Note di Matematica **20,** n. 2, 2000/2001, 21–26.

On a generalization of Posthumus graphs

Domenico Lenzi
Dipartimento di Matematica "E. De Giorgi", Università di Lecce, 73100 Lecce, Italy

Received: 14 January 2000; accepted: 3 October 2000.

Abstract. In graph theory one often deals with 1-graphs (*i. e.*: given two vertices u and v, there is at last one arc that incides from u to v) of order $m = p^n$, where p and n are natural number greater than 1. These are regular graphs of degree p and diameter n, which have a certain importance in some problems of telecommunication (cf. [2], p.229: EXAMPLE), since vertices and arcs can respectively represent stations and one-way connections of a telecommunication net-work.
It seems that the first construction of these graphs, with $m = 2^n$, is due to Ir. K. Posthumus, who stated a very interesting conjecture, concerning some cycles of digits 0 or 1, proved in [1] by N. G. De Bruijn.
In the study of these graphs the condition $m = p^n$ is heavily relied on. In this paper we adapt that construction to the case in which $p^{n-1} < m \leq p^n$; so we find again several interesting properties of the previous particular case.
Among other things, we get regular 1-graphs of degree p, such that for any two different vertices u and v there exists at least a path from u to v of length less than, or equal to, n.
The research here reported has been motivated by a problem brought to my attention by G. Cancellieri.

Keywords: graph

MSC 2000 classification: 05Cxx

Introduction

We shall deal only with natural numbers, thus we shall only use for them the terms "integer" or "number".

Now, given a number $m \geq 2$, let $[[0, m-1]]$ be the set $\{0, \ldots, m-1\}$ of the numbers smaller than m[1]. Furthermore, let us consider two numbers p and n such that $p^{n-1} < m \leq p^n$.

If $m = p^n$, then we can give $[[0, m-1]]$ a graph structure in a very simple way. In fact if we represent the numbers in basis p, then any element of $[[0, p^n-1]]$ is given by a sequence $t_n t_{n-1} \cdots t_2 t_1$ of n integers less than p. Thus we can associate to any such $t_n t_{n-1} \cdots t_2 t_1$ the p elements $t_{n-1} \cdots t_1 t$ (where $t = 0, \ldots, p-1$); as a consequence, $t_n t_{n-1} \cdots t_2 t_1$ is associated just to the p elements $t t_n t_{n-1} \cdots t_2$. Hence $[[0, p^n-1]]$ becomes a regular 1-graph of degree p. Moreover, it is obvious

[1] More generally, if a and b are numbers such that $a < b$, then $[[a, b]]$ will be the set of the number x such that $a \leq x \leq b$.

that, if u and v are different elements belonging to $[[0, p^n–1]]$, then one can go from u to v through a path of length less than or equal to n. Furthermore the diameter of this graph is n, since it is clear that, if $t_1 \neq t$, then from $t_n t_{n-1} \cdots t_2 t_1$ to the constant n-ple $t \cdots t$ there is a distance equal to n.

The recalled construction has several interesting practical applications. In fact vertices and arcs of the previous graph can respectively represent stations and one-way connections of a telecommunication net-work. Anyway, a net-work could have a number of stations which is different from a power of an integer; thus it is useful to consider the more general case in which $p^{n-1} < m \leq p^n$. To this end let the symbols "$+$", "$-$" and "$\cdot$" represent the usual operations modulo m. Moreover, if a is a natural number less than m, let $-a$ be the opposite of a with respect to $+$. At the same time let the symbols "+", "–" and "·" represent the usual arithmetical operations. In our formulas however we shall omit almost always the symbol "·".

