NUMBER THEORETIC DESIGNS FOR DIRECTED REGULAR GRAPHS OF SMALL DIAMETER[*]

WILLIAM D. BANKS[†], ALESSANDRO CONFLITTI[‡], AND IGOR E. SHPARLINSKI[§]

Abstract. In 1989, F. R. K. Chung gave a construction for certain directed h-regular graphs of small diameter. Her construction is based on finite fields, and the upper bound on the diameter of these graphs is derived from bounds for certain very short character sums. Here we present two similar constructions that are based on properties of discrete logarithms and exponential functions in residue rings modulo a prime power. Accordingly, we use bounds for certain sums with additive and multiplicative characters to estimate the diameter of our graphs. We also give a third construction that avoids the use of bounds for exponential sums.

Key words. exponential sums, character sums, extremal problems, graphs

AMS subject classifications. 05C35, 11L07, 11L40

DOI. 10.1137/S0895480101396676

1. Introduction. We recall that, in a directed graph G, the distance between two vertices is defined to be the length of the shortest directed path joining them, and the diameter $D(G)$ of G is defined to be the maximum distance over all possible pairs of vertices.

We say the a directed graph G is *h-regular* if the in-degree and the out-degree at every node is equal to h.

In many applications, such as in the design of communication networks, it is required that the underlying h-regular graphs have sufficiently many nodes, and it is desirable not only to keep h as small as possible (in order to reduce the complexity of the network), but also to minimize the diameter (so that information can be transmitted efficiently).

In [2], a construction of graphs with the above properties is proposed using finite fields of the form $\mathbb{F}_{q^n}$. Namely, for any prime q and any integer $n \geq 2$ with $q > (n-1)^2$, the construction produces q-regular graphs $G(q, n)$ with $q^n - 1$ nodes and with diameter

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

In [11], a more flexible construction has been proposed that produces h-regular graphs for any $h \geq q^{1/2+\varepsilon}$, $\varepsilon > 0$.

The inequality (1) of [2] is based on bounds for very short character sums considered in [1, 7], while the result of [11] is based on bounds for even shorter sums in [10]. All of these estimates are derived from the celebrated Weil bound.

There are several other similar constructions and bounds for character sums; see [3, 9]. An alternative approach to bounding the diameter of $G(q, n)$, which in

some cases gives improved estimates, is described in [4, 5]. This method makes use of the Weil bound in a more direct way, but it applies only when q is extremely large relative to n.

In this paper, we show that similar constructions can be applied to the design of directed h-regular graphs with small diameter over the residue ring $\mathbb{Z}_{p^n}$, where p is an odd prime. One construction is an exact analogue of the construction of [2]. The other is an additive variant whose analogue over finite fields does not seem possible owing to a general lack of good bounds for short sums of additive characters with exponential functions. We also give a third construction, again over $\mathbb{Z}_{p^n}$, which has small diameter and small regularity for certain choices of the parameters. Our estimates for this last construction do not depend on bounds for exponential sums.

For any integer h, we denote by S_h the set consisting of the first h positive integers that are not divisible by p. In our first design (the multiplicative case), we specify vertices of our graph by elements of $\mathbb{Z}_{p^n}^*$, and then we select an integer h and connect vertices $u \to v$ if and only if $uv^{-1} \in S_h$. We denote the corresponding graph by $\mathcal{G}_\times(h, p, n)$.

Next, let ϑ be a fixed primitive root modulo p^n. For every element $a \in \mathbb{Z}_{p^n}^*$, we can define the discrete logarithm $\operatorname{ind} a$ uniquely by the conditions

$$\vartheta^{\operatorname{ind} a} \equiv a \pmod{p^n}, \qquad 0 \le \operatorname{ind} a < (p-1)p^{n-1}.$$

In our second design (the additive case), we specify vertices of our graph by elements of $\mathbb{Z}_{p^n}$ and connect vertices $u \to v$ if and only if $u - v \in \mathbb{Z}_{p^n}^*$ and $\operatorname{ind}(u - v) \in [1, h]$. We denote the corresponding graph by $\mathcal{G}_+(h, p, n)$

In our third design, we specify the vertices of our graph by elements of $\mathbb{Z}_m$, where m is any integer greater than 1, and connect vertices $u \to v$ if and only if the integer $u - v$, reduced modulo m, has precisely one nonzero digit when written in base g. We denote the corresponding graph by $\overline{\mathcal{G}}(m, g)$. For a wide range of parameters, these graphs have a smaller diameter than the corresponding graphs from [2] with the same number of nodes and the same regularity.

