On a modular domination game

Sylvain Gravier∗ Mehdi Mhalla† Eric Tannier‡

November 20, 2002

Abstract

We present a generalization of the so-called σ-game, introduced by Sutner [9], a combinatorial game played on a graph, with relations to cellular automata, as well as odd domination in graphs. A configuration on a graph is an assignment of values in \{0, \ldots, p - 1\} (where \(p\) is an arbitrary positive integer) to all the vertices of \(G\). One may think of a vertex \(v\) of \(G\) as a button the player can press at his discretion. If vertex \(v\) is chosen, the value of all the vertices adjacent to \(v\) increases by 1 modulo \(p\). This defines an equivalence relation between the configurations: two configurations are in relation if it is possible to reach one from the other by a sequence of such operations. We investigate the number of equivalence classes that a given graph has, and we give formulas for trees and special regular graphs.

1 Introduction

The “modular domination game” is a combinatorial game, special cases of which were studied in terms of “σ-game”, “σ+-game” [9], [10], [3] or “mod 2 domination” [2], [1], [6]. It has strong relationship with the computation of the rank of adjacency or incidence matrices of graphs or hypergraphs over finite fields [5], [4]. It is also related to the additive cellular automata on graphs with state space a monoid [8].

For a graph \(G\) and a positive integer \(p\), a configuration is an assignment of values in \(\mathbb{Z}_p = \{0, \ldots, p - 1\}\) to all the vertices of \(G\). One may think of a vertex \(v\) in \(G\) as a button that the player can press at his discretion. If

∗CNRS, Laboratoire Leibniz, 46 avenue Félix Viallet, 38031 Grenoble Cedex, France
†INPG, Laboratoire Leibniz, 46 avenue Félix Viallet, 38031 Grenoble Cedex, France
‡UJF, Laboratoire Leibniz, 46 avenue Félix Viallet, 38031 Grenoble Cedex, France
vertex \( v \) is chosen, the value of all the vertices adjacent to \( v \) will increase by 1 modulo \( p \). Now, suppose that the opponent picks two configurations on \( G \), say \( X_s \) (the source) and \( X_t \) (the target). To win, the player has to find a sequence of moves that transforms configuration \( X_s \) into \( X_t \).

When \( p = 2 \), this game corresponds to Sutner’s \( \sigma \)-game \([9]\) \([10]\). Here, \( p \) is an arbitrary fixed positive integer, but to keep on with this notation, we speak about \( \sigma^- \)-game if the value of the neighbors of the chosen vertex increases by one, and about \( \sigma^+ \)-game if, in addition to his neighbors, the value of the chosen vertex itself increases. \( \sigma \) should be read indifferently \( \sigma^+ \) or \( \sigma^- \).

For a fixed \( p \), let us denote by \( \mathcal{C}_G \) the set of all configurations of \( G \). Consider the relation \( \alpha \) defined by \( X \alpha Y \) if the pair \((X, Y)\) is a winning pair. Clearly \( \alpha \) is an equivalence relation. We note \( \mathcal{CL}_G(\sigma) \) the set of equivalent classes of the \( \sigma \)-game in \( G \).

Thus let \( NC^+_p(G) \) denotes the number of classes of the \( \sigma^+ \) game in \( G \), that is \( |\mathcal{CL}_G(\sigma^+_p)| \). Analogously let \( NC^-_p(G) = |\mathcal{CL}_G(\sigma^-_p)| \) (we will use \( NC_p(G) \) for both games). A special interesting case is when all pairs are winning pairs, that is \( NC_p(G) = 1 \). In this case we will say that \( G \) is \( p \)-universal for the \( \sigma \)-game.

In section 2, we discuss the link between the computation of \( NC_p(G) \) and systems of linear equations in \( \mathbb{Z}/p\mathbb{Z} \). This gives us some tools to compute \( NC_p(G) \), that we use in section 3 to compute \( NC_p(G) \) for some classes of regular graphs \( G \) containing cycles and complete graphs (extending the results in \([4, 1]\)). Finally, section 4 is dedicated to the quasi-complete study of \( NC_p \) for trees (which generalizes the result in \([2]\)).

### 2 Systems of Equations over \( \mathbb{Z}/p\mathbb{Z} \)

Let \( G \) be a graph, with vertices \( \{1, \ldots, n\} \). A configuration \( X \in \mathcal{C}_G \) can be seen as an element of the group \( \mathbb{Z}_p^n \). Let \( A \) be the adjacency matrix of \( G \) (for \( i, j \in \{1, \ldots, n\} \), \( A_{i,j} = 1 \) if \( \{i, j\} \) is an edge of \( G \), otherwise \( A_{i,j} = 0 \)).

The application \( \sigma_G \), defined by \( \sigma_G(X) = AX \) (all operations are mod \( p \)) is linear over \( \mathbb{Z}_p^n \). Let \( \text{im}(\sigma_G) \) and \( \text{ker}(\sigma_G) \) be respectively the image and the kernel of \( \sigma_G \). Both are subgroups of \( \mathbb{Z}_p^n \).

It is easy to see that a pair \((X, Y)\) is winning for the \( \sigma^- \)-game if and only if there exists \( U \in \mathbb{Z}_p^n \) such that \( X + \sigma_G(U) = Y \), that is, if \( Y - X \) is in the image of \( \sigma^-_G \). And there is a similar relation for \( \sigma^+ \), replacing matrix \( A \) by \( A + I \), where \( I \) is the \( n \times n \) identity matrix. So we may speak of \( \sigma \)
instead of $\sigma^+$ or $\sigma^-$. Any equivalence class $C \in C\mathcal{L}_{G}(\sigma)$ is in consequence a translation of $\text{im}(\sigma_{G})$, let a configuration $U$ in $C$, $C = \{U + V, V \in \text{im}(\sigma_{G})\}$, and the set of equivalence classes $C\mathcal{L}_{G}(\sigma)$ is the quotient group $\mathbb{Z}_p^n / \text{im}(\sigma_{G})$.