1 On some particular 1-graphs

Obviously, if $m = p^n$, then one has:

$$t_{n-1} \cdots t_1 t = t_n t_{n-1} \cdots t_2 t_1 \cdot p + t \tag{1}$$

Equality (1) suggests us to study also in the case $p^{n-1} < m \leq p^n$ the graph $\mathbf{G}$ whose vertices are the elements of $[[0, m–1]]$ and whose arcs connect any vertex u to the p elements of the following set:

$$f(u) = \{u \cdot p, u \cdot p + 1, \ldots, u \cdot p + (p-1)\}.$$

Then p arcs incide from any vertex of $\mathbf{G}$, and $\mathbf{G}$ has mp arcs. We shall say that $\mathbf{G}$ is a "generalized Posthumus graph".

Now we can associate to the arc from the vertex u to the vertex $u \cdot p + r$ (with $0 \leq r < p$) the number up+r. In such a manner we determine a function from the set of the mp arcs into the set $[[0, mp–1]]$.

This function is surjective and hence it is bijective too. In fact whenever $n \in [[0, mp–1]]$, one has $n = qp$+r, with $r \leq p$–1; hence $q \in [[0, m–1]]$ and n corresponds to the arc from q to $q \cdot p + r$.

Moreover, the mp arcs of $\mathbf{G}$ individually incide in a cyclic order and in sequence to the m vertices of $\mathbf{G}$. Thus p arcs incide to any vertex of $\mathbf{G}$. This fact is stated in a more precise way in the following remark.

Remark 1. Given a vertex v, in order to determine a vertex u such that there is an arc from u to v, let us fix an integer $i \leq p$–1. Then we can consider the numbers u_i and r_i such that $r_i \leq p$–1 and v+$im = u_i p$+r_i.

Obviously, since $i \leq p{-}1$ and $v < m$, we have that $v{+}im < pm$, hence u_i is a number smaller than m. Moreover $u_i \cdot p + r_i = v$, hence an arc incides from u_i to v. As a consequence, since one has $u_{i'} < u_{i''}$ whenever $i' < i''$, then exactly p arcs incide to v.

In particular, if $m = pq$, then both $v{+}im$ and $v{+}(i{+}1)m$ have the same rest with respect to the division by p. As a consequence, in this case the numbers r is the same for every $i \leq p{-}1$ and $u_i = u_0{+}iq$. □

Now let us consider the function F that associates to every non empty subset $H \subseteq [[0, m{-}1]]$ the set $\cup_{u \in H} f(u)$.

It is obvious that if we consider two vertices u and $u{+}1$ then, since $(u{+}1){\cdot}p = u \cdot p + p$ we have:

$$F\{u, u{+}1\} = \{u{\cdot}p, u{\cdot}p{+}1, \ldots, u{\cdot}p{+}(p{-}1), u{\cdot}p{+}p, u{\cdot}p{+}p{+}1, \ldots, u{\cdot}p{+}2p{-}1\}.$$

Therefore, if H is a set of h consecutive vertices starting from u, and $hp < m$, then FH is a set of hp consecutive vertices starting from $u \cdot p$; in particular, $F[[0, h{-}1]] = [[0, hp{-}1]]$. On the contrary, if $m \leq hp$, then $FH = [[0, m{-}1]]$. Hence, if $h < m$, then $[[0, h{-}1]] \subset F[[0, h{-}1]]$. Furthermore, for a fixed vertex u, by iterating F we have that, if c is a number such that $m \leq p^c$, then $F^c\{u\} = [[0, m{-}1]]$; on the other hand, if $p^c < m$, then $F^c\{u\}$ has exactly p^c consecutive vertices starting from $u \cdot p^c$.

Theorem 1. **G** *is a regular and strongly connected 1-graph of degree* p *and diameter* n*.*

Proof. In fact, since $m \leq p^n$, we have $F^n\{u\} = [[0, m{-}1]]$ for any vertex u. Thus for any two vertices u and v there exists at least a path from u to v having at most n elements. Moreover, $\{0\} \subset F\{0\} \subset \cdots \subset F^{n-1}\{0\} \subset F^n\{0\} = [[0, m{-}1]]$, thus $F^{n-1}\{0\} \neq [[0, m{-}1]]$; hence there are some vertices whose distance from 0 is n. These properties tell us that **G** is strongly connected and the diameter $\delta(\mathbf{G})$ is n.

