

## Matemàtiques que milloren la comunicació

03/2007 - **Telecomunicacions, Electrònica i Informàtica.** El soroll indesitjat en la comunicació digital distorsiona el missatge a transmetre, per la qual cosa els investigadors estudien com dissenyar bons codis de canal, una eina matemàtica que permet detectar i corregir els errors que es produeixen en la transmissió d'informació. Investigadors de la UAB han aconseguit definir nous codis de canal que permeten d'obtenir millors paràmetres de qualitat.



Il·lustració: Agnès Capella Sala

Els canals de comunicació digital permeten transmetre informació entre punts diferents i s'espera d'ells que la informació que arriba al receptor coincideixi amb l'enviada per l'emissor. Molt sovint però, aquests mitjans no poden garantir que la informació arribi intacta al receptor degut a sorolls de diversa naturalesa. És el cas, per exemple, de les trucades amb pèrdua de senyal. Els codis de canal són una eina matemàtica emprada per a la transmissió d'informació que permet detectar i corregir un determinat nombre de possibles errors produïts en la transmissió d'informació a través dels canals digitals.

Des dels primers treballs sobre teoria de la informació de Claude Shannon [10] han estat molts els esforços per donar codis amb bons paràmetres. La recerca de codis que fossin òptims asimptòticament va posar molt d'interès en els anomenats codis algebraico-geomètrics, definits per mitjà de corbes algebraiques i funcions sobre aquestes. Resultats de gran importància dins la geometria algebraica, com el teorema de Riemann-Roch, donarien fites pels paràmetres d'aquests codis. Un bon resum dels codis algebraico-geomètrics i de les seves propietats asimptòtiques es pot trobar a [4].

Si la geometria algebraica va fer-se un lloc en la teoria de codis, veurem com la democràcia també va fer-hi la seva aportació. Un dels algorismes existents per a la detecció i correcció d'errors en codis algebraico-geomètrics, l'algoritme de Berlekamp-Massey-Sakata [9], es pot millorar a partir d'un procés democràtic de votacions [2,3]. Per determinar uns valors necessaris per a la descodificació es defineix un conjunt de votants i cadascun d'ells aposta per un valor. D'entre tots els valors, es pot demostrar que el que realment és vàlid és el més votat.

No s'ha d'obviar però, que la democràcia, sense voler-ne desmerèixer les virtuts, és injusta amb les minories. I més amb aquelles que suposen més costos. En aquesta línia trobem un conjunt molt petit dels possibles errors del canal que requereixen molts més passos per a la seva correcció que no pas la resta d'errors. De la resta d'errors, que són la gran majoria, se'n diu errors genèrics [6,7]. En aquest treball hem estudiat la correcció dels errors genèrics i hem definit codis pels que, almenys la correcció dels errors genèrics és garantida, deixant de banda els errors de la minoria més difícil de corregir. Això permet d'obtenir paràmetres molt més bons.

Finalment, en aquest treball tornem a fer èmfasi en els semigrups numèrics, ja explicats a l'article [Com reduir les errades en la transmissió de dades? Les matemàtiques donen la resposta](#). Es demostra com la coneguda classe dels semigrups numèrics

d'Arf [1,5,8] pot ser caracteritzada en termes dels codis que s'obtenen quan garantim exclusivament la correcció dels errors genèrics. En efecte, els semigrups d'Arf són aquells pels quals es tenen els mateixos requeriments per a descodificar un error dels cars que per descodificar un error genèric. Són exactament els que no discriminen.

- [1] Arf, C.: Une interprétation algébrique de la suite des ordres de multiplicité d'une branche algébrique, Proc. London Math. Soc. 50 (2), 256–287, (1948)
- [2] Duursma, I.M.: Majority coset decoding, IEEE Trans. Inform. Theory 39 (3), 1067–1070, (1993)
- [3] Feng, G.L., Rao, T.R.N.: Decoding algebraic-geometric codes up to the designed minimum distance, IEEE Trans. Inform. Theory 39 (1), 37–45, (1993)
- [4] Høholdt, T., van Lint, J.H., Pellikaan, R.: Algebraic geometry codes, Amsterdam: North-Holland, 871–961, (1998)
- [5] Lipman, J.: Stable ideals and Arf rings, Am. J. Math. 93, 649–685, (1971)
- [6] O'Sullivan, M.E.: Decoding of Hermitian codes beyond  $(d_{\min}-1)/2$ , In Proceedings of the 1997 IEEE Int. Symp. on Inform. Theory, 384, Ulm, (1997)
- [7] Pellikaan, R.: On decoding by error location and dependent sets of error positions, Discrete Math. 106/107, 369–381, (1992)
- [8] Rosales, J.C., García-Sánchez, P.A., García-García, J.I., Branco, M.B.: Arf numerical semigroups, J. Algebra 276 (1), 3–12, (2004)
- [9] Sakata, S.: Extension of the Berlekamp–Massey algorithm to N dimensions, Inform. Comput. 85 (2), 207–239, (1990)
- [10] Shannon, C.E.: A mathematical theory of communication, Bell System Tech. J. 27, 379–423, 623–656, (1948) 2

Maria Bras Amorós i Michael E. O'Sullivan

Departament d'Enginyeria de la Informació i de les Comunicacions

Universitat Autònoma de Barcelona

"The correction capability of the Berlekamp–Massey–Sakata algorithm with majority voting". Maria Bras Amorós, Michael E. O'Sullivan. APPLICABLE ALGEBRA IN ENGINEERING, COMMUNICATION AND COMPUTING. (Volume 17, Number 5/October, 2006).