

On 0-1 Polytopes with Many Facets

Imre Bárány¹

*Rényi Institute of Mathematics, Hungarian Academy of Sciences,
POB 127, Budapest, 1364 Hungary; and
Department of Mathematics, University College London,
Gower Street, London WC1E 6BT, United Kingdom
E-mail: barany@renyi.hu*

and

Attila Pór²

*Department of Geometry, Eötvös University, Kecskeméti u. 11–13,
Budapest, 1053 Hungary
E-mail: porati@cs.elte.hu*

Communicated by Erwin Lutwak

Received May 18, 2000; accepted February 9, 2001;
published online June 26, 2001

There exist n -dimensional 0-1 polytopes with as many as $(\frac{cn}{\log n})^{n/4}$ facets. This is our main result. It answers a question of Komei Fukuda and Günter M. Ziegler.

© 2001 Academic Press

1. INTRODUCTION

A 0-1 polytope is, by definition, the convex hull of some 0-1 vectors from n -space. Properties of 0-1 polytopes, especially structured ones, play an important role in combinatorial optimization where the target is, quite often, a complete or concise description of the facets of the polytope. This task turned out to be difficult for several classes of 0-1 polytopes, most notably for the traveling salesman polytope [GP, ABCC] and for the cut polytope [DL]. We don't know for instance the answer to the innocent question: "How many facets has the traveling salesman polytope? Or the cut polytope?" It was Fukuda and Ziegler who, in several lectures and

¹ Partially supported by Hungarian National Foundation Grants T 029255 and T 032452.

² Partially supported by the Soros Foundation, Grant 2223886.

papers [F, KRSZ, Z] have drawn attention to this attractive and important problem, and asked for good estimates for the maximum number of facets an n -dimensional 0-1 polytope can have. Write $g(n)$ for this maximum. It is almost elementary to see that $2n!$ is an upper bound for $g(n)$. Stronger is the result of Fleiner *et al.* [FKR],

$$g(n) \leq 30(n-2)!$$

for large enough n . Using the blowing up technique [KRSZ] and Christof's construction of a 13-dimensional 0-1 polytope with more than 3.6^{13} facets, it can be shown that, again for large enough n ,

$$g(n) > 3.6^n.$$

Earlier, Fukuda gave a similar example with 3.26^n facets (see [KRSZ]), based on the computational experience [F] concerning the behaviour of the number of facets in random 0-1 polytopes, as the number of vertices changes. The main result of this paper is that $g(n)$ grows superexponentially:

THEOREM 1.1. *There is a positive constant c such that*

$$g(n) > \left(\frac{cn}{\log n} \right)^{n/4}.$$

The construction giving this lower bound is random. It is perhaps instructive to see here how the number of facets of random polytopes behave. The best analogy comes from the random polytope $P_N = P_N^n$ whose vertices v_1, \dots, v_N are chosen randomly, independently and uniformly from the sphere S^{n-1} . The expected number of facets, $E[f_{n-1}(P_N)]$, of P_N is asymptotically $\text{const}N$ when n is fixed and $N \rightarrow \infty$. But here we are interested in the case when $n \rightarrow \infty$ and $N < 2^n$. There is a simple formula in Buchta *et al.* [BMT] which can be used to show that in the range $2n < N < 1.5^n$, say,

$$\left(c_1 \log \frac{N}{n} \right)^{n/2} < E[f_{n-1}(P_N)] < \left(c_2 \log \frac{N}{n} \right)^{n/2}$$

with suitable positive constants c_1 and c_2 .

Note that a 0-1 polytope has all of its vertices on a sphere. It is tempting to believe that a random 0-1 polytope, K_N , on N vertices behaves similarly.

This may be even true for arbitrary 0-1 polytopes as well. In particular, it seems likely that

$$g(n) < (c_3 n)^{n/2}.$$

Here and throughout the paper c, c_1, \dots and b, b_1, \dots denote positive constants that are independent of n and N . For further information on 0-1 polytopes the reader is advised to consult Ziegler's thorough and recent survey [Z].

2. THE MODEL, THE RESULT, AND THE IDEA

Write $C = C^n = [-1, 1]^n$ for the n -dimensional ± 1 cube. (This is more convenient to work with.) Let Z be a random variable distributed uniformly over $\{-1, 1\}$, and let Z_1, \dots, Z_n be independent random variables each distributed like Z . Set $\underline{Z} = (Z_1, \dots, Z_n)$. Thus \underline{Z} is uniformly distributed over the 2^n vertices of C . Take N independent copies of \underline{Z} , namely $\underline{Z}_1, \dots, \underline{Z}_N$ and define

$$K_N = \text{conv}\{\underline{Z}_1, \dots, \underline{Z}_N\},$$

the convex hull of the vectors $\underline{Z}_1, \dots, \underline{Z}_N$. This is going to be our random 0-1, or rather ± 1 , polytope on N vertices. Note, however, that some vertices may be repeated. (K_N is one of the usual models of random ± 1 polytopes.)

We can state our main result now. Assume

$$\exp\{c_4(\log n)^2\} < N < \exp\left\{c_5 \frac{n}{\log n}\right\}. \quad (*)$$

Here one can take any constants $c_4 \leq 1$ and $c_5 \geq 1$.

THEOREM 2.1. *Under condition (*)*

$$E[f_{n-1}(K_N)] > (c_6 \log N)^{n/4}.$$

If the expected number of facets is large, then, of course, there has to be an example where the number of facets is large. We will, in fact, prove this stronger statement in a form that implies Theorem 2.1.

THEOREM 2.2. *Under condition (*), there exists a polytope K_N with*

$$f_{n-1}(K_N) > (c_7 \log N)^{n/4}.$$

The proof of this result is based on several lemmas, some of them quite involved. So we first present the basic idea, which is simple, rather informally. Assume $x \in C$ and define

$$p(x, N) = \text{Prob}[x \in K_N].$$

General principles would tell that, for most $x \in C$, $p(x, N)$ is either close to one or close to zero. To be more specific, set

$$P(t) = \{x \in C : p(x, N) \geq t\}.$$

Our approach is based on the fact that for all small $\varepsilon > 0$ and large n $P(1 - \varepsilon) \subset P(\varepsilon)$, of course, but the drop from $1 - \varepsilon$ to ε is very abrupt: $P(\varepsilon)$ is in a small neighbourhood of $P(1 - \varepsilon)$. This shows that $P(1 - \varepsilon) \subset K_N$ with high probability. But only a tiny fraction of K_N lies outside $P(\varepsilon)$: most of the boundary of $P(\varepsilon)$ is outside K_N . Thus most of the boundary of $P(\varepsilon)$ is cut off by facets of K_N . These facets lie outside $P(1 - \varepsilon)$. Comparing the surface area of $P(\varepsilon)$ with the amount a facet can cut off from it gives the lower bound.

