# A BOUND FOR THE NUMBER OF VERTICES OF A POLYTOPE WITH APPLICATIONS

Alexander Barvinok

August 2011

Abstract. We prove that the number of vertices of a polytope of a particular kind is exponentially large in the dimension of the polytope. As a corollary, we prove that an $n$-dimensional centrally symmetric polytope with $O(n)$ facets has $2^{\Omega(n)}$ vertices and that the number of $r$-factors in a $k$-regular graph is exponentially large in the number of vertices of the graph provided $k \geq 2r+1$ and every cut in the graph with at least two vertices on each side has more than $k/r$ edges.

## 1. Introduction and main results

Let $\mathbb{R}^n$ be Euclidean space with the standard scalar product $\langle \cdot, \cdot \rangle$ and the associated Euclidean norm $\| \cdot \|$. A polytope $P \subset \mathbb{R}^n$ is the convex hull of a finite set of points. We say that $P$ is *$n$-dimensional* if $P$ has a non-empty interior. The intersection of $P$ with a supporting affine hyperplane is called a *face* of $P$. Faces of $P$ of dimension 0 are called *vertices* and faces of codimension 1 are called *facets* of $P$.

In this paper we prove the following result.

**(1.1) Theorem.** *For every $\alpha \geq 1$ there is $\gamma = \gamma(\alpha) > 0$ such that the following holds.*

*Suppose that $P \subset \mathbb{R}^n$ is a polytope containing the set*

$$\Big\{ x \in \mathbb{R}^n : \quad |\langle x, u_i \rangle| \ \leq \ 1 \quad \text{for} \quad i=1, \ldots, m \Big\}$$

*where $\|u_i\| \leq 1$ for $i=1, \ldots, m$ and $m \leq \alpha n$. Suppose further that $P$ lies inside the ball*

$$\Big\{ x \in \mathbb{R}^n : \quad \|x\| \ \leq \ \alpha \sqrt{n} \Big\}.$$

*Then $P$ has at least $2^{\gamma n}$ vertices.*

---

*Key words and phrases.* polytope, regular graph, factor.

This research was partially supported by NSF Grant DMS 0856640, by a United States - Israel BSF grant 2006377 and by ERC Advanced Grant No 267195.

Our first corollary is a lower bound for the number of vertices of a *centrally symmetric* polytope $P$, that is, a polytope $P$ satisfying $P = -P$.

**(1.2) Corollary.** *For every $\alpha \geq 1$ there exists $\gamma = \gamma(\alpha) > 0$ such that if $P$ is an $n$-dimensional centrally symmetric polytope with not more than $\alpha n$ facets then $P$ has at least $2^{\gamma n}$ vertices.*

By duality, an $n$-dimensional centrally symmetric polytope with $O(n)$ vertices has $2^{\Omega(n)}$ facets. Figiel, Lindenstrauss and Milman proved [F+77] that for an $n$-dimensional centrally symmetric polytope with $v$ vertices and $f$ facets one has

$$(\log v) \cdot (\log f) \;\geq\; \gamma n \tag{1.2.1}$$

for some absolute constant $\gamma > 0$. In particular, if $f = O(n)$ then inequality (1.2.1) implies that $v = 2^{\Omega(n/\log n)}$ and hence the estimate of Corollary 1.2 is sharper than (1.2.1) in this case.

Our second application is combinatorial.

Let $G$ be a $k$-regular graph with a finite set $V$ of vertices and a set $E$ of edges. Thus every vertex $v \in V$ is incident to precisely $k$ edges of $G$ (we do not allow multiple edges or loops). An $r$-regular subgraph $H$ of $G$ with the same set $V$ of vertices is called an *$r$-factor* of $G$. In particular, a 1-factor is also known as a *perfect matching* in $G$. For a set $U \subset V$ of vertices, we denote by $\delta(U) \subset E$ the *cut* associated with $U$, that is, the set of edges of $G$ with exactly one endpoint in $U$. We denote by $|X|$ the cardinality of a finite set $X$.

We prove that the number of $r$-factors in a $k$-regular graph without cuts of small size is exponentially large in the number of vertices of the graph.

