

Alain Bretto; Alain Faisant

Another way for associating a graph to a group

*Mathematica Slovaca*, Vol. 55 (2005), No. 1, 1--8

Persistent URL: <http://dml.cz/dmlcz/131571>

## Terms of use:

© Mathematical Institute of the Slovak Academy of Sciences, 2005

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://project.dml.cz>

## ANOTHER WAY FOR ASSOCIATING A GRAPH TO A GROUP

ALAIN BRETTO\* — ALAIN FAISANT\*\*

(Communicated by Stanislav Jakubec)

**ABSTRACT.** This article introduces a new type of graph associated to a group. We give some basic properties of these graphs, called  $\mathbb{G}$ -graphs, and we show that many of classical graphs are  $\mathbb{G}$ -graphs.

### 1. Introduction

The group theory, especially the finite group theory, is one of the main parts of modern mathematics. Groups are objects constructed for the study of symmetries and symmetric structures, and therefore many sciences have to deal with them. Some popular representations of a group by a graph are the CAYLEY representation ([5], [9]), coset representation [9], maps and hypermaps [7], [8] . . . . A lot of work has been done about these graphs ([3]). These graphs have very both nice properties and highly-regularity properties. The regularity and the underlying algebraic structure of CAYLEY graphs make them good candidates for the applications such as optimization on parallel architectures ([1]), or for the study of interconnection networks ([2]), see also [4].

The purpose of this paper is to introduce a new type of graphs called  $\mathbb{G}$ -graphs constructed from a group. The algorithm to construct them is simple. These graphs, like the graphs cited above, have both nice and regular properties. Consequently these graphs can be used in any areas of science where CAYLEY graphs, coset graphs or hypermaps occur. However, CAYLEY graphs are always regular, a property that can be a limitation in some cases;  $\mathbb{G}$ -graphs can be either regular or non-regular. CAYLEY graphs cannot give any information on their corresponding groups, all groups of the same order give the same graphs if  $S = G$ , where  $S$  is the set of elements chosen for constructing the graphs, two

---

2000 Mathematics Subject Classification: 05C25, 20B25.

Keywords: graph theory, computational group theory, graphical representation of groups, symmetric graphs, semisymmetric graphs.

$\mathbb{G}$ -graphs will never give the same graph if groups are abelian. In this paper, after a presentation of the  $\mathbb{G}$ -graphs, we will give some basic properties. A list of classical graphs which are  $\mathbb{G}$ -graphs will be established.

## 2. Groups

We consider the category whose *objects* are couples  $(G; S)$  where  $G$  is a group and  $\emptyset \neq S \subset G$ ; and *morphisms* are  $f: (G_1; S_1) \rightarrow (G_2; S_2)$  where

- ◊  $f: G_1 \rightarrow G_2$  is a morphism of groups,
- ◊  $f(S_1) \subset S_2$ .

The composition of morphisms is clear;

$f: (G_1; S_1) \rightarrow (G_2; S_2)$  is an *isomorphism* if and only if

- ◊  $f: G_1 \rightarrow G_2$  is an isomorphism of groups,
- ◊  $f(S_1) = S_2$

We denote by  $\langle S \rangle$  the subgroup generated by  $S$ .

## 3. Graphs

The graphs  $\Gamma = (V; E; \varepsilon)$  considered here are undirected, with multi-edges and loops:

$V$  is the set of vertices,

$E$  is the set of edges,

$\varepsilon$  is the incidence map ( $\varepsilon: E \rightarrow \mathcal{P}(V)$ ) that assigns to every edge  $e \in E$  the *extremities* of  $e$ :  $\{x, y\}$ , or  $\{x\}$  for a loop; we use the notation  $\varepsilon(e) = [x, y]$  for bring together the two cases.

If  $x, y \in V$ , the set  $\{e \in E : \varepsilon(e) = [x, y]\}$  is called a *multi-edge* (a *n-edge* if the cardinality of this set is  $n$ ).

