REPORTS@SCM

AN ELECTRONIC JOURNAL OF THE SOCIETAT CATALANA DE MATEMÀTIQUES

Volume 1, num. 1, 2014

ISSN (electronic edition): 2385 - 4227

http://reportsascm.iec.cat

Institut d'Estudis Catalans

REPORTS@SCM

AN ELECTRONIC JOURNAL OF THE
SOCIETAT CATALANA DE MATEMÀTIQUES

Volume 1, number 1

October 2014

http://reportsascm.iec.cat
ISSN electronic edition: 2385 - 4227

Societat Catalana de Matemàtiques

Institut d'Estudis Catalans

Focus and Scope

Reports@SCM is a non-profit electronic research journal on Mathematics published by the Societat Catalana de Matemàtiques (SCM) which originated from the desire of helping students and young researchers in their first steps into the world of research publication.

Reports@SCM publishes short papers (maximum 10 pages) in all areas of pure mathematics, applied mathematics, and mathematical statistics, including also mathematical physics, theoretical computer science, and any application to science or technology where mathematics plays a central role. To be considered for publication in Reports@SCM an article must be written in English (with an abstract in Catalan), be mathematically correct, and contain some original interesting contribution. All submissions will follow a peer review process before being accepted for publication.

Research announcements containing preliminary results of a larger project are also welcome. In this case, authors are free to publish in the future any extended version of the paper elsewhere, with the only condition of making an appropriate citation to Reports@SCM.

We especially welcome contributions from researchers at the initial period of their academic careers, such as Master or PhD students. We wish to give special attention to the authors during the whole editorial process. We shall take special care of maintaining a reasonably short average time between the reception of a paper and its acceptance, and between its acceptance and its publication.

All manuscripts submitted will be **peer reviewed** by at least one reviewer. Final decisions on the acceptance of manuscripts are taken by the editorial board, based on the reviewer's opinion.

Edited by Societat Catalana de Matemàtiques, Institut d'Estudis Catalans (IEC)
Carrer del Carme 47, 08001 Barcelona.
http://scm.iec.cat Telèfon: (+34) 93 324 85 83
scm@iec.cat Fax: (+34) 93 270 11 80

Linguistic revision by Enric Ventura.

Institut d'Estudis Catalans
http://www.iec.cat
informacio@iec.cat

http://reportsascm.iec.cat
ISSN electronic edition: 2385-4227

Reports@SCM
Volume 1, number 1, 2014

Table of Contents

REPORTS@SCM
AN ELECTRONIC JOURNAL OF THE
SOCIETAT CATALANA DE MATEMÀTIQUES

On computing flat outputs through Goursat normal form

*Jaume Franch
Universitat Politècnica de Catalunya
jfranch@ma4.upc.edu

Ana Manzanera
Universitat Politècnica de Catalunya
anamanzaneragarrido@gmail.com

Gemma Valero
Universitat Politècnica de Catalunya
gemmavaleromartinez@gmail.com

*Corresponding author

Resum *(CAT)*
Aquest article estudia el càlcul de les sortides planes mitjançant la forma normal de Goursat del sistema de Pfaff associat a qualsevol sistema de control en variables d'estat. L'algorisme consta de tres passos: i) transformació del sistema de control en el seu sistema de Pfaff equivalent; ii) càlcul de la forma normal de Goursat; iii) reescriptura de les equacions en les noves variables d'estat. Aquí, una realimentació simplifica les equacions i, per tant, les sortides planes es calculen de manera senzilla. L'algorisme s'aplica a un vehicle amb rodes extensibles. Gràcies a la propietat de planitud diferencial, s'obtenen les trajectòries entre dos punts donats.

Abstract *(ENG)*
This paper is devoted to computation of flat outputs by means of the Goursat normal form of the Pfaffian system associated to any control system in state space form. The algorithm consists of three steps: i) transformation of the system into its Pfaffian equivalent; ii) computation of the Goursat normal form; iii) rewriting of the state space equations in the new variables. Here, a feedback law simplifies the equations and, therefore, the flat outputs can be easily computed. The algorithm is applied to a car with expanding wheels. Point to point trajectories are obtained thanks to the property of differential flatness.

Keywords: *Feedback linearization, differential flatness, nonlinear control.*
MSC (2010): *93B18, 93B29, 93C10.*
Received: *October 25th, 2013.*
Accepted: *January 29th, 2014.*

Acknowledgement
The authors want to thank the support of *Ministerio de Ciencia e Innovación* of the Spanish Government under the project MTM2011-22585.

Societat Catalana de Matemàtiques
Institut d'Estudis Catalans

1. Introduction

Since 1980, the problem of feedback linearization for nonlinear control systems has been considered by different authors in several frameworks. Different routes to linearization have been traced; namely, linearization by static feedback; linearization by prolongations; linearization by dynamic feedback, and finally flatness. The main mathematical tool to study these problems is differential geometry. Notions such as Lie brackets and involutive fields or distributions, which can be found in basic books of nonlinear control theory [9, 14], have been followed by differential forms and Pfaffian systems [3, 15].

Differential flatness was introduced in the 90's by Michel Fliess and coworkers [5]. A differentially flat nonlinear system can perform any point-to-point desired trajectory. Other systems do not hold this property. Differentially flat systems are dinamically feedback equivalents to linear systems based on chains of integrators. Initial and final conditions are transferred, through diffeomorphism, to the equivalent linear system where the required inputs are designed. Inputs of the nonlinear system are obtained by application of the diffeomorphism and the feedback law.

Unfortunately, necessary and sufficient conditions to check flatness for a general nonlinear system do not exist. Since mid nineties, extensive work has been done in this direction, but only some particular cases have been solved [6, 11, 12].

Control systems are usually presented in state space form. In this paper, we convert state space form control systems into their equivalent Pfaffian systems [3, 15]. A Pfaffian system consists in a set of independent one forms. These one forms are written in the Goursat normal form which, when transformed again in state space equations, become very simple equations by addition of a feedback law and, hence, allow to find the flat outputs in an easily manner.

This paper is organized as follows: Section 2 contains a summary on how to compute Goursat normal forms for a set of independent one forms, as well as a brief introduction to nonlinear control systems. In Section 3 the relationship between control systems in state space form and its equivalent Pfaffian system is explained. The main contribution of this paper is the link between the Goursat normal form and the computation of the flat outputs. The inclusion of a feedback law plays a crucial role in this sense. Details on how to compute the flat outputs once the Goursat normal form is achieved are also explained. Section 4 is devoted to illustrate the whole process through an example, which corresponds to a system with expanding wheels [1]. Simulations are given in Section 5, where an additional control law is applied to overcome errors in the initial conditions. The paper ends with the conclusions. A reduced version of this paper has been accepted for publication at European Control Conference 2014 [7].

2. Background

2.1 Normal form for differential one forms

This section provides a very brief summary on how to compute normal forms for differential one forms. A detailed approach can be found, for example, in [3, 15]. In the sequel, all the vector fields an differential forms are supposed to be $\mathcal{C}^\infty$.

Definition 2.1. A system of the form

$$\alpha_1 = \alpha_2 = \cdots = \alpha_s = 0,$$

where the α_i are independent 1-forms on an n-dimensional manifold, is called a *Pfaffian system*.

Definition 2.2. A *smooth codistribution* smoothly associates a subspace of the cotangent space at each point $p \in M$.

Definition 2.3. The sequence of decreasing codistributions

$$I^{(k)} \subset I^{(k-1)} \subset \cdots \subset I^{(1)} \subset I^{(0)}$$

is called the *derived flag* of $I^{(0)}$, where

$$I^{(k+1)} = \{\lambda \in I^{(k)} : d\lambda \equiv 0 \mod I^{(k)}\}.$$

Definition 2.4. Let $\alpha \in \Omega^1(M)$. The integer r defined by $(d\alpha)^r \wedge \alpha \neq 0$ and $(d\alpha)^{r+1} \wedge \alpha = 0$ is called *rank* of α.

We are interested in transforming the generators of Pfaffian systems into a normal form by means of a coordinate transformation. Let us study first Pfaffian systems of codimension 1, or systems consisting of a single equation $\alpha = 0$. The following theorem allows us, under a rank condition, to write α in a normal form.

Theorem 2.5 (Pfaff Theorem). *Let $\alpha \in \Omega^1(M)$ have constant rank r in a neighborhood of p. Then, there exists a coordinate chart (U, z) such that, in these coordinates,*

$$\alpha = dz_1 + z_2 dz_3 + \cdots + z_{2r} dz_{2r+1}.$$

The proof is constructive and is based on finding functions $f_1, \dots, f_{r+1}$ and $g_1, \dots, g_r$ ($2r+1 < n$, where $\dim M = n$) such that

$$(d\alpha)^r \wedge \alpha \wedge df_1 = 0,$$
$$(d\alpha)^{r-1} \wedge \alpha \wedge df_1 \wedge df_2 = 0,$$

up to f_r,

$$\begin{aligned} d\alpha \wedge \alpha \wedge df_1 \wedge df_2 \wedge \cdots \wedge df_r &= 0, \\ \alpha \wedge df_1 \wedge df_2 \wedge \cdots \wedge df_r &\neq 0, \end{aligned}$$

so that,

$$\alpha = df_{r+1} + g_1 df_1 + \cdots + g_r df_r.$$

A new set of variables, diffeomorphic to the state space variables, is defined as follows:

$$z_1 = f_{r+1}, \quad z_{2i} = g_i, \quad z_{2i+1} = f_i,$$

with $1 \leq i \leq r$.

For Pfaffian systems of codimension two, a particular case is given by Pfaffian system with four variables. The algorithm to transform the one forms into a canonical form is obtained in Engel's theorem:

Theorem 2.6 (Engel's Theorem). *Let I be a dimension two codistribution, spanned by $I = \langle \alpha_1, \alpha_2 \rangle$ of four variables. Setting $I^{(0)} = I$, if the derived flag satisfies*

$$dim\ I^{(1)} = 1,$$
$$dim\ I^{(2)} = 0,$$

then there exist coordinates z_1, z_2, z_3, z_4 such that

$$I = \{dz_4 - z_3 dz_1, dz_3 - z_2 dz_1\}.$$

The proof is also constructive and uses the previous theorem.

Engel's theorem can be generalized to a system with n configuration variables and $n-2$ constraints. The following theorem states the conditions required in order to convert a Pfaffian system into its Goursat normal form.

Theorem 2.7 (**Goursat Normal Form).** *Let I be a Pfaffian system spanned by s 1-forms, $I = \{\alpha_1, \dots, \alpha_s\}$, on a space of dimension $n = s+2$, such that*

$$d\alpha_s \not\equiv 0 \mod I.$$

Assume also that there exists an exact form π, with $\pi \neq 0 \mod I$, satisfying the Goursat congruences

$$d\alpha_i \equiv -\alpha_{i+1} \wedge \pi \mod \alpha_1, \dots, \alpha_i, \quad 1 \leq i \leq s-1.$$

Then there exists a coordinate system $z_1, z_2, \dots, z_n$ in which the Pfaffian system is in Goursat normal form,

$$I = \{dz_3 - z_2 dz_1, dz_4 - z_3 dz_1, \dots, dz_n - z_{n-1} dz_1\}.$$

Finally, in order to study Pfaffian systems of codimension greater than two, we will use the extended Goursat normal form. That is, a Pfaffian system of codimension $m+1$ and generated by n constraints of the form

$$I = \{dz_i^j - z_{i-1}^j dz_0 : i = 1, \dots, s_j;\ j = 1, \dots, m\}.$$

Conditions to convert a Pfaffian system into the extended Goursat normal form are given in the following theorem:

Theorem 2.8 (**Extended Goursat Normal Form).** *Let I be a Pfaffian system of codimension $m+1$ in $\mathbb{R}^{n+m+1}$. The system can be put into the extended Goursat normal form if, and only if, there exists a set of generators $\{\alpha_i^j : i = 1, \dots, s_j;\ j = 1, \dots, m\}$ for I and an exact one-form π such that, for all j,*

$$\begin{aligned} d\alpha_i^j &\equiv -\alpha_{i+1}^j \wedge \pi \qquad \mod I^{(s_j - i)}, \quad i = 1, \dots, s_j - 1, \\ d\alpha_i^j &\not\equiv 0 \qquad\qquad\ \ \mod I. \end{aligned}$$

All the proofs of these theorems are constructive and are outlined in [3, 15].

2.2 Feedback linearization of control systems

Definition 2.9. A nonlinear control system

$$\dot{x} = f(x) + \sum_{i=1}^{m} g_i(x) u_i \quad x \in \mathbb{R}^n \tag{1}$$

is said to be *static feedback linearizable* if it is possible to find a feedback

$$u = \alpha(z) + \beta(z) v, \quad u \in \mathbb{R}^m, \quad v \in \mathbb{R}^m, \quad z \in \mathbb{R}^n,$$

and a local diffeomorphism

$$z = \phi(x)$$

such that the original system is transformed into a linear controllable system

$$\dot{z} = Az + Bv,$$

where A and B are matrices of appropriate size.

Necessary and sufficient conditions to check static feedback linearization were given in [8, 10]. A generalization of the static feedback linearization is a dynamic feedback transformation [4].

Definition 2.10. A nonlinear system

$$\dot{x} = f(x, u), \quad x \in \mathbb{R}^n, \quad u \in \mathbb{R}^m, \tag{2}$$

is said to be *dynamic feedback linearizable* if there exists:

1. A regular dynamic compensator
$$\begin{cases} \dot{z} = a(x, z, v) \\ u = b(x, z, v) \end{cases} \tag{3}$$
with $z \in \mathbb{R}^q$ and $v \in \mathbb{R}^m$. The regularity assumption implies the invertibility of (3) with input v and output u.

2. A local diffeomorphism
$$\psi = \Psi(x, z) \tag{4}$$
with $\psi \in \mathbb{R}^{n+q}$, such that the original system (2) with the dynamic compensator (3), after applying (4), becomes a constant linear controllable system:
$$\dot{\psi} = A\psi + BV.$$

A system is dynamic feedback linearizable if, and only if, it is differentially flat. Differential flatness was introduced by M. Fliess and coworkers in [5].

Definition 2.11. Let (1) be a nonlinear system with m inputs. Roughly speaking, this system is differentially flat if there exist m functions $(y_1, \dots, y_m)$, equal in number to the number of inputs, such that:

1. Each variable y_i is a function of the states, the inputs, and a finite number of the inputs derivatives.

2. The states and the inputs can be expressed as functions of the variables $(y_1, \dots, y_m)$ and their derivatives up to a certain order.

The variables $(y_1, \dots, y_m)$ are called *flat outputs*.

The relationship between Goursat normal form of Pfaffian systems and nonholonomic [13] control systems in state space form is as follows. Given a two input driftless system

$$\dot{x} = g_1 u_1 + g_2 u_2, \quad x \in \mathbb{R}^n,$$

in state space form, its equivalent Pfaffian system can be obtained by finding $n-2$ one forms α_i, such that $\alpha_i \lrcorner g_1 = 0$ and $\alpha_i \lrcorner g_2 = 0$ for all $i = 1, \dots, n-2$.

By applying one of the above theorems, the Goursat normal form can be found. As explained above, this includes the definition of a new set of state variables $z_1, \dots, z_n$. The dynamics associated to the system in these new variables is got by differentiation of each of these variables, which leads to

$$\dot{z} = g_1(z)u_1 + g_2(z)u_2.$$

Finally, the above system can be expressed as

$$\begin{array}{rcl} \dot{z}_1 & = & \overline{u}_1, \\ \dot{z}_2 & = & \overline{u}_2, \\ \dot{z}_3 & = & z_2\overline{u}_1, \\ & \vdots & \\ \dot{z}_n & = & z_{n-1}\overline{u}_1, \end{array} \tag{5}$$

by application of a feedback law. A similar algorithm can be applied to any nonholonomic system. The structure of system (5) is very convenient in order to find the flat outputs.

3. Algorithm to find flat outputs

Consider the system given by

$$\dot{x} = \sum_{i=1}^{\overline{m}} g_i u_i, \quad x \in \mathbb{R}^{\overline{n}},$$

where $\overline{m}$ is the number of controls and $\overline{n}$ the dimension of state space.

First of all, an equivalent formulation of the system in differential forms will be given. In order to achieve this goal, $\overline{n}-\overline{m}$ differential forms that annihilate the control vector fields must be found. Then, the Pfaffian system consists in $\overline{n}-\overline{m}$ equations:

$$\omega_1 = \omega_2 = \ldots = \omega_{\overline{n}-\overline{m}} = 0,$$

where $\omega_i \in \langle g_1, \ldots, g_{\overline{m}} \rangle^{\perp}, \quad i = 1, \ldots, \overline{n}-\overline{m}$. Given a Pfaffian system in $\mathbb{R}^{n+m+1}$, where $\overline{n} = n+m+1$ and $\overline{m} = m+1$ is the transforming system codimension, these forms are expressed in their extended Goursat canonical form

$$I = \{\omega_i^j = dz_i^j - z_{i+1}^j dz_0 : i = 1, \ldots, s_j, \; j = 1, \ldots, m\},$$

where s_j satisfies that $\overline{n} = m + 1 + \sum_{j=1}^{m} s_j$.

At this point, the goal is to rewrite the system using vector fields. In order to do this, we must find $m+1$ vector fields that vanish on the ideal of forms, i.e., vector fields expressed in a generic form for $k = 0, \ldots, m$ as

$$\overline{g}_k = \left(a_0, a_1^1, \ldots, a_{s_1}^1, a_{s_1+1}^1, \ldots, a_1^m, \ldots, a_{s_m}^m, a_{s_m+1}^m\right)$$

meeting the following conditions:

$$\overline{g}_k \lrcorner \left\{ \begin{array}{c} dz_1^j - z_2^j \, dz_0 \\ dz_2^j - z_3^j \, dz_0 \\ \vdots \\ dz_{s_j}^j - z_{s_j+1}^j \, dz_0 \end{array} \right\} = 0, \quad j = 1, \ldots, m.$$

A possible solution is $\overline{g}_0$ such that:

$$\begin{array}{rcl} a_0 & = & 1 \\ a_1^j & = & z_2^j \\ & \vdots & \\ a_{s_j}^j & = & z_{s_j+1}^j \\ a_{s_j+1}^j & = & 0 \end{array}$$

and

$$\overline{g}_j = \frac{\partial}{\partial z^j_{s_j+1}}, \quad j = 1, \dots, m$$

so that, in the new variables, the system reads:

$$\left\{ \begin{array}{ccc} \dot{z}_0 & = & u_0 \\ \dot{z}^1_1 & = & z^1_2 u_0 \\ & \vdots & \\ \dot{z}^1_{s_1} & = & z^1_{s_1+1} u_0 \\ \dot{z}^1_{s_1+1} & = & u_1 \\ \dot{z}^2_1 & = & z^2_2 u_0 \\ & \vdots & \\ \dot{z}^2_{s_2} & = & z^2_{s_2+1} u_0 \\ \dot{z}^2_{s_2+1} & = & u_2 \\ & \vdots & \\ \dot{z}^m_1 & = & z^m_2 u_0 \\ & \vdots & \\ \dot{z}^m_{s_m} & = & z^m_{s_m+1} u_0 \\ \dot{z}^m_{s_m+1} & = & u_m. \end{array} \right. \tag{6}$$

Remark. The system obtained by application of the above algorithm and the system obtained by differentiation of the system variables $\left\{ z^j_i,\ i = 1, \dots, s_j,\ j = 1, \dots, m \right\}$ can be different. To get the same system a feedback law must be included.

From equations (6), it is straightforward to obtain the flat outputs. Consider $y_0 = z_0$ and $y_1 = z^1_1$ as the first flat outputs. Then, $z^1_2, \dots, z^1_{s_1+1}$, can be expressed in terms of y_0, y_1 and its derivatives, dividing both sides by u_0. The same happens for the remaining equation blocks. Therefore, the flat outputs are

$$\begin{array}{ccc} y_0 & = & z_0, \\ y_1 & = & z^1_1, \\ & \vdots & \\ y_m & = & z^m_1, \end{array}$$

and the remaining variables are expressed as:

$$\left\{ \begin{array}{c} z^j_2 = \dot{z}^j_1 / u_0 = \dot{y}_j / \dot{y}_0, \\ z^j_3 = \dot{z}^j_2 / u_0 = z^j_3 \left(\dot{y}_0, \ddot{y}_0, \dot{y}_j, \ddot{y}_j \right) \\ \vdots \\ z^j_{s_j+1} = \dot{z}^j_{s_j} / u_0 = z^j_{s_j+1} \left(\dot{y}_0, \dots, y_0^{(s_j)}, \dot{y}_j, \dots, y_j^{(s_j)} \right). \end{array} \right.$$

Considering $s_0 = \max\{s_1, \dots, s_m\}$, we need $s_0 + \overline{n}$ variables to describe $\overline{n}$ variables. So that, the system has to be prolonged as follows:

$$\begin{array}{ccc} z^0_1 & = & u_0, \\ & \vdots & \\ z^0_{s_0} & = & u_0^{(s_0-1)}, \\ v & = & \dot{z}^0_{s_0}. \end{array}$$

So far we have two well defined diffeomorphisms: one between the original state variables $(x_1, \dots, x_{\overline{n}})$ and the new state variables $(z_1, \dots, z_{\overline{n}})$ and the second one between $(z_1, \dots, z_{\overline{n}})$ and the flat outputs and their derivatives. So that, given a set of initial and final conditions for the original system, these conditions are mapped into system (6) through the diffeomorphism. These conditions, plus additional conditions for the extended variables, are transferred to initial and final conditions for the flat outputs by using the second diffeomorphism.

Given $2\,(s_j+1)$, $j=0,\dots,m$, initial and final conditions for each flat output and its derivatives, there exists a unique $2s_j+1$ degree polynomial that meets these conditions. Once the polynomial has been defined, the controls $u_j(t)$, $j=0,\dots,m$, must be found from these equations:

$$\begin{aligned} w_0 &= y_0^{(s_0+1)} = v, \\ w_j &= y_j^{(s_j+1)} = \frac{\mathrm{d}^{s_j+1}}{\mathrm{d}t^{s_j+1}} z_1^j, \quad j=1,\dots,m. \end{aligned}$$

Control laws for the original system are found by mapping back the control laws trough the feedback transformation.

4. Example

Consider the system corresponding to a vehicle with equal and expanding back wheels and equal front wheels with a fixed radius l, that was studied in [1, 2]. The vehicle dynamics is described by

$$\begin{pmatrix} \dot r \\ \dot\theta_1 \\ \dot\theta_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ -(\tan\alpha)/l \end{pmatrix} u_1 + \begin{pmatrix} 0 \\ 1 \\ r/l \end{pmatrix} u_2 = f_1 u_1 + f_2 u_2, \tag{7}$$

where θ_1 and θ_2 are, respectively, the variables defining the angular position of the front and rear wheels, α is a constant corresponding to the angle between the horizontal and the line obtained joining the wheel centers, and r is the radius of the back wheels that varies with time. A diagram of the system is plotted in Fig. (1).

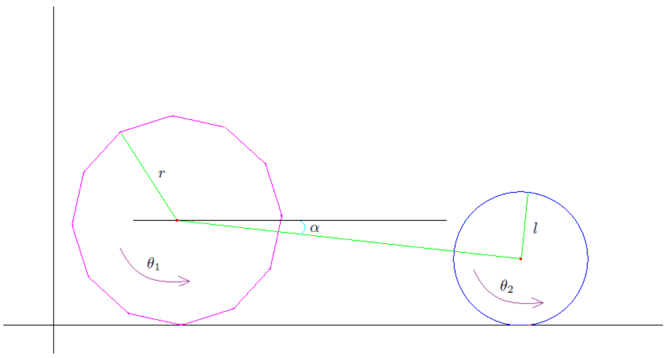


Figure 1: System diagram.