**(1.3) Corollary.** *Let us fix positive integers $k$ and $r$ such that $k \geq 2r+1$. Then there exists $\gamma = \gamma(k, r) > 0$ such that the following holds.*

*Suppose that $G$ is a $k$-regular graph with a set $V$ of vertices such that*

$$\left|\delta(U)\right| \;>\; \frac{k}{r}$$

*for every $U \subset V$ such that $2 \leq |U| \leq |V| - 2$. Then the number of $r$-factors of $G$ is at least $2^{\gamma|V|}$.*

Note that the complement to an $r$-factor is a $(k-r)$-factor, so our result also produces an estimate for the number of factors of degree greater than one half of the degree of the graph.

The most tantalizing situation is that of $k = 3$ and $r = 1$, when Corollary 1.3 asserts that the number of perfect matchings of a 3-regular (also known as *cubic*) graph is exponentially large in the number $|V|$ of vertices of the graph, provided $\left|\delta(U)\right| \geq 4$ as long as $2 \leq |U| \leq |V| - 2$. This falls short of the recent result of [E+10], where it is proven that it suffices to have $\left|\delta(U)\right| \geq 2$, and hereby the Lovász-Plummer conjecture is confirmed. We hope, however, that our method can be sharpened to provide an alternative (and, perhaps, simpler) proof of the conjecture.

We prove Theorem 1.1 and Corollary 1.2 in Section 2 and Corollary 1.3 in Section 3.

The idea of the proof of Theorem 1.1 is, roughly, as follows. We consider the maximum of a random linear function on $P$. We argue that if the number of vertices of $P$ is small, then the maximum is also small. We then argue that if we go from the origin along a random direction then we stay long enough inside $P$. This proves that the maximum of a random linear function on $P$ is large enough and hence $P$ has sufficiently many vertices. A similar argument is used in Section VI.8 of [Ba02] in the proof of the Figiel-Lindenstrauss-Milman inequality (1.2.1).

To prove Corollary 1.2, we apply a linear transformation so that the image of $P$ satisfies the conditions of Theorem 1.1. To prove Corollary 1.3, we consider a polytope $P_r(G)$ whose vertices correspond to $r$-factors of $G$ and then apply Theorem 1.1.

Paper [BS07] describes a general method of asymptotic counting of combinatorial structures through optimization of a random linear function.

## 2. Proofs of Theorem 1.1 and of Corollary 1.2

Let us fix the standard Gaussian probability measure in $\mathbb{R}^n$ with the density

$$\frac{1}{(2\pi)^{n/2}} \exp\left\{-\frac{\|x\|^2}{2}\right\} \quad \text{for} \quad x \in \mathbb{R}^n.$$

**(2.1) Lemma.**

(1) *We have*

$$\mathbf{Pr}\left(y \in \mathbb{R}^n: \ \|y\|^2 \ \leq \ \frac{n}{2}\right) \ \leq \ \exp\left\{-\frac{n}{16}\right\}.$$

(2) *Let $a \in \mathbb{R}^n$ be a point. Then*

$$\mathbf{Pr}\Big(y \in \mathbb{R}^n: \ \langle y, a\rangle \ \geq \ \tau\Big) \ \leq \ \frac{1}{2}\exp\left\{-\frac{\tau^2}{2\|a\|^2}\right\} \quad \textit{for any} \quad \tau \geq 0.$$

(3) *For any $\beta \geq 0$ and any vectors $u_1, \ldots, u_m \in \mathbb{R}^n$ such that $\|u_i\| \leq 1$ for $i = 1, \ldots, m$, we have*

$$\mathbf{Pr}\Big(y \in \mathbb{R}^n: \ |\langle u_i, y\rangle| \leq \beta \quad \textit{for} \quad i = 1, \ldots, m\Big) \ \geq \ \left(1 - \exp\left\{-\frac{\beta^2}{2}\right\}\right)^m.$$

*Proof.* The inequality of Part (1) can be found, for example, in Corollary V.5.5 of [Ba02].

The function $y \longmapsto \langle y, a \rangle$ is a centered Gaussian random variable with variance $\|a\|^2$ and Part (2) follows by the standard Gaussian tail estimate.

