PROBABILISTIC SOLUTION OF YAO'S MILLIONAIRES' PROBLEM

MARIYA BESSONOV, DIMA GRIGORIEV, AND VLADIMIR SHPILRAIN

ABSTRACT. We offer a probabilistic solution of Yao's millionaires' problem that gives correct answer with probability (slightly) less than 1 but on the positive side, this solution does not use any one-way functions.

1. INTRODUCTION

The "two millionaires problem" introduced by Yao in [5] is:

> Alice has a private number a and Bob has a private number b, and the goal of the two parties is to solve the inequality $a \leq b$? without revealing the actual values of a or b, or more stringently, without revealing any information about a or b other than $a \leq b$ or $a > b$.

We note that all known solutions of this problem (including Yao's original solution) use one-way functions one way or another. Informally, a function is *one-way* if it is efficient to compute but computationally infeasible to invert on "most" inputs. One problem with those solutions is that it is not known whether one-way functions actually exist, i.e., the functions used in the aforementioned solutions are just *assumed* to be one-way. Also, solutions that use one-way functions inevitably use assumptions of limited computational power of the parties, and this assumption is arguably more "physical" than "mathematical" in nature, although there is a mathematical theory of computational complexity with a (somewhat arbitrary) focus on distinction between polynomial-time and non-polynomial-time complexity of algorithms.

Speaking of physics, in our earlier papers [4] and [3] we offered several solutions of Yao's millionaires' problem without using one-way functions, but using real-life procedures (not implementable on a Turing machine). What is important is that some of these solutions can be used to build a public-key encryption protocol secure against a computationally unbounded (passive) adversary, see [3].

Here we make an assumption that both private numbers a and b are uniformly distributed on integers in a public interval $[1, n]$. This assumption may be questionable as far as the millionaires' problem itself is concerned, but we keep in mind potential applications to cryptographic primitives, in which case the above assumption could be just fine. We also note that this assumption can be relaxed to a and b being identically (not necessarily uniformly) distributed on integers in

Research of the first author was partially supported by the NSF grant DMS-1515800.

Research of the third author was partially supported by the ONR (Office of Naval Research) grant N000141512164.

$[1,n]$ because in that case, a monotone function $\mathcal{F}$ can be applied to both a and b so that $\mathcal{F}(a)$ and $\mathcal{F}(b)$ become uniformly distributed (on a different interval though), see [2, Section 2.2.1]. This is called the *inverse transform method.*

We also note that our solution of the millionaires' problem has a "symmetric" as well as "asymmetric" version. In the "asymmetric" version, only one of the two parties ends up knowing whether $a < b$ or not, even if the other party is computationally unbounded. (Of course, she can then share this information with the other party if she chooses to.) This implies that a third party (a passive observer) will not know whether $a < b$ either, and this is the key property for building a public-key encryption protocol secure against a computationally unbounded (passive) adversary, see [3] for details.

The way our solution in this paper works is roughly as follows. Alice applies a randomized function F to her private number a and obtains the result $A = F(a)$ that she either keeps private ("asymmetric" version) or makes public ("symmetric" version). Bob applies a randomized function G to his private number b and obtains the result $B = G(b)$ that he makes public. Then Alice, based on a,A and B, makes a judgement whether $a < b$ or not. Specifically, in our protocol in Section 2, she concludes that $a < b$ if and only if $A < B$. We show in Section 3 that, with appropriate choice of parameters, this judgement is correct with probability converging to 1 as n (the interval length) goes to infinity. Computer simulations suggest (see Section 4) that this convergence is actually rather fast.

2. Protocol

Recall that in a *simple symmetric random walk*, a point on a horizontal line moves one unit left with probability $\frac{1}{2}$ or one unit right with probability $\frac{1}{2}$. Below is our protocol for a probabilistic solution of Yao's millionaires' problem, under the assumption that both private numbers a and b are uniformly distributed on integers in a public interval $[1,n]$.

1. Alice's private number a is the starting point of her random walk. Alice does a simple symmetric random walk with $f(n)$ steps, starting at a. Let A be the end point of Alice's random walk. Alice either keeps A private ("asymmetric" version) or makes it public ("symmetric" version).
2. Bob's private number b is the starting point of his random walk. Bob does a simple symmetric random walk with $g(n)$ steps, starting at b. Let B be the end point of Bob's random walk. Bob makes B public.
3. Alice concludes that $a < b$ if and only if $A < B$.
4. In case Alice has published her A ("symmetric" version), Bob, too, concludes that $a < b$ if and only if $A < B$.

