

Open Problems from Coding, Complexity and Sparsity Workshop

Martin J. Strauss

August 18, 2011

Abstract

This document lists some open problems discussed at the Coding, Complexity and Sparsity Workshop, The University of Michigan, August 1–4, 2011. Edited with help from the question authors. See <http://www.math.lsa.umich.edu/conferences/coding/index.html>.

1 Barrington-Straubing-Thérien conjecture (Atri Rudra)

For fixed m , consider constant-depth, polynomial-size, unbounded fanin circuits with only MOD_m gates. Barrington, Straubing, and Thérien conjectured that OR cannot be recognized by circuits of this type [BST90]. (They proved the conjecture when m is a prime power. The conjecture is open for all non-prime powers, e.g. $m = 6$.)

A possible approach builds on Hansen-Koucký [HK10]. They give a random collection \mathcal{S} of sets such that, for any non-zero boolean vector x , there is some $S \in \mathcal{S}$ such that $\|x_S\|_0 = 1$, where $\|\cdot\|_0$ denotes the number of non-zero components. That is, for any non-zero x ,

$$\bigvee_S \left(\left(\sum_{i \in S} x_i \right) \bmod m \right) = 1.$$

A set \mathcal{S} of size $\ell = O(\log^2 n)$, where for each $0 \leq i \leq \log n$, there is a set $S_{i,j}$ for $j \in [O(\log n)]$. In particular, every element in $[n]$ is in $S_{i,j}$ with probability 2^{-i} . So if $\|x\|_0 \approx 2^{-i}$ then $\|x_{S_{i,j}}\|_0 = 1$ with sufficient probability. This technique is common in sparse recovery algorithms.¹

Revisit the BST conjecture with tools of sparse recovery. In particular, can one de-randomize the Hansen-Koucký construction? Or prove that it cannot be derandomized?

2 Linear Forms and Bounded-depth Circuits (Shachar Lovett)

Consider the following circuit class.

Given input x of length n , suppose we take $N = n^{O(1)}$ linear forms over $GF(2)$ $\ell_1(x), \ell_2(x), \dots, \ell_N(x)$, then take an AC^0 circuit of size $\text{poly}(n)$ whose inputs are $\ell_1(x), \ell_2(x), \dots, \ell_N(x)$. What linear forms are possible to compute / approximate this way? Conjecture: only linear forms which are sparse linear combination of ℓ_1, \dots, ℓ_N with sparsity $\text{poly}(\log(n))$.

3 Subspace-evasive Set (Venkatesan Guruswami)

Consider the field \mathbb{F}_q^n , for $q \approx n$.

¹One still needs to show that the OR of $O(\log^2 n)$ bits can be computed by a constant depth circuit with polynomially many MOD_m gates. [BST90] show that OR on $\log n$ bits can be computed by constant depth circuits with polynomially many MOD_m gates. Finally, note that OR on $O(\log^2 n)$ bits can be computed by a polynomial sized depth two circuit with OR gates on $\log n$ input bits.

A set $W \subseteq \mathbb{F}_q^n$ is called (s, ℓ) -subspace-evasive if for any s -dimensional subspace $S \in \mathbb{F}_q^n$, we have $|W \cap S| \leq \ell$. Note that $\ell = q^s$ is the trivial bound.

Think of s as a constant (i.e., it is independent of n, q). Even specific small values of s , like 5 or 6, would be interesting. The goal is to find large subspace-evasive set W with small ℓ .

It can be shown that a random W of size $|W| \approx q^{(1-\epsilon)n}$ is $(s, O(s/\epsilon))$ -subspace-evasive. Explicit constructions are desired (the motivation comes from a recent application to list-decodable codes, see <http://arxiv.org/abs/1106.0436>, but this seems like a very natural problem in pseudorandomness in itself). Even a construction with $|W| = q^{n/2}$ that is $(s, 2^{O(s)})$ -subspace-evasive would be very interesting to begin with.

Speculation ensued as to candidate constructions and candidate refutations of the same. This included product sets, bent functions, affine extractors, etc. A connection of the problem over the binary field ($q = 2$) and bipartite Ramsey graphs was also alluded to.

4 Unbalanced Bipartite Expanders for Compressed Sensing (Atri Rudra)

A bipartite graph² $G : [n] \times [d] \rightarrow [m]$ is a (K, ϵ) -expander if for every subset $S \subseteq [n]$ such that $|S| \leq K$, the number of its right neighbors is at least $|S| \cdot d \cdot (1 - \epsilon)$. It is known that a random bipartite left regular graph is a (K, ϵ) -expander with $d = O(\log(n/m)/\epsilon)$ and $m = O(Kd/\epsilon)$. In complexity applications, one wants to obtain explicit constructions that *simultaneously* achieve the best possible bound on d in terms of n and the best possible bound on m in terms of k and d . The best explicit construction is due to Guruswami, Umans and Vadhan [GUV09] who for any constant $\alpha > 0$ obtain, $d = O(\log n \log K/\epsilon)^{1+1/\alpha}$ and $m = O(d^2 K^{1+\alpha})$.

It is known that an $(O(k), \epsilon)$ -expander leads to an ℓ_1/ℓ_1 for all compressed sensing matrix with sparsity parameter k [IR08]. However, there are two relaxations on what is needed from expanders in the typical complexity applications:

1. One cares about the expansion of subsets of left vertices of size $\Theta(k)$ only; and
2. More importantly, the value of d is not that important— it is more critical to obtain a value of m that is closer to the $O(k \log n/\epsilon^2)$ bound that is achieved by random expanders. (Actually because of the previous requirements, the random construction achieve $O(k \log(n/k)/\epsilon)$).

With the above in mind, GUV leads to $O(k^{1+\alpha} \cdot (\log n \log k/\epsilon)^{2+2/\alpha})$ number of measurements for the resulting compressed sensing matrix, which is not that great. However, combining the GUV construction with an earlier expander construction for constant ϵ , one can obtain an expander with $(k \log n)^{1+o(1)}$ many measurements [INR10].³ Two open questions spring to mind:

1. Can one obtain an $(O(k), \epsilon)$ -expander with $(k \log n)^{1+o(1)} \cdot (1/\epsilon)^{O(1)}$ many right vertices?
2. Given that the compressed sensing application has the two weaker constraints, can one construct even better explicit compressed sensing matrices using expanders?

5 Other/miscellaneous

What are the main challenges? Answer: See Andrew McGregor's blog: <http://polylogblog.wordpress.com/>

²That is, G has n left vertices and m right vertices with G being left regular with degree d .

³The combination of expanders is a folklore result and was pointed out to the authors of [INR10] by Chris Umans.

References

- [BST90] David A. Mix Barrington, Howard Straubing, and Denis Thérien. Non-uniform automata over groups. *Inf. Comput.*, 89(2):109–132, 1990.
- [GUV09] Venkatesan Guruswami, Christopher Umans, and Salil P. Vadhan. Unbalanced expanders and randomness extractors from parvaresh–vardy codes. *J. ACM*, 56(4), 2009.
- [HK10] Kristoffer Arnsfelt Hansen and Michal Koucký. A new characterization of ACC^0 and probabilistic CC^0 . *Computational Complexity*, 19(2):211–234, 2010.
- [INR10] Piotr Indyk, Hung Q. Ngo, and Atri Rudra. Efficiently decodable non-adaptive group testing. In *SODA*, pages 1126–1142, 2010.
- [IR08] Piotr Indyk and Milan Ruzic. Near-optimal sparse recovery in the l1 norm. In *FOCS*, pages 199–207, 2008.