By the Sidak Lemma, see, for example, [Ba01], we have

$$\mathbf{Pr}\Big(y \in \mathbb{R}^n: \ |\langle u_i, y \rangle| \leq \beta \quad \text{for} \quad i=1, \ldots, m\Big) \ \geq \ \prod_{i=1}^m \mathbf{Pr}\Big(y \in \mathbb{R}^n: \ |\langle u_i, y \rangle| \leq \beta\Big).$$

Since $y \longmapsto \langle u_i, y \rangle$ is a centered Gaussian random variable of variance $\|u_i\|^2 \leq 1$, the proof of Part (3) follows from Part (2). $\square$

**(2.2) Proof of Theorem 1.1.**

Without loss of generality we assume that $n \geq 16$.

We choose a sufficiently large $\beta = \beta(\alpha) > 0$ such that the following two inequalities hold:

$$\text{(2.2.1)} \qquad \left(1 - \exp\left\{-\frac{\beta^2}{2}\right\}\right)^{\alpha n} \ \geq \ 2 \exp\left\{-\frac{n}{16}\right\} \quad \text{for all} \quad n \geq 16$$

and

$$\text{(2.2.2)} \qquad \frac{1}{8\alpha^2 \beta^2} + \alpha \ln\left(1 - \exp\left\{-\frac{\beta^2}{2}\right\}\right) \ \geq \ \gamma \ > \ 0$$

for some $\gamma = \gamma(\alpha) > 0$.

Let us consider the polyhedron

$$Q = \Big\{y \in \mathbb{R}^n: \ |\langle y, u_i \rangle| \ \leq \ \beta \quad \text{for} \quad i = 1, \ldots, m\Big\}.$$

By Part (3) of Lemma 2.1 we have

$$\mathbf{Pr}\Big(y: \ y \in Q\Big) \ \geq \ \left(1 - \exp\left\{-\frac{\beta^2}{2}\right\}\right)^{\alpha n}.$$

We consider the maximum value of the linear function $x \longmapsto \langle x, y \rangle$ on $P$. Since for every $y \in Q$ we have $\beta^{-1} y \in P$ we conclude that

$$\text{(2.2.3)} \qquad \max_{x \in P} \langle x, y \rangle \ \geq \ \left\langle y, \ \frac{1}{\beta} y \right\rangle = \frac{1}{\beta}\|y\|^2 \quad \text{for all} \quad y \in Q.$$

By Part (1) of Lemma 2.1, by (2.2.3) and by (2.2.1), we have

$$\text{(2.2.4)} \qquad \mathbf{Pr}\left(y: \ \max_{x \in P} \langle x, y \rangle \ \geq \ \frac{n}{2\beta}\right) \ \geq \ \frac{1}{2}\left(1 - \exp\left\{-\frac{\beta^2}{2}\right\}\right)^{\alpha n}$$

provided $n \geq 16$.

On the other hand, the maximum value of a linear function on a polytope is attained, in particular, at a vertex of $P$. Therefore, taking $W$ to be the set of vertices of $P$, from Part (2) of Lemma 2.1, we conclude that

$$\begin{aligned}\mathbf{Pr}\left(y: \ \max_{x \in P}\langle x, y\rangle \ \geq \ \tau\right) \ &\leq \ \sum_{a \in W} \mathbf{Pr}\ (y: \ \langle y, a\rangle \ \geq \ \tau) \ \leq \ \frac{1}{2}\sum_{a \in W} \exp\left\{-\frac{\tau^2}{2\|a\|^2}\right\} \\ &\leq \frac{|W|}{2}\exp\left\{-\frac{\tau^2}{2\alpha^2 n}\right\}.\end{aligned}$$

Substituting

$$\tau = \frac{n}{2\beta},$$

we obtain

$$\mathbf{Pr}\left(y: \ \max_{x \in P}\langle x, y\rangle \ \geq \ \tau\right) \ \leq \ \frac{|W|}{2}\exp\left\{-\frac{n}{8\alpha^2\beta^2}\right\}.$$