Since $\mathbb{Z}_p^n = \text{im}(\sigma_{G}) \oplus \ker(\sigma_{G})$ we have:

**Proposition 1** For all $G$, $\ker(\sigma_{G})$ is isomorphic to $C\mathcal{L}_{G}(\sigma)$, and then $NC_p(G) = | \ker(\sigma_{G}) |$.

In consequence $NC_p$ is the number of solutions of the system of modular equations $Ax = 0 \mod p$ (or $(A + I)x = 0 \mod p$). The reader has probably already noticed that when $p$ is a prime integer, $\mathbb{Z}_p$ is a field, and any known linear algebraic algorithm finds $NC_p$. In [6], a combinatorial algorithm is written for $p = 2$, equivalent to the gaussian elimination, with a generalization to directed graphs, that makes the problem exactly equivalent to solving $Ax = 0 \mod 2$ for an arbitrary square matrix $A$. This method can be easily adapted to compute $NC_p$ for any prime $p$. Generally, the problem is equivalent to linear diophantine equations (get rid of the module by solving $Ax + pIy = 0$ - $A$ is an arbitrary integer square matrix and $x, y$ is the unknown), and the problem is treated for example in [7], using theory of lattices.

Here we try to give formula for $NC_p$, uniquely depending on combinatorial parameters of a graph, as it is done in the two following sections.

### 3 Some regular graphs

In this section, we use the principles developed in the previous one and some elementary tools from arithmetic, in order to compute $NC_p(G)$ for some classes of regular graphs.

We start with a general remark concerning regular graphs.

**Proposition 2** Let $G$ be a $\Delta$ regular graph. Then $NC_p^{-}(G) \geq \gcd(\Delta, p)$ and $NC_p^{+}(G) \geq \gcd(\Delta + 1, p)$.

**Proof.** Let $G$ be a $\Delta$ regular graph of order $n$. Let $w(Y) = \sum y_i$ for any $Y = (y_1, \ldots, y_n) \in C_G$. For any $X = (x_1, \ldots, x_n)$ and $U = (u_1, \ldots, u_n)$ in $C_G$, by linearity of $w$, we have $w(X + \sigma^{-}(U)) = w(X) + w(U).\Delta$ (respectively, $w(X + \sigma^{+}(U)) = w(X) + w(U).(\Delta + 1)$). Hence every pair $X, Y$ of configurations in the same equivalence class satisfies $w(X) = w(Y) \mod \gcd(\Delta, p)$. 

Therefore, the configurations \((i,0\ldots0)\) with \(i\in[0,\ldots,\gcd(\Delta,p)-1]\) (respectively \([0,\ldots,\gcd\Delta+1,p)-1]\)) are in different classes. \(\square\)

Now, we consider some special regular graphs \(G\) for which we compute \(NC_p(G)\). By similarity with the definition of connectivity in hypergraphs from [4], we define here the neighbor-connectivity for \(r\)-regular directed graphs. Here \(\Gamma^+(v)\) will denote all the out-neighbors of \(v\), plus \(v\) itself. A \(r\)-regular directed graph \(G\) is neighbor-connected if for all pair of vertices \(v,v'\), there exists a sequence of vertices \(v = v_0,v_1,\ldots,v_t = v'\), such that \(|\Gamma^+(v_i)\cap\Gamma^+(v_j)| = r\) for \(i\in[1,t]\). We give a general formula for \(NC_p^+(G)\) in \(r\)-regular neighbor-connected directed graphs.

First, we need a few more definitions. We define an equivalence relation on \(V(G)\): \(x\approx y\) if there is a sequence \(x = x_0,x_1,\ldots,x_s = y\), such that for all \(i\in[1,s]\), there exist \(x_{i-1}',x_i'\in V(G)\), such that \(\Gamma^+(x_{i-1}')\Delta\Gamma^+(x_i') = \{x_{i-1},x_i\}\) (where here \(\Delta\) denotes the symmetric difference). Obviously \(\approx\) is an equivalence relation, let \(\lambda_G\) be the number of equivalence classes and \(V_1,\ldots,V_{\lambda_G}\) these classes. The following proposition is proved in [4]:

**Proposition 3** For all \(i = 1,\ldots,\lambda_G\), and for any \(v,v'\in V(G)\), \(|\Gamma^+(v)\cap V_i| = |\Gamma^+(v')\cap V_i|\).

We call \(b_i\) the cardinality of the intersection of \(V_i\) with any \(\Gamma^+(v)\), \(v\in V(G)\). Then we have the following characterization, which extends the result in [4] for any integer \(p\) whenever the hypergraph has the same number of edges and vertices.

**Theorem 1** For a \(r\)-regular neighbor-connected directed graph \(G\),

\[
NC_p(G) = p^{\lambda_G-1}\gcd(p,b_1,\ldots,b_{\lambda_G})
\]

**Proof.** Let \(c_i\) be the characteristic vector of \(V_i\) in \(\mathbb{Z}_p^n\). We prove that for any configuration \(X, X \in \ker(\sigma_G)\) if and only if \(X = \sum_{i=1,\ldots,\lambda_G} a_i c_i\), with \(\sum_{i=1,\ldots,\lambda_G} a_i b_i = 0\).