Throughout the paper, $\log z$ denotes the natural logarithm of z. For any integer m, we denote by $\mathbf{e}_m$ the additive character $\mathbf{e}_m(z) = \exp(2\pi i z/m)$. Constants in the "$O$" symbol depend only on p.

2. Preparations. Let X be the set of $(p-1)p^{n-1}$ multiplicative characters modulo p^n, and let $X^* \subset X$ be the subset of all nonprincipal characters.

We need the following well-known statements.

LEMMA 1. *For any $z \in \mathbb{Z}_{p^n}^*$,*

$$\sum_{\chi \in X} \chi(z) = \begin{cases} (p-1)p^{n-1} & \text{if } z = 1, \\ 0 & \text{otherwise.} \end{cases}$$

LEMMA 2. *For any $z \in \mathbb{Z}_{p^n}$,*

$$\sum_{a=0}^{p^n - 1} \mathbf{e}_{p^n}(az) = \begin{cases} p^n & \text{if } z = 0, \\ 0 & \text{otherwise.} \end{cases}$$

As we have already mentioned, our results are based on bounds for short character sums. The first one is essentially Exercise 8 in Chapter 9 of [6] (note that the largest element of S_h is $hp/(p-1) + O(1)$).

LEMMA 3. *Let $p \geq 3$ be a fixed prime number and let $\chi \in X^*$. For any integer h, $p^2 \leq h \leq (p-1)p^{n-1}$, we define $r = n \log p / \log h$ so that $h^r = p^n$. Then the bound*

$$\left| \sum_{x \in S_h} \chi(x) \right| = O\left(h^{1 - \alpha/r^2} \right)$$

holds for some absolute constant $\alpha > 0$.

Our second result is a combination of Lemma 2 (for $r \leq 3/2$) and Theorem 4 (for $r > 3/2$) of [8].

LEMMA 4. *Let $p \geq 3$ be a fixed prime number, let ϑ be a primitive root modulo p^n, and suppose that $\gcd(a, p) = 1$. For any integer h, $2 \leq h \leq (p-1)p^{n-1}$, let $r = n \log p / \log h$ as before. Then the bound*

$$\left| \sum_{x=1}^{h} \mathbf{e}_{p^n}(a\vartheta^x) \right| = O\left(h^{1 - \beta/r^2} \right)$$

holds for some absolute constant $\beta > 0$.

LEMMA 5. *Let $p \geq 3$ be a fixed prime number, let ϑ be a primitive root modulo p^k, and suppose that $\gcd(a, p) = 1$. Then*

$$\sum_{x=1}^{(p-1)p^{k-1}} \mathbf{e}_{p^k}(a\vartheta^x) = \begin{cases} -1 & \text{if } k = 1, \\ 0 & \text{if } k \geq 2. \end{cases}$$

Proof. We have

$$\sum_{x=1}^{(p-1)p^{k-1}} \mathbf{e}_{p^k}(a\vartheta^x) = \sum_{x \in \mathbb{Z}_{p^k}^*} \mathbf{e}_{p^k}(ax) = \sum_{x=1}^{p^k} \mathbf{e}_{p^k}(ax) - \sum_{x=1}^{p^{k-1}} \mathbf{e}_{p^k}(apx),$$

and the result follows from Lemma 2. □

3. Main results. We can now prove our main results.

THEOREM 6. *Let $p \geq 3$ be a fixed prime number. For any integer h in the range $p^2 \leq h < (p-1)p^{n-1}$, let $r = n \log p / \log h$. Then the bound*

$$D\left(\mathcal{G}_\times(h, p, n) \right) = O(r^3)$$

holds, provided that $r = o(n^{1/3})$.