Comparing the last inequality with (2.2.4) and using (2.2.2), we conclude that

$$|W| \ \geq \ \exp\left\{\frac{n}{8\alpha^2\beta^2}\right\}\left(1 - \exp\left\{-\frac{\beta^2}{2}\right\}\right)^{\alpha n} \ \geq \ \exp\{\gamma n\}$$

as desired. □

**(2.3) Proof of Corollary 1.2.**

We can write

$$P = \Big\{x \in \mathbb{R}^n: \quad |\langle u_i, x\rangle| \ \leq \ \alpha_i \quad \text{for} \quad i = 1, \ldots, m\Big\},$$

where $u_1, \ldots, u_m$ are the unit normals to the facets of $P$ and $\alpha_i > 0$. Applying to $P$ an invertible linear transformation, we may assume, additionally, that $P$ contains the unit ball and is contained in the ball of radius $\sqrt{n}$, both balls centered at the origin (see, for example, Sections V.2 and VI.8 of [Ba02]). Since $P$ contains the unit ball, we must have $\alpha_i \geq 1$ for all $i = 1, \ldots, m$ and the proof follows by Theorem 1.1. □

## 3. Proof of Corollary 1.3

**(3.1) The polytope.** Let $G$ be a graph with a set $V$ of vertices and a set $E$ of edges. We denote by $\mathbb{R}^E$ the Euclidean space of all real-valued functions $x: E \longrightarrow \mathbb{R}$. We use the standard scalar product

$$\langle x, y\rangle = \sum_{e \in E} x(e)y(e) \quad \text{for all} \quad x, y \in \mathbb{R}^E$$

and the corresponding Euclidean norm $\|x\| = \sqrt{\langle x, x\rangle}$.

For a subset $H \subset E$ we consider a vector (indicator function) $[H] \in \mathbb{R}^E$ defined as follows:

$$[H](e) = \begin{cases} 1 & \text{if } e \text{ is an edge of } H \\ 0 & \text{otherwise.} \end{cases}$$

We define the *r-factor polytope* $P_r(G)$ as the convex hull

$$P_r(G) = \operatorname{conv}\Bigl([H] : \quad H \text{ is an } r\text{-factor of } G\Bigr).$$

We will need the following description of $P_r(G)$ by a system of linear inequalities (3.1.1)–(3.1.3), see Corollary 33.2a of [Sc03] (recall that $\delta(U)$ denotes the set of edges of $G$ with precisely one endpoint in a set $U \subset V$ of vertices):

$$0 \ \leq \ x(e) \ \leq \ 1 \quad \text{for all} \quad e \in E, \tag{3.1.1}$$

$$\sum_{e \in \delta(v)} x(e) = r \quad \text{for all} \quad v \in V, \tag{3.1.2}$$

and

$$\begin{aligned} \sum_{e \in \delta(U) \setminus F} x(e) - \sum_{e \in F} x(e) \ \geq 1 - |F| \quad &\text{for all} \quad U \subset V, F \subset \delta(U) \\ &\text{such that} \quad r|U| + |F| \quad \text{is odd.} \end{aligned} \tag{3.1.3}$$

Our first goal is to show that if $G$ is $k$-regular graph without small cuts then the vector $a \in \mathbb{R}^E$ with $a(e) = r/k$ for all $e \in E$ lies sufficiently deep inside polytope $P_r(G)$.

**(3.2) Lemma.** *Suppose that $G$ is $k$-regular, that $k \geq 2r+1$ and that*

$$\bigl|\delta(U)\bigr| \ > \ \frac{k}{r}$$

*for all $U \subset V$ such that $2 \leq |U| \leq |V| - 2$. Let us choose an $\epsilon = \epsilon(k, r) > 0$ as follows:*

*if $k/r$ is integer, we let*

$$\epsilon = \min\left\{\frac{r}{k} - \frac{1}{1 + \frac{k}{r}}, \quad \frac{1}{2k}\right\} \quad \textit{and}$$

*if $k/r$ is not integer, we let*

$$\epsilon = \min\left\{\frac{r}{k} - \frac{1}{\lceil \frac{k}{r} \rceil}, \quad \frac{1}{2k}\right\}.$$

*Let $a \in \mathbb{R}^E$ be the vector such that*

$$a(e) = \frac{r}{k} \quad \textit{for all} \quad e \in E$$

*and let $y \in \mathbb{R}^E$ be a vector such that*

$$\sum_{e \in \delta(v)} y(e) = 0 \quad \textit{for all} \quad v \in V$$

*and*

$$|y(e)| \ \leq \ \epsilon \quad \textit{for all} \quad e \in E.$$

*Then for $x = a + y$ we have $x \in P_r(G)$.*

*Proof.* Clearly, vector $x$ satisfies (3.1.1) and (3.1.2). Moreover,

$$\frac{2r-1}{2k} \ \leq \ x(e) \ \leq \ \frac{2r+1}{2k} \quad \text{for all} \quad e \in E.$$

