Europ. J. Combinatorics (1985) **6**, 101–114

Sidon Sets in Groups and Induced Subgraphs of Cayley Graphs

LÁSZLÓ BABAI* AND VERA T. SÓS

Let S be a subset of a group G. We call S a Sidon subset of the first (second) kind, if for any $x, y, z, w \in S$ of which at least 3 are different, $xy \neq zw$ ($xy^{-1} \neq zw^{-1}$, resp.). (For abelian groups, the two notions coincide.) If G has a Sidon subset of the second kind with n elements then every n-vertex graph is an induced subgraph of some Cayley graph of G. We prove that a sufficient condition for G to have a Sidon subset of order n (of either kind) is that $|G| \geqslant cn^3$. For elementary Abelian groups of square order, $|G| \geqslant n^2$ is sufficient. We prove that most graphs on n vertices are not induced subgraphs of any vertex transitive graph with $< cn^2/\log^2 n$ vertices. We comment on embedding trees and, in particular, stars, as induced subgraphs of Cayley graphs, and on the related problem of product-free (sum-free) sets in groups. We summarize the known results on the cardinality of Sidon sets of infinite groups, and formulate a number of open problems.

We warn the reader that the sets considered in this paper are different from the Sidon sets Fourier analysts investigate.

1. INTRODUCTION

One of the problems Paul Erdös never misses to mention in his countless 'Problems and results in additive number theory' lectures was proposed in 1933 by the eccentric Hungarian mathematician Simon Sidon in connection with his work in Fourier analysis [30], [31]. Sidon called a sequence $a_1 < a_2 < \cdots$ of positive integers a B_2 sequence if all the pairwise sums $a_i + a_j$ ($i \leqslant j$) are different. The question was, how large the density of such a sequence can be.

Let $A_S(n)$ denote the number of terms $\leqslant n$ in a sequence S. There is a major gap between the known lower and upper bounds: for every Sidon sequence, $A_S(n) \leqslant C(n/\log n)^{1/2}$ infinitely often (P. Erdös, cf. [36], p. 133) and for some Sidon sequence, $A_S(n) \geqslant c(n \log n)^{1/3}$ for every n (Ajtai, Komlós, Szemerédi [1]).

Such an $n^{1/3}$ *vs.* $n^{1/2}$ gap is quite typical for this subject.

In the first paper on the density of Sidon sequences, Erdös and Turán [18] investigated the finite version of this problem: let $\Phi(n) = \max k$ such that there is a k-term Sidon B_2 sequence $1 \leqslant a_1 < \cdots < a_k \leqslant n$. They proved $(1/\sqrt{2} - o(1))\sqrt{n} < \Phi(n) < (1 + o(1))\sqrt{n}$. Later Chowla and Erdös observed that the lower bound can be improved to $(1 - o(1))\sqrt{n}$ using the perfect difference set derived from the Singer automorphism of finite Desarguesian projective planes.

It is natural to ask the analogous questions mod n, and more generally, for finite groups. For a group G of order n, an $O(n^{1/2})$ upper bound on the size of our generalized Sidon sets will be immediate from the definition (below). On the other hand, our lower bound, obtained by a probabilistic argument, is $cn^{1/3}$, so we experience a gap here similar in magnitude to that in Sidon's original problem, although the difficulty may be of different nature. The existence of large Sidon subsets is, in a sense, an anti-Ramsey problem for certain coloured graphs. The result of [5] appears to indicate that any attempt to improve the $cn^{1/3}$ lower bound has to rely on specific (algebraic?) information on the structure of the group G. We succeed only in highly particular cases (elementary Abelian groups, cyclic groups). The proofs of the improved lower bounds (Section 5) are slight modifications of the original Erdös–Turán construction [18] (cf. Remark 5.5).

* Currently visiting the Department of Computer Science, University of Chicago.

0195-6698/85/020101+14 $02.00/0

It is worth noting that the $cn^{1/3}$ lower bound holds more generally when we seek Sidon subsets from a given n-subset W of the group G, but our improved lower bound constructions do not generalize to this situation. For cyclic groups, a $cn^{1/2}$ lower bound still holds (Komlós, Sulyok, Szemerédi [26]), but the question remains open even for elementary Abelian groups.

In generalizing the notion of Sidon sequences to Abelain groups, some care has to be exercised in order to avoid ruling out involutions.

DEFINITION 1.1. We call a subset S of an Abelian group G a *Sidon set* if for any x, y, z, $w \in S$ of which at least three are different,

$$x+y \neq z+w.$$

Equivalently, $x-z \neq w-y$. There are thus two natural ways to generalize this notion to non-Abelian groups.

DEFINITION 1.2. We call a subset S of a group G a *Sidon set of the first kind* if for any x, y, z, $w \in S$ of which at least three are different,

$$xy \neq zw.$$

DEFINITION 1.3. $S \subseteq G$ is a *Sidon set of the second kind* if

$$xy^{-1} \neq zw^{-1}$$

for any x, y, z, $w \in S$ of which at least three are different.

Sidon sets of the second kind are closely related to the problem of embedding graphs as induced subgraphs in Cayley graphs (Section 2).

We warn the reader that another type of 'lacunary' subsets of groups are commonly called Sidon sets in harmonic analysis (cf. [23, ch. 9. § 37], [28]).

2. CAYLEY GRAPHS

Let G be a group and C a subset of G. We assume $1 \notin C = C^{-1}$. The *Cayley graph* $\Gamma = \Gamma(G, C)$ is defined to have vertex set G and edge set

$$\{\{g, xg\}: g \in G, x \in C\}.$$

Clearly, g, $h \in G$ are adjacent in Γ if and only if $gh^{-1} \in C$. If G has $n = 1+k+2l$ elements where k is the number of elements of order 2, then G has 2^{k+l} Cayley graphs.

