# CAYLEY GRAPHS GENERATED BY SMALL DEGREE POLYNOMIALS OVER FINITE FIELDS 

IGOR E. SHPARLINSKI


#### Abstract

We improve upper bounds of F. R. K. Chung and of M. Lu, D. Wan, L.-P. Wang, X.-D. Zhang on the diameter of some Cayley graphs constructed from polynomials over finite fields.


## 1. Introduction

Let $\mathcal{P}_{d}$ be the set of monic polynomials of degree $d$ over a finite field $\mathbb{F}_{q}$ of $q$ elements, that are powers of some irreducible polynomial, that is

$$
\begin{aligned}
\mathcal{P}_{d}=\left\{g \in \mathbb{F}_{q}[X]:\right. & \operatorname{deg} g=d, g=h^{k} \\
& \left.h \in \mathbb{F}_{q}[X] \text { monic and irreducible, } k=1,2, \ldots,\right\}
\end{aligned}
$$

For a root $\alpha$ of an irreducible polynomial $f \in \mathbb{F}_{q}[X]$ of degree $n$, thus $\mathbb{F}_{q}(\alpha)=\mathbb{F}_{q^{n}}$, we define

$$
\mathcal{E}(\alpha, d)=\left\{g(\alpha): g \in \mathcal{P}_{d}\right\}
$$

It is easy to see that for $d<n$ we have

$$
\# \mathcal{E}(\alpha, d)=\# \mathcal{P}_{d}=(1+o(1)) \frac{q^{d}}{d}
$$

as $d \rightarrow \infty$, see also (3) below.
Following Lu, Wan, Wang and Zhang [6], we now define the directed Cayley graph $\mathfrak{G}(\alpha, d)$ on $q^{n}-1$ vertices, labelled by the elements of $\mathbb{F}_{q^{n}}^{*}$, where for $u, v \in \mathbb{F}_{q^{n}}^{*}$ the edge $u \rightarrow v$ exists if and only if $u / v \in \mathcal{E}(\alpha, d)$. These graphs are similar to those introduced by Chung [1] however are a little spraser: they are $\# \mathcal{P}_{d}$-regular rather than $q^{d}$-regular as in [1].

It has been shown in [6] that the graphs $\mathfrak{G}(\alpha, d)$ have very attractive connectivity properties. In particular, we denote by $D(\alpha, d)$ the diameter of $\mathfrak{G}(\alpha, d)$. Using bounds of multiplicative character sum from [7, Theorem 2.1], Lu, Wan, Wang and Zhang [6] have shown that for $n<q^{d / 2}+1$ the graph $\mathfrak{G}(\alpha, d)$ is connected and its diameter satisfies the inequality

$$
\begin{equation*}
D(\alpha, d) \leq \frac{2 n}{d}\left(1+\frac{2 \log (n-1)}{d \log q-2 \log (n-1)}\right)+1 \tag{1}
\end{equation*}
$$

Here we augment the argument of [6] with some new combinatorial and analytic considerations and improve the bound (11).

First we assume that $d \geq 2$.
Theorem 1. For $d \geq 2$ and a root $\alpha$ of an irreducible polynomial $f \in \mathbb{F}_{q}[X]$ of degree $\operatorname{deg} f=n$ with $2 d+1 \leq n<q^{d / 2}+1$, we have

$$
D(\alpha, d) \leq \frac{2 n}{d}\left(1+\frac{\log (n-1)-1}{d \log q-2 \log (n-1)}\right)+\frac{4 \log (n-1)+7}{d \log q-2 \log (n-1)}
$$

For $d=1$ the bound (1) is exactly the same as the bound of Wan [7, Theorem 3.3] which improves slightly the bound of Chung [1, Theorem 6]. For $d=1$, we set $\Delta(\alpha)=D(\alpha, 1)$. For a sufficiently large $q$, Katz [4, Theorem 1] has improved the results of Chung [1] and showed that $\Delta(\alpha) \leq n+2$, provided that $q \geq B(n)$ for some inexplicit function $B(n)$ of $n$. Furthermore, Cohen [2] shows that one can take $B(n)=(n(n+2)!)^{2}$ in the estimate of Katz 4].