The if part is obvious. Conversely, let \(X \in \ker(\sigma_G)\). Then for \(u,u'\) such that \(u \approx u', X(u) = X(u')\). Indeed, if there exist \(v,v'\in V(G)\), such that \(\Gamma^+(v)\Delta\Gamma^+(v') = \{u,u'\}\), then \(\sigma_G(X) = 0\) implies \(\sum_{w\in\Gamma^+(v')} X(w) = 0\) and \(\sum_{w\in\Gamma^+(v')} X(w) = 0\). Subtracting the two, we obtain \(X(u) = X(u')\). It extends naturally for a sequence \(u = u_0,u_1,\ldots,u_s = u'\), where \(X(u) = X(u_0) = \ldots = X(u_s) = X(u')\). So there exist a \(\lambda_G\)-uplet \((a_1,\ldots,a_{\lambda_G})\),
For two positive integers \(u, v\) to the equation \(\sum_{i=1}^{\lambda_G} a_i c_i = 0\), then \(\sigma_G(X) = 0\) translates exactly in \(\sum_{i=1}^{\lambda_G} c_i a_i b_i = 0\).

So the number of elements in \(\ker(\sigma_G)\) is equal to the number of \(a_1, \ldots, a_{\lambda_G}\), such that \(\sum_{i=1}^{\lambda_G} a_i b_i = 0\), and it can be shown using Euclidean algorithm (see for instance [7]), that for arbitrary non null integers \(a_1, \ldots, a_n\), the number of solutions in \(\mathbb{Z}^n\) to the equation \(\sum_{i=1}^{k} a_i x_i \equiv 0 \mod p\) is equal to \(p^{k-1} \gcd(p, a_1, \ldots, a_k)\). And we get the formula.

As corollaries, we have the characterization of \(NC_p^+(k, n)\) for powers of cycles. For two positive integers \(n\) and \(k \leq \lfloor \frac{n}{2} \rfloor\) with \(k \geq 1\), we define the graph \(C(k, n) = (V, E)\) where \(V = \{0, \ldots, n-1\}\) and \(E = \{(i, j)\}\) such that \(i \neq j\) and \(|i-j| \leq k\) or \(|n-i-j| \leq k\) (there is an edge between the distinct vertices \(i\) and \(j\) if their cyclic distance in \(\mathbb{Z}_n\) is smaller than \(k\)).

This graph is usually called the \(k\)th power of the cycle on \(n\) vertices, denoted by \(C_n\). For instance, \(C(1, n) = C_n\) and \(C(k, n)\) is the complete graph on \(n\) vertices, denoted by \(K_n\), whenever \(k = \lfloor \frac{n}{2} \rfloor\). The power of cycle is trivially neighbor-connected for the extended neighboring for which all \(b_i\)'s are equal. We do not know any non-directed regular neighbor-connected graph different from a power of cycle.

**Corollary 1** \(NC_p^+(K_n) = p^{n-1}\) and \(NC_p^+(C(n, k)) = p^{l-1} \gcd(p, (2k + 1)/l)\), where \(l = \gcd(n, 2k + 1)\).

**Proof.** If \(G\) is a complete graph on \(n\) vertices then, for any distinct vertices \(u\) and \(v\), \(\Gamma^+(u) \Delta \Gamma^+(v) = \emptyset\). Thus each vertex \(u\) defines an equivalence class of \(\approx\), \(V_u\) and so \(\lambda_G = n\) and \(b_i = 1\) for all \(i\).

Now assume that \(G = C(k, n)\) with \(k < \lfloor \frac{n}{2} \rfloor\). Then for each vertex \(u\), \(\Gamma^+(u) = \{u \equiv i \mod n, i \leq k\}\). Thus, if it exists an integer \(\alpha\) such that \(v - u \equiv \alpha(2k + 1) \mod n\) then \(u \approx v\). Indeed, the path \(u = u_0, \ldots, u_\alpha = v\), with \(u_i \equiv u_{i-1} + 2k+1 \mod n\), \(u_{i-1} \equiv u_{i-1} + k \mod n\) and \(u_{i} \equiv u_{i} - k \mod n\), satisfies \(\Gamma^+(u_{i-1}) \Delta \Gamma^+(u_{i}) = \{u_{i-1}, u_{i}\}\).

If \(n = 2k + 2\) then \(n\) is prime with \(2k + 1\), thus for every pair of vertices \(u, v\), it exists an integer \(\alpha\) such that \(u \equiv v + \alpha(2k + 1) \mod n\) and so \(\lambda_G = 1 = \gcd(n, 2k + 1)\) and \(b_i = |\Gamma^+(u)| = (2k + 1)\) for all \(i\).

If \(n > 2k + 2\), let \(u, v\) be two vertices such that \(u \approx v\). By definition of \(\approx\), there exists a sequence \(u = u_0, \ldots, u_\alpha = v\) such that for all \(i \in [1, \alpha]\), there exist \(u'_{i-1}, u'_i \in V(G)\), such that \(\Gamma^+(u'_{i-1}) \Delta \Gamma^+(u'_i) = \{u_{i-1}, u_i\}\).

\(\Gamma^+(u'_{i-1})\) does not contain the vertices \(u'_{i-1} + k + 1 \mod n\) and \(u'_{i-1} + k - 1 \mod n\) which are distinct vertices since \(n > 2k + 2\).
Remark that every vertex containing both \( u'_{i-1} + k + 1 \mod n \) and \( u'_{i-1} - k - 1 \mod n \) in its extended neighborhood is not adjacent to \( u'_{i-1} \). Therefore, we can assume that \( u'_{i-1} - k - 1 \mod n \not\in \Gamma^+(u'_i) \). If \( u'_{i-1} + k + 1 \mod n \not\in \Gamma^+(u'_i) \) then \( \Gamma^+(u'_{i-1}) \cap \Gamma^+(u'_i) = \emptyset \), which contradicts \( |\Gamma^+(u'_{i-1}) \Delta \Gamma^+(u'_i)| = 2 \) since \( k > 0 \).

