Bevan, David (2017) Large butterfly Cayley graphs and digraphs. Discrete Mathematics, 340 (10). pp. 2432-2436. ISSN 0012-365X , http://dx.doi.org/10.1016/j.disc.2017.05.012

Large butterfly Cayley graphs and digraphs

David Bevan[†]

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 $M_{d,k} = 1 + \frac{d}{d-2}\big((d-1)^k - 1\big)$ if $d > 2$. In the directed case, it is $DM_{d,k} = \frac{1}{d-1}\big(d^{k+1} - 1\big)$ if $d > 1$. In both cases, the Moore bound has asymptotic order d^k.

[†]Department of Computer and Information Sciences, University of Strathclyde, Glasgow, Scotland.
2010 Mathematics Subject Classification: 05C25, 05C20, 05C35.

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 $k\left(\frac{d}{2}\right)^k$ for even k, and $2k\left(\frac{d}{2}\right)^k$ for odd k. Our construction yields Cayley digraphs whose order is asymptotically kd^{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 is $\frac{d^k}{e^2 k}$, 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 $k\left(\frac{d}{3}\right)^k$. For $d - k \not\equiv 3 \pmod 4$, we construct Cayley graphs whose order is asymptotically $k\left(\frac{d}{2}\right)^{k-1}$. 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 $\frac{1}{e^2 k}\left(\frac{d}{2}\right)^k$, a factor of $\frac{1}{e^2 k^2}\left(\frac{3}{2}\right)^k$ 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 $\mathbb{Z}_t \times \ldots \times \mathbb{Z}_t$, 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

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

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 $rt^r = (k-1)(d-k+3)^{k-1}$.

As generators for 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

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

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 $DM_{d,k}/ek$, 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 $2t+r-3+(d-k \mod 2) = d$. 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 $r \geqslant 4$. $\square$

Macbeth, Šiagiová, Širáň & Vetrík [5] present, for any $k \geqslant 3$ and $d \geqslant 5$, a family of Cayley graphs with diameter at most k, degree d, and order no greater than $k\left(\frac{d+1}{3}\right)^k$.[1] Their constructions also use the group G, with a different generating set. For large enough d, these graphs are bigger than those of Theorem 2. However, for $k \geqslant 27$, the graphs of Theorem 2 are larger than those of Macbeth, Šiagiová, Širáň & Vetrík for any $d - k \not\equiv 3 \pmod 4$ satisfying

$$3k + 6\ln k \quad < \quad d \quad < \quad 2\left(\tfrac{3}{2}\right)^k\left(1 - \tfrac{1}{k}\right) - k^2.$$

For specific values of the degree, we can do much better. If we set $d = k^2 - 2k$, then the graphs of Theorem 2 have orders exceeding those in [5] by a factor of at least $\frac{2}{ek^2}\left(\frac{3}{2}\right)^k$, which exceeds 1 for $k \geqslant 14$.

3 The second construction

In our second construction, we conceive of the vectors of length r as being partitioned into $k-1$ *long* blocks, each of length ℓ, and a single *short* block, of length m.

Again, the directed case is presented first, since it is simpler.

Theorem 3. *For any $k, \ell, t \geqslant 2$ and positive $m < \ell$, there exist Cayley digraphs that have diameter k, outdegree $t^\ell + (r-1)t^m - 1$, and order rt^r, where $r = (k-1)\ell + m$.*

Proof. As before, let $G = \mathbb{Z}_t^r \rtimes \mathbb{Z}_r$, of order rt^r. As generators for the Cayley digraph, we use the t^ℓ *long* elements $(a_1, \ldots, a_\ell, 0, \ldots, 0; \ell)$, $a_i \in \mathbb{Z}_t$, together with the additional $(r-1)t^m - 1$ nonzero *short* elements $(a_1, \ldots, a_m, 0, \ldots, 0; s)$, $a_i \in \mathbb{Z}_t$, $s \neq \ell$. Thus the digraph has outdegree $t^\ell + (r-1)t^m - 1$. Long elements shift by ℓ and modify a long block; short elements shift arbitrarily and modify a short block.

