, \vec{\theta}_V)$ the similar quantities that also include voter 0's strategic vote s, and $g^{\dagger}_{0:V}$, $\mathrm{GM}(t, \vec{\theta}_V)$ the truthful geometric median, which results from voter 0's truthful reporting of t.

4.1 Infinite Limit

Consider the limit where V ! 1. The distribution $\bar{\theta}$ defines its own average-of-distance function:

$$L_\infty(z) \;,\; \mathbb{E}_{\theta \sim \bar{\theta}}[\|z - \theta\|_2] \,. \tag{3}$$

We say that g_∞ is a geometric median of the distribution $\bar{\theta}$ if it minimizes the loss L_∞. Under Assumption 1, the support of $\bar{\theta}$ is of full dimension d, which guarantees the uniqueness of the geometric median (Proposition 12 in Appendix C). We denote by H_∞ , $r^2 L_\infty(g_\infty)$ the Hessian at the geometric median. The properties of this matrix will be central to the strategyproofness of the geometric median.

Remark 1 (on the smoothness assumption)**.** *Note that Assumption 1 is a mild technical assumption, which intuitively guarantees that, for a sufficiently large number of voters, the infinite limit case will be approximately recovered. This will allow us to invoke some statistics of $\bar{\theta}$ to derive our strategyproofness bounds. In practice, assuming there are sufficiently many voters, then $\bar{\theta}$ may be estimated by the empirical distribution of the reported vectors.*

4.2 The Geometric Median is Asymptotically α-Strategyproof

One of our main results is that the geometric median is asymptotically α-strategyproof, for some appropriate value of α that depends on the skewness of the Hessian matrix H_∞. We define the skewness of a positive definite matrix S by

$$\begin{aligned} \mathrm{SKEW}(S) \;,\; \sup_{x \neq 0} \left\{ \frac{\|x\|_2 \|Sx\|_2}{x^T S x} \quad 1 \right\} \\ = \sup_{\|\mathbf{u}\|_2 = 1} \left\{ \frac{\|S\mathbf{u}\|_2}{\mathbf{u}^T S \mathbf{u}} \quad 1 \right\} . \end{aligned} \tag{4}$$

This quantity bounds the angle between a vector x and its linear transformation Sx. It is straightforward that $\mathrm{SKEW}(\beta S) = \mathrm{SKEW}(S)$ for all $\beta > 0$. Also the identity matrix has no skewness ($\mathrm{SKEW}(I) = 0$). Intuitively, the more S distorts the space, typically by having very different eigenvalues, the more skewed it is. In Section 4.4, we derive upper and lower bounds on SKEW. We can now present our main theorem.

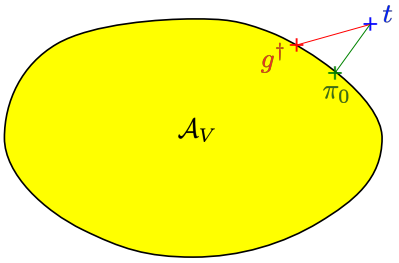

Figure 3: Illustration of our proof strategy. For a large number of voters, the achievable set $\mathcal{A}_V$ is approximately an ellipsoid. To derive the strategyproof bounds, we study the orthogonal projection π_0 of the target vector t. Strategyproofness then depends on the angle between $t \quad g^\dagger$ and $t \quad \pi_0$, which we derive from the skewness of the positive definite matrix that approximately defines the ellipsoid.

Theorem 2. *Under Assumption 1, the geometric median is asymptotically* SKEW(H_∞)*-strategyproof.*

Intuitively, the more the distribution of the reported vectors is flattened along some dimensions, which can be interpreted as more polarized dimensions, the worse the strategyproofness bound is. The proof of this theorem is given in Appendix C.2. In the next section, we provide a brief proof sketch to help the readers follow our reasoning.

4.3 Proof Techniques and Technical Challenges

The proof of Theorem 2 relies on the following steps:

1. Approximating the Achievable Set with an Ellipsoid. We first consider the infinite-case assuming a strategic voter with a very small voting power ε where the voting power of each voter is the magnitude of their pull compared to the sum of all pulls (see Section 2.2). By analyzing the Taylor's approximation of the gradient of the loss function for other voters, we show that the achievable set for the strategic voter (defined in (1)) becomes approximately an ellipsoid as $\varepsilon \; ! \; 0$. Now, as shown in Figure 3, since the ellipsoid is convex, the best-possible achievable point for the strategic voter is the orthogonal projection π_0 of the target vector t on the ellipsoid. By comparing the distance between t and π_0 to the distance between t and the geometric median $g^\dagger$ obtained by a truthful reporting of t, we then obtain what the strategic voter can gain by behaving strategically, in the infinite-voter case where they have a very small voting power ε. Intuitively, the more flattened the ellipsoid, the more the strategic voter can gain; conversely, for a quasi-hyperspherical ellipsoid, the strategic voter cannot gain by misreporting.

2. Deriving a Finite-voter Case from the Infinite One. To obtain meaningful strategyproofness guarantees, we consider the finite-voter case with a large (but not infinite) number of voters. Unfortunately, the finite-voter case is trickier than the infinite-voter case. To retrieve the strategyproofness bound, we need in addition to bound the divergence between the finite-voter case and the infinite-voter case. Fortunately, for V large enough, the voting power of a single strategic voter is small, which allows us to quasi-reduce the finite-voter case to the infinite-voter case. In fact, one important challenge of the proof is to leverage the well-behaved smoothness of the infinite-voter case to derive bounds for the finite-voter case, where singularities and approximation bounds make the analysis trickier. Indeed, while the infinite-voter loss function is smooth enough everywhere (under Assumption 1), the finite-voter loss function is not differentiable everywhere. At any point θ_v, it yields a nontrivial set of subgradients. This complicates the analysis, as we exploit higher order derivatives.

To address this difficulty, we identify different regions around the infinite-voter geometric median where the finite-voter loss function is well-behaved enough as shown in Figure 4. Namely, in high dimensions, assuming a smooth distribution θ, the distances between any two randomly drawn vectors are large. Concentration bounds allow us to guarantee that, with high probability, other voters' vectors θ_v are all far away from the infinite geometric median g_∞ (Lemma 14 in the Appendix). This has two important advantages. First, it guarantees the absence of singularities in a region around g_∞. Second, and more importantly, it allows us to control the variations of higher-order derivatives in this region (Lemma 16). This turns out to be sufficient to guarantee that the finite-voter geometric median is necessarily within this region.

3. Controlling the Largeness of the Third Derivative Tensor. Another challenge that we encountered was to guarantee that the achievable set in the finite-voter setting is convex. This condition is indeed critical to provide an upper bound on α, since it enables us to determine the strategic voter's optimal strategy by studying the orthogonal projection of the target vector onto the achievable set. To prove this condition, we identify a sufficient condition, which involves the third derivative tensor of the finite-voter loss function (lemmas 11 and 13). Fortunately, just as we manage to guarantee that the finite-voter geometric median is necessarily close enough to the infinite-voter geometric median (Lemma 15), using similar arguments based on concentration bounds, we successfully controlled the largeness of the third derivative tensor (Lemma 18). Therefore, for a large number of voters and with high probability, the achievable set is convex. Additionally, it is approximately an ellipsoid, which is characterized by the infinite-voter Hessian matrix H_∞. As a result, and since "rounder" ellipsoids yield better strategyproofness guarantees, when the number of voters is sufficiently large, the strategic gain of a strategic voter is upper-bounded by how skewed the infinite-voter Hessian matrix H_∞ is.

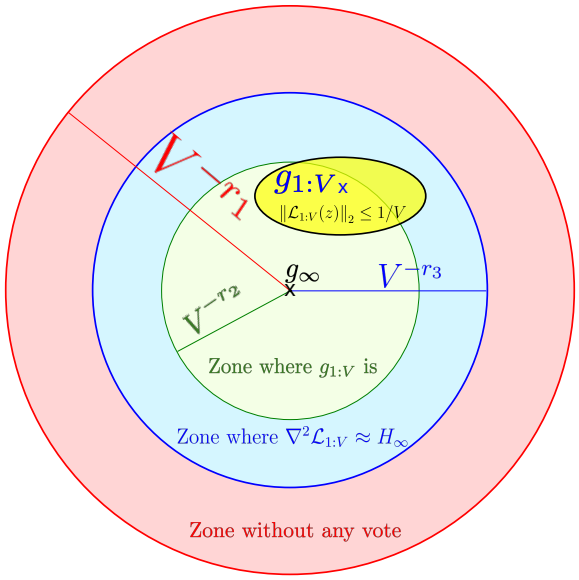

Figure 4: Illustration of the proof strategy for Theorem 2, which is based on the following claims that hold with high probability, for $2/d < 2r_1 < r_3 < r_2 < 1/2$, and for V large enough. First, there is no vote in $B(g_\infty, V^{-r_1})$ (a ball centered on g_∞, and of radius V^{-r_1}). Thus, $L_{1:V}$ is infinitely differentiable there. Moreover, the second and third derivatives of $L_{1:V}$ cannot be too different from the second and third derivatives of L_∞ in $B(g_\infty, V^{-r_3})$. Plus, $g_{1:V}$ lies in $B(g_\infty, V^{-r_2})$, and the set of geometric medians that voter 0 can obtain by misreporting their preferences is approximately an ellipsoid centered on $g_{1:V}$. This ellipsoid lies completely inside $B(g_\infty, V^{-r_3})$.

4.4 Bounds on SKEW

As we saw, the asymptotic strategyproofness of the geometric median depends on the skewness of the Hessian matrix H_∞, defined in Equation (4). In this section, we derive upper and lower bounds on the skewness function based on the ratio of the extreme eigenvalues of the matrix. Intuitively, the more different the eigenvalues of S are, the more skewed S is. We formalize this intuition with upper and lower bounds, whose proofs are given in Appendix C.3.

Proposition 2. *Denote* , $\frac{\max \text{SP}(S)}{\min \text{SP}(S)}$ *the ratio of extreme eigenvalues of* S. *Then* $\frac{1+}{2\sqrt{}}$ 1 SKEW(S) 1. *In dimension 2, the lower-bound inequality is an equality.*

5 SKEWNESS GENERALIZATIONS

We generalize our main result in two aspects. First, we consider skewed preferences where users give different weights to different dimensions. Second, we study the skewed geometric median which can be derived by rescaling the space before computing the geometric median.

5.1 Skewed Preferences

Our analysis so far rested on the assumption that voters have single-peaked preferences, which depend on the Euclidean distance between the geometric median and their preferred vectors. While this makes our analysis simpler, in practice, this assumption is not easy to justify. In fact, it seems reasonable to assume that some dimensions have greater importance for voters than others.

This motivates us to introduce S-skewed preferences, for a positive definite matrix S. More precisely, we say that a voter v has an S-skewed preference if they aim to minimize $kg \quad \theta_v k_S$, where g is the result of the vector vote and kzk_S , $kSzk_2$ is the S-Mahalanobis norm. Intuitively, the matrix S allows us to highlight which directions of space matter more to voter v. For instance, if $S = \begin{pmatrix} Y & 0 \\ 0 & 1 \end{pmatrix}$, with Y 1, it means that the voter gives a lot more importance to the first dimension than to the second dimension.

5.2 The Skewed Geometric Median

Intuitively, to counteract voters' strategic exaggeration incentives, we could make it more costly to express strong preferences along the more polarized and more important dimensions. In other words, voters would have a unit force along less polarized dimensions, and a less-than-unit force along more polarized dimensions. We capture this intuition by introducing " -skewed geometric median" for a positive definite matrix 0.

Skewed Loss. We define the -skewed infinite loss as

$$L_\infty(z, \theta) \text{ , } \mathsf{E}_{\theta \sim \theta} kz \quad \theta k \text{ ,}$$

using the -Mahalanobis norm (kzk , k zk_2), and we call -skewed geometric median g_∞ its minimum. We also introduce their finite-voter equivalents, for $1 + V$ voters, by

$$L_{0:V}(s, z) \text{ , } \frac{1}{1+V} ks \quad zk \ + \frac{1}{1+V} \sum_{v \in [V]} k\theta_v \quad zk \text{ ,}$$

and $g_{0:V} = \arg\min_z L_{0:V}(s, z)$. Intuitively, this is equivalent to mapping the original space to a new space using the linear transformation , and computing the geometric median in this new space (Lemma 23 in Appendix D).

Remark 2. *Interestingly, we also show that this skewed geometric median can be interpreted as modifying the way we measure the norm of voters' forces in the original space, thereby guaranteeing its consistency with the fairness principle* "one voter, one vote with a unit force". *The formal discussion is given in Appendix E.*

5.3 Strategyproofness of the Skewed Geometric Median for Skewed Preferences

For any skewing positive definite matrix , we define H_∞ , $r^2 L_\infty(g_\infty)$ the Hessian matrix of the skewed loss at the skewed geometric median. We then have the following asymptotic strategyproofness guarantee for an appropriately skewing matrix. The sketch of the proof is provided in Appendix D.

Theorem 3. *Under Assumption 1, the -skewed geometric median is asymptotically* $\textsc{Skew}(S^{-1}H_\infty S^{-1})$*-strategyproof for a voter with S-skewed preferences. In particular, if $H_\infty = S^{1/2}$, then the -skewed geometric median is asymptotically strategyproof for this voter.*

Interpretation. Let us provide additional insights into what the theorem says. Intuitively, the theorem asserts that the strategyproofness of the normal geometric median ($= I$) depends on how much an individual cares about polarized dimensions. More precisely, the more the voter cares about polarized dimensions, the less strategyproof the geometric median is.

Indeed, suppose that the first dimension is both highly polarized and very important to voter 0. The fact that it is polarized would typically correspond to a Hessian matrix of the form $H_\infty = \begin{pmatrix} 1 & 0 \\ 0 & X^2 \end{pmatrix}$, with X 1 (see the proof of Theorem 1). The fact that voter 0 cares a lot about the first dimension would typically correspond to a skewed preference matrix $S = \begin{pmatrix} Y & 0 \\ 0 & 1 \end{pmatrix}$, with Y 1. We then have $S^{-1}H_\infty S^{-1} = \begin{pmatrix} Y^{-2} & 0 \\ 0 & X^2 \end{pmatrix}$. By Proposition 2, we then have $\textsc{Skew}(S^{-1}H_\infty S^{-1}) = \frac{X^2+Y^{-2}}{2\sqrt{X^2Y^{-2}}}$ $1 = (XY)$, which is very large for X, Y 1. In particular, this makes the normal geometric median unsuitable for voting problems where some dimensions are much more polarized and regarded as important by most voters. Now, interestingly, if we find a skewing matrix that weakens the voters' pulls in the first dimensions, making the Hessian matrix approximately H_∞ $\begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{Y^2} \end{pmatrix}$, then the resulting geometric median becomes asymptotically strategyproof.

Remarks on the Skewed Hessian Matrix. In general, g_∞ g_∞ (Proposition 8 in Appendix A). This makes identifying a skewing matrix such that $H_\infty = S^{1/2}$ challenging. In particular, it is hard to determine how such a matrix relates to the statistics of . We note however the following connection between the Hessian matrix $r^2 L_\infty(z)$ of the -skewed loss and the Hessian matrix $r^2 L_\infty(z)$ of the Euclidean loss. The proof is given in Appendix D.2.

Proposition 3. *For any z $\mathbb{R}^d$, we have* $r^2 L_\infty(z) = (r^2 L_\infty)(z,)$.

Note that in particular, if $g_\infty^{(H_1^{1/2})} = g_\infty$ and if $r^2 L_\infty(H_\infty^{-1/2} z, H_\infty^{-1/2}) = H_\infty$, then the $H_\infty^{-1/2}$-skewed geometric median is asymptotically strategyproof. This will be the case if the support of g_∞ lies in the union of the eigenspaces of , as this implies that, when θ is drawn from , the vectors θ g_∞ and θ g_∞ are colinear and point in the same direction with probability 1. But, in general, these assumptions do not hold. This makes the computation of the appropriate skewing challenging. We thus leave open the problem of proving the existence and uniqueness (up to overall homothety) of such a matrix, as well as the design of algorithms to compute it.

6 NUMERICAL EXPERIMENT

Strategyproofness is commonly studied purely theoretically, as empirical strategyproofness evaluation is hard to perform in a meaningful and fair way. Indeed, it requires identifying optimal attacks against a system, which often amounts to solving an intractable optimization problem. In particular, if such an empirical evaluation fails to find an effective attack, it is unclear if this is because no such attack exists, or because no such attack has been found. Nevertheless, here we provide a simple experiment to evaluate the effect of the (skewness of the) underlying distribution on the strategic gain α when using the geometric median to aggregate voters' vectors. First, we sample 500000 vectors from a 2 dimensional Gaussian distribution with mean 0 and covariance matrix of $\begin{pmatrix} c & 0 \\ 0 & \frac{1}{c} \end{pmatrix}$ for a parameter c. Note that as shown in Proposition 2, c is closely related to the skewness of distribution . We assume the strategic voters have a 1% voting power, i.e., we simulate 5000 strategic voters all with the same target vector t. Then, to find a vulnerable target vector, we use a heuristic idea similar to that of Figure 2. Essentially, in each dimension, we find the extreme achievable geometric median for the strategic voters. The target vector t is then the combination of these extreme values of both dimensions. Finally, We approximately find the maximum strategic gain by performing a grid search of the best reported vector s in a neighborhood of t. Figure 5 shows the dependence of the strategic gain α on parameter c and validates the intuition that the more skewed the space, the less strategyproof geometric median is. This experiment demonstrates that the skewness of the underlying distribution is a crucial factor to consider when assessing the strategyproofness of geometric median.

7 RELATED WORK

Strategyproofness in one dimension has been extensively studied (Moulin, 1980; Procaccia and Tennenholtz, 2013; Feigenbaum and Sethuraman, 2015). It was shown (Moulin, 1980) that a generalized form of the median is group strategyproof, and that the randomized Con-

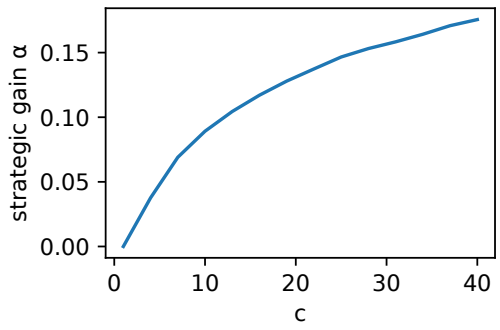

Figure 5: Dependence of the maximum strategic gain α on parameter c, where c is the square root of condition number of the underlying distribution's covariance matrix.

dorcet voting system is also group strategyproof for single-peaked preferences (Hoang, 2017). The one-dimension median was also leveraged for mechanism design without payment (Procaccia and Tennenholtz, 2013).

However, generalizing the median to higher dimensions is not straightforward (Lopuhaa and Rousseeuw, 1989). A common generalization known as the *coordinate-wise median*, was shown to be strategyproof, but not group strategyproof (Sui and Boutilier, 2015). The extent to which the generalized coordinate-wise median and the quantile mechanism are α-(group)-strategyproof have been studied by Sui and Boutilier (2015), though their definition slightly diverges from ours (their error is additive, not multiplicative). Remarkably, it was shown by Kim and Roush (1984) that, in dimension 2, the only strategyproof, anonymous and continuous voting system is the (generalized) coordinate-wise median.

Without restricting the dimension, but assuming the vectors to be taken from compact subsets of Euclidean spaces, strategyproof voting systems were characterized assuming all voters have generalized single-peaked preferences (Barberà et al., 1998). This approach built upon Border and Jordan (1983) which characterized strategyproof voting systems for Cartesian product ranges. In both cases, the set of strategyproof voting systems was defined as the class of *generalized (coordinate-wise) median voter schemes* which were shown in the case of Barberà et al. (1998) to also satisfy the intersection property introduced by[5] Barberà et al. (1997).

Overall, the coordinate-wise median has more desirable strategyproofness than the geometric median (Farhadkhani et al., 2021). It is also important to notice that, as opposed to the coordinate-wise median, the geometric median guarantees that the output vector belongs to the convex hull of voters' vectors (Proposition 9). This makes the coordinate-wise median unsuitable for problems where the space of relevant vectors is the convex hull of the input vectors. This holds, for instance, for the budget allocation problem, whose decision vector z must typically satisfy $z \quad 0$ and $\sum z[i] = 1$. In dimension 3, if three voters have preferences $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$, then the coordinate-wise median would output $(0,0,0)$ which may be undesirable. On the other hand, the geometric median would output $(1/3,1/3,1/3)$, which seems more desirable. Similarly, the coordinate-wise median is unfit to aggregate covariant matrices, which must be symmetric and semi-definite positive.

Another line of work focused on bounding the approximation ratio, which is the extent to which social cost is lost by using alternative aggregation rules like coordinate-wise median (Goel and Hann-Caruthers, 2020; Lu et al., 2009; Walsh, 2020). Several papers also consider other variations of this problem, e.g., choosing k facility locations instead of one (Escoffier et al., 2011), assigning different weights to different nodes (Zhang and Li, 2014), and assuming that the nodes lie on a network represented by a graph (Alon et al., 2010). Others have addressed the computational complexity of the geometric median (Cohen et al., 2016). Another work (Brady and Chambers, 1995) shows that for three agents the geometric median is the only rule that satisfies anonymity, neutrality, and Maskin-Monotonicity.

8 CONCLUSION

We analyzed different flavors of strategyproofness for the geometric median, an instrumental component of the secure machine learning toolbox. First, we showed that, in general, there can be no guarantee of approximate-strategyproofness, by exhibiting worst-case situations. However, we proved that, assuming that voters' vectors follow some distribution $\vec{\theta}$, asymptotic α-strategyproofness can be ensured. We then generalized our results to the case where some dimensions may matter more to the voters than other dimensions. In this setting, we proved that the geometric median becomes *less* strategyproof, when some dimensions are more polarized and more important than others. Finally, we showed how the skewed geometric median can improve asymptotic strategyproofness, by providing more voting rights along more consensual dimensions. Overall, our analysis helps better identify the settings where the geometric median can indeed be a suitable solution to high dimensional voting.

Acknowledgements

We thank Rafael Pinot for the very helpful comments on the presentation of the paper. We thank the anonymous reviewers for their constructive comments. This work has been supported in part by the Swiss National Science Foundation (SNSF) project 200021_200477.

[5]This property roughly guarantees a certain level of coordination between the decisions taken on each coordinate.

References

Abadi, M., Agarwal, A., Barham, P., Brevdo, E., Chen, Z., Citro, C., Corrado, G., Davis, A., Dean, J., Devin, M., Ghemawat, S., Goodfellow, I., Harp, A., Irving, G., Isard, M., Jia, Y., Jozefowicz, R., Kaiser, L., Kudlur, M., Levenberg, J., Mané, D., Monga, R., Moore, S., Murray, D., Olah, C., Schuster, M., Shlens, J., Steiner, B., Sutskever, I., Talwar, K., Tucker, P., Vanhoucke, V., Vasudevan, V., Viégas, F., Vinyals, O., Warden, P., Wattenberg, M., Wicke, M., Yu, Y., and Zheng, X. (2015). TensorFlow: Large-scale machine learning on heterogeneous distributed systems.

