Max cliques in gcd-graphs

Aditya Siripuram

CONTENTS

Abstract

Max cliques for arbitrary N

I. Setup

Given N, and a set of divisors $\mathcal{D}$ of N, construct the graph $\mathscr{G}(\mathcal{D})$ (or $\mathscr{G}_N(\mathcal{D})$ if N is not apparent from context) with vertices the elements of $\mathbb{Z}_N$, and an edge (i, j) whenever

$$(i - j, N) \in \mathcal{D}.$$

Here $(i - j, N)$ denotes the greatest common divisor (GCD) of $i - j$ and N. Interested in understanding

- Size of max cliques in $\mathscr{G}$
- Conditions on $\mathcal{D}$ under which the clique and chromatic number are equal

Both questions are easy when N prime power (next section), attempt to generalize to arbitrary N via the Chinese remainder theorem. Literature review would include [1] [2] [3]. These gcd-graphs are also called Cayley graphs, and unitary cayley graphs when the divisor set is a singleton. Results in literature on unitary cayley graphs include those on perfectness, clique number etc, of such graphs, and the complements of such graphs. Some works also explore the relation to ramanujan graph and expander properties [4]. Not much work on gcd-graphs when the divisor sets is of size more than two.

Some notations -

- Chromatic number of $\mathscr{G}$ is $\chi(\mathscr{G})$
- Clique number/size of max clique in $\mathscr{G}$ is $\mu(\mathscr{G})$
- for a tuple $(i_1, i_2, \ldots)$ we denote by $(i_l)_{l \in L}$ the tuple $(i_{l_1}, i_{l_2}, \ldots)$ where $L = \{l_1, l_2, \ldots\}$.

II. Prime power case

Suppose $N = p^M$ is a prime power. The set of divisors $\mathcal{D}$ is some set of powers of p, which we will find convenient to write as $p^{\mathcal{L}}$. Here $\mathcal{L} \subseteq [0 : N-1]$ is the powers of p that make up $\mathcal{D}$.

We use the base p expansions of the numbers in $\mathbb{Z}_N$ and the relation between the digits of the expansions and the greatest common divisor. The elementary, technical result we need is

Lemma 1: For $z \in \{0, 1, 2, \ldots, p^M - 1\}$ let $z = \sum_{j=0}^{M-1} a_j p^j$, where $a_j \in [-(p-1) : p-1]$. Let $i = \min\{j : a_j \neq 0\}$, i.e., i is the index of the first nonzero coefficient among the a_j. Then $(z, p^M) = p^i$.

This may not hold when the coefficients a_j are not constrained to lie in $[-(p-1) : p-1]$. Observe in particular that if for some s the expansion of z does not involve the coefficient corresponding to p^s, i.e. if $a_s = 0$, then $(z, p^M) \neq p^s$.

Proof: Clearly, $p^i \mid z$ and so $(z, p^M) \geq p^i$. Suppose $(z, p^M) = p^t$ for some $t > i$ and write

$$z = \sum_{j=0}^{M-1} a_j p^j = \sum_{j=0}^{t-1} a_j p^j + \sum_{j=t}^{M-1} a_j p^j. \tag{1}$$

Now, p^t divides the second term in (1), but it does not divide the first term, for the absolute value of the first term is

$$\left| \sum_{j=0}^{t-1} a_j p^j \right| \leq \sum_{j=0}^{t-1} |a_j| p^j \leq (p-1) \sum_{j=0}^{t-1} p^j = p^t - 1,$$

and so is not divisible by p^t. Thus we cannot have $p^t \mid z$ for $t > i$. ■

Suppose $\mathbf{i}, \mathbf{j} \in \mathbb{Z}_N$ have their base$-p$ expansions as

$$\mathbf{i} = \sum_{m=0}^{M-1} i_m p^m, \quad \mathbf{j} = \sum_{m=0}^{M-1} j_m p^m,$$