For  $x \in V$  the degree of  $x$  is

$$d(x) = \text{card}\{e : e \in E \ \& \ (\exists y \in V)(y \neq x \ \& \ \varepsilon(e) = \{x, y\})\} \\ + 2 \text{card}\{e : e \in E \ \& \ \varepsilon(e) = \{x\}\}.$$

A graph  $\Gamma = (V; E; \varepsilon)$  is *connected* if for every  $x, y \in V$  there exists a *walk* from  $x$  to  $y$ :  $e_1, \dots, e_n \in E$  ( $n \geq 1$ ) such that if  $\varepsilon(e_i) = [x_i, y_i]$ ,  $1 \leq i \leq n$ , one has  $x_1 = x$  and  $y_n = y$ .

$\varphi: \Gamma_1 = (V_1; E_1; \varepsilon_1) \rightarrow \Gamma_2 = (V_2; E_2; \varepsilon_2)$  is a *morphism* if  $\varphi = (f, f^\#)$  where

- ◇  $f: V_1 \rightarrow V_2$  is a map,
- ◇◇  $f^\#: E_1 \rightarrow E_2$  is a map,
- ◇◇◇  $(\forall e_1 \in E_1)(\varepsilon_2(f^\#(e_1)) = f(\varepsilon_1(e_1)))$ .

*Composition* of morphisms:  $(g, g^\#) \circ (f, f^\#) := (g \circ f, g^\# \circ f^\#)$

A morphism  $\varphi: \Gamma_1 = (V_1; E_1; \varepsilon_1) \rightarrow \Gamma_2 = (V_2; E_2; \varepsilon_2)$ ,  $\varphi = (f, f^\#)$ , is an *isomorphism* if there exists a morphism  $\psi: \Gamma_2 = (V_2; E_2; \varepsilon_2) \rightarrow \Gamma_1 = (V_1; E_1; \varepsilon_1)$ ,  $\psi = (g, g^\#)$ , such that

$$(g, g^\#) \circ (f, f^\#) = (\text{Id}_{V_1}, \text{Id}_{E_1}) \quad \text{and} \quad (f, f^\#) \circ (g, g^\#) = (\text{Id}_{V_2}, \text{Id}_{E_2}).$$

## 4. $k$ -Graphs

The graph  $\Gamma = (V; E; \varepsilon)$  is said to be  $k$ -partite ( $k \geq 1$ ) if there exists a partition  $V = \bigsqcup_{i \in I} V_i$  such that  $\text{card } I = k$  and

$$(\forall x, y \in V)(\forall i \in I)(\forall e \in E)((\varepsilon(e) = [x, y] \ \& \ x, y \in V_i) \implies x = y).$$

$\Gamma$  is a  $k$ -graph if it is 1-partite (just loops as edges) or if it is  $k$ -partite,  $k \geq 2$ , and not  $(k-1)$ -partite. We use the notation  $\Gamma = \left( \bigsqcup_{i \in I} V_i; E; \varepsilon \right)$ .

A  $*$ -partite graph is a  $k$ -partite graph for some  $k \geq 1$ .

*Morphism* of  $*$ -partite graphs is

$$\varphi: \Gamma_1 = \left( \bigsqcup_{i \in I_1} V_i; E_i; \varepsilon_1 \right) \longrightarrow \Gamma_2 = \left( \bigsqcup_{j \in I_2} W_j; E_j; \varepsilon_2 \right)$$

where

- ◇  $\varphi = (f, f^\#)$  is a morphism of graphs,
- ◇◇  $(\forall i \in I_1)(\exists j \in I_2)(f(V_i) \subset W_j)$ .

It is clear that if  $\varphi$  is a  $*$ -isomorphism, then  $\text{card } I_1 = \text{card } I_2$ ; we note  $\Gamma_1 \simeq_* \Gamma_2$  when  $\Gamma_1$  and  $\Gamma_2$  are isomorphic  $*$ -partite graphs.

## 5. Associating a $*$ -partite graph to $(G; S)$

From now on the groups considered are finite; the unit element of  $G$  is denoted by 1.