Acharya, A., Hashemi, A., Jain, P., Sanghavi, S., Dhillon, I. S., and Topcu, U. (2022). Robust training in high dimensions via block coordinate geometric median descent. In Camps-Valls, G., Ruiz, F. J. R., and Valera, I., editors, *Proceedings of The 25th International Conference on Artificial Intelligence and Statistics*, volume 151 of *Proceedings of Machine Learning Research*, pages 11145–11168. PMLR.

Alistarh, D., Allen-Zhu, Z., and Li, J. (2018). Byzantine stochastic gradient descent. In Bengio, S., Wallach, H., Larochelle, H., Grauman, K., Cesa-Bianchi, N., and Garnett, R., editors, *Advances in Neural Information Processing Systems*, volume 31. Curran Associates, Inc.

Allouah, Y., Guerraoui, R., Hoang, L., and Villemaud, O. (2022). Robust sparse voting. *CoRR*, abs/2202.08656.

Alon, N., Feldman, M., Procaccia, A., and Tennenholtz, M. (2010). Strategyproof approximation mechanisms for location on networks. *Center for Rationality and Interactive Decision Theory, Hebrew University, Jerusalem, Discussion Paper Series*.

Barberà, S., Massó, J., and Neme, A. (1997). Voting under constraints. *journal of economic theory*, 76(2):298–321.

Barberà, S., Massó, J., and Serizawa, S. (1998). Strategyproof voting on compact ranges. *games and economic behavior*, 25(2):272–291.

Bhat, P. and Klein, O. (2020). Covert hate speech: white nationalists and dog whistle communication on Twitter. In *Twitter, the Public Sphere, and the Chaos of Online Deliberation*, pages 151–172. Springer.

Blanchard, P., Mhamdi, E. M. E., Guerraoui, R., and Stainer, J. (2017). Machine learning with adversaries: Byzantine tolerant gradient descent. In Guyon, I., von Luxburg, U., Bengio, S., Wallach, H. M., Fergus, R., Vishwanathan, S. V. N., and Garnett, R., editors, *Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017, 4-9 December 2017, Long Beach, CA, USA*, pages 119–129.

Border, K. C. and Jordan, J. S. (1983). Straightforward elections, unanimity and phantom voters. *The Review of Economic Studies*, 50(1):153–170.

Brady, R. L. and Chambers, C. P. (1995). A spatial analogue of may's theorem. *Social Choice and Welfare*, 71.

Brandt, F., Conitzer, V., Endriss, U., Lang, J., and Procaccia, A. D. (2016). *Handbook of computational social choice*. Cambridge University Press.

Brimberg, J. (2017). The fermat—weber location problem revisited. *Mathematical Programming*, 49.

Chen, Y., Su, L., and Xu, J. (2017). Distributed statistical machine learning in adversarial settings: Byzantine gradient descent. *Proc. ACM Meas. Anal. Comput. Syst.*, 1(2).

Chung, K.-S. and Ely, J. C. (2007). Foundations of dominant-strategy mechanisms. *The Review of Economic Studies*, 74(2):447–476.

Cohen, M. B., Lee, Y. T., Miller, G. L., Pachocki, J., and Sidford, A. (2016). Geometric median in nearly linear time. In Wichs, D. and Mansour, Y., editors, *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, pages 9–21. ACM.

Dinh, C. T., Tran, N. H., and Nguyen, T. D. (2020). Personalized federated learning with moreau envelopes. In Larochelle, H., Ranzato, M., Hadsell, R., Balcan, M., and Lin, H., editors, *Advances in Neural Information Processing Systems 33: Annual Conference on Neural Information Processing Systems 2020, NeurIPS 2020, December 6-12, 2020, virtual*.

El-Mhamdi, E.-M., Guerraoui, R., and Rouault, S. (2018). The hidden vulnerability of distributed learning in Byzantium. In Dy, J. and Krause, A., editors, *Proceedings of the 35th International Conference on Machine Learning*, volume 80 of *Proceedings of Machine Learning Research*, pages 3521–3530. PMLR.

Escoffier, B., Gourvès, L., Kim Thang, N., Pascual, F., and Spanjaard, O. (2011). Strategy-proof mechanisms for facility location games with many facilities. In Brafman, R. I., Roberts, F. S., and Tsoukiàs, A., editors, *Algorithmic Decision Theory*, pages 67–81, Berlin, Heidelberg. Springer Berlin Heidelberg.

Farhadkhani, S., Guerraoui, R., Gupta, N., Pinot, R., and Stephan, J. (2022a). Byzantine machine learning made easy by resilient averaging of momentums. In Chaudhuri, K., Jegelka, S., Song, L., Szepesvari, C., Niu, G., and Sabato, S., editors, *Proceedings of the 39th International Conference on Machine Learning*, volume 162 of *Proceedings of Machine Learning Research*, pages 6246–6283. PMLR.

Farhadkhani, S., Guerraoui, R., and Hoang, L.-N. (2021). Strategyproof learning: Building trustworthy user-generated datasets. *ArXiV*.

Farhadkhani, S., Guerraoui, R., Hoang, L.-N., and Villemaud, O. (2022b). An equivalence between data poisoning and byzantine gradient attacks. In *Proceedings of*

the 39th International Conference on Machine Learning, Proceedings of Machine Learning Research.

Feigenbaum, I. and Sethuraman, J. (2015). Strategyproof mechanisms for one-dimensional hybrid and obnoxious facility location models. *AAAI Workshops*.

Fotakis, D. and Tzamos, C. (2013). On the power of deterministic mechanisms for facility location games. In Fomin, F. V., Freivalds, R., Kwiatkowska, M., and Peleg, D., editors, *Automata, Languages, and Programming*, pages 449–460, Berlin, Heidelberg. Springer Berlin Heidelberg.

Gibbard, A. (1973). Manipulation of voting schemes: a general result. *Econometrica: journal of the Econometric Society*, pages 587–601.

Goel, S. and Hann-Caruthers, W. (2020). Coordinate-wise median: Not bad, not bad, pretty good. *CoRR*, abs/2007.00903.

Gu, Z. and Yang, Y. (2021). Detecting malicious model updates from federated learning on conditional variational autoencoder. In *2021 IEEE International Parallel and Distributed Processing Symposium (IPDPS)*, pages 671–680.

Han, S., Topcu, U., and Pappas, G. J. (2015). An approximately truthful mechanism for electric vehicle charging via joint differential privacy. In *2015 American Control Conference (ACC)*, pages 2469–2475.

Hansen, P., Peeters, D., Richard, D., and Thisse, J.-F. (1985). The minisum and minimax location problems revisited. *Operations Research*, 33(6):1251–1265.

Hoang, L. N. (2017). Strategy-proofness of the randomized condorcet voting system. *Soc. Choice Welf.*, 48(3):679–701.

Hoang, L. N. (2020). Science communication desperately needs more aligned recommendation algorithms. *Frontiers in Communication*, 5:115.

Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., D'Oliveira, R. G. L., Eichner, H., Rouayheb, S. E., Evans, D., Gardner, J., Garrett, Z., Gascón, A., Ghazi, B., Gibbons, P. B., Gruteser, M., Harchaoui, Z., He, C., He, L., Huo, Z., Hutchinson, B., Hsu, J., Jaggi, M., Javidi, T., Joshi, G., Khodak, M., Konecný, J., Korolova, A., Koushanfar, F., Koyejo, S., Lepoint, T., Liu, Y., Mittal, P., Mohri, M., Nock, R., Özgür, A., Pagh, R., Qi, H., Ramage, D., Raskar, R., Raykova, M., Song, D., Song, W., Stich, S. U., Sun, Z., Suresh, A. T., Tramèr, F., Vepakomma, P., Wang, J., Xiong, L., Xu, Z., Yang, Q., Yu, F. X., Yu, H., and Zhao, S. (2021). Advances and open problems in federated learning. *Foundations and Trends® in Machine Learning*, 14(1–2):1–210.

Karimireddy, S. P., He, L., and Jaggi, M. (2022). Byzantine-robust learning on heterogeneous datasets via bucketing. In *International Conference on Learning Representations*.

Kim, K. and Roush, F. (1984). Nonmanipulability in two dimensions. *Mathematical Social Sciences*, 8(1):29–43.

Kyropoulou, M., Ventre, C., and Zhang, X. (2019). Mechanism design for constrained heterogeneous facility location. In *Algorithmic Game Theory: 12th International Symposium, SAGT 2019, Athens, Greece, September 30 – October 3, 2019, Proceedings*, page 63–76, Berlin, Heidelberg. Springer-Verlag.

Lopuhaa, H. P. and Rousseeuw, P. J. (1989). On the relation between s-estimators and m-estimators of multivariate location and covariance. *The Annals of Statistics*, pages 1662–1683.

Lu, P., Wang, Y., and Zhou, Y. (2009). Tighter bounds for facility games. In Leonardi, S., editor, *Internet and Network Economics*, pages 137–148, Berlin, Heidelberg. Springer Berlin Heidelberg.

Lubin, B. and Parkes, D. C. (2012). Approximate strategyproofness. *Current Science*, 103(9):1021–1032.

McMahan, B., Moore, E., Ramage, D., Hampson, S., and Arcas, B. A. y. (2017). Communication-Efficient Learning of Deep Networks from Decentralized Data. In Singh, A. and Zhu, J., editors, *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, volume 54 of *Proceedings of Machine Learning Research*, pages 1273–1282. PMLR.

Mena, P. (2020). Cleaning up social media: The effect of warning labels on likelihood of sharing false news on Facebook. *Policy & internet*, 12(2):165–183.

Michelman, P. (2020). Can we amplify the good and contain the bad of social media? *MIT Sloan Management Review*, 62(1):1–5.

Minsker, S. (2015). Geometric median and robust estimation in banach spaces. *Bernoulli*, 21(4):2308–2335.

Moulin, H. (1980). On strategy-proofness and single peakedness. *Public Choice*, 35(4):437–455.

Noothigattu, R., Gaikwad, S. N. S., Awad, E., Dsouza, S., Rahwan, I., Ravikumar, P., and Procaccia, A. D. (2018). A voting-based system for ethical decision making. In McIlraith, S. A. and Weinberger, K. Q., editors, *Proceedings of the Thirty-Second AAAI Conference on Artificial Intelligence, (AAAI-18), the 30th innovative Applications of Artificial Intelligence (IAAI-18), and the 8th AAAI Symposium on Educational Advances in Artificial Intelligence (EAAI-18), New Orleans, Louisiana, USA, February 2-7, 2018*, pages 1587–1594. AAAI Press.

Pillutla, K., Kakade, S. M., and Harchaoui, Z. (2022). Robust aggregation for federated learning. *IEEE Transactions on Signal Processing*, 70:1142–1154.

Polyak, B. T. and Juditsky, A. B. (1992). Acceleration of stochastic approximation by averaging. *SIAM Journal on Control and Optimization*, 30(4):838–855.

Procaccia, A. D. and Tennenholtz, M. (2013). Approximate mechanism design without money. *ACM Trans. Econ. Comput.*

Rajput, S., Wang, H., Charles, Z., and Papailiopoulos, D. (2019). Detox: A redundancy-based framework for faster and more robust gradient aggregation. In Wallach, H., Larochelle, H., Beygelzimer, A., d'Alché-Buc, F., Fox, E., and Garnett, R., editors, *Advances in Neural Information Processing Systems*, volume 32. Curran Associates, Inc.

Ribeiro, M. H., Jhaver, S., Zannettou, S., Blackburn, J., Cristofaro, E. D., Stringhini, G., and West, R. (2020). Does platform migration compromise content moderation? evidence from r/the_donald and r/incels. *CoRR*, abs/2010.10397.

Satterthwaite, M. A. (1975). Strategy-proofness and arrow's conditions: Existence and correspondence theorems for voting procedures and social welfare functions. *Journal of economic theory*, 10(2):187–217.

Smith, D. J. and Vamanamurthy, M. K. (1989). How small is a unit ball? *Mathematics Magazine*, 62(2):101–107.

So, J., Güler, B., and Avestimehr, A. S. (2021). Byzantine-resilient secure federated learning. *IEEE Journal on Selected Areas in Communications*, 39(7):2168–2181.

Sui, X. and Boutilier, C. (2015). Approximately strategyproof mechanisms for (constrained) facility location. In *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*, AAMAS '15, page 605–613, Richland, SC. International Foundation for Autonomous Agents and Multiagent Systems.

Tang, P., Yu, D., and Zhao, S. (2020). Characterization of group-strategyproof mechanisms for facility location in strictly convex space. In *Proceedings of the 21st ACM Conference on Economics and Computation*, EC '20, page 133–157, New York, NY, USA. Association for Computing Machinery.

Walsh, T. (2020). Strategy proof mechanisms for facility location in euclidean and manhattan space. *CoRR*, abs/2009.07983.

Wang, Q., Ye, B., Xu, T., Lu, S., and Guo, S. (2015). Approximately truthful mechanisms for radio spectrum allocation. *IEEE Transactions on Vehicular Technology*, 64(6):2615–2626.

Whitten-Woodring, J., Kleinberg, M. S., Thawnghmung, A., and Thitsar, M. T. (2020). Poison if you don't know how to use it: Facebook, democracy, and human rights in myanmar. *The International Journal of Press/Politics*, 25(3):407–425.

Wu, Z., Ling, Q., Chen, T., and Giannakis, G. B. (2020). Federated variance-reduced stochastic gradient descent with robustness to Byzantine attacks. *IEEE Transactions on Signal Processing*, 68:4583–4596.

Yue, N. (2019). The" weaponization" of facebook in myanmar: A case for corporate criminal liability. *Hastings LJ*, 71:813.

Zhang, Q. and Li, M. (2014). Strategyproof mechanism design for facility location games with weighted agents on a line. *Journal of Combinatorial Optimization*, 28(4):756–773.

Zinkevich, M., Weimer, M., Li, L., and Smola, A. (2010). Parallelized stochastic gradient descent. In Lafferty, J., Williams, C., Shawe-Taylor, J., Zemel, R., and Culotta, A., editors, *Advances in Neural Information Processing Systems*, volume 23. Curran Associates, Inc.

Appendix

Organization

The appendices are organized as follows:

- Appendix A proves some useful preliminary results about the geometric median that are needed in this paper.
- Appendix B includes the proofs of the results presented in Section 3 (in particular, the proof of Theorem 1).
- Appendix C includes some proofs and deferred results from Section 4 (in particular, the proof of Theorem 2).
- Appendix D includes some proofs and deferred results from Section 5 (in particular, the proof of Theorem 3).
- Appendix E discusses the notion of alternative unit forces and proves auxiliary results on the equivalence between ℓ_p penality and ℓ_q-unit force vote for $\frac{1}{p} + \frac{1}{q} = 1$ and the equivalence between -skewed geometric median, and $^{-1}$-unit forces.

A GEOMETRIC MEDIAN: PRELIMINARIES

In this section, we characterize a few properties of the geometric median, many of which are useful for our subsequent proofs. For the sake of exposition, we consider in this section a geometric median restricted to the voters $v \in [V]$, in which case, the loss function would be

$$L(\vec{\theta}, z) \triangleq \frac{1}{V} \sum_{v \in [V]} \|z - \theta_v\|_2 . \tag{5}$$

The generalization to $1 + V$ voters is straightforward.

A.1 Unit Forces

We first show that the geometric median verifies the fairness principle *"one voter, one vote with a unit force"*. Consider a system in which each voter v pulls the output of voting z towards their location θ_v with a unit force. Voter v's force is then given by the unit vector $\mathbf{u}_{z-\theta_v}$ in the direction of $z - \theta_v$. Any equilibrium of this process must then be a point z where all the forces cancel out, i.e., we must essentially have $\sum_{v \in V} \mathbf{u}_{z-\theta_v} = 0$. Lemma 2 shows that this condition is equivalent to the computation of a geometric median. But first, let us characterize the gradient of the ℓ_2-norm.

Lemma 1. *The gradient of the Euclidean norm is a unit vector. More precisely, for all $z \in \mathbb{R}^d$, we have $\nabla \|z\|_2 = \mathbf{u}_z$, where $\mathbf{u}_z \triangleq z/\|z\|_2$ if $z \neq 0$, and otherwise $\mathbf{u}_0 \triangleq B(0,1)$ is the unit ball centered at the origin.*

In the latter case, the ℓ_2 norm thus actually has a large set of subgradients.

Proof. Assume $z \neq 0$. We have $\nabla \|z\|_2^2 = 2z$. As a result, $\nabla \|z\|_2 = \nabla \sqrt{\|z\|_2^2} = \nabla \|z\|_2^2 / 2\sqrt{\|z\|_2^2} = z/\|z\|_2 = \mathbf{u}_z$.

Now consider the case $z = 0$. Then note that for all $x \in \mathbb{R}^d$, we have $\|x\|_2 - \|z\|_2 = x^T \mathbf{u}_x - x^T h$ for any vector h of Euclidean norm at most 1. This proves that $\nabla_{z=0} \|z\|_2 \subset B(0,1)$. On the other hand, if $\|h\|_2 > 1$, then we have $\|\varepsilon \mathbf{u}_h\|_2 = \varepsilon < \varepsilon \|h\|_2 = (\varepsilon \mathbf{u}_h)^T h$. Thus h cannot be a subgradient, and thus $\nabla_{z=0} \|z\|_2 = B(0,1) = \mathbf{u}_0$. □

As an immediate corollary, the following condition characterizes the geometric medians.

Lemma 2. *The sum of voters' unit pulls cancel out on $g \triangleq \text{GM}(\vec{\theta})$, i.e., $0 \in \sum_{v \in [V]} \mathbf{u}_{g-\theta_v}$.*

Proof. By Lemma 1, $\nabla_z \|z - \theta_v\|_2 = \mathbf{u}_{z-\theta_v}$. Therefore, $V \nabla_z L(\vec{\theta}, z) = \sum_{v \in [V]} \mathbf{u}_{z-\theta_v}$. The optimality condition of g then implies $0 \in \nabla_z L(\vec{\theta}, g)$ and hence $0 \in \sum_{v \in [V]} \mathbf{u}_{g-\theta_v}$. □

Before moving on, we make one last observation about the second derivative of the Euclidean norm, which is very useful for the rest of the paper.

Lemma 3. *Suppose $z \neq 0$. Then $r^2 \|z\|_2 = \frac{1}{\|z\|_2}\left(I \quad \mathbf{u}_z\mathbf{u}_z^T\right)$ is a positive semi-definite matrix. The vector z is an eigenvector of the matrix associated with eigenvalue 0, while the hyperplane orthogonal to z is the $(d-1)$-dimensional eigenspace of $r^2\|z\|_2$ associated with eigenvalue $1/\|z\|_2$.*

Notation: We denote by $z[i]$, the i-th coordinate of vector z.

Proof. For clarity, let us denote $\ell_2(z) := \|z\|_2$. By Lemma 1, we know that $r\,\ell_2(z) = \mathbf{u}_z = z/\ell_2(z)$. We then have

$$\partial^2_{ij}\ell_2(z) = \frac{1}{\ell_2(z)^2}\left(\ell_2(z)\partial_j z[i] \quad z[i]\partial_j\ell_2(z)\right) = \frac{1}{\ell_2(z)}\left(\delta_i^j \quad \frac{z[i]}{\ell_2(z)}\frac{z[j]}{\ell_2(z)}\right), \tag{6}$$

where $\delta_i^j = 1$ if $i = j$, and 0 if $i \neq j$. Combining all coordinates then yields

$$r^2\ell_2(z) = \frac{1}{\|z\|_2}\left(I \quad \frac{z}{\|z\|_2}\frac{z^T}{\|z\|_2}\right) = \frac{1}{\|z\|_2}\left(I \quad \mathbf{u}_z\mathbf{u}_z^T\right). \tag{7}$$

It is then clear that $r^2\ell_2(z)z = \frac{1}{\|z\|_2}\left(z \quad \mathbf{u}_z\mathbf{u}_z^T z\right) = 0$. Meanwhile, if $x \perp z$, then $\mathbf{u}_z^T x = 0$, which then results in $r^2\ell_2(z)x = x/\|z\|_2$. This proves the lemma. □

Intuitively, the lemma says that the pull of z on 0 does not change if we slightly move z along the direction z. However, this pull is indeed changed if we move z in a direction orthogonal to z. Moreover, the further away z is from 0, the weaker is this change in direction.

A.2 Existence and Uniqueness

In dimension one, the definition of the geometric median coincides with the definition of the median. As a result, the geometric median may not be uniquely defined. Fortunately, in higher dimensions, the uniqueness can be guaranteed, under reasonable assumptions. We first prove a few useful lemmas about the strict convexity of convex and piecewise strictly convex functions.

Lemma 4. *If f is convex on $[0,1]$, and strictly convex on $(0,1)$, then it is strictly convex on $[0,1]$.*

Proof. Consider $x, y \in [0,1]$, with $x < y$, $\lambda \in (0,1)$ and $\mu := 1 - \lambda$. Denote $z = \lambda x + \mu y$. It is straightforward to verify that $z \in (0,1)$. Define $x' := \frac{x+z}{2}$ and $y' := \frac{z+y}{2}$. Clearly, we have $x', y' \in (0,1)$. Moreover, $\lambda x' + \mu y' = \frac{1}{2}(\lambda x + \mu y) + \frac{1}{2}(\lambda + \mu)z = z$. By strict convexity of f in $(0,1)$, we then have $f(z) < \lambda f(x') + \mu f(y')$. Moreover, by convexity of f in $[0,1]$, we also have $f(x') \leq \frac{1}{2}f(x) + \frac{1}{2}f(z)$ and $f(y') \leq \frac{1}{2}f(y) + \frac{1}{2}f(z)$. Combining the three inequalities yields $f(z) < \frac{1}{2}\left(\lambda f(x) + \mu f(y)\right) + \frac{1}{2}f(z)$, from which we derive $f(z) < \lambda f(x) + \mu f(y)$. This allows to conclude. □

Lemma 5. *If $f : [0,1] \to \mathbb{R}$ is convex, and if there is $w \in (0,1)$ such that f is strictly convex on $(0,w)$ and strictly convex on $(w,1)$. Then, for any $x < w < y$, we have $f(w) < \frac{y-w}{y-x}f(x) + \frac{w-x}{y-x}f(y)$.*

Proof. Define $x' := \frac{x+w}{2}$ and $y' := \frac{w+y}{2}$. Since f is strictly convex on $(0,w)$, by Lemma 4, we know that it is strictly convex on $[0,w]$. As a result, we have $f(x') < \frac{1}{2}f(x) + \frac{1}{2}f(w)$. Similarly, we show that $f(y') < \frac{1}{2}f(y) + \frac{1}{2}f(w)$. Note now that $\frac{y-w}{y-x}x' + \frac{w-x}{y-x}y' = \frac{1}{2}\frac{(y-w)x+(w-x)y}{y-x} + \frac{w}{2} = w$. Using the convexity of f over $[0,1]$, we then have $f(w) \leq \frac{y-w}{y-x}f(x') + \frac{w-x}{y-x}f(y') < \frac{y-w}{y-x}\left(\frac{1}{2}f(x) + \frac{1}{2}f(w)\right) + \frac{w-x}{y-x}\left(\frac{1}{2}f(y) + \frac{1}{2}f(w)\right) = \frac{1}{2}\left(\frac{y-w}{y-x}f(x) + \frac{w-x}{y-x}f(y)\right) + \frac{1}{2}f(w)$. Rearranging the terms yields the lemma. □

Lemma 6. *If $f : [0,1] \to \mathbb{R}$ is convex, and if there is $w \in [0,1]$ such that f is strictly convex on $(0,w)$ and strictly convex on $(w,1)$, then f is strictly convex on $[0,1]$.*

Proof. Consider $x, z, y \in [0,1]$, with $x < z < y$. We denote $\lambda := \frac{z-x}{y-x} \in (0,1)$ and $\mu := 1 - \lambda$. We then have $z = \lambda x + \mu y$. If $x \neq w$ or $y \neq w$, then by Lemma 4, we know that $f(z) < \lambda f(x) + \mu f(y)$. Moreover, Lemma 5 yields the same equation for the case $x < z = w < y$.

