Bounds on List Decoding Gabidulin Codes

Antonia Wachter-Zeh
Institute of Communications Engineering, Ulm University, Ulm, Germany and
Institut de Recherche Mathématique de Rennes, Université de Rennes 1, Rennes, France
antonia.wachter@uni-ulm.de

Gabidulin codes can be seen as the analogs of Reed–Solomon (RS) codes in rank metric. There are several efficient decoding algorithms up to half the minimum rank distance. However, in contrast to RS codes, there is no polynomial-time list decoding algorithm; it is not even known, whether such an algorithm can exist or not. An exponential lower bound on the number of codewords in a ball of radius τ around the received word would prohibit polynomial-time list decoding since the list size can be exponential, whereas a polynomial upper bound would show that it might be possible.

We provide a lower and an upper bound on the list size. The lower bound shows that the list size can be exponential in the length when the radius is at least the Johnson radius and therefore in this region, no polynomial-time list decoding is possible. The upper bound uses the properties of subspaces and gives a good estimate of the number of codewords in such a ball, but is exponential in the length and therefore does not provide an answer to polynomial-time list decodability in the region up to the Johnson bound.

Let q be a power of a prime, let $\mathbb{F}_q$ denote the finite field of order q and let $\mathbb{F}_{q^m}$ be the extension field of degree m over $\mathbb{F}_q$. Let $\mathcal{G}(n,k)$ denote a linear Gabidulin code of length n and dimension k over $\mathbb{F}_{q^m}$ with $n \leq m$, which is the set of all codewords, which are the evaluation of q-degree restricted linearized polynomials $f(x) \in \mathbb{F}_{q^m}[x]$ with $\deg_q f(x) < k$. Moreover, $\mathcal{B}_\tau(\mathbf{a})$ denotes a ball of radius τ in rank metric around a word $\mathbf{a} \in \mathbb{F}_{q^m}^n$ and $\left[{n \atop s}\right] \overset{\text{def}}{=} \prod_{i=0}^{s-1} \frac{q^n - q^i}{q^s - q^i}$ denotes the Gaussian binomial.

Theorem 1 (Lower Bound on the List Size) *Let the Gabidulin code $\mathcal{G}(n,k)$ over $\mathbb{F}_{q^m}$ with $n \leq m$ and $d = n-k+1$ be given. Let $\tau < d$. Then, there exists a word $\mathbf{r} \in \mathbb{F}_{q^m}^n$ such that*

$$\ell \geq |\mathcal{B}_\tau(\mathbf{r}) \cap \mathcal{G}| \geq \frac{\left[{n \atop n-\tau}\right]}{(q^m)^{n-\tau-k}} = q^m q^{\tau(m+n)-\tau^2-md}, \tag{1}$$

and for the special case of $n = m$: $\ell \geq q^n q^{2n\tau-\tau^2-nd}$.

For $n = m$, we can rewrite (1) by $\ell \geq q^{n(1-\epsilon)} \cdot q^{2n\tau-\tau^2-nd+n\epsilon}$, where the first part is exponential in n for any $0 \leq \epsilon < 1$. The second exponent is positive for

$$\tau \geq n - \sqrt{n(n-d+\epsilon)} \overset{\text{def}}{=} \tau_{LB}.$$

Therefore, our lower bound (1) shows that the maximum list size is exponential in n for $\tau \geq \tau_{LB}$. For $\epsilon = 0$, the value τ_{LB} gives exactly the Johnson radius for Hamming metric.

This reveals a difference between the known limits to list decoding of Gabidulin and RS codes. For RS codes, polynomial-time list decoding up to the Johnson radius is guaranteed by the Guruswami–Sudan algorithm. However, it is not proven that the Johnson radius is tight for RS codes, i.e., it is not known if the list size is polynomial between the Johnson radius and the known exponential lower bounds.

Theorem 2 (Upper Bound on the List Size) *Let the Gabidulin code $\mathcal{G}(n,k)$ over $\mathbb{F}_{q^m}$ with $n \leq m$ and $d = n-k+1$ be given. Let $\tau < d$. Then, for any word $\mathbf{r} \in \mathbb{F}_{q^m}^n$ and hence, for the maximum list size, the following holds*

$$\begin{aligned} \ell = \max_{\mathbf{r} \in \mathbb{F}_{q^m}^n} \left(|\mathcal{B}_\tau(\mathbf{r}) \cap \mathcal{G}|\right) &\leq \sum_{t=\left\lfloor \frac{d-1}{2} \right\rfloor+1}^{\tau} \frac{\left[{n \atop 2t+1-d}\right]}{\left[{t \atop 2t+1-d}\right]} \\ &\leq 4 \sum_{t=\left\lfloor \frac{d-1}{2} \right\rfloor+1}^{\tau} q^{(2t-d+1)(n-t)} \leq 4\left(\tau - \left\lfloor \tfrac{d-1}{2} \right\rfloor\right) \cdot q^{(2\tau-d+1)(n-\lfloor (d-1)/2 \rfloor-1)}. \end{aligned}$$

Thus, we have proved an upper bound on the maximum list size of a Gabidulin code. Unfortunately, this upper bound is exponential in $n \leq m$ for any $\tau > \lfloor (d-1)/2 \rfloor$ and therefore does not provide any conclusion if polynomial-time list decoding is possible or not in the region up to the Johnson bound.

This work was supported by the German Research Council "Deutsche Forschungsgemeinschaft" (DFG) under Grant No. Bo 867/21-2.