A Johnson-Type Bound for Group Codes and Lattices

Malihe Aliasgari, Mohammad-Reza Sadeghi
Amirkabir University of Technology (Iran)

Daniel Panario
Carleton University (Canada)

ariyadokht@aut.ac.ir

Extended abstract

In this work we give and analyze a Johnson-type bound for group codes considering the G-norm. Johnson bounds have been given for binary and q-ary codes [5, 7, 8] with respect to the Hamming distance. We borrow the idea of the G-norm from [3] and define a new distance for codewords: the G-semidistance. We extend the Johnson-type bounds for binary and q-ary codes to the G-semidistance and give a relation between these bounds and our G-semidistance. By means of this, we present an upper bound on the number of codewords inside a G-ball and an l_1-ball, within a certain given radius, for both group codes and lattices.

Johnson-type bounds provide an upper bound on the number of codewords in a Hamming ball with a specified radius. The original proof is based on linear algebra [5, 8]; proofs with a geometric view are presented in [1]. The extension of Johnson-type bounds for q-ary codes is given in [7]. In all of these works the Johnson-type bounds use Hamming balls. Here we consider G-balls with an arbitrary received vector as the G-ball's center, given a specified radius; we find an upper bound for the number of codewords in the G-ball. Roughly speaking, we investigate the number of codewords such that their G-semidistances from the received word is less than the radius of the G-ball.

Recently the question of list decoding under the Hamming metric has become an important trend in coding theory. In addition, list decoding for lattices are given in [6, 9]. Our Johnson-type bound, when applied to some recent works [2, 3], may lead to list decoding of q-ary codes, group codes and lattices via the G-norm.

Let $\mathbf{x} = (x_1, \ldots, x_n)$ be in a group code G. The G-norm for $\mathbf{x}$ is defined as $\|\mathbf{x}\|_G = x_1 + x_2 + \cdots + x_n$ where the operations are performed in $\mathbb{R}$ [3].

Definition 1 *Let $G = \mathbb{Z}_{g_1} \times \cdots \times \mathbb{Z}_{g_n}$. For any vectors $\boldsymbol{a}, \boldsymbol{b} \in G$ we define the G-semidistance of $\boldsymbol{a}$ and $\boldsymbol{b}$ with respect to the G-norm, denoted by $d_G(\boldsymbol{a}, \boldsymbol{b})$, as follows*

$$d_G(\boldsymbol{a}, \boldsymbol{b}) = \min\{\|\boldsymbol{a} - \boldsymbol{b}\|_G, \|\boldsymbol{b} - \boldsymbol{a}\|_G\}.$$

Our main contributions are twofolded:

- a Johnson-type bound for group codes, and
- a Johnson-type bound for lattices.

In order to obtain our first result we prove the following theorem.

Theorem 2 *Let $\mathcal{C}$ be a block code in $G = \mathbb{Z}_{g_1} \times \cdots \times \mathbb{Z}_{g_n}$ and $\alpha = d_H/n$ where d_H is the minimum Hamming distance of the code, $0 < \alpha < 1$. Consider $\omega = ng\beta$ where $0 < \beta < 1$ and $g = \max\{g_1, \ldots, g_n\}$. If $g \geq 3$ and $\beta < \sqrt{\alpha}$, then $|\mathcal{B}_{\mathcal{C}}(\omega)| \leq 2ng$, where $|\mathcal{B}_{\mathcal{C}}(\omega)|$ is the number of codewords with G-semidistance from 0 less than ω.*

Now, using the above theorem we present the following method to show that for a received word $\mathbf{a} \in G$ and a specific radius ω, the upper bound for $|\mathcal{B}_{\mathcal{C}}(\mathbf{a}, \omega)|$ is at most $2ng$.

Method. Let $\mathbf{a}$ be an arbitrary vector in G and ω a real number, $0 < \omega < ng$. Our goal is to find $|\mathcal{B}_{\mathcal{C}}(\mathbf{a}, \omega)|$, that is, the number of codewords in $\mathcal{C}$ with G-semidistance from $\mathbf{a}$ less than ω. Accordingly, we consider the following two block codes

$$\mathcal{A}_1 = \mathbf{a} - \mathcal{C} = \{\mathbf{a} - \mathbf{c} | \mathbf{c} \in G\} \quad \text{and} \quad \mathcal{A}_2 = \mathcal{C} - \mathbf{a} = \{\mathbf{c} - \mathbf{a} | \mathbf{c} \in G\}.$$