Assume now \( u'_{i-1} + k + 1 \mod n \in \Gamma^+(u'_i) \) hence \( u'_{i-1} - k \mod n \not\in \Gamma^+(u'_i) \) which implies that \( \Gamma^+(u'_{i-1}) \Delta \Gamma^+(u'_i) = \{ u'_{i-1} - k \mod n, u'_{i-1} + k + 1 \mod n \} \) or equivalently \( u'_i \equiv u'_{i-1} + 1 \mod n \).

Thus \( u'_i \equiv u'_{i-1} + 1 \mod n \) and \( u_i \equiv u_{i-1} \pm 2k + 1 \mod n \). Then \( u \approx v \iff v - u \equiv \alpha(2k + 1) \mod n \) which implies that \( \lambda_G = l = \gcd(n, 2k + 1) \) and \( b_i = (2k + 1)/l \) for all \( i \). \( \square \)

A direct consequence of this corollary is the following corollary.

**Corollary 2** \( C(k, n) \) is \( p \)-universal for \( \sigma^+ \)-game if and only if \( \gcd(n, 2k + 1) = \gcd(p, 2k + 1) = 1 \). \( \square \)

Now we compute \( NC^-_p(C(k, n)) \).

**Proposition 4** \( NC^-_p(K_n) = \gcd(p, n - 1) \).

**Proof.** By Proposition 1 and by definition of \( K_n \), we have:

\[
X = (x_0, \ldots, x_{n-1}) \in \ker K_n \text{ if and only if for every vertex } i, \text{ we have } x_0 + \ldots + x_{i-1} + x_{i+1} + \ldots + x_{n-1} \equiv 0 \mod p. \quad (1)
\]

Denote \( q(i) = x_0 + \ldots + x_{i-1} + x_{i+1} + \ldots + x_{n-1} \) and let \( X = (x_0, \ldots, x_{n-1}) \in \ker K_n \). By (1), for every \( i \), we have \( q(i) + 1 - q(i) = x_i - x_{i+1} \equiv 0 \mod p \). Thus, \( x_i \equiv x_j \mod p \) for all \( i, j \). Finally (1) is equivalent to \( (n - 1).x_0 \equiv 0 \mod p \) which has precisely \( \gcd(p, n - 1) \) solutions. \( \square \)

Now we complete for all other power of cycles.

To solve the problem for \( \sigma^- \)-game, we will need the following notion. The *valuation* of 2 in the factorization of an integer \( n \), denoted by \( \text{val}_2(n) \), is the largest integer \( k \) such that \( 2^k \) divides \( n \).

Let \( k < \frac{n}{2} \), \( l = \gcd(n, k) \) and \( q = \gcd(n, k + 1) \). Then \( a = \frac{k}{l} \) and \( b = \frac{n}{q} \) are integers.

6
Theorem 2

For $l$ and $\frac{n}{q}$ even and $\text{val}_2(p) > \max\{\text{val}_2(a),\text{val}_2(b)\}$:

$$NC_p^-(C(k,n)) = (2p^{l-1} \cdot \gcd(p,a) \cdot \gcd(p,b))^q.$$ 

For $l$ and $\frac{n}{q}$ even and $\text{val}_2(p) \leq \max\{\text{val}_2(a),\text{val}_2(b)\}$:

$$NC_p^-(C(k,n)) = (p^{l-1} \cdot \gcd(p,a) \cdot \gcd(p,b))^q.$$ 

For $l$ and $\frac{n}{q}$ odd:

$$NC_p^-(C(k,n)) = (p^{l-1} \cdot \gcd(p,2a))^q.$$ 

For $l$ and $\frac{n}{q}$ with different parity:

$$NC_p^-(C(k,n)) = (p^{l} \cdot \gcd(p,a))^q.$$ 

In order to prove Theorem 2, we will need the following lemma:

**Lemma 1** Let $p$ be an integer $\geq 2$, $a, b, u \in \{0, \ldots, p-1\}$. The number of pairs $(x, y)$ satisfying

$$\begin{align*}
a.(x + y) &\equiv 0 \mod p \\
b.(x - y) &\equiv 2bu \mod p
\end{align*}$$

is equal to

$$S(a, b, p) = \begin{cases} 2 \cdot \gcd(p, a) \cdot \gcd(p, b) & \text{if } \text{val}_2(p) > \max\{\text{val}_2(a),\text{val}_2(b)\} \\ \gcd(p, a) \cdot \gcd(p, b) & \text{otherwise} \end{cases}$$

**Proof.** We have precisely $s = \gcd(p, a) \cdot \gcd(p, b)$ pairs $(x + y, x - y)$ satisfying (2). These pairs $(x + y, x - y)$ are

$$\begin{align*}
(x + y) &\equiv \frac{\alpha p}{\gcd(p,a)} \mod p \\
(x - y) &\equiv \frac{\beta p}{\gcd(p,b)} + 2u \mod p
\end{align*}$$

for all $\alpha \in \{0, \ldots, \gcd(p,a)-1\} = I_\alpha$ and all $\beta \in \{0, \ldots, \gcd(p,b)-1\} = I_\beta$. Equivalently, we consider the pairs $(2x, x - y)$ satisfying

$$\begin{align*}
(x - y) &\equiv \beta' p + 2u \mod p \\
2x &\equiv \alpha' p + \beta' p + 2u \mod p
\end{align*}$$
Where \( \alpha' = \frac{ap}{\gcd(p,a)} \) and \( \beta' = \frac{bp}{\gcd(p,b)} \). The number of pairs \((x,y)\), denoted by \( s_2 \), is equal to the number of \( x \) satisfying:

\[
2x = \alpha' + \beta' \mod p.
\]

If \( p \) is odd then 2 is invertible in \( \mathbb{Z}_p \) thus each pair \((\alpha',\beta')\) determines exactly one solution \( x \) of (3) and so \( s_2 = s \).