We emphasize that in the "asymmetric" version, only Alice ends up knowing (with significant probability) whether or not $a < b$. Neither Bob nor a third party observer end up knowing this information unless Alice chooses to share it.

In this paper, we focus on the arrangement where $f(n) = g(n)$, i.e., the parties do the same number of steps. Other arrangements are possible, too; in particular, as we remark in Section 3.1, Alice can (slightly) improve the probability of coming to the correct conclusion on $a < b$? if she does not walk at all, i.e., if $f(n) = 0$. This arrangement is "highly asymmetric" but it is useful to keep in mind for future work.

3. PROBABILITIES

We start with the following

Remark 1. *If a and b are independent random variables and each is uniformly distributed on $\{1,2,\dots,n\}$, then the expected value of $|a-b|$ is $E(|a-b|) = \frac{(n^2-1)}{3n}$, which is asymptotically equal to $\frac{n}{3}$.*

Indeed, note that $|a-b| = \max(a,b) - \min(a,b)$. By symmetry,

$$E(\max(a,b)) = n+1-E(\min(a,b)),$$

hence

$$E(|a-b|) = n+1-2E(\min(a,b)).$$

Now direct computation gives

$$E(\min(a,b)) = \sum_{k=1}^{n} k\cdot(\frac{2}{n}\cdot\frac{n-k}{n}+\frac{1}{n^2}) = n+1+\frac{(n+1)(1-4n)}{6n}.$$

Then

$$E(|a-b|) = n+1-2E(\min(a,b)) = \frac{(n^2-1)}{3n}.$$

Remark 2. *If t is a positive integer and a and b are independent and uniformly distributed on $\{1,2,\dots,n\}$, then $P(|a-b|<t) < 2t/n$.*

To see this,

$$\begin{aligned}
P(|a-b|<t) &= \sum_{j=1}^{n} P(\{|a-b|<t\}\cap\{a=j\}) \\
&< \sum_{j=1}^{n} P(b\in\{j-(t-1), j-t+2,\dots,j+t-1\}\cap a=j) \\
&= \sum_{j=1}^{n} P(b\in\{j-t+1, j-t+2,\dots,j+t-1\})P(a=j) \\
&= \frac{2t}{n}\cdot\frac{1}{n}\cdot n = \frac{2t}{n}
\end{aligned}$$

Thus, a and b are likely to be sufficiently far apart, which explains why the probability that our solution is correct is sufficiently high.

Recall that the probability of our solution being correct is the conditional probability $P(a<b \mid A<B)$. It depends on the functions $f(n)$ and $g(n)$, and we consider a couple of cases here, focusing on the case where $f(n) = g(n)$. First we recall

Theorem 1 (see [1, Theorem 2.2 and Remark 2.6])**.** *Let S_m be the location of the simple symmetric random walk on $\mathbb{Z}$ after m steps with $S_0 = 0$. Let $1/2 < \alpha < 1$. Then*

$$\lim_{m\to\infty} m^{1-2\alpha} \log P\left(S_m > xm^{\alpha}\right) = -\frac{x^2}{2} \tag{1}$$

That is, for large enough m,

$$P\left(S_m > xm^{\alpha}\right) \approx e^{-\frac{x^2 m^{2\alpha-1}}{2}} \to 0 \text{ as } m \to \infty,$$

for $x = 1$,

$$P\left(S_m > m^{\alpha}\right) \approx e^{-\frac{m^{2\alpha-1}}{2}} \to 0 \text{ as } m \to \infty,$$

so the probability that the displacement from the starting point is greater than $O(\sqrt{m})$ tends to 0.

If $g(n) = O(n^{2-2\varepsilon})$, n is fixed, and $\varepsilon \to 0$, then $P(a < b|A < B)$ will not be close to 1 since the typical displacement is $O(n^{1-\varepsilon})$. This probability $P(a < b|A < B)$ will tend to 1 for any fixed $\varepsilon > 0$ and $n \to \infty$.