The codistribution defined as

$$I^{(0)} = \Delta^{\perp} = \{\omega \in \Lambda^1 \mid f_i \;\lrcorner\, \omega = 0,\ \forall f_i \in \triangle\}$$

has to be found. A possible solution is

$$\omega = \tan\alpha\, dr - r\, d\theta_1 + l\, d\theta_2.$$

The goal is to put ω into the Goursat normal form. This one form fulfills $(d\omega)\wedge\omega \neq 0$ and $(d\omega)^2\wedge\omega = 0$, so $\mathrm{rang}(\omega) = 1$ and Pfaff theorem can be applied. First of all, a function f_1 such that

$$d\omega \wedge \omega \wedge df_1 = 0$$

has to be found. Actually this is a degree four form in a three dimensional space. Hence, it vanishes everywhere and any f_1 function works out. For simplicity, we choose

$$f_1(r, \theta_1, \theta_2) = r.$$

A second function f_2 has to satisfy

$$\begin{aligned} \omega \wedge df_1 \wedge df_2 &= 0, \\ df_1 \wedge df_2 &\neq 0. \end{aligned}$$

Note that this is a degree three form in a three dimensional space. A possible function could be

$$f_2(r, \theta_1, \theta_2) = \theta_2 l - \theta_1 r,$$

so that,

$$\omega = df_2 + g_1\, df_1 = dz_3 - z_2\, dz_1.$$

The new variables expressed in terms of the original ones are

$$\begin{aligned} z_1 &= r, \\ z_2 &= -\theta_1 - \tan\alpha, \\ z_3 &= \theta_2 l - \theta_1 r. \end{aligned}$$

And the system expressed in the new variables is

$$\begin{pmatrix} \dot z_1 \\ \dot z_2 \\ \dot z_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ z_2 \end{pmatrix} u_1 + \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix} u_2. \qquad (8)$$

Note that system (8) is not in the Goursat canonical form. As remarked before, a feedback law must be applied in order to get a system like in equation (5). In this case, this feedback is

$$\begin{aligned} \overline{u}_1 &:= u_1, \\ \overline{u}_2 &:= -u_2. \end{aligned}$$

Hence, system (8) becomes

$$\begin{pmatrix} \dot z_1 \\ \dot z_2 \\ \dot z_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ z_2 \end{pmatrix} \overline{u}_1 + \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \overline{u}_2.$$

The flat outputs are easy to obtain from this canonical form,

$$y_1 = z_3,$$
$$y_2 = z_1,$$

so that

$$\dot{y}_1 = \dot{z}_3 = z_2\overline{u}_1,$$
$$\dot{y}_2 = \dot{z}_1 = \overline{u}_1.$$

From here we extract

$$z_2 = \frac{\dot{y}_1}{\dot{y}_2}.$$

The variables $z = (z_1, z_2, z_3)$ are expressed in terms of $y = (y_1, \dot{y}_1, y_2, \dot{y}_2)$.

In order to define a diffeomorphism between $z = (z_1, z_2, z_3)$ and $y = (y_1, \dot{y}_1, y_2, \dot{y}_2)$, the system has to be prolonged as follows

$$z_4 = \overline{u}_1,$$

and two new controls,

$$v_1 = \dot{\overline{u}}_1, \quad v_2 = \overline{u}_2,$$

are defined. Therefore, the system becomes

$$\begin{cases} \dot{z}_1 &= z_4 \\ \dot{z}_2 &= v_2 \\ \dot{z}_3 &= z_2 z_4 \\ \dot{z}_4 &= v_1. \end{cases}$$

The diffeomorphism linking the two sets of variables ($z = (z_1, z_2, z_3, z_4)$ and $y = (y_1, \dot{y}_1, y_2, \dot{y}_2)$) is

$$y_1 = z_3,$$
$$y_2 = z_1,$$
$$\dot{y}_1 = z_2 z_4,$$
$$\dot{y}_2 = z_4.$$

In the flat variables, the system reduces to a pair of second-order integrators

$$\begin{cases} \ddot{y}_2 = w_1 \\ \ddot{y}_1 = w_2. \end{cases}$$

The feedback law relating the control laws is:

$$\begin{cases} v_1 = w_1 \\ v_2 = (w_2 - z_2 w_1)/z_4. \end{cases}$$

Each flat output has to pass through four conditions (two initial conditions and two final conditions), so there exist two unique third degree polynomials such that

$$P_3(t) = y_1(t),$$

$$Q_3(t) = y_2(t).$$

5. Simulations

A set of initial and final conditions have been chosen as follows

$$
\begin{aligned}
x(0) &= (r(0), \theta_1(0), \theta_2(0)) = (1, \pi, \pi/2)\,, \\
x(1) &= (r(1), \theta_1(1), \theta_2(1)) = (2, 0, 0)\,, \\
z(0) &= (z_1(0), z_2(0), z_3(0)) = (1, -\pi - 1, \pi/2)\,, \\
z(1) &= (z_1(1), z_2(1), z_3(1)) = (2, -1, 0)\,.
\end{aligned}
$$

Adding $z_4(0) = 1$ and $z_4(1) = 3$, through the diffeomorphism, we obtain the following conditions for the flat outputs

$$
\begin{aligned}
y(0) &= (y_1(0), \dot{y}_1(0), y_2(0), \dot{y}_2(0)) = (-\pi/2, -\pi - 1, 1, 1)\,, \\
y(1) &= (y_1(1), \dot{y}_1(1), y_2(1), \dot{y}_2(1)) = (0, -3, 2, 3)\,.
\end{aligned}
$$

The polynomials meeting these conditions are

$$
\begin{aligned}
P_3(t) &= (-2\pi - 4)t^3 + (5 + 7\pi/2)t^2 + (-\pi - 1)t - \pi/2, \\
Q_3(t) &= 2t^3 - 2t^2 + t + 1.
\end{aligned}
$$

Once the polynomials have been found, the inputs are obtained by double differentiation:

$$
w_2 = \frac{\mathrm{d}^2}{\mathrm{d}t^2} y_1 = \frac{\mathrm{d}^2}{\mathrm{d}t^2} P_3(t),
$$

$$
w_1 = \frac{\mathrm{d}^2}{\mathrm{d}t^2} y_2 = \frac{\mathrm{d}^2}{\mathrm{d}t^2} Q_3(t).
$$

By applying inverse feedback, the controls $v_1(t)$ and $v_2(t)$ are found. Since $\overline{u}_2(t) = v_2(t)$ and $\dot{\overline{u}}_1(t) = v_1(t)$, the original controls can be obtained by integration:

$$
\begin{aligned}
u_1(t) &= 1 - 4t + 6t^2, \\
u_2(t) &= \frac{3(-2 + 4t + 4t^2 - \pi + 6t^2\pi)}{(1 - 4t + 6t^2)^2}.
\end{aligned}
$$

Replacing the controls obtained in the original system, trajectories for the system variables are found through numerical integration. These trajectories are depicted in Fig.(2):

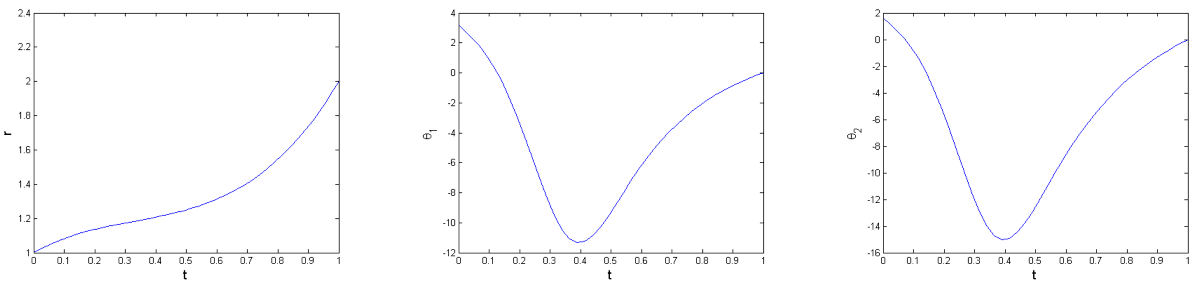


Figure 2: Behavior of system variables.

In order to circumvent errors in the initial conditions, a linear controller is added to the linear system corresponding to the flat output space. With the addition of this controller, errors in the final conditions are minimized.

The original initial and final conditions are

$$(r(0), \theta_1(0), \theta_2(0)) = (1, \pi, \pi/2)\,,$$
$$(r(1), \theta_1(1), \theta_2(1)) = (2, 0, 0)\,,$$

and the perturbed initial conditions are

$$(r(0), \theta_1(0), \theta_2(0)) = (1/2, 7/2, 2)\,.$$

In the next figure, we can observe how the modified trajectories converge quickly to the desired trajectory, which is the trajectory obtained by the unperturbed initial conditions plotted in Fig. (3):

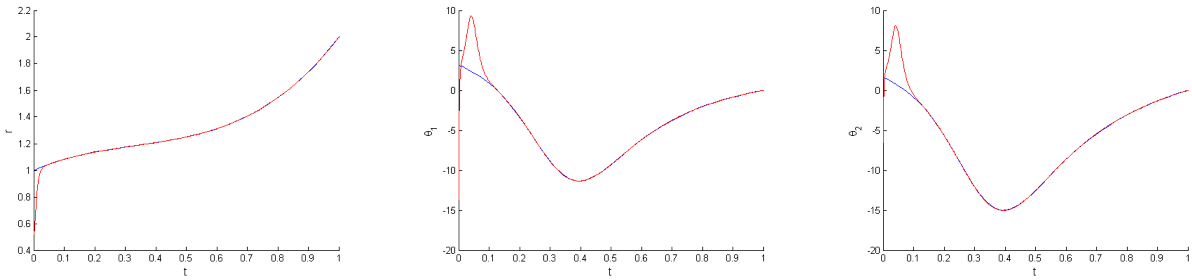


Figure 3: Trajectories of the system variables with disturbance in the initial conditions.

6. Conclusions

An algorithm to find flat outputs has been explained. This algorithm consists in finding the equivalent Pfaffian system to a control system and transforming this Pfaffian system into the Goursat normal form. This Goursat normal form, when it is written again in the state space form, is very useful in order to find the flat outputs of the system if a feedback law is included in order to simplify the equations.

As an example, point to point trajectories for a car with expanding wheels are simulated. The control laws have been obtained by transforming the system into its equivalent trivial linear system in the flat variables (chains of integrators), and designing the control laws by interpolation of the initial and final conditions. The control laws for the nonlinear system are obtained mapping back the diffeomorphisms and the feedback laws.

Future works using Goursat canonical forms include application of this algorithm to more complex control systems, as well as possible reinterpretation of existing results in the literature that have been obtained in the framework of vector fields.

References

[1] S.K. Agrawal, J. Yan. "A three-wheel vehicle with expanding wheels: differential flatness, trajectory planning, and control", *Proceedings of the 2003 IEEWRSJ, Intl. Conference on Intelligent Robots and Systems*, Las Vegas (2003).

[2] S.K. Agrawal, J. Yan, J. Rochester. "Analytics and motion planning of a novel four-wheel vehicle with expanding wheels", *Proc. ASME. 36533, Vol. 5: 27th Biennial Mechanisms and Robotics Conference 1225* (2002).

[3] R.L. Bryant, S.S. Chern, R.B. Gardner, H.L. Goldschmidt, P.A. Griffiths. *Exterior Differential Systems*, Springer-Verlag (1990).

[4] B. Charlet, J. Lévine, R. Marino. "On dynamic feedback linearization", *System and Control Letters* **13** (1989), 143–151.

[5] M. Fliess, J. Levine, Ph. Martin, P. Rouchon. "Flatness and defect of nonlinear systems: introductory theory and examples", *International Journal of Control* **61** (1995), 1327–1361.

[6] E. Fossas, J. Franch. "Linearization by prolongations: new bounds on the number of integrators", *European Journal of Control* **11** (2005), 171–179.

[7] J. Franch, A. Manzanera, G. Valero. "On computing flat outputs through Goursat normal form", *Proceedings of the European Control Conference 2014, to appear*.

[8] L.R. Hunt, R. Su, G. Meyer. "Design for multi-input nonlinear systems", *Differential geometric control theory*, R. Brockett, R. Millmann, H. Sussmann, Eds. Boston: Birkhäuser (1983), 268–298.

[9] A. Isidori. "Nonlinear Control Systems", Springer-Verlag (1995).

[10] B. Jacubczyk, W. Respondek. "Remarks on equivalence and linearization of nonlinear systems", *Bull. Acad. Pol. Sci., Ser. Sci. Math.*, **18** (1980), 517–522.

[11] Ph. Martin. "Contribution à l'étude des systèmes différentiellement plats", *Thèse de Doctorat, École Nationale Supérieure des Mines de Paris* (1992).

[12] Ph. Martin, P. Rouchon. "Feedback linearization and driftless systems". *Mathematics of control, signal and systems* **7** (1994), 235–254.

[13] R. Murray, Z. Li, S.S. Sastry. "A mathematical introduction to robotic manipulation", *CRC Press* (1994).

[14] H. Nijmeijer, A.J. van der Schaft. "Nonlinear dynamical control systems", Springer-Verlag (1990).

[15] S. Sastry. "Nonlinear Systems. Analysis, Stability, and Control", Springer-Verlag (1999).

REPORTS@SCM
AN ELECTRONIC JOURNAL OF THE
SOCIETAT CATALANA DE MATEMÀTIQUES

A quantitative Runge's Theorem in Riemann surfaces

*Daniel Lear
Instituto de Ciencias Matemáticas
(CSIC-UAM-UC3M-UCM)
daniel.lear@icmat.es

*Corresponding author

Resum *(CAT)*
Donem una versió quantitativa del teorema de Runge per a superfícies de Riemann, la qual inclou una fita superior de l'ordre dels pols. Juguen un paper essencial tant la funció de Green com les estimacions L^2 ponderades per a l'equació de Cauchy-Riemann no homogènia.

Abstract *(ENG)*
We give a quantitative version of Runge's theorem for Riemann surfaces that includes an upper bound of the order of the poles. Green's Functions and the weighted L^2-estimates for the inhomogeneous Cauchy–Riemann equation play an essential role.

Societat Catalana de Matemàtiques

Institut d'Estudis Catalans

Keywords: *Runge's theorem, Riemann surfaces, Green's function.*
MSC (2010): *30D30, 30F15, 31A05.*
Received: *October 22, 2013.*
Accepted: *May 15, 2014.*

Acknowledgement
This research was carried out while the author enjoyed a master's grant from the Institut de Matemàtiques de la Universitat de Barcelona (IMUB).

1. Introduction

In complex analysis, Runge's theorem (also known as Runge's approximation theorem) is named after the German mathematician Carl Runge who first proved it in the year 1885. It states the following:

Theorem 1.1. *Let K be a compact subset of the extended complex plane $\hat{\mathbb{C}} \equiv \mathbb{C} \cup \{\infty\}$ and suppose that f is holomorphic on an open set containing K. Let Q be a subset of $\hat{\mathbb{C}} \backslash K$ such that each connected component of $\hat{\mathbb{C}} \backslash K$ contains a point of Q. Then f can be approximated uniformly on K by rational functions with poles in Q.*

In particular, if K is a compact subset of the complex plane, and if the complement of K is connected, then each holomorphic function in a neighborhood of K can be approximated uniformly on K by polynomials. Runge's theorem has many applications in the theory of functions of a complex variable and in functional analysis. The proofs of this theorem and its applications can be found in any monograph of complex analysis as [5, 10, 11].

The main contribution of this paper is a new proof of Runge's theorem. The proof generalizes to the following theorem for Riemann surfaces.

Theorem 1.2. *Let X be a compact Riemann surface and let $K \subset X$ be a compact subset. Moreover, let Q be any subset of $X \backslash K$ which contains precisely one point from each connected component of $X \backslash K$. Then any holomorphic function on a neighborhood of K can be approximated uniformly on K by meromorphic functions on X whose poles lie in Q.*

The proof is based on Hörmander's L^2-estimates for the inhomogeneous $\bar{\partial}$-equation. More precisely, a smooth approximant is obtained by multiplying f by a cut-off function χ adapted to K. Then, the rational function of the form $g = \chi f - u$ will provide us the desired approximation of f on K. This leads to the $\bar{\partial}$-equation $\bar{\partial} u = f \bar{\partial} \chi$, where u must be small on K and with controlled growth near Q (so that g is meromorphic with poles only on Q). This is achieved by constructing an appropriate subharmonic weight with singularities located on Q and applying Hörmander's result.

A clear advantage of this method is that it controls the order of the poles. This explains the word "quantitative" in the title.

In the next section we give a detailed account of the Riemann sphere case $\hat{\mathbb{C}}$ in order to illustrate the main difficulties. This case, although easier than the general case of Riemann surfaces, introduces the general procedure and is conceptually easier to understand. The general case is dealt with in Section 3.

2. A particular case: the Riemann sphere

Let K be a compact set in $\hat{\mathbb{C}}$ such that $\hat{\mathbb{C}} \backslash K$ has finitely many regions $\Omega_1, \dots, \Omega_n$. We fix one point z_i in each of the components Ω_i. In order to prove Runge's theorem we need to see that given $f \in \mathcal{H}(K)$ [1] and $\varepsilon > 0$ there is a rational function $g = p/q$ with poles only in $z_1, z_2, \dots, z_n$ such that $\sup_K |f - g| \leq \varepsilon$.

Remark. The degree of q depends on f, the position of the points $z_1, \dots, z_n$ and ε. However, the precise dependence is not clear when looking at the standard proofs. Our goal is to prove Runge's theorem with control on the poles of g.

[1] By definition, $f \in \mathcal{H}(K)$ if there exists an open set U with $K \subset U \subset \hat{\mathbb{C}}$ s.t. f is holomorphic on U.

The main tools in our proof are Hörmander L^2-estimates and potential theory, for which we refer to [3, 4, 9] respectively.

To make it simpler we will split the proof into several steps.

Step 1. Green's function for Ω_i with pole z_i. Recall the definition of Green's function.

Definition 2.1. Let D be a proper subdomain of $\hat{\mathbb{C}}$. A Green's function for D is a map $g_D : D \times D \longrightarrow (-\infty, \infty]$ such that for each $\omega \in D$:

(a) $g_D(\cdot, \omega)$ is harmonic on $D \backslash \{\omega\}$ and bounded outside any neighbourhood of ω.

(b) $g_D(\omega, \omega) = \infty \quad \text{and} \quad \lim_{z \to \omega} g_D(z, \omega) = \begin{cases} \log|z| + O(1) & \omega = \infty \\ -\log|z - \omega| + O(1) & \omega \neq \infty \end{cases}$.

(c) $\lim\limits_{z \to \zeta} g_D(z, \omega) = 0$ for nearly everywhere [2] $\zeta \in \partial D$.

Specifically, we consider the case in which $D = \Omega_i$ and $\omega = z_i$. Since Ω_i is a regular[3] domain in $\hat{\mathbb{C}}$ such that $\partial \Omega_i$ is non-polar[4], there exists a unique Green's function

$$G_i(z) := g_{\Omega_i}(z, z_i) \quad z \in \Omega_i.$$

In particular,

- $G_i(\cdot) = g_{\Omega_i}(\cdot, z_i) > 0$,
- $\lim_{z \to \zeta} G_i(z) = \lim_{z \to \zeta} g_{\Omega_i}(z, z_i) = 0 \quad \text{for } \zeta \in \partial \Omega_i$.

Moreover, we can extend G_i to the whole $\hat{\mathbb{C}}$ by declaring $G_i \equiv 0$ outside of Ω_i, $i = 1, \dots, n$.

As $f \in \mathcal{H}(K)$ and $G_i(z) \in \mathcal{C}(\overline{\Omega}_i \backslash \{z_i\})$ with $G_i(z) \geq 0$ in $\overline{\Omega}_i$ and $G_i(z) \equiv 0$ on $\partial \overline{\Omega}_i$, there exists $\delta_i > 0$ small enough such that f is defined in $\widetilde{U}_i := \{z \in \Omega_i : G_i(z) < \delta_i\}$, see Figure 1.

Take now δ such that $0 < \delta \leq \min\{\delta_1, \dots, \delta_n\}$, so that f is defined in $U_i := \{z \in \Omega_i : G_i(z) < \delta\}$ for every $i = 1, \dots, n$. At the moment δ is freely chosen in the region $0 < \delta \leq \min\{\delta_1, \dots, \delta_n\}$. However, further on we will give δ a specific value.

So far we have $G_i(z) - \delta \in \mathcal{C}(\overline{\Omega}_i \backslash \{z_i\})$ with $G_i(z) - \delta \equiv 0$ in $\partial \overline{U}_i$. The next step is to extend $G_i(z) - \delta$ to the entire plane $\hat{\mathbb{C}}$; define finally $\mathcal{G}_i(\cdot) : \hat{\mathbb{C}} \longrightarrow [0, \infty]$ as:

$$\mathcal{G}_i(z) := \begin{cases} G_i(z) - \delta & \text{if } z \in \Omega_i \backslash \overline{U}_i, \\ 0 & \text{if } z \notin \Omega_i \backslash \overline{U}_i. \end{cases}$$

[2] A property is said to hold nearly everwhere (n.e.) on a subset S of $\mathbb{C}$ if it holds everywhere on $S \backslash E$, for some Borel polar set E.

[3] Let D be a proper subdomain of $\hat{\mathbb{C}}$, and let $\xi_0 \in \partial D$. A barrier at ξ_0 is a subharmonic function b defined on $D \cap N$, where N is an open neighborhood of ξ_0 satisfying

$$b < 0 \text{ on } D \cap N \quad \text{and} \quad \lim_{z \to \xi_0} b(z) = 0$$

A boundary point at which a barrier exists is called regular. If every $\xi \in \partial D$ is regular, then D is called a regular domain.

[4] In the area of classical potential theory, polar sets are the "negligible sets", similar to the way in which sets of measure zero are the negligible sets in measure theory.

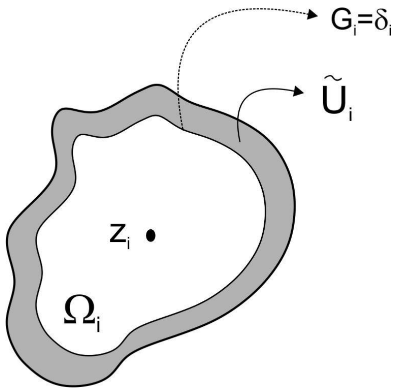


Figure 1: Definition of $\widetilde{U}_i$.

Step 2. Construction of a subharmonic weight $\phi_\delta(z)$ *in* $\hat{\mathbb{C}}\backslash\{z_1,\dots,z_n\}$. Notice that $\mathcal{G}_i(\cdot) \equiv G_i(\cdot) - \delta$ on $\Omega_i\backslash\overline{U}_i$. In particular $\mathcal{G}_i$ is subharmonic in $(\Omega_i\backslash\overline{U}_i)\backslash\{z_i\}$. We conclude that $\mathcal{G}_i(\cdot)$ is subharmonic on $\hat{\mathbb{C}}\backslash\{z_1,\dots,z_n\}$, $i = 1,\dots,n$.