Let  $(G; S)$  be as in §2. We shall construct:

$$(G; S) \xrightarrow{\mathcal{F}} \Gamma = \left( \bigsqcup_{s \in S} V_s; E; \varepsilon \right)$$

in the following way:

1) vertices:

for all  $s \in S$  let  $g_s: G \rightarrow G$ ,  $x \mapsto sx$ , the left  $s$ -translation,  $g_s \in \mathfrak{S}_G$ , be decomposed into disjoint cycles:  $g_s = \alpha_1 \circ \alpha_2 \circ \dots \circ \alpha_{r_s}$  ( $r_s \geq 1$ ) where

$$\begin{aligned} \alpha_1 &= (1, s, s^2, \dots, s^{\alpha-1}), \\ \alpha_2 &= (x, sx, \dots, s^{\alpha-1}x), \\ &\vdots \end{aligned}$$

$\alpha = \text{ord}(s)$  is the order of  $s$  in  $G$ , and one has  $r_s = \frac{\text{ord}(G)}{\text{ord}(s)}$ ;  
let  $V_s := \{\alpha_i : 1 \leq i \leq r_s\}$  and  $V = \bigsqcup_{s \in S} V_s$ .

**NOTATION.**

$$\begin{aligned} \text{cycle } \alpha &= (x, sx, \dots, s^{\alpha-1}x) && \text{denoted by } (s)x, \\ \text{supp } \alpha &= \{x, sx, \dots, s^{\alpha-1}x\} && \text{denoted by } \langle s \rangle x, \end{aligned}$$

2) edges:

for  $(s)x, (t)y \in V$ , if  $\#(\langle s \rangle x \cap \langle t \rangle y) = p$ ,  $p \geq 1$ , one constructs a  $p$ -edge between  $(s)x$  and  $(t)y$ : precisely the edges are labelled  $e = [(s)x, (t)y], u$  where  $u$  varies in the set  $\langle s \rangle x \cap \langle t \rangle y$ ; one settles  $\varepsilon(e) = [(s)x, (t)y]$ .

So every vertex  $(s)x \in V_s$  has an  $\text{ord}(s)$ -loop, and the graph is  $k$ -partite, where  $k = \#S$  (since if  $y \notin \langle s \rangle x$  one has  $\langle s \rangle x \cap \langle s \rangle y = \emptyset$ ).

It is easy to prove that this procedure is polynomial in time:  $0(n^3)$ .

**Remark.** Indeed the loops could be omitted (giving superfluous data) but it is convenient to keep these data, because, by Proposition 4, a morphism of groups gives rise to a morphism of graphs (cf. also Proposition 6).

## 6. Properties

**PROPOSITION 1.** *If  $\#S = k$ , then  $\mathcal{F}(G; S)$  is a  $k$ -graph.*

*Proof.* If  $k = 1$ , the result is clear. If  $k \geq 2$  and  $\Gamma = \mathcal{F}(G; S)$  were  $k'$ -partite,  $k' < k$ , then  $\Gamma$  would be  $k'$ -colorable; but  $1 \in \bigcap_{s \in S} \langle s \rangle$ ; and if we consider  $W = \{(s)1 : s \in S\}$ , we get for every  $s, t \in S$ : there exists at least an edge between  $(s)1$  and  $(t)1$  ( $1 \in \langle s \rangle \cap \langle t \rangle$ ) and  $\#W = k$  so the induced sub-graph defined by  $W$  cannot be  $k'$ -colorable:  $W$  is a clique with  $k$  edges.  $\square$

**PROPOSITION 2.**

- i)  $(\forall v \in V_s)(d(v) = \text{ord}(s)(1 + \#S)),$
- ii)  $\#E = \frac{\#S(1+\#S)}{2} \cdot \#G.$

*Proof.* Easy computation. □

**PROPOSITION 3.**  $\mathcal{F}(G; S)$  is connected if and only if  $\langle S \rangle = G$ .

*Proof.*

- ◊ If  $\langle S \rangle = G$ , let  $(s)x, (t)y \in V$ ; one has  $y = s_1 \cdots s_n x$ ,  $s_i \in S$ , hence

$$\begin{aligned} x &\in \langle s \rangle x \cap \langle s_n \rangle x, \\ sx &\in \langle s_n \rangle x \cap \langle s_{n-1} \rangle s_n x, \\ &\vdots \\ s_2 \cdots s_n x &\in \langle s_2 \rangle s_3 \cdots s_n x \cap \langle s_1 \rangle s_2 \cdots s_n x, \\ y &\in \langle s_1 \rangle s_2 \cdots s_n x \cap \langle t \rangle y; \end{aligned}$$

this gives a walk from  $(s)x$  to  $(t)y$ .