For m fixed and $\alpha \in [1/2, 1]$, one has

$$\begin{aligned} P(S_m \geq m^{\alpha}) &= P\left(e^{S_m m^{\alpha-1}} \geq e^{m^{2\alpha-1}}\right) \\ &\leq \exp\left(-m^{2\alpha-1}\right) E\left(\exp\left(S_m m^{\alpha-1}\right)\right) \\ &= \exp\left(-m^{2\alpha-1}\right)\left(E\left(e^{\left(X m^{\alpha-1}\right)}\right)\right)^m \\ &= \exp\left(-m^{2\alpha-1} + m \ln\left(\cosh(m^{\alpha-1})\right)\right) \leq \exp\left(-\frac{m^{2\alpha-1}}{2}\right), \end{aligned}$$

where X is a random variable taking on 1 and -1 with equal probability (the step distribution of the simple symmetric random walk). The first inequality is an application of Markov's inequality and the last inequality holds because $\ln\cosh(x) \leq \frac{x^2}{2}$ for all $x \in \mathbb{R}$.

It will follow that if there are $m = n^{\lambda}$ steps in Alice's and in Bob's random walks, then for any

$$\alpha \in (1/2, \min\{1, \ln(n/2)/\lambda \ln(n)\}),$$

one has

$$\begin{aligned} &P(a < b|A < B) \\ &\geq \left(1 - \exp\left(-\frac{m^{2\alpha-1}}{2}\right)\right)^2 \left(\frac{(n-2m^{\alpha}+1)(n-2m^{\alpha})}{n^2-n}\right)\left(1-\frac{1}{n}\right), \end{aligned} \tag{2}$$

which approaches 1 in the limit as $n \to \infty$.

To see why (2) is true, consider

$$P(a < b|A < B) = \frac{P\left(\{a < b\} \cap \{A < B\}\right)}{P(A < B)} = \frac{P(A < B|a < b)P(a < b)}{P(A < B)}. \tag{3}$$

The denominator of (3), $P(A < B) < 1/2$. Indeed, given that Alice's and Bob's random walks have the same number of steps and are denoted A_k and B_k, the difference between their random walks $Y_k = B_k - A_k$ for $k = 0, 1, \ldots, m$ is a lazy symmetric random walk with probability $1/2$ of staying in place and probabilities $1/4$ each of moving two steps to the left or to the right. Since the random walks are symmetric and the starting points a and b are selected uniformly and independently of each other on the same interval, by symmetry,

$$P(A<B)=P(Y_m>0)=P(Y_m<0)=P(A>B),$$

and $P(A=B)=P(Y_m=0)=O(1/\sqrt{m})$.

Then, $P(a<b)=\frac{n^2-n}{2n^2}$ since a and b are chosen independently and uniformly at random on $\{1,2,\ldots,n\}$. There are n^2 different ordered pairs (a,b), n of which have $a=b$, and half of the remaining n^2-n ordered pairs have $a<b$.

For the other term in the numerator of (3), let E be the event that $b-a\geq 2m^{\alpha}$ and assume α is such that $2m^{\alpha}$ is an integer. Then

(4)
$$\begin{aligned}P(A<B|a<b)&\geq P(\{A<B\}\cap E|a<b)\\&=P\left(A<B|\{b-a\geq 2m^{\alpha}\}\cap\{a<b\}\right)\cdot P\left(b-a\geq 2m^{\alpha}|a<b\right)\\&=P\left(A<B|b-a\geq 2m^{\alpha}\right)\cdot P\left(b-a\geq 2m^{\alpha}|a<b\right).\end{aligned}$$

For the second term in (4), recall that there are $\frac{n^2-n}{2}$ ordered pairs (a,b) with $a<b$, each ordered pair equally likely. Thus, we have

$$\begin{aligned}P\left(b-a\geq 2m^{\alpha}|a<b\right)&=\sum_{j=2m^{\alpha}}^{n-1}P\left(b-a=j|a<b\right)\\&=\frac{(n-2m^{\alpha})+(n-2m^{\alpha}-1)+\ldots+1}{\frac{n^2-n}{2}}\\&=\frac{2\cdot\frac{(n-2m^{\alpha}+1)(n-2m^{\alpha})}{2}}{n^2-n}\\&=\frac{(n-2m^{\alpha}+1)(n-2m^{\alpha})}{n^2-n}.\end{aligned}$$

If $m=n^{\beta}$, this expression is greater than 0 when $\alpha<\frac{\ln(n/2)}{\lambda\ln n}$.

