

# ENGINY

REVISTA DE LA ESCOLA POLITÈCNICA SUPERIOR. ISSN: 1889-4771

ENGINY recull els millors treballs docents i de recerca que durant el curs s'han realitzat a les titulacions de les branques d'Enginyeria i Matemàtiques

**SECCIÓ OBERTA:** Les probabilitats als Jutjats /  
Edificis que amaguen històries. Càtedra Sampol /  
Càtedra Endesa. **TREBALLS DOCENTS /**  
**TREBALLS DE RECERCA**

3

ANY 2011  
CURS  
2010/11

# EDITORIAL

## **BARTOMEU ALORDA**

Grup de Sistemes Electrònics  
Departament de Física  
Universitat de les Illes Balears

Una vegada més la bona feina feta dins les aules de l'escola politècnica Superior veu la llum amb una nova edició de la revista *enginy@eps*. A partir d'aquest número la revista s'editarà només en la seva edició digital per donar lloc a una nova versió en paper que s'anomenarà **ENGINY**. L'objectiu d'aquest canvi és el de promocionar l'espai divulgatiu de la revista fora de la Universitat de les Illes Balears i així convertir-se en un mitjà de difusió de les bones pràctiques dels futurs titulats que passarà a ser gestionada des del servei d'Edicions UIB.

L'objectiu de les dues revistes serà el mateix i és basarà en un esperit divulgador de la tasca que dia a dia es realitza a dins les aules tant per part dels alumnes com dels professors. Donar a conèixer els millors treballs permet ajudar als futurs estudiants a millorar-se contínuament, és un repte pels estudiants actuals, i una eina docent excel·lent pels professors per a mantenir la motivació envers les activitats docents que es planifiquen a dins les assignatures. La principal diferència entre les dues revistes consistirà en que l'edició digital *enginy@eps* mantindrà la dinàmica actual de donar a conèixer els millors treballs realitzats dins l'Escola Politècnica Superior i així ajudar a millorar la motivació envers les titulacions de l'escola i la qualitat de les activitats educatives que sí desenvolupen. Mentre que l'edició en paper **ENGINY** perseguirà una segona revisió dels treballs publicats a la versió digital amb unes fites de qualitat majors i obrirà la possibilitat de que altres universitats o escoles politècniques puguin participar d'aquest nou espai. Així doncs, aquest serà el darrer número de l'edició en paper de la revista *enginy@eps* que passarà a ser exclusivament una versió en digital i donarà lloc a la nova revista **ENGINY** ambdues acollides dins el catàleg de revistes del servei d'Edicions UIB.

Voldria aprofitar aquesta fita dins la història de la revista *enginy@eps* per agrair a totes les persones que van donar el seu suport, dedicant-hi hores de revisió i creant propostes publicables per donar vida a la revista. Voldria també convidar a continuar fent-ho per a mantenir l'espai divulgatiu que ha creat *enginy@eps* i que ha esdevingut tant important per l'escola. Voldria agrair especialment als col·laboradors de la revista per les seves aportacions econòmiques que han possibilitat editar en paper fins a quatre números consecutius, esperant continuar contant amb el seu suport en aquesta nova etapa. Moltes gràcies a tots i continuem el camí plegats.

Aquest número proposa a la secció de Treballs Docents un total de 9 memòries d'activitats docents proposades a diverses assignatures. Aquests treballs han servit per avaluar als seus autors i, finalment, han estat seleccionats pel professor de cada assignatura per a la seva publicació a la revista. També a la secció de Recerca-Divulgació es recull un total de 5 excel·lents propostes entre treballs de divulgació de professors i projectes final de carrera.

De nou encoratjo a la comunitat universitària a participar en la propera edició de la revista *enginy@eps* per a continuar gaudint d'aquest saludable exercici de divulgació i exposició pública de les tasques docents i de recerca.

# LES PROBABILITATS EN ELS JUTJATS. EL CAS DEL POBLE CONTRA ELS COLLINS.

JAUME SUÑER

La història de la humanitat és plena d'exemples curiosos on s'ha aplicat el càlcul de probabilitats de manera més o menys acurada. La publicitat enganyosa n'és un bon exemple: si ens diuen que 9 de cada 10 estrelles de cinema utilitzen un determinat sabó, tendim a pensar que si utilitzam aquest sabó, serem com estrelles de cinema; és a dir, que la probabilitat condicionada d'esser estrella de cinema, sabent que feim servir aquest tipus de sabó, val 9/10:  $p(\text{estrella de cinema} / \text{sabó}) = 9/10$ .

En canvi, el que diu l'anunci és que, suposant que som una estrella de cinema, la probabilitat d'usar aquest sabó és 9/10:  $p(\text{sabó} / \text{estrella de cinema}) = 9/10$ . Per tant, del fet d'utilitzar aquesta marca de sabó determinada, no en treim cap informació del nostre futur com a grans artistes. Un exemple més exagerat seria un anunci de l'estil: 9 de cada 10 dentistes consultats han recomanat aquesta pasta de dents concreta. I els que no han estat consultats, hi estarien d'acord? I com han triat els dentistes que han consultat?

En aquest escrit, parlaré d'un altre exemple de mal ús del càlcul de probabilitats, en aquest cas corresponent a un judici real, la causa judicial del Poble contra els Collins, celebrada a Califòrnia els anys seixanta. Vegem-ne els detalls.

Dia 18 de juny de 1964, una dona gran anava passejant per un carrer de l'àrea de San Pedro, a Los Angeles. Arrossegava un carro amb la compra, caminava amb l'ajut d'un bastó i, de cop, li varen envestir i va caure en terra. Quan va aconseguir aixecar-se, va comprovar que li havien pres la cartera, i va veure una dona jove que fugia corrents. La dona jove va ser descrita amb cabells rossos formant una cua i duguent quelcom negre. Un altre testimoni va veure que una dona amb aquesta descripció pujava a un cotxe groc conduït per un afroamericà amb barba i mostatxo. En resum, es varen establir sis característiques referents als criminals:

*A:* fugen en un automòbil parcialment groc

*B:* home amb mostatxo

*C:* dona amb coa de cavall

*D:* dona amb cabells rossos

*E:* afroamericà amb barba

*F:* parella interracial en cotxe

El matrimoni Collins satisfieia aquestes característiques, i el testimoni abans esmentat el va triar a ell en una roda de reconeixement, encara que amb certs dubtes perquè no duia barba. Així, després de diversos interrogatoris, els Collins varen ser acusats de l'atracament i, finalment, es va celebrar el judici.

Un moment donat, per reforçar la identificació dels culpables, el fiscal va cridar com a testimoni un expert en probabilitats, qui explicà al jurat la propietat del producte: si una col·lecció de successos són independents, aleshores la probabilitat de l'ocurrència simultània de tots els successos és el producte de les probabilitats individuals de cada succés.



Per tant, la probabilitat que passi l'anterior en una parella qualsevol de les  $N$  és

$$p(N_S = 1) = N \cdot p \cdot (1 - p)^{N-1}$$

Ara, la probabilitat que estrictament més d'una parella satisfaci les sis característiques  $A - F$  és

$$p(N_S > 1) = p(N_S \geq 1) - p(N_S = 1)$$

és a dir,

$$p(N_S > 1) = 1 - (1 - p)^N - N \cdot p \cdot (1 - p)^{N-1}$$

Finalment, sabent que com a mínim una parella satisfà  $A - F$ , la probabilitat que més d'una ho satisfaci és

$$p(N_S > 1 / N_S \geq 1) = \frac{p(N_S > 1, N_S \geq 1)}{p(N_S \geq 1)} = \frac{p(N_S > 1)}{p(N_S \geq 1)}$$

i, afegint les probabilitats calculades anteriorment, obtenim

$$p(N_S > 1 / N_S \geq 1) = \frac{1 - (1 - p)^N - N \cdot p \cdot (1 - p)^{N-1}}{1 - (1 - p)^N}$$

Si ara agafam les dades de l'acusació, és a dir,  $p = \frac{1}{12 \cdot 10^6}$ , obtenim una probabilitat

$$p(N_S > 1 / N_S \geq 1) = \frac{1 - (1 - \frac{1}{12 \cdot 10^6})^N - N \cdot \frac{1}{12 \cdot 10^6} \cdot (1 - \frac{1}{12 \cdot 10^6})^{N-1}}{1 - (1 - \frac{1}{12 \cdot 10^6})^N}$$

El problema aquí rau en com determinar  $N$ , el nombre total de parelles que poden haver estat vistes al lloc del robatori de San Pedro. Per cert que l'advocat va aprofitar aquest fet per deixar palesa una altra dificultat en l'ús de la teoria de les probabilitats per establir la identitat dels autors del crim. De totes formes, podem suposar que  $N$  és molt gran, que fàcilment superarà varis milions. De fet, si agafam  $N = 12 \cdot 10^6$ , resulta una probabilitat superior a 0.41.

En general, si agafam  $p = \frac{1}{N}$ , tenim

$$p(N_S > 1 / N_S \geq 1) = \frac{1 - (1 - 1/N)^N - (1 - 1/N)^{N-1}}{1 - (1 - 1/N)^N}$$

i, si feim tendir  $N$  cap a infinit, resulta un límit

$$\lim_{N \rightarrow \infty} p(N_S > 1 / N_S \geq 1) = \frac{1 - e^{-1} - e^{-1}}{1 - e^{-1}} = \frac{e - 2}{e - 1} \approx 0.418$$

Aquest fet va conduir al tribunal a acceptar el recurs presentat, de manera que els Collins varen ser posats en llibertat.

Per acabar, fem un petit comentari a aquest cas; deixant de banda el fet que la probabilitat  $\frac{1}{12 \cdot 10^6}$  fos obtinguda de manera errònia (es va considerar independència on no n'hi havia), el raonament del fiscal en el judici és un exemple del que es coneix com fal·làcia de l'acusador. En aquest cas, l'error és confondre la probabilitat ( $\frac{1}{12 \cdot 10^6}$ ) que una parella satisfaci les sis característiques  $A - F$  amb la probabilitat que la parella acusada, que les satisfà, sigui innocent. I és que, com hem vist abans, la probabilitat que com a mínim una parella satisfaci les sis característiques, dins d'un grup de  $N$  parelles, val  $p(N_S \geq 1) = 1 - (1 - \frac{1}{12 \cdot 10^6})^N$ , que per a  $N = 12 \cdot 10^6$  és de l'ordre de 0.63. I aquest valor és independent del fet que entre les  $N$  parelles hi hagi o no els vertaders culpables. Aquesta fal·làcia ha estat comesa més d'una vegada en la identificació dels culpables de delictes, generalment per error, ja que un ús deliberat podria conduir a sancions.



Per tant, la probabilitat que passi l'anterior en una parella qualsevol de les  $N$  és

$$p(N_S = 1) = N \cdot p \cdot (1 - p)^{N-1}$$

Ara, la probabilitat que estrictament més d'una parella satisfaci les sis característiques  $A - F$  és

$$p(N_S > 1) = p(N_S \geq 1) - p(N_S = 1)$$

és a dir,

$$p(N_S > 1) = 1 - (1 - p)^N - N \cdot p \cdot (1 - p)^{N-1}$$

Finalment, sabent que com a mínim una parella satisfà  $A - F$ , la probabilitat que més d'una ho satisfaci és

$$p(N_S > 1 / N_S \geq 1) = \frac{p(N_S > 1, N_S \geq 1)}{p(N_S \geq 1)} = \frac{p(N_S > 1)}{p(N_S \geq 1)}$$

i, afegint les probabilitats calculades anteriorment, obtenim

$$p(N_S > 1 / N_S \geq 1) = \frac{1 - (1 - p)^N - N \cdot p \cdot (1 - p)^{N-1}}{1 - (1 - p)^N}$$

Si ara agafam les dades de l'acusació, és a dir,  $p = \frac{1}{12 \cdot 10^6}$ , obtenim una probabilitat

$$p(N_S > 1 / N_S \geq 1) = \frac{1 - (1 - \frac{1}{12 \cdot 10^6})^N - N \cdot \frac{1}{12 \cdot 10^6} \cdot (1 - \frac{1}{12 \cdot 10^6})^{N-1}}{1 - (1 - \frac{1}{12 \cdot 10^6})^N}$$

El problema aquí rau en com determinar  $N$ , el nombre total de parelles que poden haver estat vistes al lloc del robatori de San Pedro. Per cert que l'advocat va aprofitar aquest fet per deixar palesa una altra dificultat en l'ús de la teoria de les probabilitats per establir la identitat dels autors del crim. De totes formes, podem suposar que  $N$  és molt gran, que fàcilment superarà varis milions. De fet, si agafam  $N = 12 \cdot 10^6$ , resulta una probabilitat superior a 0.41.

En general, si agafam  $p = \frac{1}{N}$ , tenim

$$p(N_S > 1 / N_S \geq 1) = \frac{1 - (1 - 1/N)^N - (1 - 1/N)^{N-1}}{1 - (1 - 1/N)^N}$$

i, si feim tendir  $N$  cap a infinit, resulta un límit

$$\lim_{N \rightarrow \infty} p(N_S > 1 / N_S \geq 1) = \frac{1 - e^{-1} - e^{-1}}{1 - e^{-1}} = \frac{e - 2}{e - 1} \approx 0.418$$

Aquest fet va conduir al tribunal a acceptar el recurs presentat, de manera que els Collins varen ser posats en llibertat.

Per acabar, fem un petit comentari a aquest cas; deixant de banda el fet que la probabilitat  $\frac{1}{12 \cdot 10^6}$  fos obtinguda de manera errònia (es va considerar independència on no n'hi havia), el raonament del fiscal en el judici és un exemple del que es coneix com fal·làcia de l'acusador. En aquest cas, l'error és confondre la probabilitat ( $\frac{1}{12 \cdot 10^6}$ ) que una parella satisfaci les sis característiques  $A - F$  amb la probabilitat que la parella acusada, que les satisfà, sigui innocent. I és que, com hem vist abans, la probabilitat que com a mínim una parella satisfaci les sis característiques, dins d'un grup de  $N$  parelles, val  $p(N_S \geq 1) = 1 - (1 - \frac{1}{12 \cdot 10^6})^N$ , que per a  $N = 12 \cdot 10^6$  és de l'ordre de 0.63. I aquest valor és independent del fet que entre les  $N$  parelles hi hagi o no els vertaders culpables. Aquesta fal·làcia ha estat comesa més d'una vegada en la identificació dels culpables de delictes, generalment per error, ja que un ús deliberat podria conduir a sancions.

#### BIBLIOGRAFIA

David A. Sklansky: Evidence: Cases, Commentary, and Problems. WoltersKluwer, Aspen Publishers, 2008.

# EDIFICIS QUE AMAGUEN HISTÒRIES

**MATEO MOYÀ**

Col·legi Oficial d'Aparelladors, Arquitectes Tècnics i Enginyers d'Edificació

**D**e vegades, la intervenció en un edifici antic, encara que no tingui especial rellevància arquitectònica, et permet descobrir petites joies constructives o fins i tot, com em va ocórrer en el transcurs d'una ITE, trossos d'històries desconegudes per la majoria i que, possiblement així romanguin.

Un company de pis de la meua època d'estudiant em va demanar que revisés l'edifici en el qual viu a l'efecte de fer les reparacions oportunes abans de realitzar la ITE. Es tracta d'un edifici antic de diverses plantes que va construir el seu avi i que, en l'actualitat té ocupats els diferents habitatges per descendents membres de la família.

Quan em vaig interessar per l'estat de les bigues de coberta que són les que solen estar en mal estat en aquests casos, em van comentar orgullosos que per això no em preocupés; que eren bigues de fusta de la millor qualitat possible i que estaven en perfecte estat ja que el seu avi havia comprat la fusta del vaixell NIXE que va pertànyer a l'Arxiduc Luis Salvador i que es va desballestar a Palma sobre l'any 1925 i amb ella havia confeccionat les bigues de la coberta de l'edifici.

Efectivament així era. Es tractava de bigues d'una fusta d'aspecte molt sa i resistent d'una escuadria d'uns 15x20 cm.

En interessar-me pel tema, em van comentar que quedava una altra "reliquia" del NIXE. Quan es va iniciar la guerra civil, el seu avi va construir un refugi sota l'edifici: una estreta galeria a uns 4 metres de profunditat amb dues entrades. Doncs bé, la corda que serveix de passamans

per baixar l'escala fins al refugi és una de les maromes del NIXE. Cal dir que es troba en perfecte estat. Quant a l'efectivitat del refugi jo crec que hauria estat una tomba perfecta en el cas que l'edifici s'hagués desplomat per l'efecte d'una bomba.

Per tant vaig tenir la sort de veure i tocar les restes d'un vaixell mític, almenys per a Mallorca i trepitjar un refugi de la guerra civil.

Finalment, en el soterrani de l'edifici, que durant molts anys havia estat una fleca de les de "tota la vida" vaig poder veure el que va anar el forn més gran de Mallorca amb una volta de maó d'uns 6 metres de diàmetre i unes pesades portes de fosa.

Això em recorda una altra anècdota que em va ocórrer fa molts anys en visitar una "posseïció" a la qual em van convidar. Evidentment, estava plena de mobles antics que eren una autèntica delícia però, la cosa que em va cridar l'atenció va ser un petit llum d'escriptori d'estil modernista. L'amfitrió, en veure el meu interès, em va començar a explicar-me la història del fet que la mirés bé. Llavors em vaig adonar que tenia una inscripció en el peu del llum. Es tractava d'una dedicatòria que deia més o menys el següent: "Al meu amic xxx, Antonio Gaudí". Es tractava d'un regal que li havia fet Gaudí al seu avi durant la seva estada a Mallorca. Un treball desconegut de Gaudí a Mallorca!

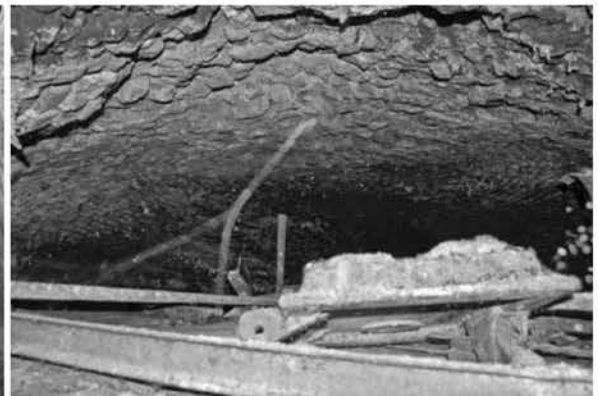
Quantes històries estaran amagades dins dels edificis esperant que algú les expliqui.



Bigues de coberta procedents del NIXE.



Refugi de la guerra civil amb el passamans fet amb una maroma del NIXE.



Interior del major forn de pa de Palma, actualment en desús.

# LA CÀTEDRA ENDESA ES PREOCUPA DE LA PREVENCIÓ DE RISCOS LABORALS

**MIQUEL ROCA ADROVER**

Director Càtedra Endesa Red d'Innovació Energètica de la UIB.

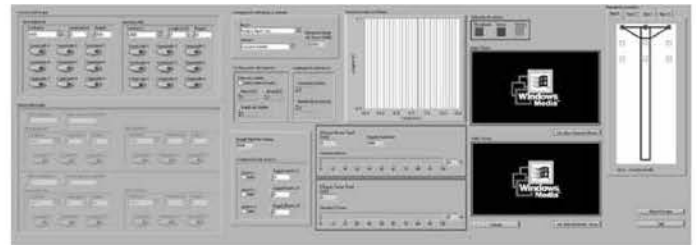
10

La prevenció d'accidents laborals és un repte molt important en qualsevol empresa, en particular en els departaments de recursos humans o departaments de prevenció. La frase, o "eslògan", si és que es pot dir així, "Zero Accidents" "No accidents" als entorns de treball ha passat a ser un objectiu primordial dins de la societat en general i dins de les empreses en particular. L'empresa EndesaRed no està al marge de l'assoliment d'aquests objectius i la seva preocupació per aquests temes és important.

D'aquesta manera, a la Universitat de les Illes Balears dins del marc de la Càtedra EndesaRed que dirigeixo, hem estat treballant en un projecte de recerca dins d'aquesta temàtica. En particular ens hem preocupat per la seguretat laboral dels treballadors que realitzen tasques de reparacions i manteniment de torres de distribució elèctrica de mitja i baixa tensió.

En particular hem treballat en el desenvolupament d'una eina informàtica que, a partir d'una descripció d'una topologia determinada de poste o torre i vans connectats, es capaç de fer una estimació de la perillositat en el treball en altura, dit en altres paraules ens calcula el moment torçor i el moment flexor al qual es veu sotmesa la torre. La comparació d'aquests moments amb els valors màxims que pot suportar el poste ens proporciona el que hem definit com a índex de perillositat.

Per tal d'obtenir els moments abans esmentats, hem definit tot un conjunt de torres o postes que podem trobar a la xarxa de les Illes Balears, juntament amb les seves característiques (tipus de poste i els moments torçors i flexors màxims que pot suportar). Per a la obtenció d'aquests valors llindars fem cas de les especificacions del fabricant, si bé també hem realitzat una tasca experimental de mesura de moments màxims de ruptura a postes de fusta i ciment, de manera que en funció de l'edat i del lloc on es troba localitzat el poste considerar un factor corrector. S'ha comprovat com un poste de fusta de 20 anys emplaçat en un entorn rural suporta més càrrega abans de la ruptura que un poste igual, de la mateixa edat situat en un entorn de ciutat (enterrat en una vorera de ciment), fet que es pot explicar si consideram que la terra dreña millor l'aigua de la pluja que no el ciment.



El programa permet introduir la topologia de vans i postes de manera senzilla, a l'igual que el vent, l'obrer, la part per on puja l'obrer, etc. ... Amb totes aquestes dades, emprant un model simple de masses concentrades es realitza el càlcul del moments abans esmentats i es comparen amb els assignats al poste seleccionat, indicant amb un semàfor el nivell de perillositat (possibilitat de trencament del poste i per tant possible accident de caiguda de l'obrer a la tasca de manteniment o reparació).

L'objectiu del programa es la conscienciació dels obrers de que s'han de prendre totes les mesures estipulades en aquests tipus de treballs. S'està fent una tasca de divulgació, mitjançant la generació d'un vídeo demostratiu i actualment s'està en el procés d'homologació del software dins de l'empresa EndesaRed, per poder ser emprat pels treballadors implicats.

Voldria afegir que aquest projecte s'ha presentat al certamen "Ciència en Acció" dins de l'apartat dedicat a "Electricidad y Sociedad" i ha estat seleccionat com un dels tres finalistes per a la seva presentació a la fase final que s'ha celebrat a Lleida el mes d'octubre de 2011. A la foto ens podeu veure a l'estand que es va muntar al Parc Tecnològic Agroalimentari de Lleida. Malauradament no hem aconseguit aquest guardó, però estam satisfets d'haver pogut participar i quedar finalistes del certamen.



# CÀTEDRA SAMPOL D'EFICIÈNCIA I GESTIÓ ENERGÈTICA

**ANDREU MOIÀ POL I VÍCTOR MARTÍNEZ MOLL**  
Co-Directors de la Càtedra

**S**ampol Ingeniería y Obras S.A és una empresa familiar amb més de 75 anys de història i de capital íntegrament balear, que sota la direcció del seu president Don Gabriel Sampol ha aconseguit comptar actualment amb delegacions i projectes tant en l'àmbit nacional com internacional.

L'activitat de l'empresa es centra al voltant de quatre grans línees de negoci: les infraestructures elèctriques, la generació energètica, l'obra civil i les aplicacions tecnològiques. En totes aquestes àrees l'empresa destaca per la cerca de l'excel·lència en la recerca de l'eficiència energètica.

**La Càtedra Sampol d'eficiència i gestió energètica** es l'evolució natural de la càtedra Sampol inicialment creada l'any 2008 entre *Sampol Ingeniería y Obras S.A* i la *Universitat de les Illes Balears*, que té com objectius: promoure les activitats docents en l'àrea de la gestió energètica i les energies renovables, l'organització i participació en activitats divulgatives de la gestió integral i de l'eficiència energètica, i fonamentalment la realització de tasques de recerca y desenvolupament (I+D) conjunta (*UIB-Sampol Ingeniería y Obras S.A*).

En el marc d'aquestes línees de treball, la càtedra ha realitzat al llarg del curs acadèmic 2010-2011 les següents activitats:

Referent a la docència, l'activitat portada a terme per la càtedra Sampol a consistit en donar suport a les accions formatives de l'assignatura optativa *Energies Renovables (4705)* del programa lectiu d'enginyeria Tècnica Industrial, Especialitat en Electrònica Industrial. Que en el present curs acadèmic l'han cursada 58 estudiants.

En el marc de l'organització i participació en activitats divulgatives de la gestió integral i de l'eficiència energètica, els membres de la Càtedra Sampol han participat en les següents activitats:

Participació a les *Jornades de debat i Reflexió sobre l'Energia, sostenibilitat i impactes*. Organitzada per la direcció General d'Energia. Govern de les Illes Balears. 27-28 de maig de 2010. Comunicació oral.

Participació al programa radiofònic de IB3 Radio "*Al Dia*" del co-director de la càtedra Sr. Andreu Moià Pol, en el marc

d'un programa especial que va versar sobre la implantació del vehicle elèctric a les Illes Balears. Novembre 2010.

Participació en el programa de IB3 Televisió "*El Matí*" del co-director de la càtedra Sr. Andreu Moià Pol, en el marc d'un programa que va versar sobre la implantació del vehicle elèctric a les Illes Balears. Març 2011

Participació en el *1<sup>er</sup> Congrés Canvi Climàtic i Món Local: La Gestió Energètica al Municipi*. Reus, Espanya. Abril 2011. On es va presentar una comunicació oral del treball/projecte "*SmartGrid, cas del Parc Bit i la UIB*"

En el marc de les actuacions conjuntes de recerca i desenvolupament (I+D) que s'han portat a terme de forma conjunta per part dels membres de la càtedra Sampol de la UIB i el membres de la divisió I+D del departament d'Energia de *Sampol Ingeniería y Obras S.A*, cal remarcar-ne les següents per la seva rellevància:

Pel que fa a la recerca en xarxes de districte energètic, s'ha treballat en la realització de les auditories energètiques dels diferents edificis del Campus de la UIB amb l'ajuda de l'equip facultatiu de patrimoni de la *Universitat de les illes Balears*, i l'empresa concessionària del manteniment.

També s'ha treballat en la modificació i promoció del projecte *Smart District* en la seva part d'implantació en la xarxa de districte de la UIB, com a passa prèvia a la participació en futures convocatòries de projectes FP7.

En el que fa referència als sistemes combinats de producció d'energia a partir de l'ús d'energies renovables i la cogeneració, s'han iniciat els estudis preliminars per iniciar una nova línea de recerca conjunta entre els membres de la càtedra Sampol de la UIB i el departament de I+D de *Sampol Ingeniería y Obras S.A*.

Finalment la tasca més important portada a terme al llarg del present curs acadèmic ha versat en la recerca en sistemes de recàrrega de vehicles elèctrics on s'han realitzat, en el marc del projecte *SmartBit*:

Un estudi de l'estat de l'art del sistemes i les tecnologies de recàrrega actualment existents.

Els projectes de desenvolupament y implantació d'un sistema recarrega avançat al Parc Bit (ja implantat) i del Campus de la UIB (en breu es realitzarà la seva implantació).



# LTE-Advanced

Alberto Ballesteros<sup>#1</sup>, Adrián Petit<sup>#2</sup>

<sup>#</sup>Universitat de les Illes Balears

Cra. de Valdemossa km 7.5. Palma (Illes Balears)

<sup>1</sup>ballesteros.alberto@gmail.com

<sup>2</sup>adrian.petit@gmail.com

**Abstract**—En las últimas décadas hemos vivido la expansión y desarrollo de las redes de telefonía móvil, desde los sistemas analógicos, hasta las actuales redes 3G, que permiten el intercambio de datos a grandes velocidades. Este documento explica, de manera general, el contexto y la evolución de la telefonía móvil, para luego centrarse en LTE-Advanced, el estándar de cuarta generación más relevante en la actualidad.

## I. INTRODUCCIÓN

La ITU (Unión Internacional de Telecomunicaciones) es el organismo, creado por la ONU, que se encarga de regular las telecomunicaciones a nivel internacional. Una de sus secciones, la ITU-R, es la responsable de las comunicaciones radioeléctricas. Principalmente, gestiona el espectro de frecuencias radioeléctricas y las órbitas de los satélites. De la misma manera, es el organismo encargado de especificar las características de las diferentes generaciones de telefonía móvil.

En base a estas especificaciones, se definen diferentes estándares de telecomunicación. Una de las entidades encargadas de ello es el 3GPP (3<sup>rd</sup> Generation Partnership Project). Se trata de un consorcio de varios organismos internacionales, que tiene como objetivo unificar criterios en materia de telefonía móvil. Lo forman: ETSI (Europa), ARIB/TTC (Japón), CCSA (China), ATIS (América del Norte) y TTA (Corea del Sur). Este acuerdo de colaboración ha definido varias de las tecnologías de telefonía móvil más extendidas en el mundo, algunas de las más conocidas son: GSM, GPRS o UMTS. En la tabla I se muestran las generaciones de telefonía móvil, las entidades creadoras y sus diferentes tecnologías [9].

TABLA I

EVOLUCIÓN DE LA TELEFONÍA MÓVIL

Generación	Organización	Tecnología
2G	GSM/3GPP	<b>GSM</b>
	3GPP2	CdmaOne
	AMPS	D-AMPS
2G Transición	GSM/3GPP	<b>GPRS</b> , EDGE/EGPRS
	3GPP2	CDMA2000
3G	3GPP	<b>UMTS</b>
	3GPP2	EV-DO
3G Transición	3GPP	HSDPA, <b>LTE</b>
	3GPP2	EV-DO
4G	3GPP	<b>LTE Advanced</b>
	WiMAX	IEEE 802.16m

Actualmente, en España, las tecnologías más usadas son GSM (2G) y UMTS (3G). La primera se usa para voz, ya que es un estándar muy robusto y barato, tecnológicamente. La segunda se utiliza, además, para datos, pero a diferencia de GSM, tiene unos requerimientos de calidad de señal elevados y un gasto energético mayor.

Con el rápido crecimiento del número de terminales móviles, es necesario contar con estándares capaces de proporcionar grandes velocidades de transmisión, a un número mayor de usuarios y con un coste tecnológico reducido. Bajo estas directrices, la ITU-R define las características que debe cumplir un estándar para auto-denominarse 4G.

En ese momento varios organismos empiezan a trabajar en nuevos estándares para esta generación. 3GPP ha desarrollado LTE a partir de UMTS, y aunque dispone de características muy avanzadas, no alcanza todos los requisitos 4G. Por esta razón se le considera 3.9G o pre-4G.

LTE-Advanced (LTE-A) surge como una evolución de LTE y pretende ser el estándar global válido para 4G, ya que cumple sobradamente los requerimientos mínimos impuestos por la ITU-R. Sin embargo, no se puede considerar, actualmente, un estándar válido, ya que todavía se encuentra en fase de desarrollo.

En este documento, primero, se explica el impacto que van a tener las tecnologías de cuarta generación, para luego introducir LTE. Finalmente se pondrán de manifiesto las principales características que convierten a LTE-A en el estándar 4G más importante, en la actualidad. Después de las conclusiones se definen varios conceptos básicos para facilitar la comprensión del presente artículo.

## II. DE 3G A 4G

Esta nueva generación pretende ser un nuevo paso en las telecomunicaciones hacia la movilidad y accesibilidad universal. Para superar a 3G, 4G incorpora las siguientes características:

- Unificación de las distintas tecnologías de red bajo el protocolo IP.
- Velocidades de descarga desde los 100 Mbps hasta los 1 Gbps, dependiendo de la velocidad a la que se desplace el terminal.
- Asignación dinámica de recursos de red, para conseguir un mayor número de usuarios por celda.
- Plena compatibilidad con los estándares actuales, lo que incluye *handover*.
- Servicios en red de alta velocidad como: vozIP, juegos en línea o streaming de video.

Todo esto plantea una serie de retos técnicos difíciles de superar. Sin embargo, en los últimos años se han hecho grandes avances, en varios frentes, que propician el cambio a esta nueva generación. Por ejemplo, en el canal radio, el multiplexado OFDMA y los esquemas MIMO.

### III. LTE

Este estándar de telefonía móvil fue creado a partir de UMTS (3G), y pretendía ser el primer estándar válido para 4G. Sin embargo, aunque implementa la mayoría de requisitos de 4G, no los cumple todos. Por ejemplo, no consigue la velocidad de bajada de 1 Gbps. Por lo tanto, es un estándar entre dos generaciones (3.9G). Sus principales características son:

- Velocidades de 300 Mb/s de bajada y 75 Mb/s de subida.
- Ancho de banda regulable de hasta 20 MHz.
- Multiplexado OFDMA para el canal de bajada y SC-FDMA para el canal de subida.
- Tamaños de celda de 5 a 100 km, dependiendo del número de usuarios y la velocidad de transmisión.
- El *handover* con las tecnologías actuales, 2G y 3G, se realiza de manera transparente
- Posibilidad de usar técnicas MIMO.

Uno de los pilares de las tecnologías de telefonía móvil es la manera en que los datos son transmitidos al medio. LTE utiliza OFDMA, un tipo de multiplexado por frecuencia que permite aprovechar al máximo el ancho de banda disponible.

#### A. OFDMA: Orthogonal Frequency Division Multiple Access

Esta tecnología divide el ancho de banda en múltiples bandas de frecuencia equiespaciadas. Cada banda tiene una sub-portadora que transporta una porción de la información. Cada una de estas sub-portadoras es ortogonal al resto, con lo que se consigue que, aunque estén traslapadas, como se observa en la figura 1, no exista interferencia entre ellas.

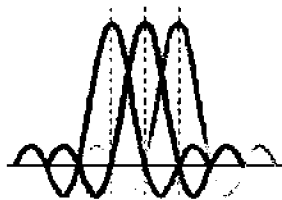


Fig. 1 Sub-portadoras ortogonales

El flujo de datos se divide en N (el número de sub-portadoras asignadas) flujos paralelos que transmiten a una tasa N veces menor. De esta manera, se consigue transmitir a la misma velocidad, pero con flujos de información más lentos, lo que hace más improbable que se produzcan errores de transmisión. Cuanto mayor es el número de sub-portadoras del que dispone un usuario, mayor es la velocidad o la calidad de la transmisión.

El hecho de poder asignar fácilmente sub-portadoras a los usuarios, permite repartir el ancho de banda de manera óptima, consiguiendo una buena relación velocidad/calidad de transmisión, global.

#### B. MIMO

Multiple-Input Multiple-Output engloba todas aquellas técnicas de procesamiento de señal que utilizan varias antenas en el receptor y/o en el transmisor. Estas técnicas permiten aprovechar los diferentes flujos de datos que aparecen, debido al efecto multi-camino. La figura 2 muestra una comunicación con dos antenas en el nodo transmisor y dos en el nodo receptor. Las flechas que aparecen entre estas, simulan los diferentes caminos que toma la información.

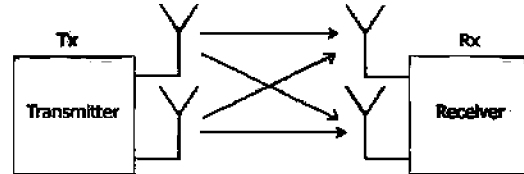


Fig. 2 Esquema de transmisión MIMO 2x2

La principal ventaja de utilizar MIMO es que aumenta el rendimiento y la fiabilidad sin necesidad de incrementar el ancho de banda o la potencia de transmisión.

En LTE se permite esquema de transmisión MIMO de hasta 4 antenas en el transmisor y 4 en el receptor.

### IV. LTE-ADVANCED

LTE-Advanced es una ampliación de LTE, es por ello que posee todas sus características, además de varias mejoras. Las principales novedades que incluye este estándar respecto a su versión anterior son:

- Mayor velocidad: 1 Gb/s de bajada y 500 Mb/s de subida.
- Mayor ancho de banda para transmitir datos.
- Mejor cobertura y/o rendimiento con la transmisión multipunto coordinada.
- Aumento del rendimiento gracias a la tecnología MIMO.

Como se ha comentado, la ITU-R establece las características para que un protocolo pueda autodenominarse 4G. En concreto, establece varios requerimientos de eficiencia y capacidad. La tabla II resume estos requerimientos así como los valores obtenidos de LTE y LTE-A [1-3]. Es fácil ver que LTE no cumple la mayoría de ellos. Sin embargo, LTE-A no solo iguala sino que supera con creces los valores mínimos requeridos.

Son 4 los pilares sobre los que se apoya LTE-A para superar a su predecesor y colocarse en la cabeza de las tecnologías 4G. Para poder obtener una tasa de transmisión de 1 Gbps, se implementa agregado de portadora, que permite aumentar el ancho de banda hasta los 100 MHz. Para mejorar la eficiencia espectral se estudian optimizaciones de las técnicas MIMO. Debido a la reutilización de frecuencias, LTE sufre una gran interferencia inter-celda. Para mitigar este efecto, y así aumentar el rendimiento, se adopta la técnica de transmisión/recepción coordinada multipunto. Finalmente, la posibilidad de poder desplegar nodos de comunicación, dentro de las celdas, permite extender la cobertura y/o aumentar el rendimiento en zonas determinadas.

TABLA II

REQUISITOS PARA 4G Y COMPARATIVA ENTRE LTE Y LTE-A

	DL/ UL	Conf. antena	LTE	LTE-A	Req. 4G
Tasa trans.	DL	-	300 Mbps	1 Gbps	1 Gbps
	UL	-	75 Mbps	500 Mbps	500 Mbps
Eficiencia espectral [bps/Hz/celda]	DL	-	15	30	15
	UL	-	3,75	15	6,75
Capacidad [bps/Hz/celda]	DL	2x2	1,69	2,4	-
		4x2	1,87	2,6	2,2 <sup>(*)</sup>
		4x4	2,67	3,7	-
	UL	1x2	0,74	1,2	-
		2x4	-	2	1,4 <sup>(*)</sup>

<sup>(\*)</sup> Valores requeridos para entornos urbanos

A. Agregado de portadora

Para llegar hasta el 1 Gbps LTE-A permite aumentar el ancho de banda hasta 100 MHz [1-3] frente a los 20MHz de LTE. Para ello divide este espectro en 5 bloques básicos de 20 MHz, pudiendo asignar de manera dinámica a los usuarios el bloque que mejor se adapte a sus necesidades y a las de la red, soportando así asignaciones contiguas y no contiguas tal y como muestra la Figura 3.

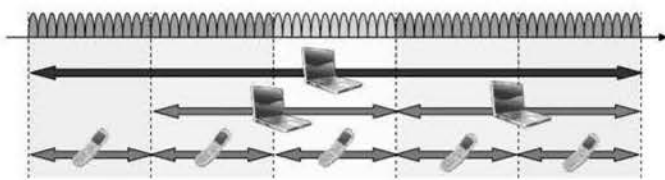


Fig. 3 Asignación dinámica del espectro

Cada uno de los bloques básicos, llamados componente de portadora (CC), se añade como se muestra en la Figura 4. Los parámetros de radio que se incluyen en cada bloque se basan en los de LTE, así, estos usuarios pueden acceder a ellos. De esta manera un usuario con un equipo con tecnología LTE puede incorporarse a una red LTE-A sin necesidad de cambiar su dispositivo o realizar modificaciones en él.

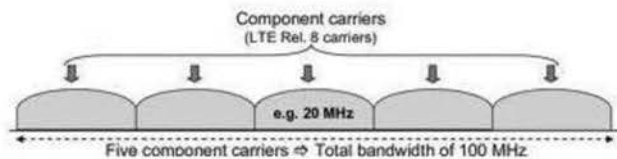


Fig. 4 Agregado de portadora

B. Multiplexado espacial avanzado

LTE-A estudia mejoras sobre los esquemas MIMO usados por LTE, tanto para el canal de bajada como para el canal de subida [7]. De hecho, permite el uso de un número mayor de antenas: 8 en la estación base y 4 en el terminal móvil.

En el canal de bajada se tiene especial interés en los esquemas multi-usuario para proporcionar, por ejemplo, mejoras en la supresión de interferencias entre usuarios.

En el canal de subida, el estudio de la transmisión mono-usuario está considerado como uno de los puntos clave a mejorar con respecto a LTE.

Las especificaciones y requisitos del sistema para todas las mejoras MIMO son aún objeto de debate para el 3GPP.

C. Coordinación multipunto de transmisión y recepción

El objetivo de la coordinación multipunto, o CoMP, es aumentar el rendimiento del sistema, con un incremento mínimo de la complejidad [4-6]. Aunque un terminal móvil está siempre ligado a una estación base, que es la encargada de enviar información de sincronización y control, las estaciones base cercanas pueden aliarse para enviar o recibir, hasta o desde el terminal. El funcionamiento interno de esta técnica se basa en MIMO, en su manera de aprovechar el efecto multi-camino, pero en este caso las antenas se encuentran distribuidas en zonas alejadas [8].

La figura 5 muestra un ejemplo de CoMP en el canal de bajada con dos usuarios, UE1 y UE2. eNB1 es la estación base principal de UE1 y las otras dos cooperan con esta para crear una transmisión multipunto [7].

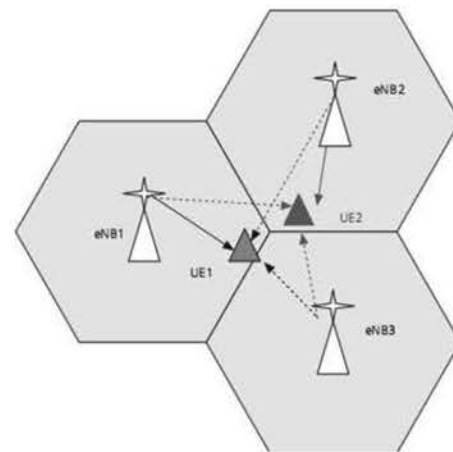


Fig. 5 Esquema CoMP en el canal de bajada

Se distinguen dos puntos de vista a la hora de implementar CoMP en el canal de bajada:

- Coordinación de sincronización y/o *beamforming*: La transmisión la realiza la estación base principal. Sin embargo, la sincronización, incluyendo el *beamforming*, se coordina entre las estaciones base para controlar y/o reducir la interferencia entre las transmisiones.
- Procesamiento y transmisión conjunta: Varias estaciones base transmiten a la vez a un terminal. Este esquema tiene un mayor rendimiento, pero depende de una buena comunicación entre estaciones base, a fin de simular una única transmisión.

CoMP, en el canal de subida, implica la recepción en múltiples puntos geográficamente separados. Las decisiones de sincronización se toman de manera coordinada a fin de controlar la interferencia.

#### D. Redes heterogéneas

Debido a los obstáculos del entorno y al uso de altas frecuencias, que implica mayor atenuación, para conseguir tasas de transmisión elevadas las estaciones base deben encontrarse cerca de los usuarios. La idea de las redes heterogéneas consiste en distribuir nodos de comunicación, más simples y baratos, dentro de las celdas. Estos nodos se comportan como puentes, entre los terminales móviles y las estaciones base.

Se definen varias clases de estos nodos: Pico-estación base, femto-estación base, nodo *relay* y DAS (sistemas distribuidos de antena). Sin embargo, LTE-A se centra en los nodos *relay*, que son dispositivos similares a las estaciones base, pero mucho más sencillos [10]:

- Tipo 1: Permite extender la cobertura de la celda a la que está ligada. Se comporta como una estación base, y de hecho tiene su propio identificador de celda, por lo que no es transparente para el usuario.
- Tipo 2: Permite aumentar la calidad y capacidad de una zona, gracias a su colocación y al aprovechamiento del efecto multi-camino. A pesar de ello, se trata de un dispositivo transparente para el usuario.

La utilización de este tipo de nodos, como puede observarse en la figura 6, permite extender la cobertura y/o aumentar el rendimiento en zonas determinada.

