# Approximation Algorithms, exercise sheet 11

January 31, 2014

## 1. The mixing property of expander graphs

Let $G$ be a $d$-regular expander graph with $n$ vertices that has expansion parameter $\lambda = 0.9$. This means that for any set $S$ of vertices in $G$, the following holds. If $s$ is a random vertex in $S$ and $t$ is the vertex that is reached after a random walk of lenth $k$ which starts in $s$, then $\Pr[t \in S] \leq |S|/n + \lambda^k$. Let $F$ be a set containing exactly an $\epsilon$-fraction of edges in $G$. Let $W = \langle i_1, \ldots, i_\ell + 1 \rangle$ be a random walk of length $\ell$ in $G$. What lower bound can you find for the probability that $W$ contains an edge that belongs to $F$?

## 2. The sum verifier

The original proof of the PCP theorem is more algebraic than the Dinur proof. In that proof multivariate low-degree polynomials are used as coding objects. That are polynomials from $F^n$ to $F$, where $F$ is some finite field with $|F|$ being prime. The max-degree (i.e. the largest degree that one of the variables has) of such polynomials should be much less than $|F|$. For example: $p : \{0, 1, \ldots, 31\}^4 \to \{0, 1, \ldots, 31\}$ defined as $p(x_1, x_2, x_3, x_4) := x_1^3 + 5x_2x_3^2x_4^2 - 2x_1x_3 + 21$. One of the problems that has to be solved is the following. Suppose you have access to a low-degree polynomial $p : F^n \to F$ and you want to know whether $\sum_{x \in \{0,1\}^n} p(x) = 0$, but you want to make only $\mathrm{O}(\mathrm{poly}(n))$ queries. Can you design a verifier which meets this query bound, always accepts in case $\sum_{x \in \{0,1\}^n} p(x) = 0$ and a correct proof is given and rejects with high probability in case $\sum_{x \in \{0,1\}^n} p(x) \neq 0$ no matter what proof is given.