We see that $\phi_\delta(z) := \max\{0,\mathcal{G}_1(z),\mathcal{G}_2(z),\dots,\mathcal{G}_n(z)\}$ is subharmonic on $\hat{\mathbb{C}}\backslash\{z_1,\dots,z_n\}$, since the maximum of subharmonic functions is again subharmonic. The explicit expression of ϕ_δ is

$$\phi_\delta(z) = \begin{cases} \mathcal{G}_i(z) = G_i(z) - \delta & \text{if } z \in \Omega_i\backslash\overline{U}_i \\ 0 & \text{if } z \in K \cup \bigcup_{j=1}^N \overline{U}_j. \end{cases}$$

Step 3. A cut-off function adapted to K. In this step we construct a suitable smooth cut-off function χ, so that χf is a smooth extension of f which is still holomorphic in K.

Consider a parameter $t > 0$ small enough, which will be fixed later. We look for a smooth cut-off function $\chi(z) \in \mathcal{C}^\infty(\mathbb{C})$ such that $\chi = 0$ when $G_i(z) \geq \delta$ and $\chi = 1$ when $z \in K$ or $G_i(z) \leq \delta - t\delta/2$, see Figure 2. The easier way to achieve this is to take $\chi(z) = \varphi_\delta(\sum_i G_i(z))$ with $\varphi_\delta \in \mathcal{C}^\infty(\mathbb{R})$ such that:

$$\varphi_\delta(x) = \begin{cases} 1 & \text{if} \quad x \leq \delta - t\delta/2, \\ 0 & \text{if} \quad x \geq \delta. \end{cases}$$

Since by construction

$$\sum_i G_i(z) = \begin{cases} G_i(z) & \text{if } z \in \Omega_i, \\ 0 & \text{otherwise,} \end{cases}$$

we obtain:

$$\chi(z) = \begin{cases} 0 & \text{if} \quad z \in \{z \in \Omega_i : G_i(z) \geq \delta\}, \\ 1 & \text{if} \quad z \in K \cup \bigcup_{i=1}^n \{z \in \Omega_i : G_i(z) \leq \delta - t\delta/2\}. \end{cases}$$

Note that

$$\mathrm{Supp}(\bar{\partial}\chi) \subset \bigcup_{i=1}^n \{z \in \Omega_i : \delta - t\delta/2 \leq G_i(z) \leq \delta\}$$

and

$$|\bar{\partial}\chi| \sim |1/(t\delta/2)|. \tag{1}$$

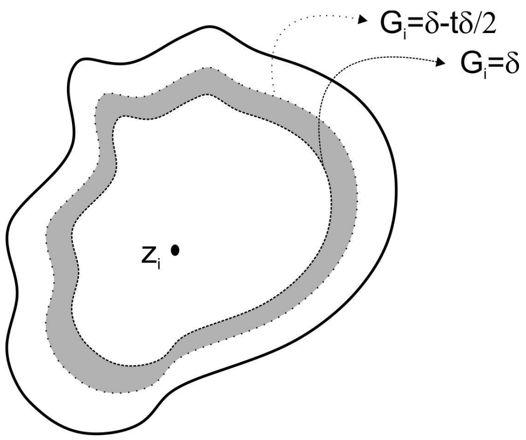


Figure 2: Definition of χ.

Step 4. The $\bar{\partial}$-equation. Here the smooth extension χf will be corrected, with the help of an appropriate solution to a $\bar{\partial}$-equation, to make the resulting function rational with poles on z_j. The function approximating f will be of the form $g = \chi f - u$, where $\bar{\partial} u = f \bar{\partial}\chi$ on $\hat{\mathbb{C}}\backslash\{z_1, \dots, z_n\}$.

We will use the solution u given by the following theorem of Hörmander's. This solution has minimal norm in $L^2(e^{-\phi})$.

Theorem 2.2. [3, pp. 13] *Let Ω be a domain in $\hat{\mathbb{C}}$ and suppose $\phi \in \mathbb{C}^2(\Omega)$ with $\Delta\phi \geq 0$. Then, for any $f \in L^2_{\text{loc}}(\Omega)$ there is a solution u to $\bar{\partial} u = f$ satisfying*

$$\int |u|^2 e^{-\phi} \leq \int \frac{|f|^2}{\Delta\phi} e^{-\phi}.$$

Step 5. The measure $\Delta\phi_\delta \geq 0$ is the harmonic measure of $\{G_i = \delta\}$ with respect to z_i in $\Omega_i\backslash\overline{U}_i$. Hörmander's theorem provides a solution u with

$$\int |u|^2 e^{-\phi} \leq \int \frac{1}{\Delta\phi} |f\bar{\partial}\chi|^2 e^{-\phi},$$

whenever $\Delta\phi \geq 0$.

Our first candidate is $\phi = \phi_\delta$, which is subharmonic on $\hat{\mathbb{C}}\backslash\{z_1, \dots, z_n\}$. We see that the Radon measure $\Delta\phi_\delta$ has

$$\Delta\phi_\delta\big|_{K\cup U_1\cup\cdots\cup U_n} \equiv 0 \quad \text{and} \quad \Delta\phi_\delta\big|_{(\Omega_i\backslash\overline{U}_i)\backslash\{z_i\}} \equiv 0 \qquad i = 1, 2, \dots, n.$$

Therefore, $\Delta\phi_\delta$ is supported in the union $\bigcup_{i=1}^n \partial U_i$, that is, in the curve $\{G_i(z) = \delta\}$.

We shall see next that $\Delta\phi_\delta$ is the harmonic measure of $\{G_i = \delta\}$ with respect to z_i in the domain $\Omega_i\backslash\overline{U}_i$.

Definition 2.3. Let D be a proper subdomain of $\hat{\mathbb{C}}$, and denote by $\mathcal{B}(\partial D)$ the σ-algebra of Borel subsets of ∂D. A harmonic measure for D is a function $\omega_D : D \times \mathcal{B}(\partial D) \longrightarrow [0, 1]$ such that:

(a) for each $z \in D$, the map $B \mapsto \omega_D(z, B)$ is a Borel measure on ∂D,

(b) if $\phi : \partial D \longrightarrow \mathbb{R}$ is a continuous function, then $H_D\phi = P_D\phi$ on D, where $P_D\phi$ is the generalized Poisson integral and $H_D\phi$ is the Perron function of ϕ on D.

The harmonic measure of $E \in \mathcal{B}(\partial D)$ at $z \in D$ relative to D is the Perron solution $u(z)$ of the Dirichlet problem in D with boundary values 1 on E and 0 on $\partial D \backslash E$. Summarising, if χ_E denotes the indicator function of $E \subset \partial D \backslash E$ then

$$u(z) = \sup\Big\{ v(z) : v \text{ subharmonic in } D \text{ and } \limsup_{\omega \to \zeta} v(\omega) < \chi_E(\zeta) \text{ for } \zeta \in \partial D \Big\}.$$

We shall prove now that

$$\Delta \phi_\delta(\zeta) = 2\pi \sum_{i=1}^{n} \omega_{\Omega_i \backslash \overline{U}_i}(z_i, \zeta), \tag{2}$$

where $\omega_{\Omega_i \backslash \overline{U}_i} : \Omega_i \backslash \overline{U}_i \times \mathcal{B}\left(\partial(\Omega_i \backslash \overline{U}_i)\right) \longrightarrow [0,1]$ is the harmonic measure for $\Omega_i \backslash \overline{U}_i$, and we denote by $\mathcal{B}(\partial(\Omega_i \backslash \overline{U}_i))$ the σ-algebra of Borel subsets of $\partial(\Omega_i \backslash \overline{U}_i)$.

Take in the definition $D = \Omega_i \backslash \overline{U}_i$ and fix $z_i \in \Omega_i \backslash \overline{U}_i$. Since $\partial\left(\Omega_i \backslash \overline{U}_i\right)$ is non-polar there exists a unique harmonic measure satisfying (a) and (b). We then repeat the same reasoning for each of the "holes".

By definition, the generalized Laplacian acts on test functions as:

$$\int_D \psi \Delta \phi_\delta = \int_D \phi_\delta \Delta \psi \, dA \qquad \psi \in C_c^\infty(D) \qquad D = \hat{\mathbb{C}} \backslash \{z_1, \dots, z_n\}.$$

Since $\sup(\Delta \phi_\delta) \subset \bigcup_{i=1}^n \{z \in \Omega_i : G_i(z) = \delta\}$ and $\phi_\delta \equiv 0$ in $K \cup \overline{U}_1 \cup \cdots \cup \overline{U}_n$, if $\psi \in C_c^\infty(D)$, the previous expression becomes

$$\sum_{i=1}^{n} \int_{\{z \in \Omega_i : G_i(z) = \delta\} \equiv \partial(\Omega_i \backslash \overline{U}_i)} \psi \Delta \phi_\delta = \sum_{i=1}^{n} \int_{(\Omega_i \backslash \overline{U}_i) \backslash \{z_i\}} \phi_\delta \Delta \psi \, dA.$$

Thus, in order to prove (2) we need to see that

$$\int_{(\Omega_i \backslash \overline{U}_i) \backslash \{z_i\}} \phi_\delta(\zeta) \Delta \psi(\zeta) \, dA = 2\pi \int_{\{z \in \Omega_i : G_i(z) = \delta\} \equiv \partial(\Omega_i \backslash \overline{U}_i)} \psi(\zeta) \, d_{\omega_{\Omega_i \backslash \overline{U}_i}}(z_i, \zeta).$$

To see this, we are going to use the relationship between the harmonic measure and the normal derivative of Green's function, which is the Poisson kernel.

Theorem 2.4. [5, pp. 409] *Let D be a bounded domain with piecewise smooth boundary. Fix $\zeta \in D$ and let $g_D(z, \zeta)$ be the Green's function for D (with pole at ζ). Then for any Borel mesurable set $B \in \mathcal{B}(\partial D)$ we have*

$$-\frac{1}{2\pi} \int_B \frac{\partial g_D}{\partial n}(z, \zeta) \, ds = \omega_D(\zeta, B).$$

Going back to the proof of the identity above, we consider the particular case $D = \Omega_i \backslash \overline{U}_i$ with $\zeta = z_i$, and repeating the computations for each hole, we get

$$-\frac{1}{2\pi} \int_B \frac{\partial \phi_\delta}{\partial n}(z, z_i) \, ds = \omega_{\Omega_i \backslash \overline{U}_i}(z_i, B),$$

for $i = 1, \dots, n$. Therefore, applying Stoke's theorem, we obtain

$$\begin{aligned}
2\pi \int_{\partial(\Omega_i \setminus \overline{U}_i)} \psi(\zeta)\, d_{\omega_{\Omega_i\setminus\overline{U}_i}}(z_i,\zeta) &= 2\pi \left[-\frac{1}{2\pi} \int_{\partial(\Omega_i\setminus\overline{U}_i)} \psi(\zeta)\, \frac{\partial \phi_\delta}{\partial n}(z, z_i)\, ds \right] \\
&= 2\pi \left[\psi(z_i) + \frac{1}{2\pi} \int_{\Omega_i\setminus\overline{U}_i} \phi_\delta(\zeta)\Delta\psi(\zeta)\, dA \right] \\
&= 2\pi\psi(z_i) + \int_{\Omega_i\setminus\overline{U}_i} \phi_\delta(\zeta)\Delta\psi(\zeta)\, dA.
\end{aligned}$$

Taking $\varepsilon > 0$ small enough and splitting the last integral

$$\begin{aligned}
\int_{\Omega_i\setminus\overline{U}_i} \phi_\delta(\zeta)\Delta\psi(\zeta)\, dA &= \int_{(\Omega_i\setminus\overline{U}_i)\setminus B(z_i,\varepsilon)} \phi_\delta(\zeta)\Delta\psi(\zeta)\, dA + \int_{B(z_i,\varepsilon)} \phi_\delta(\zeta)\Delta\psi(\zeta)\, dA \\
&= \lim_{\varepsilon\to 0^+} \left[\int_{(\Omega_i\setminus\overline{U}_i)\setminus B(z_i,\varepsilon)} \phi_\delta(\zeta)\Delta\psi(\zeta)\, dA + \int_{B(z_i,\varepsilon)} \phi_\delta(\zeta)\Delta\psi(\zeta)\, dA \right] \\
&= \int_{(\Omega_i\setminus\overline{U}_i)\setminus\{z_i\}} \phi_\delta(\zeta)\Delta\psi(\zeta)\, dA + \lim_{\varepsilon\to 0^+} \int_{B(z_i,\varepsilon)} \phi_\delta(\zeta)\Delta\psi(\zeta)\, dA.
\end{aligned}$$

We compute the second integral:

$$\begin{aligned}
\int_{B(z_i,\varepsilon)} \phi_\delta(\zeta)\Delta\psi(\zeta)\, dA &= \int_{B(z_i,\varepsilon)} \left(\phi_\delta(\zeta) - \log\frac{1}{|\zeta - z_i|} + \log\frac{1}{|\zeta - z_i|} \right) \Delta\psi(\zeta)\, dA \\
&= \int_{B(z_i,\varepsilon)} \left(\phi_\delta(\zeta) - \log\frac{1}{|\zeta - z_i|} \right) \Delta\psi(\zeta)\, dA - \int_{B(z_i,\varepsilon)} \log|\zeta - z_i|\, \Delta\psi(\zeta)\, dA \\
&= \int_{B(z_i,\varepsilon)} \underbrace{\Delta\left(\phi_\delta(\zeta) - \log\frac{1}{|\zeta - z_i|} \right)}_{0} \psi(\zeta)\, dA - \int_{B(z_i,\varepsilon)} \psi(\zeta)\, \underbrace{\Delta(\log|\zeta - z_i|)}_{2\pi\delta_{z_i}(\zeta)} \\
&= -2\pi\psi(z_i),
\end{aligned}$$

since $\phi_\delta(\zeta)$ has a logarithmic singularity and so $\phi_\delta(\zeta) - \log\frac{1}{|\zeta - z_i|}$ is harmonic in $\{z_i\}$, and also on $B(z_i,\varepsilon)$ for ε small enough. Thus, we have

$$2\pi \int_{\partial(\Omega_i\setminus\overline{U}_i)} \psi(\zeta)\, d_{\omega_{\Omega_i\setminus\overline{U}_i}}(z_i,\zeta) = \int_{(\Omega_i\setminus\overline{U}_i)\setminus\{z_i\}} \phi_\delta(\zeta)\Delta\psi(\zeta)\, dA,$$

as desired.

Step 6. The curve $\{G_i = \delta\}$ is smooth and $\Delta\phi_\delta$ is comparable to the length of the curve. We have seen that $\Delta\phi_\delta$ is the harmonic measure of $\{G_i = \delta\}$ with respect to z_i in the domain $\Omega_i\setminus\overline{U}_i$. Here we prove that the curve $\{G_i = \delta\}$ is smooth; later we shall use the smoothness to prove that $\Delta\phi_\delta$ is comparable to the length of the curve.

Recall that $F \equiv \sum_{i=1}^n G_i$ is harmonic in its domain of definition $\bigsqcup_{i=1}^n (\Omega_i\setminus\overline{U}_i)\setminus\{z_i\}$. Let us fix here δ, taking $0 < \delta \le \min\{\delta_1, \dots, \delta_n\}$ such that if $F(z) = \delta$, then the vector $\nabla F(z) = (F_x(z), F_y(z)) \neq (0,0)$. To prove that such δ exists we recall Sard's theorem.

Theorem 2.5. [1, pp. 34] *Let $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$ be $\mathcal{C}^k$ with $k \ge 2$. Let X denote the critical set of f, $X = \{x \in \mathbb{R}^2 : \nabla f(x) = (0,0)\}$. Then the image $f(X)$ has Lebesgue measure 0 in $\mathbb{R}$.*

The existence of δ is proved by contradiction. Assume that for all $\delta \in (0, \min\{\delta_1, \dots, \delta_n\}]$ there exists at least a point z_δ in the curve $\{F = \delta\}$ such that $\nabla F(z_\delta) = (0,0)$. Define $M := \{z_\delta : 0 <$

$\delta \leq \min\{\delta_1, \dots, \delta_n\}\}$. By Sard's theorem $F(M)$ has measure zero; however it is clear that $F(M) = (0, \min\{\delta_1, \dots, \delta_n\}]$, so $m(F(M)) = \min\{\delta_1, \dots, \delta_n\} > 0$, and we get a contradiction.

Therefore, according to the implicit function theorem, the curve $\{F = \delta\}$ (or equivalently $\{G_i = \delta\}$) is smooth.

In order to prove that $\Delta\phi_\delta$ is comparable to the length of the curve we use that the gradient at a point is perpendicular to the level set at that point:

$$\nabla\phi_\delta \equiv -\frac{\partial\phi_\delta}{\partial n}.$$

Since $\nabla\phi_\delta \equiv \nabla F \neq (0,0)$ over the smooth curve $\{G_i = \delta\}$, we can extend this property by continuity to a "thin strip" $\{z : \delta - k\delta \leq G_i(z) \leq \delta\}$. Using that $0 \neq -\frac{\partial\phi_\delta}{\partial n}(z) \equiv \nabla\phi_\delta(z)$ on the "thin strip", we see that there exist $c_1 < c_2 < 0$ such that $c_1 \leq \frac{\partial\phi_\delta}{\partial n} \leq c_2 < 0$ on it. Hence:

$$-\frac{c_1}{2\pi} l(B) = -\frac{1}{2\pi}\int_B c_1\, ds \geq -\frac{1}{2\pi}\int_B \frac{\partial\phi_\delta}{\partial n}(z,\zeta)\, ds = \omega_D(\zeta, B),$$
$$-\frac{c_2}{2\pi} l(B) = -\frac{1}{2\pi}\int_B c_2\, ds \leq -\frac{1}{2\pi}\int_B \frac{\partial\phi_\delta}{\partial n}(z,\zeta)\, ds = \omega_D(\zeta, B).$$

Combining both inequalities, we obtain

$$-c_2/2\pi\, l(B) = C_2 \cdot l(B) \leq \omega_D(\zeta, B) \leq C_1 \cdot l(B) = -c_1/2\pi\, l(B).$$

As a result, the harmonic measure is comparable to the length of the curve and consequently, $\Delta\phi_\delta$ is also comparable to the length of the curve.

Remark. In order to derive an estimate from Hörmander's theorem, it is necessary to have $\Delta\phi_\delta \geq \lambda > 0$, for some $\lambda \in \mathbb{R}$.

Step 7. A function ϕ as an average of ϕ_δ's and a lower bound for $\Delta\phi$. The most natural approach is to replace the weight ϕ_δ by an average of ϕ_δ which distributes the Laplacian from the border to a neighborhood. To do this, we consider

$$\phi := \frac{1}{t\delta}\int_{\delta - t\delta}^{\delta} \phi_s\, ds.$$

Splitting the domain of definition into three regions we see that

$$\phi(z) = \begin{cases} 0 & \text{in } K \cup \{z \in \Omega_i : G_i(z) < \delta - t\delta\}, \\ \frac{1}{2t\delta}[G_i(z) - (\delta - t\delta)]^2 & \text{in } \{z \in \Omega_i : \delta - t\delta \leq G_i(z) \leq \delta\}, \\ G_i(z) - (\delta - t\delta/2) & \text{in } \{z \in \Omega_i : G_i(z) > \delta\}. \end{cases}$$

In particular ϕ is harmonic in $K \cup \{z \in \Omega_i : G_i(z) < \delta - t\delta \text{ or } G_i(z) > \delta\}$ and the support of $\Delta\phi$ is contained on the "thin strips" $\{z \in \Omega_i : \delta - t\delta \leq G_i(z) \leq \delta\}$.

To prove that $\Delta\phi$ is bounded below in $\{z \in \Omega_i : \delta - t\delta \leq G_i(z) \leq \delta\}$, we use the expression $\phi(z) = \frac{1}{2t\delta}[G_i(z) - (\delta - t\delta)]^2$ in $\{z \in \Omega_i : \delta - t\delta \leq G_i(z) \leq \delta\}$. We have

$$\Delta\phi(z) = \frac{1}{2t\delta}\left[\Delta(G_i(z)^2) + \overbrace{\Delta(\delta - t\delta)^2}^{0} - 2(\delta - t\delta)\overbrace{\Delta G_i(z)}^{0}\right] = \frac{1}{2t\delta}\Delta(G_i(z)^2)$$
$$= \frac{1}{t\delta}\left[\left(\frac{\partial G_i}{\partial x}\right)^2 + \left(\frac{\partial G_i}{\partial y}\right)^2\right](z).$$

The last identity follows from the fact that $\Delta(G_i)^2 = 2(\nabla G_i)^2$, which is a well-known property of harmonic functions:

$$\Delta(G_i)^2 = \nabla(\nabla G_i^2) = \nabla(2G_i\nabla G_i) = 2(\nabla G_i \nabla G_i + G_i \Delta G_i) = 2(\nabla G_i)^2.$$

However, $\nabla G_i(z) \neq 0$ in $\{z \in \Omega_i : \delta - t\delta \leq G_i(z) \leq \delta\}$, so $\Delta(G_i(z)^2) > 0$ too. Since G_i is continuous on it, according to Weierstrass' theorem there exists $\widetilde{\lambda} > 0$ such that $\Delta(G_i(z)^2) \geq \widetilde{\lambda}$. Therefore, there exists $\lambda > 0$ such that $\Delta\phi \geq \lambda$ on $\{z \in \Omega_i : \delta - t\delta \leq G_i(z) \leq \delta\}$ and in particular on $\operatorname{Supp}\bar{\partial}\chi$, since we have the following inclusion of sets

$$\operatorname{Supp}\bar{\partial}\chi \subset \{z \in \Omega_i : \delta - t\delta/2 \leq G_i(z) \leq \delta\} \subset \{z \in \Omega_i : \delta - t\delta \leq G_i(z) \leq \delta\}.$$

Furthermore,

$$\Delta\phi = \frac{1}{t\delta}\int_{\delta - t\delta}^{\delta} \Delta\phi_s \, ds.$$

Since, as we have seen, $\Delta\phi_\delta$ is the harmonic measure, which is comparable with the length of the curve, we obtain

$$\Delta\phi(E) = \frac{1}{t\delta}\int_{\delta - t\delta}^{\delta} \Delta\phi_s(E)\, ds \approx m(E \cap \text{"strip"}).$$

Step 8. Hörmander's estimate with the weight ϕ and the final approximant function. Since ϕ is subharmonic on $\hat{\mathbb{C}}\backslash\{z_1, \ldots, z_n\}$ and satisfies $\Delta\phi \geq \lambda > 0$ on $\operatorname{Supp}\bar{\partial}\chi$, Hörmander's theorem with the subharmonic weight function $M\phi$, with $M >> 0$ to be fixed later, yields:

$$\begin{aligned}\int_{\hat{\mathbb{C}}\backslash\{z_1,\ldots,z_n\}} |u|^2 e^{-M\phi} &\leq \int_{\hat{\mathbb{C}}\backslash\{z_1,\ldots,z_n\}} |f\bar{\partial}\chi|^2 \frac{e^{-M\phi}}{M\Delta\phi} = \int_{\operatorname{Supp}\bar{\partial}\chi} |f\bar{\partial}\chi|^2 \frac{e^{-M\phi}}{M\Delta\phi} \\ &\leq \frac{1}{M\lambda}\int_{\cup_i\{z\in\Omega_i:\delta - t\delta/2 \leq G_i(z) \leq \delta\}} |f\bar{\partial}\chi|^2 e^{-M\phi} \\ &\leq \frac{1}{M\lambda}\int_{\cup_i\{z\in\Omega_i:\delta - t\delta/2 \leq G_i(z) \leq \delta\}} |f\bar{\partial}\chi|^2 e^{-Mt\delta/8}.\end{aligned}$$

The last inequality is a consequence of the fact that if $z \in \Omega_i$ with $\delta - t\delta/2 \leq G_i(z) \leq \delta$, then $\phi(z) \geq t\delta/8$.