The right translations $\rho_g: x \mapsto xg$ $(x, g \in G)$ are automorphisms of Γ. They form a transitive subgroup of Aut Γ. Graphs with a transitive group of automorphisms are called *vertex-transitive*. (Note that not every vertex-transitive graph is a Cayley graph, cf. [29], [20].)

The following result was proved in [3].

THEOREM 2.1. *Every graph is an induced subgraph of some Cayley graph of any sufficiently large group.*

We note that in our definition of Cayley graphs, the set C was not required to generate G. Such an additional requirement would, however, not change either the validity of Theorem 2.1 or the estimates given in this paper. As a matter of fact, if a connected graph X is an induced subgraph of $\Gamma(G, C)$ then it is an induced subgraph of $\Gamma(H, C)$ where

$H=\langle C\rangle$, the subgroup generated by C, and therefore X is an induced subgraph of $\Gamma(G, C')$ where $C'=C\cup(G\backslash H)$ generates G.

We remark that if $C=D\cup D^{-1}$ where D is required to be irredundant (no member of D is generated by the other members), then 2.1 fails and questions of entirely different nature arise [4], [35].

Thus, C will be required neither to be irredundant nor to generate G.

In this paper we are concerned with the problem, how large the group has to be in order that 2.1 holds. For $\mathcal{G}$ a class of groups, let $f(n, \mathcal{G})$ denote the smallest cardinal such that every graph on n vertices is an induced subgraph of some Cayley graph of G for all $G\in\mathcal{G}$, $|G|\geq f(n, \mathcal{G})$. Let $f(n)=f(n, \{\text{all groups}\})$.

For infinite n, the determination of $f(n)$ was reasonably well settled by a Ramsey argument [3], (cf. Section 7), but the estimate obtained for the finite case was quite poor: $f(n)<1\cdot 02^{6^n}$. In fact, using a better Ramsey-bound of Erdös and Hajnal [13], the argument of [3] actually yields $f(n)<c^{n^7}$. This was improved by Godsil and Imrich [21] to c^{n^2}, using a different method. As it turns out, we shall be able to reduce these bounds drastically using a simple probabilisitc estimate for Sidon sets of the second kind. Our main result says $f(n)<cn^3$.

THEOREM 2.2. *If X is a finite graph on n vertices and G is a group of order at least c_1n^3, then X is an induced subgraph of some Cayley graph of G.*

(See Corollary 4.3.)

For some particular classes of groups (cyclic groups, elementary abelian groups of square order), $|G|\geq c_2n^2$ guarantees embeddability of any n-vertex graph in some Cayley graph of G (Section 5). This is best possible apart from the constant, as seen by an easy counting argument (see Section 6):

PROPOSITION 2.3. *If G is a group of order less than c_3n^2, then there exist n-vertex graphs not isomorphic to an induced subgraph of any Cayley graph of G.* ($C_3=\frac{1}{2}+o(1)$.)

Let $g(n)$ denote the smallest integer such that every graph on n vertices is an induced subgraph of some vertex transitive graph having $\leq g(n)$ vertices. We prove

THEOREM 2.4. $c_4n^2/\log^2 n<g(n)<c_2n^2$.

The upper bound follows from the remark after Theorem 2.2. To establish the lower bound (Theorem 6.6), we need an upper bound on the total number of vertex transitive graphs on a given set of vertices (Theorem 6.1).

We show that every tree of order n is an induced subgraph of some Cayley graph of every group of order $\geq n^2$ (Theorem 7.1). This bound seems far from best possible; we have no nonlinear lower bounds.

The problem of induced n-stars of Cayley graphs is equivalent to finding large *product-free* (sum-free) *sets* in groups. We comment on this problem in Section 7.

3. SIDON SETS

The link between Sidon sets of the second kind and induced subgraphs of Cayley graphs is immediate.

PROPOSITION 3.1. *For a subset S of a group G the following four conditions are equivalent.*
(*A*) *S is a Sidon set of the second kind.*

(*B*) *For any* $x, y, z, w \in S$, *if* $x \neq y$ *then*

$$xy^{-1} = zw^{-1} \quad \textit{implies } \{x, y\} = \{z, w\}.$$

(*C*) *For any triple of distinct elements* $x, y, z \in S$

$$(i) \quad xy^{-1} \neq yz^{-1},$$

and for any quadruple of distinct elements $x, y, z, w \in S$,

$$(ii) \quad xy^{-1} \neq zw^{-1}.$$

(*D*) *Any graph with vertex set* S *is an induced subgraph of some Cayley graph of* G.

PROOF. The equivalence of (A), (B) and (C) is a straightforward exercise. We prove that (B) and (D) are equivalent.

Assuming (B), let $X = (S, E)$ be a graph and set $C = \{xy^{-1} : \{x, y\} \in E\}$. Clearly $1 \notin C = C^{-1}$, and (A) guarantees that the induced subgraph of $\Gamma(G, C)$ on S is indeed X.

Assuming now that (B) fails, let $x^{-1}y = z^{-1}w$, $x \neq y$ while $\{x, y\} \neq \{z, w\}$. Let E consist of the single edge $\{x, y\}$. Now if $X = (S, E)$ is a subgraph of some Cayley graph $\Gamma(G, C)$ of $G(C = C^{-1})$, then $xy^{-1} \in C$ hence $zw^{-1} \in C$ and therefore $\{z, w\}$ is an edge of $\Gamma(G, C)$, proving that X is *not* an induced subgraph of $\Gamma(G, C)$.

