Math 735: Algebraic Methods in Combinatorics
Sep. 16, 2008 **Scribe: Thành Nguyen**

In this lecture note, we describe some properties of convex sets and their connection with a more general model in topological spaces. In particular, we discuss Tverberg's theorem, Borsuk's conjecture and related problems.

First we give some basic properties of convex sets in $\mathbb{R}^d$.

1 Radon, Helly and Carathéodory theorems

Definition 1. *A set $S \subset \mathbb{R}^d$ is* convex *if for any $a_1, .., a_N \in S$ and $\alpha_1, .., \alpha_N \geq 0; \sum_i \alpha_i = 1$, $\sum_i \alpha_i a_i$ is also in S.*

Definition 2. Convex hull *of a set A, denoted by $conv(A)$, is the set of all convex combination of points in A. That is:*

$$conv(A) = \{x | \exists a_1, ..., a_N \in A, \alpha_1, .., \alpha_N \geq 0; \sum_{i=1}^{N} \alpha_i = 1; x = \sum_{i=1}^{N} \alpha_i a_i.\}$$

Equivalently, a convex hull of A is the intersection of all convex sets containing A.

To see the equivalence in Definition 2, observe that every convex set containing A also contain $conv(A)$, thus all we need to show is that $conv(A)$ as given by the formula is convex. This is true because a convex combination of some convex combinations of a set $A' \subset A$ is also a convex combination of A'.

Theorem 1 (Radon)**.** *Let $a_1, a_2, ..., a_m \in \mathbb{R}^d, m \geq d+2$, then there is a partition of $\{1, .., m\}$ into I and J such that the convex hull of $\{a_i, i \in I\}$ and $\{a_j, j \in J\}$ is nonempty.*

Proof. Consider $b_i := (a_i, 1)$. We have $m \geq d + 2$ vectors in $d + 1$ dimensional space, thus they are linearly dependent. That is, there exists $\alpha_1, ..., \alpha_m$ not all zero such that:

$$\sum_{i=1}^{m} \alpha_i b_i = 0.$$

Set $I = \{i | \alpha_i \geq 0\}$ and $J = \{j | \alpha_j < 0\}$. Because the last coordinate of b_i is 1 we have:

$$\sum_{i \in I} \alpha_i = -\sum \alpha_{j \in J} = \alpha \neq 0.$$

Now the vector

$$\sum_{i \in I} \frac{\alpha_i}{\alpha} a_i = \sum_{j \in J} \frac{-\alpha_j}{\alpha} a_j$$

is in both the convex hull of $\{a_i | i \in I\}$ and $\{a_j | j \in J\}$, which proves the theorem.

□

Theorem 2 (Helly). *Let the sets $K_1, .., K_n \in \mathbb{R}^d$ be convex and compact. If any $d+1$ of these sets intersect, then all the sets intersect.*

Proof. We prove by induction on n. When $n = d+1$ the theorem is trivial. Assume that $n > d+1$. By induction, there is $a_i \in \cap_{j \neq i} K_j$ for every i. Now, by Radon theorem, we can partition $\{1, .., n\}$ into 2 sets I, J such the convex hulls $conv\{a_i | i \in I\}$ and $conv\{a_j | j \in J\}$ intersect. Let y be a point in the intersection. We can show that $y \in K_l \ \forall l$. Without loss of generality, assume that $l \in I$, then for all $j \in J, a_j \in K_l$ because of the definition of a_j. But K_l is a convex set, hence $conv\{a_j | j \in J\} \subset K_l$. Therefore $y \in conv\{a_j | j \in J\} \subset K_l$. □

Theorem 3 (Carathéodory). *For $S \subset \mathbb{R}^d$, if $x \in conv(S)$ then $x \in conv(R)$ for some $R \subset S, |R| \leq d+1$.*

Proof. Assume that $x = \sum_{i|x_i \in S} \alpha_i x_i$, such that $\alpha_i > 0$; $\sum_i \alpha_i = 1$ and $|S| > d+1$. We will show that there exists a set S' of size smaller than $|S|$, such that $x \in conv(S')$. And by this, we can always reduce the size of the set whose convex hull contains x until we get R of size at most $d+1$.