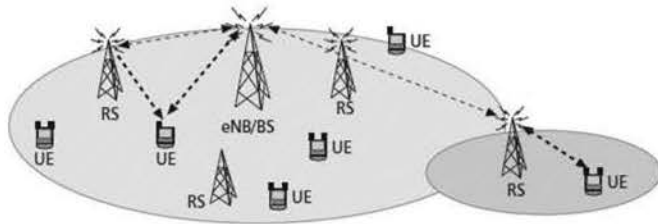


Fig. 6 Esquema de una celda con nodos *relay*

Esta técnica utiliza estrategias colaborativas (como CoMP) que permitan cooperar a todos los nodos y estaciones base, entre sí.

#### V. CONCLUSIONES

LTE-A, que actualmente es el único estándar válido para 4G en el mundo, es una evolución del estándar LTE, mejorando la velocidad de transmisión de datos, la cobertura de la red, el rendimiento y la latencia en el envío de paquetes.

Sus características permiten velocidades de transmisión de datos superiores a muchas conexiones cableadas domésticas, demostrando que las redes móviles son tan o más importantes que las conexiones cableadas. Este estándar está respaldado por el organismo 3GPP que es un acuerdo de colaboración sobre telefonía móvil entre numerosos países.

Finalmente, LTE-A es el estándar 4G más importante en la actualidad, dado que es el único que ha demostrado superar, con creces, los requisitos impuestos por la ITU-R.

#### VI. VOCABULARIO

**Celda:** Área de cobertura que proporciona una estación base.

**Handover:** Sistema utilizado en comunicaciones móviles celulares con el objetivo de transferir el servicio de una estación base a otra. Este mecanismo garantiza la calidad del servicio cuando un móvil se traslada a lo largo de su zona de cobertura.

**Ancho de banda:** Es el rango de frecuencias en la que se concentra la mayor parte de la potencia de la señal. Se mide en Hz.

**Efecto multi-camino:** En las transmisiones inalámbricas es corriente que la información encuentre obstáculos. En estos casos la señal se dispersa, lo que provoca, no sólo que ésta se degrade, sino que varias copias de la misma información lleguen al receptor, en instantes de tiempo diferentes. Esto puede provocar una disminución general de rendimiento y fiabilidad.

**Beamforming:** Técnica de procesamiento de señal, con múltiples antenas, que incrementa la ganancia y inmunidad a interferencias de una transmisión.

#### REFERENCIAS

- [1] 3GPP, TR36.814(V1.0.0), Feb. 2009.
- [2] 3GPP, TR36.913 (V8.0.1), Mar. 2009.
- [3] 3GPP, TS36.104 (V9.0.0), May 2009.
- [4] 3GPP TSG-RAN WG1, "R1-090914 Downlink CoMP", Meeting #56, Athens, Greece, 9 – 13 February, 2009.
- [5] 3GPP TSG-RAN WG1, "R1-090725 Setup of CoMP cooperation areas", Meeting #56, Athens, Greece, 9 – 13 February, 2009.
- [6] 3GPP TSG-RAN WG1, "R1-091064 Way forward of CoMP Clustering & Active Set", Meeting #56, Athens, Greece, 9 – 13 February, 2009.
- [7] LTE-Advanced: The Path towards Gigabit/s in Wireless Mobile Communications.
- [8] 3G and 4G Wireless Blog: Coordinated Multi-Point (CoMP) transmission and reception.
- [9] Cellular networks, artículo de Wikipedia.
- [10] Relay Technologies for WiMAX and LTE-Advanced Mobile Systems, IEEE Communications Magazine – October 2009

*Asignatura:* Xarxes de comunicacions mòbils

*Profesor:* Jaume Ramis Bibiloni



**Adrián Petit** es Ingeniero Técnico en Informática de Gestión y actualmente está realizando su proyecto de final de carrera de Ingeniería Informática.  
*adrian.petit@gmail.com*



**Alberto Ballesteros** es Ingeniero Técnico en Informática de Sistemas y actualmente está realizando su proyecto de final de carrera de Ingeniería Informática.  
*ballesteros.alberto@gmail.com*

# Estudi numèric dels Shock filters

Adrià Alcalá Mena, David Sánchez Charles

Assignatura de Càlcul Numèric de 4t de la Llicenciatura de Matemàtiques

**Abstract**—Un dels objectius de l'informàtica és proporcionar-nos eines per a simplificar la nostra vida quotidiana. Un dels problemes que ha de resoldre és el tractament d'imatges: Per exemple, un fons que, amb el pas del temps, s'han deteriorat i volem recuperar part de l'informació, o que les nostres càmeres digitals arreglin els desperfectes que es produeixen a la fotografia per la nostra inexperiència en el maneig d'aquesta eina. Aquests són alguns dels usos que l'informàtica resol i que a les seves solucions es troben unes eines matemàtiques consolidades.

**Index Terms**—Shock filters, equacions en derivades parcials, càlcul numèric, aproximació numèrica, tractament d'imatges, enfocament.

## I. INTRODUCCIÓ

LA passada dècada ha hagut un gran augment de l'utilització d'equacions en derivades parcials dins el camp de la visió per ordinador i el processament d'imatges. S'han desenvolupat aplicacions, amb una rigorosa teoria al darrera, que tenen objectius com la millora d'imatges i eliminació del soroll, segmentació, seguiment d'objectes i molt més. Es pot veure més sobre aquestes aplicacions a [2]. A [1] Osher i Rudin proposen una equació hiperbòlica, anomenada *shock filter* que pot servir com un algorisme estable per a l'enfocament d'imatges aproximant deconvolucions, una convolució és una generalització de fer una mitja ponderada. En el cas d'imatges sol referir-se a que l'imatge s'ha difuminat. Una deconvolució és el procés invers que, matemàticament, és un problema mal posat. Vegem en el cas unidimensional un exemple. En la figura 1 veim la funció signe i el resultat de la convolució amb un nucli de Gauss. L'objectiu dels Shock Filters és partint de la convolució recuperar la funció inicial.

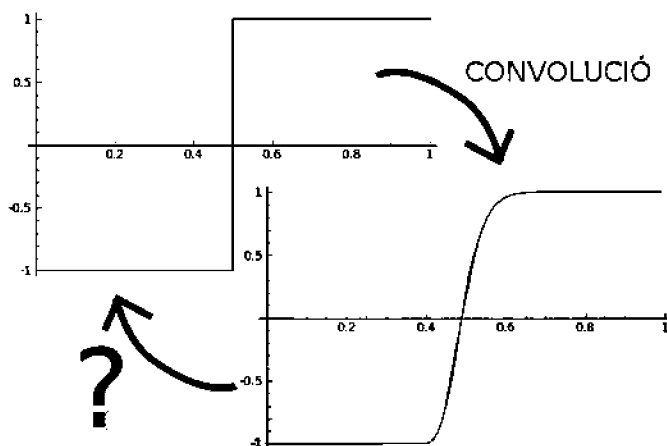


Fig. 1. Aquesta gràfica representa una convolució, el que volem trobar és el mètode que ens retorna la funció original.

## II. PLANTEJAMENT DEL PROBLEMA

La formulació de l'equació diferencial del shock filter, proposada per Osher i Rudin, és:

$$u_t = -|u_x|F(u_{xx}), \quad x \in (a, b), t > 0, \quad (1)$$

on  $F$  satisfà  $F(0) = 0$ ,  $F(s) \cdot \text{sign}(s) \geq 0$ . A més, la solució del problema que cercam tendrà com a condicions inicials  $u(x, 0) = u_0(x)$  i condicions de frontera de Neumann<sup>1</sup>. Si definim  $F(s) = \text{sign}(s)$  ens queda l'equació clàssica del shock filter

$$u_t = -|u_x|\text{sign}(u_{xx}). \quad (2)$$

En el cas bidimensional l'equació del shock filter es sol generalitzar amb

$$u_t = -\text{sign}(\Delta u)|\nabla u|, x \in \Omega, t > 0, \quad (3)$$

on  $\nabla u$  és el gradient<sup>2</sup> de  $u$  i  $\Delta u$  el Laplacian<sup>3</sup> de  $u$ .

Algunes propietats generals del shock filter són

- En els punts d'inflexió<sup>4</sup> el valor de la funció no canvia.
- Els extrems locals no varien al llarg del temps ni se'n creen de nous.
- La solució estacionària és constant a trossos, amb discontinuïtats als punts d'inflexió de  $u_0$ .
- El procés aproxima la deconvolució.

## III. CAS UNIDIMENSIONAL

En el cas unidimensional el nostre objectiu és trobar una funció  $u : (a, b) \times (0, +\infty) \rightarrow \mathbb{R}$  solució de l'equació diferencial (2) amb condicions inicials  $u(x, 0) = u_0(x)$  i satisfent les condicions de frontera Neumann.

El valor de  $u(x, T)$  ens proporcionarà l'evolució en l'instant  $T$  de la condició inicial  $u_0(x)$ .

### A. Esquema numèric

El mètode numèric que hem fet servir per resoldre aquesta equació diferencial és un mètode que ens permet obtenir una aproximació del valor de la funció en uns punts triats.

Volem obtenir la solució en un interval  $[a, b]$ , definim  $h = \frac{b-a}{M}$  on  $M$  serà el nombre de passes desitjades i  $x_m = a + m \cdot h$  ( $m = 0, \dots, M$ ) serà la  $m$ -èsima passa. Per altra banda, per a la variable temporal escollim uns valors  $T$  i  $N$ , on  $T$  serà

<sup>1</sup>  $\frac{\partial u}{\partial n} = 0$  on  $n$  és la direcció perpendicular a la frontera

<sup>2</sup> El vector  $(u_x, u_y)$

<sup>3</sup>  $u_{xx} + u_{yy}$

<sup>4</sup> La segona derivada és zero

el temps final que volem calcular i  $N$  el nombre d'iteracions que volem fer, i definim  $k = \frac{T}{N}$ ,  $t_n = n \cdot k$  ( $n = 0, \dots, N$ )<sup>5</sup>.

Denotarem per  $(u)_m^n$  l'aproximació de la funció  $u$  en el punt  $(x_m, t_n)$ .

Amb la notació anterior, l'esquema numèric pel cas unidimensional és:

$$u_m^{n+1} = u_m^n - k \cdot |(u_x)_m^n| F((u_{xx})_m^n),$$

on aproximam la primera derivada per

$$(u_x)_m^n = \text{minmod} \left( \frac{u_m^n - u_{m-1}^n}{h}, \frac{u_{m+1}^n - u_m^n}{h} \right). \quad (4)$$

La funció minmod es defineix com

$$\text{minmod}(x, y) = \frac{\text{sign}(x) + \text{sign}(y)}{2} \min\{|x|, |y|\}.$$

Amb la funció *minmod* obtenim una bona aproximació de la derivada  $u_x$  en el punt que desitjam:

- Si la derivada té signes diferents en les dues direccions, a prop tenim un mínim/màxim i per tant aproximam la derivada per 0.
- En altre cas, es queda amb la derivada més petita.

Aproximam la segona derivada de  $u$  amb l'esquema clàssic de tres punts.

$$(u_{xx})_m^n = \frac{u_{m+1}^n + u_{m-1}^n - 2u_m^n}{h^2}. \quad (5)$$

En ambdues aproximacions podríem tenir problemes en el cas  $m = 0$  (i  $m = M$ ) ja que en les fórmules hauríem de conèixer  $u_{-1}^n$  (o  $u_{M+1}^n$ ) que no hem definit. Emprant la condició de frontera

$$\frac{\partial u}{\partial n}(x) = 0 \quad x \in \partial[a, b]$$

que es tradueix per

$$u_x(x) = 0 \quad x = a \text{ o } b$$

i aproximant aquesta derivada amb un esquema de diferències centrades<sup>6</sup> obtenim que

$$u_{-1}^n = u_1^n \quad u_{M+1}^n = u_{M-1}^n$$

### B. Algorisme

L'algorisme per a la resolució numèrica amb aquest esquema es pot resumir en

- 1)  $u_m^0 = u_0(x_m)$
- 2)  $n = 0$
- 3)  $u_m^{n+1} = u_m^n + |(u_x)_m^n| F((u_{xx})_m^n)$  fent ús de les aproximacions esmentades.
- 4) Incrementar  $n$ , si hem arribat a  $n = N$  param. Si no, tornar a la passa 2.

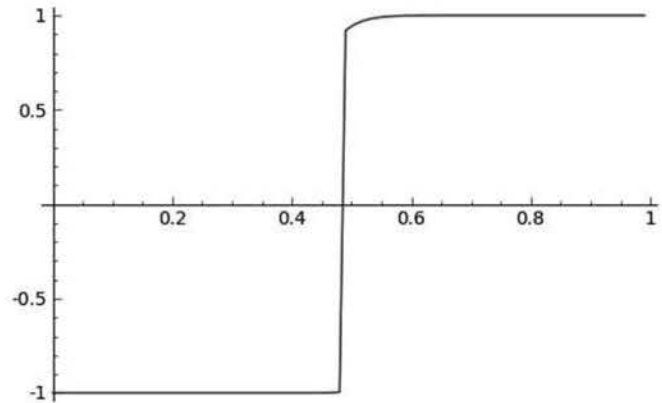


Fig. 2. Shock filter de la convolució de  $u(x) = \text{sign}(x)$  ( $h = 0.01$  i  $k = 0.005$  amb 20 iteracions)

### C. Exemples

Vegem primer de tot que passa si a la funció que era la convolució de  $u(x) = \text{sign}(x - 0.5)$  (Fig 1) li aplicam el shock filter (Fig 2)

Per tant en un principi, segons podem observar a Fig 2, el shock filter és una deconvolució.

Vegem ara un altre exemple d'aplicar l'algorisme a la funció  $u_0(x) = x \cdot \cos x$ .

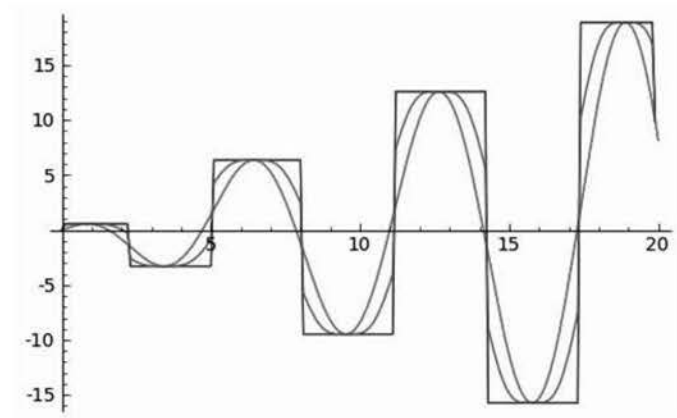


Fig. 3. Shock filter amb  $u_0(x) = x \cos(x)$ , amb 100 i 2000 iteracions ( $h = 0.1$ ,  $k = 0.01$ )

Observem a Fig. 3 que als extrems relatius i als punts d'inflexió el valor de la funció no varia. També es pot apreciar que el mètode esglaona la funció conservant aquests punts *conflictius* (extrems relatius i punts d'inflexió).

Fins ara no hem imposat cap condició als valors de  $h$  i  $k$ , però és necessari que compleixi una certa condició coneguda com *condició CFL*. Podem observar a Fig. 4 que si agafam uns valors no apropiats, el mètode pot produir errors no desitjats. Aquesta condició CFL determina l'estabilitat del mètode, que com es pot veure a [1], el mètode serà estable si  $\frac{k}{h} \leq 1/2$

<sup>5</sup>En aquest cas hem fet la partició de l'interval  $[0, T]$

<sup>6</sup> $u_m^n = \frac{u_{m+1}^n - u_{m-1}^n}{h}$

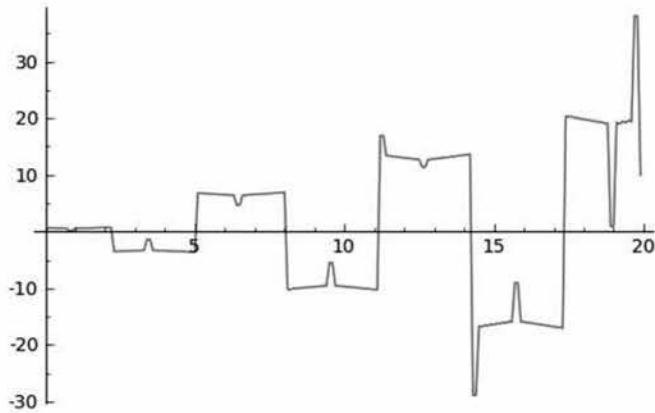


Fig. 4. Shock filter amb  $u_0(x) = x \cos(x)$ , amb 200 iteracions ( $h = 0.1$ ,  $k = 0.2$ )

#### IV. CAS BIDIMENSIONAL

A continuació farem un petit estudi de l'equació del Shock Filter en el cas bidimensional. Sigui  $\Omega \subseteq \mathbb{R}^2$  obert, volem trobar una funció  $u : \Omega \times (0, +\infty) \rightarrow \mathbb{R}$  solució de l'equació diferencial

$$u_t = -|\nabla u|F(\Delta u), \quad x \in \Omega, t > 0,$$

amb condicions inicials  $u(x, y, 0) = u_0(x, y)$  i les condicions de frontera Neumann <sup>7</sup>.

Aquesta equació diferencial manté les propietats mencionades pel cas general ja que les relacions necessàries entre  $|u_x|$  i  $u_{xx}$  es mantenen per  $|\nabla u|$  i  $\Delta u$  <sup>8 9 10</sup>.

El valor de  $u(x, y, T)$  ens proporcionarà l'evolució en l'instant  $T$  de la funció  $u_0(x, y)$ .

##### A. Esquema

Tal com hem fet en el cas unidimensional, farem una partició del nostre domini  $\Omega$ , que considerarem rectangle. En el nostre cas volem aplicar el mètode sobre una imatge, per tant la discretització de la funció ja ve donada pels píxels de l'imatge. Només ens queda escollir el temps final,  $T$ , i el nombre d'iteracions,  $N$ , que volem calcular.

En aquest cas denotam per  $u_{i,j}^n$  el nivell de gris del píxel  $(i, j)$  en el temps  $t_n = n \cdot \frac{T}{N}$  ( $n = 0, \dots, N$ ).

Amb aquesta notació el nostre esquema és:

$$u_{i,j}^{n+1} = u_{i,j}^n - |(\nabla u)_m^n| F((\Delta u)_m^n).$$

Recordam que

$$|\nabla u| = \sqrt{u_x^2 + u_y^2} \quad \Delta u = u_{xx} + u_{yy},$$

on, per aproximar aquests valors, farem ús de les mateixes fórmules (4) i (5) utilitzades en el cas unidimensional, per aproximar  $u_x$ ,  $u_y$ ,  $u_{xx}$  i  $u_{yy}$ .

<sup>7</sup>  $\frac{\partial u}{\partial n}(x, y) = 0, (x, y) \in \partial\Omega$

<sup>8</sup> En tot mínim/màxim,  $|\nabla u| = 0$

<sup>9</sup> En tot mínim,  $\Delta u > 0$

<sup>10</sup> En tot màxim,  $\Delta u < 0$



Fig. 5. D'esquerra a dreta: Imatge original,  $T = 0.2$  i  $N = 4$ ,  $T = 1.8$  i  $N = 36$

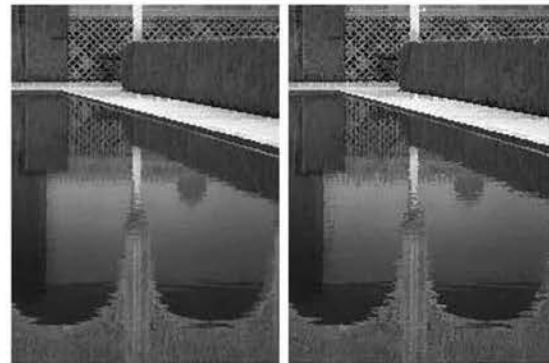


Fig. 6. A dalt tenim la imatge original. A l'esquerra la imatge processada amb 4 iteracions fins a arribar al temps  $T = 0.2$ . A la dreta després de 36 iteracions per a arribar al temps  $T = 1.8$ .

##### B. Exemples

Vegem com es comporta aquest mètode sobre imatges. Primer ho farem sobre una imatge artificial per a veure el seu comportament bàsic. Totes les proves s'han fet amb un increment  $h = 0.1$  per a la variable espacial (tant en la component  $X$  com en la  $Y$ ). Recordem que és necessari que els valors de  $h$  i  $k$  satisfacin la condició CFL que, en el cas bidimensional, és  $\frac{k}{h} \leq 1/4$ , ja que  $F(x) = \text{sign}(x)$  [1]

A Fig. 5 podem observar el mateix efecte que es produeix a la Fig. 3 però sobre una imatge. El mètode esglaona aquesta imatge borrosa fins que recuperam, bantant bé, uns rectangles ben definits.

Anem a veure com funciona el mètode sobre imatges reals. Primer hem fet ús d'aquest mètode per a veure com es comporta sobre el reflexe en aigua (Fig. 6)

Vegem ara que passa si aplicam el mètode a una imatge clàssica dins el tractament d'imatges després d'haver-la desenfocada (Fig 7). Notem que hem aconseguir part del nostre objectiu, les vores de la imatge es veuen més nítides. Però, hem pagat un preu per aquesta nitidesa, i és que les vores comencen

a pixelar-se molt. En l'exemple on la imatge *original* és molt més borrosa, encara que el mètode aconsegueix realçar les seves vores, obtenim un resultat més artificial, quasi pareix un dibuix.



Fig. 7. A l'esquerra tenim dos emborrnaments de l'imatge original, i a la dreta tenim la imatge després de 40 iteracions amb  $k = 0.025$ .

## V. CONCLUSIONS

La poca quantitat d'equacions diferencials que tenen solució analítica ha fet que els matemàtics comencessin a desenvolupar eines per a obtenir una aproximació numèrica d'aquestes ja en el segle XVIII: Leonhard Euler (1707-1783) inventà el primer mètode per resoldre'n, època en que era impensable l'existència d'unes màquines que ens poguessin executar aquests mètodes amb rapidesa. Ara que ja tenim una maquinaria suficientment potent, els matemàtics, i no matemàtics, s'han donat compte de la potència de la resolució numèrica d'equacions diferencials. No només pel tractat en aquest article, sinó en innombrables escenaris com poden ser el càlcul de la trajectòria de satèl·lits, modelatge del creixement d'una població o de la oferta i demanda d'un producte, etc.

## AGRAÏMENTS

Amb la col·laboració de la Dra. Catalina Sbert Juan, doctora en Informàtica per la Universitat de les Illes Balears

## REFERENCES

- [1] L. I. Rudin, S. Osher, *Feature-Oriented Image Enhancement with Shock Filters*, SIAM J. Numer. Anal. 27, pp. 919-940, 1990
- [2] G. Gilboa, N.A. Sochen, and Y.Y. Zeevi, *Regularized Shock Filters and Complex Diffusion*, in Proc. ECCV (1), 2002, pp.399-413.



# Ús de corbes el·líptiques en la criptografia i SAGE

Adrià Alcalá Mena, David Sánchez Charles

*Assignatura de Codificació i Criptografia de 4t de la Llicenciatura de Matemàtiques*

**Abstract**—El desenvolupament d'internet ha fet que les nostres comunicacions es realitzin mitjançant aquesta xarxa. La criptografia ens proporciona eines perquè la nostra informació es pugui transmetre de manera segura per aquesta xarxa pública. En aquest treball farem una implantació utilitzant SAGE per a utilitzar corbes el·líptiques dins la criptografia de clau pública.

**Index Terms**—Corbes el·líptiques, eGamal, criptografia, SAGE

22

## I. INTRODUCCIÓ

CADA vegada és més habitual la compra d'articles per internet. Perquè aquestes compres siguin exitoses s'haurien de complir dos requisits bàsics: secret i autenticació. La transmissió de la informació s'ha de fer de manera secreta; no es vol que una altra persona pugui, per exemple, aconseguir les nostres dades bancàries. També, qui rep la informació ha de poder autenticar l'autoria de l'emissor; en el nostre exemple la tenda virtual ha d'estar segura que som nosaltres qui hem fet la compra.

La criptografia dona solució a aquests dos problemes: Els algoritmes de xifrat i desxifrat ens asseguren que la transmissió de les dades per internet es fa de manera segura (secret). D'altra banda, també ens proporciona algoritmes de *firma* que asseguren al receptor qui és qui ha enviat el missatge (autenticació).

La criptografia moderna es basa en l'ús d'unes aplicacions (generalment tothom coneix com són aquestes aplicacions) que tenen per paràmetre el missatge que es vol xifrar o desxifrar i una clau. L'èxit d'aquests mètodes rau en què, sense la clau, és computacionalment molt difícil xifrar i desxifrar els missatges de la mateixa manera que l'emissor original.

Dins la criptografia moderna ens volem centrar en els criptosistemes de clau pública (proposats per Diffie Hellman en 1976). Aquests criptosistemes tenen 2 claus: Una de privada, que només coneix el propi usuari; i una de pública, que coneixen tots els possibles usuaris de la xarxa. Els usuaris que es vulguin comunicar amb un usuari determinat, han d'agafar la seva clau pública i fer ús de l'algoritme de xifrat amb aquesta clau. Quan l'usuari rep el missatge xifrat ha d'agafar la seva clau privada i fer ús de l'algoritme de desxifrat per retrobar el missatge original.

En aquest article farem un petit estudi d'un algoritme que fa ús de les corbes el·líptiques per al xifrat i desxifrat de missatges. Hem programat aquest algoritme sobre SAGE; una eina matemàtica de programari lliure que ens proporciona l'accés a diverses llibreries ja implementades.

July 30, 2011

## II. RSA

Al febrer de 1978 Ron Rivest, Adi Shamir i Leonard Adleman proposen un criptosistema de xifrat de clau pública: RSA, el qual consisteix en associar als missatges originals un valor numèric i aleshores xifrar el missatge per blocs de la mateixa longitud i amb un valor numèric comprès entre un cert rang.

Suposem  $m \in [2, n - 1]$ , l'algoritme de xifrat es redueix al càlcul d'una exponencial on la clau és el parell de nombres  $(e, n)$ :

$$c = E_{(e,n)}(m) = m^e \pmod{n}$$

L'algoritme de desxifrat per poder obtenir  $m$  a partir de  $c$  consisteix també en una exponenciació, essent la clau ara un altre parell de nombres  $(d, n)$ .

$$m = D_{(d,n)}(c) = c^d \pmod{n}$$

<sup>1</sup> Donat  $\varphi(n)$  és fàcil generar el parell de nombres  $e$  i  $d$  tal que  $e \cdot d = 1 \pmod{\varphi(n)}$ . No obstant això, calcular  $d$  coneixent  $e$  i  $n$  és molt complicat computacionalment sense coneixer  $\phi(n)$ . La fortalesa d'aquest criptosistema va lligada a la dificultat de la factorització de  $n$ .

Per tant, si tenim una manera simple d'obtenir  $\varphi(n)$ , obtindrem un bon esquema de xifrat i desxifrat. Rivest, Shamir i Adleman suggereixen l'algoritme d'obtenció de les claus que es pot veure a la Fig 1.

**Require:** Dos nombres primers  $p, q$ .

**Ensure:** La clau pública i privada de l'usuari.

- 1:  $n \leftarrow p \cdot q$ .
- 2: Es calcula  $\phi(n) = (p - 1)(q - 1)$ .
- 3: S'agafa un nombre sencer  $0 < e < \phi(n)$  tal que  $\text{mcd}(e, \phi(n)) = 1$ .
- 4: Es calcula  $d = e^{-1} \pmod{\phi(n)}$ .
- 5: **return** Clau pública  $(n, e)$ , Clau privada  $(d)$

Fig. 1. algoritme d'obtenció de les claus

Recordem que quan calculam la  $d$  feim l'invers dins de l'anell  $\mathbb{Z}_{\phi(n)}$  i aquest invers sempre existeix ja que  $\text{mcd}(e, \phi) = 1$ .

<sup>1</sup>El teorema d'Euler assegura que  $D_{(d,n)}(E_{(e,n)}(m)) = m$  si  $e \cdot d = 1 \pmod{\phi(n)}$

A. Exemple

```
sage:p,q,e,e2=23,19,17,29
sage:CLAUA=Claves(p,q,e)
      CLAUB=Claves(p,q,e2)
sage:CLAUA
[23, 19, 437, 396, 17, 233]
sage:CLAUB
[23, 19, 437, 396, 29, 41]
sage:missatge="RSA vs CE"
sage:send=EnviarMensaje2(missatge,CLAUA,CLAUB)
R -> 82 -> 54 -> 104
S -> 83 -> 11 -> 7
A -> 65 -> 145 -> 350
  -> 32 -> 288 -> 200
v -> 118 -> 423 -> 234
s -> 115 -> 115 -> 115
  -> 32 -> 288 -> 200
C -> 67 -> 249 -> 15
E -> 69 -> 46 -> 69
sage:RecibirMensaje2(send,CLAUA,CLAUB)
104 -> 54 -> 82 -> R
7 -> 11 -> 83 -> S
350 -> 145 -> 65 -> A
200 -> 288 -> 32 ->
234 -> 423 -> 118 -> v
115 -> 115 -> 115 -> s
200 -> 288 -> 32 ->
15 -> 249 -> 67 -> C
69 -> 46 -> 69 -> E
'RSA vs CE'
```

III. CORBES EL-LÍPTIQUES

Una corba el·líptica sobre nombres reals es defineix com el conjunt de punts  $(x, y)$  que satisfan l'equació de Weierstrass simplificada

$$y^2 = x^3 + ax + b$$

Les corbes el·líptiques sobre cossos finits  $\mathbb{Z}_p$ , amb un valor de  $p$  gran, ofereixen una alternativa en la criptografia de clau pública, com veurem posteriorment.

Si es compleix que  $4a^3 + 27b^2 \neq 0$ , la corba no té arrels repetides i podrem formar un grup additiu que a més tindrà un producte escalar,  $(G, +, *)$ , on  $G$  és el conjunt de punts de la corba, l'operació  $+$  és la suma de punts (que definirem més endavant) i  $*$  és el producte escalar. També afegirem un punt especial  $0$ , que anomenarem *infinít*, que serà el neutre del grup.

A. Aritmètica en corbes el·líptiques dins el cos del nombres reals

1) *Suma de punts d'una corba el·líptica:* Donats dos punts de la corba  $P$  i  $Q$ , podem traçar la recta que passa per ells. Si aquesta recta talla la corba en un tercer punt, el reflectirem a través de l'eix de les  $x$ , i dona lloc a un nou punt  $R$ . Direm que  $R$  és la suma de  $P$  i  $Q$ . En el cas que la recta que passa per  $P$  i  $Q$  no talli la corba en un tercer punt poden passar dues coses:

- 1) La recta és tangent a la corba en un dels dos punts. Amb la qual cosa la suma seria el simètric del punt on és tangent.
- 2) La recta no és tangent a la corba en cap punt. En aquest cas  $P + Q = 0$

En el cas en que  $P = Q$ , es fa la mateixa construcció però amb la recta tangent a la corba que passa per  $P$ .

L'explicació de l'operació suma es pot veure més fàcilment a la Fig 2

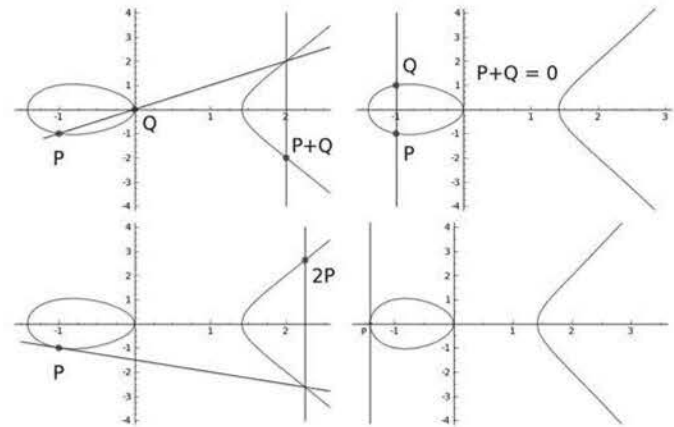


Fig. 2. Exemple de suma de punts en la corba el·líptica  $y^2 = x^3 - 2x$

2) *Punt invers dins una corba el·líptica:* Podem definir el punt invers, o simètric, de  $P = (x, y)$ , com la seva reflexió sobre l'eix  $x$ , és a dir:

$$-P = (x, -y)$$

Aquesta definició és consistent, ja que si un punt  $P$  és de la corba  $-P$  també ho és, ja que tota corba el·líptica és simètrica respecte l'eix  $x$ , si  $y^2 = x^3 + ax + b$  aleshores  $(-y)^2 = x^3 + ax + b$ .

3) *Producte d'un punt per un escalar:* De la mateixa manera que podem sumar dos punts, el podem sumar amb ell mateix (Fig 2) i de manera recursiva podem definir que:

$$k \cdot P = ((k - 1) \cdot P) + P$$

Així com les definicions de suma de punts i de punt invers tenien una explicació geomètrica, en aquest cas no.

4) *Aritmètica dins corbes el·líptiques amb cossos finits:* De la mateixa manera que hem definit les operacions sobre corbes el·líptiques en els reals, les podem definir sobre un  $\mathbb{Z}_p$ , i com era d'esperar, coincideixen amb el cas real però fent la reducció mòdul  $p$ . En aquest cas les definicions perden l'explicació geomètrica, ja que en un  $\mathbb{Z}_p$  una corba el·líptica és un conjunt de punts sense cap continuïtat visual ( veure Figura 8).

B. Algoritme ElGamal

En primer lloc necessitem obtenir les claus, per això hem de construir la clau pública i privada amb l'algoritme que es pot veure a la Fig. 3. Un cop tenim les claus podem xifrar

**Require:** Una corba el·líptica  $CE$  i un punt  $P$ .

**Ensure:** La clau pública i privada de l'usuari.

- 1: Calculam l'ordre  $r$  de la corba (el nombre de punts de la corba el·líptica).
- 2: Elegim un enter  $d \in [2, r - 2]$ .
- 3:  $clau = d * P$
- 4: **return** Clau pública  $(P, clau, r)$ , Clau privada  $(d, P, r)$

Fig. 3. algoritme d'obtenció de les claus

**Require:** Una corba el·líptica  $CE$  d'ordre  $r$ , la clau pública  $clau$  amb el punt  $P$  i el punt que es vol enviar  $M$ .

**Ensure:** El punt  $M$  xifrat.

- 1: Elegim un enter  $k \in [2, r - 2]$ .
- 2:  $C1 = k * P$ .
- 3:  $C2 = M + k * clau$
- 4: **return**  $(C1, C2)$

Fig. 4. algoritme de xifrat

**Require:** Una corba el·líptica  $CE$ , la clau privada  $d$  i el missatge rebut  $(C1, C2)$

**Ensure:** El missatge  $(C1, C2)$  desxifrat.

- 1:  $M = C2 - d * C1$
- 2: **return**  $M$

Fig. 5. algoritme de desxifrat

amb l'algoritme que es pot veure en la Fig. 4 i desxifrar el missatge rebut amb l'algoritme que es pot veure en la Fig. 5.

L'algoritme de firma d'un missatge  $M$  és pot trobar en la Fig. 6, per altra part per a comprovar l'autenticitat de l'emissor farem ús de l'algoritme que es pot veure a la Fig. 7. Aquests algorismes utilitzen un tipus d'aplicacions anomenades funcions de hash<sup>2</sup>.

**Require:** Una corba el·líptica  $CE$  i el seu ordre  $r$ , la clau privada  $(d, P)$  i un hash del missatge  $H(M)$ .

**Ensure:** La firma  $(R, S)$  del missatge  $M$ .

- 1:  $k \in [2, r - 2]$
- 2:  $x, y =$  components de  $k * P$
- 3:  $R = x \pmod{r}$
- 4:  $S = k^{-1}(H(M) + R \cdot d) \pmod{r}$
- 5: **return**  $(R, S)$

Fig. 6. algoritme de firma

**Require:** Una corba el·líptica  $CE$  i el seu ordre  $r$ , la clau pública  $(P, Q)$ , el hash  $M$  del missatge rebut i la seva firma  $(R, S)$ .

**Ensure:** L'acceptació, o no, de la firma.

- 1:  $w = S^{-1} \pmod{r}$
- 2:  $u_1 = M \cdot w, u_2 = R \cdot w$
- 3:  $x, y =$  components de  $u_1 * P + u_2 * Q$
- 4: **return** És  $x = R \pmod{r}$

Fig. 7. algoritme de verificació de la firma

### C. Exemple

Comencem amb un primer exemple senzill dins  $\mathbb{Z}_{23}$ . La corba el·líptica amb la que farem feina és

<sup>2</sup>Una funció de hash transforma un objecte en una cadena de bits de longitud constant, però no es coneix cap manera eficient d'obtenir, si existeix, l'invers d'aquest tipus d'aplicacions.

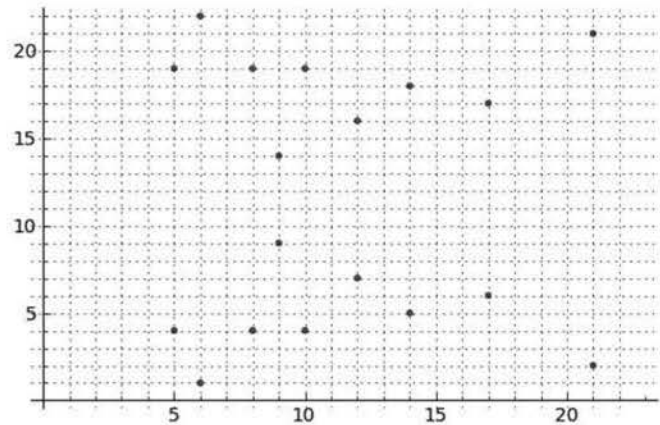


Fig. 8. Gràfica de la corba el·líptica  $y^2 = x^3 + 9x + 7$  dins  $\mathbb{Z}_{23}$

```
sage:E = CorbaEl·líptica(y+2==x+3+9*x+7, 23)
```

Comprovem que l'ordre sigui primer

```
sage: E.order()
19
```

Amb el SAGE també la podem dibuixar amb la instrucció `E.plot()` que ens retorna la figura que es pot veure a Fig 8.

Definim tres punts i vegem com podem sumar punts amb SAGE:

```
sage:P, Q, M=E([8, 4, 1]), E([9, 9, 1]), E([14, 5, 1])
sage: (P+Q).xy()
(8, 19)
sage: (5*P).xy()
(6, 22)
```

La instrucció `.xy()` és simplement per a veure les coordenades del punt.

Ara farem ús de la llibreria *EIGamalArt*<sup>3</sup> per a xifrar el missatge  $M$ . Primer hem de crear les claus dels dos usuaris que es volen comunicar.

```
sage: publicaP, privadaP=Clau(E,P)
sage: publicaP
((8 : 4 : 1), (17 : 6 : 1), 19)
sage: privadaP
(4, (8 : 4 : 1), 19)
sage: publicaQ, privadaQ=Clau(E,Q)
sage: publicaQ, privadaQ
((9 : 9 : 1), (17 : 6 : 1), 19), (17, (9 : 9 : 1), 19))
```

Cada usuari utilitza un punt diferent, d'una corba el·líptica comuna, per a obtenir el seu parell de claus. La clau pública està formada per un punt  $R$  (en el nostre exemple els punts  $P$  i  $Q$ ), un múltiple seu  $d \cdot R$  i, per qüestions d'optimització, l'ordre de la corba el·líptica. D'altra banda, la clau privada està formada per l'escalar  $d$  i, per comoditat, els punts  $R$  i l'ordre de la corba el·líptica.

El primer usuari vol enviar el missatge  $M$ , per a xifrar el missatge ha d'utilitzar la clau pública del receptor

```
sage: send=Xifrar(E, publicaQ, M)
sage: send
((6 : 22 : 1), (10 : 19 : 1))
```

Per tant l'emissor enviaria `send` al receptor. I, en el cas que el volgués firmar, el podria enviar amb la firma del nombre

<sup>3</sup>Aquesta llibreria està feta per nosaltres, si a qualqu li interessa es pot posar en contacte amb nosaltres mitjançant els correus dscharles@gmail.com o adria.alcala@gmail.com

19<sup>4</sup>

```
sage: firma=Firmar(E,privadaP,19)
sage: firma
(10,3)
```

Per tant l'emissor enviaria `send` juntament amb `firma`.

Ara, quan el receptor rebés el missatge, primer desxifra el missatge per a obtenir el missatge original

```
sage: Desxifrar(E,privadaQ,send)
(14 : 5 : 1)
```

i si vol verificar l'autoria del missatge, ha de calcular el hash del missatge desxifrat (en aquest cas,  $19 = 14 + 5$ ) i fer-ne us de l'algorisme d'autenticació

```
sage: VerificarFirma(E,publicaP,19, firma)
True
```

#### IV. COMPARACIÓ DE CRIPTOSISTEMES

Anem a comparar ara la velocitat del criptosistema RSA amb el de corbes el·líptiques utilitzant ElGamal. Per a comparar la velocitat no podem agafar tamanyes de claus iguals, si no que han de ser proporcionals a la dificultat de rompre el criptosistema, per exemple una clau de 512 bits a RSA és equivalentment segura a una de 106 bits a corbes el·líptiques. Taules comparatives de tamanyes de claus es poden trobar a [1] i en podem veure una a la Fig. 9

##### A. 1024 bits RSA vs 160 bits CE

Vegem primer el que tarda en xifrar un punt qualssevol amb una corba amb un ordre de 160 bits.

```
Xifrar: 5 loops, best of 3: 60.1 ms per loop
Desxifrar: 25 loops, best of 3: 29.5 ms per loop
```

I ara vegem el que tarda en xifrar un nombre sencer qualssevol amb RSA amb una clau de 1024 bits.

```
Xifrar: 125 loops, best of 3: 2.25 ms per loop
Desxifrar: 125 loops, best of 3: 2.23 ms per loop
```

##### B. 2048 bits RSA vs 192 bits CE

Vegem primer el que tarda en xifrar un punt qualssevol amb una corba amb un ordre de 192 bits.

```
Xifrar: 5 loops, best of 3: 75.7 ms per loop
Desxifrar: 25 loops, best of 3: 37 ms per loop
```

I ara vegem el que tarda en xifrar un de sencer amb RSA amb una clau de 2048 bits.

```
Xifrar: 25 loops, best of 3: 16.6 ms per loop
Desxifrar: 25 loops, best of 3: 16.8 ms per loop
```

##### C. 521 bits CE vs 15034 bits i 4048 bits RSA

Vegem primer el que tarda en xifrar un punt qualssevol amb una corba amb un ordre de 521 bits.

```
Xifrar: 5 loops, best of 3: 231 ms per loop
Desxifrar: 5 loops, best of 3: 113 ms per loop
```

Vegem el que tarda en xifrar un nombre sencer qualssevol amb RSA amb una clau de 4048 bits.

```
Xifrar: 5 loops, best of 3: 164 ms per loop
Desxifrar: 5 loops, best of 3: 170 ms per loop
```

I ara vegem el que tarda en xifrar un de sencer amb RSA amb una clau de 15034 bits.

```
Xifrar: 5 loops, best of 3: 4.37 s per loop
Desxifrar: 5 loops, best of 3: 3.92 s per loop
```

<sup>4</sup>Hem escollit la suma de les coordenades del punt, però hauríem pogut escollir qualssevol altra funció de hash

Nivell de seguretat	RSA	CE
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Fig. 9. Tamany de clau recomanat per NIST

#### V. CONCLUSIONS

La primera conclusió que obtenim és que l'algorisme per a corbes el·líptiques necessita claus molt més petites que RSA, i aquesta diferència és fa més gran a mesura que el tamany de les claus augmenta. També observem que quan augmentem el tamany de la clau el temps que tarda RSA en xifrar i desxifrar augmenta moltíssim, per altra part l'algorisme ElGamal per a corbes el·líptiques no té un augment tan agressiu com el RSA. Això pot ser degut als càlculs amb xifres de molts de dígit que ha de fer RSA.

