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 $P_d$ 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

$P_d = \{ g \in \mathbb{F}_q[X] : \deg g = d, \ g = h^k, \ h \in \mathbb{F}_q[X] \text{ monic and irreducible}, \ k = 1, 2, \ldots \}$.

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

$\mathcal{E}(\alpha, d) = \{ g(\alpha) : g \in P_d \}$.

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

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

as $d \to \infty$, 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 $u \to v$ exists if and only if $u/v \in \mathcal{E}(\alpha, d)$. These graphs are similar to those introduced by Chung [1] however a little sparser: they are $\#P_d$-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

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

(1)
Here we augment the argument of [6] with some new combinatorial and analytic considerations and improve the bound (1).

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 $\deg f = n$ with $2d + 1 \leq n < q^{d/2} + 1$, we have

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

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 (1) 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 $\deg f = n$ with $3 \leq n < q^{1/2} + 1$, we have

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

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 compare the bound (1) with Theorems 1 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

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

Let \( \mathcal{X}_n \) be the set of multiplicative characters of \( \mathbb{F}_{q^n} \) and let \( \mathcal{X}_n^* = \mathcal{X}_n \setminus \{\chi_0\} \) 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

\[
S_{\alpha,d}(\chi_0) = \sum_{g \in \mathcal{P}_d} \Lambda(g) = q^d,
\]

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

\[
|S_{\alpha,d}(\chi)| \leq (n - 1)q^{d/2}.
\]

We also consider the set \( \mathcal{I}_d \) of irreducible polynomials of degree \( d \), that is,

\[
\mathcal{I}_d = \{ h \in \mathbb{F}_q[X] : \deg h = d, \ h \in \mathbb{F}_q[X] \text{ irreducible} \},
\]

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

\[
\sum_{\chi \in \mathcal{X}_n} |T_{\alpha,d}(\chi)|^{2m} \leq m!(q^n - 1)(\#\mathcal{I}_d)^m.
\]

**Proof.** Using the orthogonality of characters, we see that

\[
\sum_{\chi \in \mathcal{X}_n} |T_{\alpha,d}(\chi)|^{2m} = (q^n - 1)N,
\]
where \( N \) is the number of solutions to the equation
\[
h_1(\alpha) \ldots h_m(\alpha) = h_{m+1}(\alpha) \ldots h_{2m}(\alpha),
\]
with some \( h_1, \ldots, h_{2m} \in \mathcal{I}_d \). Since \( dm < n \) this implies the identity
\[
h_1(X) \ldots h_m(X) = h_{m+1}(X) \ldots h_{2m}(X)
\]
in the ring of polynomials over \( \mathbb{F}_q \). Thus, using the uniqueness of polynomial factorisation, we obtain
\[
W \leq m!(\#\mathcal{I}_d)^m,
\]
which concludes the proof. \( \square \)

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

\[
\#\mathcal{I}_d = \frac{1}{d} \sum_{s|d} \mu(s)q^{d/s},
\]

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 \( \square \)

Let as before \( m = \lceil n/d \rceil - 1 \). For an integer \( k > 2m \) and \( v \in \mathbb{F}_q^* \), we consider
\[
M_k(\alpha, d; v) = \sum_{g_1, \ldots, g_{k-2m} \in \mathcal{P}_d} \sum_{h_1, \ldots, h_{2m} \in \mathcal{I}_d} \Lambda(g_1) \ldots \Lambda(g_{k-2m}).
\]
Clearly, if for some \( k \) we have \( M_k(\alpha, d; v) > 0 \) for every \( v \in \mathbb{F}_q^* \) 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
\[
M_k(\alpha, d; v) = \frac{1}{q^n - 1} \sum_{g_1, \ldots, g_{k-2m} \in \mathcal{P}_d} \sum_{h_1, \ldots, h_{2m} \in \mathcal{I}_d} \Lambda(g_1) \ldots \Lambda(g_{k-2m})
\]
\[
\sum_{\chi \in \chi_n} \chi(g_1(\alpha) \ldots g_{k-2m}(\alpha) h_1(\alpha) \ldots h_{2m}(\alpha)v^{-1}).
\]
Changing the order of summation, separating the term corresponding to $\chi_0$, and recalling (2), we derive

$$M_k(\alpha, d; v) = \frac{q^{d(k-2m)}(\#I_d)^{2m}}{q^n - 1} = \frac{1}{q^n - 1} \sum_{\chi \in X_n} \chi(v^{-1}) S_{\alpha,d}(\chi)^{k-2m} T_{\alpha,d}(\chi)^{2m}.$$ 

