The Goldreich-Levin Algorithm with Reduced Complexity

Ameriah Salem Abdouli, Khalifa University of Science,
Technology and Research,Abu Dhabi, UAE;
Ilya Dumer, UC Riverside,USA;
Grigory Kabatiansky, KUSTAR, UAE
on leave from IITP RAS, Russia;
Cedric Tavernier, tavernier.cedric@gmail.com

June 18, 2012

Problem. *For a given boolean function* $g(x_1, \ldots, x_m)$ *find all enough good linear approximations*
$L_{g,\varepsilon} = \{a(x) = a_1x_1 + \ldots + a_mx_m : \ d(g, a) \leq 2^m(1/2 - \varepsilon)\}$
The deterministic, error-free, Green algorithm (=FFT) performs complete maximum likelihood decoding with complexity $n \ln^2 n$, where $n = 2^m$.
The celebrated Goldreich-Levin algorithm performs randomized list decoding achieves a low decoding error probability of 2^{-s} with a polylogarithmic complexity sm/ϵ^4.
We combine the two algorithms and reduce the complexity of the Goldreich-Levin algorithm to the order of sm/ϵ^2.

We independently and uniformly pick up l vectors $U = \left\{u_{(1)}, ..., u_{(l)}\right\}$ from $\mathbb{F}_2^m$ and consider the linear subspace

$$\mathbb{U} = \left\{ \sum_{i=1}^{l} y_{(i)} u_i \mid y_i = 0, 1 \right\}. \qquad (1)$$

Consider restrictions of all linear function $a(x)$ on $\mathbb{U}$ in the form $a(x) = a(x)_{|\mathbb{U}} = \sum_{i=1}^{l} h_i y_i$, where $x = \sum_{i=1}^{l} y_i u_{(i)}$. To find $a(x)$ is the same as to find $a(e_i)$. Note that

$$a(e_i) = a(u) + a(u + e_i), \quad u \in \mathbb{U}, \quad i = 1, ..., m. \qquad (2)$$

Here the unknown outputs $a(u + e_i)$ will be replaced by the corresponding channel outputs $g(u + e_i)$. The algorithm GL then estimates each $a(e_i)$ taking the 2^l-majority vote

$$\tilde{a}(e_i) = \mathrm{Maj}_{u \in \mathbb{U}} \left\{ a(u) + g(u + e_i) \right\}, \quad i = 1, ..., m. \qquad (3)$$

Improved GL algorithm uses many mutually independent estimates of $a(e_i)$. We first replace the unit vector e_i in equalities (2) and (3) with any point z.
A function $a(x)$ can be estimated at any point z as

$$\tilde{a}(z) = \mathrm{Maj}_{u \in \mathbb{U}} \left\{ a(u) + g(u + z) \right\}. \tag{4}$$

Similarly, we evaluate the same function $a(x)$ at the point $z + e_i$,

$$\tilde{a}(z + e_i) = \mathrm{Maj}_{u \in \mathbb{U}} \left\{ a(u) + g(u + z + e_i) \right\} \tag{5}$$

Now estimate the coefficient $a(e_i)$ as a function of the point $z = z_{(j)}$ as follows

$$\tilde{a}_j(e_i) = \tilde{a}(z_j) + \tilde{a}(z_j + e_i) \tag{6}$$

Finally, we take k random points $z_{(j)}$ in such a way that they belongs to different cosets of $\mathbb{U}$. Then

$$\tilde{a}(e_i) = \mathrm{Maj}_{j=1,\dots,k}\,\{\tilde{a}_j(e_i)\}, \tag{7}$$

where estimates $\tilde{a}_j(e_i)$ are mutually independent r.v. and one can apply corresponding EXP inequalities, e.g., Hoeffding.

Our improvement is based on the following observation. Consider the majority voting performed on the vector $g(u + z_j)$ in (4). Given any $z = z_{(j)}$, we choose in favor of some constant $\tilde{a}(z)$ in (4) instead of $\tilde{a}(z) + 1$ if the corresponding affine function $a(x) + \tilde{a}(z)$ is closer to $g(u + z)$ than the opposite function. Thus, the estimates $\tilde{a}_b(y)$ can be derived simultaneously for different $b \in \mathbb{F}_2^l$, by decoding vector $g(u + z)$ into the list of $L = 2^l$ closest affine functions. It reduces complexity from $1/\varepsilon^4$ to from $1/\varepsilon^2$.

1. O. Goldreich and L. A. Levin, A hard-core predicate for all one-way functions ,in 21 st ACM Symp. Theory of Computing, Seattle, WA, USA, May 14 - 17, pp. 25–32,1989.
2. L. A. Levin, Randomness and Nondeterminism, J. Symb. Logic, vol. 58, pp. 1102-1103, 1993.
3. O. Goldreich, Foundations of Cryptography, vol. 1, Cambridge, New York, 2001.
4. L. Trevisan, Some applications of coding theory in computational complexity , Quaderni di matematica, vol. 13, pp. 347-424, 2004.

One problem on boolean fucntions

Let $F(x, y)$ be one-to-one function $\{0,1\}^{2n} \to \{0,1\}^{2n}$, which can be represented as

$$F(x, y) = f_1(x) + f_2(y),$$

where $f_1(x), f_2(x)$ be vectorial boolean functions $\{0,1\}^n \to \{0,1\}^{2n}$.

Conjecture There exists vector $a \in \{0,1\}^{2n}$ such that for f_1 or f_2 $(a, f(x)) = 0$ for all $x \in \{0,1\}^n$.

Thank you!