Discrete Mathematics 340 (2017) 2432–2436

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Note

Large butterfly Cayley graphs and digraphs

David Bevan

Department of Computer and Information Sciences, University of Strathclyde, Glasgow, Scotland G1 1XH, United Kingdom

ARTICLE INFO

Article history:
Received 31 July 2015
Received in revised form 25 May 2017
Accepted 29 May 2017

Keywords:
Cayley graph
Degree-diameter problem
Butterfly network

ABSTRACT

We present families of large undirected and directed Cayley graphs whose construction is related to butterfly networks. One approach yields, for every large k and for values of d taken from a large interval, the largest known Cayley graphs and digraphs of diameter k and degree d. Another method yields, for sufficiently large k and infinitely many values of d, Cayley graphs and digraphs of diameter k and degree d whose order is exponentially larger in k than any previously constructed. In the directed case, these are within a linear factor in k of the Moore bound.

1. Introduction

The goal of the *degree-diameter problem* is to determine the largest possible order of a graph or digraph, perhaps restricted to some special class, with given maximum (out)degree and diameter. For an overview of progress on a wide variety of approaches to this problem, see the survey by Miller & Širáň [6].

Our concern here is with large *Cayley* graphs and digraphs. Recall that, for a group G and a unit-free generating subset S of G, the *Cayley digraph* of G generated by S has vertex set G and a directed edge from g to gs for all $g \in G$ and $s \in S$. If S is symmetric, i.e. $S = S^{-1}$, then the corresponding undirected simple graph is the *Cayley graph* of G generated by S. The Cayley (di)graph is thus regular of (out)degree $|S|$ and vertex-transitive.

We are interested in graphs and digraphs of degree d and diameter k, for arbitrary large k and varying d. If a construction yields graphs of order $n_{d,k}$, we say that it has *asymptotic order* $f(d, k)$ if, for fixed k,

$$\lim_{d\to\infty} \frac{n_{d,k}}{f(d,k)} = 1.$$

No graph or digraph can be larger than the corresponding *Moore bound*. For undirected graphs, this bound is $\mathrm{M}_{d,k} = 1 + \frac{d}{d-2}\big((d-1)^k - 1\big)$ if $d > 2$. In the directed case, it is $\mathrm{DM}_{d,k} = \frac{1}{d-1}\big(d^{k+1} - 1\big)$ if $d > 1$. In both cases, the Moore bound has asymptotic order d^k.

Previously, for arbitrary degree and diameter, the largest known directed Cayley graphs were obtained by Vetrík [7] and Abas & Vetrík [1], whose constructions have asymptotic order $k\big(\frac{d}{2}\big)^k$ for even k, and $2k\big(\frac{d}{2}\big)^k$ for odd k. Our construction yields Cayley digraphs whose order is asymptotically $(k-1)d^{k-1}$. For fixed diameter $k \geqslant 8$, these digraphs are larger than those in [7] and [1] for every value of d in a large interval. We also construct, for fixed k and infinitely many values of d, Cayley digraphs whose asymptotic order exceeds $\frac{d^k}{e^2 k}$, a factor of $\frac{2^{k-1}}{e^2 k^2}$ larger than those of Abas & Vetrík, and within a linear factor in k of the Moore bound.

The undirected case is similar. Previously, the largest known Cayley graphs were obtained by Macbeth, Šiagiová, Širáň & Vetrík [5], whose construction has asymptotic order $k\big(\frac{d}{3}\big)^k$. For $d - k \not\equiv 3 \pmod 4$, we construct Cayley graphs whose order

E-mail address: david.bevan@strath.ac.uk.

http://dx.doi.org/10.1016/j.disc.2017.05.012

is asymptotically $(k-1)\left(\frac{d}{2}\right)^{k-1}$. For sufficiently large diameter k, these graphs are larger than those in [5] for every suitable value of d in a large interval. We also construct, for given k and infinitely many values of d, Cayley graphs whose asymptotic order is at least $\frac{1}{e^2k}\left(\frac{d}{2}\right)^k$, a factor of $\frac{1}{e^2k^2}\left(\frac{3}{2}\right)^k$ larger than those in [5].

Our constructions are based on a two-parameter family of groups. For $t \geqslant 2$, let $\mathbb{Z}_t = \mathbb{Z}/t\mathbb{Z}$ be the additive group of integers modulo t, and for $r \geqslant 2$, let $\mathbb{Z}_t^r$ denote the product $\mathbb{Z}_t \times \cdots \times \mathbb{Z}_t$, where $\mathbb{Z}_t$ occurs r times, considered as an additive group of vectors. Let α be the automorphism of $\mathbb{Z}_t^r$, defined by $\alpha(v_0, \ldots, v_{r-1}) = (v_{r-1}, v_0, \ldots, v_{r-2})$, that cyclically shifts coordinates rightwards by one, and consider the semidirect product $G = \mathbb{Z}_t^r \rtimes \mathbb{Z}_r$, of order rt^r, with the group operation given by $(u, s)\cdot(v, s') = (u + \alpha^s(v), s + s')$, for $u, v \in \mathbb{Z}_t^r$ and $s, s' \in \mathbb{Z}_r$. We write elements of G in the form $(v_0, \ldots, v_{r-1}; s)$, where each $v_i \in \mathbb{Z}_t$ and $s \in \mathbb{Z}_r$. Using this notation, the group operation is

$$(u_0, \ldots, u_{r-1};\ s)\cdot(v_0, \ldots, v_{r-1};\ s') = (u_0 + v_{r-s},\ \ldots,\ u_{s-1} + v_{r-1},\ u_s + v_0,\ \ldots,\ u_{r-1} + v_{r-1-s};\ s + s'),$$

arithmetic in the subscripts being performed modulo r. The group G is used to create all our Cayley graphs and digraphs.