Furthermore, since from any vertex of **G** exactly p arcs incide and to any vertex of **G** exactly p arcs incide from p different vertices, then **G** is a regular 1-graph of degree p. QED

Now let ϕ be the involution that maps any $u \in [[0, m{-}1]]$ into the element $\phi(u) := m{-}1{-}u = -1 - u$. Thus we have a kind of "symmetry" on $[[0, m{-}1]]$, since (u, v) is an arc of **G** if and only if $(\phi(u), \phi(v))$ is an arc of **G**. Indeed if (u, v) is an arc, then $v = u \cdot p + t$, where $t \in [[0, p{-}1]]$. Hence we have:

$$\begin{aligned} \phi(v) &= -1 - (u \cdot p + t) = p - p - 1 - u \cdot p - t = \\ &= (-1 - u) \cdot p + p - 1 - t = \phi(u) \cdot p + (p{-}1{-}t). \end{aligned}$$

Since $0 \leq p{-}1{-}t \leq p{-}1$, the assertion immediately follows.

The above property ensures that ϕ is an automorphism of the 1-graph $\mathbf{G}$. In general, it is difficult to describe all the automorphisms of $\mathbf{G}$. However, if $m = p^n$ this is very simple, since one can represent the numbers in basis p. Indeed, if g is a permutation of the set of the numbers smaller than p and if ψ is the map that to any $t_{n-1}t_{n-2}\cdots t_0 \in [[0, p^n{-}1]]$ associates the number $g(t_{n-1})g(t_{n-2})\cdots g(t_0)$, then ψ is an automorphism of this graph, since both $(t_{n-1}t_{n-2}\cdots t_0, t_{n-2}\cdots t_0 t)$ and $(g(t_{n-1})g(t_{n-2})\cdots g(t_0), g(t_{n-2})\cdots g(t_0)g(t))$ are arcs. It is easily verified that the maps of this type are the only automorphisms of this graph.

Through $\mathbf{G}$ one can construct several other regular 1-graphs of degree p and diameter not higher than n, such that their vertices are the elements of $[[0, m{-}1]]$. In fact $f(0) = [[0, p{-}1]]$ and $f(m{-}1) = [[m{-}p, m{-}1]]$. Therefore 0 and $m{-}1$ are loop vertices of $\mathbf{G}$. Moreover, since $p < m$, one has $m{-}1 \notin f(0)$ and $0 \notin f(m{-}1)$. Thus the ordered pairs $(0, m{-}1)$ and $(m{-}1, 0)$ are not arcs of $\mathbf{G}$. Consequently, if $\Im$ is the set of the loop vertices of $\mathbf{G}$, then one can give $\Im$ a structure of regular 1-graph of degree 1 in such a manner that, if the loops of $\mathbf{G}$ are replaced by the arcs of $\Im$, then $\mathbf{G}$ is transformed into another strongly connected and regular 1-graph $\mathbf{G}'$ of degree p and diameter not higher than n[2].

If $m = 4$ and $p = 3$, so that $\delta(\mathbf{G}) = n = 2$, we can give $\Im$ a structure of regular 1-graph of degree 1, in such a manner that the diameter of $\mathbf{G}'$ is 1. In fact it is easily verified that in this case all the vertices of $\mathbf{G}$ are loop vertices. Thus we can take $(0,3), (3,0), (1,2)$ and $(2,1)$ as the arcs of $\Im$. Therefore — since the other arcs of $\mathbf{G}$ are $(0,1), (1,0), (0,2), (2,0), (1,3), (3,1), (2,3)$ and $(3,2)$ — if u and v are distinct elements of $\{0,1,2,3\}$, then (u,v) is an arc of $\mathbf{G}'$. Hence $\delta(\mathbf{G}') = 1$.