Now assume $x < z < w < y$. By Lemma 5, we have $f(w) < \frac{y-w}{y-x} f(x) + \frac{w-x}{y-x} f(y)$. We also know that $z = \frac{w-z}{w-x} x + \frac{z-x}{w-x} w$. By strict convexity, we thus have $f(z) < \frac{w-z}{w-x} f(x) + \frac{z-x}{w-x} f(w) < \frac{w-z}{w-x} f(x) + \frac{z-x}{w-x} \left(\frac{y-w}{y-x} f(x) + \frac{w-x}{y-x} f(y) \right) = \lambda f(x) + \mu f(y)$.

The last case $x < w < z < y$ is dealt with similarly. □

Lemma 7. *Assume that $f : [0,1] \to \mathbb{R}$ is convex, and that there is a finite number of points $w_0 = 0 < w_1 < \ldots < w_{K-1} < w_K = 1$ such that f is strictly convex on (w_{k-1}, w_k) for $k \in [K]$. Then f is strictly convex on $[0,1]$.*

Proof. We prove this result by induction on K. For $K = 1$, we simply invoke Lemma 4. Now assume that it holds for $K - 1$, and let us use this to derive it for K. By induction, we know that f is strictly convex on $(0, w_{K-1})$ (we can use the induction hypothesis more rigorously by defining $g(x) = f(x w_{K-1})$). Yet, by assumption, f is also known to be convex on $(w_{K-1}, 1)$. Lemma 5 thus applies, and implies the strict convexity of f on $[0,1]$. □

In what follows, we define the dimension of the tuple $\vec{\theta}$ of preferred vectors as the dimension of the affine space spanned by these vectors, i.e., $\dim \vec{\theta} = \dim \{\theta_v - \theta_w \mid v, w \in [V]\}$. We then have the following result.

Proposition 4. *$z \mapsto L(\vec{\theta}, z)$ is infinitely differentiable for all $z \notin \{\theta_v \mid v \in [V]\}$. Moreover, if $\dim \vec{\theta} \geq 2$, then for all such z, the Hessian matrix of the sum of distances is positive definite, i.e., $\nabla_z^2 L(\vec{\theta}, z) > 0$. In particular, L is then strictly convex on $\mathbb{R}^d$, and has a unique minimum.*

Proof. Define $\ell_2(z) = \|z\|_2 = \sqrt{z^T z} = \sqrt{\sum_{i \in [d]} z_i^2}$. This function is clearly infinitely differentiable for all points $z \neq 0$. Since $L(\vec{\theta}, z) = \frac{1}{V} \sum \ell_2(z - \theta_v)$, it is also infinitely differentiable for $z \notin \{\theta_v \mid v \in [V]\}$.

Moreover, by using triangle inequality and absolute homogeneity, we know that, for any $\lambda \in [0,1]$ and any $\theta_v \in \mathbb{R}^d$, we have

$$\ell_2 \left((\lambda z + (1 - \lambda) z') - \theta_v \right) = \ell_2 \left(\lambda (z - \theta_v) + (1 - \lambda)(z' - \theta_v) \right) \tag{8}$$

$$\ell_2(\lambda (z - \theta_v)) + \ell_2((1 - \lambda)(z' - \theta_v)) = \lambda \ell_2(z - \theta_v) + (1 - \lambda) \ell_2(z' - \theta_v), \tag{9}$$

which proves the convexity of $z \mapsto \ell_2(z - \theta_v)$. Since the sum of convex functions is convex, we also know that $z \mapsto L(\vec{\theta}, z)$ is convex too.

Now, we know that $\dim(z, \vec{\theta}) - \dim(\vec{\theta}) \geq 2$. Therefore, there exists $v, w \in [V]$ such that $a = z - \theta_v$ and $b = z - \theta_w$ are not colinear. This implies that $-1 < \mathbf{u}_a^T \mathbf{u}_b < 1$. By Lemma 3, we then have

$$\nabla_z^2 L(\vec{\theta}, z) \geq \frac{1}{V \|a\|_2} \left(I - \mathbf{u}_a \mathbf{u}_a^T \right) + \frac{1}{V \|b\|_2} \left(I - \mathbf{u}_b \mathbf{u}_b^T \right) \tag{10}$$

$$\geq \frac{1}{V \max\{\|a\|_2, \|b\|_2\}} \left(2I - \mathbf{u}_a \mathbf{u}_a^T - \mathbf{u}_b \mathbf{u}_b^T \right) \tag{11}$$

$$\geq \frac{1}{V \max\{\|a\|_2, \|b\|_2\}} \left(2I - \frac{1}{2} (\mathbf{u}_a + \mathbf{u}_b)(\mathbf{u}_a + \mathbf{u}_b)^T - \frac{1}{2} (\mathbf{u}_a - \mathbf{u}_b)(\mathbf{u}_a - \mathbf{u}_b)^T \right) \tag{12}$$

$$= \frac{2}{V \max\{\|a\|_2, \|b\|_2\}} \left(I - \frac{1 + \mathbf{u}_a^T \mathbf{u}_b}{2} \frac{(\mathbf{u}_a + \mathbf{u}_b)(\mathbf{u}_a + \mathbf{u}_b)^T}{\|\mathbf{u}_a + \mathbf{u}_b\|_2^2} - \frac{1 - \mathbf{u}_a^T \mathbf{u}_b}{2} \frac{(\mathbf{u}_a - \mathbf{u}_b)(\mathbf{u}_a - \mathbf{u}_b)^T}{\|\mathbf{u}_a - \mathbf{u}_b\|_2^2} \right), \tag{13}$$

where we used $\|\mathbf{u}_a + \mathbf{u}_b\|_2^2 = 2 + 2\mathbf{u}_a^T \mathbf{u}_b$ and $\|\mathbf{u}_a - \mathbf{u}_b\|_2^2 = 2 - 2\mathbf{u}_a^T \mathbf{u}_b$. This last matrix turns out to have eigenvalues equal to $\frac{1 - \mathbf{u}_a^T \mathbf{u}_b}{V \max\{\|a\|_2, \|b\|_2\}}$ in the direction $\mathbf{u}_a + \mathbf{u}_b$, $\frac{1 + \mathbf{u}_a^T \mathbf{u}_b}{V \max\{\|a\|_2, \|b\|_2\}}$ in the direction $\mathbf{u}_a - \mathbf{u}_b$, and $\frac{1}{V \max\{\|a\|_2, \|b\|_2\}}$ in directions orthogonal to a and b. Since $-1 < \mathbf{u}_a^T \mathbf{u}_b < 1$, all such quantities are strictly positive. Thus all eigenvalues of $\nabla_z^2 L(\vec{\theta}, z)$ are strictly positive. This implies that along any segment (x, y) that contains no θ_v, then $z \mapsto L(\vec{\theta}, z)$ is strictly convex. Given that $z \mapsto L(\vec{\theta}, z)$ is convex everywhere, and that there is only a finite number of points θ_v, Lemma 7 applies, and proves the strict convexity of $z \mapsto L(\vec{\theta}, z)$ everywhere and along all directions. Uniqueness follows immediately from this.

To prove the existence of the geometric median, we observe that $L(z) \to L(0)$, for z large enough. More precisely, denote $\Delta = \max\{\|\theta_v\|_2 \mid v \in [V]\}$. Then $L(0) \leq \Delta$. Yet if $\|z\|_2 \geq 3\Delta$, then $\|z - \theta_v\|_2 \geq \|z\|_2 - \|\theta_v\|_2 \geq \|z\|_2 - \Delta \geq 3\Delta - \Delta = 2\Delta$,

which implies $L(z) \quad 2 \quad$. Thus $\inf_{z \in \mathbb{R}^d} L(z) = \inf_{z \in \mathcal{B}(0, \quad)} L(z)$, where $B(0, \quad)$ is a ball centered on 0, and of radius . By continuity of L and compactness of $B(0, \quad)$, we know that this infimum is reached by some point in $B(0, \quad)$. □

A.3 Symmetries

We contrast here the symmetry properties of the average, the geometric median and the coordinate-wise median.

Proposition 5. *Assuming uniqueness, the ordering of voters does not impact the average, the geometric median and the coordinate-wise median of their votes. This is known as the* anonymity *property.*

Proof. All three operators can be regarded as minimizing an anonymous function, namely, the sum of square distances, the sum of distances and the sum of ℓ_1 distances (see Section E). All such functions are clearly invariant under re-ordering of voters' labels. □

Proposition 6. *Assuming uniqueness, the average, the geometric median and the coordinate-wise median are invariant under translation and homothety. The average and the geometric median are also invariant under any orthogonal transformation, but, in general, the coordinate-wise median is not.*

Proof. The average and the geometric median can both be regarded as minimizing a function that only depends on Euclidean distances. Since any Euclidean isometry M is distance-preserving, if AVG and GM are the average and the geometric median of $\vec{\theta}$, and if $\tau \; 2 \; \mathbb{R}^d$ and $\lambda > 0$, it is clear that $\lambda M \text{AVG}(\vec{\theta}) + \tau$ and $\lambda M \text{GM}(\vec{\theta}) + \tau$ is the average and the geometric median of the family $\lambda M \vec{\theta} + \tau$.

In Section E, we show that the coordinate-wise median CW(.) minimizes a function that depends on ℓ_1 distances. By the same argument as above, this guarantees that the coordinate-wise median of $\lambda \vec{\theta} + \tau$ is $\lambda \text{CW}(\vec{\theta}) + \tau$. Now consider the vectors $\theta_1 \; , \; (0,0)$, $\theta_2 \; , \; (1,2)$ and $\theta_3 \; , \; (2,1)$. The coordinate-wise median of these vectors is $\text{CW}(\vec{\theta}) = (1,1)$. Now consider the rotation $R = \frac{\sqrt{2}}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ of these vectors around $(0,0)$ by an anti-clockwise eighth of a turn. We then obtain the vectors $R\theta_1 \; , \; (0,0)$, $R\theta_2 \; , \; \frac{\sqrt{2}}{2}(\quad 1,3)$ and $R\theta_3 \; , \; \frac{\sqrt{2}}{2}(1,3)$. Thus the coordinate-wise median of $R\vec{\theta}$ is $\text{CW}(R\vec{\theta}) = \frac{\sqrt{2}}{2}(0,3)$. However, $R\text{CW}(\vec{\theta}) = \frac{\sqrt{2}}{2}(0,2)$. Thus $\text{CW}(R\vec{\theta}) \neq R\text{CW}(\vec{\theta})$. □

Proposition 7. *Assuming uniqueness, if z is a center of symmetry of $\vec{\theta}$, then it is the average, the geometric median and the coordinate-wise median.*

Proof. We can pair all vectors of $\vec{\theta}$ different from z by their symmetry with respect to z. For any vote, the pull of each pair on z cancels out. Thus the sum of pulls vanishes. □

Proposition 8. *The average is invariant under any invertible linear transformation, but, even assuming uniqueness, in general, the geometric median and the coordinate-wise median are not.*

This proposition might appear to be a weakness of the geometric median. Note that Section 5.2 actually leverages this to define the *skewed geometric median* and improve strategyproofness.

Proof. The average is linear. Thus, for any matrix $M \; 2 \; \mathbb{R}^{d \times d}$, we have $\text{AVG}(M\vec{\theta}) = M\text{AVG}(\vec{\theta})$. Moreover, the case of the coordinate-wise median follows from Proposition 6.

To see that the geometric median is not invariant under invertible linear transformation, consider $\theta_1 \; , \; (1,0)$, $\theta_2 \; , \; (\cos(\tau/3), \sin(\tau/3)) = (\quad 1/2, \quad \sqrt{3}/2)$ and $\theta_3 \; , \; (\cos(2\tau/3), \sin(2\tau/3)) = (\quad 1/2, \quad \sqrt{3}/2)$, where $\tau \quad 6.28$ corresponds to a full turn angle. Then $\text{GM}(\vec{\theta}) = 0$, since the sum of pulls at 0 cancel out. Now let us stretch space in the y-axis, using the matrix $M = \begin{pmatrix} 1 & 0 \\ 0 & 2/\sqrt{3} \end{pmatrix}$. Clearly 0 is invariant under this stretch, as $M0 = 0$. Moreover, we have $M\theta_1 = (1,0)$, $M\theta_2 = (\quad 1/2, 1)$ and $M\theta_3 = (\quad 1/2, \quad 1)$. The unit-force pull on 0 by voter 2 is then $M\theta_2 / \|M\theta_2\|_2 = 2/\sqrt{5}(\quad 1/2, 1)$, while that of voter 3 is $M\theta_3 / \|M\theta_3\|_2 = 2/\sqrt{5}(\quad 1/2, \quad 1)$. Finally, voter 1 still pulls with a unit force towards the right. The sum of forces along the horizontal axis is then equal to $1 \quad 2/\sqrt{5} > 0$. Thus despite being invariant, 0 is no longer the geometric median.

The case of the coordinate-wise median follows from Proposition 6. □

Proposition 9. *The average and the geometric median of a tuple of vectors belong to the convex hull of the vectors. In general, the coordinate-wise median does not.*

Proof. Consider z not in the convex hull. Then there must exist a separating hyperplane, with a normal vector h, which goes from the convex hull to z. But then all vectors pull z in the direction of h. The projection of the sum of forces on h thus cannot be nil, which shows that z cannot be an equilibrium.

Now, to show that the coordinate-wise median may not lie within the convex hull of voters' vote, consider $\theta_1 = (1,0,0)$, $\theta_2 = (0,1,0)$ and $\theta_3 = (0,0,1)$. Then the coordinate-wise median is $(0,0,0)$. This clearly does not belong to the convex hull of $\vec{\theta}$. □

Proposition 10. *The geometric median is continuous on all points of $\vec{\theta}$, if* $\dim \vec{\theta}$ 2.

Proof. Consider $\vec{\theta}$ 2 $\mathbb{R}^{d\times V}$ with $\dim \vec{\theta}$ 2. By Proposition 4, there is a unique geometric median g , $\text{GM}(\vec{\theta})$.

To prove the continuity of GM, let us consider a sequence of families $\vec{\theta}^{(n)}$ such that $\vec{\theta}^{(n)}$! $\vec{\theta}$, and let us prove that this family eventually has a unique geometric median $g^{(n)}$, which converges to g as n ! 1 .

First note that the set of families $\vec{x}$ 2 $\mathbb{R}^{d\times V}$ for which $\dim \vec{x}$ 1 is isomorphic to the set of matrices of $\mathbb{R}^{d\times V}$ of rank at most 1. It is well-known that this set is closed for all norms in $\mathbb{R}^{d\times V}$ (this can be verified by considering the determinants of all 2 2 submatrices, which are all continuous functions). Thus the set of families $\vec{x}$ such that $\dim \vec{x}$ 2 is open. In particular, there is a ball centered on $\vec{\theta}$ whose points $\vec{x}$ all satisfy $\dim \vec{x}$ 2. Since, for n N_0 large enough, $\vec{\theta}^{(n)}$ must belong to this ball, it must eventually satisfy $\dim \vec{\theta}^{(n)}$ 2. This guarantees the uniqueness of $g^{(n)}$, $\text{GM}(\vec{\theta}^{(n)})$ for n N_0.

Now consider any convergent subsequence $g^{(n_k)}$! g^*. Since the geometric median minimizes the loss L, for any n_k 2 $\mathbb{N}$, we know that $L(g^{(n_k)}, \vec{\theta}^{(n_k)})$ $L(g, \vec{\theta}^{(n_k)})$. Taking the limit then yields $L(g^*, \vec{\theta})$ $L(g, \vec{\theta})$. Since g is the geometric median of $\vec{\theta}$, we thus actually have $L(g^*, \vec{\theta}) = L(g, \vec{\theta})$. But Proposition 4 guarantees the uniqueness of the geometric median. Therefore, we actually have $g^* = g$. Put differently, any convergent subsequence of $g^{(n)}$ converges to g.

Now by contradiction, assume $g^{(n)}$ does not converge to g. Thus, for any $\varepsilon > 0$, there is an infinite subsequence $g^{(n_i)}$ of $g^{(n)}$ lies outside the open ball $B(g,\varepsilon)$. But since the geometric median belongs to the convex hull of the vectors (Proposition 9), for n N_0, $g^{(n_i)}$ is clearly also bounded. Thus, by the Bolzano-Weierstrass theorem, the subsequence $g^{(n_i)}$ must have at least one converging subsequence, whose limit $g^\dagger$ lies outside the open ball $B(g,\varepsilon)$. But this contradicts the fact that every convergent subsequence of $g^{(n)}$ converges to g. Therefore, $g^{(n)}$ must converge to g. This proves that the geometric median is continuous with respect to $\vec{\theta}$. □

A.4 Approximation of the Average

One interesting feature of the geometric median and of the coordinate-wise median is that they are provably a good approximation of the average. Note that the uniqueness of the geometric median or of the coordinate-wise median is not needed for the following well-known proposition.

Proposition 11 (Minsker (2015))**.** *Denote by* $(\vec{\theta})$ *the covariance matrix of $\vec{\theta}$ defined by*

$$_{ij}(\vec{\theta}) \text{ , } \frac{1}{V}\sum_{v\in[V]} (\theta_v[i] \quad \text{AVG}(\vec{\theta})[i])(\theta_v[j] \quad \text{AVG}(\vec{\theta})[j]). \tag{14}$$

Then $\left\|\text{AVG}(\vec{\theta}) \quad \text{GM}(\vec{\theta})\right\|_2 \quad \sqrt{\text{TR}\left(\quad (\vec{\theta})\right)}$ *and* $\left\|\text{AVG}(\vec{\theta}) \quad \text{CW}(\vec{\theta})\right\|_2 \quad \sqrt{\text{TR}\left(\quad (\vec{\theta})\right)}$.

Proof. We start with the geometric median. Recall that $\text{GM}(\vec{\theta})$ minimizes z 7! $\mathbb{E}_v[k\theta_v \quad zk_2]$, where v is drawn uniformly randomly from $[V]$. It thus does better to minimize this term than $\text{AVG}(\vec{\theta})$. We then have

$$\left\|\text{AVG}(\vec{\theta}) \quad \text{GM}(\vec{\theta})\right\|_2 = \left\|\mathbb{E}_v[\theta_v] \quad \text{GM}(\vec{\theta})\right\|_2 \quad \mathbb{E}_v\left[\left\|\theta_v \quad \text{GM}(\vec{\theta})\right\|_2\right] \tag{15}$$

$$\mathbb{E}_v\left[\left\|\theta_v \quad \text{AVG}(\vec{\theta})\right\|_2\right] \quad \sqrt{\mathbb{E}_v\left[\left\|\theta_v \quad \text{AVG}(\vec{\theta})\right\|_2^2\right]} = \sqrt{\text{TR}\left(\quad (\vec{\theta})\right)}, \tag{16}$$

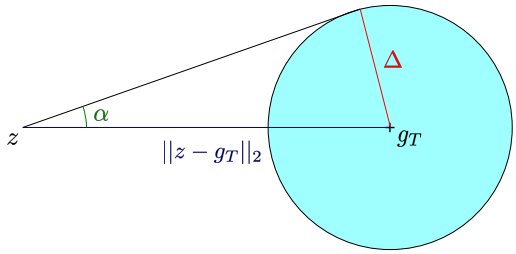

Figure 6: Resilience of the geometric median against coordinated attacks by a minority of strategic voters S, who pull on z in the opposite direction from a strict majority of truthful voters T, whose vectors are all in the ball centered on g_T and of radius .

where we also used Jensen's inequality twice for the function $x \mapsto \|x\|_2$ and $t \mapsto t^2$.

We now address the case of the coordinate-wise median. On dimension i, using similar arguments as in the proof above, this square of the discrepancy can be upper-bounded by the variance of θ along dimension i. In other words, we have $\left|\text{AVG}(\vec{\theta})[i] - \text{CW}(\vec{\theta})[i]\right| \leq \sqrt{V_{ii}(\vec{\theta})}$. Squaring this inequality, and summing over all coordinates then yields $\left\|\text{AVG}(\vec{\theta}) - \text{CW}(\vec{\theta})\right\|_2^2 \leq \sum_i V_{ii}(\vec{\theta}) = \text{TR}\left(V(\vec{\theta})\right)$. Taking the square root yields the second inequality of the proposition. □

B PROOFS OF SECTION 3

B.1 Proof of Proposition 1

Proof. Let us denote $[V] = T \sqcup S$ a decomposition of the voters into two disjoint subsets of truthful and strategic voters. We assume a strict majority of truthful voters, i.e., $|T| > |S|$. Denote $g_T \triangleq \text{GM}(\vec{\theta}_T)$ the geometric median of truthful voters' preferred vectors, and $\Delta \triangleq \max\{\|\theta_t - g_T\|_2 \mid t \in T\}$ the maximum distance between a truthful voters' preferred vector and the geometric median g_T.