But how to find the sets $P(1 - \varepsilon)$ and $P(\varepsilon)$? This is the point where we extensively use a beautiful result of Dyer *et al.* [DFM]. Their target was to determine the threshold $N = N(n)$ such that K_N contains most of the volume of C . As they prove, this happens at $N = (2/\sqrt{e})^n$. Their method describes where $p(x, N)$ drops from one to zero as $n \rightarrow \infty$ and $N = e^{2n}$. The analysis carries over for other values of N . In our case higher precision is required as we need a good estimate on how fast $p(x, N)$ drops from one to zero. We were able to control this only where the curvature of the boundary of $P(\varepsilon)$ behaves nicely. This is perhaps the spot where the exponent $n/2$ for P_N (the random spherical polytope) is lost and we only get $n/4$ for K_N .

The paper is organized the following way. The next section is a slight digression where we give another upper bound on the number of facets of a 0-1 polytope. Then we state four lemmas related to $p(x, N)$. Section 5 gives some geometric background, together with the proof of Theorems 2.1 and 2.2. The proofs of the probabilistic lemmas are in Sections 7 and 8. Geometric lemmas are proved in Section 9. Some auxiliary material is given in Section 6; their proofs are postponed to the last part.

3. ANOTHER UPPER BOUND

In the range given by condition (*) we can improve the bound of Fleiner *et al.* [FKR]. In fact, the bound below is better as long as N is less than exponential in n .

THEOREM 3.1. *Every n -dimensional 0-1 polytope with N vertices has at most*

$$\left(c_8 n \log \frac{N}{n} \right)^{n/2}$$

facets.

Proof. We are going to use the following volume estimate from [BáF, CP]. Given points x_1, \dots, x_N from B^n , the euclidean unit ball of R^n ,

$$\frac{\text{vol conv}\{x_1, \dots, x_N\}}{\text{vol } B^n} \leq \left(\frac{c_0}{n} \log \frac{N}{n} \right)^{n/2},$$

where c_0 is a universal constant.

Now let z_1, \dots, z_N be some vertices of the cube. Define the polytope P as $P = \text{conv}\{z_1, \dots, z_N\}$. Let π_i stand for the projection onto the subspace $x_i = 0$. Note that all the vertices of $\pi_i(P)$ lie in an $(n-1)$ -dimensional ball of radius $\sqrt{n-1}$ (actually, on its boundary). The above estimate gives then

$$\frac{\text{vol}_{n-1} \pi_i(P)}{\text{vol}_{n-1} \sqrt{n-1} B^{n-1}} \leq \left(\frac{c_0}{n-1} \log \frac{N}{n-1} \right)^{(n-1)/2}.$$

Let L_1, \dots, L_m be the facets of P . Note that $\text{vol}_{n-1} \pi_i(L_j)$ cannot be zero for all i , and it is at least $1/(n-1)!$ if it is nonzero. So summing the equalities $\sum_1^m \text{vol}_{n-1} \pi_i(L_j) = 2 \text{vol}_{n-1} \pi_i(P)$ for all i we get

$$\begin{aligned} \frac{m}{(n-1)!} &\leq \sum_{j=1}^m \sum_{i=1}^n \text{vol}_{n-1} \pi_i(L_j) = \sum_{i=1}^n \sum_{j=1}^m \text{vol}_{n-1} \pi_i(L_j) \\ &= 2 \sum_1^n \text{vol}_{n-1} \pi_i(P) \\ &\leq 2n \text{vol}_{n-1} \sqrt{n-1} B^{n-1} \left(\frac{c_0}{(n-1)} \log \frac{N}{n-1} \right)^{(n-1)/2}. \end{aligned}$$

The estimate in the theorem follows now readily. ■

4. DYER, FÜREDI, AND MCDIARMID

From now on we will denote vectors (or points) by underlining in order to distinguish them from scalars. (We actually used this notation for the random vertex \underline{Z} .) So given a vector $\underline{x} \in C$ define

$$q(\underline{x}) = \inf\{\text{Prob}[\underline{Z} \in H] : \underline{x} \in H, H \text{ a halfspace}\}$$

and for $\beta > 0$ define

$$Q^\beta = \{ \underline{x} \in C : q(\underline{x}) \geq \exp\{-\beta n\} \}.$$

Note that Q^β is a convex polytope. In fact, it is the k -core of the vertices of C (with $k = 2^n e^{-\beta n}$); see [BP, E]. We introduce the function

$$f(x) = \frac{1}{2}(1+x) \log(1+x) + \frac{1}{2}(1-x) \log(1-x),$$

defined for $x \in (-1, 1)$; at $x = \pm 1$ the limit exists and equals $\log 2$. For $\underline{x} = (x_1, \dots, x_n)$ we set

$$F(\underline{x}) = \frac{1}{n} \sum_1^n f(x_i).$$

Again, for positive β we define

$$F^\beta = \{ \underline{x} \in C : F(\underline{x}) \leq \beta \}.$$

f and consequently F is a nicely behaving, strictly convex function whose connection to K_N will become clear soon. To explain how q and F are related we are going to show, following [DFM],

LEMMA 4.1. *For $\underline{x} \in (-1, 1)^n$, we have $q(\underline{x}) \leq \exp\{-nF(\underline{x})\}$.*

