Rough

$\Pr\left(X\cdot Y_m = 0 \,\middle|\, X\cdot Y_1 = a_1 \ldots X\cdot Y_{m-1} = a_{m-1},\ X\cdot e_2 = x_2, \ldots, X\cdot e_p = x_p\right)$

$X \sim U_n$

$m-1+p$ lin eq

$2^{n-(m-1+p)}$ dimensional subspace of $\{0,1\}^n$

solns to a system of linear eq^ns = $n-m$ where n is the # of variables & m is the # of constraints. Now each $(n-m)$ soln is linearly independent which means that if each variable can take K values, then the # elements (dimension of the space?) = K^{n-m}

4.2.2 (i guess)
7:39

$\frac{1}{\sqrt{2^l}} \otimes \rho_{YE}$

2^m

4.2.2 conflicting not^n for m

K entropy

d larger the seed? (a) X

$(1-p)n \gg m$

Rough for §4.3, problems.

(2) $\Pr(X=x_0)=1$, $\Pr(X\neq x_0)=0$

$\sum_x \left(\Pr(X=x)\right)^2 = 1$

$\begin{pmatrix}1&0\\0&0\end{pmatrix} - \begin{pmatrix}\frac12&\frac12\\\frac12&\frac12\end{pmatrix}$

$\begin{pmatrix}\frac12&-\frac12\\-\frac12&-\frac12\end{pmatrix} - \frac{1}{\sqrt2}$

$\Pr(X=x_0) = 2^{-n}$

$\sum_{x'=1}^{2^n} \left|\Pr(X=x')\right|^2 = 2^{-2n}\sum_{x'=1}^{2^n} 1 = 2^{-2n}\cdot 2^n = 2^{-n}$

0°

$\left(\frac{\sqrt3}{2}\right)^2 = \frac{3}{4}$

$\frac{1}{4}$ $\frac{1}{4}$

P guess

$\rho_0 = |0\rangle\langle 0|$

$\rho_1 = |+\rangle\langle +|$

$\rho = \frac12 \rho_0 + \frac12 \rho_1$

$M_0 = |0\rangle\langle 0|$

$M_1 = |1\rangle\langle 1|$

$P_{guess} = M_0 \frac12 \rho_0 + M_1 \frac12 \rho_1$

$= \frac12 |0\rangle\langle 0| + \frac12 |0\rangle\langle 0| \left(\frac{|0\rangle+|1\rangle}{\sqrt2}\right)\otimes\left(\frac{\langle 0|+\langle 1|}{\sqrt2}\right)$

$\frac12 + \frac{\sqrt2}{4} = 0.853$

$\frac{\sqrt2}{2} = 0.707\ldots$

$\frac12\cdot\frac12\,\frac{|0\rangle}{\cancel{\sqrt2}}\otimes\frac{\langle 0| + \cancel{\langle 1|}}{\cancel{\sqrt2}}$

$\frac12\cdot 1 + \frac12\cdot\frac12 = \frac12 + \frac14$

$= \frac34$

$= \frac12 + \frac14 = \frac24 + \frac14 = \frac34$

$\frac12 + \frac12\left(\frac{1}{\sqrt2}\right)$

$\left(|0\rangle\langle 0| - |+\rangle\langle +|\right) =$

$\frac12 + \frac{\sqrt2}{4\sqrt2\cdot\sqrt2} = \frac12 + \frac{\sqrt2}{4\cdot 2}$

$\frac12 |0\rangle\langle 0|$

$\frac12\left(1+\frac{1}{2\sqrt2}\right)$

$\frac12 + \frac12 \|\rho_0 - \rho_1\|_1$

$\frac12 + \frac{1}{4\sqrt2}$

$\begin{pmatrix}\frac12-\frac14 & -\frac14\\ -\frac14 & -\frac14\end{pmatrix} = \begin{pmatrix}\frac14 & -\frac14\\ -\frac14 & -\frac14\end{pmatrix}$

$\underbrace{\frac12 |0\rangle\langle 0|}_{=\begin{pmatrix}\frac12 & 0\\ 0 & 0\end{pmatrix}}$ $\underbrace{\frac12 |+\rangle\langle +|}_{}$ $-\frac14\begin{pmatrix}1&1\\1&1\end{pmatrix}$

$\frac{1}{2\sqrt2}$

$\lambda_1 = \frac{-1}{2\sqrt{2}}$, $\lambda_2 = \frac{1}{2\sqrt{2}}$ $v_- = (1+\sqrt{2}, 1)$ $v_+ = (1-\sqrt{2}, 1)$

$\pi_0 = v_+$
$\pi_- = v_-$

$\Pr_{f \in \mathcal{F}} [f(x) = z \;\&\; f(x') = z'] = \frac{1}{2^{2n}}$

$\Pr [Z(x, y) = z \;\&\; Z(x', y) = z'] = \frac{1}{2^{2n}}$

$\Updownarrow ?$

$\Pr(y; z) = \frac{1}{2^{2n}}$

dependent

random var.

independent

indepen

$Z(X, Y)$

$\Pr[Z(X = x, Y) = z]$

X

$\Pr[f(x) = z] = \frac{1}{2^m}$

$\Pr(f(X) = z)$

$\Pr(X = x) =$ distr.