# The chromatic number of graph powers 

NOGA ALON ${ }^{1} \dagger$ and $\mathrm{BOJAN} \mathrm{MOHAR}^{2} \ddagger$<br>${ }^{1}$ Department of Mathematics, Tel Aviv University<br>Tel Aviv, Israel<br>${ }^{2}$ Department of Mathematics, University of Ljubljana<br>1111 Ljubljana, Slovenia

It is shown that the maximum possible chromatic number of the square of a graph with maximum degree $d$ and girth $g$ is $(1+o(1)) d^{2}$ if $g=3,4,5$ or 6 , and is $\Theta\left(d^{2} / \log d\right)$ if $g \geq 7$. Extensions to higher powers are considered as well.

## 1. Introduction

The square $G^{2}$ of a graph $G=(V, E)$ is the graph whose vertex set is $V$ in which two distinct vertices are adjacent if and only if their distance in $G$ is at most 2 . What is the maximum possible chromatic number of $G^{2}$, as $G$ ranges over all graphs with maximum degree $d$ and girth $g$ ?

Our (somewhat surprising) answer is that for $g=3,4,5$ or 6 this maximum is $(1+$ $o(1)) d^{2}$ (where the $o(1)$ term tends to 0 as $d$ tends to infinity), whereas for all $g \geq 7$, this maximum is of order $d^{2} / \log d$.

To state this result more precisely, define, for every two integers $d \geq 2$ and $g \geq 3$, $f_{2}(d, g)$ to be the maximum possible value of $\chi\left(G^{2}\right)$ over all graphs with maximum degree $d$ and girth $g$. Since the maximum degree of $G^{2}$ is at most $d+d(d-1)=d^{2}$, it follows that for every $g$

$$
\begin{equation*}
f_{2}(d, g) \leq d^{2}+1 \tag{1}
\end{equation*}
$$

Equality holds in (1) for $d=2$ and $g \leq 5$, as shown by the 5 -cycle, for $d=3$ and $g \leq 5$, as shown by the Petersen graph, and for $d=7$ and $g \leq 5$, as shown by the Hoffman-Singleton graph, see [HS]. Moreover, by Brooks Theorem (c.f., e.g., [Bo1]) it follows that equality can hold in (1) only for $g \leq 5$ and only if there exists a $d$-regular graph of diameter 2 on $d^{2}+1$ vertices. As proved in [HS] if such a graph exists then
$\dagger$ Research supported in part by a USA-Israel BSF grant and by a grant from the Israel Science Foundation.
$\ddagger$ Supported in part by the Ministry of Science and Technology of Slovenia, Research Project J1-0502-0101-98.
$d \in\{2,3,7,57\}$, and it is known to exist for $d \in\{2,3,7\}$, whereas the case $d=57$ is still open.

It is also not difficult to see that $f_{2}(2, g)=4$ for all $g \geq 6$ as shown, for example, by the disjoint union of a $g$-cycle and a cycle of length $l \geq g$ where $l$ is not divisible by 3 .

In this short paper we prove the following.

Theorem 1.1. (i) There exists a function $\varepsilon(d)$ that tends to 0 as $d$ tends to infinity such that for all $g \leq 6$

$$
(1-\varepsilon(d)) d^{2} \leq f_{2}(d, g) \leq d^{2}+1
$$

(ii) There are absolute positive constants $c_{1}, c_{2}$ such that for every $d \geq 2$ and every $g \geq 7$

$$
c_{1} \frac{d^{2}}{\log d} \leq f_{2}(d, g) \leq c_{2} \frac{d^{2}}{\log d}
$$

Theorem 1.1 exhibits an interesting "phase transition:" As $g$ grows from 3 to $6, f_{2}(d, g)$ stays roughly the same, while it drops significantly when $g$ increases from 6 to 7 , and then it stays essentially the same as $g$ keeps increasing.