Let F_{α} be the event that each of Alice's and Bob's random walks traveled distance no more than m^{α}. Each random walk has probability less than $e^{-m^{2\alpha-1}/2}$ of traveling more than m^{α} from its starting point. Thus, since the distance traveled of each walk is independent of the starting points and since the random walks are independent of each other,

$$\begin{aligned}P\left(A<B|b-a\geq 2m^{\alpha}\right)&\geq P(F_{\alpha}|b-a\geq 2m^{\alpha})=P(F_{\alpha})\\&\geq\left(1-\exp\left(-\frac{m^{2\alpha-1}}{2}\right)\right)^2.\end{aligned}$$

Then (2) follows.

An improvement to the lower bound on $P(a<b|A<B)$ for smaller values of n can be obtained by improving the bound in (4)

(5) $$P(A<B|a<b)=P(\{A<B\}\cap E|a<b)+P(\{A<B\}\cap E^c|a<b)$$

For the second term on the right of (5),

(6)

$$
\begin{aligned}
P(\{A<B\}\cap E^c|a<b) &= P(A<B|0<b-a<2m^{\alpha})\cdot P(b-a<2m^{\alpha}|a<b)\\
&> (1/2)\cdot\left(1-\frac{(n-2m^{\alpha}+1)(n-2m^{\alpha})}{n^2-n}\right),
\end{aligned}
$$

where we use

$$P(A<B|0<b-a<2m^{\alpha}) = P(Y_m>0|0<Y_0<2m^{\alpha})>1/2,$$

since Y_k is a symmetric random walk. Then, combining (3), (4), (5), and (6),

$$
\begin{aligned}
&P(a<b|A<B)\\
&\geq \left(1-\exp\left(-\frac{m^{2\alpha-1}}{2}\right)\right)^2\left(\frac{(n-2m^{\alpha}+1)(n-2m^{\alpha})}{n^2-n}\right)\left(1-\frac{1}{n}\right) \qquad (7)\\
&+(1/2)\cdot\left(1-\frac{(n-2m^{\alpha}+1)(n-2m^{\alpha})}{n^2-n}\right)\left(1-\frac{1}{n}\right).
\end{aligned}
$$

3.1. **What if Alice does not walk?** If Alice does not walk and makes a judgement based on her point a and the terminal point B of Bob's walk, then the probability in question is $P(a<b|a<B)$. The (somewhat informal) argument below shows that this probability is, in fact, greater than $P(a<b|A<B)$, although computer simulation shows that the difference is rather small. Thus, for the purpose of solving the millionaires problem itself, it is preferable to use $f(n)=0$ and $g(n)=n^{\frac{4}{3}}$ for the number of steps in Alice's and Bob's random walk, respectively. However, if one has in mind a possible conversion of such a solution to an encryption scheme, then having $f(n)=0$ is not optimal from the security point of view. We leave this discussion to another paper though, while here we explain why $P(a<b|a<B)>P(a<b|A<B)$.

Note that if Alice does not walk, the difference between Bob's and Alice's position is a simple symmetric random walk, X_k, with probability 1/2 each of moving to the right or left 1 step.

On the other hand, if both walk, then the difference between Bob's and Alice's position is a lazy random walk, Y_k, with probability 1/2 of staying in place and 1/4 each of moving to the right or left 2 steps. Then

$$P(a<b|a<B)>P(a<b|A<B) \iff P(X_0>0|X_m>0)>P(Y_0>0|Y_m>0).$$

It is well known that the mean squared displacement is greater for the lazy walk. Specifically, in our situation,

$$E(X_m^2)=m,\;\; E(Y_m^2)=2m.$$

Based on this, we indeed have $P(X_0>0|X_m>0)>P(Y_0>0|Y_m>0)$, so

$$P(a<b|a<B)>P(a<b|A<B).$$

3.2. **The case of $n^{\frac{4}{3}}$ steps in random walks.** Using MAPLE, we found the maximum over $\alpha \in (1/2, \frac{\ln(n/2)}{\lambda \ln n})$ of (7) for several values of n, with $n^{4/3}$ steps in both Alice's and Bob's random walks (see Table 1). We emphasize that these are lower bounds; the actual speed of convergence to 1 appears to be faster. For example, computer simulations suggest that already for $n = 1000$, $P(a < b|A < B)$ is about 0.9. If $n = 2000$, then $P(a < b|A < B)$ is about 0.99.

n	$P(a<b\|A<B)$	α
10^3	≥ 0.586	≈ 0.574
10^4	≥ 0.743	≈ 0.574
10^5	≥ 0.859	≈ 0.568
10^6	≥ 0.927	≈ 0.563
10^7	≥ 0.963	≈ 0.557
10^8	≥ 0.982	≈ 0.553
10^9	≥ 0.991	≈ 0.549