Proof (from [DFM]). Check, first, that $K(t)$, the so-called cumulant generating function equals

$$K(t) = \log E[\exp\{tZ\}] = \log \cosh t.$$

Then $K'(t) = \tanh t$ and for each $x \in (-1, 1)$ there is a unique t with $x = K'(t) = \tanh t$, and

$$t = h(x) = \frac{1}{2} \log \frac{1+x}{1-x}.$$

Note, further, that

$$f(x) = -K(h(x)) + xh(x) \quad \text{and} \quad h(x) = f'(x).$$

Assume now that $F(\underline{x}) = \beta$ ($\beta > 0$). Then \underline{x} is on the boundary of F^β . In order to estimate $q(\underline{x})$ we need to find a halfspace H of the form $\{ \underline{z} : \underline{t}(\underline{z} - \underline{x}) \geq 0 \}$ with $\text{Prob}[\underline{Z} \in H]$ as small as possible. Consider the halfspace $H(\underline{x})$ (with $\underline{0} \notin H(\underline{x})$) whose bounding hyperplane is tangent to F^β at \underline{x} . So

$$H(\underline{x}) = \{ \underline{z} : \underline{t}(\underline{z} - \underline{x}) \geq 0 \}$$

with $t_j = f'(x_j)$ $j = 1, \dots, n$. Markov's inequality says $\text{Prob}[X \geq 0] \leq E[e^X]$. Using this

$$\begin{aligned} q(\underline{x}) &\leq \text{Prob}[Z \in H(\underline{x})] = \text{Prob}\left[\sum_{j=1}^n t_j(Z_j - x_j) \geq 0\right] \\ &\leq E\left[\exp\left\{\sum_{j=1}^n t_j(Z_j - x_j)\right\}\right] = \prod_{j=1}^n E[\exp\{t_j(Z_j - x_j)\}] \\ &= \prod_{j=1}^n \exp\{K(t_j) - x_j t_j\} = \exp\left\{-\sum_{j=1}^n (x_j t_j - K(t_j))\right\} \\ &= \exp\{-nF(\underline{x})\}. \quad \blacksquare \end{aligned}$$

It is surprising that this trivial estimate is sharp. Dyer, Füredi, and McDiarmid show, for certain values of \underline{x} , that

$$q(\underline{x}) \geq \exp\{-n(F(\underline{x}) + \Delta)\}$$

with Δ "small." We will make this statement quantitative in Lemma 4.3.

We have to set a few parameters next. Let α be defined as

$$\alpha = \frac{\log N}{n} \quad \text{or} \quad N = e^{\alpha n}.$$

Then condition (*) reads as

$$c_4 \frac{(\log n)^2}{n} < \alpha < c_5 \frac{1}{\log n}.$$

We will need several small ε_i that are all of the form (with constant $b_i > 0$)

$$\varepsilon_i = b_i \sqrt{\frac{\alpha}{n}} = b_i \frac{\sqrt{\log N}}{n}.$$

The main discovery of Dyer, Füredi, and McDiarmid is that Q^α and F^α are close to each other and both of them approximate K_N quite well as $N = e^{\beta n}$ (β a constant) and $n \rightarrow \infty$. We will use several results from [DFM]. The next one is essentially part (b) of Lemma 2.1 of [DFM].

LEMMA 4.2. *For large enough n*

$$\text{Prob}[Q^{\alpha - \varepsilon_1} \subset K_N] > 0.99.$$

Define $C^* = \frac{1}{10}C$; this is a shrunk copy of C . Dyer, Füredi, and McDiarmid prove (the proof is hard) that $F^\beta \subseteq Q^\alpha$ for every $\alpha > \beta$ if n is large. We make this statement quantitative within C^* .

LEMMA 4.3. *For large enough n*

$$F^{\alpha - \varepsilon_2} \cap C^* \subseteq Q^{\alpha - \varepsilon_1}.$$

The next result is simple and is related to part (a) of Lemma 2.1 of [DFM]

LEMMA 4.4. *For large enough n , at least half of the surface area of $F^{\alpha + \varepsilon_3}$ lying in C^* is missed by K_N with probability at least 0.99.*

One of our targets will be achieved once the last three lemmas have been proved. Namely, the part of K_N lying in C^* is weakly sandwiched between $F^{\alpha - \varepsilon_2}$ and $F^{\alpha + \varepsilon_3}$ with high probability. Here “weakly sandwiched” means that

$$F^{\alpha - \varepsilon_3} \cap C^* \subseteq K_N$$

and K_N misses half of $C^* \cap \partial F^{\alpha + \varepsilon_3}$.

5. GEOMETRIC LEMMAS AND PROOF OF THEOREM 2.2

We will need some geometric properties of

$$C^* \cap \partial F^\beta,$$

where $\beta = \alpha \pm \varepsilon_i$.

LEMMA 5.1. $\text{vol}_{n-1}(C^* \cap \partial F^\beta) \geq \frac{1}{2}(0.99 \sqrt{2n\beta})^n \text{vol}_{n-1} S^{n-1}$.

LEMMA 5.2. *Let H be a closed halfspace which is disjoint from $C^* \cap F^{\alpha - \varepsilon_2}$. Then H contains at most*

$$(3n(\varepsilon_2 + \varepsilon_3))^{(n-1)/2} \text{vol}_{n-1} S^{n-1}$$

of the surface area of $C^ \cap \partial F^{\alpha + \varepsilon_3}$.*

Using Lemmas 4.2, 4.4, 5.1, 5.2 we can now given the proof of Theorem 2.2.

Proof. As we have seen, K_N is weakly sandwiched between $F^{\alpha-\varepsilon_2}$ and $F^{\alpha+\varepsilon_3}$ with probability at least 0.98. Let K_N be such a ± 1 polytope. Each facet of K_N cuts off at most

$$(3n(\varepsilon_2 + \varepsilon_3))^{(n-1)/2} \text{vol}_{n-1} S^{n-1}$$

of the surface area of $C^* \cap \partial F^{\alpha+\varepsilon_3}$. In view of weak sandwiching, at least half of the surface area is cut off. Thus there are at least

$$\frac{0.5(0.99 \sqrt{2n(\alpha + \varepsilon_3)})^n}{(3n(\varepsilon_2 + \varepsilon_3))^{(n-1)/2}} \geq (c_7 \log N)^{n/4}$$

facets. ■

Of course this proves Theorem 2.1 as well: The random ± 1 polytope K_N is weakly sandwiched with high probability so

$$E[f_{n-1}(K_N)] \geq 0.98(c_7 \log N)^{n/4}.$$

6. AUXILIARY LEMMAS

We fix the one-to-one correspondence between $x \in (-1, 1)$ and $t \in R$ via

$$t = f'(x) = h(x) = \frac{1}{2} \log \frac{1+x}{1-x} \quad \text{and} \quad x = K'(t) = \tanh t$$

throughout the paper. This induces a one-to-one correspondence between $\underline{x} \in \text{int } C$ and $\underline{t} \in R^n$ with

$$\underline{t} = n \text{ grad } F(\underline{x}).$$

LEMMA 6.1. *The function*

$$g(t) = \frac{f(\tanh t)}{t^2} = -\frac{1}{t^2} \log \cosh t + \frac{\tanh t}{t}$$

is strictly decreasing on $[0, \infty)$. Its limit at $t=0$ is $1/2$.