We also use our idea in the case $d=1$ and obtain an improvement of (11) and thus of the bounds of Chung [1, Theorem 6] and Wan [7, Theorem 3.3].

Theorem 2. For a root $\alpha$ of an irreducible polynomial $f \in \mathbb{F}_{q}[X]$ of degree $\operatorname{deg} f=n$ with $3 \leq n<q^{1 / 2}+1$, we have

$$
\Delta(\alpha) \leq 2 n\left(1+\frac{\log (n-1)-1}{\log q-2 \log (n-1)}\right)+\frac{3 \log (n-1)+3}{\log q-2 \log (n-1)}
$$

We use the same idea for the proofs of Theorems 1 and 2, however the technical details are slightly different.

We also note that the additive constants 7 and 3 in the bounds of Theorems 1 and 2, respectively, can be replaced by a slightly smaller (but fractional values).

To compre the bound (1) with Theorems 11 and 2, we assume that $n=q^{(\vartheta+o(1)) d}$ for some fixed positive $\vartheta<1 / 2$.

The Theorems 1 and 2, imply that for any $d \geq 1$,

$$
D(\alpha, d) \leq\left(\frac{2-2 \vartheta}{1-2 \vartheta}+o(1)\right) \frac{n}{d}
$$

while (1) implies a weaker bound

$$
D(\alpha, d) \leq\left(\frac{2}{1-2 \vartheta}+o(1)\right) \frac{n}{d}
$$

## 2. Preparation

We define the polynomial analogue of the von Mangoldt function as follows. For $g \in \mathbb{F}_{q}[X]$ we define

$$
\Lambda(g)= \begin{cases}\operatorname{deg} h, & \text { if } g=h^{k} \text { for some irreducible } h \in \mathbb{F}_{q}[X] \\ 0, & \text { otherwise }\end{cases}
$$

Let $\mathcal{X}_{n}$ be the set of multiplicative characters of $\mathbb{F}_{q^{n}}$ and let $\mathcal{X}_{n}^{*}=$ $\mathcal{X}_{n} \backslash\left\{\chi_{0}\right\}$ be the set of non-principal characters; we appeal to [3] for a background on the basic properties of multiplicative characters, such as orthogonality.

For any $\chi \in \mathcal{X}_{n}$ we also define the character sum

$$
S_{\alpha, d}(\chi)=\sum_{g \in \mathcal{P}_{d}} \Lambda(g) \chi(g(\alpha)) .
$$

A simple combinatorial argument shows that for the principal character $\chi_{0}$ we have

$$
\begin{equation*}
S_{\alpha, d}\left(\chi_{0}\right)=\sum_{g \in \mathcal{P}_{d}} \Lambda(g)=q^{d} \tag{2}
\end{equation*}
$$

see, for example, [5, Corollary 3.21].
As in [6], we recall that by [7, Theorem 2.1] we have:
Lemma 3. For any $\chi \in \mathcal{X}_{n}^{*}$ we have

$$
\left|S_{\alpha, d}(\chi)\right| \leq(n-1) q^{d / 2}
$$

We also consider the set $\mathcal{I}_{d}$ of irreducible polynomials of degree $d$, that is,

$$
\mathcal{I}_{d}=\left\{h \in \mathbb{F}_{q}[X]: \operatorname{deg} h=d, h \in \mathbb{F}_{q}[X] \text { irreducible }\right\}
$$

and the sums

$$
T_{\alpha, d}(\chi)=\sum_{h \in \mathcal{I}_{d}} \chi(h(\alpha)) .
$$

Our new ingredient is the following bound "on average".
Lemma 4. Let $m=\lceil n / d\rceil-1$. Then

$$
\sum_{\chi \in \mathcal{X}_{n}}\left|T_{\alpha, d}(\chi)\right|^{2 m} \leq m!\left(q^{n}-1\right)\left(\# \mathcal{I}_{d}\right)^{m}
$$