Consider $x_2 - x_1, x_3 - x_1, .., x_{d+2} - x_1$, these vectors are linearly dependent. Therefore there exist $\beta_2, .., \beta_{d+2}$ not all zero such that:

$$\sum_{i=2}^{d+2} \beta_i (x_i - x_1) = 0.$$

Let $\beta_1 = -\sum_{i \geq 2} \beta_i$ and $\beta_j = 0$ for $j > d+2$, we have $\sum_i \beta_i x_i = 0$ and $\sum_i \beta_i = 0$. Now,

$$x = \sum_i \alpha_i x_i = \sum_i \alpha_i x_i - \lambda \sum_i \beta_i x_i \text{ for all } \lambda$$

$$x = \sum_i (\alpha_i - \lambda \beta_i) x_i \text{ for all } \lambda$$

Thus, we can choose a λ such that all $\alpha'_i = \alpha_i - \lambda \beta_i \geq 0$ and at least one such value is 0.

But because $\alpha'_i \geq 0, \sum_i \alpha'_i = \sum_i \alpha_i = 1$, we obtain another convex representation of x whose support has size smaller than $|S|$. As argued above, by this, we have proved the theorem. □

Remark: The theorems above are among the most basic properties of convex sets. There are more general forms of these theorems. In particular, the topological version of Randon's theorem is as follows:

> Let f be a continuous function from the boundary of a $(d+1)$ dimensional simplex to $\mathbb{R}^d$, $f : \partial^{d+1} \to \mathbb{R}^d$ then there are two disjoint proper faces of the simplex such that their images intersect.

Radon theorem is a special case when f is affine. Based on this theorem, a topological version of Helly's theorem can be given as follows:

Let K_i be sets in $\mathbb{R}^d$ such that the intersection of any collection of sets is either empty or contractible. A set is contractible if there is a point in a set such that for every other point in the set the whole interval is also in the set. If any of $d+1$ sets intersect then all the sets intersect.

2 Tverberg's theorem

In this section we discuss a generalization of Radon theorem: Tverberg's theorem. This theorem was first proved by Tverberg [5] in 1966. The original proof was involved and difficult. Barány [1] in 1982 gave a generalization of Carathéodory's theorem, and it came as a surprise when Sarkaria [6] discovered that this version of Carathéodory's theorem implies Tverberg's theorem in an elegant way. We now state the Tverberg's theorem.

Theorem 4 (Tverberg)**.** *Given at least* $(r-1)(d+1)+1$ *points in* $\mathbb{R}^d$*, we can always partition these points into* r *parts such that the convex hull of these parts intersect.*

Example. For a simple case: when we have 7 points in the plane we can always partition them in 3 parts such that their convex hulls intersect. See Figure 1.

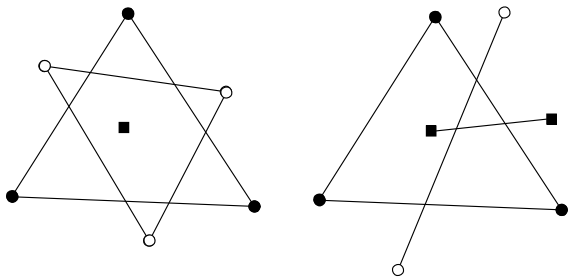


Figure 1: A simple example.