where i_m, j_m are digits which take values in $\{0, 1, 2, \ldots, p-1\}$ Suppose $(\mathbf{i}, \mathbf{j})$ is an edge in $\mathscr{G}$, i.e. $(\mathbf{i} - \mathbf{j}, N) \in p^{\mathcal{L}}$. Considering $\mathbf{i} - \mathbf{j} = \sum (i_m - j_m) p^m$, we observe that we cannot have

$$i_m = j_m \text{ for all } m \in \mathcal{L},$$

because then $(\mathbf{i} - \mathbf{j}, N) \notin \mathcal{D}$ by Lemma 1. Thus whenever $(\mathbf{i}, \mathbf{j})$ is an edge, $(i_m)_{m \in \mathcal{L}} \neq (j_m)_{m \in \mathcal{L}}$. So $(i_m)_{m \in \mathcal{L}}$ forms a *coloring* of the graph $\mathscr{G}$. In particular, the number of colors used is $p^{|\mathcal{L}|}$, and $\chi(\mathscr{G}) \leq p^{|\mathcal{L}|}$. We will next construct a clique of size $p^{|\mathcal{L}|}$, thus establishing that $\chi(\mathscr{G}) = \mu(\mathscr{G}) = p^{|\mathcal{L}|}$.

Construct the clique $(\mathbf{i}_1, \mathbf{i}_2, \ldots)$ from their base$-p$ expansions

$$\mathbf{i}_k = \sum_{m=0}^{M-1} i_{mk} p^m,$$

By setting $(i_{mk})_{k \in \mathcal{L}^c}$ to zero, and $(i_{mk})_{k \in \mathcal{L}}$ to all possible distinct $|\mathcal{L}|-$tuples. This is a clique, and of size $p^{|\mathcal{L}|}$. Thus the chromatic number and clique number are both equal to $p^{|\mathcal{L}|}$, *for any* $\mathcal{D} = p^{\mathcal{L}}$.

1) Examples: Let $N = 2^4$ and suppose $\mathcal{D}(h) = \{2^1\}$, a singleton. If we are to have $\mathbf{i}_k - \mathbf{i}_\ell \in \mathcal{Z}(h)$ then we need

$$(\mathbf{i}_k - \mathbf{i}_\ell, 2^4) = 2,$$

The situation is described more completely in the display

$$\begin{array}{cc|c|cc}
 & 2^0 & 2^1 & 2^2 & 2^3 \\
\mathbf{i}_0 & i_{00} & i_{01} & i_{02} & i_{03} \\
\mathbf{i}_1 & i_{10} & i_{11} & i_{12} & i_{13} \\
\mathbf{i}_2 & i_{20} & i_{21} & i_{22} & i_{23} \\
\vdots & \vdots & \vdots & \vdots & \vdots
\end{array}$$

where we mark (box) the column of digits corresponding to the zero-set divisors, in this case a single column. The map $\mathbf{i}_k \mapsto i_{mk}$ is a coloring, and a max clique is given by

$$\begin{array}{cc|c|cc}
 & 2^0 & 2^1 & 2^2 & 2^3 \\
\mathbf{i}_0 & 0 & 0 & 0 & 0 \\
\mathbf{i}_1 & 0 & 1 & 0 & 0
\end{array}$$

III. Extensions

Consider generalizing the arguments described in the previous section to the case when N is not a prime power. For now assume $N = P_1 P_2$, where $P_1 = p_1^{M_1}$ and $P_2 = p_2^{M_2}$ are prime powers (we assume $p_1 < p_2$), and consider the isomorphism given by the Chinese remainder theorem

$$\mathbf{i} \leftrightarrow (\mathbf{i} \mod P_1, \; \mathbf{i} \mod P_2)\,.$$

Constructing base$-p_1$ and base$-p_2$ expansions respectively for $\mathbf{i} \mod P_1$ and $\mathbf{i} \mod P_2$, we could expect a procedure similar to that of Section II to work. Every $\mathbf{i} \in \mathbb{Z}_N$ corresponds to a tuple of the form

$$\left(\sum_{m=0}^{M_1-1} i_{1,m} p_1^m, \sum_{m=0}^{M_2-1} i_{2,m} p_2^m \right).$$