TABLE 1. Case of $n^{4/3}$ steps

3.3. **The case of $n^{\frac{5}{3}}$ steps in random walks.** The maximum over $\alpha \in (1/2, \frac{\ln(n/2)}{\lambda \ln n})$ of (7) for several values of n in this case is given in Table 2. Again, the actual speed of convergence to 1 appears to be faster. Computer simulations suggest that for $n = 1000$, $P(a < b|A < B)$ is about 0.75 in this case.

n	$P(a<b\|A<B)$	α
10^3	≥ 0.453	≈ 0.500
10^4	≥ 0.466	≈ 0.517
10^5	≥ 0.514	≈ 0.526
10^6	≥ 0.586	≈ 0.529
10^7	≥ 0.667	≈ 0.530
10^8	≥ 0.743	≈ 0.530
10^9	≥ 0.807	≈ 0.529

TABLE 2. Case of $n^{5/3}$ steps

3.4. **The probability to guess the other party's number.** Another probability that we are interested in is the probability for Alice to correctly guess Bob's private number b based on the public B. The most likely position of the point b is $b = B$ (assuming that $g(n)$ is even), and the probability for that to actually happen is (using Stirling's formula) approximately $\sqrt{\frac{2}{\pi g(n)}}$. Thus, we have:

1. For $f(n) = g(n) = n$, Alice's best guess for b has probability about $\sqrt{\frac{2}{\pi n}}$ to be correct.

2. For $f(n) = g(n) = n^{\frac{4}{3}}$, Alice's best guess for b has probability about $\sqrt{\frac{2}{\pi n^{\frac{4}{3}}}} = \frac{\sqrt{2}}{n^{\frac{2}{3}}\sqrt{\pi}}$ to be correct.
3. For $f(n) = g(n) = n^{\frac{5}{3}}$, Alice's best guess for b has probability about $\sqrt{\frac{2}{\pi n^{\frac{5}{3}}}}$ to be correct.

These probabilities can be compared to the *a priori* probability for either party to guess the other party's number correctly (with or without knowing the probability distribution), which is

$$\frac{1}{n}\sum_{k=1}^{n}\frac{1}{k} \approx \frac{\ln n}{n}. \tag{8}$$

Indeed, if the range for a and b is $[N_1, N_2]$, and Bob's integer b happens to be equal to N_1, then, after having found out that $a \leq b$, Bob knows that Alice's integer is $a = N_1$. Then, if $b = N_1 + 1$, the information $a \leq b$ tells Bob that either $a = N_1$ or $a = N_1 + 1$, so he can guess a correctly with probability 1/2. Thus, in the "ideal" situation where an oracle just tells Bob that, say, $a \leq b$, the total probability for Bob to guess a correctly is (8).

As another point of comparison, we mention a very simple solution of the millionaires' problem from [3]:

(1) Alice begins by breaking the set of n integers from the interval $[1, n]$ into approximately $\sqrt{n}$ subintervals with approximately $\sqrt{n}$ integers in each, in such a way that her integer a is an endpoint of one of the subintervals.

(2) Alice then sends the endpoints of all the subintervals to Bob. (Alternatively, she can send just a compact description of the endpoints.)

(3) Bob tells Alice in which subinterval his integer b is. By the above property of Alice's subintervals, all elements of the subinterval pointed at by Bob are either less than (or equal to) a or greater than a, so Alice now has a solution of the inequality $a \leq b$?.

It is obvious that the probability for Bob to guess Alice's integer a correctly, as well as the probability for Alice to guess Bob's integer b correctly, is approximately $\frac{1}{\sqrt{n}}$.

As a side remark, we note that in this solution Alice ends up with exactly the same information about Bob's number b as a third party observer does, and this information is deterministic, so Alice does not get any advantage over a third party in case she is thinking of using this solution to send encrypted information to Bob. See [3] for details on situations where a solution of the millionaires' problem can be used to build a public-key encryption scheme.