Sidon sets of the first kind do not appear to have such a connection to Cayley graphs.

PROPOSITION 3.2. *For a subset* S *of a group* G *the following are equivalent.*

(*A*) S *is a Sidon set of the first kind.*

(*B*) *For any* $x, y, z, w \in S$, *if* $x \neq y$ *then*

$$xy = zw \quad \textit{implies } \{x, y\} = \{z, w\}.$$

(*C*) *For any triple of distinct elements* $x, y, z \in S$

$$(i) \quad xy \neq z,$$

$$(ii) \quad x^2 \neq yz,$$

and for any quadruple of distinct elements $x, y, z, w \in S$,

$$(iii) \quad xy \neq zw.$$

PROOF. Clear.

REMARK 3.3. Let $W \subseteq G$ be an n-subset of a group G. Let $S \subseteq W$ be a Sidon subset of either kind. An upper bound for $s = |S|$ follows from the inequality $\binom{s}{2} \leq n$. If G has no involutions, then $s(s-1) \leq n$ holds for Sidon sets of the second kind. These inequalities yield an $s = O(n^{1/2})$ upper bound. We do not know of any class of pairs (G, W) where $s = o(n^{1/2})$ would be forced. On the other hand, our lower bound (Theorem 4.2) is $s \geq cn^{1/3}$ and we are unable to close this gap. Only for very particular Abelian groups G and only under the assumption $W = G$ is $s \geq cn^{1/2}$ known (Section 5). The only groups G for which $s \geq cn^{1/2}$ is known for any $W \subseteq G$ are the cyclic groups (Komlós, Sulyok, Szemerédi [26]).

4. A Probabilistic Lower Bound for Sidon Sets

A *hypergraph* $\mathcal{H} = (V, E)$ consists of a set V (vertices) and a collection E of nonempty subsets of V (edges). A subset S of V is *independent* if it contains no edges. $\alpha(\mathcal{H})$ denotes the maximum cardinality of independent sets in $\mathcal{H}$. $\mathcal{H}$ is *r-uniform* if every edge has r elements.

It follows by a probabilistic argument that *sparse hypergraphs have large independent sets.* More specifically, Spencer [34] shows that if an r-uniform hypergraph $\mathcal{H}$ has n vertices and e edges then

$$\alpha(\mathcal{H}) > n/(2t)$$

where $t = (2re/n)^{1/(r-1)}$.

For non-uniform hypergraphs, the same argument yields the following.

PROPOSITION 4.1. *Let e_r denote the number of edges of size r in the hypergraph $\mathcal{H}$ with n vertices. Let*

$$f(k)=\sum_r e_r\binom{k}{r}\Big/\binom{n}{r}.$$

Then

$$\alpha(\mathcal{H})\geqslant\max\{k-f(k):\ 1\leqslant k\leqslant n\}.$$

PROOF. Let $V(\mathcal{H})=V$. For any r-set $R\subseteq V$, the probability that R is contained in a random k-subset of V is $\binom{k}{r}/\binom{n}{r}$. Let x_r denote the number of r-edges of $\mathcal{H}$ contained in a random k-subset of V. Then $E(x_r)=e_r\binom{k}{r}/\binom{n}{r}$. Consequently the expected number of edges contained in a random k-subset of V is $f(k)$, and therefore some k-subset K of V contains at most $f(k)$ edges. Removing a point of each of these edges from K we obtain an independent set, hence the assertion follows.

In order to find an $\Omega(n^{1/3})$ lower bound for the size of Sidon sets in general groups, we apply Proposition 4.1 to the hypergraph of 'bad' triples and quadruples, characterized in Proposition 3.1 (C) and Proposition 3.2 (C), respectively.

THEOREM 4.2. *Let G be a (finite or infinite) group and $W\subset G$ a finite subset, $|W|=n$. Then W contains Sidon subsets of both kinds, of size*

$$(c+o(1))n^{1/3}$$

where $c=3\sqrt[3]{2}/8\approx 0{\cdot}47247\cdots$. Furthermore, V contains a subset of size

$$(3/8+o(1))n^{1/3}$$

which is simultaneously a Sidon subset of both kinds.

PROOF. Let us define the hypergraph $\mathcal{H}^1=(W, E_3^1\cup E_4^1)$ corresponding to the 'bad' subsets for Sidon sets of the first kind (Proposition 3.2(C)), i.e. E_3^1 consists of those triples $\{x, y, z\}$ of distinct elements of W satisfying $xy=yz$ or $x^2=yz$; and E_4^1 consist of those quadruples $\{x, y, z, w\}\subset W$ satisfying $xy=zw$. Analogously, let $\mathcal{H}^2=(W, E_3^2\cup E_4^2)$ where E_3^2 consists of the triples $\{x, y, z\}$ with $x^{-1}y=y^{-1}z$ and E_4^2 consists of the quadruples $\{x, y, zw\}$ with $x^{-1}y=z^{-1}w$ [cf. Proposition 3.1(C)].

Setting $e_i^p=|E_i^p|$ $(p\in\{1,2\},\ i\in\{3,4\})$, we have

$$e_3^p\leqslant 2n(n-1),\qquad e_4^p\leqslant n(n-1)(n-2).$$

Applying Proposition 4.1 with $k=\lfloor(n/4)^{1/3}\rfloor$ we obtain the first part of our claim. The second part follows setting $k=\lfloor(n/8)^{1/3}\rfloor$.

