Linear Consistency Testing

MADHU SUDAN

Laboratory for Computer Science

Massachusetts Institute of Technology

CAMBRIDGE, MA

Joint work with:

- Yonatan Aumann (Bar-Ilan U.)
- Johan Håstad(Royal Inst. of Tech.)
- Michael O. Rabin (Hebrew U. & Harvard U.)

Linearity and Consistency

G, H finite abelian groups.

Defn: Function $f : G \longrightarrow H$ is linear if

$$\forall x, y \in G, \quad f(x) + f(y) = f(x + y)$$

(Also called homomorphism.)

Defn: $f_1, f_2, f_3 : G \longrightarrow H$ linear-consistent if

$$\forall x, y \in G, \quad f_1(x) + f_2(y) = f_3(x + y)$$

Linear-Consistency ?

Informally: f_1, f_2, f_3 are all offsets of the same linear function.

Formally:

Proposition: f_1, f_2, f_3 are linear-consistent iff $\exists$ linear function $\phi : G \longrightarrow H$ and $a_1, a_2 \in H$ s.t.

$$f_1(x) = \phi(x) + a_1$$

$$f_2(x) = \phi(x) + a_2$$

$$f_3(x) = \phi(x) + a_1 + a_2$$

Linearity testing [BLR '90]

- Pick $x, y \in G$ at random and accept if

$$f(x) + f(y) = f(x + y)$$

- Linear functions accepted w.p. 1.

- Functions "close" to linear accepted w.h.p.

  Defn: f ϵ-close to g if

$$\Pr_{x \in G}[f(x) \neq g(x)] \leq \epsilon.$$

- Hope ... functions that are not close to linear are rejected w.h.p.

Linearity testing (contd.)

Thm: [BLR '90] If probability of rejection (δ) is small ($< 2/9$) then f is (δ-)close to linear.

Applications:

- Program Checking [BLR '90].
- Prob. Checkable Proofs [ALMSS '92, ...].

Thm: [BCHKS '95] $G = Z_2^n, H = Z_2$.
If probability of rejection is δ
Then f is δ-close to linear.

- Applications to PCP [BGS '95].

Linear-consistency testing

- Pick $x, y \in G$ at random and accept if

$$f_1(x) + f_2(y) = f_3(x + y)$$

- Linear-consistent triples accepted w.p. 1.
- Triples "close" to linear-consistent accepted w.h.p.
- f_1, f_2, f_3 linear but inconsistent implies rejected w.h.p.
- Hope ... if f_1, f_2, f_3 not close to any linear-consistent triple g_1, g_2, g_3 then test rejects w.h.p.

Linear-consistency testing

Thm: If probability of rejection (δ) is small ($< 2/9$) then f_1, f_2, f_3 are (δ-)close to linear-consistent triple g_1, g_2, g_3.

[BLR '90] result spl. case with $f_1 = f_2 = f_3$.

Thm: $G = Z_2^n, H = Z_2$.
If probability of rejection is $\delta = \frac{1}{2} - \gamma$, $\gamma > 0$. Then f_1, f_2, f_3 are $\frac{1}{2} - \frac{2}{3}\gamma$-close to linear-consistent triple.

- Non-trivial rejection rate implies non-trivial proximity.
- Application to Multiple-Prover Interactive Proofs (MIP).

Motivation:MIP vs. PCP

Defn: (r, q)-restricted PCP verifier V on input $x \in \{0,1\}^n$ tosses $r(n)$ coins and makes $q(n)$ Boolean queries to an oracle and then outputs accept/reject based on $x, \$$ and responses to queries.

Defn: $L \in \mathrm{PCP}_{c,s}[r, q]$ if there exists a (r, q)-restricted PCP verifier V satisfying:
Completeness:
$x \in L \;\Rightarrow\; \exists$ oracle s.t. V accepts w.p. $\geq c$.
Soundness:
$x \notin L \;\Rightarrow\; \forall$ oracles V accepts w.p. $\leq s$.

