Progress report - Zeev Dvir (Princeton)

Locally correctable codes [BDWY11, BDSS11]

A locally correctable code (LCC) is an error correcting code which has the additional property that a codeword can be corrected in a local way. More precisely, given an index in a corrupted codeword, there is a probabilistic algorithm that can correct that position by looking in at most q other positions, where q is some number which is much smaller than the total length of the codeword. We call such a code a q-LCC. LCCs are very important tools in computational complexity and have played a role in several different areas ranging from PCPs to polynomial identity testing. There are huge gaps between the lower and upper bounds on the rate of such codes.

In a joint work with PIs Wigderson and Barak and with Postdoc Yehudayoff (to appear in STOC 2011), we study the question of 2-LCCs over fields of characteristic zero. This non standard setting (allowing for infinite alphabet) is motivated by my recent result (reported on last year) connecting LCCs to circuit complexity. In this setting we show that there are *no* 2-LCCs. This result follows by a lower bound on the rank of matrices with certain pattern of zeros and non zeros. Our work also shows a connecting between LCCs and theorems in combinatorial geometry known as 'Sylvester-Gallai' type theorems. Our result translate into bounds on the number of intersection lines in real space can have with each other, strengthening substantially the known results in this area.

In a following joint work with Bhattacharia, Saraf (center postdoc) and Shpilka we study the question of 2-LCC's over finite fields. It was known that these codes, which do exist over these fields, require encoding length 2^n when the message size is n. This exponential lower bound was tight over fields of characteristic two but there was still a gap finite fields of larger characteristic. We close this gap, showing that, over a field of characteristic p, the encoding length is $p^{\Omega(n)}$ which is the best possible bound. Our proof uses, and extends, known tools from additive combinatorics, further strengthening the (already strong) connection between these tools and the study of computational complexity. The work was submitted for publication to FOCS 2011.

The entropy of polynomial mappings [DGRV11]

In a joint work with Gutfreund, Rothblum (center postdoc) and Vadhan (ICS 2011). We investigate the complexity of the following computational problem: Given a low-degree polynomial mapping $p : \mathbb{F}^n \mapsto \mathbb{F}^m$, where $\mathbb{F}$ is a finite field, approximate the the output entropy $H(p(U_n))$, where U_n is the uniform distribution on $\mathbb{F}^n$. Our work contains both hardness and algorithmic results: On the hardness side, we show that approximating the Shannon entropy of degree 3 polynomials $p : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ over $\mathbb{F}_2$ to within an additive constant (or even $n^{.9}$) is complete for $\mathbf{SZKP_L}$, the class of problems having statistical zero-knowledge proofs where the honest verifier and its simulator are

computable in logarithmic space. ($\mathbf{SZKP_L}$ contains most of the natural problems known to be in the full class **SZKP**.) Thus, this problem can serve as a starting point for finding combinatorial or number-theoretic complete problems for $\mathbf{SZKP_L}$, giving worst-case/average-case reductions for $\mathbf{SZKP_L}$, and/or finding (possibly quantum) algorithms for $\mathbf{SZKP_L}$.

On the algorithmic side, we give a factor-2 approximation algorithm for the entropy of degree two mappings over fields of characteristic three or more. This algorithm is based on a new formula for the Renyi entropy of $p(U_n)$ in terms of the rank of directional derivatives of p. We also obtain a polynomial factor approximation algorithm for general degree d polynomials (over the field of size two). This algorithm is based on relating the max-entropy to the dimension of the $\mathbb{F}_2$-span of the p's components $p_1, \ldots, p_m \in \mathbb{F}_2[x_1, \ldots, x_n]$.

References

[BDSS11] A. Bhattacharyya, Z. Dvir, S. Saraf, and A. Shpilka. Tight lower bounds for 2-query LCCs over finite fields. Manuscript, 2011.

[BDWY11] B. Barak, Z. Dvir, A. Wigderson, and A. Yehudayoff. Rank bounds for design matrices with applications to combinatorial geometry and locally correctable codes. STOC 2011 (to appear), 2011.

[DGRV11] Z. Dvir, D. Gutfreund, G. Rothblum, and S. Vadhan. On approximating the entropy of polynomial mappings. In *Proceedings of the Second Symposium on Innovations in Computer Science (ICS 2011), Beijing, China, 7-9 January 2011*, 2011.