ABSTRACT

The main result of this paper is a near-optimal derandomization of the affine homomorphism test of Blum, Luby and Rubinfeld [11].

We show that for any groups G and gamma, and any expanding generating set S of G, the natural deramdomized version of the BLR test in which we pick an element x randomly from G and y randomly from S and test whether f(x) _ f(y) = f(x _ y), performs nearly as well (depending of course on the expansion) as the original test. Moreover we show that the underlying homomorphism can be found by the natural local \belief propagation decoding".

We note that the original BLR test uses 2 $\log_2$ jGj random bits, whereas the derandomized test uses only (1+o(1)) $\log_2$ jGj random bits. This factor of 2 savings in the randomness complexity translates to a near quadratic savings in the length of the tables in the related locally testable codes (and possibly probabilistically checkable proofs which may use them).

Our result is a significant generalization of the recent result of [12], who proved such a result only for the groups G = $Z_{m\,p}$ and _ = Z_p. It is also an explicit version of the nonconstructive result of [18].

We use a simple combinatorial arguments and the transitivity of Cayley graphs (and this analysis gives optimal results up to constant factors). Previous techniques used the Fourier transform, a method which seems unextendable to general groups (and furthermore gives suboptimal bounds).

Finally, we provide a polynomial time (in jGj) construction of a (somewhat) small (jGj_) set of expanding generators for every group G, which yield e_cient testers of randomness (1+_) log jGj for every group G. This follows a simple derandomization of the probabilistic construction of [5], who showed that almost all logarithmicsize sets are expanding.

Our work motivates further study of similar derandomizations of other natural property testing procedures, especially those more relevant to the local testing of better codes and to PCPs.