The rest of the paper contains the proof of the theorem and an extension of Theorem 1.1 for higher powers of graphs. Throughout the paper, all logarithms are in base $e$.

## 2. The upper bounds

The proof of the upper bounds in parts (i) and (ii) of Theorem 1.1 are rather simple (given the main result in [AKS]). The upper bound in part (i) follows from (1). To prove the upper bound in (ii), we need the following result of [AKS].

Theorem 2.1 ([AKS]). There is an absolute constant $c$ such that for every integer $\Delta$ and every real number $t, 2 \leq t \leq \Delta^{2}$, the chromatic number of any graph $H$ with maximum degree at most $\Delta$ in which for every vertex $v$, the induced subgraph on the set of all neighbors of $v$ spans at most $\Delta^{2} / t$ edges, satisfies

$$
\chi(H) \leq c \frac{\Delta}{\log t}
$$

We can now prove that there is a constant $c_{2}$ such that for all $g \geq 7$

$$
\begin{equation*}
f_{2}(d, g) \leq c_{2} \frac{d^{2}}{\log d} \tag{2}
\end{equation*}
$$

Let $G=(V, E)$ be a graph with maximum degree $d$ and girth $g \geq 7$. Let $H=G^{2}$. Then the maximum degree of $H$ is at most $d+d(d-1)=d^{2}$. It is not difficult to check that if $u, v \in V$ are adjacent in $H$, then they have less than $2 d$ common neighbors in $H$. It follows that each neighborhood of a vertex of $H$ spans less than $\frac{d^{2} .2 d}{2}=d^{3}$ edges. (In fact, the induced subgraph on each neighborhood consists of at most $d+1$ edge-disjoint cliques of size at most $d$ each, implying it spans at most $(d+1) d(d-1) / 2<d^{3} / 2$ edges.) Applying Theorem 2.1 with $\Delta=d^{2}$ and $t=d$, we conclude that (2) holds.

## 3. The lower bounds

In this section we prove the lower bounds in Theorem 1.1. The bound in part (i) is simple. If $d=q+1$ for some prime power $q$, then the bipartite incidence graph of the lines and points of the finite projective plane of order $q$ form a $d$-regular bipartite graph $G$ on $2\left(q^{2}+q+1\right)$ vertices. The girth of $G$ is 6 and its square contains two cliques of size $q^{2}+q+1=d^{2}-d+1$ each, and hence $\chi\left(G^{2}\right) \geq d^{2}-d+1$. (It is, in fact, easy to check that $\chi\left(G^{2}\right)=d^{2}-d+1$.)

Remark: It is not difficult to check that if $G$ has girth 6 and maximum degree $d$, then the maximum clique in $G^{2}$ is of size at most $d^{2}-d+1$. To see this, fix a vertex $v$ in a maximum clique of $G^{2}$. Then, in $G^{2}, v$ is connected to the set $N(v)$ of its neighbors in $G$, where $|N(v)| \leq d$, and to the set $N^{2}(v)$ of the vertices at distance 2 from $v$, where $\left|N^{2}(v)\right| \leq d^{2}-d$. Since the girth is 6 , any member of $N(v)$ is connected in $G^{2}$ to at most $d-1$ members of $N^{2}(v)$. It follows that if the clique contains more than $d-1$ members of $N^{2}(v)$ then it contains no member of $N(v)$. Thus, the size of the clique is at most $1+d^{2}-d$. The main result of Reed in [Re] asserts that there is some absolute positive constant $\epsilon$ such that for every graph $H$ with maximum degree $\Delta$, maximum clique size $\omega$ and chromatic number $\chi$, the inequality $\chi \leq \epsilon \omega+(1-\epsilon)(\Delta+1)$ holds. This implies that if $G$ has girth 6 and maximum degree $d>2$ then $\chi\left(G^{2}\right) \leq d^{2}-\Omega(d)$, showing that the example above is nearly tight.