COROLLARY 4.3. *Let X be a graph on n vertices, G a (finite or infinite) group and $W\subset G$ a subset of at least $(c+o(1))n^3$ elements, where $c=256/27=9{\cdot}48\ldots$. Then some Cayley graph of G has an induced subgraph on a subset of W which is isomorphic to X.*

PROOF. Find a Sidon set of the second kind, $S\subset W$, $|S|=n$ by Thorem 4.2. Apply Proposition 3.1 (A)$\Rightarrow$(D) to construct the Cayley graph.

5. SIDON SETS IN ABELIAN GROUPS

Next we construct fairly large Sidon sets for some particular classes of finite Abelian groups. We shall comment on the infinite case in Section 8.

The constructions given in this section are slight modifications of the original Erdös–Turán construction [18]. The case $q=2^t$ of Proposition 5.1 appears in Lindström [27].

PROPOSITION 5.1. *Let q be a prime power and G the elementary Abelian group of order q^2. Then G has a Sidon subset of size q.*

PROOF. Let $F=F_q$ denote the field of q elements. G can be identified with the additive group of the 2-dimensional space F^2 over F. Set

$$S=\{v(x): x\in F\},$$

where

$$v(x)=(x, x^2), \qquad \text{if } q \text{ is odd,}$$

and

$$v(x)=(x, x^3), \qquad \text{if } q \text{ is even.}$$

We claim that S is a Sidon set.

We have to prove that for $x\neq y$, the pair $\{x, y\}$ is determined by $v(x)+v(y)$ (cf. 3.2 (B)). Let $v(x)+v(y)=(a, b)$. Now if q is odd then

$$x+y=a$$
$$x^2+y^2=b$$

hence x, y are the roots of the polynomial

$$p(w)=2w^2-2aw+(a^2-b).$$

If q is even and $x\neq y$ then

$$x+y=a\neq 0,$$
$$x^3+y^3=b$$

hence x, y are the roots of the polynomial

$$p(w)=aw^2+a^2w+(a^3+b).$$

REMARK 5.2. In the case of odd q this bound is sharp since in an Abelian group G of odd order, the size $s=|S|$ of any Sidon subset clearly satisfies $s(s-1)\leq n-1$. (All pairwise differences are distinct.) For elementary Abelian 2-groups, however, we still have a gap of a factor of $\sqrt{2}$, the upper bound being $\binom{s}{2}\leq n-1$.

PROPOSITION 5.3. *Let G be the direct sum of cyclic groups $G=Z_{n_1}\oplus\cdots\oplus Z_{n_k}$. Assume that p is an odd prime such that $2p^2\leq n_i$ for $i=1, \ldots, k$. Then G has a Sidon set of size $\lfloor p/2\rfloor^k$.*

PROOF. Identifying Z_m with the set $\{0, 1, \ldots, m-1\}\subset Z$ we obtain an injection $\varphi: G\to Z^k$ which is a 'local isomorphism' in the sense that if $x, y\in G$ and the ith coordinates of both x and y are less than $n_i/2$ then $\varphi(x+y)=\varphi(x)+\varphi(y)$. Let $q=p^k$ and $F=F_q$ be the field of q elements. The additive group of F is isomorphic to Z_p^k; let $\psi: F\to Z^k$ denote the analogous 'local isomorphism' (for addition). Let $\psi(x)=(\psi_1(x), \ldots, \psi_k(x))$ $(0\leq \psi_i(x)\leq p-1)$. Set $R=\{x\in F: \psi_i(x)<p/2 \text{ for } i=1, \ldots, k\}$ The set R has $\lfloor p/2\rfloor^k$ elements.

Set

$$w(x)=\psi(x)+p\psi(x^2), \qquad x\in F,$$

and

$$v(x)=\varphi^{-1}(w(x)).$$

This is a well defined member of G since $\psi_i(x)+p\psi_i(x^2) \leq p^2-1 < n_i$. Let

$$S=\{v(x): x \in R\}.$$

We claim that S is a Sidon set in G.

The proof is modelled after the proof of Proposition 5.1. Let $x, y \in R$, $v(x)+v(y)=v \in G$. We have to determine the pair $\{x, y\}$, given v. As in 5.1, it suffices to determine $x+y$ and x^2+y^2; to this end, we only need $\psi(x+y)$ and $\psi(x^2+y^2)$.

For any $x \in F$, we have $\psi_i(x)+p\psi_i(x^2) < p^2 \leq n_i/2$, hence by the 'local isomorphism' property, $w =_{\text{def}} \varphi(v) = w(x)+w(y)$. Now,

$$w = \psi(x)+\psi(y)+p(\psi(x^2)+\psi(y^2)) \in Z^k.$$

Let $0 \leq z_i \leq p-1$, $z_i \equiv \psi_i(x)+\psi_i(y) \bmod p$. Clearly

$$z_i = \psi_i(x)+\psi_i(y) = \psi_i(x+y) \qquad (\text{since } \psi_i(x), \psi_i(y) < p/2).$$

It follows that

$$\psi(x+y) = z = (z_1, \ldots, z_k).$$

Now, $\psi(x^2)+\psi(y^2) = (w-z)/p =_{\text{def}} (t_1, \ldots, t_k)$. Let $0 \leq t_1' \leq p-1$, $t_1' \equiv t_i \bmod p$. Then

$$\psi(x^2+y^2) = (t_1', \ldots, t_k').$$

COROLLARY 5.4. *Let $G = Z_m^k$. Then G has a Sidon set of size $(m/2+o_m(1)))^{k/2}$.*

PROOF. Select a prime p such that

$$(1-\varepsilon_m)m < 2p^2 < m,$$

and apply Proposition 5.3.