Remark. Tverberg's theorem is a generalization of Radon's theorem where $r = 2$. The minimum number of points in the theorem is tight as shown by the example in Figure 2. In this example, we have $3(r-1)$ points in the plane, $r-1$ point on each "ray". We show that we cannot partition these points into r parts such that their convex hull intersect. Assume that we have such a partition $X_1, .., X_r$. Because we have on each ray $r-1$ points, thus there exists a set, say X_1, that does not contain any point from A, and there is a set, say X_2, that does not contain any point from B . But then the convex hull of X_1, X_2 can only intersect at a point in the convex hull of C. However, C also contains only $r-1$ points, thus, there is a set X_3 that does not contain any point from C. Therefore $conv(X_3)$ is disjoint from $conv(X_1) \cap conv(X_2)$.

We now describe the proof of Tverberg's theorem given by Sarkaria. We start with the colorful Carathéodory's theorem given by Barány.

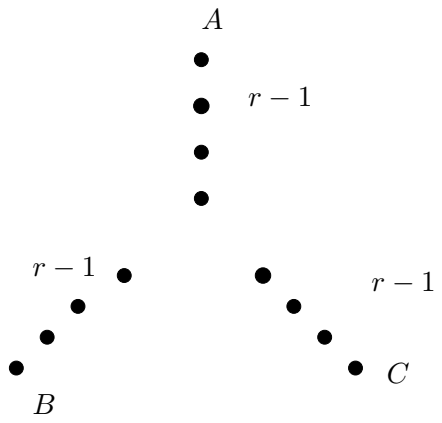


Figure 2: Tight example in the plane.

Theorem 5 (Barány)**.** *Let $A_1, A_2, \ldots, A_{d+1}$ be $d+1$ sets in R^d. Suppose that $x \in conv(A_1) \cap conv(A_2) \cap conv(A_3) \cap \cdots \cap conv(A_{d+1})$. Then there is a set $A = \{a_1 \in A_1, a_2 \in A_2, \ldots, a_{d+1} \in A_{d+1}\}$ such that $x \in conv(a_1, a_2, \ldots, a_{d+1})$.*

Proof. We can assume that A_i are finite. Take a set $A = \{a_1, .., a_{d+1}\}$ such that $a_i \in A_i \forall i$ and the convex hull $C = conv(A)$ is as close to x as possible. If $x \in C$ we are done. Assume by contradiction that $x \notin C$, let c be the point nearest to x in C. Thus, c in on one of the facets of C. We can apply Carathéodory's theorem for $d-1$ dimensional space: c can be written as a convex combination of at most d of a_i. Assume that the first point a_1 is not used in the presentation of c. Then a_1 can be replaced by any element of A_1 without increasing the distance between x and C. Now, consider the hyperplane through c and orthogonal to $x - c$. It separates x from a_1. By the condition that the convex hull of A_1 contains x thus, there is a $a_1' \in A_1$ being on the same side of the hyperplane as x. It is easy to see now that the distance from x to the convex hull of $\{a_1', a_2, .., a_{d+1}\}$ in smaller than that to C. We obtained a contradiction. □

We are ready to prove the Tverberg's theorem:
Proof of Tverberg theorem Writing $n = (d+1)(r-1)$. We can assume that $X = \{x_0, x_1, ..., x_n\}$, where $x_i \in \mathbb{R}^d \forall i$, is the set that we need to partition. Let y_i be the $(d+1)$ dimensional vector whose first d coordinates are x_i's coordinates and whose last one is 1: $y_i = (x_i, 1)$.

Here is the nontrivial idea introduced by Sarkaria: Choose vectors $v_1, ..., v_r \in \mathbb{R}^{r-1}$ with the restriction that the only linear dependence (apart from a scalar multiplier) is

$$v_1 + ... + v_r = 0.$$

Consider the $(r-1) \times (d+1)$ sized matrices $v_j y_i^T$. Define:

$$A_i = \{v_1 y_i^T, v_2 y_i^T, .., v_r y_i^T\} \text{ for every } i = 0, 1, ..., n.$$