Now consider any point $z \notin B(g_T, \Delta)$. The sum of forces on z by truthful voters has a norm equal to

$$\left\|\sum_{t\in T} \mathbf{u}_{\theta_t - z}\right\|_2 \geq \left(\sum_{t\in T} \mathbf{u}_{\theta_t - z}\right)^T \mathbf{u}_{g_T - z} = \sum_{t\in T} \mathbf{u}_{\theta_t - z}^T \mathbf{u}_{g_T - z} \tag{17}$$

$$= |T| \cos\alpha = |T| \sqrt{1 - \sin^2\alpha} = |T| \sqrt{1 - \frac{\Delta^2}{\|z - g_T\|_2^2}}, \tag{18}$$

where α is defined in Figure 6 as the angle between $g_T - z$ and a tangent to $B(g_T)$ that goes through z. But then the sum of all forces at z must be at least

$$\left\|\sum_{t\in T} \mathbf{u}_{\theta_t - z} + \sum_{v\in S} \mathbf{u}_{s - z}\right\|_2 \geq \left\|\sum_{t\in T} \mathbf{u}_{\theta_t - z}\right\|_2 - \left\|\sum_{v\in S} \mathbf{u}_{s - z}\right\|_2 \tag{19}$$

$$\geq |T| \sqrt{1 - \frac{\Delta^2}{\|z - g_T\|_2^2}} - \sum_{v\in S} \|\mathbf{u}_{s-z}\|_2 = |T| \sqrt{1 - \frac{\Delta^2}{\|z - g_T\|_2^2}} - |S| > 0, \tag{20}$$

as long as we have $\|z - g_T\|_2 > \frac{|T|}{\sqrt{|T|^2 - |S|^2}}\Delta$. A value of z that satisfies this strict inequality can thus not be a geometric median. Put differently, no matter what strategic voters do, we have

$$\text{GM}(\vec{\theta}_T, s) \in B\left(\text{GM}(\vec{\theta}_T), \left(1 - \frac{|S|^2}{|T|^2}\right)^{-1/2} \max_{t\in T} \left\|\theta_t - \text{GM}(\vec{\theta}_T)\right\|_2\right). \tag{21}$$

This concludes the proof. □

B.2 Proof of Theorem 1

To obtain Theorem 1, we make use of a technical lemma that characterizes the achievable set for the the strategic voter. Consider the set $A_V \triangleq \left\{z \in \mathbb{R}^d \,\middle|\, \exists h \in \partial_z L(\vec{\theta}, z),\ \|h\|_2 \leq 1/V\right\}$, of points z where the loss restricted to other voters $v \in [V]$ has a subgradient of norm at most $1/V$. We now observe that, by behaving strategically, voter 0 can choose any value for the geometric median within A_V.

Lemma 8. *For any $s \in \mathbb{R}^d$, $\mathrm{GM}(s, \vec{\theta}) \in A_V$. Moreover, for $\dim \vec{\theta} \geq 2$ and $s \in A_V$, we have $\mathrm{GM}(s, \vec{\theta}) = s$.*

Proof. Define $\ell_2(z) \triangleq \|z\|_2$. Now note that $(1+V)\,\partial_z L\left(s, \vec{\theta}, z\right) = \partial_z \ell_2(z - s) + V\,\partial_z L(\vec{\theta}, z)$. In other words, for any subgradient $h_{0:V} \in \partial_z L\left(s, \vec{\theta}, z\right)$, there exists $h_0 \in \partial_z \ell_2(z - s)$ and $h_{1:V} \in \partial_z L\left(\vec{\theta}, z\right)$ such that $(1+V)h_{0:V} = h_0 + Vh_{1:V}$. Note that any subgradient of ℓ_2 has at most a unit ℓ_2-norm (Lemma 1). Thus, $\|h_0\|_2 \leq 1$.

Now, assume $z \notin A_V$. Then for any $h_{1:V} \in \partial_z L\left(\vec{\theta}, z\right)$, we must have $\|h_{1:V}\|_2 > 1/V$. As a result,

$$(1+V)\,\|h_{0:V}\|_2 \geq \|Vh_{1:V} + h_0\|_2 \geq V\,\|h_{1:V}\|_2 - 1 > 0. \tag{22}$$

Thus, $0 \notin \partial_z L\left(s, \vec{\theta}, z\right)$, which means that z cannot be a geometric median. For any $s \in \mathbb{R}^d$, we thus necessarily have $\mathrm{GM}(s, \vec{\theta}) \in A_V$.

Now assume that $s \in A_V$. Then there must exist $h_{1:V} \in \partial_z L\left(\vec{\theta}, s\right)$ such that $V\,\|h_{1:V}\|_2 \leq 1$. Thus $h_0 \triangleq -Vh_{1:V} \in \partial_z \ell_2(z - s)$, for $z = s$, since the set of subgradients of ℓ_2 at 0 is the unit closed ball. We then have $h_0 + Vh_{1:V} = 0 \in \partial_z L\left(s, \vec{\theta}, s\right)$. Thus s minimizes $L\left(s, \vec{\theta}, \cdot\right)$. The uniqueness of the geometric median for $\dim(s, \vec{\theta}) \geq \dim \vec{\theta} \geq 2$ (Proposition 4) then implies that $\mathrm{GM}(s, \vec{\theta}) = s$. □

We now provide the detailed proof of Theorem 1 by formalizing the example of Figure 2.

Proof of Theorem 1. Define $\theta_1 = (-X, -1)$, $\theta_2 = (-X, 1)$, $\theta_3 = (X, -1)$ and $\theta_4 = (X, 1)$, with $X \geq 8$. We define the sum of distance restricted to these four inputs as

$$L_0(z) \triangleq \frac{1}{4}\sum_{v=1}^{4} \|\theta_v - z\|_2 . \tag{23}$$

Since 0 is a center of symmetry of the four inputs, it is the geometric median. Moreover, it can then be shown that the Hessian matrix at this optimum is

$$H \triangleq \nabla_z^2 L_0(0) = \frac{1}{4}(1+X^2)^{-3/2}\begin{pmatrix} 1 & 0 \\ 0 & X^2 \end{pmatrix}. \tag{24}$$

Note that the ratio between the largest and smallest eigenvalues of this Hessian matrix H is X^2, which can take arbitrarily large values. This observation turns out to be at the core of our proof. The eigenvalues also yield bounds on the norm of a vector to which H was applied. Using the inequality $X \geq 1$,

$$\frac{1}{32X^3}\|z\|_2 \leq \|Hz\|_2 \leq \frac{1}{4X}\|z\|_2 \leq \|z\|_2 . \tag{25}$$

In the vicinity of 0, since $\nabla_z L_0(0) = 0$ and since L_0 is infinitely differentiable in 0, we then have

$$\nabla_z L_0(z) = Hz + \varepsilon(z), \tag{26}$$

where $\|\varepsilon(z)\|_2 = O(\|z\|_2^2)$ when $z \to 0$. In fact, for $X \geq 1$, we know that there exists A such that, for all $z \in B(0,1)$, where $B(0,1)$ is the unit Euclidean ball centered on 0, we have $\|\varepsilon(z)\|_2 \leq A\|z\|_2^2$. We also define

$$\lambda \triangleq \inf_{z \in \mathcal{B}(0,1)} \min \mathrm{Sp}(\nabla_z^2 L_0(z)) \quad \text{and} \quad \mu \triangleq \sup_{z \in \mathcal{B}(0,1)} \max \mathrm{Sp}(\nabla_z^2 L_0(z)) \tag{27}$$

the minimal and maximal eigenvalues of the Hessian matrix of L_0 over the ball $B(0,1)$. By continuity (Lemma 20) and strong convexity, we know that $\mu \geq \lambda > 0$. We then have $\lambda I \preceq \nabla_z^2 L_0(z) \preceq \mu I$ over $B(0,1)$. From this, it follows that

$$\lambda \|z\|_2 \leq \|\nabla_z L_0(z)\|_2 \leq \mu \|z\|_2, \tag{28}$$

for all $z \in B(0,1)$. Now, since $\nabla_z^2 L_0(z) \succeq 0$ for all $z \in \mathbb{R}^d$, from this we also deduce that $\|\nabla_z L_0(z)\|_2 \geq \lambda$ if $z \notin B(0,1)$.

Now consider V honest voters such that $V/4 \in \mathbb{N}$ and $\theta_{4k+j} = \theta_j$, for $j \in [4]$ and $k \in [V/4 - 1]$. We denote by $\vec{\theta}_V$ this vector family. For any voter 0's strategic vote s, we then have

$$(1+V)L(s, \vec{\theta}_V, z) = \|s - z\|_2 + VL_0(z). \tag{29}$$

Note that we then have

$$(1+V)\nabla_z L(s, \vec{\theta}_V, z) = \mathbf{u}_{z-s} + V\nabla L_0(z), \tag{30}$$

where $\mathbf{u}_x \coloneqq \frac{x}{\|x\|_2}$ is the unit vector in the same direction as x. For all $z \notin B(0,1)$, we then have

$$\left\| \nabla_z L(s, \vec{\theta}_V, z) \right\|_2 \geq \frac{V\|\nabla L_0(z)\|_2 - \|\mathbf{u}_{z-s}\|_2}{1+V} \geq \frac{V\lambda - 1}{1+V} > 0, \tag{31}$$

for $V > 1/\lambda$. Thus, for $V > 1/\lambda$, we know that, for any s, we have $\textsc{Gm}(s, \vec{\theta}_V) \in B(0,1)$, where the inequality $\|\varepsilon(z)\|_2 \leq A\|z\|_2^2$ holds.

Since L_0 is strictly convex, there exists a unique $\alpha_V > 0$ such that $\left\| \nabla_z L_0(\alpha_V(X^3, 1)) \right\|_2 = 1/V$. Denote $g_V \coloneqq \alpha_V(X^3, 1)$. Now define

$$t = t(V) \coloneqq g_V + \frac{1}{\sqrt{V}} \nabla_z L_0(g_V). \tag{32}$$

The force of t on g_V is then the unit force with direction $t - g_V = \frac{1}{\sqrt{V}} \nabla_z L_0(g_V)$. Since $\|\nabla_z L_0(g_V)\|_2 = 1/V$, this unit vector must be $V\nabla_z L_0(g_V)$. Plugging this into the gradient of L (Equation (30)) shows that $\nabla_z L(t, \vec{\theta}_V, g_V) = 0$. Therefore, Lemma 2 and the uniqueness of the geometric median (Proposition 4) allow us to conclude that g_V is the geometric median of the true preferred vectors, i.e., $g_V = \textsc{Gm}(t, \vec{\theta}_V)$. Also, we have

$$\left\| t - \textsc{Gm}(t, \vec{\theta}_V) \right\|_2 = \frac{1}{\sqrt{V}} \|\nabla_z L_0(g_V)\|_2 = V^{-3/2}. \tag{33}$$

Since g_V is a geometric median of t and $\vec{\theta}_V$, we know that, for $V > 1/\lambda$, we have $g_V \in B(0,1)$. As a result, we have $\lambda \|g_V\|_2 \leq 1/V = \|\nabla_z L_0(g_V)\|_2 \leq \mu \|g_V\|_2$, and thus

$$1/\mu V \leq \|g_V\|_2 \leq 1/\lambda V. \tag{34}$$

Now, suppose that, instead of reporting t, voter 0 reports s, which is approximately the orthogonal projection of t on the ellipsoid $\{z \mid \|Hz\|_2 \leq 1/V\}$. More precisely, voter 0's strategic vote is defined as

$$s = s(V) \coloneqq t - \frac{2}{\sqrt{V}} \frac{g_V^T HHHg_V}{\|HHg_V\|_2^2} HHg_V \tag{35}$$

$$= g_V + \frac{1}{\sqrt{V}} \nabla_z L_0(g_V) - \frac{2}{\sqrt{V}} \frac{g_V^T HHHg_V}{\|HHg_V\|_2^2} HHg_V. \tag{36}$$

Given the inequalities $\|Hz\|_2 \leq \|z\|_2$ (Equation (25)) and $\|g_V\|_2 \leq 1/\lambda V$, the norm of s can be upper-bounded by

$$\|s\|_2 \leq \|g_V\|_2 + \frac{1}{\sqrt{V}} \|\nabla_z L_0(g_V)\|_2 + \frac{2}{\sqrt{V}} \frac{\|Hg_V\|_2 \|HHg_V\|_2}{\|HHg_V\|_2} \leq \frac{1 + (2+\lambda)V^{-1/2}}{\lambda V}. \tag{37}$$

Assuming $V \geq 1 + 3/\lambda$ then implies $\|s\|_2 \leq (3+\lambda)/\lambda V \leq 1$ and $\|s\|_2 = O(1/V)$. As a result, $\|\varepsilon(s)\|_2 \leq A\|s\|_2^2 = O(1/V^2)$. Thus

$$\|\nabla_z L_0(s)\|_2^2 = \|Hs + \varepsilon(s)\|_2^2 \tag{38}$$

$$\|Hs\|_2^2 + 2\|s\|_2 \|\varepsilon(s)\|_2 + \|\varepsilon(s)\|_2^2 \tag{39}$$

$$\|Hs\|_2^2 + O(1/V^3), \tag{40}$$

where the hidden constant in $O(1/V^3)$ depends on λ and A. Moreover, given that $\|g_V\|_2 = O(1/V)$ (Equation (34)) and $r_z L_0(g_V) = Hg_V + \varepsilon(g_V)$, by Equation (36), we have

$$\|Hs\|_2^2 = \|Hg_V\|_2^2 + \frac{2}{V}(Hg_V)^T H\left(Hg_V + \varepsilon(g_V) \quad 2\frac{g_V^T HHHg_V}{\|HHg_V\|_2^2} HHg_V\right) + O(1/V^3) \tag{41}$$

$$= \|r_z L_0(g_V) \quad \varepsilon(g_V)\|_2^2 + \frac{2}{V} g_V^T HHHg_V \quad \frac{4}{V} g_V^T HHHg_V + O(1/V^3) \tag{42}$$

$$\|r_z L_0(g_V)\|_2^2 \quad \frac{2}{V} g_V^T HHHg_V + O(1/V^3) \tag{43}$$

$$\frac{1}{V^2} \quad \frac{2}{V} g_V^T HHHg_V + O(1/V^3). \tag{44}$$

The hidden constants in $O(1/V^3)$ depend on λ, A, H and X. Since H has strictly positive eigenvalues and does not depend on V, we know that $g_V^T HHHg_V = (\|g_V\|_2^2) = (1/V^2)$. In particular, for V large enough $\frac{2}{V} g_V^T HHHg_V = (1/V^{2.5})$ takes larger values than $O(1/V^3)$. We then have $\|r_z L_0(s)\|_2 < 1/V$, which means that s lies inside the achievable set A_V. Therefore, Lemma 8 implies that for V large enough, by reporting s instead of t, voter 0 can move the geometric median from g_V to s, i.e., we have $\text{GM}(s, \vec{\theta}_V) = s$. But then, the distance between voter 0's preferred vector t and the manipulated geometric median is given by

$$\left\|\text{GM}(s, \vec{\theta}_V) \quad t\right\|_2 = \left\|\frac{2}{V} \frac{g_V^T HHHg_V}{\|HHg_V\|_2^2} HHg_V\right\|_2 = \frac{2}{V} \frac{(Hg_V)^T (HHg_V)}{\|HHg_V\|_2}. \tag{45}$$

Now recall that $g_V = \alpha_V(X^3, 1)$. Moreover, $\alpha_V \left\|H(X^3, 1)\right\|_2 = \|Hg_V\|_2 = \|r_z L_0(g_V) \quad \varepsilon(g_V)\|_2 = 1/V + O(1/V^2)$. Since $H(X^3, 1) = \frac{1}{4}(1 + X^2)^{-3/2}(X^3, X^2) = \frac{1}{4}X^2(1 + X^2)^{-3/2}(X, 1)$, we have $\left\|H(X^3, 1)\right\|_2 = \frac{1}{4}X^2(1 + X^2)^{-1}$. Thus, $\alpha_V = 4X^{-2}(1 + X^2)/V + O(1/V^2)$. As a result, we have $HHg_V = \frac{1}{16}\alpha_V X^3(1 + X^2)^{-3}(1, X)$. The norm of this vector is then $\|HHg_V\|_2 = \frac{1}{16}\alpha_V X^3(1 + X^2)^{-5/2}$. Moreover, its scalar product with Hg_V yields $(Hg_V)^T(HHg_V) = \frac{1}{32}\alpha_V^2 X^6(1 + X^2)^{-9/2}$. We thus have

$$\left\|\text{GM}(s, \vec{\theta}_V) \quad t\right\|_2 = \frac{\alpha_V}{V} \frac{X^6(1 + X^2)^{-9/2}}{X^3(1 + X^2)^{-5/2}} \tag{46}$$

$$= \frac{4X}{(1 + X^2)V^{3/2}} + O(V^{-5/2}) \tag{47}$$

$$= \frac{4X}{1 + X^2} \left\|t \quad \text{GM}(t, \vec{\theta}_V)\right\|_2 + O(V^{-5/2}). \tag{48}$$

In particular, for V large enough, we can then guarantee that

$$\left\|t \quad \text{GM}(t, \vec{\theta}_V)\right\|_2 > \frac{1 + X^2}{8X} \left\|\text{GM}(s, \vec{\theta}_V) \quad t\right\|_2 \tag{49}$$

$$= \left(1 + \frac{X^2 \quad 8X + 1}{8X}\right) \left\|\text{GM}(s, \vec{\theta}_V) \quad t\right\|_2. \tag{50}$$

This proves that the geometric median fails to be $\frac{X^2 - 8X + 1}{8X}$-strategyproof. But our proof holds for any value of X, and $\frac{X^2 - 8X + 1}{8X} \; ! \; 1$ as $X \; ! \; 1$. Thus, there is no value of α such that the geometric median is α-strategyproof. □

C PROOFS AND DIFFERENT RESULTS FROM SECTION 4

In this section we provide a formal proof for the main result of our paper which is Theorem 2. We start by proving a few useful facts about the infinite geometric median g_∞ defined on the distribution of the reported vectors.

C.1 Preliminary Results for the Infinite Limit Case

Lemma 9. *Under Assumption 1, with probability 1, we have* $\dim \vec{\theta}_V = \min\{V \quad 1, d\}$.

Proof. We prove this by induction over V. For $V = 1$, the lemma is obvious.

Assume now that the lemma holds for $V \quad d$. Then $\dim \vec{\theta}_V = V \quad 1$ with probability 1. The affine space generated by $\vec{\theta}_V$ is thus a hyperplane, whose Lebesgue measure is zero. Assumption 1 then implies that the probability of drawing a point on this hyperplane is zero. In other words, with probability 1, θ_{V+1} does not belong to the hyperplane, which implies that $\dim \vec{\theta}_{V+1} = \dim \vec{\theta}_V + 1 = (V + 1) \quad 1 \quad d$, which proves the induction.

Now assume that the lemma holds for $V \quad d + 1$. Then $\dim \vec{\theta}_V = d$ with probability 1. We then have $\dim \vec{\theta}_{V+1} \quad \dim \vec{\theta}_V = d$. Since this dimension cannot be strictly larger than d, we must then have $\dim \vec{\theta}_{V+1} = d$. This concludes the proof. □

Combing Lemma 9 with Proposition 4 guarantees the uniqueness of the geometric median for $V \quad 3$ under Assumption 1.

Lemma 10. *If $d \quad k + 1$, then $x \mapsto kxk_2^{-k}$ is integrable in $B(0,1)$, and $\int_{B(0,\varepsilon)} kxk_2^{-k}\, dx = O(\varepsilon)$ as $\varepsilon \to 0$.*

Proof. Consider the hyperspherical coordinates $(r, \varphi_1, \ldots, \varphi_{d-1})$, where $x_j = r\left(\prod_{i=1}^{j-1} \cos\varphi_i\right) \sin\varphi_j$. We then have $dx = r^{d-1}dr\left(\prod_{i=1}^{d-1} \cos^{d-i-1}\varphi_i d\varphi_i\right)$. The integral becomes

$$\int_{B(0,1)} kxk_2^{-k} = C(d)\int_0^1 r^{-k}r^{d-1}dr = C(d)\int_0^1 r^{d-1-k}dr, \tag{51}$$

where $C(d)$ is obtained by integrating appropriately all the angles of the hyperspherical coordinates, which are clearly integrable. But $\int_0^1 r^{d-1-k}dr$ is also integrable when $d \quad 1 \quad k \quad 0$. We conclude by noting that we then have $\int_0^\varepsilon r^{d-1-k}dr \;/\; \varepsilon^{d-k} = O(\varepsilon)$ for $d \quad k \quad 1$. □

Proposition 12. *Under Assumption 1, L_∞ is five-times continuously differentiable with a strictly positive definite Hessian matrix on . As a corollary, the geometric median g_∞ is unique and lies in .*

Proof. Let $z \; 2$ and $\delta > 0$ such that $B(z,\delta)$. By Leibniz's integral rule, we obtain

$$\nabla L_\infty(z) = \int \nabla_z kz \quad \theta k_2\, p(\theta)d\theta = \int \mathbf{u}_{z-\theta}p(\theta)d\theta. \tag{52}$$

To deal with the singularity at $\theta = z$, we first isolate the integral in the ball $B(z,\varepsilon)$, for some $0 < \varepsilon \quad \delta$. On this compact set, p is continuous and thus upper-bounded. We can then apply the previous lemma for $k = 0$ to show that this singularity is negligible as $\varepsilon \to 0$. Moreover, Leibniz's integral rule does apply, since $\mathbf{u}_{z-\theta}p(\theta)$ can be upper-bounded by $p(\theta)$ outside of $B(z,\delta)$, which is integrable by Assumption 1. This shows that L_∞ is continuously differentiable. To prove that it is twice-differentiable, we note that Leibniz's integral rule applies again. Indeed, we have

$$\nabla^2 L_\infty(z) = \int \nabla_z^2 kz \quad \theta k_2\, p(\theta)d\theta = \int \frac{I \quad \mathbf{u}_{z-\theta}\mathbf{u}_{z-\theta}^T}{kz \quad \theta k_2}p(\theta)d\theta, \tag{53}$$

But note that each coordinate of the matrix $\frac{I-\mathbf{u}_{z \;\theta}\mathbf{u}_{z \;\theta}^T}{\|z-\theta\|_2}$ is at most $\frac{1}{\|z-\theta\|_2}$. By virtue of the previous lemma, for $d \quad 2$, this is integrable in z. Moreover, by isolating the integration in the ball $B(z,\varepsilon)$, we show that the impact of the integration in this ball is negligible as $\varepsilon \to 0$. Finally, the rest of the integration is integrable, as $\frac{1}{\|z-\theta\|_2}p(\theta)$ can be upper-bounded by $\frac{1}{\delta}p(\theta)$ outside of $B(z,\delta)$, which is integrable by Assumption 1.

The cases of the third, fourth, and fifth derivatives are handled similarly, with now the bounds $\left|\partial^3_{ijk} kz \quad \theta k_2\right|$ $6/kz \quad \theta k_2^2$, $\left|\partial^4_{ijkl} kz \quad \theta k_2\right| \quad 36/kz \quad \theta k_2^3$ and $\left|\partial^5_{ijklm} kz \quad \theta k_2\right| \quad 300/kz \quad \theta k_2^4$, and using $d \quad 5$.

To prove the strict convexity, consider a point $z \; 2$ such that $p(z) > 0$. By continuity of p, for any two orthogonal unit vectors $\mathbf{u}_1$ and $\mathbf{u}_d$ and $\eta > 0$ small enough, we must have $p(z + \eta\mathbf{u}_1) > 0$ and $p(z + \eta\mathbf{u}_d) > 0$. For any $\varepsilon > 0$, there must then be a strictly positive probability to draw a point in $B(z,\varepsilon)$, a point in $B(z + \eta\mathbf{u}_1, \varepsilon)$, and a point in $B(z + \eta\mathbf{u}_d, \varepsilon)$. Moreover, for ε much smaller than η, then the three points thereby drawn cannot be colinear. We then obtain a situation akin to the proof of Proposition 4. By the same argument, this suffices to prove that the Hessian matrix must be positive definite. Therefore, L_∞ is strictly convex.