En relació amb el temps que tarda l'algorisme de ElGamal, podem observar com xifrar tarda dues vegades el de desxifrar, que es la diferència de multiplicacions que hi ha en l'algorisme. Pareix que aquestes multiplicacions són el que més temps, i recursos, consumeixen. A [2] han trobat un tipus més concret de corbes el·líptiques on el temps de càlcul es pot millorar fins a un 50%.

Per últim, quan siguin necessaris unes claus més fiables aquesta tècnica serà molt més eficaç. De fet, ja comença a ser útil a certs casos crítics: per exemple, el DNI electrònic utilitza una clau RSA d'uns 4000 bits. Com ja hem vist, aquest cas té un cost computacional paregut al de ElGamal amb una clau d'uns 520 bits, emperò ElGamal en aquest cas proporciona molta més seguretat.

#### AGRAÏMENTS

Amb la col·laboració del Dr. Llorenç Huguet Rotger, CU en Ciències de la Computació i Intel·ligència Artificial a la Universitat de les Illes Balears i professor de l'assignatura *Codificació i Criptografia* de la llicenciatura de Matemàtiques.

#### REFERENCES

- [1] T.Beth, F.Schaefer, *Non Supersingular Elliptic Curves for Public Key Cryptosystem*, Advances in Cryptology- EUROCRYPT'91, pag 316-327
- [2] Robert P. Gallant, Robert J. Lambert, and Scott A. Vanstone, *Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms*, Advances in Cryptology - CRYPTO 2001, pag 190-200
- [3] L. Huguet, *Apunts de l'assignatura Codificació i Criptografia*, curs 2010-11.

# Mesura de la resposta freqüencial d'un filtre passa-banda

Margalida Amengual Jaume<sup>1</sup>, Vicenç Blanco Rosselló<sup>2</sup> i Margalida Rosselló Canals<sup>3</sup>

Tercer curs d'Enginyeria Tècnica Industrial, Especialitat en Electrònica Industrial

<sup>1</sup> lidamja@hotmail.com

<sup>2</sup> vicensblanco@hotmail.com

<sup>3</sup> margus\_hemingwai@hotmail.com

Aquest article descriu la primera pràctica de l'assignatura Instrumentació Electrònica II en la que s'implementa un analitzador de xarxes virtual. Un analitzador de xarxes és un element que mesura la resposta freqüencial d'un sistema lineal en règim permanent sinusoidal. La implementació és virtual perquè es fa a través d'instrumentació controlable mitjançant bus GPIB. Es tracta d'excitar un filtre passa-banda amb un senyal sinusoidal conegut tot monitoritzant-ne la seva resposta freqüencial.

mostreig d'acord a les especificacions per representar el Diagrama de Bode i calcular el factor de qualitat (Q), les freqüències de tall baixa i alta ( $f_L$  i  $f_H$ ), l'amplada de banda (BW) i la freqüència de ressonància ( $f_{res}$ ). La Q és un indicador de la forma que tindrà la gràfica del mòdul i de quan selectiu és el filtre. Les  $f_L$  i  $f_H$  ens indiquen freqüències de tall baixa i alta respectivament. El resultat de la resta d'ambdues es concix com el BW i representa el rang de freqüències no atenuades pel sistema. La  $f_{res}$  és la freqüència central del BW i per tant, la que el sistema deixa passar amb l'atenuació més baixa possible.

26

## I. INTRODUCCIÓ

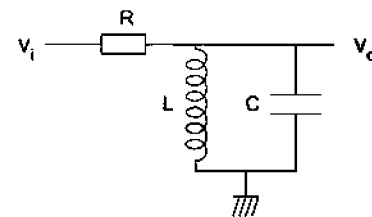
Una de les maneres més comuns de conèixer la resposta freqüencial d'un sistema és realitzar un escorbat de freqüències, que s'apliquen a l'entrada, i mesurar l'amplitud i el desfasament de la senyal a la sortida. Per conèixer la resposta freqüencial, s'han d'extreure dues gràfiques. En ambdues la freqüència, en escala logarítmica, ocupa l'eix x mentre que en una d'elles, -a l'eix y- hi ha el guany en decibels i a l'altra la diferència entre fases en graus. El conjunt d'aquests dos gràfics s'anomena Diagrama de Bode. En el Bode es veu clarament quin és el guany i el desfasament de cada freqüència en travessar el sistema i, en el cas d'un filtre, els valors de freqüència que aquest deixa passar o atenua.

Per poder realitzar totes aquestes mesures i transportar-les a l'ordinador comptant amb un generador de funcions, un oscil·loscopi i un multimetre digitals, tots ells controlables via GPIB.

La pràctica consistirà en elaborar el Diagrama de Bode d'un filtre passa-banda, entre un rang de freqüències definit per l'usuari. Aquest podrà, des de l'ordinador, escollir paràmetres com l'amplitud del senyal d'entrada, la freqüència d'inici d'escorbat ( $f_{inicial}$ ), la freqüència final ( $f_{final}$ ), el nombre de mostres que es prendran o el tipus d'escorbat, lineal o logarítmic. Això vol dir que en seleccionar el mostreig lineal es prendran N mostres equidistants, i en seleccionar un mostreig logarítmic, la separació entre cada una de les mostres seguirà un patró de base logarítmica. A més, es podrà seleccionar la ruta on guardar els arxius de text que es creen amb les mesures de les gràfiques. Quan l'usuari hagi introduït els paràmetres de la mesura, el programa realitzarà un

## II. CÀLCULS PREVIS

El tipus de filtre a analitzar és un passa-banda passiu, i aquest és el seu esquema elèctric:



S'obté la seva funció de transferència:

$$H(s) = \frac{V_o}{V_i} = \frac{Z_L \parallel Z_C}{Z_L \parallel Z_C + R} = \frac{\frac{Ls}{LCs^2 + 1}}{\frac{Ls}{LCs^2 + 1} + R} = \frac{Ls}{RLCs^2 + Ls + R}$$

$$H(s) = \frac{\frac{s}{RC}}{s^2 + \frac{s}{RC} + \frac{1}{LC}}$$

Comparant amb la funció d'una passa-banda:

$$H(s) = \frac{K \left( \frac{\omega_0}{Q} \right) s}{s^2 + \frac{\omega_0}{Q} s + \omega_0^2} \quad \text{D'aquí s'obté:} \quad \begin{aligned} \omega_0 &= \frac{1}{\sqrt{LC}} \\ Q &= R \cdot \sqrt{\frac{C}{L}} \\ K &= 1 \text{ (Filtre passiu)} \end{aligned}$$

Sabem que:

$$BW = \frac{f_0}{Q} = \frac{\omega_0}{2\pi Q}; \quad BW = \frac{\omega_H - \omega_L}{2\pi}; \quad (1) \quad \omega_0 = \sqrt{\omega_H \cdot \omega_L}; \quad (2)$$

De l'equació (2) s'aïlla  $\omega_H$  i l'(1) s'igual a 0. Seguidament, es substitueix  $\omega_H$  dins (1) i s'obté una equació de segon grau amb  $\omega_L$  d'incògnita:

$$\omega_L^2 + 2\pi \cdot BW \cdot \omega_L - \omega_0^2 = 0$$

D'aquí s'obté  $\omega_L$  i substituint a l'equació (2)  $\omega_H$ .

Els valors dels components dels que disposem són:

$$R = 1K\Omega \quad C = 4'7nF \quad L = 10mH$$

Si aplicam valors a les equacions anteriors, obtenim:

$$\omega_0 = 145'865K \frac{rad}{s} \longrightarrow f_0 = \frac{\omega_0}{2\pi} = 23'2K \text{ Hz}$$

$$Q \approx 0'68 \quad BW = 34'117K \text{ Hz}$$

$$\omega_L = 73'861K \frac{rad}{s} \longrightarrow f_L = \frac{\omega_L}{2\pi} = 11'755K \text{ Hz}$$

$$\omega_H = 288K \frac{rad}{s} \longrightarrow f_H = \frac{\omega_H}{2\pi} = 45'836K \text{ Hz}$$

### III. DESCRIPCIÓ DEL DESENVOLUPAMENT

L'entorn de programació que s'utilitza és el *LabView*, que té dos espais de treball diferenciats. Un, anomenat Panell Frontal, que és on tenim la interfície de l'Instrument Virtual (en endavant VI) amb l'usuari i l'altre, anomenat diagrama de blocs, on hi trobam l'estructura interna de l'VI.

Al Panell Frontal, s'hi poden trobar tant els controls com els indicadors dels resultats obtinguts en la mesura. A la Figura 1, es pot apreciar com estan col·locats els diferents elements.

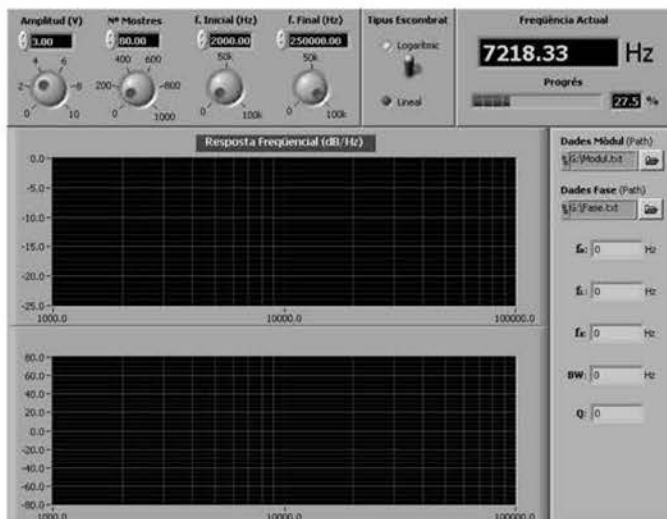


Fig. 1 Distribució dels elements en el Panell Frontal

Els controls, paràmetres que l'usuari pot escollir, són:

- L'amplitud del senyal d'entrada.
- El número de mostres que es duran a terme per realitzar l'escombrat de freqüències.
- La freqüència inicial i la final de l'escombrat.
- El tipus d'escombrat, logarítmic o lineal.
- Les rutes on es guardaran els arxius de text amb les dades resultants, tant de mòdul com de fase de la mesura.

Els indicadors que hi podem trobar són:

- Les gràfiques que representen el diagrama de Bode (la gràfica freqüència-mòdul i la freqüència-fase).
- La freqüència actual a la que es troba l'escombrat.
- El factor de qualitat (Q), l'amplada de banda (BW), la freqüència de ressonància ( $f_{res}$ ) i la freqüència de tall alta i baixa ( $f_H$  i  $f_L$ ).

La Figura 2 mostra el Diagrama de flux que segueix l'VI per fer la mesura.

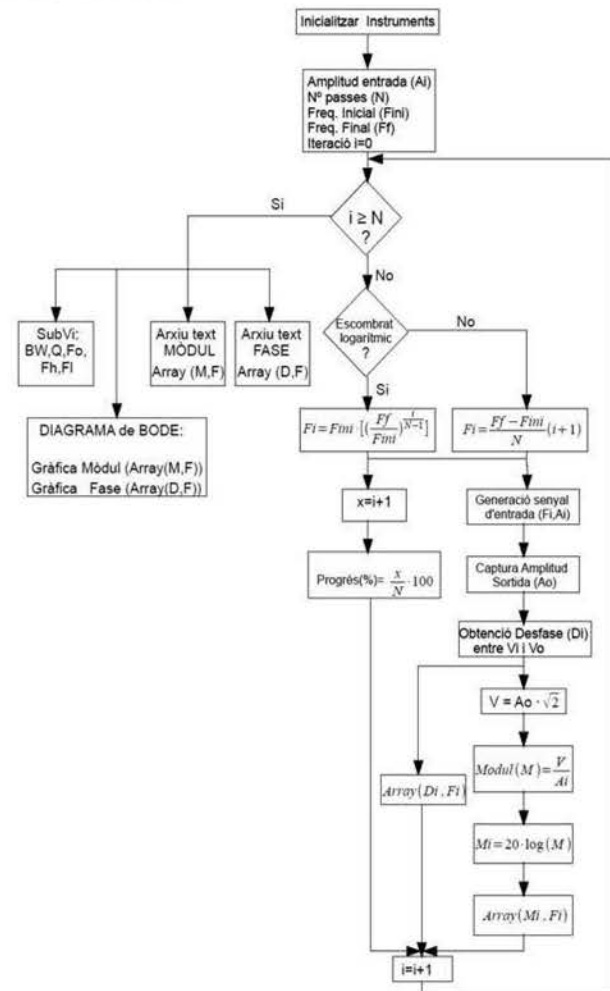


Fig. 2 Diagrama de flux de l'VI

Com hem comentat, el diagrama de blocs descriu l'estructura del programa. A més, representa el camí que seguiran les nostres dades, i les transformacions que patiran durant aquest. La Figura 5 mostra el diagrama de blocs del programa.

Dins el Diagrama de Blocs s'hi distingeixen clarament dues parts; una emmarcada per un bucle *for* i una altra fora del bucle. La part emmarcada pel bucle *for* està formada per un requadre (una estructura *case*) a la part superior que ens tria el tipus d'escombrat mentre que els requadres continuats de la part inferior (estructura *flat sequence*) forcen l'esdevenir seqüencial de les accions que s'hi especifiquen. D'aquesta manera, s'assegura que primer s'introdueixi el senyal, després s'espera un temps, perquè passi el transitori, es faci la lectura de la sortida i finalment es calculi la diferència entre les fases de la senyal d'entrada i de sortida. De no emprar aquesta estructura, no es seguiria aquest ordre.

Per a la generació de l'ona d'entrada, el primer que s'ha de fer és inicialitzar el dispositiu i assignar-li una direcció GPIB. Ambdues coses es fan a fora del bucle *for* perquè s'ha de fer tan sols una vegada, no a cada iteració. A més, en el cas del multimetre s'ha d'especificar també el tipus de lectura que es fa, com per exemple, si la lectura és de corrent continu o altern.

Com que les mesures que fan els multimetres són en valor eficaç, multiplicam la sortida per arrel de dos per tenir l'amplitud real del voltatge de sortida. Aquest, a la vegada, es divideix entre el senyal d'entrada i s'obté el mòdul. Ara bé, aquest mòdul no es troba en decibels (dB) sinó en escala decimal. Per això, es calcula el logaritme del guany i es multiplica per vint -ja que es tracta de tensió-. Així, el mòdul està en dB, enllestint per posar a l'eix Y de la gràfica del mòdul.

Per mesurar la diferència entre la ona d'entrada i la de sortida s'utilitza l'oscil·loscopi. El bloc que simbolitza el subprojecte encarregat del desfasament s'inclourà en el darrer dels requadres continuats i el seu funcionament s'explica en el diagrama de flux de la Figura 4.

Fora del bucle *for*, a més de la representació del Diagrama de Bode, hi trobam un bloc de color morat que simbolitza un subVI BW,fo,Q (Figura 3).

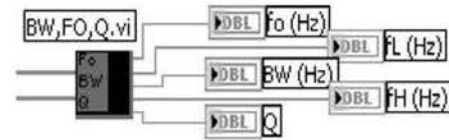


Fig. 3 Diagrama de flux del subVI del desfasament.

En ell s'hi fan els càlculs pertinents per extreure el factor de qualitat Q, l'amplada de banda BW, la freqüència de ressonància i les freqüències de tall baixa i alta ( $f_L$  i  $f_H$ ).

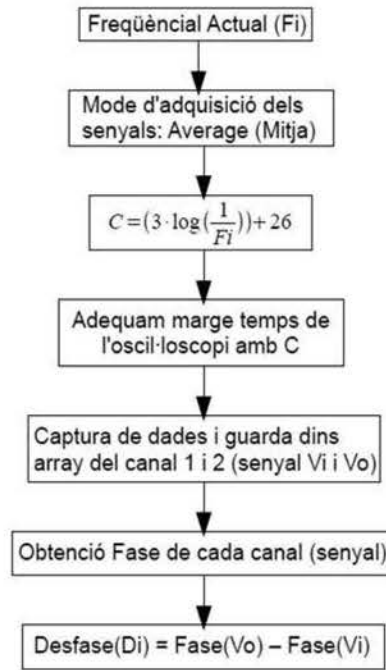


Fig. 4 Diagrama de flux dels càlculs

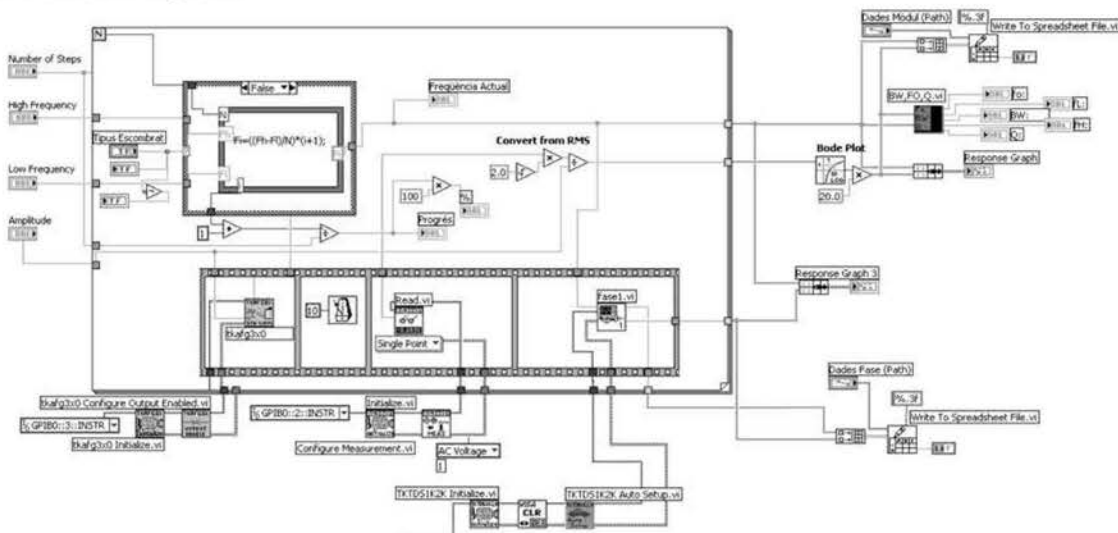


Fig. 5 Diagrama de Blocs del VI

La Figura 6 mostra el Diagrama de flux que descriu el procediment per obtenir aquestes dades.

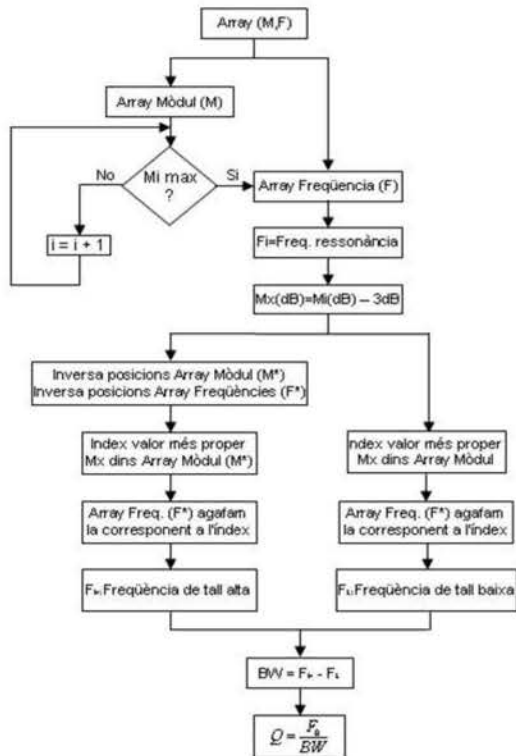


Fig. 6 Diagrama de flux del subVI dels càlculs

Finalment defora del bucle for, hi trobam dos conjunt de blocs pràcticament iguals i que realitzen la mateixa funció, crear un arxiu de text en què s'hi emmagatzemen les dades. Cada conjunt, crea un arxiu per les dades que rep. Un, per les freqüències amb el seu corresponent mòdul, i un altre per les freqüències amb la corresponent diferència entre fases.

#### IV. RESULTATS OBTINGUTS

La Figura 7, mostra el resultat quan l'escombrat ha acabat.

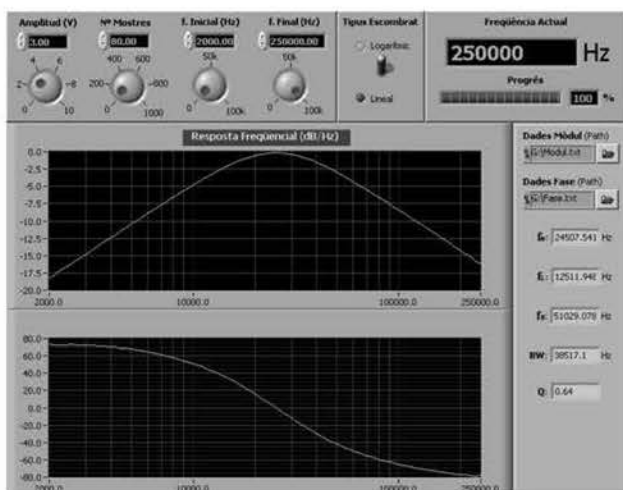


Fig. 7 Panell Frontal amb les dades de la sortida

Les Figures 8 i 9 mostren les dades que es guarden a l'arxiu de text de la carpeta que hem especificat.

1000.000	-23.897	999.686	68.385
1389.495	-21.269	1389.637	71.479
1930.698	-18.538	1931.093	72.827
2682.696	-15.764	2682.595	72.913
3727.594	-12.967	3727.716	71.512
5179.475	-10.176	5179.455	67.402
7196.857	-7.426	7197.339	59.985
10000.000	-4.773	9999.758	51.754
13894.955	-2.382	13894.272	37.550
19306.977	-0.644	19306.872	18.505
26826.958	-0.155	26826.491	-4.073
37275.937	-1.153	37275.763	-26.437
51794.747	-3.169	51794.206	-43.103
71968.567	-5.673	71969.337	-56.168
100000.000	-8.369	99995.010	-65.006

Fig. 8 i 9 Contingut de l'arxiu de dades del mòdul i la fase

#### V. CONCLUSIONS

Com s'ha pogut comprovar la instrumentació virtual ens permet mesurar magnituds d'un sistema de manera més ràpida, acurada i eficient que de manera manual. A més a més, l'entorn de programació ens permet fàcilment realitzar càlculs sobre aquestes mesures i arrossegar errors, cosa que resultaria bastant tediosa si es fes manualment, sense comptar amb possibles errors humans.

A més, en aquest cas, mitjançant el software del Labview hem aconseguit implementar funcions, com ara la mesura del desfasament, que d'entrada l'oscil·loscopi no és capaç de mesurar per si mateix, amb la qual cosa obtenim un valor afegit important.

ASSIGNATURA: Instrumentació Electrònica II  
PROFESSOR: Jaume Verd



**Margalida Amengual Jaume** (Biniamar)  
Estudiant d'Enginyeria Tècnica Industrial  
Especialitat Electrònica Industrial a la UIB.  
[lidamja@hotmail.com](mailto:lidamja@hotmail.com)



**Vicenç Blanco Rosselló** (Felanitx)  
Estudiant d'Enginyeria Tècnica Industrial  
Especialitat Electrònica Industrial a la UIB.  
[vicensblanco@hotmail.com](mailto:vicensblanco@hotmail.com)



**Margalida Rosselló Canals** (Bunyola)  
Estudiant d'Enginyeria Tècnica Industrial  
Especialitat Electrònica Industrial a la UIB.  
[Margus\\_hemingwai@hotmail.com](mailto:Margus_hemingwai@hotmail.com)



# Geolocalització i Serveis Basats en Localització

Cristina Rodríguez Aguado

Tercer curs d'Enginyeria Tècnica en Telecomunicacions, especialitat Telemàtica  
cristina.raguado@gmail.com

**Resum**— La geolocalització i els serveis basats en localització permeten obtenir tot tipus d'informació en temps real relacionada amb la seva localització en un mapa amb gran precisió. Són una de les manifestacions més populars del desenvolupament de les Tecnologies de la Informació i les Comunicacions (TIC) en els darrers anys. Especialment important és la seva expansió als dispositius mòbils, gràcies a l'aparició de telèfons intel·ligents o "smartphones" que permeten no sols la mobilitat d'un dispositiu mòbil sinó també una connexió permanent de banda ampla a Internet.

En aquest article s'explica el funcionament de diversos sistemes de localització i posicionament, es mostren algunes de les aplicacions més populars de geolocalització i s'analitzen els aspectes més importants de la privacitat en aquestes aplicacions.

## I. INTRODUCCIÓ

Les tecnologies de geolocalització són aquelles que obtenen informació vinculada a una localització geogràfica. Els Sistemes d'Informació Geogràfica (SIG) són el conjunt de hardware, software i dades que permeten gestionar, interpretar, visualitzar i analitzar aquesta informació.

Els serveis basats en localització utilitzen els SIG per oferir als usuaris un servei personalitzat en funció de la seva ubicació geogràfica en temps real.

Dins la geolocalització es poden diferenciar tres categories:

- Georeferenciació: localització física d'un objecte o un individu en un sistema de coordenades, per posteriorment accedir a informació específica d'aquesta posició.
- Geocodificació: cerca d'informació i localització física d'aquesta informació en un mapa.
- Geotiquetat: afegir informació geogràfica a un contingut ja generat com, per exemple, una fotografia.

## II. SISTEMES DE LOCALITZACIÓ I POSICIONAMENT

Els darrers anys s'han desenvolupat múltiples mecanismes que permeten la localització geogràfica d'un dispositiu. Les més rellevants són les següents:

### A. Localització per satèl·lit

Els sistemes de localització per satèl·lit són aquells que utilitzen satèl·lits per localitzar y posicionar un element a la superfície terrestre.

Les xarxes de satèl·lits com GPS, GALILEO o GLONASS proporcionen als receptors la informació necessària per calcular la seva posició. Per fer aquest càlcul es necessari determinar la distància a tres satèl·lits de posició coneguda a partir del temps que tarda en arribar el senyal des de cada un

d'ells fins al dispositiu. Conegudes aquestes distàncies es pot calcular la posició del dispositiu per triangulació, és a dir, formant triangles i aplicant fórmules trigonomètriques.

És necessari que el dispositiu que volem localitzar incorpori un receptor GPS que interpreti els senyals dels satèl·lits.

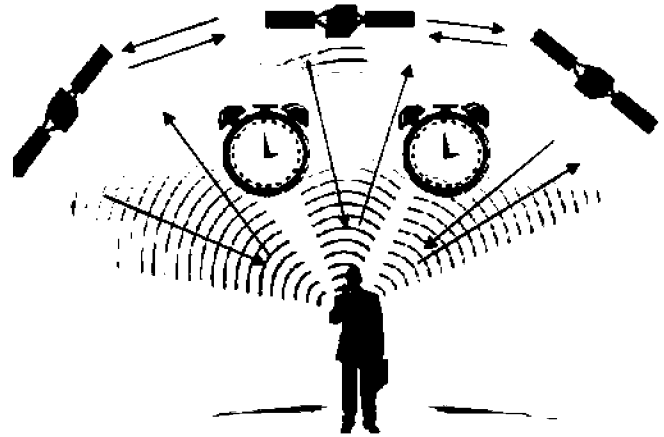


Fig. 1 Esquema de localització per satèl·lit

### B. Localització per la xarxa de telefonia mòbil

Quan un dispositiu es connecta a una estació base (BTS) de la xarxa de telefonia mòbil la seva posició queda definida dins el radi de cobertura d'aquesta estació. Si aquest radi és molt gran la precisió de la localització serà baixa. Per millorar la precisió es calcula la distància a altres BTS a partir de la potència dels senyals que arriben al dispositiu. Una vegada conegudes aquestes distàncies s'utilitzen tècniques de triangulació per determinar la posició del dispositiu.

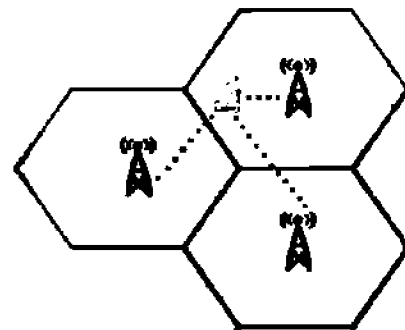


Fig. 2 Esquema de localització per la xarxa de telefonia mòbil

### C. Localització per xarxes sense fils de petit abast

Actualment els senyals dels satèl·lits no es poden utilitzar en entorns d'interior perquè no sempre són suficientment potents per travessar els obstacles que impedeixen la visió directa entre satèl·lit i dispositiu. D'altra banda els sistemes de localització per la xarxa de telefonia mòbil ofereixen una precisió insuficient per entorns d'interior. Per tant, és necessari utilitzar tecnologies sense fils alternatives que siguin eficients i ofereixin cobertura i precisió en aquest tipus d'entorns. Les tecnologies RFID, Bluetooth i Wi-Fi, entre d'altres, són xarxes sense fils de petit abast que compleixen aquests requeriments.

En aquest tipus de localització hi ha tres elements bàsics:

- Una etiqueta o tag al dispositiu a localitzar.
- Punts d'accés (AP) situats en punts de referència.
- Una aplicació software que calcula la posició de l'etiqueta a partir de la informació rebuda dels punts d'accés.

Cada punt d'accés calcula la distància al dispositiu a partir de la potència dels senyals que rep d'aquest. Amb la informació de tres o quatre punts d'accés, l'aplicació software és capaç de calcular la posició, en un determinat mapa carregat prèviament i sobre el que s'ha realitzat un estudi de cobertura. També s'ha de conèixer prèviament la ubicació de tots els punts d'accés que formen el sistema. La Figura 3 mostra aquest funcionament.

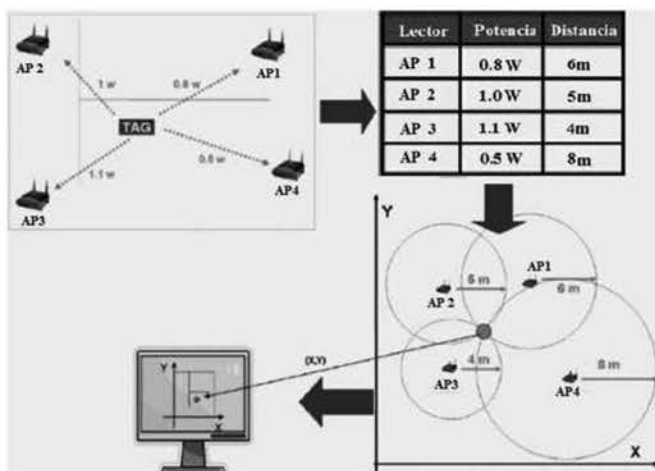


Fig. 3 Esquema de localització per xarxes sense fils de petit abast

### D. Localització per l'adreça IP

Aquest sistema es basa en la utilització de bases de dades on es guarden les assignacions de les adreces IP als proveïdors de Internet i la seva distribució geogràfica. És el sistema amb menys precisió, ens proporciona la localització del dispositiu en una zona geogràfica, però no la posició concreta on es troba.

## III. APLICACIONS I SERVEIS BASATS EN LA LOCALITZACIÓ

Les aplicacions pràctiques de la geolocalització són molt variades. Les seves funcionalitats van des de la cerca d'una estació de servei propera, fins a l'obtenció de rutes de navegació en cotxe amb informació del tràfic en temps real, passant per aplicacions tan noves com les de realitat augmentada.

A continuació es fa una descripció d'algunes de les aplicacions més populars:

### A. Mapes

En aquest conjunt trobam aquelles aplicacions destinades a la cerca d'informació a mapes. La posició geogràfica de l'usuari és un element important en la cerca d'aquest tipus d'informació.

Els serveis típics que ofereixen aquestes aplicacions són la consulta de diversos tipus de mapes (geogràfics, físics o de carrers), el càlcul de rutes o la creació de mapes personalitzats.

Alguns exemples d'aplicacions de mapes són:

- Google Maps: probablement el servei de mapes més popular.
- Google Earth: combina les funcionalitats de diversos serveis amb recreacions en 3D de la superfície de la Terra, la Lluna i Mart.
- MyTracks: aplicació Android que permet gravar recorreguts geolocalitzats i integrar-los a les xarxes socials.

### B. Navegació GPS

En aquest conjunt es troben les aplicacions destinades a la navegació fent ús d'un dispositiu GPS.

Alguns exemples d'aplicacions de navegació GPS són:

- Tom Tom Navigator: És el navegador més utilitzat, funciona sobre plataformes hardware pròpies i també en dispositius mòbils.
- Google Maps Navigation: Navegador GPS de Google que integra mapes i funcionalitats del servei Google Maps i ofereix informació del tràfic en temps real.
- Waze: Sistema de navegació GPS que incorpora informació del tràfic i d'incidències a la carretera. Disponible per iOS, Android, Windows Mobile i Symbian.

### C. Xarxes socials i geosocials

En els darrers anys les xarxes socials han integrat la geolocalització entre els seus serveis, de manera que els usuaris poden publicar i compartir la seva posició en qualsevol moment. Alguns exemples són les aplicacions "Facebook Places", "Twitter Places" o "Tuenti Sitios".

A més, recentment han sorgit les xarxes geosocials que es basen en la geolocalització. Permeten als usuaris compartir la seva posició, valorar els llocs que visiten, consultar les valoracions d'altres usuaris i accedir a la informació d'interès del seu entorn com llocs més turístics, tendes amb descomptes

o restaurants afins als seus gustos. També permeten als comerciants i les marques captar i fidelitzar clients, oferint promocions a aquells usuaris que facin “check-in” en els seus establiments o als que comparteixin la seva opinió sobre els seus productes.

Els exemples més importants són:

- Foursquare: És la xarxa geosocial amb més expansió, actualment té més de 8 milions d'usuaris a tot el món. Els usuaris poden fer “check-in” per compartir la seva ubicació i amb aquesta informació participar a jocs socials, promocions i altres esdeveniments. Grans empreses com “Starbucks”, “H&M” o “McDonald’s” aprofiten aquesta xarxa per oferir descomptes i captar clients. També la Universitat de Harvard utilitza Foursquare per oferir rutes pels llocs més emblemàtics del campus.
- Gowalla: El seu funcionament bàsic és molt similar al de Foursquare. Afegeix una línia temporal dels “check-in” dels teus amics i permet escriure comentaris en cada un d'ells.
- Google Latitude: És un servei de geolocalització per dispositius mòbils. Aquesta aplicació es troba integrada en la majoria de serveis de Google.

Aquest tipus d'aplicacions són les que presenten una major difusió dins l'àmbit de la geolocalització en dispositius mòbils.

*D. Realitat augmentada*

Les aplicacions de realitat augmentada permeten a l'usuari combinar informació extreta d'Internet amb la seva visió del món real. Es basen en determinar la posició de l'usuari i la direcció en la que està mirant a través dels sistemes de posicionament i a sensors de moviment i orientació. Mentre l'usuari captura la imatge del món real a través de la càmera del dispositiu, l'aplicació afegeix a la pantalla la informació obtinguda a Internet.



Fig. 4 Aplicació de realitat augmentada

Layar és una aplicació de realitat augmentada per smartphones que permet carregar diferents capes de contingut. Les capes més conegudes són la que permet localitzar cases en venda o la que mostra els Tweets (de Twitter) geoposicionats al nostre entorn mostrant la imatge de l'usuari i el tweet enviat. A Espanya destaquen les capes de idealista.com, metro de Barcelona i una guia turística de l'Alhambra.

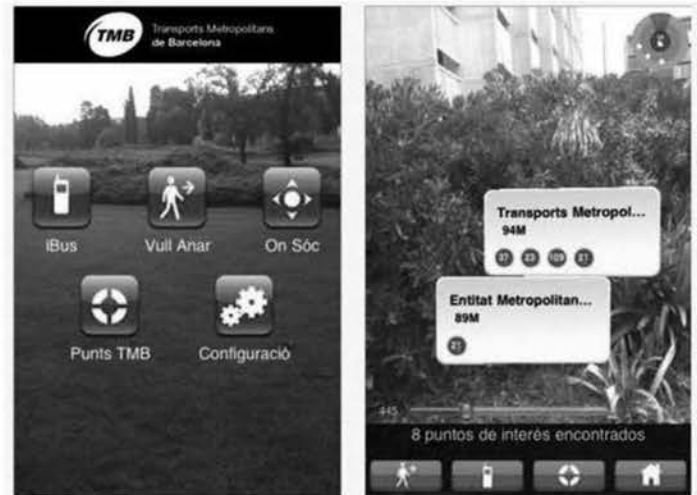


Fig. 5 Aplicació de realitat augmentada pel transport públic de Barcelona

*E. Altres aplicacions*

Actualment moltes empreses tenen aplicacions que mostren on es troben els seus establiments més propers a la nostra ubicació. Un exemple és el servei mòbil de cerca d'oficines i caixers de “La Caixa” que va ser una de les primeres entitats financeres en aplicar aquesta tecnologia.



Fig. 6 Aplicació de “la Caixa” que mostra les oficines més properes a la posició de l'usuari.

També alguns ajuntaments ofereixen aplicacions que mostren informació d'interès públic com on es troba el centre de salut o la comissaria més propera a la nostra posició i ens indiquen la ruta més ràpida.

Existeixen moltes altres aplicacions: des de les que permeten monitoritzar pacients amb problemes i controlar on es troben, fins les aplicacions de consulta del temps d'espera de l'autobús, la localització d'emergències o localització de vehicles robats.

#### IV. PRIVACITAT

Les dades que manegen les aplicacions sobre la localització d'un usuari son especialment sensibles ja que afecten a la seva privacitat. Pot ser perillós que no existeixi una restricció a l'àmbit en que aquestes dades estaran disponibles, sobretot en el cas de que aquesta informació s'integri a les xarxes socials amb altres dades personals.

El fet de que qualsevol persona pugui conèixer la posició d'un usuari en tot moment implica riscos com robatori de dades o robatori físic i pot derivar en la creació de perfils que es podrien utilitzar per estudis de mercat o enviament de publicitat.

A més, és important configurar correctament aquelles aplicacions que permeten que terceres persones ens etiquetin a una localització de forma que no és pugui publicar la nostra posició sense el nostre consentiment.

Els problemes més greus de privacitat solen estar causats per el tractament irresponsable de les dades per part de les empreses. Per això és important que les empreses que ofereixin aquests serveis tinguin una política de privacitat estricta, que ha de ser respectada en tot moment.

A continuació es fan recomanacions que cal seguir per fer un ús segur i responsable dels serveis de geolocalització:

- Llegir sempre les clàusules sobre la privacitat i configurar correctament els serveis de geolocalització i les xarxes socials.
- Restringir la informació que s'ofereix de forma pública.
- Adequar la precisió de les publicacions sobre la localització.
- Evitar anunciar localitzacions o desplaçaments habituals.

#### V. CONCLUSIONS

Les aplicacions de geolocalització i els serveis basats en localització es poden convertir en una excel·lent font d'informació sempre que es faci un ús responsable. El problema de la privacitat pot ser un obstacle important al que s'han d'enfrontar totes les empreses que vulguin fer-ne ús. Els usuaris han de poder elegir quan volen activar aquestes aplicacions i restringir l'àmbit de les seves publicacions.

El nombre d'usuaris que utilitzen aquestes aplicacions encara es petit però augmenta cada dia, gràcies a la gran expansió que tenen els smartphones. El caràcter social de moltes d'aquestes aplicacions i la possibilitat d'oferir ofertes personalitzades suposa una gran oportunitat de negoci no tan sols per grans empreses sinó també per a petits comerços, que es podran aprofitar del gran potencial per captar i fidelitzar clients a través de promocions o descomptes.

S'espera que en un futur pròxim també augmentin les aplicacions que ofereixen informació i serveis locals per part dels ajuntaments de manera que la geolocalització sigui utilitzada a la vida diària per trobar qualsevol tipus d'informació que pugui ser d'interès pels usuaris.

#### REFERÈNCIES

*Sistemas de localización e información geográfica. Observatorio regional de la Sociedad de la Información. Consejería de Fomento. Junta de Castilla y León:* [http://issuu.com/orsicyl/docs/localizacion\\_geografica?mode=a\\_p](http://issuu.com/orsicyl/docs/localizacion_geografica?mode=a_p)

*Guía sobre seguridad y privacidad de las herramientas de geolocalización. Observatorio ITECO*

<http://www.foursquare.com/>

<http://www.realidadaugmentada-fundaciontelefonica.com/page-llip:pagellip.html>

Assignatura: Serveis Telemàtics

Professor : Magdalena Payeras-Capellà



Cristina Rodríguez Aguado  
Estudiant d'Enginyeria Tècnica en  
Telecomunicacions, especialitat  
Telemàtica. Actualment realitzant el  
projecte final de carrera.

# Codi per a Recorre un Laberint

Pedro Barea Jaume, Javier González Maimó.

*Enginyeria Tècnica de Telecomunicacions, Especialitat en Telemàtica*

*pedro\_barea@hotmail.com, javig181@gmail.com*

**Resum**— Aquest article és el resum de la implementació d'un codi que permeti a un vehicle recorre un laberint. El desplaçament ha de ser des d'un punt inicial a un punt final d'arribada. La trajectòria del vehicle l'ha d'assegurar la lectura de tres sensors de llum infraroja a la part davantera del vehicle (amb l'objectiu de poder detectar obstacles) i uns altres dos a la part inferior del vehicle (amb l'objectiu de poder detectar l'arribada al punt final).

gir, ja que havíem d'aconseguir calibrar els dos motors per aconseguir un gir òptim.

Per això hem hagut d'implementar funcions per rectificar continuament la direcció del cotxe calculant la distància amb els sensors i realitzant les operacions pertinents. a més, d'haver d'implementar les funcions de gir corresponents a l'esquerra i la dreta dependent d'on vulgui girar el cotxe.

Per poder realitzar aquestes funcions i que es pugui resoldre el laberint s'han de tenir en compte:

- A. *Els sensors infrarojos*: el vehicle conté cinc sensors: tres superiors per poder detectar les parets i obstacles (n'hi ha tant a l'esquerra, la dreta, com en el centre), i dos sensors inferiors per poder detectar el final del laberint detectant en el nostre cas un canvi de color.
- B. *Els motors continus*: el vehicle conté dos motors, els quals, es poden regular les velocitats a partir de la modulació d'un senyal quadrat PWM (això es realitza des del PIC).
- C. *Conversor A/D*: Permet la lectura del valor dels sensors infrarojos, per tal de conèixer si el vehicle està aprop d'un obstacle o lluny i poder decidir l'acció que hem de realitzar (Aquesta conversió es fa totalment des del PIC).

## I. INTRODUCCIÓ

Aquesta pràctica consisteix en programar un vehicle que sigui capaç de seguir el camí d'un laberint amb l'ajuda d'uns sensors de llum infraroja.

El laberint és desconegut per nosaltres però per realitzar proves hem utilitzat el circuit de la Figura 1 que es va resoldre l'any passat, ja que les característiques d'aquest son parecudes al del laberint que hem d'aconseguir resoldre [3]. El laberint compleix les següents característiques: El color de les parets és blanc per a permetre la reflexió de la llum i el terra del circuit és tot de color negre, excepte el punt d'arribada que és de color blanc per poder detectar els sensors inferiors del cotxe el punt d'arribada i fer que l'aturi.



Figura 1 Esquema del laberint de proves

Per fer que el cotxe sigui capaç d'arribar a l'arribada hem d'aconseguir evitar les col·lisions amb les parets del circuit i que aconseguixi fer tots els girs de forma efectiva. Per tant, hem de solucionar problemes com la variació dels dos motors que provoquen la col·lisió amb les parets i a més els problemes de

El model del vehicle que emprarem és un prototipus "Formula Flowcode" controlat per un microcontrolador PIC16F876 com es mostra a la Figura 2.

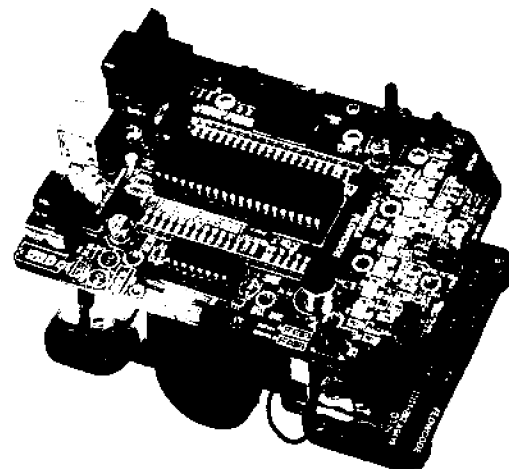


Figura 2 Vehicle "Formula Flowcode"



El projecte es divideix en tres parts:

*1a- Lectura dels sensors infrarojos:* Els senyals que rebem dels sensors son analògiques, per tant s'han de convertir a digital per poder ser tractades, per tant, es passen al convertidor A/D del microcontrolador[1] i es tradueix el valor binari que indica la proximitat o la llunyania d'un obstacle.