Here $i_{1,m}$ are base$-p_1$ digits taking values in $\{0, 1, 2 \ldots, p_1 - 1\}$ and $i_{2,m}$ are base$-p_2$ digits taking values in $\{0, 1, 2 \ldots, p_2 - 1\}$. Note the summation runs upto $M_1 - 1$ (and $M_2 - 1$ for the second element of the tuple). It will be convenient to let the summation run up to M_1 (and M_2 for the second element of the tuple) by defining i_{1,M_1} and i_{2,M_2}. We allow for i_{1,M_1} and i_{2,M_2} to be arbitrary integers, while noting that we completely ignore their values (or set them to 0) while constructing $\mathbf{i}$ from the digits $i_{1,m}$ and $i_{2,m}$. Thus the number of possible values of $i_{1,m}$ is thus p_1 (as they are base p_1 digits), so long as $m < M_1$. Summarizing,

$$N_{k,m} := \text{ Number of possible } i_{k,m} = \begin{cases} p_k \text{ if } m < M_1 \\ \infty \text{ otherwise .} \end{cases}$$

We can think of $N_{k,m}$ as the number of colors used in the map $\mathbf{i} \mapsto i_{k,m}$.

The question of when the clique number $\mu(\mathscr{G})$ and chromatic number $\chi(\mathscr{G})$ are equal depends on the structure of $\mathcal{D}$ involved, unlike in Section II. Start with the singleton case $\mathcal{D} = \{p_1^a p_2^b\}$.

For $\mathbf{i}$ and $\mathbf{j}$ to have an edge in $\mathscr{G}$, we must have

$$(\mathbf{i} - \mathbf{j} \mod P_1, P_1) = p_1^a, \text{ and } (\mathbf{i} - \mathbf{j} \mod P_2, P_2) = p_2^b.$$

So for $\mathbf{i}$ and $\mathbf{j}$ to have an edge in $\mathscr{G}$, we must have $i_{1,a} \neq j_{2,a}$ *and* $i_{1,b} \neq j_{2,b}$. Thus the maps $\mathbf{i} \mapsto i_{1,a}$ and $\mathbf{i} \mapsto i_{1,a}$ are both colorings of $\mathscr{G}$, and so

$$\chi(\mathscr{G}) \leq \min\{N_{1,m}, N_{2,m}\} = \begin{cases} p_1 \text{ if } a < M_1 \\ p_2 \text{ otherwise.} \end{cases}$$

Similar to the above, when $a < M_1$ we can construct a clique of size p_1 as

	p_1^0	p_1^1	$\ldots$	p_1^a	$\ldots$	p_2^0	p_2^1	$\ldots$	p_2^b	$\ldots$
$\mathbf{i}_0$	0	0	$\ldots$	0	$\ldots$	0	0	$\ldots$	0	$\ldots$
$\mathbf{i}_1$	0	0	$\ldots$	1	$\ldots$	0	0	$\ldots$	1	$\ldots$
$\mathbf{i}_2$	0	0	$\ldots$	2	$\ldots$	0	0	$\ldots$	2	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ldots$	0	0	$\ldots$	$\vdots$	$\ldots$
$\mathbf{i}_{p_1-1}$	0	$\ldots$	0	$p_1 - 1$	$\ldots$	0	0	$\ldots$	$p_1 - 1$	$\ldots$

Thus the clique number and chromatic number are both equal to p_1. Similarly when $a = M_1$ we can construct a clique of size p_2 as

$$\begin{array}{c|ccc|cccc|c}
 & p_1^0 & p_1^1 & \dots & p_2^0 & p_2^1 & \dots & p_2^b & \dots \\
\mathbf{i}_0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & \dots \\
\mathbf{i}_1 & 0 & 0 & \dots & 0 & 0 & \dots & 1 & \dots \\
\mathbf{i}_2 & 0 & 0 & \dots & 0 & 0 & \dots & 2 & \dots \\
\vdots & \vdots & \vdots & \vdots & 0 & 0 & \dots & \vdots & \dots \\
\mathbf{i}_{p_2-1} & 0 & \dots & 0 & 0 & 0 & \dots & p_2-1 & \dots
\end{array}$$

Remark 1: Incidentally, the case when $\mathcal{D}$ is a singleton (or the complement of a singleton) has been very well studied in combinatorics as unitary Cayley graphs and their complements [5] [4] [1], to name a few. The fact that the clique and chromatic number are equal when $\mathcal{D}$ is a singleton can easily be seen from a similar property of unitary Cayley graphs- see for e.g. [1, Theorem 1].