It follows straightforwardly from this that the geometric median is unique. Its existence can be derived by considering a ball $B(0, A)$ of probability at least $1/2$ according to $\tilde{\theta}$. If $\|z\|_2 \geq A + 2\mathbb{E}\|\theta\|_2$, then

$$L_\infty(z) \geq \frac{1}{2}(A + 2\mathbb{E}\|\theta\|_2 - A) \geq \mathbb{E}\|\theta\|_2 = L_\infty(0). \tag{54}$$

Thus L_∞ must reach a minimum in $B(0, A + 2\mathbb{E}\|\theta\|_2)$. Finally, we conclude that the geometric median must belong to , by re-using the argument of Proposition 9. □

C.2 Proof Steps for Theorem 2

In this section, we provide the full proof of Theorem 2 that consists of the following steps. First, in Section C.2.1, we find the sufficient conditions under which for a given function F the set $\{z : \|\nabla F(z)\|_2 \leq 1\}$ is convex. We then use this result to find sufficient conditions for the geometric median to become α-strategyproof in Section C.2.2. Then in Section C.2.3 we show that these conditions are satisfied with high probability when the number of voters is large enough. Next, Section C.2.4 proves that the SKEW function is continuous which is necessary for the proof of our theorem. Finally, Section C.2.5 combines these steps (lemmas 13, 14, 15,18, and 16) to prove Theorem 2 .

C.2.1 Higher Derivatives and Unit-norm Gradients

Note that our analysis involves the third derivative tensor to guarantee the convexity of the achievable set (defined in (1)). Therefore, here we provide a discussion about higher-order derivatives. We consider here a three-times continuously differentiable convex function F, and we study the set of points z such that $\|\nabla F(z)\|_2 \leq 1$. In particular, we provide a sufficient condition for the convexity of this set, based on the study of the first three derivatives of F. This convexity guarantee then allows us to derive a sufficient condition on $L_{1:V}$ to guarantee α-strategyproofness.

To obtain such guarantee, let us recall a few facts about higher derivatives. In general, the n-th derivative of a function $F : \mathbb{R}^d \to \mathbb{R}$ at a point z is a (symmetric) tensor $\nabla^n F(z) : \underbrace{\mathbb{R}^d \times \ldots \times \mathbb{R}^d}_{n \text{ times}} \to \mathbb{R}$, which inputs n vectors and outputs a scalar. This tensor $\nabla^n F(z)$ is linear in each of its n input vectors. More precisely, its value for input $[x_1 \; \ldots \; x_n]$ is

$$\nabla^n F(z)[x_1 \; \ldots \; x_n] = \sum_{i_1 \in [d]} \ldots \sum_{i_n \in [d]} (x_1[i_1]\, x_2[i_2] \ldots x_{n-1}[i_{n-1}]\, x_n[i_n])\, \partial^n_{i_1 \ldots i_n} F(z), \tag{55}$$

where $\partial^n_{i_1 \ldots i_n} F(z)$ is the n-th partial derivative of F with respect to the coordinates i_1, i_2, …, i_n (by the symmetry of derivation, the order in which F is derived along the different coordinates does not matter).

For $n = 1$, we see that $\nabla F(z)$ is simply a linear form $\mathbb{R}^d \to \mathbb{R}$. By Euclidean duality, $\nabla F(z)$ can thus be regarded as a vector, called the *gradient*, such that $\nabla F(z)[x] = x^T \nabla F(z)$. Note that if F is assumed to be convex, but not differentiable, $\nabla F(z)$ represents its set of subgradients at point z, i.e., $h \in \nabla F(z)$ if and only if $F(z + \delta) \geq F(z) + h^T\delta$ for all $\delta \in \mathbb{R}^d$. From this definition, it follows straightforwardly that z minimizes F if and only if $0 \in \nabla F(z)$.

For $n = 2$, $\nabla^2 F(z)$ is now a bilinear form $\mathbb{R}^d \times \mathbb{R}^d \to \mathbb{R}$. By isomorphism between (symmetric) bilinear forms and (symmetric) matrices, $\nabla^2 F(z)$ can equivalently be regarded as a (symmetric) matrix, called the *Hessian matrix*, such that $\nabla^2 F(z)[x \; y] = x^T \left(\nabla^2 F(z)\right) y$.

A bilinear form $B : \mathbb{R}^d \times \mathbb{R}^d \to \mathbb{R}$ is said to be *positive semi-definite* (respectively, *positive definite*), if $B[x \; x] \geq 0$ for all $x \in \mathbb{R}^d$ (respectively, $B[x \; x] > 0$ for all $x \neq 0$). If so, we write $B \succeq 0$ (respectively, $B \succ 0$). Moreover, given any $x \in \mathbb{R}^d$, the function $y \mapsto B[x \; y]$ becomes a linear form, which we denote $B[x]$. When the context is clear, $B[x]$ can equivalently be regarded as a vector. Finally, given two bilinear form $A, B : \mathbb{R}^d \times \mathbb{R}^d \to \mathbb{R}$, we can define their composition $A \circ B : \mathbb{R}^d \times \mathbb{R}^d \to \mathbb{R}$ by $A \circ B[x \; y] \triangleq A[x \; B[y]] = x^T ABy$, where, in the last equation, A and B are regarded as matrices.

We also need to analyze the third derivative of F, which can thus be regarded as a 3-linear form $\nabla^3 F(z) : \mathbb{R}^d \times \mathbb{R}^d \times \mathbb{R}^d \to \mathbb{R}$. Note as well that, for any 3-linear form W and any fixed first input $w \in \mathbb{R}^d$, the function $(x \; y) \mapsto W[w \; x \; y]$ is now a bilinear (symmetric) form $\mathbb{R}^d \times \mathbb{R}^d \to \mathbb{R}$. This (symmetric) bilinear form will be written $W[w]$ or $W \circ w$, which can thus equivalently be regarded as a (symmetric) matrix. Similarly, $W[x \; y]$ can be regarded as a linear form $\mathbb{R}^d \to \mathbb{R}$, or, by Euclidean duality, as a vector in $\mathbb{R}^d$.

Finally, we can state the following lemma, which provides a sufficient condition for the convexity of the sets of $z \in \mathbb{R}^d$ with a unit-norm F-gradient.

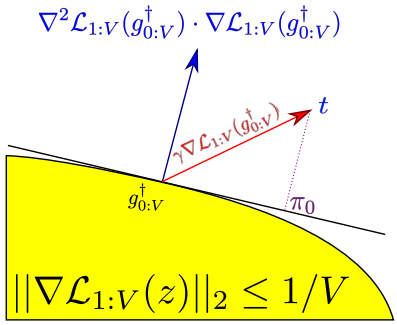

Figure 7: Illustration of what can be gained for target vector t , $g^\dagger_{0:V} + \gamma r L_{1:V}(g^\dagger_{0:V})$. The orthogonal projection π_0 of t on the tangent hyperplane of the achievable set going through $g^\dagger_{0:V}$ yields a lower bound on what can be achieved by voter 0 through their strategic vote s. This lower bound depends on the angle between $r L_{1:V}(g^\dagger_{0:V})$ and the normal to the hyperplane $r^2 L_{1:V}(g^\dagger_{0:V})$ $r L_{1:V}(g^\dagger_{0:V})$.

Lemma 11. *Assume that* C $\mathbb{R}^d$ *is convex and that* $r^2 F(z)$ $r^2 F(z) + r^3 F(z)$ $r F(z)$ 0 *for all* z C. *Then* z ?! $k r F(z) k_2^2$ *is convex on* C.

Proof. Fix i $[d]$. By Taylor approximation of $\partial_i F$ around z, for δ ! 0, we have

$$\partial_i F(z + \delta) = \partial_i F(z) + \sum_{j\in[d]} \delta_j \partial^2_{ij} F(z) + \frac{1}{2} \sum_{j,k\in[d]} \delta_j \delta_k \partial^3_{ijk} F(z) + o(k\delta k_2^2). \tag{56}$$

This equation can equivalently be written:

$$r F(z + \delta) = r F(z) + r^2 F(z)[\delta] + \frac{1}{2} r^3 F(z)[\delta \quad \delta] + o(\delta^2). \tag{57}$$

Plugging this into the computation of the square norm of the gradient yields:

$$k r F(z + \delta) k_2^2 = \left\| r F(z) + r^2 F(z)[\delta] + \frac{1}{2} r^3 F(z)[\delta \quad \delta] + o(\delta^2) \right\|_2^2 \tag{58}$$

$$= k r F(z) k_2^2 + 2 r^2 F(z) [r F(z) \quad \delta] + \left\| r^2 F(z)[\delta] \right\|_2^2 + r^3 F(z) [r F(z) \quad \delta \quad \delta] + o(k\delta k_2^2) \tag{59}$$

$$= k r F(z) k_2^2 + 2 r^2 F(z) [r F(z) \quad \delta] + \left(r^2 F(z) \quad r^2 F(z) + r^3 F(z) \quad r F(z) \right) [\delta \quad \delta] + o(k\delta k_2^2). \tag{60}$$

Therefore, matrix $2\left(r^2 F(z) \quad r^2 F(z) + r^3 F(z) \quad r F(z) \right)$ is the Hessian matrix of z ?! $k r F(z) k_2^2 = r F(z)^T r F(z)$. Yet a twice differentiable function with a positive semi-definite Hessian matrix is convex. □

Lemma 12. *Assume that* F *is convex, and that there exists* z^* $\mathbb{R}^d$ *and* $\beta > 0$ *such that, for any unit vector* $\mathbf{u}$, *there exists a subgradient* h $r F(z^* + \beta \mathbf{u})$ *such that* $\mathbf{u}^T h > 1$. *Then the set* A , $\left\{ z \; \mathbb{R}^d \;\middle|\; \exists h \; r F(z), \; k h k_2 \quad 1 \right\}$ *of points where* $r F$ *has a subgradient of at most a unit norm is included in the ball* $B(z^*, \beta)$.

Proof. Let z $B(z^*, \beta)$. Then there must exist $\gamma \quad \beta$ and a unit vector $\mathbf{u}$ such that $z \quad z^* = \gamma \mathbf{u}$. Denote $z_\mathbf{u}$, $z^* + \beta \mathbf{u}$. We then have $z \quad z_\mathbf{u} = (\gamma \quad \beta)\mathbf{u}$. Moreover, we know that there exists $h_{z_\mathbf{u}}$ $r F(z_\mathbf{u})$ such that $\mathbf{u}^T h_{z_\mathbf{u}} > 1$. By convexity of F, for any h_z $r F(z)$, we then have

$$(z \quad z_\mathbf{u})^T \left(h_z \quad h_{z_\mathbf{u}} \right) = (\gamma \quad \beta) \mathbf{u}^T \left(h_z \quad h_{z_\mathbf{u}} \right) \quad 0. \tag{61}$$

From this, it follows that $k h_z k_2 \quad \mathbf{u}^T h_z \quad \mathbf{u}^T h_{z_\mathbf{u}} > 1$. Thus z A. □

C.2.2 Sufficient Conditions for α-Strategyproofness

Recall from (1) that the achievable set A_V consists of the points z such that there exists a subgradient h $r_z L_{1:V}(z)$ such that $k h k_2 \quad 1/V$. Below, we identify a sufficient condition on A_V to guarantee α-strategyproofness. Note that as explained in the previous section, this analysis involves the third derivative tensor to guarantee the convexity of the achievable set, so that the proof ideas illustrated in Figure 7 are applicable.

Lemma 13. *Assume that* $\dim \vec{\theta}_V \geq 2$ *and that the following conditions hold for some* $\beta > 0$*:*

- **Smoothness:** $L_{1:V}$ *is three-times continuously differentiable on* $B(g_{1:V}, 2\beta)$.
- **Contains** A_V**:** *For all unit vectors* $\mathbf{u}$, $\mathbf{u}^T \nabla L_{1:V}(g_{1:V} + \beta\mathbf{u}) > 1/V$.
- **Convex** A_V**:** $\forall z \in B(g_{1:V}, \beta),\ \nabla^2 L_{1:V}(z) \succeq \nabla^2 L_{1:V}(z) + \nabla^3 L_{1:V}(z) \cdot \nabla L_{1:V}(z) \geq 0$.
- **Bounded skewness:** $\forall z \in B(g_{1:V}, \beta),\ \text{SKEW}(\nabla^2 L_{1:V}(z)) \leq \alpha$.

Then the geometric median is α*-strategyproof for voter* 0*.*

Proof. Given Lemma 8, we know that, for $t \in A_V$, we have $\left\|\text{GM}(t, \vec{\theta}_V) - t\right\|_2 = 0$, which guarantees α-strategyproofness for such voters.

Now assume $t \notin A_V$, and recall that we defined $g^\dagger_{0:V} \triangleq \text{GM}(t, \vec{\theta}_V)$ as the truthful geometric median. By Lemma 8, we know that $g^\dagger_{0:V} \in A_V$. Thus $t \neq g^\dagger_{0:V}$. Moreover, applying Lemma 12 to $F \triangleq VL_{1:V}$ guarantees that $A_V \subset B(g_{1:V}, \beta)$. The first condition shows that $L_{1:V}$ is 3-times differentiable in a neighborhood of $g^\dagger_{0:V}$. Plus, given the third condition, by Lemma 11, we know that A_V is a convex set.

Now, by definition, $g^\dagger_{0:V}$ must minimize the loss $L_{0:V}(t, \cdot)$, i.e., we must have

$$0 = \nabla L_{0:V}(t, g^\dagger_{0:V}) = \mathbf{u}_{g^\gamma_{0:V} - t} + V \nabla L_{1:V}(g^\dagger_{0:V}). \tag{62}$$

Equivalently, we have $\mathbf{u}_{t - g^\gamma_{0:V}} = V \nabla L_{1:V}(g^\dagger_{0:V})$. This means that $\left\|\nabla L_{1:V}(g^\dagger_{0:V})\right\|_2 = 1/V$, and that there must exist $\gamma > 0$ such that $t = g^\dagger_{0:V} + \gamma \nabla L_{1:V}(g^\dagger_{0:V})$.

For $\delta \in \mathbb{R}^d$ small enough, Taylor approximation then yields

$$\left\|\nabla F(g^\dagger_{0:V} + \delta)\right\|_2^2 = \left\|\nabla F(g^\dagger_{0:V}) + \nabla^2 F(g^\dagger_{0:V})[\delta] + o(\|\delta\|_2)\right\|_2^2 \tag{63}$$

$$= \left\|\nabla F(g^\dagger_{0:V})\right\|_2^2 + 2\nabla^2 F(g^\dagger_{0:V})\left[\nabla F(g^\dagger_{0:V}) \cdot \delta\right] + o(\|\delta\|_2) \tag{64}$$

$$= 1 + 2h^T\delta + o(\|\delta\|_2), \tag{65}$$

where $h \triangleq \nabla^2 F(g^\dagger_{0:V}) \cdot \nabla F(g^\dagger_{0:V})$.

Since $z \mapsto \|\nabla F(z)\|_2^2$ is convex on $B(g_{1:V}, \beta)$, we know that, in this ball, $2h$ is thus a subgradient of $z \mapsto \|\nabla F(z)\|_2^2$ at $g^\dagger_{0:V}$. Thus, in fact, for all $\delta \in B(g_{1:V} - g_{0:V}, \beta)$, we have $\left\|\nabla F(g^\dagger_{0:V} + \delta)\right\|_2^2 \geq 1 + 2h^T\delta$. Now assume that $g^\dagger_{0:V} + \delta \in A_V$. Then we must have $2h^T\delta \geq \left\|\nabla F(g^\dagger_{0:V} + \delta)\right\|_2^2 - 1 \geq 0$. In other words, we must have $A_V \subset H$, where $H \triangleq \left\{z \in \mathbb{R}^d \,\middle|\, h^T z \geq h^T g^\dagger_{0:V}\right\}$ is the half space of the hyperplane that goes through the truthful geometric median $g^\dagger_{0:V}$, and whose normal direction is h.

Using Lemma 8 and the inclusion $A_V \subset H$ then yields

$$\inf_{s \in \mathbb{R}^d} \left\|\text{GM}(s, \vec{\theta}_V) - t\right\|_2 = \inf_{z \in A_V} \|z - t\|_2 \geq \inf_{z \in \mathcal{H}} \|z - t\|_2 . \tag{66}$$

Yet the minimal distance between a point t and a half space H is reached by the orthogonal projection π_0 of t onto H, as depicted in Figure 7. We then have

$$\|t - \pi_0\|_2 = \left(\gamma \nabla L_{1:V}(g^\dagger_{0:V})\right)^T \frac{h}{\|h\|_2} = \frac{\gamma \nabla^2 L_{1:V}(g^\dagger_{0:V})\left[\nabla L_{1:V}(g^\dagger_{0:V}) \cdot \nabla L_{1:V}(g^\dagger_{0:V})\right]}{\left\|\nabla^2 L_{1:V}(g^\dagger_{0:V}) \cdot \nabla L_{1:V}(g^\dagger_{0:V})\right\|_2} \tag{67}$$

$$\geq \frac{\gamma \left\|\nabla L_{1:V}(g^\dagger_{0:V})\right\|_2}{1 + \text{SKEW}(\nabla^2 L_{1:V}(g^\dagger_{0:V}))} \geq \frac{\left\|\gamma \nabla L_{1:V}(g^\dagger_{0:V})\right\|_2}{1 + \alpha}, \tag{68}$$

using our fourth assumption. Yet note that $\left\| g^{\dagger}_{0:V} \quad t \right\|_2 = \left\| \gamma \, r \, L_{1:V}(g^{\dagger}_{0:V}) \right\|_2$. We thus obtain $\left\| g^{\dagger}_{0:V} \quad t \right\|_2 \quad (1 + \alpha) \, kt \quad \pi_0 k_2 \quad (1 + \alpha) \inf_{s \in \mathbb{R}^d} \left\| \textsc{Gm}(s, \vec{\theta}_V) \quad t \right\|_2$, which is the lemma. □

C.2.3 Finite-voter Guarantees

We show here that for a large enough number of voters and with high probability, finite-voter approximations are well-behaved and, in some critical regards, approximate correctly the infinite case. The global idea of the proof is illustrated in Figure 4. In particular, we aim to show that, when V is large, the achievable set A_V is approximately an ellipsoid within a region where $L_{1:V}$ is infinitely differentiable. In particular, we show that, with arbitrarily high probability under the drawing of other voters' vectors, for V large enough, the conditions of Lemma 13 are satisfied for $\beta \; , \quad (V^{-1})$ and $\alpha \; , \; \textsc{Skew}(H_\infty) + \varepsilon$.

An Infinitely-differentiable Region. Now, in order to apply Lemma 13, we need to identify a region near g_∞ where, with high probability, the loss function $L_{1:V}$ is infinitely differentiable. To do this, we rely on the observation that, in high dimensions, random points are very distant from one another. More precisely, the probability of randomly drawing a point ε-close to the geometric median g_∞ is approximately proportional to ε^d, which is exponentially small in d. This allows us to prove that, with high probability, none of the first V voters will be V^{-r_1}-close to the geometric median, where $r_1 > 1/d$ is a positive constant.

Lemma 14. *Under Assumption 1, for any $\delta_1 > 0$, and $r_1 > 1/d$, there exists $V_1(\delta_1) \in \mathbb{N}$ such that, for $V \quad V_1(\delta_1)$, with probability at least $1 \quad \delta_1$, we have $k\theta_v \quad g_\infty k_2 \quad V^{-r_1}$ for all voters $v \in [V]$. In particular, in such a case, $L_{1:V}$ is then infinitely differentiable in $B(g_\infty, V^{-r_1})$.*

Proof. Denote $p_\infty \; , \; 1 + p(g_\infty)$ the probability density at g_∞. Since p is continuous, we know that there exists $\varepsilon_0 > 0$ such that $p(z) \quad p_\infty$ for all $z \in B(g_\infty, \varepsilon_0)$. Thus, for any $0 < \varepsilon \quad \varepsilon_0$, we know that $\mathbb{P}[\theta \in B(g_\infty, \varepsilon)] \quad volume_d(\varepsilon) p_\infty$, where $volume_d(\varepsilon)$ is the volume of Euclidean d-dimensional ball with radius ε. Yet this volume is known to be upper-bounded by $8\pi^2 \varepsilon^d / 15$ (Smith and Vamanamurthy, 1989). Thus for $V \quad \varepsilon_0^{-1/r_1}$ (and thus $V^{-r_1} \quad \varepsilon_0$), we have $\mathbb{P}[\theta \in B(g_\infty, V^{-r_1})] \quad \frac{8\pi^2}{15} p_\infty V^{-r_1 d}$. Now note that

$$\mathbb{P}\left[\forall v \in [V], \; \theta_v \notin B(g_\infty, V^{-r_1})\right] = 1 \quad \mathbb{P}\left[\exists v \in [V], \; \theta_v \in B(g_\infty, V^{-r_1})\right] \tag{69}$$

$$1 \quad \sum_{v \in V} \mathbb{P}\left[\theta_v \in B(g_\infty, V^{-r_1})\right] \quad 1 \quad \frac{8\pi^2}{15} p_\infty V^{1 - r_1 d}. \tag{70}$$

Now recall that $r_1 > \frac{1}{d}$. We thus have $\frac{8\pi^2}{15} p_\infty V^{1 - r_1 d} \; ! \; 0$ as $V \; ! \; 1$. But now taking $V \quad V_1(\delta_1) \; , \; \max\left\{ \varepsilon_0^{-1/r_1}, (8\pi^2 p_\infty / 15\delta_1)^{1/(r_1 d - 1)} \right\}$, we see that, with probability at least $1 \quad \delta_1$, no voter $v \in [V]$ is V^{-r_1}-close to g_∞. Given the absence of singularity in $B(g_\infty, V^{-r_1})$ in such a case, $L_{1:V}$ is infinitely differentiable in this region. □

Approximation of the Infinite Geometric Median. The following lemma shows that as V grows, $g_{1:V}$ gets closer to g_∞ with high probability.

Lemma 15. *Under Assumption 1, for any $\delta_2 > 0$, and $0 < r_2 < 1/2$, there exists $V_2(\delta_2) \in \mathbb{N}$ such that, for all $V \quad V_2(\delta_2)$, with probability at least $1 \quad \delta_2$, we have $k g_{1:V} \quad g_\infty k_2 \quad V^{-r_2}$.*

Proof. Since $r \, L_\infty(g_\infty) = 0$ and L_∞ is three times differentiable, using Taylor's theorem around g_∞, for any $z \in B(0, 1)$, we have $r \, L_\infty(g_\infty + z) = H_\infty z + O(k z k_2^2)$. In particular, there exist a constant A such that for any $z \in B(0, 1)$, we have $k \, r \, L_\infty(g_\infty + z) \quad H_\infty z k_2 \quad A k z k_2^2$.