The digraph has diameter k. Every element is the product of a single short element (establishing m components of the vector and guaranteeing the final shift value) and $k-1$ long elements (establishing the remaining $(k-1)\ell = r - m$ components of the vector). On the other hand, $(1, \ldots, 1; 0)$ cannot be obtained as a product of fewer than k generators. $\square$

The Cayley digraph of Theorem 3 contains both of the butterfly networks $B_{t^\ell}(r)$ and $B_{t^m}(r)$ as subdigraphs. Its edges can be partitioned into $rt^{r-\ell}$ copies of the t^ℓ-butterfly, from the long elements, $r(r-2)t^{r-m}$ copies of the t^m-butterfly, from the short elements that have nonzero shift, and a collection of directed cycles from the short elements with zero shift.

[1] The graphs in [5] are slightly larger than those of Macbeth, Šiagiová & Širáň [4], whose order is at most $k\left(\frac{d+1}{3}\right)^k - k$.

Given k, ℓ and t, for judicious choice of m, these digraphs are larger than those of Abas & Vetrík [1]. For example, if we let $t = 2$, then for all $k \geqslant 31$ and sufficiently large ℓ, the order of our digraphs is greater than that of those in [1] if

$$\ell - k - \log_2 \ell + 2 \quad < \quad m \quad < \quad \ell - \log_2 k\ell - \tfrac{2}{k}(\log_2 k + 2).$$

If m is chosen optimally, we can do much better than that.

Corollary 4. *For any $k \geqslant 3$, there are arbitrarily large values of d for which there exist Cayley digraphs that have diameter k, outdegree d, and order at least $\frac{1}{k}\big(\frac{k}{k+2}(d+1)\big)^k$.*

Proof. We use the construction of Theorem 3. Let $t = 2$, and let ℓ be any sufficiently large positive integer such that $\log_2 k^2\ell \leqslant \frac{3}{4}\ell$. Let $r = \lceil k\ell - \log_2 k^2\ell \rceil$, and $m = r - (k-1)\ell$, so $r = (k-1)\ell + m$. Note that $0 < m < \ell$.

The digraph has diameter k and order $r2^r$, which (rounding r down) is at least

$$n_0 \;=\; (k\ell - \log_2 k^2\ell)2^{k\ell - \log_2 k^2\ell} \;=\; \left(\frac{1}{k} - \frac{\log_2 k^2\ell}{k^2\ell}\right)2^{k\ell}.$$

Its degree is $d = 2^\ell + (r-1)2^m - 1$, which (substituting for m and rounding r up) is less than

$$d^+ \;=\; 2^\ell \;+\; (k\ell - \log_2 k^2\ell)2^{k\ell - \log_2 k^2\ell + 1 - (k-1)\ell} \;-\; 1 \;=\; \left(1 + \frac{2}{k} - \frac{2\log_2 k^2\ell}{k^2\ell}\right)2^\ell \;-\; 1.$$

Let $\theta = \frac{\log_2 k^2\ell}{k\ell}$. Note that the condition on ℓ implies that $\theta \leqslant \frac{3}{4k} \leqslant \frac{1}{4}$, since $k \geqslant 3$.

Now,

$$kn_0\left(\frac{k}{k+2}(d^+ + 1)\right)^{-k} \;=\; (1-\theta)\left(1 + \frac{2\theta}{k+2-2\theta}\right)^k \;>\; (1-\theta)\left(1 + \frac{2k\theta}{k+2-2\theta}\right),$$

which is at least 1 if $k \geqslant 2$ and $0 \leqslant \theta \leqslant \frac{k-2}{2k-2}$. Since $k \geqslant 3$ and $\theta \leqslant \frac{1}{4}$, the result follows. □

These digraphs have asymptotic order exceeding $\frac{d^k}{e^2 k}$, 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.