Taking $M = \frac{16}{t\delta}\log\left(1/(\pi r^2)^{1/2}\varepsilon\right)$, where r will be fixed in the next lines, we see that $e^{-Mt\delta/8} = \pi r^2 \cdot \varepsilon^2$. This and (1) show that

$$\int_{\hat{\mathbb{C}}\backslash\{z_1,\ldots,z_n\}} |u|^2 e^{-M\phi} \leq \left(\frac{4}{M\lambda(t\delta)^2}\int_{\cup_i\{z\in\Omega_i:\delta - t\delta/2 \leq G_i(z) \leq \delta\}} |f|^2\right) \pi r^2 \varepsilon^2 \lesssim \pi r^2 \varepsilon^2.$$

The last inequality follows from the fact that f is holomorphic in the domain of integration, which is compact. Using $\phi|_{K\cup U_i} \equiv 0$ we have that

$$\int_{K\cup U_i} |u|^2 \leq \int_{\hat{\mathbb{C}}\backslash\{z_1,\ldots,z_n\}} |u|^2 e^{-M\phi},$$

and so

$$\int_{K\cup U_i} |u|^2 \lesssim \pi r^2 \varepsilon^2.$$

We wish to take advantage of the last inequality to deduce that $\sup_K |u| \lesssim \varepsilon$. Since $\bar{\partial}u = f\bar{\partial}\chi$ on $\hat{\mathbb{C}}\backslash\{z_1, \ldots, z_n\}$ and $\chi \equiv 1$ in a small neighborhood of K, we have that $\bar{\partial}\chi = 0$ there. It follows that

$\bar\partial u = 0$ and thus u is holomorphic on this small neighborhood. In particular $|u|^2$ is subharmonic and, by the sub-mean value property, for $r > 0$ small enough (say, $0 < r < d(K, U_i^c)$, $i = 1, \dots, n$), we have

$$|u(z)|^2 \leq \frac{1}{\pi r^2}\int_{B(z,r)} |u(\zeta)|^2\, dA(\zeta) \leq \frac{1}{\pi r^2}\int_{K\cup U_i} |u(\zeta)|^2\, dA(\zeta) \qquad (z \in K).$$

Therefore,

$$\sup_K |u|^2 \lesssim \pi r^2 \varepsilon^2/\pi r^2 = \varepsilon^2.$$

Using the previous inequality and the fact that $\chi \equiv 1$ in K, we get

$$\sup_K |u| = \sup_K |g - \chi f| = \sup_K |g - f| \lesssim \varepsilon.$$

Moreover, as $g = \chi f - u$, we get $\bar\partial g = \chi\bar\partial f$. Since $f \in \mathcal{H}(K \cup U_i)$ we have $\bar\partial f \equiv 0$ in $K \cup U_i$. This and the fact that $\chi \equiv 0$ in $\Omega\backslash U_i$ show that $\chi\bar\partial f \equiv 0$. Therefore $\bar\partial g = 0$ in $\hat{\mathbb{C}}\backslash\{z_1, \dots, z_n\}$, or equivalently g is holomorphic in $\hat{\mathbb{C}}\backslash\{z_1, \dots, z_n\}$.

Let us see next that the singularities z_i must be poles, and let's quantify their order.

Consider $B_i \equiv B(z_i, r_i)\backslash\{z_i\}$. It is clear that $\chi = 0$ in B_i (for r_i small enough). Near any of the singularities z_i, $g = u$, and thus $\int_{B_i} |g|^2 e^{-M\phi} < \infty$. On the other hand, the sizes of ϕ and ϕ_δ are very similar in size. In B_i

$$\phi_\delta(z) \approx \begin{cases} -\log|z - z_i| + O(1) & z_i \neq \infty, \\ \log|z| + O(1) & z_i = \infty. \end{cases}$$

As a consequence,

$$e^{-M\phi} \approx e^{-M\phi_\delta} \approx \begin{cases} e^{M\log|z-z_i|} = |z - z_i|^M & z_i \neq \infty \\ e^{-M\log|z|} = |z|^{-M} & z_i = \infty \end{cases}$$

and therefore,

$$\int_{B_i} |g|^2 e^{-M\phi} \approx \begin{cases} \int_{B_i} |g|^2 |z - z_i|^M < \infty & z_i \neq \infty \Longrightarrow |g(z)| \approx |z - z_i|^{-\alpha/2} \text{ with } \alpha \leq M \\ \int_{B_i} |g|^2 |z|^{-M} < \infty & z_i = \infty \Longrightarrow |g(z)| \approx |z|^{\alpha/2} \text{ with } \alpha \leq M. \end{cases}$$

Hence, g can only have poles on the z_i and on ∞, and the order of such poles is at most $M/2$.

Finally, in the Riemann sphere $\hat{\mathbb{C}}$ the field of meromorphic functions is simply the field of rational functions over the complex field. Therefore, the meromorphic function g can be written as the rational function p/q, where the degree of g is smaller than $M/2$ with $M \approx \log(1/\varepsilon)$. Thus, the degree of q is smaller than $C\log(1/\varepsilon)$ with

$$C = \tfrac{8}{t\delta}\, \tfrac{\log\left((\pi r^2)^{1/2}\varepsilon\right)}{\log\varepsilon} \approx \tfrac{8}{t\delta}.$$

We finish with the explanation of the geometric meaning of the parameter δ, which gives the size of the final estimate. By hypothesis, $f \in \mathcal{H}(K)$, which means that there exists U open with $K \subset U \subset \hat{\mathbb{C}}$ and such that f is holomorphic in U. Then δ measures the size of this extension, i.e

$$\delta \approx d(K, U^c).$$

As expected, the estimate shows that the order of the poles is inversely proportional to the size of the extension. A greater holomorphy domain for a function will result in a smaller order of its poles. In the extremal case where the starting function is entire, the order of the poles vanishes and the approximating function is polynomial.

3. The general case: Riemann surfaces

In the previous section, we have proved the classical Runge's theorem. This proof, although conceived for compact subsets of the Riemann sphere has the advantage that works *mutatis mutandis* on any Riemann surface X, with meromorphic functions on X playing the role of rational functions.

The result we now present is essentially equivalent to the Behnke-Stein generalization of the Runge approximation theorem [2]. Let us highlight that the former is a key tool used in a wide amount of problems in the context of open Riemann surfaces. It can be stated in several ways, for instance:

Theorem 3.1. (Behnke-Stein [1948]) *Let X be a Riemann surface and K a compact subset of X. Every holomorphic function in a neighborhood of K is uniformly approximable on K by holomorphic functions on X if and only if $X \backslash K$ has no connected components with compact closure in X.*

If X is a compact Riemann surface, then the theorem is vacuous. This is the reason why we say "the Behnke-Stein theorem for open Riemann surfaces".

The Behnke-Stein theorem gives a relationship between analytical and topological results. We start assuming the analytical part and we will prove the topological implication. We do this by contradiction.

Assuming the approximation condition, we consider U a relatively compact component of the complement of K and fix p a point in U. Let us now use the following results:

Proposition 3.2. [8, pp. 31] *Let X and Y be Riemann surfaces. If $\Psi : X \longrightarrow Y$ is a nonconstant holomorphic mapping, then the fiber $\Psi^{-1}(x)$ over each point $x \in Y$ is discrete in X (i.e. $\Psi^{-1}(x)$ has no limit points in X).*

Proposition 3.3. [8, pp. 89] *Let P be a discrete subset of an open Riemann surface X. If $\xi_p \in \mathbb{C}$ for each $p \in P$, then there exists a function $h \in \mathcal{H}(X)$ with $h(p) = \xi_p$ for every $p \in P$.*

Let f be a holomorphic function that vanishes at p, let $P := f^{-1}(0)$ be the (discrete) zero set of f, and consider the holomorphic function h given by the previous proposition such that

$$h(P - \{p\}) = 0 \qquad \text{and} \qquad h(p) = 1.$$

Define the meromorphic function

$$g := h/f.$$

It is clear that g has only one singularity (the point p), so it is holomorphic on K. Furthermore, the previous assumptions assert that we can find a sequence $\{g_n\}_n$ of holomorphic functions on X converging uniformly on K to g: for all $\varepsilon > 0$ there exists $n_0 = n_0(\varepsilon)$ such that:

$$\sup_K |g - g_n| \leq \varepsilon \qquad \forall n \geq n_0.$$

Then the sequence fg_n converges to h uniformly on K. Note that this result still holds for the boundary of U. Hence, by the maximum principle, if converges uniformly to h on U, that is

$$\sup_{\overline{U}} |h - fg_n| \leq \tilde{\varepsilon} \qquad \forall n \geq n_0.$$

This contradicts the fact that fg_n vanishes at p. Therefore, U cannot be relatively compact.

Also, it is easy to see that the analytical part of Behnke-Stein follows from the topological part applying the following result [12], which is similar to classical Runge's theorem.

Theorem 3.4. *Let X be a compact Riemann surface, and $K \subset X$ a compact subset. Let Q be any subset of $X \backslash K$ which contains (precisely) one point q_i from each connected component W_i of $X \backslash K$. Then, any holomorphic function on a neighborhood of K can be approximated uniformly on K by meromorphic functions on X whose poles lie in Q.*

Remark. Any relatively compact open subset of *any* Riemann surface can also be regarded as an open subset of a compact Riemann surface.

Let us now state a couple of propositions that will be useful in our proof. First, recall that an open set $Y \subset X$ is said to be *geometrically Runge* in X if $X \backslash Y$ has no compact connected components. Moreover, we have the following exhaustion result.

Proposition 3.5. [14, pp. 127] *Suppose X is an open Riemann surface. Then there exists a sequence $Y_0 \subset\subset Y_1 \subset\subset Y_2 \subset\subset \cdots$ of relatively Runge domains with $\bigcup Y_\nu = X$ so that every Y_ν has a regular boundary.*

On the other hand, we recall here the so-called *Schottky double*. This construction can be performed as follows.

If M is a complex manifold with $C_1, C_2, \dots, C_m$ boundary components, one can consider an exact duplicate of it, say $\widetilde{M}$, with the same number of boundary components, say $\widetilde{C_1}, \widetilde{C_2}, \dots, \widetilde{C_m}$. Obviously, for each point $x \in M$ there is a "symmetric" point $\widetilde{x} \in \widetilde{M}$. The *Schottky double* M^* is formed as a disjoint union $M \sqcup \widetilde{M}$ and identifying each point $x \in C_i$ with its symmetric point $\widetilde{x} \in \widetilde{C_i}$ for $1 \leq i \leq m$.

Proposition 3.6. [13, pp. 217] *Let Y be relatively Runge domain with regular boundary on a Riemann surface X. Then the Schottky double Y^* obtained by gluing Y and its mirror image $\widetilde{Y}$ together along the boundary is a compact Riemann surface.*

We are now ready to prove the analytical implication. By hypotesis, X is an open Riemann surface and K a compact subset of X such that $X \backslash K$ has no connected components with compact closure in X. Denote by $\{Y_\nu\}_\nu$ the exhaustion sequence of X given by Proposition 3.5. It is clear that there exists ν_0 such that $K \subset Y_\nu, \widetilde{K} \subset \widetilde{Y_\nu}$ for all $\nu \geq \nu_0$.

Let Q be any subset of $\widetilde{X} \backslash \widetilde{K}$ which contains (precisely) one point $\widetilde{q_i}$ from each connected component $\widetilde{W_i}$ of $\widetilde{X} \backslash \widetilde{K}$. Considering Y_ν^* with $\nu \geq \nu_0$, we are in the hypothesis of theorem 3.4, therefore any holomorphic function on a neighborhood of K can be approximated uniformly on K by meromorphic functions on Y_ν^* whose poles lie in Q for all $\nu \geq \nu_0$.

In particular, for $\varepsilon > 0$ and $f \in \mathcal{H}(K)$ there exist $g_0 \in \mathcal{M}(Y^*_{\nu_0+1})$ (so $g_0 \in \mathcal{H}(Y_{\nu_0+1})$) such that

$$\sup_{z \in K} |(f - g_0)(z)| < \varepsilon/2.$$

The idea is to apply the theorem to each pair $\{(Y_{\nu_0+(i+2)}, \overline{Y_{\nu_0+i}})\}_{i\geq 0}$ to see that there exist functions

$$\begin{array}{lll} g_1 \in \mathcal{H}(Y_{\nu_0+2}) & \text{such that} & |g_1 - g_0| < \varepsilon/2^2 \text{ on } \overline{Y_{\nu_0}}, \\ g_2 \in \mathcal{H}(Y_{\nu_0+3}) & \text{such that} & |g_2 - g_1| < \varepsilon/2^3 \text{ on } \overline{Y_{\nu_0+1}}, \\ \quad \dots & \quad \dots & \\ g_n \in \mathcal{H}(Y_{\nu_0+(n+1)}) & \text{such that} & |g_n - g_{n-1}| < \varepsilon/2^n \text{ on } \overline{Y_{\nu_0+(n-1)}}. \end{array}$$

To check that the family $\mathcal{F} = \{g_n\}_{n\geq 0}$ is normal in X it is enough to prove that it is uniformly bounded in compact subsets of X. However, if $\widetilde{K}$ is an arbitrary compact set of X, it is clear that there exists n_0

such that $\tilde{K} \subset Y_{\nu_0+n}$ for all $n \geq n_0$. As $g_{n_0} \in \mathcal{H}(Y_{\nu_0+(n_0+1)})$, we have $g_{n_0} \in \mathcal{H}(\tilde{K})$, so $\sup_{\tilde{K}} |g_{n_0}| \leq \widetilde{C_{\tilde{K}}}$. Moreover, using our construction, we observe that for all $n \geq n_0$, we have:

$$\sup_{\tilde{K}} |g_n| \leq \sup_{\tilde{K}} |g_n - g_{n_0}| + \sup_{\tilde{K}} |g_{n_0}| \leq \sup_{\overline{Y_{\nu_0+n}}} |g_n - g_{n_0}| + \sup_{\tilde{K}} |g_{n_0}| \leq \varepsilon + \widetilde{C_{\tilde{K}}} = C_{\tilde{K}}.$$

Applying Montel's theorem, there exists a subsequence $\{g_{n_k}\}_k$ which converges uniformly on every compact subset of X. And by Weierstrass' theorem:

$$g := \lim_{k\to\infty} g_{n_k} \in \mathcal{H}(X).$$

Finally, note that:

$$\sup_{z\in K} |(f-g)(z)| \leq \sup_{z\in K} |(f-g_0)(z)| + \sup_{z\in K} |(g_0 - g)(z)| < \varepsilon.$$

Therefore, every holomorphic function in a neighborhood of K can be uniformly approximated on K by holomorphic functions on X, as desired.

Remark. Theorem 3.4 becomes the classical Runge's theorem when:

i) $X = \hat{\mathbb{C}} \equiv \mathbb{C} \cup \{\infty\}$ is the Riemann sphere and $K \subset \mathbb{C}$,

ii) $q_\infty = \infty$ for the component W_∞ of $X \backslash K$ containing ∞.

We now turn our attention to the proof of theorem 3.4. For this purpose, we shall follow the same procedure that we have detailed in the case of the Riemann sphere. We will only focus on the details of the challenges posed by the new construction.

The two new problems that arise when we try to generalize our result are:

1. the existence of Green's functions in Riemann surfaces,

2. estimates for the solution to the $\bar{\partial}$-equation in Riemann surfaces.

Obtaining a subharmonic weight function from the Green's functions of the holes can be achieved in a simple way.

1. Existence of Green's functions in Riemann surfaces. There is not always a Green's function for a Riemann surface. From the viewpoint of potential theory a Riemann surface can be classified as:

(1) hyperbolic, if it has a non-constant bounded subharmonic function,

(2) elliptic, if it is compact, or

(3) parabolic, otherwise.

We call this classification potential-theoretic because the condition of having a bounded subharmonic function is equivalent to the existence of a Green's function.

Given this, it is necessary to impose that the holes W_i are hyperbolic. This follows from the fact that holes are regular domains, see Figure 3.

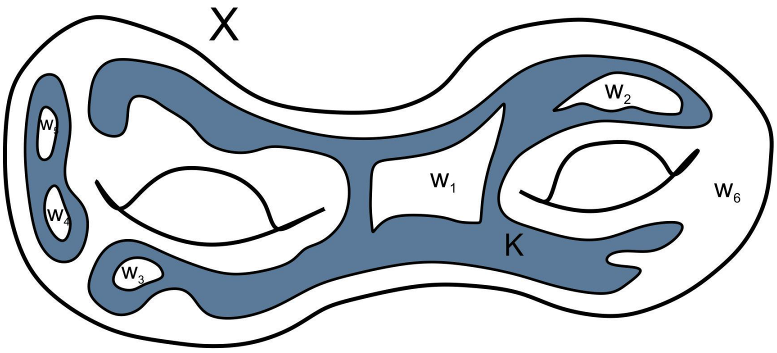


Figure 3: Example of our setting.

Proposition 3.7. [6, pp. 95] *Let $\xi \in \partial\Omega$. If the connected component of $\partial\Omega$ containing ξ consists of more that one point, then ξ is a regular point for Ω. In particular, if Ω is simply connected, then every point of $\partial\Omega$ is a regular point.*

Proposition 3.8. [14, pp. 118] *Let X be a Riemann surface and let $\Omega \subset X$ be an open subset all of whose boundary points are regular. Then the Dirichlet problem has a solution on Ω.*

We have that $\Omega = W_i$ is hyperbolic. Let us give now the definition of Green's function.

Definition 3.9. Let M be a Riemann surface. A Green's function for M is a map $g_M : M \times M \longrightarrow (-\infty, \infty]$ such that for each $x \in M$:

(a) $g_M(\cdot, x)$ is harmonic on $M \backslash \{x\}$ (superharmonic on M),

(b) if z is any local coordinate in a neighborhood U of x which $z(x) = 0$ then

$$g_M(\cdot, x) - \log \frac{1}{|z(\cdot)|}$$

is harmonic on U,

(c) if H is any other superharmonic function satisfying (a) and (b) then

$$g_M(\cdot, x) \leq H(\cdot).$$

In our case, identifying M with W_i and x with q_i,

$$G_i(z) := g_{W_i}(z, q_i) \quad z \in W_i.$$

Remark. On a Riemann surface M with boundary, a Green's function is a solution of the distributional boundary value problem

$$i\partial\bar{\partial} g_M(\cdot, x) = 2\pi\delta_x \qquad g_M(\cdot, x)\big|_{\partial M} = 0$$

as x varies over the points of the interior of M.

2. $\bar{\partial}$-estimates in Riemann surfaces. The version of Hörmander's theorem that we want to use involves properties of holomorphic line bundles over Riemann surfaces. It will be detailed further on, in the statement of theorem 3.10. For a more through approach to these we refer the reader to [4, 14].

Now we shall see that we are under the conditions of theorem 3.10. Fix a Hermitian metric

$$\omega = e^{-\psi}\frac{i}{2}\,dz\wedge d\bar{z}$$

for the compact Riemann surface X and note that a Riemannian metric for X is a Hermitian metric for $T_X^{1,0} \equiv (K_X)^*$, where $T_X^{1,0}$ and K_X are the holomorphic tangent and canonical bundles of X, respectively. As every Riemann surface admits a line bundle that has a metric of strictly positive curvature $c(\cdot)$, there is a holomorphic line bundle $L \longrightarrow X$ and a smooth Hermitian metric $e^{-\varphi}$ for L such that $i\partial\bar{\partial}\varphi$ is a strictly positive $(1,1)$-form. This means that

$$ic(\varphi) = i\partial\bar{\partial}(\varphi) = l\omega,$$

with l a strictly positive function.

We note that if F and F' are line bundles over X, we can form a new line bundle $F\otimes F'$ by taking tensor products on the fibers. Moreover if ϕ is a metric on F and ϕ' is a metric on F' then $\phi+\phi'$ is a metric on $F\otimes F' \equiv F + F'$.

Thus, the holomorphic line bundle $L \longrightarrow X$ with hermitian metric $e^{-\varphi}$ is strictly positive. Now we modify this line bundle $L \longrightarrow X$ to achieve our goal. For this purpose we introduce a new free-parameter $k >> 0$, which we will later establish, and we consider $L^{\otimes k} = kL$ the product of L with itself k times. As the metric on L is represented by a smooth function φ, then the metric on $L^{\otimes k}$ is given by $k\varphi$.

Now we consider the Picard group Pic(X) of holomorphic line bundles on a complex manifold X. We have $L^{\otimes k} \longrightarrow X$ a holomorphic line bundle with Hermitian metric $e^{-k\varphi}$, and it is clear that $i\partial\bar{\partial}(k\varphi)$ is a strictly positive $(1,1)$-form. More precisely

$$ic(k\varphi) = i\partial\bar{\partial}(k\varphi) = k\, i\partial\bar{\partial}(\varphi) = k\, l\omega,$$

with l a strictly positive function. However, we find a technical difficulty: Hörmander's estimate for the $\bar{\partial}$-equation deals with $(1,1)$-forms rather than $(0,1)$-forms. We can always twist the line bundle $L^{\otimes k}$ with the canonical bundle to shift from $(0,1)$-forms to $(1,1)$-forms. The bundle $L^{\otimes k}$ can be expressed as $L^{\otimes k} = K_X + F_k$ where K_X is the canonical line bundle and

$$F_k = L^{\otimes k} - K_X = L^{\otimes k} + (K_X)^* = L^{\otimes k} + T_X^{1,0}.$$

As we have $L^{\otimes k}$ with the metric $k\varphi$ and $T_X^{1,0}$ with the metric inherited from the Hermitian metric on X, then the metric on F_k is

$$k\varphi + \psi.$$

Thus, we obtain

$$\begin{aligned} \text{section on } L^{\otimes k} \quad &\longleftrightarrow \quad (1,0) \text{ section on } F_k \\ (0,1)\text{-form on } L^{\otimes k} \quad &\longleftrightarrow \quad (1,1)\text{-form valued on } F_k. \end{aligned}$$

Since X is a compact Riemann surface, taking $k >> 0$ big enough we see that the metric of F_k is strictly positive. This means:

$$ic(k\varphi+\psi) = i\partial\bar{\partial}(k\varphi+\psi) = \tilde{g}\omega$$

with $\tilde{g}$ a strictly positive function. The key is that φ is strictly positive and X is a compact Riemann surface.

We have finished the first part of the proof. In the next one, we will focus on the open (non-compact) Riemann surface $X\backslash\{q_1,\dots,q_n\}$, where all the results of the first part also apply.

The following step is to modify the metric $k\varphi$ of $L^{\otimes k}$ so that the problem can be solved. In order to do so, we will use the following fact: if $k\varphi$ is a metric on $L^{\otimes k}$, then any other metric on $L^{\otimes k}$ can be written as $k\varphi + \Upsilon$ where Υ is a function. In our case, $\Upsilon \equiv M\phi$ where $M >> 0$ is a free-parameter and ϕ is the subharmonic function in $X\backslash\{q_1, \dots, q_n\}$ given by the Green's function in the holes. We have

$$ic(M\phi) = i\partial\bar{\partial}(M\phi) = M\, i\partial\bar{\partial}(\phi) = Ml'\omega$$

with l' a non-negative function.

Thus, the metric $k\varphi + M\phi$ of $L^{\otimes k}$ is strictly positive in $X\backslash\{q_1, \dots, q_n\}$. Then

$$ic(k\varphi + M\phi) = i\partial\bar{\partial}(k\varphi + M\phi) = k\, i\partial\bar{\partial}(\varphi) + M\, i\partial\bar{\partial}(\phi) = (kl + Ml')\omega$$

with l a strictly positive and l' a non-negative function.