Returning to the proof of the lower bound in part (i) of Theorem 1.1 for general $d$, we simply choose the largest prime power $q$ satisfying $q+1 \leq d$, and take the graph constructed above for $q$ together with some extra pendant edges to make sure that the maximum degree is precisely $d$. By the known results on the distribution of primes (see, e.g., $[\mathrm{Hu}]), q^{2}+q+1 \geq(1-\varepsilon(d)) d^{2}$, where $\varepsilon(d)$ tends to 0 as $d$ tends to infinity. This proves the lower bound in Theorem 1.1 part (i) for $g=6$. The bounds for $g=3,4,5$ follow by simply adding to the example for $g=6$ a vertex disjoint copy of a cycle of length $g$.

It remains to prove the lower bound in Theorem 1.1(ii). This is done by a probabilistic construction. Note that we may assume, without loss of generality, that $d$ is sufficiently large (by choosing $c_{1}>0$ sufficiently small), and we thus assume, from now on, that $d$ is large (for example, $d \geq 10^{10}$ will be enough). We also omit all floor and ceiling signs whenever they are not crucial, to simplify the presentation.

Let $n$ be a large integer $\left(n \gg d^{g}\right)$, let $V^{\prime}=\{1, \ldots, n\}$, define $p=\frac{d}{2 n}$, and let $G^{\prime}=\left(V^{\prime}, E^{\prime}\right)$ be a random graph on $V^{\prime}$ obtained by choosing each pair of distinct elements of $V^{\prime}$, randomly and independently, to be an edge with probability $p$. The expected value of each vertex degree in $G^{\prime}$ is $\frac{d}{2 n}(n-1)<\frac{d}{2}$. However, $G^{\prime}$ will have, with high probability, about $n \cdot 2^{-\Theta(d)}$ vertices of degree higher than $d$. It will also have, with high probability, some cycles of length less than $g$ (fewer than $O\left(d^{g}\right)$ of them). By omitting all vertices of degree $>d$ and by removing an arbitrarily chosen vertex from each cycle of length $<g$ we get a graph of girth $\geq g$ and maximum degree at most $d$. (If necessary, we can add a cycle of length $g$ and some pendant edges to make sure that the maximum degree is equal to $d$ and that the girth is precisely $g$.)

As we show next, with high probability, for the graph $G$ obtained in this manner, $G^{2}$
does not contain an independent set of size bigger than $c \frac{n}{d^{2}} \log d$ for an appropriately chosen constant $c>0$, and hence $\chi\left(G^{2}\right) \geq \Omega\left(d^{2} / \log d\right)$, as needed.

The detailed proof is given in the following claims (where we make no attempt to optimize the absolute constants).

Claim 3.1. The expected number of vertices of degree $>d$ in $G^{\prime}$ is at most $n \cdot 2^{-d / 10}$. Thus, with probability $\geq 0.9$, there are at most $10 n \cdot 2^{-d / 10}$ such vertices.

Proof. The degree of any fixed vertex is a binomial random variable with parameters $n-1$ and $p=\frac{d}{2 n}$, and hence its expected degree is less than $d / 2$.

By the standard estimates for binomial distributions (see, e.g., [AS, Appendix A]), the probability that the degree of such a vertex exceeds $d$ is smaller than $2^{-d / 10}$. By linearity of expectation, the expected number of vertices of degree $>d$ is thus at most $n \cdot 2^{-d / 10}$, and hence, by Markov's inequality, the probability that there are more than $10 n \cdot 2^{-d / 10}$ such vertices is at most 0.1 . (In fact, this probability is exponentially small, but this is not needed here.)