Remark 2: We can easily see why the expressions are different for the case $a = M_1$. In this case, $\mathcal{D} = \{p_1^{M_1} p_2^b\}$, and $\mathbf{i}, \mathbf{j}$ have an edge when

$$(\mathbf{i} - \mathbf{j}, p_1^{M_1} p_2^{M_2}) = p_1^{M_1} p_2^b.$$

For this we need

$$\mathbf{i} - \mathbf{j} = 0 \mod P_1 \text{ and } (\mathbf{i} - \mathbf{j}, p_2^{M_2}) = p_2^b$$

The graph $\mathscr{G}_N(\{p_1^{M_1} p_2^b\})$ is equivalent to $\mathscr{G}_{P_2}(\{p_2^b\})$, which we know has a clique size of p_2.

Now suppose $\mathcal{D}$ is of size 2, say $\mathcal{D} = \{p_1^{a_1} p_2^{b_1}, p_1^{b_1} p_2^{b_2}\}$. Even this case gets a bit involved depending on the relationship between the exponents. First consider the case $a_1 < a_2, b_1 < b_2$. For $\mathbf{i}, \mathbf{j}$ to have an edge in $\mathscr{G}$,

$$(i_{1,a_1}, i_{1,a_2}) \neq (j_{1,a_1}, j_{2,a_2}) \text{ and } (i_{2,b_1}, i_{2,b_2}) \neq (j_{2,b_1}, j_{2,b_2}).$$

Thus $\mathbf{i} \mapsto (i_{1,a_1}, i_{1,a_2})$ and $\mathbf{i} \mapsto (i_{2,b_1}, i_{2,b_2})$ form colorings of $\mathscr{G}$, and

$$\chi(\mathscr{G}) \leq \min\{N_{1,a_1} N_{1,a_2}, N_{2,b_1} N_{2,b_2}\} = \begin{cases} p_1^2 \text{ if } a_2 < M_1 \\ p_1 p_2 \text{ otherwise.} \end{cases}$$

As in the singleton case, we can construct a clique with size equal to $\chi(\mathscr{G})$. For $a_2 < M_2$ a clique is given by

	$\dots$	$p_1^{a_1}$	$p_1^{a_2}$	$\dots$	$\dots$	$p_2^{b_1}$	$p_2^{b_2}$	$\dots$
$\mathbf{i}_0$	$\dots$	0	0	$\dots$	$\dots$	0	0	$\dots$
$\mathbf{i}_1$	$\dots$	0	1	$\dots$	$\dots$	0	1	$\dots$
$\mathbf{i}_2$	$\dots$	0	2	$\dots$	$\dots$	0	2	$\dots$
$\vdots$	$\dots$	$\vdots$	$\vdots$	$\dots$	$\dots$	$\vdots$	$\vdots$	$\dots$
$\mathbf{i}_{p_1-1}$	$\dots$	0	p_1-1	$\dots$	$\dots$	0	p_1-1	$\dots$
$\mathbf{i}_{p_1}$	$\dots$	1	0	$\dots$	$\dots$			$\dots$
$\mathbf{i}_{p_1+1}$	$\dots$	1	1	$\dots$	$\dots$	$\vdots$	$\vdots$	$\dots$
$\vdots$	$\dots$	$\vdots$	$\vdots$	$\dots$	$\dots$	$\vdots$	$\vdots$	$\dots$
$\mathbf{i}_{p_1^2-1}$	$\dots$	p_1-1	p_1-1	$\dots$	$\dots$			$\dots$