- ◊ If  $\mathcal{F}(G; S)$  is connected, let  $x \in G$ ; fix  $s_0 \in S$ : there exists a walk  $(s_0) \rightarrow (s_1)x_1 \rightarrow \cdots \rightarrow (s_n)x_n \rightarrow (s_{n+1})x_{n+1} := (s_0)x$ , hence

$$\begin{aligned} (\exists y_1)(y_1 \in \langle s_0 \rangle \cap \langle s_1 \rangle x_1) &\implies s_0^{i_0} = s_1^{j_0} x_1 \implies x_1 = s_1^{-j_0} s_0^{i_0} \in \langle S \rangle, \\ (\exists y_2)(y_2 \in \langle s_1 \rangle x_1 \cap \langle s_2 \rangle x_2) &\implies s_1^{i_1} x_1 = s_2^{j_1} x_2 \implies x_2 = s_2^{-j_1} s_1^{i_1} x_1 \in \langle S \rangle, \\ &\vdots \\ (\exists y_n)(y_n \in \langle s_{n-1} \rangle x_{n-1} \cap \langle s_n \rangle x_n) &\implies s_{n-1}^{i_{n-1}} x_{n-1} = s_n^{j_{n-1}} x_n \\ &\implies x_n = s_n^{-j_{n-1}} s_{n-1}^{i_{n-1}} x_{n-1} \in \langle S \rangle, \\ (\exists y_{n+1})(y_{n+1} \in \langle s_n \rangle x_n \cap \langle s_0 \rangle x) &\implies s_n^{i_n} x_n = s_0^{j_n} x \\ &\implies x = s_0^{-j_n} s_n^{i_n} x_n \in \langle S \rangle, \end{aligned}$$

precisely  $x = s_0^{-j_n} s_n^{i_n} s_{n-1}^{-j_{n-1}} \cdots s_2^{i_2} s_1^{i_1} s_0^{i_0}$ . □

**Remark.** Every decomposition  $x = s_{m+1}^{\alpha_{m+1}} \cdots s_1^{\alpha_1} s_0^{\alpha_0}$  gives a walk  $(s_0) \rightarrow (s_1)x_1 \rightarrow \cdots \rightarrow (s_{m+1})x_{m+1} \rightarrow (s_0)x$ .

**PROPOSITION 4.**  $\mathcal{F}$  supply a covariant functor from the category of  $(G; S)$ ,  $G$  finite, to the category of  $*$ -partite graphs.

*Proof.* If  $(G_1; S_1) \xrightarrow{h} (G_2; S_2)$  is a morphism, one defines  $\mathcal{F}(h) = (f, f^\#)$  in the following way:

$$\mathcal{F}(h): \Gamma_1 = \left( \bigsqcup_{s \in S_1} V_s; E_1; \varepsilon_1 \right) \longrightarrow \Gamma_2 = \left( \bigsqcup_{t \in S_2} W_t; E_2; \varepsilon_2 \right)$$

$$\diamond f((s)x) := (h(s))h(x),$$

$$\diamond \text{ if } e_1 = [(s)x, (s')y], u \in E_1, f^\#(e_1) := ([f((s)x), f((s')y)], h(u)) \in E_2$$

One can verify that  $\mathcal{F}(h \circ h') = \mathcal{F}(h) \circ \mathcal{F}(h')$ .  $\square$

Also we have  $\mathcal{F}(\text{Id}_G) = \text{Id}_{\mathcal{F}(G)}$ , therefore:

**COROLLARY.** *If  $(G_1; S_1) \simeq (G_2; S_2)$ , then  $\mathcal{F}(G_1; S_1) \simeq_* \mathcal{F}(G_2; S_2)$ .*

The converse is false:  $(D_4; \{r, s\})$  and  $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}; S)$  where  $S = \{(\bar{1}, \bar{0}), (\bar{0}, \bar{1})\}$  have the same 2-graph associated.