Proof. Two vertices $u, v \in \mathbb{Z}_{p^n}^*$ are connected by a path of the form

$$u = w_0 \to w_1 \to \cdots \to w_d = v$$

if and only if

$$x_{i+1} = w_i / w_{i+1} \in S_h, \qquad 0 \leq i \leq d - 1.$$

Thus, u is connected to v along such a path if only if there exist integers $x_1, \dots, x_d \in S_h$ such that

$$v = u \prod_{j=1}^{d} x_j.$$

Therefore, to show that $D\left(\mathcal{G}_\times(h,p,n)\right) \leq d$, it suffices to prove that every element $w \in \mathbb{Z}_{p^n}^*$ can be represented in the form

$$(2) \qquad w = \prod_{j=1}^{d} x_j, \qquad x_1, \ldots, x_d \in S_h.$$

By Lemma 1, the number T of solutions to (2) is given by

$$T = \frac{1}{(p-1)p^{n-1}} \sum_{x_1,\ldots,x_d \in S_h} \sum_{\chi \in X} \chi\left(w^{-1} \prod_{k=1}^{d} x_k\right);$$

hence it is enough to show that $T > 0$ for every choice of w. Now, pulling off the contribution from the principal character, we have

$$T = \frac{h^d}{(p-1)p^{n-1}} + \frac{1}{(p-1)p^{n-1}} \sum_{\chi \in X^*} \chi(w^{-1}) \left(\sum_{x \in S_h} \chi(x)\right)^d.$$

By Lemma 3, we see that for some constant $C > 0$ (depending only on p),

$$\left| T - \frac{h^d}{(p-1)p^{n-1}} \right| < C^d h^{d - \alpha d/r^2} = C^d h^d p^{-\alpha n d/r^3};$$

hence T will be positive if

$$C^d p^{-\alpha n d/r^3} < \frac{1}{(p-1)p^{n-1}}.$$

This we can ensure by choosing

$$d = \left\lfloor \frac{r^3 \log p}{\alpha \log p - n^{-1} r^3 \log C} \right\rfloor + 1.$$

Consequently, if $r = o(n^{1/3})$ as $n \to \infty$, it follows that the diameter of $\mathcal{G}_\times(h,p,n)$ will be less than $2\alpha^{-1} r^3$ for sufficiently large n. □

THEOREM 7. *Let $p \geq 3$ be a fixed prime number. For any integer h in the range $2 \leq h < (p-1)p^{n-1}$, let $r = n \log p / \log h$. Then the bound*

$$D\left(\mathcal{G}_+(h,p,n)\right) = O(r^3)$$

holds, provided that $r = o(n^{1/3})$.

Proof. Two vertices $u, v \in \mathbb{Z}_{p^n}$ are connected by a path

$$u = w_0 \to w_1 \to \cdots \to w_d = v$$

if and only if $w_i - w_{i+1} \in \mathbb{Z}_{p^n}^*$, $0 \leq i \leq d - 1$, and

$$x_{i+1} = \mathrm{ind}(w_i - w_{i+1}) \in [1, h], \qquad 0 \leq i \leq d - 1.$$

Thus, u is connected to v along such a path if only if there exist integers $x_1, \ldots, x_d \in [1, h]$ such that

$$u = v + \sum_{j=1}^{d} \vartheta^{x_j}.$$

To show that $D\left(\mathcal{G}_+(h,p,n)\right) \leq d$, it suffices to prove that every element $w \in \mathbb{Z}_{p^n}$ can be represented in the form

$$(3) \qquad w = \sum_{j=1}^{d} \vartheta^{x_j}, \qquad x_1,\ldots,x_d \in [1,h].$$

By Lemma 2, the number T of solutions to (3) is given by

$$T = \frac{1}{p^n} \sum_{x_1,\ldots,x_d \in [1,h]} \sum_{b=0}^{p^n-1} \mathbf{e}_{p^n}\left(-bw + b\sum_{j=1}^{d} \vartheta^{x_j}\right)$$

$$= \frac{1}{p^n} \sum_{b=0}^{p^n-1} \mathbf{e}_{p^n}(-bw)\left(\sum_{x\in[1,h]} \mathbf{e}_{p^n}(b\vartheta^x)\right)^d$$

$$= \frac{h^d}{p^n} + \frac{1}{p^n} \sum_{b=1}^{p^n-1} \mathbf{e}_{p^n}(-bw)\left(\sum_{x\in[1,h]} \mathbf{e}_{p^n}(b\vartheta^x)\right)^d.$$