Claim 3.2. The expected number of cycles of length $<g$ in $G^{\prime}$ is

$$
\sum_{i=3}^{g-1} \frac{n(n-1) \cdots(n-i+1)}{2 i}\left(\frac{d}{2 n}\right)^{i}<\frac{1}{2} \sum_{i=3}^{g-1}\left(\frac{d}{2}\right)^{i}<d^{g}
$$

and hence with probability $\geq 0.9$, there are at most $10 d^{g}$ such cycles.
Proof. Straightforward.
Claim 3.3. There exists a constant $c, 0<c<1000$, such that almost surely (that is, with probability that tends to 1 as $n$ tends to infinity) the following holds: For every set of vertices $U \subset V^{\prime}$ of cardinality $|U|=c \frac{n}{d^{2}} \log d$, there are at least $\frac{1}{30} c^{2} n \frac{\log ^{2} d}{d^{2}}$ vertices outside $U$ that have exactly 2 neighbors in $U$.

Proof. Put $x=c \frac{n}{d^{2}} \log d$. Fix a set $U,|U|=x$, and fix a vertex $w \in V^{\prime} \backslash U$. Note that, as $d$ is large, $\left|V^{\prime} \backslash U\right| \geq \frac{3 n}{4}$. The probability of the event $E_{w}$ that $w$ has precisely two neighbors in $U$ is

$$
\begin{aligned}
q & =\binom{x}{2} p^{2}(1-p)^{x-2} \geq \frac{x(x-1)}{2}\left(\frac{d}{2 n}\right)^{2}\left(1-\frac{d}{2 n}\right)^{x} \\
& \geq \frac{x(x-1)}{2}\left(\frac{d}{2 n}\right)^{2}\left(1-\frac{x d}{2 n}\right) \geq \frac{1}{10} c^{2} \frac{\log ^{2} d}{d^{2}} .
\end{aligned}
$$

The number of vertices $w \in V^{\prime} \backslash U$ is at least $\frac{3 n}{4}$, and as the events $E_{w}$ are mutually independent, the number of vertices $w \in V^{\prime} \backslash U$ that have 2 neighbors in $U$ is a binomial random variable with parameters $\left|V^{\prime} \backslash U\right| \geq \frac{3 n}{4}$ and $q \geq \frac{1}{10} c^{2} \frac{\log ^{2} d}{d^{2}}$. The expected value of this number is at least $\frac{3}{40} c^{2} n \frac{\log ^{2} d}{d^{2}}$ and hence, by the standard estimates for binomial distributions (see, e.g., [AS, Appendix A]), the probability that it is smaller than $\frac{1}{30} c^{2} n \frac{\log ^{2} d}{d^{2}}$ is at most, say, $e^{-\frac{1}{300} c^{2} n \frac{\log ^{2} d}{d^{2}}}$.

Therefore, for each fixed set $U$, the probability that there are less than $\frac{1}{30} c^{2} n \frac{\log ^{2} d}{d^{2}}$ vertices $w \in V^{\prime} \backslash U$ with precisely 2 neighbors in $U$ is at most $e^{-\frac{1}{300} c^{2} n \frac{\log ^{2} d}{d^{2}}}$. As the total number of sets $U$ is

$$
\binom{n}{x}=\binom{n}{c \frac{n}{d^{2}} \log d} \leq\left(\frac{e d^{2}}{c \log d}\right)^{c \frac{n}{d^{2}} \log d} \leq e^{3 c \frac{n}{d^{2}} \log ^{2} d}
$$

it follows that if $\frac{c^{2}}{300}>3 c$, then with probability $1-o(1)$ every set $U$ has at least that many vertices $w$ with 2 neighbors in $U$. This completes the proof of the claim.

We can now complete the proof of Theorem 1.1. For any given $g$ and (large) $d$, choose $n \gg d^{g}$. By Claims 3.1-3.3, there exists a graph $G^{\prime}$ on $n$ vertices satisfying the conclusions of all three claims. Let $G$ be the graph obtained from $G^{\prime}$ by omitting all vertices of degree $>d$ and an arbitrarily chosen vertex from each cycle of length $<g$. Then $G$ has girth $\geq g$, maximum degree $\leq d$, and more than $n / 2$ vertices. As $G^{\prime}$ satisfies the conclusion of Claim 3.3, and as the total number of vertices omitted (which is at most $10 n \cdot 2^{-d / 10}+10 d^{g}$ ) is smaller than $\frac{c^{2}}{30} n \frac{\log ^{2} d}{d^{2}}$, it follows that $G^{2}$ contains no independent set of size $x=c \frac{n}{d^{2}} \log d$. Thus $\chi\left(G^{2}\right) \geq \frac{d^{2}}{2 c \log d}$.