A_i is a set of vectors in R^n. Observe that $0 \in conv(A_i)$ for every i, because of the condition $v_1 + ... + v_r = 0$. Thus we can apply Theorem 5 for the sets A_i: There is a set $A = \{a_0 \in A_0, ..., a_n \in A_n\}$ such that 0 is in its convex hull. That is

$$\sum_{i=0}^{n} \alpha_i a_i = 0 \text{ for some } \alpha_i \geq 0, \sum \alpha_i = 1$$

Assume $a_i = v_{\sigma(i)} y_i^T$ for some index $\sigma(i)$. We now define $I_k = \{i : \sigma(i) = k\}$. We will show that this is a partition that we are looking for. Define $z_k = \sum_{i \in I_k} \alpha_i y_i$,. We rewrite the equation $\sum_{i=0}^{n} \alpha_i a_i = 0$, by grouping $\alpha_i a_i$ according to the partition defined above:

$$0 = \sum_{i=0}^{n} \alpha_i v_{\sigma(i)} y_i^T = \sum_{k=1}^{r} v_k \sum_{j \in I_k} \alpha_j y_j^T = \sum_{k=1}^{r} v_k z_k^T.$$

Now because the only linear dependence of v_i is $v_1 + ... + v_r = 0$, we have that all the vector z_k are the same. But z_k is in a cone defined by some vectors y_i which are $(x_i, 1)$. This fact show that the convex hull of x_i in each partition I_j contain a vector z^* obtained by taking the first d coordinate of z_k divided by the last coordinate. By this, we proved the theorem. □

Remark: The proof for the existence of Tverberg's partitions above depends on the existence of a set A in Theorem 5. Until now, no polynomial time algorithms for finding such sets are known. It is also an open problem whether a polynomial time algorithm for finding Tverberg's partitions exists.

Remark: Sierksma conjectured that the number of Tverberg partitions for a set of $(r-1)(d+1)+1$ points in general position in $\mathbb{R}^d$ is at least $((r-1)!)^d$. The conjecture is still unresolved. When $r = p^k$, a prime power, Stephan Hell showed that the number of Tverberg partitions is at least:

$$\frac{1}{(r-1)!}\left(\frac{r}{k+1}\right)^{\frac{(d+1)(r-1)}{2}}$$

Remark: As in Radon's theorem, there is a topological version of Tverberg's theorem:

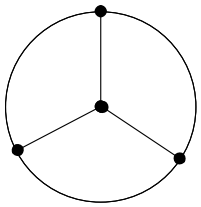
> Let $N = (r-1)(d+1)$, every continuous map f from the boundary of the N dimensional simplex to $\mathbb{R}^d$, there exist r disjoint faces $F_1, .., F_r$ of the simplex whose images under f intersect.

The proof, however, is only known when r is a prime or prime powers. See Barány, Shlosman and Szücs [2].

3 Borsuk's problem

In the previous sections we have seen some interesting properties related to convex sets and their topological generalization. In this section, we discuss another interesting problem called the Borsuk's conjecture. Let's start with simple examples.

Consider a 2 dimensional disc of diameter 1, we would like to cut the disc in pieces of smaller diameter. How many pieces do we need to cut the disc into? It is clear that we need to cut the disc into at least 3 parts. If we consider a ball in 3 dimensional space, it takes a little more effort to show that we need to cut the ball into at least 4 parts.



As we will see later, it is not hard to see that we can always cut a d dimensional ball to $d+1$ parts to reduce the diameter. But is this the optimal way? Can we extend the result to arbitrary sets in $\mathbb{R}^d$? In the early thirties Borsuk asked the following question:

Is it true that every set in $\mathbb{R}^d$ can be cut into $d+1$ pieces of smaller diameter?

For many years, many people expected the answer for the question above to be "YES", therefore call the problem the *Borsuk's conjecture*. It turned out that the conjecture is true when the set is smooth (defined later) and it is not when this condition is dropped. In the rest of this section, we show the following results:

- We can cut a d dimensional ball into $d+1$ parts of smaller diameter, and there is no way to do it with d parts.
- Any bounded "smooth" (defined later) d-dimensional set can be divided in $d+1$ parts of smaller diameter.
- There exists a convex set in $\mathbb{R}^d$ such that the number of parts we need to cut to reduce the diameter is at least $(1.01)^{\sqrt{d}}$.