Assume now that \( p \) is even and let \( J = \{ (\alpha',\beta') \text{ such that } \alpha'+\beta'+2u \text{ is even} \} \).

Each pair \((\alpha',\beta')\) determines the two solutions \( x \) and \( x + \frac{p}{2} \). So, \( s_2 = 2\cdot|J| \).

Now we will compute \(|J|\).

If \( \text{val}_2(p) \leq \text{val}_2(a) \) or \( \text{val}_2(b) \) then \(|J| = |\{(\alpha',\beta') \text{ such that } \alpha'+\beta' \text{ is odd}\}| = \frac{|I_a||I_b|}{2} = \frac{s}{2} \).

Else \( |J| = |I_a||I_b| = s \) and \(|\{(\alpha',\beta') \text{ such that } \alpha'+\beta' \text{ is odd}\}| = 0. \) \( \square \)

**Proof of Theorem 2:** By Proposition 1, by definition of \( C(k,n) \) and since \( k < \frac{n}{2} \), we have:

\[
X = (x_0, \ldots, x_{n-1}) \in \ker C(k,n) \text{ if and only if for every vertex } i, \text{ we have } x_{i-k} + \ldots + x_{i-1} + x_{i+1} + \ldots + x_{i+k} \equiv 0 \mod p \text{ (the subscripts are taken modulo } n) \tag{4}.
\]

Denote \( q(i) = x_{i-k} + \ldots + x_{i-1} + x_{i+1} + \ldots + x_{i+k} \) and let \( X = (x_0, \ldots, x_{n-1}) \in \ker C(k,n) \). By (4), for every \( i \), we have \( q(i) = x_{i+S_{i+k+1}} + x_i - x_{i+1} + x_{i-k} \equiv 0 \mod p \). Let \( S_i = x_i + x_{i+k+1} \). By the previous remark, we have \( S_{i+k} \equiv S_i \mod p \) for all \( i \).

Let \( l = \gcd(n,k) \). If \( i \equiv j \mod l \) then \( i \equiv j + \alpha k \mod n \), for some integer \( \alpha \) thus \( S_i \equiv S_j \mod p \). Then, by (4), we obtain that:

\[
(k/l)(S_0 + \ldots + S_{l-1}) \equiv 0 \mod p. \tag{5}
\]

Thus the last equation has precisely \( S = p^{l-1} \cdot \gcd(p,k/l) \) solutions \((S_0, \ldots, S_{l-1})\).

Moreover, we have that \( x_{k+1} = S_0 - x_0, x_{2(k+1)} = S_{k+1} - S_0 + x_0, \ldots \). Thus, for all \( i \leq n/\gcd(n,k+1) \), we have:

\[
x_{i,(k+1)} \equiv (-1)^i x_0 + \sum_{j=0}^{i-1} (-1)^{j+i+1} S_{j,(k+1)} \mod p. \tag{6}
\]

Let \( q = \gcd(n,k+1) \). So (6) gives:

\[
x_0 - (-1)^\frac{n}{q} x_0 \equiv (-1)^\frac{n}{q} + 1 \sum_{j=0}^{\frac{n}{q}-1} (-1)^j S_{j,(k+1)} \mod p. \tag{7}
\]
For convenience, let denotes (7) by \( L \equiv R \mod p \).

Observe that \( L = 0 \) if \( \frac{n}{q} \) is even, and \( L = 2x_0 \) otherwise. Now, we claim that:

\[
\begin{align*}
  l & \text{ divides } \frac{n}{q} \text{ and } l \text{ is relatively prime with } k + 1. & (8)
\end{align*}
\]

Indeed, since \( q \) divides \( k + 1 \), \( q \) is relatively prime with \( k \). Now, since \( q \) divides \( n \), we obtain \( l = \gcd(k, n) = \gcd(k, \frac{n}{q}) \). Similarly, since \( l \) divides \( k \) and since \( k + 1 \) is relatively prime with \( k \), \( l \) is relatively prime with \( k + 1 \).

Since \( l \) divides \( \frac{n}{q} \) and since \( S_i \equiv S_{i+l} \mod p \) for all \( i \), then each \( S_i \) in (7) occurs exactly \( \frac{n}{2ql} \) times.

Let \( S_e = \sum \text{ even } j \leq l-1 S_{j(k+1)} \) and \( S_o = \sum \text{ odd } j \leq l-1 S_{j(k+1)} \).

If \( n \) is even then \( \gcd(2(k+1), l) = 1 \). For all integer \( i \leq \frac{n}{2ql} \), let \( E_i = 2li + \{0, 2, \ldots, 2(l-1)\} \) and \( O_i = 2li + \{1, 3, \ldots, 2l-1\} = \{2li+1, 2li+3, \ldots, 2li+2l-1\} \). Since \( \gcd(k+1, l) = 1 \), we have that for each \( S_j \) (with \( j \in \{0, \ldots, l-1\} \)) there are two indices \( j_1 \) and \( j_2 \) in \( O_i \cup E_i \) such that \( S_{j(k+1)} = S_{j_2(k+1)} = S_j \). Moreover, since \( \gcd(2(k+1), l) = 1 \), \( \{S_{j(k+1)} | j \in E_i\} = \{S_j | j \in \{0, \ldots, l-1\}\} \) and so \( \{S_{j(k+1)} | j \in O_i\} = \{S_j | j \in \{0, \ldots, l-1\}\} \).

If \( \frac{n}{q} \) is even then

\[
\begin{align*}
  \sum \text{ even } j \leq \frac{n}{q} - 1 S_{j(k+1)} \equiv \sum \text{ odd } j \leq \frac{n}{q} - 1 S_{j(k+1)} \equiv \frac{n}{2ql} \sum_{j \leq l-1} S_j \mod p.
\end{align*}
\]

Finally, \( R = 0 \).