Set $\alpha_1 = d_1/n$ and $\alpha_2 = d_2/n$ where d_1, d_2 are the minimun Hamming distances of $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively. Also assume that $\omega_1 = ng\beta_1$ and $\omega_2 = ng\beta_2$. To find $|\mathcal{B}_{\mathcal{C}}(\mathbf{a}, \omega)|$ we investigate the maximum number of codewords in the block codes $\mathcal{A}_i$ with G-semidistance less than ω_i, $i = 1, 2$. Now, it is sufficient to choose $\omega = \min\{\omega_1, \omega_2\}$, equivalently to $\mathcal{A}_1$ or $\mathcal{A}_2$, the one with smaller minimum Hamming distance. Hence, by Theorem 2, the upper bound for $|\mathcal{B}_{\mathcal{C}}(\mathbf{a}, \omega)|$ is at most $2ng$ with the smaller value between α_1 or α_2, that implies the smaller value of ω_1 or ω_2.

In order to obtain our second result, we employ the Johnson-type bound for group codes in Theorem 2 to derive a Johnson-type bound for cosets of a lattice Λ. It should be noted that our group code Johnson-type bound with G-norm results in a lattice Johnson-type bound with l_1-norm.

The label code of a lattice Λ play a key role to provide a Johnson-type bound on the number of cosets for Λ. Consider a decomposition of the lattice into two parts, a label code L and an orthogonal sub-lattice $\Lambda' = \mathbb{Z}^n C(\Lambda)$ as follows

$$\Lambda = LP(\Lambda) + \mathbb{Z}^n C(\Lambda),$$

where L is a label code over G and $P(\Lambda), C(\Lambda)$ are the projection and cross section of Λ, respectively [4]. This decomposition of Λ entails that a vector $\mathbf{v} \in \mathbb{R}^n$ belongs to Λ if it can be expressed as $\mathbf{v} = \mathbf{k}C(\Lambda) + \mathbf{c}P(\Lambda)$, for some $\mathbf{k} \in \mathbb{Z}^n$ and $\mathbf{c} \in L$.

Theorem 3 *Let Λ be an arbitrary lattice in $\mathbb{R}^n$ with label code L over the alphabet sequence G. Assume that $\boldsymbol{r}$ is a received word in $\mathbb{R}^n$ and $\boldsymbol{a} \in G$ is an associated codeword of the closest coset of Λ' to $\boldsymbol{r}$ in $\mathbb{R}^n$. Consider the n components P_{Λ_i}, $1 \leq i \leq n$, of the projection of Λ, and let p be the maximum value of $|P_{\Lambda_i}|$. Then $g \geq 3$ and $\beta < \sqrt{\alpha}$ yields that the number of lattice cosets in an l_1-ball, with $\boldsymbol{r}$ as its center and radius $pn\beta$, is at most $2ng$.*

Keywords

Johnson bound, group codes, lattices, G-norm

References

[1] E. Agrell, A. Vardy and K. Zeger, "Upper bounds for constant-weight codes", *IEEE Trans. Inform. Theory,* vol. 46, pp. 2373–395, 2000.

[2] M. Aliasgari and M.-R. Sadeghi, "An algebraic method for decoding q-ary codes via submodules of $\mathbb{Z}^n$", *IEEE Commun. Letters*, to appear, 2014.

[3] M. Aliasgari, M.-R. Sadeghi and D. Panario, "Gröbner bases for lattices and an algebraic decoding algorithm", *IEEE Trans. Commun.*, vol. 61, pp. 1222–1230, 2013.

[4] A. H. Banihashemi and F. R. Kschischang, "Tanner graphs for block codes and lattices: construction and complexity", *IEEE Trans. Inf. Theory*, vol. 47, pp. 822–834, 2001.

[5] P. Elias, "Error-correcting codes for list decoding", *IEEE Trans. Inform. Theory,* vol. 37, pp. 5–12, 1991.

[6] E. Grigorescu and C. Peikert, "List decoding Barnes-Wall lattices", *in Proc. 2012 IEEE Conference on Computational Complexity*, pp. 316–325, 2012.

[7] V. Guruswami and M. Sudan, "Extensions of the Johnson bound", Available from `http://people.csail.mit.edu/madhu/papers`, 2001.

[8] S. M. Johnson, "A new upper bounds for codes and designs", *IEEE Trans. Inform. Theory,* vol. 9, pp. 198–205, 1963.

[9] Y. Song and N. Devroye, "Lattice codes for the Gaussian relay channel: decode-and-forward and compress-and-forward", *IEEE Trans. Inf. Theory*, vol. 59, pp. 4927–4948, 2013.