Notation: We use the following notation: Given $X \subset \mathbb{R}^d$, the diameter of X denoted by $diam(X)$ is defined as $\sup_{a,b \in X} l(a,b)$, where $l(a,b)$ is the Euclidean distance between a, b. We denote $b(X)$ to be the minimum number of sets that we need to partition X into sets of smaller diameter. For a dimension d, denote $b(d)$ as the supremum of the values of $b(X)$ over all bounded sets $X \in \mathbb{R}^d$.

Remark: Kahn and Kalai [3] constructed a set X as a counter example for the Borsuk's conjecture, where $b(X) \geq (1.2)^{\sqrt{d}}$. In this lecture note, we prove a slightly weaker bound. For the upper bound of $b(d)$, Schramm proved that: $\forall \epsilon > 0, \exists d(\epsilon) \;\; s.t \;\; \forall d > d(\epsilon)$:

$$b(d) < (\beta + \epsilon)^d, \text{ where } \beta = \sqrt{3/2}.$$

To prove the results in this section, we need a tool from topology . In particular the Borsuk-Ulam's theorem. For more applications of Borsuk-Ulam's theorem see a book of Matoušek [4].

Theorem 6 (Borsuk-Ulam)**.** *Any continuous function from an n-sphere into Euclidean n-space maps some pair of antipodal points to the same point. (Two points on a sphere are called antipodal if they are in exactly opposite directions from the sphere's center.)* □

Theorem 7. *Given a d dimensional ball B, $b(B) = d + 1$.*

Proof. We need to show that there is a way to partition the ball into $d+1$ parts of smaller diameter, but we cannot do it with partitions of less than $d + 1$ parts.

First we show how to cut the ball into $d+1$ parts of smaller diameter. The construction is quite natural. Take a symmetric simplex whose vertices are on the sphere. Let $\bar{0}$ be the center of the simplex and of the ball. Cut the ball into $d+1$ parts by $d+1$ cones from $\bar{0}$ to each facet of the simplex. It is clear that the diameter of each part is strictly smaller than the diameter of the ball.

Now, assume that we can partition the ball into d parts $X_1, X_2, .., X_d$ of smaller diameter. We will use this partition to define a continuous function from the boundary of the ball to $\mathbb{R}^d$ as follows: Given a $x \in S^{d-1}$, $f(x) = (l(x, X_1), l(x, X_2), .., l(x, X_d))$. Here $l(x, X_i)$ is the Euclidean distance between x and the set X_i. It is clear that this function is continuous. By Borsuk-Ulam theorem, there exists x and $-x$ such that $f(x) = f(-x)$. Without loss of generality, assume that $x \in X_1$, we have $d(x, X_1) = 0$ therefore, $l(-x, X_1) = 0$ thus, the diameter of X_1 is the same as the diameter of the original ball. A contradiction. □

We now show that every *smooth d* dimensional set can be cut into $d + 1$ sets of smaller diameter. We first give a formal definition of smooth bodies in $\mathbb{R}^d$.

Definition 3. *A set S in $\mathbb{R}^d$ is smooth if it is closed and for every point a on its boundary, there is an ϵ such that there exists a f isomorphism and continuously differentiable from $[0, 1]^{d-1}$ to the intersection of the boundary of S and the ball $B(a, \epsilon)$, i.e. the ball centered at a with diameter ϵ.*

Theorem 8. *For any bounded smooth set S in $\mathbb{R}^d$, $b(S) \leq d + 1$.*

Proof. For each point a of the boundary of the set S, consider the unit vector orthogonal to the tangent hyperplane at a that has the direction outward of the set. We call this *tangent vector* of a. Because the set is smooth, for each point on the boundary, there is an unique tangent vector.