*2a- Moviment amb els motors:* El control d'aquest tipus de motors es realitza per la generació de senyals PWM, per tant hem d'implementar aquest controls dels motors mitjançant el perifèric inclòs en el microcontrolador anomenat CCP (Capture /Compare /PWMmodule)[1], que és capaç de generar aquest tipus de senyals.

*3a- Resolució del laberint:* En aquest pas, ja tenint el valor de la distància dels sensors i havent definit el valor dels motors podem decidir cap on anem, si endavant, o a l'esquerra o la dreta i veure si en el cas d'anar recte hem de corregir molt o poc la distància de les parets.

## II. CONNEXIÓ AMB EL HARDWARE

Per a poder emprar el vehicle hem utilitzat el microcontrolador PIC16F876 de la marca Microchip. Es tracta d'un microcontrolador de 8 bits, de memòria flash, amb 14 KB de memòria de programa i 368 B de RAM. Aquest pic disposa d'un conjunt de 35 instruccions i 28 pins[2].

El senyals analògics del grup de sensors superiors arriben al microcontrolador PIC a través dels pins RA1, RA3 i RA5 del PORTA. Mentre que el grup de sensors inferiors es connecten a les entrades RB5 i RB4 del PORTB[2]. Els sensors superiors requereixen de la conversió analògica/digital per a poder disposar d'informació referent a la distància dels obstacles, mentre que als sensors inferiors no és necessari ja que només es pot tenir dos valors diferents (referents al color del terra, que pot ser blanc o negre). La gestió del grup de sensors superiors es realitza posant a "1" els pins RA0, RA2 i RA4 del PORTA, de forma que els sensors queden actius. El grup de sensors inferiors no tenen aquesta possibilitat i sempre es troben encesos.

Els senyals de control corresponents als motors es connectaran als pins RC1 i RC2 per donar-los potència, mentre que els pins RC0 i RC3 seran els encarregats de donar el sentit de gir del cada un dels motors. Aquests pins es troben connectats al PORTC[2].

També hem de dir que degut a problemes amb la sortida RA4, que no es podia configurar per activar el sensor dret hem hagut de fer una connexió especial per què RA4 pogués utilitzar el mateix canal que RA2.

A la Taula 1 es poden veure les diferents decisions de moviments a triar dependents del estats dels sensors. Els valors "0" o "1" que hi apareixen representen els valors dels sensors segons la distància límit de proximitat. Així si el valor és 1 indica que hi ha un obstacle proper, mentre que el 0 indica que no hi ha obstacle o aquest està més lluny que la distància límit.

Sensor esquerra	Sensor central	Sensor dreta	DECISIÓ
0	0	0	Endavant
0	0	1	Endavant
0	1	0	Endavant
0	1	1	Gir esquerra
1	0	0	Endavant
1	0	1	Endavant
1	1	0	Gir dreta
1	1	1	Endavant

Taula 1 Decisió del vehicle segons els valors dels sensors

Aquesta taula és imprescindible per a la decisió del cotxe, ja que sense ella no seria capaç d'elegir un moviment correcte. Un altre element important a l'hora de determinar el funcionament d'aquesta metodologia és el valor límit elegit per fer binària la resposta dels sensors, que s'ha triat segons la sensibilitat del sensor.

## III. IMPLEMENTACIÓ SOFTWARE

Mostrat gràficament a la figura 3

Primer de tot fem les inicialitzacions corresponents per poder gestionar els sensors i els moviments del vehicle a partir del PIC que serà programat.

S'activen els sensors i es configuren com entrades analògiques (tant el PORTA per sensors superiors, com el PORTB per els sensors inferiors) i es generen les senyals que implementen els motors mitjançant el PORTC.

El primer que fa el codi és comprovar l'estat dels sensors (si està prop o lluny de la paret i si hi ha obstacles a davant el vehicle) i també els sensors inferiors per detectar l'arribada i decidirà a partir de la taula de decisió (figurada) cap a on anirà. Aquest procediment es realitza de la següent manera: El sensor envia una senyal analògica que es processada per el PIC mitjançant el convertidor A/D[1]. Quan tenim el valor fem una resta d'un límit que hem posat al sensor per agafar el bit de *carry* que ens queda d'aquesta operació. Segons sigui 0 o 1

emmagatzemem dins una variable DISTANCIA (vector de 8 bits) un 0 o 1 per tal de veure si el sensor està prop o lluny de la paret. Això es fa per cada sensor al principi de cada cicle, per tant es realitzarà cada vegada i a cada sensor es ficarà aquest bit a una posició diferent de DISTANCIA (posició 2 per el sensor esquerre, posició 1 per el sensor central i posició 0 per el sensor de la dreta). com es mostra al fragment 1.

```

Sensor_central
    movlw    b'10011001'
    movwf   ADCON0
    call    estatsen
    movwf   SENCENTRAL

discen
    movlw   .14
    subwf  SENCENTRAL,w
    btfss  STATUS,C
    goto   discena
discenll
    bcf    DISTANCIA,1
    goto  Sensor_dreta
discena
    bsf    DISTANCIA,1
    
```

Fragment 1 Tractament del sensor central

```

Decisio
    movf   DISTANCIA,w
    addwf  PCL,F
    goto  endavant
    goto  endavant
    goto  endavant
    goto  esquerra
    goto  endavant
    goto  endavant
    goto  dreta
    goto  endavant
    
```

Fragment 2 Decisió després de consultar la taula

Després es llegeix el valor de la taula de decisió i segons el valor del vector DISTANCIA triam una decisió(endavant, esquerra o dreta)[1]. Això es pot comprovar al Fragment 2.

- Endavant: Es realitza operacions de rectificar tant a l'esquerra com a la dreta ja que no podem assegurar que el vehicle vagi recte, per tant el vehicle anirà corregint continuament la seva situació fent una resta dels valors del sensor esquerra menys el sensor dret, i segons el resultat d'aquesta resta decidim si rectifiquem a l'esquerra o la dreta.

```

endavant
    movf   SENDRETA,w
    subwf  SENESQUERRE,w
    btfsc  STATUS,C
    goto  esquerra_rect
    
```

Fragment 3 Implementació funció endavant

- Esquerra: per implementar aquesta funció hem de configurar un motor perquè vagi cap endavant i l'altre que vagi cap enrere. això és degut a que cada motor utilitza el nivell alt i

baix de la senyal PWM(Fragment 4).

```

esquerra
    bcf    PORTC,0
    bsf    PORTC,3
    movlw  .45
    movwf  CCPR2L
    movlw  .12
    movwf  CCPRL1
    goto  Cicle
    
```

Fragment 4 Implementació funció esquerra

- Dreta: per implementar aquesta funció hem de fer el mateix que la funció esquerra però realitzant-la amb el motor invers al de l'anterior Funció (Fragment 5).

```

dreta
    bsf    PORTC,0
    bcf    PORTC,3
    movlw  .12
    movwf  CCPR2L
    movlw  .45
    movwf  CCPRL1
    goto  Cicle
    
```

Fragment 5 Implementació funció dreta

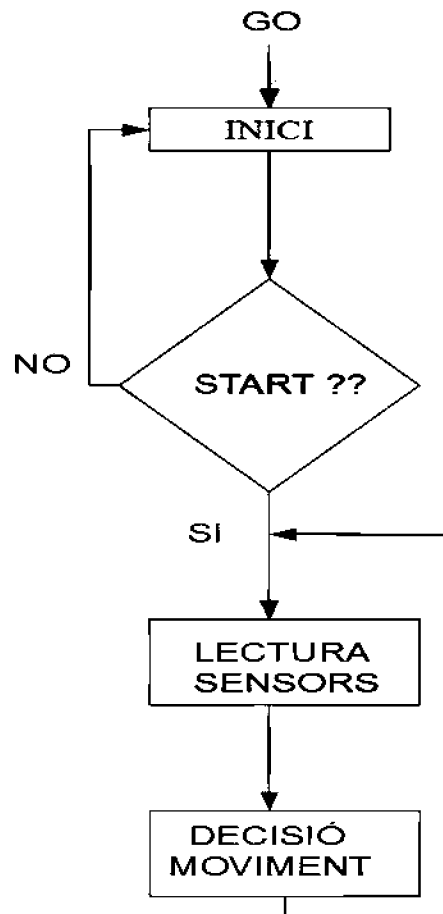


Figura 3 Diagrama de fluxe del codi

#### IV. AGRAÏMENTS

Volem agrair a tots els nostres companys l'ajuda que ens han proporcionat i als professors, per els dubtes que ens han resolt, que no han estat pocs.

#### V. CONCLUSIONS

Amb aquesta pràctica hem pogut observar el funcionament dels sensors i el seu tractament per aconseguir que el vehicle resolgui un laberint, tot això aplicant els coneixements que hem après a l'assignatura de la qual aquest n'era el projecte final com, el tractament dels sensors i l'implementació del codi que ha estat escrit en llenguatge ensamblador.

També hem pogut veure el funcionament de un PIC microcontrolador, el qual, tot s'ha de dir, ens ha dut una sèrie de contratemps que al final s'han solucionat amb ajuda de companys i professors.

#### REFERÈNCIES

- [1] Microchip PIC16F876 Data Sheet.
- [2] Apunts de l'assignatura de Microordinadors, de 2n de telemàtica. Tomeu Alorda, UIB.
- [3] Revista Enginy@eps, número 2. Any 2010, Treballs Docents curs 2009/2010, *Proposta d'un Codi per a Recorre un Laberint Conegut*, Caterina Amengual Caldentey, Juan Marcos Calafat Alhama, pàgs. 67/70.

Assignatura Microordinadors de segon curs impartida per: Bartomeu Alorda, Pere Pons.



Pedro Barea Jaume  
Batxillerat cursat al IES Na Camel·la (Manacor), actualment cursant Enginyeria Tècnica en Telecomunicació, especialitat en Telemàtica a la UIB



Javier González Maimó.  
Batxillerat cursat al IES Berenguer d'Anoia (Inca) , actualment cursant Enginyeria Tècnica en Telecomunicació, especialitat en Telemàtica a la UIB.





# Paraules $k$ -completes

Enric Gago Hobel, Pedro Francisco Agredano Amengual, Iván Núñez Fuster

*Assignatura de Models Matemàtics en l'Educació Secundària, Llicenciatura de Matemàtiques*

**Abstract**—Amb aquest article es pretén apropar al lector sobre la utilitat de les paraules  $k$ -completes de manera que es pugui fer una idea general de què són i fins i tot com obtenir de forma senzilla una paraula completa de tamany  $k$  amb  $k$  arbitrari.

## I. INTRODUCCIÓ

QUALQUE vegada ens haurem demanat com podem calcular la distància entre la Terra i un altre planeta, doncs una manera de fer-ho és mitjançant l'emissió d'un senyal en la direcció d'aquest planeta de manera que el que mesuram és el temps que triga aquest senyal a retornar rebotat. Ara bé, hem de ser capaços de detectar-lo a la tornada i no confondre'l, per exemple, amb soroll. Però, de quin tipus de senyals estam parlant? Estam parlant d'una seqüència d'estímuls que s'emeten amb una certa freqüència, separats per espais de temps. Aquests senyals els podem representar per bits, on l'1 indica que s'ha emès el senyal i el 0 que no, és a dir, un dels espais de temps en que no s'ha emès res. Aquestes representacions per bits són el que anomenam paraules binàries (paraules on les lletres són 0's i 1's). De totes maneres, tampoc no podem emetre una paraula qualsevulla ja que a l'hora de rebre-la de nou pot ocasionar confusió.

## II. PETITS EXEMPLES

Si enviam per exemple el senyal

01100101011

la idea és rebre exactament el mateix senyal o qualque cosa semblant, el problema és que si rebem

00111101110111

a causa del soroll no sabem exactament quan començam a rebre el nostre senyal i per tant no podrem determinar amb precisió quan el rebrem. Per evitar aquest problema i poder rebre el senyal igualment es varen inventar les paraules  $k$ -completes. Les paraules  $k$ -completes són paraules que no contenen cap subparaula de longitud  $k$  repetida. D'aquesta manera se soluciona el problema anterior perquè quan detectem de nou el senyal, a partir del bocí que recuperem podrem saber quant temps fa que va ser emès ja que aquests bocins de longitud  $k$  de la paraula són únics, no es repeteixen, i per tant podrem saber quan s'emeteren i a partir d'aquí determinar la distància cercada.

Facem un poc de pràctica, si consideram la paraula

1001

les seves subparaules de longitud 2 són, per ordre, 10, 00 i 01, que són totes diferents. Ara bé, no és una paraula 2-completa perquè no conté totes les subparaules de longitud dos, faltaria l'11. Podem determinar d'una manera intuïtiva la longitud d'una paraula 2-completa. El nombre màxim de paraules binàries diferents de longitud dos són 4: 00, 01, 10, 11. Si consideram la següent paraula, sí és 2-completa

10011

Ara bé, de longitud més gran que 5 és impossible ja que si tenim una paraula 2-completa de longitud 6 per exemple, serà de la forma

*abcdef*

on totes les subparaules de longitud dos són *ab, bc, cd, de, ef* i òbviament, com només n'hi ha quatre diferents, alguna de les anteriors es repetiran i per tant no podrà ser una paraula 2-completa. Si no n'hi ha de longitud 6 tampoc no n'hi haurà d'una longitud superior.

Estudiam ara un poquet les paraules 3-completes, un exemple d'una paraula on totes les subparaules de longitud tres són diferents és

100110

110, 001, 011, 110 són diferents. El nombre màxim de paraules binàries de longitud 3 és 8 ( $2^3$ ), que són

000 001 010 100  
011 101 110 111

Si consideram la paraula 3-completa

1110001011

veim que té 8 subparaules de longitud 3 diferents, és a dir, el màxim possible, i per tant no hi pot haver una amb més dígits perquè si no es repetirien algunes subparaules i ja no seria 3-completa, és a dir, les paraules 3-completes són de 10 dígits.

En general, quina és la longitud d'una paraula  $k$ -completa? Veient els exemples anteriors el raonament és molt senzill. En total hi ha  $2^k$  paraules binàries diferents de longitud  $k$  i per ser paraula  $k$ -completa les haurà de contenir totes aquestes de forma seqüencial, ara bé, quants dígits té aquesta paraula? Hem de tenir en compte que aquestes  $2^k$  subparaules estan "incloses" unes dins les altres, és a dir, del primer dígit al  $k$ -èssim és una subparaula, del segon al  $(k + 1)$ -èssim una altra diferent i així  $2^k$  vegades, és a dir, a partir de la  $k$ -èssima posició només afegim un dígit fins a  $2^k$  vegades,

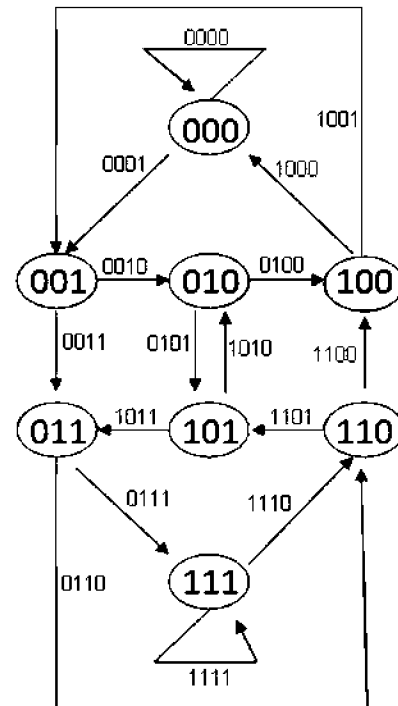
per tant, podem deduir que en total hi ha  $2^k + k - 1$  dígit.

D'aquesta manera, la longitud màxima d'una paraula 50-completa és de  $2^{50} + 50 - 1 = 1125899906842673$  dígit. Tal vegada no ens hem fixat degut a que els exemples anteriors no són massa grans però se satisfà que a les paraules  $k$ -completes els primers  $k - 1$  i darrers  $k - 1$  dígit coincideixen. A l'exemple anterior, **1110001011**.

### III. CONSTRUCCIÓ DE PARAULES $k$ -COMPLETES

Trobar paraules 2-completes i 3-completes no ha estat gaire complicat, ara bé, a mesura que  $k$  augmenta no és tan trivial trobar aquestes paraules. Per fer-ho ens ajudarem de la construcció d'un graf dirigit de manera que els nodes representin totes les paraules binàries de longitud  $k - 1$  i els arcs representin totes les paraules binàries de longitud  $k$ , de tal manera que una paraula  $k$ -completa correspongui a un circuit eulerià, és a dir, que recorre tots els arcs exactament una vegada d'aquest graf. La idea serà la següent, de cada node, que és una paraula de longitud  $k - 1$ , en sortiran dos arcs dirigits, aquests dos arcs seran les paraules que corresponen d'afegir un 0 o un 1 a la dreta del node del qual surten obtenint així una paraula binària de longitud  $k$  i es dirigiran a aquells nodes que coincideixin amb els darrers  $k - 1$  dígit de l'aresta (dit d'una altra manera, llevam el primer dígit de l'aresta i miram a quin node correspon). Per exemple, si estam a  $k = 3$ , aleshores del node 10 sortiran les arestes 100 i 101, la primera es dirigirà al node 00 i la segona al node 01.

Amb la construcció d'aquests grafs es pot construir d'una manera molt visual diferents paraules  $k$ -completes de manera molt senzilla, per exemple, ens demanam construir paraules 4-completes i 5-completes. Construïrem només el graf per a  $k = 4$ , el graf és el següent



Ara només ens hem de situar a un node i recórrer cada arc una i només una vegada. Per exemple, una paraula 4-completa que comenci amb el node 000 seria

0000111101011001000

Si començam en el vèrtex 110, obtenim per exemple,

1100001001111010110

Per a construir una paraula 5-completa s'hauria de fer la construcció del graf corresponent, després, una vegada fet ja és molt fàcil, un exemple de paraula 5-completa és

111100000100011010011101100101011111

Fins aquí hem donat un mètode per trobar paraules  $k$ -completes mitjançant la construcció de grafs com ja s'ha dit abans, ara bé, aquests grafs sempre admeten un circuit eulerià? Ja que en cas contrari no sempre podrem fer ús d'aquest mètode. La resposta és afirmativa, de fet existeix un teorema que ho corrobora, és el següent

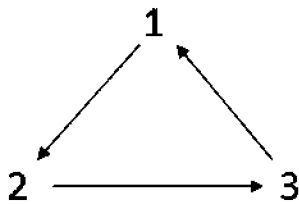
*Un graf dirigit té un circuit eulerià si i només si és connex i tots els seus nodes tenen el mateix grau de sortida que d'arribada.*

Òbviament, els nostres grafs són d'aquest estil ja que si no no tindria sentit parlar-ne d'aquest teorema.

Hem de provar les dues implicacions, la implicació cap a la dreta és més fàcil, de fet ho provarem per contrarecproc. Vegem-ho. Volem provar que si un graf no és connex o els seus nodes no tenen el mateix grau de sortida que d'arribada aleshores el graf en qüestió no és eulerià. Si el graf no és

connex òbviament no serà eulerià ja que existiran dos nodes que no es podran unir mitjançant una trajectòria sense repetir els arcs. Per altra banda, si existeix qualche node tal que el grau de sortida sigui diferent al grau d'entrada aleshores tampoc es podrà recórrer tots els arcs, per exemple, si en un node el grau de sortida és superior al grau d'entrada hi hauran sortides que no es poden recórrer i per tant no és eulerià.

Vegem ara l'altra implicació, que si un graf és connex i tots els seus nodes tenen el mateix grau de sortida que d'arribada aleshores té un circuit eulerià. Per demostrar-ho farem inducció sobre el nombre d'arcs. Vegem que per a 3 arcs és cert. Un graf dirigit que sigui connex, amb tres arcs i que el grau d'entrada a cada node sigui igual al de sortida ha de ser de la forma



que efectivament té un circuit eulerià, és  $C = (1, 2, 3, 1)$ . Suposem ara que la propietat també és certa si el nombre de arcs és  $3, 4, \dots, k - 1$ . Vegem que també és certa si el nombre d'arcs és  $k$ . La idea és construir un graf eulerià amb la hipòtesi d'inducció. El que fem és cercar un circuit qualsevol en  $G$ , suposem que hem començat en un vèrtex  $v_1$  i formem un circuit  $C_1$  que acabi en  $v_1$ , si aquest circuit ha passat per tots els vèrtexos aleshores ja hem acabat, en cas contrari el que fem serà suprimir els arcs emprats al circuit  $C_1$ . Ara s'hauran creat una o més components connexes en  $G$  i cada una satisfà que el nombre d'arcs és menor que  $k$ , i com  $G$  satisfà les hipòtesis d'inducció aleshores cada component connexa és euleriana. Ara hem d'unir-los de tal manera que aquesta unió sigui un circuit eulerià però això és molt fàcil, només hem de començar en un dels vèrtexos on s'uncixen dues o més de les components connexes i recórrer el graf com la unió de les components.

D'aquesta manera ens asseguram de que donat qualsevol  $k \geq 3$  existeixen paraules  $k$ -completes, ja que el graf que hem definit abans sempre és construïble i com acabam de demostrar que sempre podrem trobar un circuit eulerià aleshores sempre hi haurà paraules  $k$ -completes. Per a  $k = 1, 2$  també, ja que les paraules 01, 10 són 1-completes i de 2-completes ja les hem vistes abans, per tant podem concloure que per tot  $k \geq 1$  existeixen paraules  $k$ -completes.

# Visualització de un Sistema de Control en “LabView”

Antonio Nadal Mir, Álvaro Sáiz Montoro

Tercer curs d'Ingenieria Tècnica Industrial, Especialitzat en Electrònica Industrial

**Resum**—A partir d'un sistema de control per un dipòsit d'aigua implementat per al bus CAN es procedirà a visualitzar els resultats obtinguts a un PC mitjançant el port sèrie d'aquest i el software "LabView". Aquest sistema permet controlar el nivell del dipòsit obrint i tancant vàlvules de entrada i sortida, a més compta amb un sensor de temperatura i un altre de nivell, i una consigna que permet obtenir el nivell desitjat del dipòsit. El funcionament del sistema de control està explicat mes detalladament a l'article publicat a l'Enginy del 2010. En aquest article ens centrarem en com millorar l'aspecte visual a l'hora de visualitzar dades.

## I. INTRODUCCIÓ

Disposa'm d'un sistema de control on el controlador, els sensors i els actuadors estan connectats entre ells amb un bus tipus CAN i un sistema d'adquisició de dades que rep la informació a través del port sèrie del PC.

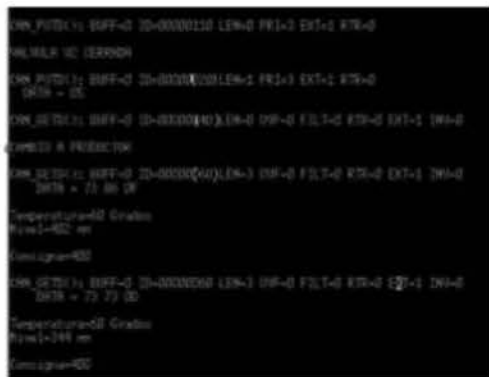


Fig. 1 Interficie RS-232

Normalment els missatges es mostren per l'interficie RS-232 (figura 1), però mitjançant un arxiu VI, ens permetrà visualitzar l'estat del sistema d'una forma més còmoda y natural. Com es pot observar, comparant la figura 1 y la figura 3, passem de rebre l'informació en forma de text a una forma molt mes comprensible i simple.

## II. SISTEMA DE CONTROL SOBRE CAN

El sistema de control haurà de regular el nivell d'un dipòsit obrint i tancant dues vàlvules. La primera vàlvula (V1) s'utilitza per buidar el dipòsit, i la segona (V2) per emplenar el dipòsit. L'usuari podrà triar entre quatre diferents nivells de consigna mitjançant un potenciòmetre de la placa, per triar el nivell desitjat del dipòsit. El sistema està format per tres nodes A, B i C connectats entre ells per un bus de tipus CAN. Dins del conjunt cada node conté les següents parts i funcions.

### A. Node A

El node A es troba connectat a tres dispositius: un sensor de temperatura (T), un sensor de nivell (N) i una vàlvula d'entrada (V2). La funció d'aquest node és captar dades dels sensors i enviar aquestes dades pel bus CAN.

### B. Node B

Aquest node executa l'algorisme de control pròpiament dit. La seva funció principal és monitoritzar els valors de nivell proporcionats pel node A i enviar ordres per obrir o tancar la vàlvula V2, en funció del nivell actual.

### C. Node C

Controla la vàlvula de sortida (V1).

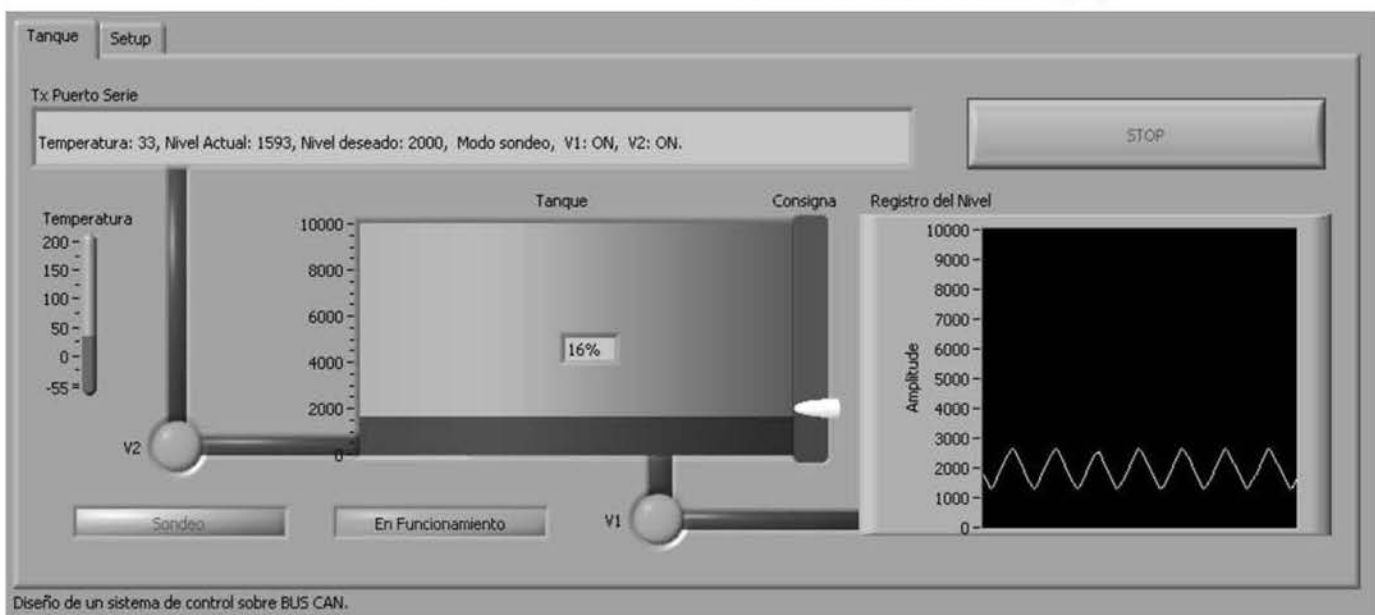


Fig. 3 Panell frontal

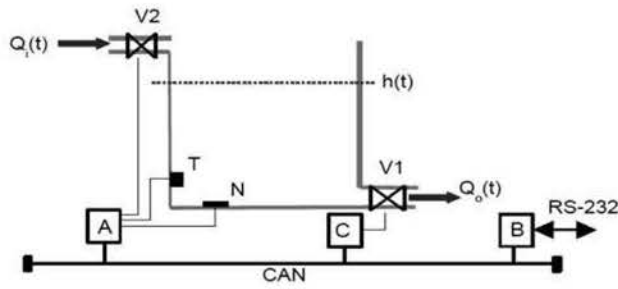


Fig. 2 Esquema del sistema

I. PANELL FRONTAL

El "LabView" és un programa que ens permet treballar amb sistemes d'adquisició de dades, el qual ens permet llegir la informació del bus mitjançant el port sèrie i ens permet visualitzar-la de forma més senzilla.

El panell frontal representa l'estat del dipòsit. En la cantonada superior esquerra s'observen dues pestanyes. La segona pestanya ens permet configurar el port per a la lectura de les dades. Just sota troba'm el missatge que es transmet pel bus CAN i a la dreta d'aquest un botó per finalitzar la visualització.

El termòmetre situat a l'esquerra de la imatge representa la temperatura del dipòsit. Les vàlvules es troben representades per dues circumferències, les quals indiquen que la vàlvula està oberta quan estan de color verd i vermell quan estan tancades. El dipòsit mostra l'alçada del líquid, així com el seu percentatge d'ompliment. A la dreta d'aquest podem observar la consigna (nivell desitjat).

També es disposa de dos indicadors (cantonada inferior esquerra) que mostren l'estat de funcionament del sistema de control actual. Pot variar entre sondeig i productor, que són mètodes diferents de comunicació entre els dos nodes. A la

seva dreta hi ha un indicador d'estat. El sistema entra en estat d'alarma en passar els límits de temperatura establerts.

El gràfic situat a la dreta de la imatge registra el nivell del dipòsit. Permet observar com evoluciona el nivell del dipòsit en temps real.

II. PROGRAMACIÓ EN "LABVIEW"

El "LabView" es basa en programació sobre mòduls. Primer de tot s'ha de configurar per poder llegir els missatges del bus CAN. Per a això crearem un arxiu subVI amb aquesta funció. Una vegada que es capaç de llegir els missatges del bus els ha d'interpretar. El podem observar amb detall a la figura 4.

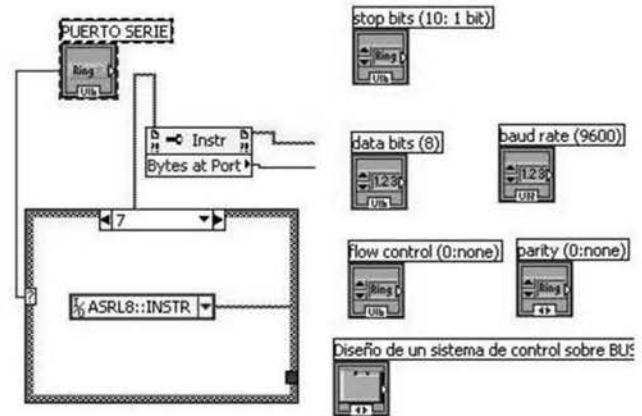


Fig. 4 Configuració del port sèrie

Els quadres que observa'm a la figura 5 representen els mòduls que formen l'VI, cadascun dels quals té una funció definida i utilitzant una combinació de diferents mòduls obtenim el nostre sistema. Les sortides d'aquest sistema seran representades de forma gràfica com podem observar a la figura 3. Els quadres que envolten diferents mòduls representen un while.

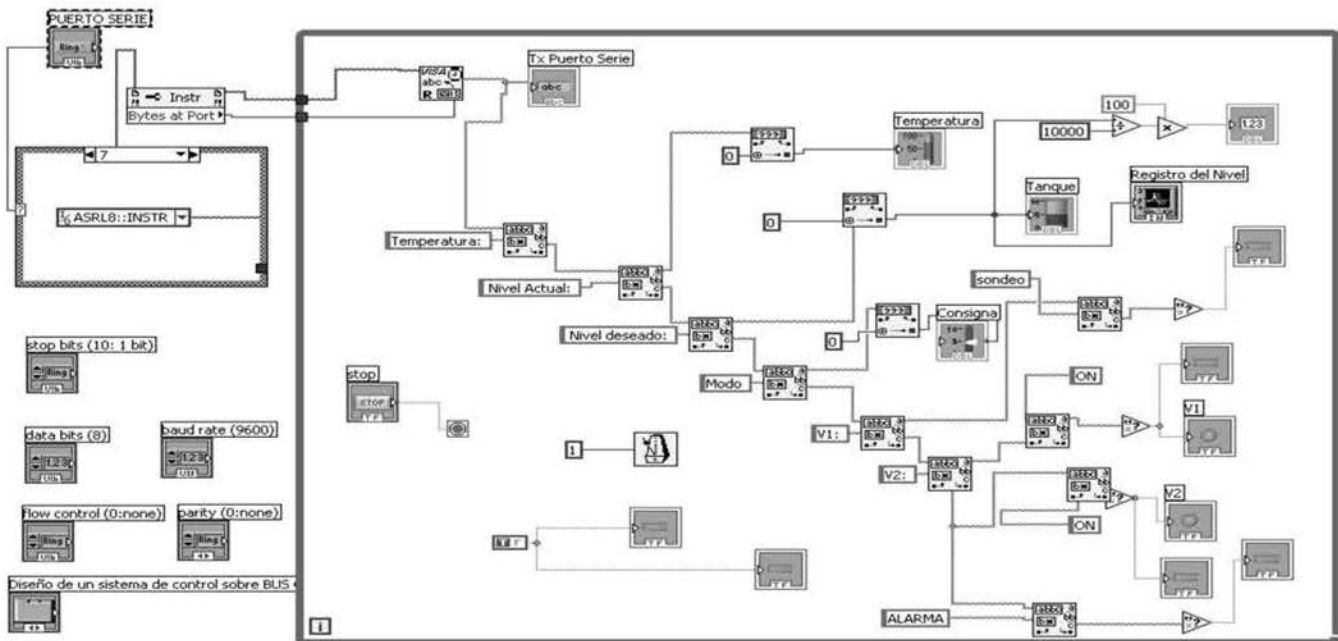


Fig. 5 VI

El primer mòdul (VISA) reconeix el text del port sèrie i ho transforma en un array de caràcters.

Tx Port Sèrie representa l'array de caràcters, podent així observar la trama sencera en el panell principal. Ho podem observar a la figura 6, que com es pot observar, es tracta del missatge que es rep per el RS-232 (figura 1).

Els següents mòduls són utilitzats per trobar paraules i dividir l'array de caràcters en tres parts. Un array amb la coincidència ("Temperatura:" o "Nivell Actual:"), un altre amb la part de l'array que precedeix a la paraula a buscar i el restant amb el següent a la coincidència.

El mètode utilitzat es repeteix durant tot l'array. Si la nostra trama observada pel port sèrie és la següent:

"Temperatura: XX, Nivell Actual: YYYY, Nivell desitjat: ZZZZ, Mode sondeig, V1: ON, V2: ON. Alarma!!!"

El primer pas és reconèixer la paraula temperatura, per a això busquem "Temperatura:" i obtenim com una de les sortides la següent trama: XX, Nivell Actual: YYYY, Nivell desitjat: ZZZZ, Manera sondejo, V1: ON, V2: ON. Alarma!!!

On XX representa el valor de la temperatura. El següent pas és aïllar aquest nombre, ja que ve seguit per la resta de la trama. Els mòduls que ho fan es mostren a continuació:

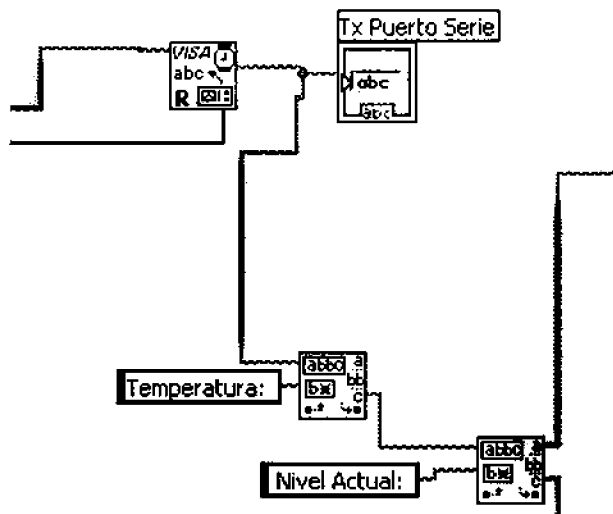


Fig. 6 Adquisició de dades

Per tant, el següent és buscar "Nivell Actual:" on passarem a tenir les 3 trames següents:

XX  
Nivell Actual:  
YYYY, Nivell desitjat: ZZZZ, Mode sondeig, V1: ON, V2:  
ON. Alarma!!!

Tenint el valor de la temperatura aïllat, podem passar a representar-ho en forma de termòmetre. Per aconseguir el valor del nivell actual utilitzem el mateix plantejament i obtenim aquestes tres trames:

YYYY  
Nivell desitjat:  
ZZZZ, Mode sondeig, V1: ON, V2: ON. Alarma!!!

Tenint el valor actual aïllat, podem passar a representar-ho en forma de dipòsit com observarem en panell frontal.

A la figura 3 també es pot observar com el valor XX se representa en forma de termòmetre y el valor YYYY en forma de dipòsit. Aprofitant el valor del nivell actual (YYYY) representa'm el registre de nivell i també es mostra el percentatge del dipòsit. A la figura 7 observa'm els mòduls de les sortides del dipòsit, la temperatura i la gràfica.

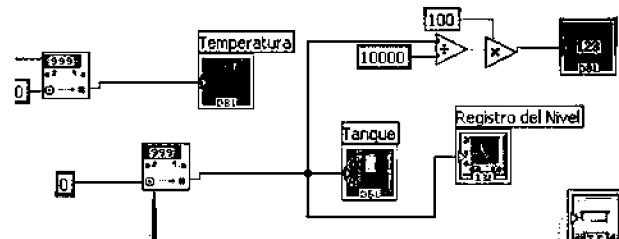


Fig. 7 Sortides

Utilitzant el mateix plantejament, aconseguim aïllar el valor de la consigna i així poder representar-ho en forma de barra. Es pot observar a la figura 3.

Per reconèixer l'estat de sondeig o productor, l'estat de les vàlvules o el mode alarma cercarem coincidències de paraules clau.

Utilitzant els mòduls per reconèixer caràcters busquem paraules clau com "ON", "sondeig" o "alarma". Per a això anem dividint la trama igual que en els casos anteriors. Aquesta vegada, no transformem els caràcters en nombres (com ocorria abans) sinó busquem que coincideixi la paraula exacta. Per tant, a la trama, si després de V1: trobem "ON" sabrem que la vàlvula V1 estarà activada i en cas de no coincidir suposarem que està tancada. Per això es tracten de paraules clau, ja que en cas de no coincidir amb aquesta paraula, sempre suposarem el cas contrari. Les sortides d'aquestes es representen amb booleancs (dues possibles solucions, si o no), podent així representar l'estat d'aquestes amb LEDS, com s'observa en el panell frontal principal.

El mòdul de stop representa el nostre botó de STOP en el nostre panell frontal principal. És utilitzat per cancel·lar el procés del while i així deixar d'utilitzar el programa.

El mòdul amb el metrònom representa el refresc del while, que en el nostre cas serà de 1 ms.

Els quadres inferiors representen una booleana sempre activa, utilitzada per a la decoració en el panell principal (simbolitzar les canonades del tanc).

### III. CONCLUSIONS

Com a conclusió d'aquest treball podem dir que amb "LabView" podem obtenir uns resultats molt vistosos, més fàcils d'interpretar i amb no massa complicació d'implementació. Aplicant els coneixements en sistemes d'adquisició de dades i utilització del software "LabView" adquirits a altres assignatures, hem obtingut un resultat molt bo per poder visualitzar la trama CAN del sistema de control del dipòsit d'aigua.

Les úniques complicacions a l'hora d'interpretar aquesta trama es anar separant-les, però seguint el procés esmentat anteriorment finalment es va aconseguir completar. Altres aspectes són els de configuració de comunicació (figura 8), que pot dur qualche problema, o el format de les dades que s'ha de canviar segons com es vulgui representar.



Fig. 8 Configuració port serie

### AGRAÏMENTS

Volem agrair aquest treball al nostre professor, Guillermo Rodríguez-Navas González per haver-nos motivat a fer la pràctica d'una forma diferent a la resta i a nosaltres mateixos.

### REFERÈNCIES

- [1] [www.wikipedia.org](http://www.wikipedia.org)
- [2] Pedro García Teodoro, Jesús Esteban Díaz Berdejo, Juan Manuel López Soler, "Transmisión de datos y redes de computadores"
- [3] Práctica de Xarxes de Comunicació Industrial, "Disseny d'un sistema de control sobre CAN.
- [4] Data sheet del PIC18F4580
- [5] Data sheet del PIC16F876A
- [6] Assignatura d'Instrumentació II ("LabView")



Alvaro Sáiz



Toni Nadal

# Disseny i implementació d'un controlador de motor BRUSHLESS

Guillem Pons, Sebastià Ferretjans, Vicenç Salas, Alfredo García i Antoni Rosselló.

Tercer curs d'Enginyeria Tècnica Industrial, Especialitat en Electrònica Industrial  
[gponsm@coitt.es](mailto:gponsm@coitt.es)

[sebastian.ferretjans@hotmail.es](mailto:sebastian.ferretjans@hotmail.es)

[salasgomila@gmail.com](mailto:salasgomila@gmail.com)

[electr-pro@hotmail.com](mailto:electr-pro@hotmail.com)

[inot.bunyola@msn.com](mailto:inot.bunyola@msn.com)

**Resum**— A aquest article s'explica el procés que s'ha seguit per al disseny i fabricació d'un controlador per un motor trifàssic brushless. Partint de l'esquema d'una placa entrenadora s'ha estodiat i modificat aquesta per aconseguir les especificacions de disseny. Aquest projecte és l'objectiu de l'assignatura Disseny i Simulació Electrònica que consisteix en aprendre a dissenyar i fabricar circuits impresos.

## I. INTRODUCCIÓ

Per a la realització de les pràctiques de tres assignatures d'Enginyeria Tècnica Industrial, Especialitat en Electrònica Industrial, s'ha proposat un projecte conjunt que consisteix en el disseny i fabricació de minimotos. Les assignatures de Sistemes Mecànics, Disseny i Simulació Electrònica i Sistemes Industrials de Potència són les encarregades de dur-lo a terme. L'assignatura de Sistemes Mecànics s'encarregarà de dissenyar la transmissió del motor amb les rodes de la minimoto. L'assignatura de Disseny i Simulació dissenyarà el controlador d'aquestes, que servirà per generar una tensió trifàsica a partir de les bateries DC. Finalment l'assignatura de Potència, implementarà el codi del microcontrolador que du la placa controladora. Aquest article es centra exclusivament a la part de Disseny i Simulació, és a dir, a la fabricació de la placa.

## II. PUNT DE PARTIDA I DEFINICIÓ DELS BLOCS

Per al disseny d'aquesta placa és parteix de l'esquema d'una placa entrenadora que compleix amb uns requeriments semblants als nostres. La diferència principal és que el nostre controlador ha de poder subministrar una potència superior, i és per això que serà necessari redissenyar la part d'alimentació del motor a més s'haurà de simplificar ja que la placa entrenadora té una sèrie de funcionalitats que podem prescindir.

Definim que el nostre controlador ha de tenir quatre parts ben diferenciades.

*A. Alimentació:* aquesta part s'encarregarà de proporcionar a tots els components de placa la tensió que necessitin, comptarà, per tant, amb tots els reguladors de tensió necessaris. En el nostre cas tindrèm els 12V que ens proporciona la bateria, 5V pels drivers, i 3'3V pel

microcontrolador, els sensors de control i el potenciòmetre del gas.

- B. Microcontrolador:* aquesta part serà de senyal, hi haurà el microcontrolador i la interfície de programació ISCP, és on s'executa el codi generant els senyals de control dels drivers en funció de la realimentació rebuda i les consignes preprogramades.
- C. Drivers:* aquesta part de la placa rebrà la tensió de referència i en funció d'aquesta generarà un corrent que serà la que alimentarà al motor. Pot ser fins a 20A i serà la part de la placa més problemàtica en el sentit que el pas de tanta corrent pot fer malbé la placa.
- D. Realimentació:* Serveix per tenir un control del motor mitjançant un sensor d'intensitat de cada una de les branques de potència del motor.