The value of $g(t)$ is 0.497... when $\tanh t = 0.1$ implying

$$\frac{1}{2.02} t^2 \leq f(\tanh t) \leq \frac{1}{2} t^2, \quad \text{for } t \in [-0.1, 0.1].$$

The last inequality shows that, when $\underline{x} = (x_1, \dots, x_n) \in \text{int } C^*$, and $\underline{t} = (t_1, \dots, t_n)$ with $x_j = \tanh t_j$,

$$\frac{1}{2.02n} |\underline{t}|^2 \leq F(\underline{x}) \leq \frac{1}{2n} |\underline{t}|^2.$$

Let $\underline{\omega} \in S^{n-1}$ be a unit vector and define $\underline{x}(\underline{\omega}, \beta)$ as the unique point (if exists) on the boundary of F^β where

$$\underline{t}(\underline{\omega}, \beta) = n \text{ grad } F(\underline{x}(\underline{\omega}, \beta)) = \mathfrak{G}(\underline{\omega}, \beta) \underline{\omega}$$

for some positive $\mathfrak{G}(\underline{\omega}, \beta)$. Define $\text{supp } \underline{\omega} = \{i \in \{1, \dots, n\} : \omega_i \neq 0\}$. We have

LEMMA 6.2. $\underline{x}(\underline{\omega}, \beta)$ is well-defined when

$$0 < \beta < \frac{|\text{supp } \underline{\omega}|}{n} \log 2$$

and $\mathfrak{G}(\underline{\omega}, \beta)$ is strictly increasing in β .

Define

$$\Omega = \left\{ \underline{\omega} \in S^{n-1} : \sqrt{\frac{n}{3 \log n}} \underline{\omega} \in C \right\}.$$

It is simple consequence of Dvoretzky's theorem [D] that for large enough n ,

$$\text{Prob}[\underline{\omega} \in \Omega \mid \underline{\omega} \in S^{n-1}] > 0.99.$$

We will use this in the proof of

LEMMA 6.3. Assume $\underline{\omega} \in \Omega$, and $\beta < \frac{1}{606 \log n}$. Then $\underline{x}(\underline{\omega}, \beta) \in C^*$.

7. PROOF OF LEMMAS 4.2 AND 4.4

Proof of Lemma 4.2. This is a copy of the proof of Lemma 2.1(b) from [DFM] with the parameters adjusted properly. Suppose K_N is full-dimensional and there exists a point $\underline{x} \in Q^\beta \setminus K_N$ (where $\beta = \alpha - \varepsilon_1$). Then there is a facet of K_N , spanned by $\underline{Z}_{i_1}, \dots, \underline{Z}_{i_n}$, such that the corresponding halfspace contains K_N but excludes \underline{x} . Let $J = \{j_1, \dots, j_n\}$ and define the event E_J :

The points $\underline{Z}_{j_1}, \dots, \underline{Z}_{j_n}$ span a hyperplane and for one of the two corresponding halfspaces H both $\text{Prob}[\underline{Z} \notin H] \geq e^{-\beta n}$ and the event $\{\underline{Z}_j : j \notin J\} \subset H$ occurs.

It is clear that in our case the event E_I with $I = \{i_1, \dots, i_n\}$ occurs. Let E denote the event that K_N is not full dimensional. Then

$$\{Q^\beta \not\subseteq K_N\} \subset E \cup \bigcup_{\text{all } J} E_J.$$

Thus, with notation $D = \{1, \dots, n\}$,

$$\begin{aligned} \text{Prob}[Q^\beta \not\subseteq K_N] &\leq \text{Prob}[E] + \sum_{\text{all } J} \text{Prob}[E_J] \\ &= \text{Prob}[E] + \binom{N}{n} \text{Prob}[E_D]. \end{aligned}$$

For any fixed set S of dimension less than n , $\text{Prob}[\underline{Z} \in S] \leq \frac{1}{2}$, so $\text{Prob}[E] \leq \binom{N}{n} 2^{-(N-n)} < 0.001$ if n is large enough.

To bound $\text{Prob}[E_D]$ suppose $\underline{Z}_1, \dots, \underline{Z}_n$ are affinely independent. Let H_1 and H_2 be the two halfspaces they determine. If $\text{Prob}[\underline{Z} \notin H_1] \geq e^{-\beta n}$, then

$$\text{Prob}[\underline{Z}_j \in H_1 : j = n+1, \dots, N] \leq (1 - e^{-\beta n})^{N-n}$$

and similarly for H_2 . Hence

$$\begin{aligned} \text{Prob}[E_D \mid Z_1, \dots, Z_n \text{ aff. indep.}] &\leq 2(1 - e^{-\beta n})^{N-n} \\ &< 2 \exp\{-(N-n)e^{-\beta n}\}. \end{aligned}$$

By removing the conditioning we get the same bound on $\text{Prob}[E_D]$. Hence

$$\begin{aligned} \text{Prob}[Q^\beta \not\subseteq K_N] &\leq \text{Prob}[E] + \binom{N}{n} \text{Prob}[E_D] \\ &< 0.001 + 2 \exp\{n \log N - (N-n)e^{-\beta n}\} \\ &< 0.001 + 2 \exp\{n(e^{-\beta n} + \log N) - Ne^{-\beta n}\}. \end{aligned}$$

Here $\beta = \alpha - \varepsilon_1$, $N = e^{2n}$, $\varepsilon_1 = b_1(\sqrt{\log N}/n)$, and consequently $Ne^{-\beta n} = e^{\varepsilon_1 n} = \exp\{b_1 \sqrt{\log N}\}$. By condition (*) this is much larger than the other term $n(e^{-\beta n} + \log N)$ in the exponent if b_1 is chosen large enough. For instance, with $b_1 \geq 3/\sqrt{c_4}$ and large enough n

$$\text{Prob}[Q^\beta \not\subseteq K_N] < 0.001 + 2 \exp\{-n^2\} < 0.01. \quad \blacksquare$$