2 On the loop vertices of G

In this section we shall determine the loop vertices of $\mathbf{G}$. If $m = p^n$ and if one represents the elements of $[[0, p^n{-}1]]$ in basis p, then the loop vertices are the constant n-ples $t\cdots t$ $(t \le p{-}1)$; because $t_n t_{n-1}\cdots t_2 t_1 = t_{n-1}\cdots t_2 t_1 t$ if and only if $t_n = t_{n-1} = \cdots = t_1 = t$. In the general case let us consider the following m-modular equation in x: $x \cdot p + t = x$, with $t \in [[0, m{-}1]]$, which is equivalent to the following one:

$$(p{-}1) \cdot x + t = 0 \qquad (2)$$

Obviously, a loop vertex of $\mathbf{G}$ is a solution of (2) such that t is smaller than p.

[2]For example, one can give $\Im$ the structure of 1-graph in which the vertices different from 0 and from $m{-}1$ are the only loop vertices. In the meantime $(0, m{-}1)$ and $(m{-}1, 0)$ are the only arcs which are not loops.

Now let $\underline{d}$ be the greatest common divisor of $p-1$ and m. Moreover let $\underline{a} := (p-1)/\underline{d}$ and $\underline{m} := m/\underline{d}$.

Remark 2. The following properties of modulo m arithmetic are obvious:

i) The solutions of $(p-1)\cdot x = 0$ are the elements of $[[0, m-1]]$ of the type $c\underline{m}$, where $c \in [[0, \underline{d}-1]]$.

ii) For a fixed $t \in [[0, m-1]]$, if v is a particular solution of (2), then the solutions of (2) are of type $v + v_0$, where v_0 is a solution of $(p-1)\cdot x = 0$. □

Remark 3. The solutions of (2) are the elements $v \in [[0, m-1]]$ such that m divides $(p-1)v+t$. Hence, if the above equation (2) has a solution, then this equation is of the following type:

$$(\underline{d}\,\underline{a})\cdot x + \underline{d}b = 0, \tag{3}$$

where b is a number less than $\underline{m}$.

Now a number v smaller than m is a solution of (3) if and only if m is a divisor of $\underline{d}\,\underline{a}v+\underline{d}b$; thus, since $m = \underline{d}\,\underline{m}$, v is a solution of (3) if and only if $\underline{m}$ is a divisor of $\underline{a}v+b$. □

Since $\underline{a}$ and $\underline{m}$ are relative primes, let $\underline{a}'$ be the unique number smaller than $\underline{m}$ such that $\underline{a}\,\underline{a}' \equiv 1 \pmod{\underline{m}}$. Thus $0 \equiv -\underline{a}\,\underline{a}'+1 \pmod{\underline{m}}$.

We have the following

Theorem 2. *If b is a number less than $\underline{m}$, then $-\underline{a}'\cdot b$ is a particular solution of $(p-1)\cdot x + \underline{d}\,b = 0$.*

PROOF. By Remark 3, we have only to verify that $\underline{m}$ is a divisor of $-\underline{a}\,\underline{a}'b+b$. To this purpose it is sufficient to observe that, since $0 \equiv -\underline{a}\,\underline{a}'+1 \pmod{\underline{m}}$, $\underline{m}$ is a divisor $-\underline{a}\,\underline{a}'+1$. QED

Theorem 3. *The loop vertices of* **G** *are all the elements of $[[0, m-1]]$ of the type $-\underline{a}'\cdot b + c\underline{m}$, where $b \in [[0, (p-1)/\underline{d}]]$ and $c \in [[0, \underline{d}-1]]$. Moreover,* **G** *admits exactly $p-1+\underline{d}$ loops.*

PROOF. The first part is an immediate consequence of Remark 2 and of Theorem 2.