REMARK 5.5. In particular, for $k=1$ we find that the *cyclic* group of order m has a Sidon set of size $(m/2)^{1/2}(1+o(1))$. This is the result of Erdös and Turán [18]; their proof has been generalized above.

REMARK 5.6. The trivial upper bound for $|S|=s$ being $s(s-1) \leq m-1$, for cyclic groups we have a gap of a factor of $\sqrt{2}$.

For $m=q^2+q+1$, where q is a prime power, there is a perfect difference set S (derived from the Singer automorphim of the projective plane of order q [32]), that is $s=|S|=q+1$. So, the upper bound is tight ($s(s-1)=m-1$) in an infinity of cases.

For the problem of Sidon sequences among the integers $1, \ldots, m$, this observation closes the $\sqrt{2}$ gap. This is, however, not the case for cyclic groups of order m: for general m, we have to select a prime power q such that $q^2+q+1 \leq m/2$ and take a perfect difference set from $\{1, \ldots, q^2+q+1\}$, obtaining, once again, a Sidon set of order $(m/2)^{1/2}(1+o(1))$.

COROLLARY 5.7. *Let $n=p^k$ and $G=Z_p^k$ be an elementary Abelian group of order n. Then G has a Sidon set of size*

$$\max((n/p)^{1/2}, n^{1/2}/(2+o_p(1))^{k/2}).$$

The term $2+o_p(1)$ never exceeds 8.

PROOF. For k even, there is a Sidon set of size $n^{1/2}$ (Proposition 5.1). For odd k, apply Proposition 5.1 to the subgroup Z_p^{k-1} on one hand, and apply Corollary 5.4 to Z_p^k

on the other hand. To obtain 8 in place of $2+o_p(1)$ we just use any prime p between $(m/8)^{1/2}$ and $(m/2)^{1/2}$ in the proof of Corollary 5.4.

COROLLARY 5.8. *Elementary Abelian groups of order n have Sidon sets of size* $n^{1/2+o(1)}$.

PROOF. If $n=p^k$ then

$$\max(p^{-1/2}, 8^{-k/2}) \geq 2^{-\sqrt{\log_2 n/12}} = n^{o(1)}.$$

PROBLEM 5.9. Does each n-subset of an elementary Abelian group contain a Sidon-subset of order $n^{1/2+o(1)}$? (Cf. Remark 3.3.)

6. On the Number of Vertex Transitive Graphs

The aim of this section is to prove that most graphs on n vertices do not embed in vertex transitive graphs smaller than $cn^2/\log^2 n$ (Theorem 6.6).

First we prove Proposition 2.3.

Let G be a group of order m. Then the number of Cayley graphs of G is at most 2^{m-1}, and the number of n-vertex induced subgraphs of these Cayley graphs is less than $\binom{m}{n}2^{m-1}$. The number of graphs on n vertices is greater than $2^{\binom{n}{2}}/n!$. Therefore, if all graphs on n vertices occur as induced subgraphs of Cayley graphs of G, then

$$2^{\binom{n}{2}}/n! < \binom{m}{n}2^{m-1},$$

hence

$$m > (n^2/2)(1+o(1)).$$

In fact, if $\binom{m}{n}2^m = o(2^{\binom{n}{2}}/n!)$, that is if $m < (n^2/2)(1+o(1))$ then most graphs on n vertices do not embed in any Cayley graph of G.

To prove a similar result for vertex-transitive graphs in general, we need the following estimate.

THEOREM 6.1. *The number of labelled vertex-transitive graphs on n vertices is less than* $n^{(1+o(1))n\log_2 n}$.

This bound is probably very far from best possible. In attempting to improve it, however, one seems to face major unsolved problems of group theory such as estimating the number of minimal transitive permutation groups of given degree.

LEMMA 6.2. *Every transitive group of degree n has a transitive subgroup generated by* $\leq \log_2 n + \log_2 \ln n + 1$ *elements.*

The result and its proof are quite similar to those in [6], although it is not clear what the common generalization ought to be. The result of [6] states that every (quasi) group G of order k possesses a sequence of $s \leq \log_2 k + \log_2 \ln k + 2$ elements $g_1, \ldots, g_s$ such that each element of G has a representation of the form $g_{i_1} \cdots g_{i_t}$, $1 \leq i_1 < \cdots < i_t \leq s$

To prove 6.2, we need a counting lemma.

LEMMA 6.3. *Let G be a transitive group acting on Ω, $|\Omega| = n$. Let Ω be partitioned as $\Omega = A \dot\cup B$. Then there exists $g \in G$ such that*

$$|B \setminus A^g|/n \leq (|B|/n)^2.$$

PROOF. Let $|G| = m$. For any $x, y \in G$, the number of those $g \in G$ which take x to y is m/n. Now

$$\frac{1}{m} \sum_{g \in G} |A^g \cap B| = \frac{1}{m} \sum_{x \in A} \sum_{y \in B} |\{g \in G: x^g = y\}| = |A||B|/n.$$

Therefore $|A^g \cap B| \geqslant |A||B|/n$ for some $g \in G$ and thus

$$|B \setminus A^g| \leqslant |B| - (|A||B|/n) = |B|^2/n.$$

Now Lemma 6.2 follows by a greedy argument. Let us fix $x_0 \in \Omega$. We select $g_1, g_2, \ldots, g_s$ from G such as to maximize at each step the set the orbit A_i of x_0 under the subgroup generated by $g_1, \ldots, g_i$. We stop when $A_s = \Omega$. Let $B_i = \Omega \setminus A_i$ and $p_i = |B_i|/n$. Clearly, $B_{i+1} \subseteq B_i \setminus A_i^{g_{i+1}}$, and thus by Lemma 6.3,

$$p_{i+1} \leqslant p_i^2.$$

Moreover,

$$p_1 \leqslant 1 - 2/n$$

and

$$p_{s-1} \geqslant 1/n.$$

Consequently,

$$1/n \leqslant p_{s-1} \leqslant p_1^{2^{s-2}} \leqslant (1-2/n)^{2^{s-2}} < \exp(-2^{s-1}/n),$$

and thus

$$s < \log_2 n + \log_2 \ln n + 1.$$

REMARK 6.4. The sharp bound seems to be $\log_2 n$ (sharp for n a power of 2). We suspect also, that every transitive group can be generated by $O(\log n)$ elements. To prove this, however, one might have to resort to the classification of finite simple groups.