Now, if \( \frac{n}{ql} \) is odd then \( R = S_e - S_o \)

Assume now that \( l \) is even. Since \( l \) is relatively prime with \( k + 1 \), then each \( S_i \) with \( i \in \{0, \ldots, l-1\} \) occurs in (7). Moreover \( k + 1 \) is odd, then \( R = (-1)^{\frac{n}{ql}+1} \frac{n}{ql}(S_e - S_o) \). Hence (5)-(7) can be written as follows:

\[
\begin{align*}
  & \begin{cases}
    \frac{k}{l}(S_e + S_o) & \equiv 0 \mod p \\
    (-1)^{\frac{n}{ql}+1} \frac{n}{ql}(S_e - S_o) & \equiv L \mod p
  \end{cases} \quad (9)
\end{align*}
\]

By (8), if \( l \) is even then \( \frac{n}{q} \) is also even. Let \( a = \frac{k}{l} \) and \( b = (-1)^{\frac{n}{ql}+1} \frac{n}{ql} \).
If \((l, n, q)\) is \((\text{EVEN, EVEN})\) then (5)-(7) can be written as follows:

\[
\begin{align*}
\{ & \ a.(S_e + S_o) \equiv 0 \mod p \\
& \ b.(S_e - S_o) \equiv 0 \mod p 
\end{align*}
\]

Thus \(x_0\) can take any value in \(\{0, \ldots, p - 1\}\). Moreover, the number of solutions of the equation \(S_e = u\) for a fixed positive integer \(u < p\) is exactly \(p^{\frac{l}{2} - 1}\); and similarly for \(S_o\). Finally, \(NC_p^-(C(k, n)) = (p^{l-1}.S(a, b, p))^q\).

If \((l, n, q)\) is \((\text{ODD, EVEN})\) then (5)-(7) can be written as follows:

\[
\begin{align*}
\{ & \ a.(S_e + S_o) \equiv 0 \mod p \\
& \ 0 \equiv 0 \mod p 
\end{align*}
\]

Thus \(x_0\) can take any value in \(\{0, \ldots, p - 1\}\). Finally, \(NC_p^-(C(k, n)) = (S, p)^q\).

If \((l, n, q)\) is \((\text{ODD, ODD})\) then (5)-(7) can be written as follows:

\[
\begin{align*}
\{ & \ a.(S_e + S_o) \equiv 0 \mod p \\
& \ S_e - S_o \equiv 2x_0 \mod p 
\end{align*}
\]

Thus \(x_0\) can take \(p\) values. Similarly as the case \((\text{EVEN, EVEN})\), the number of solutions of the equation \(S_e = u\) for a fixed positive integer \(u < p\) is exactly \(p^{\frac{l}{2} - 1}\); and \(p^{\frac{l}{2} - 1}\) for \(S_o\). Finally, we get \(NC_p^-(C(k, n)) = (p^{l-1}.S(a, 1, p))^q\). \(\square\)

Proposition 4 and Theorem 2 show that the power of cycle \(C(k, n)\) are extremal for the inequality given in Proposition 2 whenever \(\gcd(k, n) = \gcd(k + 1, n) = 1\).

This theorem extends results on the cycles and complete graphs given in [1].

A direct consequence of this theorem is the following corollary.

**Corollary 3** \(C(k, n)\) is \(p\)-universal for \(\sigma^-\)-game if and only if \(\gcd(n, k) = \gcd(p, 2k) = 1\) and \(\text{val}_2(n) \leq \text{val}_2(k + 1)\). \(\square\)

### 4 Trees

In this section, we show a method to compute \(NC_p^-(G)\) for all \(p\) if \(G\) is a tree. A constructive characterization of all trees such that \(NC_2^+(G) = 1\)
was presented in [2] (they were called “parity realizable trees”). We provide here a way of computing $NC_2^+$, and a consequence is a short proof of the mentioned result of [2], but the same method seems to fail to give a simple characterization of $NC_p^+$ when $p \geq 3$.

The following properties are true for any graph:

**Proposition 5** If $G_1$ and $G_2$ form a partition of the connected components of a graph $G$, then for all $p$, $NC_p(G) = NC_p(G_1) \times NC_p(G_2)$.

**Proof.** For any configurations $C_1 \in \mathcal{C}_{G_1}$ and $C_2 \in \mathcal{C}_{G_2}$ such that $\sigma_{G_1}(C_1) = 0$ and $\sigma_{G_2}(C_2) = 0$, let $C$ be the configuration of $\mathcal{C}_G$ such that $C(x) = C_1(x)$ when $x \in V(G_1)$ and $C(x) = C_2(x)$ otherwise. It is obvious that $\sigma_G(C) = 0$, and that it is possible to construct $NC_p(G_1) \times NC_p(G_2)$ such configurations. By Proposition 1, this implies the result. $\Box$

The following proposition is easily checked:

**Proposition 6** Let $P_1$ be the graph constituted by a unique vertex, and $P_2$ be the graph with two vertices joined by an edge. For all $p$, $NC_p^-(P_1) = NC_p^+(P_1) = 1$ and $NC_p^+(P_1) = NC_p^-(P_2) = p$.

Using this proposition, we give a principle of construction (or decomposition) for which $NC_p^-$ is invariant (see Figure 1):

![Figure 1: A way to decompose trees](image)

**Proposition 7** Let $G$ be a graph, and $T$ a subset of its vertices. Let $u, v$ be two vertices disjoint from $V(G)$. Let $G_2$ be the graph such that $V(G_2) = V(G) \cup \{u, v\}$ and $E(G_2) = \cup_{t \in T}\{ut\} \cup \{uv\} \cup E(G)$. Then for all $p$, $NC_p^-(G_2) = NC_p^-(G)$. 