Proof of Lemma 4.4. Let \underline{x} be any point of the boundary of F^β (where $\beta = \alpha + \varepsilon_3$). Then, using 4.1

$$\begin{aligned} \text{Prob}[\underline{x} \in K_N] &\leq Nq(\underline{x}) \leq N \exp\{-nF(\underline{x})\} \\ &\leq \exp\{\alpha n - \beta n\} = \exp\{-\varepsilon_3 n\} < 0.001 \end{aligned}$$

if n is large enough. Then the expectation of the surface area of $C^* \cap \partial F^\beta$ contained in K_N is at most

$$\int_{C^* \cap \partial F^\beta} \text{Prob}[\underline{x} \in K_N] d\underline{x} \leq 0.001 \text{vol}_{n-1}(C^* \cap \partial F^\beta).$$

So the probability that half of $C^* \cap \partial F^\beta$ is missed by K_N is at least 0.998. ■

8. THE PROOF OF LEMMA 4.3

The target is to show that the inequality $q(\underline{x}) \leq \exp\{-nF(\underline{x})\}$ in Lemma 4.1 is rather sharp. First we need a quantitative version of Lemma 4.4 of [DFM]. We assume $\beta = \alpha \pm \varepsilon$.

LEMMA 8.1. *For every positive integer n the following holds. If $0 \leq x_i \leq 0.1$, $t_i = h(x_i)$ ($i = 1, \dots, n$) and $nF(\underline{x}) \geq 10$, then*

$$\text{Prob} \left[\sum_{i=1}^n t_i(Z_i - x_i) \geq 0 \right] \geq \exp\{-nF(\underline{x}) - 3\sqrt{nF(\underline{x})}\}.$$

Proof. (It goes via exponential centering and a Berry–Esséen type theorem, just like in [DFM].) Let X_1, \dots, X_n be independent discrete random variables and set $X = \sum X_i$. Define new random variables W_i with distribution

$$\text{Prob}[W_i = y] = e^y \frac{\text{Prob}[X_i = y]}{E[e^{X_i}]}.$$

Set $X = \sum W_i$ and observe

$$\begin{aligned} \text{Prob}[W = y] &= \sum_{y_i: \sum y_i = y} \prod_{i=1}^n e^{y_i} \frac{\text{Prob}[X_i = y_i]}{E[e^{X_i}]} \\ &= \left(\prod_1^n E[e^{X_i}] \right)^{-1} e^y \text{Prob}[X = y]. \end{aligned}$$

Apply this with $X_i = t_i Z_i$ where, as usual, Z_i is uniform over $\{-1, 1\}$

$$\text{Prob} \left[\sum_1^n t_i Z_i = w \right] = \exp \left\{ \sum_1^n K(t_i) \right\} e^{-w} \text{Prob}[W = w].$$

It is easy to check that $E[W_i] = t_i \tanh t_i = t_i x_i$. Let $Y = W - E[W] = W - \sum t_i x_i$. With this notation

$$\begin{aligned} \text{Prob} \left[\sum_1^n t_i (Z_i - x_i) \geq 0 \right] &= \exp \left\{ \sum_1^n K(t_i) \right\} \sum_{w \geq \sum t_j x_j} e^{-w} \text{Prob}[W = w] \\ &= \exp \left\{ \sum_1^n (K(t_i) - t_i x_i) \right\} \sum_{y \geq 0} e^{-y} \text{Prob}[Y = y]. \end{aligned}$$

Here $\sum (K(t_i) - t_i x_i) = -\sum f(x_i)$ so we have to show that $\sum_{y \geq 0} e^{-y} \text{Prob}[Y = y]$ is not too small. Setting $Y_j = W_j - E[W_j]$ we have $Y = \sum Y_j$ and $E[Y_j] = 0$. Easy calculations give

$$\sigma_j^2 = E[Y_j^2] = \frac{t_j^2}{\cosh^2 t_j} \quad \text{and} \quad E[|Y_j|^3] = \left(2 \cosh t_j - \frac{1}{\cosh t_j} \right) \sigma_j^3.$$

We need a few simple estimates: when $0 \leq x_i \leq 0.1$,

$$0 \leq t_i \leq h(0.1) = 0.1003353\dots \quad \text{and} \quad 1 \leq \cosh t_i < 1.00503\dots$$

It is easy to check that

$$\frac{E[|Y_j|^3]}{E[Y_j^2]} = t_j (1 + \tanh^2 t_j)$$

is an increasing function in t_j . Thus, in the given range,

$$M = \max_j \frac{E[|Y_j|^3]}{E[Y_j^2]} \leq 0.102\dots$$

Define $\sigma = \sqrt{\sum \sigma_j^2}$. Now Berry's theorem (see [Fe]) says that, under the present conditions, for all n , the distribution of $1/\sqrt{\sigma} \sum_1^n Y_j$ differs from that of the standard normal by at most

$$\frac{33}{4} \frac{M}{\sigma}.$$

Now

$$\begin{aligned}\sigma &= \sqrt{\sum_1^n \sigma_j^2} = \sqrt{\sum_1^n \frac{t_j^2}{\cosh^2 t_j}} \geq \frac{1}{1.00503\dots} \sqrt{\sum_1^n t_j^2} \\ &\geq 0.99 \sqrt{2nF(\underline{x})} \geq 0.99 \sqrt{20} > 4.427.\end{aligned}$$

Since the standard normal between 0 and $\sqrt{\sigma} > \sqrt{4.427} > 2.1$ is larger than 0.49, Berry's theorem implies that

$$\text{Prob} \left[0 \leq \frac{\sum_j^n Y_j}{\sqrt{\sigma}} \leq \sqrt{\sigma} \right] > 0.49 - 2 \frac{33}{4} \frac{M}{\sigma} > \frac{1}{10}.$$

With this

$$\begin{aligned}\sum_{y \geq 0} e^{-y} \text{Prob}[Y = y] &\geq \sum_{0 \leq y \leq \sigma} e^{-y} \text{Prob}[Y = y] \\ &\geq e^{-\sigma} \text{Prob} \left[0 \leq \sum_1^n Y_j \leq \sigma \right] \\ &\geq \frac{1}{10} e^{-\sigma} \geq e^{-3\sqrt{nF(\underline{x})}},\end{aligned}$$

since $\sigma = \sqrt{\sum \sigma_j^2} \leq \sqrt{\sum t_j^2} \leq \sqrt{2.02nF(\underline{x})} < 3\sqrt{nF(\underline{x})} - \log 10$, because $nF(\underline{x}) \geq 10$. ■

