A note on intersecting cliques in Cayley graphs

Geňa Hahn*
Département d'Informatiques et de Récherche Operationelle
Université de Montréal
CP 6128, Succ. A
Montréal, Québec
Canada H3C 3J7

Jozef Širáň†
Comenius University
Bratislava

ABSTRACT. We show that for infinitely many n there exists a Cayley graph Γ of order n in which any two largest cliques have a nonempty intersection. This answers a question of Hahn, Hell and Poljak. Further, the graphs constructed have a surprisingly small clique number $c_\Gamma = \lfloor\sqrt{2n}\rfloor$ (and we do not know if the constant $\sqrt{2}$ can be made smaller).

1. Introduction

Cayley graphs have been widely studied in the literature for more than a century. In most cases, the research has focused on two outstanding problems. The first is the well known conjecture that every connected Cayley graph has a Hamiltonian cycle (see e.g. [1] for a survey). The second is the problem of characterization and construction of vertex-transitive graphs that are not Cayley graphs; for the recent progress in this area we refer the reader to [4].

In contrast with the above, the investigation of cliques (or, equivalently, independent sets) in Cayley graphs seems to be a largely intact area. It was observed in [3] that in incomplete Cayley graphs of abelian groups there

*Partially supported by a grant from NSERC.
†Work done while visiting the Université de Montréal and supported by the NSERC research grant of the first author.

are (at least two) disjoint largest cliques, that is, cliques whose order is the clique number. Furthermore, it is proven in [2] that this holds for Cayley graphs whose generating sets are invariant under inner automorphisms.

As we shall see, this is not true in general for non-abelian groups. The interesting extremal question is now almost immediate: *If, in a Cayley graph of a non-abelian group, any two largest cliques intersect, then how* small *can the clique number of the graph be?*

At first glance, the above intersection requirement forces the clique number to be quite large in comparison with the order of the graph. It may therefore be surprising that for infinitely many n there is a Cayley graph (of a non-abelian group) of order n with clique number $\lfloor\sqrt{2n}\rfloor$, such that any two its largest cliques meet (see Theorem 1). Moreover, we show that, in a certain class of coset constructions, the number $\lfloor\sqrt{2n}\rfloor$ is also the lower bound for the clique number of a Cayley graph of order n in which any two largest cliques intersect. This shows that the result of Theorem 1 is, in a sense, best possible.

The graphs constructed here provide counterxexamples to an unstated hypothesis of Hahn, Hell and Poljak which hoped that for any Cayley graph Γ the ultimate independent ratio $I(\Gamma)$ was equal to the independence ratio $i(\Gamma)$ of Γ (details will be found in the last section of this note).

2. Lower bounds

Let G be a finite group and let X be a symmetric unit-free subset of G, that is, $X^{-1} = X$ and $1 \notin X$. The *Cayley graph* $C(G,X)$ has vertex set G, and two vertices $a, b \in G$ are adjacent if $a^{-1}b \in X$. Note that the adjacency does not depend on the ordering of a and b, and so our Cayley graphs are undirected (and, of course, simple). Let $T \subset G$ be the vertex set of a clique in $C(G,X)$. Obviously, $T^{-1}T \subset X^*$ where $X^* = X \cup \{1\}$. Conversely, if $T^{-1}T \subset X^*$ then $a^{-1}b \in X$ for any two distinct $a, b \in T$, and so T induces a clique in $C(G,X)$. It follows that if T induces a clique in $C(G,X)$, then so does any set aT for $a \in G$ (this is also clear from the fact that the left multiplication by an element of G induces an automorphism of the graph $C(G,X)$).

For the sake of brevity, we will say that a Cayley graph $C(G,X)$ has the *largest clique intersection* property (and we will be using the acronym *LCI*) if any two cliques of largest cardinality in $C(G,X)$ (shortly, *largest cliques*) have a nonempty intersection *LCI*) if any two cliques of largest cardinality in $C(G,X)$ (shortly, *largest cliques*) have a nonempty intersection.