The main observation in the proof is that if a, b are two points whose distance is the diameter of S then their tangent vectors are antipodal. Consider the mapping f maps each point a on the boundary of S to a point on the boundary of the ball corresponding to a's tangent vector. Because S is smooth, f is a continuous mapping. It satisfies the following property: if the Euclidean distance between a and b : $l(a, b) = diam(S)$ then the distance between $f(a)$ and $f(b)$ is also the diameter of the ball. By the theorem above, we can

cut the boundary of the ball into $d+1$ sets of smaller diameter, thus the inverse image of these sets define a partition of $\partial(S)$ into $d+1$ sets of smaller diameter. Call this partition $A_1, ..., A_{d+1}$.

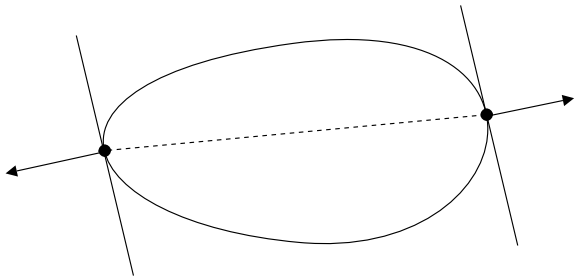


Figure 3: Tangent vectors

We now define a partition of S as follows: For every $s \in int(S)$, put s in the same set with A_i if the distance from s to A_i is the smallest among $A_1, .., A_{d+1}$, we break tie arbitrarily. We call this partition $B_1, ..., B_{d+1}$.

We need to show that by this way, we partition S in $d+1$ parts of smaller diameter. Assume by contradiction that there is a sequence (a_i, b_i) such that a_i, b_i are in the same set, say B_1 and $\lim_i l(a_i, b_i) \to diam(S)$. Because S is bounded and closed, there exists a subsequence (a_{k_i}, b_{k_i}) such that $\lim_i a_{k_i} \to a$;$\lim_i b_{k_i} \to b$; and $l(a, b) = diam(S)$. Now, we know that the maximum distance of a closed set can be achieved only at two points on the boundary. Thus a_i, b_i are in $\partial(S)$. If both of them are in A_1, then we have a contradiction, because $diam(A_1) < diam(S)$. Assume now that $a \notin A_1$. We will show that there is a sequence $a'_i \in A_1$ such that $\lim_i a'_i \to a$, and it is similar for the case $b \notin A_1$. By this way, we can still obtain the contradiction that $diam(A_1) = diam(S)$.

The reason that such a sequence a'_i exists is simple. Because $a_{k_i} \in B_1$, by the definition of B_1, there is an $a'_i \in A_1$ such that $l(a_{k_i}, a) \geq l(a_{k_i}, a'_i)$. But then $l(a, a'_i) \leq l(a_{k_i}, a) + l(a_{k_i}, a'_i) \leq 2l(a_{k_i}, a)$. However $\lim_i l(a_{k_i}, a) \to 0$, thus $\lim_i l(a'_i, a) \to 0$ meaning $\lim_i a'_i \to a$. This is what we need to show.

□

As discussed above, the most general form of Borsuk's conjecture is not true. We now describe a version of the counter example given by Kahn and Kalai in 1993 [3].

Theorem 9. *For $d >> 1$ there exists X non-smooth such that $b(X) \geq (1.01)^{\sqrt{d}}$.*

Proof. Kahn-Kalai's construction uses a theorem of Frankl and Wilson about the size of a set of some vectors such that there do not exist two orthogonal vectors. It implies that in order to partition this set of vectors into sets not containing orthogonal vectors, we need to use "many" sets. This type of statement is similar to a statement that we need to construct a counter example for the Borsuk's conjecture, except that the "metric" in Frankl-Wilson's theorem is not an Euclidean metric. To connect different metrics, we need the following simple claim:

Claim: X, Y metric spaces, $f : X \to Y$ s.t if $d(x, x') = diamX$ then $d(f(x), f(x')) = diamY$. Then $b(X) \leq b(f(X))$.