By adding to $G$, if needed, pendant edges and a disjoint copy of a cycle of length $g$ we conclude that

$$
f_{2}(d, g) \geq \frac{d^{2}}{2 c \log d}
$$

for all $d, g$, completing the proof of Theorem 1.1.

## 4. Higher powers

The $k^{\text {th }}$ power $G^{k}$ of a graph $G=(V, E)$ is the graph whose vertex set is $V$ in which two distinct vertices are adjacent if and only if their distance in $G$ is $\leq k$. Note that $G^{1}=G$. Let $f_{k}(d, g)$ denote the maximum possible value of $\chi\left(G^{k}\right)$, as $G$ ranges over all graphs of maximum degree $d$ and girth $g$. Trivially, $f_{1}(d, 3)=d+1$ for all $d \geq 2$. By the theorem of Johansson [Jo] and the known results about chromatic numbers of random graphs ( $[\mathrm{Bo} 2, \mathrm{KM}]$ ), there are absolute constants $c_{1}, c_{2}$ such that for every $d \geq 2$ and every $g \geq 4$

$$
c_{1} \frac{d}{\log d} \leq f_{1}(d, g) \leq c_{2} \frac{d}{\log d}
$$

The behavior of $f_{k}(d, g)$ for $k=2$ is determined by Theorem 1.1. For higher values of $k$, the situation is less clear, though the main parts of the proof of Theorem 1.1 can be extended. If $G$ has maximum degree $d$, then the maximum degree of $G^{k}$ is at most

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

Therefore, for every fixed $k$,

$$
f_{k}(d, g) \leq \frac{d}{d-2}\left((d-1)^{k}-1\right)+1=O\left(d^{k}\right)
$$

The known constructions of large graphs with a given maximum degree and diameter at most $k$ show that for every $k$ there exists a constant $c_{k}>0$ such that for some small values of $g$

$$
f_{k}(d, g) \geq c_{k} d^{k}
$$

For example, the DeBruijn graphs show that

$$
f_{k}(d, 3) \geq\lfloor d / 2\rfloor^{k}
$$

and the existence of generalized $m$-gons imply similar estimates for somewhat larger values of $g$. See also the constructions in $[\mathrm{BDF}],[\mathrm{LU}]$ and their references.

Finally, the proof in Section 2 and the random construction described in Section 3 can be extended to prove the following

Theorem 4.1. There exists an absolute constant $c>0$ such that for all integers $k \geq 1$, $d \geq 2$ and $g \geq 3 k+1$

$$
f_{k}(d, g) \leq \frac{c}{k} \frac{d^{k}}{\log d}
$$

For every integer $k \geq 1$ there exists a positive number $b_{k}$ such that for every $d \geq 2$ and $g \geq 3$

$$
f_{k}(d, g) \geq b_{k} \frac{d^{k}}{\log d}
$$

The proof in Section 2 easily extends to a proof of the upper bound in Theorem 4.1, and the details are left to the reader.

The proof of the lower bound follows the basic approach in Section 3, but requires somewhat more sophisticated tools in order to show that the random graph $G^{\prime}$ satisfies the following property almost surely: For an appropriately chosen constant $c_{k}$, for every set $U \subseteq V^{\prime}$ of size $|U|=c_{k} \frac{n}{d^{k}} \log d$, there are at least $\Omega\left(c_{k}^{2} \frac{n}{d^{k}} \log ^{2} d\right)$ internally vertex disjoint paths of length $k$, both whose endpoints lie in $U$, and whose other vertices lie in $V^{\prime} \backslash U$.