COROLLARY 6.5. *The number of minimal transitive subgroups of* $\mathrm{Sym}(n)$ *is less then* $\binom{n!}{s}$ *where* $s = \lfloor \log_2 n + \log_2 \ln n + 1 \rfloor$.

PROOF. Immediate by Lemma 6.2.

Now we turn to the proof of Theorem 6.1. Clearly there are at most 2^{n-1} graphs invariant under a given transitive permutation group. Therefore the total number of labelled vertex transitive graphs on n vertices is less than

$$2^{n-1}\binom{n!}{s} < n^{(1+o(1))n \log_2 n}.$$

Finally, we prove the main result of this section.

THEOREM 6.6. *For almost all graphs X on n vertices, the smallest number $v(X)$ of vertices of vertex transitive graphs containing X as an induced subgraph satisfies*

$$v(X) > (1/8 + o(1))n^2/\log_2^2 n.$$

PROOF. The total number of induced subgraphs of all vertex transitive graphs of less than v vertices is, by Theorem 6.1, less than

$$\sum_{k<v} 2^k k^{(1+o(1))k \log_2 k} < 2^v v^{(1+o(1))v \log_2 v} = o(2^{\binom{n}{2}} 2^{\binom{n}{2}})$$

if $v \leq (1/8+o(1))n^2 \log_2^2 n$.

7. Embedding Trees, Stars; Product-free Sets

THEOREM 7.1. *Let T be a tree on n vertices. Every group of order $>n^2$ has a Cayley graph of which T is an induced subgraph.*

PROOF. Let $V(T)=\{v_1, \ldots, v_n\}$, where the numbering is such that each initial segment induces a connected subgraph. Consequently, v_{i+1} is adjacent to precisely one of $v_1, \ldots, v_i$.

We define the group elements $g_1, \ldots, g_n \in G$ successively with the aim that in the end, the map $v_i \mapsto g_i$ will be an embedding of T into $\Gamma(G, S)$ where $S=\{g_i g_j^{-1}: \{v_i, v_j\} \in E(T)\}$.

We select g_1 arbitrarily. It is easy to see that the only rule we have to observe while selecting $x=g_{i+1}$ is the following. Let v_k be the unique neighbor of v_{i+1} with $k \leq i$. Then $xg_k^{-1} \neq g_p g_q^{-1}$ for $1 \leq p, q \leq i$.

This rules out $i(i-1)+1$ members of G. Hence an appropriate x can always be selected as long as $|G| \geq n(n-1)+2$.

REMARK 7.2. We do not see why this result could not be improved, perhaps even to $n^{1+o(1)}$. In fact we do not have a non-linear lower bound. On the other hand, we are unable to prove $o(n^2)$ even for cyclic groups.

The simplest sort of trees are the stars. The n-star has $n+1$ vertices, one of them adjacent to the rest.

DEFINITION 7.3. A subset S of a group G is *product-free*, if $xy \neq z$ for any $x, y, z \in S$. (For Abelian groups, these sets are often called *sum-free*.)

Note that in particular, $x^2 \neq z$ $(x, y \in S)$.

PROPOSITION 7.4. *The following two conditions on a group G are equivalent.*

(i) *G has a product-free set of size n.*

(ii) *Some Cayley graph of G has an induced n-star.*

PROOF. Assume that the Cayley graph $\Gamma(G, S)$ has an induced n-star. Then it has a n-star centered at the identity; let $g_1, \ldots, g_n$ be the neighbors of 1 in this star. Then $g_1, \ldots, g_n \in S$ and $g_i g_j^{-1} \notin S$ whence $\{g_1, \ldots, g_n\}$ is product free. The converse is equally straight forward.

PROBLEM 7.5. Does there exist a constant $c>0$ such that every group of order n has a product-free set of size $>cn$?

We shall see that it suffices to decide this question for finite simple groups. As a matter of fact, let $\alpha(G)$ denote the size of the largest product-free set in G, and $\beta(G)=\alpha(G)/|G|$.

PROPOSITION 7.6. *If N is a proper normal subgroup of G then $\beta(G) \geq \beta(G/N)$.*

PROOF. Let $\varphi: G \to G/N$ be the natural epimorphism and S a largest product-free subset of G/N. Then $\varphi^{-1}(S)$ is a product free set in G, proving the inequality.

The following is well known (see [10], [8], [37] for sharper results and upper bounds).

PROPOSITION 7.7. *For $n \geq 2$,*

$$\alpha(Z_n) = n/2, \quad \text{if } n \text{ is even,}$$

$$\alpha(Z_n) \geq \lfloor (n+1)/3 \rfloor, \quad \text{if } n \text{ is odd.}$$

PROOF. If n is even, take $S = \{1, 3, \ldots, n-1\}$.
If n is odd, take $S = \{k, k+1, \ldots, 2k-1\}$ where $k = \lfloor (n+1)/3 \rfloor$.