Now consider an orthonormal eigenvector basis $\mathbf{u}_1, \ldots, \mathbf{u}_d$ of H_∞, with respective eigenvalues $\lambda_1, \ldots, \lambda_d$. Note that since H_∞ is symmetric, we know that such a basis exists. We then define

$$\lambda_{min} \; , \; \inf_{z \in \mathcal{B}(g_1, 1)} \min Sp(r^2 L_\infty(z)), \tag{71}$$

the minimum eigenvalue of the Hessian matrix $r^2 L_\infty(z)$ over the closed ball $B(g_\infty, 1)$. Note that using the same argument as Proposition 12, we can say $r^2 L_\infty(z)$ is continuous and positive definite for all $z \in B(g_\infty, 1)$, therefore, λ_{min} is strictly

positive. Now for any $i \in [d]$, $j \in \{-1, 1\}$, and $0 < \varepsilon < 1$, we know that

$$\|\nabla L_\infty(g_\infty + j\varepsilon \mathbf{u}_i) - \lambda_i j\varepsilon \mathbf{u}_i\|_2 = \|\nabla L_\infty(g_\infty + j\varepsilon \mathbf{u}_i) - H_\infty j\varepsilon \mathbf{u}_i\|_2 \leq A\|j\varepsilon \mathbf{u}_i\|_2^2 = A\varepsilon^2. \tag{72}$$

Now define $\eta \triangleq \min\left\{\frac{1-2r_2}{4r_2}, 1\right\}$. Since $0 < r_2 < 1/2$, we clearly have $\eta > 0$. Moreover, for $\varepsilon < 1$, since $2 \geq 1 + \eta$, we have $\varepsilon^2 \leq \varepsilon^{1+\eta}$. Therefore, $\|\nabla L_\infty(g_\infty + j\varepsilon \mathbf{u}_i) - H_\infty j\varepsilon \mathbf{u}_i\|_2 \leq A\varepsilon^{1+\eta}$. For any voter $v \in [V]$, we then define the random unit vector

$$X_{ijv} \triangleq \frac{\theta_v \quad g_\infty \quad j\varepsilon \mathbf{u}_i}{\|\theta_v \quad g_\infty \quad j\varepsilon \mathbf{u}_i\|_2}. \tag{73}$$

Note that, since θ is absolutely continuous with respect to the Lebesgue measure (Assumption 1), all vectors X_{ijv}'s are well-defined with probability 1. By the definition of $L_{1:V}$ and L_∞, we then have

$$\nabla L_{1:V}(g_\infty + j\varepsilon \mathbf{u}_i) = \frac{1}{V}\sum_{v=1}^{V} X_{ijv} \quad \text{and} \quad \nabla L_\infty(g_\infty + j\varepsilon \mathbf{u}_i) = \mathbb{E}_{\theta_v}[X_{ijv}]. \tag{74}$$

Thus, for all $k \in [d]$, $\nabla L_{1:V}(g_\infty + j\varepsilon \mathbf{u}_i)[k]$ is just the average of V i.i.d. random variables within the range $[-1, 1]$, and whose expectation is equal to $\nabla L_\infty(g_\infty + j\varepsilon \mathbf{u}_i)[k]$. Therefore, by Chernoff bound, defining the event $E_{ijk}(t) \triangleq \{|\nabla L_{1:V}(g_\infty + j\varepsilon \mathbf{u}_i)[k] - \nabla L_\infty(g_\infty + j\varepsilon \mathbf{u}_i)[k]| > t\}$ for every $t > 0$, we obtain $\mathbb{P}[E_{ijk}(t)] \geq 1 - 2\exp(-t^2 V/2)$. Defining $e_{ij} = \nabla L_{1:V}(g_\infty + j\varepsilon \mathbf{u}_i) - \lambda_i j\varepsilon \mathbf{u}_i$, under event $E_{ijk}\left(A\varepsilon^{1+\eta}\right)$, by triangle inequality, we obtain

$$|e_{ij}[k]| \leq |\nabla L_{1:V}(g_\infty + j\varepsilon \mathbf{u}_i)[k] - \nabla L_\infty(g_\infty + j\varepsilon \mathbf{u}_i)[k]| + |\nabla L_\infty(g_\infty + j\varepsilon \mathbf{u}_i)[k] - \lambda_i j\varepsilon \mathbf{u}_i[k]| \tag{75}$$

$$\leq A\varepsilon^{1+\eta} + \|\nabla L_\infty(g_\infty + j\varepsilon \mathbf{u}_i) - \lambda_i j\varepsilon \mathbf{u}_i\|_2 \leq 2A\varepsilon^{1+\eta}. \tag{76}$$

Denoting E^* the event where such inequalities hold for all $i, k \in [d]$ and $j \in \{-1, 1\}$, and using union bound, we have

$$\mathbb{P}[E^*] \geq \mathbb{P}\left[\bigcap_{i\in[d]}\bigcap_{j\in\{-1,1\}}\bigcap_{k\in[d]} E_{ijk}\left(A\varepsilon^2\right)\right] = \mathbb{P}\left[\neg\bigcup_{i\in[d]}\bigcup_{j\in\{-1,1\}}\bigcup_{k\in[d]} \neg E_{ijk}\left(A\varepsilon^2\right)\right] \tag{77}$$

$$\geq 1 - \sum_{i\in[d]}\sum_{j\in\{-1,1\}}\sum_{k\in[d]} \mathbb{P}\left[\neg E_{ijk}\left(A\varepsilon^{1+\eta}\right)\right] \geq 1 - 4d^2\exp\left(-A^2\varepsilon^{2+2\eta}V/2\right). \tag{78}$$

Now note that by Proposition 4, we know that $L_{1:V}$ is convex. Therefore, for any $i \in [d]$ and $j \in \{-1, 1\}$, using the fact that $g_{1:V}$ minimizes $L_{1:V}$, we have

$$(g_{1:V} - g_\infty - j\varepsilon \mathbf{u}_i)^T \nabla L_{1:V}(g_\infty + j\varepsilon \mathbf{u}_i) = (g_{1:V} - g_\infty - j\varepsilon \mathbf{u}_i)^T(\lambda_i j\varepsilon \mathbf{u}_i + e_{ij}) \geq 0. \tag{79}$$

Rearranging the terms and noting that $\lambda_i > 0$ then yields

$$(g_{1:V} - g_\infty)^T\left(j\mathbf{u}_i + \frac{e_{ij}}{\varepsilon\lambda_i}\right) \geq (j\varepsilon \mathbf{u}_i)^T(j\mathbf{u}_i + \frac{e_{ij}}{\varepsilon\lambda_i}) = \varepsilon + \frac{j}{\lambda_i}\mathbf{u}_i^T e_{ij} \geq \varepsilon + \frac{j}{\lambda_i}e_{ij}[i]. \tag{80}$$

Now define $\varepsilon_0 \triangleq (\lambda_{min}/4dA)^{1/\eta}$. Under E^*, for $\varepsilon \leq \varepsilon_0$, this then implies $\|e_{ij}\|_\infty \leq 2A\varepsilon^{1+\eta} \leq 2A\varepsilon\varepsilon_0^\eta = \frac{\varepsilon\lambda_{min}}{2d} \leq \frac{\varepsilon\lambda_i}{2d}$. For every $i \in [d]$ and $j \in \{-1, 1\}$, we then have

$$(g_{1:V} - g_\infty)^T\left(j\mathbf{u}_i + \frac{e_{ij}}{\varepsilon\lambda_i}\right) \leq \varepsilon + \frac{1}{\lambda_i}\|e_{ij}\|_\infty \leq \varepsilon\left(1 + \frac{1}{2d}\right) \leq \frac{3\varepsilon}{2}. \tag{81}$$

Now denote $C \triangleq \|g_{1:V} - g_\infty\|_\infty$. Thus, there exist $i \in [d]$ and $j \in \{-1, 1\}$ such that $(g_{1:V} - g_\infty)[i] = jC$. We then obtain the lower bound

$$(g_{1:V} - g_\infty)^T\left(j\mathbf{u}_i + \frac{e_{ij}}{\varepsilon\lambda_i}\right) = C + \frac{(g_{1:V} - g_\infty)^T e_{ij}}{\varepsilon\lambda_i} \geq C - \frac{\|g_{1:V} - g_\infty\|_2\|e_{ij}\|_2}{\varepsilon\lambda_i} \tag{82}$$

$$\geq C - \frac{d\|g_{1:V} - g_\infty\|_\infty\|e_{ij}\|_\infty}{\varepsilon\lambda_i} \geq C - \frac{C}{2} = \frac{\|g_{1:V} - g_\infty\|_\infty}{2}, \tag{83}$$

where we used $\|x\|_2 = \sqrt{\sum x[k]^2} \leq \sqrt{d\|x\|_\infty^2} = \sqrt{d}\|x\|_\infty$ and the fact that $\|e_{ij}\|_\infty \leq \frac{\varepsilon\lambda_i}{2d}$. Combining Equations (81) and (83) then yields, under E^*, the bound $\|g_{1:V} - g_\infty\|_2 \leq \sqrt{d}\|g_{1:V} - g_\infty\|_\infty \leq 3\varepsilon\sqrt{d}$.

Now note that if $V \geq (3\sqrt{d}\varepsilon_0)^{-1/r_2}$, then we have $\varepsilon_V = V^{-r_2}/3\sqrt{d} \leq \varepsilon_0$. Thus, under E^* defined with ε_V, the previous argument applies, which implies $\|g_{1:V} - g_\infty\|_2 \leq V^{-r_2}$, as required by the lemma.

Now take $V \geq V_2(\delta_2) = \max\left\{\left(\frac{2(9d)^{1+\eta}}{A^2}\ln\frac{4d^2}{\delta_2}\right)^{\frac{1}{1-2r_2-2\eta r_2}}, (3\sqrt{d}\varepsilon_0)^{-1/r_2}\right\}$. By definition of η, we have $\eta \leq \frac{1-2r_2}{4r_2}$. As a result, using also the assumption $r_2 < 1/2$, we then have $1 - 2r_2 - 2\eta r_2 \geq \frac{1-2r_2}{2} > 0$. It then follows that $V^{1-2r_2-2\eta} \geq \frac{2(9d)^{1+\eta}}{A^2}\ln\frac{4d^2}{\delta_2}$. We then have

$$\mathsf{P}[E^*] \geq 1 - 4d^2\exp\left(-A^2\varepsilon_V^{2+2\eta}V/2\right) = 1 - 4d^2\exp\left(-\frac{A^2V^{1-2r_2-2\eta r_2}}{2(9d)^{1+\eta}}\right) \geq 1 - \delta_2, \tag{84}$$

which is what was needed for the lemma. □

Approximation of the Infinite Hessian Matrix. To apply Lemma 13, we need to control the values of the Hessian matrix of $L_{1:V}$. In this section, we show that, similar to the finite-voter geometric median $g_{1:V}$, which is now known to be close to the infinite geometric median g_∞, the Hessian matrix is close to the infinite Hessian matrix H_∞ at the infinite geometric median g_∞.

Lemma 16. *Under Assumption 1, for $0 < 2r_1 < r_3$, for any $\varepsilon_3, \delta_3 > 0$, there exists $V_3(\varepsilon_3, \delta_3) \in \mathbb{N}$ such that, for all $V \geq V_3(\varepsilon_3, \delta_3)$, with probability at least $1 - \delta_3$, there is no vote in the ball $B(g_\infty, V^{-r_1})$ and, for all $z \in B(g_\infty, V^{-r_3})$, we have $\left\|\nabla^2 L_{1:V}(z) - H_\infty\right\|_\infty \leq \varepsilon_3$.*

Before proving Lemma 16, we first start with an observation about unit vectors.

Lemma 17. *For any $0 < r_1 < r_3$, if $\|z\|_2 \leq V^{-r_1}$ and $\|\rho\|_2 \leq V^{-r_3}$, then for any $i \in [d]$, we have*

$$|\mathbf{u}_z[i] - \mathbf{u}_{z+\rho}[i]| = O(V^{r_1-r_3}) \tag{85}$$

Proof. We have the inequalities

$$|\mathbf{u}_z[i] - \mathbf{u}_{z+\rho}[i]| = \left|\frac{z[i]}{\|z\|_2} - \frac{(z+\rho)[i]}{\|z+\rho\|_2}\right| = \left|\frac{\|z+\rho\|_2 z[i] - \|z\|_2(z+\rho)[i]}{\|z\|_2\|z+\rho\|_2}\right| \tag{86}$$

$$\left|\frac{(\|z+\rho\|_2 - \|z\|_2)|z[i]| - \|z\|_2\rho[i]}{\|z\|_2(\|z\|_2 - \|\rho\|_2)}\right| \tag{87}$$

$$\left|\frac{\|z+\rho\|_2 - \|z\|_2}{\|z\|_2 - \|\rho\|_2}\right| + \left|\frac{\rho[i]}{\|z\|_2 - \|\rho\|_2}\right| \tag{88}$$

$$\frac{2\|\rho\|_2}{\|z\|_2 - \|\rho\|_2}, \tag{89}$$

where we used the fact that $\|z+\rho\|_2 - \|z\|_2 \leq \|\rho\|_2$. We then have

$$|\mathbf{u}_z[i] - \mathbf{u}_{z+\rho}[i]| \leq \frac{2V^{-r_3}}{V^{-r_1} - V^{-r_3}} \leq \frac{2V^{r_1-r_3}}{1 - V^{r_1-r_3}} = O(V^{r_1-r_3}), \tag{90}$$

which is the lemma. □

We now move on to the proof of Lemma 16.

Proof of Lemma 16. Applying Lemma 14 shows that for $V \geq V_1(\delta_3/2)$, under an event $E_{no-voter}$ that holds with probability at least $1 - \delta_3/2$, the ball $B(g_\infty, V^{-r_1})$ contains no voters' preferred vectors.

For any voter $v \in [V]$, and any $i, j \in [d]$, we define

$$a_{ijv} = \nabla^2\ell_2(g_\infty - \theta_v)[i,j] = \frac{(I - \mathbf{u}_{g_\infty-\theta_v}\mathbf{u}_{g_\infty-\theta_v}^T)[i,j]}{\|g_\infty - \theta_v\|_2}. \tag{91}$$

Since $\vec{\theta}$ is absolutely continuous with respect to the Lebesgue measure, we know that a_{ijv} is well-defined with probability 1. We then have

$$\nabla^2 L_{1:V}(g_\infty)[i,j] = \frac{1}{V}\sum_{i=1}^{V} a_{ijv} \quad \text{and} \quad H_\infty[i,j] = \nabla^2 L_\infty(g_\infty)[i,j] = \mathsf{E}_{\theta_v}[a_{ijv}]. \tag{92}$$

Moreover, we can upper-bound the variance of a_{ijv} by

$$\mathsf{Var}[a_{ijv}] \quad \mathsf{E}_{\theta_v}[a_{ijv}^2] = \int \left(\frac{(I \quad \mathbf{u}_{g\,1\,-\theta}\mathbf{u}_{g\,1\,-\theta}^T)[i,j]}{k g_\infty \quad \theta k_2} \right)^2 p(\theta) d\theta \quad \int \frac{1}{k g_\infty \quad \theta k_2^2} p(\theta) d\theta. \tag{93}$$

By Lemma 10, we know that this integral is bounded, thus, we have $\mathsf{Var}[a_{ijv}] < 1$. We then define the maximal variance σ^2 , $\max_{i,j} \mathsf{Var}[a_{ijv}]$ of the elements of the Hessian matrix. Since the voters' preferred vectors are assumed to be i.i.d, we then obtain

$$\mathsf{Var}\left[r^2 L_{1:V}(g_\infty)[i,j] \right] = \frac{1}{V^2} \sum_{v=1}^{V} \mathsf{Var}[a_{ijv}] \quad \frac{\sigma^2}{V}. \tag{94}$$

Now applying Chebyshev's inequality on $r^2 L_{1:V}(g_\infty)[i,j]$ yields

$$\mathsf{P}\left[\left| r^2 L_{1:V}(g_\infty)[i,j] \quad H_\infty[i,j] \right| \quad \varepsilon_3/2 \right] \quad \frac{4\mathsf{Var}\left[r^2 L_{1:V}(g_\infty)[i,j] \right]}{\varepsilon_3^2} \quad \frac{4\sigma^2}{V\varepsilon_3^2}. \tag{95}$$

Using a union bound, we then obtain

$$\mathsf{P}\left[\forall i,j \in [d], \left| r^2 L_{1:V}(g_\infty)[i,j] \quad H_\infty[i,j] \right| \quad \varepsilon_3/2 \right] \quad \frac{4d^2\sigma^2}{V\varepsilon_3^2}. \tag{96}$$

Therefore, taking $V \quad \frac{8d^2\sigma^2}{\delta_3 \varepsilon_3^2}$, the event $E_{Hessian}$, $\left\{ \forall i,j \in [d], \left| r^2 L_{1:V}(g_\infty)[i,j] \quad H_\infty[i,j] \right| \quad \varepsilon_3/2 \right\}$ occurs with probability at least $1 \quad \delta_3/2$. Taking a union bound shows that, for $V \quad \max\left\{ V_1(\delta_3/2), \frac{8d^2\sigma^2}{\delta_3\varepsilon_3^2} \right\}$, the event E , $E_{no-vote} \setminus E_{Hessian}$ occurs with probability at least $1 \quad \delta_3$.

We now bound the difference between finite-voter Hessian matrices at g_∞ and at a close point z, by

$$V \left| r^2 L_{1:V}(z)[i,j] \quad r^2 L_{1:V}(g_\infty)[i,j] \right| = \left| \sum_{v\in[V]} \frac{(I \quad \mathbf{u}_{z-\theta_v}\mathbf{u}_{z-\theta_v}^T)[i,j]}{kz \quad \theta_v k_2} \quad \frac{(I \quad \mathbf{u}_{g\,1\,-\theta_v}\mathbf{u}_{g\,1\,-\theta_v}^T)[i,j]}{k g_\infty \quad \theta_v k_2} \right| \tag{97}$$

$$\sum_{v\in[V]} \left| \frac{(I \quad \mathbf{u}_{z-\theta_v}\mathbf{u}_{z-\theta_v}^T)[i,j]}{kz \quad \theta_v k_2} \quad \frac{(I \quad \mathbf{u}_{g\,1\,-\theta_v}\mathbf{u}_{g\,1\,-\theta_v}^T)[i,j]}{k g_\infty \quad \theta_v k_2} \right| \tag{98}$$

$$\sum_{v\in[V]} \left| \frac{I[i,j](k g_\infty \quad \theta_v k_2 \quad kz \quad \theta_v k_2)}{kz \quad \theta_v k_2\, k g_\infty \quad \theta_v k_2} \right| + \left| \frac{\mathbf{u}_{z-\theta_v}[i]\mathbf{u}_{z-\theta_v}[j]}{k g_\infty \quad \theta_v k_2} \quad \frac{\mathbf{u}_{g\,1\,-\theta_v}[i]\mathbf{u}_{g\,1\,-\theta_v}[j]}{kz \quad \theta_v k_2} \right|. \tag{99}$$

Note that, under E, for all voters $v \in [V]$, we have $k g_\infty \quad \theta_v k_2 \quad V^{-r_1}$. Now assume $z \in B(g_\infty, V^{-r_3})$, Lemma 17 then applies with ρ , $kz \quad g_\infty k_2 \quad V^{-r_3}$, yielding $|\mathbf{u}_{g\,1\,-\theta_v}[i] \quad \mathbf{u}_{z-\theta_v}[i]| = O(V^{r_1-r_3}) \quad 1$ for all $i \in [d]$. Also, we have $|\mathbf{u}[i]| \quad k\mathbf{u}k_2 = 1$ for all unit vectors. Under E, we then have

$$\begin{aligned} &\left| \frac{\mathbf{u}_{z-\theta_v}[i]\mathbf{u}_{z-\theta_v}[j]}{k g_\infty \quad \theta_v k_2} \quad \frac{\mathbf{u}_{g\,1\,-\theta_v}[i]\mathbf{u}_{g\,1\,-\theta_v}[j]}{kz \quad \theta_v k_2} \right| \quad \left| \frac{\mathbf{u}_{z-\theta_v}[i]\mathbf{u}_{z-\theta_v}[j]}{k g_\infty \quad \theta_v k_2} \quad \frac{\mathbf{u}_{z-\theta_v}[i]\mathbf{u}_{g\,1\,-\theta_v}[j]}{k g_\infty \quad \theta_v k_2} \right| \\ &\quad + \left| \frac{\mathbf{u}_{z-\theta_v}[i]\mathbf{u}_{g\,1\,-\theta_v}[j]}{k g_\infty \quad \theta_v k_2} \quad \frac{\mathbf{u}_{z-\theta_v}[i]\mathbf{u}_{z-\theta_v}[j]}{k g_\infty \quad \theta_v k_2} \right| + \left| \frac{\mathbf{u}_{z-\theta_v}[i]\mathbf{u}_{z-\theta_v}[j]}{k g_\infty \quad \theta_v k_2} \quad \frac{\mathbf{u}_{g\,1\,-\theta_v}[i]\mathbf{u}_{g\,1\,-\theta_v}[j]}{kz \quad \theta_v k_2} \right| \end{aligned} \tag{100}$$

$$O(V^{2r_1-r_3}) + \frac{2jk g_\infty \quad \theta_v k_2 \quad kz \quad \theta_v k_2 j}{k g_\infty \quad \theta_v k_2\, kz \quad \theta_v k_2} \quad O(V^{2r_1-r_3}) + \frac{2V^{-r_3}}{V^{-r_1}(V^{-r_1} \quad V^{-r_3})} = O(V^{2r_1-r_3}), \tag{101}$$

where, in the last line, we used the triangle inequality, which implies $|k g_\infty \quad \theta_v k_2 \quad kz \quad \theta_v k_2| \quad k g_\infty \quad zk_2 \quad V^{-r_3}$ and $kz \quad \theta_v k_2 \quad k g_\infty \quad \theta_v k_2 \quad k g_\infty \quad zk_2 \quad V^{-r_1} \quad V^{-r_3}$. Therefore, under E, we have

$$\left| r^2 L_{1:V}(z)[i,j] \quad r^2 L_{1:V}(g_\infty)[i,j] \right| \quad \frac{1}{V} \sum_{v\in[V]} O(V^{2r_1-r_3}) = O(V^{2r_1-r_3}). \tag{102}$$

We now use the fact that $2r_1 < r_3$, which implies $V^{2r_1-r_3} \; ! \; 0$. Thus, for any $\varepsilon_3 > 0$, there exists a $V_3'(\varepsilon_3)$ such that, for $V \quad V_3'(\varepsilon_3)$, we have

$$\left| r^2 L_{1:V}(z)[i,j] \quad r^2 L_{1:V}(g_\infty)[i,j] \right| \quad \varepsilon_3/2. \tag{103}$$

Choosing $V \quad V_3(\varepsilon_3, \delta_3)$, $\max\left\{ V_1(\delta_3/2), \frac{8d^2\sigma^2}{\delta_3\varepsilon_3^2}, V_3'(\varepsilon_3) \right\}$, and combining the above guarantee with the guarantee about event E proved earlier, yields the result. □

Third-derivative Approximation. Finally, to apply Lemma 13, we also need to control the third-derivative of $L_{1:V}$ near the geometric median $g_{1:V}$. In fact, for our purposes, it will be sufficient to bound its norm by a possibly increasing function in V, as long as this function grows slower than V.