45

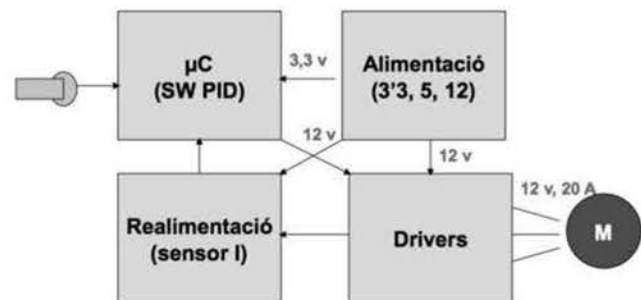


Fig. 1 Digrana de blocs de partida.

## III. DISSENY ESQUEMÀTIC

Una vegada tenim ben fixat els blocs podem passar a dissenyar l'esquemàtic, com ja hem comentat abans, treballam damunt l'esquema de la placa entrenadora.



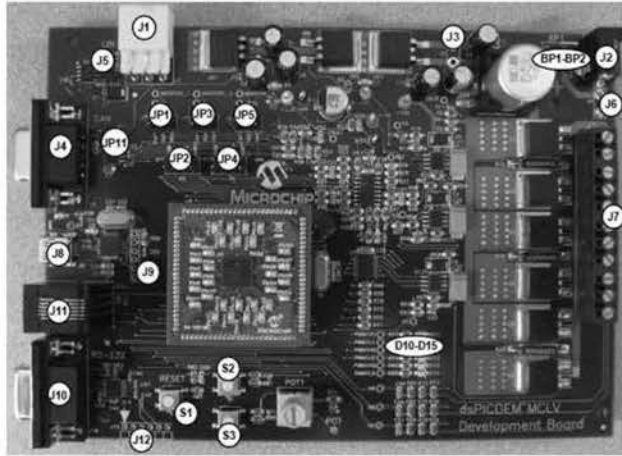


Fig. 2 Placa entrenadora de Microchip.

La placa entrenadora compta amb:

- 1) Programació del  $\mu$ C (Port Serie, Interfície CAN, USB, ISCP i LIN).
- 2) Alimentació (Polsador de reset, reguladors: 15, 5 i 3V)
- 3) Drivers motor.
- 4) Realimentació (Per efecte hall, per tensió de referència i per control de corrent).
- 5) Altres components per diferents funcionalitats com: leds i polsadors.

D'aquesta placa prescindim de de tots els ports de programació manco ISCP, els sensors d'efecte hall i tensió de referència, tots els leds i tots els polsadors manco el de reset. A més adaptam la resta de funcionalitats per aconseguir les nostres especificacions de disseny.

Canviem l'alimentació per treballar amb una tensió màxima de 12V de la bateria, convertir-la a 5 i després a 3'3V. D'aquesta manera obtenim les tres tensions que necessitam a les diferents parts de la placa.

La placa entrenadora esta pensada per donar una intensitat màxima de 5A mentre que els nostres motors en necessiten 20A per fase. És per això que haurem de redissenyar aquesta part. Canviem els transistors que són els que donen el corrent al motor, i a més les resistències de potència.

El control d'aquest corrent és fa posant un resistència i mesurant la diferència de potencial als seus bornes. Si volem els mateixos increments de tensió per poder usar un circuit igual al de la placa entrenadora, si per 5A teniem una resistència de 5m $\Omega$ , per 20A necessitam una resistència 4 vegades menor (1'25m $\Omega$ ).

Una vegada tenim això podem començar a passar l'esquemàtic al programa EAGLE. Aquest programa serveix per dissenyar circuits impresos.

L'esquema de la placa el dividim en 10 parts:

- Microcontrolador (DSPIC33FJ1MC202).
- Conector de programació (Connector RJ-12).
- Polsador de reset.
- Potenciòmetre – Accelerador.
- Condensadors d'alimentació del  $\mu$ C.
- Fonts d'alimentació (Reguladors de tensió).
- Bornes de sortida de la placa.
- Amplificadors i sensors d'intensitat.
- Buffer, drivers i transistors.
- Connectors interconnexió de plaques.

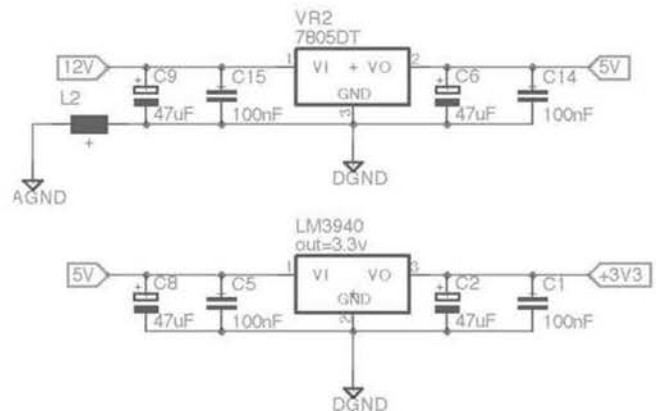


Fig. 3 Esquemàtic Fonts d'alimentació.

Degut a les limitacions de la versió per estudiants del programa EAGLE el qual limita el tamany de placa i el número de components vam haver dividir el projecte en dues parts i implementar-lo en dues plaques:

Placa digital:

- Microcontrolador (DSPIC33FJ1MC202).
- Conector de programació (Connector RJ-12).
- Polsador de reset.
- Potenciòmetre – Accelerador.

Placa potència:

- Condensadors d'alimentació del  $\mu$ C.
- Fonts d'alimentació (Reguladors de tensió).
- Bornes de sortida de la placa.
- Amplificadors i sensors d'intensitat.
- Buffer, drivers i transistors.
- Connectors interconnexió de plaques.

Per fer aquesta divisió requereix haver de connectar les dues plaques entre elles.

Cal assenyalar que per aquest apartat vam haver de crear llibreries de components ja que no tots els que necessitavem hi estaven definits.

#### IV. DISSENY DEL LAYOUT

Pel disseny del layout s'ha fet ús del mateix programa, EAGLE, on a partir de l'esquema definit a l'apartat anterior es genera el Layout.

El primer pas és definir el tamany de la placa, a continuació ve una de les parts més importants que és l'ubicació dels components a la placa, tant a la cara superior com l'inferior. La millor manera de fer-ho és anar analitzant l'esquema i col·locant els diferents components per proximitat entre ells. Moltes vegades, a mesura que avança el disseny, s'han de recol·locar component ja fixats.

Una vegada es tenen els components fixats és comença la tasca de connexió entre ells, enrutament. Aquesta tasca s'ha de fer de manera manual i suposa una gran inversió de temps fins que s'aconsegueix tot l'enrutament. Amb l'ús dels plans d'alimentació i massa es simplifica la tasca de l'enrutament a més d'evitar la problemàtica derivada als dissenys de plaques.

L'enrutament no només es tracta de connectar els components sino fer-ho aplicant les tècniques de reducció d'interferències, explicades pel professor. D'aquestes destacam:

- Interferències per soroll: L'aplicació d'aquesta tècnica consisteix en evitar que les pistes tinguin angles 90°.
- Interferències conductives: L'aplicació d'aquesta tècnica es basa en la creació de diferents plans d'alimentació i terra, aconseguint la connexió a massa i alimentació en un sol punt. Evitant així els llaços de corrent no desitjats.
- Tècniques de desacoblament a nivell de tarjeta. Fent ús de condensadors de desacoblament sobre els circuits integrats, reguladors...

Per tal de que la placa suporti els corrents que necessita la placa, les pistes de potència hauràn de tenir la màxima superfície possible. Per aquest motiu ho implementam fent servir plans d'alimentació, tal com es pot veure a la Fig. 5.

Una utilitat adicional amb que compta el programa EAGLE és poder fer una exportació per a visualitzar el resultat final en 3D.

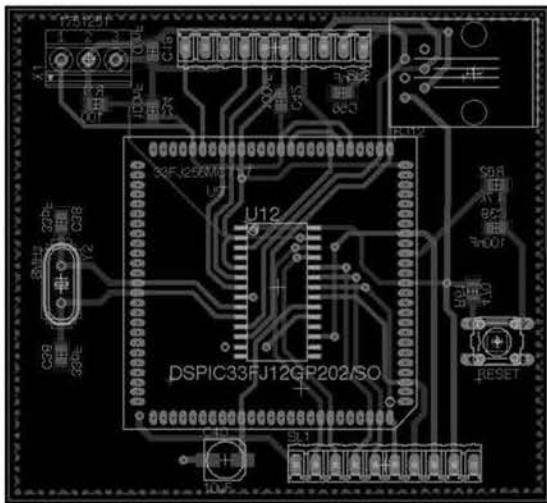


Fig. 4 Layout placa Digital.

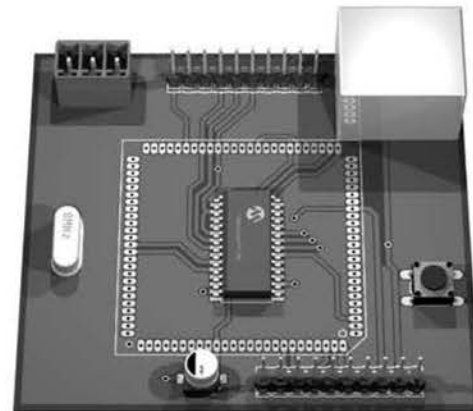


Fig. 6 Vista simulada placa Digital.

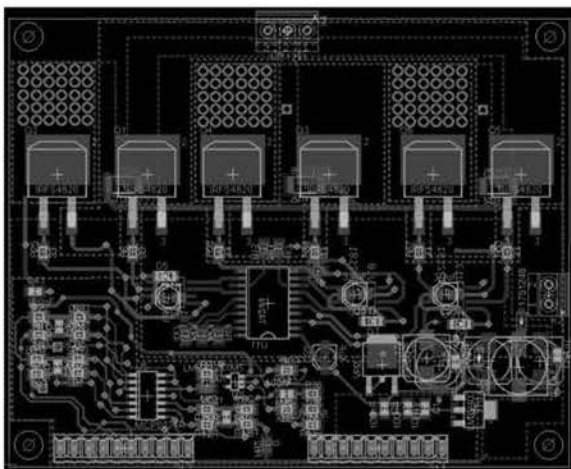


Fig. 5 Layout placa Potència.

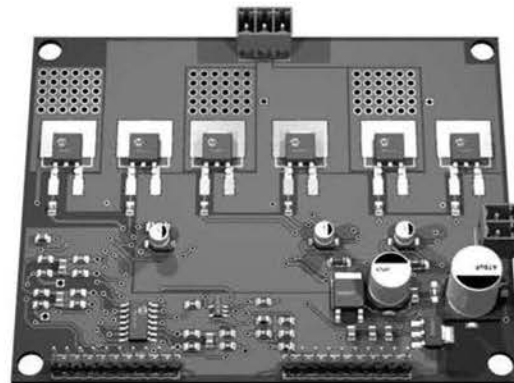


Fig. 7 Vista simulada placa Potència.

## V. MUNTATGE DE LA PLACA

Una vegada finalitzat el layout comença el procés de fabricació de les plaques. D'on s'obté el circuit imprès on hi soldarem els components per obtenir el muntatge final.

Degut a que els components són SMD s'ha de tenir molta cura a l'hora de soldar-los. Sempre començant pels components més petits que un cop identificats i conegut el lloc on van, es solden a la placa. És fa un ús d'un soldador de punta fina i pasta de soldadura.

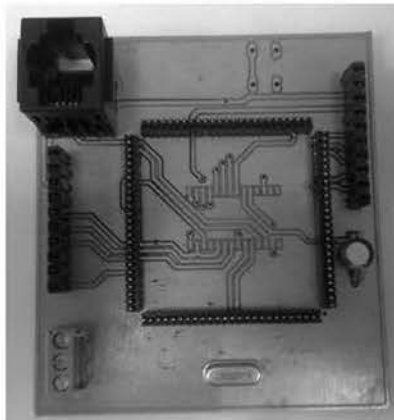


Fig. 4 Placa Digital.

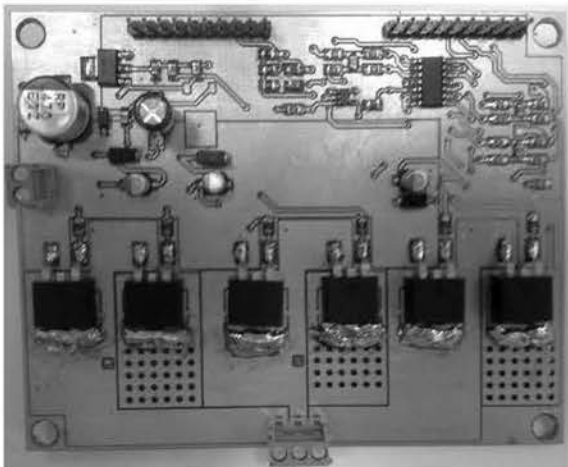


Fig. 4 Placa Digital.

## CONCLUSIONS

Amb la realització d'aquest projecte hem pogut conèixer el procés de disseny i fabricació de circuits impresos: concepte, disseny i fabricació.

Cal citar que podent ésser una assignatura molt aprofitosa i atractiva per nosaltres, ens ha resultat, per varis motius, un projecte d'una dificultat exagerada. On problemes fàcilment resolubles se'ns han allargat per falta d'atenció i coordinació dels professors.

Per aquest motiu, juntament amb els canvis introduïts al disseny final degut a les limitacions del programa, el qual no podia amb la magnitud del projecte, hem hagut de suportar exigències molt majors a les esperades. Hem pogut aconseguir-ho sacrificant moltes hores, amb una bona coordinació del grup i gràcies als coneixaments que tenien alguns membres del grup, no adquirits a aquesta assignatura.

És per això que ens sentim gratament satisfets amb el nostre resultat final.

## REFERÈNCIES

- [1] DSPICDEM DEVELOPMENT BOARD USERS GUIDE. Microchip technology Inc.
- [2] Tutorial EAGLE Sparkfun Electronics-
- [3] Electronics\_EAGLE\_3D Tutorial <http://eagle.pcbpics.es/3dbasico.pdf>
- [4] Presentacions de l'assignatura Disseny i Simulació Electrònica. Bartomeu Alorda- UIB

# Análisis asintótico de relaciones de recurrencia en complejidad algorítmica mediante la teoría de ecuaciones en diferencia

Oscar Valero\*

Departamento de Ciencias Matemáticas e Informática  
Universidad de las Islas Baleares  
Ctra. de Valldemossa km. 7.5, 07122, Palma de Mallorca, Spain  
o.valero@uib.es

**Resumen**—La teoría de ecuaciones en diferencias permite modelar satisfactoriamente múltiples procesos que surgen de modo natural en diversas áreas de las ciencias aplicadas. En concreto, las ecuaciones en diferencias resultan de gran utilidad en Ciencia de la Computación. El objetivo del presente artículo es introducir a los estudiantes de las titulaciones de Grado en Matemáticas y Grado en Ingeniería Informática, así como a los futuros investigadores que se forman cursando el título de Máster en Tecnologías de la Información, en las técnicas de resolución de un tipo particular de ecuaciones en diferencias, las denominadas ecuaciones en diferencias finitas lineales, y mostrar su aplicabilidad al análisis de complejidad algorítmica.

## I. MOTIVACIÓN

En lo sucesivo las letras  $\mathbb{N}$ ,  $\mathbb{Z}^+$ ,  $\mathbb{R}$ ,  $\mathbb{R}^+$  y  $\mathbb{R}_0^+$  denotarán el conjunto de los números enteros positivos, el conjunto de los números enteros no negativos, el conjunto de los números reales, el conjunto de los número reales no negativos y el conjunto de los número reales positivos, respectivamente.

En Ciencia de la Computación el análisis de la complejidad de un algoritmo se basa en determinar matemáticamente la cantidad de recursos (**coste computacional** o **coste de ejecución**) que dicho algoritmo necesita para resolver el problema para el que ha sido diseñado. Dos de los recursos típicos, los cuales juegan un papel fundamental en el análisis de la complejidad algorítmica, son el tiempo empleado por el algoritmo bajo estudio para resolver un problema (**tiempo de computación** o **tiempo de ejecución**), y la memoria (**espacio**) empleada por la computadora que ejecuta el algoritmo al resolver el problema bajo estudio.

Por otro lado, es habitual que existan varios algoritmos que resuelvan un problema dado. Por este motivo, uno de los objetivos principales del análisis de complejidad algorítmica es discernir cuál de todos los algoritmos que resuelven un problema lo hace con menos coste computacional. Este hecho motiva que, para averiguar qué algoritmo es más eficiente (en términos de coste), sea necesario comparar sus costes de computación. Para poder llevar a cabo la mencionada comparación se requiere el uso de herramientas matemáticas que permitan representar para cada algoritmo su coste computacional. Así, en el análisis de complejidad algorítmica, el coste de computación de un algoritmo es denotado por una

función  $T : \mathbb{N} \rightarrow [0, \infty)$  de modo que  $T(n)$  representa el coste empleado por el algoritmo en resolver el problema bajo consideración cuando el dato de entrada del algoritmo tiene un tamaño  $n$ .

El método de representación introducido presenta un pequeño inconveniente, ya que el coste de ejecución de un algoritmo no depende exclusivamente del tamaño del dato de entrada  $n$ , sino que éste también depende de la distribución particular de los datos de entrada. Obviamente, y como ejemplo ilustrativo, si se considera un algoritmo de ordenación de modo que, dado un vector de  $n$  entradas numéricas, el algoritmo proporcione como resultado el vector con los datos almacenados en orden creciente (ejemplos de este tipo de algoritmos son Merge-sort y Quicksort), entonces no tardará lo mismo en resolver el problema nuestro algoritmo si el vector está totalmente ordenado o si está completamente desordenado (los datos almacenados están en orden decreciente). Por tanto, el coste puede variar sustancialmente al procesar ejemplares diferentes (con distinta distribución) de los datos de entrada con un mismo tamaño. Con el objetivo de resolver este inconveniente, en el análisis de complejidad algorítmica se distinguen tres posibles comportamientos en cuanto a coste computacional se refiere. Estos son los denominados **mejor caso**, **peor caso** y **caso promedio** en coste de ejecución.

Para un algoritmo dado y un tamaño de dato fijado, se define el **mejor caso** (peor caso) en coste de ejecución como el coste de ejecución empleado por el algoritmo en cuestión para procesar aquel dato, del tamaño fijado, cuya distribución requiere menos (más) coste de procesado o, de manera equivalente,

$$C_M = \min_{|X|=n} C_X \quad (C_P = \max_{|X|=n} C_X),$$

donde por  $C_X$  se ha representado el coste empleado por el algoritmo para resolver el problema con un dato de entrada con distribución  $X$ , y se ha indicado que el tamaño de los datos de entrada es  $n$  mediante la expresión  $|X| = n$ .

El análisis algorítmico basado en el comportamiento en el peor y mejor caso en coste computacional permite acotar la complejidad de un algoritmo, ya que para todos aquellos datos cuya distribución no se corresponda con la del peor (mejor) caso, el coste de ejecución será menor (mayor). Por este motivo el análisis basado en estos dos casos es el más extendido. Sin embargo, hay ocasiones en las que un algoritmo se emplea muchas veces sobre datos de entrada con distinta distribución pero mismo tamaño y, por tanto, resulta más útil

\*Este trabajo ha sido elaborado en el marco del proyecto de investigación MTM2009-10962 que desarrolla actualmente el grupo Lógica Borrosa y Fusión de la Información (LOBFI) de la UIB, y que ha sido financiado por el Ministerio de Ciencia e Innovación.

conocer su coste de ejecución en media, es decir, el caso promedio en coste de ejecución. Así, para un algoritmo dado y un tamaño de dato fijado, se define el caso promedio en coste de ejecución como el promedio de los costes de ejecución empleados por el algoritmo al procesar todas las posibles distribuciones de los datos de entrada con el tamaño fijado, o equivalentemente

$$C_{Prom} = \sum_{|X|=n} C_X \cdot Pr(X),$$

donde por  $Pr(X)$  se ha denotado la probabilidad de que los datos de entrada tengan la distribución  $X$ .

Con el fin de eliminar cualquier posible ambigüedad al representar por  $T(n)$  el coste de ejecución de un algoritmo, debe ser siempre especificado el tipo de distribución de los datos de entrada que el algoritmo bajo estudio está procesando.

En general, determinar exactamente cuál es la función que describe el coste computacional de un algoritmo es una tarea ardua. Por este motivo en muchas ocasiones se pretende obtener información sobre dicha función de un modo "aproximado", es decir, se desconoce exactamente el valor de  $T(n)$  para cada tamaño de dato  $n$  pero se saben ciertas propiedades respecto al comportamiento de  $T$ . Una de las técnicas más empleadas para realizar un análisis aproximado de la complejidad de un algoritmo se conoce bajo el nombre de **análisis de complejidad algorítmica asintótico**. Éste se basa fundamentalmente en el hecho siguiente: supongamos que tenemos un algoritmo y una distribución de los datos de entrada. Estamos interesados en conocer su coste computacional  $T$  pero, por otro lado, no tenemos ninguna técnica para poder explicitar la expresión de  $T(n)$  para cada  $n$ . Sin embargo es posible deducir que existen  $n_0 \in \mathbb{N}$ ,  $c_1, c_2 \in \mathbb{R}^+$  y una función  $U : \mathbb{N} \rightarrow [0, \infty)$  tales que

$$c_2 U(n) \leq T(n) \leq c_1 U(n)$$

para todo  $n \geq n_0$  (habitualmente denotado por  $T \in \Theta(U)$ ). Entonces la función  $U$  acota asintóticamente de modo superior e inferior a la función  $T$  y, así, nos proporciona una información aproximada del coste computacional, para la distribución de los datos de entrada considerada, del algoritmo que está siendo estudiado. De hecho si  $T \in \Theta(U)$ , se tiene que el coste computacional  $T(n)$  será como máximo (mínimo) el valor proporcionado por la función  $c_1 U(n)$  ( $c_2 U(n)$ ) para cada  $n \geq n_0$ . Obsérvese que la acotación se verifica para tamaños de dato superiores a un umbral  $n_0$ , y que este hecho significa que los costes de ejecución de nuestro algoritmo al procesar todos aquellos datos de tamaño  $n$  con  $n < n_0$  son conocidos. Por tanto, uno de los objetivos fundamentales del análisis de complejidad algorítmica consistirá en la obtención de la función  $U$  que proporciona la información asintótica (aproximada) de la función  $T$  y, por tanto, del coste computacional, fijada la distribución de los datos, de nuestro algoritmo bajo estudio.

A pesar de que en muchos casos tan sólo se puede obtener una estimación del tiempo de computación de un algoritmo mediante la técnica de acotación asintótica, existe un gran número de algoritmos cuyo coste puede ser determinado de

modo exacto, es decir, dada una distribución de los datos a procesar, para cada tamaño  $n \in \mathbb{N}$  se puede determinar exactamente la expresión de  $T(n)$  y, así, es posible obtener su comportamiento asintótico de un modo sencillo. Estos algoritmos son aquellos cuyo coste computacional satisface una **relación de recurrencia**.

Los algoritmos que siguen estrategias del tipo **Divide y Vencerás** son un ejemplo representativo de este tipo de situación. En efecto, en muchos casos el coste computacional de estos algoritmos recursivos satisface una **relación de recurrencia** del tipo siguiente:

$$T(n) = \begin{cases} bn^\alpha & \text{si } 1 \leq n \leq c \\ aT(\frac{n}{c}) + bn^\alpha & \text{si } n > c \end{cases}, \quad (1)$$

donde  $a, b \in \mathbb{R}_0^+$ ,  $\alpha \in \mathbb{Z}^+$  y  $c \in \mathbb{N}$  con  $c > 1$ . En términos generales,  $bn^\alpha$  representa el coste de descomponer el problema inicial en  $a$  subproblemas, cada uno de ellos con datos de entrada de tamaño  $\frac{n}{c}$ , y el de componer las soluciones de tales subproblemas para producir la solución del problema original a resolver.

Ejemplos típicos de algoritmos, que siguen estrategias Divide y Vencerás, cuyo coste computacional verifica una relación de recurrencia de tipo (1) son Mergesort (en el mejor, peor y caso promedio) y Quicksort (en el mejor caso).

Algunas referencias básicas sobre algorítmica y análisis de complejidad computacional, donde puede encontrarse una discusión detallada sobre los conceptos aquí expuestos, son [1], [2] y [3].

Obviamente, para poder realizar el estudio del comportamiento asintótico del coste de ejecución empleado por los algoritmos que siguen una estrategia de tipo Divide y Vencerás se requiere demostrar que las relaciones de recurrencia (1) admiten una única solución, ya que si éstas admitiesen más de una solución habría que discernir cuál de todas las posibles soluciones obtenidas representa el coste de ejecución del algoritmo bajo estudio. Además, una vez garantizada la existencia y unicidad de solución, se requiere analizar el comportamiento asintótico de dicha solución. El propósito fundamental de este trabajo es ilustrar que ambos objetivos pueden ser alcanzados con técnicas sencillas mediante el uso de la teoría de las ecuaciones en diferencias. Así, en la Sección II se introducen los conceptos básicos de ecuaciones en diferencias y las técnicas de resolución de los problemas de valor inicial asociados a éstas. La Sección III está dedicada a aplicar los conceptos expuestos en la Sección II al análisis asintótico de las soluciones de las relaciones de recurrencia de tipo (1) que representan el coste computacional de algunos algoritmos recursivos que siguen estrategias de tipo Divide y Vencerás. Finalmente, en la Sección IV se presentarán algunas ventajas de las técnicas introducidas frente a otras que también pueden ser encontradas en la bibliografía.

## II. UNA BREVE INTRODUCCIÓN A LAS ECUACIONES EN DIFERENCIAS FINITAS

Dada una sucesión  $(x_n)_{n \in \mathbb{N}} \subset \mathbb{R}$ , se dice que es **recurrente** si existen  $k \in \mathbb{N}$  y una función  $\Phi : \mathbb{R}^{k+1} \rightarrow \mathbb{R}$  tal que

$$x_n = \Phi(x_{n-1}, x_{n-2}, \dots, x_{n-k}, n) \quad (2)$$

para todo  $n > k$ . El número natural  $k$  recibe el nombre de **orden de recurrencia** de la sucesión  $(x_n)_{n \in \mathbb{N}}$ .

Una **ecuación en diferencias finitas**, o simplemente **ecuación en diferencias**, es una sucesión recurrente del tipo (2) de la cual se desea conocer la expresión de su término general. Al número natural  $k$  se le denomina **orden** de la ecuación en diferencias finitas.

En el siguiente ejemplo se ilustra la definición precedente.

**Ejemplo 1.**

1.  $x_n = 4x_{n-1} + 2^n \quad \forall n > 1$  (orden 1).
2.  $x_n = x_{n-1} + x_{n-2} + 4 \quad \forall n > 2$  (orden 2).
3.  $x_n = 5x_{n-1} - 8x_{n-2} + 4x_{n-3} \quad \forall n > 3$  (orden 3).

□

Dada una ecuación en diferencias finitas de tipo (2) y un conjunto de valores  $s_1, s_2, \dots, s_{k-1}, s_k \in \mathbb{R}$ , llamaremos **problema de valor inicial** asociado a (2) e inducido por  $s_1, s_2, \dots, s_{k-1}, s_k$  al problema de obtener todas aquellas soluciones de la ecuación en diferencias finitas (2) que satisfacen  $x_1 = s_1, x_2 = s_2, \dots, x_{k-1} = s_{k-1}$  y  $x_k = s_k$ .

A continuación se proporcionan algunos ejemplos de problemas de valor inicial.

**Ejemplo 2.**

1.  $\begin{cases} x_n = 4x_{n-1} + 2^n & \forall n > 1 \\ x_1 = 4 \end{cases}$
2.  $\begin{cases} x_n = x_{n-1} + x_{n-2} + 4 & \forall n > 2 \\ x_1 = 2 \\ x_2 = 10 \end{cases}$
3.  $\begin{cases} x_n = 5x_{n-1} - 8x_{n-2} + 4x_{n-3} & \forall n > 3 \\ x_1 = 1 \\ x_2 = -8 \\ x_3 = 10 \end{cases}$

□

La primera cuestión que puede ser planteada de modo natural es, si dada una ecuación en diferencias finitas, cada problema de valor inicial asociado a dicha ecuación tiene una única solución o admite más de una en general. La respuesta a esta pregunta nos la proporciona el siguiente resultado cuya demostración puede ser encontrada en [4].

**Teorema 1.** *Sea una ecuación en diferencias finitas del tipo (2). Entonces cada problema de valor inicial asociado a (2) admite una única solución.* □

Existe una gran diversidad de ecuaciones en diferencias finitas, sin embargo nosotros, con el propósito de proporcionar herramientas que nos permitan determinar el comportamiento asintótico del coste computacional de un algoritmo de tipo Divide y Vencerás, nos centraremos en una familia concreta, las denominadas **ecuaciones en diferencias finitas lineales con coeficientes constantes** de orden 1. Este tipo de ecuaciones son aquellas para las que existen  $\alpha \in \mathbb{R}_0^+$  y una sucesión  $(y_n)_{n \in \mathbb{N}} \subset \mathbb{R}$  tales que la función  $\Phi$ , en la expresión (2), verifica que:

$$\Phi(x_{n-1}, n) = \alpha x_{n-1} + y_n.$$

Así una ecuación en diferencias finitas lineal con coeficientes constantes de orden 1 es una ecuación en diferencias finitas que admite, para todo  $n > 1$ , la expresión general

$$x_n = \alpha x_{n-1} + y_n, \quad (3)$$

donde  $(y_n)_{n \in \mathbb{N}} \subset \mathbb{R}$  y  $\alpha \in \mathbb{R}_0^+$ .

Un ejemplo de ecuación en diferencias finitas lineal con coeficientes constantes de orden 1 y un problema de valor inicial asociado a ella nos lo proporcionan el Ejemplo 1 y el Ejemplo 2, respectivamente.

Tras conocer, por el Teorema 1, que todo problema de valor inicial asociado a una ecuación en diferencias finitas lineal de orden 1 admite una única solución, tan sólo queda plantearse cómo puede ser obtenida dicha solución. El siguiente resultado nos proporciona una técnica para lograr ese fin (véase [4] y [1]).

**Teorema 2.** *Sean  $p(n)$  un polinomio con  $\text{grado}(p(n)) = d$ ,  $\gamma, \beta \in \mathbb{R}$  y  $\lambda \in \mathbb{R}_0^+$ . El problema de valor inicial*

$$\begin{cases} x_n = \lambda x_{n-1} + \beta^n p(n) & \forall n > 1 \\ x_1 = \gamma \end{cases}$$

*admite como única solución la sucesión  $(x_n)_{n \in \mathbb{N}}$  cuyo término general viene dado por*

$$x_n = \left( \frac{\gamma - \beta q(1)}{\lambda} \right) \lambda^n + \beta^n n^\delta q(n)$$

*para todo  $n \in \mathbb{N}$ , siendo  $q(n)$  un polinomio con  $\text{grado}(q(n)) \leq d$  y*

$$\delta = \begin{cases} 0 & \text{si } \beta \neq \lambda \\ 1 & \text{si } \beta = \lambda \end{cases}$$

□

**Nota 1.** Los coeficientes del polinomio  $q(n)$  se obtienen exigiendo que la expresión  $\beta^n n^\delta q(n)$  satisfaga la ecuación

$$x_n = \lambda x_{n-1} + \beta^n p(n).$$

El siguiente ejemplo clarifica el resultado anterior.

**Ejemplo 3.** Consideremos el problema de valor inicial siguiente:

$$\begin{cases} x_n = 4x_{n-1} + 2^n & \forall n > 1 \\ x_1 = 4 \end{cases}$$

La solución a dicho problema la obtendremos aplicando el Teorema 2 con  $p(n) = 1 \quad \forall n \in \mathbb{N}$ ,  $\lambda = 4$ ,  $\beta = 2$ ,  $\gamma = 4$  y  $\delta = 0$ . Por tanto, el mencionado teorema nos garantiza que la solución al problema de valor inicial propuesto viene dada por la sucesión  $(x_n)_{n \in \mathbb{N}}$  cuyo término general satisface la expresión

$$x_n = \left( \frac{4 - 2D}{4} \right) 4^n + D 2^n \quad \forall n \in \mathbb{N},$$

donde  $q(n) = D \forall n \in \mathbb{N}$ . Para determinar el valor de la constante  $D$  debemos exigir, siguiendo la Nota 1, que la expresión  $D2^n$  verifique la ecuación en diferencias

$$x_n = 4x_{n-1} + 2^n,$$

es decir exigiendo que

$$D2^n = 4D2^{n-1} + 2^n.$$

De esta última expresión se deduce inmediatamente que  $D = -1$ . En consecuencia se tiene que

$$x_n = \frac{3}{2}4^n - 2^n \quad \forall n \in \mathbb{N}.$$

□

Finalizamos esta sección mediante el estudio de un problema de valor inicial que jugará un papel fundamental en el análisis asintótico de las relaciones de recurrencia de tipo (1) en la Sección III.

Sean  $\gamma, \lambda, b \in \mathbb{R}$ ,  $c \in \mathbb{N}$  ( $c > 1$ ) y  $\alpha \in \mathbb{Z}^+$ . Veamos como obtener, aplicando el Teorema 2, la solución del siguiente problema de valor inicial:

$$\begin{cases} x_n = \lambda x_{n-1} + b(c^\alpha)^n & \forall n > 1 \\ x_1 = \gamma \end{cases} \quad (4)$$

Para ello distinguiremos dos casos posibles y tendremos en cuenta que  $p(n) = b \forall n \in \mathbb{N}$ :

Caso 1.  $c^\alpha \neq \lambda$ . En este caso  $\delta = 0$  y, así, la expresión de la solución del problema (4) que nos proporciona el Teorema 2 viene dada por

$$x_n = \left( \frac{\gamma - c^\alpha D}{\lambda} \right) \lambda^n + D(c^\alpha)^n$$

(obsérvese que  $q(n) = D \forall n \in \mathbb{N}$ ). Exigiendo, tal y como nos indica la Nota 1, que la expresión  $D(c^\alpha)^n$  verifique la ecuación en diferencias que induce el problema bajo estudio se obtiene que

$$D = \frac{bc^\alpha}{c^\alpha - \lambda}.$$

De este modo la expresión de la solución se reduce a

$$x_n = \left( \frac{\gamma - \frac{bc^\alpha}{c^\alpha - \lambda}}{\lambda} \right) \lambda^n + \frac{bc^\alpha}{c^\alpha - \lambda} (c^\alpha)^n.$$

Caso 2.  $c^\alpha = \lambda$ . En este caso  $\delta = 1$  y, así, la expresión de la solución del problema (4) que nos proporciona el Teorema 2 viene dada por

$$\begin{aligned} x_n &= \left( \frac{\gamma - c^\alpha D}{\lambda} \right) \lambda^n + Dn(c^\alpha)^n \\ &= \left( \frac{\gamma - c^\alpha D}{c^\alpha} \right) (c^\alpha)^n + Dn(c^\alpha)^n \\ &= \left[ \left( \frac{\gamma}{c^\alpha} - D \right) + Dn \right] (c^\alpha)^n \end{aligned}$$

(nótese que  $q(n) = D \forall n \in \mathbb{N}$ ). Exigiendo, tal y como nos indica la Nota 1, que la expresión  $Dn(c^\alpha)^n$  verifique la

ecuación en diferencias que induce el problema bajo estudio se obtiene que  $D = b$ . De este modo la expresión de la solución se reduce a

$$x_n = \left[ \left( \frac{\gamma}{c^\alpha} - b \right) + bn \right] (c^\alpha)^n$$

### III. ANÁLISIS DE COMPLEJIDAD ALGORÍTMICA Y ECUACIONES EN DIFERENCIAS FINITAS

En lo que sigue nos centraremos en obtener el comportamiento asintótico de la solución de la relación de recurrencia (1). Para ello aplicaremos la técnica de resolución de problemas de valor inicial inducidos por ecuaciones en diferencias finitas lineales con coeficientes constantes de orden 1 descrita en el Teorema 2.

En primer lugar debemos observar el hecho de que la relación de recurrencia (1) no satisface la expresión (2) y, así, la definición de ecuación en diferencias. Por este motivo es necesario manipular la expresión (1), realizando un cambio de variable, para poder aplicar la técnica de resolución expuesta en la Sección II.

En lo que sigue consideraremos la relación de recurrencia

$$T(n) = \begin{cases} bn^\alpha & \text{si } 1 \leq n < c \\ aT\left(\frac{n}{c}\right) + bn^\alpha & \text{si } n \in \mathbb{N}_c \end{cases}, \quad (5)$$

donde  $a, b \in \mathbb{R}_0^+$ ,  $\alpha \in \mathbb{Z}^+$ ,  $c \in \mathbb{N}$  con  $c > 1$  y  $\mathbb{N}_c = \{c^k : k \in \mathbb{N}\}$ .

Obsérvese que en la relación de recurrencia (5) se ha considerado que el tamaño de los datos de entrada  $n$  recorre el conjunto  $\mathbb{N}_c$ , esto es debido a que el comportamiento asintótico en el caso más general, en el que  $n \in \mathbb{N}$ , puede ser analizado utilizando la información deducida de este caso particular. En primer lugar estudiaremos la relación de recurrencia (5) y posteriormente abordaremos el análisis asintótico de la relación de recurrencia (1).

Con el objetivo de abordar el estudio de la relación de recurrencia (5), y teniendo en cuenta que  $n \in \mathbb{N}_c$ , realizamos la siguiente identificación para todo  $k \in \mathbb{N}$ :

$$x_k = T(c^k).$$

De donde se tiene que

$$T\left(\frac{n}{c}\right) = T(c^{k-1}) = x_{k-1}.$$

A continuación planteamos el siguiente problema de valor inicial:

$$\begin{cases} x_k = ax_{k-1} + b(c^\alpha)^k & \forall n > 1 \\ x_1 = ab + bc^\alpha \end{cases} \quad (6)$$

Nótese que  $ab + bc^\alpha = T(c)$ .

Observe que el problema de valor inicial precedente ha sido estudiado en la Sección II con  $\lambda = a$  y  $\gamma = ab + bc^\alpha$ . Siguiendo el esquema de resolución planteado en la sección mencionada se obtienen dos casos posibles que nos conducen a la expresión de la solución:

Caso 1.  $c^\alpha \neq a$ . En este caso la expresión de la solución del problema (6) viene dada por

$$\begin{aligned} x_k &= \left( \frac{ab+bc^\alpha - \frac{c^{2\alpha}b}{c^\alpha - a}}{a} \right) a^k + \frac{bc^\alpha}{c^\alpha - a} (c^\alpha)^k \\ &= \frac{ab}{a-c^\alpha} a^k + \frac{bc^\alpha}{c^\alpha - a} (c^\alpha)^k. \end{aligned}$$

Caso 2.  $c^\alpha = a$ . En este caso la expresión de la solución del problema (6) viene dada por

$$\begin{aligned} x_k &= \left( \frac{ab+bc^\alpha}{c^\alpha} - b + bk \right) (c^\alpha)^k \\ &= \left( \frac{ab}{c^\alpha} + bk \right) (c^\alpha)^k. \end{aligned}$$

Una vez resuelto el problema de valor inicial (6), se obtiene inmediatamente la solución de la relación de recurrencia (5). En efecto, teniendo en cuenta que  $n \in \mathbb{N}_c$  ( $k = \log_c(n)$ ) y que  $x_k = T(c^k)$  se tiene lo siguiente:

Caso 1. ( $c^\alpha \neq a$ ). En este caso la solución se corresponde con la expresión

$$T(n) = \begin{cases} bn^\alpha & \text{si } 1 \leq n < c \\ \frac{ab}{a-c^\alpha} a^{\log_c(n)} + \frac{bc^\alpha}{c^\alpha - a} n^\alpha & \text{si } n \in \mathbb{N}_c \end{cases}. \quad (7)$$

Nótese que  $a^{\log_c(n)} = n^{\log_c(a)}$  y, por tanto, la expresión (7) puede ser reescrita del modo siguiente:

$$T(n) = \begin{cases} bn^\alpha & \text{si } 1 \leq n < c \\ \frac{ab}{a-c^\alpha} n^{\log_c(a)} + \frac{bc^\alpha}{c^\alpha - a} n^\alpha & \text{si } n \in \mathbb{N}_c \end{cases}. \quad (8)$$

Caso 2. ( $c^\alpha = a$ ). En este caso la solución se corresponde con la expresión

$$T(n) = \begin{cases} bn^\alpha & \text{si } 1 \leq n < c \\ \frac{ab}{c^\alpha} n^\alpha + bn^\alpha \log_c(n) & \text{si } n \in \mathbb{N}_c \end{cases}. \quad (9)$$

Tras resolver la relación de recurrencia (5) estamos en condiciones de plantearnos el estudio de su comportamiento asintótico. Para ello, necesitaremos introducir la notación siguiente: dadas dos funciones  $f, g : \mathbb{N} \rightarrow [0, \infty)$  y  $c \in \mathbb{N}$  con  $c > 1$ , diremos que  $f \in \Theta_{\mathbb{N}_c}(g)$  si existen  $c_1, c_2 \in \mathbb{R}^+$  y  $n_0 \in \mathbb{N}$  tales que

$$c_2 g(n) \leq f(n) \leq c_1 g(n)$$

para todo  $n \in \mathbb{N}_c$  con  $n \geq n_0$ .

Teniendo en cuenta que

$$f \in \Theta_{\mathbb{N}_c}(g) \Leftrightarrow 0 < \lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} < \infty,$$

el estudio asintótico se reduce a los discusión de los siguientes casos posibles:

Caso 1. ( $c^\alpha \neq a$ ). En este caso debemos, a su vez, distinguir dos nuevos casos:

Caso 1.1.  $c^\alpha > a$ . En este caso, de la expresión (8) y del hecho de que  $\alpha > \log_c(a)$  se deduce que

$$\lim_{n \rightarrow \infty} \frac{T(n)}{n^\alpha} = \frac{bc^\alpha}{c^\alpha - a} > 0.$$

Con lo cual se tiene que

$$T \in \Theta_{\mathbb{N}_c}(n^\alpha).$$

Caso 1.2.  $c^\alpha < a$ . En este caso, de la expresión (8) y del hecho de que  $\alpha < \log_c(a)$  se deduce que

$$\lim_{n \rightarrow \infty} \frac{T(n)}{n^{\log_c(a)}} = \frac{ab}{a - c^\alpha} > 0.$$

Con lo cual se tiene que

$$T \in \Theta_{\mathbb{N}_c}(n^{\log_c(a)}).$$

Caso 2.  $a = c^\alpha$ . En este caso, de la expresión (9) y del hecho de que  $\log_c(n) \geq 1$  se deduce que

$$\lim_{n \rightarrow \infty} \frac{T(n)}{n^\alpha \log_c(n)} = b > 0.$$

En consecuencia  $T \in \Theta_{\mathbb{N}_c}(n^\alpha \log_c(n))$ .

El análisis realizado del comportamiento asintótico de la relación de recurrencia (5) nos va a permitir estudiar dicho comportamiento para la relación de recurrencia general (1). Para este fin será necesario emplear los siguientes conceptos.

Dada una función  $f : \mathbb{N} \rightarrow [0, \infty)$ , diremos que es **asintóticamente no decreciente** si existe  $n_0 \in \mathbb{N}$  tal que para todo  $n \geq n_0$  se verifica  $f(n) \leq f(n+1)$ . Además, una función asintóticamente no decreciente  $f$  es  **$r$ -armónica** ( $r \in \mathbb{N}$  con  $r \geq 2$ ) si la función  $f_r : \mathbb{N} \rightarrow [0, \infty)$  satisface la condición  $f_r \in \Theta(f)$ , donde  $f_r(n) = f(rn)$ .

Obsérvese que toda función verificando la relación de recurrencia (1) es asintóticamente no decreciente.