Let $C(G,X)$ be a graph with the LCI property and let $S \subset G$ induce a largest clique in $C(G,X)$. Then, for each $a \in G$, the set aS induces a largest clique as well. The intersection property implies that $aS \cap S \neq \emptyset$ for each $a \in G$. The latter is equivalent to saying that $a \in SS^{-1}$ for every

$a \in G$, or briefly, $G = SS^{-1}$. We see that if S induces a largest clique in a Cayley graph $C(G, X)$ in which every two largest cliques meet, then $S^{-1}S \subset X^*$ and $SS^{-1} = G$. The converse is not true in general: Even if such a set S exists in $C(G, X)$, apart from the sets aS there may well be other sets inducing largest cliques in the graph, and these may violate the LCI property.

We now turn to our extremal problem of determining the smallest possible size of a largest clique in Cayley graphs with the LCI property. For any graph Γ let n_Γ be its order and let c_Γ denote its *clique number*, i.e., the number of vertices in a largest clique in Γ.

Let $S \subset G$ induce a largest clique in a Cayley graph $\Gamma = C(G, X)$. Without loss of generality we may assume that S contains the unit element of the group, i.e., $1 \in S$. For every $a \in G$ we introduce the set $S(a) = \{(r, s) \in S \times S;\ rs^{-1} = a\}$, and let $\sigma(a) = |S(a)|$. The system $\{S(a)\}_{a \in G}$ is clearly a partition of $S \times S$ (note that, in general, some of the sets $S(a)$ may be empty). Therefore,

$$\sum_{a \in G} \sigma(a) = |S|^2 = c_\Gamma^2 \,. \tag{1}$$

Observe that for the unit element we have $|S(1)| = |S|$, and so $\sigma(1) = c_\Gamma$. Now, if the graph Γ has the LCI property, then $SS^{-1} = G$, which implies that $\sigma(a) \geq 1$ for *every* element $a \in G$. From (1) we then immediately obtain:

Lemma 1. *Let $\Gamma = C(G, X)$ be a Cayley graph (of a nontrivial group) with the LCI property. Then $c_\Gamma > \sqrt{n_\Gamma}$.*

This lower bound on the clique number can be improved in some cases. Let Δ_Γ denote the valency of the Cayley graph $\Gamma = C(G, X)$; clearly $\Delta_\Gamma = |X|$.

Lemma L.*et $\Gamma = C(G, X)$ with $n_\Gamma \geq 3$ have the LCI property and let $\Delta_\Gamma \leq 2c_\Gamma - 3$. Then $c_\Gamma > \sqrt{2n_\Gamma}$.*

Proof: Let $S \subset G$ induce a largest clique in Γ and let $1 \in S$. We show that our assumptions imply $\sigma(a) \geq 2$ for every $a \in G$. Indeed, take an $a \in G$, $a \neq 1$. Since $SS^{-1} = G$, there exist $r_1, r_2 \in S$ such that $a = r_1 r_2^{-1}$, and so $(r_1, r_2) \in S(a)$. Consider the sets $X_i = \{x \in X;\ r_i x \in S\}$ for $i = 1, 2$; note that $|X_i| = c_\Gamma - 1$. Using the valency assumption we obtain $|X_1 \cup X_2| \leq |X| = \Delta_\Gamma \leq 2c_\Gamma - 3$. Therefore, $|X_1 \cap X_2| \geq 1$. Let $y \in X_1 \cap X_2$. Then, $r_i y \in S$ and $(r_1 y)(r_2 y)^{-1} = r_1 r_2^{-1} = a$. It follows that also $(r_1 y, r_2 y) \in S(a)$, and we have $\sigma(a) \geq 2$ for each $a \in G$, $a \neq 1$. Substituting this into (1) and taking into account that $\sigma(1) = c_\Gamma$ yields $c_\Gamma > \sqrt{2n_\Gamma}$ for $n_\Gamma \geq 3$. □

Another source of better lower bounds comes from special choice of the set S. Let $C(G,X)$ be a Cayley graph with the LCI property and assume it is not complete. Clearly, if $S \subset G$ induces a largest clique in $C(G,X)$ then S cannot be a subgroup of G. This suggest to consider unions of cosets of some subgroup of G as good candidates for S. For the sake of simplicity we confine ourselves to unions of two cosets.