To show that $T > 0$, it suffices to show that the summation on the right is less than h^d in absolute value. To do this, we collect terms with $\gcd(b,p^n) = p^{n-k}$, $k = 1,\ldots,n$, which gives

$$\left|\sum_{b=1}^{p^n-1} \mathbf{e}_{p^n}(-bw)\left(\sum_{x\in[1,h]} \mathbf{e}_{p^n}(b\vartheta^x)\right)^d\right| \leq \sum_{k=1}^{n} \sum_{\substack{b=1 \\ \gcd(b,p^n)=p^{n-k}}}^{p^n-1} \left|\sum_{x\in[1,h]} \mathbf{e}_{p^n}(b\vartheta^x)\right|^d$$

$$= \sum_{k=1}^{n} \sum_{\substack{a=1 \\ \gcd(a,p)=1}}^{p^k-1} \left|\sum_{x\in[1,h]} \mathbf{e}_{p^k}(a\vartheta^x)\right|^d.$$

For $p^{k-1}(p-1) \geq h$, we apply Lemma 4 directly to obtain

$$\left|\sum_{x\in[1,h]} \mathbf{e}_{p^k}(a\vartheta^x)\right| \ll h^{1-\beta\log^2 h/k^2\log^2 p} \leq h^{1-\beta\log^2 h/n^2\log^2 p} = hp^{-\beta n/r^3}.$$

For $p^{k-1}(p-1) < h$, write h in the form $h = p^{k-1}(p-1)i + j$ with $i \geq 1$ and $0 \leq j \leq p^{k-1}(p-1) - 1$. If $k \geq 2$, then we use Lemma 5 together with Lemma 4 to derive

$$\left|\sum_{x\in[1,h]} \mathbf{e}_{p^k}(a\vartheta^x)\right| = \left|\sum_{\nu=0}^{i-1} \sum_{x=\nu p^{k-1}(p-1)+1}^{(\nu+1)p^{k-1}(p-1)} \mathbf{e}_{p^k}(a\vartheta^x) + \sum_{x=ip^{k-1}(p-1)+1}^{p^{k-1}(p-1)i+j} \mathbf{e}_{p^k}(a\vartheta^x)\right|$$

$$= \left|\sum_{x=1}^{j} \mathbf{e}_{p^k}(a\vartheta^x)\right| \ll j^{1-\beta\log^2 j/k^2\log^2 p}$$

$$\ll h^{1-\beta\log^2 h/n^2\log^2 p} \ll hp^{-\beta n/r^3}.$$

For $k = 1$, using Lemma 5, we obtain

$$\left| \sum_{x \in [1,h]} \mathbf{e}_p(a\vartheta^x) \right| = \left| \sum_{\nu=0}^{i-1} \sum_{x=\nu(p-1)+1}^{(\nu+1)(p-1)} \mathbf{e}_p(a\vartheta^x) + \sum_{x=i(p-1)+1}^{(p-1)i+j} \mathbf{e}_p(a\vartheta^x) \right|$$

$$\leq i + j < h/(p-1) + p \leq 2h/p,$$

provided that h is sufficiently large. Consequently, for some constant $C > 0$ (depending only on p), we have

$$\sum_{k=1}^{n} \sum_{\substack{a=1 \\ \gcd(a,p)=1}}^{p^k-1} \left| \sum_{x \in [1,h]} \mathbf{e}_{p^k}(a\vartheta^x) \right|^d < (p-1)(2h/p)^d + C^d h^d p^{n-\beta nd/r^3}$$

$$< 2(2h/3)^d + C^d h^d p^{n-\beta nd/r^3},$$

$$< \frac{h^d}{2} + C^d h^d p^{n-\beta nd/r^3},$$

provided that $d \geq 4$ and h is sufficiently large. Hence, T will be positive for large values of h if $d \geq 4$, and

$$C^d h^d p^{n-\beta nd/r^3} < \frac{h^d}{2},$$

which we can ensure by choosing

$$d = \left\lfloor \frac{r^3 \log p + n^{-1} r^3 \log 2}{\beta \log p - n^{-1} r^3 \log C} \right\rfloor + 4.$$