La conexión entre los dos últimos conceptos introducidos y el análisis asintótico nos la proporciona el siguiente resultado (véase [1]), el cual será clave para poder culminar nuestro estudio.

**Proposición 1.** Sea  $r \in \mathbb{N}$  con  $r \geq 2$ . Si  $g : \mathbb{N} \rightarrow [0, \infty)$  es una función  $r$ -armónica y  $f : \mathbb{N} \rightarrow [0, \infty)$  es una función asintóticamente no decreciente tal que  $f \in \Theta_{\mathbb{N}_r}(g)$ , entonces  $f \in \Theta(g)$ .  $\square$

En virtud de la proposición anterior se concluye nuestro estudio mediante la siguiente discusión:

Caso 1.  $c^\alpha > a$ . En este caso se tiene que  $T \in \Theta_{\mathbb{N}_c}(n^\alpha)$ . Del hecho de que la función  $n^\alpha$  es  $c$ -armónica concluimos, por la Proposición 1, que  $T \in \Theta(n^\alpha)$ .

Caso 2.  $c^\alpha < a$ . En este caso se tiene que  $T \in \Theta_{\mathbb{N}_c}(n^{\log_c(a)})$ . Como la función  $n^{\log_c(a)}$  es  $c$ -armónica concluimos, por la Proposición 1, que  $T \in \Theta(n^{\log_c(a)})$ .



Caso 3.  $a = c^\alpha$ . En este caso se tiene que  $T \in \Theta_{\mathbb{N}_c}(n^\alpha \log_c(n))$ . Puesto que la función  $n^\alpha \log_c(n)$  es  $c$ -armónica concluimos, por la Proposición 1, que  $T \in \Theta(n^\alpha \log_c(n))$ .

#### IV. CONCLUSIONES

En Ciencia de la Computación se requiere determinar matemáticamente el coste de ejecución de los algoritmos que se emplean para resolver los problemas para los que han sido diseñados. Para poder llevar a cabo dicho objetivo, el coste de computación de un algoritmo es denotado por una función  $T : \mathbb{N} \rightarrow [0, \infty)$  tal que  $T(n)$  representa el coste empleado por el algoritmo en resolver el problema bajo consideración cuando el dato de entrada del algoritmo tiene un tamaño  $n$ . En general, dado un algoritmo, determinar exactamente la expresión de la función que representa su coste computacional es una tarea ardua y, por ese motivo, en la práctica tan sólo se requiere obtener una información aproximada del coste mediante la acotación de los valores  $T(n)$  para cada tamaño de dato de entrada  $n$ . Dichas cotas pueden ser obtenidas mediante técnicas matemáticas de naturaleza muy distinta. En particular, en este trabajo hemos mostrado que la teoría de ecuaciones en diferencias finitas constituye una herramienta útil para ese fin en aquellos casos en los que el coste computacional del algoritmo satisface una relación de recurrencia. Concretamente se han aplicado las técnicas de resolución de problemas de valor inicial asociados a ecuaciones en diferencias finitas lineales con coeficientes constantes para analizar el comportamiento asintótico de algoritmos recursivos que siguen estrategias de tipo Divide y Vencerás. Los resultados asintóticos obtenidos para este tipo de algoritmos coinciden con los que se obtienen mediante el uso de otros métodos conocidos y ampliamente extendidos en la literatura, como son el método de sustitución, el método del árbol de recursión y el método maestro (véase [3]). Sin embargo, las técnicas basadas en el uso de las ecuaciones en diferencias presentan la ventaja, con respecto a las ya mencionadas, de permitir llevar a cabo un razonamiento estructurado y mecanizado al analizar la complejidad algorítmica que, además, destaca por su simplicidad y elegancia.

#### REFERENCIAS

- [1] G. Brassard, P. Bratley, *Algorítmica: Concepción y Análisis*, Editorial Masson, Barcelona, 1990.
- [2] G. Brassard, P. Bratley, *Fundamentos de algoritmia*, Prentice-Hall, Madrid, 1997.
- [3] T.H. Cormen, C.E. Leiserson, L.R. Rivest, C. Stein, *Introduction to Algorithms*, MIT Press, Massachusetts, 2001.
- [4] P. Cull, M. Flahive, R. Robson, *Difference Equations: From Rabbits to Chaos*, Springer, New York, 2005.

# Diseño de sfiCAN: un inyector físico de fallos para redes CAN basado en una topología en estrella

David Gessner, Manuel Barranco, Alberto Ballesteros, Julián Proenza  
 Dpt. Matemàtiques i Informàtica, Universitat de les Illes Balears, Spain  
 {david.gessner, manuel.barranco, julian.proenza}@uib.es

**Abstract**— Este artículo presenta el diseño y parcial implementación de sfiCAN: un inyector físico de fallos para el bus CAN que permite la creación de una gran variedad de escenarios de fallos. El inyector de fallos reemplaza la topología bus de CAN por una estrella, cuyo elemento central es un *hub* con mecanismos de inyección de fallos. El inyector de fallos es fácilmente configurable, desde un PC conectado a un puerto dedicado del *hub*. Para ello se usa una especificación de inyección de fallos, la cual es traducida a un protocolo de configuración por encima de CAN. Este protocolo sólo es usado entre tests y por ello no interfiere en la ejecución de éstos. El propósito del inyector de fallos es comprobar el comportamiento de los nodos de una red CAN en presencia de errores en el canal. En particular, el comportamiento de los controladores CAN de los nodos y del *software* que se ejecuta en ellos, para los cuales la topología de estrella es transparente.

## I. INTRODUCCIÓN

Controller Area Network (CAN) [1] es un bus de campo ampliamente usado en sistemas distribuidos empotrados (DÉS) y entornos hostiles. Aunque CAN posee múltiples mecanismos que lo hacen robusto en tales entornos, los fallos son todavía posibles. Por lo tanto, en aplicaciones críticas, se requiere un estudio preciso de la respuesta del sistema ante tales fallos. Para ello, la inyección de fallos, que consiste en la generación artificial de fallos, es particularmente útil.

Los fallos artificiales pueden ser generados en un modelo simulado del sistema o en un prototipo físico. El primero tiene la ventaja de que puede ser testeado antes de que el prototipo esté disponible, pero es menos realista y preciso. Por lo tanto, para sistemas críticos se recomienda evaluar el sistema con un inyector físico de fallos, una vez el prototipo está disponible. Esta evaluación debe incluir, particularmente, los nodos del DÉS, que deben asemejarse lo más posible a los de producción, es decir, deben ser evaluados con el *software* de producción. Es más, el comportamiento del sistema debe ser testeado bajo una variedad de fallos suficiente, que puede incluir escenarios de fallo complejos y/o no deseados, como fallos de inconsistencia, es decir, fallos que afectan sólo a algunos nodos. Hasta donde sabemos, en el momento de la redacción de este artículo, no existe ningún inyector de fallos para CAN que satisfaga estos requerimientos. Este artículo presenta el diseño y preliminar implementación de un inyector físico de fallos para CAN que los satisface.

El inyector utiliza una topología de estrella para CAN, la cual es transparente desde el punto de vista de los nodos. La figura 1 muestra la arquitectura de sfiCAN. Cada nodo se conecta al *hub*, donde reside un módulo de inyección de fallos,

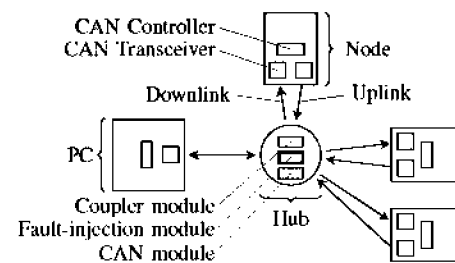


Fig. 1. Arquitectura de inyección de fallos.

por medio de un enlace dedicado, compuesto por un *uplink* y un *downlink*. El controlador CAN del nodo se conecta a su enlace mediante dos *transceivers* usando una configuración idéntica a la utilizada en CANcentrate [2]. Dentro del *hub*, un *módulo de acoplamiento* implementa la AND cableada de CAN, realizando una AND lógica de las señales del *uplink*, para después transmitir el resultado a través de todos los *downlinks*. El bus CAN se implementa de manera lógica, pero con la ventaja de poder inyectar los fallos localmente en los nodos, con suficiente granularidad para afectar únicamente a la señal entrante o saliente. El *hub* también posee un *módulo CAN*. Su función es observar la señal acoplada, obtenida del módulo de acoplamiento, y informa al módulo de inyección de fallos el campo y el bit de la trama transmitida en el instante. Si se añaden más módulos al *hub*, el inyector de fallos puede ser usado en topologías CAN de estrella más avanzadas, por ejemplo, si se implementa el módulo de tratamiento de fallos de CANcentrate [2], el inyector de fallos puede usarse para inyectar fallos en una red CANcentrate.

El *hub* posee un puerto dedicado al que se conecta un computador personal (PC). Este enlace no se divide en *up-* y *downlink* ya que no se inyectan fallos en él. Además, esto permite conectar el PC usando una controladora CAN estándar.

La conexión PC-*hub* permite configurar de manera sencilla el módulo de inyección de fallos. Esto es posible gracias a que este módulo es una instancia de un *componente de red configurable* (NCC), es decir, un componente conectado a la red que puede recibir su configuración desde esta misma red.

El resto del artículo se organiza de la siguiente manera. La sección II describe los modos de funcionamiento de un NCC, mientras que la sección III explica como se especifica la configuración que va a ser aplicada al módulo de inyección de fallos. La sección IV describe, a grandes rasgos, la implementación de este módulo. La sección V describe un ejemplo de inyección de fallos y la sección VI trabajos relacionados. Finalmente, la sección VII concluye este artículo

y pone énfasis al trabajo futuro.

## II. MODOS DE OPERACIÓN DE UN NCC

Un componente de red configurable puede trabajar en cuatro modos: *modo de configuración*, *modo ocioso*, *modo de espera* y *modo de ejecución*.

Un NCC entra en modo de configuración cuando el PC envía una trama *entra-modo-configuración*. El identificador de esta trama es el de mayor prioridad, que está reservado para ser transmitido exclusivamente por el PC.

Durante el modo de configuración el PC transmite *comandos de configuración* codificados en tramas CAN. Es más, cada NCC se identifica mediante un *identificador de NCC*. Este ID es un identificador CAN corriente, pero durante el modo de configuración se interpreta como un NCC ID. Esto permite enviar comandos de configuración a un componente en particular sin que sea interpretado por otro, es decir, direccionamiento *unicast*. Por otro lado, los identificadores CAN pueden ser usados por los nodos para sus propósitos durante el funcionamiento normal de la red.

El único NCC implementado actualmente es el módulo de inyección de fallos. Éste posee su propio conjunto de comandos de configuración. Si más tarde se añaden nuevos NCCs, sería necesario crear nuevos conjuntos de comandos de configuración para éstos.

La configuración de un NCC acaba con una *trama entra-modo-ocioso* o *trama entra-modo-espera*. La primera obliga al NCC a entrar en modo ocioso, mientras que la segunda le obliga a entrar en modo de espera. Un componente en modo ocioso ignora todas las tramas excepto la de *entra-modo-configuración*; en el modo de espera, ignora todas las tramas excepto la de *entra-modo-configuración* y la de *entra-modo-ejecución*. La trama de *entra-modo-ejecución* es transmitida por el PC a todos los nodos simultáneamente, indicando el principio del modo de ejecución. En el modo de ejecución los componentes empiezan a realizar su tarea, por ejemplo, un inyector de fallos inyecta fallos según su configuración.

La distinción entre el modo ocioso y el modo de espera permite deshabilitar NCCs en un test determinado.

## III. ESPECIFICACIÓN DE INYECCIÓN DE FALLOS

La configuración del módulo de inyección de fallos se realiza mediante la especificación de un fichero de texto: la *especificación de inyección de fallos*. El listado 1 muestra su definición en la forma de Backus-Naur (BNF) con la sintaxis de ISO/IEC 14977 [3]. La especificación contiene una serie de *configuraciones de inyección* etiquetadas, que son un conjunto de tuplas clave-valor, cada una de las cuales denominamos *parámetro de configuración*. Por brevedad, del BNF se omite el carácter de final de línea, que debe suceder cada parámetro de configuración, así como la definición de una cadena de caracteres o *string*, un número *natural* y un valor *boolean*, cuya definición es la corriente.

Los parámetros de configuración indican qué, dónde y cuando inyectar. Qué inyectar se define mediante un *valor de inyección*, por ejemplo, un valor dominante (`stuckDominant`) o una secuencia de bits (`bitFlip`, definiendo la secuencia

```

specification = { '[', string, ']', fi_config }
fi_config = value, link, time ;
value = 'value_type', '=', value_type_value,
        ['value_bfvalue', '=', {'0'|'1'} ] ;
link = 'link', '=', link_value ~ 'coupled' ;
time = mode, start_trig, start,
        end, [end_trig] ;
start_trig = 'start_trig_count', '=', natural,
            'start_trig_filter', '=', filter_value,
            'start_trig_field', '=', field_value,
            'start_trig_link', '=', link_value,
            ['start_trig_role', '=', role_value ] ;
start = 'start_field', '=', field_value,
        'start_bit', '=', natural,
        'start_offset', '=', natural ;
end = 'end_bc', '=', natural
     | 'end_field', '=', field_value,
     | 'end_bit', '=', natural ;
end_trig = 'end_trig_count', '=', natural,
          'end_trig_filter', '=', filter_value,
          'end_trig_field', '=', field_value,
          'end_trig_link', '=', link_value,
          ['end_trig_role', '=', role_value ] ;
mode = 'full' | 'iterative' | 'selective' ;
value_type_value = 'stuckDominant' | 'stuckRecessive' |
                  'bitFlip' | 'inverse' ;
filter_value = ('0'|'1'|'x'), {'0'|'1'|'x'} ;
link_value = 'port0up' | 'port0dw' | 'port1up'
            | 'port1dw' | 'port2up' | 'port2dw'
            | 'port3up' | 'port3dw' | 'coupled' ;
field_value = 'idle' | 'id' | 'rlr' | 'res'
            | 'dlc' | 'data' | 'crc' | 'crcdelim'
            | 'ack' | 'ackdelim' | 'eof'
            | 'interfield' | 'errflag' | 'errdelim' ;
role_value = 'dont_care' | 'tr' | 're' ;

```

Listing 1. Especificación de la inyección de fallos en BNF.

con `value_bfvalue`). Dónde inyectar se define mediante un *enlace destino de inyección*, por ejemplo, el *downlink* del puerto 1 (`link = port1dw`). La especificación de cuándo inyectar es más compleja. Primero, el *trigger de inicio* indica la condición que debe satisfacerse antes de inyectar un fallo. Por ejemplo, un *trigger de inicio* puede ser la tercera recepción de un CRC (`start_trig_field = crc`, `start_trig_count = 3`) que empieza con el prefijo '0101' o '0111' (`start_trig_filter = 01x1`) y es detectado en el *downlink* del puerto 2 (`start_trig_link = port2dw`) cuando el nodo conectado al enlace destino de la inyección es el transmisor (`start_trig_role = tr`). La trama que satisface el *trigger de inicio* se denomina la *trama de inicio*. Seguidamente, es necesario especificar el conjunto de bits a inyectar. Para este propósito se definen dos grupos de tuplas clave-valor, denominados *start* y *end*. El primero especifica el primer bit en el que inyectar, mientras que el segundo indica la duración de la inyección. Esta duración se define como una cuenta de bits o una condición: el campo y bit que ya no debe ser inyectado. También es posible definir un *trigger de fin*. Un *trigger de fin* es una condición que debe satisfacerse para detener la inyección. Se define de la misma manera que un *trigger de inicio*, excepto por la posibilidad de omitirlo, lo que indica una inyección ilimitada, es decir, un fallo permanente. La trama que satisface el *trigger de fin* se denomina *trama de fin*. Entre las tramas de inicio y fin pueden ser transmitidas varias tramas. El *modo de inyección de fallos* define cómo se inyecta en estas tramas. En el modo *full-range*, se inyecta en todos los bits desde *start*, en la trama de inicio, hasta *end*, en la trama de fin. En el modo *iterative* *start* y *end* indican el rango, dentro de cada trama entre la trama de inicio y fin, donde se llevará a cabo la inyección. El modo *selective* es igual

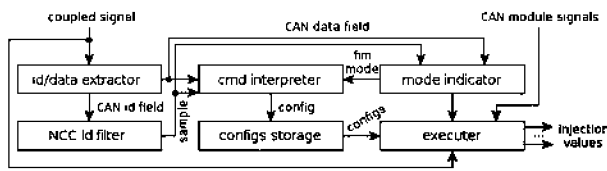


Fig. 2. Diagrama del módulo de inyección de fallos.

al iterativo, excepto que la inyección sólo se lleva a cabo en las tramas que satisfacen la condición del *trigger* de inicio.

No todas las especificaciones sintácticas correctas son válidas semánticamente. Por ejemplo, en el arbitraje (campo ID) la especificación de un rol es inválida, ya que éste solo se puede determinar al final del arbitraje.

Cada parámetro de configuración es codificado por el PC como una o varias instrucciones de configuración, cada una de los cuales se convierte en una trama CAN. Estas tramas poseen el NCC ID del módulo de inyección de fallos destino. Para configurar el módulo de inyección de fallos, el PC transmite la trama global de entra-modo-configuración para después hacer lo propio con las instrucciones de configuración. El módulo de inyección de fallos decodifica estas instrucciones y se auto-configura en consecuencia.

#### IV. ASPECTOS DE IMPLEMENTACIÓN

Implementamos tres módulos en el *hub*: acoplamiento, CAN y inyección de fallos. El de acoplamiento y CAN se han reutilizado de CANcentrate[2], mientras que el módulo de inyección de fallos es nuevo. Se ha sintetizado todo en una FPGA Xilinx Spartan-3 XC3S1000.

La figura 2 muestra el interior del módulo de inyección de fallos. Contiene los siguientes submódulos. (I) El *ID/data extractor* extrae el campo ID y el campo de datos de la última trama transmitida. (II) El *NCC ID filter* comprueba si el ID anteriormente extraído concuerda con el NCC ID del módulo de inyección de fallos. En caso afirmativo, genera una señal que provoca que tanto el *mode indicator* como el *command interpreter* lean el campo de datos facilitado por el *ID/data extractor*. (III) El *mode indicator* comprueba si el campo de datos se corresponde con una instrucción de cambio de modo, por ejemplo, desde el modo de configuración al ocioso. En tal caso, señala el nuevo modo al *command interpreter* y al *executer*. (IV) El *command interpreter*, durante el modo de configuración, comprueba si el campo de datos recibido contiene una instrucción de configuración de un parámetro, en vez de uno de cambio de modo. A partir de todas estas instrucciones construye una configuración de inyección de fallos física, que es enviada al módulo *configurations storage* cuando la instrucción de final de configuración es recibido. (V) El *configurations storage* almacena todas las configuraciones de inyección de fallos y las hace disponibles para el módulo *executer*. (VI) El *executer* contiene un conjunto de *ejecutores de configuración programables*, que son módulos que, durante el modo de configuración, son programados según una de las configuraciones almacenadas. Durante el modo de ejecución estos módulos llevan a cabo, según su programación, la inyección de fallos.

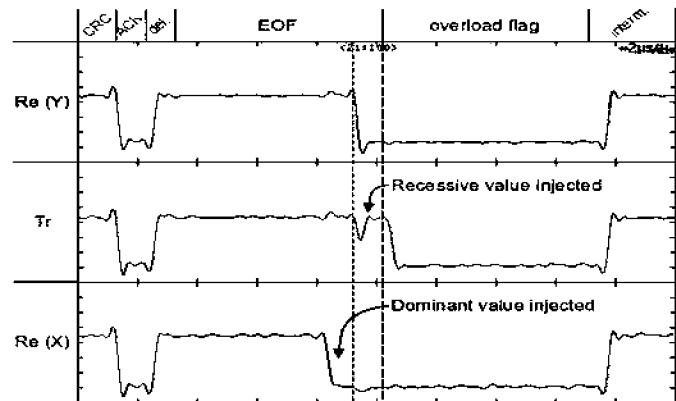


Fig. 3. Escenario IMO.

#### V. EJEMPLO DE USO

La figura 3 muestra una captura tomada con un osciloscopio digital Yokogawa DL7440. La imagen fue tomada mientras el inyector de fallos inyectaba los fallos que conducen a un escenario de inconsistencia por omisión de mensaje, descrito en [4]. Se ha insertado una anotación, a la izquierda de la captura, con el rol del nodo correspondiente a cada señal mostrada. Re(Y) y Re(X) son las señales del *downlink* de los nodos receptores Y y X, respectivamente; Tr es la señal del *downlink* del nodo transmisor. Además, en la parte superior, se muestran los campos de la trama CAN transmitida, vista por el nodo etiquetado como Y. Las marcas en el eje X no delimitan bits, sino intervalos de  $2 \mu\text{s}$ . Las dos líneas verticales discontinuas en el centro de la imagen marcan los límites del último bit del campo *end of frame*.

Como se muestra en la captura, un bit dominante es inyectado en el penúltimo bit del *downlink* del nodo etiquetado como X, el cual, consecuentemente genera un *error flag*. El primer bit de este *error flag*, sin embargo, no es detectado por el transmisor, etiquetado como Tr, gracias a un bit recessivo inyectado en su *downlink*. En el nodo etiquetado como Y no se inyecta ningún error, el cual, por tanto, detecta el primer bit del error flag. El comportamiento de los nodos se describe en [4]: el nodo X rechaza la trama, el nodo Y la acepta y el nodo Tr no la retransmite.

El listado 2 muestra la especificación usada para generar el escenario IMO. Sin embargo, debido al limitado espacio se obvia su descripción.

#### VI. TRABAJO RELACIONADO

En 2003, se propuso un inyector físico de fallos para CAN [5], afirmando ser el único capaz de generar escenarios de fallo complejos. En este artículo, sólo se consideran el citado inyector y un segundo, siendo los únicos inyectores físicos de fallos para CAN publicados entre 2003 y la fecha de escritura de este artículo.

El inyector de fallos presentado en [5] utiliza una herramienta *software* llamada CANfidant, y varios *inyectores de fallos individuales* (IFI), que son circuitos *hardware* insertados entre el *transceiver* y el controlador CAN de cada nodo. Este inyector de fallos requiere, a priori, un completo conocimiento de las tramas transmitidas en el bus. Conociendo el tráfico, CANfidant ayuda al ingeniero en el diseño del escenario de

error, simulando el comportamiento bit a bit y generando las instrucciones para los IFIs. Los IFIs, posteriormente, inyectan cada fallo contando las tramas y bits desde el principio del test. De este modo, si las tramas no se transmiten en el orden esperado, lo cual no es difícil en redes CAN dirigidas por eventos, la inyección se realiza incorrectamente. Por el contrario, sfiCAN, además de poder generar complejos escenarios de fallo, no requiere de un conocimiento previo del tráfico. No obstante, es posible usarlo junto con un simulador. Por ejemplo, es factible simular con CANfidant escenarios específicos, para posteriormente crear una especificación de inyección de fallos para sfiCAN.

En [6] se presenta un inyector de fallos que puede ser acoplado a una red CAN existente, como un nodo más. Aunque este acercamiento tiene la ventaja de no requerir una modificación de la red o de los *transceivers* de los nodos, proporciona una baja resolución espacial en la inyección, ya que éstas siempre afectan a toda red. Por lo tanto, este acercamiento no permite generar escenarios de inconsistencia como los descritos anteriormente. Además, las posibilidades de configuración son mucho más restringidas que en sfiCAN.

## VII. CONCLUSIONES Y TRABAJO FUTURO

En este artículo se presenta sfiCAN: un inyector de fallos, configurable por red, basado en una topología de estrella, que permite la creación de escenarios de fallo complejos mediante la inyección de fallos físicos en una red CAN. El uso de la topología en estrella, con un hub central, cuyos enlaces están separados en *uplink* y *downlink*, permite que los fallos sean inyectados con una alta resolución espacial; mientras que el módulo CAN residente en el *hub*, que lleva el seguimiento del campo y bit de la trama transmitida, permite inyecciones de fallos con alta resolución temporal. Además, el hecho de poder almacenar y ejecutar múltiples configuraciones simultáneamente, en el módulo de inyección de fallos, y que éstos pueden ser especificados usando diferentes parámetros de configuración (como se ha ilustrado en el BNF del listado 1), hacen de sfiCAN un inyector muy flexible y potente. Finalmente, el impacto sobre el sistema de test es muy bajo: introduce un pequeño retardo, que puede ser tratado como un retardo adicional en la transmisión, y requiere la reserva de un identificador CAN durante la ejecución del test.

Se proponen dos usos para este inyector de fallos. Primero, comprobar como los controladores y el software de una red CAN responden ante fallos en el canal, en cuyo caso modificar la topología a una estrella no es relevante, ya que no es el canal lo que se comprueba. Segundo, comprobar topologías CAN en estrella —en particular los sistemas (Re)CANcentrate desarrollados bajo el proyecto CANbids<sup>1</sup>.

Este artículo también aborda el uso de NCCs en CAN. En general, es una solución muy flexible, ya que permite desplegar componentes heterogéneos dentro de los nodos u otros dispositivos de la red CAN. El uso de diferentes NCC permite la construcción de una infraestructura de test automatizada para CAN.

<sup>1</sup><http://srv.uib.es/project/12>

```

1  [[fault injection 1]]
2  value_type      = stuckDominant
3  link            = port1dw
4  start_trig_count = 1
5  start_trig_filter = 10110101010
6  start_trig_field = id
7  start_trig_link  = coupled
8  start_trig_role  = re
9  start_field      = eof
10 start_bit        = 5
11 start_offset     = 0
12 end_bc           = 1
13 mode            = full
14 [[fault injection 2]]
15 value_type      = stuckRecessive
16 link            = port0dw
17 start_trig_count = 1
18 start_trig_filter = 10110101010
19 start_trig_field = id
20 start_trig_link  = coupled
21 start_trig_role  = tr
22 start_field      = eof
23 start_bit        = 6
24 start_offset     = 0
25 end_bc           = 1
26 mode            = full
    
```

Listing 2. Ejemplo especificación de una inyección de fallos

Un NCC relevante que se planea añadir al *hub* es el *logging module*. Su propósito es capturar información valiosa durante la fase de ejecución de un test, para después transmitir estos datos en la fase de configuración, cuando se le requiera. El hecho de situar este NCC dentro del *hub* le otorga una visión privilegiada del sistema, lo que le permite conocer qué ha sido transmitido hacia y desde cada nodo, así como información del estado interno de otros módulos residentes dentro del *hub*. Por otro lado, la transmisión de todos esos datos al PC permitirá su correcto análisis.

## RECONOCIMIENTO

Este trabajo ha recibido el apoyo del Ministerio Español de Ciencia e Innovación con la subvención DPI2008-02195 y financiación de FEDER, además de la portuguesa Fundação para Ciência e a Tecnologia con la subvención SFRH/BP-D/70317/2010.

## REFERENCES

- [1] Robert Bosch GmbH, "CAN Specification Version 2.0," 1991. [Online]. Available: <http://www.semiconductors.bosch.de/pdf/can2spec.pdf>
- [2] M. Barranco, J. Proenza, G. Rodríguez-Navas, and L. Almeida, "An Active Star Topology for Improving Fault Confinement in CAN Networks," *IEEE Transactions on Industrial Informatics*, vol. 2, no. 2, pp. 78–85, May 2006. [Online]. Available: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1377714>
- [3] "International Standard ISO/IEC 14977 - Information technology - Syntactic metalanguage - Extended BNF," 1996.
- [4] J. Proenza and J. Miro-Julia, "MajorCAN: A Modification to the Controller Area Network Protocol to Achieve Atomic Broadcast," *IEEE International Workshop on Group Communication and Computations, Taipei, Taiwan*, 2000.
- [5] G. Rodríguez-Navas, J. Jiménez, and J. Proenza, "An architecture for physical injection of complex fault scenarios in CAN networks," in *Proc. 9th IEEE Int. Conf. on Emerging Technologies and Factory Automation*, vol. 2, 2003. [Online]. Available: <http://home.david/Documents/bibliography/papers/arch-for-phys-fault-inj-in-CAN.pdf>
- [6] M. S. Recordá and M. Violante, "On-line analysis and perturbation of CAN networks," in *Proc. 19th IEEE Int. Symp. on Defect and Fault Tolerance in VLSI Systems, 2004*. [Online]. Available: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1347867>

# Disseny i Implementació d'un Receptor GPS per Aplicacions amb Microcontroladors

T. R. Parets i B. Alorda

*Enginyeria Tècnica Industrial, Especialitat en Electrònica Industrial*  
 tomas.parets@gmail.com

**Resum**— El present document recull el resultats obtinguts en el projecte final de carrera basat en el disseny i la implantació d'un receptor de posicionament global o *Global Positioning System* (GPS) per aplicacions basades amb microcontroladors. Es descriuen tant el programari, com el maquinari dissenyat en la implementació. El receptor GPS es transforma en una plataforma que permet la programació per a múltiples aplicacions fent que la informació de posicionament sigui accessible en múltiples formats. El sistema es dissenya tant per proporcionar informació de la posició actual en temps real, com la possibilitat de realitzar trases o seqüència de punts que són emmagatzemades a dins la memòria del sistema per després poder ser enviades a un ordinador o a un altre sistema electrònic pel seu posterior processat.

## 1. INTRODUCCIÓ

Avui en dia existeix una creixent demanda d'aparells que disposin d'aplicacions les quals precisen d'informació sobre posicionament geogràfic. És per aquest motiu que el receptor GPS és un element cada vegada més comú en els dissenys de sistemes electrònics. El posicionament per GPS es basa en un sistema d'orientació i navegació que mitjançant la recepció i el processament de la informació emesa per una constel·lació de 24 satèl·lits (NAVSTAR) que orbiten al voltant de la terra, com es mostra a l'esquema de la Figura 1. Aquesta distribució de satèl·lits és capaç d'establir les coordenades geoplanetàries on es troba el receptor [1].

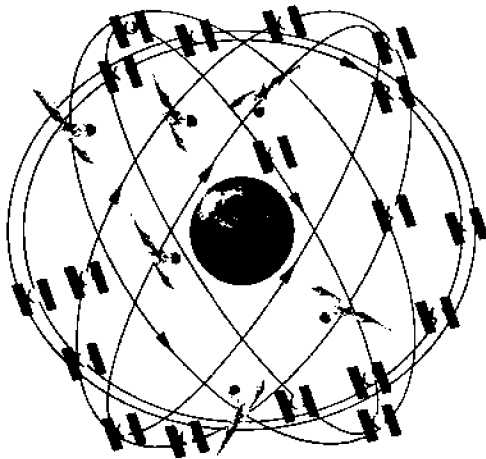


Fig. 1 Estructura general del sistema

Els receptors GPS, formats per una antena i un circuit receptor i descodificador del senyal, es comuniquen amb altres sistemes mitjançant un protocol de comunicació molt usat entre instruments d'ús marí i definit per la *National Marine Electronics Association* dels EEUU (NMEA 0183) [2]. El protocol NMEA es basa en la transmissió usant el protocol

de transmissió físic RS232 de trames de dades en codi ASCII de forma asíncrona. Aquestes trames són generades pel receptor de forma contínua sense interrupció, per tant no es tracta d'un tipus *mestre-esclau* on la informació de posicionament només sigui transmesa en el cas en que el mestre la sol·liciti. El receptor des del moment en que rep alimentació comença a enviar trames amb el format NMEA i ha de ser el sistema que llegeix les trames l'encarregat de determinar quan les trames són correctes, quines són les trames que interessin segons l'aplicació i sobretot, quina és la posició global del sistema. És per aquest motiu, que es vol dissenyar un sistema microcontrolat que sigui capaç de llegir aquestes trames i proporcioni la informació de posicionament només quan se li sigui sol·licitada o que sigui capaç d'emmagatzemar diferents trases de ruta seguint qualche regla temporal o d'espai entre preses de posició. D'aquesta forma s'allibera al sistema principal de la tasca de llegir constantment les trames rebudes des del receptor GPS i la seva posterior interpretació.

Per a realitzar la localització GPS, la informació és emesa per cada satèl·lit en format digital. La informació emesa es distribueix en dues sèries de dades conegudes com *ALMANAQUE* i *EFEMÉRIDES* [3]. Les dades que contenen aquestes dues sèries informen sobre l'estat operatiu del satèl·lit, la seva situació orbital, data i hora juntament amb l'identificador del satèl·lit.

A partir d'aquestes dades es determinen la posició del receptor sobre la terra mitjançant triangulació. És per això que es necessita la recepció de senyal de almenys tres satèl·lits.

El sistema que es proposa està pensat per a poder ser emprat com a receptor GPS portàtil. Aquest anirà instal·lat dins una capsa i alimentat amb bateries per a poder ser transportat. Així es podrà funcionar independentment o conjuntament amb un altre sistema més complexa al qual es connectarà com un perifèric més. Es disposarà de connexions tipus USB i SPI per a facilitar la interconnexió amb altres sistemes.

Les passes seguides en aquest projecte per arribar al disseny definitiu són:

- *Disseny de l'estructura i funcions del sistema.* S'han determinat les característiques/funcions de les que disposa el sistema per, en funció d'aquestes, determinar el número i tipus de components necessaris: perifèrics, dispositius per interactuar l'usuari amb el sistema, etc.
- *Selecció de components.* Una vegada es tenen definides les funcions, es seleccionen els components que les realitzaran. Aquesta selecció s'ha fet amb criteris d'espai dins la capsa i cost del component.

- *Disseny d'una placa de circuit imprès* pel suport/interconnexió dels diferents components.
- *Procés de soldadura*. En aquesta etapa s'han soldat tots els components que formen el sistema un darrera l'altre, realitzant les comprovacions per a verificar el correcte funcionament.
- *Desenvolupament de Drivers*. S'han realitzat les tasques de programació i verificació de les funcions per interactuar amb els perifèrics disponibles.
- *Desenvolupar una petita aplicació exemple* que emmagatzemi dades de posicionament GPS i sigui capaç de transferir-les a un PC o a un altre dispositiu electrònic connectat o bé al port SPI (Serial Peripheral Interface) o bé al port USB (Universal Serial Bus).

## II. DEFINICIÓ DEL SISTEMA

A l'hora de dissenyar un sistema GPS el primer element a seleccionar és en el receptor. En aquest cas s'ha seleccionat un receptor GPS Fastrax UC322 [4] del qual, es disposa d'un entrenador, que ha permès la verificació dels requeriments proposats en el projecte, una primera introducció al llenguatge NMEA 0183 i al funcionament del circuit receptor. L'esquema del sistema complet es mostra a la Figura 1 on es poden veure altres elements a més del receptor GPS: un sistema de memòria externa, un mòdul de comunicacions per USB mitjançant una pasarel·la RS232-USB del fabricant FTDI [5] i un sistema de comunicacions amb un altre sistema extern mitjançant les especificacions del bus SPI.

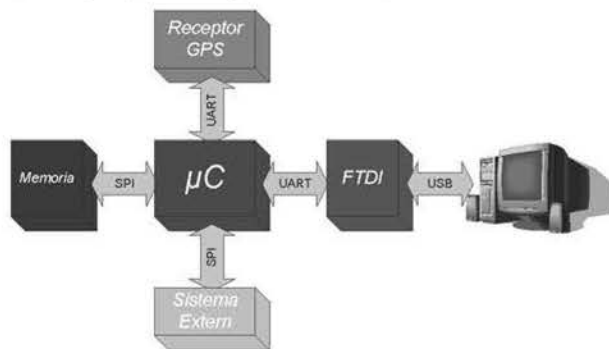


Fig. 2 Estructura general del sistema

A la Figura 2, es pot veure com el microcontrolador és l'element central del sistema dissenyat i el pont de comunicació entre els diferents perifèrics, d'aquesta manera, les trames del receptor GPS són processades i enviades de diverses formes a la resta de perifèrics. Així, el microcontrolador podria actuar tant fent tasques senzilles de traducció de protocols com tasques més complexes on s'analitzés la trama rebuda i s'acongués la informació de posicionament.

Les quatre funcions proposades en l'aplicació seran:

- *Passarel·la*, on es farà una captura de les trames NMEA del receptor i es transmetran a través dels ports USB/SPI.
- *Captura de posicions continua*, en aquest cas es capturaran constantment les dades de posicionament i amb intervals de temps fixats s'aniran guardant a la memòria.

- *Captura de posicions aleatòria*, en aquest cas s'aniran capturant les dades de posicionament contínuament, però només s'emmagatzemaran a la memòria quan l'usuari premi el botó.
- *Bolcat de dades*. Aquesta funció s'implementa per a transferir les dades que s'han anat emmagatzemant a la memòria tant en el mode de captura contínua com en el mode aleatori via els ports USB/SPI.

## III. IMPLEMENTACIÓ DEL SISTEMA

Un dels requisits considerat com important és la capacitat d'adaptació del sistema a múltiples aplicacions. Per aquest motiu es van incorporar opcions que donessin lloc al treball aïllat del sistema, però també que permetés el treball conjunt amb altres sistemes de forma senzilla. A més, es volia poder disposar de la possibilitat per desconnectar el receptor GPS i poder-lo connectar amb un altre microcontrolador per a dotar al conjunt de major potència o introduir millores posteriors. Amb tots aquests requeriments es va definir l'estructura de la Figura 3. Aquesta estructura no es va concebre en una única PCB, sinó que tot el sistema es va dividir en dues parts ben diferenciades: El receptor GPS i les seves opcions de programació, juntament amb els buffers i la selecció de modes es va implementar en una PCB que s'ha anomenat PCB\_RECEPTOR, mentre que la resta de components que estaven més lligats a una possible aplicació final s'ha implementat en una segona PCB anomenada PCB\_APLICACIÓ.

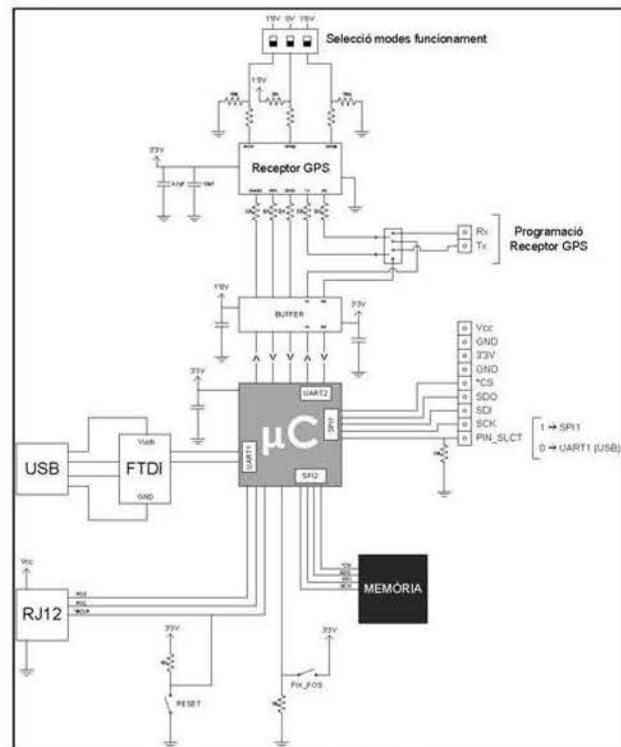


Fig. 3 Esquema complet del sistema proposat

L'esquema mostrat a la Figura 3 es va implementar usant l'eina EAGLE [6] que conté tant un entorn per disseny d'esquemàtics, com un entorn per disseny de les PCBs.

Vegem a continuació una descripció més detallada de cada un dels blocs que formen part de la implementació feta.

### A. Font d'Alimentació

El sistema requereix de dos nivells d'alimentació: alimentació de 3.3v per a tots els circuits de control i d'aplicació i 1.8v pels senyals que provenen del receptor GPS. Degut a que la principal font d'alimentació del sistema és una bateria de 9V del tipus LR6, es decideix dissenyar una font d'alimentació amb una configuració en cascada (Figure 4). La primera etapa es connecta directament al pla d'alimentació de la

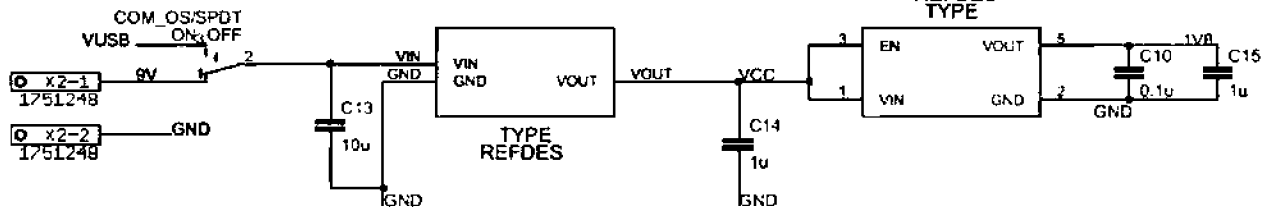


Fig. 4 Detall de l'esquema de la font d'alimentació en cascada usada per proporcionar 3.3v i 1.8v a partir d'una bateria de 9v.

### B. Detector Nivell Bateria

Per a poder detectar la condició de nivell de la bateria baixa s'empra un detector de tensió, més concretament un TC54 de la casa MICROCHIP. Aquest detector disposa de tres pins, veure Figura 5. Un primer pin és el d'entrada. Aquest pin es connecta al node anomenat Vcc sortida del primer regulador de tensió.

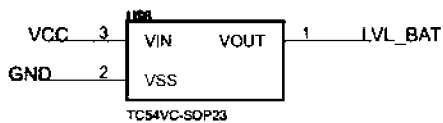


Fig. 5 Esquemàtic del circuit detector Nivell Bateria

El pin de sortida del detector va connectat directament al pin RC4 del PIC com es mostra a la Figura 6 amb l'etiqueta LVL\_BAT. Aquest senyal s'activarà quan la bateria es trobi amb càrrega baixa.

### C. Microcontrolador

El microcontrolador elegit és el PIC18F46J50. La principal característica d'aquest model és que disposa de dos ports RS232 i una matriu interna de reconexió de pins que permet connectar qualsevol pin exterior amb gairebé qualsevol perifèric intern.

Els perifèrics usats en el disseny són:

- 1) *EUSART*: La comunicació amb el receptor GPS es realitza amb un port de comunicació asíncron UART. Aprofitant un dels dos ports EUSART dels que disposa el PIC es realitzarà la comunicació.
- 2) *MSSP (Master Synchronous Serial Port)*: Com en el cas dels ports EUSART, els dos ports SPI disponibles en el PIC estan controlats per un mòdul hardware intern anomenat MSSP. Aquest perifèric intern s'emprarà en el disseny proposat per a comunicar amb la memòria externa i oferir l'accés a un port extern SPI per part d'un altre sistema.

PCB\_APLICACIÓ, d'aquesta manera es fa arribar el voltatge de 3.3V (Vcc) a tots els components.

Després del primer regulador, es connecta un segon regulador amb sortida a 1.8V que proporciona l'alimentació requerida a la PCB\_RECEPTOR. A més, i per mantenir les tensions de sortida estables, s'afegeixen una sèrie de capacitats, d'entrada i sortida, per tal de minimitzar senyals de renou sobre l'alimentació. La Figura 4 mostra amb detall l'esquema seguit per a implementar aquesta alimentació en cascada.