This can be proved using Talagrand's Inequality [Ta] (cf. also [AS], Chapter 7) and implies the assertion of Theorem 4.1 following the reasoning of the proof in Section 3. We proceed with the details.

Throughout the proof we assume, whenever this is needed, that $d$ is sufficiently large as a function of $k$, and omit, as before, all floor and ceiling signs whenever these are not crucial. Let $V^{\prime}=\{1,2, \ldots, n\}$, suppose $n \gg d^{g}$, and let $G^{\prime}=\left(V^{\prime}, E^{\prime}\right)$ be a random graph on $V^{\prime}$ obtained by choosing each pair of distinct elements of $V^{\prime}$, randomly and independently, to be an edge with probability $p=\frac{d}{2 n}$. Define $x=c_{k} \frac{n}{d^{k}} \log d$, where $c_{k}>0$ will be chosen later.

Lemma 4.1. For an appropriate choice of $c_{k}$, the following holds almost surely. For every set of vertices $U \subset V^{\prime}$ of cardinality $|U|=x$, there are at least $\frac{c_{k}^{2} n \log ^{2} d}{2^{k+5} d^{k}}$ internally vertex disjoint paths of length $k$, both of whose endpoints lie in $U$, and whose other vertices lie in $V^{\prime} \backslash U$.

Proof. We shall apply Talagrand's Inequality. To do so, fix a set $U \subset V^{\prime},|U|=x$. Call any path of length $k$, whose endpoints lie in $U$ and whose internal vertices lie outside $U$, a $U$-path. Let $X=X\left(G^{\prime}\right)$ be the random variable counting the maximum number of internally vertex disjoint $U$-paths. We first show that the expected value of $X$ satisfies

$$
\begin{equation*}
E(X) \geq \frac{c_{k}^{2} n \log ^{2} d}{2^{k+2} d^{k}} \tag{3}
\end{equation*}
$$

Indeed, the expected number of $U$-paths is

$$
\begin{aligned}
\mu & =\binom{x}{2}(n-x)(n-x-1) \cdots(n-x-k+2) p^{k} \\
& >0.49 \frac{c_{k}^{2} n^{k+1}}{d^{2 k}} \log ^{2} d p^{k}=0.49 \frac{c_{k}^{2} n}{2^{k} d^{k}} \log ^{2} d
\end{aligned}
$$

where here we used the fact that $d$ is sufficiently large.
Let $\Delta$ denote the expected number of pairs of $U$-paths that share at least one common internal vertex. We claim that, as $n \gg d \gg k, \Delta<\mu / 3$ (with room to spare).

Indeed, the expected number of such pairs that share only one endpoint and its unique neighbor is at most

$$
\mu n^{k-2} x p^{k-1}=\frac{\mu c_{k} \log d}{2^{k-1} d}
$$

It is not difficult to check that for $n \gg d \gg k$, the expected number of pairs of internally intersecting $U$-paths of any other type is much smaller, and the number of types is bounded by a function of $k$.

By omitting an arbitrarily chosen path from each pair of internally intersecting $U$ paths we get a collection of internally pairwise vertex disjoint $U$-paths. It follows, by linearity of expectation, that $E(X) \geq \mu-\Delta$, implying (3).

To apply Talagrand's Inequality (in the form presented, for example, in [AS, Chapter 7]), note that $X$ is a Lipschitz function, i.e., $\left|X\left(G^{\prime}\right)-X\left(G^{\prime \prime}\right)\right| \leq 1$ if $G^{\prime}, G^{\prime \prime}$ differ in at most one edge. This is because $X$ counts internally vertex disjoint paths, which are edge disjoint, and hence no single edge can change the value of $X$ by more than 1 . Note also that $X$ is $f$-certifiable for $f(s)=k s$, that is, when $X\left(G^{\prime}\right) \geq s$ there is a set of at most $k s$ edges of $G^{\prime}$ so that for every graph $G^{\prime \prime}$ that agrees with $G^{\prime \prime}$ on these edges, $X\left(G^{\prime \prime}\right) \geq s$.