Therefore, $k\varphi + M\phi + \psi$ is also a strictly positive metric on F_k. This means that

$$ic(k\varphi + M\phi + \psi) = i\partial\bar{\partial}(k\varphi + M\phi + \psi) = g\omega$$

with g a strictly positive function.

We use a more general version of Hörmander's theorem for complete Kähler manifolds –and in particular for Stein manifolds– which we can find in [4]. Here, we use that a connected Riemann surface is a Stein manifold if and only if it is open (not-compact). As X is a compact Riemann surface, then $X\backslash\{q_1, \dots, q_n\}$ is an open Riemann surface and therefore $X\backslash\{q_1, \dots, q_n\}$is a Stein manifold.

Theorem 3.10. [4, pp. 38] *Let F be a holomorphic line bundle endowed with a metric Φ over a Riemann surface M which has some complete Kähler metric. Assume the metric Φ on F has (strictly) positive curvature and that $ic(\Phi) = i\partial\bar{\partial}(\Phi) = g\omega$, with g a strictly positive function and ω is a Kähler metric on M.*

Let α be a $\bar{\partial}$-closed $(1,1)$-form with values on F. Then there is a $(1,0)$-form u with values on F such that:

$$\bar{\partial}u = \alpha \qquad \text{and} \qquad ||u||^2 \leq \frac{1}{g}||\alpha||^2,$$

provided the right hand side is finite.

We must stress that we do not need to assume that the Kähler metric appearing in the final estimate is complete, only that the manifold has some complete metric.

Note that if $\alpha = s\xi \otimes d\bar{z}$, then we have

$$||u||^2 = \int_M |u|^2 e^{-\Phi}\omega \leq \frac{1}{g}\int_M |s|^2 e^{-\Phi}\frac{i}{2}\,dz \wedge d\bar{z} = \frac{1}{g}||\alpha||^2.$$

Remark. Set

$$M \equiv X\backslash\{q_1, \dots, q_n\},$$
$$F \equiv F_k = L^{\otimes k} + T_X^{1,0}, \qquad L \equiv L^{\otimes k},$$
$$\Phi \equiv k\varphi + M\phi + \psi, \qquad \alpha \equiv (f\bar{\partial}\chi)\xi \otimes d\bar{z}, \qquad s \equiv f\bar{\partial}\chi.$$

Then there is the correspondence

$(1,1)$-form with values on $F \equiv L + T_M^{1,0}$ $\longleftrightarrow$ $(0,1)$-form with values on L

$(1,0)$-form with values on $F \equiv L + T_M^{1,0}$ $\longleftrightarrow$ $(0,0)$-form (function) with values on L.

In particular, we have the following estimate:

$$\int_{X\setminus\{q_1,\dots,q_n\}} |u|^2 e^{-(k\varphi+M\phi)}\omega \le \frac{1}{g}\int_{X\setminus\{q_1,\dots,q_n\}} |f\bar\partial\chi|^2 e^{-(k\varphi+M\phi)}\frac{i}{2}\,dz\wedge d\bar z.$$

Since φ is a smooth function in X, which is compact, φ is bounded above and below in X and, in particular, in $X\setminus\{q_1,\dots,q_n\}$. Thus there exist C_1, C_2 such that $C_1 \le e^{-k\varphi} \le C_2$, and we get a new estimate that is similar to the one we obtained for the Riemann sphere:

$$C_1\int_{X\setminus\{q_1,\dots,q_n\}} |u|^2 e^{-M\phi}\omega \le \frac{C_2}{g}\int_{X\setminus\{q_1,\dots,q_n\}} |f\bar\partial\chi|^2 e^{-M\phi}\frac{i}{2}\,dz\wedge d\bar z.$$

On the other hand $\mathrm{Supp}(\bar\partial\chi) \subset \bigcup_{i=1}^n\{z\in W_i : \delta - t\delta/2 \le G_i(z) \le \delta\}$, and there exists $\lambda > 0$ such that

$$i\partial\bar\partial(M\phi) \ge M\lambda\,\omega$$

and so

$$g \ge M\lambda,$$

both on Supp $(\bar\partial\chi)$. Therefore:

$$\begin{aligned}
C_1\int_{X\setminus\{q_1,\dots,q_n\}} |u|^2 e^{-M\phi}\omega &\le \frac{C_2}{g}\int_{X\setminus\{q_1,\dots,q_n\}} |f\bar\partial\chi|^2 e^{-M\phi}\frac{i}{2}\,dz\wedge d\bar z\\
&\le \frac{C_2}{M\lambda}\int_{\mathrm{Supp}(\bar\partial\chi)} |f\bar\partial\chi|^2 e^{-M\phi}\frac{i}{2}\,dz\wedge d\bar z\\
&\le \frac{C_2}{M\lambda}\int_{\cup_i\{z\in W_i:\delta-t\delta/2\le G_i(z)\le\delta\}} |f\bar\partial\chi|^2 e^{-M\phi}\frac{i}{2}\,dz\wedge d\bar z.
\end{aligned}$$

A final remark: this proof does not work for $\mathbb{C}^n$ and therefore it cannot be generalized for n-dimensional complex manifolds with $n > 1$. This is so because one of the main tools of our method are Green's functions, which are subharmonic but not plurisubharmonic, as we would require in the case of several variables.

References

[1] T. Aubin: *A Course in Differential Geometry*. Graduate Studies in Mathematics, **27**, Am. Math. Soc., (2001).

[2] H. Behnke and K. Stein: *Entwicklung analytischer Funklionen auf Riemannschen Flächen*. Math. Ann. **120**, pp. 430–461, (1948).

[3] B. Berndtsson: *L^2-methods for the $\bar\partial$-equation*. Kass University Press, (1995).

[4] B. Berndtsson: *An introduction to things $\bar\partial$*. Lecture notes from the PCMI, (2010).

[5] T.W. Gamelin: *Complex Analysis*. UTM Springer-Verlag, (2001).

[6] J. Garnett and D. Marshall: *Harmonic Measure*. Cambridge University Press, (2005).

[7] L. Hörmander: *L^2-estimates and existence theorems for the $\bar\partial$-operator*. Acta Math **113**, (1965).

[8] T. Napier and M. Ramachandran: *An Introduction to Riemann Surfaces*. Birkhäuser, (2010).

[9] T. Ransford: *Potential Theory in the Complex Plane*. London Mathematical Society, Student Texts **28**, (1995).

[10] W. Rudin: *Real and Complex Analysis*. McGraw-Hill, (1966).

[11] D. Sarason: *Notes on Complex Function Theory*. Lecture notes, (1994).

[12] R.R. Simha: *The Behnke-Stein theorem for open Riemann surfaces*. Proc. Amer. Math. Soc., **105**(4), pp. 876–880, (1989).

[13] G. Springer: *Introduction to Riemann Surfaces*. Addison-Wesley, (1957).

[14] D. Varolin: *Riemann Surfaces by Way of Complex Analytic Geometry*. Graduate Studies in Mathematics **125**, (2011).

REPORTS@SCM
AN ELECTRONIC JOURNAL OF THE
SOCIETAT CATALANA DE MATEMÀTIQUES

Some characterizations of Howson PC-groups

*Jordi Delgado
Universitat Politècnica de Catalunya
jorge.delgado@upc.edu

∗Corresponding author

Resum *(CAT)*
Es demostra que, a la classe dels grups parcialment commutatius, les condicions d'ésser Howson, ésser totalment residualment lliure, i ésser producte lliure de grups lliure-abelians, són equivalents.

Abstract *(ENG)*
We show that, within the class of partially commutative groups, the conditions of being Howson, being fully residually free, and being a free product of free-abelian groups, are equivalent.

Societat Catalana de Matemàtiques

Institut d'Estudis Catalans

Keywords: *PC-group, residually free, Howson group.*
MSC (2010): *20Exx.*
Received: *May 9, 2014.*
Accepted: *May 20, 2014.*

Acknowledgement
The author gratefully acknowledges the support of *Universitat Politècnica de Catalunya* through PhD grant number 81--727, and the partial support from the MEC (Spanish Government) through research project number MTM2011-25955.

In [10], the authors study the family of finitely generated partially commutative groups for which the fixed points subgroup of every endomorphism is finitely generated. Concretely, they characterize this family as those groups consisting in (finite) free products of finitely generated free-abelian groups.

In this note we provide an elementary proof for two extra characterizations of this same family, namely: being Howson, and being a limit group. Moreover, we observe that, for some of the properties, no restriction in the cardinal of the generating set is needed, and the result holds in full generality (i.e. for every — possibly infinitely generated — partially commutative group).

1. Preliminaries

We call *partially commutative groups* (*PC-groups*, for short) the groups that admit a presentation in which all the relations are commutators between generators, i.e. a presentation of the form $\langle X \mid R \rangle$, where R is a subset of $[X, X]$ (the *set* of commutators between elements in X).

We can represent this situation in a very natural way through the (simple) graph $\Gamma = (X, E)$ having as vertices the generators in X, and two vertices $x, y \in X$ being adjacent if and only if its commutator $[x, y]$ belongs to R; then we say that the PC-group is *presented* by the graph Γ, and we denote it by $\langle \Gamma \rangle$. Recall that a *simple graph* is undirected, loopless, and without multiple edges; so, Γ is nothing more than a symmetric and irreflexive binary relation in X.

A subgraph of a graph $\Gamma = (X, E)$ is said to be *full* if it has exactly the edges that appear in Γ over the same vertex set, say $Y \subseteq X$. Then, it is called the *full subgraph of* Γ *spanned by* Y, and we denote it by $\Gamma[Y]$. If Γ has a full subgraph isomorphic to a certain graph Λ, we will abuse the terminology and say that Λ is (or appears as) a full subgraph of Γ; we denote this situation by $\Lambda \leqslant \Gamma$. When none of the graphs belonging to a certain family $\mathcal{F}$ appear as a full subgraph of Γ, we say that Γ is $\mathcal{F}$*-free*. In particular, a graph Γ is Λ*-free* if it does not have any full subgraph isomorphic to Λ.

It is clear that every graph Γ presents exactly one PC-group; that is, we have a surjective map $\Gamma \mapsto \langle \Gamma \rangle$ between (isomorphic classes of) simple graphs and (isomorphic classes of) PC-groups. A key result proved by Droms in [5] states that this map is, in fact, bijective. Therefore, we have an absolutely transparent geometric characterization of isomorphic classes of PC-groups: we can identify them with simple graphs.

This way, the PC-group corresponding to a graph with no edges is a free group, and the one corresponding to a complete graph is a free-abelian group (in both cases, with rank equal to the number of vertices). So, we can think of PC-groups as a generalization of these two extreme cases including all the intermediate commutativity situations between them.

Similarly, disjoint unions and *joins of graphs* (i.e. disjoint unions with all possible edges between distinct constituents added) correspond to free products and weak direct products of PC-groups, respectively. So, for example, the finitely generated free-abelian times free group $\mathbb{Z}^m \times F_n$ is presented by the join of a complete graph of order m and an edgeless graph of order n.

All these facts are direct from definitions, and make the equivalence between the conditions in the following lemma almost immediate as well.

Lemma 1.1. *Let Γ be an arbitrary simple graph, and $\langle \Gamma \rangle$ the corresponding PC-group. Then, the following conditions are equivalent:*

(i) the path on three vertices P_3 is not a full subgraph of Γ (i.e. Γ is P_3-free),

(ii) the reflexive closure of Γ is a transitive binary relation,

(iii) Γ *is a disjoint union of complete graphs,*

(iv) $\langle\,\Gamma\,\rangle$ *is a free product of free-abelian groups.* □

The next lemma, for which we provide an elementary proof, is also well known. We will use it in the proof of Theorem 2.1.

Lemma 1.2. *Let* Γ *be an arbitrary simple graph, and* Y *a subset of vertices of* Γ*. Then, the subgroup of* $\langle\,\Gamma\,\rangle$ *generated by* Y *is isomorphic to the PC-group presented by* $\Gamma[Y]$*.*

Proof. Let X be the set of vertices of Γ (then $Y \subseteq X$), and consider the following two homomorphisms:

$$\begin{array}{ccc} \langle\,\Gamma[Y]\,\rangle & \xrightarrow{\alpha} & \langle\,\Gamma\,\rangle \\ y & \longmapsto & y \end{array} \quad , \qquad \begin{array}{rcc} \langle\,\Gamma\,\rangle & \xrightarrow{\rho} & \langle\,\Gamma[Y]\,\rangle \\ Y \ni y & \longmapsto & y \\ X \setminus Y \ni x & \longmapsto & 1 \end{array} .$$

It is clear that both α and ρ are well defined homomorphisms (they obviously respect relations). Moreover, note that the composition $\alpha\rho$ (α followed by ρ) is the identity map on $\langle\,\Gamma[Y]\,\rangle$. Therefore, α is a monomorphism, and thus $\langle\,\Gamma[Y]\,\rangle$ is isomorphic to its image under α, which is exactly the subgroup of $\langle\,\Gamma\,\rangle$ generated by Y, as we wanted to prove. □

A group is said to satisfy the *Howson property* (or to be *Howson*, for short) if the intersection of any two finitely generated subgroups is again finitely generated. It is well known that free and free-abelian groups are Howson (see, for example, [1] and [6] respectively).

However, not every PC-group is Howson: for example, a free-abelian times free group (studied in [4]) turns out to be Howson if and only if it does not have $\mathbb{Z} \times F_2$ as a subgroup. So, it is a natural question to ask for a characterization of Howson PC-groups, and we will see in Theorem 2.1 that the very same condition (not containing $\mathbb{Z} \times F_2$ as a subgroup) works for a general PC-group.

For limit groups there are lots of different equivalent definitions. We shall use the one using fully residual freeness (see [12] for details): a group G is *fully residually free* if for every finite subset $S \subseteq G$ such that $1 \notin S$, there exist an homomorphism φ from G to a free group such that $1 \notin \varphi(S)$. Then, a *limit group* is a finitely generated fully residually free group. From this definition, it is not difficult to see that both free and free-abelian groups are fully residually free, and that subgroups and free products of fully residually free groups are again fully residually free.

2. Characterizations

As proved by Rodaro, Silva, and Sykiotis [10, Theorem 3.1], if we restrict to finitely generated PC-groups, Lemma 1.1 describes exactly the family of those having finitely generated fixed point subgroup for every endomorphism (or equivalently, those having finitely generated periodic point subgroup for every endomorphism).

In the following theorem, we provide two extra characterizations for the PC-groups described in Lemma 1.1 (including the infinitely generated case). For completeness in the description, we summarize them in a single statement together with the conditions discussed above.

Theorem 2.1. *Let* Γ *be an arbitrary (possibly infinite) simple graph, and* $\langle\, \Gamma \,\rangle$ *the PC-group presented by* Γ*. Then, the following conditions are equivalent:*

(a) $\langle\, \Gamma \,\rangle$ *is fully residually free,*

(b) $\langle\, \Gamma \,\rangle$ *is Howson,*

(c) $\langle\, \Gamma \,\rangle$ *does not contain* $\mathbb{Z} \times F_2$ *as a subgroup,*

(d) $\langle\, \Gamma \,\rangle$ *is a free product of free-abelian groups.*

Moreover, if Γ *is finite, then the following additional conditions are also equivalent:*

(e) For every $\varphi \in \operatorname{End} \langle\, \Gamma \,\rangle$*, the subgroup* $\operatorname{Fix} \varphi = \{g \in \langle\, \Gamma \,\rangle \;:\; \varphi(g) = g\}$ *of fixed points of* φ *is finitely generated.*

(f) For every $\varphi \in \operatorname{End} \langle\, \Gamma \,\rangle$*, the subgroup* $\operatorname{Per} \varphi = \{g \in \langle\, \Gamma \,\rangle \;:\; \exists n \geq 1\ \varphi^n(g) = g\}$ *of periodic points of* φ *is finitely generated.*

Proof. $(a) \Rightarrow (b)$. Dahmani obtained this result for limit groups (i.e. assuming $\langle\, \Gamma \,\rangle$ finitely generated) as a consequence of them being hyperbolic relative to their maximal abelian non-cyclic subgroups (see [3, Corollary 0.4]). We note that the finitely generated condition is superfluous for this implication since the Howson property involves only finitely generated subgroups, and every subgroup of a fully residually free group is again fully residually free.

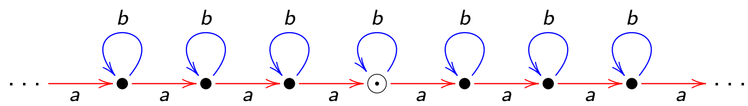
$(b) \Rightarrow (c)$. It is enough to prove that the group $\mathbb{Z} \times F_2$ does not satisfy the Howson property. The following argument is described as a solution to exercise 23.8(3) in [1] (see also [4]). Indeed, if we write $\mathbb{Z} \times F_2 = \langle\, t \mid - \,\rangle \times \langle\, a, b \mid - \,\rangle$, then the subgroups

$$H = \langle a, b \rangle = F_2 \leqslant \mathbb{Z} \times F_2, \text{ and}$$
$$K = \langle ta, b \rangle = \{w(ta, b) \mid w \in F_2\} = \{t^{|w|_a} w(a, b) \mid w \in F_2\} \leqslant \mathbb{Z} \times F_2$$

are both finitely generated, but its intersection

$$H \cap K = \{t^0 w(a, b) \mid w \in F_2,\ |w|_a = 0\} = \langle\!\langle b \rangle\!\rangle_{F_2} = \langle a^{-k} b a^k,\ k \in \mathbb{Z} \rangle$$

is infinitely generated, as you can see immediately from its Stallings graph



(see [11] and [8]), or using this alternative argument: suppose $H \cap K$ is finitely generated, then there exists $m \in \mathbb{N}$ such that $a^{m+1} b a^{-(m+1)} \in \langle a^{-k} b a^k,\ k \in [-m, m] \rangle$, and thus a^{m+1} equals the reduced form of some prefix of $w(a^m b a^{-m}, \ldots, b, \ldots, a^{-m} b a^m)$, for some word w. However, the sum of exponents of a in any such prefix must be in $[-m, m]$, which is a contradiction.

Note that both H and K are free groups of rank two whose intersection is infinitely generated. This fact, far from violating the Howson property of free groups, means that both H and K are not simultaneously contained in any free subgroup of $\mathbb{Z} \times F_2$.

$(c) \Rightarrow (d)$. From Lemma 1.2, if $\langle \Gamma \rangle$ does not contain the group $\mathbb{Z} \times F_2$ (which is presented by P_3) as a subgroup, then P_3 is not a full subgraph of Γ. Equivalently, $\langle \Gamma \rangle$ is a free product of free-abelian groups (see Lemma 1.1).

$(d) \Rightarrow (a)$. This is again clear, since free-abelian groups are fully residually free, and free products of fully residually free groups are again fully residually free. Note here, that no cardinal restriction is needed; neither for the rank of the free-abelian groups, nor for the number of factors in the free product, since the definition of fully residually freeness involves only finite families.

Finally, for the equivalence between (d), (e) and (f) under the finite generation hypothesis, see [10, Theorem 3.1]. □

Observe that an immediate corollary of Lemma 1.2 is that the PC-group presented by any full subgraph $\Lambda \leqslant \Gamma$ is itself a subgroup of the PC-group presented by Γ, i.e. for every pair of graphs Γ, Λ,

$$\Lambda \leqslant \Gamma \;\Rightarrow\; \langle \Lambda \rangle \leqslant \langle \Gamma \rangle .$$

This property provides a distinguished family of subgroups (which we will call visible) of any given PC-group. More precisely, we will say that a PC-group $\langle \Lambda \rangle$ is a *visible subgroup of* a PC-group $\langle \Gamma \rangle$ — or that $\langle \Lambda \rangle$ is *visible in* $\langle \Gamma \rangle$ — if Λ appears as a full subgraph of Γ.

Of course, visible subgroups are PC-groups as well, but not every partially commutative subgroup of a PC-group is visible (for example, F_3 is obviously not visible in F_2).

Note that although "visibility" is a relative property (a PC-group can be visible in a certain group, and not in another one), there exist PC-groups which are visible in every PC-group in which they appear as a subgroup; we will call them *explicit*. That is, a given PC-group $\langle \Lambda \rangle$ (or the graph Λ presenting it) is *explicit* if for every graph Γ,

$$\Lambda \leqslant \Gamma \;\Leftrightarrow\; \langle \Lambda \rangle \leqslant \langle \Gamma \rangle .$$

For example, it is straightforward to see that the only explicit edgeless graphs are the ones with zero, one, and two vertices: the first two cases are obvious, and for the third one, note that if $F_2 \leqslant G$ then G can not be abelian. Finally, for $n \geq 3$, it is sufficient to note (again) that F_n is not a visible subgroup of F_2.

At the opposite extreme, a well-known result [9, Lemma 18] states that the maximum rank of a free-abelian subgroup of a f.g. PC-group $\langle \Gamma \rangle$ coincides with the maximum size of a complete subgraph in Γ. An immediate corollary is that every (finite) complete graph is explicit.

In the last years, embedability between PC-groups has been a matter of growing interest and research (see [7], [9] and [2]). In particular, new examples of explicit graphs are known, such as the square C_4 (proved by Kambites in [7]), or the path on four vertices P_4 (proved by Kim and Koberda in [9]).

To end with, we just remark that our characterization theorem (Theorem 2.1) immediately provides a new member of this family.

Corollary 2.2. *The path on three vertices* P_3 *is explicit.* □

Acknowledgements. I want to express my gratitude to Enric Ventura for his constant support, and his insightful comments and suggestions.

References

[1] Oleg Bogopolski. *Introduction to Group Theory*. European Mathematical Society Publishing House, Zurich, Switzerland, February 2008.

[2] Montserrat Casals-Ruiz, Andrew Duncan, and Ilya Kazachkov. Embedddings between partially commutative groups: Two counterexamples. *Journal of Algebra*, 390:87–99, September 2013.

[3] François Dahmani. Combination of convergence groups. *Geometry & Topology*, 7:933–963, December 2003.

[4] Jordi Delgado and Enric Ventura. Algorithmic problems for free-abelian times free groups. *Journal of Algebra*, 391:256–283, October 2013.

[5] Carl Droms. Isomorphisms of graph groups. *Proceedings of the American Mathematical Society*, 100(3):407–407, March 1987.

[6] Thomas W. Hungerford. *Algebra*. Springer, 1974.

[7] Mark Kambites. On commuting elements and embeddings of graph groups and monoids. *Proceedings of the Edinburgh Mathematical Society (Series 2)*, 52(01):155–170, 2009.

[8] Ilya Kapovich and Alexei Myasnikov. Stallings foldings and subgroups of free groups. *Journal of Algebra*, 248(2):608–668, February 2002.

[9] Sang-hyun Kim and Thomas Koberda. Embedability between right-angled artin groups. *Geometry & Topology*, 17(1):493–530, April 2013.

[10] Emanuele Rodaro, Pedro V. Silva, and Mihalis Sykiotis. Fixed points of endomorphisms of graph groups. *Journal of Group Theory*, 16(4):573–583, January 2013.

[11] John R. Stallings. Topology of finite graphs. *Inventiones Mathematicae*, 71:551–565, March 1983.

[12] H. J. R. Wilton. An introduction to limit groups. March 2005.