Consequently, if $r = o(n^{1/3})$ as $n \to \infty$, it follows that the diameter of $\mathcal{G}_+(h,p,n)$ will be less than $2\beta^{-1}r^3$ for sufficiently large n. □

THEOREM 8. *For any integer $m \geq 2$ and any base $g \geq 2$, $\overline{\mathcal{G}}(m,g)$ is regular of degree $h = (g-1)K$ and diameter $D\left(\overline{\mathcal{G}}(m,g)\right) = K$, where*

$$K = \left\lfloor \frac{\log(m-1)}{\log g} \right\rfloor + 1.$$

Proof. Two vertices $u, v \in \mathbb{Z}_m$ are connected by a path

$$u = w_0 \to w_1 \to \cdots \to w_d = v$$

if and only if $w_i - w_{i+1}$, reduced modulo m, has at most one nonzero digit when written in base g; that is, $w_i - w_{i+1} \equiv ag^j \pmod{m}$ with $1 \leq a \leq g-1$ and $0 \leq j \leq K-1$. Since every element $w \in \mathbb{Z}_m$ can be expressed in the form

$$w = \sum_{j=0}^{K-1} a_j g^j,$$

the diameter of $\overline{\mathcal{G}}(m,g)$ is $d = K$. Since every node u is connected only to elements of the form $u + ag^j$, we also see that $\overline{\mathcal{G}}(m,g)$ is regular of degree $h = (g-1)K$. □

In particular, taking m equal to a power q^n, if $g = \lfloor q^{1/2} \rfloor + 1$ and $q \geq (2n+1)^2$, then $h \leq q$ and $D\left(\overline{\mathcal{G}}(q^n, g)\right) \leq 2n+1$, which is stronger than the bound (1) implies for the graphs constructed in [2]. Moreover, one sees that for any $\varepsilon \geq 0$, there exists $A > 0$ such that for $g = \lfloor q^{2/(2+\varepsilon)} \rfloor + 1$, $q > n^A$, and sufficiently large n, our graphs have q^n nodes of degree $h < q$ and diameter at most $(1+\varepsilon)n$. Indeed, taking $A = 1 + 3/\varepsilon$, for these parameters we obtain $K \leq (1 + \varepsilon/2)n + 1 \leq (1+\varepsilon)n < q^{\varepsilon/(2+\varepsilon)}$, provided that n is large enough.

We also note that the graphs $\overline{\mathcal{G}}(m, g)$ have an obvious algorithm for finding the shortest path between two nodes using only $O(K)$ arithmetic operations in $\mathbb{Z}_m$.

REFERENCES

[1] L. Carlitz, *Distribution of primitive roots in a finite field*, Quart. J. Math., Oxford Ser. (2), 4 (1953), pp. 4–10.
[2] F. R. K. Chung, *Diameters and eigenvalues*, J. Amer. Math. Soc., 2 (1989), pp. 187–196.
[3] F. R. K. Chung, *Spectral Graph Theory*, CBMS Reg. Conf. Ser. Math. 92, AMS, Providence, RI, 1997.
[4] S. D. Cohen, *Polynomial factorization, graphs, designs and codes*, in Finite Fields: Theory, Applications, and Algorithms, Contemp. Math. 168, AMS, Providence, RI, 1994, pp. 23–32.
[5] S. D. Cohen, *Polynomial factorization and an application to regular directed graphs*, Finite Fields Appl., 4 (1998), pp. 316–346.
[6] A. A. Karatsuba, *Basic Analytic Number Theory*, Springer-Verlag, Berlin, 1993.
[7] N. M. Katz, *An estimate for character sums*, J. Amer. Math. Soc., 2 (1989), pp. 197–200.
[8] N. M. Korobov, *On the distribution of digits in periodic fractions*, Mat. Sb. (N.S.), 89 (1972), pp. 654–670 (in Russian).
[9] W. W.-C. Li, *Number Theory with Applications*, World Scientific, Singapore, 1996.
[10] G. I. Perel'muter and I. E. Shparlinski, *Distribution of primitive roots in finite fields*, Uspekhi Mat. Nauk, 45 (1990), pp. 185–186 (in Russian).
[11] I. E. Shparlinski, *On parameters of some graphs from finite fields*, European J. Combin., 14 (1993), pp. 589–591.