It is worth briefly explaining the choice of values for t and r in the proof of Corollary 4. Suppose we fix t and r (and hence the order rt^r), and also fix the diameter k. What is the optimal choice for ℓ, that minimises the degree $t^\ell + (r-1)t^{r-(k-1)\ell} - 1$? Differentiating with respect to ℓ and equating to zero yields $\ell = \frac{1}{k}\big(r + \log_t(k-1)(r-1)\big)$. Solving for r then gives

$$r \;=\; \frac{1}{\ln t}W\!\left(\frac{t^{k\ell-1}\ln t}{k-1}\right) \;+\; 1,$$

where W is the *Lambert W function*, defined implicitly by $W(z)e^{W(z)} = z$. Asymptotically, $W(z) = \ln z - \ln\ln z + o(1)$. Applying this approximation for W then yields $r \approx k\ell - \log_t k^2\ell$.

Using this value for r results in a digraph whose order is asymptotically at least $\frac{1}{k}\left(\frac{k}{k+t}(d+1)\right)^k$. Setting $t = 2$ makes this maximal.

The results in the undirected case are similar. As before, we just add elements to the generating set to make it symmetric.

Theorem 5. *For any $k, \ell, t \geqslant 2$ and positive $m < \ell$, there exist Cayley graphs that have diameter k, degree $2t^\ell + (2r-3)t^m - r$, and order rt^r, where $r = (k-1)\ell + m$.*

Proof. Let $G = \mathbb{Z}_t^r \rtimes \mathbb{Z}_r$. As generators for the Cayley graph of G with these parameters, we use:

- the t^ℓ long elements $(a_1, \dots, a_\ell, 0, \dots, 0; \ell)$, $a_i \in \mathbb{Z}_t$
- their t^ℓ inverses $(0, \dots, 0, a_1, \dots, a_\ell; -\ell)$
- the $(r-2)(t^m-1)$ short elements $(a_1, \dots, a_m, 0, \dots, 0; s)$, $a_i \in \mathbb{Z}_t$ not all zero, $s \notin \{0, \ell\}$
- their $(r-2)(t^m-1)$ inverses $(0, \dots, 0, \overbrace{a_1, \dots, a_m, 0, \dots, 0}^{s}; -s)$
- the $t^m - 1$ nonzero short elements $(a_1, \dots, a_m, 0, \dots, 0; 0)$; this set is symmetric
- the $r-3$ short elements $(0, \dots, 0; s)$, $s \notin \{0, \pm\ell\}$; this set is also symmetric

Thus the graph has degree $2t^\ell + (2r-3)t^m - r$. As in the directed case, it has order rt^r and diameter k. □

Given k, ℓ and t, for appropriate choice of m, these graphs are larger than those of Macbeth, Šiagiová, Širáň & Vetrík [5]. For example, if we let $t = 2$, then for all $k \geqslant 69$ and sufficiently large ℓ, the order of our graphs is greater than that of those in [5] if

$$\ell + k - \log_2 3^k \ell + 1 \quad < \quad m \quad < \quad \ell - \log_2 k\ell - \tfrac{3}{k}(\log_2 k + 2) - 1.$$

If m is chosen optimally, we have the following.

Corollary 6. *For any $k \geqslant 3$, there are arbitrarily large values of d for which there exist Cayley graphs that have diameter k, degree d, and order at least*

$$\tfrac{1}{k}\left(\tfrac{k}{2k+4}\left(d \; + \; k\log_2 \tfrac{d}{2} \; - \; \log_2\log_2 d \; - \; \log_2 8k^2\right)\right)^k.$$

Proof. We use the construction of Theorem 5. As in the proof of Corollary 4, let $t = 2$, and let ℓ be any sufficiently large positive integer such that $\log_2 k^2\ell \leqslant \frac{3}{4}\ell$. Let $r = \lceil k\ell - \log_2 k^2\ell \rceil$, and $m = r - (k-1)\ell$, so $r = (k-1)\ell + m$.