REPORTS@SCM

AN ELECTRONIC JOURNAL OF THE
SOCIETAT CATALANA DE MATEMÀTIQUES

Gossiping in circulant graphs

*Romain Gay
École Normale Supérieure de Cachan
rgay@ens-cachan.fr

∗Corresponding author

Resum *(CAT)*
Investiguem el problema de fer safareig, en el qual els nodes d'una xarxa d'intercomunicació comparteixen informació mitjançant un protocol de comunicació per rondes. Considerem dos tipus de protocols: per rutes disjuntes en vèrtexs, i per rutes disjuntes en arestes. Donem una fita inferior general per la complexitat dels algoritmes de xafarderies en termes de la funció isoperimètrica de la xarxa. Ens centrem en els grafs de Cayley i donem algorismes òptims per subclasses de grafs de Cayley i, en particular, pels grafs circulants.

Abstract *(ENG)*
We investigate the gossiping problem, in which nodes of an intercommunication network share information initially given to each one of them according to a communication protocol by rounds. We consider two types of communication protocols: vertex-disjoint path mode, and edge-disjoint path mode. We give a general lower bound on the complexity of gossiping algorithms in terms of the isoperimetric function of the graph. We focus on Cayley graphs and give optimal algorithms for subclasses of Cayley graphs and, in particular, for circulant graphs.

Keywords: *Gossiping, isoperimetric function, Cayley graphs, circulant graphs, cube.*
MSC (2010): *05C85, 68R10.*
Received: *November 21, 2013.*
Accepted: *May 9, 2014.*

Acknowledgement
This work has been developed during a research stay in the research group Combgraph at the Universitat Politècnica de Catalunya under the supervision of Prof. Oriol Serra.

1. Introduction and definitions

1.1 Motivation

In this paper, we study the gossiping problem, in which we disseminate information among an intercommunication network. Initially, each node of the network has some private piece of information. The nodes exchange information through the network, in consecutive rounds, where in each round they can receive or send information, with some constraints according to the communication protocol. The information exchange is complete when each node has learned every piece of information. A gossiping algorithm decides at each round who communicates with whom. We want to find an algorithm which completes the exchange of information in a minimal number of rounds.

We study two communication protocols, the vertex-disjoint path (VDP) mode, and the edge-disjoint path (EDP) mode. In these modes, a node can communicate with another node if they are connected by a path. In every round, the gossiping algorithm selects paths between pairs of nodes that communicate with each other. In the VDP mode, the selected paths need to be vertex-disjoint, that is, they do not have any vertex in common. Similarly, in the EDP mode, the selected paths need to be edge-disjoint, that is, they do not have any edge in common. Moreover, a node can communicate with only one other node during one round. We measure the complexity of a gossiping algorithm by the number of rounds it needs to run. We call the gossip complexity of a network the minimal number of rounds needed by any gossiping algorithm to complete the exchange of information. We choose to study VDP and EDP modes because they are at the same time realistic, and powerful enough to achieve relatively fast gossiping. They have been introduced in [1]. They are widely used in real life applications, and have been extensively studied, see [2, 7, 8, 9, 13, 14]. Each of these modes of communication admits two different versions; they can either be a full duplex or a half duplex mode. In the full duplex version, when two nodes communicate with each other along a path, they both send and receive their information at the same time, whereas for the half duplex version, only one node sends its information and the other receives it. Full duplex modes are well suited for undirected graphs, which are the graphs we study in this paper. Therefore, we only deal with the full duplex version of the VDP and EDP modes.

In order to have good gossip complexity, the intercommunication network needs to have good structural properties. That is why we focus on Cayley graphs, and on circulant graphs, which are a subclass of Cayley graphs. These are popular network topologies.

1.2 Synopsis

In Section 2 we give a general lower bound for the gossip complexity of any graph, in terms of the isoperimetric function of the graph. It is a generalization of the lower bound obtained by Klasing [10]. Thanks to this lower bound, we prove that our gossiping algorithms are optimal, up to a $\log\log(n)$ factor, where n is the order of the graph.

In Section 3, we recall some notions and known results on gossiping. In particular we recall the gossip complexity of the hypercube graph, which is one of the best graphs for the gossiping problem, that is, its gossip complexity is less than the gossip complexity of any other graph. Knödel describes an optimal gossiping algorithm for the hypercube in [11]. Therefore, naturally, for graphs that have a similar structure to the hypercube, we try to use a similar gossiping algorithm. Indeed, many graphs embed into the hypercube graphs. We define the concept of embedding in the same Section 3. With this tool, we can simulate the gossiping algorithm of the hypercube graph in many other graphs, and get almost optimal algorithms. This is done for cube-connected cycles and butterfly networks by Hromkovic, Klasing and Stöhr [7], for the grid by Hromkovic, Klasing, Stöhr and Wagener [8], or more recently for circulant graphs (whose definition is given in Section 4) by Mans and Shparlinski [15]. These are standard graphs, structurally close to the hypercube. In [15], the gossiping algorithm given by the authors only works for the subclass of circulant graphs whose generator set is of size two.

In Section 4, we give an algorithm which works in almost optimal time for a wider subclass of circulant graphs, in particular for circulant graphs whose generator set is of any size. Finally, we extend the gossiping algorithm working for the circulant graphs to a more general class of Cayley graphs.

1.3 Definitions and notations

We recall here some basic definitions of graph theory. Throughout, $[n]$ denotes the set $\{1, \dots, n\}$. Let G be a *graph*. Except if mentioned explicitly, the graphs we consider are undirected and connected. We denote by $V(G)$ its set of vertices, and by $E(G)$ its set of edges. A *path* in G is a sequence of distinct vertices $u_0u_1 \cdots u_l$, where for all i in $\{0, \dots, l-1\}$, $\{u_i, u_{i+1}\}$ is an edge of G. The length of the path, l, may be equal to 0, in which case the path is reduced to the vertex u_0. We denote by $P(G)$ the set of all paths in G. We say that an edge $e \in E(G)$ *belongs* to the path $p \in P(G)$ if we have $p = u_0u_1 \cdots u_l$ and $e = \{u_i, u_{i+1}\}$, for some $i \in \{0, \dots, l-1\}$. Similarly, u *belongs* to p if we have $u = u_i$ for some $i \in \{0, \dots, l\}$. We say that two paths p and p' of $P(G)$ are *vertex-disjoint* if and only if there is no vertex u of $V(G)$ that belongs to p *and* p'. Similarly, they are *edge-disjoint* if and only if there is no edge e in $E(V)$ belonging to p *and* p'. For any path $p = u_0 \cdots u_l \in P(G)$, we call the vertices u_0 and u_l the extremities of p.

Here we give the definition of a broadcast algorithm, an accumulation algorithm, and a gossiping algorithm, which are of fundamental importance. A *communication algorithm A for the VDP mode (resp. EDP mode) in the graph G* is defined by a sequence of $t(A)$ rounds $E_1, E_2, \dots, E_{t(A)}$, with a round E_i being a set of pairwise vertex-disjoint paths of G (resp. pairwise edge-disjoint paths of G). The integer $t(A)$ is the *complexity* of A. Moreover, each node of $V(G)$ can not be the extremity of more than one path of E_i. For every vertex $v \in V(G)$ and for all $r \in \{0, \dots, t(A)\}$, we denote by $I_v(r)$ the set of information known to v after the r-th round of algorithm A. $I_v(r)$ is defined recursively by $I_v(0) = \{v\}$, and $I_v(r) = I_v(r-1) \cup I_w(r-1)$ if there exists a path p of the form $p = v, \dots, w$ or $p = w, \dots, v$ in E_r; $I_v(r) = I_v(r-1)$ otherwise.

A is a *broadcast algorithm* for the set of vertices $U \subseteq V(G)$ if for all v in $V(G)$, we have $U \subseteq I_v(t(A))$. Similarly, A is an *accumulation algorithm* for the set of vertices $U \subseteq V(G)$ if $\bigcup_{u \in U} I_u(t(A)) = V(G)$. A is a *gossiping algorithm* if for all v in $V(G)$, we have $I_v(t(A)) = V(G)$. In other words, a gossiping algorithm performs communication between the nodes in such a way that at the end of the algorithm, every node knows the secret of every other node. We call the *gossip complexity* of a graph the minimal number of rounds to achieve the gossiping in this graph. More precisely, if we denote by $\mathsf{A}^{\mathsf{G}}_{\mathsf{VDP}}$ the set of all gossiping algorithms for the VDP mode in G (resp. $\mathsf{A}^{\mathsf{G}}_{\mathsf{EDP}}$ for the EDP mode), the gossip complexity of G for the VDP mode, $\mathsf{g}_{\mathsf{VDP}}(G)$, is

$$\mathsf{g}_{\mathsf{VDP}}(G) = \min_{A \in \mathsf{A}^{\mathsf{G}}_{\mathsf{VDP}}} \{t(A)\}, \qquad (\text{resp. } \mathsf{g}_{\mathsf{EDP}}(G) = \min_{A \in \mathsf{A}^{\mathsf{G}}_{\mathsf{EDP}}} \{t(A)\}).$$

We define similarly the broadcast complexity and the accumulation complexity for a set of vertices $U \subseteq V(G)$ of a graph G, which we denote, respectively, by $\mathsf{b}_{\mathsf{VDP}}(G, U)$ and $\mathsf{a}_{\mathsf{VDP}}(G, U)$ for the VDP mode, and $\mathsf{b}_{\mathsf{EDP}}(G, U)$ and $\mathsf{a}_{\mathsf{EDP}}(G, U)$ for the EDP mode.

2. A lower bound for the gossip complexity

In this section, we give a general lower bound on the gossip complexity of any graph for the VDP and EDP modes. In [8], J. Hromkovic et al. prove a lower bound on the gossip complexity of any graph, depending on its bisection width. We can actually prove a more general lower bound, which depends on the isoperimetric number of the graph. We first give the definition of the two notions of bisection width and isoperimetric number of a graph. Then, in Theorem 2.1, we generalize the lower bound of J. Hromkovic et al. [8]. In [10], R. Klasing gives a slightly better lower bound on the gossip complexity of a graph in terms of its bisection width. It is also possible to generalize this lower bound, and obtain Theorem 2.2.

Let $G = (V, E)$ be a graph. For every $U \subseteq V$, we denote by $\partial_{\text{in}}(U)$ the *inner vertex-boundary of* U, defined by

$$\partial_{\text{in}}(U) = \{u \in U : \exists v \in V \setminus U, \{u, v\} \in E\}.$$

Similarly, we denote by $e(U)$ the *inner edge-boundary of* U, defined by

$$e(U) = \{\{u, v\} \in E : u \in U, v \in V \setminus U\}.$$

The *vertex bisection width* $\text{vbw}(G)$ *of* G is defined by

$$\text{vbw}(G) = \min\left\{|\partial_{\text{in}}(U)| : U \subset V, \left\lfloor \frac{|V|}{2} \right\rfloor \le |U| \le \left\lceil \frac{|V|}{2} \right\rceil\right\}.$$

Similarly, the *edge bisection width* $\text{ebw}(G)$ of G is defined by replacing $|\partial_{\text{in}}(U)|$ by $|e(U)|$ in the above definition. More generally, the *vertex isoperimetric number* of G is

$$\text{vi}(G, t) = \min\{|\partial_{\text{in}}(U)| : U \subset V, |U| = t\},$$

and the *edge isoperimetric number* $\text{ei}(G, t)$ is obtained by replacing $|\partial_{\text{in}}(U)|$ by $|e(U)|$ in the above definition. Intuitively, the isoperimetric number tells us if there is a bottleneck in a given graph, which would imply a high gossip complexity.

We can now state the theorem for the VDP mode.

Theorem 2.1. *Let* $G = (V, E)$ *be a graph and* (V_1, V_2) *a partition of its vertex set into parts of size* $|V_1| = n_1$ *and* $|V_2| = n_2$*. Let* $k = |\partial_{\text{in}}(V_1)|$ *and* $l = |e(V_1)|$*. Then*

$$g_{\text{VDP}}(G) \;\ge\; \log(n_1 n_2) - \log(k) - \log(\log(n_1)) - 2$$

and

$$g_{\text{EDP}}(G) \;\ge\; \log(n_1 n_2) - \log(l) - \log(\log(n_1)) - 2.$$

In particular, the inequality holds for $k = \max_t \text{vi}(G, t)$*, and* $l = \max_t \text{ei}(G, t)$*.*

We give the proof of Theorem 2.1 for the VDP mode. The proof for the EDP mode is obtained similarly, replacing the inner boundary $\partial_{\text{in}}(V_1)$ by the edge boundary $e(V_1)$.

Proof. Let $G = (V, E)$ be a graph, (V_1, V_2) a partition of its vertex set into parts of size $|V_1| = n_1$ and $|V_2| = n_2$, and $k = |\partial_{\text{in}}(V_1)|$. The idea of the proof is to estimate how much information can flow from V_1 to V_2.

Let $A = E_1, \dots, E_{t(A)}$ be a gossiping algorithm for G. For all $r \in \{0, \dots, t(A)\}$, $I_v(r)$ is the information known by v after the rth round, as defined in Section 1.3. We define $I_v^1(r)$ as $I_v^1(r) := I_v(r) \cap V_1$, and $I(r) := \bigcup_{v \in V_2} I_v^1(r)$. The value $I(r)$ represents the information that has gone from V_1 to V_2 during the first r rounds. Since A is a gossiping algorithm, every node $v \in V_2$ knows the information of all nodes in V_1 after $t(A)$ rounds, that is, it must be

$$I(t(A)) \ \geq \ |V_1| \cdot |V_2| = n_1 n_2. \tag{1}$$

Now we give an upper bound on $I(t(A))$. For all $r \in \{0, \dots, t(A)\}$, we define

$$\widehat{I}(r) := \bigcup_{v \in \partial_{\text{in}}(V_1)} I_v^1(r).$$

The value $\widehat{I}(r)$ represents the amount of information that can go from V_1 to V_2 in round r. We observe that the amount of information of a node can be at most doubled in each round. That is, for all v in V_1 and for all r in $\{0, \dots, \lfloor \log(n_1) \rfloor\}$, we have $I_v^1(r) \leq 2^r$. Therefore, we have

$$\widehat{I}(r) \ \leq \ k \min(2^r, n_1). \tag{2}$$

The amount of information from V_1 already present in V_2 in round r can be at most doubled in round $r + 1$:

$$I(r+1) \ \leq \ 2I(r) + \widehat{I}(r). \tag{3}$$

Combining equations (2) and (3), we get:

- For all $0 \leq r \leq \log(n_1)$, $\quad I(r+1) \leq 2I(r) + k2^r$.
- For all $\log(n_1) \leq r$, $\quad I(r+1) \leq 2I(r) + kn_1$.

By induction, $I(r) \leq r \cdot k \cdot 2^{r-1}$ for all $0 \leq r \leq \log(n_1)$. Moreover, for all $r > \log(n_1)$, we obtain that $I(r) \leq k \cdot 2^{r-1} (\log(n_1) + 1) - \frac{n_1 k}{2}$. In particular, for $r = t(A)$, equation (1) yields

$$n_1 n_2 \ \leq \ I(r) \ \leq \ k \cdot 2^{t(A)-1}(\log(n_1) + 1).$$

Therefore, by taking logarithms to both sides of the inequality, we get

$$\log(n_1 n_2) - \log(k) - \log(\log(n_1)) - 2 \leq t.$$

The result for the EDP mode can be obtained similarly. □

In [10], R. Klasing proves that we can improve the lower bound of J. Hromkovic et al. [8]. More precisely, he shows that we have a gossip complexity of at least $2\log(n) - \log(k) - \log(\log(k)) + O(1)$ for any graph of order n and bisection width k. We can generalize the lower bound in [8] to obtain the following theorem.

Theorem 2.2. *Let $G = (V, E)$ be a graph and (V_1, V_2) a partition of its vertex set, of size $|V_1| = n_1$ and $|V_2| = n_2$. We denote by $k = |\partial_{\text{in}}(V_1)|$ and $l = |e(V_1)|$. Then*

$$g_{\text{VDP}}(G) \geq \log(n_1 n_2) - \log(k) - \log(\log(k)) + O(1)$$

and

$$g_{\text{EDP}}(G) \geq \log(n_1 n_2) - \log(l) - \log(\log(l)) + O(1).$$

In particular, the inequality holds for $k = \max_t \text{vi}(G, t)$, and $l = \max_t \text{ei}(G, t)$. □

We omit the proof due to lack of space. It can be found in [6].

3. Basic examples, embeddings and three phase algorithms

In this section we recall the gossip complexity of some basic graphs, including the hypercube. Then we present the concept of embedding, thanks to which we can extend the gossiping algorithm for the hypercube to other similar graphs. Finally we present the so-called three phase algorithm strategy which will prove useful later on.

3.1 Basic examples

We first give a general lower bound for the gossip complexity in any graph.

Lemma 3.1. *For any graph $G = (V, E)$, for all v in V and for all $0 \leq r \leq \lfloor \log(n) \rfloor$, $|I_v(r)| \leq 2^r$. In particular,*

$$g_{\mathrm{VDP}}(G) \;\geq\; g_{\mathrm{EDP}}(G) \;\geq\; \log n.$$

Proof. By induction on r. Let $v \in V$. For $r = 0$ we have $|I_v(0)| = 1$. For all $r < \lfloor \log(n) \rfloor$, either there exists w in V such that $|I_v(r+1)| = |I_v(r) \cup I_w(r)| \leq 2^{r+1}$, or $|I_v(r+1)| = |I_v(r)| \leq 2^r \leq 2^{r+1}$. □

The hypercube is a widely used graph which is known to have good communication properties, especially for the gossiping problem. We recall its definition here.

Definition 3.2. For all $k \geq 2$, $d \geq 1$, the k-ary *hypercube* of dimension d, $H(k, d)$, is the graph defined by the set of vertices $V = \{0, \ldots, k-1\}^d$, and the set of edges E such that $\forall \alpha = a_1 \cdots a_n$, $\beta = b_1 \cdots b_n \in V$, $\{\alpha, \beta\} \in E$ if and only if $\exists i \in \{1, \ldots, d\}$ such that $b_i \neq a_i$ and, $\forall j \in \{1, \ldots, d\} \backslash \{i\}$, $b_j = a_j$.

Theorem 3.3 (Hromkovic, Klasing, Stöhr, [7])**.** *For all $k \geq 2$ and $d \geq 1$,*

$$d \lceil \log(k) \rceil \;\leq\; g_{\mathrm{EDP}}(H(k, d)) \;\leq\; g_{\mathrm{VDP}}(H(k, d)) \;\leq\; d(\lceil \log(k) \rceil + 1).$$

According to this theorem, the hypercube is the best graph for gossiping, together with the complete graph. For the latter, we have the following result by Knödel [11].

Theorem 3.4 (Knödel [11])**.** *For all $n \in \mathbb{N}$, let K_n be the complete graph of size n. Then*

$$\lceil \log(n) \rceil \;\leq\; g_{\mathrm{VDP}}(K_n) \;=\; g_{\mathrm{EDP}}(K_n) \;\leq\; \lceil \log(n) \rceil + 1.$$

3.2 Embeddings

We have seen that we can gossip in a really efficient way in the hypercube. In many other graphs, we can use similar algorithms to gossip efficiently. More generally, many graphs "contain" other subgraphs in which we know how to gossip efficiently. In order to transfer results from the subgraph to the super-graph, we use the concept of embedding.

We give the definitions of an embedding, its load, and its vertex and edge-congestion, which can be found in Kolman [12]. We also introduce new definitions, such as vertex and edge-congestion *for an algorithm A*, which will be useful in the next section.

- Let G and H be two undirected graphs. An *embedding* of the graph G into the graph H is a mapping f of the vertices of G into the vertices of H, together with a mapping g of edges of G into paths in H, such that g assigns to each edge $\{u, v\} \in E(G)$ a path from $f(u)$ to $f(v)$ in $P(H)$.

- The *load* of the embedding is the maximum number of vertices of G mapped to a single vertex of H:

$$\mathrm{load}(f, g) \;=\; \max_{v \in V(H)} \left|\{u \in V(G) : f(u) = v\}\right|.$$

  The *edge-congestion* $\mathrm{e_{cong}}(f, g)$ is defined by

$$\mathrm{e_{cong}}(f, g) \;=\; \max_{e \in E(H)} \left|\{e' \in E(G) : e \text{ belongs to } g(e')\}\right|.$$

  Similarly, the *vertex-congestion* $\mathrm{v_{cong}}(f, g)$ is defined by

$$\mathrm{v_{cong}}(f, g) \;=\; \max_{u \in V(H)} \left|\{e' \in E(G) : u \text{ belongs to } g(e')\}\right|.$$

- We do not need all paths in $g(E(G))$ to be pairwise vertex or edge disjoint, because not all edges are used at the same time by a communication algorithm. That is why we introduce a weaker notion. Let $A = E_1, E_2, \dots, E_{t(A)}$ be a communication algorithm.

  For all $e \in E(G)$ and for all $r \in \{1, \dots, t(A)\}$, we say that e is *active* in round r if and only if there exists a path $p \in E_r$ such that e belongs to p. We denote by $\mathrm{AE}(r)$ the set of *active edges* in round r.

  In the same way, for all $u \in V(G)$, we say that u is active in round r if and only if there exists a path $p \in E_r$ such that u belongs to p. We denote by $\mathrm{AV}(r)$ the set of *active vertices* in round r.

  We define the *vertex congestion for algorithm A*, ${\mathrm{v_{cong}}}^A(f, g)$, by

$${\mathrm{v_{cong}}}^A(f, g) \;=\; \max_{r \in \{1,\dots,t(A)\}, u \in V(H)} \left|\{e' \in \mathrm{AE}(r) : u \text{ belongs to } g(e')\}\right|.$$

  Similarly,

$${\mathrm{e_{cong}}}^A(f, g) \;=\; \max_{r \in \{1,\dots,t(A)\}, e \in E(H)} \left|\{e' \in \mathrm{AE}(r) : e \text{ belongs to } g(e')\}\right|.$$

  Finally, we define $\mathrm{load}^A(f, g)$ by

$$\mathrm{load}^A(f, g) \;=\; \max_{r \in \{1,\dots,t(A)\}, v \in V(H)} \left|\{u \in \mathrm{AV}(r) : f(u) = v\}\right|.$$

With the above definitions we can now state our theorem. This theorem in implicit in [7, 8, 9, 15].

Theorem 3.5. *Let $G = (V(G), E(G))$ and $H = (V(H), E(H))$ be two graphs. If A is a gossiping algorithm for G in the VDP mode (resp., EDP mode), which runs in $t(A)$ rounds; and if f,g is an embedding of G into H such that $\mathrm{load}^A(f, g) = 1$, and ${\mathrm{v_{cong}}}^A(f, g) = 1$ (resp. ${\mathrm{e_{cong}}}^A(f, g) = 1$), then we can gossip among the set of vertices $f(V(G))$ in H in less than $t(A)$ rounds in the VDP mode (resp., the EDP mode).*

Proof. We extend the function $g : E(G) \to P(H)$ on the paths of G via

$$g(u_0 u_1 \cdots u_l) \;=\; g(\{u_0, u_1\}) g(\{u_1, u_2\}) \cdots g(\{u_{l-1} u_l\})$$

for all $u_0 u_1 \cdots u_l \in P(G)$, i.e., we concatenate the images of all edges of the path $u_0 u_1 \cdots u_l$.