- 3) *RESET*: El mateix PIC disposa d'un pin (\*MCLR) que implementa aquesta funció. Aquest pin és actiu per nivell baix. Per a tenir la possibilitat de resetejar el PIC en el moment desitjat es preveu un polsador que força el nivell baix al pin \*MCLR. Dit polsador va connectat mitjançant una resistència de pull-up per forçar el nivell alt al pin sempre i quan no es premi el polsador.
- 4) *FIX\_POS*: Es disposa d'un polsador d'usuari per a poder interactuar el sistema. Aquest polsador s'ha proposat amb la funció de fixar posicions GPS a la memòria en el moment en que es premi. Encara que també pot ésser emprat per altres funcions, només cal que es programi tal com es desitja.
- 5) *Encoder*: A més d'aquest darrer polsador, per a poder interactuar amb el PIC es té també un *encoder*. Aquest *encoder* permet seleccionar el mode en el qual es vol que funcioni el PIC. Els diferents modes s'estableixen en el codi i són configurables.
- 6) *LED*: Com a mètode per a visualitzar l'estat o mode en que es troba funcionant el PIC s'empra un LED. Aquest està connectat a un pin de sortida del PIC. Així es poden elegir diferents freqüències d'intermitència per a distingir entre un mode o altre. Per a limitar el corrent que passa per aquest LED es col·loca una resistència en sèrie com es mostra a la Figura 6.
- 7) *Programació*: Per a programar el PIC és necessari dissenyar algun tipus de connector per tal de poder emprar el programador. En aquest cas es programa en llenguatge C i s'utilitza un ICD-U64 de la firma CCS [7]. El programador ICD-U64 disposa d'un connector del tipus RJ11. Es dissenya un adaptador que permeti passar del connector RJ11 a un tipus de connector que es pugui ubicar a sobre la placa. Degut a que el connector RJ11 femella que es necessita ocupa molt



d'espai a sobre la PCB, s'opta per emprar un altre tipus de connector i fabricar un adaptador per estalviar espai, facilitar la col·locació de la resta de components a

sobre la PCB i aconseguir utilitzar una caps de perfil baix per a tot el sistema.

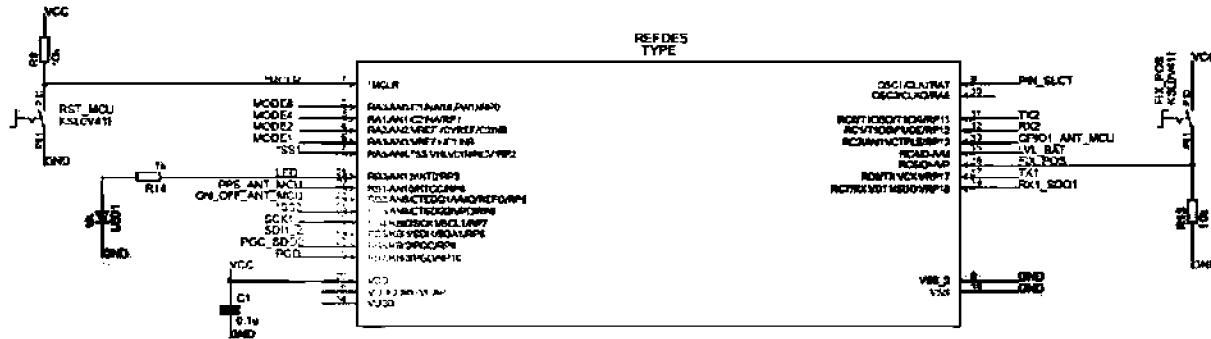


Fig. 6 Esquemàtic Microcontrolador

**D. Buffer**

El *buffer* es troba ubicat entre el PIC i el receptor GPS. Les tensions de funcionament del receptor GPS són diferents a les de la resta de components del sistema i té la funció de convertir els nivells de tensió dels senyals del PIC i del receptor GPS.

**E. Receptor**

El receptor que s'ha seleccionat per a integrar dins el present projecte està format per un transductor i una circuiteria que es capaç de processar la informació rebuda per tal de transmetre-la a través del port UART en format NMEA. La Figura 6 mostra un esquema de interconnexió del receptor usat i dels senyals que es connecten amb el microcontrolador.

S'haurà d'emprar un dels ports EUSART del PIC i 4 pins per a poder interactuar entre el PIC i el receptor. A més del port UART del receptor es disposa d'una entrada que activarà o desactivarà el receptor (pin ON\_OFF) i, en el cas en que no es precisi de la recepció de dades de geoposicionament, tenir l'opció d'aturar el receptor per tal d'estalviar energia.

Els senyals GPIO6 i GPIO2 permeten seleccionar el mode de funcionament del receptor. Es disposa de tres mètodes de funcionament tal com es mostra a la Taula 1.

En aquesta implementació, s'ha decidit utilitzar el format NMEA amb una velocitat de 57.600 bauds, encara que aquesta velocitat i mode de funcionament es podran seleccionar mitjançant un *switch* disponible sobre la PCB\_RECEPTOR.

TAULA I  
MODES DE FUNCIONAMENT DEL RECEPTOR

Configuració	1	2	3
GPIO6 input	low	high	low
GPIO2 input	low	low	high
Protocol	NMEA 3.01	SIRF binary	NMEA 3.01
Baud	4800,n,8,1	57600,n,8,1	57600,n,8,1

**F. Memòria**

La memòria seleccionada és del tipus *EEPROM* i s'accedeix a ella mitjançant un bus *SPI*. Concretament es

tracta d'una 25LC256 de la casa MICROCHIP [8]. Per seleccionar la memòria s'ha tingut en compte el format i longitud de les dades que s'emmagatzemaran. Cada dada referent a la posició està representada per una sèrie de caràcters. Aquests caràcters ocupen una longitud total de 32 bytes. El nombre posicions màxim a desar s'ha fixat a 1.000. Així doncs, es pot determinar que el nombre màxim de bytes d'una ruta de 1.000 punts serà de 32.000 bytes que en bits equival a 256kbits.

Es voldrà una velocitat d'accés a la memòria elevada, ja que, les dades enviades pel receptor GPS, es transferiran amb una velocitat màxima de 57.600 bauds d'aquesta manera no es perdrà informació del receptor GPS. Per aconseguir-ho es farà servir el perifèric intern MSSP que s'ocuparà de transmetre les dades a la memòria mentre la CPU dedica l'atenció a analitzar les trames NMEA.

**G. FTDI**

El PIC seleccionat disposa d'un mòdul de comunicació destinat exclusivament a les comunicacions USB. El motiu per el qual no s'ha emprat aquest mòdul i s'ha fet servir un mòdul extern al PIC és degut a la flexibilitat i facilitat que ens permetia aquest mòdul FTDI extern al PIC i permetre alliberar a la CPU de la gestió de la comunicació USB.

Emprant només dos pins del PIC, una com a senyal de transmissió de dades i l'altre com a recepció, s'aconsegueix establir una comunicació sèrie asíncrona amb el mòdul FTDI i aquest realitza les funcions de gestió de l'enviament USB. Així es descarrega el PIC del volum de dades que hauria de processar per a gestionar aquesta comunicació USB directament.

**IV. FABRICACIÓ DEL SISTEMA RECEPTOR**

Una vegada es tenen definits tots el components que aniran a sobre la PCB així com també les interconnexions que hi haurà entre aquests, s'ha passat a realitzar la tasca de localització i encaminament per a la qual s'ha emprat l'editor de plaques del mateix programa EAGLE.

El sistema complet es distribueix en dues PCB: la PCB\_RECEPTOR i la PCB\_APLICACIÓ. La implementació definitiva de les dues plaques es mostra a les Figures 7 i 8 on a la dreta es mostren les cares de la PCB\_RECEPTOR i a l'esquerra es mostren les cares de la PCB\_APLICACIÓ. A la

cara superior de la PCB\_RECEPTOR de la Figura 7 es pot identificar el receptor GPS amb les resistències i capacitats recomanades pel fabricant.

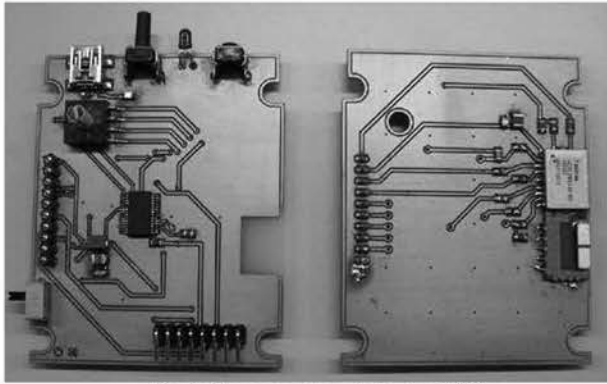


Fig. 7 Cares superiors de les dues PCBs

Sobre la capa superior de la PCB\_APLICACIÓ s'hi han localitzat el connector de programació, l'encoder, els botons d'usuari i de reset, el led, la pasarel·la FTDI i el connector mini-USB per a la connexió amb el PC.

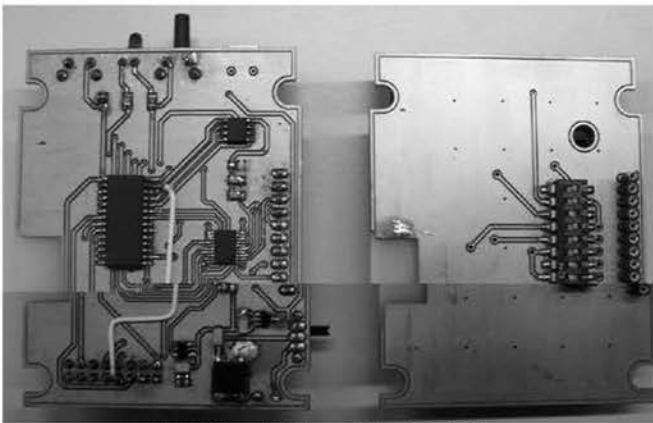


Fig. 8 Cares inferiors de les dues PCBs

A la capa interior de la PCB\_RECEPTOR mostrada a la Figura 8 s'hi identifica el selector dels modes de funcionament del receptor GPS. Mentre que a la cara inferior de la PCB\_APLICACIÓ es veuen el microcontrolador usat, la memòria EEPROM, el sistema d'alimentació i el circuit de buffers. Una vegada muntades les dues PCBs s'han dut a terme una sèrie de processos de comprovació del correcte funcionament de cada un dels elements per separat.

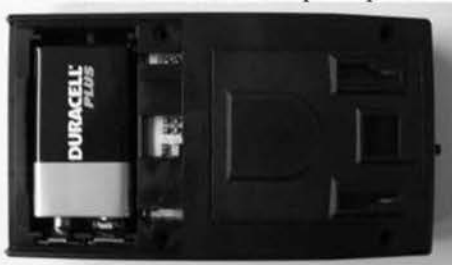


Fig. 9 Fotografia on es pot identificar la bateria i les PCBs situades dins la capsa. A la cara de la dreta sobresurt el boti d'usuari.

El sistema acabat es presenta en una capsa portàtil on tots els connectors i botons són accessibles des de l'exterior com es mostra a la Figura 9.

## V. PROGRAMACIÓ

Com a eina de programació s'ha decidit emprar el compilador CCS, (PIC C Compiler) [7]. Aquest compilador ha estat seleccionat per oferir la possibilitat de poder programar en llenguatge C. El programa principal s'ha estructurat en tres seccions. En primer lloc s'ha configurat el PIC ajustant la velocitat del rellotge, l'activació o no del *watchdog*, el tipus d'interrupcions actives, els valors de configuració dels perifèrics, etc. A continuació s'han definit els comportaments de cadascun dels ports de comunicació així com també els diferents pins d'entrada i sortida del PIC. Recordem que aquest model de PIC disposa d'una matriu interna de connexió que permet configurar els perifèrics interns amb diverses configuracions de pins d'entrada/sortida.

Finalment, s'ha dissenyat l'estructura principal del programa tal com es mostra a la Figura 10.

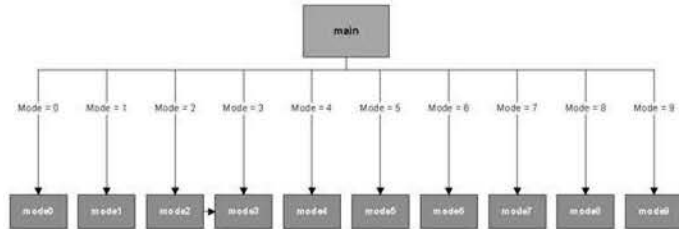


Fig. 10 Cares inferiors PCBs

Aquesta secció s'encarrega de fer una lectura de l'encoder (recordem que aquest dispositiu permet indicar el mode en el qual l'usuari vol que el sistema treballi) i, en funció del valor que s'ha llegit fer una cridada a un dels deu subprogrames anomenats *mode0...9* a la Figura 10.

En l'aplicació desenvolupada en aquest projecte s'han definit 4 modes amb les següents funcions:

- *mode0*, funció passarel·la. El PIC s'encarrega de rebre les dades del receptor GPS i enviar-les, directament i sense processar, cap a un PC connectat al port USB. La Figura 11 mostra una captura de pantalla amb les dades llegides pel port USB de l'ordinador en aquest mode i el traçat identificat amb el programa VisualGPS [9]. Així a la dreta de la Figura 11 apareixen el llistat de les diferents trames NMEA rebudes, cada línia és una trama diferent amb les dades que contenen. La gràfica de barres que apareix al costat esquerra superior mostra els identificadors dels satèl·lits que detecta el receptor i la qualitat del seu senyal. Quan més alta sigui la barra millor és la qualitat del senyal rebut. La gràfica polar en fons negre mostra la constel·lació de satèl·lits que veu el receptor com si s'estàs mirant al cel. A la zona central del programa es pot veure la traça històrica de punts validats que s'han aconseguit així el perfil d'altura d'aquesta ruta. Tota aquesta informació la proporcionen les diferents trames NMEA a mesura que el receptor GPS és capaç de calcular-les. Els programes com visualGPS (s'ha triat aquest programa en concret per tenir una llicència gratuïta) són capaços d'interpretar les trames NMEA directament i com es mostra a la Figura 11, aquest mode s'ha testejat amb aquest tipus de programa amb èxit.

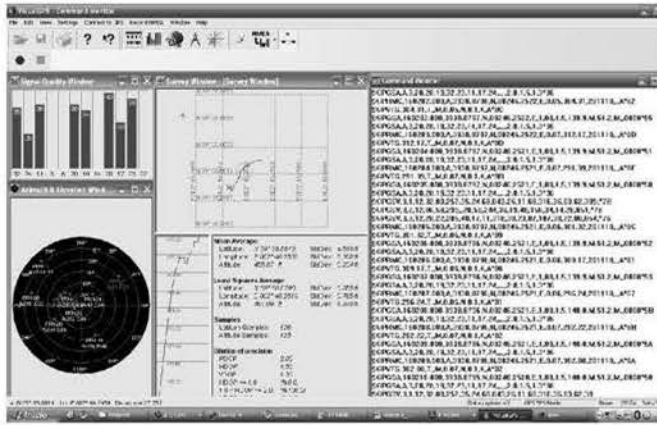


Fig. 11 Captura de dades en mode 0

- *mode1*, aquest segon mode emmagatzema, a la memòria EEPROM, les dades de posicionament vàlides amb intervals de temps predefinitos. Les dades desades dins la EEPROM són localitzacions geogràfiques vàlides. És a dir, s'espera a que el receptor GPS obtingui una posició vàlida i només es desen localitzacions correctes.
- *mode2*, ofereix un funcionament semblant al *mode1* però en aquest cas es guarden les dades de posicionament cada vegada que es premi el polsador del sistema. En aquest mode és l'usuari qui indica cada quan es desa una posició validada a la EEPROM.
- *mode3*, aquest mode s'empra per a fer el bolcat de dades. Es connecta el sistema a un PC a través del port USB i quan es prem el polsador d'usuari es fa un bolcat de totes les posicions que hi ha emmagatzemades a la memòria del sistema. La Figura 12 mostra una voltat realitzat en un experiment usant aquest mode.

```

\DA135003,000,3938,8737N00246,2430E\00
\DA135004,000,3938,8739N00246,2432E\00
\DA135005,000,3938,8743N00246,2436E\00
\DA135006,000,3938,8747N00246,2440E\00
\DA135007,000,3938,8751N00246,2444E\00
\DA135008,000,3938,8755N00246,2449E\00
\DA135009,000,3938,8759N00246,2453E\00
\DA135011,000,3938,8767N00246,2461E\00
\DA135012,000,3938,8770N00246,2464E\00
\DA135013,000,3938,8774N00246,2468E\00
\DA135014,000,3938,8777N00246,2471E\00
\DA135016,000,3938,8783N00246,2477E\00
\DA135017,000,3938,8785N00246,2480E\00
\DA135018,000,3938,8787N00246,2486E\00
\DA135019,000,3938,8790N00246,2490E\00
\DA135020,000,3938,8790N00246,2488E\00
\DA135021,000,3938,8787N00246,2477E\00
\DA135022,000,3938,8783N00246,2466E\00
\DA135023,000,3938,8780N00246,2453E\00
\DA135024,000,3938,8776N00246,2445E\00
\DA---- Mode 3 ----\00
    
```

Fig. 12 Cares inferiors PCBs

## VI. CONCLUSIONS

S'ha aconseguit desenvolupar un sistema GPS que com a apimpcipal avanatge presenta la possibilitat d'integrar-se en molts altres sistemes que no disposin d'aquest tipus de receptor. D'aquesta manera s'aconsegueixen augmentar les prestacions d'aquests tipus de sistemes.

A més hi ha la possibilitat de reprogramar el dispositiu receptor, ja que s'ha mantingut una connexió de programació

que aconseguiria adaptar el receptor GPS a les característiques del nou sistema.

La flexibilitat que ofereix al sistema a l'hora de modificar el programari del PIC no es troba en molts altres dispositius que es puguin trobar al mercat, d'aquesta manera es crea una sistema únic que pot esser exportat a diferents àmbits d'aplicació com puguin esser automoció, electrònica de consum, etc.

## REFERÈNCIES

- [1] <http://www.navstarinc.com> (on-line 2011)
- [2] <http://www.nmea.org> (on-line 2011)
- [3] <http://www.gps.gov> (on-line 2011)
- [4] <http://www.fastraxgps.com/products/gpsantennamodules/300series/uc322/> (on-line 2011)
- [5] <http://www.ftdi-chip.com> (on-line 2011)
- [6] <http://www.eagle.org> (on-line 2011)
- [7] <http://www.ccs-info.com> (on-line 2011)
- [8] <http://www.microchip.com/25LC256> (on-line 2011)
- [9] <http://www.visualGPS.org> (on-line 2011)



Tomàs R. Parets Fiol va realitzar aquest treball com a projecte final de carrera de la titulació d'enginyeria tècnica industrial especialitat electrònica industrial. Té el títol de postgrau d'especialista universitari en domòtica i gestió energètica. Ha rebut el certificat de KNK partner en instal·lacions domòtiques i actualment ocupa un lloc tècnic a I2M en el departament tècnic.

Bartomeu Alorda. Enginyer de Telecomunicacions (UPC, 2000) i Doctor en Física (UIB, 2005). És professor del Departament de Física a la Universitat de les Illes Balears en el grup de recerca de Sistemes Electrònics.

# RCG: Creació d'un Repositori per Impartir Competències Genèriques

José Calvo Fullana, Joe Miró, Antoni Jaume-i-Capó

*PFC d'Enginyeria en Informàtica*

jcfjose@gmail.com, joe.miro@uib.es, antoni.jaume@uib.es

**Resum**— Amb l'entrada dels nous plans d'estudis les competències genèriques han adquirit una importància que enfronta als professors a la necessitat de cercar activitats que ajudin al seu ensenyament. Per aquest motiu s'ha proposat crear, emprant l'esforç col·laboratiu, un repositori que reculli totes aquestes activitats i les posi a disposició del professorat. D'aquesta manera ha sorgit el Repositori de Competències Genèriques, un espai col·laboratiu entre professors a on aquests poden crear activitats, cercar-les, classificar-les, comentar-les i votar-les, facilitant així la tasca de recollir i organitzar aquestes competències. La direcció del portal és <http://rcg.uib.es>.

través d'Internet que faciliti l'accés a les activitats existents a la resta de professorat. Aquests processos inclouen l'estudi de viabilitat del nou sistema, l'anàlisi i definició dels requeriments, el disseny de l'arquitectura, la seva implementació i el posterior manteniment necessari per a que la aplicació segueixi en actiu. Aquest repositori de material permet al professorat publicar activitats, cercar les que hagin publicat altres professors, comentar i valorar les ja existents. Poden cercar una activitat, descarregar-la, adaptar-la a la seva metodologia a les classes i utilitzar-la lliurement en la seva docència. Poden crear noves activitats, tant amb material nou com amb noves versions de les activitats emprades anteriorment, i afegir comentaris de com les fan servir, tot creant un sistema d'ensenyament col·laboratiu.

D'aquesta manera s'ajudarà al professorat en l'ensenyament de les competències genèriques, posant a la seva disposició un material que d'altra manera consumiria molt de temps per a trobar, valorar, recollir i organitzar de manera adequada.

68

## I. INTRODUCCIÓ

Una de les novetats que apareixen als plans d'estudis de l'Espai Europeu d'Educació Superior és la importància explícita que es dona a les competències genèriques, aquelles que són necessàries en un titulat universitari però que no estan relacionades amb els seus coneixements tècnics. Degut a aquest motiu un dels problemes al que s'enfronten els professors dintre del marc de l'EEES és que es desconeix com ensenyar aquestes competències i com integrar-les en la docència.

Actualment ja existeixen moltes activitats dissenyades i llestes per fer-ne ús en l'ensenyança. El que és difícil és trobar-les, valorar-les, determinar si són adequades al nivell de l'assignatura, trobar la documentació associada, etc. Recollir i organitzar aquesta informació facilita que tots els professors, sense necessitat de tenir grans coneixements de la competència en sí, puguin integrar en les seves assignatures les activitats que faran que els seus alumnes obtinguin les competències transversals.

Al 2008 s'inicia un projecte d'innovació i millora de la qualitat docent per donar una solució a l'ensenyament d'aquestes competències, a on es decidí resoldre aquesta dificultat mitjançant l'esforç col·laboratiu de tots els professors, ja que quasi tots tenen alguna idea o han provat alguna activitat. Aquest fet fa que ja hi hagi tot una base de documents i activitats de gran interès que facilitaria la tasca a tots els professors interessats si tinguessin un fàcil accés a ells. És per aquest motiu que es proposa la creació d'un repositori per a gestionar d'una manera més senzilla aquestes activitats.

## II. OBJECTIUS

La finalitat del projecte que aquí s'exposa ha estat realitzar tots els passos del procés del cicle de vida de software necessaris per aconseguir implantar una eina col·laborativa a

## III. ANÀLISI

### A. Requeriments

Durant la primera fase del projecte s'ha analitzat quins són els requeriments necessaris per a la creació de l'aplicació que dona aquest suport. Per a obtenir-los s'ha emprat la tècnica de recopilació de dades basada en entrevistes, ja que aquesta és la més utilitzada degut a la seva productivitat a l'hora de determinar les necessitats del sistema [1]. D'aquest anàlisi han sortit els requeriments d'usuari, que ens han permès saber els diferents tipus d'usuaris que interactuaran amb el sistema. A la Fig. 1 es pot veure el diagrama d'usuaris del repositori, que estableix la jerarquia que aquests tenen dintre del sistema.

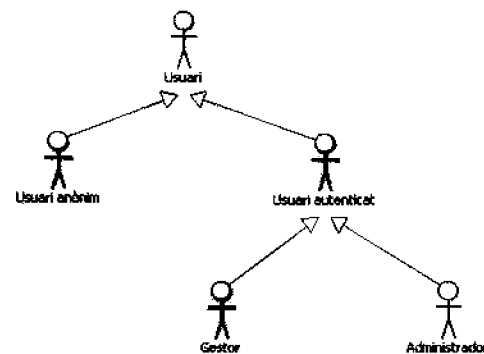


Fig. 1 Diagrama d'usuaris del sistema

Quan ja s'han definit els requeriments d'usuari aquests s'han emprats per treure els requeriments de sistema, necessaris per a la definició de les característiques que ha de tenir el sistema i les funcions que aquest ha d'oferir.

### B. Funcionalitats del Repositori

La unitat principal del repositori és l'activitat. Una activitat és una tasca que es duu a terme en una assignatura per l'obtenció dels objectius específics d'aquesta, i a més, els objectius de la competència transversal. Els usuaris poden crear activitats al repositori, editar-les i adjuntar-hi arxius. Aquestes activitats consten del nom de l'activitat, les assignatures a les que va destinada i una descripció. Se li poden afegir etiquetes per a realitzar una classificació, especificant quines competències treballa l'activitat, a quin curs es pot compartir i a quins estudis va destinada, així com també comentaris per part d'altres usuaris.

Una altra possibilitat és la de crear *enquestes*, les quals es caracteritzen per una pregunta que formula l'usuari i un seguit de respostes que els altres integrants del repositori poden contestar. A més, de la mateixa manera que a les activitats, els usuaris també poden fer-li comentaris.

La funcionalitat més important al repositori són les *cerques*, les quals es realitzen a partir de la classificació per categories que ha fet l'autor de l'activitat. A l'usuari se li presenten diferents opcions per trobar el material, per a què pugui triar la que millor escaigui a les seves necessitats. També disposen d'una opció per realitzar cerques a altres repositoris i de la possibilitat de fer cerques predefinides per etiquetes. Aquesta és la cerca més precisa, a on a l'usuari se li presenten les diferents etiquetes existents per a cada categoria. Aquest selecciona les que vol que estiguin en els seus criteris de cerca i llavors se li mostra un llistat amb tot el material disponible per a les etiquetes elegides.

Finalment, el repositori permet l'ús tant del català com del castellà, i els usuaris tenen en tot moment la possibilitat de canviar d'idioma entre un i l'altre. A més, quan un usuari crea una activitat, aquest pot afegir una categoria que indica en quin idioma estan els arxius que hi adjunta.

### C. Estudi de les Eines Existents

Per a realitzar aquest projecte ha estat necessari crear una eina que permeti gestionar el contingut que s'anirà recopilant durant el seu ús. Per aquest motiu s'ha elegit utilitzar com a tecnologia base un sistema gestor de continguts (Content Management System, CMS). Aquests sistemes són programes que permeten crear una estructura de suport per a la creació i administració de continguts, principalment a pàgines web, per part dels participants [2]. Els CMS donen la possibilitat de compartir qualsevol tipus d'arxiu, ja sigui text, vídeo, àudio, imatges... com a contingut web. A més, alguns poden crear fluxos de treball per a la creació de contingut i la seva aprovació.

Per a decidir quin CMS emprar s'ha fet un estudi que determina quins cobreixen les necessitats del sistema, seguint el camí de la Universitat d'apostar per l'ús de programari lliure. Els dos sistemes analitzats han sigut Drupal i Joomla,

dos dels CMS més destacats dels darrers anys [3]. Aquests són paquets de programari lliure amb llicència GNU/GPL [4], escrits en PHP i emprant el sistema de base de dades MySQL per a emmagatzemar la informació. A la Fig. 2 es pot veure a mode il·lustratiu un exemple de les capes en l'arquitectura tecnològica de Drupal. Aquest manté les mateixes que Joomla, però a més implementa una capa d'abstracció que transforma les consultes SQL en consultes genèriques, permetent emprar diferents tipus de bases de dades sense haver de canviar el codi.

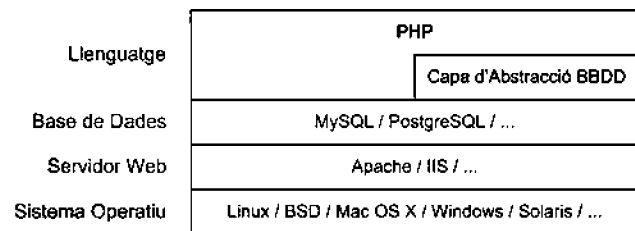


Fig. 2 Capes en l'arquitectura tecnològica de Drupal

A l'hora de realitzar la comparació, els aspectes que s'han tingut en compte s'han seleccionat per poder avaluar les capacitats dels dos sistemes en diferents àmbits necessaris a l'hora de crear el repositori, els quals es poden veure a la següent llista:

- Facilitat d'instal·lació
- Facilitat de creació d'una web
- Facilitat d'administració de contingut
- Flexibilitat gràfica i estructural
- Rols d'usuaris i flux de treball
- Suport multi idioma
- Extensibilitat i integració
- Manteniment del repositori i suport.

Els resultats obtinguts han determinat que Joomla és útil si es vol tenir un lloc senzill de manera ràpida i sempre que es pugui afrontar una categorització de contingut rígida i unes opcions de configuració i de disseny limitades. Per altra banda es pot usar Drupal si es vol alt rendiment, escalabilitat, un bon gestor de continguts i una flexibilitat de disseny significativa. Però això sí, s'ha d'estar preparat per a invertir molt de temps en aconseguir un lloc web professional.

D'aquesta manera s'ha elegit Drupal com a sistema gestor de continguts per al repositori, ja que compleix la major part dels requeriments obtinguts al principi de la fase d'anàlisi.

## IV. DISSENY

La següent fase en la creació d'un software és la de disseny, a on es realitza el modelat del sistema en base als requeriments de sistema obtinguts, i a on s'extreu posteriorment el document de casos d'ús. Aquests serveixen per indicar com ha d'actuar el sistema amb l'usuari per aconseguir un objectiu específic, i és la tècnica més habitual per al modelat del comportament d'un sistema [5].

### A. Descomposició del sistema

Per a realitzar un bon disseny és necessària una bona descomposició del sistema. Per aquest motiu la descomposició dels casos d'ús s'ha fet tenint en compte la *cohesió*, una mesura de la relació funcional entre els elements d'un mòdul que s'empra a la fase de disseny del cicle de vida d'un projecte de software [6]. Les funcionalitats dels mòduls amb una alta cohesió han d'executar entre ells una tasca ben definida en un programa. És a dir, les unitats de software que s'agrupen en un conjunt és degut a què estan relacionades en el desenvolupament d'una única funció específica.

Amb aquesta idea en ment s'han agrupat els diferents casos d'ús segons la funció bàsica que realitzen: l'autenticació, gestió d'usuaris, gestió de contingut i consultes. Aquests casos d'ús s'han dividit a la seva vegada en altres grups de subcasos d'ús, tal com es mostra a la Fig. 3. Aquí cada grup final conté els casos d'ús associats a aquesta funcionalitat. Per exemple, el CU2: *Gestió d'usuaris* és un grup final que conté els subcasos d'ús corresponents a les funcions relacionades amb els usuaris que interaccionen amb el sistema i que apareixen a la Fig. 1: crear un compte, validar-lo, denegar-lo, assignar un rol i modificar les dades personals.

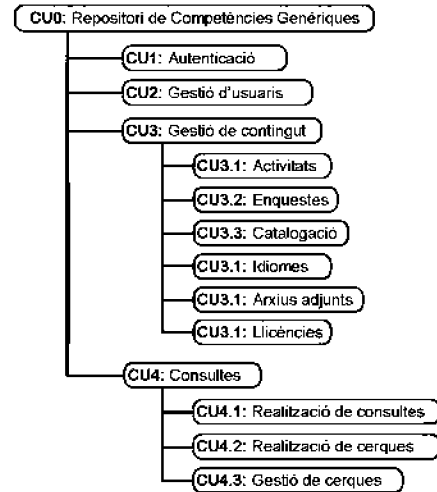


Fig. 3 Organització jeràrquica dels grups de casos d'ús.

concretament el que defineix el cas d'ús 0, i que apareix com a primer nivell a la Fig. 3.

### B. Definició dels casos d'ús

Els casos d'ús s'han realitzat mitjançant una sèrie d'apartats que els defineixen, creant un document per a cada un d'ells a on es detallen les seves característiques. Primer apareix una *descripció* del cas d'ús tractat, especificant el que el sistema ha de permetre realitzar als usuaris que es defineixen. Després apareixen les *precondicions*, que descriuen l'estat del sistema abans d'executar-se el cas d'ús. Tot seguit es contemplen les *postcondicions* en cas d'èxit i en cas de fracàs, que descriuen respectivament l'estat del sistema després d'executar-se el cas d'ús en cas de finalitzar amb el resultat esperat per part dels usuaris principals i en cas de finalitzar sense aconseguir el resultat esperat. Després apareix la llista d'*usuaris* que empraran la funcionalitat, seguits per el *trigger* o acció que inicia la seva execució.

Al segon bloc es descriu la *seqüència normal* que segueix un cas d'ús, detallant pas a pas les accions que s'han de realitzar, per obtenir el resultat desitjat. De la mateixa manera, també es detallen les *excepcions*, mostrant una llista amb els passos i les accions que el sistema ha de realitzar en el cas que aparegui una situació que provoca una excepció.

Finalment, al darrer bloc apareixen el *súper cas d'ús*, que correspon al cas d'ús de nivell immediatament superior, i els *subcasos d'ús*, mitjançant una llista amb els de nivell immediatament inferior.

### C. Diagrames dels casos d'ús

Una vegada que s'ha definit l'estructura que han de seguir els casos d'ús s'han creat cada un d'ells per a cada requeriment de sistema, fent servir UML per al disseny dels diagrames.

Aquest és un llenguatge gràfic de modelat de software emprat per especificar, dissenyar, construir i documentar sistemes, essent actualment el més conegut i utilitzat [7]. A la Fig. 4, es pot veure un exemple d'un diagrama de cas d'ús,

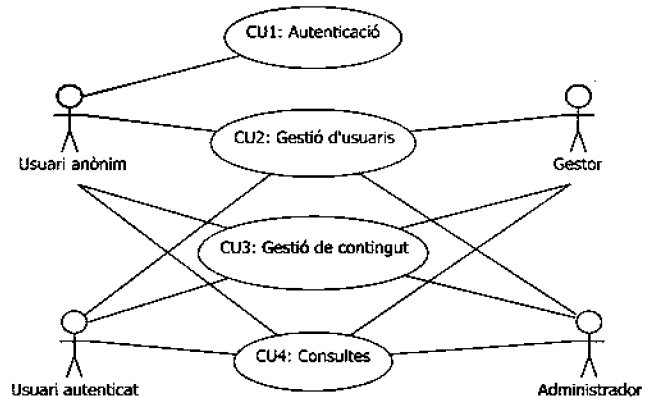


Fig. 4 Exemple per al diagrama del cas d'ús 0

## V. IMPLEMENTACIÓ

La següent fase en el cicle de vida de creació del software és la implementació del nou sistema. Una vegada que ja s'ha fet l'estudi durant la fase d'anàlisi de quina és la millor eina per a la creació del repositori i s'han definit les seves funcions en la fase de disseny és necessari començar la seva implementació. Primer de tot s'ha realitzat l'instal·lació del CMS al servidor, per permetre així començar a configurar el gestor de continguts per a què compleixi amb els nostres requeriments.

Drupal ve amb una sèrie de capacitats implementades al seu nucli, fet que ha ajudat a elegir aquest sistema ja que moltes d'elles satisfan gran part dels requeriments establerts. A més, de cara als requeriments que no es satisfan nativament, permet una gran flexibilitat i adaptabilitat gràcies a la possibilitat d'ampliació mitjançant mòduls complementaris. A continuació es detallen les funcionalitats que s'hi poden trobar, juntament amb el procés que s'ha seguit per crear-les.

### A. Gestió d'usuaris

Primer de tot, els usuaris s'han de poder registrar al repositori. Aquesta funcionalitat s'ha satisfet mitjançant el mòdul de Drupal *User*, que administra el registre d'usuaris i el sistema d'inici de sessió, permetent que així qualsevol usuari pugui crear un compte al repositori. Degut a què és un mòdul de sistema no es pot modificar el codi, i s'han d'utilitzar les opcions de configuració que proporciona Drupal per adaptar-lo a les pròpies necessitats.

En el nostre cas s'ha creat un formulari que els nous usuaris han d'omplir amb les seves dades: nom, llinatges, universitat i estudis. Una vegada omplit, aquest compte queda a l'espera de que un gestor el validi, moment en el qual el nou usuari rebrà una confirmació de que ja pot accedir al repositori.

### B. Rols i permisos

Els rols d'usuari permeten ajustar al detall la seguretat i l'administració del sistema. Al repositori s'han creat quatre tipus diferents de rols, alguns dels quals s'assignen automàticament quan l'usuari fa certes accions, i altres s'han d'assignar manualment. Concretament, els tipus de rol d'usuari que s'han creat són quatre: *usuari anònim*, *usuari autènticat*, *gestor* i *administrador*.

L'usuari anònim s'empra per als usuaris que no tenen compte o que encara no s'han autènticat. Quan un usuari accedeix amb el navegador al repositori automàticament se li assigna a aquella sessió un identificador, juntament amb el tipus de rol. En aquest cas, mentre que l'usuari no s'identifiqui la seva sessió té el rol d'usuari anònim. D'aquesta manera, l'usuari veu les activitats del repositori, però no els seus arxius adjunts.

L'usuari autènticat s'assigna automàticament a tots els usuaris que s'autèntiquen al repositori. Els usuaris autènticats tenen la possibilitat d'accedir al seu compte i canviar les seves dades, crear activitats i editar-les, pujar arxius, veure les activitats dels altres usuaris juntament amb els arxius adjunts i descarregar-los. També poden crear enquestes i votar-hi.

El rol de gestor l'ha d'assignar manualment un usuari administrador, i s'empra per a què els usuaris amb aquest rol puguin acceptar o denegar les peticions de nou compte d'usuari. No es vol que tothom pugui accedir al repositori simplement creant-se un compte, per aquest motiu existeix el rol de gestor: quan un usuari crea un compte aquest queda a l'espera de que un gestor el validi, el qual rep un correu avisant-lo de que hi ha un nou usuari al repositori. Aquesta funcionalitat s'ha aconseguit amb el mòdul *User registration notification*, el qual permet notificar a certs rols quan un nou usuari ha creat un compte.

Finalment, el rol d'administrador és el que permet utilitzar qualsevol tipus d'opció al repositori, i és aquest el que s'empra quan s'han de configurar funcions noves al sistema.

### C. Creació i edició de contingut

Els usuaris registrats han de poder crear contingut al repositori: activitats i enquestes. Per aconseguir-ho s'han configurat dos tipus de contingut nous a Drupal mitjançant el mòdul de sistema Node, el qual permet enviar i mostrar

contingut. En el cas de les enquestes també és necessari un altre mòdul de sistema, *Poll*, que permet capturar vots sobre diferents temes en forma de preguntes d'opció múltiple. Aquests continguts es creen adherits a una de les sis llicències *Creative Commons*, gràcies al mòdul *Creative Commons Lite*.

Drupal per defecte mostra una llista d'arxius adjunts a cada node creat, però l'estil que els hi aplica no especifica visualment quin tipus d'arxiu és. El que s'ha fet és, mitjançant el mòdul *shiny upload*, afegir una icona a cada arxiu segons el seu tipus MIME. A la Fig. 5. es veu un exemple de com apareixien els arxius adjunts a l'inici i com apareixen emprant aquest mòdul:

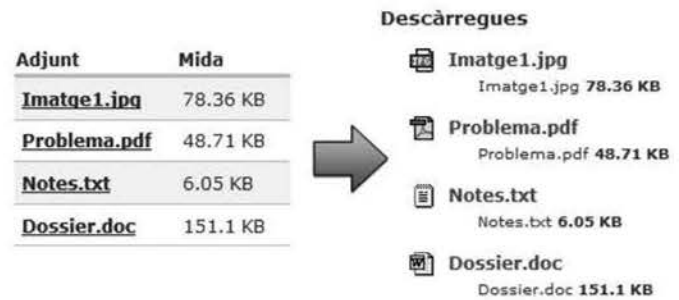


Fig. 5 Arxius adjunts emprant icones segons el tipus MIME.

Finalment, de cara a l'edició d'aquest contingut, s'ha optat per configurar el mòdul *Wysiwyg*, que permet que els usuaris puguin editar contingut amb un editor visual.

### D. Consultes i cerques

És evident que de res serveix anar creant contingut si després no es té cap mètode per a poder visualitzar-ho. Tot el contingut de Drupal una vegada es crea automàticament ja està llest per a ser consultat. El problema ve en que aquest contingut s'ha d'agrupar d'alguna manera per a tenir-ho tot al mateix lloc i fer així les consultes més senzilles i ràpides. Per solucionar-ho s'ha emprat el mòdul *Views*, que permet crear llistes personalitzades i consultes a la base de dades. Amb aquest s'ha creat un llistat amb tot el contingut ordenat per data de creació, i mostrant el títol, el text del contingut, les paraules clau associades, el nom dels arxius adjunts i els comentaris que han escrit altres usuaris.

També és possible emprar el cercador del repositori. El motor de cerca de Drupal manté un índex de les paraules trobades al contingut del lloc, i aquest es va actualitzant automàticament cada vegada que es crea un nou contingut.



Fig. 6 Exemple de núvols d'etiquetes creats al repositori.

A més del motor de cerca, i per a què l'usuari tingui una visió general del tipus de material que pot trobar i la quantitat de material que hi ha a cada categoria, se li proporciona també un núvol d'etiquetes. Aquest consisteix en una representació visual de les etiquetes usades per a catalogar el contingut, ordenades alfabèticament i a on les més utilitzades es representen amb un tamany de lletra més gran que la resta. Aquesta funcionalitat s'aconsegueix mitjançant el mòdul *Tagadelic*, que crea distints núvols d'etiquetes com els que apareixen a la Fig.6.

L'inconvenient que té aquest mòdul és que no permet de forma nativa la traducció del contingut que mostra. Per solucionar-ho s'ha canviat part del codi modificant la funció *theme\_tagadelic\_weighted*, quedant com es mostra a continuació:

```
function theme_tagadelic_weighted($terms) {
  $output = '';
  foreach ($terms as $term) {
    if (module_exists("i18ntaxonomy")) {
      $terms = i18ntaxonomy_localize_terms($terms);
    }
    $output .= l($term->name,
      taxonomy_term_path($term),
      array( 'attributes' =>
        array( 'class' => 'tagadeliclevel'
          . $term->weight,
            'rel' => 'tag' )))
      . "\n";
  }
  return $output;
}
```

Codi 1. Modificació del mòdul Tagadelic per admetre traduir etiquetes.

D'aquesta manera quan el mòdul processa cada terme primer comprova si està activat el mòdul *i18ntaxonomy* (que permet la traducció de vocabulari) i l'empra per traduir cada un dels termes abans de crear la sortida i mostrar-ho per pantalla.

**E. Cerques a altres repositoris**

Per aconseguir aquesta funcionalitat s'ha emprat el mòdul *Services*, una API per crear web services i així poder intercanviar dades entre els distints repositoris. Emprant un web service es pot aconseguir que una aplicació externa tingui accés als serveis que ofereix el repositori, sense haver de intercanviar usuaris ni claus d'accés a la pròpia base de dades.

Per a l'intercanvi de dades s'ha emprat XML-RPC, un protocol de crida a procediments remots que fa servir XML per codificar les crides HTTP com a mecanisme de transport de dades [8]. A la Fig. 7. es pot veure el modelat del comportament que es segueix en aquestes cerques:

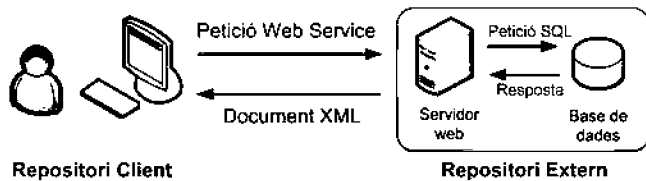


Fig. 7 Flux de dades durant una petició al web service.

El client fa una cerca escrivint les paraules clau a cercar i envia la petició. Aquesta es connecta al web service que ofereix el servidor, rep la petició i fa la cerca a la base de dades, de manera totalment independent de la transacció rebuda. Al obtenir les dades aquest retorna un document XML al repositori client, a on es visualitzen els resultats cercats.

Per a complementar aquesta estructura de petició-resposta, i ja que no s'ha trobat cap mòdul que s'ajusti a les nostres necessitats, s'ha creat *RCG Share*. Aquest nou mòdul permet capturar les paraules clau a cercar, crear la petició al web service, rebre el document XML de resposta, processar-lo i visualitzar els resultats. Basant-se en el protocol XML-RPC, permet la connexió a altres repositoris modificant la funció *search* de Drupal. El codi de la funció principal es pot veure a continuació:

```
function rcg_share_search($keys) {
  $web_services = array();
  //Recorrem i cerquem a cada un dels web services.
  $find = array();
  foreach ($web_services as $url)
  {
    $results = xmlrpc($url, 'search.nodes', $keys);
    if (xmlrpc_error()) {
      $error = xmlrpc_error();
    } else {
      $find = array_merge($find, $results);
    }
  }
  return $find;
}
```

Codi 2. Funció principal del mòdul de cerques RCG Share.