LEMMA 8.2. Assume $\alpha_i > 0$ for $i = 1, \dots, m$. Then

$$\text{Prob} \left[\sum_1^m \alpha_i (Z_i - 0.1) \geq 0 \right] \geq \frac{1}{m^2} \exp\{-mf(0.1)\}.$$

Proof. Let H^* , H respectively be the halfspaces

$$\begin{aligned}H^* &= \left\{ \underline{x} \in R^m : \sum_1^m \alpha_i (x_i - 0.1) \geq 0 \right\}, \\ H &= \left\{ \underline{x} \in R^m : \sum_1^m (x_i - 0.1) \geq 0 \right\}.\end{aligned}$$

Define $\sigma: R^m \rightarrow R^m$ to be the cyclic shift of the components of x , that is, $\sigma(x_1, \dots, x_m) = (x_m, x_1, \dots, x_{m-1})$. The orbit of \underline{x} under σ is, by definition, $\{\underline{x}, \sigma(\underline{x}), \sigma^2(\underline{x}), \dots\}$. As $\sigma^m(\underline{x}) = \underline{x}$, any orbit has at most m elements. If

$\underline{x} \in H$ then so is $\sigma(\underline{x})$. At least one element of each orbit with $\underline{x} \in H$ is in H^* as otherwise

$$\sum_{j=1}^m \alpha_j (\sigma^k(\underline{x})_j - 0.1) < 0 \quad \text{for all } k = 0, 1, \dots, m-1.$$

Summing these inequalities for all k we get

$$\sum_{j=1}^m (\alpha_1 + \dots + \alpha_m)(x_j - 0.1) < 0,$$

a contradiction. Now we see that

$$\begin{aligned} \text{Prob} \left[\sum_1^m \alpha_i (Z_i - 0.1) \geq 0 \right] &= \text{Prob}[\underline{Z} \in H^*] \\ &\geq \frac{1}{m} \text{Prob}[|\{i: Z_i = 1\}| \geq 0.55m] \\ &= \frac{1}{m} \frac{1}{2^m} \sum_{k=0.55m}^m \binom{m}{k} \\ &\geq \frac{1}{m^2} \exp\{-mf(0.1)\} \end{aligned}$$

as a simple calculation using Stirling formula reveals. ■

Proof of Lemma 4.3. We have to show that $q(\underline{x}) \geq \exp\{-(\alpha - \varepsilon_1)n\}$ for each $\underline{x} \in F^{\alpha - \varepsilon_2} \cap C^*$, or, in other words, every halfspace H intersecting $F^{\alpha - \varepsilon_2} \cap C^*$ contains at least $2^n \exp\{-(\alpha - \varepsilon_1)n\}$ vertices of C . It suffices to show this for halfspaces H whose bounding hyperplane H^o is tangent to $F^{\alpha - \varepsilon_2} \cap C^*$.

We show first that H contains a point \underline{x} with $F(\underline{x}) = \alpha - \varepsilon_2$ on its boundary. If H^o touches $F^{\alpha - \varepsilon_2}$ then the point of tangency satisfies this condition. If not, then H contains a point \underline{y} with $F(\underline{y}) < \alpha - \varepsilon_2$ and there is a smallest face of C^* containing \underline{y} . Since the vertices of C^* are not contained in $F^{\alpha - \varepsilon_2}$ there is a point \underline{x} on this face with $F(\underline{x}) = \alpha - \varepsilon_2$.

By symmetry we can suppose that all components of \underline{x} are nonnegative and in increasing order. Let $n_1 \in \{1, \dots, n\}$ be such that $x_{n_1} < 0.1$ and $x_{n_1+1} = 0.1$. Set $\underline{t} = n \text{ grad } F(\underline{x})$ and let \underline{t}^* be the normal to H^o . We will

prove the lemma assuming that \underline{t}^* is in the relative interior of the normal cone to $F^{\alpha-\varepsilon_2} \cap C^*$ at the point \underline{x} ; this assumption means that

$$\begin{aligned} t_i^* &= t_i & \text{for } i = 1, \dots, n_1 \\ t_i^* &> t_i & \text{for } i = n_1 + 1, \dots, n. \end{aligned}$$

The statement of the lemma for general \underline{t}^* follows from this easily.

Next we have to consider cases according to where the terms of the sum $\sum_1^n f(x_i) = n(\alpha - \varepsilon_2)$ are concentrated. If $n_1 \geq n - 2000$, then Lemma 8.1 applies: check that $\sum_1^{n_1} f(x_i) \geq n(\alpha - \varepsilon_2) - 2000f(0.1) > 10$ if n is large. Choose the last, at most 2000, Z_i to be 1 ($i = n_1 + 1, \dots, n$). We get

$$\begin{aligned} &\text{Prob} \left[\sum_{i=1}^n t_i^*(Z_i - x_i) \geq 0 \right] \\ &\geq 2^{-2000} \text{Prob} \left[\sum_{i=1}^{n_1} t_i(Z_i - x_i) \geq 0 \right] \\ &\geq 2^{-2000} \exp \left\{ - \sum_{i=1}^{n_1} f(x_i) - 3 \sqrt{\sum_{i=1}^{n_1} f(x_i)} \right\} \\ &\geq \exp \left\{ -n(\alpha - \varepsilon_2) - 3 \sqrt{n(\alpha - \varepsilon_2)} - 2000 \log 2 \right\} \\ &\geq \exp \left\{ -n(\alpha - \varepsilon_1) \right\}. \end{aligned}$$

The last inequality follows when n and thus N is large enough if one chooses here, with $\varepsilon_i = b_i(\sqrt{\log N/n})$, $i = 1, 2$,

$$b_2 \geq 2b_1 + 3.$$

If $n_1 < n - 2000$, then set $n_2 = n_1 + 2000$ and write

$$\begin{aligned} &\text{Prob} \left[\sum_{i=1}^n t_i^*(Z_i - x_i) \geq 0 \right] \\ &\geq \text{Prob} \left[\sum_{i=1}^{n_2} t_i(Z_i - x_i) \geq 0 \right] \\ &\quad \times \text{Prob} \left[\sum_{i=n_1+1}^{n_2} (t_i^* - t_i)(Z_i - x_i) + \sum_{i=n_2+1}^n t_i^*(Z_i - x_i) \geq 0 \right]. \end{aligned}$$