Proof of the claim: The proof is simple, given a *good partition* on Y (by good partition, we mean a partition that reduces the diameter of the original set), we can define a partition on X as the inverse image of f. Because of the condition on f, it is clear that this partition is also a *good partition* of X.

Now, let $\mathbb{R}P^{n-1}$ be the collection of lines through origin in $\mathbb{R}^n$, and define a metric between two lines as the angle between them. The maximum distance in this metric is $\frac{\pi}{2}$.

$$\text{Let } X = \{\overrightarrow{v} \in \{\pm 1\}^n, v_1 = 1, \text{the number of 1's in } \overrightarrow{v} \text{ is even}\}.$$

We have: $|X| = 2^{n-2}, diam(X) = \frac{\pi}{2}$ and $A \subset X, diam(A) < \frac{\pi}{2} \iff \forall u, v \in A \;\; u^T v \neq 0$. We use the following theorem of Frankl and Wilson:

> (**Frankl-Wilson**): *Let p be an odd prime number, and put $n = 4p$. If $A \subseteq X$ and $a^T a' \neq 0$ for all $a, a' \in A$, then $|A| \leq \sum_{j=0}^{p-1} \binom{n}{j}$.*

For now, assume that Frankl-Wilson's theorem is true, we will show how this leads to a counter example of Borsuk's conjecture. In order to have a partition with smaller diameter on X, we need at least

$$\frac{2^{(n-2)}}{\sum_{j=0}^{p-1} \binom{n}{j}} \text{ sets.}$$

Here $n = 4p$, and thus we have : $\sum_{j=0}^{p-1} \binom{n}{j} < \frac{n}{4}\binom{n}{n/4} < (1.9)^n$. Therefore,

$$b(X) \geq \frac{|X|}{(1.9)^n} = \frac{2^{n-2}}{(1.9)^n} > (1.01)^n, \text{ where } n \text{ is big enough.}$$

We now need to define a mapping from X to a Euclidean space. The mapping is defined as follows: $f : \mathbb{R}P^n \to \mathbb{R}^{n^2}$, here the dimension of the space is $d = n^2$.

$$f(x) = x \times x^T, \text{ where the length of } x \text{ is } 1$$

Given $z \in \mathbb{R}^{n^2} : ||z||^2 = \sum z_{ij}^2 = tr(zz^T)$, we have:

$$d(f(x), f(y))^2 = ||xx^T - yy^T||^2 = tr((xx^T - yy^T)^2)$$

$$= tr(xx^T xx^T) = tr(yy^T yy^T) - tr(xx^T yy^T) - tr(yy^T xx^T)$$

$$= ||x||^4 + ||y||^4 - 2(x^T y)^2 = 2(1 - (x^T y)^2)$$

Thus, $d(x, y) = diam(X) \iff x^T y = 0 \iff d(f(x), d(f(y))) = diam f(X)$. Therefore as proved above $b(f(X)) \geq b(X) \geq (1.01)^n = (1.01)^{\sqrt{d}}$ □

For the completeness, we now provide a proof of Frankl-Wilson's theorem.

Theorem 10 (Frankl-Wilson)**.** *Let p be an odd prime number, and put $n = 4p$. Define*

$$X = \{\overrightarrow{v} \in \{\pm 1\}^n, v_1 = 1, \textit{the number of 1's in } \overrightarrow{v} \textit{ is even}\}.$$

If $A \subseteq X$ and $a \cdot a' \neq 0$ for all $a, a' \in A$, then $|A| \leq \sum_{j=0}^{p-1} \binom{n}{j}$.

Proof. It is clear that $a \cdot a = n$, which is divisible by p. For $a \neq a'$, we first show that $a \cdot a'$ cannot be divisible by p.