11
Proof. In this proof, \( \sigma \) will stand for \( \sigma^- \), \( NC \) for \( NC^-_p \), and \( \ker{G} \) for \( \ker{G}(\sigma_G) \). We construct two injections, one from \( \ker{G} \) to \( \ker{G}_2 \), and one from \( \mathcal{CL}_G^2 \) to \( \mathcal{CL}_G \), and since \( \ker{G} \) is isomorphic to \( \mathcal{CL}_G \) for any graph \( G \), this will prove the result.

First, for \( X \in \ker{G} \), let \( f(X) \in \ker{G}_2 \) be such that \( f(X)(x) = X(x) \) if \( x \in V(G) \), \( f(X)(u) = 0 \), and \( f(X)(v) = -\sum_{t \in T} X(t) \). The application \( f \) is trivially an injection from \( \ker{G}(\sigma_G) \) into \( \ker{G}_2(\sigma_G) \).

Conversely, for \( C2 \in \mathcal{CL}_G^2 \), take \( X2(\in C2 \text{ such that } X2(u) = X2(v) = 0 \) (such a configuration always exists: if \( X2' \in C2 \text{ doesn't satisfy } X2'(v) = 0 \), then \( X2 = X2' + \sigma(Z) \), with \( Z \) such that \( Z(x) = 0 \) if \( x \in V(G) \), \( Z(u) = -X2'(v) \), and \( Z(v) = -X2'(u) \)).

Then define \( f2(C2) \) as the class containing the restriction of \( X2 \) to \( \mathcal{CL}_G \). Suppose that \( f2 \) is not an injection: for \( X2, Y2 \in C2 \text{ in different classes of } G \) (and \( X2(u) = X2(v) = Y2(u) = Y2(v) = 0 \)), let \( X, Y \) be in the respective images of the classes by \( f2 \), and suppose that \( X \) and \( Y \) are in the same class. Then there exists \( Z \in C_G \), such that \( X = Y + \sigma(Z) \). Define \( Z2 \in C_G \): \( Z2(x) = Z(x) \) if \( x \in V(G) \), \( Z2(u) = 0 \), and \( Z2(v) = -\sum_{t \in T} Z(t) \). Then \( X2 = Y2 + \sigma(Z2) \), which is a contradiction. \( \square \)

We call the \( \sigma^- \)-decomposition of a graph \( G \) the operation of deletion of a vertex of degree 1, and its neighbor, if its degree is at least 2 (getting \( G \) from \( G2 \) in the last proposition). The total \( \sigma^- \)-decomposition is achieved if no further \( \sigma^- \)-decomposition is possible (in other words, \( G \) has no path of length at least 2 ending with a vertex of degree 1). The following theorem gives a constructive characterization of \( NC^-_p \) for trees:

**Theorem 3** Let \( cc^-_p(G) \) be the number of isolated vertices after the total \( \sigma^- \)-decomposition of a tree \( G \). Then \( NC^-_p(G) = p^{cc^-_p(G)} \).

**Proof.** By Proposition 7, the operation of decomposition preserves \( NC^-_p(G) \) for all \( p \). Apply proposition 7 to decompose the tree as long as it is possible. Then the remaining components \( C_i \) are only graphs isomorphic to \( P1 \) or \( P2 \). By proposition 5, \( NC^-_p(G) = \Pi NC^-_p(C_i) \), and by proposition 6, \( NC^-_p(G) = p^{cc^-_p(G)} \). \( \square \)

The following corollary is immediate. We call a path of length \( n \) a path with \( n \) vertices and \( n - 1 \) edges.

**Corollary 4** If \( G \) is a path, \( NC^-_p(G) = 1 \) if \( G \) has even length, and \( NC^-_p(G) = p \) otherwise.
A similar decomposition works for the computation of $NC^+_2$, generalizing and providing a simple proof of the main result of [2]. The following two propositions are an equivalent to Proposition 7 for $NC^+_p$ (see Figure 2):

![Figure 2: Another way to decompose trees](image)

**Proposition 8** Let $G$ be a graph, and $T$ a subset of its vertices. Let $u, v, w$ be three vertices disjoint from $V(G)$. Let $G_2$ be the graph such that $V(G_2) = V(G) \cup \{u, v, w\}$ and $E(G_2) = \cup_{t \in T}\{ut\} \cup \{uv\} \cup \{vw\} \cup E(G)$. Then $NC^+_p(G_2) = NC^+_p(G)$.

**Proof.** We follow the same scheme as in the proof of Proposition 7. $\sigma$ will stand for $\sigma^+$, $NC$ for $NC^+_p$, and ker$_G$ for ker$_G(\sigma_G)$. We construct two injections between ker$_G$ and ker$_{G_2}$.

First, for $X \in$ ker$_G$, let $f(X) \in$ ker$_{G_2}$ be such that $f(X)(x) = X(x)$ if $x \in V(G)$, $f(X)(u) = 0$, and $f(X)(v) = -\sum_{t \in T}X(t)$ and $f(X)(w) = \sum_{t \in T}X(t)$. The application $f$ is trivially an injection from ker$_G(\sigma_G)$ into ker$_{G_2}(\sigma_{G_2})$.

Conversely, for $C_2 \in CL_{G_2}$, take $X_2 \in C_2$ such that $X_2(u) = X_2(v) = X_2(w) = 0$ (such a configuration always exists: if $X_2' \in C_2$ does not satisfy $X_2'(u) = X_2'(v) = X_2'(w) = 0$, take $X_2 = X_2' + \sigma(Z)$, with $Z$ such that $Z(x) = 0$ if $x \in V(G)$, $Z(u) = X_2'(w) - X_2'(v)$, $Z(v) = -X_2'(u) + X_2'(v) - X_2'(w)$, and $Z(w) = X_2'(u) - X_2'(v)$).