Lemma 8.1 applies to the first probability since $\sum_{i=1}^{n_2} f(x_i) \geq 2000f(0.1) > 10$. It gives

$$\text{Prob} \left[\sum_{i=1}^{n_2} t_i(Z_i - x_i) \geq 0 \right] \geq \exp \left\{ - \sum_{i=1}^{n_2} f(x_i) - 3 \sqrt{\sum_{i=1}^{n_2} f(x_i)} \right\}.$$

Lemma 8.2 works for the second factor and shows that it is at least

$$\frac{1}{(n - n_1)^2} \exp\{-(n - n_1) f(0.1)\}.$$

The last two inequalities combine to

$$\begin{aligned} \text{Prob} \left[\sum_{i=1}^n t_i^* (Z_i - x_i) \geq 0 \right] \\ \geq \exp\{ -nF(\underline{x}) - 3 \sqrt{nF(\underline{x})} - 2000f(0.1) - 2 \log(n - n_1) \}. \end{aligned}$$

The exponent here is $-n(\alpha - \varepsilon_2) - 3 \sqrt{n(\alpha - \varepsilon_2)} - 2000f(0.1) - 2 \log(n - n_1)$ which is larger than $-n(\alpha - \varepsilon_1)$, if, in the definition of ε_2 , the constant b_2 is chosen large enough. ■

9. PROOF OF THE GEOMETRIC LEMMAS

Proof of Lemma 5.1. A routine argument shows how to compute the product curvature $\kappa(\underline{x})$ of the surface given implicitly by $F(\underline{x}) = \beta$: it gives, at the point \underline{x} ,

$$\frac{1}{\kappa(\underline{x})} = \frac{|\text{grad } F(\underline{x})|^n}{\det F''} = \frac{|\underline{t}|^n}{\prod_{i=1}^n \frac{1}{1 - x_i^2}} \geq \frac{(2n\beta)^{n/2}}{(0.99)^{-n}} \geq (0.99 \sqrt{2n\beta})^n$$

since $\underline{x} \in C^*$ implies $x_i^2 \leq 0.01$. We use this in the well-known formula [BF] giving the surface area as the integral of $1/\kappa(\underline{x})$ on S^{n-1} . Now with $\beta = \alpha + \varepsilon_3$

$$\begin{aligned} \text{vol}_{n-1}(\partial F^\beta \cap C^*) \\ = \int_{\underline{\omega} \in S^{n-1}} \frac{1}{\kappa(\underline{x})} d\underline{\omega} \\ \geq \int_{\underline{\omega} \in \Omega} (0.99 \sqrt{2n\beta})^n d\underline{\omega} \geq \frac{1}{2} (0.99 \sqrt{2n\beta})^n \text{vol}_{n-1} S^{n-1}. \quad \blacksquare \end{aligned}$$

Proof of Lemma 5.2. We can assume that the touching hyperplane H° of the halfspace H is tangent to $F^{\alpha - \varepsilon_2} \cap C^*$ at the point \underline{x} with $F(\underline{x}) = \alpha - \varepsilon_2$.

We assume, by symmetry, that all $x_i \geq 0$. If \underline{x} is in $\text{int } C^*$ then H is well-defined with normal $\underline{t} = n \text{ grad } F(\underline{x})$.

If \underline{x} is not in $\text{int } C^*$ then we can assume (as in the proof of Lemma 4.3) that the outer normal \underline{t}^* of H is in the relative interior of the normal cone to $C^* \cap F^{\alpha-\varepsilon_2}$ at \underline{x} . Then \underline{t}^* can be chosen so that

$$\begin{aligned} t_i^* = t_i = f'(x_i) & \quad \text{for } 0 \leq x_i \leq 0.1, & \quad \text{and} \\ t_i^* \geq t_i = f'(0.1) & \quad \text{for } x_i = 0.1. \end{aligned}$$

Assume $\underline{y} \in H \cap C^*$. Then, as $y_i - x_i \leq 0$ if $x_i = 0.1$,

$$\sum_{i=1}^n t_i(y_i - x_i) \geq \sum_{i=1}^n t_i^*(y_i - x_i) \geq 0,$$

showing that $H \cap C^* \subset \{\underline{z}: \underline{t}(\underline{z} - \underline{x}) \geq 0\}$. So we may assume that the normal vector of H is just $\underline{t} = n \text{ grad } F(\underline{x})$.

Now let $\underline{w} \in H \cap F^{\alpha+\varepsilon_3} \cap C^*$. Set $\underline{u} = \underline{w} - \underline{x}$ which is clearly in $2C^*$. Then with suitable $\zeta_i \in [0, x_i]$ we have

$$\begin{aligned} F(\underline{w}) &= F(\underline{x}) + (\underline{w} - \underline{x}) \text{ grad } F(\underline{x}) + \frac{1}{2} (\underline{w} - \underline{x})^T F''(\underline{x})(\underline{w} - \underline{x}) \\ &\quad + \frac{1}{6} \sum_{i=1}^n \frac{f'''(\zeta_i)}{n} (w_i - x_i)^3 \\ &\geq \alpha - \varepsilon_2 + \frac{1}{2n} \sum_{i=1}^n \frac{1}{1-x_i^2} u_i^2 + \frac{1}{6n} \sum_{i=1}^n \frac{2\zeta_i}{(1-\zeta_i^2)^2} u_i^3 \\ &\geq \alpha - \varepsilon_2 + \frac{1}{2n} \sum_{i=1}^n u_i^2 \left(\frac{1}{1-x_i^2} - \frac{2x_i}{3(1-x_i^2)^2} u_i \right) \geq \alpha - \varepsilon_2 + \frac{|\underline{u}|^2}{3n} \end{aligned}$$