Let $A = E_1 E_2 \cdots E_{t(A)}$ be the gossiping algorithm of G for the VDP mode. We construct an algorithm A' which performs the gossiping among $f(V(G))$ in H in $t(A)$ rounds as follows: whenever the vertex $u \in V(G)$ communicates with $v \in V(G)$ through the path $p \in P(G)$, $f(u) \in V(H)$ communicates with $f(v) \in V(H)$ through the path $g(p) \in P(H)$. It is well defined because $f(u) \neq f(v)$, since $\mathrm{load}^A(f,g) = 1$. Let $r \in \{1, \dots, t(A)\}$ such that $E_r = \{p_1, \dots, p_l\}$, $l \geq 1$. Since $\mathrm{v_{cong}}^A(f,g) = 1$, $\{g(p_1), \dots, g(p_l)\}$ is a set of vertex-disjoint paths of $P(H)$. At the end of algorithm A', for each vertex $u \in V(G)$,

$$I_{f(u)}(t(A)) = \bigcup_{v \in V(G), f(v) = f(u)} f(I_v(t(A)),$$

so $I_{f(u)}(t(A)) = f(V(G))$. Therefore A' performs the gossiping among $f(V(G))$ properly for the VDP mode. An analogous argument works for the EDP mode. □

3.3 Three phases algorithm

In most of the hypercube-like graphs, we use a gossiping algorithm that first accumulates the information of the entire graph into a subgraph, then gossip in the subgraph as in the hypercube, and finally broadcast the information to the whole graph. This is called a three-phase algorithm.

Definition 3.6. We say a gossiping algorithm is a *three-phase algorithm* if it performs an accumulation phase, then a gossiping phase, and finally a broadcast phase:

1. **Accumulation phase:** G is divided into connected components (called *accumulation components*), each component containing exactly one accumulation node. This node accumulates the information from the nodes lying in its component.

2. **Gossip phase:** Let $a(G)$ be the set of all accumulation nodes in G. A gossiping algorithm is performed among the nodes in $a(G)$. All nodes in $V(G) - a(G)$ are considered to have no information, and they are only used to build disjoint paths between receivers and senders from $a(G)$.

3. **Broadcast phase:** Every node in $a(G)$ broadcasts the information to its component.

Here we present a useful lemma on the number of rounds needed to accumulate all the information of the path of length $n \in \mathbb{N}^*$ into one vertex at the end of the path.

Lemma 3.7 (Feldmann, Hromkovic, Monien, Madhavapeddy and Mysliwietz, [4])**.** *For all $n \in \mathbb{N}^*$, let P_n be the path of length n, i.e the graph with vertex set $\{0, \dots, n-1\}$ and edge set $E = \{\{i, i+1\}, i \in \{0, \dots, n-2\}\}$. Then*

$$\mathrm{b_{VDP}}(P_n, \{0\}) = \mathrm{a_{VDP}}(P_n, \{0\}) = \mathrm{b_{EDP}}(P_n, \{0\}) = \mathrm{a_{EDP}}(P_n, \{0\}) \leq \lceil \log(n) \rceil.$$

4. Gossiping in circulant graphs

In this section, we present the main results of this paper. Mans and Shparlinski [15] gave an optimal gossiping algorithm for some circulant graphs whose generator set is of size two. We exhibit a gossiping algorithm for more general circulant graphs whose generator set can be of any size.

We recall here the definitions of Cayley graphs and circulant graphs, which are a particular type of Cayley graphs.

Let $(G, +)$ be an additively written group, and let $S \subseteq G$ be a subset of G. The *Cayley graph* $\Gamma(G, S)$ is the graph with vertex set $V = G$ and set of arcs E such that for all $u, v \in V$, $(u, v) \in E$ if and only if there exists $s \in S$ such that $v = u + s$. If $\Gamma(G, S)$ is to be connected, S must be a generating set of G. If we want $\Gamma(G, S)$ to be undirected, S must be symmetric, i.e. of the form $S = \{\pm s_1, \dots, \pm s_r\}$.

For example, for $k \geq 2$ and $d \geq 1$, the k-ary hypercube of dimension d, $H(k, d)$, is the Cayley graph $\Gamma(\mathbb{Z}_k^d, S)$, with $S = \bigcup_{i\in[d]}\{\pm\lambda \cdot e_i : \lambda \in [k-1]\}$, where e_i is the vector whose coordinates are all zero except for the i-th coordinate, which is 1. We can generalize Theorem 3.3 for the k-ary hypercube of dimension d in the following way.

Theorem 4.1. *Let $d \geq 1$, $k_1, k_2, \dots, k_d \geq 2$. Let $S = \bigcup_{i\in[d]}\{\pm\lambda \cdot e_i : \lambda \in [k_i - 1]\}$. Then*

$$\begin{aligned}\sum_{i\in[d]} \lceil \log(k_i) \rceil &\leq g_{\mathrm{EDP}}(\Gamma(\mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \cdots \times \mathbb{Z}_{k_d}, S)) \\ &\leq g_{\mathrm{VDP}}(\Gamma(\mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \cdots \times \mathbb{Z}_{k_d}, S)) \\ &\leq \sum_{i\in[d]} (\lceil \log(k_i) \rceil + 1).\end{aligned}$$

Proof. The lower bound comes from Lemma 3.1. For the upper bound, we use Algorithm 1.

Algorithm 1 Gossip$\left(\Gamma\left(\prod_{i=1}^{d} \mathbb{Z}_{k_i}, S\right)\right)$

for $i = 1$ to d **do**
  for all $\alpha \in \prod_{j=1}^{i-1} \mathbb{Z}_{k_j}$ and $\beta \in \prod_{l=i+1}^{d} \mathbb{Z}_{k_l}$ **do in parallel**
    gossip in $L_{\alpha,\beta} = \{\alpha m \beta : m \in \{0, \dots, k_i - 1\}\}$
  end do in parallel
end for

procedure Gossip in $L_{\alpha,\beta} = \{\alpha m \beta : m \in \{0, \dots, k_i - 1\}\}$
  do in parallel
    Gossip in $\{\alpha m \beta : m \in \{0, \dots, \left\lfloor \frac{k_i}{2} \right\rfloor - 1\}\}$ **and**
    Gossip in $\{\alpha m \beta : m \in \{\left\lfloor \frac{k_i}{2} \right\rfloor, \dots, k_i - 1\}\}$
  end do in parallel
  for $l = 0$ to $\left\lfloor \frac{k_i}{2} \right\rfloor - 1$ **do in parallel**
    exchange information between $\alpha l \beta$ and $\alpha(m - l - 1)\beta$
  end do in parallel
end procedure

For all $i \in [d]$, and for all $\alpha \in \prod_{j=1}^{i-1} \mathbb{Z}_{k_j}$, $\beta \in \prod_{l=i+1}^{d} \mathbb{Z}_{k_l}$, the subgraph $L_{\alpha,\beta}$ induced by the set of vertices $\{\alpha m \beta : m \in \{0, \dots, k_i - 1\}\}$ is a clique, so we can gossip in $L_{\alpha,\beta}$ with the procedure Gossip of Algorithm 1. This procedure uses the algorithm of the complete graph K_{k_i}, which works in at most $\lceil \log(k_i) \rceil + 1$ rounds according to Theorem 3.4. So the total number of rounds needed to gossip in $\Gamma(\mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \cdots \times \mathbb{Z}_{k_d}, S)$ is at most $\sum_{i\in[d]}(\lceil \log(k_i) \rceil + 1)$. □

When $G = \mathbb{Z}_n$ is the cyclic group and $S = -S \subseteq \mathbb{Z}_n$ is a symmetric subset of $\mathbb{Z}_n$, the Cayley graph $\Gamma(\mathbb{Z}_n, S)$ is called a *circulant graph*, and will be denoted by $C(n, S)$. In the next theorem, we give a lower bound of the gossip complexity for any circulant graph using Theorem 2.2. The result was obtained by Mans and Shparlinski [15].

Theorem 4.2. *For all $n,r \in \mathbb{N}^*$, for all $S = \{\pm s_1, \dots, \pm s_r\} \subseteq \mathbb{Z}_n$ such that $s_1 \le s_2 \le \cdots \le s_r$,*

$$g_{\mathrm{VDP}}(C(n,S)) \ \ge\ 2\log(n) - \log(s_r) - \log(\log(s_r)) + O(1)$$

and

$$g_{\mathrm{EDP}}(C(n,S)) \ \ge\ 2\log(n) - \log(rs_r) - \log(\log(rs_r)) + O(1).$$

Proof. We number the nodes from 0 to $n-1$. Let $V_1 = \{0, \dots, \lfloor \frac{n}{2} \rfloor - 1\}$ and $V_2 = \{\lfloor \frac{n}{2} \rfloor, \dots, n-1\}$. Then $\partial^G_{\mathrm{in}}(V_1) \subseteq \{0, \dots, s_r - 1\} \cup \{\lfloor \frac{n}{2} \rfloor - s_r, \dots, \lfloor \frac{n}{2} \rfloor - 1\}$, because for all $u \in \{s_r, \dots, \lfloor \frac{n}{2} \rfloor - s_r - 1\}$, and all v in V_2, we have that $v - u > s_r \bmod n$, so $\{u, v\} \notin E$. Thus, $|\partial^G_{\mathrm{in}}(V_1)| \le 2s_r$. Theorem 2.2 then yields

$$\begin{aligned} g_{\mathrm{VDP}}(C(n,S)) \ &\ge\ \log\left(\left\lfloor \frac{n}{2} \right\rfloor \cdot \left\lceil \frac{n}{2} \right\rceil\right) - \log(s_r) - \log(\log(s_r)) + O(1) \\ &\ge\ 2\log(n) - \log(s_r) - \log(\log(s_r)) + O(1). \end{aligned}$$

It is easy to check that $|\mathrm{e}(V_1)| \le 2\sum_{i=1}^{r} s_i \le 2rs_r$; for further details, see [15]. Theorem 2.2 yields

$$\begin{aligned} g_{\mathrm{EDP}}(C(n,S)) \ &\ge\ \log\left(\left\lfloor \frac{n}{2} \right\rfloor \cdot \left\lceil \frac{n}{2} \right\rceil\right) - \log(2rs_r) - \log(\log(2rs_r)) + O(1) \\ &\ge\ 2\log(n) - \log(rs_r) - \log(\log(rs_r)) + O(1). \end{aligned}$$

This concludes the proof. □

For particular instances of S, we know an algorithm which matches the previous lower bound. For instance, when $S = \{\pm 1, \pm n^{1/r}, \dots, \pm n^{(r-1)/r}\}$, then $C(n,S)$ admits the grid $Gr(n^{\frac{1}{r}}, r)$ as a spanning subgraph. So we can apply the algorithm of the grid of [8] which matches the lower bound. But in the general case, we do not know whether the previous lower bound is tight. In this paper, we find an algorithm for a general class of circulant graphs, which (almost) matches the lower bound. Such an approach can be found in [15], where B. Mans and I. E. Shparlinski find an (almost) optimal gossiping algorithm for circulant graphs where $r = 2$. More precisely, they prove that if $S = \{\pm 1, \pm s_2\}$ and $s_2 \le 2\lfloor p/s_2 \rfloor$, then the lower bound of Theorem 4.2 is tight. In fact, they give an algorithm which performs in (almost) optimal time. We have generalized this approach to arbitrary r.

Theorem 4.3. *Let $n \in \mathbb{N}^*$, and $C(n,S)$ be a circulant graph with generating set $S = \{\pm s_1, \dots, \pm s_r\}$. If $s_1 = 1$, $s_1 < s_2 < \cdots < s_r$ and $\left\lceil \frac{s_{i+1}}{s_i} \right\rceil \le 2\frac{n}{s_r}$ for all $i \in [r-1]$, then*

$$2\log(n) - \log(s_r) + 2r \ \ge\ g_{\mathrm{VDP}}(C(n,S)) \ \ge\ 2\log(n) - \log(s_r) - \log(\log(s_r)) + O(1)$$

and

$$2\log(n) - \log(s_r) + 2r \ \ge\ g_{\mathrm{EDP}}(C(n,S)) \ \ge\ 2\log(n) - \log(rs_r) - \log(\log(rs_r)) + O(1).$$

Proof. We exhibit a three phase algorithm that works in at most $2\log(n) - \log(s_r) + 2r$ rounds for the VDP mode.

Accumulation phase:

We number the nodes of $C(n, S)$ from 0 to $n-1$, and identify each node with its number. We choose the accumulation nodes $a(G)$ to be $\{0, \dots, s_r - 1\}$, and the accumulation components to be

$$A_j = \{i \in \mathbb{Z}_n : i = j \bmod s_r\}, \qquad \text{for all } j \in \{0, \dots, s_r - 1\}.$$

All accumulation components are of size at most $\lfloor (n-1)/s_r \rfloor + 1$. So the accumulation phase takes at most $\lceil \log(\lfloor (n-1)/s_r \rfloor + 1) \rceil$ many rounds, which in turn is at most $\log(n/s_r) + 1$.

Gossip phase:

To simplify the proof, we suppose that

$$\frac{s_{i+1}}{s_i} = q_i \in \mathbb{N} \qquad \text{for all } i \in [r-1]. \tag{4}$$

Let $S' = \bigcup_{i \in [r-1]} \{\pm\lambda \cdot e_i : \lambda \in [q_i - 1]\}$. The Cayley graph $\Gamma(\mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_{r-1}}, S')$ is embedded into $C(n, S)$, where $f : \prod_{i=1}^{r-1} \mathbb{Z}_{q_i} \to \mathbb{Z}_n$ is defined for all $a_1 a_2 \cdots a_{r-1} \in \prod_{i=1}^{r-1} \mathbb{Z}_{q_i}$ by

$$f(a_1 a_2 \cdots a_{r-1}) = \sum_{i=1}^{r-1} a_i \cdot s_i \in \mathbb{Z}_n.$$

Let $u = a_1 \cdots a_{r-1}$ be a node in $\prod_{l=1}^{r-1} \mathbb{Z}_{q_l}$, and $v = a_1 \cdots a_{i-1} a'_i a_{i+1} \cdots a_{r-1}$, with $a_i < a'_i$. Then $g(u, v)$ is defined to be the path which goes from vertex $f(u) = \sum_{j \in [r-1]} a_j \cdot s_j$ to $\sum_{j \in [r-1]} a_j \cdot s_j + t_{a,b} \cdot s_r$ through $t_{a,b}$ chords $+s_r$, then to vertex

$$\sum_{j \in [r-1] \setminus \{i\}} a_j \cdot s_j + a'_i \cdot s_i + t_{a,b} \cdot s_r$$

through $a'_i - a_i$ chords $+s_i$, and finally to vertex

$$\sum_{j \in [r-1] \setminus \{i\}} a_j \cdot s_j + a'_i \cdot s_i$$

through $t_{a,b}$ chords $-s_r$. We choose $t_{a,b} = \lfloor \frac{b-a}{2} \rfloor$. For an illustration of the embedding (f, g), see Figure 1.

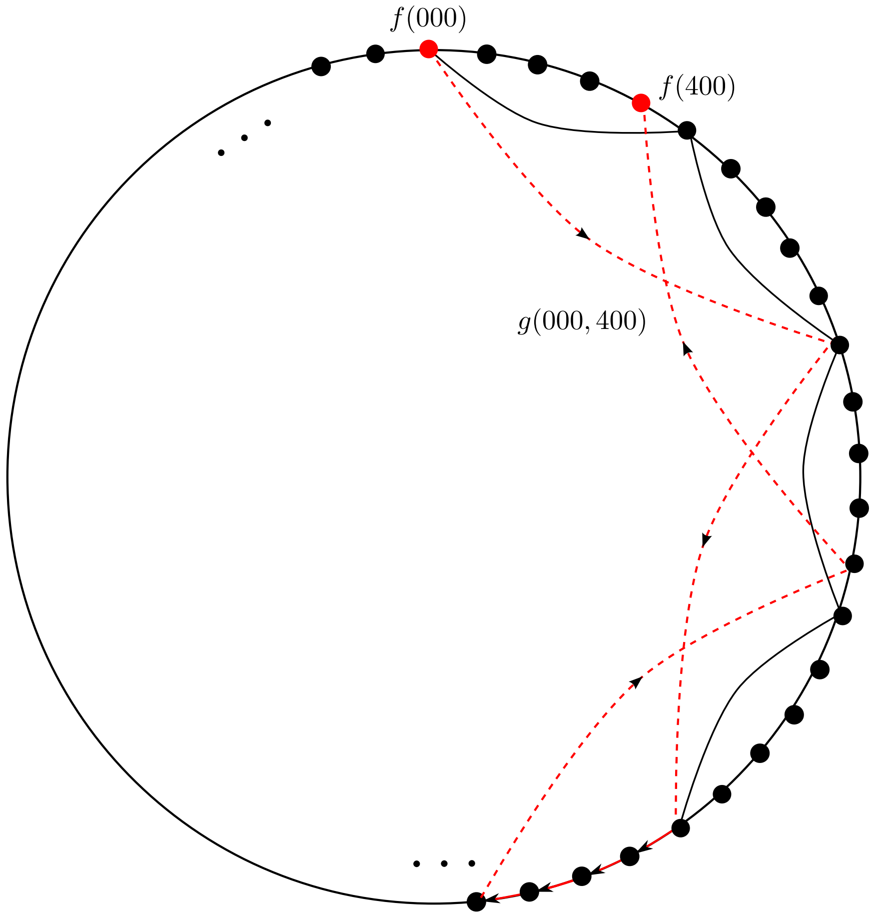
According to Theorem 3.4, there is a gossiping algorithm A for $\Gamma(\prod_{i=1}^{r-1} \mathbb{Z}_{q_i}, S')$ for the VDP mode, which works in at most $\sum_{i=1}^{r-1} (\lceil \log(q_i) \rceil + 1) \le \log(s_r) + 2(r-1)$ rounds. It is easy to check that the load of the embedding f, g for algorithm A is one. We show that $\mathrm{v_{cong}}^A(f, g) = \mathrm{e_{cong}}^A(f, g) = 1$. In Algorithm A, in each round, the exchanges of information are of the form

$a = a_1 \cdots a_{r-1} \in \prod_{i=1}^{r-1} \mathbb{Z}_{q_i}$ exchanges its information with $a' = a_1 \cdots a_{i-1} a'_i a_{i+1} \cdots a_{r-1}$, with $a_i < a'_i$.

Suppose that in the same round,

$b = b_1 \cdots b_{r-1}$ exchanges its information with $b' = b_1 \cdots b_{i-1} b'_i b_{i+1} \cdots b_{r-1}$, with $b_i < b'_i$.

By the construction of algorithm A (see Algorithm 1), $b_i < a_i$ and $a'_i < b'_i$, or $a_i < b_i$ and $b'_i < a'_i$. So $t_{a,a'} \ne t_{b,b'}$, and $\mathrm{v}^{\mathrm{A}}_{\mathrm{cong}}(f, g) = 1$. Therefore, by Theorem 3.5, there is an algorithm A' that performs the gossiping in $f(\prod_{i=1}^{r-1} \mathbb{Z}_{q_i}) = \{0, \dots, s_r - 1\}$ in at most $\log(s_r) + 2(r-1)$ rounds for the VDP mode. A' is described in Algorithm 2.



$\Gamma(\mathbb{Z}_5 \times \mathbb{Z}_2)$ is embedded into $C(n, S)$.

Figure 1: $C(n, S)$, with $S = \{\pm 1, \pm 5, \pm 10\}$

Broadcast phase:

By symmetry, the broadcast phase takes at most $\log(p/s_r) + 1$ rounds, just like the accumulation phase. Therefore the total number of rounds needed to gossip in $C(n, S)$ is at most $2\log(n) - \log(s_r) + 2r$.

In the case where we do not assume condition (4) anymore, we need to slightly modify Algorithm 2, but the essential arguments remain the same. This concludes the proof of Theorem 4.3. □

We have exhibited an algorithm that matches the lower bound on the gossip complexity for some circulant graphs (up to a $\log(\log(n))$ factor, n being the size of the graph). We must note that, even if the condition for the generating set is a generalization of the one imposed by Mans and Shparlinsky, the number of generating sets satisfying it is asymptotically small. Thus the problem of providing a gossiping for circulant graphs is still open.

The results we have found for circulant graphs can be extended to more general Cayley graphs. Let p be a prime number, $d \geq 1$, and $S \subseteq \mathbb{Z}_p^d$. We investigate gossiping in $\Gamma(\mathbb{Z}_p^d, S)$, and note that circulant graphs are the particular case where $d = 1$. We can give an upper bound of the bisection width of these graphs, and therefore bound their gossip complexity. We do so in Theorem 4.4. In Theorem 4.5, we show

Algorithm 2 Gossip($C(n, S)$)

for $i = 1$ to $r-1$ **do**
  for all $\alpha \in \prod_{j=1}^{i-1} \mathbb{Z}_{q_j}$ and $\beta \in \prod_{l=i+1}^{r-1} \mathbb{Z}_{q_l}$, **do in parallel**
    Gossip in $L_{\alpha,\beta} = \{f(\alpha m \beta), m \in \{0, \dots, q_i - 1\}\}$, where $f(a_1 \dots a_{r-1}) = \sum_{i=1}^{r-1} a_i \cdot s_i$
  end do in parallel
end for
procedure GOSSIP $L_{\alpha,\beta}$
  do in parallel
    Gossip $\left\{f(\alpha m \beta), m \in \left\{0, \dots, \left\lfloor \frac{q_i}{2} \right\rfloor - 1\right\}\right\}$ **and**
    Gossip $\left\{f(\alpha m \beta), m \in \left\{\left\lfloor \frac{q_i}{2} \right\rfloor, \dots, r-1\right\}\right\}$
  end do in parallel
  for $l = 0$ to $\left\lfloor \frac{q_i}{2} \right\rfloor - 1$ **do in parallel**
    exchange information between $f(\alpha l \beta)$ and $f(\alpha(q_i - 1 - l)\beta)$
through the path $g(\alpha l \beta, \alpha(q_i - 1 - l)\beta)$, with g defined in the proof of Theorem 4.3.
  end do in parallel
end procedure

that this lower bound is tight (up to a $\log(\log(n))$ factor, where n is the size of the graph).

Theorem 4.4. *Let $S = \{\vec{u_1}, \dots, \vec{u_r}\} \subseteq \mathbb{Z}_p^d$. For all $i \in [r]$, we write $\vec{u_i} = (u_1^i \dots, u_d^i)$. For all $l \in [d]$, we write $M_l = \max_{j \in [r]} u_l^j$, and $S_l = \sum_{j=1}^{r} u_l^j$. Then*

$$g_{\text{VDP}}\left(\Gamma(\mathbb{Z}_p^d, S)\right) \;\geq\; (d+1)\log(p) - \log \min_{l \in [d]} M_l$$

and

$$g_{\text{EDP}}\left(\Gamma(\mathbb{Z}_p^d, S)\right) \;\geq\; (d+1)\log(p) - \log \min_{l \in [d]} S_l.$$

Proof. The idea is the same as in Theorem 4.2. Let $l \in [d]$. We take $V_1 = \mathbb{Z}_p^{l-1} \times \{0, \dots, \lfloor \frac{p}{2} \rfloor - 1\} \times \mathbb{Z}_p^{d-l}$ and $V_2 = \mathbb{Z}_p^l \times \{\lfloor \frac{p}{2} \rfloor, \dots, p-1\} \times \mathbb{Z}_p^{d-l-1}$. Then

$$\partial_{\text{in}}^G(V_1) \;\subseteq\; \mathbb{Z}_p^{l-1} \times \{0, \dots, M_l - 1\} \cup \left\{\lfloor \tfrac{p}{2} \rfloor - M_l, \dots, \lfloor \tfrac{p}{2} \rfloor - 1\right\} \times \mathbb{Z}_p^{d-l},$$

because

$$v_l - u_l \;>\; M_l \bmod p$$

for all $u = (u_1, \dots, u_d) \in \mathbb{Z}_p^{l-1} \times \{M_l, \dots, \lfloor p/2 \rfloor - M_l - 1\} \times \mathbb{Z}_p^{d-l}$ and all $v = (v_1, \dots, v_d) \in V_2$, so that $\{u, v\} \notin E$. Thus, $|\partial_{\text{in}}^G(V_1)| \leq 2M_l p^{d-1}$. This is true for any $l \in [d]$, so $\text{vbw}(G) \leq 2\min_{l \in [d]} M_l p^{d-1}$. So applying Theorem 2.2, we get the result of Theorem 4.4. Similarly, we can show that $|\text{e}(V_1)| \leq 2S_l$ for any $l \in [d]$ and then get the result of Theorem 4.4 for the EDP mode. □

Consider the Cayley graph $\Gamma(\mathbb{Z}_p^d, S)$ with generating set $S = \{\pm s_1, \dots, \pm s_r\}$. For this graph to be connected, we need to have d linearly independent vectors in the set $\{s_1, \dots, s_r\}$, thus in particular $r \geq d$. Moreover, if $r = d$ then $\Gamma(\mathbb{Z}_p^d, S)$ admits the grid $Gr(p, d)$ as a spanning subgraph, and applying the algorithm of [8] gives an optimal gossiping algorithm. So the interesting case is when $r > d$.