Definition 6. *We denote* $\nabla^3 L(z)[i,j,k]$*, the third derivative of* $L(z)$ *with respect to* $z[i]$*,* $z[j]$*, and* $z[k]$*, and* $\left\|\nabla^3 L(z)\right\|_\infty = \max_{i,j,k}\left|\nabla^3 L(z)[i,j,k]\right|$.

Lemma 18. *Under Assumption 1, for* $r_1, r_3 > 0$*, there exists* $K \in \mathbb{R}$ *such that, for any* $\delta_4 > 0$*, there exists* $V_4(\delta_4) \in \mathbb{N}$ *such that, for all* $V \geq V_4(\delta_4)$*, with probability at least* $1 - \delta_4$*, no other voter's vector lies in the ball* $B(g_\infty, V^{-r_1})$ *and, for all* $z \in B(g_\infty, V^{-r_3})$*, we have* $\left\|\nabla^3 L_{1:V}(z)\right\|_\infty = K(1 + V^{3r_1 - r_3})$.

Proof. We use the same proof strategy as the previous Lemma. First note that using Lemma 10 for $d \geq 5$, the variance of each element of the third derivative of $L_{1:V}$ is bounded, i.e.,

$$\forall (i,j,k) \in [d]^3, \mathrm{Var}\left[\nabla^3 L_{1:V}(g_\infty)[i,j,k]\right] = O\left(\int \frac{1}{\|g_\infty - \theta\|_2^4} p(\theta)d\theta\right), \quad \sigma^2 < 1. \tag{104}$$

Similarly to the previous proof, we define the events

$$E_{\nabla^3}(t) \triangleq \left\{\forall i,j,k \in [d], \left|\nabla^3 L_{1:V}(g_\infty)[i,j,k] - \nabla^3 L_\infty(g_\infty)[i,j,k]\right| \leq t\right\}, \tag{105}$$

$$E_{no-vote} \triangleq \left\{\forall v \in [V], \theta_v \notin B(g_\infty, V^{-r_3})\right\} \quad \text{and} \quad E \triangleq E_{\nabla^3}(V^r) \setminus E_{no-vote}, \tag{106}$$

where $r \triangleq \max\{0, 3r_1 - r_3\} \geq 0$. Using Chebyshev's bound and union bound, we know that, $\mathbb{P}[E_{\nabla^3}(t)] \geq 1 - d^3\sigma^2/Vt^2$, where the O hides a constant derived from the upper bound on the variance of $\nabla^3 L_{1:V}(g_\infty)[i,j,k]$, and which depends only on θ. Therefore, we have $\mathbb{P}[E_{\nabla^3}(V^r)] \geq 1 - d^3\sigma^2 V^{-(1+2r)}$. Now, assuming $V \geq V_4(\delta_4) \triangleq \max\left\{\left(2d^3\sigma^2/\delta\right)^{\frac{1}{1+2r}}, V_1(\delta_4/2)\right\}$, we know that the event E occurs with probability at least $1 - \delta_4$.

Now, we bound the deviation of $\nabla^3 L_{1:V}(z)$ from $\nabla^3 L_{1:V}(g_\infty)$ for any $z \in B(g_\infty, V^{-r_3})$. It can be shown that $\nabla^3 \ell_2(z)[i,j,k] = \frac{f(z)[i,j,k]]}{\|z\|_2^2}$, where

$$f(z)[i,j,k] \triangleq \begin{cases} 3\mathbf{u}_z[i]^3 - 3\mathbf{u}_z[i], & \text{if } i = j = k \\ 3\mathbf{u}_z[j]^2\mathbf{u}_z[i] - \mathbf{u}_z[i], & \text{if } i \neq j = k \\ 3\mathbf{u}_z[i]\mathbf{u}_z[j]\mathbf{u}_z[k], & \text{if } i \neq j \neq k \end{cases}. \tag{107}$$

Since $|\mathbf{u}[i]| \leq 1$ for all unit vectors $\mathbf{u}$ and all coordinates $i \in [d]$, we see that $|f(g_\infty - \theta_v)[i,j,k]| \leq 6$. Moreover, using Lemma 17, for any $i,j,k \in [d]$, we have

$$|f(z)[i,j,k]] - f(g_\infty)[i,j,k]| = O(V^{r_1 - r_3}). \tag{108}$$

Recall also that, like in the previous proof, under event E, for all voters $v \in [V]$, we have $\|g_\infty - \theta_v\|_2 \geq V^{-r_1}$, $\|z - \theta_v\|_2 \geq V^{-r_1} - V^{-r_3} \geq (V^{-r_1})$ and $|\|g_\infty - \theta_v\|_2 - \|z - \theta_v\|_2| \leq \|g_\infty - z\|_2 \leq V^{-r_3}$ (using the triangle

inequality). We then have

$$\left| r^3 L_{1:V}(z)[i,j,k] \quad r^3 L_{1:V}(g_\infty)[i,j,k] \right| = \left| \sum_{v\in[V]} \frac{f(z \quad \theta_v)[i,j,k]}{kz \quad \theta_v k_2^2} \quad \sum_{v\in[V]} \frac{f(g_\infty \quad \theta_v)[i,j,k]}{kg_\infty \quad \theta_v k_2^2} \right| \tag{109}$$

$$\frac{1}{V}\sum_{v\in[V]} \left| \frac{f(z \quad \theta_v)[i,j,k]}{kz \quad \theta_v k_2^2} \quad \frac{f(g_\infty \quad \theta_v)[i,j,k]}{kz \quad \theta_v k_2^2} \right| + \left| \frac{f(g_\infty \quad \theta_v)[i,j,k]}{kz \quad \theta_v k_2^2} \quad \frac{f(g_\infty \quad \theta_v)[i,j,k]}{kg_\infty \quad \theta_v k_2^2} \right| \tag{110}$$

$$\frac{1}{V}\sum_{v\in[V]} \frac{O(V^{r_1-r_3})}{kz \quad \theta_v k_2^2} + 6\frac{\left|kz \quad \theta_v k_2^2 \quad kg_\infty \quad \theta_v k_2^2\right|}{kz \quad \theta_v k_2^2 kg_\infty \quad \theta_v k_2^2} \tag{111}$$

$$\frac{O(V^{r_1-r_3})}{(V^{-r_1})^2} + \frac{6}{V}\sum_{v\in[V]} jkz \quad \theta_v k_2 \quad kg_\infty \quad \theta_v k_2 j \frac{kz \quad \theta_v k_2 + kg_\infty \quad \theta_v k_2}{kz \quad \theta_v k_2^2 kg_\infty \quad \theta_v k_2^2} \tag{112}$$

$$O(V^{3r_1-r_3}) + \frac{6}{V}\sum_{v\in[V]} V^{-r_3}\left(\frac{1}{kz \quad \theta_v k_2 kg_\infty \quad \theta_v k_2^2} + \frac{1}{kz \quad \theta_v k_2^2 kg_\infty \quad \theta_v k_2}\right) \tag{113}$$

$$O(V^{3r_1-r_3}) + \frac{12V^{-r_3}}{(V^{-r_1})^3} \quad O(V^{3r_1-r_3}). \tag{114}$$

Combining this with the guarantee of event E then yields

$$\left| r^3 L_{1:V}(z)[i,j,k] \right| \quad \left| r^3 L_\infty(g_\infty)[i,j,k] \right| + \left| r^3 L_\infty(g_\infty)[i,j,k] \quad r^3 L_{1:V}(g_\infty)[i,j,k] \right| + \left| r^3 L_{1:V}(g_\infty)[i,j,k] \quad r^3 L_{1:V}(z)[i,j,k] \right| \tag{115}$$

$$O(1) + O(V^r) + O(V^{3r_1-r_3}) = O(1) + O(V^{3r_1-r_3}), \tag{116}$$

using the definition of r. Given that $\mathsf{P}[E] \quad 1 \quad \delta_4$, taking a bound K that can replace the O yields the lemma. □

C.2.4 Skewness is Continuous

The last piece that is required for the proof of Theorem 2 is the fact that the function SKEW is continuous. To get there, we first prove a couple of lemmas about symmetric matrices.

Definition 7. *We denote* SYM_d *the set of symmetric* $d \quad d$ *real matrices. We denote* $X[i,j]$ *the element of the* i*-th row and* j*-th column of the matrix* X*, and* $kXk_\infty \ , \ \max_{i,j} jX[i,j]j$.

Lemma 19. *For any symmetric matrices* $H, S \ 2 \ \text{SYM}_d$, $j\min \text{SP}(H) \quad \min \text{SP}(S)j \quad d\,kH \quad Sk_\infty$.

Proof. Consider a unit vector $\mathbf{u}$. We have

$$\mathbf{u}^T H\mathbf{u} \quad \mathbf{u}^T S\mathbf{u} = \mathbf{u}^T(H \quad S)\mathbf{u} = \sum_{i,j\in[d]} (H[i,j] \quad S[i,j])\mathbf{u}[i]\mathbf{u}[j] \tag{117}$$

$$\sum_{i,j\in[d]} jH[i,j] \quad S[i,j]j\,j\mathbf{u}[i]j\,j\mathbf{u}[j]j \quad kH \quad Sk_\infty \left(\sum_{i\in[d]} j\mathbf{u}[i]j\right)\left(\sum_{j\in[d]} j\mathbf{u}[j]j\right) \tag{118}$$

$$= kH \quad Sk_\infty k\mathbf{u}k_1^2 \quad d\,kH \quad Sk_\infty k\mathbf{u}k_2^2 = d\,kH \quad Sk_\infty, \tag{119}$$

where we used the well-known inequality $kxk_1^2 \quad d\,kxk_2^2$ (which follows from the convexity of $t \ \overline{?} \ t^2$). Now consider $\mathbf{u}_{min}$ a unit eigenvector of the eigenvalue $\min \text{SP}(S)$ of the symmetric matrix S. Then $\min \text{SP}(H) \quad \mathbf{u}_{min}^T H\mathbf{u}_{min} \quad \mathbf{u}_{min}^T S\mathbf{u}_{min} + d\,kH \quad Sk_\infty = \min \text{SP}(S) + d\,kH \quad Sk_\infty$. Inverting the role of H and S then yields the lemma. □

Lemma 20. *The minimal eigenvalue is a continuous function of a symmetric matrix.*

Proof. This is an immediate corollary of the previous lemma. As $S \ ! \ H$, we clearly have $\min \text{SP}(S) \ ! \ \min \text{SP}(H)$. □

Lemma 21. SKEW *is continuous.*

Proof. Consider $H, S \succ 0$ two positive definite symmetric matrices. We have

$$|\text{SKEW}(H) - \text{SKEW}(S)| = \left| \sup_{\|\mathbf{u}\|_2=1} \left\{ \frac{\|H\mathbf{u}\|_2}{\mathbf{u}^T H\mathbf{u}} - 1 \right\} - \sup_{\|\mathbf{u}\|_2=1} \left\{ \frac{\|S\mathbf{u}\|_2}{\mathbf{u}^T S\mathbf{u}} - 1 \right\} \right| \tag{120}$$

$$\leq \sup_{\|\mathbf{u}\|_2=1} \left\{ \left| \frac{\|H\mathbf{u}\|_2}{\mathbf{u}^T H\mathbf{u}} - \frac{\|S\mathbf{u}\|_2}{\mathbf{u}^T S\mathbf{u}} \right| \right\} \tag{121}$$

$$= \sup_{\|\mathbf{u}\|_2=1} \left\{ \left| \frac{\|H\mathbf{u}\|_2 (\mathbf{u}^T S\mathbf{u}) - \|S\mathbf{u}\|_2 (\mathbf{u}^T H\mathbf{u})}{(\mathbf{u}^T H\mathbf{u})(\mathbf{u}^T S\mathbf{u})} \right| \right\} \tag{122}$$

$$\leq \sup_{\|\mathbf{u}\|_2=1} \left\{ \left| \frac{\|H\mathbf{u}\|_2 (\mathbf{u}^T S\mathbf{u} - \mathbf{u}^T H\mathbf{u})}{(\mathbf{u}^T H\mathbf{u})(\mathbf{u}^T S\mathbf{u})} \right| + \left| \frac{\|H\mathbf{u}\|_2 - \|S\mathbf{u}\|_2}{\mathbf{u}^T S\mathbf{u}} \right| \right\} \tag{123}$$

$$\leq \sup_{\|\mathbf{u}\|_2=1} \left\{ (\text{SKEW}(H) + 1) \left| \frac{(\mathbf{u}^T S\mathbf{u} - \mathbf{u}^T H\mathbf{u})}{\mathbf{u}^T S\mathbf{u}} \right| + \left| \frac{\|H\mathbf{u}\|_2 - \|S\mathbf{u}\|_2}{\mathbf{u}^T S\mathbf{u}} \right| \right\}. \tag{124}$$

Now, for any unit vector $\mathbf{u}$, we have

$$|\mathbf{u}^T S\mathbf{u} - \mathbf{u}^T H\mathbf{u}| \leq \sum_{i,j\in[d]} |\mathbf{u}[i]| |\mathbf{u}[j]| |S[i,j] - H[i,j]| \leq \|S - H\|_\infty \sum_{i,j\in[d]} |\mathbf{u}[i]| |\mathbf{u}[j]| \tag{125}$$

$$= \|S - H\|_\infty \|\mathbf{u}\|_1^2 = d\|S - H\|_\infty \|\mathbf{u}\|_2^2 = d\|S - H\|_\infty, \tag{126}$$

using the inequality $\|x\|_1^2 \leq d\|x\|_2^2$. Moreover, by triangle inequality, we also have

$$|\|H\mathbf{u}\|_2 - \|S\mathbf{u}\|_2| \leq \sqrt{\sum_{i\in[d]} \left(\sum_{j\in d} |H[i,j] - S[i,j]| |\mathbf{u}[j]| \right)^2} \tag{127}$$

$$\sqrt{\sum_{i\in[d]} \left(\sum_{j\in d} \|H - S\|_\infty |\mathbf{u}[j]| \right)^2} \leq \|H - S\|_\infty \sqrt{d\|\mathbf{u}\|_1^2} \tag{128}$$

$$\|H - S\|_\infty \sqrt{d^2 \|\mathbf{u}\|_2^2} \leq d\|H - S\|_\infty \|\mathbf{u}\|_2. \tag{129}$$

Finally, note that $\mathbf{u}^T S\mathbf{u} \geq \min \text{SP}(S)$. Combining it all then yields

$$|\text{SKEW}(H) - \text{SKEW}(S)| \leq \frac{2 + \text{SKEW}(H)}{\min \text{SP}(S)} d\|H - S\|_\infty. \tag{130}$$

By continuity of the minimal eigenvalue (Lemma 20), we know that $\min \text{SP}(S) \to \min \text{SP}(H)$ as $S \to H$. This allows us to conclude that $|\text{SKEW}(H) - \text{SKEW}(S)| \to 0$ as $S \to H$, which proves the continuity of the SKEW function. □

C.2.5 Proof of Theorem 2

Finally, we can prove Theorem 2.

Proof of Theorem 2. Let $\varepsilon, \delta > 0$. Choose r_1, r_2, r_3 such that[6] $2/d < 2r_1 < r_3 < r_2 < 1/2$, and set $\delta_1 = \delta_2 = \delta_3 = \delta_4 = \delta/4$. Define also $\lambda_{min} = \min \text{SP}(r^2 L_\infty(g_\infty))$ and $\varepsilon_3 = \min\{\lambda_{min}/2, \varepsilon_5\}$, where ε_5 will be defined later on, based on the continuity of SKEW at H_∞.

Now consider V sufficiently large to satisfy the requirements of lemmas 14, 15, 16, and 18. Denoting E_V the event that contains the intersection of the guarantees of these lemmas, by union bound, we then know that $\mathbb{P}[E_V] \geq 1 - \delta$. We will now show that, for V large enough, under E_V, the geometric median restricted to the first $1 + V$ voters is $(\text{SKEW}(H_\infty) + \varepsilon)$-strategyproof for voter 0. To do so, it suffices to prove that, under E_V, the assumptions of Lemma 13 are satisfied, for $\beta = 2/\lambda_{min} V$.

[6] clearly for $d \geq 5$ such r_1, r_2, r_3 exist

First, let us show that for V large enough, under E_V, the ball $B(g_{1:V}, 2\beta)$ contains no preferred vector from the first V voters. To prove this, let $z \in B(g_{1:V}, \beta)$. By triangle inequality, we have $\|z - g_\infty\|_2 \le \|z - g_{1:V}\|_2 + \|g_{1:V} - g_\infty\|_2 \le 2\beta + V^{-r_2} = O(V^{-1} + V^{-r_2}) = o(V^{-r_1})$, since $r_1 < r_2 < 1$. Thus, for V large enough, we have $z \in B(g_\infty, V^{-r_1})$. But by Lemma 14, under E_V, this ball contains none of the preferred vectors from the first V voters. As a corollary, $L_{1:V}$ is then infinitely differentiable in $B(g_{1:V}, 2\beta)$. The first condition of Lemma 13 thus holds.

We now move on to the second condition. Note that, under event E_V, by virtue of Lemma 16, for all $z \in B(g_{1:V}, \beta) \subset B(g_{1:V}, 2\beta) \subset B(g_\infty, V^{-r_1})$, we have $\left\| \nabla^2 L_{1:V}(z) - H_\infty \right\|_\infty \le \varepsilon_3 = \lambda_{min}/2$. Lemma 19 then yields $\min \mathrm{Sp}(\nabla^2 L_{1:V}(z)) \ge \min \mathrm{Sp}(H_\infty) - \left\| \nabla^2 L_{1:V}(z) - H_\infty \right\|_\infty \ge \lambda_{min} - \lambda_{min}/2 = \lambda_{min}/2$. By Taylor's theorem, we then know that, for any unit vector $\mathbf{u}$, there exists $z \in [g_{1:V}, g_{1:V} + \beta\mathbf{u}]$ such that

$$\mathbf{u}^T \nabla L_{1:V}(g_{1:V} + \beta\mathbf{u}) = \mathbf{u}^T \left(\nabla L_{1:V}(g_{1:V}) + \nabla^2 L_{1:V}(z)[\beta\mathbf{u}] \right) = \beta \nabla^2 L_{1:V}(z)[\mathbf{u}, \mathbf{u}] \tag{131}$$

$$\beta \min \mathrm{Sp}(\nabla^2 L_{1:V}(z)) \ge \frac{2}{\lambda_{min} V} \lambda_{min} = 2/V > 1/V, \tag{132}$$

where we used the fact that $\nabla L_{1:V}(g_{1:V}) = 0$. Thus the second condition of Lemma 13 holds too.

We now move on to the third condition. We have already shown that, under E_V and for all $z \in B(g_{1:V}, \beta)$, we have $\min \mathrm{Sp}(\nabla^2 L_{1:V}(z)) \ge \lambda_{min}/2$. From this, it follows that, for all $z \in B(g_{1:V}, \beta)$, we have $\min \mathrm{Sp}(\nabla^2 L_{1:V}(z) + \nabla^2 L_{1:V}(z)) \ge \lambda_{min}^2/4$. But now note that, for any coordinates $i, j \in [d]$, we have

$$\left| \nabla^3 L_{1:V}(z)[\cdot, i, j] \right| = \left| \sum_{k \in [d]} \nabla^3 L_{1:V}(z)[i, j, k] \nabla L_{1:V}(z)[k] \right| \tag{133}$$

$$\sum_{k \in [d]} \left| \nabla^3 L_{1:V}(z)[i, j, k] \right| \left| \nabla L_{1:V}(z)[k] \right| \le d \left\| \nabla^3 L_{1:V}(z) \right\|_\infty \left\| \nabla L_{1:V}(z) \right\|_\infty \tag{134}$$

$$Kd(1 + V^{3r_1 - r_3})\beta = O(V^{-1} + V^{3r_1 - r_3 - 1}). \tag{135}$$

But since $2r_1 < r_3 < 1/2$, we have $3r_1 - r_3 - 1 = r_1 - 1 < -1/2 < 0$. Thus the bound above actually goes to zero, as $V \to +\infty$. In particular, for V large enough, we must have $\left\| \nabla^3 L_{1:V}(z) - \nabla L_{1:V}(z) \right\|_\infty \le \lambda_{min}^2/8$. As a result, by Lemma 19, for all $z \in B(g_{1:V}, \beta)$ and under E_V, we then have

$$\min \mathrm{Sp}\left(\nabla^2 L_{1:V}(z) - \nabla^2 L_{1:V}(z) + \nabla^3 L_{1:V}(z) - \nabla L_{1:V}(z) \right) \tag{136}$$

$$\ge \min \mathrm{Sp}(\nabla^2 L_{1:V}(z) - \nabla^2 L_{1:V}(z)) - \left\| \nabla^3 L_{1:V}(z) - \nabla L_{1:V}(z) \right\|_\infty \tag{137}$$

$$\ge \frac{\lambda_{min}^2}{4} - \frac{\lambda_{min}^2}{8} \ge \frac{\lambda_{min}^2}{8}. \tag{138}$$

Therefore $\nabla^2 L_{1:V}(z) - \nabla^2 L_{1:V}(z) + \nabla^3 L_{1:V}(z) - \nabla L_{1:V}(z) \ge 0$, which is the third condition of Lemma 13.

Finally, the fourth and final condition of Lemma 13 holds by continuity of the function SKEW (Lemma 21). More precisely, since $H_\infty \ge 0$, we know that SKEW is continuous in H_∞. Thus, there exists $\varepsilon_5 > 0$ such that, if A is a symmetric matrix with $\|A - H_\infty\| \le \varepsilon_5$, then $A \ge 0$ and $\mathrm{SKEW}(A) \le \mathrm{SKEW}(H_\infty) + \varepsilon$. Yet, by definition of ε_3 and Lemma 16, we know that all hessian matrices $\nabla^2 L_{1:V}(z)$ for $z \in B(g_{1:V}, \beta)$ satisfy the above property. Therefore, we know that for all such z, we have $\mathrm{SKEW}(\nabla^2 L_{1:V}(z)) \le \mathrm{SKEW}(H_\infty) + \varepsilon$, which is the fourth condition of Lemma 13 with $\alpha = \mathrm{SKEW}(H_\infty) + \varepsilon$.

