1- the learning parity with noise problem

Let n and tau in (0,1).
The (search version of) the learning parity with noise problem is to find a in Z_2^n from arbitrarily many samples of the form (a_i, <a_i,s>+e_i) in Z_2^{n+1}, where the a_i's are iid uniform and the ei's are from a Bernoulli distribution of parameter tau.
The decision version consists in distinguishing such samples from a uniform s, from uniform samples in Z_2^{n+1}.
(give the oracle based definition, give the distinguishing advantage)

Give the search to decision reduction?

Remarks.

- this is like decoding a random linear code in the low-weight error regime, but with an arbitrary code length. Draw a matrix.
- Tau is known.
- Tau =0 => trivially easy
- Tau=1/2 => trivially hard
- Tau <=1 without loss of generality

Given an s, how to check it's the correct one?
Take bi-<ai,s>. It's either uniform, or Bernoulli. How to distinguish? Majority test.
Pr [N>= m*tau* (1+delta) or <= m*tau* (1-delta)] <= 2*exp(-m*tau*delta^2/3)

To distinguish with error less than eps, take delta such that
m tau(1+delta) <= m *1/2 * (1-delta). For example, delta = (1/2-tau)/2. And m linear in ln(1/eps)/(tau*delta^2).

2- Aleknovitch's encryption

KeyGen: $[A, As+e] =: B$

$pk := B$; $sk := e$ or s.

Enc $(M \in \{0,1\})$: sample $b^\perp$ unif. in $B^\perp$; e' Bernoulli of τ.

if $M=0$: $b^\perp + e'$

if $M=1$: u unif

Dec: $\langle c, e \rangle = \begin{cases} \text{unif if } M=1 \\ \underbrace{\langle b^\perp, e\rangle}_{=0} + \underbrace{\langle e, e'\rangle}_{0?} \end{cases}$

There are $\simeq \tau m$ indices i: $e_i \neq 0$

We want that for all of these $e'_i = 0$

This happens with probability $\exp(+\tau m \ln(1-\tau)) \simeq \exp(-\tau^2 m)$

over the randomness of b'. $\rightsquigarrow$ Take $\tau = o(1/\sqrt{m})$.

$0 \longrightarrow 0$ with pr $\simeq 1$

$1 \longrightarrow \begin{cases} 0 \text{ with pr} = 1/2 \\ 1 \text{ with pr} = 1/2 \end{cases}$

repeat and use an error correcting code to boost correctness.

Security: . under LPN, $B \simeq^c$ unif.

. under LPN for code $B^\perp$, $b^\perp + e'$ is $\simeq^c$ unif. $\blacksquare$

③ The BKW algorithm

- sample lots of $a_i, b_i = \langle a_i, s\rangle + e_i$.
- put them in buckets, according to their first ℓ entries: 2^ℓ buckets
- take a pair of samples (a_i, b_i), (a_j, b_j) of the same bucket, and map them to $(a_i+a_j, b_i+b_j) = (a_i+a_j, \langle a_i+a_j, s\rangle + (e_i+e_j))$.

This maps L samples in dim n with param τ to $L/2$ samples in dim $n-\ell$ with param $2\tau(1-\tau)$.
($e_i=0 \wedge e_j=1$ or $e_i=1 \wedge e_j=0$)

at a cost of $\lesssim \max(L, 2^\ell)$

Repeat n/ℓ times. At the last step, we ensure that $a_i+a_j = 0\cdots01$ rather than $0\cdots0$.
This gives samples of the form $0\cdots01, s_n+e_i$, $i=1\ldots$

Noise rate at the end: $\tau^{end} = \frac{1}{2} - \frac{1}{2}(1-2\tau)^{2^{n/\ell}}$ (proof by induction)

$$\left(2\cdot\left[\tfrac{1}{2}-\tfrac{1}{2}(1-2\tau)^{2^i}\right]\left[1-\tfrac{1}{2}+\tfrac{1}{2}(1-2\tau)^{2^i}\right] = \tfrac{1}{2}-\tfrac{1}{2}(1-2\tau)^{2^{i+1}} \right)$$

We want to use a major rule to distinguish. By what we did earlier, we could do with $\lesssim n / \tau^{end}\cdot(\frac{1}{2}-\tau^{end})^2$

$$\lesssim n / (1-(1-2\tau)^{n/\ell})(1-2\tau)^{2^{n/\ell}} \quad \text{samples}$$

To balance out the costs, we make τ^{end} not too small. $\lesssim$) what matters
(else we could decrease ℓ i.e., repeat more times) is $(1-2\tau)^{-2^{n/\ell}}$.

Cost $\lesssim 2^\ell + (1-2\tau)^{-2^{n/\ell}}$. Take $\ell = \frac{n}{\ln\left(\frac{n}{\tau^2 \ln n}\right)}$ $(\tau = O(1))$

$$\Rightarrow \boxed{2^{O\left(\frac{n}{\ln(n/\tau)}\right)}}$$

■