## 7. Case $S = G$

We denote  $\mathcal{F}(G; G)$  by  $\Gamma_G$ ; for  $d \geq 1$  let  $\text{ord}_d(G) := \#\{x \in G : \text{ord}(x) = d\}$ . Consider for the (finite) groups  $G_1, G_2$  the properties:

$$(P_1) \quad G_1 \simeq G_2,$$

$$(P_2) \quad \Gamma_{G_1} \simeq_* \Gamma_{G_2},$$

$$(P_3) \quad (\forall d \in \{1, 2, \dots\}) (\text{ord}_d(G_1) = \text{ord}_d(G_2))$$

**PROPOSITION 5.** *We have:*

$$(P_1) \xrightarrow{\implies} (P_2) \xrightarrow{\implies} (P_3),$$

**P r o o f .**

$(P_2) \implies (P_3)$ : there exists a  $*$ -isomorphism

$$\Gamma_{G_1} = \left( \bigsqcup_{s \in G_1} V_s; E_1; \varepsilon_1 \right) \xrightarrow{(f, f^\#)} \Gamma_{G_2} = \left( \bigsqcup_{t \in G_2} W_t; E_2; \varepsilon_2 \right),$$

$f: \bigsqcup_{s \in G_1} V_s \rightarrow \bigsqcup_{t \in G_2} W_t$  induces a bijection  $g: G_1 \rightarrow G_2$  such that  $f(V_s) = W_{g(s)}$ ;

also

$$\#E_i = \frac{\text{ord}(G_i)^2(\text{ord}(G_i) + 1)}{2}, \quad i = 1, 2 \quad (\text{Proposition 2}).$$

Hence  $\#G_1 = \#G_2 =: n$ .

Let  $s \in G_1$ ,  $\text{ord}(s) = d$ ; to this correspond  $\frac{n}{d}$  vertices: the elements of  $V_s$ ; for every  $v \in V_s$

$$d(v) = \text{ord}(s)(\text{ord}(G_1) + 1) = d(\text{ord}(G_1) + 1),$$

hence  $f(v) \in W_{g(s)}$  has degree  $d \cdot (\text{ord}(G_2) + 1)$ ; but every  $w \in W_{g(s)}$  has degree  $d(w) = \text{ord}(g(s))(\text{ord}(G_2) + 1)$ ; we conclude that  $\text{ord}(g(s)) = d = \text{ord}(s)$ .

(P<sub>3</sub>)  $\not\Rightarrow$  (P<sub>2</sub>): there exist three non isomorphic groups  $G_1, G_2, G_3$  of order 81 verifying (P<sub>3</sub>):  $(\forall d \in \{1, 2, \dots\})(\text{ord}_d(G_1) = \text{ord}_d(G_2) = \text{ord}_d(G_3))$  with  $\Gamma_{G_1} \simeq_* \Gamma_{G_2} \not\equiv_* \Gamma_{G_3}$ .  $\square$

As a consequence  $\Gamma_{D_4} \not\equiv_* \Gamma_{\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}$  since for  $D_4$  (dihedral group with 8 elements) there exist 2 elements of order 4, and for  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  there exist 4 elements of order 4.

**COROLLARY.** *If  $G_1, G_2$  are abelian and  $\Gamma_{G_1} \simeq_* \Gamma_{G_2}$ , then  $G_1 \simeq G_2$ .*

*P r o o f.* It is well know that two abelian groups having the same number of elements of each order are isomorphic.  $\square$

Cyclic groups have special graphs:

**PROPOSITION 6.** *If  $\text{ord}(G) = n$  and for every  $d, d \mid n$ , there exist exactly  $\frac{n}{d}\varphi(d)$   $d$ -loops in  $\Gamma_G$  ( $\varphi$  Euler characteristic), then  $G$  is cyclic.*

*P r o o f.* If  $\text{ord}(x) = d$ , we have  $\frac{n}{d}$  vertices with a  $d$ -loop, hence if  $\text{ord}_d := \#\{x \in G : \text{ord}(x) = d\}$ , then

$$(\forall d \in \{1, 2, \dots\})(d \mid n \implies \#\{v \in V : v \text{ has a } d\text{-loop}\} = \frac{n}{d} \text{ord}_d).$$

Consequently the  $d$ -loops number is  $\frac{n}{d} \text{ord}_d$ . By hypothesis one have  $\frac{n}{d} \text{ord}_d \leq \frac{n}{d} \varphi(d)$ , so  $n = \sum_{d \mid n} \text{ord}_d \leq \sum_{d \mid n} \varphi(d) = n$ . That leads to  $\text{ord}_d = \varphi(d)$ , and if  $d = n$ , then  $\text{ord}_n = \varphi(n)$  and  $G$  is cyclic.  $\square$

Especially for  $G = \mathbb{Z}/p\mathbb{Z}$ ,  $p$  prime,  $\Gamma_G$  has  $p$  vertices with 1-loop and  $p - 1$  vertices with  $p$ -loop.

