1011-68-255 **Eli Ben-Sasson**, **Swastik Kopparty** and **Jaikumar Radhakrishnan*** (jaikumar@tifr.res.in), 1427 E 60th Street, 2nd Floor, Chicago, IL 60637. *The list-decoding radius for Reed-Solomon codes.* Preliminary report.

We consider the list decoding problem for Reed-Solomon codes, where given a field $\mathbb{F}$ of size N, a word $w : \mathbb{F} \to \mathbb{F}$ and integers $a, d \geq 1$, we are required to list all polynomials of degree at most d that agree with w on at least a points. Johnson's bound implies that if $a > \sqrt{Nd}$, then the list has at most $O(N^2)$ polynomials. In this case, an algorithm of Guruswami and Sudan can produce this list in polynomial time. However, it is not known if Johnson's bound is tight or the list is of polynomial size even if we require significantly less than $\sqrt{Nd}$ agreements.

We show that for all $\delta \in (0, 1)$ and $\epsilon > 0$, for infinitely many N, there is a word $w : \mathbf{F} \to \mathbf{F}$ such that the number of polynomials of degree N^δ with agreement at least $N^{\sqrt{\delta}-\epsilon}$ is $N^{\Omega(\log N)}$. Thus, for $d = \sqrt{N}$ there cannot be a polynomial time algorithm list decoding algorithm when $a = N^{0.7}$ (say). Before this work, such a superpolynomial lower bound on the number of polynomials was know for $a = 2\sqrt{N}$. Note that for this setting of parameters, Johnson's bound implies that the list is of size $O(N^2)$ when $a < N^{0.75}$. (Received August 29, 2005)