Theorem 4.5. *Let p be a prime, and let $d, r \in \mathbb{N}^*$ such that $r > d$. Let $S = \{\pm\vec{u_1}, \dots, \pm\vec{u_r}\} \subseteq \mathbb{Z}_p^d$ such that S generates $\mathbb{Z}_p^d$. For all $i \in [r]$, we write $\vec{u_i} = (u_1^i, \dots, u_d^i)$, and assume that $\vec{u_i} = \lambda_i e_i$ for all $i \in [d-1]$, where e_i is the i-th standard vector as above and $\lambda_i \in \mathbb{Z}_p$.*

If $u_d^d = 1$, $u_d^d < u_d^{d+1} < \cdots < u_d^r$, and $\left\lceil \frac{u_d^{i+1}}{u_d^i} \right\rceil \leq 2\frac{p}{u_d^r}$ for all $i \in \{d, \dots, r-1\}$, then

$$\begin{aligned} g_{\mathrm{VDP}}(\Gamma(\mathbb{Z}_p^d, S)) &\leq (d+2)\log(p) + \log(u_d^r) + 2r - \log(\log(p)) + O(1), \\ g_{\mathrm{VDP}}(\Gamma(\mathbb{Z}_p^d, S)) &\geq 2\log(p) - \log(u_d^r) - \log(\log(u_d^r)) + O(1), \end{aligned}$$

and

$$\begin{aligned} g_{\mathrm{EDP}}(\Gamma(\mathbb{Z}_p^d, S)) &\leq (d+2)\log(p) + \log(u_d^r) + 2r - \log(\log(p)) + O(1), \\ g_{\mathrm{EDP}}(\Gamma(\mathbb{Z}_p^d, S)) &\geq 2\log(p) - \log(ru_d^r) - \log(\log(ru_d^r)) + O(1). \end{aligned}$$

We omit the proof of this theorem, which can be found in [6].

5. Conclusion and open problems

We have given an (almost) optimal gossiping algorithm for a class of circulant graphs. Furthermore, we have shown that we can extend this algorithm to a more general class of Cayley graphs. Finding an optimal gossiping algorithm for all circulant graphs remains an open problem.

It would also be interesting to look for a general algorithm that performs gossiping for a larger class of Cayley graphs. This may also involve looking for better lower bounds for Cayley graphs.

Furthermore, there are other graphs whose structure is close to the hypercube for which we don't know any optimal gossiping algorithm. This the case for the De Bruijn graph. In [6], a gossiping algorithm for this graph is given, but it still far from the known lower bound. In general, any graphs that are good expanders are worth studying for the gossiping problem.

Another interesting problem would be to investigate different kinds of gossiping algorithms. For instance, random gossiping algorithms have been studied for the complete graph [5], for the hypercube [3], or for the grid, but to the best of our knowledge, no such results are known for circulant or Cayley graphs.

References

[1] B. Baker and R. Shostak. Gossips and telephones. *Discrete Mathematics*, 2:191–193, 1972.

[2] S. Even and B. Monien. On the Number of Rounds Necessary to Disseminate Information (Extended Abstract). In *First ACM Symposium on Parallel Algorithms and Architectures (SPAA)*, pages 318–327. ACM, 1989.

[3] Uriel Feige, David Peleg, Prabhakar Raghavan, and Eli Upfal. Randomized broadcast in networks. *Random Struct. Algorithms*, 1(4):447–460, 1990.

[4] R. Feldmann, J. Hromkovic, B. Monien, S. Madhavapeddy, and P. Mysliwietz. Optimal algorithms for dissemination of information in generalized communication modes. *Discrete*

Applied Mathematics, 53:55–78, 1994.

[5] A.M. Frieze and G.R. Grimmett. The shortest-path problem for graphs with random arc-lengths. *Discrete Applied Mathematics*, 10:57–77, 1985.

[6] R. Gay. Gossiping in Cayley graphs. Technical report, ENS Cachan, France, 2013.

[7] J. Hromkovic, R. Klasing, and E.A. Stöhr. Dissemination of information in vertex-disjoint paths mode. *Computers and Artificial Inteligence*, 15:295–318, 1996.

[8] J. Hromkovic, R. Klasing, E.A. Stöhr, and H. Wagener. Gossiping in vertex-disjoint paths mode in d-dimensional grids and planar graphs. *Information and Computation*, 123:17–28, 1995.

[9] J. Hromkovic, R. Klasing, W. Unger, and H. Wagener. Optimal algorithms for broadcast and gossip in the edge-disjoint path modes. *Information and Computation*, 133:1–33, 1997.

[10] Ralf Klasing. The relationship between gossiping in vertex-disjoint paths mode and bisection width. *Discrete Applied Mathematics*, 83(1-3):229–246, March 1998.

[11] W. Knödel. New gossips and telephones. *Discrete Mathematics*, 13:95, 1975.

[12] P. Kolman. *Searching for Edge Disjoint Paths on Hypercube-like Topologies*. PhD thesis, Faculty of Mathematics and Physics Charles University, Prague, September 1998.

[13] D. W. Krumme, G. Cybenko, and K. N. Venkataraman. Gossiping in minimal time. *SIAM J. on Computing*, 21:111–139, 1992.

[14] R. Labahn and I. Warnke. Quick gossiping by telegraphs. *Discrete Mathematics*, 126:421–424, 1994.

[15] B. Mans and I. E. Shparlinski. Random walks and bisections in random circulant graphs. *LATIN*, pages 542–555, 2012.

REPORTS @SCM
AN ELECTRONIC JOURNAL OF THE
SOCIETAT CATALANA DE MATEMÀTIQUES

A polynomial time algorithm for the conjugacy problem in $\mathbb{Z}^n \rtimes \mathbb{Z}$

Bren Cavallo
CUNY Graduate Center
bcavallo@gc.cuny.edu

***Delaram Kahrobaei**
CUNY Graduate Center
and
New York City College of Technology
dkahrobaei@gc.cuny.edu

*Corresponding author

Resum *(CAT)*
En aquest article introduïm un algorisme que, en temps polinomial, resol el problema de la conjugació (en les seves dues variants, de decisió i de cerca) per a grups de la forma lliure abelià per infinit cíclic, amb els inputs donats en forma normal. Fem això adaptant els resultats de Bogopolski–Martino–Maslakova–Ventura a [1] i de Bogopolski–Martino–Ventura a [2], als grups en qüestió i, en certs casos, usem un algorisme de Kannan–Lipton [7] per a resoldre el problema de l'òrbita a $\mathbb{Z}^n$ en temps polinomial.

Abstract *(ENG)*
In this paper we introduce a polynomial time algorithm that solves both the conjugacy decision and search problems in free abelian-by-infinite cyclic groups, where the inputs are elements in normal form. We do this by adapting the work of Bogopolski–Martino–Maslakova–Ventura in [1] and Bogopolski–Martino–Ventura in [2], to free abelian-by-infinite cyclic groups, and in certain cases apply a polynomial time algorithm for the orbit problem over $\mathbb{Z}^n$ given by Kannan–Lipton in [7].

Societat Catalana de Matemàtiques
Institut d'Estudis Catalans

Keywords: *Conjugacy problem, semidirect product.*
MSC (2010): *20F10, 20E06.*
Received: *September 13, 2014.*
Accepted: *October 6, 2014.*

Acknowledgement
The second author is partially supported by the Office of Naval Research grant N00014120758, the American Association for the Advancement of Science, a PSC-CUNY grant from the CUNY research foundation, as well as the City Tech foundation.

1. Introduction

The conjugacy decision problem in a finitely presented group G, is determining if there is a solution to the equation $v = xux^{-1}$ where $u, v, x \in G$. The decision problem also has the search variant, given u and v conjugate, find an explicit x that conjugates u to v. The conjugacy decision problem is in general undecidable [8], whereas the search problem is decidable in every recursively presented group [9].

Due to the rise of applications of group theory to computer science and cryptography, more research has been directed towards studying the algorithmic complexity of group theoretic algorithms rather than solely investigating decidability. Other polynomial time algorithms for the conjugacy problem in solvable groups are due to Vassileva in free solvable groups [13] and Diekert–Miasnikov–Weiß in solvable Baumslag-Solitar groups [3]. Some very related results can also be seen in the work of Sale [11, 12], in which he shows that for a special class of the groups studied in this paper, the conjugacy length function is bounded from above by a linear function. Namely, for any two conjugate elements in these groups, there exists a conjugator of geodesic length less than a constant multiple of the sum of the geodesic lengths of the elements.

In the following sections we introduce a polynomial time algorithm that solves both the conjugacy decision and search problems in free abelian-by-infinite cyclic groups, where elements are given in terms of their normal forms. This family of groups is polycyclic so it is well known that they have a solvable conjugacy problem. This fact is due originally to Formanek [6] and Remesslennikov [10], who independently proved that virtually polycyclic groups are conjugacy separable: for any two $u, v \in G$ that are not conjugate, there exists a finite homomorphic image in which the images of u and v are not conjugate. Conjugacy can be solved in such groups by conjugating u by elements of G and checking if the result is v, while simultaneously enumerating all homomorphisms from G into a finite group and checking if the images of u and v are conjugate. One of the processes is guaranteed to stop which then provides an answer to the problem. This algorithm is brute force and clearly may take very long even in simple cases.

We start the paper with a review of free abelian-by-infinite cyclic groups and the twisted conjugacy problem. We then detail the algorithm due to Bogopolski–Martino–Maslakova–Ventura from [1] and prove that it, along with the solution to the orbit problem due to Kannan–Lipton [7], solves both the conjugacy decision and search problems in polynomially many steps with respect to the lengths of the inputs in normal form. Finally we end with a complexity analysis of the algorithm and discuss how the complexity changes when inputs are considered in their geodesic forms rather than normal forms.

2. Free abelian-by-infinite cyclic groups

We say that a group G is *free abelian-by-cyclic* if G fits into a short exact sequence of the form:

$$1 \to \mathbb{Z}^n \to G \to C \to 1,$$

where C is a cyclic group. If $C \simeq \mathbb{Z}$, then we say G is *free abelian-by-infinite cyclic*. In this case, G splits as $\mathbb{Z}^n \rtimes_\phi \mathbb{Z}$ for some $\phi \in \mathrm{GL}_n(\mathbb{Z})$. Therefore, G has the presentation:

$$\langle g_1, g_2, \dots, g_n, t \mid tg_it^{-1} = \phi(g_i), [g_i, g_j] = 1\rangle,$$

where $1 \le i < j \le n$ and where we view the g_i as the generators of $\mathbb{Z}^n$ and t as the generator of $\mathbb{Z}$. As such, any $g \in G$ can be written as $w_1t^{k_1}w_2t^{k_2}\cdots w_mt^{k_m}$ where each $w_i \in \mathbb{Z}^n$ and $k_i \in \mathbb{Z}$. Applying the relations of the form $tg_it^{-1} = \phi(g_i)$ multiple times, one can move all the t^{k_i} over to the right side of the word, thus representing each element as wt^k where $w \in \mathbb{Z}^n$ and $k \in \mathbb{Z}$. For any $g \in G$ we call such a representative its *normal form*. Multiplication in normal forms can then be carried out as:

$$wt^k \cdot w't^{k'} = w\phi^k(w')t^{k+k'}.$$

Namely, every time we need to move t^k to the right, over a word in $\mathbb{Z}^n$, we can do so at the price of applying ϕ^k. It can additionally be seen (see [4]) that each group element's normal form is unique.

For the remainder of this paper, we will be working entirely with elements in their normal forms and as such assume in the following algorithm that elements are given in their normal form. We also define a length function, $|\cdot|$, over elements of G where if $g =_G wt^k$, then:

$$|g| = |wt^k| = |w|_{\mathbb{Z}^n} + |k|,$$

where $|w|_{\mathbb{Z}^n}$ is the standard geodesic length of $w \in \mathbb{Z}^n$.

3. The twisted conjugacy problem

Definition 3.1. Given a finitely presented group G, an autormorphism $\phi \in \mathrm{Aut}(G)$, and $u, v \in G$ we say u and v are *twisted conjugate* by ϕ if there exists $x \in G$ such that

$$v = xu\phi(x^{-1}).$$

If u and v are twisted conjugate by ϕ we write: $u \sim_\phi v$.

Notice that the standard conjugacy problem is a special case of the twisted conjugacy problem by taking ϕ to be the identity.

In [1] Bogopolski–Martino–Maslakova–Ventura introduced an algorithm that relates the conjugacy problem in free-by-infinite cyclic groups to the twisted conjugacy problem in free groups. Following that work, Bogopolski–Martino–Ventura [2] adapted the algorithm from [1] to solve the conjugacy problem in a variety of groups created by extensions. What follows is an adaptation of their algorithm for free abelian-by-cyclic groups.

4. The algorithm

The following lemma and proof is taken directly from the beginning of section 2 in [1] and adapted to free abelian-by-infinite cyclic groups.

Lemma 4.1. *Let $u = wt^s$ and $v = xt^r$ in $\mathbb{Z}^n \rtimes_\phi \mathbb{Z}$ be conjugate. Then $s = r$ and there exists $e \in \mathbb{Z}$ such that $\phi^e(w) \sim_{\phi^s} x$ in $\mathbb{Z}^n$. Additionally, if $\phi^s = \phi^r$ is the identity, then $x = \phi^e(w)$ for some $e \in \mathbb{Z}$.*

Proof. Let $a = bt^e \in \mathbb{Z}^n \rtimes_\phi \mathbb{Z}$ be such that $v = aua^{-1}$. Therefore,

$$xt^r = (bt^e)wt^s(bt^e)^{-1} = bt^e wt^s t^{-e} b^{-1} = b\phi^e(w)t^s b^{-1} = b\phi^e(w)\phi^s(b^{-1})t^s.$$

As such, we have $xt^r = b\phi^e(w)\phi^s(b^{-1})t^s$, which implies $s = r$ and $\phi^e(w) \sim_{\phi^s} x$ by b. □

Given u and v as above, the lemma shows that there are two cases one must consider to solve the conjugacy decision and search problems in $\mathbb{Z}^n$-by-$\mathbb{Z}$ groups. First, check if $s = r$. If not, then u and v are not conjugate. If the exponents are the same, then there are two cases:

- If ϕ^s is trivial, we have to decide whether $\exists e \in \mathbb{Z}$ such that $x = \phi^e(w)$.
- Otherwise, we have to decide if there exists e such that $\phi^e(w) \sim_{\phi^s} x$.

The first case, namely given two vectors $w, x \in \mathbb{Z}^n$ and $\phi \in \mathrm{GL}_n(\mathbb{Z})$ determine if there exists $e \in \mathbb{Z}$ such that $x = \phi^e(w)$, is known as the orbit problem over $\mathbb{Z}^n$. In [7], Kannan–Lipton provide a polynomial time algorithm that solves the orbit problem over $\mathbb{Q}^n$. Since the orbit problem over $\mathbb{Z}^n$ is a special case of their work, this algorithm provides a polynomial time solution to the twisted conjugacy problem over $\mathbb{Z}^n$ in the case that ϕ^s is trivial. If such an e is found satisfying the orbit problem, then we have that $v = t^e u t^{-e}$.

For the second case, we use the fact from the lemma that $\exists b \in \mathbb{Z}^n$, $e \in \mathbb{Z}$ such that $x = b\phi^e(w)\phi^s(b^{-1})$. Before we begin the algorithm, we state [1, Lemma 1.7].

Lemma 4.2. *For any group G, $\phi \in \mathrm{Aut}(G)$, and $u \in G$, $u \sim_\phi \phi(u)$.*

Proof. $\phi(u) = u^{-1}u\phi(u)$. Therefore u is twisted conjugate over ϕ to $\phi(u)$, by u^{-1}. □

As such, $\phi^e(w) \sim_{\phi^s} \phi^{e \pm ks}(w)$ for any $k \in \mathbb{Z}$. Therefore, if there exists an e that satisfies the equation $\phi^e(w) \sim_{\phi^s} x$, then we can find such an e among $\{0, 1, \dots, |s| - 1\}$. This is where it is important that we are in the second case and so, $s \neq 0$.

We can now proceed with the full algorithm. Due to the fact that $x, w \in \mathbb{Z}^n$ and $\phi \in \mathrm{GL}_n(\mathbb{Z})$ it is more convenient to put the equation $x = b\phi^e(w)\phi^s(b^{-1})$ into additive notation. As such we write $x = b + \phi^e(w) - \phi^s(b)$. This gives the equation

$$x - \phi^e(w) = (\mathrm{Id}_n - \phi^s)b,$$

where Id_n is the $n \times n$ identity matrix. In this way, each e yields a system of linear equations, which we solve for the vector b. There will be a solution to the conjugacy problem, as long as there is some e for which the solution b is in $\mathbb{Z}^n$. Moreover, we know that if there is a solution to the conjugacy problem, such an e must lie in the set $\{0, 1, \dots, |s| - 1\}$. If there exists such an e, $u \sim v$ and bt^e is a conjugator. As such, we proceed by solving the system of linear equations given by each of the possible e's and then checking if the solution, b, is in $\mathbb{Z}^n$. In the case that $\mathrm{Id}_n - \phi^s$ is invertible, namely, ϕ^s does not have 1 as an eigenvalue, then we can also write:

$$b = (\mathrm{Id}_n - \phi^s)^{-1}(x - \phi^e(w)).$$

For a complete description of the algorithm in pseudo-code on inputs $wt^s, xt^r \in \mathbb{Z}^n \rtimes_\phi \mathbb{Z}$, see Algorithm 1. We have the algorithm return **FALSE** if the elements are not conjugate, and a conjugating element if they are.

5. Complexity analysis

In the algorithm above we have two cases each of which can be dealt with in polynomially many steps with respect to n and $|s|$. If $s = r \neq 0$, we find solutions of an $n \times n$ linear system at most $|s|$ times. On the

Algorithm 1 Conjugacy Algorithm for $\mathbb{Z}^n \rtimes_\phi \mathbb{Z}$

```
if s ≠ r then
    return FALSE
else if φ^s is the identity then
    Run Kannan-Lipton algorithm.
    if Kannan-Lipton returns k then
        return t^k
    else return FALSE
    end if
else
    e := 0
    while e < |s| do
        if ∃b ∈ Z^n such that x − φ^e(w) = (Id_n − φ^s)b then
            return bt^e
        else e := e + 1
        end if
    end while
    return FALSE
end if
```

other hand, if $s = r = 0$, we use Kannan–Lipton algorithm, which runs in polynomial time. Therefore, this algorithm is at most polynomial in terms of n and the lengths of the input words.

It is worth pointing out that unlike many of the algorithms group theorists study, this algorithm takes as inputs words in their polycyclic normal forms as opposed to in their geodesic form or just in any general form. This affects the complexity of the algorithm as all forms have different lengths. It is worth noting that the geodesic form of a word in a polycyclic group can be logarithmic with respect to the length in normal form. For instance in the group:

$$G = \mathbb{Z}^2 \rtimes_\phi \mathbb{Z} = \langle g_1, g_2, t \mid [g_1, g_2], tg_1t^{-1} = g_1^2 g_2, tg_2t^{-1} = g_1 g_2 \rangle,$$

where $\phi(t) = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, we have that:

$$t^n abt^{-n} = a^{F(2n+2)} b^{F(2n+1)},$$

where $F(n)$ is the n-th element of the Fibonacci sequence $F = \{1, 1, 2, 3, 5, ...\}$. In this way, normal forms in G can be exponentially longer than their geodesic forms. As such, collecting words in geodesic form and then performing the algorithm would take an exponential number of steps with respect to the geodesic length since the process of collecting involves writing out a word that is exponentially longer than the original word. On the other hand, in a practical setting, converting words to normal forms is fast (see [5]) and the main complexity involved in the algorithm has to do with the exponent above the generator t after collection, which is just the sum of the exponents above the t's in a general word. As such, after collection, the exponent above t contributes to the length of the word at most what it contributed prior to collection. In that vein, even though a word may grow in size exponentially after collection, most of the additional steps are involved in collection rather than in actually solving the conjugacy problem.

Acknowledgements. We would like to thank the Universitat Politècnica de Catalunya where much of this research was conducted and our host Enric Ventura. Finally, we would like to thank the referee for his/her comments.

References

[1] O Bogopolski, A Martino, O Maslakova, and E Ventura. The conjugacy problem is solvable in free-by-cyclic groups. *Bulletin of the London Mathematical Society*, 38(05):787–794, 2006.

[2] Oleg Bogopolski, Armando Martino, and Enric Ventura. Orbit decidability and the conjugacy problem for some extensions of groups. *Transactions of the American Mathematical Society*, 362(4):2003–2036, 2010.

[3] Volker Diekert, Alexei Miasnikov, and Armin Weiß. Conjugacy in baumslag's group, generic case complexity, and division in power circuits. *arXiv preprint arXiv:1309.5314*, 2013.

[4] B. Eick. *Algorithms for Polycyclic Groups*. Habilitationsschrift, Universitat Kassel, 2001.

[5] Bettina Eick and Delaram Kahrobaei. Polycyclic groups: A new platform for cryptology? *arXiv preprint math/0411077*, 2004.

[6] Edward Formanek. Conjugate separability in polycyclic groups. *Journal of Algebra*, 42(1):1–10, 1976.

[7] Ravindran Kannan and Richard J Lipton. Polynomial-time algorithm for the orbit problem. *Journal of the ACM (JACM)*, 33(4):808–821, 1986.

[8] Charles F Miller III. Decision problems for groups, survey and reflections. In *Algorithms and classification in combinatorial group theory*, pages 1–59. Springer, 1992.

[9] Alexei Myasnikov, Vladimir Shpilrain, and Alexander Ushakov. *Group-based Cryptography*. Springer, 2008.

[10] Vladimir N Remeslennikov. Conjugacy in polycyclic groups. *Algebra and Logic*, 8(6):404–411, 1969.

[11] Andrew W Sale. Short conjugators in solvable groups. *arXiv preprint arXiv:1112.2721*, 2011.

[12] Andrew W Sale. Conjugacy length in group extensions. *arXiv preprint arXiv:1211.3144*, 2012.

[13] Svetla Vassileva. Polynomial time conjugacy in wreath products and free solvable groups. *Groups, Complexity, Cryptology*, 3(1):105–120, 2011.

Reports@SCM
Volume 1, number 1, 2014

Table of Contents