Lemma 3. *Let $\Gamma = C(G,X)$ be a Cayley graph with the LCI property. Assume that a largest clique in Γ is induced by the set S of the form $S = Hg \cup Hh$ where H is a subgroup of G and $g, h \in G$. Then, $c_\Gamma \geq \lfloor\sqrt{2n_\Gamma}\rfloor$.*

Proof: We use the notation introduced before Lemma 1. Let $a \in H$ be an arbitrary element. For every $b \in S = Hg \cup Hh$ we have $ab \in S$ and $b^{-1} \in S^{-1}$. The fact that $a = (ab)b^{-1}$ now implies that $\sigma(a) = |S(a)| \geq |S|$ for every $a \in H$. By (1),

$$c_\Gamma^2 = \sum_{a\in H} \sigma(a) + \sum_{a\in G\setminus H} \sigma(a) \geq |H||S| + |G \setminus H|.$$

Since $|S| = 2|H| = c_\Gamma$, it follows that $c_\Gamma^2 \geq c_\Gamma^2/2 + (n - c_\Gamma)$, and hence $c_\Gamma \geq \lfloor\sqrt{2n_\Gamma}\rfloor$. □

As we shall see in the next section, this lower bound is best possible for infinitely many values of n_Γ in the class of Cayley graphs where a largest clique is induced by a union of two cosets.

3. The construction

Let $GF(q)$ be the Galois field of order $q = p^\alpha \equiv 3 \pmod 4$ where $p \geq 7$ is prime, and let d be a fixed primitive element of $GF(q)$. Let G be the (obvious) index 2 subgroup of the 1-dimensional affine group on $GF(q)$ corresponding to the even powers of d. More formally, G consists of all transformations $f : GF(q) \to GF(q)$ such that $f(x) = d^{2k}x + b$ where k is an integer and $b \in GF(q)$. Observe that $|G| = q(q-1)/2$. Let $H = Stab_G(0)$ be the subgroup of G which fixes the zero element of $GF(q)$, that is, $H = \{g;\ g(x) = d^{2k}x\}$. Clearly, $|H| = (q-1)/2$. Further, let $h \in G$ be the transformation $h(x) = x + d$ where d is the fixed primitive element of the field; note that $h \notin H$. Consider the set $S = H \cup Hh = \{g;\ g(x) = d^{2k}(x + \delta d),\ \delta \in \{0,1\}\}$. It follows that $S^{-1} = H \cup h^{-1}H = \{g;\ g(x) = d^{2k}x - \delta d,\ \delta \in \{0,1\}\}$. For the product of these sets we have $S^{-1}S = H \cup Hh \cup h^{-1}H \cup h^{-1}Hh$, or explicitly, $S^{-1}S = \{g;\ g(x) = d^{2k}(x + \delta d) - \delta' d,\ \delta, \delta' \in \{0,1\}\}$. For each k, $0 < k < (q-1)/2$ we thus have 4 transformations in $S^{-1}S$ with coefficient d^{2k} at x, and only three of them for $k = 0$; it follows that $|S^{-1}S| = 2q - 3$. Now let $X^* = S^{-1}S$ and let $X = X^* \setminus \{id\}$ where id is the identity element of G. The set X is obviously a symmetric ($X^{-1} = X$) and unit-free subset of G. We therefore may define the Cayley graph $\Gamma_q = C(G, X)$.

In the following series of auxiliary result we investigate the properties of Γ_q that are related to its largest cliques.

Lemma 4. *The set S is a largest clique in Γ_q.*

Proof: A subset $T \subset G$ is a clique in Γ_q if and only if $T^{-1}T \subset X^*$. Thus, by the definition of X, our set S is a clique in Γ_q. Clearly, $|S| = q-1$. We show that $|T| \leq q-1$ for any other clique T in Γ_q.

Let T be a clique in Γ_q. Suppose that T contains (for some integer k) three different transformations f_i such that $f_i(x) = d^{2k}x + b_i$, $1 \leq i \leq 3$. By our assumption $T^{-1}T \subset X^*$ we have $f_i^{-1}f_j \in X$. But $f_i^{-1}f_j(x) = x + d^{-2k}(b_j - b_i)$, and the only transformations in X with coefficient 1 at x and non-zero shift are $h(x) = x + d$ and $h^{-1}(x) = x - d$. Therefore for every i, j, $1 \leq i, j \leq 3$ we have $d^{-2k}(b_j - b_i) = \pm d$. It is easy to check that three distinct b_i's cannot satisfy this condition if the characteristic of the field is $\neq 3$ (which is true in our case). Hence every even power of d gives rise to no more than two transformations in T, and so $|T| \leq q-1$. (As a by-product, we see that if $f_1(x) = d^{2k}x + b_1$ and $f_2(x) = d^{2k}x + b_2$ are in a clique T then, without loss of generality, $b_2 = b_1 + d^{2k+1}$.) □