Given $a \neq a'$, we can partition $[n]$ into the following four parts:

$$B_1 = \{i \in [n] : a_i = 1, a'_i = 1\}, \quad B_2 = \{i \in [n] : a_i = 1, a'_i = -1\},$$

$$B_3 = \{i \in [n] : a_i = -1, a'_i = 1\}, \quad B_4 = \{i \in [n] : a_i = -1, a'_i = -1\}.$$

Let $\alpha = |B_1|$, $\beta = |B_2|$, $\gamma = |B_3|$, and $\delta = |B_4|$. Then

$$a \cdot a' = \alpha - \beta - \gamma + \delta = (\alpha + \beta + \delta + \gamma) - 2(\beta + \gamma) = 4p - 2(\beta + \gamma).$$

By the definition of X:

$$2 \mid \gamma + \delta, \quad 2 \mid \delta + \beta,$$

We have $2 \mid \beta + \gamma$. Therefore, $4 \mid a \cdot a'$. Suppose that $p \mid a \cdot a'$, then the only choices for $a \cdot a'$ are $-n$, n or 0. However,

$$a \neq a' \Rightarrow a \cdot a' < n,$$

By the definition of A, $a \cdot a' \neq 0$. We also have that a and a' agree on the first coordinate $\Rightarrow a \cdot a' > -n$, therefore $a \cdot a'$ cannot be divisible by p.

Now for each $a \in A$, we define a polynomial $f_a \in \mathbb{Z}_p[X]$:

$$f_a(x) = \prod_{j=1}^{p-1} (a \cdot x - j), \quad \text{for } x \in X.$$

From what we have proved above, it is straightforward to see that $f_a(a') \neq 0$ if and only if $a = a'$.

Expanding $f_a(x)$, we put

$$f_a(x) = \sum_{\alpha} \beta_\alpha x^\alpha, \quad \text{where } \alpha = (\alpha_1, \ldots, \alpha_\ell), \text{and } x^\alpha := x_1^{\alpha_1} \cdots x_\ell^{\alpha_\ell}.$$

Then we apply the following technique called *multi-linearization*: replace all x_i^k in $f_a(x)$ by x_i if k is odd, and by 1 if k is even. Denote the resulting polynomial as $g_a(x)$, then each $g_a(x)$ is square free. Let V be the set of all square free polynomials over $\mathbb{Z}_p$ on n variables with degree at most $p-1$, then each $g_a(x)$ is a member of V and they are pairwise different (as $g_a(a') \neq 0 \Leftrightarrow a = a'$). But since the dimension of V is exactly $\sum_{j=0}^{p-1} \binom{n}{j}$, if we can show that $g_a(x)$'s are linearly independent in V, then the theorem follows. But this is straightforward: suppose $\sum_a \alpha_a g_a = 0$, then

$$0 = 0(a') = \sum_a \alpha_a g_a(a') = \alpha_{a'} g_{a'}(a'),$$

as $g_{a'}(a') \neq 0$, we get $\alpha_{a'} = 0$. This is true for every a', so $g_a(x)$'s are linearly independent on V, and therefore

$$|A| \leq \dim V = \sum_{j=0}^{p-1} \binom{n}{j}.$$

□

References

[1] I. Barány, *A generalization of Carathéodory's theorem.* Discrete Math., 40, (1982).

[2] I. Barány, S.B. Shlosman, and A. Szücs, *On a topological generation of a theorem of Tverberg.* J. London Math. Soc. 23. 1981.

[3] J. Kahn and G.K. Kalai, *A Counterexample to Borsuk's Conjecture.* Bull. Amer. Math. Soc. 29, 60-62, 1993.

[4] J. Matoušek, *Using the BorsukUlam theorem*, Springer Verlag, Berlin, 2003

[5] H. Tverberg, *A generalization of Radon's theorem.* J. London Math. Soc., 41, (1966).

[6] K.S. Sarkaria, *Tverberg's theorem via number fields.* Israel J. math., 79, (1992).