4. SUGGESTED PARAMETERS FOR PRACTICAL USE AND EXPERIMENTAL RESULTS

We recommend selecting an interval of length $n = 8000$ and selecting $n^{\frac{4}{3}} = 160,000$ steps in the parties' random walks. If a and b are uniformly distributed on integers in an interval $[1,N]$ with $N<n$, then they are identically (although not uniformly) distributed on integers in $[1,n]$, in which case one can use the *inverse transform method* mentioned in our Introduction to reduce to the case of the uniform distribution on $[1,n]$. If $N>n$, then the parties can represent their private numbers in the form $\sum c_k n^k$ with $c_k<n$ and compare the coefficients c_k, starting with the largest k.

With $n=8000$ and $m=160,000$ steps, the probability for Alice to guess Bob's private number b is $\frac{\sqrt{2}}{n^{\frac{2}{3}}\sqrt{\pi}} \approx 0.002$ (see our Section 3.4) and, according to computer simulations, $P(a<b|A<B)\approx 0.99$.

With these parameters, simulation of a random walk takes 0.05 sec on a regular desktop computer.

5. CONCLUSIONS

Recall that n is the length of an interval from which the two parties' private integers are selected.

- We see that, when choosing n^{λ} steps of the parties' random walks, λ should be less than 2 for $P(a<b|A<B)$ to converge to 1 as $n\to\infty$. If $\lambda\geq 2$, then $P(a<b|A<B)$ does not converge to 1 as $n\to\infty$.

- In choosing a particular $\lambda<2$, there is a trade-off between the probability for Alice to correctly solve $a\leq b$? and the the probability for Alice to guess Bob's private number b. More specifically, the closer the number of steps of the parties' random walks is to n^2, the slower is the convergence of $P(a<b|A<B)$ to 1, but at the same time, the bigger the spread of the public point B around the private point b is, thus reducing the probability for Alice to guess Bob's number b.

- We choose $n^{\frac{4}{3}}$ steps as the "equilibrium" in this trade-off. Lower bounds for $P(a<b|A<B)$ in this case, as computed in our Section 3.2, can make an impression that our method is very inefficient since n has to be very large for $P(a<b|A<B)$ to become close to 1. However, the actual speed of convergence to 1 appears to be faster. For example, computer simulations suggest that already for $n=1000$, $P(a<b|A<B)$ is about 0.9 in that case.

- Our recommendation for the choice of parameters is: $n=8000$, and the number of steps in the parties' random walks is $n^{\frac{4}{3}}=160,000$. With these parameters, $P(a<b|A<B)\approx 0.99$, and the probability for Alice to guess Bob's private number b is about $\frac{\sqrt{2}}{n^{\frac{2}{3}}\sqrt{\pi}}\approx 0.002$.

- In this paper, the focus is on the arrangement where Alice and Bob do the same number of steps in their random walks. Other arrangements are possible, too; in particular, as we remark in Section 3.1, Alice can (slightly) improve the probability of coming to the correct conclusion on $a\leq b$? if she does not walk at all. This arrangement is "highly asymmetric" but it is nevertheless useful to keep in mind.

REFERENCES

[1] P. Eichelsbacher and M. Löwe, *Moderate Deviations for I.I.D. Random Variables*, ESAIM: Probability and Statistics **7** (2003), 209–218.

[2] P. Glasserman, *Monte Carlo Methods in Financial Engineering (Stochastic Modelling and Applied Probability)*, Springer, 2003.

[3] D. Grigoriev, L. Kish, V. Shpilrain, *Yao's millionaires' problem and public-key encryption without computational assumptions*, Int. J. Foundations Comp. Sci., to appear. http://eprint.iacr.org/2016/189

[4] D. Grigoriev and V. Shpilrain, *Yao's millionaires' problem and decoy-based public key encryption by classical physics*, Int. J. Foundations Comp. Sci. **25** (2014), 409–417.

[5] A. C. Yao, *Protocols for secure computations* (Extended Abstract), 23rd annual symposium on foundations of computer science (Chicago, Ill., 1982), 160–164, IEEE, New York, 1982.

DEPARTMENT OF MATHEMATICS, NEW YORK CITY COLLEGE OF TECHNOLOGY, CUNY
E-mail address: mbessonov@citytech.cuny.edu

CNRS, MATHÉMATIQUES, UNIVERSITÉ DE LILLE, 59655, VILLENEUVE D'ASCQ, FRANCE
E-mail address: dmitry.grigoryev@math.univ-lille1.fr

DEPARTMENT OF MATHEMATICS, THE CITY COLLEGE OF NEW YORK, NEW YORK, NY 10031
E-mail address: shpil@groups.sci.ccny.cuny.edu