Lemma 13 thus applies. It guarantees that, for V large enough, under the event E_V which occurs with probability at least $1 - \delta$, the geometric median is $(\mathrm{SKEW}(H_\infty) + \varepsilon)$-strategyproof for voter 0. This corresponds to saying that the geometric median is asymptotically $\mathrm{SKEW}(H_\infty)$-strategyproof. □

C.3 Upper and Lower Bounds for Skewness (Proof of Proposition 2)

Proof. We first prove the upper-bound. Consider an orthonormal eigenvector basis of S of vectors $\mathbf{u}_1, \ldots, \mathbf{u}_d$, with respective eigenvalues $\lambda_1, \ldots, \lambda_d$. We now focus on a unit vector x in the form $x = \sum \beta_i \mathbf{u}_i$ with $\sum \beta_i^2 = 1$. Note that $\sum \beta_i^2 \lambda_i$ and $\sum \beta_i^2 \lambda_i^2$ can then be viewed as weighted averages of λ_i's and of their squares. As a result, we have $\sum \beta_i^2 \lambda_i \ge \lambda_{min}$ and $\sum \beta_i^2 \lambda_i^2 \le \lambda_{max}^2$. As a result, we have

$$\frac{\|Sx\|_2^2}{(x^T S x)^2} = \frac{\sum \beta_i^2 \lambda_i^2}{\left(\sum \beta_i^2 \lambda_i\right)^2} \le \frac{\lambda_{max}^2}{\lambda_{min}^2}. \tag{139}$$

Taking the square root and subtracting one proves the upper-bound. We now move on to proving the lower-bound. Denote λ_1 and λ_d the two extreme eigenvalues of S, and u_1 and u_d their orthogonal unit eigenvectors. Define $x = \frac{\mathbf{u}_1}{\sqrt{\lambda_1}} + \frac{\sqrt{\beta}\mathbf{u}_d}{\sqrt{\lambda_d}}$. We then have $Sx = \sqrt{\lambda_1}\mathbf{u}_1 + \sqrt{\beta\lambda_d}\mathbf{u}_d$, $\|x\|_2^2 = \lambda_1^{-1} + \beta\lambda_d^{-1}$, $x^TSx = 1 + \beta$, and $\|Sx\|_2^2 = \lambda_1 + \beta\lambda_d$. Combining this yields a ratio

$$R(\beta) \;,\; \frac{\|x\|_2^2\,\|Sx\|_2^2}{(x^TSx)^2} = \frac{(\lambda_1^{-1} + \beta\lambda_d^{-1})(\lambda_1 + \beta\lambda_d)}{(1+\beta)^2} = \frac{\beta^2 + L\beta + 1}{\beta^2 + 2\beta + 1} = 1 + \frac{L \quad 2}{2 + \beta + \beta^{-1}}, \tag{140}$$

where $L \;,\; \lambda_1^{-1}\lambda_d + \lambda_1\lambda_d^{-1} \quad 2$. Note that, similarly, we have $\beta + \beta^{-1} \quad 2$. This implies $R(\beta) \quad 1 + \frac{L-2}{4}$, with equality for $\beta = 1$. The skewness is then greater than $\sqrt{R(1)} \quad 1$. In two dimensions, the skewness is, in fact, equal to $\sqrt{R(1)} \quad 1$ since x represents essentially all possible vectors in this case. Multiplying the numerator and denominator of $R(1)$ by $\lambda_1\lambda_d$ then yields the proposition. □

D PROOFS AND DIFFERENT RESULTS FROM SECTION 5

D.1 Sketch of Proof for Theorem 3

Proof. We provide a sketch of proof, which is based on Figure 8. By Taylor series and given concentration bounds, for V large enough and $z \;!\; g_\infty$, the gradient of the skewed loss for $1 + V$ voters is then approximately given by

$$(1+V)\,r\,L_{0:V}(s,\vec{\theta},z) \quad \frac{(z \quad s)}{\|z \quad s\|} + VH_\infty(z \quad g_\infty) + o(\|z \quad g_\infty\|_2) \tag{141}$$

$$= \quad \mathbf{u}_{\,z- \;\; s} + VH_\infty(z \quad g_\infty) + o(\|z \quad g_\infty\|_2). \tag{142}$$

This quantity must cancel out for $z = g_{0:V}$. Thus we must have $^{-1}H_\infty(g_{0:V} \quad g_\infty) \quad \frac{1}{V}\mathbf{u}_{\,s- \;\; g_{0:V}}$, which implies $\|\;^{-1}H_\infty(g_{0:V} \quad g_\infty)\|_2^2 = 1/V^2$. The achievable set A_V is thus approximately the ellipsoid $\{g_\infty + z \,|\, z^TH_\infty \;^{-2}H_\infty z \quad 1/V^2\}$. In particular, for V large enough, A_V is convex.

Meanwhile, denote $g_{0:V}^{\dagger}$ the skewed geometric median when the strategic voter truthfully reports their preferred vector t. By Equation (142), we must have $(t \quad g_{0:V}^{\dagger}) \;/\; H_\infty(g_{0:V}^{\dagger} \quad g_\infty)$, which implies $t \quad g_{0:V}^{\dagger} \;/\; ^{-2}H_\infty(g_{0:V}^{\dagger} \quad g_\infty)$.

Now let us skew the space by matrix S, i.e., we map each point z in the original space to a point $x \;,\; Sz$ in the S-skewed space. Interestingly, since $\|z \quad \theta_v\|_S = \|x \quad S\theta_v\|_2$, a voter with S-skewed preferences in the original space now simply wants to minimize the Euclidean distance in the S-skewed space. Now, note that since S is a linear transformation and since A_V is convex, so is SA_V. This allows us to re-use the orthogonal projection argument. Namely, denoting π_0 the orthogonal projection of St onto the tangent hyperplane to SA_V, we have

$$\inf_{s\in\mathbb{R}^d} \left\|t \quad \textsc{Gm}\;(s,\vec{\theta}_{1:V})\right\|_S = \inf_{s\in\mathbb{R}^d} \left\|St \quad S\textsc{Gm}\;(s,\vec{\theta}_{1:V})\right\|_2 \tag{143}$$

$$= \inf_{x\in SA_V} \|St \quad x\|_2 \quad \|St \quad \pi_0\|_2\,. \tag{144}$$

To compute π_0, note that, for a large number of voters and with high probability, the achievable set SA_V in the S-skewed space is approximately the set of points $Sg_\infty + Sz$ such that $z^TH_\infty \;^{-2}H_\infty z \quad 1/V^2$. Equivalently, this corresponds to the set of points $Sg_\infty + x$ with $x \;,\; Sz$ (and thus $z = S^{-1}x$) such that $(S^{-1}x)^TH_\infty \;^{-2}H_\infty(S^{-1}x) = x^T(S^{-1}H_\infty \;^{-2}H_\infty S^{-1})x \quad 1/V^2$. This is still an ellipsoid. The normal to the surface of SA_V at $x_0 = Sg_{0:V}^{\dagger} \quad Sg_\infty$ is then given by $S^{-1}H_\infty \;^{-2}H_\infty S^{-1}x_0 = S^{-1}H_\infty \;^{-2}H_\infty(g_{0:V}^{\dagger} \quad g_\infty)$.

Meanwhile, since $t \quad g_{0:V}^{\dagger} \;/\; ^{-2}H_\infty(g_{0:V}^{\dagger} \quad g_\infty)$, we know that there exists $\gamma > 0$ such that $St \quad Sg_{0:V}^{\dagger} = \gamma S \;^{-2}H_\infty(g_{0:V}^{\dagger} \quad g_\infty)$. Then

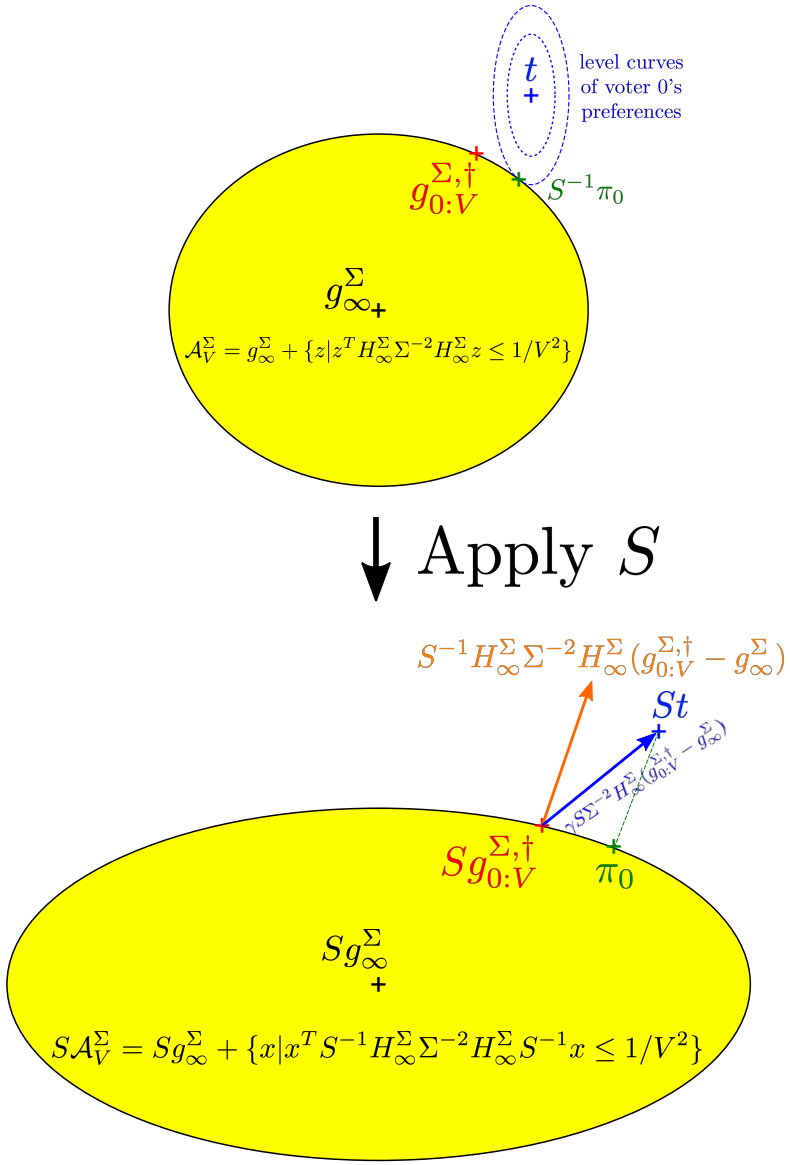

Figure 8: Proof techniques to determine the asymptotic strategyproofness of the -skewed geometric median for S-skewed preferences. We skew space using S, so that in the skewed space, voter 0 wants to minimize the Euclidean distance between their preferred vector and the skewed geometric median. Strategyproofness then depends on the angle between the blue and orange vectors in the skewed space, as depicted in the figure.

$$\frac{\left\| t \quad \textsc{Gm}(t, \vec{\theta}_{1:V}) \right\|_S}{\left\| t \quad \textsc{Gm}(s, \vec{\theta}_{1:V}) \right\|_S} \quad \frac{\left\| St \quad S g_{0:V}^{\dagger} \right\|_2}{k St \quad \pi_0 k_2} \tag{145}$$

$$\frac{\gamma \left\| S \quad {}^{-2}H_{\infty}(g_{0:V}^{\dagger} \quad g_{\infty}) \right\|_2}{(\gamma S \quad {}^{-2}H_{\infty}(g_{0:V}^{\dagger} \quad g_{\infty}))^T \frac{S \quad {}^{1}H_{1} \quad {}^{2}H_{1}(g_{0:V}^{y} - g_{1})}{k S \quad {}^{1}H_{1} \quad {}^{2}H_{1}(g_{0:V}^{y} - g_{1}) k_2}} \tag{146}$$

$$= \frac{\left\| S \quad {}^{-2}H_{\infty}(g_{0:V}^{\dagger} \quad g_{\infty}) \right\|_2 \left\| S^{-1}H_{\infty} \quad {}^{-2}H_{\infty}(g_{0:V}^{\dagger} \quad g_{\infty}) \right\|_2}{(S \quad {}^{-2}H_{\infty}(g_{0:V}^{\dagger} \quad g_{\infty}))^T (S^{-1}H_{\infty} \quad {}^{-2}H_{\infty}(g_{0:V}^{\dagger} \quad g_{\infty}))} \tag{147}$$

$$= \frac{k y_0 k_2 \left\| S^{-1} H_{\infty} S^{-1} y_0 \right\|_2}{y_0^T S^{-1} H_{\infty} S^{-1} y_0} \quad 1 + \textsc{Skew}(S^{-1} H_{\infty} S^{-1}), \tag{148}$$

by defining $y_0 \; , \; S^{-2} H_\infty (g_{0:V}^{\dagger} \quad g_\infty)$. This concludes the sketch of the proof. A more rigorous proof would need to follow the footsteps of our main proof (Theorem 2). □

D.2 Proof of Proposition 3

Proof. Let $i, j \; 2 \; [d]$. Note that $\partial_j ((\quad z)[i]) = \partial_j (\sum_k (\quad)[i,k] z[k]) = (\quad)[i,j]$. As a result, using Lemma 24, we have

$$\partial_{ij} \|z\| = \frac{\partial_j ((\quad z)[i]) \|z\| \quad (\quad z)[i] \partial_j \|z\|}{\|z\|^2} \tag{149}$$

$$= \frac{(\quad)[i,j]}{\|z\|} \quad \frac{(\quad z)[i](\quad z)[j]}{\|z\|^3} \tag{150}$$

$$= \left(\frac{}{\|z\|} \right) [i,j] \quad \left(\frac{z z^T}{\|z\|^3} \right) [i,j] \tag{151}$$

$$= \left(\quad \left(\frac{1}{\| \quad z\|_2} \left(I \quad \left(\frac{z}{\| \quad z\|_2} \right) \left(\frac{z}{\| \quad z\|_2} \right)^T \right) \right) \quad \right) [i,j]. \tag{152}$$

Combining all coordinates, replacing z by $z \quad \theta_v$, and averaging over all voters then yields the lemma. □

D.3 The computation of -skewed Geometric Median

Intuitively, the computation of the -skewed geometric median corresponds to skewing the space using the linear transformation , computing the geometric median in the skewed space, and de-skewing the computed geometric median by applying $^{-1}$. The following two lemmas formalize this intuition.

Lemma 22. $L_\infty(z, \theta) = L_\infty(\quad z, \quad \theta)$ *and* $L_{0:V}(s, \vec{\theta}, z) = L_{0:V}(\quad s, \quad \vec{\theta}, \quad z)$.

Proof. This is straightforward, by expanding the definition of the terms. □

Lemma 23. $g_\infty(\theta) = \quad ^{-1} g_\infty(\quad \theta)$ *and* $g_{0:V}(s, \vec{\theta}) = \quad ^{-1} g_{0:V}(\quad s, \quad \vec{\theta})$.

Proof. By definition of $g_\infty(\quad \theta)$, we know that it minimizes $y \; ? \; L_\infty(y, \quad \theta)$. It is then clear that $^{-1} g_\infty(\quad \theta)$ minimizes $z \; ? \; L_\infty(\quad z, \quad \theta)$. The case of $g_{0:V}$ is similar. □

D.4 No Shoe Fits Them All

In practice, we may expect different voters to assign a different importance to different dimensions. Unfortunately, this leads to the following impossibility theorem for asymptotic strategyproofness of any skewed geometric median.

Corollary 1. *Suppose voters v, w have S_v and S_w-skewed preferences, where the matrices S_v and S_w are not proportional. Then no skewed geometric median is asymptotically strategyproof for both.*

Proof. Asymptotic strategyproofness for S_v requires using a -skewed geometric median such that $\textsc{Skew}(S_v^{-1} H_\infty S_v^{-1}) = 0$. By Proposition 2, this means that all eigenvalues of $S_v^{-1} H_\infty S_v^{-1}$ must be equal, which implies that $S_v^{-1} H_\infty S_v^{-1} \; / \; I$. But then, we must have $H_\infty \; / \; S_v^2$. As a result, we then have $S_w^{-1} H_\infty S_w^{-1} \; / \; S_w^{-1} S_v^2 S_w^{-1}$. But, given our assumption about these matrices, this cannot be proportional to the identity. Proposition 2 then implies that $\textsc{Skew}(S_w^{-1} H_\infty S_w^{-1}) > 0$, which means that the -skewed geometric median is not asymptotically strategyproof for voter w. □

We leave however open the problem of determining what shoe "most fits them all". In other words, assuming a set S of skewing matrices, each of which may represent how different voters' preferences may be skewed, which (S)-skewed geometric median guarantees asymptotic α-strategyproofness for all voters, with the smallest possible value of α? And what is this optimal uniform asymptotic strategyproofness guarantee $\alpha(S)$ that can be obtained?

E ALTERNATIVE UNIT FORCES

In this section we show that the fairness principle "one voter, one vote with a unit force" can be generalized to other vector votes when we use the right norm to measure the norm of voters' forces. First we consider the skewed geometric median, and then we analyze the minimizer of ℓ_p distances.

E.1 Skewed Geometric Median

Interestingly, we can also interpret the skewed geometric median as an operator that yields unit forces to the different voters, albeit the norm of the forces is not measured by the Euclidean norm. To understand how forces are measured, let us better characterize the derivative of the skewed norm.

Lemma 24. *For all $z \in \mathbb{R}^d \setminus \{0\}$, we have $\nabla \|z\| = z/\|z\|$.*

Proof. Note that $\|z\|^2 = \|z\|_2^2 = \sum_i (z)[i]^2 = \sum_i \left(\sum_j [i,j]x[j]\right)^2$. We then have

$$\partial_i \|z\|^2 = \sum_j 2 [j,i](z)[j] = 2\sum_j \sum_k [j,i] [j,k]z[k] \tag{153}$$

$$= 2\sum_k \left(\sum_j [i,j] [j,k]\right) z[k] = 2\sum_k (\quad)[i,k]z[k] = 2(\quad z)[i]. \tag{154}$$

From this, it follows that

$$\partial_i \|z\| = \partial_i \sqrt{\|z\|^2} = \frac{\partial_i \|z\|^2}{2\sqrt{\|z\|^2}} = \frac{(\quad z)[i]}{\|z\|}. \tag{155}$$

Combining all coordinates yields the lemma. □

It is noteworthy that, using a -skewed loss, the gradient $\nabla \|z\|$ is no longer colinear with z. In fact, it is not even colinear with z, which is the image of z as we apply the linear transformation to the entire space. Similarly, this pull is no longer of Euclidean unit force. Nevertheless, it remains a unit force, as long as we measure its force with the appropriate norm.

Lemma 25. *For all $z, \theta_v \in \mathbb{R}^d$, we have $\|\nabla \|z\| \quad \theta_v\| \quad \|_1 = 1$. Put differently, using the -skewed loss, voters have $^{-1}$-unit forces.*

Proof. Applying Lemma 24 yields

$$\|\nabla \|z\| \quad \theta_v\| \quad \|_1 = \left\| \frac{z}{\|z\|} \right\| \quad \|_1 = \frac{\| \quad ^{-1} \quad z\|_2}{\|z\|} = \frac{\| \quad z\|_2}{\|z\|} = 1, \tag{156}$$

which is the lemma. □

E.2 ℓ_p Norm

Interestingly, we prove below that considering other penalties measured by ℓ_p distances is equivalent to assigning ℓ_q-unit forces to the voters. In particular, the coordinate-wise median can be interpreted as minimizing the ℓ_1 distances or, equivalently, assigning votes of ℓ_∞ unit force. In particular, the coordinate-wise median, which is known to be strategyproof, indeed implements the principle *"one voter, one unit-force vote"*. In other words, this principle can guarantee strategyproofness; this requires a mere change of norm.

Proposition 13. *Assume $\frac{1}{p} + \frac{1}{q} = 1$, with $p, q \in [1, \infty]$. Then considering an ℓ_p penalty is equivalent to considering that each voter has an ℓ_q-unit force vote. More precisely, any subgradient of the ℓ_p penalty has at most a unit norm in ℓ_q.*

Proof. Assume $x \neq 0$ and $1 < p, q < \infty$. Then we have

$$\left|\partial_j \|x\|_p\right|^q = \left|\partial_j \left(\sum_{j\in[d]} |x[j]|^p\right)^{1/p}\right|^q = \left|\frac{1}{p}\left(\sum_{j\in[d]} |x[j]|^p\right)^{(1/p)-1} \left(p|x[j]|^{p-1}\,sign(x[j])\right)\right|^q \tag{157}$$

$$= \|x\|_p^{q(1-p)}\,|x[j]|^{q(p-1)} = \frac{|x[j]|^p}{\|x\|_p^p}, \tag{158}$$

using the equality $q(p-1) = p$ derived from $\frac{1}{p} + \frac{1}{q} = 1$. Adding up all such quantities for $j \in [d]$ yields

$$\left\| \nabla \|x\|_p \right\|_q = \left(\sum_{j\in[d]} \frac{|x[j]|^p}{\|x\|_p^p}\right)^{1/q} = \left(\frac{1}{\|x\|_p^p} \sum_{j\in[d]} |x[j]|^p\right)^{1/q} \tag{159}$$

$$= \left(\frac{1}{\|x\|_p^p}\,\|x\|_p^p\right)^{1/q} = 1. \tag{160}$$

Thus the gradient of the ℓ_p norm is unitary in ℓ_q norm, when $x \neq 0$. Note then that a subgradient g at 0 must satisfy $g^T x \leq \|x\|_p$ for all $x \in \mathbb{R}^d$. This corresponds to saying that the operator norm of $x \mapsto g^T x$ must be at most one with respect to the norm ℓ_p. Yet it is well-known that this operator norm is the ℓ_q norm of g.

In the case $p = 1$, then each coordinate is treated independently. On each coordinate, the derivative is then between -1 and 1 (and can equal $[-1, 1]$ if $x[j] = 0$). This means that the gradients are of norm at most 1.

The last case left to analyze is when $p = \infty$. Denote $J^{max}(x) = \{j \in [d] \,|\, |x[j]| = \|x\|_\infty\}$. When $|J^{max}(x)| = 1$, denoting j the only element of $J^{max}(x)$ and $\mathbf{u}_j$ the j-th vector of the canonical basis, then the gradient of the ℓ_∞ is clearly $\mathbf{u}_j$, which is unitary in ℓ_1 norm. Moreover, note that if $k \notin J^{max}(x)$, then we clearly have $\partial_k \|x\|_\infty = 0$.

Now, denote $g \in \nabla \|x\|_\infty$, let $y \in \mathbb{R}^d$, and assume for simplicity that $x \neq 0$. We know that

$$\|x + \varepsilon y\|_\infty \leq \|x\|_\infty + \varepsilon g^T y. \tag{161}$$

For $\varepsilon > 0$ small enough, we then have

$$\|x\|_\infty + \varepsilon \max_{j\in J^{max}(x)} |y[j]| \leq \|x\|_\infty + \varepsilon \sum_{j\in J^{max}(x)} g[j]y[j], \tag{162}$$

from which it follows that

$$\sum_{j\in J^{max}(x)} g[j]y[j] \geq \max_{j\in J^{max}(x)} |y[j]|. \tag{163}$$

Considering $y[j] = \pm 1$ for $j \in J^{max}(x)$ and $y[k] = 0$ for all $k \neq j$ then implies $|g[j]| \geq 1$, which yields $|g[j]| \geq 1$. Generalizing it for all j's implies that $|g| \geq 1$. Now, considering $y[j] = 1$ for all $j \in J^{max}(x)$ then yields $\sum_{j\in J^{max}(x)} g[j] = \|g\|_1 \geq 1$, which concludes the proof for $x \neq 0$. The general case can be derived by considering axial symmetries. □