Program 7.6: Correcting Low-Degree Polynomial

input $\mathbf{x} \in F^k$;
oracle Function g which is δ-close to $f \in F_{d,k}$ and line-table T;
output $f(\mathbf{x})$;
begin
  Randomly choose in $\mathbf{s} \in F^k$;
  Randomly choose $t \in F$;
  if $P_{\mathbf{x},\mathbf{s}}(t) \neq g(\mathbf{x}+\mathbf{s}t)$ **then**
    return NO
  else
    return $P_{\mathbf{x},\mathbf{s}}(0)$
end.

line-table T*, returns the value* $f(\mathbf{x})$ *with probability at least* $1-2\sqrt{\delta}-d/q$ *(no matter what the line-table contains).*

PROOF For any line l in $L_{\mathbf{x}}$, recall that P_l^f denotes the univariate polynomial of degree d that best describes f on l. The only case in which Program 7.6 returns a wrong value occurs when the polynomial $P_{\mathbf{x},\mathbf{s}}$ in T corresponding to the randomly chosen line $l = l_{\mathbf{x},\mathbf{s}}$ is different from P_l^f. We now show that, in this case, $P_{\mathbf{x},\mathbf{s}}$ does not agree with g at most elements of l. Hence, Program 7.6 returns NO with high probability.

To prove that $P_{\mathbf{x},\mathbf{s}}$ does not agree with g at most elements of l, we use the fact that, for at least $(1-\sqrt{\delta})q^k$ lines in $L_{\mathbf{x}}$, P_l^f agrees with g at $(1-\sqrt{\delta})q$ elements of l (see Exercise 7.5). Let L_{good} be the set of such lines and let $l \in L_{\text{good}}$. Since two distinct polynomials in $F_{d,1}$ agree at no more than d points in F, then every polynomial in $F_{d,1}$ distinct from P_l^f agrees with g at no more than $d+(1-(1-\sqrt{\delta}))q = d+\sqrt{\delta}q$ elements of l. In particular, this is true for $P_{\mathbf{x},\mathbf{s}}$ (see Fig. 7.4, where the gray region denotes elements of l at which P_l^f and g agree, the dotted region denotes elements of l at which P_l^f, $P_{\mathbf{x},\mathbf{s}}$, and g agree, and, finally, the white region denotes elements of l at which $P_{\mathbf{x},\mathbf{s}}$ and g agree).

Hence, the probability that Program 7.6 returns a wrong value is bounded by the probability that $l_{\mathbf{x},\mathbf{s}}$ does not belong to L_{good} plus the probability that t is an element at which $P_{\mathbf{x},\mathbf{s}}$ and g agree. This probability is at most

$$1-(1-\sqrt{\delta})+\sqrt{\delta}+d/q = 2\sqrt{\delta}+d/q$$

QED and the theorem is proved.

As in the case of linear functions, the bound on the error probability stated by the above theorem is larger than the bound immediately implied by the