Observe that if n is odd and $n \geq 3$ then

$$\lfloor (n+1)/3 \rfloor \geq 2n/7.$$

COROLLARY 7.8. *If G is a solvable group of order $n \geq 2$ then*

$$\alpha(G) \geq 2n/7.$$

PROOF. Combine 7.6 and 7.7.

Propositions 7.6 and 7.7 yield a lower bound for $\alpha(G)$ whenever G has a nontrivial cyclic factor group.

PROBLEM 7.9. Does 7.5 hold for the alternating groups A_m and for the special linear groups $\mathrm{SL}(m, q)$?

A negative answer would imply a non-linear lower bound for induced trees (cf. Remark 7.2).

PROPOSITION 7.10. *If G has a subgroup of index $k \geq 2$ then*

$$\alpha(G) \geq n/k.$$

PROOF. Any coset Hg, $g \in G \setminus H$ (H a proper subgroup) is product free.

REMARK 7.11. It appears, that, using the classifiation of finite simple groups, 7.10 should suffice for the proof of an $\alpha(G) > cn^{2/3}$ bound for all groups g of order n.

PROBLEM 7.12. Let W be subset of a group G. How large a product-free subset can be found in W (in terms of $n = |W|$)?

Clearly, any maximal (w.r. to inclusion) product-free subset of W has size $\geq (n/3)^{1/2}$. What is the minimum size of maximal product-free sets in a group G of order n? Is it bounded by $O(n^{1/2})$? The answer is yes for an infinity of groups (elementary abelian groups of odd square order).

8. SIDON SETS IN INFINITE GROUPS

For an infinite subset W of a group G let S be a subset of W maximal with respect to the condition that

(*) for any quadruple of distinct elements $x, y, z, w \in S$,

$$xy^{-1} \neq zw^{-1} \quad \text{and} \quad xy \neq zw.$$

Then clearly $|S| = |W|$ and S generates the same subgroup as W.

(**) Therefore, when seeking Sidon sets of maximum cardinality in an infinite subset W of a group, we may assume (*) holds in W, and we only have to discard the triples x, y, z of distinct elements of W such that

(I) $$xy^{-1} = yz^{-1}$$

(for Sidon sets of the second kind), or

(II) $$xy = yz, \text{ or}$$

(III) $$x^2 = yz$$

(for Sidon sets of the first kind, cf. Propositions 3.1 (C) and 3.2 (C)).

PROPOSITION 8.1. *An infinite subset of a group contains an infinite subset which is a Sidon subset of both kinds simultaneously.*

LEMMA 8.2. *Let G be a group and*

$$E = \{\{x, y, z\}: x, y, z \in G, x \neq y \neq z \neq x, \text{ and at least one of } (I), (II), (III) \text{ holds}\}.$$

Then the 3-hypergraph (G, E) does not contain a clique of size 21.

PROOF. Assume $W \subset G$ induces a clique, $|W| = k$. Given $x, y \in G$ there is exactly one $z \in G$ satisfying any one of (I), (II) and (III). Hence the number of E-edges in W does not exceed $3k(k-1)$. Hence $\binom{k}{3} \leq 3k(k-1)$ and consequently $k \leq 20$.

Now, in view of (**), a Sidon subset in W is precisely an independent set in the hypergraph (W, E_W) where $E_w = [W]^3 \cap E$. Proposition 8.1 thus follows by Ramsey's theorem.

More generally, using results of the Erdös–Rado partition calculus [16], [15], [14], one arrives at the following conclusion.

THEOREM 8.3. *If W is a subset of cardinality $\geq f(\kappa)$ of a group G then W contains a subset of cardinaltiy κ which is a Sidon set of both kinds simultaneously. Here $f(\kappa) = \kappa$ if κ is a weakly compact cardinal (in particular if $\kappa = \omega$);*

$$f(\kappa) \leq \left(\sum_{\lambda < \kappa} 2^{\lambda}\right)^{+}$$

where $+$ indicates the successor cardinal. In particular, under the Generalized Continuum Hypothesis we have

$$f(\kappa) \leq \kappa^{+}.$$

For definitions and details of references cf. [2, Section 2]. The major open question here is whether $f(\omega_1) = \omega_1$, i.e.

PROBLEM 8.4. Does each uncountable group (and/or each of its uncountable subsets) contain an uncountable Sidon subset (of either kind)?

We remark that for Sidon sets of the second kind, 8.3 was proved as Lemma 3.2 in [2]. The corresponding 3-hypergraph (G, E') defined by the relation (I) was shown not to contain an 8-clique [2, sublemma 3.3]. For Sidon sets of the second kind, results similar to 8.3 were found independently by Vance Faber [19]. The countable case was settled,

by more direct methods, by A. Souslin [33] and by J. Hickman and B. H. Neumann [25] as well.

The situation is simpler for *infinite Abelian groups.* R. G. Gurevich [22] and J. Hickman and B. H. Neumann [25] prove, independently, that an infinite Abelian group G always contains a Sidon set of cardinality $|G|$. A stronger result is proved in [7, proposition 6.5]:

Every Abelian group is generated by a Sidon subset.

In fact, a slight modification of the proof in [7] yields, that *any set of generators of an Abelian group contains a Sidon subset, generating the group.*

PROBLEM 8.4. Does there exist a group with no Sidon-set (of either kind) of generators?

If exists, such a group must be non-Abelian and not finitely generated.

ACKNOWLEDGEMENT

The authors wish to thank Peter Frankl for his valuable comments.