Then define $f_2(C_2)$ as the class containing the restriction of $X_2$ to $CL_G$. Suppose that $f_2$ is not an injection: for $X_2, Y_2$ in different classes of $G_2$ (and $X_2(u) = X_2(v) = X_2(w) = Y_2(u) = Y_2(v) = Y_2(w) = 0$), let $X, Y$ be in
the respective images of the classes by \( f_2 \), and suppose that \( X \) and \( Y \) are in the same class. Then there exists \( Z \in C_G \), such that \( X = Y + \sigma(Z) \). Define \( Z_2 \in C_{G_2} \): \( Z_2(x) = Z(x) \) if \( x \in V(G) \), \( Z_2(u) = 0 \), \( Z_2(v) = -\sum_{t \in T} X(t) \) and \( Z_2(w) = \sum_{t \in T} X(t) \). Then \( X_2 = Y_2 + \sigma(Z_2) \), which is a contradiction. \( \Box \)

**Proposition 9** Let \( G \) be a graph, and \( t \) one of its vertices. Let \( u_1, \ldots, u_p \) be \( p \) vertices disjoint from \( V(G) \). Let \( G_2 \) be the graph such that \( V(G_2) = V(G) \cup \{u_1, \ldots, u_p\} \) and \( E(G_2) = \{tu_1, \ldots, tu_p\} \cup E(G) \). Then \( NC_p^+(G_2) = NC_p^+(G) \).

**Proof.** We follow the same scheme as in the previous proof. \( \sigma \) will stand for \( \sigma^+ \), \( NC \) for \( NC_2^+ \), and \( \ker_G \) for \( \ker_G(\sigma_G) \). We construct two injections between \( \ker_G \) and \( \ker_{G_2} \).

First, for \( X \in \ker_G \), let \( f(X) \in \ker_{G_2} \) be such that \( f(X)(x) = X(x) \) if \( x \in V(G) \), and \( f(X)(u_i) = -X(t) \) for all \( i = 1, \ldots, p \). Since \( p(\sigma(X(t))) \equiv 0 \) mod \( p \), the application \( f \) is trivially an injection from \( \ker_G(\sigma_G) \) into \( \ker_{G_2}(\sigma_{G_2}) \).

Conversely, for \( C_2 \in CL_{G_2} \), take \( X_2 \in C_2 \) such that \( X_2(u_i) = 0 \) for all \( i \) (such a configuration always exists: if \( X_2' \in C_2 \) doesn’t satisfy \( X_2'(u_i) = 0 \) for all \( i \), take \( X_2 = X_2' + \sigma(Z) \), with \( Z \) such that \( Z(x) = 0 \) if \( x \in V(G) \) and \( Z(u_i) = -X_2'(u_i) \) for all \( i \)).

Then define \( f_2(C_2) \) as the class containing the restriction of \( X_2 \) to \( CL_G \).

Suppose that \( f_2 \) is not an injection: for \( X_2, Y_2 \) in different classes of \( G_2 \) (and \( X_2(u_i) = Y_2(u_i) = 0 \) for all \( i \)), let \( X, Y \) be in the respective images of the classes by \( f_2 \), and suppose that \( X \) and \( Y \) are in the same class. Then there exists \( Z \in C_G \), such that \( X = Y + \sigma(Z) \). Define \( Z_2 \in C_{G_2} \): \( Z_2(x) = Z(x) \) if \( x \in V(G) \), and \( Z_2(u_i) = -Z(t) \) for all \( i \). Then \( X_2 = Y_2 + \sigma(Z_2) \), which is a contradiction. \( \Box \)

We call the \( \sigma_2^+ \)-decomposition of a tree \( G \) the following operation: for an arbitrary root \( r \in V(G) \), let \( x \) be the vertex at longest distance from \( r \). The degree of \( x \) is one since \( G \) is a tree. Let \( y \) be its unique neighbor. If \( y \) has degree two, then delete \( x, y \) and its second neighbor. If \( y \) has degree larger than three, delete \( x \), and one of the neighbors of \( y \) at same distance from \( r \) as \( x \). (In other words, obtain \( G \) from \( G_2 \) in one of the two previous propositions whenever \( p = 2 \).) The total \( \sigma_2^+ \)-decomposition is achieved if no further \( \sigma_2^+ \)-decomposition is possible (the graph is composed with isolated vertices or isolated edges). The following theorem gives a constructive characterization of \( NC_2^+ \) for trees:
Theorem 4 Let $cc^+(G)$ be the number of isolated edges after the total $\sigma^+_2$-decomposition of a tree $G$. Then $NC^+_2(G) = 2^{cc^+(G)}$.

Proof. By Propositions 8 and 9 with $p = 2$, the operation of decomposition preserves $NC^+_2(G)$. Decompose the tree as long as it is possible. Then the remaining components $C_i$ are only graphs isomorphic to $P_1$ or $P_2$. By proposition 5, $NC^+_2(G) = \prod NC^+_2(C_i)$, and by proposition 6, $NC^+_2(G) = 2^{cc^+(G)}$. $\square$

Now, we mention two corollaries, which are immediate consequence of Theorem 4 and Propositions 8 and 6 and which was also obtained by Sutner [8, 10].

Corollary 5 Let $G$ be a path of length $n$. Then $NC^+_p(G) = 1$ if $n \equiv 0, 1 \mod 3$, and $NC^+_p(G) = p$ otherwise.

Corollary 6 The total $\sigma^+_2$-decomposition of a tree $G$ consists of isolated points iff $N^+_2(G) = 1$.

References