Next suppose $a_1 = a_2$ and $b_1 < b_2$. Similar to the above, for $\mathbf{i}, \mathbf{j}$ to have an edge we need the condition

$$i_{1,a_1} \neq j_{1,a_1} \text{ and } (i_{2,b_1}, i_{2,b_2}) \neq (j_{2,b_1}, j_{2,b_2}).$$

The maps $\mathbf{i} \mapsto i_{1,a_1}$ and $\mathbf{i} \mapsto (i_{2,b_1}, i_{2,b_2})$ form colorings of $\mathscr{G}$,

$$\chi(\mathscr{G}) \leq \min\{N_{1,a_1}, N_{2,b_1}N_{2,b_2}\} = \begin{cases} p_1 \text{ if } a_1 < M_1 \\ p_2^2 \text{ otherwise.} \end{cases}$$

A max clique can be constructed as before with these sizes, and hence $\chi(\mathscr{G}) = \mu(\mathscr{G})$.

Example clique for the case $\mathcal{D} = \{p_1^a p_2^{b_1}, p_1^a p_2^{b_2}\}$.

	$\dots$	p_1^{a}	$\dots$	$\dots$	$p_2^{b_1}$	$p_2^{b_2}$	$\dots$
$\mathbf{i}_0$	$\dots$	0	$\dots$	$\dots$	0	0	$\dots$
$\mathbf{i}_1$	$\dots$	1	$\dots$	$\dots$	0	1	$\dots$
$\mathbf{i}_2$	$\dots$	2	$\dots$	$\dots$	0	2	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\dots$	$\dots$	$\vdots$	$\vdots$	$\dots$
$\mathbf{i}_{p_1-1}$	$\dots$	p_1-1	$\dots$	$\dots$	0	p_1-1	$\dots$

Now for the case when $b_1 = b_2$, and $a_1 \leq a_2$, the clique size depends on whether p_1^2 is bigger or smaller than p_2.

$$\chi(\mathscr{G}) \leq \min\{N_{1,a_1}N_{1,a_2}, N_{2,b_1}\} = \begin{cases} \min\{p_1^2, p_2\} \text{ if } a_1, a_2 < M_1, b_1 < M_2 \\ p_1^2 \text{ if } b_1 = M_2 \\ p_2 \text{ if } a_2 = M_1. \end{cases}$$

In all cases, cliques can be constructed similar to above. For e.g. if $a_1, a_2 < M_1, b_1 < M_2$ and $p_1^2 < p_2$, a clique is constructed as

$$\begin{array}{ccccc|cccc}
\cdots & p_1^{a_1} & p_1^{a_2} & \cdots & \cdots & p_2^{b_1} & \cdots \\
\cdots & 0 & 0 & \cdots & \cdots & 0 & \cdots \\
\cdots & 0 & 1 & \cdots & \cdots & 1 & \cdots \\
\cdots & 0 & 2 & \cdots & \cdots & 2 & \cdots \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \cdots \\
\cdots & 1 & 0 & \cdots & \cdots & p_1 & \cdots \\
\cdots & 1 & 1 & \cdots & \cdots & p_1+1 & \cdots \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \cdots \\
\cdots & p_1-1 & p_1-1 & \cdots & 0 & p_1^2-1 & \cdots
\end{array}$$

Finally, consider the case $a_1 < a_2$, $b_2 < b_1$. We will argue that for this case, any max clique has in $\mathscr{G}(\{p_1^{a_1}p_2^{b_1}, p_1^{a_2}p_2^{b_2}\})$ is a max clique in either $\mathscr{G}(\{p_1^{a_1}p_2^{b_1}\})$ or $\mathscr{G}(\{p_1^{a_1}p_2^{b_1}\})$.