La variable *\$web\_services* és un array que emmagatzema les direccions del servidor de cada repositori habilitat per rebre peticions. Així, el mòdul accedeix a la variable, i per cada direcció que hi troba realitza una connexió XML-RPC al web service *search.nodes* amb les paraules clau sol·licitades. Si aquesta petició resulta en error (per exemple, si no ha trobat resultats) es guarda per a què Drupal pugui mostrar un missatge posteriorment de que no hi ha resultats. En cas de que no hi hagi error, es van afegint els resultats a la variable *\$find* fins que no queden més repositoris per consultar. Llavors es retorna aquesta variable creada amb l'estructura necessària per a què Drupal l'emprí per a visualitzar els resultats.

**F. Puntuació de contingut**

Els usuaris registrats també poden votar el contingut creat, gràcies al mòdul *Fivestar*. Aquest ofereix un sistema de vots a cada activitat que es crea al repositori, com es pot veure a la Fig. 8:

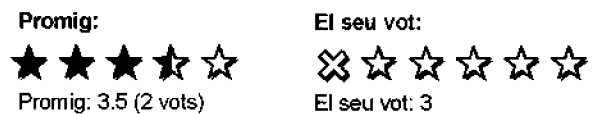


Fig. 8 Exemple de vots per a una activitat.



### G. Vocabulari i sistema de classificació

Per a realitzar la classificació s'ha decidit utilitzar etiquetes, paraules clau associades al contingut que donen una gran flexibilitat a l'hora de fer cerques i catalogacions. El mòdul emprat ha estat *Taxonomy*, configurat per a què quan un usuari crea una activitat li apareixi una pàgina a on pot triar les categories que vol assignar-li, basant-se en les que ja hi ha definides.

Les categories definides són cinc: competència transversal, estudis, assignatura, curs i idioma del contingut adjunt, basant-se en les etiquetes de competències transversals definides en el Llibre Blanc del títol de grau en Enginyeria Informàtica [9]. Les categories tenen un conjunt inicial d'etiquetes, exceptuant la d'assignatura, que és de format lliure. Tal com es veu a la Fig. 9, és el propi usuari el que pot escriure el que vulgui, deixant llibertat en el títol de l'assignatura.

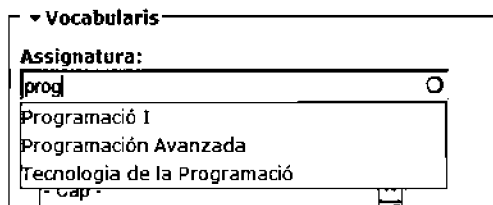


Fig. 9 Mostra de la catalogació segons l'assignatura amb format lliure.

### II. Aspecte gràfic

S'ha optat per una distribució de tres columnes, ja que és un esquema àmpliament utilitzat i no suposa un disseny estrany de cara a l'usuari. A la Fig. 10, es pot veure el disseny del repositori. La columna de l'esquerra conté el menú de navegació, la columna de la dreta mostra varies seccions com el canvi d'idioma, el cercador, etc., i a la columna central és a on apareix tota la informació.

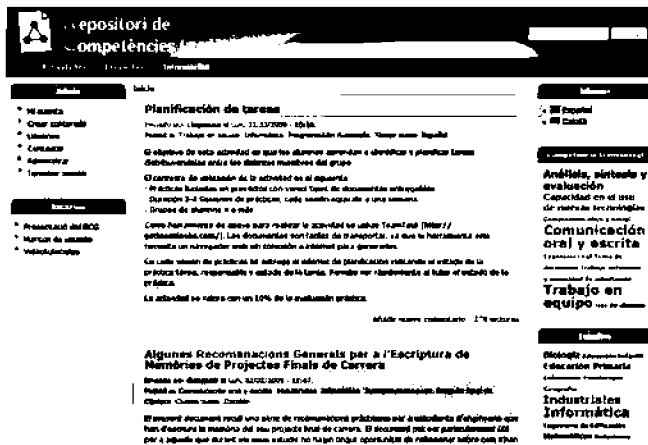


Fig. 10 Mostra del disseny del repositori a on es pot veure la distribució de tres columnes que s'ha emprat.

## VI. CONCLUSIONS

Amb aquest projecte aquí presentat ha sorgit el Repositori de Competències Genèriques, un espai col·laboratiu entre professors a on aquests poden crear activitats, cercar-les,

classificar-les, comentar-les i votar-les. Poden consultar activitats creades per altres professors, descarregar-se el contingut, adaptar-lo a la seva metodologia de treball i utilitzar-lo en la seva docència. El recent inici de l'EEES requereix de contribucions com la que s'ha implementat en aquest projecte, i hem pogut comprovar que aquesta eina era necessària.

Per altra banda, com a tot projecte de software, el seu cicle de vida no acaba després de la implementació i la seva posterior instal·lació. Per a què el projecte pugui mantenir-se és necessari el seu manteniment, de manera que l'eina no quedi desfasada. Aquesta darrera fase contempla les modificacions del producte, tant de codi com de documentació, les possibles migracions a un nou entorn, el suport als usuaris, etc. A més també s'han de tenir en compte les modificacions necessàries en cas de desitjar noves funcionalitats.

Finalment, és necessària l'activitat continuada al repositori per part dels administradors i gestors, ja que són aquests els encarregats d'acceptar o denegar les peticions d'alta de nous usuaris al sistema. D'aquesta manera el repositori podrà seguir en marxa permetent l'accés a nous usuaris amb nou material, facilitant així al professorat la tasca de recollir i organitzar les competències genèriques.

### REFERÈNCIES

- [1] E. Amengual, X. Gilabert, A. Mas, *Tècniques de recopilació de dades*. Apunts d'Enginyeria del Software I. Tema 6, diapositiva 5. Universitat de les Illes Balears.
- [2] Wikipedia, la enciclopèdia lliure (2011) Sistema de Gestión de Contenidos. [Online]. Disponible: [http://es.wikipedia.org/wiki/Sistema\\_de\\_gestion\\_de\\_contenidos](http://es.wikipedia.org/wiki/Sistema_de_gestion_de_contenidos)
- [3] Packt Publishing, Llista de guanyadors i premis otorgats als Annual Open Source CMS Awards. [Online]. Disponible: <http://www.packtpub.com/article/open-source-cms-award-previous-winners>.
- [4] Free Software Foundation, GNU General Public License. Versió 3. [Online]. Disponible: <http://www.gnu.org/copyleft/gpl.html>.
- [5] G. Fontanet, *Requeriments d'usuari i de sistema*. Apunts d'Enginyeria del Software II, pàgina 3. Universitat de les Illes Balears.
- [6] E. Amengual, *El procés de Disseny del Sistema d'Informació II*. Apunts d'Enginyeria del Software I. Tema 10, diapositiva 80. Universitat de les Illes Balears.
- [7] Object Management Group, Getting Started with UML. [Online]. Disponible: <http://www.uml.org/>
- [8] Wikipedia, la enciclopèdia lliure, XML-RPC. [Online]. Disponible: <http://ca.wikipedia.org/wiki/XML-RPC>
- [9] J. Casanovas, *Libro Blanco. Título de grado en Ingeniería Informática*. ANECA. Juny 2005.

# Estudi i disseny de diverses alternatives per a fer més estable una memòria SRAM

Pau Ricra Benito, Bartomeu Alorda Ladaria

*PFC d'Enginyeria Tècnica Industrial, Especialitat en Electrònica Industrial*

paurierabenito@gmail.com

**Resum**— Les memòries SRAM actualment estan en constant creixement tant a nivell d'utilització com d'investigació i es possible trobar memòries SRAM en un gran nombre d'aparells electrònics.

Malauradament, la miniaturització de la tecnologia CMOS presenta greus problemes per a les memòries SRAM, en aquest tipus de memòries el procés d'escalat o miniaturització té un impacte gran sobre l'estabilitat de les dades emmagatzemades a la cel·la SRAM. Per aquesta raó el grup de Sistemes Electrònics de la UIB va proposar estudiar el comportament de tres memòries SRAM amb diferents configuracions de cel·la cada una. En aquest document s'explica el procediments que s'han dut a terme per al disseny de les tres configuracions de memòria SRAM i els resultats obtinguts de la simulació d'aquets dissenys.

## I. INTRODUCCIÓ

A causa del gran desenvolupament dels processadors, quan aquets començaren a tenir velocitats de rellotge cada vegada majors, i funcionaven més i més ràpids, els temps d'accés a la memòria Ram Dinàmica(DRAM) no era suficient per a seguir el ritme al processador i obtenir el màxim rendiment.

Una de les solucions a aquest problema seria la memòria SRAM( Static Random Access Memory), és un tipus de memòria basada en semiconductors que és capaç de mantenir les dades sense necessitat d'un circuit de refresc. De totes maneres, es tracta d'una memòria volàtil, és a dir, perd tota la informació quan s'interromp l'alimentació elèctrica. És una memòria d'accés aleatori, que significa que les posicions a la memòria poden ser escrites o llegides en qualsevol ordre, independentment de quina fos la darrera posició accedida de la memòria.

La memòria SRAM és més cara, però més ràpida i amb un menor consum que la memòria DRAM. Per tant, es utilitzada quan es necessita disposar d'un menor temps d'accés, un consum reduït o una de les dues coses alhora. Les memòries SRAM són molt utilitzades i tenen molt d'usos en l'actualitat com: telèfons mòbils, càmeres fotogràfiques, electrònica de l'automòbil, ordenadors personals, etc...

Una de les problemàtiques que presenten les memòries SRAM és l'impacte que produeix la miniaturització de les memòries sobre l'estabilitat d'aquesta. Els principals problemes es centren en la fluctuació aleatòria del procés de fabricació i la manca de repetibilitat del voltatge llindar. Ambdós problemes es preveu que redueixin l'estabilitat de les cel·les amb un factor 4 entre les tecnologies de 250nm i 50nm. Una de les metodologies tradicionals de millorar l'estabilitat de la cel·la SRAM es basa en la variació de les dimensions dels transistors que formen la cel·la. Avui en dia s'estudien

altres alternatives com la modificació de l'estructura de la cel·la SRAM proposant cel·les de 8 o més transistors.

L'objectiu d'aquest PFC ha estat, dissenyar, estudiar i comparar la velocitat de lectura/escriptura, el consum, l'àrea de la memòria i el paràmetre d'estabilitat (Static Noise Margin, SNM) de tres configuracions de memòries SRAM proposades en el grup de Sistemes Electrònics de la Universitat de les Illes Balears amb el software "Cadence" i usant una tecnologia comercial de 65nm CMOS:

-Memòria SRAM amb cel·les de 8 transistors:

Amb les cel·les de 8 transistors (8T) el que es vol obtenir és una separació de la lectura i l'escriptura mitjançant una nova configuració de la cel·la respecte de la típica 6T, d'aquesta manera s'espera millorar la problemàtica de les cel·les 6T durant les operacions de lectura i per tant millorar l'estabilitat de la memòria.

-Memòria SRAM amb cel·les de 8 transistors i un selector de voltatge.

D'aquesta memòria a l'anterior, tan sols varia la utilització de dos voltatges per la línia de selecció de fila diferents durant les operacions de lectura i d'escriptura. D'aquesta manera aconseguim reforçar el procés de lectura i seguir enfortint la memòria SRAM per tant, aquest tipus de memòria es podria considerar una evolució de la memòria amb cel·les 8T, encara que el selector de voltatge seria aplicable a una memòria SRAM 6T.

-Memòria SRAM amb cel·les de 11 transistors.

La memòria SRAM amb cel·les 11T proposa la modificació de l'estructura de la cel·la 8T de la memòria SRAM, però enlloc de variar un voltatge, es modifica l'arquitectura de la cel·la per a obtenir un consum de la memòria mínim, a més d'impedir que qualsevol cel·la menys la seleccionada operi i per tant pugui donar lloc a errors d'estabilitat.

## II. INTRODUCCIÓ A LES MEMÒRIES SRAM

A mode de resum, les memòries SRAM són memòries basades en materials semiconductors, a més aquest tipus de memòries a diferència de les memòries DRAM no necessiten un circuit de refresc. La SRAM es tracta d'una memòria volàtil, és a dir, perd tota la informació emmagatzemada quan es desconnecta de l'alimentació. De la mateixa manera, les memòries SRAM són memòries d'accés aleatori, es possible accedir a qualsevol posició sense necessitat de seguir un ordre preestablert.

Finalment, cal dir que les memòries SRAM són més ràpides i amb un menor consum que les memòries DRAM, en canvi tenen un major cost en termes de fabricació que les DRAM.

Més concretament, l'arquitectura d'una memòria SRAM és la que es presenta a la figura 1, on es pot observar que la memòria està formada per la matriu de  $n \times m$  cel·les (element principal), per a direccionar aquesta matriu s'utilitzen dos descodificadors, un de files i un de columnes com es pot apreciar. També es pot veure com a la part superior i inferior de la figura hi ha els blocs de precàrrega, aquets blocs s'encarreguen de carregar a '1' les línies per les quals circularà la informació emmagatzemada a la memòria. Es fan necessaris dos blocs de precàrrega ja que les línies inferiors de la memòria estan separades de les línies superiors mitjançant el descodificador de columnes.

Tot seguit trobam el bloc Bit, aquest és l'encarregat d'introduir el valor del bit a escriure a la memòria. El bloc Sense Amplifier(SA) s'encarrega d'amplificar la diferència de tensions per a la posterior lectura del valor dels bits de la memòria a llegit mitjançant el latch D. La unitat de control es l'encarregada de generar les senyals pertinents per al correcte funcionament de la memòria.

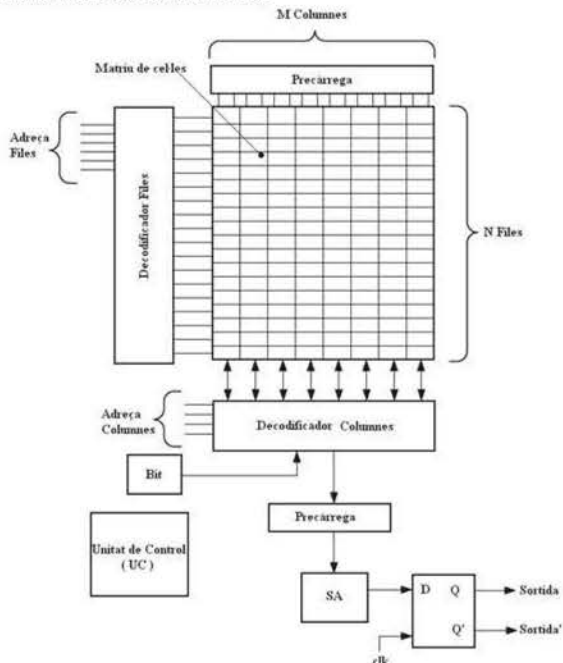


Fig.1 Disseny i arquitectura de la memòria SRAM

Coneixent l'arquitectura de la memòria es procedirà a explicar l'arquitectura de les cel·les que formen la matriu de cel·les de la memòria SRAM. En aquest cas s'explicarà l'arquitectura de les cel·les de 6 transistors(Figura 2).

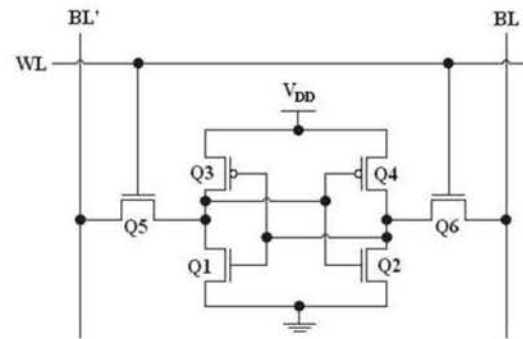


Fig.2 Arquitectura d'una cel·la SRAM 6T.

La cel·la està formada per els transistors Q1-Q2-Q3-Q4, que formen els 2 transistors realimentats que s'encarreguen d'emmagatzemar el valor del bit i dos transistors(Q5 i Q6) activats per la senyal WL(senyal de sortida del descodificador de files) que s'encarreguen de permetre l'accés a la cel·la per a la seva escriptura o lectura. Les línies BL i BL'(Bit lines) s'encarreguen de transportar el valor dels bits a escriure/llegir per a cada columna de la memòria SRAM.

Finalment, el disseny intern d'una columna de la memòria mostrada a la figura 1, es pot observar a la figura 3, on s'observen els blocs de precàrrega, la cel·la, el bloc bit i el sense amplifier.

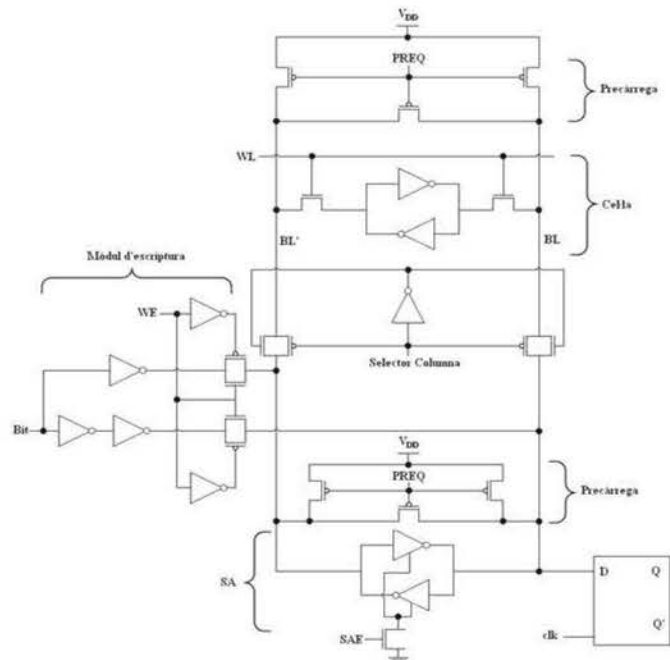


Fig.3 Disseny i arquitectura interna d'una columna de la memòria SRAM.

### III. PROBLEMES D'ESTABILITAT A LES MEMÒRIES SRAM

L'estabilitat durant una operació de lectura de la memòria SRAM es defineix amb el paràmetre SNM.

Aquest paràmetre es mesura com el valor del costat del quadrat que es pot formar a una de les ales de l'anomenada papallona o butterfly que generen els dos inversors realimentats, i es defineix com el mínim voltatge necessari per a que els inversors canviïn d'estat.

A la figura 4 es pot veure com l'SNM de les senyals generades pels inversors realimentats mentrestant que la cel·la es troba aïllada es veu reduït respecte l'SNM durant una operació de lectura. Aquesta reducció de l'SNM provocaria que els inversors canviïn d'estat bruscament a causa del renou o d'una petita variació de tensió.

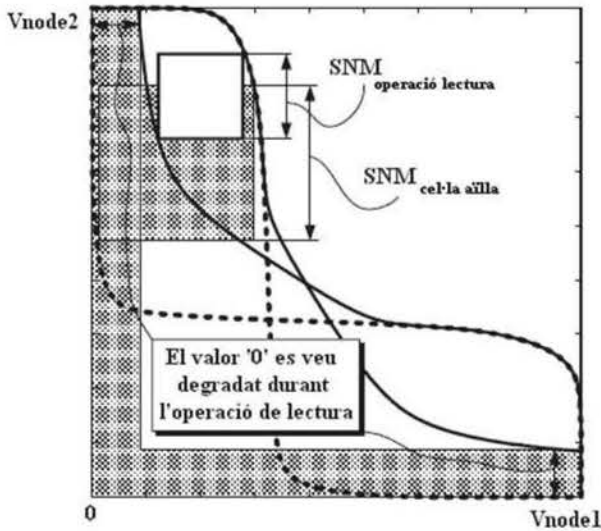


Fig.4 Corbes de tensió dels inversors realimentats

El que succeeix a la cel·la durant una operació lectura és el següent (figura 5), les dues Bit Lines es troben precarregades a '1' quan sobren els transistors d'accés a cel·la. És en aquest moment quan un dels transistors d'accés es talla degut a que el node intern de la cel·la també hi ha un '1', mentre els transistors Q5 i Q1 estan escrivint un '0' a la Bit line negada.

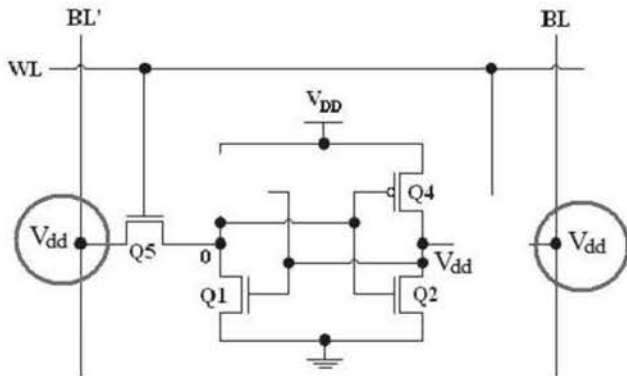


Fig.5 Comportament de la cel·la 6T durant una operació de lectura

Aquesta mateixa situació també es dona lloc durant una operació de lectura a les cel·les on no s'hi està escrivint, ja que com es pot veure a la figura 6 la WL provinent del descodificador de files activa tots els transistors d'accés a la cel·la de tota la fila, en canvi el procés d'escriptura tan sols succeeix en una cel·la. D'aquesta manera a les altres cel·les de la fila s'obren els transistors d'accés havent-hi les dues bit lines precarregades a '1' com es mostra a la figura 5.

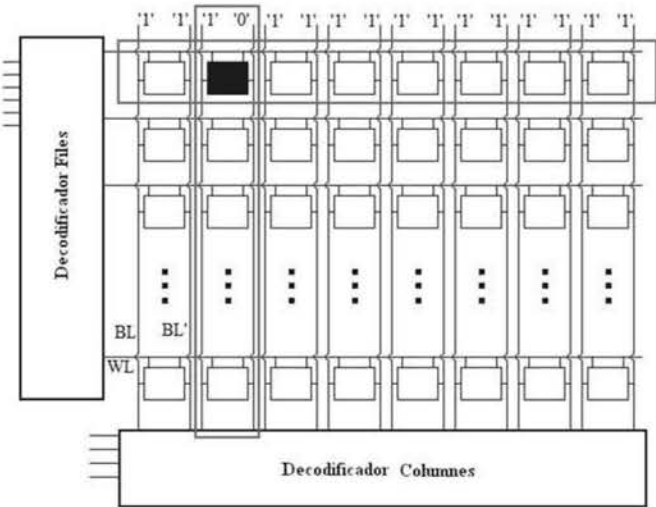


Fig.6 Comportament de la matriu de cel·les durant una operació d'escriptura

### IV. MEMÒRIA SRAM 8T

La memòria SRAM 8T separa el procés de lectura del d'escriptura per tal de reduir el problema d'estabilitat durant aquesta operació (explicat al punt anterior) i per tant fer una cel·la més robusta.

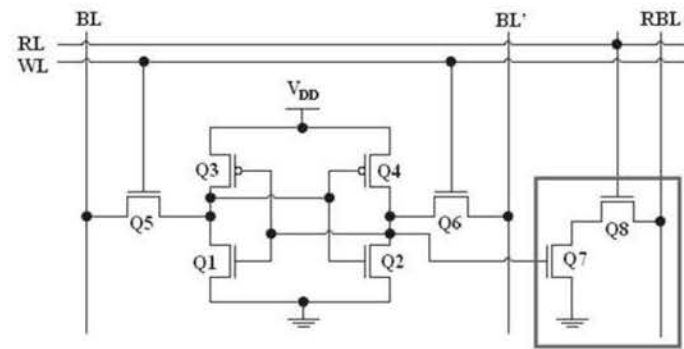


Fig.7 Arquitectura d'una cel·la SRAM 8T

Com es pot apreciar a la figura 7, la configuració de la cel·la per al procés d'escriptura mantén la mateixa configuració que la cel·la 6T en canvi el circuit per a la lectura es compon per els transistors Q7 i Q8. Aquest buffer de lectura està connectat a la bit line negada, per tant alhora actua de negador, és a dir, si el bit a llegir és un 1 i a la bit line

negada hi ha un 0, el transistor Q7 es talla i la RBL es mantén a 1, en el cas contrari en que es vol llegir un 0, com que a la bit line negada hi tenim un 1 s'obre el transistor Q7 i es carrega un 0 a la RBL. A la nova cel·la 8T es pot apreciar una separació a l'hora d'activar els transistors per a una lectura i per a una escriptura, els transistors Q5 i Q6 s'activen durant una lectura mitjançant la senyal WL, en canvi el transistor Q8 s'activa durant una lectura mitjançant la senyal RL. Aquestes dues senyals provenen de la sortida del descodificador de files separades tant per a l'escriptura com per a la lectura.

La configuració de la memòria SRAM amb les cel·les 8T es pot veure a la figura 8, on es pot apreciar com tan sols hi ha dos canvis rellevants respecte la configuració amb cel·les 6T. Un dels canvis és la introducció dels blocs de selecció d'operació entre els descodificadors i la matriu de cel·les, per tal de separar les operacions de lectura i escriptura. En segon lloc s'ha pogut eliminar el bloc sense amplificador(S.A) ja que ara tan sols el procés de lectura es realitza per una sola línia(RBL).

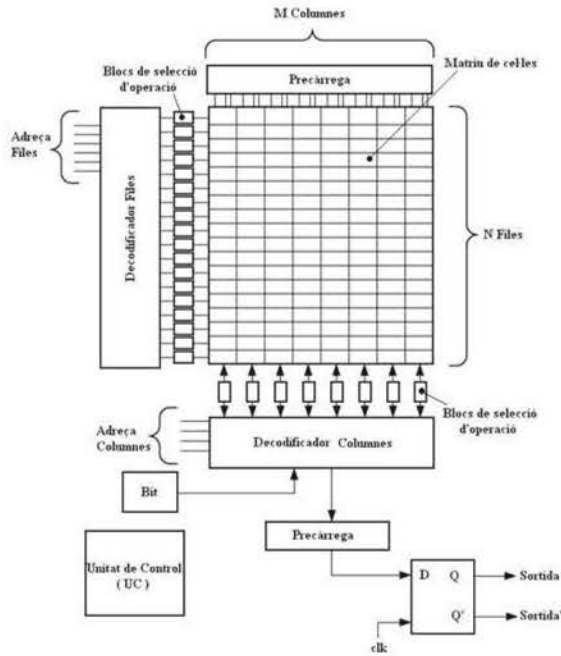


Fig.8 Disseny i arquitectura de la memòria SRAM 8T.

L'arquitectura interna d'una columna de la memòria SRAM 8T(figura 9) també conserva l'estructura de la SRAM 6T introduint-li els pertinents canvis que implica la nova estructura de la cel·la, com és el cas de les diferents senyals per a separar les operacions de lectura i escriptura(WL, RL i Selector Columna Escriptura, Selector Columna Lectura).

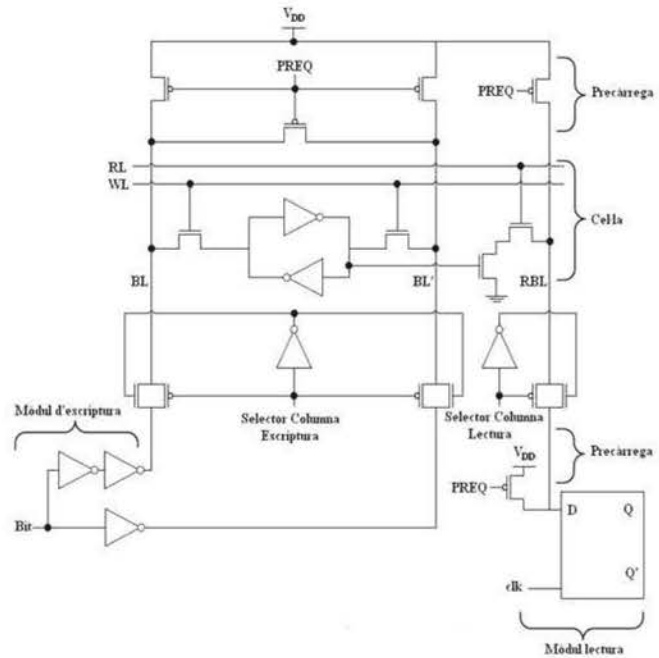


Fig.9 Disseny i arquitectura interna d'una columna de la memòria SRAM 8T.

### V. MEMÒRIA SRAM 8T AMB SELECTOR DE VOLTATGE

La gràfica de la figura 10 forma part d'un estudi realitzat per el Grup de Sistemes Electrònics de la Universitat de les Illes Balears, en el qual es comprova com reduint el valor del voltatge de la word-line s'aconsegueix augmentar el valor del SNM, com es pot veure a la gràfica. On els valors de SNM màxim i mínim són els valors mentres que la cel·la es troba aïlla i durant una operació de lectura, respectivament.

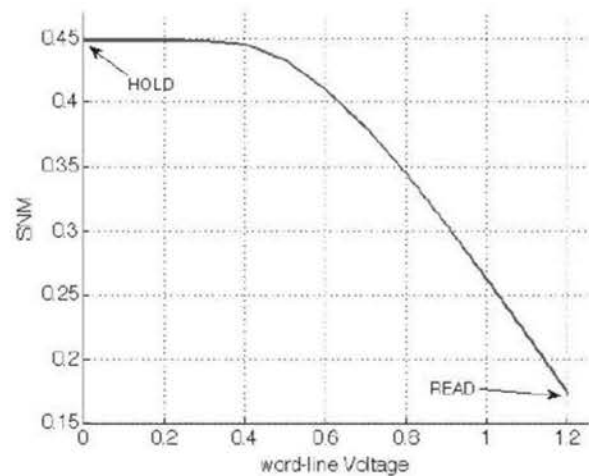


Fig.10 Disseny i arquitectura de la memòria SRAM 8T.

En aquest cas el que s'estudiarà és el comportament de la memòria i el valor del SNM introduint a la configuració de cel·la 8T un selector de voltatge de la word-line de tal manera que aquesta línia, durant les operacions de lectura tingui un voltatge de 1V i durant la resta d'operacions tingui un voltatge 1.2V.

L'estructura del mòdul encarregat de la selecció del voltatge (figura 11) segons el tipus d'operació a realitzar per la memòria es compon per dos transistors PMOS (ja que aquest tipus de transistors passen millor els valors de tensió alts) que s'activen mitjançant la senyal RW, aquesta senyal està a 0 quan s'està executant una operació de lectura i a 1 durant la resta d'operacions, per aquesta raó s'ha introduït un inversor entre la senyal i el transistor encarregat de la selecció d'1V.

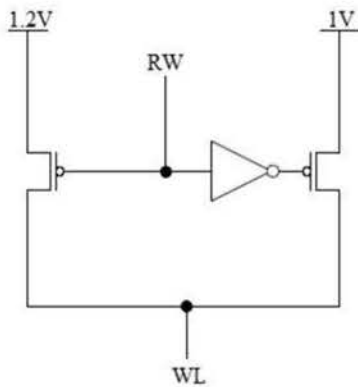


Fig.11 Disseny i arquitectura de la memòria SRAM 8T.

## VI. MEMÒRIA SRAM 11T

La memòria SRAM amb cel·les 11T (Figura 12) proposa la modificació de l'estructura de la cel·la 8T de la memòria SRAM, però enlloc de variar un voltatge, es modifica l'arquitectura de la cel·la per a obtenir un consum de la memòria mínim, a més d'impedir que qualsevol cel·la menys la seleccionada operi i per tant pugui donar lloc a errors d'estabilitat.

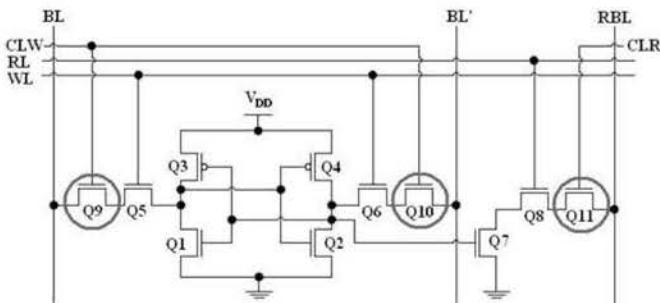


Fig.12 Arquitectura d'una cel·la SRAM 11T.

Amb la senyal CL podem escollir la cel·la exacta a la que volem accedir sense necessitat d'obrir l'accés a totes les

cel·les d'una mateixa fila com passa en els casos de les cel·les 6T i 8T. Com es pot apreciar a l'arquitectura de la cel·la (Figura 12) aquesta senyal CL també es separa en senyal de lectura (CLR) i senyal d'escriptura (CLW)

Com es pot apreciar a la figura 13, l'arquitectura d'una columna de la memòria no es gaire modificada amb la nova arquitectura de la cel·la, l'únic canvi són les senyals CLW i CLR encarregades de seleccionar la cel·la concreta per a escriptura o lectura mitjançant les senyals Selector Columna Escripció i Lectura. També es pot apreciar com ha estat necessari incloure una etapa d'inversors a les dues senyals CL per tal d'obtenir un bon funcionament de la cel·la.

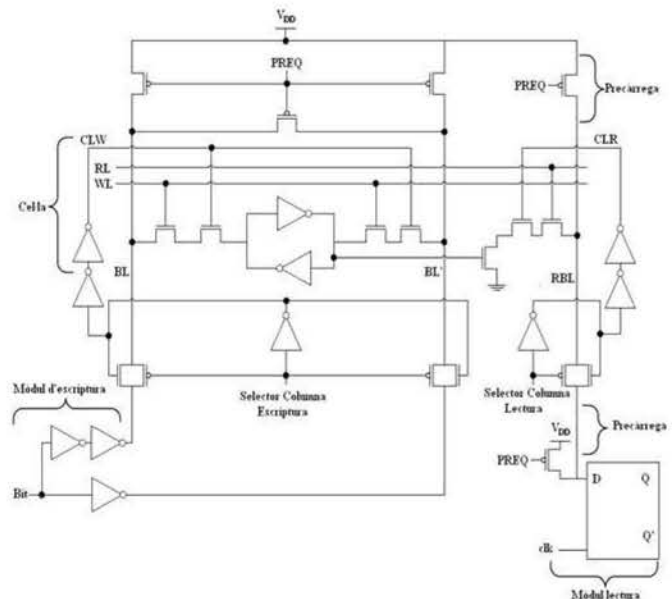


Fig.13 Disseny i arquitectura interna d'una columna de la memòria SRAM 11T.

## VII. SIMULACIONS DE FUNCIONAMENT

Les següents simulacions s'han realitzat amb la memòria SRAM 8T, es tracta de l'escriptura (figura 14) i lectura (figura 15) d'un '1'.

A la figura 14, es poden apreciar (de dalt a baix) les senyals: En/EnFil/PreQ corresponents a l'eneable general de memòria, l'eneable de la fila seleccionada i la senyal de precàrrega. RW es l'encarregada de seleccionar si es tracta d'una operació de lectura o escriptura, en aquest cas, com que la senyal està a '1' sabem que es tracta d'una operació d'escriptura. OutDesccol/Outdecfil/EnWrite, les dues primeres són les senyals de sortida dels descodificadors per a seleccionar la cel·la indicada, i EnWrite és la senyal (WL anomenada així a les figures d'arquitectura de les cel·les) es la senyal la qual la seva activació provoca l'obertura dels transistors Q5 i Q6 d'accés a la cel·la.

La senyal BL és el valor que s'escriurà a la cel·la, i BL' aquest valor negat.  
 El senyal MemBL es el valor que contindrà l'interior de la cel·la SRAM, en aquest cas, s'aprecia com MemBL augmenta a '1' i el seu valor negat (MemBL') baixa a '0'.

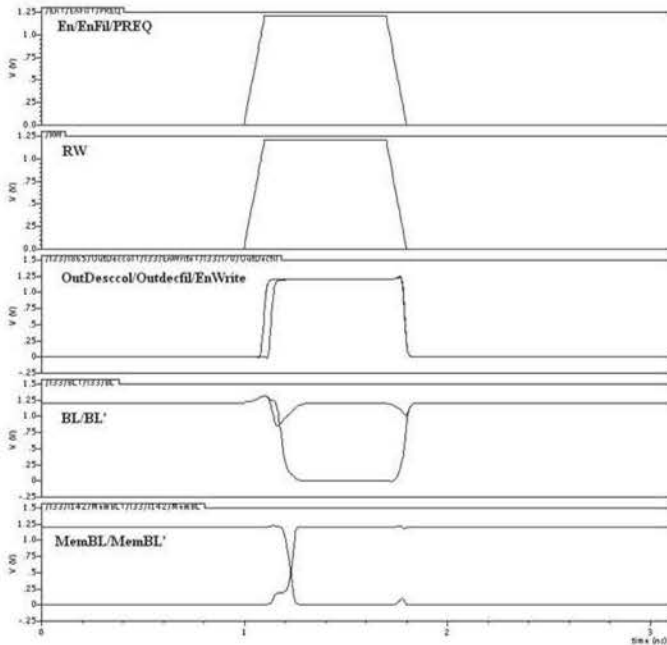


Fig.14 Simulació d'una operació d'escriptura a una cel·la SRAM 8T.

Per a la simulació de lectura (figura 15) observem les noves senyals que intervenen en aquesta operació: EnRead, s'encarrega d'obrir el transistor Q8 encarregat de l'accés al valor de la cel·la. RBL, es el valor emmagatzemat a l'interior de la cel·la (en aquest cas un '1'). Finalment la senyal OUT, és la sortida de la memòria on es pot apreciar el valor llegit ('1') i aquest valor negat (OUT')

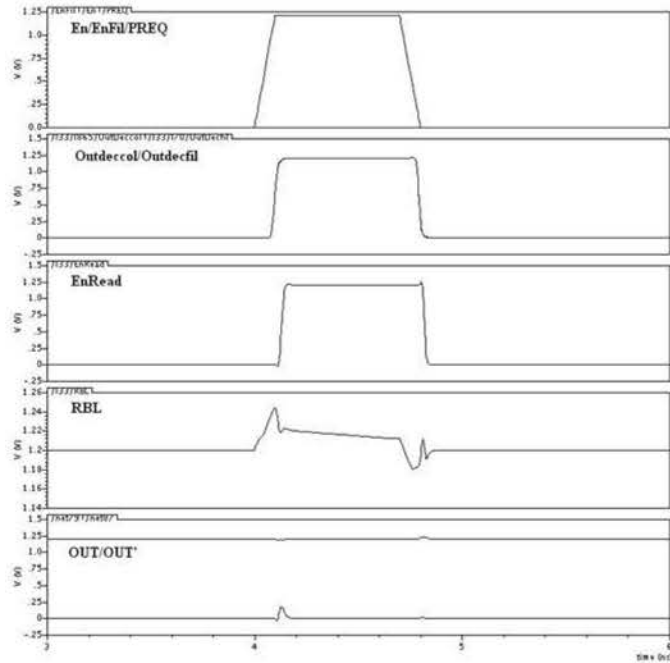


Fig.15 Simulació d'una operació de lectura a una cel·la SRAM 8T.

VIII. RESULTATS OBTINGUTS I CONCLUSIONS

- Àrea:

8T	8TSV	11T
57.1392(um) <sup>2</sup>	57.1392(um) <sup>2</sup>	140.0832(um) <sup>2</sup>

- Velocitat d'escriptura:

OP	8T(ps)		8TSV(ps)		11T(ps)	
	Esc'1'	Esc'0'	Esc'1'	Esc'0'	Esc'1'	Esc'0'
1 <sup>a</sup> F-8 <sup>a</sup> C	186	163	220	194	387	383
32 <sup>a</sup> F-4 <sup>a</sup> C	186	163	219	192	387	383
64 <sup>a</sup> F-2 <sup>a</sup> C	185	163	218	192	387	384

- Velocitat de lectura:

OP	8T(ps)	8TSV(ps)	11T(ps)
	Lec'0'	Lec'0'	Lec'0'
1 <sup>a</sup> F-8 <sup>a</sup> C	407	424	651
32 <sup>a</sup> F-4 <sup>a</sup> C	393	422	653
64 <sup>a</sup> F-2 <sup>a</sup> C	408	423	653



- Consum escriptura:

OP	8T(mW)		8TSV(mW)		11T(mW)	
	Esc'1'	Esc'0'	Esc'1'	Esc'0'	Esc'1'	Esc'0'
1 <sup>a</sup> F-8 <sup>a</sup> C	0.89	0.82	0.86	0.81	0.5	0.6
32 <sup>a</sup> F-4 <sup>a</sup> C	0.77	0.7	0.77	0.79	0.55	0.5
64 <sup>a</sup> F-2 <sup>a</sup> C	0.77	0.8	0.78	0.81	0.6	0.55

- Consum lectura:

OP	8T(mW)	8TSV(mW)	11T(mW)
	Lec'0'	Lec'0'	Lec'0'
1 <sup>a</sup> F-8 <sup>a</sup> C	0.23	0.23	0.3
32 <sup>a</sup> F-4 <sup>a</sup> C	0.23	0.24	0.3
64 <sup>a</sup> F-2 <sup>a</sup> C	0.23	0.23	0.3

- SNM:

SNM (cel·la atllada) = 398mV

SNM (Escriptura incompleta)		
8T	8TSV	11T
175mV	249mV	398mV

Amb els resultats obtinguts es pot observar com la memòria SRAM 8T es la més ràpida a les operacions de lectura i escriptura de la cel·la, on l'arquitectura 8TSV obté uns resultats de velocitats molt similars i la 11T es la més lenta en aquest apartat.

A nivell de consum, s'observa com la memòria 11T és la que té un menor consum Durant l'escriptura però en canvi obté el major consum Durant la lectura.

El valor de l'SNM obté el seu màxim valor durant les operacions realitzades amb la cel·la 11T, i obté el seu valor mínim amb les operacions realitzades amb la 8T, es pot apreciar com el selector de voltatge de la 8T millora aquest valor fins als 249mV.

Finalment cal observar com l'àrea de la cel·la 11T és un poc més del doble de gran que l'àrea de les cel·les 8T i 8TSV que tenen la mateixa àrea.

Per tant, amb aquests resultats, es podria dir que la millor arquitectura és la 8TSV ja que millora el valor del SNM mantenint la velocitat de lectura i escriptura i l'àrea de la cel·la 8T original.

## AGRAÏMENTS

Al tutor del meu projecte per haver-me ajudat en tots els dubtes i problemes que me anat trobant durant la realització d'aquest projecte, i als meus pares, amics i família, per tot el suport que m'han sabut donar.

## REFERÈNCIES

[1] ITRS 2007 (International Technology Roadmap for Semiconductors).

[2] Andrei Pavlov and Manoj Sachdev. "CMOS SRAM Circuit Design and Parametric Test in Nano-Scaled Technologies". 2008 Springer Science + Business Media B.V.

[3] Andrei Pavlov and Manoj Sachdev. "CMOS SRAM Circuit Design and Parametric Test in Nano-Scaled Technologies". 2008 Springer Science Business Media B.V.

[4] Andrei Pavlov and Manoj Sachdev. "CMOS SRAM Circuit Design and Parametric Test in Nano-Scaled Technologies". 2008 Springer Science Business Media B.V.

[5] B. Alorda, G. Torrens, S. Bota and J. Segura. "Static-Noise Margin Analysis during Read Operation of 6T SRAM Cells". Univ. de les Illes Balears, Dept. Física, Cra. Valldemossa, km. 7.5, 07071 Palma de Mallorca, Spain. 2009

[6] Andrei Pavlov and Manoj Sachdev. "CMOS SRAM Circuit Design and Parametric Test in Nano-Scaled Technologies". 2008 Springer Science Business Media B.V.

[7] Evert Seevinck, Frans J.List and Jan Lohstroh. "Static-Noise Margin Analysis of MOS SRAM Cells". IEEE Journal of solid-state cricuits, Vol. SC-22, NO. 5, October 1987.

[8] B. Alorda, G. Torrens, S. Bota and J. Segura. "Static-Noise Margin Analysis during Read Operation of 6T SRAM Cells". Univ. de les Illes Balears, Dept. Física, Cra. Valldemossa, km. 7.5, 07071 Palma de Mallorca, Spain. 2009