Proof. Using the orthogonality of characters, we see that

$$
\sum_{\chi \in \mathcal{X}_{n}}\left|T_{\alpha, d}(\chi)\right|^{2 m}=\left(q^{n}-1\right) N
$$

where $N$ is the number of solutions to the equation

$$
h_{1}(\alpha) \ldots h_{m}(\alpha)=h_{m+1}(\alpha) \ldots h_{2 m}(\alpha)
$$

with some $h_{1}, \ldots, h_{2 m} \in \mathcal{I}_{d}$. Since $d m<n$ this implies the identity

$$
h_{1}(X) \ldots h_{m}(X)=h_{m+1}(X) \ldots h_{2 m}(X)
$$

in the ring of polynomials over $\mathbb{F}_{q}$. Thus, using the uniqueness of polynomial factorisation, we obtain

$$
W \leq m!\left(\# \mathcal{I}_{d}\right)^{m}
$$

which concludes the proof.
Finally, we recall the well-know formula (see, for example, [5, Theorem 3.25])

$$
\begin{equation*}
\# \mathcal{I}_{d}=\frac{1}{d} \sum_{s \mid d} \mu(s) q^{d / s}, \tag{3}
\end{equation*}
$$

where $\mu(s)$ is the Möbius function, that is,

$$
\mu(s)= \begin{cases}(-1)^{\nu} & \text { if } s \text { is a product } \nu \text { distinct primes } \\ 0 & \text { otherwise }\end{cases}
$$

## 3. Proof of Theorem 1

Let as before $m=\lceil n / d\rceil-1$. For an integer $k>2 m$ and $v \in \mathbb{F}_{q^{n}}^{*}$ we consider

$$
M_{k}(\alpha, d ; v)=\sum_{\substack{g_{1}, \ldots, g_{k-2 m} \in \mathcal{P}_{d} \\ g_{1}(\alpha) \ldots, \ldots g_{k-2 m}(\alpha) h_{1}(\alpha) \ldots, h_{2 m} \in \mathcal{I}_{d} \\ g_{1}(\alpha)=v}} \Lambda\left(g_{1}\right) \ldots \Lambda\left(g_{k-2 m}\right) .
$$

Clearly, if for some $k$ we have $M_{k}(\alpha, d ; v)>0$ for every $v \in \mathbb{F}_{q^{n}}^{*}$ then $D(\alpha, d) \leq k$.

We now closely follow the same path as in the proof of [6, Theorem 15]. In particular, using the orthogonality of characters we write

$$
\begin{aligned}
M_{k}(\alpha, d ; v)=\frac{1}{q^{n}-1} & \sum_{g_{1}, \ldots, g_{k-2 m} \in \mathcal{P}_{d}} \sum_{h_{1}, \ldots, h_{2 m} \in \mathcal{I}_{d}} \Lambda\left(g_{1}\right) \ldots \Lambda\left(g_{k-2 m}\right) \\
& \sum_{\chi \in \mathcal{X}_{n}} \chi\left(g_{1}(\alpha) \ldots g_{k-2 m}(\alpha) h_{1}(\alpha) \ldots h_{2 m}(\alpha) v^{-1}\right) .
\end{aligned}
$$

Changing the order of summation, separating the term corresponding to $\chi_{0}$, and recalling (2), we derive

$$
\begin{aligned}
& M_{k}(\alpha, d ; v)-\frac{q^{d(k-2 m)}\left(\# \mathcal{I}_{d}\right)^{2 m}}{q^{n}-1} \\
&=\frac{1}{q^{n}-1} \sum_{\chi \in \mathcal{X}_{n}^{*}} \chi\left(v^{-1}\right) S_{\alpha, d}(\chi)^{k-2 m} T_{\alpha, d}(\chi)^{2 m}
\end{aligned}
$$

Therefore

$$
\begin{aligned}
& \left|M_{k}(\alpha, d ; v)-\frac{q^{d(k-2 m)}\left(\# \mathcal{I}_{d}\right)^{2 m}}{q^{n}-1}\right| \\
& \quad \leq \frac{1}{q^{n}-1} \sum_{\chi \in \mathcal{X}_{n}^{*}}\left|S_{\alpha, d}(\chi)\right|^{k-2 m}\left|T_{\alpha, d}(\chi)\right|^{2 m} .
\end{aligned}
$$