Lemma 5. *If T is a largest clique in Γ_q then $T = K \cup Kh$ for a suitable subset $K \subset G$, $|K| = (q-1)/2$.*

Proof: Let T be a clique in Γ_q such that $|T| = q-1$. The preceding proof shows that for every k such that $0 \leq k < (q-1)/2$ there are exactly two elements c_k and c'_k such that T contains the transformations $f_k(x) = d^{2k}x + c_k$ and $f'_k(x) = d^{2k}x + c'_k$. By the concluding remark of that proof, we may assume that $c'_k = c_k + d^{2k+1}$, which is equivalent to saying that $f'_k = f_k h$. Now, denoting the set of the transformations f_k by K we see that $Kh = \{f'_k;\ f_k \in K\}$, and thus $T = K \cup Kh$. □

Lemma 6. *Let T be a largest clique in Γ_q. If $id \in T$ and $h \in T$ then $T = S$.*

Proof: According to Lemma 5, $T = K \cup Kh$ where K is a suitable set of transformations of the form $f_k(x) = d^{2k}x + c_k$, $0 \leq k < (q-1)/2$. To prove our statement it is sufficient to show that $\{id, h\} \subset T$ implies $c_k = 0$ for all k, $0 \leq k < (q-1)/2$. (Indeed, if this is the case, then $K = H$ and so $T = S$.)

Take an arbitrary but fixed k such that $0 \leq k < (q-1)/2$ and consider the set of transformations $M = \{f_k, f_k h, h^{-1}f_k, h^{-1}f_k h\}$. By our assumption we have $\{id, h^{-1}\} \subset T^{-1}$, and therefore $M \subset T^{-1}T \subset X^*$ (the last inclusion holds because T is a clique). Starting from $f_k(x) = d^{2k}x + c_k$, an easy computation yields $f_k h(x) = d^{2k}x + c_k + d^{2k+1}$, $h^{-1}f_k(x) = d^{2k}x + c_k - d$, and finally $h^{-1}f_kh(x) = d^{2k}x + c_k + d^{2k+1} - d$. Since all these transformations are in X^* and they have the same coefficient d^{2k} at x, the set M is equal to the set of the transformations g of the form $g(x) = d^{2k}(x+\delta d) - \delta' d$, $\delta, \delta' \in \{0,1\}$ (see the definition of the set $X^* = S^{-1}S$). Consequently, the corresponding sets of shift coefficients are equal, that is,

$$\{c_k, c_k + d^{2k+1}, c_k - d, c_k + d^{2k+1} - d\} = \{0, d^{2k+1}, -d, d^{2k+1} - d\}. \quad (2)$$

If $d^{2k} \neq \pm 1$ then each of the sets in (1) contains 4 distinct elements. Clearly, if (1) holds then the sum of the 4 elements in each of the sets is the same. However, this is possible only if $4c_k = 0$, which implies that $c_k = 0$ (recall that the characteristic of our field is ≥ 7). If $d^{2k} \in \{1, -1\}$ then each set in (1) has exactly three distinct elements. Their equality then implies (by a similar argument) that $3c_k = 0$, and so $c_k = 0$ again. Lemma 6 follows. □

Lemma 7. *Every largest clique in Γ_q has the form gS for a suitable $g \in G$.*

Proof: Let T be a largest clique in Γ_q. By Lemma 5, $T = K \cup Kh$ for some $K \subset G$. Take an arbitrary $g \in K$ and consider the clique $g^{-1}T = g^{-1}K \cup g^{-1}Kh$. Since $id \in g^{-1}K$ and $h \in g^{-1}Kh$, we see that $g^{-1}T$ contains both id and h. Invoking Lemma 6, $g^{-1}T = S$, and hence $T = gS$. □

Now we are ready to prove the main result of this section.