If in (3.1.3) we increase $|F|$ by 1 then the left hand side decreases at most by $(2r+1)/k$ while the right hand side decreases by 1. Therefore, it suffices to check (3.1.3) when $|F| = 0$. Furthermore, if $|U| = 1$ or if $|V \setminus U| = 1$, inequality (3.1.3) follows by (3.1.2).

If $|F| = 0$ then the left hand side of (3.1.3) is at least

$$\big|\delta(U)\big|\left(\frac{r}{k} - \epsilon\right) \ \geq \ 1$$

and (3.1.3) holds. □

**(3.3) Proof of Corollary 1.3.**

All implied constants in $O(\cdot)$ and $\Omega(\cdot)$ notation below may depend on $k$ and $r$ only.

Since $G$ is $k$-regular, we have $|E| = k|V|/2$. Let $L \subset \mathbb{R}^E$ be the subspace defined by the equations

$$\sum_{e \in \delta(v)} x(e) = 0 \quad \text{for all} \quad v \in V.$$

Hence

$$n = \dim L \ \geq \ |E| - |V| = \left(\frac{k}{2} - 1\right)|V| = \Omega(V).$$

We identify $L$ with $\mathbb{R}^n$. Let $P = P_r(G) - a$, where $a$ is the vector of Lemma 3.2. Then $P \subset \mathbb{R}^n$ by (3.1.2). Since

$$\|[H]\| \ = \sqrt{\frac{r|V|}{2}}$$

for any $r$-factor $H$ of $G$ and

$$\|a\| = \frac{r}{k}\sqrt{\frac{k|V|}{2}},$$

we conclude that $P$ lies in a ball of radius $O\left(\sqrt{n}\right)$ centered at the origin.

Moreover, by Lemma 3.2, polytope $P$ contains the set

$$\Big\{x \in \mathbb{R}^n : \quad |\langle u_e, x\rangle| \ \leq \ \epsilon \quad \text{for all} \quad e \in E\Big\},$$

where $u_e$ is the orthogonal projection of $[e]$ onto $L$. In particular, $\|u_e\| \leq 1$ for all $e \in E$. Since $|E| = O(n)$ and $\epsilon = \Omega(1)$, the proof is obtained by applying Theorem 1.1 to the dilated polytope $\epsilon^{-1}P$. □


## Acknowledgment

The author is grateful to Alex Samorodnitsky for many useful discussions and comments on a draft of this paper and to Alfréd Rényi Institute of Mathematics (Budapest) for hospitality during his work on this paper.


## References


[Ba01] K. Ball, *Convex geometry and functional analysis*, Handbook of the Geometry of Banach Spaces, Vol. I, North-Holland, Amsterdam, 2001, pp. 161–194.

[Ba02] A. Barvinok, *A Course in Convexity*, Graduate Studies in Mathematics, 54, American Mathematical Society, Providence, RI, 2002.

[BS07] A. Barvinok and A. Samorodnitsky, *Random weighting, asymptotic counting, and inverse isoperimetry*, Israel J. Math. **158** (2007), 159–191.

[E+10] L. Esperet, F. Kardos, A. King, D. Kral and S. Norine, *Exponentially many perfect matchings in cubic graphs*, preprint `arXiv:1012.2878` (2010).

[F+77] T. Figiel, J. Lindenstrauss and V.D. Milman, *The dimension of almost spherical sections of convex bodies*, Acta Math. **139** (1977), 53–94.

[Sc03] A. Schrijver, *Combinatorial Optimization. Polyhedra and Efficiency. Vol. A. Paths, Flows, Matchings. Chapters 1–38*, Algorithms and Combinatorics, vol. 24, A, Springer-Verlag, Berlin, 2003.



Department of Mathematics, University of Michigan, Ann Arbor, MI 48109-1043, USA

*E-mail address*: `barvinok@umich.edu`