Sub-linear time algebraic algorithms

Madhu Sudan
Scribe: Agnieszka Kozubek

October 6, 2007

1 Linearity testing

Let $\mathcal{F}_{hom}$ be the space of all homomorhisms $\mathbb{F}_2^n \to \mathbb{F}_2$.

Theorem 1. *Let us assume that $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is such that*

$$\Pr_{x,y}[f(x) + f(y) = f(x+y)] = \delta_0.$$

Then $\delta(f, \mathcal{F}_{hom}) \le \delta_0$.

Proof. We may identify $\mathbb{F}_2$ with $\{-1, +1\}$. From now on we will think of f as $f : \mathbb{F}_2^n \to \{-1, +1\}$. Then

$$\begin{aligned} \Pr_{x,y}[f(x) \cdot f(y) = f(x+y)] = \\ &= \Pr_{x,y}[f(x) \cdot f(y) \cdot f(x+y) = 1] = \\ &= \frac{1 + \mathop{E}_{x,y}[f(x) \cdot f(y) \cdot f(x+y)]}{2}. \end{aligned}$$

Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_2^n$ and let $L_\alpha : \mathbb{F}_2^n \to \{-1, 1\}$ be defined as

$$L_\alpha(x_1, \ldots, x_n) = (-1)^{\langle \alpha, x \rangle},$$

where $\langle \alpha, x \rangle = \Sigma_{i=1}^n \alpha_i x_i$ (in $\mathbb{F}_2$).

The functions L_α are all possible homomorphisms. Moreover, they form an orthonormal basis of functions from $\mathbb{F}_2^n \to \mathbb{R}$. Hence $\delta(f, \mathcal{F}_{hom}) = \min_\alpha \{\delta(f, L_\alpha)\}$.

Let $\langle f, g \rangle \triangleq \mathop{E}_{x \in \mathbb{F}_2^n}[f(x)g(x)]$, where $f, g : \mathbb{F}_2^n \to \mathbb{R}$. It is easy to note the following:

- If $f, g : \mathbb{F}_2^n \to \{-1, 1\}$, then $\langle f, g \rangle = 1 - 2\delta(f, g)$.
- $\langle L_\alpha, L_\alpha \rangle = 1$
- $\langle L_\alpha, L_\beta \rangle = 0$, if $\alpha \ne \beta$

- If $\alpha = 0$, then $L_\alpha(x) = 1$ for all x.
  If $\alpha \neq 0$, then $\underset{x}{Pr}[L_\alpha(x) = 1] = \frac{1}{2}$.
- $L_\alpha(x + y) = L_\alpha(x)L_\alpha(y)$
- $L_{\alpha+\beta}(x) = L_\alpha(x)L_\alpha(y)$

Let us define $\hat{f}_\alpha \triangleq \langle f, L_\alpha \rangle$.

Proposition 1. *Let $f : \mathbb{F}_2^n \to \mathbb{R}$. $f(x) = \Sigma \hat{f}_\alpha \cdot L_\alpha(x)$*

We will now consider the expression:

$$\underset{x,y}{E}[f(x) \cdot f(y) \cdot f(x + y)] =?$$

Two things to consider:

1. How does this look like for the basis functions?
2. Extend to all functions using Fourier coefficients.

First note that

- $\underset{x,y}{E}[L_\alpha(x)L_\alpha(y)L_\alpha(x + y)] = 1$
- $\underset{x,y}{E}[L_\alpha(x)L_\alpha(y)L_\beta(x + y)] = \underset{x,y}{E}[L_\alpha(x)L_\beta(x)L_\alpha(y)L_\beta(y)] = \underset{x,y}{E}[L_\alpha(x)L_\beta(x)]\underset{x,y}{E}[L_\alpha(y)L_\beta(y)] = 0$, where $\alpha \neq \beta$.
- Similarly we may show that if $\alpha \neq \beta \neq \gamma \neq \alpha$ then $\underset{x,y}{E}[L_\alpha(x)L_\beta(y)L_\gamma(x + y)] = 0$

Hence

$$\begin{aligned}
\underset{x,y}{E}[f(x)f(y)f(x + y)] = \\
&= \underset{x,y}{E}[\Sigma_\alpha \hat{f}_\alpha L_\alpha(x) \Sigma_\beta \hat{f}_\beta L_\beta(y) \Sigma_\gamma \hat{f}_\gamma L_\gamma(x + y)] \\
&= \Sigma_{\alpha,\beta,\gamma} \hat{f}_\alpha \hat{f}_\beta \hat{f}_\gamma \underset{x,y}{E}[L_\alpha(x)L_\beta(y)L_\gamma(x + y)] \\
&= \Sigma_\alpha \hat{f}_\alpha^3
\end{aligned}$$

Proposition 2. *Let $f : \mathbb{F}_2^n \to \mathbb{R}$. Then $\Sigma_\alpha \hat{f}_\alpha^2 = \langle f, f \rangle$.*

Proof. Verify using the definitions.

$$\begin{aligned}
\langle f, f \rangle &= \langle \Sigma_\alpha \hat{f}_\alpha L_\alpha(x), \Sigma_\beta \hat{f}_\beta L_\beta(x) \rangle \\
&= \Sigma_{\alpha,\beta} \hat{f}_\alpha \hat{f}_\beta \langle L_\alpha(x), L_\beta(x) \rangle \\
&= \Sigma_\alpha \hat{f}_\alpha^2
\end{aligned}$$

$\square$

Therefore, if $f : \mathbb{F}_2^n \to \{-1, +1\}$ then $\langle f, f \rangle = 1$.

Proposition 3. $\Sigma \hat{f}_\alpha^3 \leq \max_\alpha \{\hat{f}_\alpha\}$

Proof.

$$\begin{aligned}\Sigma_\alpha \hat{f}_\alpha^3 &\leq \Sigma_\alpha (\max_\beta \{\hat{f}_\beta\}) \cdot \hat{f}_\alpha^2 \\ &\leq \max_\beta \{\hat{f}_\beta\} \cdot \Sigma_\alpha \hat{f}_\alpha^2 \\ &= \max_\beta \{\hat{f}_\beta\}\end{aligned}$$

□

We have proved that

$$\text{if } Pr[\text{test rejects}] = \delta_0 \text{ then } E[f(x)f(y)f(x+y)] = 1 - 2\delta_0.$$

We also proved that

$$E[f(x)f(y)f(x+y)] \leq \max_\beta \{\hat{f}_\beta\}.$$

But $\max_\beta \{\hat{f}_\beta\} = 1 - 2\delta(f, \mathcal{F}_{hom})$ and hence $\delta(f, \mathcal{F}_{hom}) \leq \delta_0$.

□

2 Dictator testing

Definition 1. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$. The function f is a* Dictatorship *if there exists i such that $f(x_1, \ldots, x_n) = x_i$.*

We are interested in testing this property.

Definition 2. *The function f is k-*Non-Dictatorship *if f depends on more than k variables.*

Dictator Testing:

1. If f is a Dictatorship then accept with probability $\to 1$
2. If f is far from every function that depends on less than k variables then accept with probability $\to \frac{1}{2}$.