By Talagrand's Inequality we conclude that for every $b$ and $t$

$$
\begin{equation*}
\operatorname{Pr}[X \leq b-t \sqrt{k b}] \cdot \operatorname{Pr}[X \geq b] \leq e^{-t^{2} / 4} \tag{4}
\end{equation*}
$$

Let $B$ denote the median of $X$. Without trying to optimize the constants, we prove that

$$
\begin{equation*}
B \geq \frac{c_{k}^{2} n \log ^{2} d}{2^{k+4} d^{k}} \tag{5}
\end{equation*}
$$

Indeed, assume this is false and apply (4) with $b=\frac{c_{k}^{2} n \log ^{2} d}{2^{k+3} d^{k}}$ and $t=\frac{1}{2} \sqrt{\frac{b}{k}}$ to conclude that

$$
\operatorname{Pr}\left[X \leq \frac{b}{2}\right] \cdot \operatorname{Pr}[X \geq b] \leq e^{-\frac{b}{16 k}}
$$

Since, by assumption, $B \leq \frac{b}{2}$, it follows that $\operatorname{Pr}[X \leq b / 2] \geq 1 / 2$, and hence $\operatorname{Pr}[X \geq b] \leq$
$2 e^{-\frac{b}{16 k}}$. However, as $X\left(G^{\prime}\right)<n$ for every $G^{\prime}$, this implies that

$$
E(X) \leq b+n 2 e^{-\frac{b}{16 k}}=b+2 n e^{-\frac{c_{k}^{2} n \log ^{2} d}{2^{k+7} d^{k} k}}=b+o(1)=\frac{c_{k}^{2} n \log ^{2} d}{2^{k+3} d^{k}}+o(1)
$$

contradicting (3) and thus proving (5).
We can now apply (4) again with $b=\frac{c_{k}^{2} n \log ^{2} d}{2^{k+4} d^{k}}$ and $t=\frac{1}{2} \sqrt{\frac{b}{k}}$ to conclude that

$$
\operatorname{Pr}\left[X \leq \frac{b}{2}\right] \operatorname{Pr}[X \geq b] \leq e^{-\frac{b}{16 k}}
$$

By (5), $\operatorname{Pr}[X \geq b] \geq 1 / 2$, and hence

$$
\operatorname{Pr}\left[X \leq \frac{b}{2}\right] \leq 2 e^{-\frac{b}{16 k}}=2 e^{-\frac{c_{k}^{2} n \log ^{2} d}{2^{k+8} d^{k} k}} .
$$

We have thus proved that for every fixed $U$, the probability that there are less than $\frac{b}{2}=\frac{c_{k}^{2} n \log ^{2} d}{2^{k+5} d^{k}}$ internally vertex disjoint $U$-paths is at most $2 e^{-\frac{c_{k}^{2} n \log ^{2} d}{2^{k+d_{d}^{k} k}}}$. Since the total number of sets $U$ is at most

$$
\binom{n}{x} \leq\left(\frac{e n}{x}\right)^{x} \leq\left(\frac{e d^{k}}{c_{k} \log d}\right)^{c_{k} \frac{n}{d^{k}} \log d} \leq e^{c_{k} k \frac{n}{d^{k}} \log ^{2} d}
$$

it follows that if, say

$$
\frac{c_{k}^{2}}{2^{k+8} k}>2 k c_{k}
$$

then with probability $1-o(1)$ for every set $U$ there are at least $\frac{c_{k}^{2} n \log ^{2} d}{2^{k+5} d^{k}}$ pairwise internally vertex disjoint $U$-paths. This completes the proof of the lemma.