### Short list of classical graphs which are $\mathbb{G}$ -graphs.

We give here some examples of  $\mathbb{G}$ -graphs. This list has been established using GAP ([5]). More examples can be found in [6]. The corresponding groups are indicated between parenthesis:

1. Bipartite complete graphs ( $G = C_n \times C_k, S = \{(1, 0)(0, 1)\}$ ),
2. The 3-prism ( $G = C_3 \times C_3, S = \{(1, 0)(0, 1)\}$ ),
3. The cuboctahedral graph  
( $G = C_2 \times C_2 \times C_2, S = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ ),
4. The square ( $G$  is the Klein's group,  $G = \{e, a, b, ab\}$ , and  $S = \{a, b\}$ ),
5. The generalized Petersen's graph  $P_{8,3}$   
( $G = \text{SmallGroup}(24, 3), S = \{f1, f1*f2\}$ ),
6. The cube ( $G = A_4, S = \{(123), (134)\}$ ),
7. The hypercube ( $G = \text{SmallGroup}(32, 6), S = \{f1, f1*f2\}$ ),
8. The  $2 \times 2$  grid on a 3D torus ( $G = Q_2, S = \{a, b\}$ ),
9. The  $3 \times 3$  grid on a 3D torus ( $G = D_6, S = \{s \in G : \text{ord}(s) = 2\}$ ),
10. The  $4 \times 4$  grid on a 3D torus ( $G = \text{SmallGroup}(32, 6), S = \{f1, f1*f2\}$ ),



## REFERENCES

- [1] ANNEXSTEIN, F.—BAUMSLAG, M.—ROSENBERG, A. L. : *Group action graphs and parallel architectures*, SIAM J. Comput **19** (1990), 544–569.
- [2] AKERS, S.—KRISHNAMURTHY, B. : *Group graphs as interconnection networks*. In: Proc. 14th Internat. Conf. Fault Tolerant Comput., 1984, pp. 422–427.
- [3] BABAI, L. : *Automorphism groups, isomorphism, reconstruction*. In: Handbook of Combinatorics, Vol. 1–2 (R. Graham, M. Grötschel, R. Lovasz, eds.), Elsevier Science B.V., Amsterdam, 1995, Chap. 27.
- [4] COOPERMAN, G.—FINKELSTEIN, L.—SARAWAGI, N. : *Applications of Cayley graphs*. In: Appl. Algebra and Error-Correcting Codes. Lecture Notes in Comput. Sci. 508, Springer-Verlag, Berlin, 1991, pp. 367–378.
- [5] The GAP Team (06May 2002) : *GAP — Reference Manual*, Release 4.3, <http://www.gap-system.org>.
- [6] GILLIBERT, L. : *Représentation graphique et informatique des groupes*. Mémoire de DEA Informatique, Université de Caen, Département d’informatique, Directeur A. Bretto, 2003.
- [7] JONES, G. A. : *Graphs, groups and surfaces*, Rend. Sem. Mat. Messina Ser. II **24** (2002), 71–85.
- [8] JONES, G. A.—SINGERMAN, D. : *Theory of maps on orientable surfaces*, Proc. London Math. Soc. (3) **37** (1978), 273–307.
- [9] LAURI, J.—SCAPELLATO, R. : *Topics in Graphs Automorphisms and Reconstruction*. London Math. Soc. Stud. Texts 54, Cambridge University Press, Cambridge 2003.
- [10] MCKAY, B. D. : *Nauty User’s Guide, Version 2.2*, Computer Science Department, Australian National University.

Received September 12, 2003

Revised February 24, 2004

\* *Univ. Caen GREYC CNRS UMR 6072  
Campus II  
Bd Maréchal Juin BP 5186  
14032 Caen cedex  
FRANCE  
E-mail: bretto@info.unicaen.fr*

\*\* *Laboratoire d’Arithmétique et d’Algèbre  
Univ. St-Etienne  
23 rue Michelon 42023  
Saint-Etienne cedex 2  
FRANCE  
E-mail: faisant@univ-st-etienne.fr*