Theorem 1. *Any two largest cliques of the Cayley graph $\Gamma_q = C(G, X)$ have a nonempty intersection.*

Proof: It follows from Lemma 7 that all largest cliques in Γ_q have the form gS, $g \in G$. By transitivity of Γ_q, it is sufficient to prove that $gS \cap S \neq \emptyset$ for every $g \in G$. The latter is easily seen to be equivalent to saying that $SS^{-1} = G$. The inclusion $SS^{-1} \subset G$ is trivial. To show that the reverse is also true, take an arbitrary $g \in G$, $g(x) = d^{2k}x + b$. If $b = 0$ then $g \in H \subset SS^{-1}$, so we may assume $b \neq 0$. Since d is a primitive element of our field $GF(q)$ and $q \equiv 3 \pmod 4$, each such b can be written in the form $b = \lambda d^{2m+1}$ where $\lambda = \pm 1$. But then,

$$g(x) = d^{2k}x + \lambda d^{2m+1} = d^{2m}(d^{2(k-m)}x + \lambda d) = g_2 h^{\lambda} g_1(x)$$

where $g_1(x) = d^{2(k-m)}x$ and $g_2(x) = d^{2m}x$. Notice that $g_1, g_2 \in H$, and therefore $g = g_2 h^{\lambda} g_1 \in HhH \cup Hh^{-1}H \subset SS^{-1}$. The proof is complete. □

We have seen that the Cayley graph Γ_q constructed above has $n = q(q-1)/2$ vertices ($q = p^{\alpha}$, $p \geq 7$ a prime) and its largest clique has size $|S| = q - 1 = \lfloor\sqrt{2n}\rfloor$. This shows that the lower bound obtained in Lemma 3 is best possible (when restricted to the "two-coset" constructions) for infinitely many values of n. In general, we do not know of any family of Cayley graphs Γ with the LCI property with $c_\Gamma = c\sqrt{n_\Gamma}$, $c < \sqrt{2}$. Note that by Lemma 1, $c > 1$.

4. Application to independence ratio

The box product (cartesian product) $\Gamma \square \Gamma'$ of two graphs Γ and Γ' is well known and is defined by $(V(\Gamma) \times V(\Gamma'), E)$ with $E = \{(u,x)(v,y) \in V(\Gamma) \times V(\Gamma') :$ either $u = v$ and $xy \in E(\Gamma')$, or $uv \in E(\Gamma)$ and $x = y\}$. It is well known - and easy to see - that this product is commutative and associative (up to isomorphism). We define $\Gamma^1 = \Gamma$ and, for $k > 1$, put $\Gamma^k = \Gamma \square \Gamma^{k-1}$. We denote by $\alpha(\Gamma)$ the *independence number* of Γ. The *independence ratio* of Γ is the fraction $i(\Gamma) = \alpha(\Gamma)/|V(\Gamma)|$, and the *ultimate independence ratio* of Γ is defined as $I(\Gamma) = \lim_{k\to\infty} i(\Gamma^k)$ (the limit is known to exist, see, for example, [2]).

The work of [2] shows that $I(\Gamma) = i(\Gamma)$ whenever $\Gamma = C(G,X)$ is a Cayley graph such that X is setwise invariant under all inner automorphisms of the group G. In particular, $I(\Gamma) = i(\Gamma)$ for every Cayley graph Γ of an abelian group. This fact gave rise to a working hypothesis of Hahn, Hell and Poljak, claiming that the equality $I(\Gamma) = i(\Gamma)$ might be true for *any* Cayley graph Γ.

As an application of results of the preceding section, we show that there are counterexamples to this working hypothesis.

Corollary 1. *There exist infinitely many Cayley graphs* Γ *with* $I(\Gamma) < i(\Gamma)$.

Proof: Consider the complements of the graphs constructed previously in Theorem 1; these are Cayley graphs again, and the LCI property translates to the corresponding property of largest independent sets. But it is shown in [2] that if any two largest independent sets intersect non-trivially in a graph Γ of order n with independence number $\alpha < n$, then $I(\Gamma) \le \frac{\alpha-1}{n-1} < i(\Gamma)$.□

References

[1] J.A. Gallian and D. Witte, A survey: Hamiltonian cycles in Cayley graphs, *Discrete Math.* **51** (1984), 293-304.

[2] G. Hahn, P. Hell and S. Poljak, The ultimate independence ratio of a graph, *European J. of Combinatorics* (to appear).

[3] P. Hell, X. Yu and H. Zhou, Independence ratio of graph powers, *Preprint* (1991).

[4] B. McKay and C. Praeger, Vertex-transitive graphs which are not Cayley graphs I and II, *Preprint* (1993), submitted.