New lower bounds on the generalized Hamming weights of AG codes

Maria Bras-Amorós

Universitat Rovira i Virgili, Tarragona, Spain

(Joint work with Kwankyu Lee, Albert Vico-Oton)

The generalized Hamming weights of a linear code are, for each given dimension, the minimum size of the support of the linear subspaces of that dimension. They were first used by [12] to analyze the performance of the wire-tap channel of type II introduced in [9] and in connection to t-resilient functions. See also [7]. The connections with the wire-tap channel have been updated recently in [10], this time using network coding. The notion itself has also been generalized for network coding in [8]. The generalized Hamming weights have also been used in the context of list decoding [4, 3] and for bounding the covering radius of linear codes [6].

In this contribution we deal with generalized Hamming weights of one-point AG codes from the perspective of the associated Weierstrass semigroup, that is, the set of pole orders at the defining one-point of the rational functions having only poles in that point. One first result on the maximum gap of an ideal of a numerical semigroup will then give a lower bound on the generalized Hamming weights via the so-called Feng-Rao numbers.

A numerical semigroup is a subset of $\mathbb{N}_0$ that contains 0, is closed under addition, and has a finite complement in $\mathbb{N}_0$. The elements in this complement are called the gaps of the semigroup and the number of gaps is the genus. The maximum gap is usually referred to as the Frobenius number of the semigroup and the conductor is the Frobenius number plus one. By the pigeonhole principle it is easy to prove that the Frobenius number is at most twice the genus minus one, and there are semigroups attaining this bound (called symmetric semigroups).

An ideal of a numerical semigroup is a subset of the semigroup such that any element in the subset plus any element of the semigroup add up to an element of the subset. Again the ideal will be a subset of $\mathbb{N}_0$ with finite complement in it. The elements in this complement are called gaps of the ideal. Our first result is an analogous of the upper bound on the Frobenius number for the largest gap of an ideal. Indeed, we prove that the largest gap of an ideal is at most the size of the complement of the ideal in the semigroup plus twice the genus minus one. This generalizes the bound on the Frobenius number since that bound can be derived from this bound by taking the ideal to be the whole semigroup.

A nice tool for takling the generalized Hamming weights for AG codes are the generalized order bounds introduced in [5], involving Weierstrass semigroups. In [1], a constant depending only on the semigroup and the dimension of the Hamming weights was introduced, from which the order bounds could be completely determined for codes of rate low enough. This constant was called Feng–Rao number in the same reference. In the present contribution, using the upper bound on the maximum gap of an ideal, we derive a lower bound on the so-called Feng-Rao numbers and so a new bound on the Hamming weights. The main tool is analyzing the intervals of consecutive gaps of the Weierstrass semigroup. Consecutive gaps were already used in [2] for bounding the minimum distance of codes and in [11] for bounding the generalized Hamming weights.

In the last section we study the intervals of consecutive gaps for Hermitian codes and for codes in one of the Garcia-Stichtenoth towers of codes attaining the Drinfeld-Vlăduţ bound.

References

[1] J. I. Farrán and C. Munuera. Goppa-like bounds for the generalized Feng-Rao distances. *Discrete Appl. Math.*, 128(1):145–156, 2003. International Workshop on Coding and Cryptography (WCC 2001) (Paris).

[2] Arnaldo García, Seon Jeong Kim, and Robert F. Lax. Consecutive Weierstrass gaps and minimum distance of Goppa codes. *J. Pure Appl. Algebra*, 84(2):199–207, 1993.

[3] Parikshit Gopalan, Venkatesan Guruswami, and Prasad Raghavendra. List decoding tensor products and interleaved codes. In *STOC'09—Proceedings of the 2009 ACM International Symposium on Theory of Computing*, pages 13–22. ACM, New York, 2009.

[4] Venkatesan Guruswami. List decoding from erasures: bounds and code constructions. *IEEE Trans. Inform. Theory*, 49(11):2826–2833, 2003.

[5] Petra Heijnen and Ruud Pellikaan. Generalized Hamming weights of q-ary Reed-Muller codes. *IEEE Trans. Inform. Theory*, 44(1):181–196, 1998.

[6] H. Janwa and A. K. Lal. On generalized Hamming weights and the covering radius of linear codes. In *Applied algebra, algebraic algorithms and error-correcting codes*, volume 4851 of *Lecture Notes in Comput. Sci.*, pages 347–356. Springer, Berlin, 2007.

[7] Carlos Munuera. Generalized Hamming weights and trellis complexity. *Advances in Algebraic Geometry Codes, E. Martinez-Moro, C. Munuera, D. Ruano (eds.), World Scientific*, pages 363–390, 2008.

[8] Chi-Kin Ngai, Raymond W. Yeung, and Zhixue Zhang. Network generalized Hamming weight. *IEEE Trans. Inform. Theory*, 57(2):1136–1143, 2011.

[9] L. H. Ozarow and A. D. Wyner. Wire-tap channel II. In *Advances in cryptology (Paris, 1984)*, volume 209 of *Lecture Notes in Comput. Sci.*, pages 33–50. Springer, Berlin, 1985.

[10] Salim El Rouayheb, Emina Soljanin, and Alex Sprintson. Secure network coding for wiretap networks of type II. *IEEE Trans. Inform. Theory*, 58(3):1361–1371, 2012.

[11] Lizhong Tang. Consecutive Weierstrass gaps and weight hierarchy of geometric Goppa codes. *Algebra Colloq.*, 3(1):1–10, 1996.

[12] Victor K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory*, 37(5):1412–1418, 1991.

Universitat Rovira i Virgili, Departament d'Enginyeria Informàtica i Matemàtiques
Av. Països Catalans, 26 , Campus Sescelades, 43007 Tarragona
maria.bras@urv.cat