The graph has diameter k and order $r2^r$, which is at least

$$n_0 \; = \; (k\ell - \log_2 k^2\ell)2^{k\ell - \log_2 k^2\ell} \; = \; \left(\frac{1}{k} - \frac{\log_2 k^2\ell}{k^2\ell}\right) 2^{k\ell}.$$

Its degree is $d = 2^{\ell+1} + (2r-3)2^m - r$, which (substituting for m and rounding r up in the second term) is less than

$$2^{\ell+1} + (2k\ell - 2\log_2 k^2\ell - 1)2^{k\ell - \log_2 k^2\ell + 1 - (k-1)\ell} - r = \left(2 + \frac{4}{k} - \frac{1 + 4\log_2 k^2\ell}{k^2\ell}\right)2^\ell - r.$$

Thus, $\frac{1}{2}(d+r)$ is less than $q = \left(1 + \frac{2}{k} - \frac{2\log_2 k^2\ell}{k^2\ell}\right)2^\ell$, and by the argument in the proof of Corollary 4 (with $q = d^+ + 1$), we know that $kn_0 > \left(\frac{kq}{k+2}\right)^k > \left(\frac{k}{2k+4}(d+r)\right)^k$.

It remains to establish the appropriate lower bound for r.

Now, $kn_0 < 2^{k\ell}$ and $q > \frac{d}{2}$, so $2^\ell > \frac{kd}{2k+4}$ and thus $\ell > \log_2 \frac{kd}{2k+4} = \log_2 \frac{d}{2} - \log_2\left(1 + \frac{2}{k}\right)$.

Since $\left(1 + \frac{2}{k}\right)^k < e^2 < 2^3$, we have $\log_2\left(1 + \frac{2}{k}\right) < \frac{3}{k}$ and thus $\ell > \log_2 \frac{d}{2} - \frac{3}{k}$.

Now, $r \geqslant k\ell - \log_2 k^2\ell$, so

$$r > k\log_2 \tfrac{d}{2} - 3 - \log_2 k^2 - \log_2\left(\log_2 \tfrac{d}{2} - \tfrac{3}{k}\right),$$

which is greater than $k\log_2 \frac{d}{2} - \log_2\log_2 d - \log_2 8k^2$, as required. □

These graphs have asymptotic order exceeding $\frac{1}{e^2k}\left(\frac{d}{2}\right)^k$, a factor of $\frac{1}{e^2k^2}\left(\frac{3}{2}\right)^k$ larger than those of Macbeth, Šiagiová, Širáň & Vetrík.

Acknowledgements

The author is very grateful to Grahame Erskine for pointing out errors in earlier drafts, and also to an assiduous referee whose detailed comments greatly improved the quality of this paper.

S.D.G.

References

[1] Marcel Abas and Tomáš Vetrík. Large Cayley digraphs and bipartite Cayley digraphs of odd diameters. *Discrete Math.*, 340(6):1162–1171, 2017.

[2] Fred Annexstein, Marc Baumslag, and Arnold L. Rosenberg. Group action graphs and parallel architectures. *SIAM J. Comput.*, 19(3):544–569, 1990.

[3] N. G. de Bruijn. A combinatorial problem. *Nederl. Akad. Wetensch., Proc.*, 49:758–764, 1946.

[4] Heather Macbeth, Jana Šiagiová, and Jozef Širáň. Cayley graphs of given degree and diameter for cyclic, Abelian, and metacyclic groups. *Discrete Math.*, 312(1):94–99, 2012.

[5] Heather Macbeth, Jana Šiagiová, Jozef Širáň, and Tomáš Vetrík. Large Cayley graphs and vertex-transitive non-Cayley graphs of given degree and diameter. *J. Graph Theory*, 64(2):87–98, 2010.

[6] Mirka Miller and Jozef Širáň. Moore graphs and beyond: A survey of the degree/diameter problem. *Electron. J. Combin.*, 20(2): Dynamic survery 14v2, 92 pp, 2013.

[7] Tomáš Vetrík. Large Cayley digraphs of given degree and diameter. *Discrete Math.*, 312(2):472–475, 2012.