Suppose $\mathbf{i}, \mathbf{j}$ have an edge in $\mathscr{G}(\{p_1^{a_1}p_2^{b_1}, p_1^{a_2}p_2^{b_2}\})$, and that $i_{1,a_1} \neq j_{1,a_1}$, for example shown in Fig 1.

$$\begin{array}{ccccc|cccc}
 & \cdots & p_1^{a_1} & p_1^{a_2} & \cdots & \cdots & p_2^{b_2} & p_2^{b_1} & \cdots \\
\mathbf{i} & 0 & 0 & * & \cdots & \cdots & i_{2,b_2} & i_{2,b_1} & \cdots \\
\mathbf{j} & 0 & 1 & * & \cdots & \cdots & j_{2,b_2} & j_{2,b_1} & \cdots
\end{array}$$

Fig. 1

Then by Lemma 1, $i_{2,b_2} = j_{2,b_2}$ and $i_{2,b_1} \neq j_{2,b_1}$. This is the basis for our next observation.

Lemma 2: Suppose $N = p_1^{M_1}p_2^{M_2}$ and $\mathcal{D} = \{d_1, d_2\}$ with

$$d_1 = p_1^{a_1}p_2^{b_1}, \quad d_2 = p_1^{a_2}p_2^{b_2} \quad \text{with } a_1 < a_2, b_2 < b_1.$$

Then any clique in $\mathscr{G}_N(\mathcal{D})$ is a clique in either $\mathscr{G}_N(\{d_1\})$ or $\mathscr{G}_N(\{d_2\})$.

In particular when $\gcd(d_1, d_2) = 1$, *Proof:* Consider any max clique, and construct its representation as pair consisting of base$-p_1$ and base$-p_2$ expansions. Sort them lexicographically using the first element of the pair (the base $-p_1$ expansion), so that a clique is of the form

$p_1^{a_1}$	$p_1^{a_2}$	$p_2^{b_2}$	$p_2^{b_1}$
0	0	0	$\dots$
0	1	1	$\dots$
0	2	2	$\dots$
$\vdots$	$\vdots$		$\dots$
1	0	$\dots$	$\dots$
1	1	p_1+1	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\dots$
1	p_1-1		
2	0	$\dots$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\dots$
p_1-1	p_1-1	p_1^2-1	$\dots$

For two elements $\mathbf{i}, \mathbf{j}$ that are in different such row blocks, then by the observation above, we must have $i_{2,b_2} = j_{2,b_2}$. Thus as long as there are at least two row blocks, all the entries i_{2,b_2} are equal. This means each row block is of size 1, and the given max clique is a max clique for $\{p_1^{a_1} p_2^{b_1}\}$. On the other hand, we could only have one row block, which corresponds to a max clique for $\{p_1^{a_2} p_2^{b_2}\}$.

∎

Thus the clique number and chromatic number are equal, and can be derived from the singleton case.

- $\mathcal{D} = \{1, p^2, pq\}$ - clique and chromatic no unequal/ clique no does not divide product of p and q
- $\mathcal{D} = p_1^{M_1}\{p_2^{b_1}, p_2^{b_2}, \dots, \} \cup p_2^{M_2}\{p_1^{a_1}, p_1^{a_2}, \dots, \} \cup \{p_1^{a_1} p_2^{b_1}, p_1^{a_1} p_2^{b_2}, \dots\}$ - what of max cliques for CVM sets/ formed from specific structure ?

References

[1] W. Klotz and T. Sander, "Some properties of unitary Cayley graphs," *Electronic Journal of Combinatorics*, vol. 14, no. 1, p. R45, 2007.

[2] M. Bašić and A. Ilić, "On the clique number of integral circulant graphs," *Applied Mathematics Letters*, vol. 22, no. 9, pp. 1406–1411, 2009.

[3] A. Ilić and M. Bašić, "On the chromatic number of integral circulant graphs," *Computers & Mathematics with Applications*, vol. 60, no. 1, pp. 144–150, 2010.

[4] X. Liu and S. Zhou, “Spectral properties of unitary cayley graphs of finite commutative rings,” *arXiv preprint arXiv:1205.5932*, 2012.

[5] R. Akhtar, M. Boggess, T. Jackson-Henderson, I. Jiménez, R. Karpman, A. Kinzel, and D. Pritikin, “On the unitary cayley graph of a finite ring,” *the electronic journal of combinatorics*, vol. 16, no. 1, p. R117, 2009.