Therefore

$$\left| M_k(\alpha, d; v) - \frac{q^{d(k-2m)}(\#I_d)^{2m}}{q^n - 1} \right| \leq \frac{1}{q^n - 1} \sum_{\chi \in X_n} |S_{\alpha,d}(\chi)|^{k-2m} |T_{\alpha,d}(\chi)|^{2m}.$$ 

Using Lemma 3 and then (after extending the summation over all $\chi \in X_n$) using Lemma 4, we derive

$$\left| M_k(\alpha, d; v) - \frac{q^{d(k-2m)}(\#I_d)^{2m}}{q^n - 1} \right| \leq \frac{m^d}{(n-1)^{q^n-1}} q^{d(k/2-m)} (\#I_d)^m.$$ 

Thus, if for some $v \in F_q^*$ we have $M_k(\alpha, d; v) = 0$ then

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

or

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

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

$$\#I_d \geq \frac{q^d}{d} - \frac{2q^{d/2}}{d}.$$ 

Hence (5) implies that

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

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

$$m! \leq \sqrt{2\pi m}^{m+1/2} e^{-m+1/12m} \leq \sqrt{2\pi m}^{m+1/2} e^{-m+1/24}.$$ 

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

$$m! d^m \leq \sqrt{2\pi m}^{1/2} (n-1)^m e^{-m+1/24}.$$
Since \( d \geq 2 \) and \( 2d + 1 \leq n < q^{d/2} + 1 \) 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

\[
(1 - 2q^{-d/2})^{-m} \leq (1 - 2q^{-d/2})^{-q^{d/2}/2} \leq (1 - 2/5)^{-5/2} < 3.6.
\]

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

\[
\left( \frac{q^{d/2}}{n - 1} \right)^k < 3.6\sqrt{2\pi m^{1/2}(n - 1)^{-m} q^n e^{-m+1/24}}
\]

\[
\leq \sqrt{\pi (n - 1)^{-m+1/2} q^n e^{-m+1/24}}
\]

\[
\leq \sqrt{\pi (e(n - 1))^{-m+1/2} q^n e^{-11/24}}.
\]

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

\[
m - \frac{1}{2} > \frac{n}{d} - 2.
\]

Therefore,

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

which finally implies

\[
k \leq 2 \frac{n \log q - (n/d - 2)(1 + \log(n - 1)) + \log(3.6\sqrt{\pi}) - 11/24}{d \log q - 2 \log(n - 1)}
\]

\[
\leq 2 \frac{n \log q - (n/d - 2)(1 + \log(n - 1)) + 1.4}{d \log q - 2 \log(n - 1)}
\]

\[
= \frac{2n}{d} \left( 1 + \frac{\log(n - 1) - 1}{d \log q - 2 \log(n - 1)} \right) + \frac{4 \log(n - 1) + 6.8}{d \log q - 2 \log(n - 1)},
\]

which concludes the proof.

### 4. Proof of Theorem 2

We now put \( m = n - 1 \). Note that the set \( P_1 \) is the set of \( q \) linear polynomials \( X + u, u \in \mathbb{F}_q \). For an integer \( k > 2m \) and \( v \in \mathbb{F}_q^* \), we consider

\[
N_k(\alpha; v) = \sum_{u_1 + \ldots + u_k = v} 1.
\]

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

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

\[
\left| N_k(\alpha; v) - \frac{q^k}{q^n - 1} \right| \leq m!(n - 1)^{k-2m} q^{k/2} = (n - 1)! (n - 1)^{k-2n+2} q^{k/2}.
\]
Thus if for some \( v \in \mathbb{F}_q^n \) we have \( N_k(\alpha; v) = 0 \) then

\[
\left( \frac{q^{1/2}}{n-1} \right)^k \leq (n-1)!(n-1)^{-2n+2}(q^n - 1).
\]

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

\[
\left( \frac{q^{d/2}}{n-1} \right)^k \leq \sqrt{2\pi}(n-1)^{-n+3/2}q^ne^{-n+1+1/12(n-1)}.
\]

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

\[
k \leq 2n \log q - (n - 3/2) \log(n-1) - n + 2
\]

\[
= 2n \left( 1 + \frac{\log(n-1) - 1}{\log q - 2\log(n-1)} \right) + \frac{3\log(n-1) + 2}{\log q - 2\log(n-1)},
\]

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