Using Lemma 3 and then (after extending the summation over all $\chi \in$ $\mathcal{X}_{n}$ ) using Lemma 4, we derive

$$
\begin{align*}
\mid M_{k}(\alpha, d ; v)- & \left.\frac{q^{d(k-2 m)}\left(\# \mathcal{I}_{d}\right)^{2 m}}{q^{n}-1} \right\rvert\,  \tag{4}\\
& \leq m!(n-1)^{k-2 m} q^{d(k / 2-m)}\left(\# \mathcal{I}_{d}\right)^{m} .
\end{align*}
$$

Thus, if for some $v \in \mathbb{F}_{q^{n}}^{*}$ we have $M_{k}(\alpha, d ; v)=0$ then

$$
\frac{q^{d(k-2 m)}\left(\# \mathcal{I}_{d}\right)^{2 m}}{q^{n}-1} \leq m!(n-1)^{k-2 m} q^{d(k / 2-m)}\left(\# \mathcal{I}_{d}\right)^{m}
$$

or

$$
\begin{equation*}
\left(\frac{q^{d / 2}}{n-1}\right)^{k} \leq m!(n-1)^{-2 m}\left(q^{n}-1\right) q^{m}\left(\# \mathcal{I}_{d}\right)^{-m} \tag{5}
\end{equation*}
$$

Now, as in the proof of [6, Theorem 9] we note that

$$
\# \mathcal{I}_{d} \geq \frac{q^{d}}{d}-\frac{2 q^{d / 2}}{d}
$$

Hence (5) implies that

$$
\left(\frac{q^{d / 2}}{n-1}\right)^{k} \leq m!(n-1)^{-2 m} d^{m}\left(q^{n}-1\right)\left(1-2 q^{-d / 2}\right)^{-m}
$$

Note that since $n>2 d+1$, we have $m \geq 2$. Hence, by the Stirling inequality,

$$
\begin{equation*}
m!\leq \sqrt{2 \pi} m^{m+1 / 2} e^{-m+1 / 12 m} \leq \sqrt{2 \pi} m^{m+1 / 2} e^{-m+1 / 24} . \tag{6}
\end{equation*}
$$

Thus, using that $m \leq(n-1) / d$, we see that

$$
\begin{equation*}
m!d^{m} \leq \sqrt{2 \pi} m^{1 / 2}(n-1)^{m} e^{-m+1 / 24} \tag{7}
\end{equation*}
$$

Since $d \geq 2$ and $2 d+1 \leq n<q^{d / 2}+1$ we have $q^{d / 2}>4$. Thus $q^{d / 2} \geq 5$. Furthermore, since $m \leq(n-1) / 2<q^{d / 2} / 2$, we also have

$$
\begin{equation*}
\left(1-2 q^{-d / 2}\right)^{-m} \leq\left(1-2 q^{-d / 2}\right)^{-q^{d / 2} / 2} \leq(1-2 / 5)^{-5 / 2}<3.6 \tag{8}
\end{equation*}
$$

Hence, recalling that $m \leq(n-1) / d \leq(n-1) / 2$, we derive from (7) and (8) that

$$
\begin{aligned}
\left(\frac{q^{d / 2}}{n-1}\right)^{k} & <3.6 \sqrt{2 \pi} m^{1 / 2}(n-1)^{-m} q^{n} e^{-m+1 / 24} \\
& \leq \sqrt{\pi}(n-1)^{-m+1 / 2} q^{n} e^{-m+1 / 24} \\
& \leq \sqrt{\pi}(e(n-1))^{-m+1 / 2} q^{n} e^{-11 / 24}
\end{aligned}
$$

Since $m \geq(n-1) / d-1$, we conclude that

$$
m-\frac{1}{2} \geq \frac{n}{d}-2
$$

Therefore,

$$
(e(n-1))^{-m+1 / 2} \leq(e(n-1))^{-n / d+2}
$$

which finally implies

$$
\begin{aligned}
k & \leq 2 \frac{n \log q-(n / d-2)(1+\log (n-1))+\log (3 \cdot 6 \sqrt{\pi})-11 / 24}{d \log q-2 \log (n-1)} \\
& \leq 2 \frac{n \log q-(n / d-2)(1+\log (n-1))+1.4}{d \log q-2 \log (n-1)} \\
& =\frac{2 n}{d}\left(1+\frac{\log (n-1)-1}{d \log q-2 \log (n-1)}\right)+\frac{4 \log (n-1)+6.8}{d \log q-2 \log (n-1)}
\end{aligned}
$$

which concludes the proof.