We can now complete the proof of Theorem 4.1. For any given $g$ and $k$, and any (large) $d$ and sufficiently large $n$ there exists a graph $G^{\prime}$ satisfying the conclusions of Claim 3.1, Claim 3.2 and Lemma 4.1. Let $G$ be the graph obtained from $G^{\prime}$ by omitting all vertices of degree greater than $d$ and an arbitrarily chosen vertex from each cycle of length $<g$. Then $G$ has girth $\geq g$, maximum degree $\leq d$, and more than $n / 2$ vertices. As $G^{\prime}$ satisfies the conclusion of Lemma 4.1, and as the total number of vertices omitted from it to create $G$ is at most

$$
10 n \cdot 2^{-d / 10}+10 d^{g}<\frac{c_{k}^{2} n \log ^{2} d}{2^{k+5} d^{k}}
$$

it follows that $G^{k}$ contains no independent set of size $x=c_{k} \frac{n \log d}{d^{k}}$. Therefore $\chi\left(G^{k}\right) \geq$ $\frac{d^{k}}{2 c_{k} \log d}$.

By adding to $G$, if needed, pendant edges and a disjoint copy of a cycle of length $g$ this implies that for an appropriately defined $b_{k}>0$,

$$
f_{k}(d, g) \geq b_{k} \frac{d^{k}}{\log d}
$$

for all $d, g$, completing the proof of Theorem 4.1.

Note that for $k=1$ and 2 , the function $f_{k}(d, g)$ exhibits a drastic change when $g$
changes from $3 k$ to $3 k+1$. It would be interesting to decide if this is the case for higher values of $k$ as well. The results mentioned in this section do suggest that for every $k$ there is some integer $g_{k}$ such that

$$
f_{k}(d, g)=\Theta_{k}\left(d^{k}\right), \quad \text { for } g \leq g_{k}
$$

and

$$
f_{k}(d, g)=\Theta_{k}\left(d^{k} / \log d\right), \quad \text { for } g>g_{k}
$$

At the moment, however, we are unable to prove the existence of such a $g_{k}$.
Acknowledgement. Part of this work was done during a visit at the workshop on Graph Coloring organized by Pavol Hell in the PIMS Institute at the Simon Fraser University in July, 2000. We would like to thank Pavol and the other hosts at PIMS for their hospitality.

## References

[AS] N. Alon and J. H. Spencer, The Probabilistic Method, Second Edition, Wiley, New York, 2000.
[AKSy. Alon, M. Krivelevich, and B. Sudakov, Coloring graphs with sparse neighborhoods, J. Combin. Theory Ser. B 77 (1999) 73-82.
[BDE].-C. Bermond, C. Delorme, and G. Farhi, Large graphs with given degree and diameter, II, J. Combin. Theory Ser. B 36 (1984) 32-48.
[Bo1B. Bollobás, Extremal Graph Theory, Academic Press, London and New York, 1978.
[Bo2B. Bollobás, Chromatic number, girth and maximal degree, Discrete Math. 24 (1978), 311314.
[HS] A. J. Hoffman and R. R. Singleton, On Moore graphs with diameters 2 and 3, IBM J. Res. Develop. 4 (1960) 497-504.
[ Hu$] \mathrm{M} . \mathrm{N}$. Huxley, On the difference between consecutive primes, Invent. Math. 15 (1972) 164170.
[Jo] A. R. Johansson, Asymptotic choice number for triangle free graphs, to appear.
[KMA. V. Kostochka and N. P. Mazurova, An inequality in the theory of graph coloring (in Russian), Metody Diskret. Analiz. 30 (1977) 23-29.
[LU]F. Lazebnik and V. A. Ustimenko, New examples of graphs without small cycles and of large size, European J. Combin. 14 (1993) 445-460.
[Re] B. Reed, $\omega, \Delta$, and $\chi$, J. Graph Theory 27 (1998) 177-212.
[Ta] M. Talagrand, Concentration of measure and isoperimetric inequalities in product spaces, Inst. Hautes Études Sci. Publ. Math. 81 (1995) 73-205.