MIP vs. PCP (contd.)

Defn: (r,p)-restricted MIP verifier V on input $x \in \{0,1\}^n$ tosses $r(n)$ coins and makes one Boolean query each to $p(n)$ non-interacting provers and then outputs accept/reject based on $x, \$$ and responses to queries.

Defn: $L \in \text{MIP}_{c,s}[r,p]$ if there exists a (r,p)-restricted MIP verifier V satisfying:

Completeness:

$x \in L \;\Rightarrow\; \exists$ provers s.t. V accepts w.p. $\geq c$.

Soundness:

$x \notin L \;\Rightarrow\; \forall$ provers V accepts w.p. $\leq s$.

MIP vs. PCP (contd.)

- Obvious: $\mathrm{MIP}_{c,s}[r,p] \subseteq \mathrm{PCP}_{c,s}[r,p]$.
- Other direction? Containment not obvious!
- Example: PCP $\longrightarrow$ Optimization
  - 2 query PCP $\longrightarrow$ Quadratic objective.
  - 2 prover MIP $\longrightarrow$ Bilinear objective.
  - q query PCP $\longrightarrow$ Degree q objective.
  - q query MIP $\longrightarrow$ Multilinear objective.
- Extremal example: MAX CUT on general vs. bipartite graphs!

MIP vs. PCP (contd.)

Thm:[Håstad'97]

$$\forall \epsilon > 0, \mathrm{NP} = \mathrm{PCP}_{1-\epsilon,\frac{1}{2}}[\log, 3].$$

Thm:[Here] $\forall \epsilon > 0, \mathrm{NP} = \mathrm{MIP}_{1-\epsilon,\frac{1}{2}}[\log, 3]$.

- Characterization tight (also in [Håstad'97]).
- Role of linear-consistency:
  - In PCP characterization, single oracle f is tested for linearity.
  - In MIP characterization, the three provers f_1, f_2, f_3 are tested for linear-consistency.

Analysis of Linear-consistency testing

- General case similar to [BLR '90].
- Z_2 case similar to [BCHKS '95].

Highlights of Z_2 case

Defn: Bias(f_1, f_2, f_3)

$$= \Pr[\text{Test accepts}] - \Pr[\text{Test rejects}]$$

Case of interest: Bias is positive but small.

Fourier analysis

For $\alpha \subseteq \{1, \ldots, n\}$, let

$$l_\alpha(x) = \sum_{i \in \alpha} x_i (\mathrm{mod} 2).$$

Let α-th Fourier coefficient of f be the "correlation" between f and the linear function i.e.,

$$\hat{f}_\alpha = \Pr_x[f(x) = l_\alpha(x)] - \Pr_x[f(x) \neq l_\alpha(x)].$$

Goal: Bias non-neg. $\Rightarrow$ some Fourier coeff. large.

Fourier analysis (contd.)

Amazing power of Fourier analysis yields:

Bias(f_1, f_2, f_3)

$$= \sum_{\alpha,\beta,\gamma} \hat{f}_{1,\alpha}\hat{f}_{2,\beta}\hat{f}_{3,\gamma}\,\text{Bias}(l_\alpha, l_\beta, l_\gamma)$$

$$= \sum_{\alpha} \hat{f}_{1,\alpha}\hat{f}_{2,\alpha}\hat{f}_{3,\alpha}$$

Eventually (Parseval's + Cauchy-Schwartz etc.)

$$\text{Bias} \le \max_\alpha\{|\hat{f}_{1,\alpha}|\}$$

$$\text{Bias} \le \max_\alpha\left\{\min_{i\in\{1,2,3\}}\left\{\left|\frac{3}{2}\hat{f}_{i,\alpha}\right|\right\}\right\}$$

Conclusions

- Linear consistency testing: Old problem; new abstraction.
- More applications?
- Tight analysis for Z_2 case.