The Cayley digraph generated by elements of G of the form $(a, 0, \ldots, 0; 1)$, $a \in \mathbb{Z}_t$ is isomorphic to the base-t order-r (wrapped) *butterfly network*, $B_t(r)$, so called because it is composed of rt^{r-1} edge-disjoint *t-butterflies* (copies of the complete bipartite graph $K_{t,t}$); see [2, Figure 2]. Butterfly networks are closely related to the *de Bruijn graphs* [3], the directed base-t order-r de Bruijn graph being a coset graph of $B_t(r)$ [2, Theorem 4.4].

Cayley graphs and digraphs of G were used previously by Macbeth, Šiagiová, Širáň & Vetrík [5] and Vetrík [7] in the constructions mentioned above, though in neither case is the connection to the butterfly networks made explicit. Each of our results is a consequence of choosing an appropriate set of generators for G. We make use of two distinct constructions.

2. The first construction

We present the directed case first, since it is slightly simpler.

Theorem 1. *For any $k \geqslant 4$ and $d \geqslant k-1$, there exist Cayley digraphs that have diameter k, outdegree d, and order $(k-1)(d-k+3)^{k-1}$.*

Proof. Let $r = k-1$ and $t = d-k+3$, and let the underlying group of the Cayley digraph be $G = \mathbb{Z}_t^r \rtimes \mathbb{Z}_r$. The order of G is $rt^r = (k-1)(d-k+3)^{k-1}$.

To generate the Cayley digraph we use the t *shift and add* elements $(a, 0, \ldots, 0; 1)$, for each $a \in \mathbb{Z}_t$, together with the remaining $r-2$ nonzero *cyclic shift* elements $(0, \ldots, 0; s)$, for $2 \leqslant s \leqslant r-1$. Thus the digraph has outdegree $t + r - 2 = d$.

It also has diameter $r + 1 = k$. Every element is the product of r shift and add operations (establishing the vector) and possibly a single cyclic shift (to establish the final shift value if it is nonzero). On the other hand, if $s \neq 0$ then $(1, \ldots, 1; s)$ cannot be obtained as a product of fewer than k generators. □

Clearly, the butterfly network $B_t(r)$ is a subdigraph of the Cayley digraph of Theorem 1. The additional edges in our construction, corresponding to the cyclic shift elements, consist of t^r vertex-disjoint copies of the complete digraph on r vertices with a directed r-cycle removed.

Vetrík [7] presents, for any $k \geqslant 3$ and $d \geqslant 4$, a family of Cayley digraphs of diameter k, degree d, and order $k\lfloor \frac{d}{2} \rfloor^k$. For odd diameters, Abas & Vetrík [1] improve this result by a factor of two, constructing Cayley digraphs of diameter at most k and degree d of order $2k\lfloor \frac{d}{2} \rfloor^k$. Clearly, for large enough d, these digraphs are bigger than those of Theorem 1. However, for any given diameter $k \geqslant 8$, it can be confirmed (using a computer algebra system, or otherwise) that the digraphs of Theorem 1 are larger than those of Vetrík and Abas & Vetrík if

$$2k + 2\ln k \quad < \quad d \quad < \quad 2^{k-1}\left(1 - \tfrac{1}{k}\right) - k^2.$$

For specific values of the degree, we can do much better. If we set $d = k^2 - 3k$, then the digraphs of Theorem 1 have orders at least $\mathrm{DM}_{d,k}/ek$, within a linear factor of the Moore bound, and exceeding those of Abas & Vetrík by a factor of at least $2^{k-1}/ek^2$, which exceeds 1 for $k \geqslant 9$.

For the undirected case, we simply add elements to the generating set to make it symmetric.

Theorem 2. *For any $k \geqslant 5$ and $d \geqslant k$ such that $d - k \not\equiv 3 \pmod 4$, there exist Cayley graphs that have diameter k, degree d, and order $(k-1)\left(\lfloor \frac{d-k}{2} \rfloor + 2\right)^{k-1}$.*

Proof. Let $r = k-1$ and $t = \lfloor \frac{d-k}{2} \rfloor + 2$, and let $G = \mathbb{Z}_t^r \rtimes \mathbb{Z}_r$. As generators for the Cayley graph of G we use the t elements $(a, 0, \ldots, 0; 1)$, along with their inverses $(0, \ldots, 0, -a; -1)$, and the remaining $r-3$ nonzero elements $(0, \ldots, 0; s)$ for $2 \leqslant s \leqslant r-2$. In addition, if $d - k \equiv 1 \pmod 4$, in which case t is even, then the involution $(0, \ldots, 0, \frac{t}{2}; 0)$ is also included as a generator.

Thus the graph has degree $2t + r - 3 + (d - k \bmod 2) = d$. As in the directed case, it has diameter $r + 1 = k$. Every element is the product of $k-1$ shift and add operations and possibly a single cyclic shift. On the other hand, if $s \notin \{-1, 0, 1\}$ then $(1, \ldots, 1; s)$ cannot be obtained as a product of fewer than k generators, and G has such an element since $r \geqslant 4$. □