On the other hand $\underline{w} \in F^{\alpha+\varepsilon_3}$, so

$$\alpha + \varepsilon_3 \geq F(\underline{w}) \geq \alpha - \varepsilon_2 + \frac{|\underline{u}|^2}{3n}$$

implying

$$|\underline{u}| \leq \sqrt{3n(\varepsilon_2 + \varepsilon_3)}.$$

This shows that the cut-off from $\partial F^{\alpha+\varepsilon_3}$ by the halfspace H is contained in a ball of radius $\sqrt{3n(\varepsilon_2 + \varepsilon_3)}$ so its surface area is at most

$$(3n(\varepsilon_2 + \varepsilon_3))^{(n-1)/2} \text{vol}_{n-1} S^{n-1}. \quad \blacksquare$$

10. PROOF OF THE AUXILIARY RESULTS

Proof of Lemma 6.1. It is elementary to see that $\lim_{t \rightarrow 0} g(t) = 1/2$. We have to show that, for all $t \in (0, \infty)$, $g'(t) \leq 0$, or, what is the same, $t^3 g'(t) \leq 0$. Direct computation gives

$$h(t) = t^3 g'(t) = 2 \log \cosh t - 2t \tanh t + \frac{t^2}{\cosh^2 t}.$$

As $\lim_{t \rightarrow 0} h(t) = 0$, it is enough to see that $h'(t)$ is nonpositive:

$$h'(t) = -\frac{2t^2 \sinh t}{\cosh^3 t} \leq 0. \quad \blacksquare$$

Proof of Lemma 6.2. Fix $\underline{\omega}$. Let $\vartheta \in (0, \infty)$ and define

$$x_i = \tanh \vartheta \omega_i, \quad i = 1, \dots, n.$$

This gives a point $\underline{x} \in C$ with $n \operatorname{grad} F(\underline{x}) = \vartheta \underline{\omega}$. For fixed $\underline{\omega} \in S^{n-1}$, the mapping $\vartheta \rightarrow F(\underline{x}) = \frac{1}{n} \sum_{i=1}^n f(\tanh \vartheta \omega_i)$ is strictly increasing and continuous, it is 0 at $\vartheta = 0$ and its limit at $\vartheta \rightarrow \infty$ is $\frac{1}{n} |\operatorname{supp} \underline{\omega}| \log 2$. This proves the first part of the statement. The second part follows from the monotonicity of $\vartheta \rightarrow \frac{1}{n} \sum_{i=1}^n f(\tanh \vartheta \omega_i)$. \blacksquare

Proof of Lemma 6.3. Define $\lambda = \sqrt{n/(3 \log n)}$. As $\underline{\omega} \in \Omega$, $\lambda \underline{\omega} \in C$ and $\frac{\lambda}{10} \underline{\omega} \in C^*$, so there is a point $\underline{x} \in C$ with $n \operatorname{grad} F(\underline{x}) = \frac{\lambda}{10} \underline{\omega}$. We may assume, by symmetry, that all $\omega_i \geq 0$. Of course $x_i = \tanh \frac{\lambda}{10} \omega_i$. At this point

$$F(\underline{x}) \geq \frac{1}{2.02n} \left| \frac{\lambda}{10} \underline{\omega} \right|^2 > \frac{1}{606 \log n}.$$

Monotonicity implies then, that

$$\begin{aligned} 0 &\leq x(\underline{\omega}, \beta)_i = \tanh \vartheta(\underline{\omega}, \beta) \omega_i \\ &< \tanh \frac{\lambda}{10} \omega_i \leq \tanh 0.1 < 0.1 \end{aligned}$$

for all $i = 1, \dots, n$. \blacksquare

REFERENCES

- [ABCC] D. Applegate, R. Bixby, V. Chvátal, and W. Cook, On the solution of traveling salesman problems, in "International Congress of Mathematics, Berlin, 1998," Documenta Math., Vol. III, pp. 645–656, ICM, 1998.

- [BP] I. Bárány and M. Perles, The Carathéodory number for the k -core, *Combinatorica* **10** (1990), 185–194.
- [BáF] I. Bárány and Z. Füredi, Computing the volume is difficult, *Discrete Comput. Geom.* **2** (1987), 319–326.
- [BF] T. Bonnesen and W. Fenchel, “Theorie der konvexen Körper,” Springer-Verlag, Berlin, 1934.
- [BMT] C. Buchta, J. Müller, and R. F. Tichy, Stochastic approximation of convex bodies, *Math. Ann.* **271** (1985), 225–235.
- [CP] B. Carl and A. Pajor, Gelfand numbers of operators with values in a Hilbert space, *Invent. Math.* **94** (1988), 479–504.
- [DL] M. M. Deza and M. Laurent, “Geometry of Cuts and Metrics,” Algorithms and Combinatorics, Vol. 15, Springer-Verlag, Berlin/Heidelberg, 1997.
- [D] A. Dvoretzky, Some near-sphericity results, in “Proc. Sympos. Pure Math.,” Vol. VII, pp. 203–210, Amer. Math. Soc., Providence, 1963.
- [DFM] M. E. Dyer, Z. Füredi, and C. McDiarmid, Volumes spanned by random points in the hypercube, *Random Structures Algorithms* **3** (1992), 91–106.
- [E] J. Eckhoff, Helly, Radon, and Carathéodory type theorems, in “Handbook of Convex Geometry” (P. M. Gruber and J. Wills, Eds.), pp. 389–448, North-Holland, Amsterdam, 1993.
- [Fe] W. Feller, “An Introduction to Probability Theory and Its Applications,” Vol. II, Wiley, New York, 1971.
- [FKR] T. Fleiner, V. Kaibel, and G. Rote, Upper bounds on the maximal number of faces of $0/1$ -polytopes, *European J. Combin.* **21** (2000), 121–130.
- [F] K. Fukuda, Lecture, Oberwolfach, 1995.
- [GP] M. Grötschel and M. Padberg, Polyhedral theory/polyhedral computations, in “The Traveling Salesman Problem” (E. L. Lawler, J. K. Lenstra, A. H. G. Rinnoy Kan, and D. B. Shmoys, Eds.), pp. 251–360, Wiley, New York, 1988.
- [KRSZ] U. Kortenkamp, J. Richter-Gebert, A. Sarangarajan, and G. M. Ziegler, Extremal properties of $0/1$ -polytopes, *Discrete Comput. Geom.* **17** (1997), 439–448.
- [Z] G. M. Ziegler, Lectures on $0/1$ polytopes, in “Polytopes—Combinatorics and Computation” (G. Kalai and G. M. Ziegler, Eds.), pp. 1–44, DMV Seminars, Birkhäuser, Basel, 2000.