## 4. Proof of Theorem 2

We now put $m=n-1$. Note that the set $\mathcal{P}_{1}$ is the set of $q$ linear polynomials $X+u, u \in \mathbb{F}_{q}$. For an integer $k>2 m$ and $v \in \mathbb{F}_{q^{n}}^{*}$ we consider

$$
N_{k}(\alpha ; v)=\sum_{\substack{u_{1}, \ldots, u_{k} \in \mathbb{F}_{q} \\\left(u_{1}+\alpha\right) \ldots\left(u_{k}+\alpha\right)=v}} 1
$$

Clearly, if for some $k$ we have $N_{k}(\alpha ; v)>0$ for every $v \in \mathbb{F}_{q^{n}}^{*}$ then $\Delta(\alpha) \leq k$.

Using the same argument as in the proof Theorem 1, we obtain the following analogue of (4)

$$
\left|N_{k}(\alpha ; v)-\frac{q^{k}}{q^{n}-1}\right| \leq m!(n-1)^{k-2 m} q^{k / 2}=(n-1)!(n-1)^{k-2 n+2} q^{k / 2}
$$

Thus if for some $v \in \mathbb{F}_{q^{n}}^{*}$ we have $N_{k}(\alpha ; v)=0$ then

$$
\begin{equation*}
\left(\frac{q^{1 / 2}}{n-1}\right)^{k} \leq(n-1)!(n-1)^{-2 n+2}\left(q^{n}-1\right) \tag{9}
\end{equation*}
$$

The inequality (9) together with the Stirling inequality (6) imply that, for $n \geq 3$,

$$
\left(\frac{q^{d / 2}}{n-1}\right)^{k} \leq \sqrt{2 \pi}(n-1)^{-n+3 / 2} q^{n} e^{-n+1+1 / 12(n-1)}
$$

Using the inequality

$$
\log \left(\sqrt{2 \pi} e^{1+1 / 12(n-1)}\right)=\frac{25}{24}+\frac{1}{2} \log (2 \pi) \leq 2
$$

that holds for $n \geq 3$, we obtain

$$
\begin{aligned}
k & \leq 2 \frac{n \log q-(n-3 / 2) \log (n-1)-n+2}{\log q-2 \log (n-1)} \\
& =2 n\left(1+\frac{\log (n-1)-1}{\log q-2 \log (n-1)}\right)+\frac{3 \log (n-1)+2}{\log q-2 \log (n-1)},
\end{aligned}
$$

and the result now follows.

## Acknowledgements

This work was finished during a very enjoyable stay of the author at the Max Planck Institute for Mathematics, Bonn. It was also supported in part by ARC grant DP140100118.

## References

[1] F. R. K. Chung, 'Diameters and eigenvalues', J. Amer. Math. Soc. 2 (1989), 187-196.
[2] S. D. Cohen, 'Polynomial factorization and an application to regular directed graphs', Finite Fields and Their Appl., 4 (1998), 316-346.
[3] H. Iwaniec and E. Kowalski, Analytic number theory, Amer. Math. Soc., Providence, RI, 2004.
[4] N. M. Katz, 'Factoring polynomials in finite fields: an application of Lang-Weil to a problem in graph theory', Math. Ann., 286 (1990), 625-637.
[5] R. Lidl and H. Niederreiter, Finite Fields, Cambridge Univ. Press, Cambridge, 1997.
[6] M. Lu, D. Wan, L.-P. Wang, X.-D. Zhang, 'Algebraic Cayley graphs over finite fields', Preprint, 2013, (available from http://arxiv.org/abs/1303.3449).
[7] D. Wan, 'Generators and irreducible polynomials over finite fields', Math. Comp., 66 (1997), 1195-1212.

Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia

E-mail address: igor.shparlinski@unsw.edu.au