Now, since b can assume $(p-1)/\underline{d}+1$ values and c can assume $\underline{d}$ values, then **G** admits exactly $p-1+\underline{d}$ loops. QED

Corollary 1. *If d is a nontrivial divisor of m, then all the elements of $[[0, m-1]]$ are loop vertices if and only if $p = m+1-d$.*

3 A generalization and concluding remarks

We can give a simple generalization of the previous construction of generalized Posthumus graphs. Indeed we can consider the 1-graph $\mathbf{G}'$ whose vertices are the elements of $[[0,m–1]]$ and whose arcs connect any element $u \in [[0,m–1]]$ with the p elements of $f'(u) = \{u \cdot p + k, u \cdot p + 1 + k, \ldots, u \cdot p + (p–1) + k\}$.

Remark 4. It is clear that the loop vertices of $\mathbf{G}'$ are the solution of the equation (2) in section 3, with $t \in \{k, 1 + k, \ldots, (p–1) + k\}$.

Moreover (by the previous remarks) we have that if c is a number such that $p^c < m$ and if F' is the function that associates to every non empty subset H of $[[0,m–1]]$ the set $\cup_{u \in H} f'(u)$ then, for any $u \in [[0,m–1]]$, $F'^c(u)$ has exactly p^c consecutive elements, otherwise $F'^c(u)$ coincides with $[[0,m–1]]$.

In particular, if n is the smallest natural number such that $m \le p^n$, and u is a loop vertex, then we have (cf. the proof of Theorem 1, where $u = 0$) $\{u\} \subset F'(u) \subset \cdots \subset F'^{n-1}(u) \subset F'^n(u) = [[0,m–1]]$, hence $F'^{n-1}(u) \ne [[0,m–1]]$. Thus $\mathbf{G}'$ is a regular and strongly connected 1-graph whose diameter is n. □

We conclude with the following theorem that generalizes Theorem 3. Here $\underline{d}$, $\underline{m}$, $\underline{a}$ and $\underline{a}'$ are the same as in section 3.

Theorem 4. *The loop vertices of* $\mathbf{G}'$ *are the elements of* $[[0,m–1]]$ *of type* $-\underline{\mathrm{a}}' \cdot b + c\underline{\mathrm{m}}$, *where* $c \in [[0,\underline{\mathrm{d}}–1]]$ *and* b *is a number such that* $\underline{\mathrm{d}}b \in \in \{k, 1 + k, \ldots, (p–1) + k\}$.

If $\underline{\mathrm{d}}$ *is a divisor of* k, *then* $\mathbf{G}'$ *has* $p–1+\underline{\mathrm{d}}$ *loops; otherwise,* $\mathbf{G}'$ *has* $p–1$ *loops.*

Proof. The first part of the proof is an immediate consequence of the above results; the second one depends on the fact that, given a divisor d of $p–1$ and a set H of p consecutive numbers with minimum element k, if k is a multiple of d, then in H there are $[(p–1)/d]+1$ multiple of d; otherwise in H there are $(p–1)/d$ multiples of d. *QED*

Let us remark that the second part of Theorem 4 can be useful in practical applications. In fact the loops of a graph somehow are superfluous, since they do not determine effective connections.

References

[1] G. Cancellieri, A. Del Ferro, M. Mazzone: *State diagram for cyclic block codes*, IEEE Melecom 96, Bari (1996) 1011–1013.

[2] G. Cancellieri, L. Laici: *Input-output enumerating function of RSC codes and turbo codes*, 4th Eur. Conf. Satellite Comm., Rome (1997) 422–427.

[3] G. Cancellieri, F. Vatta: *Feedback concatenation of convolutional codes*, SoftCom 2001, Dubrovnik (2001) 57–63.

[4] N. G. De Bruijn: *A combinatorial problem.* Proc. Konink. Nederl. Akad. Wetensch., **49** (1946) 758–764.

[5] C. Berge: Graphes et hypergraphes. Dunod, Paris (1970).

[6] F. Harary: Graph Theory. Addison–Wesley Pub. Company (1972).