REFERENCES

1. M. Ajtai, J. Komlós and E. Szemerédi, A dense infinite Sidon sequence, *Europ. J. Comb.* **2** (1981), 1-11.
2. L. Babai, Infinite digraphs with given regular automorphism groups, *J. Combin. Theory, Ser. B* **25** (1978), 26-46.
3. L. Babai, Embedding graphs in Cayley graphs, in: *Probl. Comb. Theorie des Graphes*, Proc. Conf. Paris-Orsay 1976, J-C. Bermond *et al.*, eds. C.N.R.S., Paris 1978, pp. 13-15.
4. L. Babai, Chromatic number and subgraphs of Cayley graphs, in: *Theory and Applications of Graphs*, Y. Alavi, D. R. Lick, eds. *Springer Lect. Notes in Math.* 642. Springer-Verlag, Berlin, 1978, pp. 10-22.
5. L. Babai, An anti-Ramsey theorem, *Graphs and Combinatorics* **1** (1985), 23-28.
6. L. Babai and P. Erdös, Representation of group elements as short products, in: *Theory and Practice of Combinatorics*, A. Rosa *et al.* eds. *Ann. Discrete Math.* **12** (1982), 27-30.
7. L. Babai and W. Imrich, Tournaments with given regular group, *Aequationes Math.* **19** (1979), 232-244.
8. P. H. Diananda and H. P. Yap, Maximal sum-free sets of elements of finite groups, *Proc. Japan Acad.* **45** (1969), 1-5.
9. P. Erdös, Problems and results in additive number theory, in: *Colloque sur la Théorie des Nombres*, Bruxelles, 1955, pp. 127-137.
10. P. Erdös, Extremal problems in numbr theory, *Proc. Sympos. Pure Math.* 8. A. M. S., Providence, RI, 1965, pp. 181-189.
11. P. Erdös, Some applications of Ramsey's theorem to additive number theory, *Europ. J. Comb.* **1** (1980), 43-46.
12. P. Erdös and R. L. Graham, Old and new problems and results in combinatorial number theory, *L'Enseignement Mathématique, Monographie No. 28*, Université de Geneve, 1980.
13. P. Erdös and A. Hajnal, On Ramsey-like theorems, problems and results, in: *Combinatorics*, Proc. Conf. Comb. Math., Oxford 1972, Inst. Math. Appl., Southend-on-Sea, 1972, pp. 123-140.
14. P. Erdös, A. Hajnal, A. Máté and R. Rado, Combinatorial Set Theory: The Ordinary Partition Relation, Akadémiai Kiadó, Budapest, 1984.
15. P. Erdös, A. Hajnal and R. Rado, Partition relations for cardinal numbers, *Acta Math. Acad. Sci. Hung.* **16** (1965), 93-196.
16. P. Erdös and R. Rado, A partition calculus in set theory, *Bull. Amer. Math. Soc.* **62** (1956), 427-489.
17. P. Erdös and J. Spencer, *Probabilistic Methods in Combinatorics*, Academic Press, N.Y., 1974.
18. P. Erdös and P. Turán, On a problem of Sidon in additive number theory and some related problems, *J. London Math. Soc.* **16** (1941), 212-215.
19. V. Faber, private communication by B. H. Neumann, 1975.
20. C. D. Godsil, More odd graph theory, *Discrete Math.* **32** (1980), 205-207.
21. C. D. Godsil, W. Imrich, private communication, 1982.
22. R. G. Gurevich (Leningrad), private communication, 1974.
23. E. Hewitt and K. A. Ross, *Abstract Harmonic Analysis, Vol. II.*, Springer-Verlag, Berlin, 1970.
24. G. Higman, Enumerating p-groups I, *Proc. London Math. Soc.* **10** (1960), 24-30.
25. J. Hickman and B. H. Neumann, A question of Babai on groups, *Bull. Austral. Math. Soc.* **13** (1975), 355-368.

26. J. Komlós, M. Sulyok and E. Szemerédi, Linear problems in combinatorial number theory, *Acta Math. Acad. Sci. Hung.* **26** (1975), 113-121.
27. B. Lindström, Determination of two vectors from the sum, *J. Combin. Theory* **6** (1969), 402-407.
28. W. Rudin, Fourier analysis on groups, Interscience, 1962.
29. G. Sabidussi, Vertex transitive graphs, *Monatshefte für Math.* **68** (1964), 426-438.
30. S. Sidon, Ein Satz über trigonometrische Polynome und seine Anwendungen in der Theorie der Fourier-Reihen, *Math. Ann.* **106** (1932), 539.
31. S. Sidon, Über die Fourier Konstanten der Funktionen der Klasse L_p für $p>1$, *Acta Sci. Math. (Szeged)* **7** (1935), 175-176.
32. J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* **43** (1938), 377-385.
33. A. Souslin (Leningrad), private communication by R. G. Gurevich, 1974.
34. J. Spencer, Turán's theorem for k-graphs, *Discrete Math.* **2** (1972), 183-186.
35. J. Spencer, What's not inside a Cayley graph, *Combinatorica* **3** (1983), 239-241.
36. A. Stöhr, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlen II, *J. Reine und Angew. Math.* **194** (1955), 111-140.
37. H. P. Yap, Maximal sum free sets in finite Abelian groups I-II, *Bull. Austral. Math. Soc.* **4** (1971), 217-233 and **5** (1971), 43-54.

Received 25 April 1984

László Babai
Department of Algebra, Eötvös University,
Budapest, Hungary H-1088

and

Vera T. Sós
Department of Analysis, Eötvös University
Budapest, Hungary H-1088